Journal of Number Theory **72**, 183–235 (1998)
Article No. NT982276

Dynamique des fractions continues à contraintes périodiques

Brigitte Vallée

Département d'Informatique GREYC-URA 1526, Université de Caen, 14302 Caen Cedex, France
E-mail: Brigitte.Vallee@info.unicaen.fr

Communicated by V. T. Sós

Received March 26, 1997; revised January 20, 1998

dimension de Hausdorff de l'ensemble des réels contraints, la densité des rationnels et des irrationnels quadratiques contraints. Puis, on analyse le comportement moyen de l'algorithme d'Euclide sur ces rationnels contraints ainsi que la longueur moyenne de la période des irrationnels quadratiques contraints et la valeur moyenne de la constante de Lévy des irrationnels quadratiques contraints. En associant un opérateur qui engendre cet ensemble de contraintes, on relie tous les objets étudiés aux propriétés spectrales dominantes de cet opérateur. En ce qui concerne la dimension de Hausdorff et la densité des rationnels contraints, les résultats présentés étendent à des contraintes quelconques des résultats précédents obtenus uniquement dans le cas de contraintes élémentaires. Les autres études—densité des irrationnels quadratiques contraints; comportement moyen de la hauteur et de la période d'un développement en fraction continue contraint; valeur moyenne de la constante de Lévy des irrationnels quadratiques contraints—semblent nouvelles même dans le cas d'une contrainte élémentaire.

1. INTRODUCTION

L'ensemble triadique de Cantor $\mathscr{C}$ est le premier exemple d'un sous-ensemble de réels de $[0, 1]$ obéissant à des contraintes liées à un développement en base b: dans ce cas, la base choisie est $b = 3$, et la contrainte consiste à interdire le chiffre 1. C'est un sous-ensemble de mesure nulle, qui se présente sous une forme "fractale". La dimension de Hausdorff de tels ensembles $\mathscr{F}$ est le nombre réel $s := \mathscr{H}(\mathscr{F})$ pour lequel la mesure s-dimensionnelle de $\mathscr{F}$ change de nature: de nulle, elle devient infinie. Ici, pour l'ensemble triadique de Cantor $\mathscr{C}$, on a $\mathscr{H}(\mathscr{C}) = \log_3(2)$. De manière plus générale, pour un développement en base b, où l'on ne permet à chaque

0022-314X/98 $25.00

niveau que k des b chiffres possibles, la dimension de Hausdorff de l'ensemble associé est $\log_b(k)$.

Un autre système de numération très utilisé est lié au développement en fraction continue. On peut considérer des ensembles de Cantor dont le développement en fraction continue obéit à des contraintes. L'étude est plus délicate, car le i-ème chiffre du développement n'est pas indépendant de ceux qui le précèdent et le nombre de chiffres possibles est infini. On trouve une bibliographie très complète sur le sujet dans l'article de Shallitt [Sh]. C'est Good qui a le premier étudié de tels ensembles et déterminé leur mesure de Hausdorff. Par la suite, on s'est toujours intéressé à une forme spéciale de contraintes qu'on qualifiera ici d'*élémentaires*: À une partie M de l'ensemble $N_\star$ des entiers strictement positifs, on associe l'ensemble des réels de $[0, 1]$ qui ont *tous* les chiffres de leur développement en fraction continue dans M; autrement dit, on a toujours exigé les mêmes contraintes sur chacun des chiffres du développement. Le premier ensemble de cette forme, lié à l'ensemble $M = \{1, 2\}$, a été très largement étudié par Good [Go] et Bumby [Bu]. Par la suite, Cusick [Cu] et Hensley [He1–He4] ont étudié d'autres ensembles de réels associés à des contraintes élémentaires définies par des ensembles M qui étaient toujours finis. Récemment, il y a eu une percée dans le domaine et Mauldin et Urbański ont classifié les contraintes élémentaires infinies.

Dans ce travail, nous cherchons à étudier des réels associés à des contraintes plus générales, qui peuvent varier selon le rang du chiffre considéré, mais qui reviennent périodiquement: par exemple, les chiffres de rang impair devront être égaux à 1, mais les chiffres de rang pair devront être multiples de 3. Des exemples de tels ensembles arrivent naturellement dans certains problèmes liés à la cryptographie. Ce travail a d'ailleurs été motivé au départ par une question de Tillich relative à des propriétés de fonction de hachage définies sur $SL_2(\mathbf{Z})$ [TZ1, TZ2, Ze]. De tels ensembles sont intéressants également parce qu'ils contiennent de manière naturelle des irrationnels quadratiques, et peuvent contenir aussi certains nombres transcendants explicites comme le nombre e.

Soit $\mathcal{S}$ l'ensemble des suites d'entiers strictement positifs. On considère le sous-ensemble $\mathcal{N} := M_1 \times M_2 \times \cdots \times M_k \times \cdots$ de $\mathcal{S}$ qui représente l'ensemble des développements en fraction continue admis. Cet ensemble $\mathcal{N}$ sera appelé ici l'ensemble de contraintes. On parle de contraintes périodiques quand l'ensemble $\mathcal{N}$ lui-même est périodique: il existe un entier $l \geqslant 1$ pour lequel, pour tout couple d'indices (i, j) vérifiant $i \equiv j \bmod l$, les ensembles M_i et M_j sont égaux. Un tel ensemble est complètement défini par la partie $\mathcal{M} := M_1 \times M_2 \times \cdots \times M_l$, qu'on appellera la période; l'entier l sera appelé la longueur de la période. Si $l = 1$, on obtient des contraintes élémentaires. Dans toute la suite, on exigera que l'ensemble $\mathcal{M}$ soit de cardinal $|\mathcal{M}| > 1$, mais, par contre, ce cardinal pourra être fini ou infini.

L'ensemble $\mathcal{N}$ est alors isomorphe à $\mathcal{M}^{\mathbb{N}}$, on dira qu'il est engendré par $\mathcal{M}$, et on le notera $\langle \mathcal{M} \rangle$. On désignera par $\mathcal{M}(k)$ l'ensemble des préfixes de $\langle \mathcal{M} \rangle$ de longueur k

$$\mathcal{M}(k) := M_1 := M_1 \times M_2 \times \cdots \times M_k.$$

Notons que la périodicité s'exprime par la relation $\mathcal{M}(kl) = \mathcal{M}^k$. Ainsi, l'ensemble des préfixes dont la longueur est multiple de la longueur l de la période jouera un rôle particulier, puisqu'il constitue l'ensemble des mots sur l'alphabet $\mathcal{M}$, et sera donc désigné par $\mathcal{M}^*$,

$$\mathcal{M}^* := \bigcup_{k \geqslant 1} \mathcal{M}^k = \bigcup_{k \geqslant 1} \mathcal{M}(kl).$$

Voici quelques exemples

(i) $l = 1$, $\mathcal{M} := \{1, 2\}$

(ii) $l = 1$, $\mathcal{M} := \{2, 4, 6, ..., 2n, ...\}$

(iii) $l = 3$, $\mathcal{M} := \{1\} \times \{1\} \times \{1, 2, 3, ..., n, ...\}$

(iv) $l = 2$, $\mathcal{M} := \{1, 2, 3, ..., n, ...\} \times \{1\}$

(v) $l = 5$, $\mathcal{M} := M_1 \times M_2 \times M_3 \times M_4 \times M_5$ où $M_i := \{ j \mid j \equiv i \bmod 5\}$

Ce sont de tels ensembles, de forme générale $\langle \mathcal{M} \rangle$, qui vont représenter l'ensemble des contraintes exercées sur les chiffres des développements en fraction continue des nombres considérés: On étudiera ainsi trois ensembles de nombres contraints par $\mathcal{M}$ (on dira encore $\mathcal{M}$-contraints), l'ensemble $\mathcal{R}(\mathcal{M})$ des réels de $[0, 1]$ dont le développement en fraction continue $(m_1, m_2, ..., m_k, ...)$ appartient à $\langle \mathcal{M} \rangle$, l'ensemble $\mathcal{Q}(\mathcal{M})$ des rationnels de $[0, 1]$ dont le développement en fraction continue $(m_1, m_2, ..., m_k)$ constitue un préfixe de $\langle \mathcal{M} \rangle$ et enfin l'ensemble $\mathcal{I}(\mathcal{M})$ des irrationnels quadratiques dont une période du développement en fraction continue est un élément de $\mathcal{M}^*$.

L'ensemble $\mathcal{R}(\mathcal{M})$ est ainsi associé à un système dynamique $\mathcal{M}^{\mathbb{N}}$ sur lequel l'opération de décalage est la puissance l-ième $V := U^l$ de l'opération de décalage U des fractions continues,

$$U(x) = \frac{1}{x} - \left[\frac{1}{x} \right].$$

Les travaux de Mayer [Ma1–Ma5], de Bumby [Bu], de Hensley [He1–He4], de Pollicott [Po], de Faivre [Fa], de Mauldin et Urbański [MU], et certains travaux de l'auteur [DFV, FV, Va1, Va2] ont clairement démontré le rôle important que l'analyse fonctionnelle pouvait jouer dans nombre de problèmes liés à l'étude des fractions continues. Ce travail en est un exemple supplémentaire, où des opérateurs de Ruelle–Mayer contraints vont jouer un rôle analogue aux opérateurs de Ruelle–Mayer classiques. On considère d'abord les opérateurs qui engendrent les développements en fraction continue valides, associés à une contrainte élémentaire M de $\{1, 2, ..., n, ...\}$

$$\mathcal{G}_{M,s}[f](z) := \sum_{m \in M} \left(\frac{1}{m+z}\right)^s f\left(\frac{1}{m+z}\right);$$

ils peuvent être appelés des opérateurs de Ruelle–Mayer contraints, puisque, dans le cas où il n'y a pas de contraintes, i.e., $M = N_\star = \{1, 2, ..., n...\}$, on retrouve l'opérateur de Ruelle–Mayer usuel,

$$\mathcal{G}_s[f](z) := \sum_{m \geqslant 1} \left(\frac{1}{m+z}\right)^s f\left(\frac{1}{m+z}\right).$$

Lorsqu'on a affaire à une contrainte périodique engendrée par la partie $\mathcal{M}$, l'opérateur qui engendre la période "miroir"

$$\mathcal{G}_{\mathcal{M},s} := \mathcal{G}_{M_l,s} \circ \mathcal{G}_{M_{l-1},s} \circ \cdots \circ \mathcal{G}_{M_1,s}$$

va jouer un rôle essentiel dans l'étude, via ses propriétés spectrales.

La méthodologie employée ici est très proche conceptuellement de cette de la combinatoire analytique [Fl, FS], au moins dans les deux études de nature discrète de ce travail (rationnels contraints et irrationnels quadratiques contraints). Les rationnels $\mathcal{M}$-contraints sont reliés à l'ensemble des mots finis sur l'alphabet $\mathcal{M}$ tandis que les irrationnels quadratiques font intervenir les cycles construits sur l'alphabet $\mathcal{M}$. On travaille avec l'outil des séries génératrices, qui, ici, ne sont pas des séries entières comme dans le cas classique de la combinatoire analytique, mais des séries de Dirichlet en s respectivement de la forme

$$(I - \mathcal{G}_{\mathcal{M},s})^{-1} [1](0) \qquad \text{et} \qquad \log \deg(I - \mathcal{G}_{\mathcal{M},s}).$$

Les propriétés asymptotiques des coefficients de ces séries s'étudieront grâce à des théorèmes taubériens et feront ainsi intervenir les singularités de l'application $s \to (I - \mathcal{G}_{\mathcal{M},s})^{-1}$ et donc les propriétés spectrales de l'opérateur $\mathcal{G}_{\mathcal{M},s}$. Or, l'opérateur de Ruelle–Mayer contraint a essentiellement les mêmes propriétés que l'opérateur de Ruelle–Mayer usuel; il est compact, il est même nucléaire (voir [Gr1, Gr2]) et, lorsque le paramètre s est réel, il satisfait à une propriété de positivité forte du type Perron–Frobenius (voir [Kr]) et a donc des propriétés spectrales dominantes: il a une valeur propre dominante simple strictement positive notée $\lambda(\mathcal{M}, s)$. Dans un cadre très général de contraintes "naturelles", qu'on appelle ici "ouvertes", on peut affirmer que le domaine réel de convergence de l'application $s \to \mathcal{M}, s)$ est un ouvert de la droite réelle, et on en déduit l'existence d'un unique réel $s_{\mathcal{M}}$ pour lequel

$$\lambda(\mathcal{M}, s_{\mathcal{M}}) = 1.$$

Ce nombre réel $s_{\mathcal{M}}$, qui appartient toujours à l'intervalle $[0, 2]$, est alors une singularité dominante de la fonction $s \to (I - \mathcal{G}_{\mathcal{M}, s})^{-1} [1](0)$ et joue un rôle fondamental dans l'étude qui suit, puisqu'il intervient dans les trois premiers résultats de ce travail. On montre en effet

(i) La dimension de Hausdorff de l'ensemble $\mathcal{R}(\mathcal{M})$ des réels $\mathcal{M}$-contraints est égale à $(1/2)\, s_{\mathcal{M}}$.

(ii) L'exposant de la densité de l'ensemble $\mathcal{Q}(\mathcal{M})$ des rationnels $\mathcal{M}$-contraints est égal à $s_{\mathcal{M}}$. Plus précisément, si $\mathcal{Q}_N(\mathcal{M})$ désigne le sous-ensemble de $\mathcal{Q}(\mathcal{M})$ formé par les rationnels p/q vérifiant $1 \leqslant p < q \leqslant N$ et $\mathrm{pgcd}(p, q) = 1$, on obtient le comportement asymptotique suivant, pour $N \to \infty$,

$$|\mathcal{Q}_N(\mathcal{M})| \sim c_{\mathcal{M}} N^{s_{\mathcal{M}}},$$

pour une constante $c_{\mathcal{M}}$ ne dépendant que de la contrainte $\mathcal{M}$.

(iii) L'exposant de la densité de l'ensemble $\mathcal{I}(\mathcal{M})$ des irrationnels quadratiques $\mathcal{M}$-contraints est égal à $s_{\mathcal{M}}$. Plus précisément, si $\mathcal{I}_N(\mathcal{M})$ désigne le sous-ensemble de $\mathcal{I}(\mathcal{M})$ formé par les irrationnels quadratiques x pour lesquels l'équation de Pell a une solution fondamentale $\varepsilon(x)$ inférieure ou égale à N, on obtient le comportement asymptotique suivant, pour $N \to \infty$,

$$|\mathcal{I}_N(\mathcal{M})| \sim d_{\mathcal{M}} N^{s_{\mathcal{M}}},$$

pour une constante $d_{\mathcal{M}}$ ne dépendant que de la contrainte $\mathcal{M}$.

Le premier résultat étend les résultats de Mauldin et Urbański [MU1, MU2] à des contraintes non élémentaires. Le second résultat, précédemment obtenu par Cusick [Cu] et Hensley [He1] dans le cas particulier d'une contrainte élémentaire et finie, est ici acquis par des méthodes sensiblement différentes et nettement plus simples. Le troisième résultat n'a été précédemment démontré [Po, Fa] que dans le cas où il n'y a pas de contraintes—i.e., $\mathcal{M} = \{1, 2, ..., n, ...\}$ et $s_{\mathcal{M}} = 2$.

Les trois résultats suivants décrivent le comportent moyen de la longueur du développement en fraction continue d'un rationnel $\mathcal{M}$-contraint, et le comportement moyen de deux grandeurs associées à un irrationnel quadratique $\mathcal{M}$-contraint: la longueur de la période du développement en fraction continue de cet irrationnel quadratique et aussi la constante de Lévy de cet irrationnel quadratique. Ces résultats font intervenir une grandeur qui joue un rôle analogue à celui que la constante $\pi^2/(12 \log 2)$ joue dans les problèmes non contraints. Cette constante n'est autre que la dérivée de la fonction $s \to -\lambda(N_\star, s)$ au point $s_\star = 2$ dans le cas d'un problème non-contraint et elle est aussi égale, dans un sens précis, à la moyenne des constantes de Lévy de tous les irrationnels quadratiques. C'est pourquoi on l'appelle aussi la constante de Lévy. Ici, c'est une autre constante, égale par définition à la dérivée de la fonction $s \to -(1/l)\, \lambda(\mathcal{M}, s)$ au point $s_{\mathcal{M}}$ qui va intervenir. On va montrer dans le résultat (vi) qu'elle est aussi égale, dans un sens précis, à la moyenne des constantes de Lévy de tous les irrationnels quadratiques $\mathcal{M}$-contraints. C'est pourquoi on l'appelle la constante de Lévy associée à la contrainte $\mathcal{M}$ et on la désigne par $\mathcal{L}(\mathcal{M})$.

(iv) La hauteur moyenne du développement en fraction continue d'un rationnel de $\mathcal{Q}_N(\mathcal{M})$ vérifie, pour $N \to \infty$,

$$E[E_N(\mathcal{M})] \sim \frac{1}{\mathcal{L}(\mathcal{M})} \log N,$$

où $\mathcal{L}(\mathcal{M})$ représente la constante de Lévy de l'ensemble $\mathcal{M}$.

(v) La longueur moyenne de la période du développement en fraction continue d'un irrationnel quadratique de $\mathcal{I}_N(\mathcal{M})$ vérifie, pour $N \to \infty$,

$$E[Y_N(cM)] \sim \frac{1}{\mathcal{L}(\mathcal{M})} \log N,$$

où $\mathcal{L}(\mathcal{M})$ représente la constante de Lévy de l'ensemble $\mathcal{M}$.

(vi) La valeur moyenne de la constante de Lévy d'un irrationnel quadratiqua de $\mathcal{I}_N(\mathcal{M})$ vérifie, pour $N \to \infty$,

$$E[Z_N(\mathcal{M})] \sim \mathcal{L}(\mathcal{M}),$$

où $\mathcal{L}(\mathcal{M})$ représente la constante de Lévy de l'ensemble $\mathcal{M}$.

Les résultats (iv), (v) et (vi) généralisent ainsi à une contrainte périodique quelconque des résultats précédents obtenus seulement dans le cas particulier du problème non contraint, par Heilbronn [Hei] et Dixon [Di] pour les rationnels, par Pollicott [Po] et Faivre [Fa] pour les irrationnels quadratiques. Il est à noter le parallèle frappant entre les résultats obtenus et les méthodes employées dans le cas des rationnels $\mathcal{M}$-contraints et des irrationnels quadratiques $\mathcal{M}$-contraints.

Plan du travail. On commence par définir les principaux objets étudiés, dans le cadre classique, puis dans le cadre contraint (Section 1). Puis, on décrit, dans la Section 2, les principales propriétés de l'opérateur de Ruelle–Mayer contraint, qui généralisent celles de l'opérateur de Ruelle–Mayer classique. Chacune des trois sections suivantes 3, 4, 5 est consacrée à l'étude d'un ensemble contraint: celui des réels dans la Section 3, où l'on démontre le résultat (i), puis celui des rationnels dans la Section 4, où les résultats (ii) et (iv) sont établis, enfin celui des irrationnels quadratiques dans la Section 5, où sont obtenus les résultats (iii), (v) et (vi). Le travail se termine par une section consacrée à des exemples d'utilisation et à des calculs explicites.

1. FRACTIONS CONTINUES ET OPÉRATEURS DE RUELLE–MAYER CONTRAINTS

Ici, on décrit d'abord les principaux objets liés au développement en fraction continue: homographies, continuants, intervalles fondamentaux, opérateur de Ruelle–Mayer. Ensuite, on introduit les objets similaires liés à un ensemble de contraintes.

1.1. *Opérateur des fractions continues et continuants*

L'opérateur de décalage U des fractions continues est défini pour un réel x de $\mathscr{I} = [0, 1[$ par

$$U(x) = \frac{1}{x} - \left[\frac{1}{x}\right] \qquad \text{pour} \quad x \neq 0, \quad U(0) = 0 \tag{1}$$

où $[x]$ désigne la partie entière du réel x. Cet opérateur est à la base de l'algorithme des fractions continues:

Entrée. Un réel x de $\mathscr{I}$. *Tant que* $x \neq 0$ *faire* $x := U(x)$.

À un réel x, on associe la suite $x_0 = x, x_1, x_2, ..., x_k, ...$ des itérés de x. Si le k-ème itéré existe, l'algorithme des fractions continues construit sur l'entrée x_0 un développement en fraction continue

$$x_0 = \cfrac{1}{m_1 + \cfrac{1}{m_2 + \cfrac{1}{\ddots\, \cfrac{}{m_k + x_k}}}},$$

où les entiers m_i sont supérieurs ou égaux à 1. La relation $x_0 = h(x_k)$ définit une homographie de *hauteur* k, associée à un k-uplet $m = (m_1, m_2, ..., m_k)$ d'entiers $m_i \geqslant 1$,

$$h_m(z) = h_{m_1, m_2, ..., m_k}(z) = \cfrac{1}{m_1 + \cfrac{1}{m_2 + \cfrac{1}{\ddots \, \cfrac{}{m_k + z}}}}.$$

Toutes ces homographies de hauteur k constituent ainsi toutes les branches inverses possibles du k-ème itéré de U défini en (1). Une telle homographie h s'exprime alors à l'aide des continuants

$$h_m(z) = \frac{P_k + zP_{k-1}}{Q_k + zQ_{k-1}},$$

où

$$\begin{aligned} Q_k &= Q_k(m_1, ..., m_k), \qquad & Q_{k-1} &= Q_{k-1}(m_1, ..., m_{k-1}), \\ P_k &= Q_{k-1}(m_2, ..., m_k), \qquad & P_{k-1} &= Q_{k-2}(m_2, ..., m_{k-1}). \end{aligned} \tag{2}$$

Les polynômes continuants sont définis par récurrence

$$Q_k(m_1, m_2, ..., m_k) = m_k Q_{k-1}(m_1, ..., m_{k-1}) + Q_{k-2}(m_1, ..., m_{k-2}), \tag{3}$$

avec $Q_0 = 1$, $Q_1(m_1) = m_1$. Il est bien connu que le polynôme continuant $Q_k(m)$ est aussi la somme de tous les monômes obtenus en barrant deux variables consécutives $m_i m_{i+1}$ dans le produit $m_1 m_2 \cdots m_k$. Les continuants vérifient une propriété de symétrie

$$Q_k(m_1, ..., m_k) = Q_k(m_k, ..., m_1), \tag{4}$$

et l'identité du déterminant

$$Q_k P_{k-1} - Q_{k-1} P_k = (-1)^k. \tag{5}$$

Pour une homographie h de hauteur k associée à un k-uplet m, le transformé par h du segment $\mathscr{I}$ est appelé intervalle fondamental de rang k: il est formé par tous les nombres réels dont le développement en fraction continue commence par $(m_1, m_2, ..., m_k)$. L'intervalle $\mathscr{I}$ lui-même est, à un ensemble de rationnels près, réunion disjointe de tous les intervalles fondamentaux de rang k

$$\mathscr{I} \approx \bigcup_{|h| = k} h(\mathscr{I}) \qquad \text{pour chaque} \quad k \geqslant 0.$$

L'intervalle fondamental $h(\mathscr{I})$ s'exprime en fonction des continuants:

$$h(\mathscr{I}) = \left[\frac{P_k}{Q_k}, \frac{P_{k-1} + P_k}{Q_{k-1} + Q_k} \right] \tag{6}$$

(les bornes de l'intervalle étant ordonnées ou non suivant la parité de k) et est de longueur égale à

$$u_h := |h(\mathscr{I})| = \frac{1}{Q_k(Q_k + Q_{k-1})}. \tag{7}$$

1.2. *Irrationnels quadratiques*

Les éléments x de $\mathscr{I}$ pour lesquels la suite $U^i(x)$ est périodique (sans prépériode) sont des irrationnels quadratiques qu'on appelle dans la suite réduits. Le développement en fraction continue d'un irrationnel quadratique réduit est alors clairement périodique; on désigne par p la longueur de sa période et par $\pi := (m_1, m_2, ..., m_p)$ sa période. Une grandeur fondamentale attachée à un tel nombre est le produit

$$\alpha(x) := \prod_{i=0}^{p(x)-1} U^i(x) \tag{8}$$

formé des éléments de la suite $U^i(x)$ qui engendrent la période π. À partir de cette grandeur α, on définit la constante de Lévy $\beta(x)$ du nombre x

$$\beta(x) := \frac{-1}{p(x)} \log \alpha(x) = \frac{-1}{p(x)} \sum_{i=0}^{p(x)-1} \log U^i(x). \tag{9}$$

Cette constante joue un rôle important, grâce à la relation

$$\lim_{k \to \infty} \frac{1}{k} \log Q_k(x) = \beta(x), \tag{10}$$

où $Q_k(x)$ représente le continuant d'ordre k associé à x, i.e., le dénominateur de la k-ième réduite de x. À une légère correction près due à la parité de la période, la grandeur $\alpha(x)$ est également reliée à la solution fondamentale $\varepsilon(x) := 1/2(X + \sqrt{\Delta}\, Y)$ de l'équation de Pell $X^2 - \Delta Y^2 = 4$, où Δ est le discriminant $\Delta = B^2 - 4AC$ associé à l'équation minimale de x de la forme $Ax^2 + Bx + C = 0$ avec A, B, C premiers entre eux. Posant $r = 1$ si p est pair, et $r = 2$ si p est impair, on a

$$\varepsilon(x) = \alpha(x)^{-r(x)}. \tag{11}$$

Le nombre $\varepsilon(x)$ joue, pour les irrationnels quadratiques réduits, un rôle analogue à celui du dénominateur pour les rationnels: il représente une notion naturelle de taille; en particulier la grandeur $2\log \varepsilon(x)$ est la longueur de la géodésique tracée sur la surface modulaire et reliant x à son conjugué.

Il est naturel d'étendre les définitions de α, ε et r à des mots $m = (m_1, m_2, ..., m_k)$. À un tel k-uplet, on associe l'irrationnel quadratique $m^\star$ dont le DFC a pour période $(m_1, m_2, ..., m_k)$. Il faut noter que $(m_1, m_2, ..., m_k)$ est une période du DFC de $m^\star$ mais non pas nécessairement sa période, i.e., la plus petite. On pose alors

$$\alpha(m) := \prod_{i=0}^{k-1} U^i(m^\star), \qquad \beta(m) := \beta(m^\star), \qquad \varepsilon(m) = \alpha(m)^{-r(m)}, \tag{12}$$

avec $r(m) = 1$ si k est pair et $r(m) = 2$ si k est impair. Notons que par construction, on a $\alpha(m^h) = \alpha(m)^h$. Cette égalité permet de montrer que l'application α, définie ainsi sur les mots, hérite de deux propriétés importantes qu'elle a sur les irrationnels quadratiques: elle est invariante par permutation circulaire et par effet miroir.

Par ailleurs, l'égalité

$$\alpha(m) = \frac{1}{xQ_{k-1} + Q_k} = |h'_m(m^\star)|^{1/2} \tag{13}$$

permet d'exprimer le nombre $\alpha(m)$ en fonction de l'irrationnel quadratique $m^\star$, des continuants relatifs au mot m et de l'homographie h_m associée à ce mot.

1.3. *Fractions continues contraintes*

Lorsque le problème est associé à un ensemble de contraintes périodique engendré par $\mathscr{M}$, on considère l'ensemble $\langle \mathscr{M} \rangle$ des développements en fraction continue valides, et, pour tout $k \geqslant 1$, l'ensemble des développements en fraction continue valides de longueur k, qui sont associés à l'ensemble $\mathscr{M}(k)$ des préfixes de longueur k de $\langle \mathscr{M} \rangle$. L'ensemble des homographies valides de hauteur k noté $\mathscr{H}_k(\mathscr{M})$ est alors constitué par les h_m lorsque m décrit $\mathscr{M}(k)$, et les continuants valides sont les $Q_k(m)$ définis en (3) lorsque m décrit $\mathscr{M}(k)$. Les intervalles fondamentaux valides de hauteur k sont les transformés de $\mathscr{I}$ par les homographies de $\mathscr{H}_k(\mathscr{M})$. L'ensemble

$$\mathscr{R}^{\langle k \rangle}(\mathscr{M}) := \bigcup_{h \in \mathscr{H}_k(\mathscr{M})} h(\mathscr{I})$$

est formé de tous les réels qui ont un développement en fraction continue valide jusqu'à l'ordre k et l'ensemble $\mathscr{R}(\mathscr{M})$ que l'on veut étudier est donc égal par définition à

$$\mathscr{R}(\mathscr{M}) = \bigcap_{k \geqslant 1} \mathscr{R}^{\langle k \rangle}(\mathscr{M}).$$

De même, l'ensemble

$$\mathcal{Q}^{\langle k \rangle}(\mathcal{M}) := \{h(0) \mid h \in \mathcal{H}_k(\mathcal{M})\} = \left\{ \frac{P_k(m)}{Q_k(m)} \,\middle|\, m \in \mathcal{M}(k) \right\}$$

est formé de tous les rationnels de hauteur k qui ont un développement en fraction continue valide, et l'ensemble $\mathcal{Q}(\mathcal{M})$ que l'on veut étudier est donc égal par définition à

$$\mathcal{Q}(\mathcal{M}) = \bigcup_{k \geqslant 1} \mathcal{Q}^{\langle k \rangle}(\mathcal{M}).$$

De manière analogue, on va considérer l'ensemble des nombres irrationnels quadratiques $\mathcal{M}$-contraints; ce sont les irrationnels quadratiques réduits contenus dans $\mathcal{R}(\mathcal{M})$, et donc ceux dont la période du DFC est compatible avec $\mathcal{M}$. On dira qu'un nombre irrationnel quadratique x de période π est élément de $\mathcal{I}(\mathcal{M})$ s'il existe une puissance π^k de sa période (au sens des mots) qui est élément de $\mathcal{M}^*$.

1.4. *Opérateurs de Ruelle–Mayer usuels*

Les opérateurs de Ruelle–Mayer usuels $\mathcal{G}_s$ servent à "inverser" l'opérateur de décalage U des fractions continues. Ils sont définis pour un complexe s vérifiant $\Re(s) > 1$ par la relation

$$\mathcal{G}_s[f](z) = \sum_{m \geqslant 1} \frac{1}{(m+z)^s} f\left(\frac{1}{m+z}\right). \tag{14}$$

Les itérés d'ordre k de ces opérateurs engendrent alors les continuants d'ordre k dans le sens suivant

$$\mathcal{G}_s^k[f](z) = \sum_{m_1 \cdots m_k} \frac{1}{(Q_{k-1}z + Q_k)^s} f\left(\frac{P_{k-1}z + P_k}{(Q_{k-1}z + Q_k)}\right),$$

et, en particulier

$$\mathcal{G}_s^k[f](0) = \sum_{m_1 \cdots m_k} \frac{1}{Q_k^s} f\left(\frac{P_k}{Q_k}\right) = \sum_{m_1 \cdots m_k} \frac{1}{Q_k^s} f\left(\frac{Q_{k-1}}{Q_k}\right), \tag{15}$$

la seconde égalité étant due aux propriétés de symétrie (4). Une homographie h de hauteur k a une dérivée qui, sur le segment $\mathcal{I}$, et grâce à (5), a le signe de $(-1)^k$. Cela justifie l'introduction de la fonction $\tilde{h}$ qui est l'unique fonction holomorphe qui coïncide avec

$$|h'(y)|^{1/2} = [(-1)^k h'(y)]^{1/2} = \frac{1}{(Q_{k-1}y + Q_k)} \tag{16}$$

sur le segment $\mathscr{I}$. On obtient ainsi une forme alternative pour $\mathscr{G}_s$ et ses itérés,

$$\mathscr{G}_s^k[f](z) = \sum_{|h|=k} \tilde{h}(z)^s \, f \circ h(z), \tag{17}$$

où la somme est étendue à toutes les homographies h de hauteur k.

1.5. *Opérateurs de Ruelle–Mayer contraints*

À un ensemble périodique de contraintes engendré par $\mathscr{M}$, on associe d'abord les opérateurs qui engendrent les développements en fraction continue valides associés à chaque composante M_i d'indice i $(1 \leqslant i \leqslant l)$ de la période $\mathscr{M}$

$$\mathscr{G}_{M_i, s}[f](z) := \sum_{m \in M_i} \left(\frac{1}{m+z}\right)^s f\left(\frac{1}{m+z}\right). \tag{18}$$

Puis, à l'ensemble $\mathscr{M}(k)$ des préfixes de longueur k de $\langle \mathscr{M} \rangle$, on associe l'opérateur

$$\mathscr{G}_{\mathscr{M}(k), s} := \mathscr{G}_{M_k, s} \circ \mathscr{G}_{M_{k-1}, s} \circ \cdots \circ \mathscr{G}_{M_1, s}. \tag{19}$$

Notons qu'on décide de considérer les M_i dans l'ordre-miroir, et, ce, pour des raisons qu'on va expliciter plus loin. Via la définition (16), un tel opérateur est défini alternativement de manière analogue à (17) par

$$\mathscr{G}_{\mathscr{M}(k), s}[f](z) = \sum_{h \in \hat{\mathscr{H}}_k(\mathscr{M})} \tilde{h}(z)^s \, f \circ h(z) \tag{20}$$

(où $\hat{\mathscr{H}}_k(\mathscr{M})$ représente l'ensemble des homographies associées aux préfixes miroir de $\mathscr{M}(k)$), et vérifie en $z=0$

$$\mathscr{G}_{\mathscr{M}(k), s}[f](0) = \sum_{\hat{m} \mid m \in \mathscr{M}(k)} \frac{1}{Q_k^s} f\left(\frac{P_k}{Q_k}\right) = \sum_{m \in \mathscr{M}(k)} \frac{1}{Q_k^s} f\left(\frac{Q_{k-1}}{Q_k}\right), \tag{21}$$

grâce à la propriété de symétrie des continuants vue en (4). Comme l'étude menée ici fait jouer un rôle important aux intervalles fondamentaux dont la longueur, exprimée en (7), fait intervenir les Q_k, ce sont des expressions de la forme

$$\sum_{m \in \mathscr{M}(k)} \frac{1}{Q_k^s} f\left(\frac{Q_{k-1}}{Q_k}\right),$$

qui interviennent naturellement et qui justifient l'introduction des opérateurs à effet miroir. Ces opérateurs associés aux préfixes de $\mathscr{M}(k)$ s'expriment en fonction de vraies puissances de l'opérateur qui génère la période "miroir"

$$\mathscr{G}_{\mathscr{M},s} := \mathscr{G}_{M_l,s} \circ \mathscr{G}_{M_{l-1},s} \circ \cdots \circ \mathscr{G}_{M_1,s}. \tag{22}$$

Soit en effet un indice k qui s'écrit sous la forme $k = nl + i$ avec $i \in \{1 \cdots l\}$. Alors,

$$\mathscr{G}_{\mathscr{M}(k),s} = \mathscr{G}_{\mathscr{M}(i),s} \circ \mathscr{G}^n_{\mathscr{M},s} \tag{23}$$

où maintenant $\mathscr{G}^n_{\mathscr{M},s}$ représente la puissance n-ième de l'opérateur $\mathscr{G}_{\mathscr{M},s}$.

Remarquons que, dans tous les problèmes où le seul continuant Q_k intervient au niveau k, il est équivalent de travailler avec l'opérateur de Ruelle–Mayer associé à la contrainte sans effet miroir

$$\mathscr{G}_{M_1,s} \circ \mathscr{G}_{M_2,s} \circ \cdots \circ \mathscr{G}_{M_l,s}.$$

Nous montrerons de fait, en 2.1, que ces deux opérateurs sont très semblables, puisqu'ils possèdent le même spectre.

L'opérateur de Ruelle–Mayer qui engendre la période-miroir $\mathscr{M}$ va jouer un rôle fondamental dans la suite: il intervient naturellement dans les problèmes liés à la dimension de Hausdorff $\mathscr{R}(\mathscr{M})$ (Section 3) et est adapté à l'étude des rationnels $\mathscr{M}$-contraints (Section 4) comme à l'étude des irrationnels quadratiques (Section 5). On va étudier maintenant ces opérateurs, et montrer qu'ils ont des propriétés spectrales très semblables à l'opérateur de Ruelle–Mayer usuel.

2. LES PROPRIÉTÉS SPECTRALES DES OPÉRATEURS DE RUELLE–MAYER CONTRAINS $\mathscr{G}_{\mathscr{M},s}$

On montre ici que la quasi-totalité des propriétés de l'opérateur de Ruelle–Mayer classique se généralise aux opérateurs contraints: compacité, nucléarité, réalité du spectre. On généralise aussi les formules de la trace, ce qui permet d'obtenir l'invariance du spectre quand la période $\mathscr{M}$ est modifiée par un élément du groupe diédral. On montre aussi que l'opérateur de Ruelle–Mayer contraint jouit de propriétés fortes de positivité, pour une valeur réelle du paramètre, qui restent vraies par perturbation sur un voisinage de l'axe réel. On terme par des propriétés du rayon spectral qui s'avèreront essentielles dans l'application des théorèmes taubériens.

Dans toute la suite, $\mathscr{J}$ et $\mathscr{V}$ désignent respectivement le segment et le disque ouvert de centre 1 et de rayon 5/4. On définit les opérateurs $\mathscr{G}_{\mathscr{M},s}$

sur l'ensemble $A_\infty(\mathscr{V})$ formé par les fonctions f holomorphes dans $\mathscr{V}$ et continues sur $\bar{\mathscr{V}}$. Muni de la norme sup $|\cdot|$ définie par

$$|f| = \mathrm{Sup}\{|f(z)|, z \in \mathscr{V}\},$$

cet ensemble est un espace de Banach.

Pour une partie finie M de $N_\star$, l'opérateur $\mathscr{G}_{M,s}$, défini en (18), est borné pour toute valeur du paramètre s. Si la partie M est infinie, le domaine de définition de l'opérateur $\mathscr{G}_{M,s}$ coïncide avec le domaine de convergence $\mathscr{P}_M$ de la série de Dirichlet $\zeta_M(s)$ liée à la partie M,

$$\zeta_M(s) := \sum_{m \in M} \frac{1}{m^s}. \tag{24}$$

Pour des raisons qui apparaîtront plus loin, et dans toute la suite du travail, on se limite à des parties infinies M dites ouvertes pour lesquelles l'intersection de ce domaine de convergence $\mathscr{P}_M$ avec la droite réelle est un ouvert de la forme $\Delta_M = \{s \mid s > p_M\}$. Les travaux de Mauldin et Urbański ont mis en évidence un cadre de contraintes plus générales pour lesquelles la dimension de Hausdorff existait, mais nous nous restreignons ici à des contraintes ouvertes, qui fournissent un cadre certes plus restreint, mais aussi plus naturel. L'abscisse de convergence p_M vérifie $0 \leqslant p_M \leqslant 1$ et pour tout $s \in \mathscr{P}_M$, la norme de l'opérateur $\mathscr{G}_{M,s}$ se relie à la série d'Hurwitz $\zeta_M(s)(x)$ attachée à la partie M,

$$\zeta_M(s, x) := \sum_{m \in M} \frac{1}{(m+x)^s}$$

par la relation

$$\|\mathscr{G}_{M,s}\| \leqslant \zeta_M\left(\sigma, \frac{-1}{4}\right), \qquad \text{pour} \quad \sigma := \Re(s).$$

Comme l'opérateur $\mathscr{G}_{M,s}$ agit sur un espace de fonctions analytiques, c'est aussi un opérateur compact. Par composition, l'opérateur $\mathscr{G}_{M,s}$ associé à la période $\mathscr{M}$ et défini en (22) vérifie des propriétés similaires: Son domaine de définition $\mathscr{P}_{\mathscr{M}}$ coïncide avec le domaine de convergence de la série de Dirichlet $\zeta_{\mathscr{M}}(s)$ liée à la période $\mathscr{M}$

$$\zeta_{\mathscr{M}}(s) := \sum_{m \in \mathscr{M}} \frac{1}{Q_l(m)^s}, \tag{25}$$

et vérifie

$$\mathscr{P}_{\mathscr{M}} = \bigcap_{i=1}^{l} \mathscr{P}_{M_i},$$

Comme précédemment, on se limitera à des périodes $\mathscr{M}$ de cardinal infini, dites *ouvertes* pour lesquelles l'intersection de ce domaine de convergence $\mathscr{P}_{\mathscr{M}}$ avec la droite réelle est un ouvert de la forme $\Delta_{\mathscr{M}} = \{s \mid s > p_{\mathscr{M}}\}$. Il est aisé de remarquer que $\mathscr{M}$ est ouverte dès qu'il existe une composante M_i qui vérifie les deux propriétés

(i) p_{M_i} maximal parmi les p_{M_j} pour $1 \leqslant j \leqslant l$ (ii) M_i ouverte.

Sur le demi-plan $\mathscr{P}_{\mathscr{M}}$, la norme de l'opérateur $\mathscr{G}_{\mathscr{M}, s}$ se relie à la série d'Hurwitz $\zeta_{\mathscr{M}}(s, x)$ attachée à la période $\mathscr{M}$,

$$\zeta_{\mathscr{M}}(s, x) := \sum_{m \in \mathscr{M}} \frac{1}{[Q_l(m) + sQ_{l-1}(m)]^s},$$

par la relation

$$\|\mathscr{G}_{\mathscr{M}, s}\| \leqslant \zeta_{\mathscr{M}}\left(\sigma, \frac{-1}{4}\right) \leqslant \prod_{i=1}^{l} \zeta_{M_i}\left(\sigma, \frac{-1}{4}\right) \qquad \text{pour} \quad \sigma := \Re(s), \tag{26}$$

l'opérateur est aussi compact et possède ainsi un spectre discret, avec un seul point d'accumulation en 0.

2.1. *Nucléarité des opérateurs, déterminant de Fredholm, et formules de la trace*

Soit B un espace de Banach et $B^\star$ son espace dual. Un opérateur $\mathscr{L}: B \to B$ est nucléaire d'ordre 0 s'il admet la représentation

$$\mathscr{L} = \sum_{i \in I} \mu_i e_i^\star \otimes e_i \qquad \text{ou encore:} \quad \mathscr{L}[f] = \sum_{i \in I} \mu_i e_i^\star(f)\, e_i \qquad \text{pour tout} \quad f \in B,$$

avec $e_i \in B$, $e_i^\star \in B^\star$ vérifiant $\|e_i\| = \|e_i^\star\| = 1$ et μ_i p-sommable pour tout $p > 0$ (i.e., $\sum |\mu_i|^p < +\infty$).

De tels opérateurs ont été introduits et étudiés par Grotendhieck [Gr1, Gr2]. Ils sont compacts. Mieux, on peut justifier sur cette classe la plupart des calculs matriciels classiques. On définit ainsi la trace d'un tel opérateur,

$$\operatorname{Tr} \mathscr{L} = \sum_{i \in I} \mu_i e_i^\star(e_i), \qquad \text{égale aussi à} \quad \operatorname{Tr} \mathscr{L} = \sum_{i \in I} \lambda_i,$$

où les λ_i sont les valeurs propres de $\mathscr{L}$ comptées avec leur multiplicité algébrique. Les traces des itérés de $\mathscr{L}$ sont également bien définis. Le déterminant de Fredholm de $\mathscr{L}$, qui représente l'analogue du polynôme caractéristique,

$$\det(I-u\mathscr{L}) := \prod_{i\in I} (1-\lambda_i u), \tag{27}$$

où les λ_i sont les valeurs propres de $\mathscr{L}$ comptées avec leur multiplicité algébrique, admet alors l'expression

$$\det(I-u\mathscr{L}) = \exp[\operatorname{Tr}\log(I-u\mathscr{L})] = \exp\left[-\sum_{k=1}^{\infty} \frac{u^k}{k} \operatorname{Tr} \mathscr{L}^k\right]. \tag{28}$$

Ainsi, les opérateurs nucléaires d'ordre 0 ont toutes les bonnes propriétés qui justifient un calcul matriciel sur des matrices infinies. Sur certains espaces de Banach, comme l'espace $A_\infty(\mathscr{V})$ sur lequel on travaille ici, tout opérateur borné est nucléaire d'ordre 0 [Gr1, Gr2]. Les opérateurs de Ruelle–Mayer contraints sont donc nucléaires d'ordre 0.

Par ailleurs, la trace de l'opérateur $\mathscr{G}_{\mathscr{M},s}$ et de ses itérés se calcule explicitement en fonction des grandeurs α attachées aux mots de $\mathscr{M}^*$ et définies en (12). Pour une contrainte $\mathscr{M}$ de cardinal 1 définie par un unique mot m de longueur k, le spectre de l'opérateur $\mathscr{G}_{\{m\},s}$ est une progression géométrique de la forme

$$\{\mu_n = \alpha(m)^s\,(-1)^{nk}\,\alpha(m)^{2n},\, n\in \mathrm{N}\}, \tag{29}$$

et ainsi la trace vérifie

$$\operatorname{Tr} \mathscr{G}_{\{m\},s} = \frac{\alpha^s(m)}{1-(-1)^k\,\alpha^2(m)}.$$

Dans le cas d'une période $\mathscr{M}$ quelconque, l'opérateur $\mathscr{G}_{\mathscr{M},s}$ et ses itérés s'expriment comme une somme de tels opérateurs

$$\mathscr{G}^k_{\mathscr{M},s} = \sum_{m\in\hat{\mathscr{M}}^k} \mathscr{G}_{\{m\},s},$$

où $\hat{\mathscr{M}}$ désigne le miroir de $\mathscr{M}$. Par linéarité, la trace des opérateurs de Ruelle–Mayer contraints, associés à une contrainte de période $\mathscr{M}$ de longueur l vérifie

$$\operatorname{Tr} \mathscr{G}^k_{\mathscr{M},s} = \sum_{m\in\hat{\mathscr{M}}^k} \frac{\alpha^s(m)}{1-(-1)^{kl}\,\alpha^2(m)}. \tag{30}$$

Grâce à cette relation, les propriétés de la grandeur α (invariance par permutation circulaire ou effet miroir) se transmettent au spectre des opérateurs de Ruelle–Mayer contraints. Soit ρ une permutation, élément de l'ensemble Σ_l

des permutations de $\{1, 2, ..., l\}$. On considère la période $\mathcal{M}_\sigma$ déduite de $\mathcal{M}$ par application de σ,

$$\mathcal{M}_\sigma := M_{\sigma(1)} \times M_{\sigma(2)} \times \cdots \times M_{\sigma(l)}.$$

On s'intéresse aux permutations appartenant au groupe diédral engendré par le cycle σ défini par $\sigma(i) := i+1 \bmod l$ et par l'opération miroir τ définie par $\tau(i) := l-i+1$.

Proposition 1. *Soit ρ un élément du groupe diédral engendré par σ et τ. Alors les deux opérateurs de Ruelle–Mayer contraints, associé respectivement à la période $\mathcal{M}$ et à la période $\mathcal{M}_\rho$ ont le même spectre (multiplicités comprises). C'est en particulier le cas pour l'opérateur $\mathcal{G}_{\mathcal{M}, s}$ et son miroir $\mathcal{G}_{\hat{\mathcal{M}}, s}$.*

Preuve de la Proposition. L'identité des spectres de déduit de l'égalité entre les déterminants de Fredholm. Par ailleurs, la relation (28) relie ces déterminants à la trace des itérés dont l'expression a été évaluée en (30). Ainsi, il faut comparer les deux expressions

$$\operatorname{Tr} \mathcal{G}^k_{\mathcal{M}, s} = \sum_{n \in \mathcal{N}^k} \frac{\alpha^s(n)}{1-(-1)^{kl}\, \alpha^2(n)}, \qquad \operatorname{Tr} \mathcal{G}^k_{\mathcal{M}_\rho, s} = \sum_{p \in \mathcal{N}^k_\rho} \frac{\alpha^s(p)}{1-(-1)^{kl}\, \alpha^2(p)},$$

où $\mathcal{N}$ est le miroir de $\mathcal{M}$. Lorsque p décrit l'ensemble $\mathcal{N}^k_\rho$, p s'écrit sous la forme $\bar{\rho}(n)$, où $n = (n_1, n_2, ..., n_k)$ décrit l'ensemble $\mathcal{N}^k$. Si ρ est le cycle σ défini par $\sigma(i) := i+1 \bmod l$, alors $\bar{\sigma}(n)$ s'écrit $\sigma(n_1), \sigma(n_2), ..., \sigma(n_k) = S(\tilde{n})$, où S est le cycle défini par $S(i) := i+1 \bmod kl$ et $\tilde{n}$ est le mot n dans lequel les premières composantes de chaque n_i ont été permutées selon le cycle σ^{-1}. Puisque la grandeur α est invariante par la permutation circulaire S, on a dans ce cas $\alpha(p) = \alpha(\tilde{n})$. Si τ est le miroir, l'opération $\bar{\tau}$ sur les mots de longueur lk est définie par $\bar{\tau}(n_1, n_2, ..., n_k) = (\tau(n_1), \tau(n_2), ..., \tau(n_k)$. Donc $p := \bar{\tau}(n)$ est le miroir du mot $(n_k, n_{k-1}, ..., n_1)$, et ainsi, puisque la grandeur α est invariante par effet miroir, on a $\alpha(p) = \alpha(n_k, n_{k-1}, ..., n_1)$. Dans les deux cas, les multi-ensembles $\{\alpha(n), n \in \mathcal{N}^k\}$ et $\{\alpha(p), p \in \mathcal{N}^k_\rho\}$ coïncident. ∎

La proposition montre en particulier qu'on peut enlever le chapeau (lié à l'opération miroir) dans la formule (30)

$$\operatorname{Tr} \mathcal{G}^k_{\mathcal{M}, s} = \sum_{m \in \mathcal{M}^k} \frac{\alpha^s(m)}{1-(-1)^{kl}\, \alpha^2(m)},$$

et l'on obtient facilement une identité fondamentale

$$\sum_{m \in \mathcal{M}^k} \alpha^s(m) = \operatorname{Tr} \mathcal{G}^k_{\mathcal{M}, s} - (-1)^{kl} \operatorname{Tr} \mathcal{G}^k_{\mathcal{M}, s+2}, \tag{31}$$

qui donne, via l'identité (28), une relation mettant en jeu les déterminants de Fredholm

$$-\sum_{k\geqslant 1}\frac{u^k}{k}\sum_{m\in\mathcal{M}^k}\alpha^s(m)=\log\deg(I-u\mathcal{G}_{\mathcal{M},s})-\log\deg(I-(-1)^l\,u\mathcal{G}_{\mathcal{M},s+2}). \tag{32}$$

2.2. *Positivité de l'opérateur de Ruelle–Mayer contraint associé à une valeur réelle du paramètre s*

Lorsque s est réel ($s>p_{\mathcal{M}}$), l'opérateur $\mathcal{G}_{\mathcal{M},s}$ est u_0-positif. De tels opérateurs, introduits par Krasnoselsky [Kr], généralisent les opérateurs positifs de la dimension finie et possèdent des propriétés spectrales dominantes.

Un ensemble K d'un espace de Banach réel B est appelé un cône propre si

(i) pour tout réel $\rho>0$ et tout f de K, $\rho f\in K$,

(ii) $K\cap -LK=\{0\}$.

Un cône propre est appelé reproductif si $B=K-K$, i.e., tout élément f de B s'écrit comme la différence de deux éléments de K.

Soit K un cône propre, reproductif et d'intérieur $\mathring{K}$ non vide. On dit que $\mathcal{L}$: $B\to B$ est positive (par rapport au cône K) si $\mathcal{L}(K)$ est inclus dans K. Soit u_0 un élément de $\mathring{K}$; on dit que l'opérateur positif $\mathcal{L}$ est u_0-positif par rapport au cône K si pour tout élément f non nul de K, il existe un entier p et deux réels α et β strictement positifs pour lesquels

$$\beta u_0\leqslant\mathcal{L}^p[f]\leqslant\alpha u_0, \tag{33}$$

où l'ordre est défini en relation avec K: $f\leqslant g$ si et seulement si $g-f\in K$.

Alors, d'après un théorème dû à Krasnoselsky [Kr], un opérateur $\mathcal{L}$ compact et u_0-positif satisfait à une propriété de type Perron–Frobenius: il a un unique vecteur propre g dans $\mathring{K}$ et la valeur propre associée λ est simple, positive, et strictement plus grande en valeur absolue que les autres valeurs propres.

Si s est réel ($s>p_{\mathcal{M}}$), l'opérateur $\mathcal{G}_{\mathcal{M},s}$ laisse stable l'espace $A^{\mathbf{R}}_{\infty}(\mathcal{V})$ formé par les éléments de $A_{\infty}(\mathcal{V})$ qui sont réels sur $\mathcal{J}$; c'est un espace de Banach réel, et l'ensemble K des fonctions de $A_{\infty}(\mathcal{V})$ dont la restriction à $\mathcal{J}$ est positive ou nulle y forme un cône propre, reproductif et d'intérieur $\mathring{K}$ non vide. La fonction constante $u_0=1$ est un élément de $\mathring{K}$ et on montre:

LEMME 1. *La restriction de l'opérateur $\mathcal{G}_{\mathcal{M},s}$ à $A^{\mathbf{R}}_{\infty}(\mathcal{V})$, est u_0-positif par rapport au cône K.*

Preuve. On adapte en effet aisément la preuve [Ma1] que Mayer donne pour les opérateurs usuels. Supposons que $\mathcal{G}_{\mathcal{M},s}$ ne vérifie pas (33). Il existe donc une fonction f de K pour laquelle pour tout entier k, il existe $u \in \mathcal{J}$ pour lequel $\mathcal{G}^k_{\mathcal{M},s}[f](u) = 0$. Alors, pour toute homographie de $\hat{\mathcal{H}}_{kl}(\mathcal{M})$, on a $f \circ h(u) = 0$. Comme le cardinal $|\mathcal{M}|$ est au moins égal à 2, il y a au moins 2^k homographies distinctes dans l'ensemble $\hat{\mathcal{H}}_{kl}(\mathcal{M})$, et donc 2^k points distincts où f s'annule. On en déduit donc, en faisant tendre $k \to \infty$, que f est identiquement nulle. ∎

On peut donc appliquer le théorème de Krasnoselsky à la restriction de $\mathcal{G}_{\mathcal{M},s}$ à $A^{\mathbf{R}}_\infty(\mathcal{V})$. Par ailleurs, adaptant un autre argument de Mayer [Ma3], on montre que les deux spectres—celui de $\mathcal{G}_{\mathcal{M},s}$ et celui de la restriction de $\mathcal{G}_{\mathcal{M},s}$ à $A^{\mathbf{R}}_\infty(\mathcal{V})$—coïncident.

Ce qui précède permet alors de montrer le résultat suivant.

Proposition 2. *Pour un réel $s > p_{\mathcal{M}}$, l'opérateur $\mathcal{G}_{\mathcal{M},s}$: $A_\infty(\mathcal{V}) \to A_\infty(\mathcal{V})$ a une valeur propre dominante $\lambda(\mathcal{M}, s)$ qui est simple, positive et strictement plus grande que toutes les autres valeurs propres en valeur absolue. Le vecteur propre correspondant $f_{\mathcal{M},s}$ est strictement positif sur $\mathcal{J}$. La projection $\mathcal{P}_{\mathcal{M},s}$ sur le sous-espace propre dominant est définie par $\mathcal{P}_{\mathcal{M},s}[f](z) = e_{\mathcal{M},s}[f]\, f_{\mathcal{M},s}(z)$, où la forme linéaire $e_{\mathcal{M},s}$ vérifie $e_{\mathcal{M},s}[f] > 0$ pour une fonction $f > 0$ sur $\mathcal{J}$. L'opérateur $\mathcal{G}_{\mathcal{M},s}$ admet la représentation*

$$\mathcal{G}_{\mathcal{M},s} = \lambda(\mathcal{M}, s)\, \mathcal{P}_{\mathcal{M},s} + \mathcal{N}_{\mathcal{M},s}, \tag{34}$$

où $\mathcal{P}_{\mathcal{M},s} \circ \mathcal{N}_{\mathcal{M},s} = \mathcal{N}_{\mathcal{M},s} \circ \mathcal{P}_{\mathcal{M},s} = 0$. Le rapport spectral, égal par définition au rapport entre le rayon spectral de $\mathcal{N}_{\mathcal{M},s}$ et $\lambda(\mathcal{M}, s)$ est strictement plus petit que 1. *Pour toute constante α strictement plus grande que le rapport spectral, et pour une fonction f de $A_\infty(\mathcal{V})$ strictement positive sur $\mathcal{J}$, on a*

$$\mathcal{G}^k_{\mathcal{M},s}[f](z) = \lambda(\mathcal{M}, s)^k\, \mathcal{P}_{\mathcal{M},s}[f](z)[1 + O(\alpha^k)],$$

pour tout $k \geqslant 1$ et tout z dans $\mathcal{J}$.

On obtient des minorations et des majorations indépendantes de k: Pour tout s réel $s > p_{\mathcal{M}}$, pour toute fonction f de $A_\infty(\mathcal{V})$ strictement positive sur $\mathcal{J}$, il existe deux constantes A et B dépendant de s et de f, pour lesquelles on a l'encadrement valable pour tout $k \geqslant 1$, et pour tout z de $\mathcal{J}$

$$B\lambda(\mathcal{M}, s)^k \leqslant \mathcal{G}^k_{\mathcal{M},s}[f](z) \leqslant A\lambda(\mathcal{M}, s)^k. \tag{35}$$

Pour une contrainte $\mathcal{M}$ de cardinal 1, l'opérateur $\mathcal{G}_{\mathcal{M},s}$ est positif, mais le lemme ne s'applique pas et on ne peut a priori démontrer que cet opérateur est u_0-positif. On a déjà montré qu'on connaissait explicitement son spectre (29). Lorsque s est réel, on montre aussi directement que le vecteur propre correspondant $f_{\mathcal{M},s}$ est strictement positif sur $\mathcal{J}$ et que la forme linéaire

$e_{\mathcal{M},s}$ vérifie $e_{\mathcal{M},s}[f]>0$ pour une fonction $f>0$ sur $\mathcal{J}$. La proposition est ainsi encore vraie dans ce cas.

On peut aussi montrer (mais on ne le fera pas ici) que le spectre de $\mathcal{G}_{\mathcal{M},s}$ est réel dès que s est réel: c'est une autre adaptation simple de la représentation intégrale de l'opérateur de Ruelle–Mayer non contraint.

2.3. *Propriétés liées aux perturbations du paramètre s au voisinage de l'axe réel*

Comme l'application $s \to \mathcal{G}_{\mathcal{M},s}$ définit une application holomorphe de $\{s \mid \Re(s) > p_{\mathcal{M}}\}$ dans $A_\infty(\mathcal{V})$, on peut appliquer au voisinage de l'axe réel la théorie des perturbations qui montre que l'opérateur $\mathcal{G}_{\mathcal{M},s}$ conserve ses propriétés spectrales dominantes au voisinage d'un paramètre s réel:

PROPOSITION 3. *Soit $\sigma > p_{\mathcal{M}}$ un nombre réel fixé. Il existe un voisinage complexe Ω de σ pour lequel les propriétés spectrales dominantes de $\mathcal{G}_{\mathcal{M},\sigma}$ se prolongent à $\mathcal{G}_{\mathcal{M},s}$: les quatre quantités $\lambda(\mathcal{M},s)$, $f_{\mathcal{M},s}$, $e_{\mathcal{M},s}$ (et donc $\mathcal{P}_{\mathcal{M},s}$), $\mathcal{N}_{\mathcal{M},s}$ y sont bien définies, y représentent les objets spectraux dominants de $\mathcal{G}_s$ et sont analytiques en s; de plus, le rayon spectral de $\mathcal{N}_{\mathcal{M},s}$ est strictement inférieur à $|\lambda(\mathcal{M},s)|$. Sur le même voisinage Ω, et pour toute fonction f de $A_\infty(\mathcal{V})$ strictement positive sur $\mathcal{J}$, on a*

$$\mathcal{G}^k_{\mathcal{M},s}[f](z) = \lambda(s)^k\, \mathcal{P}_{\mathcal{M},s}[f](z) + \mathcal{N}^k_{\mathcal{M},s}[f](z) \tag{36}$$

pour tout $k \geqslant 1$, et pour tout point z de $\mathcal{V}$.

2.4. *Propriétés de la valeur propre dominante*: *définition de l'abscisse $s_{\mathcal{M}}$ et de la constante de Lévy $\mathcal{L}(\mathcal{M})$*

Pour un réel $s > p_{\mathcal{M}}$, la valeur propre dominante $\lambda(\mathcal{M},s)$ peut alors être définie par

$$\lambda(\mathcal{M},s) = \lim_k \left(\sum_{m \in \mathcal{M}^k} \frac{1}{Q^s_{kl}(m)} \right)^{1/k}. \tag{37}$$

(Il suffit d'appliquer ce qui précède à la fonction constante 1 qui est un élément de $A_\infty(\mathcal{V})$.) Le plus petit des continuants Q_k est obtenu quand chacun des m_i est minimal dans sa catégorie; on désigne par a_i cette valeur minimale, et on considère le nombre $a_{\mathcal{M}}$ irrationnel quadratique dont le développement en fraction continue est périodique de période $(a_1, a_2, ..., a_l)$. Le continuant Q_k vérifie alors

$$\lim \frac{1}{k} \log Q_k = \beta(a_{\mathcal{M}})$$

où $\beta(x)$ est la constante de Lévy de l'irrationnel quadratique x, définie en ( ), ce qui monte que $s \to \lambda(\mathscr{M}, s)$ vérifie, pour tout $u \geqslant 0$

$$\lambda(\mathscr{M}, s+u) \leqslant e^{-lu\beta(a_{\mathscr{M}})} \lambda(\mathscr{M}, s), \tag{38}$$

et définit donc une fonction strictement décroissante de s le long de l'axe réel. Par ailleurs, si la partie $\mathscr{M}$ est ouverte, les deux relations

$$\lim_{s \to p_{\mathscr{M}}} \lambda(\mathscr{M}, s) = +\infty, \qquad \lim_{s \to +\infty} \lambda(\mathscr{M}, s) = 0,$$

et l'analycité de l'application $s \to \lambda(\mathscr{M}, s)$ montrent l'existence d'un unique point $s_{\mathscr{M}}$ de $]p_{\mathscr{M}}, +\infty[$ qui vérifie

$$\lambda(\mathscr{M}, s_{\mathscr{M}}) = 1.$$

Puisque par ailleurs l'application $\mathscr{M} \to \lambda(\mathscr{M}, s)$ est croissante, et vérifie

$$\lambda(\mathscr{M}, 0) = |\mathscr{M}| > 1, \qquad \text{pour } \mathscr{M} \text{ finie et } \lambda(N_\star, 2) = 1,$$

le point $s_{\mathscr{M}}$ appartient toujours à l'intervalle $]\mathrm{Max}(p_{\mathscr{M}}, 0), 2]$.

Lorsque l'ensemble $\mathscr{M}$ est fini, on peut aussi considérer le plus grand des continuants, obtenu quand chacun des m_i est maximal dans sa catégorie; on désigne par b_i cette valeur maximale, et on considère le nombre $b_{\mathscr{M}}$ irrationnel quadratique dont le développement en fraction continue est périodique de période $(b_1, b_2, ..., b_l)$. Le continuant Q_k vérifie alors

$$\lim \frac{1}{k} \log Q_k = \beta(b_{\mathscr{M}}),$$

ce qui montre que $s \to \lambda(\mathscr{M} s)$ vérifie, pour tout $u \geqslant 0$

$$\lambda(\mathscr{M}, s+u) \geqslant e^{-lu\beta(b_{\mathscr{M}})} \lambda(\mathscr{M}, s). \tag{39}$$

En particulier, en faisant tendre u vers 0, en utilisant (38) et (39), et en choisissant $s := s_{\mathscr{M}}$, on obtient l'encadrement

$$\beta(a_{\mathscr{M}}) \leqslant \mathscr{L}(\mathscr{M}) := \frac{-1}{l} \lambda'(\mathscr{M}, s_{\mathscr{M}}) \leqslant \beta(b_{\mathscr{M}}),$$

ce qui justifie déjà le nom de constante de Lévy de $\mathscr{M}$ donné à la constante $(-1/l)\, \lambda'(\mathscr{M}, s_{\mathscr{M}})$. On montrera dans le Théorème 3 de la Section 5 que la constante de Lévy $\mathscr{L}(\mathscr{M})$ est en un sens précis la moyenne des constantes de Lévy des irrationnels quadratiques $\mathscr{M}$-contraints.

Remarquons que les deux grandeurs $s_{\mathscr{M}}$ et $\mathscr{L}(\mathscr{M})$ ne dépendent que de la contrainte, et non de la manière dont elle est engendrée. deux périodes différentes $\mathscr{M}$ et $\mathscr{N}$ de la même contrainte vérifient $\mathscr{N}^n = \mathscr{M}^m$ pour deux entiers m et n et donc $\lambda(\mathcal{M}, s)^m = \lambda(\mathcal{N}, s)^n$, ce qui détermine le même point $s_{\mathcal{M}} = s_{\mathcal{N}}$ et, en dérivant en ce point, la même constante de Lévy contrainte.

Ainsi, la Proposition 1 admet pour corollaire le résultat suivant:

Corollaire 4. *Soit ρ un élément du groupe diédral engendré par σ et τ. Alors la période $\mathcal{M}$ et la période $\mathcal{M}_\rho$ définissent les mêmes grandeurs fondamentales $s_{\mathcal{M}}$ et $\mathcal{L}(\mathcal{M})$. Ainsi, les énoncés des six résultats du travail sont exactement les mêmes pour les nombres contraints par la période $\mathcal{M}$ ou par une période $\mathcal{M}_\rho$ déduite de la période $\mathcal{M}$ par action du groupe diédral. Seule la constante $c_{\mathcal{M}}$ du résultat* (ii) *dépend a priori de la période $\mathcal{M}$ elle-même et non seulement de sa classe d'équivalence modulo ce groupe diédral.*

2.5. *Propriétés du rayon spectral*

Un autre volet de résultats concerne les propriétés du rayon spectral. Le résultat principal généralise un résultat similaire obtenu par Faivre dans un contexte plus particulier et montre que, le long d'une droite verticale, le rayon spectral atteint son maximum strict sur l'axe réel.

Proposition 5. *Soit $\sigma > p_{\mathcal{M}}$ un nombre réel fixé et s un nombre complexe de la forme $s = \sigma + it$, $t \neq 0$. Alors le rayon spectral $R(\mathcal{M}, s)$ de $\mathcal{G}_{\mathcal{M},s}$ est strictement inférieur à $\lambda(\mathcal{M}, \sigma)$.*

Remarque. Ce résultat n'est pas vrai dans le cas où le cardinal $|\mathcal{M}|$ est égal à 1, comme le montre l'expression explicite (36) du spectre.

Compte-tenu de l'inégalité (38), qui prouve la décroissance stricte le long de l'axe réel, on obtient le résultat suivant qui sera essentiel lors de l'application ultérieure des théorèmes taubériens:

Corollaire 6. *Soit $\sigma > p_{\mathcal{M}}$ un nombre réel fixé. Alors pour tout s vérifiant $\Re(s) \geqslant \sigma$ et $s \neq \sigma$, le rayon spectral $R(\mathcal{M}, s)$ de $\mathcal{G}_{\mathcal{M},s}$ est strictement inférieur à $\lambda(\mathcal{M}, \sigma)$.*

Preuve de la Proposition 5. On peut toujours suppose, quitte à effectuer une permutation circulaire qui laisse le spectre invariant, que la période $\mathcal{M}$ est de la forme $M_1 \times M_2 \times \cdots \times M_l$, avec $|M_l| \geqslant 2$. Alors $\hat{\mathcal{M}}$ contient deux mots m et n qui diffèrent par leur dernière composante. Par ailleurs, le spectre étant invariant par effet miroir, on va travailler avec l'opérateur $\mathcal{G}_{\hat{\mathcal{M}},s}$. Soit λ une valeur propre de $\mathcal{G}_{\hat{\mathcal{M}},s}$ et f un vecteur propre associé. On désigne par f_σ le vecteur propre dominant de $\mathcal{G}_{\hat{\mathcal{M}},\sigma}$. Ce vecteur propre est, d'après la Proposition 2, strictement positif sur l'intervalle $\mathcal{J}$, et ne s'annule pas $\mathcal{V}$. On le normalise par la condition $f_\sigma(0) = 1$; par ailleurs, on peut toujours, quitte à multiplier f par une constante, supposer que la fonction μ définie sur $\mathscr{V}$ par

$$\mu(x) := \frac{f(x)}{f_\sigma(x)} \tag{40}$$

est de module au plus égal à 1 sur $[0, 1]$ et atteint le module 1 en un point x_0. On a toujours, compte-tenu des relations (20)

$$\begin{aligned} |\lambda|\ |f(x_0)| &= |\mathscr{G}_{\hat{\mathscr{M}}, s}[f](x_0)| \\ &\leqslant \sum_{h \in \mathscr{H}_l(\mathscr{M})} \tilde{h}(x_0)^\sigma\ |f \circ h(x_0)| \\ &\leqslant \sum_{h \in \mathscr{H}_l(\mathscr{M})} \tilde{h}(x_0)^\sigma\ f_\sigma \circ h(x_0) \\ &= \lambda(\sigma)\ f_\sigma(x_0), \end{aligned}$$

et la définition de x_0 montre alors l'inégalité large $|\lambda| \leqslant \lambda(\sigma)$.

On va alors montrer dans un premier temps le résultat général suivant, qui n'utilise pas la forme particulière des homographies. La preuve généralise des idées contenues dans des preuves analogues de Faivre [Fa] et Pollicott [Po2].

Lemme 2. *Supposons que l'on ait l'égalité*

$$\lambda = e^{ia}\lambda(\sigma) \qquad (a \in \mathbf{R}) \tag{41}$$

lorsque le réel s vérifie $s = \sigma + it$, $t \neq 0$. Alors, la fonction μ définie en (40) *est de module* 1, *est un vecteur propre commun à tous les opérateurs composantes $\mathscr{G}_{\{m\}, it}$, associé à la même valeur propre e^{ia}. De plus, les grandeurs α associées aux mots m de $\mathscr{M}$ vérifient la relation*

$$\alpha(m)^{it} = e^{ia}$$

Preuve du Lemme 2. La relation (41) montre que, pour tout ρ vérifiant $\rho\lambda(\sigma) < 1$, et u de la forme $u = \rho e^{-ia}$, on a

$$\sum_{k \geqslant 0} \lambda^k u^k = \sum_{k \geqslant 0} \lambda(\sigma)^k\ |u|^k$$

et on obtient donc la chaîne d'égalités:

$$\begin{aligned}\left|\sum_{k\geqslant 0}\lambda^k u^k f(x_0)\right| &= \left|\sum_{k\geqslant 0} u^k \sum_{h\in\mathscr{H}_{kl}(\mathscr{M})} \tilde{h}(x_0)^{\sigma+it} f\circ h(x_0)\right| \\ &= \sum_{k\geqslant 0} |u|^k \sum_{h\in\mathscr{H}_{kl}(\mathscr{M})} \tilde{h}(x_0)^{\sigma}\, |f\circ h(x_0)| \\ &= \sum_{k\geqslant 0} |u|^k \sum_{h\in\mathscr{H}_{kl}(\mathscr{M})} \tilde{h}(x_0)^{\sigma}\, f_\sigma\circ h(x_0) \\ &= \sum_{k\geqslant 0} \lambda(\sigma)^k\, |u|^k\, f_\sigma(x_0). \end{aligned} \tag{42}$$

En particulier la condition

$$\forall k\geqslant 0, \forall h\in\mathscr{H}_{kl}(\mathscr{M}) \qquad |f\circ h(x_0)| = f_\sigma\circ h(x_0)$$

est réalisée et montre que la fonction μ définie en (40) vérifie $|\mu\circ h(x_0)|=1$ pour tout homographie $\mathscr{M}$-valide. Comme tout réel de $\mathscr{R}(\mathscr{M})$ s'obtient comme une limite de points de la forme $h(x_0)$ avec h $\mathscr{M}$-valide, on obtient

$$|\mu\circ h(x)|=1 \qquad \text{pour tout } x \text{ dans } \mathscr{R}(\mathscr{M}) \text{ et toute homographie } \mathscr{M}\text{-valide.}$$

On reprend la chaîne d'égalités (42), mais cette fois en tout point x de $\mathscr{R}(\mathscr{M})$ et on obtient la condition

$$\sum_{k\geqslant 0} |u|^k \sum_{h\in\mathscr{H}_{kl}(\mathscr{M})} \tilde{h}(x)^{\sigma}\, |f\circ h(x)| = \left|\sum_{k\geqslant 0} u^k \sum_{h\in\mathscr{H}_{kl}(\mathscr{M})} \tilde{h}(x)^{\sigma+it}\, f\circ h(x)\right|.$$

On a ainsi une famille $(a_h(x))$ qui vérifie $|\sum a_h(x)| = \sum |a_h(x)|$; il existe donc un nombre complexe $\theta(x)$ de module 1 tel que $a_h(x)=\theta(x)\,|a_h(x)|$ pour tout h, et revenant au problème, on déduit l'existence, pour tout $x\in\mathscr{R}(\mathscr{M})$, d'un nombre complexe $\theta(x)$ de module 1 vérifiant, pour tout $k\geqslant 0$, pour tout $h\in\mathscr{H}_{kl}(\mathscr{M})$ l'égalité

$$u^k f\circ h(x)\, \tilde{h}(x)^{it} = \theta(x)\, |u|^k\, |f\circ h(x)| = \theta(x)\, |u|^k\, f_\sigma\circ h(x).$$

Ainsi, revenant à la fonction μ, et à a définis en (40) et (41), on a

$$\tilde{h}(x)^{it}\, \mu\circ h(x) = \theta(x)\, e^{ika},$$

ce qui montre, en choisissant $h=\mathrm{Id}$ $(k=0)$ que θ coïncide avec μ sur $\mathscr{R}(\mathscr{M})$, et finalement on obtient l'égalité valable pour tout $x\in\mathscr{R}(\mathscr{M})$, pour tout $k\geqslant 0$, pour tout $h\in\mathscr{H}_{kl}(\mathscr{M})$ l'égalité

$$\tilde{h}(x)^{it}\, \mu\circ h(x) = \mu(x)\, e^{kia}.$$

En particulier, si $x = h^\star$ est l'irrationnel quadratique point fixe de l'homographie h associée à un mot m de $\mathscr{M}^k$, on obtient l'égalité $\alpha(m)^{it} := \tilde{h}(h^\star)^{it} = e^{kia}$ et finalement

$$\tilde{h}(x)^{it}\, \mu \circ h(x) = \mu(x)\, \tilde{h}(h^\star)^{it}, \tag{43}$$

pour tout x de $\mathscr{R}(\mathscr{M})$. Les fonctions en jeu étant toutes holomorphes dans $\mathscr{V}$, l'égalité se prolonge à $\mathscr{V}$, et permet de montrer que μ est de module constant égal à 1 sur $\mathscr{J}$. En effet, pour un point y de $\mathscr{J}$, tout point x de $\mathscr{R}(\mathscr{M})$ est limite de points de la forme $h(y)$, et donc

$$|\mu(x)| = |\lim \mu \circ h(y)| = |\mu(y)|.$$

Puisque t est supposé non nul, μ est ainsi de la forme

$$\mu(x) = \exp[itL(x)]$$

où L est une fonction définie sur $\mathscr{V}$ et réelle sur $\mathscr{J}$, et le Lemme 2 est démontré. ∎

On montre maintenant que toutes ces contraintes mènent à une contradiction dans le cas où les fonctions h sont des homographies. La relation (43) montre alors l'existence d'un entier K_h pour lequel l'égalité

$$L \circ h(x) - L(x) = \log \tilde{h}(x) - \log \tilde{h}(h^\star) + \frac{2K_y\pi}{t},$$

entre L et la détermination principale du logarithme est satisfaire pour tout x de $\mathscr{J}$. Faisant tendre x vers le point fixe $h^\star$, on obtient $K_h = 0$ et donc l'égalité

$$L \circ h(x) - L(x) = \log \tilde{h}(x) - \log \tilde{h}(h^\star), \tag{44}$$

qui se prolonge sur $\mathscr{V}$ du fait que $\tilde{h}(\mathscr{V})$ est un disque du demi-plan droit. On considère alors un mot m de $\mathscr{M}$, l'homographie h associée de point fixe $h^\star$ et les homographies h^k de profondeur kl associées aux mots m^k; on fait tendre $k \to \infty$ en gardant x fixe. Le premier membre de (44) a pour limite $L(h^\star) - L(x)$, et il en est de même pour le second membre, ce qui prouve que le rapport $Q_{kl}(m^k)/Q_{kl-1}(m^k)$ a une limite $\gamma(m)$ lorsque $k \to \infty$. On obtient la relation

$$L(h^\star) - L(x) = \log \frac{h^\star + \gamma(m)}{x + \gamma(m)},$$

valable pour tout x, et donc l'identité

$$L(x)-L(y)=\log\frac{x+\gamma(m)}{y+\gamma(m)},$$

pour tous couples (x, y) d'éléments de $\mathscr{V}$. Le premier membre ne dépendant plus du mot m choisi dans $\mathscr{M}$, on en déduit que la limite $\gamma(m)$ est indépendante de m. On considère alors deux mots m et n qui diffèrent par leurs dernières composantes m_l et n_l. Les limites $\gamma(m)$ et $\gamma(n)$ sont nécessairement distinctes puisqu'elles vérifient

$$m_l<\gamma(m)<m_l+1, \qquad n_l<\gamma(n)<n_l+1,$$

ce qui fournit la contradiction cherchée. ▮

3. DIMENSION DE HAUSDORFF DE L'ENSEMBLE DES RÉELS CONTRAINTS

Cette section est, pour l'essentiel, consacrée à la preuve du résultat (i). L'étude de la dimension de Hausdorff des réels contraints a véritablement débuté avec le travail de Good [Go], qui s'est essentiellement intéressé à des contraintes finies élémentaires. Par la suite, Cusick [Cu] a relié cette dimension à l'abscisse de convergence d'une série de Dirichlet, qui n'est autre que la fonction $(I-\mathscr{G}_{\mathscr{M},s})^{-1}[1](0)$, et Bumby [Bu] a vu, le premier, les relations de ce problème avec de l'analyse fonctionnelle. Par la suite, Hensley [He1–He4] a effectivement relié l'étude de la dimension de Hausdorff à l'opérateur de Ruelle–Mayer contraint, mais uniquement dans le cas particulier d'une contrainte élémentaire finie. Enfin, Mauldin et Urbański [MU1, MU2] ont traité le cas d'une contrainte élémentaire quelconque. Nous généralisons leur résultat à une contrainte générale (i.e., non élémentaire) mais seulement ouverte. Nous travaillons ici explicitement avec les opérateurs de Ruelle–Mayer contraints, et utilisons fortement leurs propriétés spectrales dominantes.

Rappelons d'abord quelques définitions relatives aux mesures d'un sous-ensemble $\mathscr{F}$ de l'intervalle $[0, 1]$. On dit que $\mathscr{F}$ est nulle si pour tout $\varepsilon>0$, il existe un recouvrement $(U_i)_{i\in I}$ de $\mathscr{F}$ vérifiant $\sum_{i\in I}|U_i|<\varepsilon$. On dit que $\mathscr{F}$ est de mesure nulle en dimension s si pour tout $\varepsilon>0$, il existe un recouvrement $(U_i)_{i\in I}$ de $\mathscr{F}$ vérifiant $\sum_{i\in I}|U_i|^s<\varepsilon$. De même, $\mathscr{F}$ est de mesure finie en dimension s si il existe $K>0$ pour lequel pour tout $\delta>0$, il existe un recouvrement $(U_i)_{i\in I}$ de $\mathscr{F}$ vérifiant $|U_i|\leqslant\delta$ et $\sum_{i\in I}|U_i|^s\leqslant K$.

Remarquons alors, que si $\mathscr{F}$ est de mesure finie en dimension s, alors pour tout s' vérifiant $s'>s$, $\mathscr{F}$ est de mesure nulle en dimension s'. De même, si $\mathscr{F}$ est de mesure non nulle en dimension s, alors pour tout s' vérifiant $s' < s$, $\mathscr{F}$ est de mesure infinie en dimension s'. On appelle dimension de Hausdorff de $\mathscr{F}$, et on la désigne par $\mathscr{H}(\mathscr{F})$, le nombre réel s_0 où la mesure s-dimensionnelle de $\mathscr{F}$ change de nature: pour $s > s_0$, elle est nulle, pour $s < s_0$, elle est infinie. Ainsi la dimension de Hausdorff permet, en affinant la notion de mesure nulle, de départager les ensembles de mesure nulle entre eux.

THÉORÈME 1. *Soit $\langle \mathscr{M} \rangle$ un ensemble périodique de contraintes; la dimension de Hausdorff de l'ensemble $\mathscr{R}(\mathscr{M})$ qu'on désigne de manière abrégée par $\mathscr{H}(\mathscr{M})$ vérifie l'égalité*

$$\mathscr{H}(\mathscr{M}) = \tfrac{1}{2} s_{\mathscr{M}},$$

où $s_{\mathscr{M}}$ est le réel qui vérifie la relation $\lambda(\mathscr{M}, s_{\mathscr{M}}) = 1$ définie par la valeur propre dominante $\lambda(\mathscr{M}, s)$ de l'opérateur de Ruelle–Mayer $\mathscr{G}_{\mathscr{M}, s}$ associé à la période.

Preuve. La preuve se fait en trois étapes. On démontre d'abord l'inégalité $\mathscr{H}(\mathscr{M}) \leqslant (1/2)\, s_{\mathscr{M}}$. Puis, pour un ensemble $\mathscr{M}$ fini, on démontre l'inégalité inverse $\mathscr{H}(\mathscr{M}) \geqslant (1/2)\, s_{\mathscr{M}}$. On obtient donc l'égalité cherchée dans le cas où $\mathscr{M}$ est fini. On considère alors l'ensemble périodique associé à la partie $\mathscr{M}_N$ définie par

$$\mathscr{M}_N = \mathscr{M} \bigcap \{1, 2, ..., N\}^{l}.$$

On a l'égalité cherchée pour tous les ensembles $\mathscr{M}_N$ et on en déduit la relation

$$\tfrac{1}{2} s_{\mathscr{M}_N} = \mathscr{H}(\mathscr{M}_N) \leqslant \mathscr{H}(\mathscr{M}) \leqslant \tfrac{1}{2} s_{\mathscr{M}}. \tag{45}$$

Il reste à prouver dans une dernière étape utilisant les perturbations de l'ensemble $\mathscr{M}$ que la suite $s_{\mathscr{M}_N}$ converge vers $s_{\mathscr{M}}$. Les deux premières étapes généralisent des preuves classiques, la dernière étape simplifie un argument qu'Hensley [He3] a développé dans un contexte un peu différent.

On utilise dans les deux premières étapes les recouvrements de $\mathscr{R}(\mathscr{M})$ par les intervalles fondamentaux $\mathscr{M}$-valides de hauteur k. L'expression (7) de la longueur u_h de l'intervalle fondamental associé à l'homographie h permet d'évaluer la mesure s-dimensionnelle de ce recouvrement

$$\Lambda^{\langle k \rangle}_{\mathscr{M}, s} := \sum_{h \in \mathscr{H}_k(\mathscr{M})} u_h^s = \sum_{m \in \mathscr{M}(k)} \frac{1}{Q_k^s (Q_{k-1} + Q_k)^s} = \sum_{m \in \mathscr{M}(k)} \frac{1}{Q_k^{2s} (1 + Q_{k-1}/Q_k)^s}.$$

Grâce à la propriété (4) de symétrie des continuants et la relation (21), on obtient donc une expression où interviennent les contraintes avec effet miroir,

$$\Lambda^{\langle k \rangle}_{\mathcal{M},s} = \mathcal{G}_{M_k,2s} \circ \mathcal{G}_{M_{k-1},2s} \circ \cdots \circ \mathcal{G}_{M_1,2s}\left[\frac{1}{(1+z)^s}\right](0) = \mathcal{G}_{\mathcal{M}(k),2s}\left[\frac{1}{(1+z)^s}\right](0),$$

et l'opérateur du second membre s'exprime en fonction des itérés de l'opérateur de Ruelle–Mayer $\mathcal{G}_{\mathcal{M},2s}$ qui engendre la période miroir $\mathcal{M}$

$$\mathcal{G}_{\mathcal{M},2s} = \mathcal{G}_{M_l,2s} \circ \mathcal{G}_{M_{l-1},2s} \circ \cdots \circ \mathcal{G}_{M_1,2s}.$$

Première étape. On considère le cas particulier des indices k multiples de l de la forme $k = nl$,

$$\sum_{h \in \mathcal{H}_{nl}(\mathcal{M})} u_h^s = \mathcal{G}^n_{\mathcal{M},2s}\left[\frac{1}{(1+z)^s}\right](0),$$

où $\mathcal{G}^n_{\mathcal{M},2s}$ représente la puissance n-ième de l'opérateur $\mathcal{G}_{\mathcal{M},2s}$.

On utilise alors le propriétés spectrales dominantes de l'opérateur $\mathcal{G}_{\mathcal{M},2s}$ et la majoration (35): pour tout s réel $s > p_{\mathcal{M}}$, il existe un nombre $A_s > 0$ pour lequel, pour tout z de l'intervalle $\mathcal{J}$, et pour tout $n \geqslant 1$ suffisamment grand, on a

$$\left|\mathcal{G}^n_{\mathcal{M},2s}\left[\frac{1}{(1+z)^s}\right]\right| \leqslant A_s \lambda(\mathcal{M}, 2s)^n.$$

On obtient donc

$$\Lambda^{\langle k \rangle}_{\mathcal{M},s} \leqslant A_s \lambda(\mathcal{M}, 2s)^n.$$

Soit maintenant un nombre réel s vérifiant $2s > s_{\mathcal{M}}$. Alors, puisque la fonction $s \to \lambda(\mathcal{M}, s)$ est strictement décroissante, la valeur propre dominante satisfait $\lambda(\mathcal{M}, 2s) < 1$. Ainsi, il suffit de choisir n suffisamment grand pour rendre la mesure s dimensionnelle $\Lambda^{\langle k \rangle}_{\mathcal{M},s}$ arbitrairement petite. On a donc montré: pour tout s vérifiant $2s > s_{\mathcal{M}}$, l'ensemble $\mathcal{R}(\mathcal{M})$ a une mesure s-dimensionnelle nulle, et donc la dimension de Hausdorff $\mathcal{H}(\mathcal{M}$ de $\mathcal{R}(\mathcal{M})$ vérifie $\mathcal{H}(\mathcal{M}) \leqslant s$, ce qui permet de conclure la première étape. ∎

Deuxième étape. On part d'un résultat de Good [Go] qui affirme:

Lemme 3. *Soit une contrainte élémentaire finie et soit s un nombre réel strictement positif. Alors si, pour tout k suffisamment grand, on a* $\Lambda^{\langle k \rangle}_{\mathcal{M},s} \geqslant 1$, *alors* $\mathcal{H}(\mathcal{M}) \geqslant s$.

La preuve de Good utilise fortement la finitude de $\mathcal{M}$: dans ce cas, les continuants de rang k sont tous compris entre a^k et b^k pour deux constantes a et b strictement plus grandes que 1; ainsi, les continuants de rang k ne sont pas trop différents entre eux, et il en est de même des longueurs des intervalles fondamentaux de rang k. Il est clair que cette preuve s'adapte tout à fait pour une période $\mathcal{M}$ de longueur l quelconque, pourvu que $\mathcal{M}$ soit finie.

Pour un indice k qui s'écrit $k = nl + i$ avec $i \in \{1, 2, ..., l\}$, et compte tenu de (23), l'expression de la mesure s-dimensionnelle du recouvrement de hauteur k prend la forme

$$\Lambda^{\langle k \rangle}_{\mathcal{M}, s} = \mathcal{G}_{\mathcal{M}(i), 2s} \circ \mathcal{G}^n_{\mathcal{M}, 2s} \left[\frac{1}{(1+z)^s} \right] (0).$$

On utilise alors les propriétés spectrales dominantes de l'opérateur $\mathcal{G}_{\mathcal{M}, 2s}$ et la minoration (35): pour tout s réel $s > p_{\mathcal{M}}$, il existe un nombre $B_s > 0$ pour lequel, pour tout z de l'intervalle $\mathcal{J}$, et pour tout $n \geqslant 1$, on a

$$\left| \mathcal{G}^n_{\mathcal{M}, 2s} \left[\frac{1}{(1+z)^s} \right] \right| \geqslant B_s \lambda(\mathcal{M}, 2s)^n.$$

Comme les opérateurs $\mathcal{G}_{\mathcal{M}(i), 2s}$ sont positifs, ils conservent le cône K défini en 2.2, et donc

$$\Lambda^{\langle k \rangle}_{\mathcal{M}, s} \geqslant B_s \lambda(\mathcal{M}, 2s)^n \, \mathcal{G}_{\mathcal{M}(i), 2s}[1](0).$$

Si $\mathcal{M}$ est finie, tous les continuants associés à un préfixe de $\mathcal{M}(k)$ sont majorés par une quantité de la forme C^k, pour une constante $C > 1$, et on obtient

$$\text{pour tout } i \in \{1, 2, ..., l\}, \qquad \mathcal{G}_{\mathcal{M}(i), 2s}[1](0) \geqslant \frac{1}{C^{2ls}},$$

d'où l'on déduit la minoration

$$\Lambda^{\langle k \rangle}_{\mathcal{M}, s} \geqslant \frac{B_s}{C^{2ls}} \lambda(\mathcal{M}, 2s)^n.$$

Soit maintenant un nombre réel s vérifiant $2s < s_{\mathcal{M}}$. Alors, puisque la fonction $s \to \lambda(\mathcal{M}, s)$ est strictement décroissante, la valeur propre dominante satisfait $\lambda(\mathcal{M}, 2s) > 1$. Ainsi, il suffit de choisir n suffisamment grand pour rendre la mesure s dimensionnelle $\Lambda^{\langle k \rangle}_{\mathcal{M}, s}$ plus grande que 1. On applique alors le résultat de Good qui montre que la dimension de Hausdorff $\mathcal{H}(\mathcal{M})$ de $\mathcal{R}(\mathcal{M})$ vérifie $\mathcal{H}(\mathcal{M}) \geqslant s$, ce qui permet de conclure la deuxième étape. ∎

Troisième étape. Les opérateurs $\mathcal{G}_{\mathcal{M}_N, 2s}$ associé aux troncatures $\mathcal{M}_N$ de la période convergent vers l'opérateur $\mathcal{G}_{\mathcal{M}, 2s}$, grâce à la majoration

$$\|\mathcal{G}_{\mathcal{M}_N, s} - \mathcal{G}_{\mathcal{M}, s}\| \leqslant \sum_{i=1}^{l} \left(\prod_{j \neq i} \zeta_{M_j}\left(\sigma, \frac{-1}{4}\right)\right)\left(\sum_{\substack{m > N \\ m \in M_i}} \frac{1}{(m-1/4)^{\sigma}}\right),$$

obtenue à l'aide de (24), (25) et (26) et valable pour tout $\sigma := \Re(s)$ supérieur à l'abscisse de convergence $p_{\mathcal{M}}$ de l'opérateur $\mathcal{G}_{\mathcal{M}, s}$. Comme chacun des termes

$$\sum_{\substack{m > N \\ m \in M_i}} \frac{1}{(m-1/4)^{s}}$$

tend vers 0 quand N tend vers l'infini, on conclut à la convergence de la suite $\mathcal{G}_{\mathcal{M}_N, s}$ vers $\mathcal{G}_{\mathcal{M}, s}$.

Dans un premier temps, on fixe le paramètre réel s, et on pose $\mathcal{L} := \mathcal{G}_{\mathcal{M}, 2s}$, $\mathcal{L}_N := \mathcal{G}_{\mathcal{M}_N, 2s}$. Lorsque $N \to \infty$, la suite $\mathcal{L}_N$ converge vers $\mathcal{L}$. Par ailleurs, dès que N est suffisamment grand, le cardinal de $\mathcal{M}_N$ devient au moins égal à 2, et on peut appliquer à $\mathcal{L}$ et aux $\mathcal{L}_N$ les résultats de la Section 2. Désignons par λ et λ_N les valeurs propres dominantes de $\mathcal{L}$ et de $\mathcal{L}_N$. Utilisant les expressions de λ_N et λ données en (37), on en déduit que la suite λ_N est une suite croissante et majorée par λ, elle converge donc. Le résultat de perturbation suivant, cité dans Hensley [He3], va permettre de montrer que la limite est nécessairement égale à λ.

Lemme 4. *Soient $\mathcal{B}$ un espace de Banach et $\mathcal{L}: \mathcal{B} \to \mathcal{B}$ un opérateur compact. On considère une valeur propre λ de $\mathcal{L}$ de multiplicité* 1. *Alors il existe une constante $\delta > 0$ pour laquelle tout opérateur $\mathcal{T}: \mathcal{B} \to \mathcal{B}$ vérifiant $\|\mathcal{T} - \mathcal{L}\| \leqslant \delta$ a une unique valeur propre dans le disque $|z - \lambda| \leqslant \delta$.*

Désignant par $\mathcal{P}$, $\mathcal{P}_N$ les projections sur les sous-espaces dominants, respectivement de $\mathcal{L}$, $\mathcal{L}_N$, on utilise le lemme pour montrer que par la suite $\mathcal{P}_N$ converge vers $\mathcal{P}$. En vertu de l'écriture

$$\mathcal{L} = \lambda \mathcal{P} + \mathcal{L}(I - \mathcal{P}), \qquad \mathcal{L}_N = \lambda_N \mathcal{P}_N + \mathcal{L}_N(I - \mathcal{P}_N),$$

on en déduit alors que la limite de la suite λ_N est égale à λ.

On fait maintenant varier s et on reprend les notations habituelles du travail. Chacune des applications $s \to \lambda(\mathcal{M}_N, s)$ est strictement décroissante et continue et on considère donc le point $s_{\mathcal{M}_N}$ pour lequel $\lambda(\mathcal{M}_N, s) = 1$. Comme la suite $N \to \lambda(\mathcal{M}_N, s)$ est croissante et majorée par $\lambda(\mathcal{M}, s)$, la suite des points $s_{\mathcal{M}_N}$ est croissante et majorée par $s_{\mathcal{M}}$. Par ailleurs, la monotonie de la suite $N \to \lambda(\mathcal{M}_N, s)$ permet d'affirmer que la convergence de $\lambda(\mathcal{M}_N, s)$ vers $\lambda(\mathcal{M}, s)$ est uniforme sur un intervalle fermé contenant $s_{\mathcal{M}}$. On déduit alors facilement que la suite $s_{\mathcal{M}_N}$ converge vers $s_{\mathcal{M}}$, ce qui compte tenu de la relation (45) permet de montrer le résultat final. ∎

On peut aussi prouver le résultat suivant, qui, à la connaissance de l'auteur, n'apparaît pas explicitement dans la littérature, même dans le cadre couramment étudié de la contrainte élémentaire finie:

PROPOSITION 7. *Soient deux contraintes périodiques $\mathcal{M}$ et $\mathcal{N}$ de même longueur et vérifiant l'inclusion stricte $\mathcal{M} \subset \mathcal{N}$. Alors, les valeurs propres dominantes des opérateurs de Ruelle–Mayer associés vérifient l'inégalité stricte*

$$\lambda(\mathcal{M}, s) < \lambda(\mathcal{N}, s),$$

et les dimensions de Hausdorff des ensembles $\mathcal{R}(\mathcal{M})$ et $\mathcal{R}(\mathcal{N})$ vérifient l'inegalité stricte

$$\mathcal{H}(\mathcal{M}) < \mathcal{H}(\mathcal{N}).$$

Preuve. Il suffit de montrer le résultat dans le cas particulier où les deux périodes $\mathcal{M}$ et $\mathcal{N}$ ne diffèrent que d'un élément, et on peut supposer, grâce à l'invariance par permutation circulaire prouvée dans la Proposition 1, que cet élément a est situé en queue de période. Donc $\mathcal{M}$ est de la forme $\mathcal{P} \times M$ tandis que $\mathcal{N}$ est de la forme $\mathcal{P} \times (M \cup \{m\})$. Voulant comparer les deux expressions $\mathcal{G}^n_{\mathcal{M},s}[1](0)$ et $\mathcal{G}^n_{\mathcal{N},s}[1](0)$ pour s fixé, nous adoptons des notations simplifiées:

$$\mathcal{L}_1 := \mathcal{G}_{\mathcal{M},s}, \qquad \mathcal{L}_2 := \mathcal{G}_{\mathcal{P},s} \circ \mathcal{G}_{\{m\},s}, \qquad \text{et ainsi} \qquad \mathcal{L}_1 + \mathcal{L}_2 = \mathcal{G}_{\mathcal{N},s}.$$

La formule du binôme (non commutative) appliquée à $(\mathcal{L}_1 + \mathcal{L}_2)^n\,[1](0)$ produit une somme de 2^n termes, et on regroupe dans cette somme les termes selon le nombre k d'occurrences de $\mathcal{L}_2$ qu'ils contiennent, ce qui correspond à étudier les C_n^k expressions de la forme

$$\mathcal{L}_1^{n_1} \circ \mathcal{L}_2^{n_2} \circ \cdots \circ \mathcal{L}_1^{m_1} \circ \mathcal{L}_2^{m_2}[1](0)$$

avec k occurrences de l'opérateur $\mathcal{L}_2$, $n-k$ occurrences de l'opérateur $\mathcal{L}_1$. Chacune de ces expressions peut contenir un nombre h variable de "groupes" avec $h \leqslant 2k+1$.

Les propriétés de positivité des opérateurs $\mathcal{L}_1$ et $\mathcal{L}_2$, et en particulier l'existence d'une valeur propre dominante λ_1 et λ_2 pour chacun d'entre eux permettent de montrer, via (35), l'existence d'une constante $a > 0$, (qu'on peut supposer vérifier $a \leqslant 1$) telle que, pour tout $p \geqslant 1$ et tout z de $\mathscr{J}$, on ait à la fois

$$\mathscr{L}_2^p[1](z) \geqslant a\lambda_2^p, \qquad \mathscr{L}_1^p[1](z) \geqslant a\lambda_1^p.$$

Chacune des C_n^k expressions contenant h groupes est alors minorée, pour tout n et tout $k \leqslant n$, par

$$a^h \lambda_1^{n-k} \lambda_2^k \geqslant a^{2k+1} \lambda_1^{n-k} \lambda_2^k.$$

On en déduit donc la minoration

$$(\mathscr{L}_1 + \mathscr{L}_2)^n [1](0) \geqslant a \sum_{k=0}^{n} C_n^k \lambda_1^{n-k} (a^2 \lambda_2)^k = a(\lambda_1 + a^2 \lambda_2)^n,$$

et, ainsi, grâce à (37), la valeur propre dominante λ de $\mathscr{L}_1 + \mathscr{L}_2$ vérifie donc $\lambda \geqslant \lambda_1 + a^2 \lambda_2$, ce qui donne le résultat annoncé. ∎

4. DENSITÉ DES RATIONNELS CONTRAINTS ET COMPLEXITÉ MOYENNE DE L'ALGORITHME D'EUCLIDE CONTRAINT

La section est consacrée à la preuve des résultats (ii) et (iv). Les rationnels contraints ont été essentiellement étudiés par Cusick [Cu] et Hensley [He1]. Le premier, Cusick fait le lien entre l'étude des rationnels contraints et l'abscisse de convergence de la série de Dirichlet $(I - \mathscr{G}_{\mathscr{M},s})^{-1}[1](0)$. Mais il obtient seulement un équivalent asymptotique du logarithme de la densité. Par la suite, Hensley établit l'équivalent asymptotique du nombre de rationnels $\mathscr{M}$-contraints, dans le cas d'une contrainte élémentaire finie, dans une preuve longue et complexe. Il semble que le comportement moyen de l'algorithme d'Euclide contraint n'ait guère retenu l'attention. À la connaissance de l'auteur, les arguments taubériens n'ont jamais été employés dans l'étude des rationnels, à l'exception de l'auteur [FV] qui les a déjà utilisés dans le cas non-contraint, comme une alternative à la preuve des résultats d'Heilbronn [Hei] et Dixon [Di].

On veut donc étudier l'ensemble

$$\mathscr{Q}_N(\mathscr{M}) := \{(p, q) \mid p/q \in \mathscr{Q}(\mathscr{M}),\ 1 \leqslant p \leqslant q \leqslant N,\ \gcd(p, q) = 1\}.$$

On introduit des ensembles plus restreints où le dénominateur n est fixé,

$$\omega_n(\mathscr{M}) := \{p \mid p/n \in \mathscr{Q}(\mathscr{M}),\ 1 \leqslant p \leqslant n,\ \gcd(p, n) = 1\},$$

et on a clairement

$$\mathcal{Q}_N(\mathcal{M}) = \bigcup_{n \leqslant N} \omega_n(\mathcal{M}).$$

Les deux variables aléatoires $x_n(\mathcal{M})$ et $X_N(\mathcal{M})$ mesurent la hauteur du développement en fraction continue propre (i.e., ne finissant pas par 1), respectivement sur $\omega_n(\mathcal{M})$ et sur $\mathcal{Q}_N(\mathcal{M})$. On désigne par $v_{\mathcal{M},n}^{\langle k \rangle}$ le nombre d'éléments p de $\omega_n(\mathcal{M})$ pour lesquels $x_n(\mathcal{M})(p) = k$. Pour tout k fixé ($k \geqslant 1$), on considère la série de Dirichlet associée à la variable de comptage $v_{\mathcal{M},n}^{\langle k \rangle}$,

$$A_{\mathcal{M}}^{\langle k \rangle}(s) := \sum_{n \geqslant 1} \frac{v_{\mathcal{M},n}^{\langle k \rangle}}{n^s},$$

puis on introduit la série génératrice des $A_{\mathcal{M}}^{\langle k \rangle}(s)$ qui va fournir la série génératrice double des $v_{\mathcal{M},n}^{\langle k \rangle}$,

$$S_{\mathcal{M}}(s, u) := \sum_{k \geqslant 1} u^k A_{\mathcal{M}}^{\langle k \rangle}(s) = \sum_{n \geqslant 1} \frac{1}{n^s} \sum_{k \geqslant 1} u^k v_{\mathcal{M},n}^{\langle k \rangle}.$$

Sous cette dernière forme, il est clair que $S_{\mathcal{M}}(s, u)$ est une série de Dirichlet par rapport à la variable s, dont le terme générale $S_{\mathcal{M},n}(u)$ est la série génératrice associée à la variable hauteur

$$S_{\mathcal{M},n}(u) := \sum_{k \geqslant 1} u^k v_{\mathcal{M},n}^{\langle k \rangle}.$$

En particulier,

$$S_{\mathcal{M},n}(1) = |\omega_n(\mathcal{M})| \qquad \text{et} \qquad \sum_{n \leqslant N} S_{\mathcal{M},n}(1) = |\mathcal{Q}_N(\mathcal{M})|. \tag{46}$$

L'évaluation de l'espérance des variables aléatoires $x_n(\mathcal{M})$ et $X_{\mathcal{M},n}$ fait intervenir les séries génératrices dérivées

$$T_{\mathcal{M}}(s, u) := \frac{\partial S_{\mathcal{M}}(s, u)}{\partial u} = \sum_{n \geqslant 1} \frac{1}{n^s} \sum_{k \geqslant 1} k u^{k-1} v_{\mathcal{M},n}^{\langle k \rangle},$$

et

$$T_{\mathcal{M},n}(u) := S'_{\mathcal{M},n}(u) = \sum_{k \geqslant 1} k u^{k-1} v_{\mathcal{M},n}^{\langle k \rangle}$$

par les formules

$$E[x_n(\mathscr{M})] = \frac{T_{\mathscr{M},n}(1)}{S_{\mathscr{M},n}(1)}, \qquad E[X_N(\mathscr{M})] = \frac{\sum_{n \leqslant N} T_{\mathscr{M},n}(1)}{\sum_{n \leqslant N} S_{\mathscr{M},n}(1)}. \tag{47}$$

Ainsi l'espérance de $x_n(\mathscr{M})$, comme le cardinal $|\omega_n(\mathscr{M})|$ sont les coefficients des séries de Dirichlet $S_{\mathscr{M}}(s, 1)$ et $T_{\mathscr{M}}(s, 1)$. Il est bien connu que les théorèmes classiques—en particulier les théorèmes taubériens—permettent seulement d'obtenir des informations sur la somme des N premiers coefficients d'une telle série de Dirichlet. C'est pourquoi on cherche plutôt, par la suite, à évaluer l'espérance de $X_n(\mathscr{M})$, comme celle du cardinal $|\mathscr{Q}_N(\mathscr{M})|$.

Les deux résultats suivants montrent que les séries de Dirichlet $S_{\mathscr{M}}(s, 1)$ et $T_{\mathscr{M}}(s, 1)$ s'expriment en fonction des opérateurs de Ruelle–Mayer contraints.

Proposition 8. *Pour tout $k \geqslant 1$, on a*

$$A_{\mathscr{M}}^{\langle k \rangle}(s) = \mathscr{G}_{\mathscr{M}_\star(k), s}[1](0),$$

où $\mathscr{M}_\star(k)$ désigne l'ensemble des préfixes de longueur k de $\langle \mathscr{M} \rangle$ ne finissant pas par le chiffre 1.

Preuve. L'entier $v_{\mathscr{M},n}^{\langle k \rangle}$ représente exactement le nombre de fois où l'entier n est un continuant d'ordre k associé à un développement en fraction continue $\mathscr{M}$-valide et propre (i.e., ne finissant pas par le chiffre 1). Plus précisément, $v_{n,\mathscr{M}}^{\langle k \rangle}$ est le nombre de k-uplets $m = (m_1, m_2, ..., m_k)$ qui vérifient les trois conditions

$$n = Q_k(m_1, m_2, ..., m_k), \qquad m \in \mathscr{M}(k), \quad m_k \neq 1.$$

On en déduit de ce qui précède

$$A_{\mathscr{M}}^{\langle k \rangle}(s) := \sum_{n \geqslant 1} \frac{v_{\mathscr{M},n}^{\langle k \rangle}}{n^s} = \sum_{m \in \mathscr{M}_\star(k)} \frac{1}{Q_k^s}.$$

En utilisant la relation (21), on obtient le résultat cherché. ∎

Proposition 9. *Dans le cas d'une contrainte de période $\mathscr{M}$, les deux séries de Dirichlet génératrices des objets étudiés s'expriment en fonction de l'opérateur de Ruelle–Mayer $\mathscr{G}_{\mathscr{M},s}$ associé à la période*:

$$S_{\mathscr{M}}(s, 1) = \mathscr{C}_{\mathscr{M},s}(I - \mathscr{G}_{\mathscr{M},s})^{-1}[1](0)$$

$$T_{\mathscr{M}}(s, 1) = l\mathscr{C}_{\mathscr{M},s}(I - \mathscr{G}_{\mathscr{M},s})^{-2}\,\mathscr{G}_{\mathscr{M},s}[1](0) + \mathscr{D}_{\mathscr{M},s}(I - \mathscr{G}_{\mathscr{M},s})^{-1}[1](0).$$

Les opérateurs $\mathscr{C}_{\mathscr{M},s}$ *et* $\mathscr{D}_{\mathscr{M},s}$ *font intervenir les préfixes propres* $\mathscr{M}_\star(i)$ *pour* $1 \leqslant i \leqslant l$ *sous la forme suivante*:

$$\mathscr{C}_{\mathscr{M},s} := \sum_{i=1}^{l} \mathscr{G}_{\mathscr{M}_\star(i),s}, \qquad \mathscr{D}_{\mathscr{M},s} := \sum_{i=1}^{l} i\mathscr{G}_{\mathscr{M}_\star(i),s}.$$

Preuve. Comme l'ensemble de contraintes est périodique, de période l, on écrit l'indice k sous la forme $k = nl + i$ avec $i \in \{1 \cdots l\}$, et en utilisant (23), on obtient

$$\sum_{k\geqslant 1} u^k \mathscr{G}_{\mathscr{M}_\star(k),s} = \sum_{n\geqslant 0} u^{nl} \left(\sum_{i=1}^{l} u^i \mathscr{G}_{\mathscr{M}_\star(i),s} \right) \mathscr{G}^n_{\mathscr{M},s},$$

et donc, en appliquant à la fonction constante 1 au point 0, on obtient

$$\begin{aligned} S_{\mathscr{M}}(s,u) &= \left(\sum_{i=1}^{l} u^i \mathscr{G}_{\mathscr{M}_\star(i),s} \right) \left(\sum_{n\geqslant 0} u^{ln} \mathscr{G}^n_{\mathscr{M},s} \right) [1](0) \\ &= \left(\sum_{i=1}^{l} u^i \mathscr{G}_{\mathscr{M}_\star(i),s} \right) (I - u^l \mathscr{G}_{\mathscr{M},s})^{-1} [1](0) \end{aligned}$$

qui donne le premier résultat en choisissant $u = 1$, et le second résultat en dérivant par rapport à la variable u, puis en choisissant $u = 1$. ∎

Le principal outil pour étudier le comportement asymptotique des expressions étudiées (46) et (47) est alors le théorème taubérien suivant, dû à Delange [De] qui permet de relier ce comportement aux singularités des séries de Dirichlet $S_{\mathscr{M}}(s, 1)$ et $T_{\mathscr{M}}(s, 1)$.

Théorème Taubérien. *Soit* $F(s)$ *une série de Dirichlet à termes* a_n *positifs ou nuls, convergeant pour* $\Re(s) > \sigma > 0$. *Soit* w *un nombre réel vérifiant* $w > -1$. *On suppose que* F *vérifie les deux hypothèse suivantes*

(i) *F est holomorphe en tout point de la droite $\Re(s) = \sigma$ autres que σ*:

(ii) *au voisinage de σ et pour $\Re(s) > \sigma$, F s'écrit*

$$F(s) = \frac{g(s)}{(s-\sigma)^{w+1}} + h(s),$$

où g et h sont holomorphes en σ, avec $g(\sigma) \neq 0$.

Alors on a, lorsque $N \to \sigma$,

$$\sum_{n \leqslant N} a_n = \frac{g(\sigma)}{\sigma \Gamma(w+1)} N^\sigma \log^w N [1 + \varepsilon(N)].$$

Pour pouvoir appliquer ce théorème aux deux séries de Dirichlet $S_{\mathcal{M}}(s, 1)$ et $T_{\mathcal{M}}(s, 1)$, il faut donc vérifier que ces séries satisfont les hypothèses du Théorème Taubérien. Compte tenu des expressions obtenues dans la Proposition 9, la preuve repose sur les propriétés spectrales de l'opérateur $\mathcal{G}_{\mathcal{M}, s}$ et celles de sa valeur dominante $\lambda(\mathcal{M}, s)$. En particulier, le nombre $s_{\mathcal{M}}$ qui vérifie $\lambda(\mathcal{M}, s_{\mathcal{M}}) = 1$ fournira le pôle dominant des séries génératrices étudiées. Grâce aux propriétés de perturbation, ces fonctions seront méromorphes au voisinage de ce pôle dominant.

THÉORÈME 2. *Les séries de Dirichlet* $S_{\mathcal{M}}(s, 1)$ *et* $T_{\mathcal{M}}(s, 1)$ *vérifient les hypothèses du Théorème Taubérien; le paramètres correspondant sont* $\sigma = s_{\mathcal{M}}$ *et* $w = 0$ *pour* $S_{\mathcal{M}}(s, 1)$, $\sigma = s_{\mathcal{M}}$ *et* $w = 1$ *pour* $T_{\mathcal{M}}(s, 1)$.

L'exposant de la densité de rationnels p/q *ayant un développement en fraction continue* $\mathcal{M}$*-valide et vérifiant* $1 \leqslant p \leqslant q \leqslant N$, $\text{pgcd}(p, q) = 1$ *est asymptotiquement égal à, pour* $N \to \infty$

$$|\mathcal{Q}_N(\mathcal{M})| \sim c_{\mathcal{M}} N^{s_{\mathcal{M}}}.$$

La hauteur moyenne du développement en fraction continue d'un rationnel $\mathcal{M}$*-valide et vérifiant* $1 \leqslant p \leqslant q \leqslant N$, $\text{pgcd}(p, q) = 1$ *vaut asymptotiquement, pour* $N \to \infty$

$$E[X_N(\mathcal{M})] \sim \frac{-l}{\lambda'(\mathcal{M}, s_{\mathcal{M}})} \log N,$$

où l *désigne la longueur de la période, et* $\lambda'(\mathcal{M}, s)$ *représente la dérivée par rapport à* s *de l'application* $s \to \lambda(\mathcal{M}, s)$.

Preuve. Sur tout le demi-plan pointé $\mathcal{P} := \{s \mid \Re(s) \geqslant s_{\mathcal{M}}, s \neq s_{\mathcal{M}}\}$, et d'après la Proposition 5, le rayon spectral $R(\mathcal{M}, s)$ de $\mathcal{G}_{\mathcal{M}, s}$ est strictement inférieur à 1. L'opérateur $I - \mathcal{G}_{\mathcal{M}, s}$ est donc inversible, et définit des fonctions $s \to (I - \mathcal{G}_{\mathcal{M}, s})^{-1}$ et $s \to (I - \mathcal{G}_{\mathcal{M}, s})^{-2}$ holomorphes. On rappelle les expressions de $S_{\mathcal{M}}(s, 1)$ et $T_{\mathcal{M}}(s, 1)$ obtenues dans la Proposition 9,

$$S_{\mathcal{M}}(s, 1) = \mathcal{C}_{\mathcal{M}, s}(I - \mathcal{G}_{\mathcal{M}, s})^{-1}[1](0),$$
$$T_{\mathcal{M}}(s, 1) = l\mathcal{C}_{\mathcal{M}, s}(I - \mathcal{G}_{\mathcal{M}, s})^{-2}\mathcal{G}_{\mathcal{M}, s}[1](0) + \mathcal{D}_{\mathcal{M}, s}(I - \mathcal{G}_{\mathcal{M}, s})^{-1}[1](0),$$

avec

$$\mathcal{C}_{\mathcal{M}, s} := \sum_{i=1}^{l} \mathcal{G}_{\mathcal{M}_\star(i), s}, \qquad \mathcal{D}_{\mathcal{M}, s} := \sum_{i=1}^{l} i\mathcal{G}_{\mathcal{M}_\star(i), s}.$$

Comme les fonctions $s \to \mathcal{C}_{\mathcal{M}, s}$ et $s \to \mathcal{D}_{\mathcal{M}, s}$ sont aussi holomorphes, il en est de même des fonctions $s \to S_{\mathcal{M}}(s, 1)$ et $s \to T_{\mathcal{M}}(s, 1)$ sur le demi-plan pointé $\mathcal{P}$.

Ainsi, $S_{\mathscr{M}}(s,1)$ et $T_{\mathscr{M}}(s,1)$ vérifient l'hypothèse (i) du Théorème Taubérien pour $\sigma = s_{\mathscr{M}}$.

On se place maintenant dans un voisinage Ω de $\sigma = s_{\mathscr{M}}$, et on utilise le principe de Perturbation de la Proposition 3. Posant

$$c(s) := e_{\mathscr{M},s}[1]\, \mathscr{C}_{\mathscr{M},s}[f_{\mathscr{M},s}](0), \qquad d(s) := e_{\mathscr{M},s}[1]\, \mathscr{D}_{\mathscr{M},s}[f_{\mathscr{M},s}](0),$$

où $e_{\mathscr{M},s}$ et $f_{\mathscr{M},s}$ sont les objets dominants de la Proposition 1, on définit des fonctions c et d holomorphes sur Ω. Comme de plus les opérateurs $\mathscr{C}_{\mathscr{M},s}$ et $\mathscr{D}_{\mathscr{M},s}$ sont positifs (au sens de la conservation du cône K défini en 2.2), ces fonctions c et d sont strictement positives sur $\Omega \cap \mathbf{R}$. On réécrit alors (36) en

$$\mathscr{C}_{\mathscr{M},s} \circ \mathscr{G}^k_{\mathscr{M},s}[1](0) = c(s)\, \lambda(\mathscr{M},s)^k + \mathscr{C}_{\mathscr{M},s} \circ \mathscr{N}^k_{\mathscr{M},s}[1](0),$$

$$\mathscr{D}_{\mathscr{M},s} \circ \mathscr{G}^k_{\mathscr{M},s}[1](0) = d(s)\, \lambda(\mathscr{M},s)^k + \mathscr{D}_{\mathscr{M},s} \circ \mathscr{N}^k_{\mathscr{M},s}[1](0),$$

pour tout $k \geqslant 1$. Sur $\Omega \cap \mathscr{P}$, le rayon spectral $R(\mathscr{M},s)$, égal au module $|\lambda(\mathscr{M},s)|$ de la valeur propre dominante, est strictement inférieur à 1: il en est a fortiori de même pour le rayon spectral de $\mathscr{N}_{\mathscr{M},s}$. On peut alors écrire, pour $s \in \Omega \cap \mathscr{P}$

$$S_{\mathscr{M}}(s,1) = \frac{c(s)}{1-\lambda(\mathscr{M},s)} + \mathscr{C}_{\mathscr{M},s}(I - \mathscr{N}_{\mathscr{M},s})^{-1}\,[1](0),$$

$$T_{\mathscr{M}}(s,1) = \frac{lc(s)\,\lambda(\mathscr{M},s)}{(1-\lambda(\mathscr{M},s))^2} + \frac{d(s)}{1-\lambda(\mathscr{M},s)}$$
$$+ \mathscr{C}_{\mathscr{M},s}(I - \mathscr{N}_{\mathscr{M},s})^{-2}\, \mathscr{N}_{\mathscr{M},s}[1](0) + \mathscr{D}_{\mathscr{M},s}(I - \mathscr{N}_{\mathscr{M},s})^{-1}\,[1](0).$$

Au voisinage de $s = s_{\mathscr{M}}$, la dérivabilité de $s \to \lambda(\mathscr{M},s)$ permet d'écrire

$$\frac{s - s_{\mathscr{M}}}{1-\lambda(\mathscr{M},s)} = -\frac{H(s)}{\lambda'(\mathscr{M},s_{\mathscr{M}})} \qquad \text{avec } H \text{ holomorphe vérifiant } H(s_{\mathscr{M}}) = 1.$$

Pour des raisons similaires aux précédentes, les termes-reste définissent des fonctions holomorphes sur $\Omega \cap \mathscr{P}$, et finalement on écrit

$$S_{\mathscr{M}}(s,1) := \frac{-c(s)\,H(s)}{\lambda'(\mathscr{M},s_{\mathscr{M}})}\,\frac{1}{(s-s_{\mathscr{M}})} + C_1(s),$$

$$T_{\mathscr{M}}(s,1) := \frac{lc(s)\,\lambda(\mathscr{M},s) + d(s)(1-\lambda(\mathscr{M},s))}{\lambda'(\mathscr{M},s_{\mathscr{M}})^2}\,\frac{H^2(s)}{(s-s_{\mathscr{M}})^2} + D_1(s),$$

où C_1 et D_1 sont holomorphes sur $\Omega \cap \mathscr{P}$. Ainsi, $S_{\mathscr{M}}(s, 1)$ et $T_{\mathscr{M}}(s, 1)$ vérifient les hypothèses (ii) du Théorème Taubérien avec $\sigma = s_{\mathscr{M}}$. En appliquant ce théorème à $S_{\mathscr{M}}(s, 1)$ et à $T_{\mathscr{M}}(s, 1)$ on obtient

$$\sum_{n \leqslant N} S_{\mathscr{M}, n}(1) \simeq \frac{-c(s_{\mathscr{M}})}{s_{\mathscr{M}} \lambda'(\mathscr{M}, s_{\mathscr{M}})} N^{s_{\mathscr{M}}}$$

$$\sum_{n \leqslant N} T_{\mathscr{M}, n}(1) \simeq \frac{lc(s_{\mathscr{M}})}{s_{\mathscr{M}} \lambda'(\mathscr{M}, s_{\mathscr{M}})^2} S^{s_{\mathscr{M}}} \log N.$$

Compte tenu des expressions (46) et (47), la première relation fournit le premier résultat du théorème et le quotient des deux relations en fournit le second. ∎

5. IRRATIONNELS QUADRATIQUES CONTRAINTS

On veut donc étudier le cardinal de l'ensemble

$$\mathscr{I}_N(\mathscr{M}) := \{x \mid x \in \mathscr{I}(\mathscr{M}), \varepsilon(x) \leqslant N\}$$

ainsi que les variables aléatoires $Y_N(\mathscr{M})$ et $Z_N(\mathscr{M})$ qui mesurent respectivement la période du développement en fraction continue et la constante de Lévy sur $\mathscr{I}_N(\mathscr{M})$. Ces problèmes ont été abordés par Faivre [Fa] et Pollicott [Po], dans le cas non-contraint, avec des méthodes utilisant les déterminants de Fredholm. Cette section se présente à la fois comme une généralisation de ces résultats au cas contraint et une unification de ces méthodes. De fait, dans un premier temps, on va travailler non pas sur les irrationnels de $\mathscr{I}(\mathscr{M}$, mais sur les éléments m de $\mathscr{M}^*$. Cela permettra d'exprimer les séries génératrices de Dirichlet en fonction de déterminants de Fredholm associés aux opérateurs de Ruelle–Mayer contraints. On pourra, alors dans un deuxième temps, appliquer un théorème taubérien qui permettra de traiter le problème sur les mots. On reviendra dans un troisième temps aux irrationnels eux-mêmes.

Première étape. On utilise donc dans ce premier temps les définitions des grandeurs α, ε et r non plus sur les irrationnels quadratiques de $\mathscr{I}(\mathscr{M})$, mais sur les mots de $\mathscr{M}^*$. On étudie alors le cardinal de l'ensemble

$$\tilde{\mathscr{I}}_N(\mathscr{M}) := \{m \in \mathscr{M}^*, \varepsilon(m) \leqslant N\},$$

ainsi que les variables aléatoires $\tilde{Y}_N(\mathscr{M}$ et $\tilde{Z}_N(\mathscr{M}$ qui mesurent respectivement la longueur $|m|$ d'un mot m et la constante de Lévy $\beta(m)$ de ce mot (définie en (9) et (12)) sur $\mathscr{I}_N(\mathscr{M})$.

Pour tout k fixé ($k \geqslant 1$), on considère la quantité

$$I_{\mathscr{M}}^{\langle k \rangle}(s) := \sum_{m \in \mathscr{M}^k} \varepsilon^{-s}(m),$$

puis on introduit la série génératrice des $I_{\mathscr{M}}^{\langle k \rangle}(s)$,

$$\mathscr{I}_{\mathscr{M}}(s, u) := \sum_{k \geqslant 1} \frac{u^k}{k} I_{\mathscr{M}}^{\langle k \rangle}(s) = \sum_{k \geqslant 1} \frac{u^k}{k} \sum_{m \in \mathscr{M}^k} \varepsilon^{-s}(m),$$

et les trois autres séries reliées, construites par dérivation à partir de cette dernière et analogues des séries $S_{\mathscr{M}}(s, u)$ et $T_{\mathscr{M}}(s, u)$ de la Section 4 définies en (43) et (45),

$$U_{\mathscr{M}}(s, u) := \frac{\partial}{\partial u} \mathscr{I}_{\mathscr{M}}(s, u) := \sum_{k \geqslant 1} u^{k-1} I_{\mathscr{M}}^{\langle k \rangle}(s) = \sum_{k \geqslant 1} u^{k-1} \sum_{m \in \mathscr{M}^k} \varepsilon^{-s}(m), \quad (48)$$

$$V_{\mathscr{M}}(s, u) := \frac{\partial^2}{\partial u^2} \mathscr{I}_{\mathscr{M}}(s, u) := \sum_{k \geqslant 1} (k-1)\, u^{k-2}\, I_{\mathscr{M}}^{\langle k \rangle}(s)$$

$$= \sum_{k \geqslant 1} (k-1)\, u^{k-2} \sum_{m \in \mathscr{M}^k} \varepsilon^{-s}(m), \quad (49)$$

et

$$W_{\mathscr{M}}(s, u) := \frac{-\partial}{\partial s} \mathscr{I}_{\mathscr{M}}(s, u) := -\sum_{k \geqslant 1} \frac{u^k}{k} \frac{\partial}{\partial s} I_{\mathscr{M}}^{\langle k \rangle}(s)$$

$$= \sum_{k \geqslant 1} \frac{u^k}{k} \sum_{m \in \mathscr{M}^k} \log \varepsilon(m)\, \varepsilon^{-s}(m). \quad (50)$$

En particulier,

$$U_{\mathscr{M}}(s, 1) = \sum_{m \in \mathscr{M}^*} \varepsilon^{-s}(m), \quad (51)$$

sera utilisée pour déterminer le cardinal $|\tilde{I}_N(\mathscr{M})|$, tandis que

$$V_{\mathscr{M}}(s, 1) = \sum_{k \geqslant 1} (k-1) \sum_{m \in \mathscr{M}^k} \varepsilon^{-s}(m), \quad (52)$$

est reliée à l'évaluation de l'espérance de la variable aléatoire $\tilde{Y}_N(\mathscr{M})$; enfin, l'étude de l'espérance de la variable aléatoire $\tilde{Z}_N(\mathscr{M})$ fera intervenir

$$W_{\mathscr{M}}(s,1) = \sum_{k \geqslant 1} \frac{1}{k} \sum_{m \in \mathscr{M}^k} \log \varepsilon(m)\, \varepsilon^{-s}(m). \tag{53}$$

Les deux résultats suivants montrent que ces trois séries de Dirichlet généralisées $U_{\mathscr{M}}(s,1)$, $V_{\mathscr{M}}(s,1)$ et $W_{\mathscr{M}}(s,1)$, définies en (48), (49) et (50), s'expriment en fonction des opérateurs de Ruelle–Mayer contraints.

PROPOSITION 10. *Si la longueur de la période $\mathscr{M}$ est paire, on a, pour tout $k \geqslant 1$,*

$$I_{\mathscr{M}}^{\langle k \rangle}(s) = \operatorname{Tr} \mathscr{G}^k_{\mathscr{M},s} - \operatorname{Tr} \mathscr{G}^k_{\mathscr{M},s+2}.$$

Si la longueur l de la période est impaire, il y a deux cas à distinguer selon la parité de k

$$\begin{aligned} &\textit{pour } k \textit{ pair}, && I_{\mathscr{M}}^{\langle k \rangle}(s) = \operatorname{Tr} \mathscr{G}^k_{\mathscr{M},s} - \operatorname{Tr} \mathscr{G}^k_{\mathscr{M},s+2}, \\ &\textit{pour } k \textit{ impair}, && I_{\mathscr{M}}^{\langle k \rangle}(s) = \operatorname{Tr} \mathscr{G}^k_{\mathscr{M},2s} + \operatorname{Tr} \mathscr{G}^k_{\mathscr{M},2s+2}. \end{aligned} \tag{54}$$

Preuve. Le point de départ est l'identité de la trace, vue en (31)

$$\sum_{m \in \mathscr{M}^k} \alpha^s(m) = \operatorname{Tr} \mathscr{G}^k_{\mathscr{M},s} - (-1)^{kl} \operatorname{Tr} \mathscr{G}^k_{\mathscr{M},s+2},$$

ainsi que la relation (12) qui relie les deux grandeurs $\alpha(m)$ et $\varepsilon(m)$. Si la longueur l de la période est paire, il en est de même de tous les multiples lk et l'entier $r(m)$ est toujours égal à 1. Si la longueur l de la période est impaire, la parité de lk est égale à celle de k. Si k est pair, on retrouve la même formule que précédemment. Sinon, si k est impair, alors $r(m) = 2$, ce qui change s en $2s$ et le $-$ en $+$. ∎

PROPOSITION 11. *Dans le cas d'une contrainte de période $\mathscr{M}$, les trois séries de Dirichlet génératrices des objets étudiés s'expriment en fonction des dérivées logarithmiques, première et seconde, de déterminants de Fredholm liés à l'opérateur de Ruelle–Mayer $\mathscr{G}_{\mathscr{M},s}$ associé à la période aux points s, $2s$, $s+2$ et $2s+2$.*

Preuve. On rappelle l'identité qui détermine le déterminant de Fredholm,

$$\mathscr{F}_{\mathscr{M}}(s,u) := -\log \det(I - u\mathscr{G}_{\mathscr{M},s}) = \sum_{k=1}^{\infty} \frac{u^k}{k} \operatorname{Tr} \mathscr{G}^k_{\mathscr{M},s},$$

et on introduit les trois dérivées

$$\mathscr{A}_{\mathscr{M}}(s,u) := \frac{\partial}{\partial u}\mathscr{F}_{\mathscr{M}}(s,u),$$
$$\mathscr{B}_{\mathscr{M}}(s,u) := \frac{\partial^2}{\partial^2 u}\mathscr{F}_{\mathscr{M}}(s,u), \tag{55}$$
$$\mathscr{E}_{\mathscr{M}}(s,u) := -\frac{\partial}{\partial s}\mathscr{F}_{\mathscr{M}}(s,u).$$

Il y a de nouveau deux cas selon la parité de la longueur l de la période de la contrainte. Dans le premier cas (l pair), on obtient

$$\text{Pour } l \text{ pair} \qquad \mathscr{I}_{\mathscr{M}}(s,u) = \mathscr{F}_{\mathscr{M}}(s,u) - \mathscr{F}_{\mathscr{M}}(s+2,u).$$

Dans le deuxième cas, il faut différencier selon la parité de k. La partie paire de $\mathscr{I}_{\mathscr{M}}(s,u)$ est égale à la partie paire de $\mathscr{F}_{\mathscr{M}}(s,u) - \mathscr{F}_{\mathscr{M}}(s+2,u)$, tandis que la partie impaire de $\mathscr{I}_{\mathscr{M}}(s,u)$ est égale à la partie impaire de $\mathscr{F}_{\mathscr{M}}(2s,u) + \mathscr{F}_{\mathscr{M}}(2s+2,u)$. On obtient ainsi

Pour l impair

$$2\mathscr{I}_{\mathscr{M}}(s,u) = [\mathscr{F}_{\mathscr{M}}(s,u) + \mathscr{F}_{\mathscr{M}}(s,-u) + \mathscr{F}_{\mathscr{M}}(s+2,u) + \mathscr{F}_{\mathscr{M}}(s+2,-u)]$$
$$+ [\mathscr{F}_{\mathscr{M}}(2s,u) - \mathscr{F}_{\mathscr{M}}(2s,-u) + \mathscr{F}_{\mathscr{M}}(2s+2,u) - \mathscr{F}_{\mathscr{M}}(2s+2,-u)].$$

Il reste à dériver les expressions pour relier les quantités $U_{\mathscr{M}}(s,u)$, $V_{\mathscr{M}}(s,u)$, $W_{\mathscr{M}}(s,u)$ définies en (48), (49) et (50) aux quantités $\mathscr{A}_{\mathscr{M}}(s,u)$, $\mathscr{B}_{\mathscr{M}}(s,u)$ et $\mathscr{E}_{\mathscr{M}}(s,u)$ définies en (55); puis on choisit $u=1$. ∎

Deuxième étape. On cherche maintenant à évaluer les espérances de $\tilde{Y}_N(\mathscr{M})$ et $\tilde{Z}_N(\mathscr{M})$, comme celle du cardinal $|\tilde{\mathscr{I}}_N(\mathscr{M})|$. Le principal outil pour étudier le comportement asymptotique de telles expressions est alors le Théorème Taubérien suivant, qui constitue une forme un peu plus générale du Théorème Taubérien de la section précédente.

THÉORÈME TAUBEORIEN. *Soit $F(s)$ une fonction qui admet dans le demi-plan $\Re(s) > \sigma > 0$ la représentation*

$$F(s) = s\int_0^{\infty} A(x)\, e^{-sx}\, dx$$

où A est une fonction positive monotone croissante. Soit w un nombre réel vérifiant $w > -1$. On suppose que F vérifie les deux hypothèses suivantes

(i) *F est holomorphe en tout point de la droite* $\Re(s)=\sigma$ *autres que* σ:

(ii) *au voisinage de* σ *et pour* $\Re(s)>\sigma$, *F s'écrit*

$$F(s)=\frac{g(s)}{(s-\sigma)^{w+1}}+h(s),$$

où g et h sont holomorphes en σ, *avec* $g(\sigma)\neq 0$.

Alors on a, lorsque $x\to\infty$,

$$A(x)=\frac{g(\sigma)}{\sigma\Gamma(w+1)}\,e^{x\sigma}x^{w}[1+\varepsilon(x)].$$

On va appliquer ce théorème aux trois fonctions $U_{\mathscr{M}}(s,1)$, $V_{\mathscr{M}}(s,1)$ et $W_{\mathscr{M}}(s,1)$. Ces fonctions ont bien la forme cherchée et les grandeurs A relatives à ces fonctions sont respectivement

$$A_U(x):=\sum_{\substack{m\in\mathscr{M}^*\\ \log\varepsilon(m)\leqslant x}}1,$$

$$A_V(x):=\sum_{k\geqslant 1}(k-1)\sum_{\substack{m\in\mathscr{M}^k\\ \log\varepsilon(m)\leqslant x}}1,$$

$$A_W(x):=\sum_{k\geqslant 1}\frac{1}{k}\sum_{\substack{m\in\mathscr{M}^k\\ \log\varepsilon(m)\leqslant x}}\log\varepsilon(m).$$

Les deux premiers objets étudiés sont exactement

$$|\tilde{\mathscr{I}}_N(\mathscr{M})|=A_U(\log N),\qquad E[\tilde{Y}_N(\mathscr{M})]=\frac{lA_V(\log N)}{A_U(\log N)},\tag{56}$$

et le troisième objet $E(\tilde{Z}_N(\mathscr{M})]$ est relié de très près à

$$\frac{1}{l}\frac{A_W(\log N)}{A_U(\log N)}.\tag{57}$$

Il faut ensuite vérifier que ces séries satisfont les hypothèses du Théorème Taubérien. Compte tenu des expression de la Proposition 11, la preuve repose sur les propriétés spectrales de l'opérateur $\mathscr{G}_{\mathscr{M},s}$, et celles de sa valeur propre dominante $\lambda(\mathscr{M},s)$. En particulier, le nombre $s_{\mathscr{M}}$ qui vérifie $\lambda(\mathscr{M},s_{\mathscr{M}})=1$ fournira le pôle dominant des séries génératrices étudiées.

Grâce aux propriétés de perturbation, ces fonctions seront méromorphes au voisinage de ce pôle dominant.

THÉORÈME 3. *Les fonctions* $U_{\mathcal{M}}(s, 1)$, $V_{\mathcal{M}}(s, 1)$ *et* $W_{\mathcal{M}}(s, 1)$ *vérifient les hypothèses du Théorème Taubérien; les paramètres correspondant sont* $\sigma = s_{\mathcal{M}}$ *et* $w = 0$ *pour* $U_{\mathcal{M}}(s, 1)$ *et* $W_{\mathcal{M}}(s, 1)$, $\sigma = s_{\mathcal{M}}$ *et* $w = 1$ *pour* $V_{\mathcal{M}}(s, 1)$.

L'exposant de la densité des irrationnels quadratiques ayant un développement en fraction continue $\mathcal{M}$*-valide et vérifiant* $\varepsilon(x) \leqslant N$ *est asymptotiquement égal à, pour* $N \to \infty$

$$|\mathcal{I}_N(\mathcal{M})| \sim d_{\mathcal{M}} N^{s_{\mathcal{M}}} n$$

pour une constante ne dépendant que de $\mathcal{M}$.

La période moyenne du développement en fraction continue d'un irrationnel quadratique $\mathcal{M}$*-valide et vérifiant* $\varepsilon(x) \leqslant N$ *vaut asymptotiquement, pour* $N \to \infty$

$$E[Y_N(\mathcal{M})] \sim \frac{-l}{\lambda'(\mathcal{M}, s_{\mathcal{M}})} \log N.$$

La valeur moyenne de la constante de Lévy d'un irrationnel quadratique $\mathcal{M}$*-valide et vérifiant* $\varepsilon(x) \leqslant N$ *vaut asymptotiquement, pour* $N \to \infty$

$$E[Z_N(\mathcal{M})] \sim \frac{-\lambda'(\mathcal{M}, s_{\mathcal{M}})}{l},$$

où l *désigne la longueur de la période, et* $\lambda'(\mathcal{M}, s)$ *représente la dérivée par rapport à* s *de l'application* $s \to \lambda(\mathcal{M}, s)$.

Preuve. Sur tout le demi-plan pointé $\mathcal{P} := \{s \mid \Re(s) \geqslant s_{\mathcal{M}}, s \neq s_{\mathcal{M}}\}$, et d'après la Proposition 5, le rayon spectral $R(\mathcal{M}, s)$ de $\mathcal{G}_{\mathcal{M}, s}$ est strictement inférieur à 1. Il en est a fortiori de même pour les rayons spectraux $R(\mathcal{M}, 2s)$, $R(\mathcal{M}, s+2)$, $R(\mathcal{M}, 2s+2)$ sur le même demi-plan non-pointé. Les opérateurs $I + \mathcal{G}_{\mathcal{M}, s}$, $I \pm \mathcal{G}_{\mathcal{M}, 2s}$, $I \pm \mathcal{G}_{\mathcal{M}, s+2}$, $I \pm \mathcal{G}_{\mathcal{M}, 2s+2}$ sont donc inversibles, et définissent sur le demi-plan non pointé des fonctions holomorphes de s. Ainsi, seule la fonction $s \to I - \mathcal{G}_{\mathcal{M}, s}$ a une singularité dans le demi-plan non pointé, au point $s = s_{\mathcal{M}}$. Ainsi, les fonctions $U_{\mathcal{M}}(s, 1)$, $V_{\mathcal{M}}(s, 1)$ et $W_{\mathcal{M}}(s, 1)$ vérifient l'hypothèse (i) du Théorème Taubérien pour $\sigma = s_{\mathcal{M}}$.

On se place maintenant dans un voisinage Ω de $\sigma = s_{\mathcal{M}}$. Le principe de perturbation de la Proposition 3 permet de factoriser

$$\det(I - u\mathcal{G}_{\mathcal{M}, s}) = (1 - u\lambda(\mathcal{M}, s)) \det(I - u\mathcal{N}_{\mathcal{M}, s}),$$

ce qui se traduit sur les séries $\mathscr{A}$, $\mathscr{B}$ et $\mathscr{E}$ en les décompositions

$$\mathscr{A}_{\mathscr{M}}(s,u)=\frac{\lambda(\mathscr{M},s)}{1-u\lambda(\mathscr{M},s)}-\frac{\partial}{\partial u}\log\det(I-u\mathscr{N}_{\mathscr{M},s}),$$

$$\mathscr{B}_{\mathscr{M}}(s,u)=\frac{\lambda^2(\mathscr{M},s)}{(1-u\lambda(\mathscr{M},s))^2}-\frac{\partial^2}{\partial u^2}\log\det(I-u\mathscr{N}_{\mathscr{M},s}),$$

$$\mathscr{E}_{\mathscr{M}}(s,u)=\frac{-u\lambda'(\mathscr{M},s)}{1-u\lambda(\mathscr{M},s)}+\frac{\partial}{\partial s}\log\det(I-u\mathscr{N}_{\mathscr{M},s})$$

Sur $\Omega\cap\mathscr{P}$, le rayon spectral $R(\mathscr{M},s)$, égal au module $|\lambda(\mathscr{M},s)|$ de la valeur propre dominante, est strictement inférieur à 1: il en est a fortiori de même pour le rayon spectral de $\mathscr{N}_{\mathscr{M},s}$, et ainsi les seconds termes définissent des fonctions holomorphes sur $\Omega\cap\mathscr{P}$. Par ailleurs, au voisinage de $s=s_{\mathscr{M}}$, la dérivabilité de $s\to\lambda(\mathscr{M},s)$ permet d'écrire

$$\frac{s-s_{\mathscr{M}}}{1-\lambda(\mathscr{M},s)}=-\frac{H(s)}{\lambda'(\mathscr{M},s_{\mathscr{M}})}\qquad\text{avec } H \text{ holomorphe vérifiant } H(s_{\mathscr{M}})=1.$$

utilisant alors les expressions de U, V, W en fonction de $\mathscr{A}$, $\mathscr{B}$, $\mathscr{E}$ de la Proposition 11, on obtient

$$U_{\mathscr{M}}(s,1)=\rho_{\mathscr{M}}\,\frac{-\lambda(\mathscr{M},s)}{\lambda'(\mathscr{M},s_{\mathscr{M}})}\,\frac{H(s)}{(s-s_{\mathscr{M}})}+U_1(s),$$

$$V_{\mathscr{M}}(s,1)=\rho_{\mathscr{M}}\,\frac{\lambda(\mathscr{M},s^2)}{\lambda'(\mathscr{M},s_{\mathscr{M}})^2}\,\frac{H^2(s)}{(s-s_{\mathscr{M}})^2}+V_1(s),$$

$$W_{\mathscr{M}}(s,1)=\rho_{\mathscr{M}}\,\frac{\lambda'(\mathscr{M},s)}{\lambda'(\mathscr{M},s_{\mathscr{M}})}\,\frac{H(s)}{(s-s_{\mathscr{M}})}+W_1(s),$$

où H, U_1, V_1, et W_1 sont holomorphes sur $\Omega\cap\mathscr{P}$ et $\rho_{\mathscr{M}}$ vaut 1 si l est paire et 1/2 sinon. Ainsi, $U_{\mathscr{M}}(s,1)$, $V_{\mathscr{M}}(s,1)$ et $W_{\mathscr{M}}(s,1)$ vérifient les hypothèses (ii) du Théorème Taubérien avec $\sigma=s_{\mathscr{M}}$. En leur appliquant ce théorème, on obtient

$$A_U(\log N):=\sum_{\substack{m\in\mathscr{M}^*\\ \varepsilon(m)\leqslant N}}1\sim\frac{-\rho_{\mathscr{M}}}{s_{\mathscr{M}}\lambda'(\mathscr{M},s_{\mathscr{M}})}N^{s_{\mathscr{M}}}$$

$$A_V(\log N):=\sum_{k\geqslant 1}\sum_{\substack{m\in\mathscr{M}^k\\ \varepsilon(m)\leqslant N}}(k-1)\sim\frac{\rho_{\mathscr{M}}}{s_{\mathscr{M}}\lambda'^2(\mathscr{M},s_{\mathscr{M}})}N^{s_{\mathscr{M}}}\log N,$$

$$A_W(\log N):=\sum_{k\geqslant 1}\frac{1}{k}\sum_{\substack{m\in\mathscr{M}^k\\ \varepsilon(m)\leqslant N}}\log\varepsilon(m)\sim\frac{\rho_{\mathscr{M}}}{s_{\mathscr{M}}}N^{s_{\mathscr{M}}}.$$

D'après (56), la première relation fournit une estimation du cardinal $|\tilde{\mathscr{I}}_N(\mathscr{M})|$, tandis que le quotient de la deuxième par la première fournit une estimation de la longueur moyenne $E[\tilde{Y}_N(\mathscr{M}]$ d'un mot de $\tilde{\mathscr{I}}_N(\mathscr{M})$,

$$|\tilde{\mathscr{I}}_N(\mathscr{M})| \sim \frac{-\rho_{\mathscr{M}}}{s_{\mathscr{M}}\lambda'(\mathscr{M}, s_{\mathscr{M}})} N^{s_{\mathscr{M}}}, \qquad E[\tilde{Y}_N(\mathscr{M})] \sim \frac{1}{\mathscr{L}(\mathscr{M})} \log N. \quad (58)$$

Enfin, le quotient de la troisième par la première fournit une estimation de la valeur moyenne de la variable $\log \varepsilon(m)/|m|$ d'un mot de $\tilde{\mathscr{I}}_N(\mathscr{M})$. Compte tenu des expressions (9), (11) et (12), cette variable ne coïncide avec la constante de Lévy du mot m que si celui-ci est de longueur paire; dans le cas d'une longueur impaire, il y a un facteur 1/2 entre ces variables. Mais on remarque qu'on peut reprendre la preuve précédente dans le cas particulier où la longueur l est impaire et l'appliquer seulement à la partie de $U_{\mathscr{M}}(s, u)$. grâce à (54), cette série ne s'exprime qu'à l'aide des dérivées de déterminants de Fredholm aux points $2s$ et $2s+2$. Le pôle dominant est alors situé en $(1/2)\, s_{\mathscr{M}}$ et on obtient alors un équivalent asymptotique du cardinal du sous-ensemble $\tilde{\mathscr{I}}_{\star N}(\mathscr{M})$ regroupant les mots de longueur impaire de $\tilde{\mathscr{I}}_N(\mathscr{M})$

$$|\tilde{\mathscr{I}}_{\star N}(\mathscr{M})| := \sum_{\substack{m \in \mathscr{M}^* \\ \varepsilon(m) \leqslant N \\ |m| \text{ impair}}} 1 \sim \frac{-2}{s_{\mathscr{M}}\lambda'(\mathscr{M}, s_{\mathscr{M}}/2)} N^{(1/2)\, s_{\mathscr{M}}}. \quad (59)$$

Ainsi, puisque ce cardinal est négligeable devant le cardinal de $\tilde{\mathscr{I}}_N(\mathscr{M})$, la valeur moyenne de la constante de Lévy est équivalente, quand $N \to \infty$, à la valeur moyenne de la variable $\log \varepsilon(m)/|m|$ d'un mot de $\tilde{\mathscr{I}}_N(\mathscr{M})$, et donc

$$E[\tilde{Z}_N(\mathscr{M})] \sim \frac{-\lambda'(\mathscr{M}, s_{\mathscr{M}})}{l}. \quad (60)$$

Avec (58) et (60), on a donc obtenu les résultats cherchés, non pas encore sur les irrationnels quadratiques, mais sur les mots de $\mathscr{M}$.

Troisième étape. Il faut maintenant quitter les mots pour revenir aux irrationnels quadratiques de $\mathscr{I}(\mathscr{M})$. Il faut alors préciser la manière dont l'ensemble $\mathscr{M}$ est primitif, et aussi la manière dont chaque mot de $\mathscr{M}$ l'est.

Pour tout d diviseur de l, longueur de la période $\mathscr{M}$, on définit l'ensemble $\mathscr{M}_{(d)}$ comme étant l'ensemble $\mathscr{M}$ qu'on "replie" sur lui-même: L'ensemble $\mathscr{M}_{(d)}$ est de longueur d et sa i-ième composante est égale à l'intersection de tous les M_j pour $j \equiv i \bmod d$. Alors, on a l'inclusion

$$\mathscr{M}_{(d)}^{l/d} \subset \mathscr{M},$$

et même l'inclusion stricte pour $d \neq l$, car l'égalité contredirait le fait que $\mathcal{M}$ soit la période de l'ensemble de contraintes étudié. On déduit alors de la Proposition 7 l'inégalité stricte

$$\lambda(\mathcal{M}_{(d)}^{l/d}, s) = \lambda(\mathcal{M}_{(d)}, s)^{l/d} < \lambda(\mathcal{M}, s) \tag{61}$$

et dont l'inégalité stricte entre les dimensions de Hausdorff $\mathcal{H}(\mathcal{M}_{(d)} < \mathcal{H}(\mathcal{M})$.

Par ailleurs, pour un élément x de $\mathcal{I}(\mathcal{M})$, la période π de x est élément de $\mathcal{M}_{(d)}$ aussitôt que le pgcd de p et de l est égal à d. On montre ainsi l'inclusion

$$\mathcal{I}(\mathcal{M}) \subset \bigcup_{d \mid l} \mathcal{M}_{(d)}^{*}.$$

Afin d'obtenir à la fois égalité d'ensembles et réunion disjointe, il faut seulement considérer les mots primitifs, définis comme suit: À un mot m, on associe le sous-mot π qui constitue la plus petite période de ce mot, on dit encore son radical. Si m s'écrit $m = \pi^k$, le mot m est dit k-primitif, on le dit simplement primitif lorsque $k = 1$. Si $P(\mathcal{M})$ désigne les mots primitifs de $\mathcal{M}^*$, on a

$$\mathcal{M}^* = \bigcup_{k \geqslant 1} P(\mathcal{M})^k, \qquad \mathcal{I}(\mathcal{M}) = \bigcup_{d \mid l} P(\mathcal{M}_{(d)}), \tag{62}$$

les deux réunions étant désormais disjointes.

Si on désigne maintenant par $P_N(\mathcal{M})$ l'ensemble des mots m de $P(\mathcal{M})$ pour lesquels $\varepsilon(m) \leqslant N$, on a bien sûr l'inégalité $|P_N(\mathcal{M})| \leqslant |\tilde{\mathcal{I}}_N(\mathcal{M})|$ et aussi l'égalité entre les cardinaux

$$|\mathcal{I}_N(\mathcal{M})| = \sum_{d \mid l} |P_N(\mathcal{M}_{(d)})|. \tag{63}$$

Il reste à comparer $P_N(\mathcal{M})$ et l'ensemble $\tilde{\mathcal{I}}_N(\mathcal{M})$ qui est l'ensemble des mots de $\mathcal{M}^*$ vérifiant $\varepsilon(m) \leqslant N$ qu'on a étudié dans la deuxième étape. Comme $\tilde{\mathcal{I}}_n(\mathcal{M})$ est la réunion disjointe des $\tilde{\mathcal{I}}_N(\mathcal{M}) \cap P(\mathcal{M})^k$, on évalue chacun de ces cardinaux en reliant les valeurs de $\varepsilon(m)$ à celle de $\varepsilon(m^k)$. Plusieurs cas sont à considérer selon la valeur de k: pour $k \geqslant 3$, on a $\varepsilon(m) \leqslant \varepsilon(m^k)^{(2/k)}$ et ainsi

$$|\tilde{\mathcal{I}}_N(\mathcal{M}) \cap P(\mathcal{M})^k| \leqslant |P_{N^{2/k}}(\mathcal{M})| \leqslant |\tilde{\mathcal{I}}_{N^{2/k}}(\mathcal{M})|.$$

Comme ϕ^{2l} est une borne inférieure pour les $\varepsilon(m)$ lorsque m décrit $\mathscr{M}^*$, on vérifie que $\mathscr{I}_{N^{2/k}}(\mathscr{M})$ est vide dès que $k \geqslant \log_\phi N$, et en utilisant (58), on obtient

$$\sum_{k \geqslant 2} |\tilde{\mathscr{I}}_N(\mathscr{M}) \cap P(\mathscr{M})^k| = O(N^{(2/3)\, s_{\mathscr{M}}} \log N). \tag{64}$$

Pour $k = 2$, on a $\varepsilon(m^2) = \varepsilon(m)$ si la longueur de π est impaire et $\varepsilon(m) = \varepsilon(m^2)^{(1/2)}$ si la longueur de π est paire, d'où

$$|\tilde{\mathscr{I}}_N(\mathscr{M}) \cap P(\mathscr{M})^2| \leqslant |P_{N^{1/2}}(\mathscr{M})| + |\tilde{\mathscr{I}}_{N^{1/2}}(\mathscr{M})| + |\tilde{\mathscr{I}}_{\star N}(\mathscr{M})|,$$

où $P_{\star N}(\mathscr{M})$ désigne les mots primitifs de $\tilde{\mathscr{I}}_N(\mathscr{M})$ de longueur impaire. Des évaluations (58) et (59), on déduit

$$|\tilde{\mathscr{I}}_N(\mathscr{M}) \cap P(\mathscr{M})^2| = O(N^{(1/2)\, s_{\mathscr{M}}}). \tag{65}$$

On déduit alors de (64) et (65) l'équivalence asymptotique entre les cardinaux

$$|\tilde{\mathscr{I}}_N(\mathscr{M})| \sim |P_N(\mathscr{M})|, \tag{66}$$

puis, finalement, avec les relations (66), (61) et (63), l'équivalence asymptotique cherchée entre les deux cardinaux

$$|\mathscr{I}_N(\mathscr{M})| \sim |\tilde{\mathscr{I}}_N(\mathscr{M})|.$$

Comme les constantes de Lévy coïncident sur les ensembles $\mathscr{I}_N(\mathscr{M})$ et $\tilde{\mathscr{I}}_N(\mathscr{M})$ et y sont bornées, les espérances des deux variables $Z_N(\mathscr{M})$ et $\tilde{Z}_N(\mathscr{M})$ sont équivalentes quand $N \to \infty$. Il reste donc a comparer maintenant les comportements des variables longueur sur $\mathscr{I}_N(\mathscr{M})$ et $\tilde{\mathscr{I}}_N(\mathscr{M})$ en reprenant des arguments semblables aux précédents.

D'abord la relation (63) et la coïncidence des fonctions longueurs sur chacun des $P_N(\mathscr{M}_{(d)})$ correspondant aux diviseurs de l montrent que le terme principal donnant le comportement asymptotique de $Y_N(\mathscr{M})$ est obtenu pour $d = l$ sur l'ensemble $P_N(\mathscr{M})$,

$$E[\, Y_N(\mathscr{M})] \sim E[\, \tilde{Y}_N(\mathscr{M}) \mid P_N(\mathscr{M})]. \tag{67}$$

Ensuite, la partition de l'ensemble $\tilde{\mathscr{I}}_N(\mathscr{M})$ en les $\tilde{\mathscr{I}}_N(\mathscr{M}) \cap P(\mathscr{M})^k$ permet de relier l'espérance des deux variables $Y_N(\mathscr{M})$ et $\tilde{Y}_N(\mathscr{M})$; en effet, sur chaque $\tilde{\mathscr{I}}_N(\mathscr{M}) \cap P(\mathscr{M})^k$, ces dernières sont liées par relation $\tilde{Y}_N(\mathscr{M}) = k\, Y_N(\mathscr{M})$. Des évaluations (64) et (65) des cardinaux de $\tilde{\mathscr{I}}_N(\mathscr{M}) \cap P(\mathscr{M})^k$, pour $k \geqslant 2$, on déduit la relation

$$E[\, \tilde{Y}_N(\mathscr{M})] - E[\, \tilde{Y}_N(\mathscr{M}) \mid P_N(\mathscr{M})] = E[\, \tilde{Y}_N(\mathscr{M})]\; O(N^{(-1/3)\, s_{\mathscr{M}}} (\log N)^2),$$

ce qui prouve l'équivalence asymptotique

$$E[\tilde{Y}_N(\mathscr{M})] \sim E[\tilde{Y}_N(\mathscr{M}) \mid P(\mathscr{M})], \tag{68}$$

et finalement avec (67) et (68), le résultat final cherché sur l'espérance $E[Y_N(\mathscr{M})]$. ∎

6. DES MOTIVATIONS ET DES EXEMPLES NUMÉRIQUES

Ce travail a débuté à la suite d'une question qui m'a été posée par Jean-Pierre Tillich: *Y a-t-il beaucoup de rationnels qui ont tous les chiffres de leur DFC pairs? Même question si on exige que les chiffres de rang impair soient égaux à* 1, *alors que les chiffres de rang pair peuvent être quelconques*?

Ce problème arrive naturellement en relation avec l'étude d'une fonction de hachage proposée par Zémor [Ze] qui est construite à partir du groupe modulaire $\Gamma := SL_2(\mathbf{Z})$ et du groupe $\Gamma_p := SL_2(\mathbf{F}_p)$, pour un nombre premier p. On considère les générateurs S et T de Γ,

$$T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

puis les matrices A et B définies par $A := T$, $B := SAS$.

La fonction de hachage est définie comme suit: à un message binaire $0^{a_0}\, 1^{b_0}\, 0^{a_1}\, 1^{b_1} \cdots 0^{a_i}\, 1^{b_i}$, on associe la matrice M de Γ définie par

$$M := A^{a_0}\, B^{b_0}\, A^{a_1}\, B^{b_1} \cdots A^{a_i}\, B^{b_i}$$

qu'on réduit ensuite modulo p. Cette dernière matrice fournit le transformé du message. Pour "casser" une telle fonction de hachage, il faut trouver de manière efficace une décomposition de la matrice I_p identité de Γ_p sous la forme

$$I_p := A^{m_0}\, B^{n_0}\, A^{m_1}\, B^{n_1} \cdots a^{m_i}\, B^{n_i}, \tag{69}$$

où les suites m_i et n_i sont formées d'entiers positifs de somme "petite". Ainsi, on pourra intercaler le mot $0^{m_0}\, 1^{n_0}\, 0^{m_1}\, 1^{n_1} \cdots 0^{m_i}\, 1^{n_i}$ et trouver deux mots binaires distincts avec le même transformé: cela fournira ce qu'on appelle une "collision" de la fonction de hachage.

On sait qu'il existe de telles décompositions (69) avec une somme de coefficients de l'ordre de $O(\log p)$, mais on ne connaît pas d'algorithme polynomial pour en trouver une explicitement. Pourtant, Tillich a montré que ce schéma possède de grosses faiblesses, en proposant un algorithme probabiliste [TZ1, TZ2] qui utilise l'algorithme d'Euclide et semble trouver presque sûrement une factorisation où la somme des exposants est de l'ordre de $O(\log p)^{1+\varepsilon}$ pour $\varepsilon > 0$. Pour parer une telle attaque, Tillich et Zémor proposent de travailler avec d'autres couples de matrices (A, B) et suggèrent deux choix possibles:

$$A_1 := T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad B_1 := (ST)^2 = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \tag{70}$$

ou

$$A_2 := A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \qquad B_2 := B^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}. \tag{71}$$

Reprenant alors les idées de l'attaque précédente de Tillich, on est alors amené à travailler avec le sous-ensemble de rationnels dont le DFC donne un mot du monoïde engendré par A_i et B_i. Les DFC adéquats sont dans le cas (70) les développements dont les chiffres de rang impair sont égaux à 1, tandis que les chiffres de rang pair peuvent être quelconques, et dans le second cas (71), les développements formés de nombres tous pairs. Les ensembles correspondants sont donc des ensembles de rationnels $\mathscr{Q}(\mathscr{M})$ associés à l'une ou l'autre des contraintes périodiques

$$\mathscr{M}_1 := \{1\} \times N_\star \qquad \text{ou} \quad \mathscr{M} := \{2, 4, ..., 2n\}.$$

Pour répondre numériquement à la question de Tillich, nous avons repris, avec Philippe Flajolet, les algorithmes écrits lors de notre travail précédent sur l'algorithme de Gauss [DFV]. Précédemment, ces algorithmes déterminaient la valeur propre dominante de l'opérateur de Ruelle–Mayer usuel $\mathscr{G}_s$, pour un choix fixé d'un paramètre s réel. Nous les avons adoptés aux problèmes contraints. Notons que Hensley a, de manière indépendante, effectué des calculs similaires dans le cas particulier d'une contrainte élémentaire finie [He4].

L'idée du travail précédent est la suivante: on "approche" l'action de l'opérateur $\mathscr{G}_s$ sur des fonctions analytiques par son action sur les polynômes de Taylor de ces fonctions en un point a de l'intervalle $[0, 1]$. Quand il agit sur les séries entières, l'opérateur $\mathscr{G}_s$ peut être représenté par une matrice (infinie) G_s, dont le terme général $G_s[i, j]$ est le coefficient de $(x-a)^i$ dans $\mathscr{G}_s[(x-a)^j]$ et s'exprime en fonction de valeurs de la fonction ζ d'Hurwitz. Définissant k comme un degré de troncature, on considère la matrice finie $G_s^{[k]}$ obtenue en restreignant les indices i et j à l'intervalle $[0, k[$. La valeur propre dominante de la matrice $G_s^{[k]}$ fournira, pour k suffisamment grand, une approximation de celle de $\mathscr{G}_s$.

Toutes ces idées s'adaptent clairement au cas de l'opérateur de Ruelle–Mayer contraint $\mathscr{G}_{\mathscr{M}, s}$. Ce dernier est un produit d'opérateurs $\mathscr{G}_{\mathscr{M}_i, s}$. La matrice $G_{\mathscr{M}, s}^{[k]}$ est alors définie comme le produit des troncatures $G_{M_i, s}^{[k]}$ des opérateurs $\mathcal{G}_{M_i, s}$, et fournit une approximation de l'opérateur $\mathcal{G}_{\mathcal{M}, s}$ associé à la période $\mathcal{M} := M_1 \times M_2 \times \cdots \times M_l$. Chacune de ces troncatures $G^{[k]}_{M_i, s}$ fait intervenir des valeurs de la fonction ζ_{M_i} associée à la partie M_i. La valeur propre dominante de la matrice $G^{[k]}_{\mathcal{M}, s}$ fournit une valeur approchée de la valeur propre dominante $\lambda(\mathcal{M}, s)$ cherchée. Il reste alors à utiliser une méthode de la sécante pour déterminer une valeur approchée du point $s_{\mathcal{M}}$ qui donne aussi d'ailleurs une valeur approchée de la constante de Lévy $\mathcal{L}(\mathcal{M})$.

Dans nos expérimentations numériques, nous avons choisi de nous limiter à des contraintes engendrées par trois styles différents de contraintes élémentaires: finies, cofinies ou congruentielles.

La syntaxe de ces contraintes élémentaires est définie comme suit: Pour une partie finie $A \subset N_\star$ et un élément $b \in N_\star$, la notation

$$(A, b) := \{m \geqslant 1 \mid m \bmod b \in A\}$$

définit les contraintes congruentielles, tandis que les notations

$$(A) := \{m \geqslant 1 \mid m \in A\}, \qquad (\neq A) := \{m \geqslant 1 \mid m \notin A\},$$

définiront des contraintes élémentaires finies ou cofinies. Une contrainte est alors définie comme un produit fini de contraintes élémentaires. Voici quelques exemples de la syntaxe des contraintes élémentaires,

$(\{2\}, 2)$	quotients tous pairs
$(\{1\}, 1)$	pas de contraintes
$(\{19, 23\}, 37)$	congruents à 19 ou 23 modulo 37
$(\{3, 7\})$	quotients égaux à 3 ou à 7
$(\neq \{3, 4, 5\})$	quotients différents de 3, 4 et 5

et des exemples de contraintes de longueur $l > 1$: le symbole $(\{1\}, 1) \times (\{2\}, 2)$ désigne la contrainte de longueur 2 où les chiffres de rang impair sont quelconques et les chiffres de rang pair sont pairs, et la contrainte $\mathcal{M}_1$ s'écrit $(\{1\}) \times (\{1\}, 1)$.

Voici un tableau de résultats numériques, où l'on trouve le calcul des deux grandeurs principales du travail:

(i) l'abscisse $s_{\mathcal{M}}$ qui représente le double de la dimension de Hausdorff de l'ensemble des réels $\mathcal{M}$-contraints,

(ii) la constante de Lévy $\mathcal{L}(\mathcal{M})$ égale à $(-1/l)\lambda'(\mathcal{M}, s_{\mathcal{M}})$.

Ces résultats sont présentés par dimension de Hausdorff croissante.

En particulier, la dernière ligne du tableau correspond au cas non-contraint et les réponses aux questions de Tillich se trouvent dans la partie encadrée du tableau:

La probabilité asymptotique qu'un nombre rationnel p/q vérifiant $1 \leqslant p \leqslant q \leqslant N$, $\mathrm{pgcd}(p, q) = 1$ ait tous les chiffres de son DFC pairs est en $O(N^{-0.57})$ tandis que la probabilité asymptotique qu'un nombre rationnel p/q vérifiant $1 \leqslant p \leqslant q \leqslant N$, $\mathrm{pgcd}(p, q) = 1$ ait les chiffres de rang impair de son DFC égaux à 1 est en $O(N^{-0.41})$. Notons que, grâce à la Proposition 5 et au Corollaire 6, on montre que la probabilité asymptotique qu'un nombre rationnel p/q vérifiant $1 \leqslant p \leqslant q \leqslant N$, $\mathrm{pgcd}(p, q) = 1$ ait les chiffres de rang pair de son DFC égaux à 1 est également en $O(N^{-0.41})$.

Les constantes $c_{\mathscr{M}}$ intervenant dans le Théorème 2 peuvent être aussi déterminées numériquement. Elles semblent en général petites. Pour la contrainte $\mathscr{M}_2$ (chiffres tous pairs), elle est proche de 0.4. Pour la contrainte $\mathscr{M}_1$ (chiffres de rang impair égaux à 1), elle est proche de 0.3, pour la contrainte $\hat{\mathscr{M}}_1$ (chiffres de rang pair égaux à 1), elle est proche de 0.2. On vérifie ainsi expérimentalement que des constantes $c_{\mathscr{M}}$ associées à des périodes miroir peuvent être distinctes.

Contrainte $\mathscr{M}$	$s_{\mathscr{M}} = 2\mathscr{H}(\mathscr{M})$	$\mathscr{L}(\mathscr{M}) = -(1/l)\,\lambda'(\mathscr{M}, s_{\mathscr{M}})$
$(\{1, 20\})$	0.53510	0.99082
$(\{1, 10\})$	0.62913	0.90338
$(\{1, 2\})$	1.06256	0.63229
$(\{1\}, 19)$	1.12163	4.39147
$(\{1\}, 2) \times (\{1\})$	1.38542	1.61623
$(\{2\}, 2)$	1.43899	2.28425
$(\{1\}) \times (\{1\}, 1)$	1.59769	1.24694
$(\{1\}, 1) \times (\{2\}, 2)$	1.65790	1.78651
$(\{1, 2, 3, 4, 5, 6\}) \times (\neq \{1, 3, 5, 7\})$	1.66264	1.64067
$(\{1, 2, 3, 4, 5\})$	1.67365	0.82694
$(\{1\}, 1) \times (\neq \{1, 3, 5, 7, 9, 11\})$	1.72557	1.82183
$(\{1\}, 1) \times (\neq \{1, 3, 5\})$	1.7566	1.76017
$(\{1\}, 1) \times (\neq \{1, 3\})$	1.77934	1.70060
$(\neq \{6, 7, 8, 9, 10, 11\})$	1.90117	1.21299
$(\neq \{10\})$	1.98978	1.18525
$(\neq \{10\}) \times (\{1\})$	1.99491	1.18585
$(\{1\}, 1)$	2.00000	1.18656

REMERCIEMENTS

Tous mes remerciements à Jean-Pierre Tillich pour m'avoir posé la question qui a motivé ce travail, et à Philippe Flajolet pour son aide dans la partie numérique de ce travail. Merci aussi à Doug Hensley pour ses remarques constructives et au referee pour sa lecture attentive.

RÉFÉRENCES

[Bu] R. T. Bumby., Hausdorff dimension of sets arising in number theory, *in* "Number Theory Seminar," Lecture Notes in Mathematics, Vol. 1135, pp. 1–8, Springer-Verlag, New York, 1985.

[Cu] W. Cusik, Continuants with bounded digits, I, *Mathematika* **24** (1977), 166–172; II, *Mathematika* **25** (1978), 107–109.

[DFV] H. Daudé, P. Flajolet, et B. Vallée, "An Analysis of the Gaussian Algorithm for Lattice Reduction, ANTS 1994," Lecture Notes in Computer Science, Vol. 877, pp. 144–158; *Combin. Probab. Comput.* **6** (1997), 397–433.

[De] H. Delange, Généralisations du Théorème d'Ikehara, *Ann. Sci. École Norm. Sup.* **71** (1954), 213–242.

[Di] J. G. Dixon, The number of steps in the Euclidean algorithm, *J. Number Theory* **2** (1970), 414–422.

[Fa] C. Faivre, Distribution of Lévy constants for quadratic numbers, *Acta Arith.* **61**, No. 1 (1992), 13–34.

[Fl] P. Flajolet, Analytic analysis of algorithms, *in* "Proceedings of the 19th International Colloquium, Automata, Languages and Programming, Vienna, July 1992" (W. Kuich, Ed.), Lecture Notes in Computer Science, Vol. 623, pp. 186–210, Springer-Verlag, New York.

[FS] P. Flajolet et R. Sedgewick, "Analytic Combinatorics," livre en préparation; les chapitres séparés sont disponibles en Rapports de Recherche INRIA 1888, 2026, 2376, 2956.

[FV] P. Flajolet et B. Vallée, Continued fraction algorithms, functional operators and structure constants, *Theoret. Comput. Sci.* **194** (1998), 1–34.

[Go] I. J. Good, The fractional dimensional theory of continued fractions, *Math. Proc. Cambridge Philos. Soc.* **37** (1941), 199–228.

[Gr1] A. Grothendieck, Produits tensoriels topologiques et espaces nucléaires, *Mem. Amer. Math. Soc.* **16** (1955).

[Gr2] A. Grothendieck, La théorie de Fredholm, *Bull. Soc. Math. France* **84**, 319–384.

[Hei] H. Heilbronn, On the average length of a class of continued fractions, *in* "Number Theory and Analysis" (P. Turan, Ed.), pp. 87–96, Plenum, New York, 1969.

[He1] D. Hensley, The distribution of badly approximable rationals and continuants with bounded digits, II, *J. Number Theory* **34** (1990), 293–334.

[He2] D. Hensley, The Hausdorff dimensions of some continued fraction Cantor sets, *J. Number Theory* **33** (1989), 182–198.

[He3] D. Hensley, Continued fraction Cantor sets, Hausdorff dimension, and functional analysis, *J. Number Theory* **40** (1992), 336–358.

[He4] D. Hensley, A polynomial time algorithm for the Hausdorff dimension of a continued fraction Cantor set, *J. Number Theory* **58**, No. 1 (1996), 9–45; Erratum, *J. Number Theory* **59**, No. 2 (1996), 419.

[Hi] K. E. Hirst, Continued fractions with sequences of partial quotients, *Proc. Amer. Math. Soc.* **38** (1973), 221–227.

[Kr] M. Krasnoselsky, “Positive Solutions of Operators Equations,” Chap. 2, Noordhoff, Groningen, 1964.

[Ma1] D. H. Mayer, Continued fractions and related transformations, *in* “Ergodic Theory, Symbolic Dynamics and Hyperbolic Spaces” (M. K. Tim Bedford and C. Series, Eds.), pp. 175–222, Oxford Univ. Press, London, 1991.

[Ma2] D. H. Mayer, On composition operators on Banach spaces of holomorphic functions, *J. Funct. Anal.* **35** (1980), 191–206.

[Ma3] D. H. Mayer, Spectral properties of certain composition operators arising in statistical mechanics, *Comm. Math. Phys.* **68** (1979), 1–8.

[Ma4] D. H. Mayer, On the thermodynamic formalism for the Gauss map, *Comm. Math. Phys.* **130** (1990), 311–333.

[Ma5] D. H. Mayer, Approach to equilibrium for locally expanding maps in $\mathbf{R}^k$, *Comm. Math. Phys.* **95** (1984), 1–15.

[MR] D. H. Mayer et G. Roepstorff, On the relaxation time of Gauss's continued fraction map, I. The Hilbert space approach, *J. Statist. Phys.* **47**, No. 1/2 (1987), 149–171; II, The Banach space approach (transfer operator approach), *J. Statist. Phys.* **50** (1/2) (1988), 331–344.

[MU1] R. D. Mauldin et M. Urbański, Dimensions and measures in infinite iterated function systems, *Proc. London Math. Soc. (3)* **73** (1996), 105–154.

[MU2] R. D. Mauldin et M. Urbański, Conformal iterated function systems with applications to the geometry of continued fractions, preprint.

[Po] M. Pollicott, Distribution of closed geodesics on the modular surface and quadratics irrationals, *Bull. Soc. Math. France* **114** (1986), 431–446.

[Po2] M. Pollicott, A complex Ruelle–Perron–Frobenius Theorem and two counterexamples, *Ergodic Theory Dynamical Systems* **4** (1984), 135–146.

[Sh] J. Shallitt, “Real Numbers with Bounded Partial Quotients: A Survey in G?” (M. Rassias, Ed.), The Mathematical Heritage of Carl Friedrich Gauss, World Scientific, Singapore, 1991.

[TZ1] J.-P. Tillich et G. Zémor, Group-theoretic hash function, *in* “Proceedings of the First French-Israeli Workshop in Algebraic Coding,” Lecture Notes in Computer Science, Vol. 781, pp. 90–110, Springer-Verlag, New York/Berlin, 1993.

[TZ2] J.-P. Tillich et G. Zémor, Hashing with SL_2, *in* “Advances in Cryptology: Proceedings of Crypto'94,” Lecture Notes in Computer Science, Vol. 839, Springer-Verlag, New York,
1994.

[Va1] B. Vallée, Opérateurs de Ruelle–Mayer généralisés et analyse des algorithmes de Gauss et d'Euclide, *Acta Arith.* **81**, No. 2 (1997), 101–144.

[Va2] B. Vallée, Algorithms for computing signs of 2×2 determinants: Dynamics and average-case algorithms, *in* “Proceedings of the 8th Annual European Symposium on Algorithms, ESA'97,” Lecture Notes in Comput. Sci., Vol. 1284, pp. 486–499, Springer-Verlag, New York, 1997.

[Ze] G. Zémor, Hash functions and Cayley graphs, *Designs Codes Cryptography* **4**, No. 4 (1994), 381–394.