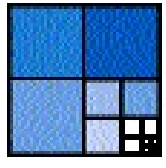
DYNa3S
Dynamique des algorithmes du pgcd : une approche Algorithmique, Analytique, Arithmétique et Symbolique

LIAFA-CNRS-Paris-France
berthe@liafa.univ-paris-diderot.fr
http ://www.liafa.univ-paris-diderot.fr/~berthe



- ANR SIMI 2
- Démarrage : 15/10/2013
- Durée : 48 mois
- Fin : 14/10/2017
- 2 partenaires
  - P7, LIAFA, V. Berthé
  - Univ. Caen Nasse Normandie, GREYC, B. Vallée

Membres

LIAFA Pôle 1

- Valérie Berthé
- Pierre Arnoux
- Fabien Durand
- Th. Fernique
- Tomás Hejda
- Damien Jamet
- Timo Jolivet
- Sébastien Labbé
- Xavier Provençal
- W. Steiner

GREYC Pôle 2

- Brigitte Vallée
- Ali Akhavi
- Julien Clément
- G. Hanrot
- Loïck Lhote
- V. Maume-Deschamps
- Frédéric Paccaut
- D. Stehlé ? ? ? ?
- Gilles Villard

Experts

- T. Plantard
- J. Cassaigne
- S. Ferenczi
- V. Delecroix
- Thierry Monteil
- Anne Siegel
- J.-O. Lachaud
- Viviane Baladi
- Anne Broise
- J. Buzzi

Finances (par pôle)

- 132 454 euros par pôle
- Versements par pôle : 26 491 euros par an
- Stages : 12 mois, 5400 euros
- Postdoc : 18 mois, 67770 euros
- Missions :
  - Missions confs : 10 000 euros
  - Invitations : 11 000
  - Missions internes : 21 000
  - Organisation confs : 10 000
  - Ordis : 1100+ Livres : 1000
- Total missions : 54 100 euros (par pôle)

Compte-rendus intermédiaires

- 6 mois
- 18 mois
- 30 mois

Retombéees

- Organization of two international conferences
- Preprints available via a collection within the Hal-Diderot open archive
- Getting young scientists interested through lectures
  - during one of the Ecoles Jeunes Chercheurs of the GDR IM
  - at master level
  - by using simple examples issued e.g. from word combinatorics and discrete geometry during Sage formation days
- Giving popular lectures (eg., Fête de la Science)
- Writing on Images des Mathématiques and Interstices
- If some potential in terms of valorisation emerges during the project, the unit Diderot Valorisation of Université Paris Diderot will follow the project.
- All the implementations will be published in Sage

Rencontres internes

- Organization of two international conferences
- Joint event with ANR HPAC (fin 2015)
  High-Peformance Computer Algebra
- 2 à 3 rencontres par an de 3 jours

Résumé

Objet : les algorithmes de type Euclide

Un algorithme de pgcd = système dynamique discret et entrées entières

- Problème du calcul du pgcd de plusieurs entiers
  pgcd ou pgcd étendu=coeff. Bezout
- Application en géométrie discrète où la compréhension des primitives basiques, les droites et les plans discrets, repose sur des algorithmes de type Euclide
  a priori coordonnées entières

Objectifs principaux

Étude extensive des algorithmes de pgcd qui sont décrits par un système dynamique

- Algorithmes de pgcd
  - Construction d'algorithmes efficaces de pgcd
  - Analyse systématique : pire cas, analyse en moyenne et en distributions
  - Comparaison transverse des performances de ces algorithmes selon une approche algorithmique, analytique, arithmétique et symbolique
- Application en géométrie discrète pour l'étude des droites discrètes et des plans discrets dont la compréhension repose sur des algorithmes de type Euclide

  $\rightsquigarrow$ un point de vue supplémentaire concernant les comparaisons entre ces algorithmes

Algorithmes de pgcd

Deux types d'algorithmes de pgcd, tous deux étant associés à des homographies par morceaux

- algorithmes de réduction dans les réseaux qui calculent des vecteurs courts
- algorithmes de fractions continues multidimensionnels qui calculent de bonnes approximations rationnelles

Comparaisons des algorithmes et description des paramètres principaux

Quand les entrées sont

- soit réelles : trajectoires génériques
- soit entières : trajectoires tronquées

Deux points de vue

- un point de vue discret, correspondant aux entrées rationnelles
- un point de vue continu, correspondant aux entrées réelles

deux cadres dynamiques considérés pour eux-mêmes, mais aussi en interaction, selon la méthodologie de l'analyse dynamique

Analyse dynamique

3 étapes principales

1. L'algorithme discret est étendu en un système dynamique continu

   les exécutions sont décrites par des trajectoires particulières : trajectoires des points rationnels

2. Les paramètres principaux de l'algorithme sont étendus et étudiés dans ce contexte continu

   l'étude des trajectoires rationnelles est remplacée par l'étude des trajectoires génériques

3. On opère un transfert du continu au discret

   $\rightsquigarrow$ le comportement probabiliste de la version discrète (trajectoires rationnelles) est très similaire au comportement continu (trajectoires génériques)

Analyse dynamique

3 étapes principales

1. L'algorithme discret est étendu en un système dynamique continu Euclide $\rightsquigarrow$ Gauss $x \mapsto \{1/x\}$

   les exécutions sont décrites par des trajectoires particulières : trajectoires des points rationnels

2. Les paramètres principaux de l'algorithme sont étendus et étudiés dans ce contexte continu

   l'étude des trajectoires rationnelles est remplacée par l'étude des trajectoires génériques

3. On opère un transfert du continu au discret

   $\rightsquigarrow$ le comportement probabiliste de la version discrète (trajectoires rationnelles) est très similaire au comportement continu (trajectoires génériques)

Outils et méthodes

Proviennent

- de la théorie ergodique et de la dynamique symbolique
- de la combinatoire analytique, de l'analyse dynamique + outils algorithmiques

Outils et méthodes

Proviennent

- de la théorie ergodique et de la dynamique symbolique
- de la combinatoire analytique, de l'analyse dynamique + outils algorithmiques

Des approches complémentaires et différentes :

- systèmes dynamiques : ergodique, symbolique, dynamique réelle
- algorithmes de réduction dans les réseaux
- arithmétique informatique
- analyse d'algorithmes

Domaine d'application

- Géométrie discrète

Focus

- LLL en dimension 3
- Algorithme de Brun
- Polynômes à coefficients dans un corps fini

Vers un vocabulaire commun

Une approche Algorithmique, Analytique, Arithmétique et Symbolique

Gcd algorithms and beyond

We want to

- compute the gcd of n numbers

Gcd algorithms and beyond

We want to

- compute the gcd of n numbers
  - $n = 3$ or n large
  - small/big size
  - same size/different sizes

Gcd algorithms and beyond

We want to

- compute the gcd of n numbers
  - $n = 3$ or n large
  - small/big size
  - same size/different sizes
- find Bezout's coefficients : extended gcd
- find simultaneous rational approximations

Gcd algorithms and beyond

We want to

- compute the gcd of n numbers
  - $n = 3$ or n large
  - small/big size
  - same size/different sizes
- find Bezout's coefficients : extended gcd
- find simultaneous rational approximations

How to compare multidimensional gcd algorithms ?

Euclid algorithm

We start with two nonnegative integers u_0 and u_1

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

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

$$\vdots$$

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

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

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

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

$$u_0 = u_1 a_1 + u_2$$

$$\vdots$$

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

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

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

Euclid's algorithm yields the digits
for the continued fraction expansion of $\frac{u_1}{u_0}$

Euclid algorithm and continued fractions

We start with two coprime integers u_0 and u_1

$$u_0 = u_1 a_1 + u_2$$

$$\vdots$$

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

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

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

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

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

Discrete dynamical system

We are given a dynamical system

$$T : X \to X$$

Discrete stands for discrete time
The set X is the set of states
The map T is the law of time evolution

Discrete dynamical system

We are given a dynamical system

$$T : X \to X$$

We consider orbits/trajectories of points of X under the action of the map T

$$\{T^n x \mid n \in \mathbb{N}\}$$

Discrete dynamical system

We are given a dynamical system

$$T : X \to X$$

We partition X in to a finite number of subsets $X = \cup_{i=1}^{d} X_i$

We code the trajectory of a point x with respect to (X_i)

$$\{T^n x \mid n \in \mathbb{N}\} \rightsquigarrow (u_n)_{n\in\mathbb{N}} \in \{1, 2, \cdots, d\}^{\mathbb{N}}$$

From geometric dynamical systems to symbolic dynamical systems and backwards

Discrete dynamical system

We are given a dynamical system

$$T : X \to X$$

- Topological dynamics describes the qualitative/topological asymptotic behaviour of trajectories/orbits
- Ergodicity describes the long term statistical behaviour of orbits
- Dynamical analysis via transfer operators captures the statistical behaviour of all orbits (rational + real) + termes de restes

Continued fractions and measure-theoeretic dynamical systems

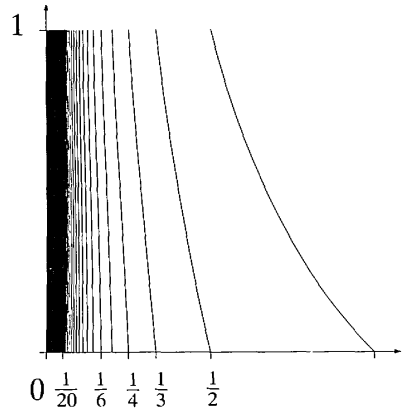
Consider the Gauss map

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

Continued fractions and measure-theoeretic dynamical systems

Consider the Gauss map

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



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

Continued fractions and measure-theoeretic dynamical systems

Consider the Gauss map

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

The Gauss measure is defined as

$$\mu(B) = \frac{1}{\log 2} \int_B \frac{1}{1+x} \mathrm{dx}$$

A measure is said to be T-invariant if
$\mu(B) = \mu(T^{-1}B), \forall B \in \mathcal{B}$

Theorem The Gauss measure is T invariant

Proof It suffices to work with intervals $[0, x)$

$$\mu([0,x)) = 1/2 \log(1+x) \qquad T^{-1}([0,x)) = \bigcup_{n=1}^{\infty} [\frac{1}{n+x}, \frac{1}{n})$$

Continued fractions and measure-theoeretic dynamical systems

Consider the Gauss map

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

Continued fractions and measure-theoeretic dynamical systems

Consider the Gauss map

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

The Gauss measure is defined as

$$\mu(B) = \frac{1}{\log 2} \int_B \frac{1}{1+x} \mathrm{dx}$$

Continued fractions and ergodicity

$$\mu(B) = \frac{1}{\log 2} \int_B \frac{1}{1+x} \mathrm{dx}, \ \mu(B) = \mu(T^{-1}B) \quad T\text{-invariance}$$

Continued fractions and ergodicity

$$\mu(B) = \frac{1}{\log 2} \int_B \frac{1}{1+x} \mathrm{dx}, \ \mu(B) = \mu(T^{-1}B) \quad T\text{-invariance}$$

Theorem The Gauss map is ergodic with respect to the Gauss measure

Definition of ergodicity $T^{-1}B = B \implies \mu(B) = 0$ or 1

Continued fractions and ergodicity

$$\mu(B) = \frac{1}{\log 2} \int_B \frac{1}{1+x} \mathrm{dx}, \ \mu(B) = \mu(T^{-1}B) \quad T\text{-invariance}$$

Theorem The Gauss map is ergodic with respect to the Gauss measure

Definition of ergodicity $T^{-1}B = B \implies \mu(B) = 0$ or 1

Ergodic theorem For a.e. x (=on a set of measure 1)

$$\frac{1}{n} \sum_{j=0}^{n-1} f(T^j x) = \int f d\mu, \ \forall f \in L_1(\mu)$$

Take $f = \mathbf{1}_B$ for some measurable set B

Time mean= Mean value along an orbit =
=mean value of f w.r.t. μ = Spatial mean

Measure-theoretic results

Sets of zero measure for the Gauss measure= sets of zero measure for the Lebesgue measure

Almost everywhere (a.e.) = on a set of measure 1

- 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 $a \geq 1$

$$\lim_{N \to \infty} \frac{1}{N} \{k \leq N;\ a_k = a\} = \frac{1}{\log 2} \log \frac{(a+1)^2}{a(a+2)}$$

- Gauss measure

$$\mu(A) = \frac{1}{\log 2} \int_A \frac{dx}{1+x}$$

Rational vs. irrational parameters

Euclid algorithm $\rightsquigarrow$ gcd $\rightsquigarrow$ rational parameters

Continued fractions $\rightsquigarrow$ irrational parameters

Is it relevant to compare generic orbits
and orbits for integer parameters ?

Rational vs. irrational parameters

- When computing a gcd, we work with integer/rational parameters
- This set has zero measure
- Ergodic methods produce results that hold only almost everywhere

Average-case analysis vs. a.e. results

Fact Orbits of rational points tend to behave like generic orbits

And their probabilistic bevaviour can be captured thanks to the methods of dynamical analysis of algorithms

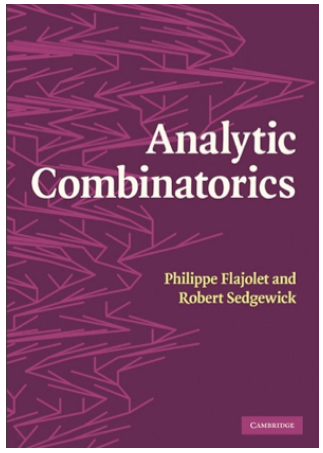
Dynamical analysis of algorithms [Vallée]

It belongs to the area of

- Analysis of algorithms [Knuth'63]

  probabilistic, combinatorial, and analytic methods

- Analytic combinatorics [Flajolet-Sedgewick]



generating functions and complex analysis,
analytic functions, analysis of the singularities

Dynamical analysis of algorithms [Vallée]

It mixes tools from

- dynamical systems (transfer operators, density transformers, Ruelle-Perron-Frobenius operators)
- analytic combinatorics (generating functions of Dirichlet type)

the singularities of (Dirichlet) generating functions
are expressed in terms of transfer operators

Average analysis of algorithms

Average analysis of algorithms

- [mean value] Computation of the asymptotic mean

$$\mathbb{E}_n[X] \underset{n\to\infty}{\sim} a_n$$

ex : what is the average bit complexity of the algorithm when the input size n is large ? Is it linear in n ? Quadratic in n ?. . .

Average analysis of algorithms

- [mean value] Computation of the asymptotic mean

$$\mathbb{E}_n[X] \underset{n\to\infty}{\sim} a_n$$

ex : what is the average bit complexity of the algorithm when the input size n is large ? Is it linear in n ? Quadratic in n ?. . .

- [variance] $\mathbb{V}_n[X] \underset{n\to\infty}{\sim} b_n$

ex : what is asymptotically the probability to be far from the mean value ?

Average analysis of algorithms

- [mean value] Computation of the asymptotic mean

$$\mathbb{E}_n[X] \underset{n\to\infty}{\sim} a_n$$

ex : what is the average bit complexity of the algorithm when the input size n is large ? Is it linear in n ? Quadratic in n ?. . .

- [variance] $\mathbb{V}_n[X] \underset{n\to\infty}{\sim} b_n$

ex : what is asymptotically the probability to be far from the mean value ?

- [limit law] What is the limit law of X

$$\mathbb{P}_n\left[\frac{X - a_n}{\sqrt{b_n}} \in [x, x + dx]\right] \underset{n\to\infty}{\sim} f(x)$$

ex : what is asymptotically the probability that X is in the interval $[a, b]$?

Number of steps in Euclid algorithm-Mean behaviour

Consider parameters (u, v) with $0 \leq u \leq v \leq N$

$$\text{Expectation of the number of steps} = \frac{\text{dimension}}{\text{entropy}} \times \log N$$

- Euclid algorithm

$$\frac{2}{\pi^2/(6\log 2)} \log N$$

[Heilbronn'69,Dixon'70,Hensley'94,Baladi-Vallée'03...]

Number of steps in Euclid algorithm-Mean behaviour

Consider parameters (u, v) with $0 \leq u \leq v \leq N$

$$\text{Expectation of the number of steps} = \frac{\text{dimension}}{\text{entropy}} \times \log N$$

- Euclid algorithm

$$\frac{2}{\pi^2/(6\log 2)} \log N$$

[Heilbronn'69,Dixon'70,Hensley'94,Baladi-Vallée'03...]

- Jacobi-Perron

[Fischer-Schweiger'75]

- Brun

[B.-Lhote-Steiner-Vallée, work in progress]

Number of steps in Euclid algorithm-Mean behaviour

Consider parameters (u, v) with $0 \leq u \leq v \leq N$

$$\text{Expectation of the number of steps} = \frac{\text{dimension}}{\text{entropy}} \times \log N$$

- Euclid algorithm

$$\frac{2}{\pi^2/(6 \log 2)} \log N$$

[Heilbronn'69,Dixon'70,Hensley'94,Baladi-Vallée'03...]

- Formal power series with coefficients in a finite field and ploynomials with degree less than m

$$\frac{2}{2\frac{q}{q-1}} m = \frac{q-1}{q} m$$

[Knopfmacher-Knopfmacher'88, Friesen-Hensley'96, Lhote-Vallée]

A substitution on words : the Fibonacci substitution

Definition A substitution σ is a morphism of the free monoid

Example

$$\sigma : 1 \mapsto 12,\ 2 \mapsto 1$$

$$\sigma^{\infty}(1) = 121121211211212\cdots$$

A substitution on words : the Fibonacci substitution

Definition A substitution σ is a morphism of the free monoid

Example

$$\sigma : 1 \mapsto 12,\ 2 \mapsto 1$$

1
12
121
12112
12112121

$$\sigma^{\infty}(1) = 1211212112112121\cdots$$

A substitution on words : the Fibonacci substitution

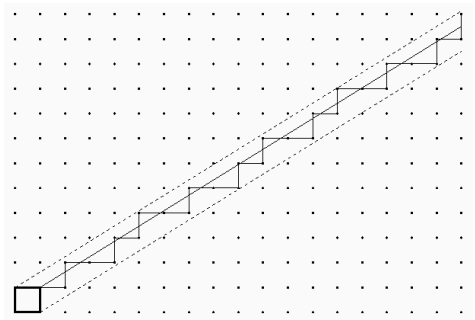
Definition A substitution σ is a morphism of the free monoid

Example

$$\sigma : 1 \mapsto 12,\ 2 \mapsto 1$$

$$\sigma^{\infty}(1) = 121121211211212\cdots$$

Ce mot infini est un codage de droite discrète

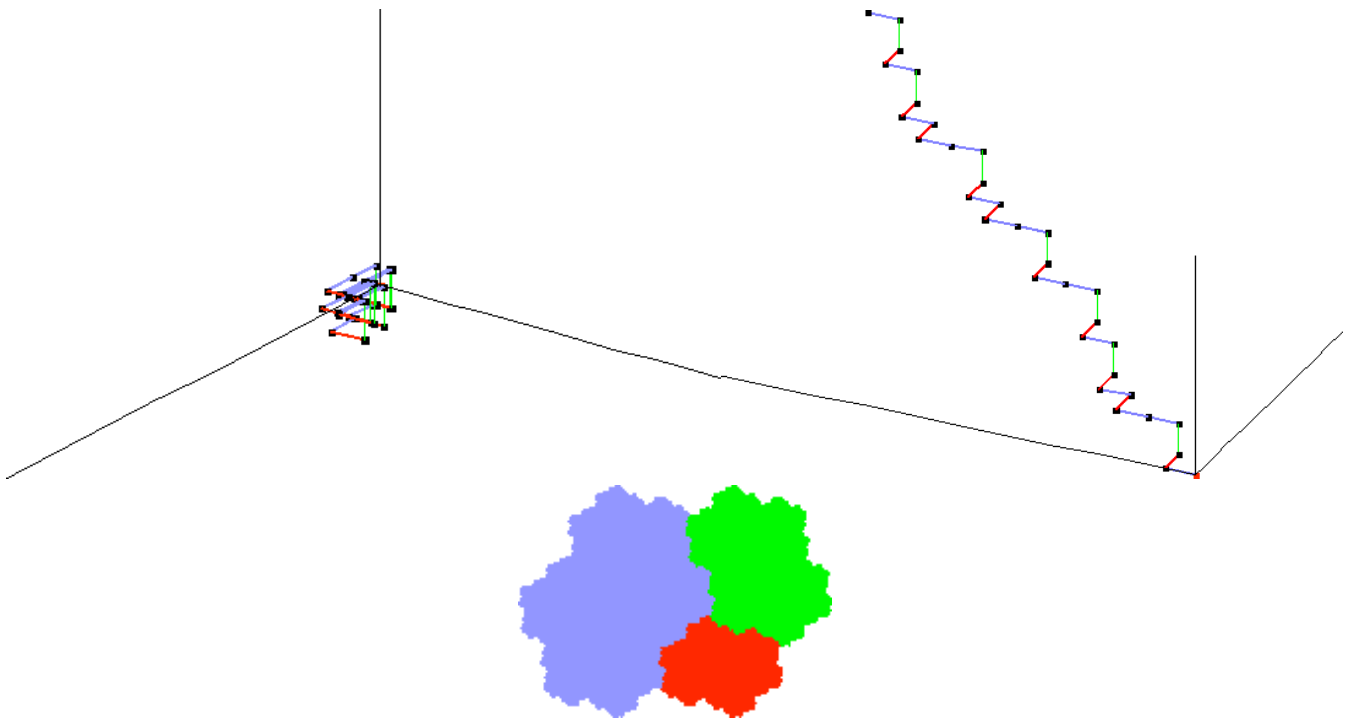


La substitution de Tribonacci [Rauzy'82]

$$\sigma : 1 \mapsto 12,\ 2 \mapsto 13,\ 3 \mapsto 1$$

$$\sigma^\infty(1) = 1213121121312121 3 \cdots$$

On représente $\sigma^\infty(1)$ comme une ligne brisée On remplace 1 par le vecteur $\vec{e}_1$ etc. On la projète selon les espaces propres de M_σ



Euclid algorithm and discrete segments

$$\begin{array}{rcl} 11 & = & 2 \cdot 4 + 3 \\ 4 & = & 1 \cdot 3 + 1 \\ 3 & = & 3 \cdot 1 + 0 \end{array}$$

$$\frac{4}{11} = \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3}}}$$

$$(11,4) \xleftarrow{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2} (3,4) \xleftarrow{\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}} (3,1) \xleftarrow{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^3} (0,1)$$

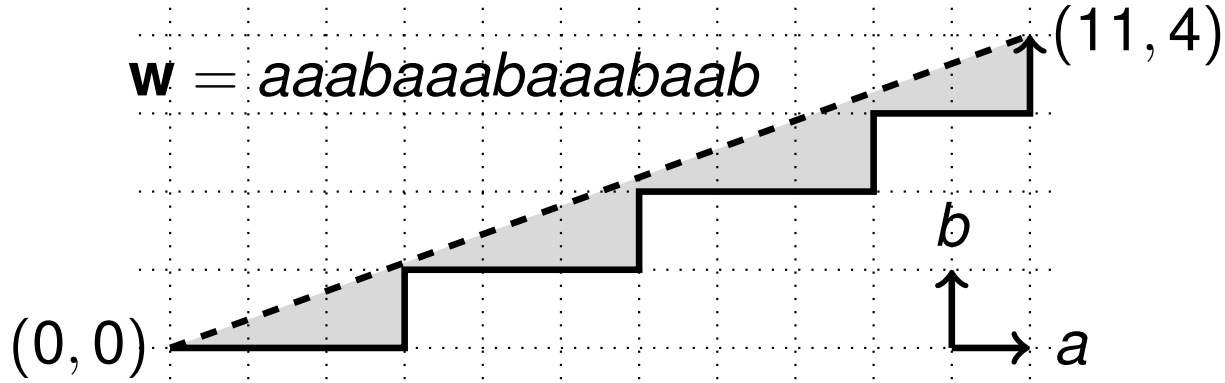
$$\begin{array}{ccccccc} a & \mapsto & a & \quad & a & \mapsto & ab & \quad & a & \mapsto & a \\ b & \mapsto & aab & & b & \mapsto & b & & b & \mapsto & aaab \end{array}$$

$$\mathbf{w} = \mathbf{w}_0 \longleftarrow \mathbf{w}_1 \longleftarrow \mathbf{w}_2 \longleftarrow \mathbf{w}_3 = b$$

Euclid algorithm and discrete segments

$$\begin{array}{rcl} 11 & = & 2 \cdot 4 + 3 \\ 4 & = & 1 \cdot 3 + 1 \\ 3 & = & 3 \cdot 1 + 0 \end{array}$$

$$\frac{4}{11} = \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3}}}$$



$$(11,4) \xleftarrow{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2} (3,4) \xleftarrow{\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}} (3,1) \xleftarrow{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^3} (0,1)$$

$$\begin{array}{ccccccc} a & \mapsto & a & a & \mapsto & ab & a & \mapsto & a \\ b & \mapsto & aab & b & \mapsto & b & b & \mapsto & aaab \end{array}$$

$$\mathbf{w} = \mathbf{w}_0 \xleftarrow{} \mathbf{w}_1 \xleftarrow{} \mathbf{w}_2 \xleftarrow{} \mathbf{w}_3 = b$$

Our strategy

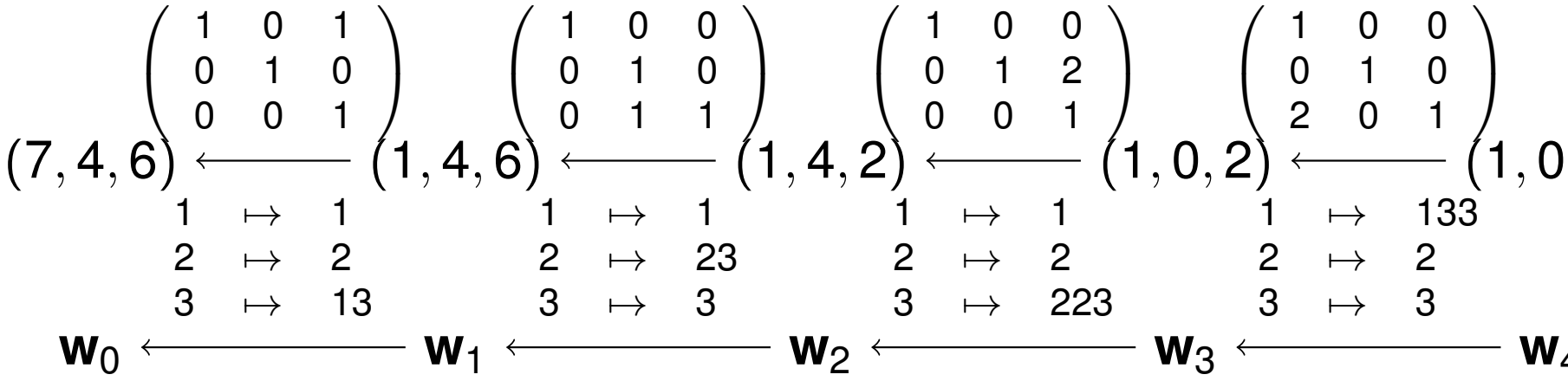
- We apply a multidimensional continued fraction algorithm to the line in $\mathbb{R}^3$ directed by a given vector $\mathbf{u} = (u_1, u_2, u_3)$
- We then associate with the matrices produced by the algorithm substitutions, with these substitutions having the matrices produced by the continued fraction algorithm as incidence matrices

$$\mathbf{u} = \mathbf{u}_0 \xleftarrow{M_1} \mathbf{u}_1 \xleftarrow{M_2} \mathbf{u}_2 \xleftarrow{M_3} \cdots \xleftarrow{M_k} \mathbf{u}_k$$

$$w = w_0 \xleftarrow{\sigma_1} w_1 \xleftarrow{\sigma_2} w_2 \xleftarrow{\sigma_3} \cdots \xleftarrow{\sigma_k} w_k \in \{1, 2, 3\}$$

$$\mathbf{u} = M_1 \cdots M_k \mathbf{u}_k$$

Applying Brun algorithm on $(7, 4, 6)$



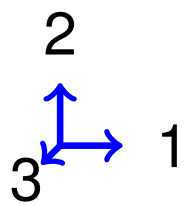
Applying Brun algorithm on $(7, 4, 6)$

$$(7,4,6) \xleftarrow{\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}} (1,4,6) \xleftarrow{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}} (1,4,2) \xleftarrow{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}} (1,0,2) \xleftarrow{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}} (1,0$$

$$\begin{array}{ccccccccc} 1 & \mapsto & 1 & & 1 & \mapsto & 1 & & 1 & \mapsto & 1 & & 1 & \mapsto & 133 \\ 2 & \mapsto & 2 & & 2 & \mapsto & 23 & & 2 & \mapsto & 2 & & 2 & \mapsto & 2 \\ 3 & \mapsto & 13 & & 3 & \mapsto & 3 & & 3 & \mapsto & 223 & & 3 & \mapsto & 3 \end{array}$$

$$\mathbf{w}_0 \xleftarrow{} \mathbf{w}_1 \xleftarrow{} \mathbf{w}_2 \xleftarrow{} \mathbf{w}_3 \xleftarrow{} \mathbf{w}_4$$

$$\mathbf{w} = \mathbf{w}_0 = 12132131321321313$$



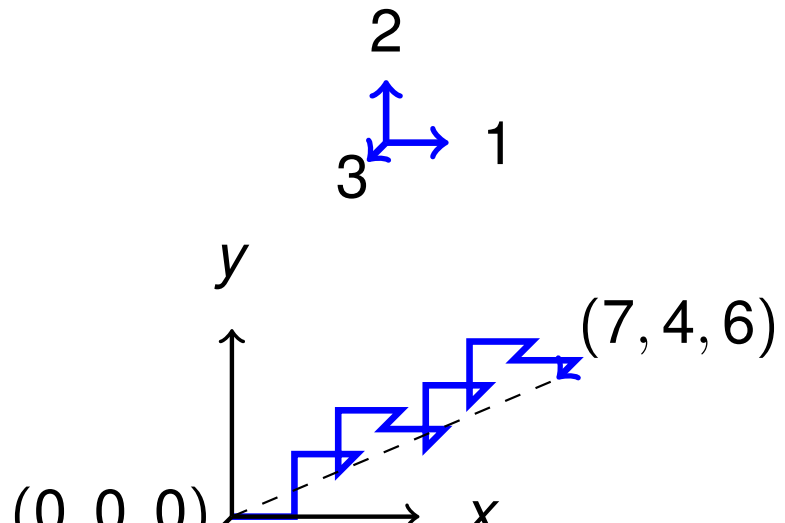
Applying Brun algorithm on $(7, 4, 6)$

$$(7,4,6) \xleftarrow{\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}} (1,4,6) \xleftarrow{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}} (1,4,2) \xleftarrow{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}} (1,0,2) \xleftarrow{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}} (1,0$$

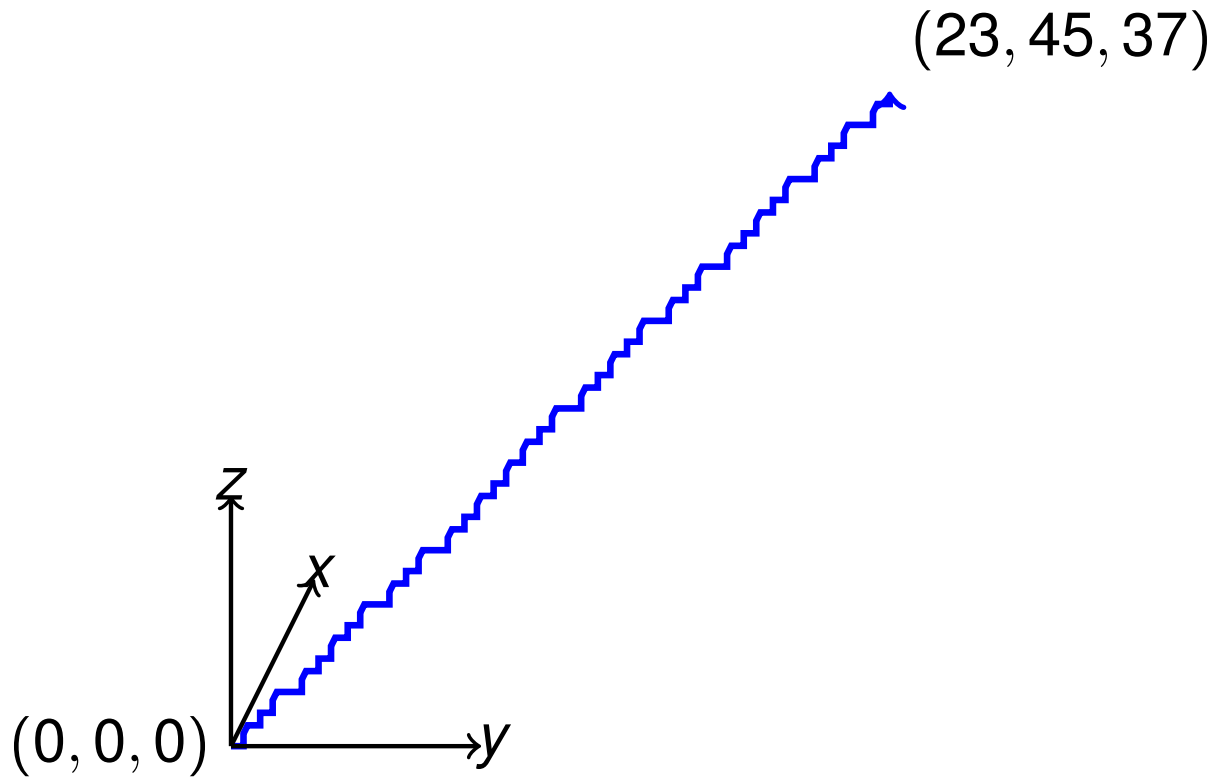
$$\begin{array}{ccccccccc} 1 & \mapsto & 1 & & 1 & \mapsto & 1 & & 1 & \mapsto & 1 & & 1 & \mapsto & 133 \\ 2 & \mapsto & 2 & & 2 & \mapsto & 23 & & 2 & \mapsto & 2 & & 2 & \mapsto & 2 \\ 3 & \mapsto & 13 & & 3 & \mapsto & 3 & & 3 & \mapsto & 223 & & 3 & \mapsto & 3 \end{array}$$

$$\mathbf{w}_0 \xleftarrow{} \mathbf{w}_1 \xleftarrow{} \mathbf{w}_2 \xleftarrow{} \mathbf{w}_3 \xleftarrow{} \mathbf{w}_4$$

$$\mathbf{w} = \mathbf{w}_0 = 12132131321321313$$



Applying Brun algorithm on $(23, 45, 37)$



S-adic expansions

Definition An infinite word ω is said *S*-adic if there exist

- a finite set of substitutions $\mathcal{S}$
- an infinite sequence of substitutions $(\sigma_n)_{n\geq 1}$ with values in $\mathcal{S}$

such that

$$\omega = \lim_{n\to+\infty} \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_n(0)$$

The terminology comes from Veech adic transformations

Context

- Fusion and hierarchical tilings

  [N. Priebe Frank, L. Sadun, Fusion : a general framework for hierarchical tilings of $\mathbb{R}^d$]

- Adic transformation

  [S. Ferenczi, A. Fisher, and M. Talet, Minimality and unique ergodicity for adic transformations]

- Arithmetic dynamics

  [N. Sidorov-A. Vershik] arithmetic codings of dynamical systems that preserve their arithmetic structure

- Numeration dynamics [Keane]

S-adic expansions

$$u = \lim_{n \to +\infty} \sigma_1 \sigma_2 \cdots \sigma_n(0)$$

Algebraically Generalized Perron–Frobenius eigendirection

One considers infinite products of matrices with entries in $\mathbb{N}$

$$M_1 \cdots M_n \cdots$$

The M_i are the incidence matrices of the substitutions

Does there exist a vector $\mathbf{u}$ such that

$$\bigcap_k M_1 \cdots M_k \left(\mathbb{R}_+^d\right) = \mathbb{R}_+ \mathbf{u} \quad ?$$

$\mathbf{u}$ is the vector of letter frequencies associated with the infinite word u

S-adic expansions

$$u = \lim_{n \to +\infty} \sigma_1 \sigma_2 \cdots \sigma_n(0)$$

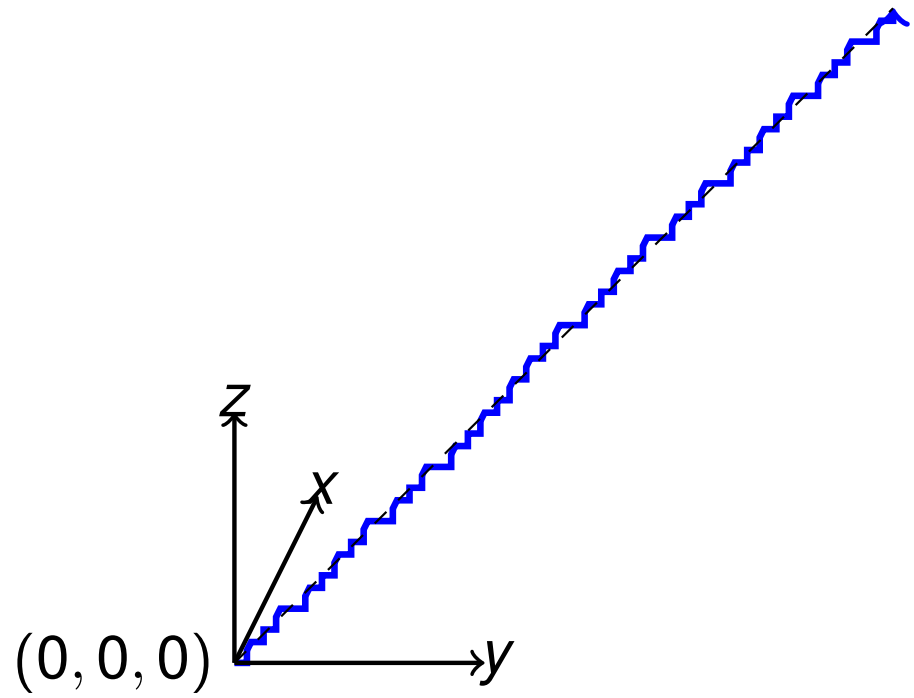
Arithmetically Weak and strong convergence of multidimensional continued fraction algorithms

Theorem There exists $\delta > 0$ s.t. for almost every (α, β), there exists $n_0 = n_0(\alpha, \beta)$ s.t. for all $n \geq n_0$

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

where p_n, q_n, r_n are produced by Brun or by Jacobi-Perron algorithm Second Lyapunov exponent < 0

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

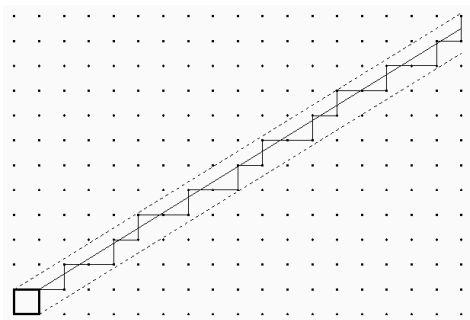

z
x
(0, 0, 0)
y

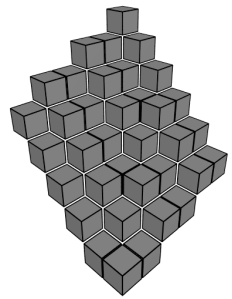
Multidimensional continued fractions

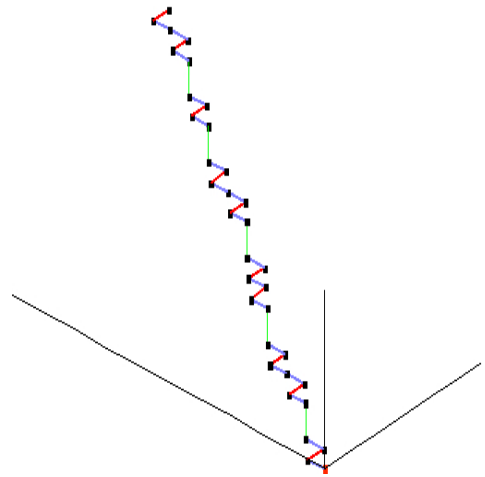
If we start with two parameters (α, β), one looks for two rational sequences (p_n/q_n) et (r_n/q_n) with the same denominator that satisfy

$$\lim p_n/q_n = \alpha, \lim r_n/q_n = \beta.$$

Geometrically







Arithmetically and dynamically

translation on the torus : $R_{\alpha,\beta} : \mathbb{T}^2 \to \mathbb{T}^2,\ (x, y) \mapsto x+(\alpha, \beta)$

action of $\mathbb{Z}^2$ on $\mathbb{T}$: $(m, n).(x, y) = m\alpha + n\beta$

Continued fractions

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

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

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

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

- Best approximation property

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

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

Every best approximation of α is a convergent

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

- $SL(2,\mathbb{N})$ 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 but we then loose unimodularity, and the sequence of best approximations heavily depends on the chosen norm [Lagarias]
- Klein polyhedra and sails [Arnold]
- unimodular multidimensional Euclid's algorithms
    - Lattice reduction (LLL) [Lagarias,Ferguson-Forcade,Just,Havas-Majewski-Matthews,Grabiner-Lagarias etc.]

Multidimensional continued fractions

There is no canonical generalization of continued fractions to higher dimensions

Several approaches are possible

- best simultaneous approximations but we then loose unimodularity, and the sequence of best approximations heavily depends on the chosen norm [Lagarias]
- Klein polyhedra and sails [Arnold]
- unimodular multidimensional Euclid's algorithms
  - Lattice reduction (LLL) [Lagarias,Ferguson-Forcade,Just,Havas-Majewski-Matthews,Grabiner-Lagarias etc.]
  - continued fractions based on the iteration of piecewise fractional linear maps
    Jacobi-Perron, Brun, Selmer, Poincaré etc. [Brentjes, Schweiger]

What is expected ?

We are given $(\alpha_1, \cdots, \alpha_d)$ which produces a sequence of basis $(B^{(k)})$ of $\mathbb{Z}^{d+1}$ and/or a sequence of approximations $(p_1^{(k)}), \cdots, p_d^{(k)}, q^{(k)})$

What is expected ?

We are given $(\alpha_1, \cdots, \alpha_d)$ which produces a sequence of basis $(B^{(k)})$ of $\mathbb{Z}^{d+1}$ and/or a sequence of approximations $(p_1^{(k)}), \cdots, p_d^{(k)}, q^{(k)})$

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

$$\max_i \text{dist}(b_i^{(k)}, (\alpha, 1)\mathbb{R}) \to_k 0$$

- and 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

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

What is expected ?

We are given $(\alpha_1, \cdots, \alpha_d)$ which produces a sequence of basis $(B^{(k)})$ of $\mathbb{Z}^{d+1}$ and/or a sequence of approximations $(p_1^{(k)}), \cdots, p_d^{(k)}, q^{(k)})$

Dynamics We also want...

- reasonable ergodic properties (ergodic invariant measure, natural extension)
- to be able to control the number of executions, the “depth” if the parameters are rational etc.
- to be able to perform a dynamical analysis à la Brigitte

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

How does LLL produce good approximations ?

LLL produces in polynomial time a vector $(b_1, \dots b_{d+1})$ such that

$$\forall j,\ |b_1^j| \leq ||b_1||_2 \leq 2^{d/4} det(M_t)^{1/d+1} = 2^{d/4} t^{1/d+1}$$

But

$$b_1 = p_1 e_1 + p_2 e_2 + \cdots + p_d e_d + q(-\alpha_1 e_1 \cdots - \alpha_d e_d + t e_{d+1})$$

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

One deduces that

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

and

$$qt \leq 2^{d/4} t^{1/d+1}$$

We deduce that for all i

$$|p_i - \alpha_i q| \leq 2^{(d+1)/4} 1/q^{1/d}$$

How does LLL produce good approximations ?

Towards continued fractions ? One has a priori to recompute everything from the beginning when one changes t

How to understand algorithms based on lattice reduction in dynamical terms ? [LLL and sandpile models, LAREDA]

For a dynamical version, see [Kraaikamp-Smeets]. For a study in the 3d case, see [Beukers]

Why working with cf algorithms ?

- They are not the best ones in terms of Diophantine approximation compared to algorithms based on lattice reduction
- They are not the fastest ones experimentally for gcd computation

There exist subquadractic gcd algorithms
[GMP= Möller'08]

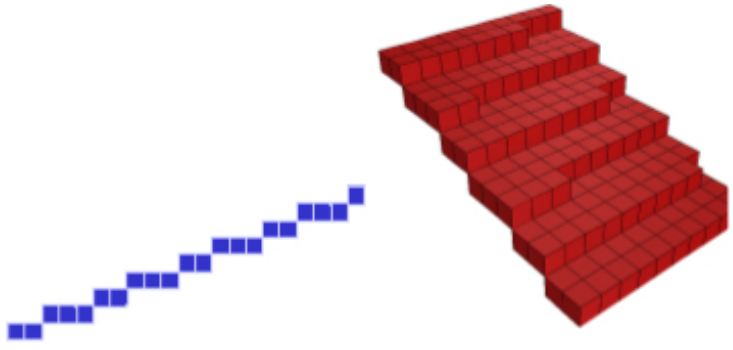
Why working with cf algorithms ?

But

- They can be described by a simple dynamical system

  $\rightsquigarrow$ dynamical analysis of multidimensional gcd algorithms

- They thus can be easily applied, for instance, in discrete geometry



Multidimensional Euclid's algorithms

- Jacobi-Perron We subtract the first one to the two other ones with $0 \leq u_1, u_2 \leq u_3$

$$(u_1, u_2, u_3) \mapsto (u_2 - [\frac{u_2}{u_1}]u_1, u_3 - [\frac{u_3}{u_1}]u_1, u_1)$$

- Brun We subtract the second largest entry and we reorder. If $u_1 \leq u_2 \leq u_3$

$$(u_1, u_2, u_3) \mapsto (u_1, u_2, u_3 - u_2)$$

- Poincaré We subtract the previous entry and we reorder

$$(u_1, u_2, u_3) \mapsto (u_1, u_2 - u_1, u_3 - u_2)$$

- Selmer We subtract the smallest to the largest and we reorder

$$(u_1, u_2, u_3) \mapsto (u_1, u_2, u_3 - u_1)$$

- Fully subtractive We subtract the smallest one to the other ones and we reorder

$$(u_1, u_2, u_3) \mapsto (u_1, u_2 - u_1, u_3 - u_1)$$