Propriétés probabilistes de l'algorithme d'Euclide ; algorithmes rapides de calcul de pgcd.

Véronique Maume-Deschamps

Séminaire d'analyse et probabilités, laboratoire de mathématiques de Brest

10 avril 2008

Institut de Science Financière et d'Assurances (ISFA), Lyon 1.

Coauteurs

Travail en commun avec : Éda Cesaratto, Julien Clément, Benoît Daireaux, Loïck Lhote, Brigitte Vallée.

Algorithmes arithmétiques : problématique.

But : Étudier des paramètres comme le nombre d'itérations, le coût en bit.... d'algorithmes arithmétiques (calcul de pgcd).
Comportement asymptotique moyen et en distribution (analyse en moyenne / en distribution).

Algorithmes arithmétiques : problématique.

But : Étudier des paramètres comme le nombre d'itérations, le coût en bit.... d'algorithmes arithmétiques (calcul de pgcd).
Comportement asymptotique moyen et en distribution (analyse en moyenne / en distribution).
Motivation : Calcul factionnaire, cryptographie à clé publique, calcul formel ....

Algorithmes arithmétiques : problématique.

But : Étudier des paramètres comme le nombre d'itérations, le coût en bit.... d'algorithmes arithmétiques (calcul de pgcd).
Comportement asymptotique moyen et en distribution (analyse en moyenne / en distribution).
Motivation : Calcul factionnaire, cryptographie à clé publique, calcul formel .... Intérêt d'algorithmes rapides.
Euclide classique $\Rightarrow$ complexité en bit moyenne $O(n^2)$ pour des entrées de taille n.
Améliorer cette vitesse par des versions récursives de l'algorithme d'Euclide.

Algorithmes arithmétiques : problématique.

But : Étudier des paramètres comme le nombre d'itérations, le coût en bit.... d'algorithmes arithmétiques (calcul de pgcd).
Comportement asymptotique moyen et en distribution (analyse en moyenne / en distribution).
Motivation : Calcul factionnaire, cryptographie à clé publique, calcul formel .... Intérêt d'algorithmes rapides.
Euclide classique $\Rightarrow$ complexité en bit moyenne $O(n^2)$ pour des entrées de taille n.
Améliorer cette vitesse par des versions récursives de l'algorithme d'Euclide. Estimer la complexité en bit moyenne des versions récursives demande des estimations probabilistes fines sur le déroulement de l'algorithme classique.

Analyse d'algorithme : les questions

Notion de taille sur les entrées, Ω_n : entrées de taille n muni de l'équiprobabilité $\mathbb{P}_n$.
Paramètres d'intérêt C : nombre d'itérations, nombre d'opérations élémentaires (complexité en bits) .... = variable aléatoire sur Ω_n.

Analyse d'algorithme : les questions

Notion de taille sur les entrées, Ω_n : entrées de taille n muni de l'équiprobabilité $\mathbb{P}_n$.
Paramètres d'intérêt C : nombre d'itérations, nombre d'opérations élémentaires (complexité en bits) .... = variable aléatoire sur Ω_n.
Analyse en moyenne $=$ comportement asymptotique de $\mathbb{E}_n(C)$.

Analyse d'algorithme : les questions

Notion de taille sur les entrées, Ω_n : entrées de taille n muni de l'équiprobabilité $\mathbb{P}_n$.
Paramètres d'intérêt C : nombre d'itérations, nombre d'opérations élémentaires (complexité en bits) .... = variable aléatoire sur Ω_n.
Analyse en moyenne $=$ comportement asymptotique de $\mathbb{E}_n(C)$.
Analyse en distribution : $C_n = C_{|\Omega_n}$, distribution asymptotique de C_n.

Analyse d'algorithme : méthodologie

séries génératrices : on veut étudier le comportement asymptotique d'une suite $(a_n)_{n\in\mathbb{N}}$, on considère les séries :

$$SD(s) = \sum_{n\in\mathbb{N}} \frac{a_n}{n^s} \text{ (série de Dirichlet).}$$

Analyse d'algorithme : méthodologie

séries génératrices : on veut étudier le comportement asymptotique d'une suite $(a_n)_{n\in\mathbb{N}}$, on considère les séries :

$$SD(s) = \sum_{n\in\mathbb{N}} \frac{a_n}{n^s} \text{ (série de Dirichlet).}$$

Singularités de la série de Dirichlet $\overset{\text{théorèmes taubériens}}{\Longrightarrow}$ comportement asymptotique des a_n.

Analyse d'algorithme : méthodologie

séries génératrices : on veut étudier le comportement asymptotique d'une suite $(a_n)_{n\in\mathbb{N}}$, on considère les séries :

$$SD(s) = \sum_{n\in\mathbb{N}} \frac{a_n}{n^s} \text{ (série de Dirichlet).}$$

Singularités de la série de Dirichlet $\overset{\text{théorèmes taubériens}}{\Longrightarrow}$ comportement asymptotique des a_n.

Analyse en distribution : série génératrice des moments $\overset{\text{Formule de Perron + Cauchy}}{\Longrightarrow}$ comportement asymptotique de la série génératrice des moments + termes de restes.

Analyse d'algorithme : méthodologie

séries génératrices : on veut étudier le comportement asymptotique d'une suite $(a_n)_{n\in\mathbb{N}}$, on considère les séries :

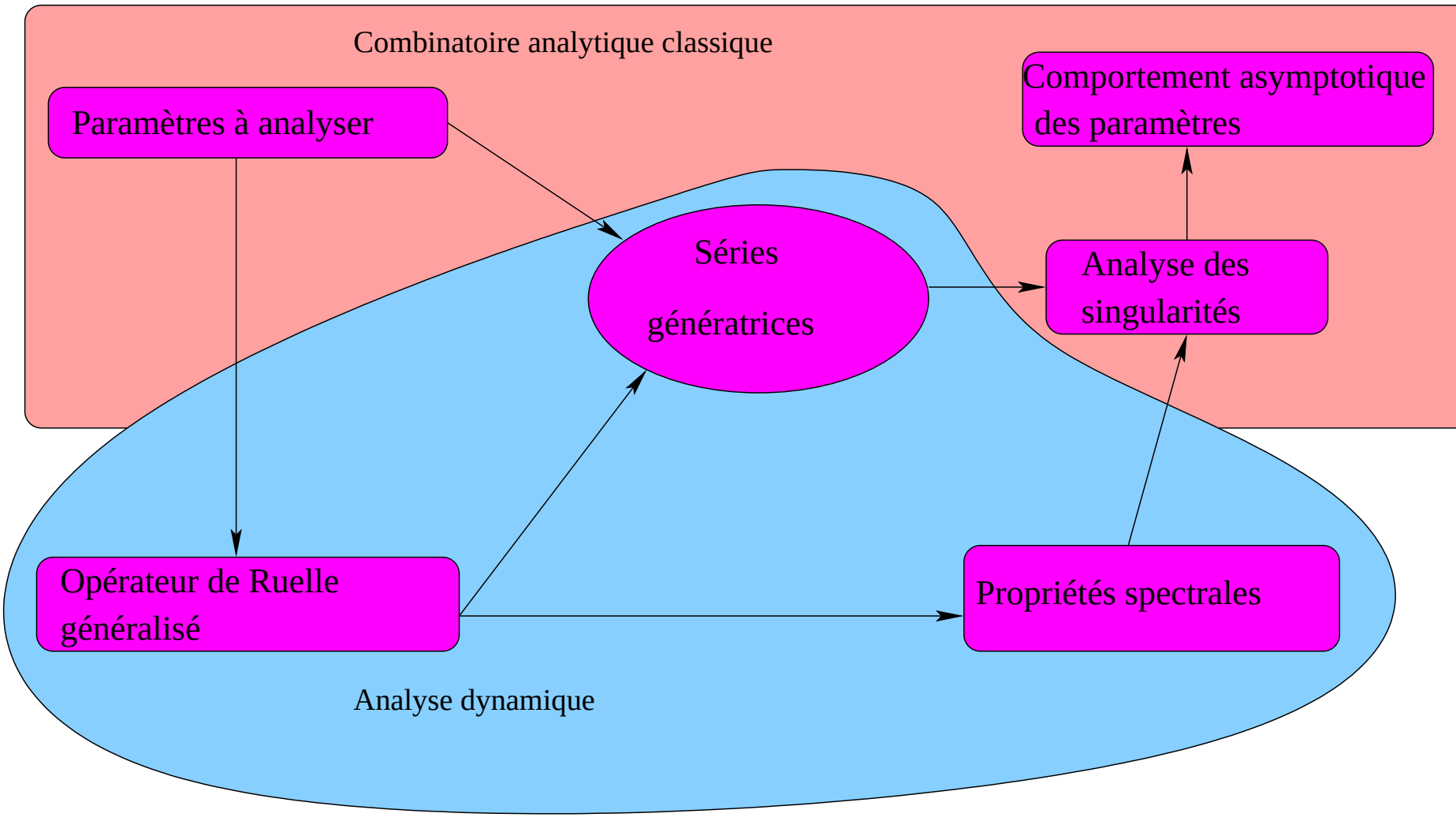
$$SD(s) = \sum_{n\in\mathbb{N}} \frac{a_n}{n^s} \text{ (série de Dirichlet).}$$

Singularités de la série de Dirichlet $\overset{\text{théorèmes taubériens}}{\Longrightarrow}$ comportement asymptotique des a_n.

Analyse en distribution : série génératrice des moments $\overset{\text{Formule de Perron + Cauchy}}{\Longrightarrow}$ comportement asymptotique de la série génératrice des moments + termes de restes.

B. Vallée : propriétés spectrales d'opérateurs associés à des systèmes dynamiques $\Rightarrow$ singularités des séries génératrices. Analyse dynamique d'algorithmes.

Analyse dynamique d'algorithmes : résumé



Calcul de pgcd

- Entrée : Deux entiers (A_1, A_0), $A_1 \leq A_0$,
- Calcul d'une suite de restes et de quotients :

$$A_k = Q_{k+1}A_{k+1} + A_{k+2} \text{ avec } Q_k = \left\lfloor \frac{A_k}{A_{k+1}} \right\rfloor,$$

- Arrêt quand $A_{p+1} = 0$.

L'exécution de l'algorithme est décrite par un produit de matrices :

$$\mathcal{A}_k = Q_{k+1}\mathcal{A}_{k+1}\ \mathcal{A}_k = \begin{pmatrix} A_{k+1} \\ A_k \end{pmatrix}\ Q_k = \begin{pmatrix} 0 & 1 \\ 1 & Q_k \end{pmatrix}.$$

$$\mathcal{A}_0 = \mathcal{M}_{(i)}\mathcal{A}_i \text{ avec } \mathcal{M}_{(i)} = Q_1 Q_2 \dots Q_i.$$

Coût de l'algorithme

Le coût (en bit) de l'algorithme est le nombre d'itérations élémentaires qu'il fait au cours de son exécution.
$\ell(a)$ désigne la taille (binaire) d'un entier a : $\ell(a) = \lfloor \log_2(a) \rfloor + 1$.
Le coût en bit d'une division de la forme $v = mu + r$ est $\ell(u) \cdot \ell(m)$ (division "à la main"). Finalement, le coût en bit de l'algorithme d'Euclide est :

$$\sum_{i=1}^{P} \ell(A_i) \cdot \ell(Q_i) \text{ où } P \text{ est le nombre d'itérations.}$$

On peut considérer des coûts plus généraux de la forme :

$$\sum_{i=1}^{P} c_1(\ell(A_i)) c_2(\ell(Q_i))$$

Quelques résultats antérieurs I

Méthodes probabilistes en théorie des nombres (Hensley) : comportement asymptotique moyen et en distribution du nombre d'itérations de l'algorithme d'Euclide standard.

Quelques résultats antérieurs I

Méthodes probabilistes en théorie des nombres (Hensley) : comportement asymptotique moyen et en distribution du nombre d'itérations de l'algorithme d'Euclide standard.

Analyse en moyenne et en distribution d'algorithmes type Euclide Résultats de Brigitte Vallée + Ali Akhavi, Viviane Baladi, Benoit Daireaux, Loïck Lhotte .... pour diverses variantes, divers coûts.

Quelques résultats antérieurs I

Méthodes probabilistes en théorie des nombres (Hensley) : comportement asymptotique moyen et en distribution du nombre d'itérations de l'algorithme d'Euclide standard.

Analyse en moyenne et en distribution d'algorithmes type Euclide Résultats de Brigitte Vallée + Ali Akhavi, Viviane Baladi, Benoit Daireaux, Loïck Lhotte .... pour diverses variantes, divers coûts.

- Comportement asymptotique moyen du coût moyen (nombre d'itérations, nombre d'apparitions d'un quotient donné ...).

Quelques résultats antérieurs I

Méthodes probabilistes en théorie des nombres (Hensley) : comportement asymptotique moyen et en distribution du nombre d'itérations de l'algorithme d'Euclide standard.

Analyse en moyenne et en distribution d'algorithmes type Euclide Résultats de Brigitte Vallée + Ali Akhavi, Viviane Baladi, Benoit Daireaux, Loïck Lhotte .... pour diverses variantes, divers coûts.

- Comportement asymptotique moyen du coût moyen (nombre d'itérations, nombre d'apparitions d'un quotient donné ...).
- Classification : algorithmes efficaces (nombre d'itérations $O(n)$) vs lents (nombre d'itération $O(n^2)$)

Quelques résultats antérieurs I

Méthodes probabilistes en théorie des nombres (Hensley) : comportement asymptotique moyen et en distribution du nombre d'itérations de l'algorithme d'Euclide standard.

Analyse en moyenne et en distribution d'algorithmes type Euclide

Résultats de Brigitte Vallée + Ali Akhavi, Viviane Baladi, Benoit Daireaux, Loïck Lhotte .... pour diverses variantes, divers coûts.

- Comportement asymptotique moyen du coût moyen (nombre d'itérations, nombre d'apparitions d'un quotient donné ...).
- Classification : algorithmes efficaces (nombre d'itérations $O(n)$) vs lents (nombre d'itération $O(n^2)$)
- Distribution asymptotique du coût moyen (dont complexité en bit).

Quelques résultats antérieurs II

Algorithme d'Euclide standard :

Analyse en moyenne : pour des coûts de la forme

$$C(A_1, A_0) = \sum_{i=1}^{P} c(\ell(A_i))$$

+ condition de moment :

$$\int_I c\varphi < \infty.$$

$\mathbb{E}_n(C) = O(n)$ avec informations précises sur la constante du O. En particulier $\mathbb{E}_n(P) = \mu n + \mu_1 + O(\theta^n)$.

Complexité en bits : $\mathbb{E}_n(B) = \frac{\log 2}{\alpha}\mu(\ell)n^2 + O(n)$.

Quelques résultats antérieurs II

Algorithme d'Euclide standard :

Analyse en moyenne : pour des coûts de la forme

$$C(A_1, A_0) = \sum_{i=1}^{P} c(\ell(A_i))$$

+ condition de moment :

$$\int_I c\varphi < \infty.$$

$\mathbb{E}_n(C) = O(n)$ avec informations précises sur la constante du O. En particulier $\mathbb{E}_n(P) = \mu n + \mu_1 + O(\theta^n)$.

Complexité en bits : $\mathbb{E}_n(B) = \frac{\log 2}{\alpha}\mu(\ell)n^2 + O(n)$.

Analyse en distribution : P_n et B_n sont asymptotiquement normales.

Système dynamique

Les constantes qui apparaissent sont reliés aux propriétés spectrales d'opérateurs de transfert généralisés (opérateurs de Ruelle), associé au système dynamique de Gauss (développement en fractions continues).

$$T(x) = \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor, T(0) = 0.$$

Système dynamique

Les constantes qui apparaissent sont reliés aux propriétés spectrales d'opérateurs de transfert généralisés (opérateurs de Ruelle), associé au système dynamique de Gauss (développement en fractions continues).

$$T(x) = \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor, T(0) = 0.$$

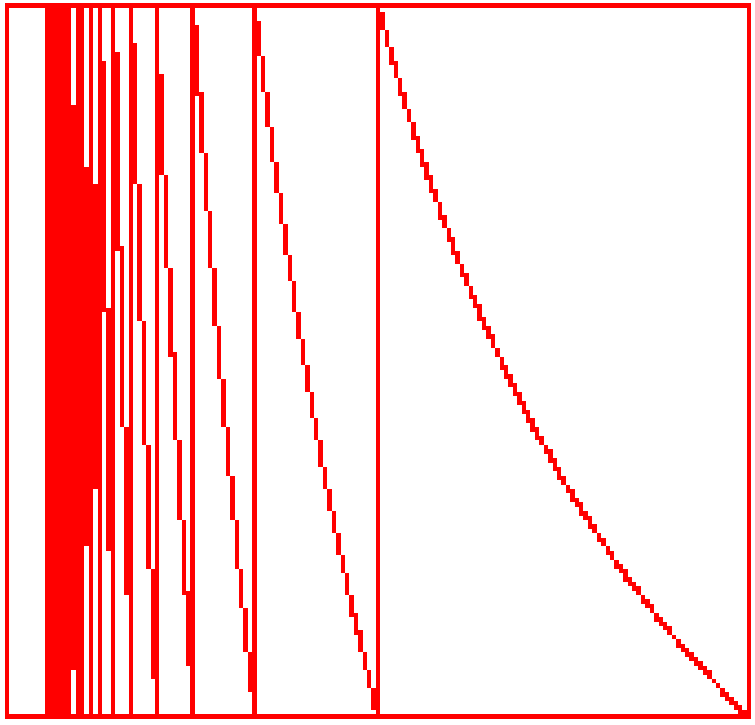
On note $\mathcal{H}$ l'ensemble des branches inverses de T :

$$\mathcal{H} = \left\{ h_q \ : [0,1] \to [\frac{1}{q+1}, \frac{1}{q}], \ / \ h_q(x) = \frac{1}{x+q}, \ q \geq 1 \right\}.$$

$\mathcal{H}^k$ désigne les branches inverses de T^k, ce sont des compositions de la forme $h = h_1 \circ \cdot \circ h_k$, $h_i \in \mathcal{H}$.
$\mathcal{H}^\star = \bigcup_{k \geq 1} \mathcal{H}^k$.

Lien avec l'algorithme d'Euclide

Étant donnée une entrée (A_1, A_0), on considère le rationnel $x = \frac{A_1}{A_0}$, il existe $k \in \mathbb{N}$ tel que $T^k(x) = 0 \Leftrightarrow x = h(0)$, $h = h_1 \circ \cdots \circ h_k$
i.e. une exécution de l'algorithme d'Euclide correspond à une orbite finie du système dynamique $\Leftrightarrow h \in \mathcal{H}^\star$.



Analyse des paramètres.

Exemple du nombre P d'itérations.

$\Omega_n = \{(u,v) \,/\, u \leq v \; \ell(v) = n\}$ ensemble des entrées de taille n.

$\widetilde{\Omega}_n = \{(u,v) \in \Omega_n \,/\, \text{pgcd}(u,v) = 1\}$ ensemble des entrées réduites de taille n.

On veut analyser la variable aléatoire $\widetilde{P}_n = P_{|\widetilde{\Omega}_n}$.

$$\widetilde{c}_P(n) = \sum_{(u,v)\in\widetilde{\Omega}_n} P(u,v),\ \widetilde{c}_P(w,n) = \sum_{(u,v)\in\widetilde{\Omega}_n} e^{wP(u,v)}.$$

$$\widetilde{\mathbb{E}}_n(P) = \frac{\widetilde{c}_P(n)}{\widetilde{c}_1(n)},\ \widetilde{\mathbb{E}}_n(e^{wP}) = \frac{\widetilde{c}_P(n,w)}{\widetilde{c}_1(n)}.$$

Séries de Dirichlet I.

On considère les séries de Dirichlet :

$$\widetilde{F}_P(s) = \sum_{(u,v)\in\widetilde{\Omega}} \frac{P(u,v)}{v^{2s}}, \quad \widetilde{S}_P(ws) = \sum_{(u,v)\in\widetilde{\Omega}} \frac{e^{wP(u,v)}}{v^{2s}}$$

que l'on peut aussi écrire :

$$\widetilde{F}_P(s) = \sum_{N\geq 1} \frac{\widetilde{\mathbf{c}}_P(N)}{N^{2s}}, \quad \widetilde{S}_P(w,s) = \sum_{N\geq 1} \frac{\widetilde{\mathbf{c}}_P(w,N)}{N^{2s}}$$

avec

$$\widetilde{c}_P(n) = \sum_{\ell(N)=n} \widetilde{\mathbf{c}}_P(N), \quad \widetilde{c}_P(w,n) = \sum_{\ell(N)=n} \widetilde{\mathbf{c}}_P(w,N) \ (N \sim 2^n).$$

Séries de Dirichlet II.

Il suffit d'étudier $\widetilde{F}_P(s)$ car on a la relation :

$$F_P(s) = \zeta(2s)\widetilde{F}_P(s).$$

Séries de Dirichlet II.

Il suffit d'étudier $\widetilde{F}_P(s)$ car on a la relation :

$$F_P(s) = \zeta(2s)\widetilde{F}_P(s).$$

On a aussi :

$$\frac{\partial \widetilde{S}(s,w)}{\partial w}|_{w=0} = \widetilde{F}_P(s).$$

Opérateurs de transfert

Opérateur transformateur de densité des systèmes dynamiques :

$$H(f)(x) = \sum_{h \in \mathcal{H}} |h'(x)| f \circ h(x).$$

Opérateurs de transfert

Opérateur transformateur de densité des systèmes dynamiques :

$$H(f)(x) = \sum_{h \in \mathcal{H}} |h'(x)| f \circ h(x).$$

Généralisation (Ruelle), s paramètre complexe

$$H_s(f)(x) = \sum_{h \in \mathcal{H}} |h'(x)|^s f \circ h(x).$$

Opérateurs de transfert

Opérateur transformateur de densité des systèmes dynamiques :

$$H(f)(x) = \sum_{h \in \mathcal{H}} |h'(x)| f \circ h(x).$$

Généralisation (Ruelle), s paramètre complexe

$$H_s(f)(x) = \sum_{h \in \mathcal{H}} |h'(x)|^s f \circ h(x).$$

Bijection entre $\widetilde{\Omega}$ et $\mathcal{H}^\star$: $\frac{u}{v} = h(0)$, on définit $P(h) = P(u,v)$. s et w paramètres complexes

$$H_{s,w}(f)(x) = \sum_{h \in \mathcal{H}} |h'(x)|^s e^{wP(h)} f \circ h(x).$$

Relations avec les séries de Dirichlet

Branches inverses = homographies $\Rightarrow |h'(0)| = \frac{1}{v^2}$.

$$\begin{aligned}\widetilde{S}(s,w) &= \sum_{(u,v)\in\widetilde{\Omega}} \frac{1}{v^{2s}} e^{wP(u,v)} \\ &= \sum_{h\in\mathcal{H}^\star} |h'(0)|^s e^{wP(h)} = (1-H_{s,w})^{-1}(1)(0).\end{aligned}$$

En dérivant par rapport à w, on obtient :

$$\widetilde{F}_P(s) = (1-H_s)^{-1} H_s (1-H_s)^{-1}(1)(0).$$

Relations avec les séries de Dirichlet

Branches inverses = homographies $\Rightarrow |h'(0)| = \frac{1}{v^2}$.

$$\begin{aligned}\widetilde{S}(s,w) &= \sum_{(u,v)\in\widetilde{\Omega}} \frac{1}{v^{2s}} e^{wP(u,v)} \\ &= \sum_{h\in\mathcal{H}^\star} |h'(0)|^s e^{wP(h)} = (1-H_{s,w})^{-1}(1)(0).\end{aligned}$$

En dérivant par rapport à w, on obtient :

$$\widetilde{F}_P(s) = (1-H_s)^{-1} H_s (1-H_s)^{-1}(1)(0).$$

$\Rightarrow$ Étude des propriétés spectrales des opérateurs $H_{s,w}$

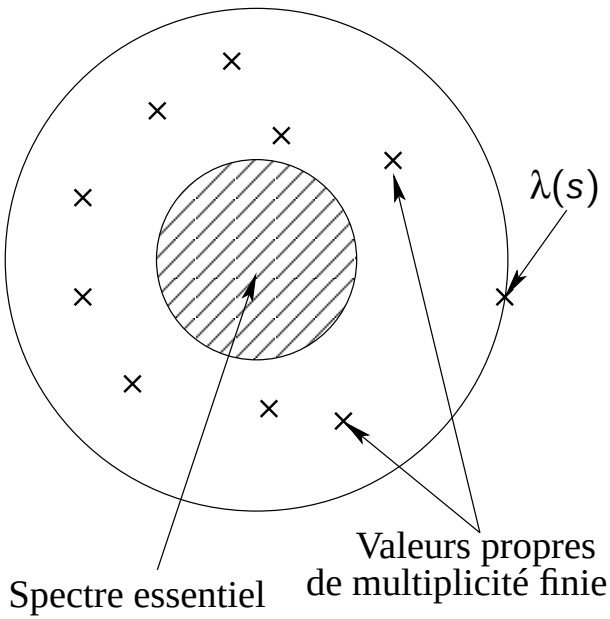
Propriétés spectrales de H_s.

Les opérateurs H_s agissent sur $C^1(I)$,
$s \mapsto H_s$ est analytique sur
$\mathcal{A} := \{s \in \mathbb{C};\ \Re s > 1/2\}$.

Propriétés spectrales de H_s.

Les opérateurs H_s agissent sur $C^1(I)$,
$s \mapsto H_s$ est analytique sur
$\mathcal{A} := \{s \in \mathbb{C};\ \Re s > 1/2\}$.

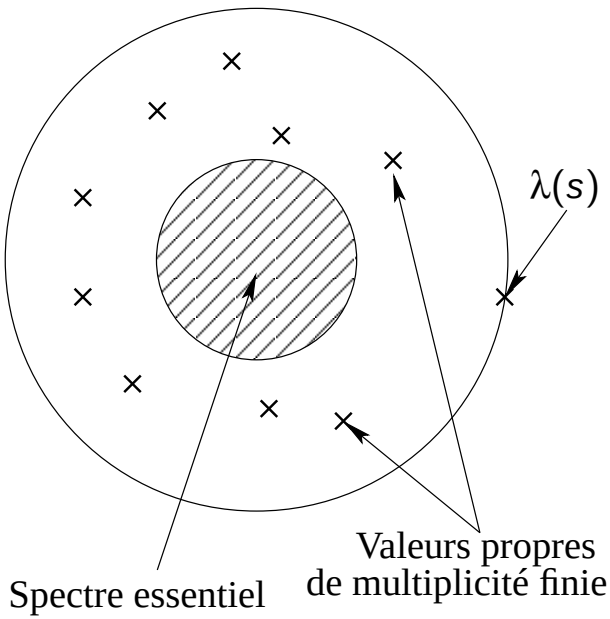
Sur un voisinage complexe de 1, quasi-compacts,
admettent une unique valeur propre dominante simple et isolée $\lambda(s)$, $\lambda(1) = 1$



Propriétés spectrales de H_s.

Les opérateurs H_s agissent sur $C^1(I)$,
$s \mapsto H_s$ est analytique sur
$\mathcal{A} := \{s \in \mathbb{C};\ \Re s > 1/2\}$.

Sur un voisinage complexe de 1, quasi-compacts,
admettent une unique valeur propre dominante simple et isolée $\lambda(s)$, $\lambda(1) = 1$



Pour $\Re(s) \geq 1$, $s \neq 1$, le rayon spectral de H_s est < 1.

Quelles propriétés spectrales pour $H_{s,w}$?

$$\widetilde{S}(s,w) = (1 - H_{s,w})^{-1}(1)(0).$$

Quelles propriétés spectrales pour $H_{s,w}$?

$$\widetilde{S}(s,w) = (1 - H_{s,w})^{-1}(1)(0).$$

Théorème des quasi-puissances (Hwang -1994)

Quelles propriétés spectrales pour $H_{s,w}$?

$$\widetilde{S}(s,w) = (1 - H_{s,w})^{-1}(1)(0).$$

Théorème des quasi-puissances (Hwang -1994)

Formule de Perron + Cauchy $\Longrightarrow$

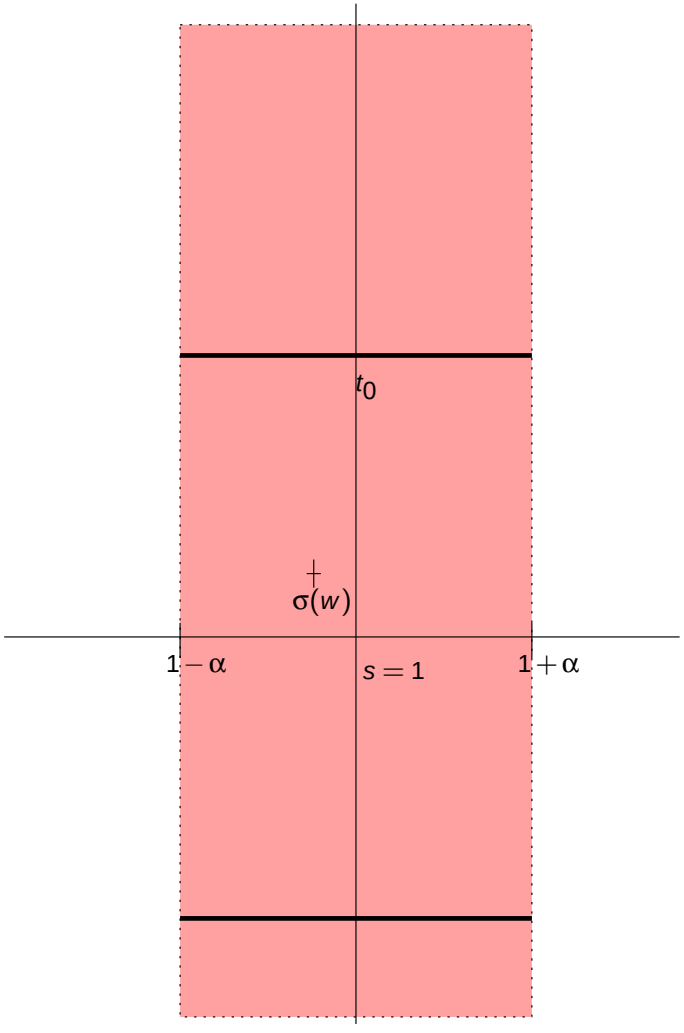
Quelles propriétés spectrales pour $H_{s,w}$?

$$\widetilde{S}(s,w) = (1 - H_{s,w})^{-1}(1)(0).$$

Théorème des quasi-puissances (Hwang -1994)

Formule de Perron + Cauchy $\Longrightarrow$

Recherche d'une bande dans laquelle on contrôle les pôles de $H_{s,w}$.



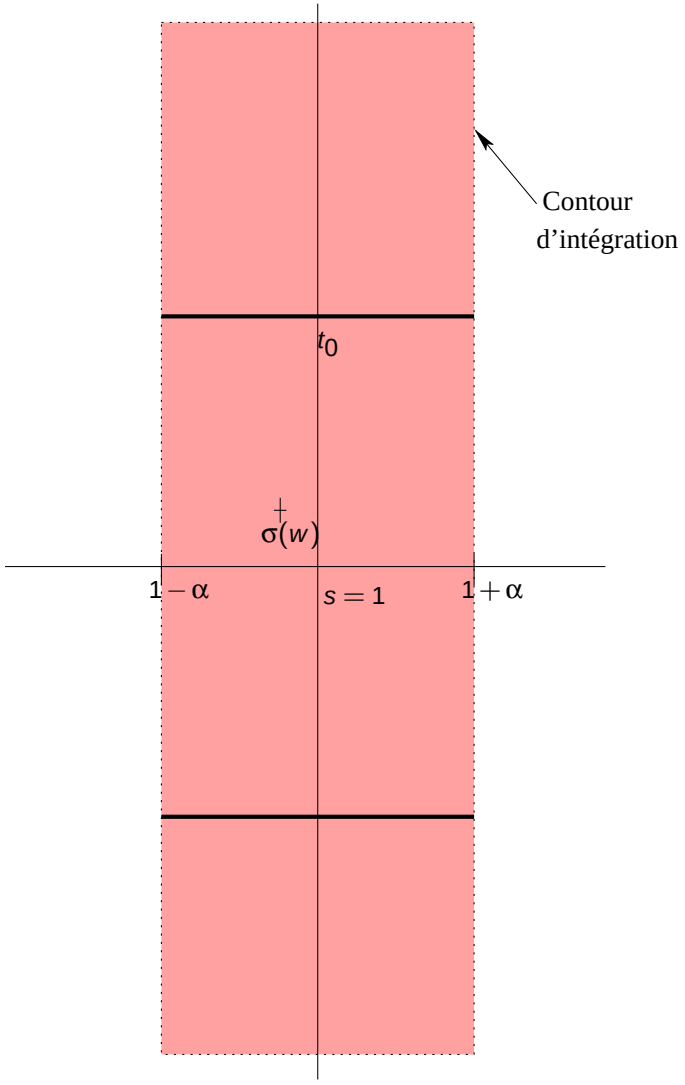
Quelles propriétés spectrales pour $H_{s,w}$?

$$\widetilde{S}(s,w) = (1 - H_{s,w})^{-1}(1)(0).$$

Théorème des quasi-puissances (Hwang -1994)

Formule de Perron + Cauchy $\Longrightarrow$

Recherche d'une bande dans laquelle on contrôle les pôles de $H_{s,w}$. Contour d'intégration : w fixé, $\{z = s + it,\ |1 - s| \leq \alpha,\ |t| \leq t_1\}$, $t_1 \longrightarrow \infty$. Contrôle de $H_{s,w}$ pour $\Im(s) > t_0$



Propriétés spectrales de $H_{s,w}$

Sur un voisinage $\mathcal{W}$ de $w = 0$, il existe un unique $s = \sigma(w)$tel que 1 est valeur propre simple dominante de $H_{s,w}$, $\sigma(0) = 1$, $\sigma(w) \sim 1$ (fonctions implicites).

Théorèmes de perturbations $\Rightarrow$

$$H_{s,w} f = \lambda_{s,w} P_{s,w}(f) + R_{s,w}(f).$$

Dépendance analytique de $\lambda_{s,w}$, $P_{s,w}$, $R_{s,w}$.

Estimations "à la Dolgopiat"

Théorème (Dolgopiat, Baladi-Vallée)

Pour $0 < \xi < \frac{1}{5}$, *il existe* $\Sigma_1 \times W_1$ *voisinage réel de* $(1,0)$ *tel que* $\exists M > 0$, $\gamma < 1$, $t_0 > 0$, *tels que* $\forall n \geq 1$, $s = \sigma + it$, $w = \nu + i\tau$, $(\sigma, \nu) \in \Sigma_1 \times W_1$, *pour* $|t| > t_0$,

$$\|H^n_{s,w}\|_{1,t} \leq M|t|^{\xi}\gamma^n.$$

$\|f\|_{1,t} = \|f\|_\infty + \frac{1}{t}\|f'\|_\infty$.

Application à la série $S(s,w)$.

Estimation de $\sum_{Q\leq N} \mathbf{c}_P(w,Q)(N-Q)$
à l'aide de la formule de Perron.

$$\sum_{Q\leq N} \mathbf{c}_P(w,Q)(N-Q) = \frac{1}{2\pi} \int_{D\pm i\infty} S(s,w) \frac{N^{2s+1}}{s(2s+1)}.$$

Application à la série $S(s,w)$.

Estimation de $\sum_{Q\leq N} \mathbf{c}_P(w,Q)(N-Q)$
à l'aide de la formule de Perron.

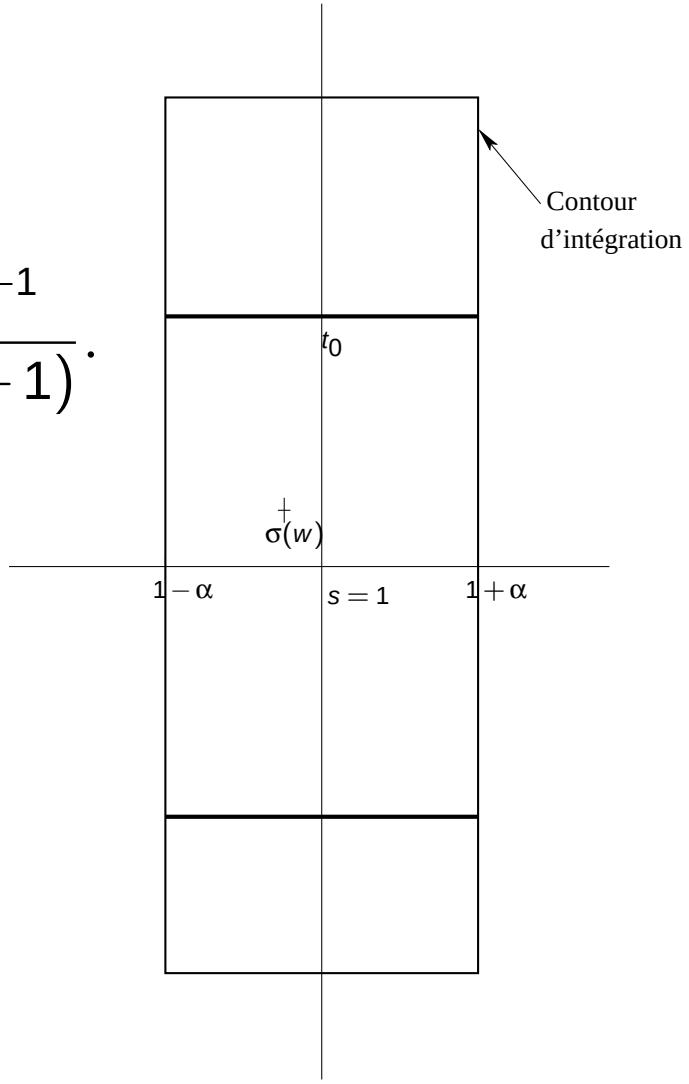
$$\sum_{Q\leq N} \mathbf{c}_P(w,Q)(N-Q) = \frac{1}{2\pi} \int_{D\pm i\infty} S(s,w) \frac{N^{2s+1}}{s(2s+1)}.$$

$$(\mathbf{1}-H_{s,w})^{-1} = \frac{\lambda(s,w)}{1-\lambda(s,w)} P_{s,w} + (\mathbf{1}-R_{s,w})^{-1}.$$

Application à la série $S(s,w)$.

Cauchy $\Rightarrow$

$$\frac{1}{2i\pi}\int_{\mathcal{C}} S(s,w)\frac{N^{2s+1}}{s(2s+1)} = \frac{E(w)N^{2\sigma(w)+1}}{\sigma(w)(2\sigma(w)+1)}.$$

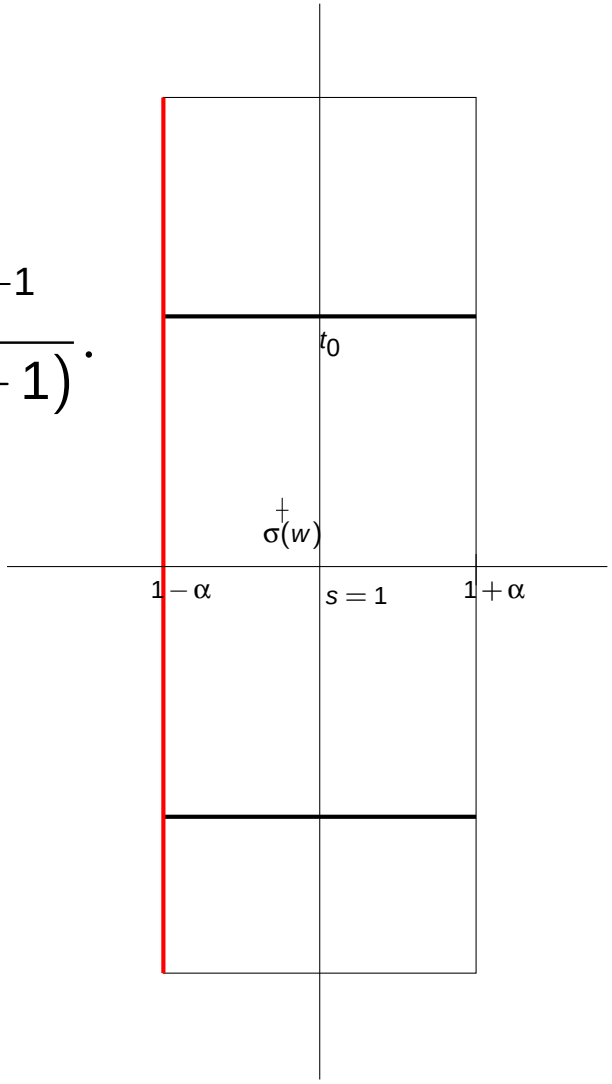


Application à la série $S(s,w)$.

Cauchy $\Rightarrow$

$$\frac{1}{2i\pi}\int_{\mathcal{C}} S(s,w)\frac{N^{2s+1}}{s(2s+1)} = \frac{E(w)N^{2\sigma(w)+1}}{\sigma(w)(2\sigma(w)+1)}.$$

$$\int_{1-\alpha-it}^{1-\alpha+it} S(s,w)\frac{N^{2s+1}}{s(2s+1)} = O(N^{3-2\alpha}).$$



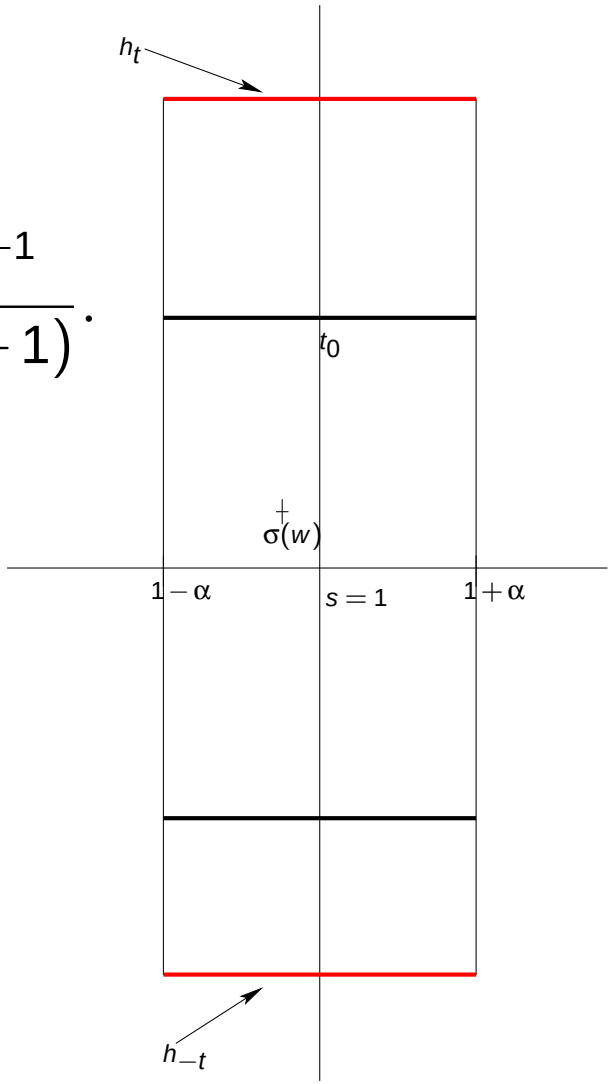
Application à la série $S(s,w)$.

Cauchy $\Rightarrow$

$$\frac{1}{2i\pi}\int_{\mathcal{C}} S(s,w)\frac{N^{2s+1}}{s(2s+1)} = \frac{E(w)N^{2\sigma(w)+1}}{\sigma(w)(2\sigma(w)+1)}.$$

$$\int_{1-\alpha-it}^{1-\alpha+it} S(s,w)\frac{N^{2s+1}}{s(2s+1)} = O(N^{3-2\alpha}).$$

$$\int_{h_{\pm t}} S(s,w)\frac{N^{2s+1}}{s(2s+1)} \xrightarrow{t\to\infty} 0.$$



TLC pour le nombre d'itérations

$$\sum_{Q\leq N} \mathbf{c}_P(w,Q)(N-Q) = \frac{E(w)N^{2\sigma(w)+1}}{\sigma(w)(2\sigma(w)+1)}(1+O(N^{-2\alpha})).$$

Théorème

$$\mathbb{P}_n\left((u,v) \,/\, \frac{P(u,v)-\mu(P)n}{\sqrt{\rho(P)n}} \leq t\right) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{t} e^{\frac{-x^2}{2}}dx + O\left(\frac{1}{\sqrt{n}}\right),$$

avec

$$\mu(P) = \frac{2\log 2}{h(T)} \; et \; \rho(P) = 2\log 2\frac{|\Lambda''(1)|}{\Lambda'(1)^3|}.$$

$\Lambda = \log\lambda$.

Complexité en bit

Pour l'algorithme d'Euclide, on montre que la complexité en bit moyenne (sur Ω_n) est $O(n^2)$ + TCL.
Accélération de l'algorithme en remplaçant des divisions sur des grands entiers par des divisions sur des entiers plus petits + quelques multiplications (rapide) sur des grands entiers.
$\Rightarrow$ idées des Lehmer, Knüth, Schönage = algorithmes récursifs ("diviser pour régner").

Propriété de Jebelean

L'idée de Lehmer est que si (A, B) et (a, b) sont tels que $\frac{A}{B}$ et $\frac{a}{b}$ sont suffisamment proches, alors les suites de quotients coïncident (sur une certaine longueur).

Propriété de Jebelean

$\gamma < 1$, (A, B) une paire de grands entiers, (a, b) tels que :

1. $\ell(b) = \lfloor \gamma \ell(B) \rfloor$,
2. $\left| \frac{A}{B} - \frac{a}{b} \right| \leq \frac{1}{b}$.

Soit a_i la suite des restes de l'algorithme d'Euclide, k le plus petit entier tel que $\ell(a_k) \leq \lfloor \gamma \ell(B)/2 \rfloor$. Alors la suite des quotients q_i calculée par l'algorithme d'Euclide sur (a, b) coïncide avec la suite de quotient Q_i calculée par l'algorithme d'Euclide sur (A, B), pour $i \leq k - 3$.

Suite d'algorithmes interrompus (sur de petits entiers). : $a, b = A, B$ tronqués (on enlève les $(1 - \gamma)$ derniers bits).

Algorithmes interrompus

Algorithm $\widehat{\mathcal{E}}_\delta(A,B)$
$n := \ell(A)$
$i := 1$
$A_1 = A, A_0 = B$
$\mathcal{M}_0 = I$
While $\ell(A_i) > (1-\delta)\cdot n$
$Q_i := \lfloor A_{i-1}/A_i \rfloor$
$A_{i+1} = A_{i-1} - Q_i A_i$
$\mathcal{M}_i = \mathcal{M}_{i-1} \cdot Q_i$
$i++$
Return $(A_{i-3}, A_{i-2}, \mathcal{M}_{i-3})$

Algorithme récursif

Algorithm $\mathcal{HG}(A,B,S)$

1 $n := \ell(B)$
2 If $n \leq S$ then return $\widehat{\mathcal{E}}_{1/2}(A,B)$
3 $\mathcal{M} := I$
4 For $i := 1$ to 2 do
5 $(a_i, b_i) := T_{\frac{1}{2}}(A,B)$
6 $(c_i, d_i, \mathcal{M}_i) := \mathcal{HG}(a_i, b_i, S)$
7 $(C_i, D_i) := \mathcal{M}_i^{-1}(A,B)$
8 $(A,B) := (C_i, D_i)$
9 $\mathcal{M} := \mathcal{M} \cdot \mathcal{M}_i$
10 Return $(A,B,\mathcal{M})$

Algorithm $\mathcal{HG}(A,B)$

$n := \ell(A)$
$S := \log^2 n$
Return $\mathcal{HG}(A,B,S)$

Algorithm $\mathcal{G}(A,B)$

1 $n := \ell(A)$
2 $T := \sqrt{n}\log n$
3 While $\ell(A) \geq T$ do
4 $(AB, \mathcal{M}_1) := \mathcal{HG}(A,B)$
5 Return $gcd(A,B)$

Multiplications rapides

Multiplication naïve de deux entiers de taille n : $O(n^2)$.
Multiplications rapides : Karatsuba, Tom-Cook, FFT, Fürer.
FFT, pour $\ell(u) = n$ et $\ell(v) = Kn$

$$A_1 Kn \log n \log\log n \leq M(u,v) \leq A_2 Kn \log n \log\log n.$$

On note $\mu(n) = n \log n \log\log n$.

Paramètres de l'algorithme interrompu

L'algorithme $\mathcal{E}_\delta$ fait P_δ itérations :

$$P_\delta = \min\{k \ / \ \ell(A_k) \leq (1-\delta)n\}.$$

On note $u_1, \ldots, u_k, \ldots$ les restes successifs produits par l'algorithme et $x_k = \frac{u_{k+1}}{u_k}$ et $x_{<\delta>} = x_k$ si $P_\delta(u,v) = k$.
L'analyse de l'algorithme récursif utilise les distributions de P_δ et $x_{<\delta>}$.
Pour f une densité de probabilité sur $[0,1]$, on considère la probabilité sur Ω_n :

$$\mathbb{P}_{n,f}(u,v) = \frac{1}{|\Omega_n|_f} f(\frac{u}{v}) \quad |\Omega_n|_f = \sum_{(u,v)\in\Omega_n} f(\frac{u}{v}).$$

Normalité asymptotique pour P_δ

On choisit δ_n tel que $\delta_n n \to \infty$ et $(1-\delta_n)n \geq \log n$.

Théorème

La variable aléatoire P_δ sur Ω_n est asymptotiquement gaussienne, avec vitesse de convergence $(\delta_n n)^{-1/3}$ et

$$\mathbb{E}_{n,f}(P_\delta) = \frac{2\log 2}{h(T)}\delta_n n + O(1),$$

$$Var_{n,f}(P_\delta) = 2\log 2 \frac{|\Lambda''(1)|}{|\Lambda'(1)^3|}\delta_n n + O(1).$$

Distribution asymptotique de $\underline{x}_{<\delta>}$.

$\underline{x}_{<\delta>}$ est une version probabilisée de $x_{<\delta>}$: on choisit W uniformément dans

$$I_n(\delta) = [2^{(1-\delta_n)n}(1-(1-\delta_n))2^{-n\rho_n}, 2^{(1-\delta_n)n}].$$

$\underline{P}_\delta$ est le premier entier tel que $u_k \leq W \Rightarrow \underline{x}_{<\delta>}$.

Théorème

$$\mathbb{P}_{nf}[\underline{x}_{<\delta>} \in J] = \int_J \Psi(t)dt \left[1 + O\left(\frac{2^{-n\delta_n}}{1-\delta_n}\right)\right].$$

Où

$$\Psi(x) = \frac{12}{\pi^2} \sum_{m\geq 1} \frac{\log(m+x)}{(m+x)(m+x+1)} \text{ proportionnel à } \frac{\partial}{\partial s} H_s|_{s=1}(\varphi).$$

$\varphi(x) = \frac{1}{\log 2}\frac{1}{1+x}$ *est la densité invariante par* T.

Algorithme de calcul de pgcd sous quadratique

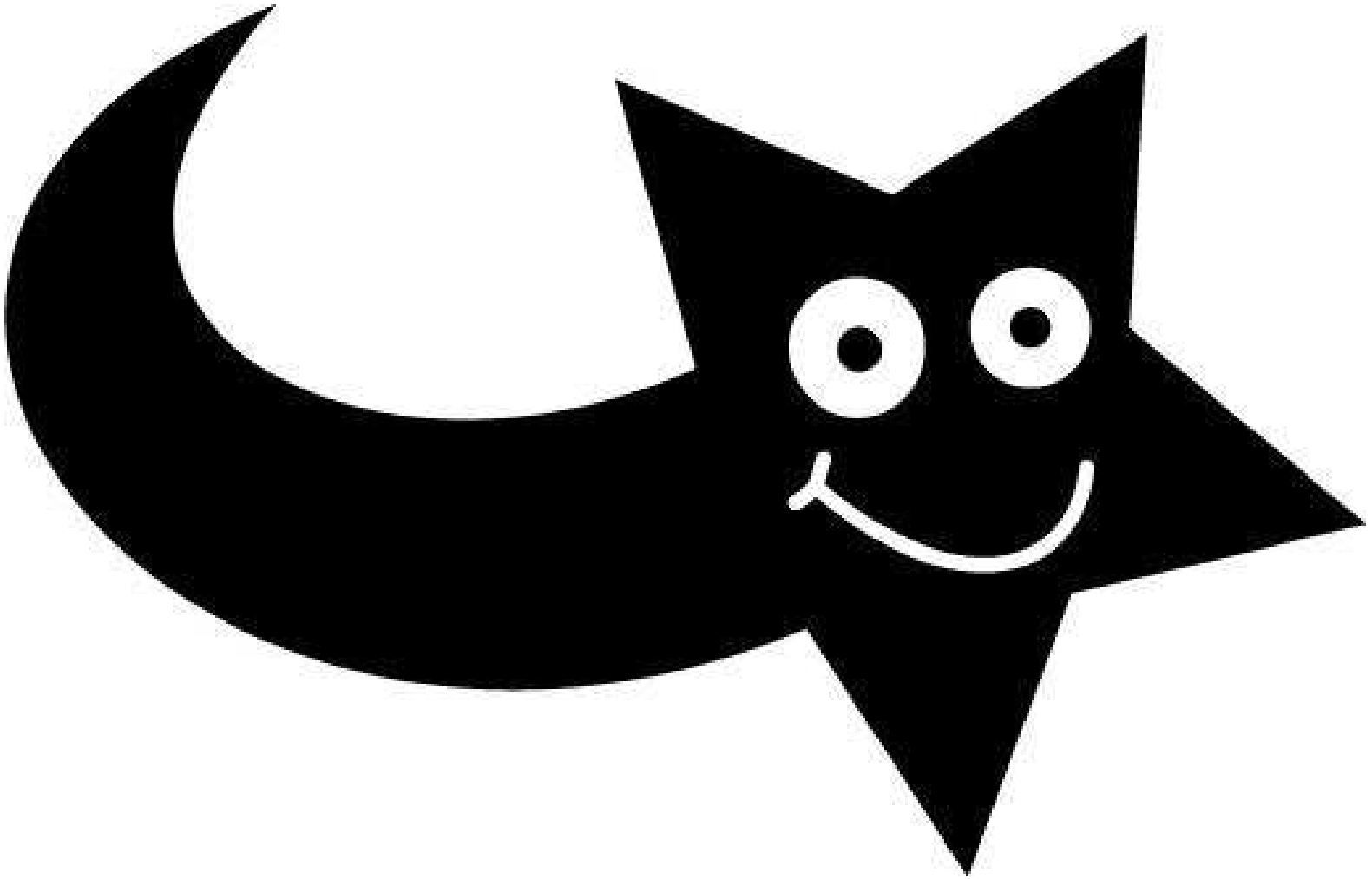
Pour une version probabilisée de l'algorithme $\mathcal{G}$, on obtient :

$$\mathbb{E}_{n,f}(G) = C(f)n(\log n)^2 \log\log n \cdot \left[1 + O\left(\frac{1}{\log\log n}\right)\right].$$

Conclusion

- Première analyse en moyenne (rigoureuse) d'un algorithme de calcul de pcgd sous quadratique,
- Renseignements précis sur le comportement de l'algorithme d'Euclide,
- Lien avec la version non probabilisée.

Merci ! !



Théorème taubérien

Théorème (Delange)

$F(s)$ une série de Dirichlet à coefficients positifs $(a_n)_{n\in\mathbb{N}^\star}$:

$$F(s) = \sum_{n\geq 1} \frac{a_n}{n^s}.$$

Retour

Théorème taubérien

Théorème (Delange)

$F(s)$ une série de Dirichlet à coefficients positifs $(a_n)_{n\in\mathbb{N}^\star}$:
$F(s) = \sum_{n\geq 1} \frac{a_n}{n^s}$. On suppose que

1. *$F(s)$ converge dans le demi-plan $\Re(s) > \sigma > 0$ et est analytique pour $\Re(s) = \sigma$, $s \neq \sigma$,*
2. *il existe $\gamma \geq 0$ tel que $F(s) = A(s)(s-\sigma)^{-\gamma-1} + C(s)$ où A et C sont analytiques en σ et $A(\sigma) \neq 0$.*

Retour

Théorème taubérien

Théorème (Delange)

$F(s)$ une série de Dirichlet à coefficients positifs $(a_n)_{n\in\mathbb{N}^\star}$:
$F(s)=\sum_{n\geq 1}\frac{a_n}{n^s}$. On suppose que

1. *$F(s)$ converge dans le demi-plan $\Re(s)>\sigma>0$ et est analytique pour $\Re(s)=\sigma$, $s\neq\sigma$,*
2. *il existe $\gamma\geq 0$ tel que $F(s)=A(s)(s-\sigma)^{-\gamma-1}+C(s)$ où A et C sont analytiques en σ et $A(\sigma)\neq 0$.*

Alors, lorsque $N\to\infty$,

$$\sum_{1\leq n\leq N} a_n = \frac{A(\sigma)}{\sigma\Gamma(\gamma+1)}N^\sigma \log^\gamma N[1+\varepsilon(N)],\ \varepsilon(N)\to 0.$$

Retour

Formule de Perron (d'ordre 2)

Pour D tel que la série $S(s,w)$ converge sur $\Re s = D$,

$$\sum_{Q \leq N} \mathbf{c}(Q,w)(N-Q) = \frac{1}{2i\pi} \int_{D-i\infty}^{D+i\infty} S_C(s,w) \frac{N^{2s+1}}{s(2s+1)} ds,$$

$$S(s,w) = \sum_{n \geq 1} \frac{\mathbf{c}(n,w)}{n^{2s}}.$$

Intro.

$H_{s,w}$.

Théorème des quasi-puissances

Théorème (Hwang)

Soit R_n une suite de variables aléatoires,

$$g_n(w) = \mathbb{E}(e^{wR_n}) \text{ la série génératrice des moments.}$$

Hypothèses :

1. *g_n est analytique sur un voisinage complexe $\mathcal{W}$ de $w = 0$*
2. *$g_n(w) = e^{\beta_n U(w)} e^{V(w)} (1 + O(\kappa_n^{-1}))$, U et V sont des fonctions analytiques sur $\mathcal{W}$, $\beta_n, \kappa_n \longrightarrow \infty$, le terme O est uniforme en $w \in \mathcal{W}$.*

Théorème des quasi-puissances

Théorème (Hwang)

Soit R_n une suite de variables aléatoires,

$$g_n(w) = \mathbb{E}(e^{wR_n}) \text{ la série génératrice des moments.}$$

Alors :

$$\mathbb{E}(R_n) = U'(0)\beta_n + V'(0) + O(\kappa_n^{-1}),$$

$$Var(R_n) = U''(0)\beta_n + V''(0) + O(\kappa_n^{-1}).$$

Théorème des quasi-puissances

Théorème (Hwang)

Soit R_n une suite de variables aléatoires,

$$g_n(w) = \mathbb{E}(e^{wR_n}) \text{ la série génératrice des moments.}$$

R_n est asymptotiquement gaussien : si $U''(0) \neq 0$,

$$\mathbb{P}\left(w \,/\, \frac{R_n(w) - U'(0)\beta_n}{\sqrt{\beta_n U''(0)}} \leq t\right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-\frac{y^2}{2}} dy + O(\kappa_n^{-1} + \beta_n^{-\frac{1}{2}}).$$

$H_{s,w}$.