ACTA ARITHMETICA
117.3 (2005)

Un théorème de la limite locale pour des algorithmes Euclidiens

par

Aïcha Hachemi (Paris)

1. Introduction. Il est devenu classique d'associer des systèmes dynamiques de l'intervalle à des algorithmes arithmétiques (voir B. Vallée [6]). Dans un article récent [1], V. Baladi et B. Vallée ont étudié certains de ces algorithmes, à savoir les algorithmes "standard", "centré", et "impair", associés à des fonctions coût à croissance modérée. Grâce à une étude du comportement spectral d'un opérateur de transfert et à la formule de Perron, elles ont obtenu un théorème de la limite centrale (théorème 2 ci-dessous) avec vitesse de convergence optimale, et un théorème de la limite locale pour des fonctions coût "réseau" avec la même vitesse de convergence. Nous montrons le deuxième théorème sans vitesse pour des fonctions coût quelconques.

Les trois algorithmes cités ci-dessus sont définis par des divisions euclidiennes. Soient u, v deux entiers tels que $v \geq u \geq 1$. La division classique (qui correspond à l'algorithme Euclidien standard $\mathcal{G}$), $v = mu + r$, produit un entier $m \geq 1$ et un reste entier r tel que $0 \leq r < u$. La *division centrée* (l'algorithme centré $\mathcal{K}$) exige que $v \geq 2u$ et prend la forme $v = mu + s$ avec $s \in [-u/2, +u/2[$. En posant $s = \varepsilon r$ avec $\varepsilon = \pm 1$ (et $\varepsilon = +1$, si $s = 0$), on obtient un reste entier r tel que $0 \leq r \leq u/2$ et un entier $m \geq 2$. La *division impaire* (l'algorithme $\mathcal{O}$) produit un quotient impair : $v = mu + s$ avec m impair et s un entier $s \in [-u, +u[$. En posant $s = \varepsilon r$ avec $\varepsilon = \pm 1$ (et $\varepsilon = +1$, si $s = 0$) on obtient un reste entier r tel que $0 \leq r \leq u$ et un entier $m \geq 1$.

Dans les trois cas, les divisions sont définies par des paires $q = (m, \varepsilon)$, appelées *digits*.

Tout couple d'entiers (u, v) engendre une suite de "transformations fractionnelles linéaires" (TFLs) h dans un ensemble $\mathcal{H}$ ($\mathcal{H}$ dépend de chaque algorithme), qui transforme le quotient r/u en une fonction de u/v. On a $h_{[m,\varepsilon]}(x) = 1/(m + \varepsilon x)$. La TFL qui apparaît dans la dernière étape appartient à $\mathcal{F} \subset \mathcal{H}$ (l'algorithme s'arrête lorsque $r = 0$).

2000 *Mathematics Subject Classification*: Primary 37C30.

Ainsi, chaque algorithme appliqué à un rationnel u/v donne une fraction continue

$$\frac{u}{v} = \cfrac{1}{m_1 + \cfrac{\varepsilon_1}{m_2 + \cfrac{\varepsilon_2}{\ddots + \cfrac{\varepsilon_{P-1}}{m_P}}}},$$

de longueur $P = P(u,v)$, et qui décompose u/v en

$$u/v = h_1 \circ \cdots \circ h_P(0) = h(0),$$

où les $h_i \in \mathcal{H}, 1 \le i \le P-1$, et $h_P \in \mathcal{F}$.

On s'intéresse aux différents coûts associés à l'exécution d'un algorithme. Le coût le plus basique est le nombre d'étapes P. En général, étant donnée une fonction coût c à valeurs non-négatives définie sur $\mathcal{H} :=$ l'ensemble des TFLs associées à l'algorithme, on considère un coût total additif de la forme

$$C(u,v) := \sum_{i=1}^{P(u,v)} c(h_i).$$

On associe à chaque algorithme un système dynamique de l'intervalle $T : \mathcal{I} \to \mathcal{I}$ (avec $\mathcal{I} =]0,1[$ pour $\mathcal{G}$, $\mathcal{I} =]0,1/2]$ pour $\mathcal{K}$ et $\mathcal{I} = [0,1]$ pour $\mathcal{O}$). T est l'extension à $\mathcal{I}$ de l'application définie sur les rationnels en associant r/u à u/v. On obtient

$$T(x) := \left|\frac{1}{x} - A\left(\frac{1}{x}\right)\right|, \qquad x \neq 0, \qquad T(0) = 0,$$

où

$$A(y) := \begin{cases} \text{la partie entière de } y \text{ pour } \mathcal{G}, \\ \text{l'entier le plus proche de } y \text{ pour } \mathcal{K}, \\ \text{l'entier impair le plus proche de } y \text{ pour } \mathcal{O}, \end{cases}$$

et l'ensemble $\mathcal{H} = \{h_{[q]}\}$ est l'ensemble des branches inverses de T. L'ensemble des branches inverses de l'itéré T^n est $\mathcal{H}^n$, ses éléments sont de la forme $h_{[q_1]} \circ \cdots \circ h_{[q_n]}$, où n est appelé *profondeur* de la branche. Les systèmes T associés aux trois algorithmes $\mathcal{G}$, $\mathcal{K}$, $\mathcal{O}$ appartiennent à la "bonne classe" des "applications complètes par morceaux", que l'on définit comme suit :

Définition 1. Une application $T : \mathcal{I} \to \mathcal{I}$ est *complète par morceaux* s'il existe un ensemble $\mathcal{Q}$ (fini ou dénombrable) et une partition d'ouverts $\{\mathcal{I}_q\}_{q\in\mathcal{Q}}$ (mod un ensemble dénombrable) de l'intervalle $\mathcal{I}$ tels que la restriction de T à $\mathcal{I}_q$ admette une extension bijective de classe $\mathcal{C}^2$ de la clôture de $\mathcal{I}_q$ dans $\mathcal{I}$.

Définition 2. Une application complète par morceaux appartient à la *bonne classe* si :

(i) T est *uniformément dilatante par morceaux*, c'est-à-dire, il existe $C > 0$ et $\widehat{\varrho} < 1$ tels que $|h'(x)| \leq C\widehat{\varrho}^n$ pour tout $h \in \mathcal{H}^n$, toute profondeur n et tout $x \in \mathcal{I}$. Le nombre ϱ défini par

$$\varrho := \limsup_{n\to\infty}(\max\{|h'(x)|\,;\, h \in \mathcal{H}^n,\, x \in \mathcal{I}\})^{1/n}$$

est appelé le *taux de contraction*.

(ii) Il existe $\widehat{K} > 0$, appelée *constante de distorsion*, telle que toute branche inverse h de T vérifie

$$|h''(x)| \leq \widehat{K}|h'(x)| \quad \text{pour tout } x \in \mathcal{I}.$$

(iii) Il existe $\sigma_0 < 1$ tel que $\sum_{h\in\mathcal{H}} \sup|h'|^\sigma < \infty$ pour tout réel $\sigma > \sigma_0$.

(iv) L'application T n'est pas conjuguée à une application affine par morceaux.

Remarque. On vérifie que pour nos algorithmes $\sigma_0 = 1/2$ (voir [3]).

Si $\mathcal{I}$ est muni d'une probabilité (initiale) de densité f_0 par rapport à la mesure de Lebesgue, alors T agit sur $\mathcal{I}$ par $(f_1 dx) = (T_\star(f_0 dx))$. L'opérateur $\mathbf{H}$ tel que $f_1 = \mathbf{H}[f_0]$ est appelé le *transformateur de densité*, ou l'*opérateur de Perron–Frobenius*. Un changement de variable donne

$$\mathbf{H}[f](x) := \sum_{h\in\mathcal{H}} |h'(x)| \cdot f \circ h(x), \qquad \mathbf{H}^n[f](x) := \sum_{h\in\mathcal{H}^n} |h'(x)| \cdot f \circ h(x).$$

Condition $\mathcal{CM}$. Soit $\mathcal{H}$ l'ensemble des branches inverses d'une application de la bonne classe. Un coût $c : \mathcal{H} \to \mathbb{R}^+$ est à *croissance modérée* si

$$\sum_{h\in\mathcal{H}} \exp[wc(h)] \cdot |h'(x)|^s$$

converge lorsque $(\Re s, \Re w) \in \Sigma_0 \times W_0$ avec $\Sigma_0 =]\widehat{\sigma}_0, \infty]$ pour $\sigma_0 \leq \widehat{\sigma}_0 < 1$, et $W_0 =]-\infty, \nu_0]$ pour $\nu_0 > 0$.

En posant $\mathcal{H}^\star := \bigcup_{k\geq 1} \mathcal{H}^k$ on peut prolonger le coût en un coût total, qui sera aussi noté c, défini sur $\mathcal{H}^\star$ par

$$c(h_1 \circ \cdots \circ h_k) := \sum_{i=1}^{k} c(h_i).$$

On peut alors définir une version perturbée et pondérée de l'opérateur de transfert dépendant de deux paramètres complexes s et w,

$$\mathbf{H}_{s,w}[f](x) := \sum_{h\in\mathcal{H}} \exp[wc(h)] \cdot |h'(x)|^s \cdot f \circ h(x).$$

Par conséquent (en utilisant la propriété d'additivité du coût total C),

$$\mathbf{H}^n_{s,w}[f](x) := \sum_{h\in\mathcal{H}^n} \exp[wc(h)] \cdot |h'(x)|^s \cdot f \circ h(x).$$

Dans la proposition suivante on cite quelques propriétés de l'opérateur $\mathbf{H}_{s,w}$.

PROPOSITION 1 ([1]). *En posant $s = \sigma + it$, $w = i\tau$, et $R(s,w)$ le rayon spectral de $\mathbf{H}_{s,w}$ et $R_{\mathrm{e}}(s,w)$ son rayon spectral essentiel, et $\mathbf{H}_\sigma := \mathbf{H}_{\sigma,0}$, on a :*

(1) *Si $\sigma \in \Sigma_0$, alors $\mathbf{H}_{s,i\tau}$ est borné sur $C^1(\mathcal{I})$, et il dépend analytiquement de $(s, i\tau)$, $R(s,i\tau) \le R(\sigma)$ et $R_{\mathrm{e}}(s,i\tau) \le \widehat{\varrho} R_{\mathrm{e}}(\sigma)$ (avec $\varrho < \widehat{\varrho} < 1$). De plus l'opérateur $\mathbf{H}_\sigma$ admet une unique valeur propre $\lambda(\sigma)$ réelle, positive, simple et de module maximal, associée à une fonction propre positive.*

(2) *Pour $\sigma \in \Sigma_0$, il existe un* trou spectral, *c'est-à-dire, le rayon spectral sous-dominant r_σ défini par $r_\sigma := \sup\{|\lambda| \,;\, \lambda \in \mathrm{Sp}(\mathbf{H}_\sigma),\ \lambda \ne \lambda(\sigma)\}$, vérifie $r_\sigma < \lambda(\sigma)$.*

(3) *Pour $\sigma \in \Sigma_0$, on définit la* pression *par $\Lambda(\sigma) = \log \lambda(\sigma)$. Notons $\Lambda''_{s^2}, \Lambda''_{\tau^2}$ les dérivées partielles d'ordre 2 de la fonction $\Lambda(s,i\tau)$. Au point $(1,0)$ la pression est strictement convexe en s, c'est-à-dire $\Lambda''_{s^2}(1,0) > 0$. De plus, si c n'est pas constante, alors la pression est strictement convexe par rapport à $i\tau$ en $(1,0)$, c'est-à-dire $\Lambda''_{\tau^2}(1,0) > 0$.*

(4) *Il existe un voisinage complexe $\mathcal{W}$ de 0 et une unique fonction $\sigma : \mathcal{W} \to \mathbb{C}$ tels que $\lambda(\sigma(i\tau), i\tau) = 1$; cette fonction est analytique, $\sigma(0) = 1$, et $\sigma''(0) \ne 0$.*

Pour la preuve voir [1, Sec. 2].

CONDITION UNI. On dit que le système dynamique T vérifie la *condition* UNI si toute branche inverse de T s'étend en une fonction $\mathcal{C}^3$, et si pour tout h, k deux branches inverses de la même profondeur, on note

$$\Psi_{h,k}(x) := \log \frac{|h'(x)|}{|k'(x)|}, \qquad \Delta(h,k) := \inf_{x \in \mathcal{I}} |\Psi'_{h,k}(x)|$$

et pour tout $\eta > 0$,

$$\mathcal{J}(h,k) := \bigcup_{k \in \mathcal{H}^n,\, \Delta(h,k) \le \eta} k(\mathcal{I}),$$

alors,

(a) Pour tout $0 < a < 1$ on a $|\mathcal{J}(h, \varrho^{an})| \ll \varrho^{an}, \forall n, \forall h \in \mathcal{H}^n$.

(b) $\sup\{|\Psi''_{h,k}(x)| \,;\, n \ge 1,\ h,k \in \mathcal{H}^n,\ x \in \mathcal{I}\} < \infty$.

Afin de supprimer l'effet du facteur $|s|$, on définit la norme suivante :

$$\|f\|_{1,t} := \|f\|_0 + \frac{\|f\|_1}{|t|} = \sup|f| + \frac{\sup|f'|}{|t|}.$$

THÉORÈME 1 (Estimations à la Dolgopyat; [1, Sec. 2]). *Soient* $(\mathcal{I}, T, c)$ *avec* T *dans la bonne classe et* c *à croissance modérée, et* ϱ *le taux de contraction, et telle que la condition* UNI *ait lieu. Soit* $\mathbf{H}_{s,w}$ *son opérateur de transfert pondéré agissant sur* $\mathcal{C}^1(\mathcal{I})$. *Pour tout* $r > 0$, *il existe un voisinage complexe* $\Sigma_1 =]1-\alpha, 1+\alpha[$ *de* 1 *et* $M > 0$ *tels que pour tout* $s = \sigma + it$ *avec* $\sigma \in \Sigma_1$ *et* $|t| \geq 1/\varrho^2$, *et tout* $\tau \in \mathbb{R}$,

$$\|(I - \mathbf{H}_{s,i\tau})^{-1}\|_{1,t} \leq M|t|^r.$$

Considérons l'ensemble $\Omega_N := \{(u,v) \in \mathbb{Z}_\star^+ \,;\, \gcd(u,v) = 1,\, u \leq v \leq N\}$, muni de la probabilité uniforme P_N. Dans [4], J. D. Dixon étudie l'algorithme standard et montre que pour $c \equiv 1$ il existe pour tout $\varepsilon > 0$ une constante $C_0 > 0$ telle que

$$|C(u,v) - (12\pi^{-2}\log 2)\log v| < (\log v)^{1/2+\varepsilon} \tag{1.1}$$

soit vérifiée pour toute paire $(u,v) \in \Omega_N$ sauf pour un nombre de paires égal au plus à $N^2 \exp[-C_0(\log N)^{\varepsilon/2}]$; puis dans [5] il montre que la proportion des paires (u,v) telles que $1 \leq u \leq v \leq N$ pour lesquelles

$$0.5 \log v \leq C(u,v) \leq 2.08(\log v + 1)$$

tend vers 1 lorsque $N \to \infty$.

Le résultat qu'on obtient dans cet article ressemble à (1.1), mais il se généralise aux algorithmes $\mathcal{G}, \mathcal{K}, \mathcal{O}$ et à des fonctions coût pas forcément égales à 1. On s'intéresse alors à l'étude de la distribution du coût total $C(u,v)$ associé à un certain coût c (à croissance modérée) ; pour cela on définit sa "fonction génératrice des moments" sur Ω_N :

$$E_N[\exp(i\tau C)] := \frac{\Phi_{i\tau}(N)}{\Phi_0(N)},$$

où $\Phi_{i\tau}(N) = \Phi_{c,i\tau}(N)$ est la valeur cumulée de $\exp(i\tau C)$ sur Ω_N :

$$\Phi_{i\tau}(N) := \sum_{(u,v)\in\Omega_N} \exp[i\tau C(u,v)], \qquad \Phi_0(N) = |\Omega_N|.$$

En suivant le principe défini dans [7], on peut remplacer la suite des fonctions génératrices des moments par une *série de Dirichlet,* qu'on appellera la *fonction génératrice des moments de Dirichlet* :

$$S(s, i\tau) := \sum_{(u,v)\in\Omega} \frac{1}{v^s} \exp[i\tau C(u,v)] = \sum_{n\geq 1} \frac{c_n(i\tau)}{n^s},$$

où

$$\Omega := \{(u,v) \in \mathbb{Z}_\star^+ \,;\, \gcd(u,v) = 1\}, \qquad c_n(i\tau) := \sum_{(u,v)\in\Omega_n,\, v=n} \exp[i\tau C(u,v)].$$

On a

$$\sum_{n\le N} c_n(i\tau) = \Phi_{i\tau}(N).$$

De plus, il est facile de montrer que

$$S(2s, i\tau) = \mathbf{F}_{s,i\tau} \circ (I - \mathbf{H}_{s,i\tau})^{-1}[1](0), \tag{1.2}$$

où

$$\mathbf{F}_{s,i\tau}[f](x) := \mathbf{H}_{s,i\tau}[f \cdot 1_{\cup_{h\in\mathcal{F}} h(\mathcal{I})}](x).$$

Parmi les résultats obtenus par V. Baladi et B. Vallée ([1, Sec. 4]), citons le CLT suivant :

THÉORÈME 2 (Théorème de la limite centrale avec vitesse de convergence). *Pour les algorithmes Euclidiens $\mathcal{G}$, $\mathcal{K}$, $\mathcal{O}$, et tout coût $c \not\equiv 0$ à croissance modérée, en posant $\Lambda(\sigma) := \Lambda(\sigma, 0)$ la fonction de la proposition* 1 : *il existe $\mu(c), \delta(c), K > 0$ tels que, pour tout $N \in \mathbb{N}^*$ et tout $y \in \mathbb{R}$,*

$$\left| P_N\left[(u,v) \;\middle|\; \frac{C(u,v) - \mu(c)\log N}{\delta(c)\sqrt{\log N}} \le y\right] - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} e^{-x^2/2}\, dx \right| \le \frac{K}{\sqrt{\log N}},$$

où

$$\mu(c) = 2\sigma'(0) \quad et \quad \delta^2 = 2\sigma''(0),$$

avec σ la fonction de la proposition 1(4).

Pour un intervalle J de $\mathbb{R}$, on note $|J|$ la mesure de Lebesgue de J. Notre résultat, montré dans la troisième partie, est le théorème suivant :

THÉORÈME 3 (Théorème de la limite locale). *Pour les algorithmes Euclidiens $\mathcal{G}$, $\mathcal{K}$, $\mathcal{O}$ et pour toute fonction coût c à croissance modérée, en posant $\mu(c), \delta^2(c)$ les constantes du théorème* 2, *on a : pour tout intervalle J de $\mathbb{R}$ et tout $\varepsilon > 0$, il existe N_0 tel que pour tout $N \ge N_0$ et tout $x \in \mathbb{R}$,*

$$\left| \sqrt{\log N}\, P_N[(C(u,v) - \mu(c)\log N - \delta(c)x\sqrt{\log N}) \in J] - |J|\, \frac{e^{-x^2/2}}{\delta(c)\sqrt{2\pi}} \right| < \varepsilon. \tag{1.3}$$

2. Estimations de la fonction génératrice des moments. Parmi les conséquences les plus utiles de la proposition 1 est que pour $(s, i\tau) \in \mathcal{W}_1$ un voisinage complexe de $(1, 0)$, on a $\mathbf{H}_{s,i\tau} = \lambda(s, i\tau)\mathbf{P}_{s,i\tau} + \mathbf{N}_{s,i\tau}$, où $\mathbf{P}_{s,i\tau}$ est la projection spectrale associée à $\lambda(s, i\tau)$ et le rayon spectral de $\mathbf{N}_{s,i\tau}$ est $\le \theta$, avec $r_1 < \theta < 1$ (r_1 de la proposition 1).

On montre de plus que pour $(s, i\tau) \in \mathcal{W}_1$,

$$(I - \mathbf{H}_{s,i\tau})^{-1} = \frac{\lambda(s, i\tau)}{1 - \lambda(s, i\tau)}\, \mathbf{P}_{s,i\tau} + (I - \mathbf{N}_{s,i\tau})^{-1}$$

a pour seule singularité dans $\mathcal{W}_1$ un pôle simple en chaque point ($s = \sigma(i\tau), i\tau$), avec résidu l'opérateur non nul

$$\mathbf{R}(i\tau) := \frac{-1}{\lambda'_s(\sigma(i\tau), i\tau)} \mathbf{P}_{\sigma(i\tau),i\tau}.$$

On veut exprimer $E_N[\exp(i\tau C)]$ en quasi-puissance. Pour cela on introduit un autre modèle probabiliste $(\overline{\Omega}_N(\xi), \overline{P}_N(\xi))$ avec $\overline{\Omega}_N(\xi) = \Omega_N$: on fixe une fonction $t \mapsto \xi(T)$, avec $0 \le \xi(T) \le 1$, puis pour un entier N, on choisit uniformément un entier Q entre $N - \lfloor N\xi(N) \rfloor$ et N, ensuite on choisit un élément (u, v) dans Ω_Q.

Dans ce qui suit, la notation $A(l) = O(B(l))$ signifie qu'il existe $M > 0$ tel que $|A(l)| \le M|B(l)|$ pour tout l.

On note $\overline{E}_N[\exp(i\tau C)]$ la fonction génératrice des moments définie sur $(\overline{\Omega}_N(\xi), \overline{P}_N(\xi))$. V. Baladi et B. Vallée [1] obtiennent :

Lemme 1. *Considérons l'un des trois algorithmes $\mathcal{G}$, $\mathcal{K}$, $\mathcal{O}$. Il existe $0 < \alpha_0 < 1/2 = \sigma_0$ (avec σ_0 de la définition 2) tel qu'en posant $\xi(N) = N^{-\alpha_0}$ on ait* :

(a) *La distance entre les distributions $\overline{P}_N(\xi)$ et P_N est $O(\xi(N))$.*

(b) *La fonction génératrice des moments $\overline{E}_N$ de C s'exprime en quasi-puissance. Plus précisément, il existe $0 < \widehat{\alpha}_0 < \alpha_0 < 1/2$ tel que pour toute fonction coût à croissance modérée on ait $1/2 = \sigma_0 < \widehat{\alpha}_0 < \alpha_0$ (avec σ_0 de la définition 2),*

$$\overline{E}_N[\exp(i\tau C)] = \frac{E(i\tau)}{E(0)\sigma(i\tau)} N^{2(\sigma(i\tau)-\sigma(0))}[1 + O(N^{-\widehat{\alpha}_0})]$$

avec un O-terme uniforme par rapport à $N \to \infty$, τ proche de 0, et

$$E(i\tau) = \mathbf{F}_{\sigma(i\tau),i\tau} \circ \mathbf{R}(i\tau)[1](0).$$

Preuve (esquisse — on renvoie à [1, Sec. 4] pour les détails). La première partie du lemme découle de la définition de $\overline{P}_N(\xi)$ et du fait que $|\Omega_N| = KN^2(1 + O((\log N)/N))$, avec $K > 0$ bien défini pour chacun des trois algorithmes (voir [1, Sec. 4.4]).

Posons

$$\Psi_{i\tau}(T) := \sum_{n \le T} c_n(i\tau)(T - n) = \sum_{N \le T} \sum_{n \le N} c_n(i\tau) = \sum_{N \le T} \Phi_{i\tau}(N).$$

En appliquant le théorème de Cauchy sur la série de Dirichlet $S(s, i\tau)$ et le rectangle

$$U(i\tau) = \{s\,;\, \Re s = 1 \pm \widehat{\alpha}\} \times \{s\,;\, \Im s = \pm U\}$$

avec $\widehat{\alpha}_0 < \widehat{\alpha}$ ($s \mapsto S(s, i\tau)$ étant méromorphe sur $U(i\tau)$ lorsque τ est proche de 0), puis la formule de Perron d'ordre 2 qui transforme l'intégrale sur

le rectangle $U(i\tau)$ en une intégrale sur une droite verticale, on obtient la formule de quasi-puissance pour la série $\Psi_{i\tau}(T)$. Ensuite la relation

$$\begin{aligned}\overline{\Phi}_{i\tau}(N) &:= \frac{1}{N\lfloor\xi(N)\rfloor}\sum_{Q=N-\lfloor N\xi(N)\rfloor}^{N}\sum_{n\le Q} c_n(i\tau)\\ &= \frac{1}{N\lfloor\xi(N)\rfloor}\left[\Psi_{i\tau}(N)-\Psi_{i\tau}(N-\lfloor\xi(N)\rfloor)\right]\end{aligned}$$

nous permet de transmettre la quasi-puissance à $\overline{\Phi}_{i\tau}(N)$, puis à $\overline{E}_N$. ∎

Définition 3. Une fonction c est dite *réseau* si elle est non nulle et s'il existe $L_c, L_0 > 0$ tels que L_0/L_c soit irrationnel, et $(c - L_0)/L_c$ à valeurs entières. Le plus grand de ces L_c est appelé *largeur* de c.

Le lemme suivant est une petite généralisation du lemme 15 de [1].

Lemme 2. *On considère l'un des algorithmes $\mathcal{G}$, $\mathcal{K}$, $\mathcal{O}$. Pour toute fonction coût c à croissance modérée, pour tout $0 < L < \infty$ (dans le cas où c est une fonction réseau de largeur L_c, on prend $0 < L \le \pi/L_c$), et tout $0 < \widetilde{\nu}_0 < L$, il existe $\gamma_0 = \gamma_0(L, \widetilde{\nu}_0) > 0$ et $Q = Q(L, \widetilde{\nu}_0) > 0$ tels que pour tout $|\tau| \in [\widetilde{\nu}_0, L]$ on ait, pour $\xi(N) = N^{-\widehat{\alpha}_0}$,*

$$\overline{E}_N[\exp(i\tau C(u,v))] \le QN^{-\gamma_0}, \qquad \forall N \in \mathbb{N}.$$

Preuve. Soit $r > 0$. Le théorème 1 assure l'existence de $\alpha > 0$ tel que pour tout s avec $\Re s = \sigma \le |1 - \alpha|$ et $|\Im s| \ge 1/\varrho^2$ et pour τ arbitraire,

$$\|(I - \mathbf{H}_{s,i\tau})^{-1}\|_{1,t} \le M|t|^r.$$

Supposons que $|t| \le 1/\varrho^2$ et $\tau \in [\widetilde{\nu}_0, L]$. La proposition 1(1), (3) et la condition UNI impliquent que $1 \notin \operatorname{Sp} \mathbf{H}_{1+it,i\tau}$ (voir [1, prop. 1]). Donc d'après la théorie de la perturbation de parties finies du spectre il existe $0 < \gamma_1 < \alpha$ tel que sur l'ensemble compact

$$\{(s,\tau) \in \mathbb{C} \times \mathbb{R}\,;\, |\sigma - 1| \le \gamma_1,\, |t| \le 1/\varrho^2,\, |\tau| \in [\widetilde{\nu}_0, L]\},$$

on ait $1 \notin \operatorname{Sp} \mathbf{H}_{\sigma+it,i\tau}$. En effet, la fonction $s \mapsto \mathbf{H}_{s,i\tau}$ est analytique sur cet ensemble, d'où l'existence de $\widetilde{Q} = \widetilde{Q}(\widetilde{\nu}_0, L)$ tel que

$$\|(I - \mathbf{H}_{1\pm\gamma_1+it,i\tau})^{-1}\|_{1,t} \le \widetilde{Q}.$$

Par conséquent, pour tout $|\tau| \in [\widetilde{\nu}_0, L]$, il existe $Q = Q(\widetilde{\nu}_0, L)$ tel que

$$\|(I - \mathbf{H}_{1\pm\gamma_1+it,i\tau})^{-1}\|_{1,t} \le Q\max(1, |t|^r), \qquad \forall t \in \mathbb{R}. \tag{2.1}$$

Grâce à (1.2), on transforme (2.1) en une estimation de $S(s, i\tau)$ qui, en tant que fonction de s, est analytique sur le rectangle $\widetilde{U}(i\tau) = \{s\,;\, \Re s = 1 \pm \gamma_1\} \times \{s\,;\, \Im s = \pm U\}$ (avec $0 < \gamma_1 < \widehat{\alpha}$, $U > 0$).

Le théorème de Cauchy et la formule de Perron nous permettent de déduire la décroissance de $\overline{\Phi}_{i\tau}(N)$ et par conséquent celle de $\overline{E}_N$ (voir [1, Sec. 5]). ∎

3. Preuve du théorème 3. Posons $n = \log N$ et $q_x(n) = \mu(c)n - \delta(c)x\sqrt{n}$. Rappelons que, par le lemme 1, $|\overline{P}_N(\xi) - P_N| = O(e^{-n\alpha_0})$; il suffit alors de démontrer (1.3) pour $\overline{P}_N$.

Soient $\overline{m}_n = \overline{m}_{x,n}$ une suite de mesures définies sur la tribu des Boréliens de $\mathbb{R}$ par

$$\overline{m}_n(J) := \overline{P}_N[(C(u,v) - q_x(n)) \in J],$$

et $m = m_x$ la mesure définie par

$$m(J) := \frac{e^{-x^2/2}}{\delta(c)\sqrt{2\pi}}\,|J|.$$

On suit la méthode de Breiman ([2, Chap. 10.2]). Pour montrer que $\sqrt{n}\,\overline{m}_n \xrightarrow{w} m$, il suffit de montrer que pour toute fonction ψ non-négative continue et dont la transformée de Fourier $\widehat{\psi}$ est à support compact on ait

$$\sqrt{n}\int \psi\, d\overline{m}_n \to \int \psi\, dm.$$

Cela signifie que pour tout ε fixé, il existe $n_0 \in \mathbb{N}$ (n_0 indépendant de x) tel que pour tout $N \geq N_0$,

$$\left|\sqrt{n}\,\overline{E}_N[\psi(C(u,v) - q_x(n))] - \frac{e^{-x^2/2}}{\sqrt{2\pi}\,\delta(c)}\int \psi(y)\,dy\right| < \varepsilon, \qquad \forall x \in \mathbb{R}.$$

Soit $[-L, +L]$ contenant le support de $\widehat{\psi}$. On a

$$\begin{aligned}\sqrt{n}\,\overline{E}_N[\psi(C(u,v) - q_x(n))] &= \frac{\sqrt{n}}{2\pi}\int_{-L}^{+L} \widehat{\psi}(\tau)\overline{E}_N[\exp(i\tau(C(u,v) - q_x(n)))]\,d\tau \\ &= \frac{\sqrt{n}}{2\pi}\int_{-L}^{+L} \widehat{\psi}(\tau)e^{-i\tau q_x(n)}\overline{E}_N[\exp(i\tau C(u,v)]\,d\tau \\ &=: I^{(n)}.\end{aligned}$$

Soit $0 < \nu_0 < \widetilde{\nu}_0$ avec $\widetilde{\nu}_0$ assez petit (comme dans le lemme 2). Décomposons l'intervalle $[-L, +L]$ en $|\tau| \leq \nu_0$ et $|\tau| \in [\nu_0, L]$, ainsi $I^{(n)}$ se décompose en $I_0^{(n)} + I_1^{(n)}$.

Montrons d'abord que $I_1^{(n)} \to 0$ lorsque $n \to \infty$. En appliquant le lemme 2, on obtient (rappelons que $\gamma_0 = \gamma_0(L, \widetilde{\nu}_0)$)

$$\begin{aligned}|I_1^{(n)}| &\leq \frac{\sqrt{n}}{2\pi}\,QN^{-\gamma_0}\int_{|\tau|\in[\nu_0,L]} |\widehat{\psi}(\tau)|\,d\tau \leq \frac{Q}{2\pi}\,\sqrt{n}\,e^{-n\gamma_0}\int_{|\tau|\in[\nu_0,L]} |\widehat{\psi}(\tau)|\,d\tau \\ &\leq \frac{\widetilde{K}}{n}\int_{|\tau|\in[\nu_0,L]} |\widehat{\psi}(\tau)|\,d\tau = \widetilde{C}/n < \varepsilon/2.\end{aligned}$$

Il suffit de prendre $N > \exp[\widetilde{C}\varepsilon^{-1}]$, où $\widetilde{C} = \widetilde{C}(L, \widetilde{\nu}, \psi)$, $\widetilde{C}$ indépendant de x.

Calculons $I_0^{(n)}$. On suit la méthode de [1, sec. 5]. Rappelons d'abord que d'après la proposition 1(4), $\sigma''(0) \neq 0$, d'où pour ν_0 suffisamment petit, on a $\delta_0 := \inf\{|\Re\sigma''(\tau)|\,;\, \tau \in [-\nu_0, \nu_0]\} > 0$.

Posons $\tau_n := ((\log n)/\delta_0 n)^{1/2}$ et décomposons l'intervalle $[-\nu_0, +\nu_0]$ en $|\tau| \leq \tau_n$ et $|\tau| \in [\tau_n, \nu_0]$. On a

$$I_0^{(n)} = \frac{\sqrt{n}}{2\pi} \int\limits_{|\tau|\leq\tau_n} \widehat{\psi}(\tau) e^{-i\tau q_x(n)} \overline{E}_N[\exp(i\tau C(u,v))]\, d\tau + \frac{\sqrt{n}}{2\pi} \int\limits_{|\tau|\in[\tau_n,\nu_0]} \widehat{\psi}(\tau) e^{-i\tau q_x(n)} \overline{E}_N[\exp(i\tau C(u,v))]\, d\tau.$$

Le 2ème terme est égal à $O(1/\sqrt{n})$. En effet, en rappelant l'expression de $\overline{E}_N$ dans le lemme 1, et que la fonction $g : z \mapsto \sigma(z) - 1 - z\sigma''(0)$ admet un point col en $z = 0$ ($g'(0) = 0$ et $g''(0) \neq 0$), on a

$$\begin{aligned}
&\frac{\sqrt{n}}{2\pi}\Big| \int\limits_{|\tau|\in[\tau_n,\nu_0]} \widehat{\psi}(\tau) e^{-i\tau q_x(n)} \overline{E}_N[\exp(i\tau C(u,v))]\, d\tau\Big| \\
&= \frac{\sqrt{n}}{2\pi}\Big| \int\limits_{|\tau|\in[\tau_n,\nu_0]} \widehat{\psi}(\tau) e^{-i\tau\delta(c)x\sqrt{n}} N^{-i\tau\mu(c)} \overline{E}_N[\exp(i\tau C(u,v))]\, d\tau\Big| \\
&\leq \frac{\sqrt{n}}{2\pi} \sup_{|\tau|\in[\tau_n,\nu_0]} |N^{-i\tau\mu(c)} \overline{E}_N[\exp(i\tau C(u,v))]| \Big| \int\limits_{|\tau|\in[\tau_n,\nu_0]} \widehat{\psi}(\tau) e^{-i\tau\delta(c)x\sqrt{n}}\, d\tau\Big| \\
&\leq \frac{\sqrt{n}}{2\pi} \sup_{|\tau|\in[\tau_n,\nu_0]} \left| e^{2n(\sigma(i\tau)-1-i\tau\sigma'(0))} \frac{E(i\tau)}{E(0)\sigma(i\tau)} (1 + O(e^{-\widehat{\alpha}_0 n}))\right| \int\limits_{\tau\in\mathbb{R}} |\widehat{\psi}(\tau)|\, d\tau.
\end{aligned}$$

On vérifie aisément que les fonctions

$$\begin{aligned}
f_1^{(n)} &: \tau \mapsto \exp[2n(\sigma(i\tau) - 1 - i\tau\sigma'(0))], \\
f_2^{(n)} &: \tau \mapsto \frac{E(i\tau)}{E(0)\sigma(i\tau)}\,(1 + O(e^{-\widehat{\alpha}_0 n}))
\end{aligned}$$

vérifient, pour $|\tau| \leq \nu_0$,

$$|f_1^{(n)}(\tau)| = O(e^{-n\tau^2\delta_0}), \tag{3.1}$$

$$|f_2^{(n)}(\tau)| = O(1 + |\tau| + e^{-n\widehat{\alpha}_0}). \tag{3.2}$$

D'où

$$\frac{\sqrt{n}}{2\pi}\Big| \int\limits_{|\tau|\in[\tau_n,\nu_0]} \widehat{\psi}(\tau)e^{-i\tau q_x(n)}\overline{E}_N[\exp(i\tau C(u,v))]\,d\tau\Big|$$

$$\leq \widetilde{D}(\psi)\,\frac{\sqrt{n}}{2\pi} \sup_{|\tau|\in[\tau_n,\nu_0]} |e^{-n\tau^2\delta_0}(1+|\tau|+e^{-n\widehat{\alpha}_0})|$$

$$\leq \sqrt{n}\,Me^{-n\tau_n^2\delta_0} = \sqrt{n}\,\frac{M}{n} = O(1/\sqrt{n})$$

avec M dépendant de ψ, $\widetilde{\nu}_0$ et indépendant de x.

Rappelons que, par le théorème 2, $\mu(c) = 2\sigma'(0)$ et $\delta^2(c)=2\sigma''(0)$; ainsi,

$$\widetilde{I}_0^{(n)} := \frac{\sqrt{n}}{2\pi} \int\limits_{|\tau|\leq\tau_n} \widehat{\psi}(\tau)e^{-i\tau q_x(n)}\overline{E}_N[\exp(i\tau C(u,v))]\,d\tau$$

$$= \frac{\sqrt{n}}{2\pi} \int\limits_{|\tau|\leq\tau_n} \widehat{\psi}(\tau)e^{-i\tau q_x(n)}e^{2n(\sigma(i\tau)-1)}\,\frac{E(i\tau)}{E(0)\sigma(i\tau)}\,(1+O(e^{-\widehat{\alpha}_0 n}))\,d\tau$$

$$= \frac{\sqrt{n}}{2\pi} \int\limits_{|\tau|\leq\tau_n} \widehat{\psi}(\tau)e^{-i\tau\delta(c)x\sqrt{n}}e^{2n(\sigma(i\tau)-1-i\tau\sigma'(0))}\,\frac{E(i\tau)}{E(0)\sigma(i\tau)}\,(1+O(e^{-\widehat{\alpha}_0 n}))\,d\tau.$$

Posons

$$J_0^{(n)} := \frac{\sqrt{n}}{2\pi} \int\limits_{|\tau|\leq\tau_n} \widehat{\psi}(\tau)e^{-i\tau\delta(c)x\sqrt{n}}e^{2n(\sigma(i\tau)-1-i\tau\sigma'(0))}\,d\tau.$$

Grâce à (3.1) et (3.2), on a

$$\frac{1}{2\pi}|\widetilde{I}_0^{(n)} - J_0^{(n)}| \leq \frac{1}{2\pi} \int\limits_{|\tau|\leq\tau_n} |\widehat{\psi}(\tau)|\,|\tau|e^{-n\tau^2\delta_0} + e^{-n\widehat{\alpha}_0} \int\limits_{|\tau|\leq\tau_n} |\widehat{\psi}(\tau)|e^{-n\tau^2\delta_0}\,d\tau$$

$$\leq \frac{1}{2\pi} \int\limits_{|\tau|\leq\tau_n} |\widehat{\psi}(\tau)|\,|\tau|\,d\tau + \frac{1}{n\widehat{\alpha}_0} \int\limits_{|\tau|\leq\tau_n} |\widehat{\psi}(\tau)|\,d\tau$$

$$\leq K_1/\sqrt{n} + K_2/n = O(1/\sqrt{n}),$$

où K_1, K_2 dépendent de ψ. Ainsi,

$$\widetilde{I}_0^{(n)} = \frac{\sqrt{n}}{2\pi} \int\limits_{|\upsilon|\leq\tau_n\sqrt{n}} \widehat{\psi}(\upsilon/\sqrt{n})e^{-i\tau\delta(c)x\sqrt{n}}e^{2n(\sigma(i\frac{\upsilon}{\sqrt{n}})-1-i\frac{\upsilon}{\sqrt{n}}\sigma'(0))}\,d\upsilon + O(1/\sqrt{n}).$$

D'autre part,

$$|e^{2n(\sigma(i\frac{\upsilon}{\sqrt{n}})-1-i\frac{\upsilon}{\sqrt{n}}\sigma'(0))} - e^{\delta^2(c)\upsilon^2/2}| = O(\upsilon^3/\sqrt{n}),$$

d'où par le théorème de la convergence dominée de Lebesgue, pour tout n suffisamment grand et indépendant de x on a

$$\left|\widetilde{I}_0^{(n)} - \widehat{\psi}(0)\int_{\mathbb{R}} e^{-i\delta(c)x\upsilon}e^{-\delta^2(c)\upsilon^2/2}\,d\upsilon\right| < \varepsilon/2, \qquad \forall x \in \mathbb{R}.$$

Ceci signifie que pour tout ε fixé et n suffisamment grand,

$$\left|I_0^{(n)} - \frac{e^{-x^2/2}}{\delta(c)\sqrt{2\pi}}\int \psi(y)\,dy\right| < \varepsilon/2,$$

uniformément en x. ∎

Remerciements. Je remercie vivement V. Baladi et B. Vallée pour les lectures de cet article et leurs remarques enrichissantes, S. Gouëzel pour sa remarque sur la méthode de Breiman, et S. Khémira et L. Pharamond pour leur précieuse aide informatique.

Références

[1] V. Baladi and B. Vallée, *Euclidean algorithms are Gaussian*, J. Number Theory, to appear.
[2] L. Breiman, *Probability*, Addison-Wesley, Reading, MA, 1968.
[3] A. Broise, *Transformations dilatantes de l'intervalle et théorèmes limites*, Astérisque 238 (1996), 5–109.
[4] J. D. Dixon, *The number of steps in the Euclidean algorithm*, J. Number Theory 2 (1970), 414–422.
[5] —, *A simple estimate for the number of steps in the Euclidean algorithm*, Amer. Math. Monthly 78 (1971), 374–376.
[6] B. Vallée, *Dynamical analysis of a class of Euclidean algorithms*, Theoret. Comput. Sci. 297 (2003), 447–486.
[7] —, *Dynamics of the binary Euclidean algorithms*: *Functional analysis and operators*, Algorithmica 22 (1998), 660–685.

Laboratoire de Géométrie et Dynamique
Institut de Mathématiques de Jussieu
F-75251 Paris, France
E-mail: hachemi@math.jussieu.fr

Reçu le 2.7.2004
et révisé le 6.12.2004 (4800)