Évolution

de la DISTRIBUTION des RATIONNELS

pendant l'exécution

de l'algorithme d'EUCLIDE

Brigitte Vallée (GREYC, CNRS and Université de Caen)

Travail commun avec :
Eda Cesaratto, Julien Clément, Benoit Daireaux,
Loick Lhote, Véronique Maume

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. $v_0 := v$; $v_1 := u; v_0 \geq v_1$

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

v_p is the gcd of u and v, the m_i's are the digits. p is the depth.

CFE of $\frac{u}{v}$:

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

Analysis of the Euclid Algorithm.

Set of inputs $\Omega_n := \{x = \frac{u}{v};\ 0 \leq u \leq v,\ \ell(v) := \lfloor \lg v \rfloor + 1 = n\}$,

endowed with the restriction of some density f on $[0,1]$ to Ω_n

$$\mathbb{P}_{n,f}(x) := \frac{f(x)}{\sum_{y \in \Omega_n} f(y)}$$

Before: Probabilistic behaviour of the main parameters of the algorithm, which may depend on digits m_i and/or remainders v_i

Study their mean value, their moments... or their distribution

Here:

Evolution of the density of $x_k := v_k / v_{k-1}$ during the execution

– first a natural problem,

– crucial in the analyses of fast versions of the algorithm.

A discrete problem. What is known about its "**continuous**" version?

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

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

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

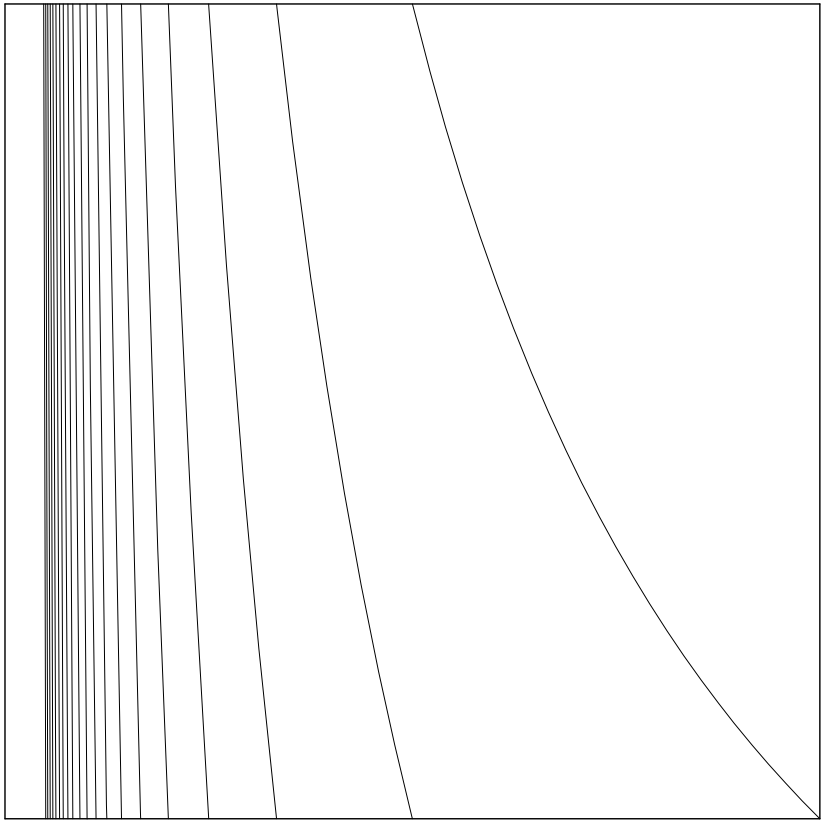
The division $v_{i-1} = m_i v_i + v_{i+1}$ is then written as

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

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

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 transfer operator in the continuous world

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 $\mathcal{H}$,

$$\mathbf{H}[f](x) := \sum_{h \in \mathcal{H}} |h'(x)| \cdot f \circ h(x) = \sum_{m \geq 1} \frac{1}{(m+x)^2} \cdot f\left(\frac{1}{m+x}\right).$$

After n steps of the process, the density f_n is $\mathbf{H}^n[f_0]$.

And for $n \to \infty$? Is there a limit for f_n?

If yes, f_∞ is fixed for $\mathbf{H}$.

Gauss remarked that $\varphi(x) := \dfrac{1}{\log 2} \dfrac{1}{1+x}$ satisfies $\mathbf{H}[\varphi] = \varphi$.

Further, it was proven that,

for any smooth f_0, the density f_n converges to φ, with an exponential speed.

The similar questions in the discrete world.

The Euclid algorithm always ends with a rational $x_p = 0$.

Then, for any initial discrete density f_0,

the final density f_∞ corresponds to a Dirac distribution at $x = 0$.

And, in the "middle" of the algorithm ? A natural question,

also very important in the analysis of fast variants of the algorithm.

The $\mathcal{HG}$ algorithm simulates the first part of the algorithm,

and stops as soon as the remainder v_i has lost $n/2$ bits.

Remind: n = the number of bits of $v = v_0$.

There exists a Divide and Conquer strategy for computing $\mathcal{HG}$.

For writing the corresponding equations,

we need knowing the evolution of densities.

Main algorithmic parameters of interest.

Consider $\delta \in [0,1]$, and denote by P the depth. We wish to study:

– the length of the remainder at the fraction δ of the depth, namely

$$V_\delta = \log v_i \qquad \text{for} \quad i = \lfloor \delta P \rfloor.$$

– the stopping time P_δ:

$$P_\delta \quad := \text{the smallest } k \text{ for which} \quad \ell(v_k) \leq (1-\delta) \cdot n.$$

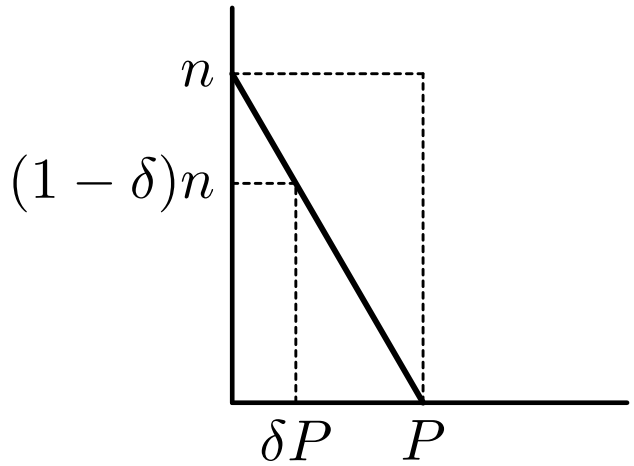
– the evolution of the densities, namely the distribution of

$$x_{<\delta>} := x_k = v_k / v_{k-1} \qquad \text{when} \quad k = P_\delta.$$

to compare with the distribution of

$$x_{[\delta]} := x_k = v_k / v_{k-1} \qquad \text{when} \quad k = \lfloor \delta P \rfloor.$$

What can be expected about V_δ?



Asymptotic gaussian law for $V_\delta := \log v_i$ for $i = \lfloor \delta P \rfloor$

Theorem 1. [Lhote-V. 05] *For any rational δ of $]0,1[$, the length V_δ is asymptotically gaussian, with speed of convergence of order $(1/\sqrt{n})$. Moreover,*

$$\mathbb{E}_{n,f}[V_\delta] = (1-\delta)\cdot n + \mu_1(\delta) + O(2^{-n\gamma}),$$

$$\mathbb{V}_{n,f}[V_\delta] = \delta(1-\delta)\frac{|\Lambda''(1)|}{|\Lambda'(1)|}\cdot n + \rho_1(\delta) + O(2^{-n\gamma}),$$

Here, $\gamma > 0$ depends on δ, and on the width σ of a strip free of pôles.

A "discrete version" of a well-known "continuous" result :

The logarithm of the n-th continuant of a real $x \in \mathcal{I}$ asymptotically follows a gaussian law, when $\mathcal{I}$ is endowed with a density of class C^1

Stopping time P_δ.

Theorem 2. [Cesaratto-Clément-Daireaux-Lhote-Maume-V.] (06) *For any $\delta \in]0,1]$, the stopping time P_δ is asymptotically gaussian on Ω_n, with a speed of convergence of order $O(1/\sqrt{n})$. Moreover,*

$$\mathbb{E}_{n,f}[P_\delta] = \frac{2\log 2}{|\Lambda'(1)|} \cdot \delta n + \mu_1(\delta) + O(2^{-n\gamma}),$$

$$\mathbb{V}_{n,f}[P_\delta] \sim 2\log 2 \left| \frac{\Lambda''(1)}{\Lambda'(1)^3} \right| \cdot \delta n + \rho_1(\delta) + O(2^{-n\gamma}).$$

Here γ depends on δ and on the width σ of a strip free of pôles.
An exact extension of the particular case $\delta = 1$, when $P_\delta = P$ is the total number of iterations.

Now, what about the distribution of rationals $x_{[\delta]}$ and $x_{<\delta>}$?

We recall:

$$x_{<\delta>} := x_k = v_k/v_{k-1} \qquad \text{when} \qquad k = P_\delta,$$

to be compared with the distribution of

$$x_{[\delta]} := x_k = v_k/v_{k-1} \qquad \text{when} \qquad k = \lfloor \delta P \rfloor.$$

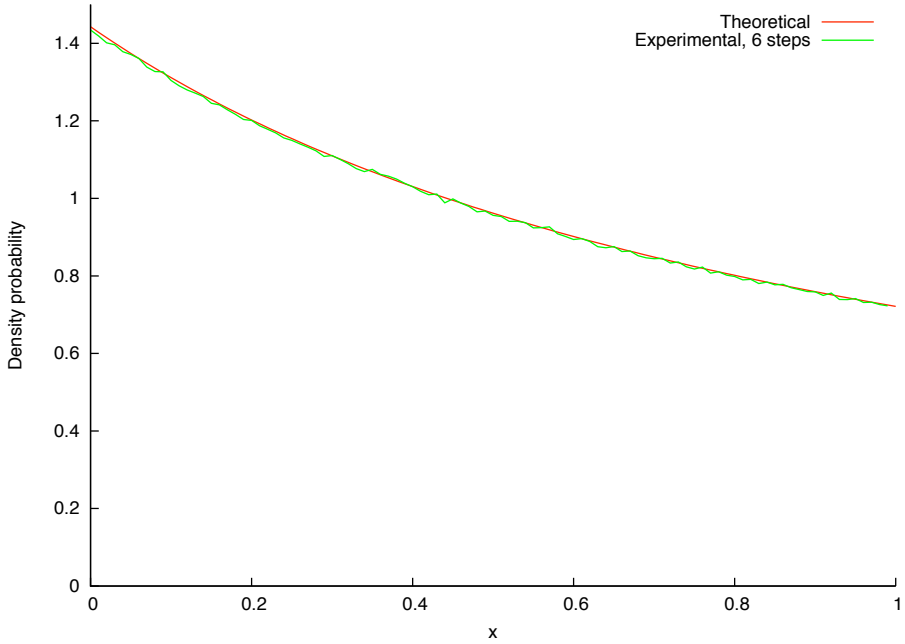
We already know that $\log v_{\lfloor \delta P \rfloor} \sim (1-\delta)n$ and $P_\delta \sim \delta P$;

We thus can expect the distributions of $x_{[\delta]}$ and $x_{<\delta>}$ to be close....

.... and involve the limit density of the continuous world,

$$\text{the Gauss density} \qquad \varphi(x) = \frac{1}{\log 2} \frac{1}{1+x}$$

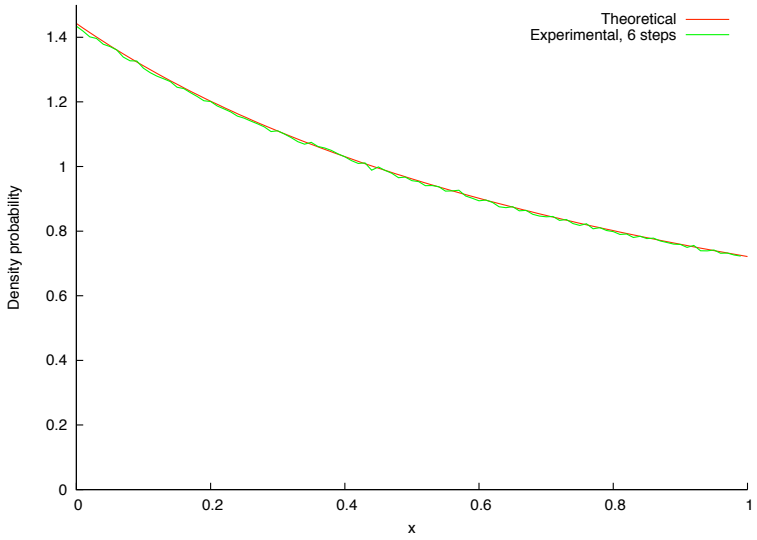
Distribution of the rationals $x_{[\delta]}$



After $k = 6$ steps.

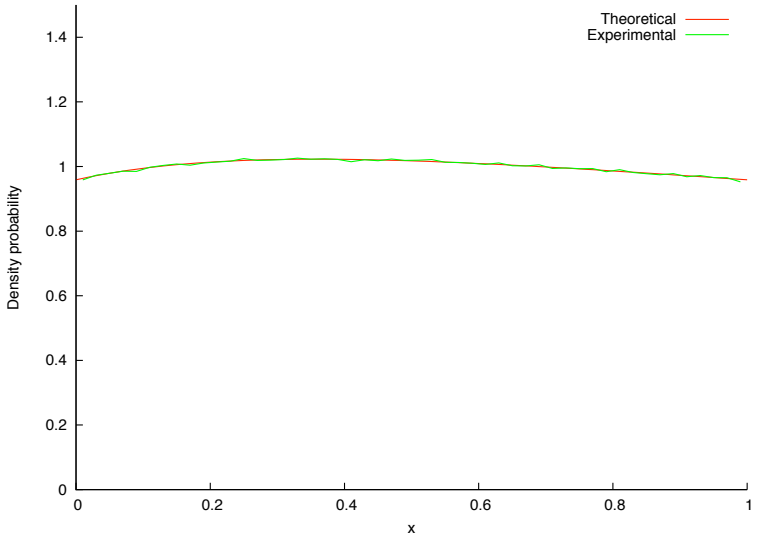
$8\,388\,608$ rational are drawn from Ω_{48} according to the uniform distribution.

Distribution of the rationals $x_{[\delta]}$ and $x_{<\delta>}$



After $k = 6$ steps.

8 388 608 rationals are drawn according to the uniform density from Ω_{48}



Case $\delta = 1/2$

3 537 944 rationals are drawn according to the density φ from Ω_{48}

Distribution of the rationals $x_{<\delta>}$ and $x_{[\delta]}$

Theorem 3. [Cesaratto-Clément-Daireaux-Lhote-Maume-V.] (06)
The probability that $x_{[\delta]}$ belongs to the interval J satisfies

$$\mathbb{P}_{n,f}[x_{[\delta]} \in J] = \left(\int_J \varphi(t)dt \right) \cdot [1 + \beta_n(\delta, J)] \,.$$

The probability that $x_{<\delta>}$ belongs to the interval J satisfies

$$\mathbb{P}_{n,f}[x_{<\delta>} \in J] = \left(\int_J \psi(t)dt \right) \cdot [1 + \beta'_n(\delta, J))]$$

with $\varphi(x) = \dfrac{1}{\log 2} \dfrac{1}{1+x}$, $\qquad \psi(x) = \dfrac{12}{\pi^2} \displaystyle\sum_{m \geq 1} \frac{\log(m+x)}{(m+x)(m+x+1)}$.

For instance: $\beta'_n(\delta, J) = O(|J|) + \dfrac{1}{|J|^{3/2}} O(2^{-\sigma(1-\delta)n}) + O\left(2^{-\frac{\sigma}{2}\delta n}\right)$

where σ is the width of the strip free of pôles.

Rôle of φ and ψ

Recall that the operator $\mathbf{H}$ is $\mathbf{H}[f](x) := \sum_{m\geq 1} \frac{1}{(m+x)^2} f\left(\frac{1}{m+x}\right)$

Extend it into a transfer operator $\mathbf{H}_s$,

$$\mathbf{H}_s[f](x) := \sum_{m\geq 1} \frac{1}{(m+x)^{2s}} f\left(\frac{1}{m+x}\right),$$

and consider its derivative $\Delta\mathbf{H}_s$ with respect to s,

$$\Delta\mathbf{H}_s[f](x) := \frac{d}{ds}\mathbf{H}_s[f](x) = -2\sum_{m\geq 1} \frac{\log(m+x)}{(m+x)^{2s}} f\left(\frac{1}{m+x}\right).$$

The Gauss density φ satisfies $\mathbf{H}[\varphi] = \varphi$.

The density ψ is proportional to $\Delta\mathbf{H}[\varphi]$, $\quad \psi(x) = \frac{12}{\pi^2} \sum_{m\geq 1} \frac{\log(m+x)}{(m+x)(m+x+1)}$

Rôle of the transfer operator in the discrete world.

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

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

Main fact. If $h : x \mapsto h(x) = \dfrac{ax+b}{cx+d}$, then $h'(x) = \dfrac{\det h}{(cx+d)^2}$

Here, for *coprime* (u,v), if $\dfrac{u}{v} = h(0)$, then $\dfrac{1}{v^2} = |h'(0)|$.

$\mathbf{H}_s^k$ *generates* the rationals of depth k.

$(I - \mathbf{H}_s)^{-1}$ is a *generating operator* for rationals wrt to their depth.

With some of its extensions, this is our main tool.

Generating functions.

The basic one is:

$$\sum_{(u,v)\in\Omega} \frac{1}{v^{2s}} = (1-\mathbf{H}_s)^{-1}[1](0) = \frac{\zeta(2s-1)}{\zeta(2s)} - 1.$$

More generally, the generating function of cost C,

$$\sum_{(u,v)\in\Omega} \frac{1}{v^{2s}} \exp[wC(u,v)]$$

involves operators $\mathbb{G}_{s,w}$ which are perturbations of $(I-\mathbf{H}_s)^{-1}$. They can be viewed as (non classical) Dynamical Zeta Functions

The singularities of $\mathbb{G}_{s,w}$ are ....
perturbations of singularities of $(I-\mathbf{H}_s)^{-1}$

The spectral properties of the operator $\mathbf{H}_s$ are now well known;

... $(I-\mathbf{H}_s)^{-1}$ possesses near $s=1$ a vertical strip free of pôles.

Example: Interpretation of the operator $\Delta\mathbf{H}_s$

The coefficient of m^{-2s} in the Dirichlet series

$$-\frac{1}{\log 2}(I-\mathbf{H}_s)^{-1}\left[\mathbf{1}_J\cdot\Delta\mathbf{H}_s\circ(I-\mathbf{H}_s)^{-1}[f]\right](0)$$

is $\displaystyle\sum_{\substack{(u,v)\in\Omega,\\ v=m}} C_J(u,v)$ where $\displaystyle C_J(u,v)=\sum_{\substack{k=1\\ x_k\in J}}^{P(u,v)}(\lg v_{k-1}-\lg v_k)$

is the number of bits lost when one goes through interval J.

Then, the (average) proportion of bits lost when going through J is

$$\frac{1}{n}\mathbb{E}_n[C_J]=\frac{\sum_{(u,v)\in\Omega_n}C_J(u,v)}{n|\Omega_n|}\sim\frac{6\log 2}{\pi^2}\int_J\Delta\mathbf{H}[\varphi](t)dt=\int_J\psi(t)dt$$

Expression of Dirichlet series of interest for studies at a fraction of the depth

Remainders at δP (for Thm 1):

$$\sum_{p\geq 1} \mathbf{H}_{s-w}^{p-\lfloor \delta p \rfloor} \circ \mathbf{H}_{s}^{\lfloor \delta p \rfloor}[f](0)$$

Distribution of $x_{[\delta]}$ (for Thm 3):

$$\sum_{p\geq 1} \mathbf{H}_{s}^{p-\lfloor \delta p \rfloor} \circ [\mathbf{1}_J \cdot \mathbf{H}_{s}^{\lfloor \delta p \rfloor}[f]](0)$$

Rôle of parameters:

s marks the size of the input, w marks the size of the remainder.

Expression of Dirichlet series of interest for studies related to stopping times

Distribution of $x_{<\delta>}$ (for Thm 3) studied via:

$$(I - \mathbf{H}_{s+w})^{-1} \circ \left[\mathbf{1}_J \cdot [\mathbf{H}_{s+w} - \mathbf{H}_s] \circ (I - \mathbf{H}_s)^{-1}[f]\right](0)$$

Stopping time P_δ (for Thm 2) studied via:

$$(I - \mathbf{H}_{s+w})^{-1} \circ [\mathbf{H}_{s+w} - \mathbf{H}_s] \circ (I - e^t \mathbf{H}_s)^{-1}[f](0)$$

Rôle of parameters:

s marks the size of the input, w marks the size of the remainder, t marks the (partial) number of iterations.

First extraction wrt w, then a second extraction wrt s

The parameter δ is not introduced at the beginning, but, after extraction of coefficients.

Main results of the talk:

Description of the densities during the execution of the algorithm.

$$\mathbb{P}_{n,f}[x_{[\delta]} \in J] = \left(\int_J \varphi(t)dt \right) \cdot [1 + \beta_n(\delta, J)]$$

$$\mathbb{P}_{n,f}[x_{<\delta>} \in J] = \left(\int_J \psi(t)dt \right) \cdot [1 + \beta'_n(\delta, J))]$$

for instance: $\beta'_n(\delta, J) = O(|J|) + \frac{1}{|J|^{3/2}} O(2^{-\sigma(1-\delta)n}) + O\left(2^{-\frac{\sigma}{2}\delta n}\right)$

Work in progress: What about phase transitions?
What does happens
at the beginning ($\delta \to 0$) or at the end ($\delta \to 1$) of the algorithm?
How does appear the Dirac distribution at $x = 0$?

Further projects: Higher dimensions
.... towards the analysis of the LLL algorithm....