EUCLIDEAN DYNAMICS

An Arithmetical Instance of Dynamical Analysis

Dynamical Analysis:=

Analysis of Algorithms + Dynamical Systems

Brigitte VALLÉE (CNRS and Université de Caen, France)

General Framework elaborated with the CAEN GROUP

Results obtained in joint works with Viviane BALADI and Philippe FLAJOLET.

The Euclid Algorithm.

On the input (u, v), it computes the gcd of u and v, together with the Continued Fraction Expansion of u/v. $v_0 := v$; $v_1 := u; v_0 \geq v_1$

$$\left\{\begin{array}{ccccccc} v_0 & = & m_1 v_1 & + & v_2 & & 0 \leq v_2 < v_1 \\ v_1 & = & m_2 v_2 & + & v_3 & & 0 \leq v_3 < v_2 \\ \ldots & = & \ldots & + & & & \\ v_{p-2} & = & m_{p-1} v_{p-1} & + & v_p & & 0 \leq v_p < v_{p-1} \\ v_{p-1} & = & m_p v_p & + & 0 & & v_{p+1} = 0 \end{array}\right\}$$

v_p is the gcd of u and v. $(m_1, m_2, \ldots, m_p)$ are the digits.

CFE of $\dfrac{u}{v}$:
$$\frac{u}{v} = \cfrac{1}{m_1 + \cfrac{1}{m_2 + \cfrac{1}{\ddots + \cfrac{1}{m_p}}}},$$

Variants of the Euclidean Algorithms.

A Euclidean algorithm:= Any algorithm which performs

a sequence of divisions $v = mu + r$.

Various possible divisions, according to

- the position of the remainder r

  (Division By–Default, By Excess, Centered)

- the parity of the quotient m

  (Odd divisions, Even divisions)

- A sequence of m subtractions may replace the division with quotient m.

A division $v = mu + r$ can be replaced by a pseudo-division where powers of 2 are removed from the remainder r, $v = mu + 2^b s$, s odd.

(Binary Algorithm, Hensel divisions)

Cost of an execution.

Given a step–cost $c : \mathbf{N}^\star \mapsto \mathbf{R}^+$ which depends only on the digit,

$$\text{the total cost } C \text{ is additive} \quad C(u, v) := \sum_{i=1}^{p} c(m_i)$$

Here, step–cost c of **moderate growth**, i.e., $c(m) = O(\log m)$

Main costs of moderate growth.

- if $c \equiv 1$, then $C = P$ is the number of iterations
- if c is the characteristic function c_{m_0} of a given digit m_0, then C is the number of occurrences of m in the CF.
- if $c(m) = \ell(m)$, the binary length of digit m, then C is the encoding length of the CF.

Important Question: Compare the behaviour of these various Euclidean algorithms with respect to different costs.

Previous results on the Average-Case Analysis

Set of possible inputs $\Omega_N := \{(u,v); \gcd(u,v) = 1, 0 \leq \frac{u}{v} \leq 1, v \leq N\}$.

First results obtained only for $C = P$ and for particular algorithms,

Due to Heilbronn, Dixon, Rieger (70), for Standard, Centered Alg.

Heuristic results by Brent (78) for the Binary Alg.

Then Dynamical Analysis provides...

a complete classification into two classes [Va 1998].

Fast Class ={Standard, Centered, Odd, Binary} $E_N[P] \sim A \log N$

Slow Class = {By-Excess, Even, Subtractive} $E_N[P] \sim B \log^2 N$

...and an analysis of a broad class of costs

[Not only additive costs relative to step–costs of moderate growth],

amongst them: the Bit–Complexity [Akhavi, Va, 2000]

New [Baladi-V. 03]: Distributional analysis of cost C on Ω_N related to a step-cost c of $\mathcal{MG}$ for three Algorithms of the Fast Class

Main result : The cost C is asymptotically Gaussian

First a **CLT Theorem**:

$$\mathbb{P}_N\left[\ \frac{C(u,v)-\mu(c)\log N}{\delta(c)\sqrt{\log N}} \le x\right] = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}dt + O\left(\frac{1}{\sqrt{\log N}}\right)$$

Also a **LLT Theorem**

for cost C with a lattice step–cost c $[\mathrm{Im}(c) \subset L\mathbf{N}$ with $L > 0]$,

$$\mathbb{P}_N[C(u,v) \sim \mu(c)\log N + x\delta(c)\sqrt{\log N}] = \frac{e^{-x^2/2}}{\delta(c)\sqrt{2\pi\log N}} + O\left(\frac{1}{\log N}\right)$$

Optimal speed of convergence in both cases (LLT and CLT)

A major improvement of previous results due to Hensley (94): our proof is more natural, our result is more general and more precise.

Numerical Experiments: Histogram of P for $N = 10^{100}$

with 10^4 inputs (u, v) randomly chosen in Ω_N.

on the x's axis : possible values of P

on the y's axis: number of occurrences of P-values

Expressions of constants $\mu(c)$ and $\delta(c)$ as mathematical functions

Central rôle played by the Pressure Fonction $\Lambda(s,w) := \log \lambda(s,w)$, where $\lambda(s,w)$ is the dominant eigenvalue of a weighted transfer operator $\mathbf{H}_{s,w}$ associated to the Euclidean Dynamical System.

Constants $\mu(c)$ and $\delta(c)$ are expressed with the first five partial derivatives of $(s,w) \longrightarrow \Lambda(s,w)$ at $(s,w) = (1,0)$.

Five main tools involved in the proofs

- The dynamical system and its weighted transfer operator $\mathbf{H}_{s,w}$
- The Quasi-Powers Theorem on the moment generating function
- Perron's formula
- Dolgopyat's results
- An intermediary probabilistic model, called a smoothed model

The Euclidean dynamical System (I).

The trace of the execution of the Euclid Algorithm on (v_1, v_0) is:

$$(v_1, v_0) \to (v_2, v_1) \to (v_3, v_2) \to \ldots \to (v_{p-1}, v_p) \to (v_{p+1}, v_p) = (0, v_p)$$

Replace the integer pair (v_i, v_{i-1}) by the rational $x_i := \dfrac{v_i}{v_{i-1}}$.

The division $v_{i-1} = m_i v_i + v_{i+1}$ is then written as

$$x_{i+1} = \frac{1}{x_i} - \left\lfloor \frac{1}{x_i} \right\rfloor \qquad \text{or} \qquad x_{i+1} = T(x_i), \qquad \text{where}$$

$$T : [0,1] \longrightarrow [0,1], \quad T(x) := \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor \quad \text{for} \ \ x \neq 0, \quad T(0) = 0$$

An execution of the Euclidean Algorithm

= A rational trajectory of the Dynamical System $([0,1], T)$ that reaches 0.

The Euclidean dynamical System (II).

A dynamical system with a denumerable system of branches $(T_{[m]})_{m\geq 1}$,

$$T_{[m]} :]\frac{1}{m+1}, \frac{1}{m}[\longrightarrow]0,1[, \qquad T_{[m]}(x) := \frac{1}{x} - m$$

The set $\mathcal{H}$ of the inverse branches of T is

$$\mathcal{H} := \{\ h_{[m]} :]0,1[\longrightarrow]\frac{1}{m+1}, \frac{1}{m}[; \qquad h_{[m]}(x) := \frac{1}{m+x} \}$$

The set $\mathcal{H}$ builds one step of the CF's.

The set $\mathcal{H}^n$ is the set of the inverse branches of T^n;

it builds CF's of depth n.

The set $\mathcal{H}^\star := \bigcup \mathcal{H}^n$ builds all the (finite) CF's.

The density transformer $\mathbf{H}$ expresses the new density f_1 as a function of the old density f_0, as $f_1 = \mathbf{H}[f_0]$. It involves the set $\mathcal{H}$

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

With a cost $c : \mathcal{H} \to \mathbf{R}^+$ defined by $c(h_{[m]}) := c(m)$ and extended to $\mathcal{H}^\star$ by additivity, it gives rise to the weighted transfer operator

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

$$\left\{\begin{matrix}\text{Multiplicative properties of the derivative} \\ \text{Additive properties of the cost}\end{matrix}\right\} \Longrightarrow$$

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

The n–th iterate of $\mathbf{H}_{s,w}$ generates the CFs of depth n. The **quasi inverse** $(I - \mathbf{H}_{s,w})^{-1} = \sum_{n\geq 0} \mathbf{H}^n_{s,w}$ generates **all the finite** CFs.

Other Euclidean Dynamical Systems.

A continuous dynamical system can be associated to each discrete division: Replace the rational u/v by a generic real x of $\mathcal{I}$.

The DS relative to a "true" division is deterministic.

The DS relative to a pseudo–division is random: It proves convenient to extend the 2-adic valuation b to a random variable B

where $\mathbb{P}[B = b] = 1/2^b$ for $b \geq 1$.

Key Property : Expansiveness of branches

$$|T'(x)| \geq \rho > 1 \text{ for all } x \text{ in } \mathcal{I}$$

When true, this implies a chaotic behaviour for trajectories and good properties for the density transformer when it acts on $\mathcal{C}^1(\mathcal{I})$. The associated algorithms are Fast and belong to the Good Class

When this condition is violated at only one fixed point, this leads to intermittency phenomena. The associated algorithms are Slow.

Main Analytical Properties of $\mathbf{H}_{s,w}$ for an algorithm of the Good Class and a digit-cost c of moderate growth.

$\mathbf{H}_{s,w}$ acts on $\mathcal{C}^1(\mathcal{I})$;

The map $(s, w) \mapsto \mathbf{H}_{s,w}$ is analytic near the reference point $(1, 0)$

For s and w real :

Property *UDE* : Unique dominant eigenvalue $\lambda(s, w)$,

Property *SG* : Existence of a spectral gap.

With perturbation theory, these properties remain true when (s, w) is near $(1, 0)$, $\lambda(s, w)$ is analytic w.r.t. s and w.

A spectral decomposition $\mathbf{H}_{s,w} = \lambda(s, w) \cdot \mathbf{P}_{s,w} + \mathbf{N}_{s,w}$.

$\mathbf{P}_{s,w}$ is the projector on the dominant eigensubspace.

$\mathbf{N}_{s,w}$ is the operator relative to the remainder of the spectrum, whose spectral radius $\rho_{s,w}$ satisfies $\rho_{s,w} \leq \theta\lambda(s, w)$ with $\theta < 1$.

.....which extends to all $n \geq 1$, $\mathbf{H}^n_{s,w} = \lambda^n(s, w) \cdot \mathbf{P}_{s,w} + \mathbf{N}^n_{s,w}$.

Then, if $\int_I f(t)dt \neq 0$, a Quasi–Power-property

$$\mathbf{H}_{s,w}^n[f] = \lambda^n(s,w) \cdot \mathbf{P}_{s,w}[f] \cdot [1 + O(\theta^n)]$$

and, a decomposition for the quasi–inverse

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

Since $\mathbf{H}_{1,0}$ is a density transformer, one has $\lambda(1,0) = 1$.

"Dominant" (polar) singularities of $(I - \mathbf{H}_{s,w})^{-1}$ near the point $(1,0)$: along a curve $s = \sigma(w)$ on which the dominant eigenvalue satisfies

$$\lambda(\sigma(w), w) = 1$$

How to prove an asymptotic gaussian law?

With the moment generating fn $\mathbb{E}_N[\exp(wC_N)]$ of cost $C_N := C|_{\Omega_N}$.

Quasi–Powers Theorem. If $\mathbb{E}_N[\exp(wC_N)]$ is a uniform quasi-power when w is near 0, then C_N is asymptotically gaussian on Ω_N.

If $\mathbb{E}_N[\exp(wC_N)] = \exp[\beta_N U(w) + V(w)] \cdot \left[1 + O\left(\frac{1}{\kappa_N}\right)\right]$

with a O-term uniform when w is near 0,

U, V *analytic*, $U''(0) \neq 0$, *and* $\beta_N, \kappa_N \to \infty$,

Then: (i) $\dfrac{C_N - U'(0) \cdot \beta_N}{\sqrt{U''(0)\beta_N}}$ *is asymptotically Gaussian,*

with a speed of convergence $O(\kappa_N^{-1} + \beta_N^{-1/2})$

(ii) *Precise estimates hold*

for the expectation $\mathbb{E}_N[C_N]$ *and the variance* $\mathbb{V}_N[C_N]$

$$\mathbb{E}_N[C_N] = \beta_N U'(0) + V'(0) + O(\kappa_N^{-1}),$$

$$\mathbb{V}_N[C_N] = \beta_N U''(0) + V''(0) + O(\kappa_N^{-1}).$$

(iii) *and for all moments of order* k

$$\mathbb{E}_N[C_N^k] = P_k(\beta_N) \; + O\left(\frac{\beta_N^{k-1}}{\kappa_N}\right)$$

with a a polynomial P_k *of degree at most* k*, with coefficients depending on the derivatives of order at most* k *at* 0 *of* U *and* V*.*

Distribution of real truncated trajectories. (I) Methods

Endow the interval $\mathcal{I}$ with density f, and consider, for any real x, the cost C_n relative to the n first digits

$$C_n(x) := \sum_{i=1}^{n} c(m_i)$$

Limit distribution of C_n when $n \to \infty$?

$$\mathbb{E}[\exp(wC_n)] = \sum_{h \in \mathcal{H}^n} \exp[wc(h)] \cdot \int_{h(\mathcal{I})} f(y)\,dy,$$ and, with $y = f(u)$,

$$= \int_{\mathcal{I}} \sum_{h \in \mathcal{H}^n} \exp[wc(h)] \cdot |h'(u)| \cdot f \circ h(u)\,du = \int_{\mathcal{I}} \mathbf{H}_{1,w}^n[f](u)\,du\,.$$

With *UDE +SG,*

$$\mathbb{E}[\exp(wC_n)] = \left(\lambda(1,w)^n \int_{\mathcal{I}} \mathbf{P}_{1,w}[f](u)\,du\right)(1 + O(\theta^n))\ ,$$

A uniform quasi power ! with $U(w) = \Lambda(1, w)$.

Distribution of real truncated trajectories. (II) Results

For a triple $(\mathcal{I}, T, c)$ of $\mathcal{GMG}$ type with non-constant c and any probability Pr on $\mathcal{I}$ with a $\mathcal{C}^1$ density, there is

An asymptotic Gaussian law for C_n:

$$\mathbb{P}\left[x \;\middle|\; \frac{C_n(x) - \hat{\mu}(c)n}{\hat{\delta}(c)\sqrt{n}} \leq Y\right] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{Y} e^{-y^2/2}\, dy + O\left(\frac{1}{\sqrt{n}}\right).$$

with $\quad \hat{\mu}(c) = \Lambda'_w(1, 0), \qquad \hat{\delta}^2(c) = \Lambda''_{w^2}(1, 0)$

[Convexity properties of Λ prove that $\Lambda''_{w^2}(1, 0) \neq 0$.]

For any θ which satisfies $r_1 < \theta < 1$, (with r_1 = the subdominant spectral radius of the density transformer $\mathbf{H}$),

$$\mathbb{E}\left[C_n\right] = \hat{\mu}(c) \cdot n + \hat{\eta}(c) + O(\theta^n), \quad \mathbb{V}\left[C_n\right] = \hat{\delta}^2(c) \cdot n + \hat{\delta}_1(c) + O(\theta^n)$$

An easy proof for a quite well-known result, and . . .

a first hint towards gaussian behaviour of RATIONAL trajectories....

Rational trajectories: The Dirichlet moment generating function (I).

Definition. Replace the sequence of MGF's $\mathbb{E}_N[\exp(wC)]$ by a unique Dirichlet moment generating function $S(s,w)$;

Two parameters s and w: s marks the size, and w marks the cost,

Ω is the set of all the possible inputs,

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

$$\text{with} \quad c_n(w) := \sum_{\substack{(u,v)\in\Omega \\ v=n}} \exp[wC(u,v)]$$

The plain moment generating function $\mathbb{E}_N[\exp(wC)]$ is expressed with coefficients of $S(s,w)$

$$\mathbb{E}_N[\exp(wC)] = \frac{\sum_{n\leq N} c_n(w)}{\sum_{n\leq N} c_n(0)}$$

The Dirichlet moment generating function (II). Link with the transfer operator.

The Euclid Algorithm builds a bijection between Ω and $\mathcal{H}^\star$:

$$(u, v) \mapsto h \quad \text{with} \quad \frac{u}{v} = h(0).$$

$$\text{Then,} \quad \frac{1}{v} = \frac{1}{D[h](0)} = |h'(0)|^{1/2}, \qquad C(u, v) = c(h),$$

and the Dirichlet series

$$S(s, w) := \sum_{(u,v)\in\Omega} \frac{1}{v^s} \exp[wC(u, v)] = \sum_{h\in\mathcal{H}^\star} |h'(0)|^{s/2} \exp[wc(h)]$$

admits an alternative expression with

the quasi inverse $(I - \mathbf{H}_{s,w})^{-1}$ of the weighted transfer operator $\mathbf{H}_{s,w}$,

$$S(2s, w) = (I - \mathbf{H}_{s,w})^{-1}[1](0)$$

Now, two main directions,

Study of all the moments ... or ... study of distribution

First direction. The study of the moment $\mathbb{E}_N[C^k]$ uses

$G_k(s) :=$ the k–th derivative of $S(s,w)$ (with respect to w, at $w=0$)

$=$ a Dirichlet series which involves k occurrences of $(I - \mathbf{H}_s)^{-1}$

Extraction of coefficients via Tauberian Theorems needs the three following properties for $\mathbf{H}_s$:

$$UDE + SG$$

$+$ Aperiodicity Condition: $1 \notin \mathrm{Sp}\, \mathbf{H}_s$ on the line $\Re s = 1, s \neq 1$

Tauberian Theorem. [Delange] Suppose that a Dirichlet series $G(s) := \sum_{n\geq 1} a_n n^{-s}$, with $a_n \geq 0$ converges for $\Re(s) > \sigma > 0$.

Assume that

(*i*) $G(s)$ is analytic on $\Re(s) = \sigma, s \neq \sigma$,

(*ii*) For some $\gamma > 0$, when s is near σ,

$$G(s) = \frac{A(s)}{(s-\sigma)^{\gamma+1}} + C(s)$$

with A, C analytic at $s = \sigma$, and $A(\sigma) \neq 0$

Then:

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

Conditions on $(I - \mathbf{H}_s)^{-1}$ needed for applying Tauberian Theorems.

$s = 1$ is the only pole

on the line $\Re s = 1$

Expansion near the pole $s = 1$

$$(I - \mathbf{H}_s)^{-1} \sim \frac{a}{s-1}$$

Half–plane of convergence $\Re s > 1$

No hypothesis needed

on the half–plane $\Re s < 1$.

Study of the moments $\mathbb{E}_N[C^k]$: Results.

For an algorithm of the Good Class and $c = 1$, $\mathbb{E}_N[P] \sim \dfrac{2}{h(\mathcal{S})} \log N$

For an algorithm of the Good Class and a cost c of moderate growth,

$$\mathbb{E}_N[C^k] \sim (\mathbb{E}_N[C])^k \qquad \text{with} \qquad \mathbb{E}_N[C] \sim \hat{\mu}(c) \cdot \mathbb{E}_N[P]$$

where $\hat{\mu}(c)$ = the average of c along the real trajectories,

= the average of c with respect to the stationary density.

Two main results.

- Similarity between the average behaviour of C on almost all real trajectories and its average behaviour on rational trajectories.
- The distribution of C is concentrated around its mean.

Two reasons for expecting the behaviour of C to be asymptotically Gaussian?

Now, a distribution study.

Extraction of coefficients via the Perron Formula of order two

For $F(s) := \sum_{n\geq 1} \frac{a_n}{n^s}$, $\qquad \sum_{n\leq N} \sum_{q\leq n} a_q = \frac{1}{2i\pi} \int_{D-i\infty}^{D+i\infty} F(s) \frac{N^{s+1}}{s(s+1)} ds$

... a first step for estimating $\mathbb{E}_N[\exp(wC)]$ ... uniformly in w.

Perron's formula relates the MGF $\mathbb{E}_N[\exp(wC)]$ to

$$\frac{1}{2i\pi} \int_{D-i\infty}^{D+i\infty} S(2s, w) \frac{N^{2s+1}}{s(2s+1)} ds$$

$$= \frac{1}{2i\pi} \int_{D-i\infty}^{D+i\infty} (I - \mathbf{H}_{s,w})^{-1}[1](0) \frac{N^{2s+1}}{s(2s+1)} ds$$

What can be expected on $(I - \mathbf{H}_{s,w})^{-1}$ for dealing with the Perron Formula?

Property US : Uniformity on Strips

There exists a strip $\mathcal{S} := \{s; |\Re(s) - 1| < \alpha\}$ *such that, uniformly w.r.t.* w *when* w *is near 0,*

(i) [Strong aperiodicity] $(I - \mathbf{H}_{s,w})^{-1}$ *has a unique pole inside* $\mathcal{S}$*; it is located at* $s = \sigma(w)$

(ii) [Uniform estimates] *On the left line* $\Re s = 1 - \alpha$*:*

$$(I - \mathbf{H}_{s,w})^{-1}[1] = O(|\Im s|^{\beta}) \text{ with } \beta < 1$$

With the Property US, it is easy to deform the contour of the Perron Formula and use Cauchy's Theorem . . .

Conditions on $(I-\mathbf{H}_{s,w})^{-1}$ needed for dealing with Perron's formula.

Near $w = 0$, remind that $\sigma(w)$ is defined by $\lambda(\sigma(w), w) = 1$

$s = \sigma(w)$ is the only pole

on the strip $|\Re s - 1| < \alpha$

Expansion

near the pole $s = \sigma(w)$

$$(I-\mathbf{H}_{s,w})^{-1} \sim \frac{a}{s - \sigma(w)}$$

Half–plane of

convergence $\Re s > \sigma(w)$

Uniform estimates needed

on the left line $\Re s = 1 - \alpha$.

Property US is not always true ; Item (i) is always false for Dynamical Systems with affine branches.

Example: a Dynamical System with two affine branches of slopes

$1/p$ and $1/q$ with $p+q=1$.

Location of poles of $(I - \mathbf{H}_s)^{-1}$ near $\Re s = 1$: Two main cases

If $\dfrac{\log p}{\log q} \in \mathbf{Q}$	If $\dfrac{\log p}{\log q} \notin \mathbf{Q}$
Regularly spaced poles on $\Re s = 1$	Only one pole at $s=1$ on $\Re s = 1$ but accumulation of poles on the left of $\Re s = 1$

Three main facts.

(a) There exists a Condition, the Condition *UNI*, that expresses that the dynamical system is quite different from a piecewise affine map.

(b) The Condition *UNI* is sufficient to imply the Property *US*.

(c) The Condition *UNI* is true in our Euclidean context.

Condition *UNI*. (Introduced by Dolgopyat)

Define a "distance" Δ between two inverse branches h and k

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

Condition *UNI* says: The inverse branches of same depth are not too often too close w.r.t. Δ.

Condition *UNI* is never true for DS with affine branches $(\Delta \equiv 0)$, but the *UNI* Condition is true in our Euclidean context. [Item (c)]

Dolgopyat (98) proves the Item (b) but only for

- Dynamical Systems with a finite number of branches
- Plain transfer operators (not weighted)

We adapt his arguments to generalize this result to our framework and prove (b).

Coming back to the proof of the asymptotic gaussian law .

Step 1. Introduce the smoothed model $\overline{\Omega}_N$. Choose first N; then draw uniformy q between N and $\lfloor N - N^{1-\gamma} \rfloor$; finally draw uniformly $(u, v) \in \Omega_q$

The Perron Formula with the *US* Property entail a uniform quasi-power behaviour for the MGF of the smoothed version of cost C,

$$\overline{\mathbb{E}}_N[\exp(wC)] = \big(1 + O(N^{-\gamma})\big) \exp\left(2[\sigma(w) - \sigma(0)] \log N + A(w)\right)$$

with a O–term uniform in w.

Step 2. The Quasi-Power Theorem proves: the Cost C_N follows asymptotically a Gaussian Law in the smoothed model.

Step 3. The two distributions of C [on Ω_N and on $\overline{\Omega}_N$] are $O(N^{-\gamma})$-close and, finally, the Cost C follows asymptotically a Gaussian Law in the plain model.

Asymptotic Gaussian Law: the Central Limit Theorem

$$\mathbb{P}_N\left[\ \frac{C(u,v)-\mu(c)\log N}{\delta(c)\sqrt{\log N}} \le x\right] = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}dt + O(\frac{1}{\sqrt{\log N}})$$

The constants $\mu(c)$ and $\delta(c)$ are expressed with the first and second derivatives of the function $w \mapsto \sigma(w)$ defined by $\Lambda(\sigma(w), w) = 0$.

$$\mu(c) = 2\sigma'(0) = \frac{-2\Lambda'_w(1,0)}{\Lambda'(1)},$$

With $L(w) := \Lambda(1+\sigma'(0)w, w)$,

$$\delta^2(c) = 2\sigma''(0) = \frac{2}{|\Lambda'(1)|}L''(0).$$

The strict positivity of $L''(0)$ is related to the *UNI* Property.

Computation of the constants. Example of the Standard Case.

Mean constants [related to the first derivatives of $\Lambda(s,w)$] admit alternative expressions which involve the stationary density f_1.

The entropy of the system $\quad h(\mathcal{S}) = \Lambda'_s(1,0) = \int_{\mathcal{I}} \log|T'(x)| \cdot f_1(x)dx$

The constants $\quad \hat{\mu}(c) = \Lambda'_w(1,0) = \sum_{h\in\mathcal{H}} c(h) \cdot \int_{h(\mathcal{I})} f_1(t)dt$

Since $\quad f_1(x) = \frac{1}{\log 2}\frac{1}{1+x},\quad$ the entropy $\quad h(\mathcal{S}) = \frac{\pi^2}{6\log 2},$

$\hat{\mu}(c_m) = \frac{1}{\log 2}\log\left(1+\frac{1}{m(m+2)}\right)\qquad$ [c_m= characteristic fn of digit m]

$\hat{\mu}(\ell) = \frac{1}{\log 2}\log\prod_{k=0}^{\infty}\left(1+\frac{1}{2^k}\right)\qquad$ [ℓ= the binary length of the digit]

Not such explicit expressions for variance constants $\delta(c)$; however, they are polynomial–time computable [Lhote].

Asymptotic Gaussian Law: the Local Limit Theorem for lattice costs

It is sufficient to consider integer costs in the smoothed model.

$$\bar{\mathbb{E}}_N[e^{i\tau C}] = \sum_{\ell \geq 0} \bar{\mathbb{P}}_N[C = \ell]\, e^{i\tau\ell} \Longrightarrow \bar{\mathbb{P}}_N[C = \ell] = \frac{1}{2\pi} \int_{-\pi}^{\pi} e^{-i\tau\ell} \cdot \bar{\mathbb{E}}_N[e^{i\tau C}]\, d\tau.$$

LLT Study $\Longrightarrow \ell$ near $q_x(n) := \lfloor \mu(c)n + \delta(c)x\sqrt{n} \rfloor$, with $n := \log N$.

$$I_n := 2\pi\sqrt{\log N} \cdot \bar{\mathbb{P}}_N[C = q_x(\log N)] = \sqrt{n} \int_{-\pi}^{+\pi} \exp[-i\tau q_x(n)] \cdot \bar{\mathbb{E}}_N[e^{i\tau C}]\, d\tau.$$

Decompose $[-\pi, +\pi]$ into $[-v, v]$ and its complement, so that

$$I_n = I_n^{(0)} + I_n^{(1)}.$$

For $I_n^{(0)}$, with the saddle–point method, $\quad I_n^{(0)} = \sqrt{2\pi}\, \frac{e^{-x^2/2}}{\delta(c)} + O\left(\frac{1}{\sqrt{n}}\right).$

For $I_n^{(1)}$, with the *UNI* Property for lattice costs,

$|\bar{\mathbb{E}}_N[\exp(i\tau C)]| \leq Q N^{-\gamma_0}, \forall |\tau| \in [v, \pi] \qquad I_n^{(1)} = O(e^{-n\gamma}).$

Conclusion

An instance of a Dynamical Analysis,

Only previously used for Average–Case Analyses,

Here used for a Distributional Analysis.

Open problems

Study of other algorithms,

Fast ones (for instance the Binary Algorithm?) or Slow ones?

Study of other costs,

with non moderate growth?

non additive [for instance the bit–complexity?]