Lattice reduction and continued fractions

V. Berthé

IRIF-CNRS-Paris-France

MACAO Workshop

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

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

Continued fractions

We represent real numbers in $(0, 1)$ as

$$\alpha = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}}$$

with the partial quotients (digits) a_i being positive integers

Continued fractions

We represent real numbers in $(0, 1)$ as

$$\alpha = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}}$$

with the partial quotients (digits) a_i being positive integers

Rational approximations are then given by

$$p_n/q_n = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}} \qquad |\alpha - p_n/q_n| \leq \frac{1}{q_n^2}$$

Dirichlet's bound and exponential convergence

Dirichlet's theorem

Given real numbers $(\alpha_d, \cdots, \alpha_d)$, for any positive integer N, there exist integers $p_1, \ldots, p_d, q$ with

$$1 \le q \le N$$

such that

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

Dirichlet's bound and exponential convergence

Dirichlet's theorem

Given real numbers $(\alpha_d, \cdots, \alpha_d)$, for any positive integer N, there exist integers $p_1, \ldots, p_d, q$ with

$$1 \leq q \leq N$$

such that

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

Dirichlet's bound $1 + 1/d$

Euclid 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 to 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

$$u_0 = u_1 a_1 + u_2$$

$$\vdots$$

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

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

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

$$\frac{u_1}{u_0} = \frac{1}{a_1 + \frac{u_2}{u_1}}$$

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

Matricial description

We start with two real numbers (x_0, x_1) in $(0,1)^2$ with $x_0 > x_1$
We divide the largest entry by the smallest and we continue

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

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

Matricial description

We start with two real numbers (x_0, x_1) in $(0,1)^2$ 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

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

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

Multidimensional continued fractions

If we start with two parameters (α, β), one looks for two sequences of rational numbers (p_n/q_n) et (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

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

Canonicity of continued fractions

- Euclid's algorithm Starting with two numbers, one subtracts the smallest to 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 $SL(3,\mathbb{N})$

Rem $SL(2,\mathbb{N})$ 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.

We also want...

- to understand generic behaviour

  Continued fractions

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

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

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

  Continued fractions

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

  For $0 < v < u \leq N$ and $\gcd(u, v) = 1$

$$\mathbb{E}_N(\ell) \sim \frac{12 \log 2}{\pi^2} \cdot \log N \qquad \text{average case}$$

Multidimensional Euclid's algorithms: a zoo of algorithms

- Jacobi-Perron [Jacobi'1868–Perron'1907]: we subtract the first one to the two other ones with $0 \leq x_1, x_2 \leq x_3$

$$(x_1, x_2, x_3) \mapsto (x_2 - [\frac{x_2}{x_1}]x_1, x_3 - [\frac{x_3}{x_1}]x_1, x_1)$$

- Brun [Brun'1919]: we subtract the second largest and we reorder with $x_1 \leq x_2 \leq x_3$

$$(x_1, x_2, x_3) \mapsto (x_1, x_2, x_3 - x_2)$$

- Poincaré: we subtract the previous one and we reorder with $x_1 \leq x_2 \leq x_3$

$$(x_1, x_2, x_3) \mapsto (x_1, x_2 - x_1, x_3 - x_2)$$

- Selmer: we subtract the smallest to the largest and we reorder with $x_1 \leq x_2 \leq x_2$

$$(x_1, x_2, x_3) \mapsto (x_1, x_2, x_3 - x_1)$$

- Fully subtractive: we subtract the smallest one to all the largest ones and we reorder with $x_1 \leq x_2 \leq x_3$

Poincaré algorithm [Nogueira'95]

$$(x_1, x_2, x_3) \mapsto (x_1, x_2 - x_1, x_3 - x_2),\ \ x_1 \le x_2 \le x_3$$

$$1/\varphi^2 + 1/\varphi = 1$$

$$\begin{array}{lll}
1/\varphi^2 & 1/\varphi & 100 \\
1/\varphi^3 & 1/\varphi^2 & 100 - 1/\varphi \\
1/\varphi^4 & 1/\varphi^3 & 100 - 1/\varphi - 1/\varphi^2 \\
\cdots & \cdots & \cdots \\
1/\varphi^{k+1} & 1/\varphi^k & 100 - \sum_{i<k} 1/\varphi^i
\end{array}$$

Jacobi-Perron algorithm

Continued fractions

$$\begin{pmatrix} 1 \\ \alpha \end{pmatrix} = \lambda_n \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha_n \end{pmatrix}$$

Jacobi–Perron algorithm

$$\begin{pmatrix} 1 \\ \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 & 1 & k \\ 1 & 0 & \ell \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \beta - \ell\alpha \\ 1 - k\alpha \\ \alpha \end{pmatrix} \text{ with } \ell = \lfloor \beta/\alpha \rfloor, k = \lfloor 1/\alpha \rfloor$$

$$\begin{pmatrix} 1 \\ \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 & 1 & k_1 \\ 1 & 0 & \ell_1 \\ 0 & 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 & k_n \\ 1 & 0 & \ell_n \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha_n \\ \beta_n \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ \alpha \\ \beta \end{pmatrix} = \lambda_n \begin{pmatrix} q_n & q_n' & q_n'' \\ p_n & p_n' & p_n'' \\ r_n & r_n' & r_n'' \end{pmatrix} \begin{pmatrix} 1 \\ \alpha_n \\ \beta_n \end{pmatrix}$$

Unimodular multidimensional continued fractions

A unimodular d-dimensional continued fraction map over $[0,1]^d$ is a map $T : [0,1]^d \to [0,1]^d$ such that for any $\boldsymbol{\alpha} \in [0,1]^d$, there is a matrix $M(\boldsymbol{\alpha})$ in $GL(d,\mathbb{Z})$ satisfying

$$\boldsymbol{\alpha} = M(\boldsymbol{\alpha})T(\boldsymbol{\alpha})$$

The associated continued fraction algorithm consists in iteratively applying the map T on a vector $\boldsymbol{\alpha} \in [0,1]^d$. This yields the following sequence of matrices, called the continued fraction expansion of $\boldsymbol{\alpha}$

$$(M(T^n(\boldsymbol{\alpha})))_{n\in\mathbb{N}}.$$

Set $M_n := M(T^n(\boldsymbol{\alpha}))$

$$\boldsymbol{\alpha} = M_1 \cdots M_n T^n(\boldsymbol{\alpha})$$

If the matrices have nonnegative entries, the algorithm is said to be nonnegative (Perron–Frobenius theory)

About nonnegative matrices

Theorem of Perron–Frobenius type [Furstenberg]

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.

Convergence speed? Type of convergence? Weak? strong?

Convergence

$$\boldsymbol{\alpha} = M_1 \cdots M_n T^n(\boldsymbol{\alpha}) \text{ with } M_1 \cdots M_n = \begin{pmatrix} q_1^{(n)} & \cdots & q_{d+1}^{(n)} \\ p_{1,1}^{(n)} & \cdots & p_{1,d+1}^{(n)} \\ & \cdots & \\ p_{d,1}^{(n)} & \cdots & p_{d,d+1}^{(n)} \end{pmatrix}$$

One considers simultaneous approximations $\left(\frac{p_{1,j}^{(n)}}{q_j^{(n)}}, \cdots, \frac{p_{d,j}^{(n)}}{q_j^{(n)}}\right)$

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 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 Brun/Jacobi-Perron algorithm

Brun [Ito-Fujita-Keane-Ohtsuki'96]
Jacobi-Perron[Broise-Guivarc'h'99]

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

Exponentiation based on Brun algorithm

An SPA resistant exponentiation based on Brun's gcd algorithm and addition chains [B.-Plantard]

One performs an exponentiation g^e for a given e for a generic group
Cut e into d blocks

$$e = \sum_{i=0}^{d-1} e_i 2^{ik/d}$$

For Brun algorithm, as the dimension d increases, the probabilty that partial quotients equal to 1 tends to 1 (one performs subtractions and not divisions) [B.-Lhote-Vallée]
$\rightsquigarrow$ Apply Brun algorithm and addition chains

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	$\lambda_2(A_B)$	$1-\frac{\lambda_2(A_B)}{\lambda_1(A_B)}$	d	$\lambda_2(A_B)$	$1-\frac{\lambda_2(A_B)}{\lambda_1(A_B)}$
2	-0.11216	1.3683	7	-0.01210	1.0493
3	-0.07189	1.2203	8	-0.00647	1.0283
4	-0.04651	1.1504	9	-0.00218	1.0102
5	-0.03051	1.1065	10	$+0.00115$	0.9943
6	-0.01974	1.0746	11	$+0.00381$	0.9799

Table: Heuristically estimated values for the second Lyapunov exponent and the uniform approximation exponent of the Brun Algorithm

Multidimensional continued fraction algorithms

- Allowed operations on numbers

$$+,\ -,\ /,\ \times,\ [\,],\ \geq$$

- Allowed operations on matrices: elementary basis transformations
  - interchanging two vectors $\rightsquigarrow$ permutation matrices
  - adding an integer multiple of one basis vector to another basis vector $\rightsquigarrow$ transvection matrices

Ex. LLL algorithm Size reduction steps and exchange steps
Decisions are taken with respect to quadratic norms

LLL approach

Lattice reduction algorithms

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

- 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 $(\delta - \mu_{i+1,i}^2)||b_i^*||^2 \leq ||b_{i+1}^*||^2$

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 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

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

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

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

Approximations and lattices

Let

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

[Lagarias'93]

$$\forall \boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_d), \forall Q,\ \exists q,\ 1 \leq q \leq Q,\ |||q\boldsymbol{\alpha}||| < \sqrt{d+1} Q^{-1/d}$$

[Lagarias'85,'94,Grabiner-Lagarias'2001]

[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 $\boldsymbol{\alpha} \notin \mathbb{Q}^d$, 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 $M_1 \cdots M_n$?