Exposants de Lyapunov, produits de matrices et fractions continues

V. Berthé, W. Steiner, J. Thuswaldner

INSTITUT DE RECHERCHE EN INFORMATIQUE FONDAMENTALE

Université Paris Cité

Séminaire Flajolet

- Multidimensional continued fractions
- On the second Lyapunov exponent
- Lattice reduction and unimodular matrices

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

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

$$||q_n\alpha|| \leq \frac{1}{q_n}$$

Euclid algorithm

We start with two nonnegative integers u_0 and u_1

$$u_0 = u_1 \left\lfloor \frac{u_0}{u_1} \right\rfloor + u_2$$

$$u_1 = u_2 \left\lfloor \frac{u_1}{u_2} \right\rfloor + u_3$$

$$\vdots$$

$$u_{m-1} = u_m \left\lfloor \frac{u_{m-1}}{u_m} \right\rfloor + u_{m+1}$$

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

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

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

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

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

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

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

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

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

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 $1 + 1/d$

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

Canonicity of continued fractions

- Euclid's algorithm Starting with two numbers, one subtracts the smallest from the largest
- Unimodularity

$$\det \begin{pmatrix} q_{n+1} & q_n \\ p_{n+1} & p_n \end{pmatrix} = \pm 1$$

- Best approximation property

  Theorem A rational number p/q is a best approximation of the real number α if every p'/q' with $1 \leq q' \leq q$, $p/q \neq p'/q'$ satifies

$$|q\alpha - p| < |q'\alpha - p'|$$

  Every best approximation of α is a convergent

From $SL(2,\mathbb{N})$ to $SL(3,\mathbb{N})$

$SL(d,\mathbb{N})$: matrices with entries in $\mathbb{N}$ and determinant 1
$GL(d,\mathbb{N})$: matrices with entries in $\mathbb{N}$ and determinant ± 1

$SL(2,\mathbb{N})$ is a finitely generated free monoid. It is generated by

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

- $SL(2,\mathbb{N})$ is a free and finitely generated monoid
- $SL(3,\mathbb{N})$ is not free
- $SL(3,\mathbb{N})$ is not finitely generated. Consider the family of matrices

$$\begin{pmatrix} 1 & 0 & n \\ 1 & n-1 & 0 \\ 1 & 1 & n-1 \end{pmatrix}$$

These matrices are undecomposable for $n \geq 3$ [Rivat]

Multidimensional continued fractions

There is no canonical generalization of continued fractions to higher dimensions

Several approaches are possible

- Best simultaneous approximations
  Every q' with $1 \leq q' < q$ satisfies $|||q(\alpha, \beta)||| < |||q'(\alpha, \beta)|||$
  But we loose unimodularity, and the sequence of best approximations depends on the chosen norm [Lagarias]
- Klein polyhedra and sails [Arnold]
- Unimodular multidimensional Euclid's algorithms
  - sequences of nested cones approximating a direction Jacobi-Perron algorithm, Brun algorithm [Brentjes, Schweiger]
  - lattice reduction (LLL) [Lagarias],[Ferguson-Forcade], [Just], [Grabiner-Lagarias][Bosma-Smeets][Beukers]

What is expected?

We are given $(\alpha_1, \cdots, \alpha_d)$ which produces a sequence of basis of $\mathbb{Z}^{d+1}$ and/or a sequence of approximations

Arithmetics A two-dimensional continued fraction algorithm is expected to

- detect integer relations for $(1, \alpha_1, \cdots, \alpha_d)$
- give algebraic characterizations of periodic expansions
- converge sufficiently fast
- provide good rational approximations

Good means "with respect to Dirichlet's theorem": there exist infinitely many $(p_i/q)_{1 \leq i \leq d}$ such that

$$\max_i |\alpha_i - p_i/q| \leq \frac{1}{q^{1+1/d}}$$

We also want...

- to understand generic behaviour
- to be able to control the number of executions if the parameters are rational etc.
- Hausdorff dimensions for bounded digit sets etc.

We also want...

- to understand generic behaviour
  Continued fractions

$$\lim \frac{\log q_n}{n} = \frac{\pi^2}{12 \log 2} = 1.18\ldots \qquad \text{for a.e. } \alpha$$

$$\lim \frac{1}{n}\{k \le n;\ a_k = a\} = \frac{1}{\log 2} \log \frac{(k+1)^2}{k(k+2)} \qquad \text{for a.e. } \alpha$$

- to be able to control the number of executions if the parameters are rational etc.
- Hausdorff dimensions for bounded digit sets etc.

We also want...

- to understand generic behaviour
- to be able to control the number of executions if the parameters are rational etc.

  Continued fractions $\ell(u, v)$: number of steps in Euclid algorithm. For $0 < v < u \leq N$ and $\gcd(u, v) = 1$

  $$\mathbb{E}_N(\ell) \sim \frac{12 \log 2}{\pi^2} \cdot \log N$$ average case [Baladi-Vallée]

- Hausdorff dimensions for bounded digit sets etc.

Multidimensional continued fractions

Aim Write $\mathbf{x} \in \Delta \subseteq [0,1]^d$ as $\mathbf{x} = \lim_{n\to\infty} \frac{\mathbf{p}^{(n)}}{q^{(n)}}$

We consider MCF algorithms given by a piecewise constant transformation

$$A:\ \Delta \to \mathrm{GL}(d+1,\mathbb{Z})$$

with associated transformations

$$T_A:\ \Delta \to \Delta, \quad \mathbf{x} \mapsto \pi\big(\iota(\mathbf{x})\,A(\mathbf{x})^{-1}\big)$$

$$\iota(x_1,\dots,x_d) = (1,x_1,\dots,x_d), \quad \pi(x_0,x_1,\dots,x_d) = \big(\tfrac{x_1}{x_0},\dots,\tfrac{x_d}{x_0}\big)$$

Toward the Gauss map

Let (x_0, x_1) with $x_0 > x_1 > 0$. We divide the largest entry by the smallest and we continue

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

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

Toward the Gauss map

Let (x_0, x_1) with $x_0 > x_1 > 0$. 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 $T(\alpha) = 1/\alpha - [1/\alpha]$.

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

Toward the Gauss map

Let (x_0, x_1) with $x_0 > x_1 > 0$. 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 $T(\alpha) = 1/\alpha - [1/\alpha]$.

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

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

Multidimensional continued fractions

We consider MCF algorithms given by a piecewise constant transformation

$$A:\ \Delta \to \mathrm{GL}(d+1,\mathbb{Z})$$

with associated transformations

$$T_A:\ \Delta \to \Delta, \quad \mathbf{x} \mapsto \pi\big(\iota(\mathbf{x})\,A(\mathbf{x})^{-1}\big)$$

$$\iota(x_1,\ldots,x_d) = (1,x_1,\ldots,x_d), \quad \pi(x_0,x_1,\ldots,x_d) = \big(\tfrac{x_1}{x_0},\ldots,\tfrac{x_d}{x_0}\big)$$

Multidimensional continued fractions

We consider MCF algorithms given by a piecewise constant transformation

$$A : \Delta \to \mathrm{GL}(d+1, \mathbb{Z})$$

with associated transformations

$$T_A : \Delta \to \Delta, \quad \mathbf{x} \mapsto \pi\big(\iota(\mathbf{x})\, A(\mathbf{x})^{-1}\big)$$

$$\iota(x_1, \ldots, x_d) = (1, x_1, \ldots, x_d), \quad \pi(x_0, x_1, \ldots, x_d) = \left(\tfrac{x_1}{x_0}, \ldots, \tfrac{x_d}{x_0}\right)$$

Regular continued fractions with $d = 1$ $A(x) = \begin{pmatrix} \lfloor \frac{1}{x} \rfloor & 1 \\ 1 & 0 \end{pmatrix}$

$$T(x) = \pi\left((1, x) \begin{pmatrix} 0 & 1 \\ 1 & -\lfloor \frac{1}{x} \rfloor \end{pmatrix}\right) = \pi\big(x, 1 - \lfloor \tfrac{1}{x} \rfloor x\big) = \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor$$

Continued fractions and dynamical systems

Consider the Gauss map

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

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

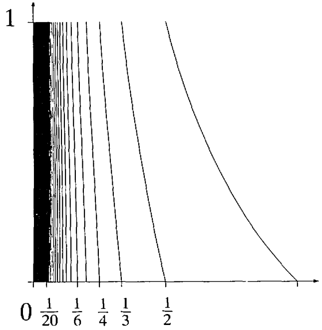
$$x = \frac{1}{a_1 + x_1} \qquad\qquad a_n = \left[\frac{1}{T^{n-1}x}\right]$$

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

Continued fractions and dynamical systems

Consider the Gauss map

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



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

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

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

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

Continued fractions

$$\alpha \mapsto \left(\frac{1}{\alpha} - \lfloor\frac{1}{\alpha}\rfloor\right)$$

$$\begin{pmatrix} 1 \\ \alpha \end{pmatrix} = \alpha_0\alpha_1 \cdots \alpha_{n-1} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha_n \end{pmatrix}$$

Jacobi–Perron

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

$$\begin{pmatrix} 1 \\ \alpha \\ \beta \end{pmatrix} = \alpha_0 \cdots \alpha_{n-1} \begin{pmatrix} q_n & q_n' & q_n'' \\ p_n & p_n' & p_n'' \\ r_n & r_n' & r_n'' \end{pmatrix} \begin{pmatrix} 1 \\ \alpha_n \\ \beta_n \end{pmatrix}$$

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]

$\rightsquigarrow$ 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, $1 \le k \le d+1$, 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. $1 - \lambda_2/\lambda_1$

Lyapunov exponents

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

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

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

$$\lim \frac{1}{n} \log(q_n^{1/d} ||q_n x||) = \frac{\lambda_1}{d} + \lambda_2 = \frac{(\lambda_2 - \lambda_3) + \cdots + (\lambda_2 - \lambda_{d+1})}{d}$$

$$\text{since } \lambda_1 + \cdots + \lambda_{d+1} = 0$$

Hence $\frac{\lambda_1}{d} + \lambda_2 = 0$ if and only if $\lambda_2 = \cdots = \lambda_{d+1} = -1/d$

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

Theorem [Duke-Rudnick-Sarnak] One has

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

What is a random matrix in $GL_n(\mathbb{Z})$?

From lattice reduction to contined fractions

In a letter to Jacobi in 1850, Hermite explained the following idea
Consider

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

Let $t > 0$. We take the corresponding lattice Λ_t of $\mathbb{R}^{d+1}$

$$\mathbb{Z}e_1 + \cdots + \mathbb{Z}e_d + \mathbb{Z}(te_{d+1} - (\alpha_1 e_1 + \cdots + \alpha_d e_d))$$

A vector of the lattice is of the form

$$\sum_{i=1}^{d}(p_i - q_t\alpha_i)e_i + qte_{d+1}$$

Take a short vector in Λ_t

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

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

- We take t small
- One has $\det(M_t) = t$

Rem: One changes the lattice at each step instead of changing the bases of a fixed lattice
The parameter t only occurs in the last line

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

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

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

Lattice reduction algorithms

Lattice reduction is based on the following elementary basis transformations on the vectors of the basis $(b_1, \ldots, b_{d+1})$

- size reduction the vector b_i is replaced by $b_i - \lambda b_j$, $1 \leq j < i$
- swaps one exchanges b_i and b_{i+1}

These operations are decided with respect to the Gram-Schmitdt orthogonalization of the basis b

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^* \qquad \mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$$

- Size reduction $|\mu_{i,j}| \leq 1/2$ for $i > j$
- Lovász condition $(\delta - \mu_{i+1,i}^2)||b_i^*||^2 \leq ||b_{i+1}^*||^2$

[Lagarias'94] Let t tend to 0 and consider Minkowski reduction. The conditions are linear in $\sqrt{t}$ but when $n = 7$, the number of inequalities is about $90,000$ for Minkowski reduction.

[Bosma-Smeets'2013] Decrease the value of t by diving it by a fixed constant.

[Beukers'2014]
Proves the linearity in $\sqrt{t}$ of the conditions in LLL.
The values of $t > 0$ for which M_t is LLL-reduced form an interval $[t_0, t_1]$.
If $\alpha \notin \mathbb{Q}^d$, the sequence of critical points is an infinite sequence descending to 0.

Toward continued fractions

One has $t \downarrow 0$

- How to change t?
- How much does one have to recompute when one changes t?
- How to choose stopping times for t?
- Can we get nonnegative matrices?
- What are the rules that provide exponential convergence?
- Can we evaluate the growth of the size of the matrices $M_1 \cdots M_n$?