

Continued Fractions, Comparison Algorithms, and Fine Structure Constants

Philippe Flajolet and Brigitte Vallée

To Jonathan Borwein, on the occasion of his award of a Doctorate Honoris Causa

ABSTRACT. There are known algorithms based on continued fractions for comparing fractions and for determining the sign of 2×2 determinants. The analysis of such extremely simple algorithms leads to an incursion into a surprising variety of domains. We take the reader through a light tour of dynamical systems (symbolic dynamics), number theory (continued fractions), special functions (multiple zeta values), functional analysis (transfer operators), numerical analysis (series acceleration), and complex analysis (the Riemann hypothesis). These domains all eventually contribute to a detailed characterization of the complexity of comparison and sorting algorithms, either on average or in probability.

Motivations

The topic of this paper is the study of one of the simplest possible algorithms for one of the simplest conceivable tasks—the comparison of two fractions. The algorithm has been proposed in the celebrated “Hackers’ Memorandum” known as HAKMEM [4], an amazing bag of tricks for computational mathematics that was collected at M.I.T. in 1972 by M. Beeler, R.W. Gosper, and R. Schroeppel. Amongst many gems relative to continued fraction algorithms and written by William Gosper, we find:

Item 101A (Gosper): Numerical comparison of continued fractions is slightly harder than in decimal, but much easier than with rationals – just invert the decision as to which is larger whenever the first discrepant terms are even-numbered. Contrast this with the problem of comparing the rationals $113/36$ and $355/113$.

The algorithm suggested here compares two rational numbers a/b and c/d by means of a continued fraction expansion algorithm applied simultaneously to the two numbers, and stopped as soon as a discrepancy of quotients is encountered. For instance,

1991 *Mathematics Subject Classification.* Primary 11Y65, 68Q25, 65U05, 37A45, 11Y60.

Key words and phrases. Continued fraction, algorithms, sorting, constants.

This work was supported in part by the ALCOM-FT Project (# IST-1999-14186) of the E.U.

we discover in three “short division” steps that

$$\alpha = \frac{224}{97} = \mathbf{2} + \frac{1}{\mathbf{3} + \frac{1}{\mathbf{4} + \frac{1}{\mathbf{3} + \frac{1}{\mathbf{2}}}}}, \quad \beta = \frac{95}{41} = \mathbf{2} + \frac{1}{\mathbf{3} + \frac{1}{\mathbf{6} + \frac{1}{\mathbf{2}}}}$$

satisfy $\alpha < \beta$ since the discrepant digits $\mathbf{4}, \mathbf{6}$ occur in the third position and satisfy $4 < 6$. In turn-of-the-millennium hacker’s parlance, one might as well describe the algorithm as two “lazy” parallel executions of the continued fraction algorithm.

For rational numbers, $x = a/b$ and $y = c/d$, the algorithm estimates the quantity $\text{sign}(a/b - c/d)$. The purest mathematician may well deem this discussion senseless. Don’t we have

$$(1) \quad \text{sign} \left(\frac{a}{b} - \frac{c}{d} \right) = \text{sign}(ad - bc),$$

or cannot we plainly compute with floating point numbers,

$$(2) \quad \text{sign} \left(\frac{a}{b} - \frac{c}{d} \right) \approx \text{sign} \left(\text{float} \left(\frac{a}{b} \right) - \text{float} \left(\frac{c}{d} \right) \right),$$

and easily determine the answers? Here is the main point. In the computational world, numbers are not “known” in the abstract, but rather accessible through finite or imperfect information only, like integral fraction forms or floating point approximations. In such a context, both *complexity* and *accuracy* of computations matter. The great advantage of the HAKMEM algorithm arises precisely from the fact that it operates within the *set precision* of data. For instance the straight evaluation (1) implies handling double precision numbers, that is, as much as 8 single-precision multiplications by naïve methods and 6 at least, when Karatsuba’s technique is used [27]; at any rate, the bit complexity is superlinear (e.g., quadratic, if standard multiplication is used), while our results imply that *the HAKMEM algorithm has linear bit complexity* on average. On another register, if divisions are performed in floating point, then wrong decisions may occur: for instance, one has

$$\frac{312689}{99532} - \frac{833719}{265381} \approx 3 \times 10^{-11},$$

and the sign is not even computed correctly with 10 digit arithmetics, although the fractions only involve 6-digit integers. To the contrary, the HAKMEM algorithm always provides the correct answer within the set precision. Such reasons explain for instance the multiple uses of the algorithm (under the name of `ab.vs.cd`) in Knuth’s design of the Metafont system: see [28].

The HAKMEM algorithm has surfaced in a diversity of contexts of which we now discuss a few. First, there are general-purpose computer arithmetics systems that are entirely based on continued fractions, a notable case being the one developed by Vuillemin around 1987 [49]; comparison of numbers in this context is likely to involve a version of the HAKMEM algorithm. Second, issues of correctness and robustness are central in the design of computational geometry systems: there, the comparison problem is identical to the problem of deciding the sign of 2×2 determinants (which means deciding the orientation of triangles); in this range of application, the HAKMEM algorithm has been rediscovered and extended by Avnaim et al. [1]. Finally, the HAKMEM algorithm is structurally very similar to an optimal algorithm proposed by Gauss for lattice reduction in dimension 2 that

is of special importance in various areas of computational number theory; the two analyses entertain very close ties as may be seen by examining references [14, 42] on which the present paper is partly based.

Our primary goal is a characterization, both on average and in probability, of the behaviour of the simple comparison algorithm whose principles have just been sketched. We also discuss in the paper an interesting generalization to sorting based on continued fraction digits. First, it turns out that the algorithms are best placed within the general framework of symbolic dynamics and expanding maps of the interval (Section 1). A whole variety of algorithms result, including two versions of the basic sign algorithm, one dependent on basic (standard) continued fractions, the other one relying on centred continued fractions. Fundamental intervals that are familiar from the elementary theory of continued fraction then conduce to slowly convergent sums, called “moment sums”, that express the average case complexity of the sign algorithms (Section 2) and of the corresponding (radix) sorting algorithms (Section 3). In the basic continued fraction case, moment sums appear to be related to multiple zeta values and Euler-Zagier constants, so that they are surrounded by a strong set of identities and fast convergent sum or integral representations (Section 4). In contrast, the centred case leads to non-analytic sums arising from the floor function and irrational multipliers so that specific series acceleration need to be developed that rely on lattice generating functions (Section 5).

Functional analysis is then brought into play in Section 6. It turns out that transfer operators of the Ruelle-Mayer type have dominant eigenvalues that precisely describe the geometric rate of decay in the probability distribution of costs of the sign-algorithms (Sections 6). As a final surprise (Section 7), the cost of sorting n numbers exhibits an asymptotic dependency on n whose character is dictated by the position of the nontrivial zeros of the Riemann zeta function, that is to say, by the Riemann hypothesis.

One of the themes of this paper is the effective computability of the constants involved in the analysis. A real number α is said to be *polynomial time computable* if an approximation of α to accuracy 10^{-d} can be computed in time $\mathcal{O}(d^r)$ for some integer r . We let \mathbf{P} denote the class of such numbers. (See [8] for an introduction to this aspect of computational mathematics.) Effective numerical procedures usually go along with proofs of membership in \mathbf{P} .

1. Expanding maps, sign algorithms, and continued fractions

Symbolic dynamics concerns itself with the interplay between properties of a continuous transformation and discrete properties of trajectories of points under iteration of the transformation. A common framework in symbolic dynamics is the one of *expanding maps of the interval* and their associated *number representation systems*. The definition involves a triplet $(\mathcal{I}, U, \mathcal{M})$ that satisfies the following conditions:

- (E_1) The set \mathcal{M} , whose elements are called digits, is a subset of the integers; there is a partition $\{I_j\}_{j \in \mathcal{M}}$ of the interval \mathcal{I} satisfying additionally the condition below.
- (E_2) The function $U(x)$ maps monotonically each I_j onto \mathcal{I} and is expanding, meaning that $|U'(x)| > 1$ on the closure \bar{I}_j of I_j .

See [38] for some of the main properties. An expanding map thus consists of finitely or denumerably many branches indexed by some set \mathcal{M} . We let $m(x) \in \mathcal{M}$

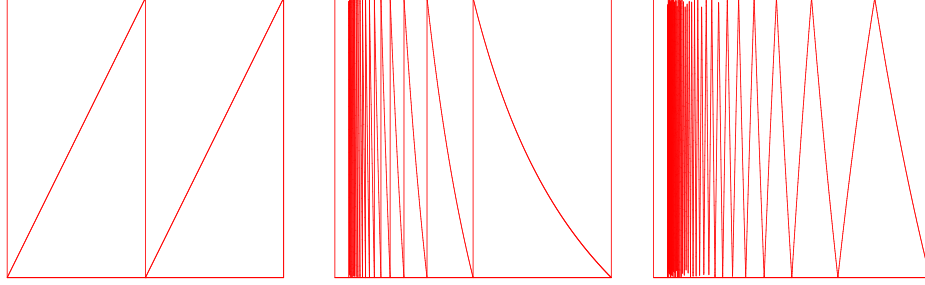


FIGURE 1. The three maps corresponding to binary representations ($\{2x\}$, left), basic continued fractions ($\{1/x\}$, middle), and centred continued fractions ($\{\{1/x\}\}$, right).

represent the branch of $U(x)$ in the domain of which x falls. A coding of a real number x is then obtained by the sequence

$$(3) \quad m(x), m(U(x)), m(U^2(x)), m(U^3(x)), \dots$$

where powers denote iteration, $U^2 = U \circ U$, etc. The sequence of *digits* of x , $\mathbf{m} = (m_1, \dots, m_k, \dots) = (m(x), \dots, m(U^k(x)), \dots)$ is then produced by the following simple algorithm.

procedure (\mathcal{I}, U, m) -**expansion**($x : \mathcal{I}$)
for $k := 1$ **to** $+\infty$ **do**
 $m_k := m(x); x := U(x);$

A special rôle is played by the set \mathcal{H}_1 of branches of the inverse function $U^{(-1)}$ of U that are also naturally numbered by the index set \mathcal{M} . If x_k and the sequence $\mathbf{m} = (m_1, \dots, m_k)$ is known, the algorithm can be run backwards, and the original x_0 is recovered by

$$x_0 = h_{\mathbf{m}}(x_k) \quad \text{where} \quad h_{\mathbf{m}}(y) = h_{m_1} \circ h_{m_2} \circ \dots \circ h_{m_k}(y).$$

The set \mathcal{H} of all compositions $h_{\mathbf{m}}$ is referred to as the set of *branches of the inverse function* or *inverse branches* for short; the index k in $h_{(m_1, \dots, m_k)}$ is called the depth of h and denoted by $|h|$. Clearly, the stochastic behaviour of a numbering system is closely related to the dynamics of $U(x)$ on the interval \mathcal{I} ; this dynamics is itself isomorphic to the dynamics of the semigroup of contractions \mathcal{H} that is generated by the depth-one inverse branches \mathcal{H}_1 .

Let $[y]$ be the integer part function of y and $\{y\} = (y \bmod 1)$ the fractional part. The scheme (3) generalises the usual binary representation of real numbers (see Fig. 1) that corresponds to fixing the choice

$$\mathcal{I} = [0, 1], \quad U(x) = \{2x\}, \quad m(x) = [2x].$$

As we shall explain in some detail, this constitutes also a very convenient framework for a discussion of continued fraction algorithms.

Sign algorithms. The basic numeration scheme relative to an abstract triplet (\mathcal{I}, U, m) gives rise to a semi-decision algorithm that determines if two numbers are distinct: in order to detect distinctness of x and x' simply expand “lazily” in parallel x and x' until the first discrepant digit is detected. The scheme is then

procedure (\mathcal{I}, U, m) -**sign** $(x, x' : \mathcal{I})$
for $k := 1$ **to** $+\infty$ **do**
 $m_k := m(x); m'_k := m(x); x := U(x); x' = U(x')$;
if $m_k \neq m'_k$ **then exit**.

Since the branches of U are by assumption each monotonic, the knowledge of the partial codings $(m_1, \dots, m_{k-1}, m_k)$ and $(m_1, \dots, m_{k-1}, m'_k)$, where k denotes the position of the first discrepant digit, fully determine the sign of the difference $x - x'$. For instance, binary representations, where every branch is monotone increasing, have $\text{sign}(x - x') = \text{sign}(m_k - m'_k)$.

In the sequel, we examine two numeration systems relative to continued fractions: the basic continued fraction system (where characteristic quantities are indicated by a bar sign $(\bar{\cdot})$) and the centred continued fraction system (indicated by a hat $(\hat{\cdot})$).

Basic continued fraction expansions. The *basic continued fraction (BCF)* system fits into the general framework. It is defined by the triplet $(\bar{\mathcal{I}}, \bar{U}, \bar{m})$

$$\bar{\mathcal{I}} = [0, 1], \quad \bar{U}(x) = \left\{ \frac{1}{x} \right\}, \quad \bar{m}(x) = \left\lfloor \frac{1}{x} \right\rfloor.$$

By convention, we take $\bar{U}(0) = 0, \bar{m}(0) = 0$.

To one step of the *BCF* expansion algorithm, there corresponds the set of inverse branches of depth 1,

$$\bar{\mathcal{H}}_1 := \{h(z) = \frac{1}{m+z} \quad m \geq 1\},$$

and the set of digits is $\bar{\mathcal{M}} = \{1, 2, \dots\}$. The inverse branches of arbitrary depth are then *linear fractional transformations* (LFT's for short). To a real number $x \in \bar{\mathcal{I}}$, the *BCF* algorithm thus associates the sequence of iterates $x_0 = x, x_1, x_2, \dots, x_k$, and (with the convention $1/0 = 0$)

$$x_0 = h_{\mathbf{m}}(x_k) \quad \text{where} \quad h(y) = \frac{1}{m_1 + \frac{1}{m_2 + \frac{1}{\ddots + \frac{1}{m_k + y}}}}.$$

The *BCF*-sign algorithm dependent on basic continued fraction expansions is exactly the HAKMEM algorithm described in the introduction. Here all branches are monotone decreasing, so that

$$\text{sign}(x - x') = (-1)^k \text{sign}(m_k - m'_k),$$

since each stage of the iteration is orientation-reversing.

Centred continued fraction expansions. Centred continued fractions are obtained when one replaces truncation (integer part function) by rounding to the nearest integer. First introduce the notations

$$[[y]] = \left\lfloor x + \frac{1}{2} \right\rfloor, \quad \{\{y\}\} = |y - [[y]]|, \quad \varepsilon(y) = \text{sign}(y - [[y]]),$$

so that the following identity holds:

$$y = [[y]] + \varepsilon(y)\{\{y\}\}.$$

Then, the *centred continued fraction (CCF)* system is defined by the triplet $(\widehat{\mathcal{I}}, \widehat{U}, \widehat{m})$ given by

$$\widehat{\mathcal{I}} = [0, \frac{1}{2}], \quad \widehat{U}(x) = \{\{\frac{1}{x}\}\}, \quad \widehat{m}(x) = \varepsilon(\frac{1}{x})[[\frac{1}{x}]],$$

with, conventionally, $\widehat{U}(0) = 0$, $\widehat{m}(0) = 0$, $1/0 = 0$.

The *CCF* expansion algorithm operates on the interval $\widehat{\mathcal{I}} = [0, \frac{1}{2}]$. By design, the allowed indices m must satisfy the condition $|m| \geq 2$, and, furthermore, the value $m = -2$ does not occur since $m(1/x) = -2$ could only arise from an x larger than $\frac{1}{2}$. In this way, the set of LFT's of depth 1 for the *CCF*-algorithm is

$$\widehat{\mathcal{H}}_1 := \left\{ h(z) = \frac{1}{m+z} \quad m \geq 2 \right\} \cup \left\{ h(z) = \frac{1}{m-z} \quad m \geq 3 \right\},$$

and the set of digits is $\widehat{\mathcal{M}} = \{+2, -3, +3, -4, +4, \dots\}$.

The relation between x_0 and x_k is described by a linear fractional transformation of depth k , which is associated to the k -tuple of signed integers $\mathbf{m} = (m_1, \dots, m_k)$

$$(4) \quad h_{\mathbf{m}}(z) = \frac{1}{|m_1| + \frac{\varepsilon_1}{|m_2| + \frac{\varepsilon_2}{\ddots \frac{\varepsilon_{k-1}}{|m_k| + \varepsilon_k z}}}}, \quad \varepsilon_j = \text{sign}(m_j).$$

The *CCF*-sign algorithm based on centred continued fractions is such that an iteration is increasing if the corresponding sign is -1 and decreasing otherwise. In that case, one has

$$\text{sign}(x - x') = \sigma \prod_{j=1}^{k-1} (-\text{sign}(m_j)),$$

where $\sigma \in \{-1, 1\}$ is $+1$ iff $m_k \succ m'_k$ in the nonstandard order over on \mathbb{Z} ,

$$0 \prec -1 \prec +1 \prec -2 \prec +2 \prec -3 \prec +3 \dots,$$

that is also the lexicographic order on $\mathbb{N} \times \{-1, +1\}$.

Note. A variety of practical implementations result from the sign algorithms based on continued fraction representations. For instance, when applied to rational numbers, inverses are effected plainly by exchanging components of integer pairs, and the sign algorithm should be halted as soon as one of the continued fraction expansions terminates, etc. When applied to real numbers in fixed precision, the number of iterations can be bounded in advance by a quantity that depends on the machine precision, or on the size of the mesh according to which numbers are considered as distinct.

2. Fundamental intervals and the sign algorithms

The overall purpose of this paper is an understanding of the complexity of the comparison algorithm and its cognates, in the context of continued fraction representations. The probabilistic model adopted is the uniform model over the set of legal inputs and the complexity measure of the sign algorithms is the number L of iterations performed (that is, the value of the index k of the first discrepant digit). Knuth [28] reports for his version of the basic HAKMEM algorithm that

“in most cases, a quick decision is reached” while Avnaim et al. [1] estimate from simulations that “the average number of iterations is [about] 1.5”.

Following good precepts, we start with an experimental approach. Simulating 10^6 executions of the *BCF* and *CCF* sign algorithms over uniform pairs of real $(0, 1)$ numbers provides empirical estimates on the probability distributions of costs as well as on the average-case complexity of the algorithms. Here is a tabulation of what we find.

	Basic CF-sign	Centred CF-sign
$\Pr(L = 1)$	0.710050	0.918003
$\Pr(L = 2)$	0.241275	0.075710
$\Pr(L = 3)$	0.038339	0.000422
$\Pr(L = 4)$	0.008424	0.000035
$\Pr(L = 5)$	0.001608	0.000005
$E(L)$	1.351612	1.088791

It is apparent that the probabilities of the main loop being executed k times decay roughly geometrically with k —somewhat like 5^{-k} for the basic algorithms and 13^{-k} for the centred algorithm. (The centred algorithm is based on a better approximation scheme that converges faster; in practice, the advantage may however be offset by a costlier internal loop.) In accordance with the geometric decay, the expectations are finite. For 10^6 simulations, counting on a statistical error of about 10^{-3} , we anticipate the values $E(\bar{L}) = 1.352 \pm 0.001$ and $E(\hat{L}) = 1.089 \pm 0.001$. These heuristic observations will receive a sound mathematical basis in the forthcoming sections: see for instance the table of Figure 6 for a final summary. We also note that alternative data and complexity models can be studied by suitable adaptations of the methods presented here; examples include discrete data [14], nonuniform input distributions [42], and bit-complexity models (work in progress).

Fundamental intervals. Let us first examine the sign algorithm in the context of a numbering system arising from a general expanding map (\mathcal{I}, U, m) . Borrowing terminology from the standard metric theory of continued fraction, we call any $h(\mathcal{I})$, the transform by h of the interval \mathcal{I} , a *fundamental interval*, and the depth of h is called the *rank* of the fundamental interval. Thus, the fundamental interval contains all real numbers whose expansion starts with the k -tuple (\mathbf{m}) indexing h ($h = h_{\mathbf{m}}$).

We adopt here the uniform probability model (Lebesgue measure) on \mathcal{I} . The probability that a number of \mathcal{I} belongs to the fundamental interval relative to the branch h is called the *fundamental measure* associated to h and is denoted by u_h . Without loss of generality, we restrict the interval to be of the type $\mathcal{I} = [0, \alpha]$ for some $\alpha > 0$. The fundamental measure is then from its definition

$$u_h = \frac{1}{\alpha} |h(0) - h(\alpha)|.$$

For analysing the 2-dimensional sign algorithm, the square $\mathcal{I} \times \mathcal{I}$ is by assumption endowed with the uniform product measure. The probabilistic event $[L \geq k+1]$ is formed with all real pairs $(x, y) \in \mathcal{I} \times \mathcal{I}$ which have expansions that coincide till depth k . Then the two real numbers x and y belong to the same fundamental interval $h(\mathcal{I})$ of rank k , and the pair (x, y) belongs to the square $h(\mathcal{I}) \times h(\mathcal{I})$. Such

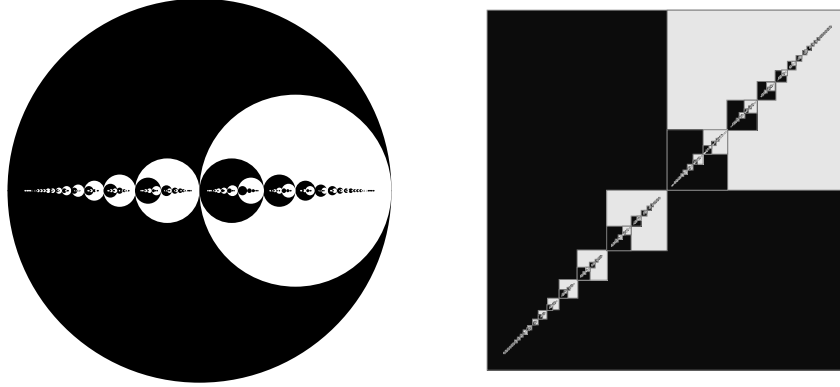


FIGURE 2. Basic continued fractions: the fundamental intervals represented by their supporting discs (left) and the fundamental squares (right). The events $[L = k]$ for ranks $k = 0..5$ are alternately represented by dark and light colours.

a square is called a *fundamental square* of rank k . The event $[L \geq k + 1]$ is thus equal to the disjoint union of all the fundamental squares of rank k ,

$$(5) \quad [L \geq k + 1] = \bigcup_{|h|=k} h(\mathcal{I}) \times h(\mathcal{I}).$$

Since fundamental squares are disjoint the probability that the Sign algorithm performs at least $k + 1$ iterations is a sum that involves the measures of fundamental squares u_h^2 , and

$$(6) \quad \Pr(L \geq k + 1) = \sum_{|h|=k} u_h^2 = \frac{1}{\alpha^2} \sum_{|h|=k} |h(0) - h(\alpha)|^2.$$

The average number of iterations is then obtained by the usual summation of probabilities,

$$(7) \quad E[L] = \sum_h u_h^2 = \frac{1}{\alpha^2} \sum_h |h(0) - h(\alpha)|^2.$$

More generally, we define the *moment sums*

$$\rho^{(\ell)} := \sum_h u_h^\ell = \frac{1}{\alpha^\ell} \sum_h |h(0) - h(\alpha)|^\ell$$

which, for integer values of ℓ , are central in the the n -sorting algorithm to be discussed in Section 3.

Continued fraction algorithms. From the expression obtained in (5), the average-case analysis of any expanding-map version of the sign-algorithm is dependent upon an evaluation or at least a numerical estimation of the simplest of all moment sums, namely $\rho^{(2)}$. We now specialize the discussion to the basic and centred continued fraction algorithms. This depends upon the characterization of all the LFT's of $\overline{\mathcal{H}}$ and $\widehat{\mathcal{H}}$ provided by elementary number theory and a theorem of Hurwitz.

— The set $\overline{\mathcal{H}}$ of all possible LFT's used by the *BCF*-algorithm is

$$\overline{\mathcal{H}} := \left\{ \frac{az + b}{cz + d} \mid (a, b, c, d) \in \mathbb{N}^4, |ad - bc| = 1, c \leq d, a \leq c, b \leq d \right\}.$$

— The set $\widehat{\mathcal{H}}$ of all possible LFT's used by the *CCF*-algorithm involves the golden ratio $\phi = (1 + \sqrt{5})/2$ (Hurwitz [25]):

$$\widehat{\mathcal{H}} := \left\{ \frac{az + b}{cz + d} \mid (b, d) \in \mathbb{N}^2, (a, c) \in \mathbb{Z}^2, \right. \\ \left. ac \geq 0, |ad - bc| = 1, \frac{-d}{\phi^2} < c < \frac{d}{\phi}, |a| \leq \frac{|c|}{2}, b \leq \frac{d}{2} \right\}.$$

It is observed that the numbers (a, b, c, d) are such that the pairs (a, c) and (b, d) are built with coprime integers, since the Bézout condition $ad - bc = \pm 1$ is satisfied. Thanks to this characterization, the expected cost of the sign algorithms falls as a ripe fruit.

THEOREM 1. *The expected cost of the basic and centred sign algorithms are expressible as sums over lattice points in \mathbb{N}^2 ,*

$$E(\overline{\mathcal{L}}) = \overline{\rho}^{(2)}, \quad E(\widehat{\mathcal{L}}) = \widehat{\rho}^{(2)},$$

where, generally, the moment sums of index ℓ satisfy

$$(8) \quad \begin{aligned} \overline{\rho}^{(\ell)} &= 1 + \frac{1}{2^\ell} + \frac{2}{\zeta(2\ell)} \sum_{d < c < 2d} \frac{1}{c^\ell d^\ell}, \\ \widehat{\rho}^{(\ell)} &= \frac{2^\ell}{\zeta(2\ell)} \sum_{d\phi < c < d\phi^2} \frac{1}{c^\ell d^\ell} \quad (\phi = (1 + \sqrt{5})/2). \end{aligned}$$

PROOF. Consider first the basic case. Each pair (c, d) that satisfies $\gcd(c, d) = 1, d \geq 2$ and $0 < c < d$ is associated to two LFT's of $\overline{\mathcal{H}}$, since a rational number interior to $(0, 1)$ admits at the same time a proper and an improper continued fraction expansion (the last digits is ≥ 2 , resp. $= 1$). Then, taking into account boundary cases, namely pairs $(0, 1)$ and $(1, 1)$, we find

$$\overline{\rho}^{(\ell)} = 1 + \frac{1}{2^\ell} + 2 \sum \frac{1}{d^\ell (c + d)^\ell},$$

where the sum is taken over all the pairs (c, d) satisfying $\gcd(c, d) = 1, d \geq 2$ and $0 < c < d$. The general term in the last sum is homogeneous of degree 2ℓ , so that the gcd condition is eliminated provided one divides the sum by $\zeta(2\ell)$.

Consider next the centred case. Each pair (c, d) that satisfies $\gcd(c, d) = 1, d \geq 1$ and $-d/\phi^2 < c < d/\phi$ is associated to a unique LFT of $\widehat{\mathcal{H}}$. Then, we find

$$\widehat{\rho}^{(\ell)} = 2^\ell \sum \frac{1}{d^\ell (2d + c)^\ell},$$

where the sum is taken over all the pairs (c, d) satisfying $\gcd(c, d) = 1, d \geq 1$ and $-d/\phi^2 < c < d/\phi$. In this case, the integer $f := 2d + c$ satisfies $d\phi < f < d\phi^2$. The gcd condition is again eliminated by means of a factor $1/\zeta(2\ell)$. \square

The moment sums of the basic and the centred algorithm look superficially similar. The summation condition is in each case determined geometrically as a sum over *lattice cones* defined by the two conditions,

$$d < c < 2d \quad \text{and} \quad [d\phi] \leq c \leq [d\phi^2].$$

However, the corresponding sums $\bar{\rho}^{(\ell)}$ and $\hat{\rho}^{(\ell)}$ belong to different classes of mathematical constants. The basic ones, $\bar{\rho}^{(\ell)}$ live in a world of identities, integral representations, and special functions. Indeed, as we shall see the mean $\bar{\rho}^{(2)}$ is reducible to $\zeta(3)$ and a polylogarithm. More generally, $\rho^{(\ell)}$ is a member of the class of Euler-Zagier sums, currently a subject of active interest. In contrast, the sums $\hat{\rho}^{(\ell)}$, starting with $\hat{\rho}^{(2)}$, have a “nonanalytic character” due to the summation condition $[d\phi] \leq c \leq [d\phi^2]$, with ϕ being irrational, and there is little hope of reducing them to some standard closed form. We shall see later that they can at least be subjected to appropriate series acceleration methods leading to efficient evaluation to high precision.

3. The sorting algorithm

The sign problem leads naturally to the more general question of testing distinctness of n real numbers, or, analogously, to the problem of sorting n numbers. For numbering systems like the ones considered here, it is the idea of *radix sorting* [26] that is natural. The principle is to determine the leading digit of each of the quantities x_1, \dots, x_n to be sorted, group them according to their leading digits, and then sort recursively the subgroups based on the following leading digits. Alternatively, one may view the algorithm as building successive refinements of the coarsest partition until the finest partition is obtained. These refinements are themselves best described as a tree called the *digital tree* or *trie*, which is one of the major data structures of computer science [26, 31]. The analysis developed here then answers the following question: How many digits in total must be determined in order to distinguish (and sort) n real numbers? In symbolic dynamical terms, it describes the way trajectories of n random points under the “shift” U evolve by sharing some common digits before branching off from each other.

Digital trees. We now formulate the sorting algorithm in its more convenient graphic tree version. To any finite set $X := \{x_1, x_2, \dots, x_n\}$ of n real numbers of \mathcal{I} , one associates a *digital tree*, $\text{trie}(X)$, defined by the two recursive rules:

- (R_1) If $X = \{x\}$ has cardinality equal to 1, then $\text{trie}(X)$ consists of a single *leaf node* that contains x .
- (R_2) If X has cardinality at least 2, then $\text{trie}(X)$ is an *internal node* represented generically by ‘ o ’ to which are attached r subtrees, where $r := \text{card } m(X)$ is the number of different head digits in X . Let b_1, b_2, \dots, b_r be the different head symbols that appear in X ; $\text{trie}(X)$ is defined by

$$\text{trie}(X) = (o, \text{trie}(X_1), \text{trie}(X_2), \dots, \text{trie}(X_r)),$$

where

$$X_i = \{U(x) \mid m(x) = b_i, x \in X\}.$$

Such a tree structure underlies classical radix sorting methods. The tree can be built by following the recursive rules (R_1), (R_2) and a suitable ordering of subtrees gives rise to an algorithm that sorts any set X either lexicographically or under the natural order on the real numbers.

Analysis of the sorting algorithm. According to standard terminology, the *level* of a node in a digital tree is the number of edges that connect it to the root. The *path length* of the tree is the sum of the levels of all leaves. The path length of $\text{trie}(X)$ is thus equal to the total number of digits that need to be examined in

$$\begin{aligned}
\phi - 1 &= / \mathbf{1}, \mathbf{1}, \mathbf{1}, 1, 1, 1, \dots / \\
\gamma &= / \mathbf{1}, \mathbf{1}, \mathbf{2}, 1, 2, 1, \dots / \\
\exp(1) - 2 &= / \mathbf{1}, \mathbf{2}, \mathbf{1}, 1, 4, 1, \dots / \\
\log 2 &= / \mathbf{1}, \mathbf{2}, \mathbf{3}, 1, 6, 3, \dots / \\
\{\exp(\pi\sqrt{163})\} &= / \mathbf{1}, \mathbf{1333462407511}, 1, 8, 1, 1, \dots / \\
2^{1/3} - 1 &= / \mathbf{3}, 1, 5, 1, 1, 4, \dots / \\
\pi - 3 &= / \mathbf{7}, \mathbf{15}, 1, 292, 1, 1, \dots /
\end{aligned}$$

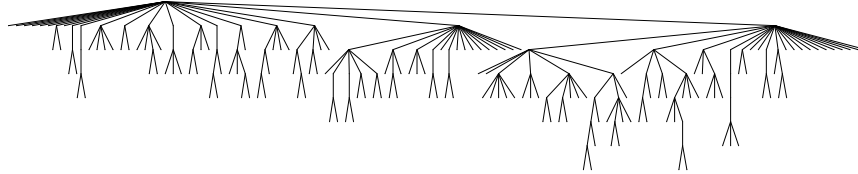


FIGURE 3. (Top) The fractional parts of 7 real numbers: the digits in bold represent the minimal prefix set of 16 digits (the sorting cost, equivalently path length) needed to distinguish the numbers from each other. (Bottom) A randomly drawn digital tree of size 100 built from basic continued fractions has path length 1323, height 16, and number of internal nodes equal to 222.

order to distinguish all elements of X and radix-sort X (see Figure 3) so that we adopt it as our definition of the *sorting cost*.

First, we discuss the case of a general numbering system. Let $P(n)$ be the expectation of the path length of $\text{trie}(X)$ when X is drawn from \mathcal{I}^n with the uniform probability measure. We claim the equality:

$$(9) \quad P(n) = \sum_{h \in \mathcal{H}} nu_h [1 - (1 - u_h)^{n-1}].$$

Indeed, let L_i be the length of the branch whose leaf contains the designated element x_i . The event $[L_i > k]$ means that there exists a fundamental interval of depth k that contains x_i and at least another element x_j . Thus, we have

$$\Pr(L_i > k) = \sum_{|h|=k} u_h [1 - (1 - u_h)^{n-1}].$$

Summing over all possible values of index i and integer k then yields equation (9).

Next, a straight binomial expansion provides an expression for $P(n)$ that reduces to a linear combination of the “moment sums”:

$$(10) \quad P(n) = n \sum_{\ell=1}^{n-1} (-1)^{\ell+1} \binom{n-1}{\ell} \rho^{(\ell+1)}.$$

In other words, $P(n)$ is nothing but an $(n-1)$ st order difference of the moment sums.

The discussion specializes immediately to tries built on continued fractions and hence to the corresponding sorting algorithms *BCF-sort* and *CCF-sort*.

THEOREM 2. *The expectations of the number of digit inspections performed by the sorting algorithms BCF-sort (basic continued fractions) and CCF-sort (centred*

continued fractions) applied to n real numbers are given by

(11)

$$\overline{P}(n) = n \sum_{\ell=1}^{n-1} (-1)^{\ell-1} \binom{n-1}{\ell} \overline{\rho}^{(\ell+1)}, \quad \widehat{P}(n) = n \sum_{\ell=1}^{n-1} (-1)^{\ell-1} \binom{n-1}{\ell} \widehat{\rho}^{(\ell+1)}.$$

There, $\overline{\rho}^{(\ell)}$ and $\widehat{\rho}^{(\ell)}$ are the moment sums of Eq. (8).

The theorem predicts

$$P(2) = 2\rho^{(2)}, \quad P(3) = 6\rho^{(2)} - 3\rho^{(3)}, \quad P(4) = 12\rho^{(2)} - 12\rho^{(3)} + 4\rho^{(4)}.$$

The form $P(2) = 2\rho^{(2)}$ is in accordance with the analysis of the sign algorithm: in this special case, there are two leaves at the same level, and this level coincides with the number of iterations of the sign algorithm. Figure 3 (bottom) displays a random trie of size 100 based on the *BCF* system and kindly communicated to us by Julien Clément from his memoir [11].

We shall see in the last section that the asymptotic behaviour of path length (when n tends to infinity) involves the location of nontrivial zeros of the zeta function and hence is related to the Riemann hypothesis.

4. Multiple zeta values and the basic sign algorithm

The moment sums associated to the basic continued fraction system are double sums of simple rational functions and it is of interest to determine to what extent they relate to other classical constants of analysis. The adequate framework is that of *multiple zeta values* (MZV's), also known as Euler–Zagier sums, that we take here under the form

$$(12) \quad \zeta^{\varepsilon_1, \dots, \varepsilon_r}(s_1, \dots, s_r) := \sum_{n_1 > \dots > n_r} \frac{\varepsilon_1^{n_1} \dots \varepsilon_r^{n_r}}{n_1^{s_1} \dots n_r^{s_r}}, \quad \varepsilon_j \in \{-1, +1\}.$$

The term “values” stresses the fact that instances at positive integer arguments are considered. The quantity $w = s_1 + \dots + s_r$ is called the weight and r is called the rank or the multiplicity of the sum. The simplest sums are those of rank 1,

$$\zeta^+(s) \equiv \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \zeta^-(s) = \sum_{n=1}^{\infty} \frac{(-1)^n}{n^s} = (2^{1-s} - 1)\zeta(s),$$

that is, the Riemann zeta function and its alternating variant. Especially relevant to the present discussion are the double zeta values

$$\begin{aligned} \zeta^{++}(s, t) \equiv \zeta(s, t) &= \sum_{n=1}^{\infty} \sum_{q=1}^{n-1} \frac{1}{n^s q^t} = \sum_{n=1}^{\infty} \frac{H_{n-1}^{(t)}}{n^s} \\ \zeta^{-+}(s, t) &= \sum_{n=1}^{\infty} \sum_{q=1}^{n-1} \frac{(-1)^n}{n^s q^t} = \sum_{n=1}^{\infty} (-1)^n \frac{H_{n-1}^{(t)}}{n^s}, \end{aligned}$$

with $H_n^{(t)} = \sum_{j \leq n} j^{-t}$ the generalized harmonic number of order t .

The origin of these sums lies in a letter of Goldbach to Euler dated December 24, 1742 (see Berndt's book [5, Ch. 9] and references therein), with evaluations like

$$\zeta(2, 1) = \sum_{n=1}^{\infty} \frac{H_{n-1}}{n^2} = \zeta(3).$$

published in 1775 by Euler and further developed by Nielsen a century later [35]. Interest was rekindled recently when Zagier in his address [51] demonstrated connections with many “deep” areas¹ of pure mathematics, at a time when, independently, Borwein and collaborators [3, 6] were discovering many surprising identities like the spectacular septic sum

$$\sum_{n=1}^{\infty} \frac{(H_{n-1})^4}{n^3} = \frac{185}{8}\zeta(7) - \frac{43}{2}\zeta(3)\zeta(4) + 5\zeta(2)\zeta(5),$$

that we leave as a challenge to the reader. (Hint: see for instance [17] for an elementary approach.) A partial evaluation is any reduction of a multiple zeta value to a polynomial form in multiple zeta values of smaller rank; a complete evaluation means a reduction to a polynomial form in zeta values $\zeta(2), \zeta(3), \dots$, and $\zeta^-(1) = -\log 2$. What is known regarding positive and alternating double zeta values is summarized in Fig. 4.

It is easy to reduce the moment sums to multiple zeta values. Start with

$$(13) \quad \sum_{d < c < 2d} \frac{1}{c^\ell d^\ell} = \sum_{c < 2d} \frac{1}{c^\ell d^\ell} - \sum_c \frac{1}{c^{2\ell}} - \sum_{c < d} \frac{1}{c^\ell d^\ell}.$$

The last sum in (13) is a non-alternating zeta value $\zeta(\ell, \ell)$ that is of the “central” type and that must reduce in accordance with what is summarized in Fig 4. Indeed, distributing the sums in an expansion of the product $\zeta(s) \times \zeta(t)$ yields the “shuffle relations”:

(14)

$$\zeta(s)\zeta(t) = \zeta(s, t) + \zeta(s+t) + \zeta(t, s), \quad \text{implying} \quad \zeta(\ell, \ell) = \frac{1}{2}(\zeta(\ell)^2 - \zeta(2\ell)).$$

The first sum in (13) is none other than the even part of an alternating zeta, namely,

$$(15) \quad \sum_{c < 2d} \frac{1}{c^\ell d^\ell} = 2^{\ell-1} \sum_{c < e} \frac{1 + (-1)^e}{c^\ell e^\ell} = 2^{\ell-1} (\zeta^{++}(\ell, \ell) + \zeta^{-+}(\ell, \ell)).$$

Thus, by (13), (14), and (15), we find

$$(16) \quad \rho^{(\ell)} = 2^{-\ell} - 2^{\ell-1} + (2^{\ell-1} - 1) \frac{\zeta(\ell)^2}{\zeta(2\ell)} + \frac{2^\ell}{\zeta(2\ell)} \zeta^{-+}(\ell, \ell).$$

This is as far as one can go for general values of ℓ , since a reduction of $\zeta^{-+}(\ell, \ell)$ is not there.

The particular case of the mean cost of the *BCF*-sign algorithm, $\ell = 2$, benefits of specific results due to Sitaramachandrarao [40] and De Doelder [15], themselves motivated by identities of Ramanujan [5]. First, Sitaramachandrarao relates $\zeta^{-+}(3, 1)$ and $\zeta^{-+}(2, 2)$ by

$$(17) \quad 32\zeta^{-+}(3, 1) + 16\zeta^{-+}(2, 2) + 5\zeta(4) = 0.$$

This nontrivial identity is Eq. (5.4) of [40]. The next step involves a special instance of the polylogarithm function [30] that is classically defined by

$$\text{Li}_m(z) = \frac{z}{1^m} + \frac{z^2}{2^m} + \frac{z^3}{3^m} + \dots.$$

¹Multiple zetas and polylogarithms are nowadays found relevant to a large body of science including knot invariants, Feynman diagrams, and even the theory of perverse sheaves.

I. Nonalternating zeta values: defined by $\varepsilon_j = +1$ in (12): $\zeta(a, b) = \sum_{m>n} \frac{1}{m^a n^b}$.

(N_0) All central double zetas are reducible: $\zeta(\ell, \ell) = \frac{1}{2}\zeta(\ell)^2 - \frac{1}{2}\zeta(2\ell)$ (Goldbach, 1742).

(N_1) All double zetas $\zeta(p, q)$ of odd weight $w = p + q$ reduce to zeta values (Borwein et al. [6]):

$$2\zeta(p, q) = - \left((-1)^q \binom{p+q}{p} + 1 \right) \zeta(p+q) + (1 - (-1)^q) \zeta(p) \zeta(q) \\ + 2(-1)^q \sum_j \left[\binom{2j-2}{p-1} + \binom{2j-2}{q-1} \right] \zeta(2j-1) \zeta(p+q-2j+1).$$

(N_2) All double zetas $\zeta(p, 1)$ reduce to zeta values (Euler):

$$\zeta(p, 1) = \frac{p}{2} \zeta(p+1) - \frac{1}{2} \sum_{k=1}^{p-2} \zeta(k+1) \zeta(p-k).$$

(N_3) The \mathbb{Q} -vector space of all nonalternating MZV's of weight w has a dimension d_w which, according to Zagier's conjecture, should satisfy $d_2 = d_3 = 1$, $d_w = d_{w-2} + d_{w-3}$. The upper-bound has been verified till order 9 in [17] and till order 12 by Hoang-Petitot [24] whose model conjecturally provides all identities. Consequently, all nonalternating MZV's (including double zetas) of "exceptional weights" $\{2, 3, 4, 5, 6, 7, 9\}$ reduce to zeta values.

II. Alternating zeta values: double ZV's defined by $\zeta^{-+}(a, b) = \sum_{m>n} \frac{(-1)^n}{m^a n^b}$.

(A_1) All alternating double zetas $\zeta^{-+}(p, q)$ of odd weight $w = p + q$ reduce to zeta values (Flajolet, Salvy [17, Thm. 7.2]):

$$2\zeta^{-+}(p, q) = (1 - (-1)^q) \zeta^{-}(p) \zeta^{-}(q) - \zeta^{-}(p+q) + 2(-1)^q \sum_k \left[\binom{p+q-2k-1}{p-1} \zeta^{-}(2k) \zeta^{-}(p+q-2k) + \binom{p+q-2k-1}{q-1} \zeta^{-}(2k) \zeta^{-}(p+q-2k) \right].$$

(A_2) All double zetas $\zeta^{-+}(1, q)$ reduce to zeta values (Sitaramachandrarao [40]):

$$2\zeta^{-+}(1, q) = -q\zeta(q+1) - 2\zeta^{-}(q+1) + \sum_{k=1}^q \zeta^{-}(k) \zeta^{-}(q+1-k).$$

(A_3) For weight 2, $\zeta^{-+}(1, 1) = -\frac{1}{2}(\log 2)^2$ (Euler; see [20]). For weight 4, a special reduction is known for $\zeta^{-+}(2, 2)$ in terms of zeta values augmented with $\text{Li}_4(1/2)$ (Sitaramachandrarao [40], De Doelder [15]). For weight 6, each of $\zeta^{-+}(2, 4)$, $\zeta^{-+}(3, 3)$, $\zeta^{-+}(4, 2)$, $\zeta^{-+}(5, 1)$ is expressible in term of any other one and zeta values. No such direct reductions seem to exist at weight 8 or higher. General relations are discussed in Borwein et al. [6].

FIGURE 4. A summary of known properties of double zeta values of type ζ^{++} and ζ^{-+} .

A relation between $\zeta^{-+}(3, 1)$ and $\text{Li}_4(1/2)$ is mentioned in [40] (see the formula preceding Eq. (1.2)). and proved by De Doelder in [15, p. 128]. Starting from the integral representation

$$\zeta^{-+}(3, 1) = -\frac{1}{2} \int_0^1 \log t \log^2(1+t) \frac{dt}{t},$$

De Doelder deduces

$$(18) \quad \zeta^{-+}(3, 1) = \frac{57}{64}\zeta(4) + \frac{7}{8}\zeta(3)\log(2) - \frac{\pi^2}{24}(\log 2)^2 + \frac{1}{24}(\log 2)^4 + \text{Li}_4\left(\frac{1}{2}\right),$$

which eventually relates the constant $\rho^{(2)}$ to the tetralogarithm.

We can state:

THEOREM 3. *The mean number $\bar{\rho}^{(2)}$ of comparisons in BCF-Sign can be expressed in terms of double zeta values as*

$$(19) \quad \begin{aligned} \bar{\rho}^{(2)} &= \frac{3}{4} + \frac{360}{\pi^4}\zeta^{-+}(2, 2) \equiv \frac{3}{4} + \frac{360}{\pi^4} \sum_{d=1}^{\infty} \frac{(-1)^d}{d^2} \sum_{c=1}^{d-1} \frac{1}{c^2} \\ &= 2 - \frac{720}{\pi^4}\zeta^{-+}(3, 1) \equiv 2 - \frac{720}{\pi^4} \sum_{d=1}^{\infty} \frac{(-1)^d}{d^3} \sum_{c=1}^{d-1} \frac{1}{c}, \end{aligned}$$

or with $\zeta(3)$ and the tetralogarithm $\text{Li}_4(\frac{1}{2})$,

$$(20) \quad \bar{\rho}^{(2)} = -\frac{60}{\pi^4} \left(24\text{Li}_4\left(\frac{1}{2}\right) - \pi^2(\log 2)^2 + 21\zeta(3)\log 2 + (\log 2)^4 \right) + 17.$$

Thus, $\bar{\rho}^{(2)}$ lies in the class \mathbf{P} of polynomial time computable constants and

$$\bar{\rho}^{(2)} = 1.35113\ 15744\ 91659\ 00179\ 38680\ 05256\ 46466\ 84404\ 78970\ 85087 \pm 10^{-50}.$$

In the case of values $\ell \geq 3$, the quantities $\bar{\rho}^{(\ell)}$ that intervene in the analysis of the sorting algorithm do not seem to reduce to known classical constants or to other simple sums like polylogarithmic values. The expressions of (16) show that everything depends on the status of the central zeta values $\zeta^{-+}(\ell, \ell)$. Since results appear scattered in the literature, we have compiled a summary table of what is known regarding the class of alternating double zetas of type ζ^{-+} in Figure 4. It is seen from this table that $\rho^{(3)}$ is expressible in terms of either one of the quantities $\zeta^{-+}(3, 3)$, $\zeta^{-+}(2, 4)$, $\zeta^{-+}(4, 2)$, $\zeta^{-+}(5, 1)$,

$$\begin{aligned} \bar{\rho}^{(3)} &= -\frac{31}{8} + \frac{2835}{\pi^6}\zeta(3)^2 + \frac{7560}{\pi^6}\zeta^{-+}(3, 3) = \dots \\ &= 18 - \frac{48195}{4\pi^6}\zeta(3)^2 + \frac{45360}{\pi^6}\zeta^{-+}(5, 1), \end{aligned}$$

so that 1000 terms of the last series $\zeta^{-+}(5, 1)$ suffice to determine

$$\bar{\rho}^{(3)} = 1.13662\ 64940 \pm 10^{-10}, \quad \text{and} \quad \bar{P}(3) = 4.69690\ 99648 \pm 10^{-10},$$

where the latter quantity is the mean cost of 3-sorting. However, simple polylogarithmic reductions cease to exist (probably) as soon $\ell \geq 3$ and alternative methods of evaluation must be sought.

Numerical calculation of $\bar{\rho}^{(\ell)}$. Regarding the numerical computation of the quantities $\bar{\rho}^{(\ell)}$ to high precision, Jon Borwein provides on his pages² efficient implementations that are visibly based on algorithms of *low* complexity (probably the

²URL: www.cecm.sfu.ca/projects/EZFace/

Euler-Maclaurin summation formula). More pragmatically, the `Pari-Gp` system includes an amazing command, `sumalt`, that is based on the general-purpose convergence acceleration process of Cohen-Villegas-Zagier [13] and gives very rapidly estimations of ζ^{-+} that appear to be in full agreement with the ones provided by Borwein's program.

Here is one *a priori* "reason" for the \mathbf{P} -character of multiple zeta values. It is closely related to investigations of the Chudnovsky brothers [10] and holds for a much wider class of constants. Following Zeilberger [52], define a function $f(z)$ analytic at the origin to be *holonomic* if it satisfies a linear differential equation with coefficients in $\mathbb{Q}(z)$. A constant that is the value $f(z_0)$ of a holonomic function at an algebraic point z_0 where $f(z)$ is regular (i.e., analytic, holomorphic) will be called a *regular holonomic constant*. Typical holonomic constants of the regular type are π , $\log 2$ or the polylogarithmic value $\text{Li}_4(1/2)$. Taylor coefficients of a holonomic function at any point satisfy linear recurrences with polynomial coefficients so that they can be determined fast and the function itself can be evaluated at high speed at any regular point that is an algebraic number (possibly using relays and analytic continuation). Consequently, all regular holonomic constants are in \mathbf{P} .

The simplest type of singularity for a linear ordinary differential equation is a Fuchsian singularity (also known as singularity of the first kind or "regular" singularity [50]). At such a point, singular expansions that mildly generalize standard power series expansions exist and are again computable fast by means of recurrences. Define a *singular holonomic constant* as the value of a holonomic function $f(z)$ at a point z_0 that is a singular point of the Fuchsian type for a defining equation. Then, previous arguments extend, and any singular holonomic constant is also in \mathbf{P} ; see [10]. A typical singular holonomic constant is $\zeta(3) = \text{Li}_3(1)$.

Any multiple zeta value is the value at ± 1 of a generating function that is holonomic and has radius of convergence 1. For instance, we have

$$\zeta^{-+}(a, b) = f(-1) \quad \text{where} \quad f(z) := \sum_{n=1}^{\infty} \frac{z^n}{n^a} H_{n-1}^b$$

satisfies the linear differential equation

$$\frac{d}{dz} \left(\frac{1-z}{z} \right) \left(z \frac{d}{dz} \right)^b \left(\frac{1-z}{z} \right) \left(z \frac{d}{dz} \right)^a f(z) = 0.$$

Therefore, any MZV is a holonomic constant. Membership of all MZV's in \mathbf{P} thus follows from general principles.

5. "Nonanalytic" lattice sums and the centred sign algorithm

In a beautiful paper [9] titled "Strange Series and High Precision Fraud", Jon and Peter Borwein present intriguing evaluations of various types of series. One of the highlights of that paper is the fact that the near-equality

$$(21) \quad \sum_{n=1}^{\infty} \frac{\lfloor n e^{\pi \sqrt{163/9}} \rfloor}{2^n} \doteq 1280640$$

is correct to at least half a billion digits, the difference between the two members of (21) being less than $10^{-500,000,000}$. Sums like (21) have a "nonanalytical" character due to the integer part function combined with irrational quantities, here present in the numerator. The moment sums of the centred continued fraction

system are of a similar nature, with terms determined by integer-part conditions appearing in the denominator. We present here ways of estimating them that build upon methods of [9] and make use of variations around lattice generating function, like

$$L_\theta(z) = \sum_{m \geq 1} z^{\lfloor m\theta \rfloor}.$$

The Borwein & Borwein constant (21) obtained by differentiation from some $L_\theta(z)$ are seen to be dual to the centred moment sums of (8) that result from iterated integration.

Examination of the basic and centred moment sums of (8) shows that these quantities are sums over *lattice cones*, where the lattice cone $\mathcal{C}(\beta, \gamma)$ is defined by

$$\mathcal{C}(\beta, \gamma) := \{(m, n) \in \mathbb{N}^2 \mid m\beta < n < m\gamma\}.$$

The basic continued fraction case corresponds to a cone $\mathcal{C}(1, 2)$ (or equivalently $\mathcal{C}(\frac{1}{2}, 1)$) and the centred case corresponds to a cone $\mathcal{C}(\phi, \phi^2)$ (or equivalently $\mathcal{C}(\phi^{-2}, \phi^{-1})$). In the latter case, what is involved in the lattice condition inherently involves the integer part function since, for an irrational θ , one has

$$m < n\theta \quad \text{if and only if} \quad m \leq \lfloor n\theta \rfloor.$$

It is a perhaps surprising fact that, despite their nonanalytical character, the centred moment sums $\hat{\rho}^{(\ell)}$ can be computed in polynomial time.

THEOREM 4. *Let $\theta < 1$ be an irrational number with sequence of continued fraction approximants $\{p_n/q_n\}_{n=0}^\infty$. One has for any integer $\ell \geq 1$*

$$(22) \quad \hat{\rho}^{(\ell)}(\theta) := \sum_{(p,q) \in \mathcal{C}(0,\theta)} \frac{1}{p^\ell q^\ell} = \sum_{n=0}^{\infty} \frac{(-1)^n}{(p_n + p_{n+1})^\ell (q_n + q_{n+1})^\ell} J_\ell\left(\frac{p_n}{p_n + p_{n+1}}, \frac{q_n}{q_n + q_{n+1}}\right)$$

where $J_s(\beta, \gamma)$ is defined for $0 < \beta, \gamma < 1$ and $\Re(s) > 1$ as

$$(23) \quad J_s(\beta, \gamma) := \frac{1}{\Gamma(s)^2} \int_0^1 \int_0^1 \frac{|\log x|^{s-1} |\log y|^{s-1}}{(1 - x^\beta y^\gamma)(1 - x^{1-\beta} y^{1-\gamma})} dx dy.$$

If θ is polynomial time computable, then $\hat{\rho}^{(\ell)}(\theta)$ is polynomial time computable for each integer value of ℓ . In particular, the average number of iterations of the CCF sign algorithm is in \mathbf{P} and it satisfies

$$\hat{\rho}^{(2)} \equiv \hat{\rho}^{(2)}\left(\frac{1}{\phi}\right) - \hat{\rho}^{(2)}\left(\frac{1}{\phi^2}\right) = 1.08922\,14740\,95380 \pm 10^{-15}.$$

The theorem follows from two types of developments: on the one hand, a simple combinatorial decomposition of lattice cones, on the other hand, a classical formula for iterated integrals.

First, we state a lemma drawn from the works of Borwein, Borwein, and Mahler, see [9], of which we propose a direct proof.

LEMMA 1. *Let $\theta < 1$ be an irrational number with convergents $\{p_n/q_n\}_{n=0}^\infty$. The generating function of the lattice cone $\mathcal{C}(0, \theta)$ is given by*

$$(24) \quad \sum_{(m,n) \in \mathcal{C}(0,\theta)} x^m y^n = \sum_{k=0}^{\infty} (-1)^k \frac{x^{q_k + q_{k+1}} y^{p_k + p_{k+1}}}{(1 - x^{q_k} y^{p_k})(1 - x^{q_{k+1}} y^{p_{k+1}})}.$$

PROOF. The sequence of convergents $\{p_n/q_n\}$ is such that the odd subsequence $\{p_{2n+1}/q_{2n+1}\}$ is decreasing, and the even sequence $\{p_{2n}/q_{2n}\}$ is increasing starting from $p_0/q_0 = 0$. Both have limit θ . Let $A + B$ and $A - B$ denote $A \cup B$ and $A \setminus B$. Then, for any irrational θ , the following decomposition holds

$$((0, \theta)) = \left(\frac{p_0}{q_0}, \frac{p_1}{q_1}\right) - \left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) + \left(\frac{p_2}{q_2}, \frac{p_3}{q_3}\right) - \dots = \sum (-1)^n \left(\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}\right)$$

between various sets of the form $((\beta, \gamma))$ defined as the intersection of the open interval (β, γ) with strictly positive rational of \mathbb{Q}^+ . A decomposition of the same type for integer open cones follows,

(25)

$$\mathcal{C}(0, \theta) = \mathcal{C}\left(\frac{p_0}{q_0}, \frac{p_1}{q_1}\right) - \mathcal{C}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) + \mathcal{C}\left(\frac{p_2}{q_2}, \frac{p_3}{q_3}\right) - \dots = \sum (-1)^n \mathcal{C}\left(\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}\right).$$

Now, the open interval $(p_n/q_n, p_{n+1}/q_{n+1})$ is the image of interval $]0, \infty[$ by the linear fractional transformation h defined as $h(x) := (p_n x + p_{n+1}) / (q_n x + q_{n+1})$. Since this LFT is of determinant ± 1 , this proves the equality

$$\mathcal{C}\left(\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}\right) = \mathcal{D} \begin{bmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{bmatrix},$$

where \mathcal{D} is defined by

$$\mathcal{D} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \left\{ (\lambda a + \mu b, \lambda c + \mu d) \mid \lambda, \mu \in \mathbb{N}, \lambda, \mu \geq 1 \right\}.$$

The generating function relative to $\mathcal{D} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is seen to be

$$\sum_{\lambda, \mu=1}^{\infty} x^{\lambda a + \mu b} y^{\lambda c + \mu d} = \frac{x^a y^c}{1 - x^a y^c} \frac{x^b y^d}{1 - x^b y^d},$$

and this identity combined with the decomposition (25) yields (24). \square

Next, a well-known formula for *iterated integration* relates power series and Dirichlet series:

$$(26) \quad \begin{aligned} \text{If } \phi(x, y) &= \sum_{p, q=1}^{\infty} \phi_{p, q} x^p y^q, \\ \text{then } \sum_{p, q=1}^{\infty} \frac{\phi_{p, q}}{p^s q^s} &= \frac{1}{\Gamma(s)^2} \int_0^{\infty} \int_0^{\infty} \phi(e^{-u}, e^{-v}) u^{s-1} v^{s-1} du dv. \end{aligned}$$

(Proof: Expand and integrate termwise!). When applied to (24), the integration formula (26) yields the two equations (22) and (23), upon the change of variables $x = e^{-u}$, $y = e^{-v}$ and proper rescaling.

Consider now integer values ℓ for the parameter s . First, we remark that

$$\begin{aligned} J_{\ell}(\beta, \gamma) &\leq \frac{1}{\beta(1-\beta)\gamma(1-\gamma)} H_{\ell} \\ \text{with } H_{\ell} &:= \frac{1}{\Gamma(\ell)^2} \int_0^1 \int_0^1 \frac{|\log(1-x)|^{\ell-1} |\log(1-y)|^{\ell-1}}{(x+y)^2} dx dy. \end{aligned}$$

Furthermore, H_{ℓ} is $O(1)$ for $\ell \rightarrow \infty$, and the convergents p_n, q_n are at least equal to the n -th Fibonacci number F_n so that the general term of the series in (22) is $O(\phi^{-2\ell n})$. This provides the geometrically convergent representation (22) for

$\widehat{\rho}^{(\ell)}(\theta)$. Full polynomial-time computability is formally established from there by observing that the integrands have easily computable series expansions that can be integrated termwise.

A mock Zeta function. We conclude this section with a mention of a few curious sums, simpler than $\widehat{\rho}^{(2)}$, that can be shown to lie in the class **P** by similar devices. For θ an arbitrary positive real ≥ 1 , define the “mock zeta function” by

$$(27) \quad \zeta_{\theta}(s) = \sum_{n=1}^{+\infty} \frac{1}{[n\theta]^s}, \quad \Re(s) > 1.$$

The basic generating function associated to the mock Zeta function, is closely related to the generating function of the cone $\mathcal{C}(0, 1/\theta)$. Using the relation (24), one finds easily for $\theta > 1$,

$$\sum_{m \geq 1} z^{[m\theta]} = \frac{z^{p_0}}{1 - z^{p_0}} - \frac{1 - z}{z} \sum_{n=0}^{\infty} (-1)^n \frac{z^{p_n}}{1 - z^{p_n}} \frac{z^{p_{n+1}}}{1 - z^{p_{n+1}}},$$

a relation that is due to Mahler. Then, via the formula for iterated integration in one variable, the mock zeta function is seen to admit the geometrically convergent representation

$$(28) \quad \zeta_{\theta}(s) = \frac{\zeta(s)}{[\theta]^s} - \frac{1}{\Gamma(s)} \sum_{n=0}^{\infty} \frac{(-1)^n}{p_n p_{n+1}^s} \int_0^{\infty} \Omega(t, p_{n+1}, \frac{p_n}{p_{n+1}}) t^{s-2} dt,$$

where

$$(29) \quad \Omega(t, p, \lambda) = \frac{e^{t/p} - 1}{t/p} \frac{t e^{-t}}{1 - e^{-t}} \frac{\lambda t e^{-\lambda t}}{1 - e^{-\lambda t}}.$$

This is the main tool for computing in polynomial time values of the mock zeta function at the integers. For instance, we obtain “quickly”

$$\zeta_{\phi}(2) := \sum_{n=1}^{\infty} \frac{1}{[n\phi]^2} = 1.29106\ 03681\ 14387\ 48950\ 47876 \pm 10^{-25}, \quad \phi = \frac{1 + \sqrt{5}}{2}.$$

6. Transfer operators and sign algorithms

In 1800, Gauss conjectured that repeated applications of the continued fraction transformation $\{1/x\}$ to a uniform real number over the interval $(0, 1)$ gives rise to a nonuniform number whose probability density is approximately

$$(30) \quad \overline{\psi}(x) = \frac{1}{\log 2} \frac{1}{1+x}.$$

Such a property, once supplemented with uniform convergence, says quite a bit about the stochastic behaviour of continued fraction representations of real numbers. For instance, the probability of observing a digit equal to d is in the asymptotic limit

$$\int_{1/(d+1)}^{1/d} \overline{\psi}(x) dx = \log_2 \frac{(d+1)^2}{d(d+2)}.$$

The situation is now well understood thanks to the works of Kuzmin, Lévy, and Wirsing, who defined the *density transformer* associated to the continued fraction

map

$$(31) \quad \overline{\mathcal{G}}[f](x) = \sum_{m=1}^{\infty} \frac{1}{(m+x)^2} f\left(\frac{1}{m+x}\right).$$

The characteristic property is that $\overline{\mathcal{G}}[f]$ describes the density of the transform of a random variable with density f by the continued fraction map \overline{U} . Gauss's assertion is then synonymous to

$$(32) \quad \overline{\mathcal{G}}^k[\mathbf{1}] \rightarrow \overline{\psi} \quad \text{as} \quad k \rightarrow +\infty,$$

since $\mathbf{1}$ is the density function of a uniform variate. The point of view has now been changed and problems concerning the metric theory of continued fractions are rephrased as questions regarding the functional-analytic properties of an (infinite dimensional) operator over some suitable function space. Spectral properties and eigenfunctions are obviously important objects in this perspective.

In the case of an arbitrary expanding map, with U the shift and \mathcal{H}_1 the set of inverse branches of depth 1, Ruelle introduced the *transfer operator* that depends on a (real or complex) parameter s ,

$$(33) \quad \mathcal{G}_s[f](x) = \sum_{h \in \mathcal{H}_1} |h'(x)|^s f \circ h(x),$$

and gives back the density transformer when $s = 1$. The interest of the extension is the increased descriptive power afforded by the extra parameter s . Here, we shall make use of the case $s = 2$ (the sign algorithm) and the case of a complex s (the sorting algorithm in Section 7).

For a general (analytic) expanding map, we assume from now on two conditions that supplement the axioms (E_1) and (E_2) of Section 1:

- (E_3) There exists a complex domain \mathcal{V} that contains \mathcal{I} where each inverse branch $h \in \mathcal{H}_1$ is analytic and satisfies $|h'(z)| \geq \delta > 1$.
- (E_4) The derivatives are summable in the sense that $\sum_{h \in \mathcal{H}_1} |h'(z)|^\eta < \infty$ for some fixed $\eta < 1$ and all z in \mathcal{V} .

Quite clearly, the transfer operator operates on space $A_\infty(\mathcal{V})$ formed with all functions f that are holomorphic in \mathcal{V} and continuous on the closed domain $\overline{\mathcal{V}}$. Endowed with the sup-norm, $A_\infty(\mathcal{V})$ is a Banach space. The operator \mathbf{G}_s is bounded for $\Re(s) > \eta$ and is also compact. (The argument uses the “selection principle” granted by Vitali's theorem and properties of normal families of functions; see [23, Ch. 15].) It follows by one of the most basic theorems of functional analysis [37] that the transfer operator has a discrete spectrum: the collection of its eigenvalues $\{\lambda_j(s)\}_{j=1}^\infty$ has no accumulation point, except 0. (More is known since Grothendieck's theory of nuclear spaces applies at full strength and the eigenvalues converge fast to zero in such a way that $\sum |\lambda_j(s)|^\varepsilon$ is summable for all $\varepsilon > 0$.) In addition, for a positive real value $s = \sigma$, the operator is in a strong sense positive; general Perron-Fronbenius properties [29] then imply that the dominant eigenvalue $\lambda_1(\sigma)$ (the one of largest modulus) is unique and simple, so that

$$\lambda_1(\sigma) > |\lambda_2(\sigma)| \geq |\lambda_3(\sigma)| \geq \dots \geq |\lambda_j(\sigma)| \rightarrow 0.$$

As a pleasant outcome of these properties, one can essentially treat the operator \mathcal{G}_σ as though it were simply a finite nonnegative matrix.

The properties specific to the transfer operator $\overline{\mathcal{G}}_s$ of the continued fraction map have been worked out by Dieter Mayer and by Babenko in a series of papers [2, 32,

33, 34]. In particular, these authors discovered the existence of a hidden Hilbert space structure resulting in the additional property that the $\bar{\lambda}_j(\sigma)$ are real for real σ . Building on their results, Hensley [21] was able to establish that the Euclidean gcd algorithm has an asymptotically Gaussian behaviour. In a different direction, the authors have demonstrated in [14, 19, 43, 45, 47] that the transfer operators can be put to use in order to analyse a variety of continued fraction algorithms.

The secant operators. For a general dynamical system, the transfer operator does not describe the moment sums $\sum_h u_h^\ell$, but a modified form due to Vallée [44] does. The *secant operator* \mathbf{G}_s is defined for complex numbers s satisfying $\Re(s) > \eta$ as

$$\mathbf{G}_s[F](x, y) = \sum_{|h|=1} \left| \frac{h(x) - h(y)}{x - y} \right|^s F(h(x), h(y)).$$

By the chain rule for secants, the iterate of order k is expressible in terms of all inverse branches of depth k

$$\mathbf{G}_s^k[F](x, y) = \sum_{|h|=k} \left| \frac{h(x) - h(y)}{x - y} \right|^s F(h(x), h(y)).$$

In particular, this identity specialized at $x = 0$ and $y = \alpha$ provides an alternative expression for the probability distribution of the cost of the sign algorithm given in (6):

$$\Pr(L \geq k + 1) = \mathbf{G}_2^k[\mathbf{1}](0, \alpha).$$

The secant operator extends Ruelle's transfer operator of (33) in the sense that "the diagonal of the secant is the tangent":

$$\mathbf{G}_s[F](x, x) = \mathcal{G}_s[f](x) \quad \text{where} \quad f(x) = F(x, x).$$

Here, asymptotic properties are needed, and they involve dominant spectral properties of the operator \mathbf{G}_s that are closely related to the corresponding ones for \mathcal{G}_s . The operator \mathbf{G}_s acts on the space $B_\infty(\mathcal{V})$ formed with all functions f that are holomorphic in the product $\mathcal{V} \times \mathcal{V}$ and continuous on the closed domain $\bar{\mathcal{V}} \times \bar{\mathcal{V}}$. Endowed with the sup-norm, $B_\infty(\mathcal{V})$ is a Banach space and the operator \mathbf{G}_s is bounded, and therefore compact (again by classical properties of bounded sequences of analytic functions). Its spectrum is thus discrete, with only an accumulation point at 0.

The spectrum of the secant operator \mathbf{G}_s is completely determined in [44]. In particular, when $s = \sigma$ is real, the dominant eigenvalue $\mu_1(\sigma)$ of \mathbf{G}_s is the same as the dominant eigenvalue $\lambda_1(\sigma)$ of \mathcal{G}_s while the subdominant eigenvalue $\mu_2(\sigma)$ satisfies $|\mu_2(\sigma)| < \mu_1(\sigma)$.

Such dominant spectral properties provide an asymptotic form for the iterates of Ruelle-Mayer operators where the k -th iterate of a positive function will have a regime dictated by $\lambda_1(\sigma)^k$ with an error term of the order of $\mu_2(\sigma)^k$. Specializing the discussion to moment sums, we thus find for the sign algorithm and an arbitrary analytic expanding map

$$\Pr(L \geq k + 1) \equiv \sum_{|h|=k} u_h^2 \equiv \mathbf{G}_2^k[\mathbf{1}](0, \alpha) = C\lambda_1(2)^k + O(\mu_2(2)^k).$$

Thus, for an arbitrary analytic expanding map, the sign algorithm exhibits an exponential decay of probabilities and the rate of decay is the dominant eigenvalue of the standard transfer operator \mathcal{G}_2 .

In the particular case of the basic continued fraction algorithm, we find, by methods discussed later in this section, a value $\bar{\lambda}_1(2) \approx 0.19945$ with at least 25 decimal places, and $\bar{\mu}_2(2) \approx -0.07573$; see (34) below. (The constant $\bar{\lambda}_1(2)$ is described under the name of “Vallée’s constant” in Finch’s repertoire of mathematical constants [16].) In the case of the centred algorithm, we estimate $\hat{\lambda}_1(2) \approx 0.07738$; see (35). These values explain quite well the empirical observations on the geometric decay of probabilities presented at the beginning of Section 3.

THEOREM 5. *The probability that the BCF–Sign Algorithm performs at least $k + 1$ iterations satisfies*

$$\Pr(\bar{L} \geq k + 1) = \bar{C} \bar{\lambda}_1(2)^k + O(\bar{\mu}_2(2)^k),$$

where $\bar{\lambda}_1(2) \approx 0.19945$ and $\bar{\mu}_2(2) \approx -0.07573$ are given by (34), $\bar{C} \approx 1.3$.

The probability that the CCF–Sign Algorithm performs at least $k + 1$ iterations satisfies

$$\Pr(\hat{L} \geq k + 1) = \hat{C} \hat{\lambda}_1(2)^k + O(\hat{\mu}_2(2)^k),$$

where $\hat{\lambda}_1(2) \approx 0.07738$ is given by (35), $|\hat{\mu}_2(2)| < \hat{\lambda}_1(2)$, and $\hat{C} > 0$.

Numerical estimates of the spectrum. We now describe a piece of experimental mathematics aimed at providing *inter alia* estimates on dominant and subdominant eigenvalues of the transfer operator \mathcal{G}_s in the particular case of the continued fraction algorithms. Let $\Pi_{m,a} f(z)$ be the operation (a “projection”) that selects the terms till order $m - 1$ inclusive in the Taylor expansion of the (analytic) function $f(z)$ at the point a . We introduce the truncated operators

$$\Pi_{m,a} \circ \mathcal{G}_s \circ \Pi_{m,a},$$

that is to say, we examine the effect of \mathcal{G}_s on initial segments of the Taylor expansion of functions. Such truncated operators are finite-dimensional. In the case of the continued fraction maps, their eigenvalues appear to convey quite a lot of information on the spectrum of the full operator \mathcal{G}_s while being accessible to numerical analysis.

The transform of a monomial x^m by a continued fraction transfer operator involves the Hurwitz zeta function that is classically defined by

$$\zeta(s, w) = \sum_{m=0}^{\infty} \frac{1}{(m + w)^s},$$

and is such that its Taylor expansion at a point a is expressible in terms of the collection of values $\zeta(s + j, a)$. Thus, viewed as acting on series expansions at $x = a$, the operator \mathcal{G}_s is expressed by an infinite matrix $M = (M_{i,j})$, where $M_{i,j}$ is the coefficient of $(x - a)^i$ in $\mathcal{G}_s[(x - a)^j]$. For instance, the BCF operator with $a = 0$ corresponds to the infinite matrix $(\bar{M})_{i,j}$ with

$$\bar{M}_{i,j} = (-1)^i \binom{2s + i + j - 1}{i} \zeta(2s + i + j),$$

and the infinite matrix for $s = 2$ starts as

$$\begin{bmatrix} \zeta(4) & \zeta(5) & \zeta(6) & \zeta(7) \\ -4\zeta(5) & -5\zeta(6) & -6\zeta(7) & -7\zeta(8) \\ 10\zeta(6) & 15\zeta(7) & 21\zeta(8) & 28\zeta(9) \\ -20\zeta(7) & -35\zeta(8) & -56\zeta(9) & -84\zeta(10) \end{bmatrix}$$

We now restrict attention to the basic continued fraction operator, and, guided by numerical experiments, adopt the value $a = 1/2$ that gives faster convergence. Using computer algebra, we have determined the eigenvalues of the truncated matrices $T^{[m]}$ for many values of $m \leq 100$ and numerical accuracy up to 200 digits. Examination of all the eigenvalues of these truncations reveals that most of them stabilize to a fixed set of definite values, with the occasional occurrence of some ghost values that eventually disappear as m increases. It is then natural to conjecture that the stable limit values do yield the complete spectrum of $\overline{\mathcal{G}}_s$.

We have developed a campaign of experiments based on the `Pari-Gp` and Maple systems (see [14] for an earlier account) in order to determine the spectrum of $\overline{\mathcal{G}}_1$ and $\overline{\mathcal{G}}_2$. It is based on the truncation principle and on the following three additional points.

- Examination of the first few values of the spectrum led us to conjecture that $\overline{\lambda}_j(\sigma)/\overline{\lambda}_{j+1}(\sigma)$ tends to $-\phi^{2\sigma}$. A heuristic reason is that the operator $\overline{\mathcal{G}}_s$ is in a sense (e.g., for large $s = \sigma$) “dominated” by its first term, which is a composition operator

$$\overline{\mathcal{C}}_s[f](x) = \frac{1}{(1+x)^s} f\left(\frac{1}{1+x}\right),$$

whose eigenfunctions and spectrum are explicit [39]. The surprise is that the approximation of the spectrum holds both for small values of σ ($\sigma = 1, 2$) and for large eigenvalue indices. This observation serves as a convergence accelerator as it enables one to filter out ghost eigenvalues, thereby making it possible to access smaller eigenvalues much faster.

- The traces of the continued fraction operators are computable in polynomial time, as shown in [14] by means of a multivariate version of Vardi’s “zeta summation trick” [48]. Filtered eigenvalues can then be confirmed by comparing with the trace $\text{Tr } \overline{\mathcal{G}}_s^2$ and this check is reliable since cancellations cannot occur for $s = \sigma$ as the spectrum is real, by virtue of the hidden Hilbert space structure [2, 32].
- For real $s = \sigma$, the estimate of the dominant eigenvalue $\overline{\lambda}_1(\sigma)$ at least can be *certified* thanks to a technique of “test functions” detailed in [14].

In this way, we have obtained highly convincing values for the first 37 eigenvalues of the basic operator $\overline{\mathcal{G}}_2$ with an accuracy almost certainly better than 10^{-25} . Here is a listing of our first estimates:

$$(34) \quad \begin{aligned} \overline{\lambda}_1(2) &\doteq +0.19945\ 88183\ 43767\ 26019\ 18456 \\ \overline{\lambda}_2(2) &\doteq -0.07573\ 95140\ 84360\ 60892\ 78089 \\ \overline{\lambda}_3(2) &\doteq +0.02856\ 64037\ 69818\ 52783\ 00174 \\ \overline{\lambda}_4(2) &\doteq -0.01077\ 74165\ 76612\ 69829\ 31408. \end{aligned}$$

The same process has also given us values of the spectrum when $s = 1$, including an estimate to more than 30 digits of accuracy of Wirsing’s constant $\overline{\lambda}_2(1)$ (that

dictates the speed on convergence to the stationary regime in (32)),

$$\bar{\lambda}_2(1) = -0.30366\ 30028\ 98732\ 65859\ 74481\ 21901 \pm 10^{-30}.$$

This has made it possible to correct some spurious values in Knuth's classic account of the subject [27]. Another application of detailed spectral estimates is the determination of Hensley's constant $H = \bar{\lambda}_1''(1)$ that expresses the variance of Euclid's algorithm, where we obtain:

$$H = 9.08037\ 31646 \dots$$

The spectrum of the centred operator $\widehat{\mathcal{G}}_2$ is at the moment less well understood. By the truncation method, we have found the dominant eigenvalue

$$(35) \quad \widehat{\lambda}_1(2) = +0.07738\ 53773\ 83629\ 09062\ 03319 \pm 10^{-25},$$

which can be certified by the already mentioned method of test functions. Some of the subdominant eigenvalues probably include values near

$$(36) \quad -0.00375\ 30752\ 61163\ 03856, \quad -0.00010\ 51799, \quad +0.00000\ 51256,$$

but the spectrum seems to obey a more complicated pattern than in the basic case.

The truncation technique being versatile enough, has also enabled Hensley [22] and Vallée [46] to determine numerically the Hausdorff dimension of various Cantor sets for continued fraction expansions.

7. Riemann hypothesis and sorting algorithms

We conclude this paper by examining the cost $\bar{P}(n)$ of sorting n uniform real numbers by means of the basic continued fraction algorithm. What is needed is a characterization of the asymptotic dependency of $\bar{P}(n)$ on n . The starting point is the exact expression of $P(n)$ provided by Theorem 2 as a difference of the moment sums $\rho^{(\ell)}$.

We make use here of a well-known fact of complex analysis: *Asymptotic properties of a number sequence are strongly related to singularities of an analytic function that extrapolates the number sequence.* In the case of finite differences, this principle is vindicated by the method of Nörlund-Rice integrals [18, 36]. Let f_n be a number sequence and $\phi(s)$ a holomorphic function that extrapolates the sequence f_n in the sense that $f_n = \phi(n)$. Then, the equality

$$(37) \quad R_n := \frac{1}{2i\pi} \int_L \phi(s) \frac{n!}{s(s-1)(s-2)\cdots(s-n)} ds = \sum_{k=1}^n \binom{n}{k} (-1)^{n-k} f_k,$$

holds, by virtue of the residue theorem, provided L is a simple contour that encircles the points $1, 2, \dots, n$ while avoiding the singularities of $\phi(s)$. What happens next is dependent upon $\phi(s)$ admitting a meromorphic continuation to the complex plane and being of moderate growth in right half-planes. Then, a shift of the contour till $\Re(s) = -T$ yields

$$(38) \quad R_n = - \sum_s \operatorname{Res} \left(\phi(s) \frac{n!}{s(s-1)\cdots(s-n)} \right),$$

where the sum is extended to all poles s of $\phi(s)$ in $\Re(s) > -T$. A simple pole of the integrand at some nonintegral point $s = s_0$ will for instance contribute a quantity

$$(39) \quad r_0 \frac{\Gamma(n+1)\Gamma(-s_0)}{\Gamma(n+1-s_0)} = r_0 \Gamma(-s_0) n^{s_0} \left(1 + O\left(\frac{1}{n}\right) \right).$$

Poles farther to the right induce “dominant” contributions, multiple poles introduce logarithmic terms (see [18] for details), and nonreal poles $s_0 = \sigma_0 + it_0$ lead to periodic fluctuations since

$$n^{s_0} = n^{\sigma_0 + it_0} = n^{\sigma_0} e^{it_0 \log n}.$$

This situation specializes to the case of the sorting cost as follows. We start from the integral representation induced by (37),

$$(40) \quad \frac{\overline{P}(n+1)}{n+1} = \frac{1}{2i\pi} \int_{1/2-i\infty}^{1/2+i\infty} \rho^{(s+1)} \frac{n!}{s(s-1)\cdots(s-n)} ds,$$

assuming that the moment sums of complex index $\rho^{(s+1)}$ exist. According to the principles expressed above, we thus need to determine the nature of the singularities of the integrand to the left of $\Re(s) = 1/2$, and more specifically when $\Re(s)$ lies in $(-\frac{3}{2}, \frac{1}{2})$.

Moment sums of complex index. The expressions stated earlier in (11) for $\rho^{(\ell)}$ with ℓ an integer clearly lift to complex values of s . In particular, we have for $\Re(s) > 1$

$$(41) \quad \rho^{(s)} = 2^{-s} - 2^{1-s} + (2^{s-1} - 1) \frac{\zeta(s)^2}{\zeta(2s)} + 2^s \frac{\zeta^{-+}(s, s)}{\zeta(2s)}$$

where ζ^{-+} is the alternating double zeta function of Section 4. The singularities arising from the zeta terms are apparent: there is a simple pole at $s = 1$ due to $\zeta(s)$ and there are poles at the zeros of the term $\zeta(2s)$ present in the denominator. So everything eventually rests on the nature of $\zeta^{-+}(s, s)$. For this function, Euler-Maclaurin summation implies that $\zeta^{-+}(s, s)$, like its simpler counterpart the alternating zeta function $\zeta^{-}(s)$, is an entire function. Furthermore, the identity

$$(42) \quad \zeta^{-+}(1, 1) = -\frac{1}{2}(\log 2)^2$$

is elementary and known since Euler’s time; see [20] and Figure 4.

Thus, $\rho^{(s)}$ is meromorphic for all s . The expansion of $\rho^{(s)}$ at $s = 1$ is then found by a simple calculation:

$$(43) \quad \rho^{(s)} = K_0 \frac{1}{s-1} + K + O(s-1),$$

with

$$K_0 = \frac{6 \log 2}{\pi^2}, \quad K = 12 \frac{\gamma \log 2}{\pi^2} + 9 \frac{(\log 2)^2}{\pi^2} - 72 \frac{\zeta'(2) \log 2}{\pi^4} - \frac{1}{2}.$$

The first order constant K_0 coincides with the inverse of Lévy’s entropic constant, that is, the entropy of the continued fraction map. The second order constant turns out to be a variant of Porter’s constant P defined classically by the constant term in the average number of steps of Euclid’s algorithm: we find by identification with the values listed in the reference site for constants [16] the equality

$$(44) \quad P = 2K - 2K_0 + \frac{1}{2}.$$

The other singularities of $\rho(s)$ in the critical strip $0 < \Re(s) < 1$ are those of the denominator $\zeta(2s)$. Each of them is at $1/2$ times a nontrivial zero of the Riemann zeta function. If such a zero is at $s_0 = \sigma + it$ and is simple, then, the contribution has an order given by (39). The details of contour surgery are easily supplied and

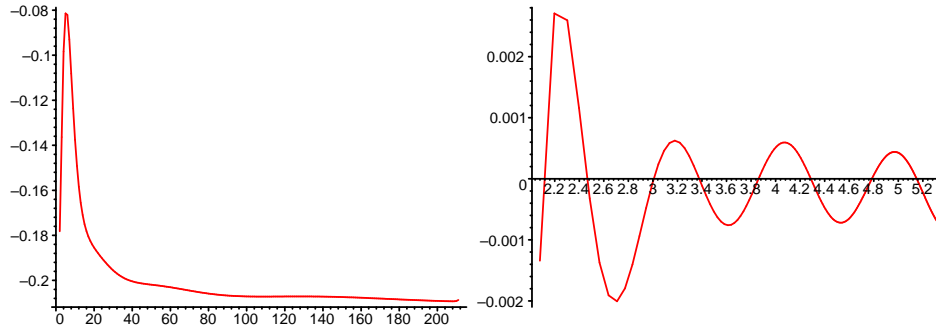


FIGURE 5. A plot (left) of $\bar{P}(n) - (K_0 n \log n + K_1 n)$ for $n = 2 \dots 200$ suggests a smooth convergence to a constant. A plot (bottom) of the empirically determined

$$P(n) - \left(K_0 n \log n + K_1 n - 0.21035 + \frac{0.365}{n} + \frac{2.02}{n^2} + \frac{13.5}{n^3} \right)$$

against $\log n$, for $n = 8 \dots 200$, reveals the first nontrivial zeros of $\zeta(s)$. In fact, both graphs represent functions that will eventually oscillate unboundedly between $-\infty$ and $+\infty$.

they are very similar to the ones used in Mellin transform asymptotics. See [18] or the treatment of sums of Gram, Ramanujan, Hardy-Littlewood, Riesz in analytic number theory [41, Ch. 14].

We then obtain:

THEOREM 6. *The expected cost of sorting n uniform real numbers given by their basic continued fraction representations satisfies*

$$\bar{P}(n) = K_0 n \log n + K_1 n + Q(n) + K_2 + o(1),$$

for constants $K_0, K_1, K_2 \in \mathbb{R}$, where K_0 is Lévy's entropic constant and K_1 is a Porter-like constant:

$$K_0 = \frac{6 \log 2}{\pi^2}, \quad K_1 = 18 \frac{\gamma \log 2}{\pi^2} + 9 \frac{(\log 2)^2}{\pi^2} - 72 \frac{\log 2 \zeta'(2)}{\pi^4} - \frac{1}{2}.$$

The function $Q(u)$ is an oscillating function with mean value 0 that satisfies

$$Q(n) = O(u^{\delta/2}),$$

where δ is any number such that

$$\delta > \sup \{ \Re(s) \mid \zeta(s) = 0 \}.$$

The overall shape of this result is given in [12] where the derivation was based on a technique of “Dirichlet depoissonization” and Mellin transforms. We add here an explicit determination of K_1 and a perhaps more straightforward approach to the asymptotic analysis via Nörlund-Rice integrals.

Comparing numerically $P(n)$ and the initial terms of its asymptotic expansion as given by Theorem 6 leads to interesting observations. Using Cohen-Villegas-Zagier acceleration of summation provided by `Pari-Gp` as discussed in Section 4, we have determined the exact values of $P(n)$ for $n = 2 \dots 220$ with at least 16 digits

of accuracy, which was achieved by determining the $\{\rho^{(\ell)}\}_{\ell=2}^{220}$ to about 100 digits of accuracy. First, in the given range, there is apparently a smooth convergence of $\overline{P}(n) - K_0 n \log n - K_1 n$ to a constant (reflecting K_2) that is near -0.2 ; see Figure 5 (left). By successive experimental adjustments—the process looks like restoring a blurred photograph in a crime fiction!—we are led to considering

$$(45) \quad B(n) = K_0 n \log n + K_1 n - 0.21035 + \frac{0.365}{n} + \frac{2.02}{n^2} + \frac{13.5}{n^3}.$$

For n in the interval $[8..220]$, the difference $\overline{P}(n) - B(n)$ then shows four slightly damped oscillations of minute amplitude that are between -0.002 and $+0.002$ and have a period slightly less than 1. However, we know that this difference must eventually tend to $\pm\infty$ with a regime of $O(n^{1/4})$ at least! The oscillations that are displayed in Fig. 5 (right) are reflexes of the nontrivial zeta zeros. In effect, corresponding to the first two nontrivial zeros at $z_0 = \frac{1}{2} \pm 14.13472i$, we have $|\Gamma(-z_0)| = 2.32 \cdot 10^{-5}$, so that the corresponding fluctuation has amplitude of the order of $10^{-4} n^{1/4}$ with an oscillating term similar to $\cos(2\pi \frac{\log n}{0.89})$. These facts match the numerical data quite well. In addition, due to the fast decay of the gamma function towards $\pm i\infty$, we estimate that any failure of the Riemann hypothesis could only be detected on $\overline{P}(n)$ for values of n well beyond the extraordinary bound of $10^{1,000,000,000}$ (see [12] for a discussion).

Constants and operators. The operator theory of Section 6 nicely completes the picture as regards the irruption of Lévy's entropic constant and of a Porter-like constant in Theorem 6. What happens is that the quantity $\rho^{(s)}$, which is the Dirichlet series of fundamental intervals, admits a representation as a quasi-inverse,

$$(46) \quad \rho^{(s)} = (I - \overline{\mathbf{G}}_s)^{-1}[\mathbf{1}](0, 1) = (I - \overline{\mathcal{G}}_s)^{-1} \left[\frac{1}{(1+x)^s} \right](0),$$

so that its pole at $s = 1$ must involve the derivative $\overline{\lambda}'(1)$ of the dominant eigenvalue function $s \rightarrow \overline{\lambda}(s)$ at $s = 1$ as its first order constant, while $\overline{\lambda}'(1)$ is otherwise known to equal the entropy of the continued fraction map as appears in K_0 . The quantity K is the second order constant in (43) and, under the operator framework (46), it must be related to derivatives of $\overline{\lambda}(s)$ and projectors at $s = 1$. The situation then parallels that of Euclid's algorithm where Porter's constant is also a second order constant at $s = 1$ in the expansion of another expression

$$(47) \quad \zeta(2s)(I - \overline{\mathcal{G}}_s)^{-1} \left[\frac{1}{(1+x)^{2s}} \right](0),$$

so that the relation between K and P is perhaps not totally unexpected.

We summarize in Fig. 6 the major constants encountered in the paper.

Open problems. We conclude this paper with a few open problems that we feel of interest.

(P_1) Why does Cohen-Villegas-Zagier acceleration work so well with the moment sums of the basic continued fraction system? It can apparently even be used to provide analytic continuation beyond the convergence region of double zeta values.

(P_2) Which of the alternating double zetas relate to other constants of analysis? What is the exact nature of relations with incomplete beta integrals, Nielsen-Ramanujan constants [16], and other polylogarithmic constants of [7]?

(P_3) Prove a version of the conjecture (Section 6) regarding the spectrum of the BCF operator $\overline{\mathcal{G}}_\sigma$.

Cost of <i>BCF</i> -sign	$\bar{\rho}^{(2)}$	1.35113 15744	\leftrightarrow double zeta $\zeta^{-+}(2, 2)$
Cost of <i>CCF</i> -sign	$\hat{\rho}^{(2)}$	1.08922 14740	Lattice sum
Prob. decay of <i>BCF</i> -sign	$\bar{\lambda}_1(2)$	0.19945 88183	Dominant eigenvalue of $\bar{\mathcal{G}}_2$
Prob. decay of <i>CCF</i> -sign	$\hat{\lambda}_1(2)$	0.07738 53773	Dominant eigenvalue of $\hat{\mathcal{G}}_2$
Sorting, 1st order (BCF)	K_0	0.42138 29566	\leftrightarrow Lévy's entropic constant
Sorting, 2nd order (BCF)	K_1	1.14815 08398	\leftrightarrow Porter's constant

FIGURE 6. The major constants encountered in the analysis of the sign and sorting algorithms.

(P_4) Why is the operator truncation method so effective (and obviously sound) for the *BCF* operator?

(P_5) Investigate theoretically and numerically the spectrum of the *CCF* operator $\hat{\mathcal{G}}_\sigma$.

(P_6) Explain the occurrence of Porter's constant in the analysis of sorting. In other words, is there some direct relation between sorting and the GCD algorithm, as possibly suggested by (46) and (47)?

(P_7) Analyse the limit distribution of characteristic parameters of the continued fraction fraction sorting algorithm. Candidates are path length, depth of nodes, and number of nodes; see [12] for what is currently known (e.g., height). In view of what exists for binary tries (the Jacquet-Régnier theorems [31]), we expect Gaussian laws for these parameters.

References

- [1] F. Avnaim, J.-D. Boissonnat, O. Devillers, F. P. Preparata, and M. Yvinec, *Evaluating signs of determinants using single-precision arithmetic*, *Algorithmica* **17** (1997), no. 2, 111–132.
- [2] K. I. Babenko, *On a problem of Gauss*, *Soviet Mathematical Doklady* **19** (1978), no. 1, 136–140.
- [3] David H. Bailey, Jonathan M. Borwein, and Roland Girgensohn, *Experimental evaluation of Euler sums*, *Experimental Mathematics* **3** (1994), no. 1, 17–30.
- [4] M. Beeler, R. W. Gosper, and R. Schroepfel, *HAKMEM*, Memorandum 239, M.I.T., Artificial Intelligence Laboratory, February 1972, Available on the WorldWide Web at <http://www.inwap.com/pdp10/hbaker/hakmem/hakmem.html>.
- [5] Bruce C. Berndt, *Ramanujan's notebooks, part I*, Springer Verlag, 1985.
- [6] David Borwein, Jonathan Borwein, and Roland Girgensohn, *Explicit evaluation of Euler sums*, *Proceedings of the Edinburgh Mathematical Society* **38** (1995), 277–294.
- [7] Jonathan Borwein, David Bradley, David Broadhurst, and Petr Lisonek, *Special values of multiple polylogarithms*, *Transactions of the American Mathematical Society* (1998), To appear.
- [8] Jonathan M. Borwein and Peter B. Borwein, *Pi and the AGM*, John Wiley, 1987.
- [9] ———, *Strange series and high precision fraud*, *American Mathematical Monthly* **99** (1992), no. 7, 622–640.
- [10] David V. Chudnovsky and Gregory V. Chudnovsky, *Computer algebra in the service of mathematical physics and number theory*, *Computers in mathematics* (Stanford, CA, 1986) (New York), Dekker, New York, 1990, pp. 109–232.
- [11] Julien Clément, *Analyse en moyenne des tries basés sur la numération en fraction continue*, Mémoire de DEA, 1996.
- [12] Julien Clément, Philippe Flajolet, and Brigitte Vallée, *Dynamical sources in information theory: A general analysis of trie structures*, Research Report 3645, Institut National de Recherche en Informatique et en Automatique, March 1999, 61 pages. To appear in *Algorithmica*, 1999.

- [13] Henri Cohen, Fernando Rodriguez Villegas, and Don Zagier, *Convergence acceleration of alternating series*, Preprint, 1999, To appear in *Experimental Mathematics*.
- [14] Hervé Daudé, Philippe Flajolet, and Brigitte Vallée, *An average-case analysis of the Gaussian algorithm for lattice reduction*, *Combinatorics, Probability and Computing* **6** (1997), no. 4, 397–433.
- [15] P. J. De Doelder, *On some series containing $\psi(x) - \psi(y)$ and $(\psi(x) - \psi(y))^2$ for certain values of x and y* , *Journal of Computational and Applied Mathematics* **37** (1991), 125–141.
- [16] Steven Finch, *Favorite mathematical constants*, Available under World Wide Web at <http://www.mathsoft.com/asolve/constant/constant.html>, 1995.
- [17] Philippe Flajolet and Bruno Salvy, *Euler sums and contour integral representations*, *Experimental Mathematics* **7** (1998), no. 1, 15–35.
- [18] Philippe Flajolet and Robert Sedgewick, *Mellin transforms and asymptotics: finite differences and Rice's integrals*, *Theoretical Computer Science* **144** (1995), no. 1–2, 101–124.
- [19] Philippe Flajolet and Brigitte Vallée, *Continued fraction algorithms, functional operators, and structure constants*, *Theoretical Computer Science* **194** (1998), no. 1–2, 1–34.
- [20] Eldon R. Hansen, *A table of series and products*, Prentice-Hall, 1975.
- [21] Doug Hensley, *The number of steps in the Euclidean algorithm*, *Journal of Number Theory* **49** (1994), no. 2, 142–182.
- [22] ———, *A polynomial time algorithm for the Hausdorff dimension of continued fraction Cantor sets*, *Journal of Number Theory* **58** (1996), no. 1, 9–45.
- [23] E. Hille, *Analytic function theory*, Blaisdell Publishing Company, Waltham, 1962, 2 Volumes.
- [24] Hoang Ngoc Minh and Michel Petitot, *Lyndon words, polylogarithms, and the Riemann zeta function*, *Discrete Mathematics* (1997), To be published.
- [25] A. Hurwitz, *Über eine besondere Art der Kettenbruch-Entwicklung reeller Grössen*, *Advances in Mathematics* **12** (1889), 367–405.
- [26] Donald E. Knuth, *The art of computer programming*, vol. 3: Sorting and Searching, Addison-Wesley, 1973.
- [27] ———, *The art of computer programming*, 2nd ed., vol. 2: Seminumerical Algorithms, Addison-Wesley, 1981.
- [28] ———, *Metafont the program*, Addison Wesley, Reading, Massachusetts, 1986, Volume D of *Computers and Typesetting*.
- [29] M. Krasnoselskii, *Positive solutions of operator equations*, P. Noordhoff, Groningen, 1964.
- [30] L. Lewin (ed.), *Structural properties of polylogarithms*, American Mathematical Society, 1991.
- [31] Hosam Mahmoud, *Evolution of random search trees*, John Wiley, New York, 1992.
- [32] D. Mayer and G. Roepstorff, *On the relaxation time of Gauss's continued fraction map. I. The Hilbert space approach*, *Journal of Statistical Physics* **47** (1987), no. 1/2, 149–171.
- [33] ———, *On the relaxation time of Gauss's continued fraction map. II. The Banach space approach (transfer operator approach)*, *Journal of Statistical Physics* **50** (1988), no. 1/2, 331–344.
- [34] Dieter H. Mayer, *On a ζ function related to the continued fraction transformation*, *Bulletin de la Société Mathématique de France* **104** (1976), 195–203.
- [35] Niels Nielsen, *Die Gammafunktion*, Chelsea Publishing Company, New York, 1965, Reprinted from *Handbuch der Theorie der Gammafunktion* (1906) and *Theorie der Integrallogarithmus und verwandter Transzendenten* (1906).
- [36] Niels Erik Nörlund, *Vorlesungen über Differenzenrechnung*, Chelsea Publishing Company, New York, 1954.
- [37] Frigyes Riesz and Béla Sz.-Nagy, *Functional analysis*, Dover, 1990, A reprint of the 1955 edition, Ungar Publishing Company.
- [38] David Ruelle, *Dynamical zeta functions for piecewise monotone maps of the interval*, CRM Monograph Series, vol. 4, American Mathematical Society, Providence, 1994.
- [39] Joel H. Shapiro, *Composition operators and classical function theory*, Springer-Verlag, New York, 1993.
- [40] R. Sitaramachandrarao, *A formula of S. Ramanujan*, *Journal of Number Theory* **25** (1987), 1–19.
- [41] E. C. Titchmarsh and D. R. Heath-Brown, *The theory of the Riemann zeta-function*, second ed., Oxford Science Publications, 1986.

- [42] Brigitte Vallée, *Algorithms for computing signs of 2×2 determinants: dynamics and average-case analysis*, Lecture Notes in Computer Science, no. 1136, 1997, Proceedings of the Fifth European Symposium on Algorithms, Graz, September 1997., pp. 486–499.
- [43] ———, *Opérateurs de Ruelle-Mayer généralisés et analyse en moyenne des algorithmes d'Euclide et de Gauss*, Acta Arithmetica **81** (1997), no. 2, 101–144.
- [44] ———, *Dynamical sources in information theory: Fundamental intervals and word prefixes*, Les cahiers du GREYC, Université de Caen, 1998, 32p. To appear in *Algorithmica*, 1999.
- [45] ———, *Dynamics of the binary Euclidean algorithm: Functional analysis and operators*, Algorithmica **22** (1998), no. 4, 660–685.
- [46] ———, *Dynamique des fractions continues à contraintes périodiques*, Journal of Number Theory **72** (1998), no. 2, 183–235.
- [47] ———, *A unifying framework for the analysis of a class of Euclidean algorithms*, Preprint, 2000, To appear in *Proceedings of LATIN'2000, Lecture Notes in Computer Science*, in press.
- [48] Ilan Vardi, *Computational recreations in Mathematics*, Addison Wesley, 1991.
- [49] Jean Vuillemin, *Exact real computer arithmetic with continued fractions*, IEEE Transactions on Computers **39** (1990), no. 8, 1087–1105.
- [50] W. Wasow, *Asymptotic expansions for ordinary differential equations*, Dover, 1987, A reprint of the John Wiley edition, 1965.
- [51] Don Zagier, *Values of zeta functions and their applications*, Proceedings of the First European Congress of Mathematics, Paris (A. Joseph et al., ed.), vol. II, Birkhäuser Verlag, 1994, (Progress in Mathematics, volume 120.), pp. 497–512.
- [52] Doron Zeilberger, *A holonomic approach to special functions identities*, Journal of Computational and Applied Mathematics **32** (1990), 321–368.

INRIA, ROCQUENCOURT, F-78150 LE CHESNAY (FRANCE)
E-mail address: Philippe.Flajolet@inria.fr

DÉPARTEMENT D'INFORMATIQUE, UNIVERSITÉ DE CAEN, F-14032 CAEN (FRANCE)
E-mail address: Brigitte.Vallee@info.unicaen.fr