

The Dynamics of Continued Fractions with Periodic Constraints

Brigitte Vallée

University of Caen

June 9, 1997

[summary by Philippe Flajolet]

Abstract

Consider rational, quadratic, or real numbers whose continued fraction representations satisfy periodic constraints. A typical instance is numbers whose continued fraction quotients are alternatively odd and even. Such sets have a somewhat fractal nature, and the Hausdorff dimension of the set of reals as well as the density of the set of rationals satisfying such constraints can be determined. Other consequences include a precise analysis of the height of constrained continued fractions. The methods rely on a transfer operator that generates the constraints and whose dominant spectral properties prove essential.

1. Introduction

The triadic Cantor set \mathcal{C} formed with numbers whose ternary representation does not contain the digit 2 is perhaps the most ancient instance of a set defined by constrained number representations. The density of triadic rationals $a/3^n$ that belong to \mathcal{C} is clearly $(2/3)^n$ and this set has a fractal Hausdorff dimension equal to $\log_3 2$; see for instance [1].

Continued fractions are of course a well-studied representation system and it is tempting to consider similarly what happens when constraints are imposed on them. The problems are more delicate since digits in continued fraction expansions are not independent in the common probabilistic sense. *Elementary* constraints are defined by a single set $M \subset \mathbb{N}$ and one imposes that all continued fraction digits (quotients) should belong to M . I. J. Good initiated this line of study in 1941 for $M = \{1, 2\}$, while recent results have been obtained by Hensley [3] for finite sets M .

Here, more general types of constraints are studied. Let $\ell \geq 1$ be an integer called the *period length*, and $\mathcal{M} = M_1 \times \cdots \times M_\ell$ a family of sets (noted multiplicatively) called the *period*. A number $x \in [0, 1]$ will be said to be \mathcal{M} -constrained if the sequence of its continued fraction digits is of type $M_1, M_2, \dots, M_\ell, M_1, M_2, \dots, M_\ell, \dots$, cyclically. For instance, we have

$$e - 2 = \exp(1) - 2 = /1, 2, 1, 1, 4, 1, 1, 6, 1, \dots/ = \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\dots}}}}$$

so that $e - 2$ obeys (for instance) the constraint $\mathcal{M} = \{1\} \times \{2, 4, 6, \dots\} \times \{1\}$ of length 3. Such sets arise naturally in connection with the robustness of hashing functions in cryptography [7].

2. Transfer Operators

The works of Mayer, Hensley, and Vallée (see, e.g., [2] for a gentle introduction) have demonstrated the importance of *transfer operators* in this range of problems. Let

$$U(x) = \frac{1}{x} - \left[\frac{1}{x} \right]$$

be the so-called continued-fraction *shift*. Classically, many features of the basic continued fraction algorithm and Euclid’s algorithm are captured by an operator (taken to act on families of analytic functions),

$$\mathcal{G}_s[f](z) := \sum_{m \geq 1} \left(\frac{1}{m+z} \right)^s f\left(\frac{1}{m+z} \right).$$

The operator \mathcal{G}_s is such that its specialization $\mathcal{G}_2[f]$ represents the probability density that results from applying one stage of the shift U to a random number drawn with initial density f . (This results from a simple argument that traces all the possible antecedents of a given real number.) It is known, since the works of Lévy, Kuzmin, and Wirsing, that properties of this operator, for instance its spectrum, are closely related to metric properties of continued fractions; see for instance [5, 6].

In the context of constrained numbers, it is then natural to introduce operators associated to an elementary constraint,

$$\mathcal{G}_{M,s}[f](z) := \sum_{m \in M} \left(\frac{1}{m+z} \right)^s f\left(\frac{1}{m+z} \right),$$

and, next in order of complexity, to a family of periodic constraints

$$\mathcal{G}_{\mathcal{M},s} := \mathcal{G}_{M_\ell,s} \circ \mathcal{G}_{M_{\ell-1},s} \circ \cdots \circ \mathcal{G}_{M_1,s}.$$

These operators play a rôle analogous to generating functions in analytic combinatorics. Algebraically (or formally), they generate all constrained continued fractions. By design, $\mathcal{G}_{M,s}$ generates all linear fractional transformations (LFT’s) of depth 1 that are constrained by M , the r th iterate $\mathcal{G}_{M,s}^r$ similarly generates all the LFT’s of depth k , and, for instance, the quasi-inverse

$$\omega(s) = (I - \mathcal{G}_{\mathcal{M},s})^{-1}[1](0)$$

yields the Dirichlet series of all rational numbers (of arbitrary depth) constrained by \mathcal{M} .

Analytically, density properties of constrained rationals are related to values of s such that $I - \mathcal{G}_{\mathcal{M},s}$ ceases to be invertible, since then objects like $\omega(s)$ become singular. Clearly, such singular values are determined by values of s such that 1 is an eigenvalue of $\mathcal{G}_{\mathcal{M},s}$.

The operator $\mathcal{G}_{\mathcal{M},s}$ is known to be compact (and even “nuclear” in the terminology of Grothendieck), which implies that its spectrum is discrete and the eigenvalues are “separated” from each other. In addition, for s real, the operator satisfies a strong positivity property visible from its definition. Thus, a generalized Perron-Frobenius theory—of which Markov chains and positive matrices are a very particular instance—applies, and there is a unique *dominant* eigenvalue that is simple and positive, $\lambda(\mathcal{M},s)$. Then, for a wide class of constraints (technically, of the so-called “open type”), the domain of existence of the function $s \mapsto \lambda(\mathcal{M},s)$ is an open set, and there exists a unique real $s_{\mathcal{M}}$ for which

$$\lambda(\mathcal{M},s_{\mathcal{M}}) = 1.$$

This number $s_{\mathcal{M}}$ is then a dominant singularity of the function $s \mapsto (I - \mathcal{G}_{\mathcal{M},s})^{-1}[1](0)$ and its rôle is essential.

In a way, the situation here is reminiscent of the analysis of the combinatorial *sequence schema*, $h(z) = (1 - g(z))^{-1}$ in the “supercritical case”, where $g(z)$ attains the value 1 before becoming singular.

3. Results

The number $s_{\mathcal{M}}$ always belongs to the interval $[0, 2]$. A first batch of results deals with metric information on constrained numbers, expressed in terms of the special quantity $s_{\mathcal{M}}$.

- (i) The Hausdorff dimension of the set $\mathbb{R}(\mathcal{M})$ of the \mathcal{M} -constrained reals is equal to $\frac{1}{2}s_{\mathcal{M}}$;
- (ii) The density of the set $\mathbb{Q}(\mathcal{M})$ of the \mathcal{M} -constrained rationals is equal to $s_{\mathcal{M}}$. This means that the subset of constrained rationals p/q satisfying $1 \leq p < q \leq N$ and $\gcd(p, q) = 1$ has a cardinality that satisfies

$$|\mathbb{Q}_N(\mathcal{M})| \sim c_{\mathcal{M}} N^{s_{\mathcal{M}}};$$

- (iii) A similar result holds for constrained quadratic irrationals of size $\leq N$. There, size is measured naturally by the smallest fundamental solution of Pell's equation, $x^2 - \Delta y^2 = 4$, with Δ the associated discriminant.

These three results have counterparts regarding characteristics of continued fraction expansions of constrained numbers, and especially the length of expansions, a parameter of great interest in the analysis of algorithms like Euclid's.

- (iv) The mean length of the continued fraction representation of a rational in $\mathbb{Q}_N(\mathcal{M})$ (i.e., a rational constrained by \mathcal{M} whose denominator is $\leq N$) satisfies

$$E[X_N(\mathcal{M})] \sim \frac{1}{\mathcal{L}_{\mathcal{M}}} \log N,$$

where $\mathcal{L}_{\mathcal{M}}$ is the so-called Lévy constant associated with the constraints \mathcal{M} ;

- (v) Similar results hold for constrained irrationals of "size" $\leq N$.

The value of Lévy's constant for unconstrained irrationals is

$$\mathcal{L} = \frac{\pi^2}{12 \log 2},$$

and, accordingly, this constant occurs in the expected number of steps of Euclid's algorithm, asymptotically $\frac{1}{\mathcal{L}} \log N$, a well-known result of Heilbronn and Dixon. In the general context of constraints, its value is related to the dominant eigenvalue $\lambda(\mathcal{M}, s)$ and to the "critical value" $s_{\mathcal{M}}$ by

$$\mathcal{L}_{\mathcal{M}} = -\frac{1}{\ell} \frac{d}{ds} \lambda(\mathcal{M}, s) \Big|_{s=s_{\mathcal{M}}}.$$

Thus, the statement (iv) vastly generalizes the Heilbronn-Dixon analysis.

The proofs rely on an algebraic description of sets and parameters of interest by means of the $\mathcal{G}_{\mathcal{M}, s}$ operators, as already explained. Then spectral properties (using positivity and Perron-Frobenius properties, as well as compactness) play an essential rôle. Finally, quantitative estimates are derived by means of Tauberian theorems applied to relevant Dirichlet series. The methods thus constitute an interesting parallel to those of analytic combinatorics, the problems being naturally more delicate, as one has to appeal to functional analysis and coefficient extraction of Dirichlet series. It is worth mentioning also that the constants appearing here can be estimated to reasonable accuracy (10 digits say), by means of truncation methods that have proved instrumental in the estimation of Wirsing's constant or Vallée's constant.

Interesting questions are also suggested by this talk that is to be presented at the *Journées Arithmétiques*, Limoges, September 1997. Along distributional lines, Hensley [4] proved in 1994 that the number of steps of Euclid's algorithm is asymptotically Gaussian. Probably, similar properties hold for constrained numbers. Can this be proved (e.g., by operator methods and simple perturbation theory)? Also, what about other types of constraints like "no two quotients equal to 1 in a row"? For strings, we know that the density is about $(\phi/2)^n$ with ϕ the golden section. It

is tempting to conjecture the existence of a fractal dimension for reals and a related density for rationals, of the form N^α . More generally, is there a theory of “regular constraints” that would be the counterpart for continued fractions of regular languages in the realm of strings?

References

- [1] Falconer (K. J.). – *The Geometry of Fractal Sets*. – Cambridge University Press, 1986, *Cambridge Tracts in Mathematics*, vol. 85, xiv+162p.
- [2] Flajolet (Philippe) and Vallée (Brigitte). – *Continued Fraction Algorithms, Functional Operators, and Structure Constants*. – Research Report n° 2931, Institut National de Recherche en Informatique et en Automatique, July 1996. 33 pages. Invited lecture at the 7th Fibonacci Conference, Graz, July 1996; to appear in *Theoretical Computer Science*.
- [3] Hensley (Doug). – Continued fraction Cantor sets, Hausdorff dimension, and functional analysis. *Journal of Number Theory*, vol. 40, n° 3, 1992, pp. 336–358.
- [4] Hensley (Doug). – The number of steps in the Euclidean algorithm. *Journal of Number Theory*, vol. 49, n° 2, 1994, pp. 142–182.
- [5] Knuth (Donald E.). – *The Art of Computer Programming*. – Addison-Wesley, 1981, 2nd edition, vol. 2: Seminumerical Algorithms.
- [6] Rockett (Andrew M.) and Szűsz (Peter). – *Continued Fractions*. – World Scientific Publishing Co. Inc., River Edge, NJ, 1992, x+188p.
- [7] Tillich (Jean-Pierre) and Zémor (Gilles). – Hashing with SL_2 . In *Advances in Cryptology. Lecture Notes in Computer Science*, vol. 839, pp. 40–49. – Berlin, 1994. Proceedings CRYPTO '94, Santa Barbara, CA, 1994.