Euclidean algorithms and dynamical systems

V. Berthé

IRIF-CNRS-Université Paris Cité

10ème anniversaire du Labex Bézout

Euclid's algorithm

We start with two nonnegative integers u_0 and u_1

$$u_0 = u_1 \left[\frac{u_0}{u_1} \right] + u_2$$

$$u_1 = u_2 \left[\frac{u_1}{u_2} \right] + u_3$$

$$\vdots$$

$$u_{m-1} = u_m \left[\frac{u_{m-1}}{u_m} \right] + u_{m+1}$$

$$u_{m+1} = \gcd(u_0, u_1)$$

$$u_{m+2} = 0$$

One subtracts the smallest number from the largest as much as we can

The oldest nontrivial algorithm that has survived to the present day [Knuth]

Analysis of algorithms-Knuth

The advent of high-speed computing machines, which are capable of carrying out algorithms so faithfully, has led to intensive studies of the properties of algorithms, opening up a fertile field for mathematical investigations. Every reasonable algorithm suggests interesting questions of a 'pure mathematical' nature; and the answers to these questions sometimes lead to useful applications, thereby adding a little vigor to the subject without spoiling its beauty. [Knuth]

[Origins of the Analysis of the Euclidean Algorithm-Shallit]

Analysis of Euclid's algorithm

- What is the expected number of steps?
- What is the worst/mean behaviour ?

Analysis of Euclid's algorithm

- What is the expected number of steps?
- What is the worst/mean behaviour ?

- Dynamical systems and Perron-Frobenius machinery
- Euclid's algorithm becomes in its continuous version the Gauss transformation

$$T\colon [0,1] \to [0,1],\ x \mapsto \{1/x\}$$

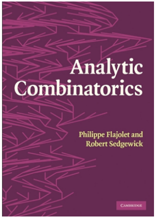
- Rational trajectories behave like generic trajectories for the Gauss transformation

Analysis of algorithms

- Analysis of algorithms [Knuth'63]

  probabilistic, combinatorial, and analytic methods

- Analytic combinatorics [Flajolet-Sedgewick]



  generating functions and complex analysis,
  analysis of the singularities

- Dynamical analysis of algorithms [Vallée]

  Transfer operators $\rightsquigarrow$ Generating functions of Dirichlet type

Euclid algorithm and continued fractions

We start with two coprime integers u_0 and u_1

$$u_0 = u_1 a_1 + u_2$$

$$\vdots$$

$$u_{m-1} = u_m a_m + u_{m+1}$$

$$u_m = u_{m+1} a_{m+1} + 0$$

$$u_{m+1} = 1 = \gcd(u_0, u_1)$$

Euclid algorithm and continued fractions

We start with two coprime integers u_0 and u_1

$$u_0 = u_1 a_1 + u_2$$

$$\vdots$$

$$u_{m-1} = u_m a_m + u_{m+1}$$

$$u_m = u_{m+1} a_{m+1} + 0$$

$$u_{m+1} = 1 = \gcd(u_0, u_1)$$

$$\frac{u_1}{u_0} = \frac{1}{a_1 + \frac{u_2}{u_1}} \qquad u_1/u_0 = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \frac{1}{a_m + \frac{1}{a_{m+1}}}}}}$$

Matricial description

We start with two positive real numbers (x_0, x_1) with $x_0 > x_1$
We divide the largest entry by the smallest and we continue

$$x_0 = \lfloor x_0/x_1 \rfloor x_1 + x_2 \qquad\qquad a_1 := \lfloor x_0/x_1 \rfloor$$

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix}$$

Matricial description

We start with two positive real numbers (x_0, x_1) with $x_0 > x_1$
We divide the largest entry by the smallest and we continue

$$x_0 = \lfloor x_0/x_1 \rfloor x_1 + x_2 \qquad\qquad a_1 := \lfloor x_0/x_1 \rfloor$$

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix}$$

- Let $\alpha := x_1/x_0$. One has $\alpha \in [0,1]$.
- Let $T(\alpha) = 1/\alpha - [1/\alpha]$.

$$\begin{pmatrix} 1 \\ \alpha \end{pmatrix} = \alpha \begin{pmatrix} [1/\alpha] & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ T(\alpha) \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ \alpha \end{pmatrix} = \alpha \cdots T^{n-1}(\alpha) \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ T^n(\alpha) \end{pmatrix}$$

Number of steps $\rightsquigarrow$ size of a product of matrices $\rightsquigarrow$ first Lyapunov exponent

Matricial description

We start with two positive real numbers (x_0, x_1) with $x_0 > x_1$
We divide the largest entry by the smallest and we continue

$$x_0 = \lfloor x_0/x_1 \rfloor x_1 + x_2 \qquad\qquad a_1 := \lfloor x_0/x_1 \rfloor$$

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix}$$

We normalize $\alpha := x_1/x_0$ and we set

$$M_n := \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 \\ \alpha \end{pmatrix} \in \bigcap_n M_1 \cdots M_n \mathbb{R}_+^2$$

$$M_1 \cdots M_n = \begin{pmatrix} q_n & q_{n-1} \\ p_n & p_{n-1} \end{pmatrix} \rightsquigarrow \text{ a sequence of lattice bases for } \mathbb{Z}^2$$

Number of steps $\ell(u, v)$

$\ell(u, v)$: number of steps in Euclid algorithm $0 < v < u$

- Worst case

$$\ell(u, v) = O(\log v) \qquad (\leq 5 \log_{10} v, \text{ Lamé } 1844)$$

- Mean case $\qquad 0 < v < u \leq N \qquad \gcd(u, v) = 1$

$$\mathbb{E}_N[\ell] = \frac{12 \log 2}{\pi^2} \cdot \log N + \eta + O(N^{-\gamma})$$

Asymptotically normal distribution

[Knuth,Heilbronn'69,Dixon'70,Porter'75,Hensley'94,Baladi-Vallée'05...]

Continued fractions and dynamical systems

Consider the Gauss map

$$T : [0,1] \to [0,1],\ x \mapsto \{1/x\}$$

$$x_1 = T(x) = \{1/x\} = \frac{1}{x} - \left[\frac{1}{x}\right] = \frac{1}{x} - a_1$$

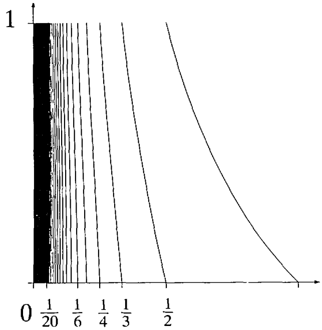
$$x = \frac{1}{a_1 + x_1} \qquad\qquad a_n = \left[\frac{1}{T^{n-1}x}\right]$$

$$x = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

Continued fractions and dynamical systems

Consider the Gauss map

$$T\colon [0,1] \to [0,1],\ x \mapsto \{1/x\}$$



$$T(x) = \{1/x\} = \frac{1}{x} - \left[\frac{1}{x}\right] = \frac{1}{x} - a_1$$

$$\frac{1}{k+1} < x \leq \frac{1}{k} \rightsquigarrow a_1 = k$$

Continued fractions and dynamical systems

Consider the Gauss map

$$T\colon [0,1] \to [0,1],\ x \mapsto \{1/x\}$$

- For a.e. $x \in [0,1]$
$$\lim \frac{\log q_n}{n} = \frac{\pi^2}{12 \log 2}$$
- For a.e. x and for $a \geq 1$
$$\lim_{N\to\infty} \frac{1}{N}\{k \leq N;\ a_k = a\} = \frac{1}{\log 2} \log \frac{(a+1)^2}{a(a+2)}$$

On the iterates of Perron–Frobenius' operator

Think of f as a density function

$$\mathcal{L}f(x) = \sum_{y\,:\,T(y)=x} \frac{1}{|T'(y)|} f(y) = \sum_{a \geq 1} \left(\frac{1}{a+x}\right)^2 f\left(\frac{1}{a+x}\right)$$

On the iterates of Perron–Frobenius' operator

Think of f as a density function

$$\mathcal{L}f(x) = \sum_{y\,:\,T(y)=x} \frac{1}{|T'(y)|} f(y) = \sum_{a \geq 1} \left(\frac{1}{a+x}\right)^2 f\left(\frac{1}{a+x}\right)$$

Let $x = [0; a_1, a_2, \cdots]$.

$$\mathcal{L}^k f(x) = \sum_{a_1, \cdots, a_k} \frac{1}{(q_{k-1}x + q_k)^2} f\left(\frac{p_{k-1}x + p_k}{q_{k-1}x + q_k}\right)$$

Perron–Frobenius On a suitable functional space, there exists $\rho < 1$ such that

$$\mathcal{L}^k f(x) = \frac{1}{\log 2} \frac{1}{1+x} \int_0^1 f(x)dx + O(\rho^k ||f||)$$

On the iterates of Perron–Frobenius' operator

Think of f as a density function

$$\mathcal{L}f(x) = \sum_{y\,:\,T(y)=x} \frac{1}{|T'(y)|} f(y) = \sum_{a\geq 1} \left(\frac{1}{a+x}\right)^2 f\left(\frac{1}{a+x}\right)$$

Ruelle operator

$$\mathcal{L}_s f(x) = \sum_{h\in\mathcal{H}} h'(x)^s \cdot f\circ h(x) \qquad s\in\mathbb{C}$$

Involving additive costs

$$\mathcal{L}_{s,w} f(x) = \sum_{h\in\mathcal{H}} h'(x)^s \cdot e^{wc(h)} \cdot f\circ h(x)$$

The parameter w will be used for the study of probabilistic limit theorems and the parameter s plays a role in the study of Hausdorff dimensions.

Continued fractions

We consider a positive real number α.

One looks for sequences of rational numbers $(p_n/q_n)_n$ that satisfies

$$\lim p_n/q_n = \alpha$$

Continued fractions allow to do it with exponential speed

$$|\alpha - p_n/q_n| \leq \frac{1}{q_n^2}$$

Multidimensional continued fractions

If we start with two parameters (α, β), one looks for two sequences of rational numbers (p_n/q_n) and (r_n/q_n) with the same denominator that satisfy

$$\lim p_n/q_n = \alpha \qquad \lim r_n/q_n = \beta$$

Expected speed 3/2

$$|\alpha - p_n/q_n| \leq 1/q_n^{3/2} \qquad |\beta - r_n/q_n| \leq 1/q_n^{3/2}$$

Dirichlet's bound and exponential convergence

Dirichlet's theorem We are given a d-dimensional real vector $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_d) \in [0,1]^d$. For any positive integer N, there exist integers $p_1, \ldots, p_d, q$ with

$$1 \leq q \leq N$$

such that

$$|p_i - q\alpha_i| < \frac{1}{N^{1/d}} \qquad i = 1, 2, \cdots, d$$

Dirichlet's bound and exponential convergence

Dirichlet's theorem We are given a d-dimensional real vector $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_d) \in [0,1]^d$. For any positive integer N, there exist integers $p_1, \ldots, p_d, q$ with

$$1 \leq q \leq N$$

such that

$$|p_i - q\alpha_i| < \frac{1}{N^{1/d}} \leq \frac{1}{q^{1/d}} \qquad i = 1, 2, \cdots, d$$

Dirichlet's bound $1 + 1/d$

$$\left| \frac{p_i}{q} - \alpha_i \right| \leq \frac{1}{q^{1+\frac{1}{d}}}$$

Jacobi-Perron algorithm (1868-1907)

Consider the Jacobi-Perron algorithm. Its projective version is defined on the unit square $[0,1]^2$ by

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

With $x = b/a, y = c/a$, its linear version is defined on the positive cone $\{(a,b,c) \in \mathbb{R}^3 | 0 < b, c < a\}$ by

$$(a,b,c) \mapsto (a_1, b_1, c_1) = (b, c - \lfloor c/b \rfloor b, a - \lfloor a/b \rfloor b).$$

Set $C = \lfloor c/b \rfloor$, $A = \lfloor a/b \rfloor$. One has

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} A & 0 & 1 \\ 1 & 0 & 0 \\ C & 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 \\ b_1 \\ c_1 \end{pmatrix} = \begin{pmatrix} A & 0 & 1 \\ 1 & 0 & 0 \\ C & 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ c - Cb \\ a - Ab \end{pmatrix}.$$

Theorem of Perron–Frobenius type

One considers an infinite product of matrices

$$E_1 \cdots E_k \cdots$$

with entries in $\mathbb{N}$. One assumes that there exists a matrix B with strictly positive entries s.t. there exist $i_1 < j_1 < \cdots < i_k < j_k$ s.t.

$$B = E_{i_1} \cdots E_{j_1}, \cdots , B = E_{i_k} \cdots E_{j_k}, \cdots .$$

Then, the intersection of the cones

$$\cap_k \; E_1 \cdots E_k(\mathbb{R}_+^n)$$

is unidimensional [Furstenberg]

$\leadsto$ Convergence

Convergence for simultaneous approximations

$$M_1 \cdots M_n = \begin{pmatrix} q_1^{(n)} & \cdots & q_{d+1}^{(n)} \\ p_{1,1}^{(n)} & \cdots & p_{1,d+1}^{(n)} \\ & \cdots & \\ p_{d,1}^{(n)} & \cdots & p_{d,d+1}^{(n)} \end{pmatrix} \rightsquigarrow \left(\frac{p_{1,j}^{(n)}}{q_j^{(n)}}, \cdots, \frac{p_{d,j}^{(n)}}{q_j^{(n)}} \right)$$

Weak convergence Convergence in angle

$$\lim_{n \to +\infty} \left(\frac{p_{1,j}^{(n)}}{q_j^{(n)}}, \cdots, \frac{p_{d,j}^{(n)}}{q_j^{(n)}} \right) = (\alpha_1, \cdots, \alpha_d)$$

Strong convergence Convergence in distance

$$\lim_{n \to +\infty} |q_j^{(n)} \alpha_i - p_{i,j}^{(n)}| = 0 \text{ for all } i, j$$

Convergence of Jacobi-Perron algorithm

Theorem [Broise-Guivarc'h'99] There exists $\delta > 0$ s.t. for almost every (α, β)

$$|\alpha - p_n/q_n| < \frac{1}{q_n^{1+\delta}}, \qquad |\beta - r_n/q_n| < \frac{1}{q_n^{1+\delta}}$$

where p_n, q_n, r_n are produced by either by Jacobi-Perron algorithm

What is the dependence of δ with respect to the number of parameters?

Lyapunov exponents

We consider a MCF algorithm given by a piecewise constant transformation

$$A:\ [0,1]^d \to \mathrm{GL}(d+1,\mathbb{Z})$$

with its associated transformation $([0,1]^d, T_A, \nu)$. We assume ν ergodic. Let

$$A^{(n)}(u) = A(u)A(T_A u)\cdots A(T_A^{n-1}u).$$

We assume $\log^+ ||A(x)||$ is ν-integrable ($\log^+(a) = \max\{\log a, 0\}$ for $a > 0$).

Then by the Oseledets Theorem the following Lyapunov exponents λ_k, $1 \leq k \leq d{+}1$, exist

$$\lambda_1 + \cdots + \lambda_k = \lim_{n\to\infty} \frac{1}{n} \log \| \wedge^k A^{(n)}(u)\| \quad \text{for } \nu\text{-a.e. } u \in \Delta.$$

Lyapunov exponents

$$A_n(x) = \begin{pmatrix} q_n & q_{n-1} \\ p_n & p_{n-1} \end{pmatrix}$$

Theorem For a.e. x,

$$\lim \frac{1}{n} \log q_n = \frac{\pi^2}{12 \log 2} = 1.18 \cdots = \lambda_1$$

λ_1 is the first Lyapunov exponent

First Lyapunov exponent $=$ "log largest eigenvalue" $\rightsquigarrow$ size of the matrices/convergents $A_n(x) \sim q_n(x) \sim e^{\lambda_1 n}$

Number of steps in Euclid's algorithm $=$ size/ log eigenvalue

$$\log N / \lambda_1$$

Second Lyapunov exponent $=$ "log of the second eigenvalue" $\rightsquigarrow$ measures the distance between column vectors

Lyapunov exponents

First Lyapunov exponent = log largest eigenvalue $\rightsquigarrow$ size of the matrices/convergents $M^{(n)}(\boldsymbol{\alpha}) \sim q_i^n(\boldsymbol{\alpha}) \sim e^{\lambda_1 n}$

Second Lyapunov exponent = "log of the second eigenvalue" $\rightsquigarrow$ measures the distance between column vectors

$$M^{(n)}(\boldsymbol{\alpha}) = \begin{pmatrix} q_1^{(n)} & \cdots & q_{d+1}^{(n)} \\ p_{1,1}^{(n)} & \cdots & p_{1,d+1}^{(n)} \\ & \cdots & \\ p_{d,1}^{(n)} & \cdots & p_{d,d+1}^{(n)} \end{pmatrix}$$

Lyapunov exponents

First Lyapunov exponent $=$ log largest eigenvalue$\rightsquigarrow$ size of the matrices/convergents $M^{(n)}(\boldsymbol{\alpha}) \sim q_i^n(\boldsymbol{\alpha}) \sim e^{\lambda_1 n}$

Second Lyapunov exponent $=$ "log of the second eigenvalue" $\rightsquigarrow$ measures the distance between column vectors

$$M^{(n)}(\boldsymbol{\alpha}) = \begin{pmatrix} q_1^{(n)} & \cdots & q_{d+1}^{(n)} \\ p_{1,1}^{(n)} & \cdots & p_{1,d+1}^{(n)} \\ & \cdots & \\ p_{d,1}^{(n)} & \cdots & p_{d,d+1}^{(n)} \end{pmatrix}$$

$$\lambda_1 \leftrightarrow \log \|M^{(n)}\|$$

$$\lambda_1 + \lambda_2 \leftrightarrow \log \| \wedge^2 M^{(n)}\| \leftrightarrow \log \|c_i^{(n)} \wedge c_j^{(n)}\|$$

λ_2 distance between column vectors

Dirichlet's bound $1 + 1/d$ vs. $1 - \lambda_2/\lambda_1$

Higher-dimensional case

Numerical experiments indicate that classical multidimensional continued fraction algorithms seem to cease to be strongly convergent for high dimensions. The only exception seems to be the Arnoux-Rauzy algorithm which, however, is defined only on a set of measure zero [B.-Steiner-Thuswaldner]

Higher-dimensional case

Numerical experiments indicate that classical multidimensional continued fraction algorithms seem to cease to be strongly convergent for high dimensions. The only exception seems to be the Arnoux-Rauzy algorithm which, however, is defined only on a set of measure zero [B.-Steiner-Thuswaldner]

d	$\lambda_2(A_J)$	$1-\frac{\lambda_2(A_J)}{\lambda_1(A_J)}$	d	$\lambda_2(A_J)$	$1-\frac{\lambda_2(A_J)}{\lambda_1(A_J)}$
2	-0.44841	1.3735	7	-0.02819	1.0243
3	-0.22788	1.1922	8	-0.01470	1.0127
4	-0.13062	1.1114	9	-0.00505	1.0044
5	-0.07880	1.0676	10	$+0.00217$	0.9981
6	-0.04798	1.0413	11	$+0.00776$	0.9933

Table: Heuristically estimated values for the second Lyapunov exponent and the uniform approximation exponent of the Jacobi–Perron Algorithm

Let $GL(n, \mathbb{Z})$ stand for the set of matrices with integer entries and determinant ± 1.

Theorem [Duke-Rudnick-Sarnak] One has

$$\{M \in GL(n, \mathbb{Z}), |m_{ij}| \leq T\} \sim c_n T^{n^2 - n}$$

How to generate "random matrices" in $GL_n(\mathbb{Z})$?

How does LLL produce good approximations?

Let

$$M_t := \begin{pmatrix} 1 & 0 & \cdots & 0 & -\alpha_1 \\ 0 & 1 & \cdots & 0 & -\alpha_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & -\alpha_d \\ 0 & \cdots & \cdots & 0 & t \end{pmatrix}$$

How does LLL produce good approximations?

Let

$$M_t := \begin{pmatrix} 1 & 0 & \cdots & 0 & -\alpha_1 \\ 0 & 1 & \cdots & 0 & -\alpha_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & -\alpha_d \\ 0 & \cdots & \cdots & 0 & t \end{pmatrix}$$

LLL produces in polynomial time a vector b_1 such that

$$||b_1|| \leq 2^{d/4} det(M_t)^{1/d+1} = 2^{d/4} t^{1/d+1}$$

One has

$$b_1 = (p_1 - q\alpha_1)e_1 + \cdots + (p_d - q\alpha_d e_d) + qte_{d+1}$$

$$\forall i, \quad |p_i - \alpha_i q| \leq 2^{d/4} t^{1/d+1} \quad \text{and} \quad qt \leq 2^{d/4} t^{1/d+1}$$

$$\rightsquigarrow \forall i, \quad |p_i - \alpha_i q| \leq 2^{(d+1)/4} 1/q^{1/d}$$