FOURIER ANNALES DE L'INSTITUT

ANNALES

DE

L'INSTITUT FOURIER

Nicolas CHEVALLIER

Meilleures approximations diophantiennes simultanées et théorème de Lévy

Tome 55, nº 5 (2005), p. 1635-1657.

<http://aif.cedram.org/item?id=AIF_2005__55_5_1635_0>

© Association des Annales de l'institut Fourier, 2005, tous droits réservés.

L'accès aux articles de la revue « Annales de l'institut Fourier » (http://aif.cedram.org/), implique l'accord avec les conditions générales d'utilisation (http://aif.cedram.org/legal/). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/

Ann. Inst. Fourier, Grenoble
55, 5 (2005), 1635–1657

MEILLEURES APPROXIMATIONS DIOPHANTIENNES SIMULTANÉES ET THÉORÈME DE LÉVY

par Nicolas CHEVALLIER

1. Introduction.

Le développement en fraction continue d'un réel x possède trois propriétés importantes :

(1) il est obtenu à partir du codage par l'application de Gauss $x \in]0,1[\to \{\frac{1}{x}\}$ ($\{t\}$ désigne la partie fractionnaire du réel t),

(2) il fournit une suite d'approximations rationnelles de x, $(\frac{p_m}{q_m})_{m\geqslant 0}$, et les couples de vecteurs $\binom{p_m}{q_m}$, $\binom{p_{m+1}}{q_{m+1}}$ forment une suite de bases du réseau $\mathbb{Z}^2$,

(3) la fraction $\frac{p_m}{q_m}$ vérifie la propriété de meilleure approximation : $\forall p \in \mathbb{Z}$, $\forall q \in \mathbb{N}^*$, $(|qx - p| < |q_m x - p_m| \Rightarrow q \geqslant q_{m+1})$.
La conjonction de ces trois propriétés est très spécifique du développement en fraction continue unidimensionnelle.

Certaines extensions multidimensionnelles du développement en fraction continue telles que l'algorithme de Jacobi-Perron, sont basées sur la propriété (1). L'application de Gauss est remplacée par une application homographique par morceaux définie sur une partie convenable de $\mathbb{R}^d$ (voir le livre de F. Schweiger, [Schw]). Lorsque les homographies sont associées à des éléments de $\mathrm{SL}(d+1,\mathbb{Z})$, la propriété (2) est alors automatique mais la propriété (3) est loin d'être satisfaite : la qualité des approximations

Mots-clés : approximations diophantiennes, théorème de Lévy, réseaux.
Classification math. : 11J13, 11J70, 22F30.

obtenues n'est en générale pas de l'ordre de grandeur prévu par le théorème de Dirichlet ([Br,Gu]).

D'autres extensions partent de la propriété (2) (voir le livre de A.J. Brentjes [Br2]) : à un élément Θ de $\mathbb{R}^d$ on associe la demi-droite $\mathbb{D} = \mathbb{R}^+\binom{\Theta}{1}$ de $\mathbb{R}^{d+1}$ et on cherche une suite de bases du réseau $\mathbb{Z}^{d+1}$ dont le cône positif contient la demi-droite $\mathbb{D}$ et "converge" vers $\mathbb{D}$. Enfin, la propriété (3) conduit naturellement à la définition des meilleures approximations diophantiennes simultanées ([Ro], [Br1,2], [Lag1,2,3,4], [Ch1,2,3,4], définition 1 ci-dessous). Cependant, J. C. Lagarias [Lag3] a montré que les propriétés (2) et (3) sont incompatibles dès la dimension 2.

Pour concilier partiellement ces deux propriétés on peut ajouter des approximations intermédiaires entre les meilleures approximations. Ainsi A.J. Brentjes a construit un algorithme 2-dimensionnel basé sur la propriété (2), qui donne toutes les meilleures approximations d'un certain type ([Br1,2]).

On peut encore affaiblir le lien entre les propriétés (2) et (3) : on sélectionne une partie des meilleures approximations et on intercale des approximations intermédiaires. Lagarias [Lag5] a défini un tel développement en toute dimension (et même pour des approximations simultanées de formes linéaires). Pour cela, il se base sur une idée d'Hermite : à un élément Θ de $\mathbb{R}^d$ et à un réel strictement positif s, on associe le réseau $\Gamma(\Theta, s)$ de l'espace $\mathbb{R}^{d+1}$ dont une base est donnée par les vecteurs colonnes de la matrice

$$B(s,\Theta) = \begin{pmatrix} s & 0 & \cdots & 0 \\ \theta_1 & 1 & & \vdots \\ \vdots & & \ddots & 0 \\ \theta_d & 0 & & 1 \end{pmatrix}.$$

Pour chaque s, le plus court vecteur du réseau $\Gamma(\Theta, s)$ fournit une meilleure approximation diophantienne simultanée de Θ appelée meilleure approximation de Hermite par Lagarias (voir la définition 2 ci-dessous). L'ensemble de ces meilleures approximations est une partie en général stricte de l'ensemble de toutes les meilleures approximations de Θ. En dimension 1, c'est-à-dire lorsque Θ est un réel, les meilleures approximations de Hermite forment simplement une sous-suite de la suite $(q_n)_{n\in\mathbb{N}}$ des dénominateurs des réduites de Θ. Pour obtenir les coefficients du développement multidimensionnel, Lagarias introduit la notion de base de Minkowski lexicographiquement réduite d'un réseau ([Lag5]). Lorsque s tend vers 0, la famille de réseaux $\Gamma(\Theta, s)$ admet une succession de bases réduites de la forme

$$B(s,\Theta)P_1,\ B(s,\Theta)P_2, ..., B(s,\Theta)P_n, ...\ ;$$

les coefficients du développement sont alors les matrices de changement de base, $A_n = P_{n-1}^{-1}P_n$, $n = 1, 2, ...$ Comme le premier vecteur d'une base de Minkowski lexicographiquement réduite d'un réseau est un plus court vecteur de ce réseau, Lagarias obtient ainsi une généralisation naturelle de l'algorithme additif du développement en fraction continue. Avec D.J. Grabiner, il a étudié en dimension 1, le lien exact entre ce développement et le développement en fraction continue classique ([Gr, Lag]).

À l'aide d'une homothétie et du changement de paramètre $s = e^t$, la famille $\Gamma(\Theta, s)$ se transforme en une famille de réseaux $\Lambda(\Theta, t)$ qui est la projection dans l'espace homogène $\mathrm{SL}(d+1,\mathbb{R})/\mathrm{SL}(d+1,\mathbb{Z})$, d'une trajectoire d'un champ de vecteur invariant de $\mathrm{SL}(d+1,\mathbb{R})$. S.G. Dani [Da], a établi une correspondance entre le comportement à l'infini de cette trajectoire et les propriétés diophantiennes de l'élément Θ de $\mathbb{R}^d$: la trajectoire est bornée si et seulement si Θ est mal approchable, et la trajectoire diverge si et seulement si Θ est irrégulier (voir [Ca] pour les définitions de mal approchable et irrégulier. Dani étudie en fait le cas plus général d'une matrice Θ). Ces résultats de Dani ont eu de nombreux prolongements (cf. l'article de synthèse de G.A. Margulis [Ma]).

Dans ce travail nous reprenons la même idée : utiliser la famille de réseaux $\Lambda(\Theta, t)$ pour étudier les propriétés diophantiennes d'un élément Θ de $\mathbb{R}^d$ ou d'une matrice Θ de $M_{d,k}(\mathbb{R})$. D'une part, nous précisons la répartition des meilleures approximations de Hermite dans l'ensemble de toutes les meilleures approximations. D'autre part, grâce à une propriété classique de non dilatation d'un flot (lemme 2) nous étendons partiellement le théorème de Lévy aux meilleures approximations simultanées de formes linéaires. Dans le cas unidimensionnel on retrouve une forme affaiblie bien connue du théorème de Lévy : *Il existe une constante C telle que pour presque tout réel x,* $\limsup_{m\to\infty} \frac{1}{m}\ln q_m \leqslant C$.

1.1. Meilleures approximations simultanées de formes linéaires.

Munissons $\mathbb{R}^d$, $\mathbb{R}^k$ et $M_{d,k}(\mathbb{R})$ des normes euclidiennes usuelles et notons les $|.|$. Pour chaque vecteur X de $\mathbb{R}^d$ et chaque matrice Θ de $M_{d,k}(\mathbb{R})$ posons

$$\|X\| = \inf\{|X - P| : P \in \mathbb{R}^d\},$$

$$\|\Theta\| = \inf\{|\Theta - N| : N \in M_{d,k}(\mathbb{Z})\}.$$

Lagarias [Lag] a défini les meilleures approximations simultanées de formes linéaires. La définition ci-dessous est un peu moins générale que celle de Lagarias, elle se trouve dans [Ch3].

DÉFINITION 1. — *Soit* Θ *un élément de* $M_{d,k}(\mathbb{R})$. *Un élément* Q *de* $\mathbb{Z}^k$ *est une meilleure approximation de* Θ *si* Q *est différent de* 0 *et si*

$$\begin{cases} \|\Theta P\| > \|\Theta Q\| & \forall P \in \mathbb{Z}^k \backslash \{0\},\ |P| < |Q|\,, \\ \|\Theta P\| \geqslant \|\Theta Q\| & \forall P \in \mathbb{Z}^k \backslash \{0\},\ |P| \leqslant |Q|\,. \end{cases}$$

L'ensemble de toutes les meilleures approximations d'une matrice Θ forme une suite infinie $(Q_m(\Theta))_{m\in\mathbb{N}}$ dès que l'image de $\mathbb{Z}^k\backslash\{0\}$ par la matrice Θ ne rencontre pas $\mathbb{Z}^d$. Ordonnons cette suite $(Q_m(\Theta))_{n\in\mathbb{N}}$ par ordre croissant des normes $q_m(\Theta) = |Q_m(\Theta)|$. Lorsque $d = k = 1$, la suite $(q_m)_m$ est simplement la suite des dénominateurs des réduites du développement en fraction continue du réel Θ. Posons enfin,

$$r_m(\Theta) = \|\Theta Q_m(\Theta)\|\,,$$

Le nombre $r_m(\Theta)$ mesure la qualité de “l'approximation rationnelle” Q_m.

Remarque. — Si l'on change les normes sur $\mathbb{R}^d$ et $\mathbb{R}^k$ on obtient en général une autre suite (q_m). Une liaison entre ces suites est donnée dans [Ch5] lorsque $k = 1$.

1.2. Réseaux et approximations diophantiennes.

Posons $n = d + k$ et $\Gamma = \mathrm{SL}(n,\mathbb{Z})$. Le quotient $\mathcal{R} = \mathrm{SL}(n,\mathbb{R})/\Gamma$ peut être identifié à l'espace des réseaux de $\mathbb{R}^n$ de déterminant 1 car les vecteurs colonnes de deux matrices A et B de $\mathrm{SL}(n,\mathbb{R})$ définissent le même réseau si et seulement si il existe $P \in \Gamma$ tel que $A = BP$. À chaque matrice Θ de $M_{d,k}(\mathbb{R})$ on associe le réseau Λ_Θ de $\mathbb{R}^n$ représenté par la matrice

$$M_\Theta = \begin{pmatrix} I_k & 0 \\ \Theta & I_d \end{pmatrix}.$$

Lagarias a montré que le plus court vecteur du réseau $\Lambda(\Theta, t) = g_t\Lambda_\Theta$ où

$$g_t = \begin{pmatrix} e^{-dt}I_k & 0 \\ 0 & e^{kt}I_d \end{pmatrix} \in \mathrm{SL}(n,\mathbb{R}),$$

fournit une meilleure approximation de Θ (voir Lemme 4 plus loin). Le comportement de la fonction longueur du plus court vecteur d'un réseau

$$\begin{aligned} \delta &: \mathcal{R} \to \mathbb{R} \\ &: \Lambda \to \inf\{|x| : x \in \Lambda\backslash\{0\}\} \end{aligned}$$

le long des trajectoires du flot $\Lambda \in \mathcal{R} \to g_t\Lambda$ devrait donc donner des informations sur le comportement asymptotique des suites $(q_m(\Theta))_{m\in\mathbb{N}}$, $\Theta \in M_{d,k}(\mathbb{R})$.

1.3. Meilleures approximations de Hermite.

Définition 2. — *Soit Θ un élément de $M_{d,k}(\mathbb{R})$. Un élément H de $\mathbb{Z}^k$ est une meilleure approximation de Hermite de Θ si il existe un réel t et un élément P de $\mathbb{Z}^d$ tels que $\binom{H}{P}$ soit un plus court vecteur du réseau représenté par la matrice $g_t M_\Theta$.*

En fait, pour Lagarias la meilleure approximation est le couple $\binom{H}{P}$ et non H seul. Mais la connaissance de H est une information suffisante car P est simplement un élément de $\mathbb{Z}^d$ qui rend minimum la norme du vecteur $\Theta H - P$.

Ordonnons la suite $(H_m(\Theta))_{m\in\mathbb{N}}$ des meilleures approximations de Hermite d'une matrice Θ par ordre croissant des normes $h_m = h_m(\Theta) = |H_m(\Theta)|$, on obtient une sous-suite de la suite $(q_n)_{n\in\mathbb{N}}$. Notons que l'on peut avoir plusieurs approximations de Hermite de même norme.

1.4. Sous-groupes de $\mathrm{SL}(n,\mathbb{R})$ associés à g_t.

$\mathrm{SL}(n,\mathbb{R})$ muni de la multiplication des matrices est un groupe de Lie dont l'algèbre de Lie $\mathrm{sl}(n,\mathbb{R})$ s'identifie avec l'ensemble des matrices de trace nulle. Appelons X la matrice diagonale de trace nulle

$$X = \begin{pmatrix} -d\, I_k & 0 \\ 0 & k\, I_d \end{pmatrix}.$$

Clairement,

$$g_t = \exp tX.$$

L'application $\mathrm{ad}\, X : Y \in \mathrm{sl}(n,\mathbb{R}) \to XY - YX \in \mathrm{sl}(n,\mathbb{R})$ est diagonalisable. Le sous-espace vectoriel $\mathcal{H}_{>0}$ engendré par les sous-espaces propres associés à des valeurs propres strictement positives est l'ensemble des matrices de la forme

$$\begin{pmatrix} 0 & 0 \\ A & 0 \end{pmatrix}$$

où A est une matrice $d\times k$. De même, le sous-espace vectoriel $\mathcal{H}_{\leqslant 0}$ engendré par les sous-espaces propres associés à des valeurs propres négatives ou nulles est l'ensemble des matrices de trace nulle de la forme

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

où A est une matrice $k \times k$, B une matrice $k \times d$ et C une matrice $d \times d$. Comme $\mathcal{H}_>$ et $\mathcal{H}_\leqslant$ sont des sous-algèbre de Lie de $\mathrm{sl}(n\mathbb{R})$, il existe des sous-groupes de Lie de $\mathrm{SL}(n, \mathbb{R})$, $H_>$ et $H_\leqslant$, dont les algèbres de Lie sont $\mathcal{H}_>$ et $\mathcal{H}_\leqslant$. Le sous-groupe $H_>$ coïncide avec l'ensemble des matrices M_Θ, $\Theta \in M_{d,k}(\mathbb{R})$ et le produit dans $H_>$ correspond à l'addition dans $M_{d,k}(\mathbb{R})$. Le sous-groupe $H_\leqslant$ coïncide avec l'ensemble des matrices de déterminant 1 de la forme

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

où A est une matrice $k \times k$, B une matrice $k \times d$ et C une matrice $d \times d$.

Résultats. — Pour établir un lien entre le comportement de la fonction longueur du plus court vecteur et les meilleures approximations, on précise le théorème de Birkhoff dans le cas du flot g_t. Grâce à la non dilatation de ce flot dans la direction $\mathcal{H}_\leqslant$ on démontre

THÉORÈME 1. — *Soit $\phi : \mathcal{R} \to \mathbb{R}_{>0}$ une fonction strictement positive et intégrable sur $\mathcal{R}$. Si $\ln \phi$ est uniformément continue sur $\mathcal{R}$ alors pour presque tout x appartenant à $H_{>0}$,*

$$\lim_{t\to\infty} \frac{1}{t} \int_0^t \phi(g_s x)\, ds = \int_{\mathcal{R}} \phi(y)\, dy.$$

Le presque tout x se rapporte à la mesure de Haar du groupe $H_{>0} = \{M_\Theta : \Theta \in M_{d,k}(\mathbb{R})\}$ ou à la mesure de Lebesgue sur $M_{d,k}(\mathbb{R})$. A l'aide d'inégalités faciles (propositions 2 et 3) sur les meilleures approximations, on en déduit

THÉORÈME 2. — *Soit d et k deux entiers $\geqslant 1$. Il existe une constante C ne dépendant que de d et k telle que pour presque toute matrice Θ appartenant à $M_{d,k}$, on ait*

$$\limsup_{m\to\infty} \frac{1}{m} \ln \frac{q_m(\Theta)}{r_m(\Theta)} \leqslant C.$$

Remarques. — 1. L'extension partielle du théorème de Lévy aux meilleures approximations simultanées de réels a déjà été prouvée dans [Ch4] grâce à une estimation asymptotique de W.M. Schmidt du nombre de solutions de certaines inéquations diophantiennes ([Schm] Theorem 3B, p. 61). Une adaptation de cette preuve aux approximations simultanées de formes linéaires devrait être possible même si les extensions aux approximations simultanées de formes linéaires de l'estimation de W.M. Schmidt ne semblent pas directement utilisables (voir [Sp]).

2. Grâce aux travaux de Lagarias on sait aussi que pour tout Θ la $\liminf_{m\to\infty} \frac{1}{m} \ln q_m(\Theta)$ est strictement positive ([Lag3]). Une question naturelle reste sans réponse : la limite $\lim_{m\to\infty} \frac{1}{m} \ln q_m(\Theta)$ existe-t-elle pour presque toute matrice Θ ?

Le théorème suivant montre que l'essentiel de l'information contenue dans la suite des meilleures approximations se retrouve dans la suite des meilleures approximations de Hermite. Le cas $d = k = 1$ correspond à une forme affaiblie des résultats de Grabiner et Lagarias ([Gr,Lag]).

Théorème 3.

1. *Il existe une constante m_0 qui ne dépend que des dimensions d et k telle pour toute matrice Θ de $M_{d,k}(\mathbb{R})$ et tout entier m, le nombre d'entiers n vérifiant*

$$h_m < q_n < h_{m+1}$$

soit inférieur à m_0.

2. *Il existe une constante C qui ne dépend que des dimensions d et k telle que pour tout entier m et toute matrice Θ de $M_{d,k}(\mathbb{R})$, on ait*

$$h_{m+1}^k \left\|\Theta H_m\right\|^d \leqslant C.$$

3. *Supposons $k = 1$. Dans ce cas, les meilleures approximations et les meilleures approximations de Hermite sont des entiers que l'on peut supposer positifs. On a alors $Q_n = q_n$ et $H_m = h_m$. Il existe une constante strictement positive c telle que pour tout vecteur colonne $\Theta \in \mathbb{R}^d$ et toute meilleure approximation q_n de Θ, il existe une meilleure approximation de Hermite h_m telle que*

$$c\left\|h_m\Theta\right\| \leqslant \left\|q_n\Theta\right\| \leqslant \left\|h_m\Theta\right\|.$$

2. Fonctions uniformément continues sur $\mathcal{R}$.

Définition 3. — *Une fonction $f : \mathcal{R} \to \mathbb{R}$ est uniformément continue sur $\mathcal{R}$ si pour tout $\varepsilon > 0$ il existe un voisinage V de l'élément neutre dans $\mathrm{SL}(n,\mathbb{R})$ tel que pour x de $\mathcal{R}$ et tout y appartenant à Vx on ait*

$$|f(x) - f(y)| \leqslant \varepsilon.$$

Proposition 1. — *Le logarithme de la fonction longueur du plus court vecteur d'un réseau, c'est-à-dire la fonction* $\ln\delta$*, est uniformément continue sur* $\mathcal{R}$*.*

Supposons que $\mathbb{R}^n$ soit munit de la norme euclidienne $|.|$ et notons $|.|_{\mathrm{Mat}}$ la norme matricielle associée sur $M_n(\mathbb{R})$,

$$|M|_{\mathrm{Mat}} = \sup\{|Mx| : x \in \mathbb{R}^n,\ |x| = 1\}.$$

La proposition est une conséquence immédiate du lemme.

Lemme 1. — *Soit* g *et* h *deux éléments de* $\mathrm{SL}(n,\mathbb{R})$*. Alors*

$$\delta(g\Gamma)(1 - |I_n - h|_{\mathrm{Mat}}) \leqslant \delta(hg\Gamma) \leqslant \delta(g\Gamma)(1 + |I_n - h|_{\mathrm{Mat}}).$$

Démonstration du Lemme. — Soit P un élément non nul de $\mathbb{Z}^n$ tel que $\delta(g\Gamma) = |gP|$. On a

$$\begin{aligned}\delta(hg\Gamma) &\leqslant\ |hgP| = |gP + hgP - gP| \\ &\leqslant\ |gP| + |h - I_n|_{\mathrm{Mat}}\,|gP| = \delta(g\Gamma)(1 + |h - I_n|_{\mathrm{Mat}}).\end{aligned}$$

De même si P est un élément non nul quelconque de $\mathbb{Z}^n$, on a

$$\begin{aligned}|hgP| =&\ |gP + hgP - gP| \\ \geqslant&\ \max(0, |gP| - |h - I_n|_{\mathrm{Mat}}\,|gP|) \\ \geqslant&\ \delta(g\Gamma)(1 - |h - I_n|_{\mathrm{Mat}})\end{aligned}$$

donc $\delta(hg\Gamma) \geqslant \delta(g\Gamma)(1 - |h - I_n|_{\mathrm{Mat}})$. □

3. Démonstration du théorème 1.

L'application $\mathrm{ad}\,X$ restreinte à $\mathcal{H}_\leqslant$ est diagonalisable et ses valeurs propres sont négatives ou nulles, à l'aide l'application exponentielle cela se traduit sous la forme :

Lemme 2. — *Soit* y *un élément de* $H_\leqslant$*. Alors pour tout* $t \geqslant 0$ *on a*

$$\left|I_n - g_t y g_t^{-1}\right|_{\mathrm{Mat}} \leqslant C\,|I_n - y|_{\mathrm{Mat}}$$

où C *ne dépend que la dimension* n*.*

Démonstration du lemme. — La matrice y est de la forme

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

où A est une matrice $k \times k$, B une matrice $k \times d$ et C une matrice $d \times d$. En effectuant le produit de matrices $g_t y g_t^{-1}$ on obtient

$$g_t y g_t^{-1} = \begin{pmatrix} A & e^{-(d+k)t} B \\ 0 & C \end{pmatrix}.$$

Par conséquent, la norme euclidienne de la matrice $I_n - g_t y g_t^{-1}$ est inférieure à celle de la matrice $I_n - y$ et par équivalence des normes cela donne l'inégalité

$$\left| I_n - g_t y g_t^{-1} \right|_{\mathrm{Mat}} \leqslant C \left| I_n - y \right|_{\mathrm{Mat}} .$$

□

L'action sur $\mathcal{R}$ du flot g_t est ergodique ; il en existe des démonstrations directes mais cela peut aussi se déduire du théorème d'ergodicité de Moore ([Be, Ma] p. 89). Le théorème de Birkhoff montre alors que pour presque tout Δ appartenant à $\mathcal{R}$ on a

$$\lim_{T\to\infty} \frac{1}{T} \int_0^T \phi(g_t \Delta) dt = \int_{\mathcal{R}} \phi(\Lambda)\, d\Lambda = C.$$

Pour $r \in]0,1]$, posons $B_{\leqslant}(r) = \{y \in H_{\leqslant} : |I_n - y|_{\mathrm{Mat}} \leqslant r\}$. Soit $\mathcal{A}$ une partie de mesure strictement positive de $H_{>}$. Comme l'application $(y,h) \in H_{\leqslant} \times H_{>} \to yh$ est un difféomorphisme sur un ouvert de $\mathrm{SL}(n,\mathbb{R})$, la partie

$$\mathcal{A}_r = B_{\leqslant}(r)\mathcal{A} = \{yh : y \in B_{\leqslant}(r),\ h \in \mathcal{A}\}$$

est de mesure strictement positive dans $\mathrm{SL}(n,\mathbb{R})$; sa projection dans $\mathcal{R}$ est donc aussi de mesure strictement positive. D'après le lemme précédent, pour tout réel positif t et tout élément y de $B_{\leqslant}(r)$, on a

$$\left| I_n - g_t y g_t^{-1} \right|_{\mathrm{Mat}} \leqslant Cr.$$

D'après l'uniforme continuité de $\ln \phi$, il existe une fonction $\omega(r)$ tendant vers 0 quand r tend vers 0 telle que pour tout h appartenant à $\mathrm{SL}(n,\mathbb{R})$, tout y appartenant à $B_{\leqslant}(r)$ et tout réel positif t,

$$\phi(g_t h\Gamma)(1-\omega(r)) \leqslant \phi(g_t y g_t^{-1} g_t h\Gamma) = \phi(g_t y h\Gamma) \leqslant \phi(g_t h\Gamma)(1+\omega(r)).$$

La première inégalité donne

$$(1-\omega(r)) \lim\sup_{T\to+\infty} \frac{1}{T} \int_0^T \phi(g_t h\Gamma)\, dt \leqslant \lim\sup_{T\to+\infty} \frac{1}{T} \int_0^T \phi(g_t y h\Gamma)\, dt.$$

Supposons que pour tout h appartenant à $\mathcal{A}$, on ait

$$\lim\sup_{T\to+\infty} \frac{1}{T} \int_0^T \phi(g_t h\Gamma)\, dt \geqslant \int_{\mathcal{R}} \phi(\Lambda)\, d\Lambda + \varepsilon.$$

Alors pour r assez petit, l'ensemble $\mathcal{A}_r\Gamma$ est une partie de mesure strictement positive de $\mathcal{R}$ telle que

$$\forall g \in \mathcal{A}_r,\ \lim\sup_{T\to+\infty} \frac{1}{T}\int_0^T \phi(g_t g\Gamma)\, dt > \int_{\mathcal{R}} \phi(\Lambda)\, d\Lambda$$

ce qui contredit le théorème de Birkhoff. Par conséquent

$$\lim\sup_{T\to+\infty} \frac{1}{T}\int_0^T \phi(g_t h\Gamma)\, dt \leqslant \int_{\mathcal{R}} \phi(\Lambda)\, d\Lambda$$

pour presque tout matrice h de la forme M_Θ. On démontre de même que

$$\lim\inf_{T\to+\infty} \frac{1}{T}\int_0^T \phi(g_t h\Gamma)\, dt \geqslant \int_{\mathcal{R}} \phi(\Lambda)\, d\Lambda$$

pour presque tout matrice h de la forme M_Θ. □

Remarque. — On peut extraire un lemme de la démonstration du théorème 1 :

Soit (X, d) un espace métrique, μ une mesure sur X masse totale finie, $g_t : X \to X$, $t \in \mathbb{R}$, un groupe d'automorphisme à un paramètre de (X, μ), Y une partie mesurable de X et ν une mesure sur Y. Supposons que

i) *pour tout y appartenant à Y il existe une partie V_y de X telle que*

$$\forall x \in V_y,\ \forall t \geqslant 0,\ d(g_t(x), g_t(y)) \leqslant Cd(x, y)$$

où C est une constante qui ne dépend pas de y,

ii) *si A est une partie de Y telle que $\nu(A)$ soit non nulle alors pour tout $r > 0$ la partie $\cup_{y\in A}(V_y \cap B(y, r))$ contient une partie A' de X de mesure non nulle.*

Alors pour toute fonction $\phi \in L^1(\mu)$, strictement positive dont le logarithme est uniformément continue, la limite

$$\lim_{T\to\infty} \frac{1}{T}\int_0^T \phi(g_t(y))\, dt$$

existe pour ν-presque tout y de Y. Si de plus, le flot est ergodique alors cette limite vaut presque sûrement $\int_X \phi(x)\, dx$.

4. Deux inégalités.

Nous aurons besoin des deux inégalités qui étendent des inégalités bien connues sur le développement en fraction continue unidimensionnelle :

– $q_{m+1}\,|q_m x - p_m| \leqslant 1$,

– $q_{m+2} \geqslant 2q_m$,

(voir [Ca] ou [Schm]). Les versions multidimensionnelles de ces deux inégalités sont des conséquences simples du principe des tiroirs. La première est prouvée dans [Ch1,2] et la seconde dans [Lag3]. La preuve du théorème 2 utilise de manière cruciale la première inégalité. La seconde inégalité est plutôt une commodité technique.

Proposition 2. — *Il existe une constante $C = C_{k,d}$ ne dépendant que de d et k telle que pour toute matrice $\Theta \in M_{d,k}(\mathbb{R})$ on ait*

$$\forall m \in \mathbb{N}_{>0},\ q_m^k(\Theta) r_{m-1}^d(\Theta) \leqslant C.$$

Remarque. — En changeant éventuellement C et en posant $r_{-1} = 1$ on voit que l'inégalité précédente reste valable pour $m = 0$.

Proposition 3. — *Il existe une constante m_1 ne dépendant que de d et k telle que pour toute matrice $\Theta \in M_{d,k}(\mathbb{R})$, on ait*

$$\forall m \in \mathbb{N},\ q_{m+m_1}(\Theta) \geqslant 2q_m(\Theta).$$

Remarque. — Lorsqu'on remplace les normes euclidiennes par des normes quelconques ces deux inégalités restent valables avec des nouvelles constantes C et m_1.

5. Démonstration du théorème 2.

Soit Θ une matrice $d \times k$. Appelons $(q_m)_{m\geqslant 0}$ la suite des normes des meilleures approximations de la matrice Θ. Pour chaque entier m, posons

$$t_m = \frac{1}{d+k} \ln\left(\frac{q_m}{r_m}\right).$$

Lemme 3. — *Soit $s > 0$. Il existe une constante $\alpha > 0$ ne dépendant que des dimensions k et d, et de s telle que*

$$\int_{t_m}^{t_m+1} \frac{1}{\delta(g_t \Lambda_\Theta)^s}\, dt \geqslant \alpha \left(\left(\frac{q_{m+1}}{q_m}\right)^{\frac{sk}{d+k}} + \left(\frac{r_{m-1}}{r_m}\right)^{\frac{sd}{d+k}} \right).$$

Démonstration. — Pour tout $t \in [t_m, t_m+1]$, on peut majorer $\delta(g_t\Lambda_\Theta)$ grâce au m-ième vecteur meilleure approximation $\binom{Q_m}{P_m}$ de Θ,

$$\begin{aligned}\delta(g_t\Lambda_\Theta) &\leqslant \left|g_t\Lambda_\Theta\begin{pmatrix}Q_m\\P_m\end{pmatrix}\right| = \left|g_t\begin{pmatrix}Q_m\\\Theta Q_m - P_m\end{pmatrix}\right| = \left|\begin{pmatrix}e^{-dt}\,Q_m\\e^{kt}|\Theta Q_m - P_m|\end{pmatrix}\right|\\ &\leqslant e^{-dt}q_m + e^{kt}r_m.\end{aligned}$$

La suite $t_m = \frac{1}{d+k}\ln\frac{q_m}{r_m}$ est définie de telle sorte que $e^{-dt_m}q_m = e^{kt_m}r_m$, donc pour $t \geqslant t_m$, on a

$$e^{-dt}q_m + e^{kt}r_m \leqslant e^{-dt_m}q_m + e^{kt}r_m = (e^{kt_m}+e^{kt})r_m \leqslant 2e^{kt}r_m.$$

Par conséquent,

$$\begin{aligned}\int_{t_m}^{t_m+1}\frac{1}{\delta(g_t\Lambda_\Theta)^s}\,dt \geqslant \int_{t_m}^{t_m+1}\frac{1}{(2r_m)^s}e^{-skt}dt &= \frac{e^{-skt_m}-e^{-sk(t_m+1)}}{sk(2r_m)^s}\\ &= \frac{1}{sk2^s}\times\frac{1}{r_m^s}\left(\frac{r_m}{q_m}\right)^{\frac{sk}{d+k}}(1-e^{-sk})\\ &= \frac{1-e^{-sk}}{sk2^s}\times\left(\frac{1}{q_m^k r_m^d}\right)^{\frac{s}{d+k}}.\end{aligned}$$

Or, d'après la proposition 2, $q_{m+1}^k r_m^d \leqslant C_{d,k}$ donc $q_m^k r_m^d \leqslant C_{d,k}\left(\frac{q_m}{q_{m+1}}\right)^k$. De même, $q_m^k r_{m-1}^d \leqslant C_{d,k}$ donc $q_m^k r_m^d \leqslant C_{d,k}\left(\frac{r_m}{r_{m-1}}\right)^d$. Finalement,

$$\int_{t_m}^{t_m+1}\frac{1}{\delta(g_t\Lambda_\Theta)^s}\,dt \geqslant \frac{1-e^{-sk}}{sk2^sC_{d,k}^{\frac{s}{d+k}}}\times\left(\frac{q_{m+1}}{q_m}\right)^{\frac{sk}{d+k}}$$

et

$$\int_{t_m}^{t_m+1}\frac{1}{\delta(g_t\Lambda_\Theta)^s}\,dt \geqslant \frac{1-e^{-sk}}{sk2^sC_{d,k}^{\frac{s}{d+k}}}\times\left(\frac{r_{m-1}}{r_m}\right)^{\frac{sd}{d+k}}.$$

□

Choisissons s strictement positif assez petit pour que l'intégrale $\int_{\mathcal{R}}\delta^{-s}(\Lambda)\,d\Lambda$ converge (voir appendice). La fonction $\ln\delta^{-s} = -s\ln\delta$ est uniformément continue, donc d'après le théorème 1, pour presque tout Θ appartenant à $M_{d,k}(\mathbb{R})$,

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T\delta(g_t\Lambda_\Theta)^{-s}\,dt = \int_{\mathcal{R}}\delta^{-s}(\Lambda)\,d\Lambda = c.$$

Fixons un tel Θ. D'après la proposition 3, il existe un entier m_1 tel que $t_{i+m_1} \geqslant 1+t_i$, pour tout entier i, donc

$$\frac{1}{t_m}\int_{t_0}^{t_m+1}\delta(g_t\Lambda_\Theta)^{-s}\,dt \geqslant \frac{1}{m_1\times t_m}\sum_{i=0}^{m}\int_{t_i}^{t_i+1}\delta(g_t\Lambda_\Theta)^{-s}\,dt.$$

Grâce au lemme précédent on obtient

$$\frac{1}{t_m}\int_{t_0}^{t_m+1}\delta(g_t\Lambda_\Theta)^{-s}\,dt \geqslant \frac{\alpha'}{t_m}\left(\sum_{i=0}^{m}\left(\frac{q_{i+1}}{q_i}\right)^{\frac{sk}{d+k}}+\sum_{i=0}^{m}\left(\frac{r_{i-1}}{r_i}\right)^{\frac{sd}{d+k}}\right)$$

où α' est une constante strictement positive ($r_{-1} = 0$). En vertu de l'inégalité entre la moyenne géométrique et la moyenne arithmétique,

$$\begin{aligned}&\frac{1}{t_m}\int_{t_0}^{t_m+1}\delta(g_t\Lambda_\Theta)^{-s}\,dt\\ &\geqslant \frac{2\alpha'(m+1)}{t_m}\left(\Pi_{i=0}^{m}\left(\frac{q_{i+1}}{q_i}\right)^{\frac{sk}{d+k}}\left(\frac{r_{i-1}}{r_i}\right)^{\frac{sd}{d+k}}\right)^{\frac{1}{2(m+1)}}\\ &\geqslant \frac{2\alpha' m}{t_m}\left(\frac{q_{m+1}}{q_0}\right)^{\frac{sk}{d+k}\frac{1}{2(m+1)}}\left(\frac{1}{r_m}\right)^{\frac{sd}{d+k}\frac{1}{2(m+1)}}.\end{aligned}$$

En posant $\gamma = \frac{1}{2}\min\left(\frac{sk}{d+k},\frac{sd}{d+k}\right)$, on obtient

$$\begin{aligned}\frac{1}{t_m}\int_{t_0}^{t_m+1}\delta(g_t\Lambda_\Theta)^{-s}\,dt &\geqslant \frac{2\alpha' m}{t_m}\left(\frac{1}{q_0}\right)^{\frac{\gamma}{m+1}}\left(\frac{q_{m+1}}{r_m}\right)^{\frac{\gamma}{m+1}}\\ &\geqslant \frac{2\alpha' m}{t_m}\left(\frac{1}{q_0}\right)^{\frac{\gamma}{m+1}}\left(\frac{q_m}{r_m}\right)^{\frac{\gamma}{m+1}}\\ &\geqslant 2\alpha'\left(\frac{1}{q_0}\right)^{\frac{\gamma}{m+1}}\frac{\exp\left(\frac{\gamma(d+k)m}{m+1}\times\frac{1}{m}t_m\right)}{\frac{1}{m}t_m}\\ &= a\frac{\exp b\frac{1}{m}t_m}{\frac{1}{m}t_m}\end{aligned}$$

où a et b sont deux constantes strictement positives. Comme t_m tend vers l'infini, pour m assez grand, on a

$$a\frac{\exp b\frac{1}{m}t_m}{\frac{1}{m}t_m} \leqslant c+1.$$

Finalement, comme la fonction $a\frac{\exp bt}{t}$ tend vers l'infini quand t tend vers l'infini, $\frac{1}{m}t_m$ est majoré pour m grand, par une constante qui ne dépend que de a, b et c. □

Remarque. — Plaçons nous dans le cas $k = 1$. Il est alors possible de définir une grandeur liée à la croissance des meilleures approximations qui soit presque sûrement constante. Considérons l'ensemble $\mathcal{N}$ des normes sur $\mathbb{R}^d$ de la forme

$$|X|_P = |PX|$$

où P appartient à $\mathrm{SL}(d,\mathbb{Z})$. Si θ est élément de $\mathbb{R}^d$, à chaque matrice P de $\mathrm{SL}(d,\mathbb{Z})$ correspond la suite des meilleures approximations de θ, $(q_n(P,\theta))_{n\in\mathbb{N}}$, définie par la norme $|.|_P$. De même à chaque matrice P de $\mathrm{SL}(n,\mathbb{Z})$ on peut associé la matrice

$$P' = \begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix} \in \mathrm{SL}(d+1,\mathbb{Z})$$

et la norme sur $\mathbb{R}^{d+1}$,

$$|X|'_P = |P'X|$$

($|.|$ désigne encore la norme euclidienne canonique sur $\mathbb{R}^{d+1}$). On définit ainsi une nouvelle fonction longueur du plus court vecteur sur l'espace des réseaux $\mathcal{R}$ par :

$$\delta_P(\Lambda) = \min\{|X|'_P : X \in \Lambda\backslash\{0\}\}.$$

Comme la matrice P' appartient à $\mathrm{SL}(d+1,\mathbb{Z})$ on a

$$\delta_P(\Lambda) = \min\{|P'X| : X \in \Lambda\backslash\{0\}\} = \delta(P'\Lambda)$$

et

$$\int_{\mathcal{R}} \frac{1}{\delta_P^s(\Lambda)}\, d\Lambda = \int_{\mathcal{R}} \frac{1}{\delta^s(\Lambda)}\, d\Lambda.$$

Avec la preuve précédente, on voit alors que pour presque tout $\theta \in \mathbb{R}^d$,

$$\limsup_{n\to\infty} \frac{1}{n} \ln q_n(P,\theta) \leqslant C$$

où C est un réel qui ne dépend pas de P. Par conséquent pour presque tout θ appartenant à $\mathbb{R}^d$ la constante

$$\gamma(\theta) = \sup_{P\in\mathrm{SL}(n,\mathbb{Z})} \left\{ \limsup_{n\to\infty} \frac{1}{n} \ln q_n(P,\theta) \right\}$$

est fini. De plus, pour $\theta \in \mathbb{R}^d$ et $P, Q \in \mathrm{SL}(n,\mathbb{Z})$, on a

$$q_n(P, Q\theta) = q_n(PQ,\theta)$$

donc

$$\gamma(Q\theta) = \gamma(\theta).$$

Par ergodicité de l'action de $\mathrm{SL}(n,\mathbb{Z})$ sur $\mathbb{R}^d/\mathbb{Z}^d$ on en déduit qu'il existe une constante $C < \infty$ telle que pour presque tout θ de $\mathbb{R}^d$, on ait

$$\gamma(\theta) = C.$$

6. Meilleures approximations simultanées de formes linéaires et meilleures approximations de Hermite.

Lemme 4 (Lagarias). — *Soit t un réel et $\binom{Q_t}{P_t}$; $Q = (q_{t,1}, ..., q_{t,k}) \in \mathbb{Z}^k \backslash \{0\}$ et $P_t = (p_{t,1}, ..., p_{t,d}) \in \mathbb{Z}^d$. Si $g_t M_\Theta \binom{Q_t}{P_t}$ est un plus court vecteur du réseau $g_t \Lambda_\Theta$, alors Q_t est une meilleure approximation de la matrice Θ pour les normes euclidiennes sur $\mathbb{Z}^k$ et $\mathbb{R}^d$.*

Nous rappelons la démonstration de ce lemme qui est très simple. Soit Q un vecteur non nul de $\mathbb{Z}^k$ tel que $|Q| < |Q_t|$ et P un élément de $\mathbb{Z}^d$. On a par définition du plus court vecteur,

$$\left| g_t M_\theta \begin{pmatrix} Q_t \\ P_t \end{pmatrix} \right| \leqslant \left| g_t M_\theta \begin{pmatrix} Q \\ P \end{pmatrix} \right|$$

donc

$$e^{-2dt} \left|Q_t\right|^2 + e^{2kt} \left|M_\Theta Q_t - P_t\right|^2 \leqslant e^{-2dt} \left|Q\right|^2 + e^{2kt} \left|M_\Theta Q - P\right|^2.$$

Or $e^{-2dt} \left|Q_t\right|^2$ est strictement supérieure à $e^{-2dt} \left|Q\right|^2$ donc

$$\left|M_\Theta Q_t - P_t\right|^2 < \left|M_\Theta Q - P_t\right|^2.$$

De même, si $|Q| = |Q_t|$ on obtient

$$\left|M_\Theta Q_t - P_t\right|^2 \leqslant \left|M_\Theta Q - P_t\right|^2,$$

donc Q_t est une meilleure approximation de Θ.

Nous avons besoin de deux lemmes qui ne se trouvent pas explicitement dans les travaux de Lagarias. Leurs démonstrations sont faciles.

Lemme 5. — *Soit $s > t$ deux réels. Si $g_t M_\Theta \binom{Q_t}{P_t}$ et $g_s M_\Theta \binom{Q_s}{P_s}$ sont des plus courts vecteurs des réseaux $g_t \Lambda_\Theta$ et $g_s \Lambda_\Theta$ alors $|Q_s| \geqslant |Q_t|$.*

Démonstration. — Notons $g_t \Lambda_\theta \binom{Q_t}{P_t} = \binom{e^{-dt} Q_t}{e^{kt} \varepsilon_t}$ et $g_s \Lambda_\theta \binom{Q_s}{P_s} = \binom{e^{-ds} Q_s}{e^{ks} \varepsilon_s}$. Comme ces vecteurs sont des plus courts vecteurs des réseaux $g_t \Lambda_\Theta$ et $g_s \Lambda_\Theta$, on a

$$\begin{aligned} e^{-2dt} \left|Q_t\right|^2 + e^{2kt} \left|\varepsilon_t\right|^2 &\leqslant e^{-2dt} \left|Q_s\right|^2 + e^{2kt} \left|\varepsilon_s\right|^2 \\ e^{-2ds} \left|Q_s\right|^2 + e^{2ks} \left|\varepsilon_s\right|^2 &\leqslant e^{-2ds} \left|Q_t\right|^2 + e^{2ks} \left|\varepsilon_t\right|^2, \end{aligned}$$

d'où (avec $n = d + k$)

$$\begin{aligned} e^{2nt}(\left|\varepsilon_t\right|^2 - \left|\varepsilon_s\right|^2) &\leqslant \left|Q_s\right|^2 - \left|Q_t\right|^2 \\ \left|Q_s\right|^2 - \left|Q_t\right|^2 &\leqslant e^{2ns}(\left|\varepsilon_t\right|^2 - \left|\varepsilon_s\right|^2). \end{aligned}$$

Par conséquent,

$$e^{2nt}(|\varepsilon_t|^2 - |\varepsilon_s|^2) \leqslant e^{2ns}(|\varepsilon_t|^2 - |\varepsilon_s|^2),$$

et comme $s > t$, on obtient successivement $|\varepsilon_t|^2 - |\varepsilon_s|^2 \geqslant 0$, puis $|Q_s| \geqslant |Q_t|$. □

Lemme 6. — *Il existe une constante m_2 ne dépendant que de d et k telle que pour toute matrice Θ appartenant à $M_{d,k}(\mathbb{R})$, on ait*

$$\forall m \in \mathbb{N},\ r_{m+m_2}(\Theta) \leqslant \frac{1}{2} r_m(\Theta).$$

Démonstration. — On va utiliser deux fois le principe des tiroirs. Il existe une constante D ne dépendant que de d telle que si $x_1, ..., x_D$ sont des points de $\mathbb{R}^d$ à une distance inférieure ou égale à r de 0 alors deux de ces points sont à une distance inférieure à $\frac{1}{2}r$. Il existe une constante K ne dépendant de k et des cônes $\mathcal{C}_1, ..., \mathcal{C}_K$ de sommets 0 inclus dans $\mathbb{R}^k$ tels que

$$\mathbb{R}^k = \mathcal{C}_1 \cup ... \cup \mathcal{C}_K$$

et

$$\forall i \in \{1, ..., K\},\ \forall x_1, x_2 \in \mathcal{C}_i,\ |x_1 - x_2| \leqslant \max(|x_1|, |x_2|).$$

Montrons que $m_2 = DK$ convient. Considérons m_2 meilleures approximations consécutives, $Q_m, ..., Q_{m+m_2-1}$. Avec un choix convenable des P_i dans $\mathbb{Z}^d$, tous les points $\Theta Q_i - P_i$ sont à une distance de 0 inférieure à $r_m(\Theta)$. En appliquant le principe des tiroirs aux cônes $\mathcal{C}_1, ..., \mathcal{C}_K$, on trouve une partie I de $\{m, ..., m + m_2 - 1\}$ de cardinal supérieur à D telle que tous les vecteurs Q_i, $i \in I$, appartiennent au même cône $\mathcal{C}_j$. Comme le cardinal de I est supérieur à D, il existe deux indices $i_1 < i_2$ appartenant à I tels que

$$|(\Theta Q_{i_2} - P_{i_2}) - (\Theta Q_{i_1} - P_{i_1})| \leqslant \frac{1}{2} r_m(\Theta).$$

Comme Q_{i_1} et Q_{i_2} appartiennent aux même cônes $\mathcal{C}_j$, le vecteur $Q = Q_{i_2} - Q_{i_1}$ vérifie

$$|Q| \leqslant \max(|Q_{i_1}|, |Q_{i_2}|) = |Q_{i_2}|,\ \|\Theta Q\| \leqslant \frac{1}{2} r_m(\Theta).$$

Par conséquent, la meilleure approximation Q_{i_0} de norme maximale inférieure ou égale à $|Q|$ vérifie

$$|Q_{i_0}| \leqslant |Q_{i_2}| \text{ et } r_{i_0}(\Theta) \leqslant \frac{1}{2} r_m(\Theta).$$

□

Démonstration du Théorème 3. — Lorsque $h_{m+1} = h_m$ il n'y a rien à démontrer. Plaçons nous dans le cas $h_{m+1} > h_m$.

1. Comme H_m et H_{m+1} sont des meilleures approximations, il existe des entiers n_0 et n_1 tels que $H_m = Q_{n_0}$ et $H_{m+1} = Q_{n_1}$. D'après le Lemme 5 (ou [Lag5]), l'ensemble des t de $\mathbb{R}$ tels que H_m soit le plus court vecteur du réseau $g_t\Lambda_\Theta$ est un intervalle. Appelons $a_m \leqslant b_m$ les extrémités de cet intervalle. Posons $s = e^{-2(k+d)b_m}$. Par définition des plus courts vecteurs et par continuité de la fonction longueur du plus court vecteur, on a

$$\Delta = \|\Theta H_m\|^2 + sh_m^2 = \|\Theta H_{m+1}\|^2 + sh_{m+1}^2$$

et pour tout meilleure approximation Q_n,

$$\|\Theta Q_n\|^2 + s\,|Q_n|^2 \geqslant \Delta.$$

D'après la proposition 3, le nombre de meilleures approximations Q_n telles que

$$\frac{1}{2}h_{m+1} < q_n \leqslant h_{m+1}$$

est inférieure à m_1. Il nous reste donc à compter le nombre de meilleures approximations telles que

$$h_m \leqslant q_n \leqslant \frac{1}{2}h_{m+1}.$$

Comme

$$\|\Theta Q_n\|^2 + sq_n^2 \geqslant \Delta = \|\Theta H_{m+1}\|^2 + sh_{m+1}^2,$$

on a

$$\|\Theta Q_n\|^2 + \frac{1}{4}sh_{m+1}^2 \geqslant \|\Theta H_{m+1}\|^2 + sh_{m+1}^2 \geqslant sh_{m+1}^2,$$

et

$$r_n^2(\Theta) = \|\Theta Q_n\|^2 \geqslant \frac{3}{4}sh_{m+1}^2 \geqslant 3sq_n^2 \geqslant sq_n^2.$$

De même,

$$\|\Theta Q_n\|^2 + sq_n^2 \geqslant \Delta = \|\Theta H_m\|^2 + sh_m^2,$$

donc

$$2r_n^2 = 2\,\|\Theta Q_n\|^2 \geqslant \|\Theta H_m\|^2 = r_{n_0}^2.$$

Finalement, le Lemme 6 donne $n - n_0 \leqslant m_2$.

2. Appelons n_2 le plus grand entiers n tel que $h_m \leqslant q_n \leqslant \frac{1}{2}h_{m+1}$. D'après ce qui précède, nous avons

$$\sqrt{2}r_{n_2} \geqslant r_{n_0}.$$

Grâce à la Proposition 2, nous avons aussi

$$q_{n_2+1}^k r_{n_2}^d \leqslant C_{d,k},$$

et comme $q_{n_2+1} \geqslant \frac{1}{2}h_{m+1}$, nous obtenons

$$\begin{aligned} h_{m+1}^k \left\|\Theta H_m\right\|^d = h_{m+1}^k r_{n_0}^d &\leqslant 2^k q_{n_2+1}^k r_{n_0}^d \\ &\leqslant 2^k q_{n_2+1}^k 2^{d/2} r_{n_2}^d \leqslant 2^{k+d/2} C_{k,d}. \end{aligned}$$

3. Par hypothèse $k = 1$. Soit q_n une meilleure approximation. Cette meilleure approximation est encadrée par deux meilleures approximations de Hermite h_m et h_{m+1}, $h_m \leqslant q_n < h_{m+1}$. Si $q_n \leqslant \frac{1}{2}h_{m+1}$, la démonstration de 1 donne

$$\frac{1}{\sqrt{2}} \left\|h_m\Theta\right\| \leqslant \left\|q_n\Theta\right\| \leqslant \left\|h_m\Theta\right\|.$$

Il nous reste à examiner le cas $\frac{1}{2}h_{m+1} \leqslant q_n < h_{m+1}$. L'inégalité

$$\frac{q_{n+1}}{q_n} \geqslant \frac{r_{n-1} - r_{n+1}}{r_n} \geqslant \frac{r_{n-1}}{r_n} - 1,$$

valable pour toute meilleure approximation, se démontre facilement (cf. [Ch1] Lemme 1.1). Nous en déduisons

$$2 \geqslant \frac{h_{m+1}}{q_n} \geqslant \frac{q_{n+1}}{q_n} \geqslant \frac{r_{n-1}}{r_n} - 1,$$

et par conséquent $r_{n-1}/r_n \leqslant 3$ pour tous les n tels que $\frac{1}{2}h_{m+1} \leqslant q_n < h_{m+1}$. Or le nombre de ces n est inférieur à m_1, donc

$$\frac{r_{n_2}}{r_n} \leqslant 3^{m_1}$$

où n_2 est le plus grand entier tel que k tel que $q_k \leqslant \frac{1}{2}h_{m+1}$. Finalement, nous obtenons

$$\frac{1}{3^{m_1}\sqrt{2}} r_{n_0} \leqslant \frac{1}{3^{m_1}} r_{n_2} \leqslant r_n.$$

□

Remarque. — Soit $\theta = [a_0, a_1, ..., a_n...]$ un réel, les meilleures approximations de Hermite du réel θ forment une sous-suite de la suite $(q_n)_{n\in\mathbb{N}}$ des dénominateurs des réduites de θ. Un examen précis de la preuve précédente montre que les q_n qui ne sont pas des meilleures approximation de Hermite sont tels que $a_{n+1} = 1$. On retrouve ainsi un résultat contenu dans l'article de Grabiner et Lagarias ([Gr,Lag]). Lorsque $\theta = \frac{1+\sqrt{5}}{2} - 2$ on a $q_0 = q_1 = 1$, $q_2 = 2$ et $q_3 = 3$. Mais q_2 n'est pas une meilleure approximation de Hermite.

On déduit immédiatement des théorèmes 2 et 3 le corollaire :

COROLLAIRE 1. — *Il existe une constante C telle que pour presque toute matrice Θ appartenant à $M_{d,k}(\Theta)$,*

$$\limsup_{m\to\infty} \frac{1}{m} \ln h_m \leqslant C.$$

7. Appendice, intégrabilité de la fonction longueur du plus court vecteur.

Notons $d\Lambda$ la mesure sur $\mathcal{R}$ invariante par multiplication à gauche par un élément de $\mathrm{SL}(n,\mathbb{R})$. ($\mathrm{SL}(n,\mathbb{R})$ est unimodulaire).

PROPOSITION 4. — *Pour s strictement positif assez petit on a :*

$$\int_{\mathcal{R}} \delta^{-s}(\Lambda)\, d\Lambda < +\infty.$$

Démonstration. — Rappelons quelques résultats d'intégration dans $\mathrm{SL}(n,\mathbb{R})$ et $\mathcal{R} = \mathrm{SL}(n,\mathbb{R})/\mathrm{SL}(n,\mathbb{Z})$ (voir [Be, Ma]).

7.1. Mesures invariantes.

Appelons $K = SO(n)$ le groupe des isométries positives de $\mathbb{R}^n$ (pour la norme euclidienne), A l'ensemble des matrices diagonales $(a_1, ..., a_n)$ où les a_i, $i = 1, ..., n$, sont des réels strictement positifs dont le produit $a_1...a_n$ vaut 1 et N l'ensemble des matrices triangulaires supérieures dont les éléments diagonaux valent tous 1. Toute matrice m de $\mathrm{SL}(n\mathbb{R})$ se décompose de manière unique sous la forme

$$m = kan$$

où $k \in K$, $a \in A$ et $n \in N$, il s'agit de la décompositions d'Iwasawa. Appelons dk, da, dn les mesures invariantes sur les groupes K, A et N (ces trois groupes sont unimodulaires). La mesure dn est simplement la mesure de Lebesgue sur $\mathbb{R}^{n(n-1)/2}$ et da est l'image de la mesure de Lebesgue sur $\mathbb{R}^{n-1}$ par la réciproque de l'isomorphisme

$$\begin{aligned} \phi : A &\to \mathbb{R}^{n-1} \\ : (a_1, ..., a_n) &\to \Big(\ln \frac{a_1}{a_2}, ..., \ln \frac{a_{n-1}}{a_n}\Big). \end{aligned}$$

Pour $a = (a_1, ..., a_n) \in A$, posons $\rho(a) = \Pi_{i<j} \frac{a_i}{a_j}$. La mesure invariante sur $\mathrm{SL}(n,\mathbb{R})$ est l'image de la mesure $\rho(a) dk\, da\, dn$ sur $K \times A \times N$ par

l'homéomorphisme $(k,a,n) \to kan$. Ainsi, pour toute fonction mesurable positive sur $\mathcal{R}$ on a

$$\int_{\mathcal{R}} f(\Lambda)\,d\Lambda = \int_K \int_A \int_N f(kan)\rho(a)\,dk\,da\,dn$$
$$\int_K \int_{\mathbb{R}^{n-1}} \int_N f(k\phi^{-1}(y)n)\rho(\phi^{-1}(y))\,dk\,dy\,dn$$

où dy est la mesure de Lebesgue sur $\mathbb{R}^{n-1}$.

7.2. Domaine de Siegel.

Soit t un réel strictement positif et u un réel. Posons

$$\begin{aligned} A_t &= \Big\{(a_1,...,a_n) \in A : \frac{a_i}{a_{i+1}} \leqslant t,\ i=1,...,n-1\Big\}, \\ N_u &= \{n=(n_{ij}) \in N : |u_{ij}| \leqslant u,\ 1 \leqslant i < j \leqslant n\}, \\ S_{t,u} &= KA_tN_u. \end{aligned}$$

Le théorème de Siegel affirme que si $t \geqslant \frac{2}{\sqrt{3}}$ et $u \geqslant \frac{1}{2}$ alors $S_{t,u}$ contient un domaine fondamental pour l'action de $\mathrm{SL}(n,\mathbb{Z})$ sur $\mathrm{SL}(n,\mathbb{R})$ (voir [Be, Ma], p. 142). On en déduit que pour toute fonction f mesurable positive sur $\mathcal{R}$ on a

$$\begin{aligned} \int_{\mathcal{R}} f(\Lambda)\,d\Lambda &\leqslant \int_K \int_{A_t} \int_{N_t} f(kan\Gamma)\rho(a)\,dk\,da\,dn \\ &= \int_K \int_{\phi(A_t)} \int_{N_t} f(k\phi^{-1}(y)n\Gamma)\rho(\phi^{-1}(y))\,dk\,dy\,dn \end{aligned}$$

où $\Gamma = \mathrm{SL}(n,\mathbb{Z})$. Clairement,

$$\phi(A_t) \subset \{(y_1,...,y_{n-1}) : y_i \leqslant \ln t,\ i=1,...,n-1\}$$

et on vérifie que

$$\rho(\phi^{-1}(y)) = \prod_{i=1}^{n-1} \exp r_i y_i$$

où les r_i sont des entiers strictement positifs. Par conséquent,

$$\int_{\mathcal{R}} f(\Lambda)\,d\Lambda \leqslant \int_K \int_{\phi(A_t)} \int_{N_t} f(k\phi^{-1}(y)n\Gamma) \prod_{i=1}^{n-1} \exp r_i y_i\,dk\,dy\,dn.$$

7.3. Majoration de $\int_{\mathcal{R}} \delta^{-s}(\Lambda)\,d\Lambda$.

La fonction longueur du plus court vecteur d'un réseau est invariante par l'action (à gauche) d'une isométrie donc l'intégration sur K ne "compte pas" :

$$\int_{\mathcal{R}} \delta^{-s}(\Lambda)\, d\Lambda \leqslant \int_K dk \int_{\phi(A_t)} \int_{N_t} \delta^{-s}(\phi^{-1}(y)n\Gamma) \prod_{i=1}^{n-1} \exp r_i y_i \, dy\, dn$$
$$\ll \int_{\phi(A_t)} \int_{N_t} \delta^{-s}(\phi^{-1}(y)n\Gamma) \prod_{i=1}^{n-1} \exp r_i y_i \, dy\, dn.$$

Minorons la fonction $\delta(\Lambda)$ pour le réseau Λ représenté par une matrice $m = an$ de AN. Appelons $X_1, ..., X_n$ les vecteurs colonnes de la matrice m. Supposons que X_{i_0} soit le vecteur de norme minimum. D'après le théorème des minima de Minkowski,

$$|X_1| \ldots |X_{i_0-1}|\, \delta(\Lambda)\, |X_{i_0+1}| \ldots |X_n| \gg 1,$$

donc

$$\frac{1}{\delta(\Lambda)} \ll |m|^{n-1}$$

où $|m|$ désigne la norme euclidienne de la matrice m. Lorsque n appartient à N_u on a $|n| \ll 1 + u$, donc si $u = \frac{1}{2}$ on a $|an| \ll |a|$. Fixons $t = \frac{\sqrt{3}}{2}$ et $u = \frac{1}{2}$. Pour $\Lambda = an$ avec $a \in A_t$ et $n \in N_u$, on a donc

$$\frac{1}{\delta(\Lambda)} \ll |a|^{n-1}.$$

D'où

$$\int_{\mathcal{R}} \delta^{-s}(\Lambda)\, d\Lambda \ll \int_{\phi(A_t)} \int_{N_u} \left|\phi^{-1}(y)\right|^{(n-1)s} \prod_{i=1}^{n-1} \exp r_i y_i \, dy\, dn,$$

et comme N_u est borné

$$\int_{\mathcal{R}} \delta^{-s}(\Lambda)\, d\Lambda \ll \int_{\phi(A_t)} \left|\phi^{-1}(y)\right|^{(n-1)s} \prod_{i=1}^{n-1} \exp r_i y_i \, dy.$$

Il nous reste à évaluer $\left|\phi^{-1}(y)\right|$ pour y dans $\mathbb{R}^{n-1}$. L'application ϕ est la composée de l'application

$$A \to H = \{(x_1, ..., x_n) \in \mathbb{R}^n : x_1 + ... + x_n = 0\}$$
$$(a_1, ..., a_n) \to (\ln a_1, ..., \ln a_n)$$

et de l'application linéaire

$$L : H \to \mathbb{R}^{n-1}$$
$$: (x_1, ..., x_n) \to (x_1 - x_2, ..., x_{n-1} - x_n).$$

Comme L est bijective, il existe une constante C telle que pour tout $y \in \mathbb{R}^{n-1}$ on ait $\left|L^{-1}(y)\right| \leqslant C\,|y|$, on en déduit que

$$\left|\phi^{-1}(y)\right| \ll \exp C\,|y|.$$

Finalement on obtient

$$\int_{\mathcal{R}} \delta^{-s}(\Lambda)\, d\Lambda \ll \int_{\phi(A_t)} \left|\phi^{-1}(y)\right|^{(n-1)s} \prod_{i=1}^{n-1} \exp r_i y_i \, dy$$

$$\ll \int_{\{(y_1,\dots,y_{n-1}):y_i \leqslant \ln t\}} \exp C(n-1)s\,|y| \prod_{i=1}^{n-1} \exp r_i y_i \, dy$$

et cette dernière intégrale est finie pour s suffisamment petit. □

BIBLIOGRAPHIE

[Be, Ma] M.B. Bekka & M. Mayer, Ergodic Theory and Topological Dynamics of Group Actions on Homogeneous Spaces, London Mathematical Society, Lecture Note Series, 269 (2000).

[Br1] A.J. Brentjes, A two-dimensional continued fraction algorithm for best approximations with an application in cubic fields, J. Reine Angew. Math., 326 (1981), 18–44.

[Br2] A.J. Brentjes, Multi-dimensional continued fraction algorithms, Mathematical Center Tracts, 145, Math. Centrum, Amsterdam, (1981).

[Br,Gu] A. Broise-Alamichel, Y. Guivarc'h, Exposants caractéristiques de l'algorithme de Jacobi-Perron et de la transformation associée, Annales Institut Fourier, 51 (2001), n° 3, 565–686.

[Ca] J.W.S. Cassels, An Introduction to Diophantine Approximation, Cambridge Tracts in Mathematics and Mathematical Physics, 45, Cambridge Univ. Press (1965).

[Ch1] N. Chevallier, Distances dans la suite des multiples d'un point du tore à deux dimensions, Acta Arith., 74 (1996), 47–59.

[Ch2] N. Chevallier, Meilleures approximations d'un élément du tore $\mathbb{T}^2$ et géométrie de la suite des multiples de cet élément, Acta Arith., 78 (1996), 19–35.

[Ch3] N. Chevallier, Géométrie des suites de Kronecker, Manuscripta Math., 94 (1997), 231–241.

[Ch4] N. Chevallier, Meilleures approximations diophantiennes d'un élément du tore $\mathbb{T}^d$, Acta Arith., 97 (2001), 219–240.

[Ch5] N. Chevallier, Meilleures approximations diophantiennes simultanées, Cahiers du séminaire de probabilités, Rennes (2002).

[Gr, Lag] D.J. Grabiner, J.C. Lagarias, Cutting Sequences for Geodesic Flow on the Modular Surface and Continued Fractions, Monatsh, 133 (2001), 295–339.

[Lag1] J.C. Lagarias, Some new results in simultaneous diophantine approximation, Proc. of the Queen's Number Theory Conference 1979 (P. Ribenboim, Ed.), Queen's Paper in Pure and Applied Math., 54 (1980), 453–474.

[Da] S.G. Dani, Divergent trajectories of flows on homogeneous spaces and Diophantine approximation, J. Reine Angew. Math., 359 (1985), 55–89.

[Lag2] J.C. Lagarias, Best simultaneous diophantine approximations I, Growth Rates of Best Approximations denominators, Trans. Amer. Math. Soc., 272, N° 2 (1982), 545–554.

[Lag3] J.C. Lagarias, Best simultaneous diophantine approximations II, behavior of consecutive best approximations, Pacific Journal of Mathematics, 102, N^o 1 (1982), 61–88.

[Lag4] J.C. Lagarias, Best diophantine approximations to a set of linear forms, J. Austral. Math. Soc. Ser. A, 34 (1983), 114–122.

[Lag5] J.C. Lagarias, Geodesic multidimensional continued fractions, Proc. London Math. Soc., (3) 69 (1994), 464–488.

[Ma] G.A. Margulis, Diophantine Approximations, Lattices and flows on Homogeneous Spaces, in A panorama of number theory or the view from Baker garden, Edit. Wüstholz, Zurich 1999, Cambridge Univ. Press, (2002), 280-310.

[Ro] C.A. Rogers, The signature of the errors of some simultaneous Diophantine approximations, Proc. London Math. Soc., 52 (1951), 186–190.

[Schm] W.M. Schmidt, A metrical theorem in diophantine approximation, Canadian J. Math., 12 (1960), 619–631.

[Schw] F. Schweiger, Multidimensional Continued Fractions, Oxford Science Publications, Oxford University Press (2000).

[Sp] V.G. Sprindžuk, Metric Theory of Diophantine Approximations, W.H. Winston Sons, Washington, C. D. (1979).

[Wa] F.W. Warner, Foundations of Differentiable Manifolds and Lie Groups, G.T.M., 94, Springer-Verlag (1983).

Manuscrit reçu le 4 janvier 2005,
Accepté le 28 février 2005.

Nicolas CHEVALLIER,
Université de Haute Alsace
4, rue des frères Lumière
68093 Mulhouse (France)
nicolas.chevallier@uha.fr