Multidimensional continued fractions and numeration

V. Berthé

LIRMM-CNRS- Univ. Montpellier II-France
berthe@lirmm.fr
http://www.lirmm.fr/~berthe

Journées numération, Prague, 2008

Ostrowski numeration system

Ostrowski numeration system is based on the numeration scale given by the sequence of denominators in the continued fraction expansion of a given real number.

The Ostrowski representation of the nonnegative integers is a generalisation of the Zeckendorf representation:

$$N = \sum_n b_n F_n, \text{ with } b_n \in \{0, 1\}, \; b_n b_{n+1} = 0.$$

One can expand via Ostrowki numeration

- integers
- real numbers in $[0, 1]$

Ostrowski expansion of integers

Let $\alpha \in (0,1)$ be an irrational number.

Let $\alpha = [0; a_1, a_2, \ldots, a_n, \ldots]$ be its continued fraction expansion with convergents $p_n/q_n = [0; a_1, a_2, \ldots, a_n]$.

Every integer N can be expanded uniquely in the form

$$N = \sum_{k=1}^{m} b_k q_{k-1},$$

where

$$\begin{cases} 0 \leq b_1 \leq a_1 - 1 \\ 0 \leq b_k \leq a_k \text{ for } k \geq 2 \\ b_k = 0 \text{ if } b_{k+1} = a_{k+1} \end{cases}$$

Ostrowski expansion of real numbers

Ostrowski's representation of integers can be extended to real numbers.

The base is given by the sequence $(\theta_n)_{n\geq 0}$, where $\theta_n = (q_n\alpha - p_n)$.

Every real number $-\alpha \leq \beta < 1-\alpha$ can be expanded uniquely in the form

$$\beta = \sum_{k=1}^{+\infty} c_k \theta_{k-1},$$

where

$$\begin{cases} 0 \leq c_1 \leq a_1 - 1 \\ 0 \leq c_k \leq a_k \text{ for } k \geq 2 \\ c_k = 0 \text{ if } c_{k+1} = a_{k+1} \\ c_k \neq a_k \text{ for infinitely many odd integers.} \end{cases}$$

Applications

This numeration system can be used to approximate β modulo 1 by numbers of the form $N\alpha$, with $N \in \mathbb{N}$.

Indeed the sequence of integers $N_n = \sum_{k=1}^{n} c_k q_{k-1}$ can be used to provide a series of best approximations to

$$\beta = \sum_{k=1}^{+\infty} c_k \theta_{k-1}, \text{ with } \theta_k = q_k \alpha - p_k.$$

Indeed, take

$$N_n \alpha = \sum_{k=1}^{n} c_k q_{k-1} \alpha \equiv \sum_{k=1}^{n} c_k (q_{k-1}\alpha - p_{k-1}) \bmod 1.$$

Applications

This numeration system can be used to approximate β modulo 1 by numbers of the form $N\alpha$, with $N \in \mathbb{N}$.

Indeed the sequence of integers $N_n = \sum_{k=1}^{n} c_k q_{k-1}$ can be used to provide a series of best approximations to

$$\beta = \sum_{k=1}^{+\infty} c_k \theta_{k-1}, \text{ with } \theta_k = q_k\alpha - p_k.$$

Indeed, take

$$N_n\alpha = \sum_{k=1}^{n} c_k q_{k-1}\alpha \equiv \sum_{k=1}^{n} c_k (q_{k-1}\alpha - p_{k-1}) \bmod 1.$$

This yields applications in

- word combinatorics for the study of Sturmian words
- Diophantine approximation/equidistribution theory
- discrete geometry: discrete lines
- cryptography via double base numerations

$$N = \sum_i 2^{a_i} 3^{b_i}$$

with $a_i, b_i \geq 0$ and $(a_i, b_i) \neq (a_j, b_j)$ if $i \neq j$.

Double base numerations

Question

How to expand an integer N as

$$N = \sum_{i,j \in \mathbb{N}} a_{i,j} 2^i 3^j, \text{ with } a_{i,j} \in \{0,1\} \text{ for all } i,j$$

such that the digit sum $\sum a_{i,j}$ is unique?

Double base numerations

Question

How to expand an integer N as

$$N = \sum_{i,j \in \mathbb{N}} a_{i,j} 2^i 3^j, \text{ with } a_{i,j} \in \{0,1\} \text{ for all } i,j$$

such that the digit sum $\sum a_{i,j}$ is unique?

Motivation

- Cryptography: scalar multiplication on elliptic curves on $\mathbb{F}_p$ et $\mathbb{F}_{2^n}$, Koblitz curves, supersingular curves in char. 3; modular exponentiation [Dimitrov-Jullien-Miller][Ciet-Sica][Dimitrov-Imbert-Mishra] [Avanzi-Ciet-Sica][Avanzi-Dimitrov-Doche-Sica]...
- Signal processing.

Question

Define a greedy algorithm for expanding an integer N as

$$N = \sum_{i,j \in \mathbb{N}} a_{i,j} 2^i 3^j, \text{ with } a_{i,j} \in \{0,1\} \text{ for all } i,j.$$

Complexity

Representing N in base 2 requires $0(\log(N))$ digits.

Theorem [Dimitrov-Jullien-Miller]

Every nonnegative integer N can be represented as a sum of at most $\mathcal{O}(\frac{\log N}{\log \log N})$ numbers of the form $2^a 3^b$.

Theorem [Tijdeman]

There exists $c > 0$ such that for all $N \in \mathbb{N}$ there exists an integer of the form $2^a 3^b$ such that

$$N - \frac{N}{(\log N)^c} < 2^a 3^b < N.$$

Greedy algorithm

Question

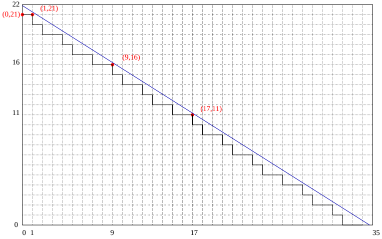
Given a nonnegative integer N, how to find the largest integer of the form 2^a3^b that satisfies $2^a3^b \leq N$, for $a, b \in \mathbb{N}$?

We are looking for a, b such that

$$2^a3^b \leq N$$

$$a \log 2 + b \log 3 \leq \log N$$

$\rightsquigarrow$ Arithmetic discrete line /nonhomogeneous approximation.



A nonhomogeneous problem

We are looking for a, b such that

$$2^a 3^b \leq N$$

$$a \log 2 + b \log 3 \leq \log N$$

We set

$$\alpha := \log_3 2, \quad \beta := \{\log_3 N\}.$$

One has $0 < \alpha < 1$, $\alpha \notin \mathbb{Q}$, $0 \leq \beta < 1$. We are looking for a, b in $\mathbb{N}$ such that

1. $2^a 3^b \leq N$
2. $-(a\alpha + b) + \beta + [\log_3 N]$ as small as possible.

$\rightsquigarrow$ Approximation by β points of the form $a\alpha$ modulo 1.

Some open questions

- Base 2^a3^b: Determination of a reasonable constant in $0(\frac{\log N}{\log\log N})$ for the number of nonzero digits in the greedy algorithm. Minimal expansions?
- Base $2^a3^b5^c$: Same questions. Tjideman's theorem still holds. Greedy algorithm?
- Complex double bases: Expansions in base $\tau^a\mu^b$ where τ and μ are two complex quadratic numbers. Same questions. Application to Koblitz curves:

$$\tau = \frac{\pm 1 + i\sqrt{7}}{2}, \quad \mu = \tau - 1.$$

Toward a multdimensional Ostrowski numeration

Question

How to define an Ostrowski expansion in higher dimension?

Motivations come from

- word combinatorics for the study of 2D Sturmian words
- Diophantine approximation/equidistribution theory
- discrete geometry: discrete planes
- Rauzy fractals
- cryptography via triple base numerations

$$N = \sum_i 2^{a_i} 3^{b_i} 5^{c_i}$$

with $a_i, b_i, c_i \geq 0$ and $(a_i, b_i, c_i) \neq (a_j, b_j, c_j)$ if $i \neq j$ (Hamming numbers).

First problems I

There is no canonical generalization of Ostrowski numeration to higher dimensions.

This is first due to the fact that there is no canonical notion of a generalization of Euclid's algorithm.

To remedy to the lack of a satisfactory tool replacing continued fractions, several approaches are possible:

- best simultaneous approximations but we then loose unimodularity, and the sequence of best approximations heavily depends on the chosen norm
- unimodular multidimensional continued fraction algorithms
  - Jacobi-Perron algorithm
  - Brun algorithm
  - Arnoux-Rauzy algorithm, Fine and Wilf algorithm [Tijdeman-Zamboni]
- Lattice reduction approaches (LLL). Ex: computation of the n-th Hamming number (see E. Dijkstra, and see M. Quersia's web page.)

First problems II

We want to define a generalized Ostrowski numeration system based on some classical unimodular multidimensional continued fraction algorithms.

Let us consider a multidimensional continued fraction algorithm producing simultaneous approximations with the same denominator

$$(\alpha, \beta) \rightsquigarrow (p_n/q_n, r_n/q_n)$$

We thus get two kinds of possible expansions

- Simultaneous approximation in $\mathbb{T}^2$

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \sum c_n \begin{pmatrix} p_n\alpha - q_n \\ r_n\alpha - q_n \end{pmatrix}$$

- Minimization of linear form in $\mathbb{T}^1$

$$x = \sum c_n(q'_n\alpha + q''_n\beta + p'_n)$$

How to define the coefficients? How to find a suitable linear form?

Back to Ostrowski numeration

- A numeration scale and a numeration defined on $\mathbb{N}$
- An odometer Od acting on the set of sequences K_α [Grabner, Liardet, Tichy]
- An isomorphism theorem

$$\begin{array}{ccc} \mathbb{R}/\mathbb{Z} & \xrightarrow{R_\alpha} & \mathbb{R}/\mathbb{Z} \\ \text{Ostr.}\downarrow & & \downarrow\text{Ostr.} \\ K_\alpha & \xrightarrow[\text{Od}]{} & K_\alpha \end{array}$$

- A numeration system for real numbers
- A skew product of the Gauss map

$$T(\alpha, \beta) = (\{1/\alpha\}, \{\beta/\alpha\}).$$

- An induction process (first return map) and associated substitutions
- An S-adic generation process for Sturmian sequences
- A natural extension and a Lagrange theorem

Ostrowski odometer

Let $\alpha = [0; a_1 + 1, a_2, \dots]$ and set

$$K_\alpha = \{(c_k)_{k\geq 1} |\ \forall k \geq 1\ (c_k \in \mathbb{N},\ 0 \leq c_k \leq a_k) \text{ and } (c_{k+1} = a_{k+1} \Rightarrow c_k = 0)\}.$$

One defines on the compact set K_α an odometer map Od. The map Od : $K_\alpha \to K_\alpha$ is onto and continuous, and $(K_\alpha,\ \mathrm{Od})$ is minimal.

Isomorphism theorem

The dynamical systems (K_α, Od) and $(\mathbb{R}/\mathbb{Z}, R_\alpha)$ are topologically conjugate, with $R_\alpha : \mathbb{R}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z},\ x \mapsto x + \alpha$.

Sturmian words and Ostrowski numeration

Let ω be a Sturmian sequence that codes the orbit of x. Let τ_0 and τ_1 be the morphisms on $\{0,1\}^*$ defined by $\tau_0(0) = 0$, $\tau_1(0) = 10$, $\tau_0(1) = 01$, $\tau_1(1) = 1$. Let τ_i' for $i \in \{0,1\}$ defined by $\tau_i'(i) = i$ and $\tau_i'(j) = ji$, for $j \neq i$. We have

$$\omega = \lim_{k \to +\infty} \tau_0^{a_1 - c_1} \circ (\tau_0')^{c_1} \circ \tau_1^{a_2 - c_2} \circ (\tau_1')^{c_2} \circ \cdots \circ \tau_{k-1}^{a_k - c_k} \circ (\tau_{k-1}')^{c_k}(1),$$

where $(a_k)_{k\geq 1}$ is the sequence of partial quotients of the slope (defined as the density of the symbol 1), while $(c_k)_{k\geq 1}$ is the sequence of digits in the arithmetic Ostrowski expansion of x.

Theorem [Ito-Nakada]

Let

$$x = \sum_{k=1}^{\infty} c_{k+1}(q_k\alpha - p_k),$$

where $(c_k)_{k\geq 1}$ is the sequence of digits in the arithmetic Ostrowski expansion of x. Suppose α is quadratic. Then $(c_k)_{k\geq 1}$ is eventually periodic if and only if $x \in \mathbb{Q}(\alpha)$.

Corollary [B., Holton, Zamboni]

A Sturmian sequence ω of slope α which codes the orbit of x is primitive substitutive if and only if α is a quadratic irrational and $x \in \mathbb{Q}(\alpha)$.

Ostrowski generalizations

- A numeration scale and a numeration defined on $\mathbb{N}$
- An odometer Od on K
- An isomorphism theorem between (K, Od) and a dynamical system (X, T)
- A numeration system for real numbers
- A skew product of the Gauss map
- An induction process (first return map) and associated substitutions
- An S-adic generation process for sequences coding the dynamical system T.
- A natural extension

Ostrowski generalizations

- A numeration scale and a numeration defined on $\mathbb{N}$
- An odometer Od on K
- An isomorphism theorem between (K, Od) and a dynamical system (X, T)
- A numeration system for real numbers
- A skew product of the Gauss map
- An induction process (first return map) and associated substitutions
- An S-adic generation process for sequences coding the dynamical system T.
- A natural extension

This program has been realized for instance for

- 3 interval exchange transformations/induction [Ito et al.]
- Pisot irreducible substitutions

Pisot substitution

Let σ be an irreducible Pisot substitution over a d-letter alphabet with super coincidence. We have

- A numeration scale and a numeration defined on $\mathbb{N}$: Dumont-Thomas substitution
- An odometer Od on K
- An isomorphism theorem between (K, Od) and a toral translation $(\mathbb{T}^{d-1}, T)$ whose fundamental domain is given by a Rauzy fractal.
- A numeration system for real numbers: Dumont-Thomas
- A fibered system (Schweiger)
- Induction and substitution

NonPisot case: [Arnoux-Furukadi-Harriss-Ito]

Nonalgebraic parameters

Let $(\alpha, \beta) \in (0,1)^2$.
Consider for instance Brun algorithm. We are looking for

- A numeration scale and a numeration defined on $\mathbb{N}$ OK
- An odometer Od on K OK
- An isomorphism theorem between (K, Od) and a toral translation $(\mathbb{T}^{d-1}, T)$ of parameters (α, β) with fundamental domain given by an S-adic Rauzy fractal Problem!
- A numeration system for real numbers OK
- A skew product of Brun algoritm OK
- An induction process and generalized substitutions [Arnoux-B.-Ito] OK
- An S-adic generation process OK

Application to the generation and recognition of arithmetic discrete planes [B.-Fernique]

Strategy I: skew product

We consider the following classical skew product of the Gauss map

$$T\colon (\alpha,\beta) \mapsto (\{1/\alpha\},\{\beta/\alpha\}) = (1/\alpha - a_1, \beta/\alpha - b_1) = (\alpha_1,\beta_1).$$

We have

$$\beta_1 = \beta/\alpha - b_1 \text{ and thus } \beta = b_1\alpha + \alpha\beta_1.$$

We deduce that

$$\beta = \sum_{k=1}^{+\infty} b_k \alpha\alpha_1 \cdots \alpha_{k-1} = \sum_{k=1}^{+\infty} b_k |q_{k-1}\alpha - p_{k-1}|.$$

Strategy I: skew product

We consider the following classical skew product of the Gauss map

$$T\colon (\alpha,\beta)\mapsto (\{1/\alpha\},\{\beta/\alpha\}) = (1/\alpha - a_1, \beta/\alpha - b_1) = (\alpha_1,\beta_1).$$

We have

$$\beta_1 = \beta/\alpha - b_1 \text{ and thus } \beta = b_1\alpha + \alpha\beta_1.$$

We deduce that

$$\beta = \sum_{k=1}^{+\infty} b_k \alpha\alpha_1\cdots\alpha_{k-1} = \sum_{k=1}^{+\infty} b_k |q_{k-1}\alpha - p_{k-1}|.$$

Indeed we use the fact that

$$\begin{pmatrix} 1 \\ \alpha_n \end{pmatrix} = \frac{1}{\alpha\cdots\alpha_{n-1}} \mathbf{M}_{a_n}^{-1}\cdots\mathbf{M}_{a_1}^{-1}\begin{pmatrix} 1 \\ \alpha \end{pmatrix} \text{ where } \mathbf{M}_a^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -a \end{pmatrix}.$$

We deduce that

$$\alpha\cdots\alpha_{n-1} = \text{ first coordinate of } (\mathbf{M}_{a_1}\cdots\mathbf{M}_{a_n})^{-1}\begin{pmatrix} 1 \\ \alpha \end{pmatrix} = \langle \mathbf{l}_1^{(n)}, (1,\alpha)\rangle.$$

We conclude by noticing

$$\mathbf{M}_a = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \mathbf{M}_{a_1}\cdots\mathbf{M}_{a_n} = \begin{pmatrix} q_n & q_{n-1} \\ p_n & p_{n-1} \end{pmatrix}$$

Strategy I: skew product

We consider the following classical skew product of the Gauss map

$$T\colon (\alpha,\beta) \mapsto (\{1/\alpha\},\{\beta/\alpha\}) = (1/\alpha - a_1, \beta/\alpha - b_1) = (\alpha_1,\beta_1).$$

We have

$$\beta_1 = \beta/\alpha - b_1 \text{ and thus } \beta = b_1\alpha + \alpha\beta_1.$$

We deduce that

$$\beta = \sum_{k=1}^{+\infty} b_k \alpha\alpha_1 \cdots \alpha_{k-1} = \sum_{k=1}^{+\infty} b_k |q_{k-1}\alpha - p_{k-1}|.$$

We then consider the following skew product of the Brun map

$$T(\alpha,\beta,\gamma) = \begin{cases} (\beta/\alpha, 1/\alpha - a_1, \gamma/\alpha - b_1) & \text{if } \beta < \alpha \\ (1/\beta - a_1, \alpha/\beta, \gamma/\beta - b_1) & \text{if } \beta > \alpha \end{cases}$$

or of the Jacobi-Perron map

$$T(\alpha,\beta,\gamma) = (\{\beta/\alpha\},\{1/\alpha\},\{\gamma/\alpha\}).$$

We get

$$\beta = \sum_{k=1}^{+\infty} b_k \langle \mathbf{l}_1^{(k)}, (1,\alpha,\beta)\rangle.$$

Second strategy: generalized substitutions

We consider the following skew product of the Brun map

$$T(\alpha,\beta,\gamma) = \begin{cases} (\beta/\alpha, 1/\alpha - a_1, \gamma/\alpha - b_1) & \text{if } \beta < \alpha \\ (1/\beta - a_1, \alpha/\beta, \gamma/\beta - b_1) & \text{if } \beta > \alpha \end{cases}$$

By applying a so-called generalized substitution, one gets

$$\mathbf{x_1} = T(\mathbf{x}) = \mathbf{M}_{a_1,\varepsilon_1}^{-1}\mathbf{x} - b_1\mathbf{v}_{\varepsilon_1}.$$

One recovers expansions of the form

$$\mathbf{x} = b_1\mathbf{M}_{a_1,\varepsilon_1}\mathbf{v}_{\varepsilon_1} + \mathbf{M}_{a_1,\varepsilon_1}\mathbf{x_1} = \sum b_k\mathbf{M}_{a_1,\varepsilon_1}\cdots\mathbf{M}_{a_k,\varepsilon_k}\mathbf{v}_{\varepsilon_k}$$

$$\mathbf{x} = \sum b_k \begin{pmatrix} p_k\alpha - q_k \\ r_k\alpha - q_k \end{pmatrix}.$$

Système fibré [Schweiger]

Un système fibré est la donnée d'un ensemble X et d'une transformation $T\colon X \to X$ pour laquelle il existe un ensemble I fini ou dénombrable, et une partition $X = \biguplus_{i\in I} X_i$ de X telle que la restriction T_i de T sur X_i est injective, pour tout $i \in I$.

Cela permet de définir une application $\varepsilon\colon X \to I$ qui associe l'index i à $x \in X$ tel que $x \in X_i$ et qui est bien définie.

Représentation q-adique

Soit $X = \mathbb{N}$, $I = \{0, 1, \ldots, q-1\}$, $X_i = i + q\mathbb{N}$. On a $\varepsilon(n) \equiv n \pmod{q}$. On considère $T\colon X \to X$ définie par $T(n) = (n - \varepsilon(n))/q$.