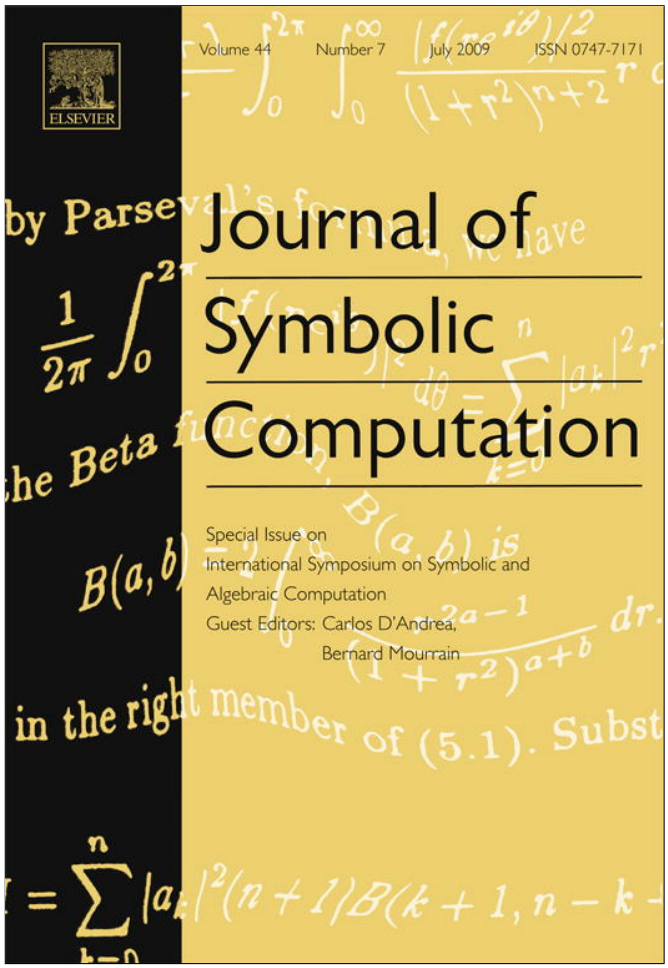
Provided for non-commercial research and education use.
Not for reproduction, distribution or commercial use.



This article appeared in a journal published by Elsevier. The attached copy is furnished to the author for internal non-commercial research and education use, including for instruction at the authors institution and sharing with colleagues.

Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.

In most cases authors are permitted to post their version of the article (e.g. in Word or Tex form) to their personal website or institutional repository. Authors requiring further information regarding Elsevier's archiving and manuscript policies are encouraged to visit:

http://www.elsevier.com/copyright

Author's personal copy

Journal of Symbolic Computation 44 (2009) 726–767

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

Regularity of the Euclid Algorithm; application to the analysis of fast GCD Algorithms☆

Eda Cesaratto[a,b], Julien Clément[a], Benoît Daireaux[c], Loïck Lhote[a], Véronique Maume-Deschamps[d], Brigitte Vallée[a]

[a] *GREYC, UMR CNRS 6072, Université de Caen and ENSICAEN, Caen, France*

[b] *Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) and Instituto de Desarrollo Humano, Universidad Nacional de Gral. Sarmiento, Buenos Aires, Argentina*

[c] *IrisResearch Center, Stavanger, Norway*

[d] *ISFA, Université de Lyon, Université de Lyon 1, Lyon, France*

ARTICLE INFO

Article history:
Received 29 November 2007
Accepted 25 April 2008
Available online 8 October 2008

Keywords:
Euclid algorithm
Divide and conquer algorithms
Fast multiplication
Analysis of algorithms
Transfer operators
Perron formula

ABSTRACT

There exist fast variants of the gcd algorithm which are all based on principles due to Knuth and Schönhage. On inputs of size n, these algorithms use a Divide and Conquer approach, perform FFT multiplications with complexity $\mu(n)$ and stop the recursion at a depth slightly smaller than $\lg n$. A rough estimate of the worst-case complexity of these fast versions provides the bound $O(\mu(n)\log n)$. Even the worst-case estimate is partly based on heuristics and is not actually proven. Here, we provide a precise probabilistic analysis of some of these fast variants, and we prove that their average bit-complexity on random inputs of size n is $\Theta(\mu(n)\log n)$, with a precise remainder term, and estimates of the constant in the Θ-term. Our analysis applies to any cases when the cost $\mu(n)$ is of order $\Omega(n\log n)$, and is valid both for the FFT multiplication algorithm of Schönhage–Strassen, but also for the new algorithm introduced quite recently by Fürer [Fürer, M., 2007. Faster integer Multiplication. In: Proceedings of STOC'07. pp. 57–66]. We view such a fast algorithm as a sequence of what we call interrupted algorithms, and we obtain two main results about the (plain) Euclid Algorithm, which are of independent interest. We precisely describe the evolution of the distribution of numbers during the execution of the (plain) Euclid Algorithm, and we exhibit

☆ This research was partly supported by the project SADA of the French ANR.
E-mail addresses: ecesarat@ungs.edu.ar (E. Cesaratto), julien.clement@info.unicaen.fr (J. Clément), Benoit.Daireaux@irisresearch.no (B. Daireaux), loick.lhote@info.unicaen.fr (L. Lhote), veronique.maume@univ-lyon1.fr (V. Maume-Deschamps), brigitte.vallee@info.unicaen.fr (B. Vallée).

0747-7171/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2008.04.018

Author's personal copy

an (unexpected) density ψ which plays a central rôle since it always appears at the beginning of each recursive call. This strong regularity phenomenon proves that the interrupted algorithms are locally "similar" to the total algorithm. This ultimately leads to the precise evaluation of the average bit-complexity of these fast algorithms. This work uses various tools, and is based on a precise study of generalised transfer operators related to the dynamical system underlying the Euclid Algorithm.

© 2008 Elsevier Ltd. All rights reserved.

1. Introduction

Gcd computation is a widely used routine in computations on long integers. It is omnipresent in rational computations, public key cryptography or computer algebra. Many gcd algorithms have been designed since Euclid. Most of them compute a sequence of remainders by successive division, which leads to algorithms with a quadratic bit-complexity (in the worst-case as well as in the average-case). Using Lehmer's ideas (1938) (which replace large divisions by large multiplications and small divisions), computations can be speeded-up by a constant factor, but the asymptotic complexity remains quadratic. Major improvements in this area are due to Knuth (1971), who designed the first subquadratic algorithm in 1970, and to Schönhage (1971) who subsequently improved it the same year. They use Divide and Conquer techniques combined with Lehmer's ideas to compute in a recursive way the quotient sequence (whose total size is $O(n)$). Moreover, if a fast multiplication with subquadratic complexity (FFT, Karatsuba…) is performed, then one obtains a subquadratic gcd algorithm (in the worst-case). Such a methodology has been recently used by Stehlé and Zimmermann (2004) to design a Least-Significant-Bit version of the Knuth–Schönhage algorithm. According to experiments due to Cesari (1998) and Möller (2008), these algorithms (with an FFT multiplication) become efficient only for integers of size larger than 10 000 words, whereas, with Karatsuba multiplication, they become efficient for smaller integers (around 100 words). A precise description of the Knuth–Schönhage algorithm can be found in Yap (1996) and Möller (2008) for instance.

1.1. Previous results

The average-case behaviour of the quadratic gcd algorithms is now well understood. First results are due to Heilbronn (1969) and Dixon (1970) in the seventies, who studied for the first time the mean number of iterations of the Euclid Algorithm. Then Brent analysed the Binary algorithm (Brent, 1976), and Hensley (1994) provided the first distributional analysis for the number of steps of the Euclid Algorithm. Since 1995, the Caen Group (Vallée, 2003, 2000, 2006) and its collaborators have performed an average-case analysis of various parameters of a large class of Euclidean algorithms. More recently, distributional results have also been obtained for the Euclid algorithm and some of its variants: first Baladi and Vallée prove that a whole class of so-called additive costs of moderate growth follows an asymptotic Gaussian law (Baladi and Vallée, 2005) (for instance, the number of iterations, the number of occurrences of a given digit, and so on…). In 2006, Lhote and Vallée (2006, 2008) showed that a more general class of parameters also follows an asymptotic Gaussian law. This class contains the length of a remainder at a fraction of the execution, and the bit-complexity. To the best of our knowledge, there are yet few results on "efficient" gcd algorithms. In Daireaux and Vallée (2004), the authors perform an average-case analysis of Lehmer's algorithm, and exhibit the average speed-up obtained using these techniques. However, as far as we know, there does not exist any probabilistic analysis of subquadratic gcd algorithms. It is the goal of this paper to perform such a study.

An extended abstract (12 pages) which contains the main results of this paper, without proofs, has appeared in the Proceedings of the ANALCO-ALENEX conference (a satellite conference of the SODA conference) in January 2007.

Author's personal copy

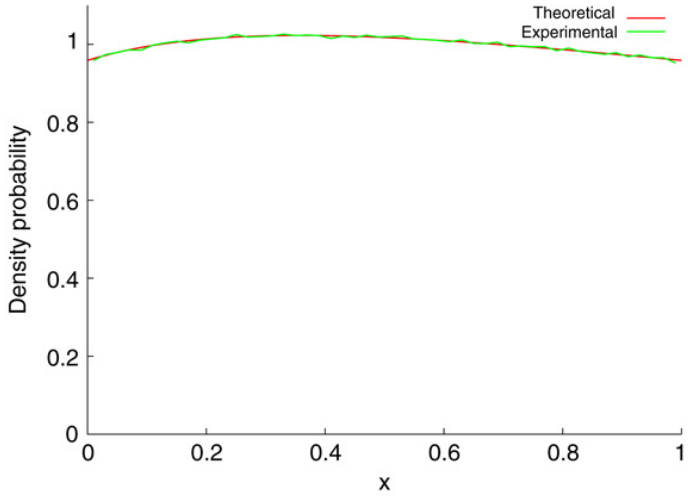


Fig. 1. Density distribution of $x_{\langle\delta\rangle}$ in the case $\delta = 1/2$, corresponding to the density distribution of the rational $x_k := A_{k+1}/A_k$ obtained as soon as $\ell(A_k)$ is smaller than $(1/2)\ell(A_0)$. The diagram compares Monte-Carlo simulations with the exact value of $\psi(x)$. For simulations, we consider 3 537 944 rationals with 48 bits, drawn according to the Gauss density φ. For estimating the density, the interval [0, 1] is subdivided into equal subintervals of length 1/50.

1.2. Our results

There are two algorithms to be analysed: the $\mathcal{HG}$ algorithm and the $\mathcal{G}$ algorithm. The $\mathcal{G}$ algorithm computes the gcd, and the $\mathcal{HG}$ algorithm (for "half-gcd" Algorithm) only simulates the "first half" of the $\mathcal{G}$ algorithm. We first show that these algorithms can be viewed as a sequence of the so-called Interrupted Euclidean algorithms. An Interrupted Euclidean algorithm is a subsequence formed by successive iterations of the plain algorithm, as we now explain: On an input (A, B), the plain Euclid algorithm builds a sequence of remainders A_i, a sequence of quotients Q_i, and a sequence of matrices $\mathcal{M}_i$ [see Section 2.1]. On an input (A, B) of binary size n, the Interrupted Euclidean algorithm $\mathcal{E}_{[\delta,\delta+\gamma]}$ starts at the index k of the execution of the Euclid Algorithm, as soon as the remainder A_k has already lost $\delta\, n$ bits (with respect to the initial A which has n bits) and stops at index $k + i$ as soon as the remainder A_{k+i} has lost $\gamma\, n$ additional bits (with respect to the remainder A_k). The $\mathcal{HG}$ algorithm just simulates the interrupted algorithm $\mathcal{E}_{[0,1/2]}$. A quite natural question is: how many iterations are necessary to lose these $\gamma\, n$ bits? Of course, it is natural to expect that this subsequence of the Euclidean algorithm is just locally similar to the "total" Euclidean Algorithm; in this case, the number of iterations would be close to $\gamma\, P$ (where P is the number of iterations of the "total" Euclid algorithm). We prove in Theorem 1 that this is indeed the case: This is why we say that the algorithm is "regular".

For a probabilistic study of fast variants, a precise description of the evolution of the distribution during the execution of the plain Euclid Algorithm is of crucial interest. For real inputs, we know that the continued fraction algorithm does not terminate (except for rationals …). Moreover, as the continued fraction algorithm is executed, the distribution of reals tends to the distribution associated to the Gauss density φ, defined as

$$\varphi(x) = \frac{1}{\log 2}\frac{1}{1+x}. \tag{1}$$

For rational inputs, we begin with a given distribution on the set of the inputs $x := A_1/A_0$ of size n, and we consider the rationals $x_k := A_{k+1}/A_k$. We focus on the first index k where the binary size of x_k is less than $(1-\delta)n$ and we denote the corresponding rational x_k by $x_{\langle\delta\rangle}$. What is the distribution of the rational $x_{\langle\delta\rangle}$? The evolution of this distribution is clearly more intricate than in the real case, since at the end of the Algorithm (when $\delta = 1$), the distribution is the Dirac measure at $x = 0$. We obtain here a precise description of this distribution (see Theorem 2 and Fig. 1) which surprisingly involves the density function

$$\psi(x) := \frac{12}{\pi^2}\sum_{m\geq 1}\frac{\log(m+x)}{(m+x)(m+x+1)}. \tag{2}$$

Author's personal copy

One of our referees writes: "The authors find the result surprising, but there is an heuristic explanation for it. Suppose one is riding various horses, some fast and some slow, on a long race, switching once a minute to a random new horse. What horse will you be riding when you cross the finish line? Probably, a fast one! Chasing down the quantitative consequences of this idea, weighting the horses in proportion to their speed, and then thinking of horses as integers Q that would express the size of the step $(A_k, A_{k-1}) \to (A_{k-1} - QA_k, A_k)$, one arrives at the authors' $\psi(x)$ density."

We also need precise results on the distribution of some truncations of remainders. This is done in Theorem 3. Then, the choice of parameters in the fast algorithms must take into account this evolution of distribution. This is why we are led to introduce some variants of the classical algorithms, denoted by $\underline{\mathcal{HG}}$ and $\underline{\mathcal{G}}$ for which the precise analysis can be performed.

The fast versions also involve other functions, which are called the Adjust functions. Such functions perform a few steps of the (plain) Euclid Algorithm. However, the bit-complexity of the Adjust functions depends on the size of the quotients which are computed during these steps. Even for estimating the worst-case complexity of the fast variants, the Adjust functions are not precisely analysed. The usual argument is "The size of a quotient is $O(1)$". Of course, this assertion is false in the worst-case, and only (perhaps) true on average, provided that the distribution on input pairs be made precise. Moreover, the Adjust functions are related to some specific steps, which happen just when the pairs have lost a fraction of their bits. We are then led to study the mean value of the size of the quotients computed at these specific steps, and we prove that it is asymptotic to a constant η which is defined in (20). And, we also need this type of result for our truncated data. This is covered by Theorem 4.

There are now two main fast multiplication algorithms, both based on FFT principles. We consider in fact a whole class of possible fast multiplication algorithms, for which the following is true:

There exist a function $a(n)$ satisfying[1] $a(n) = O(\log\log n)$, $a(n) = \Omega(1)$ *and two constants A_1, A_2 (probably large) such that, for any pair of integers u, v whose respective sizes satisfy $\ell(u) = n$ and $\ell(v) = Kn$ for some integer K, the bit-cost $M(u, v)$ of the product between two numbers u and v satisfies*

$$A_1\, K\, \mu(n) \le M(u, v) \le A_2\, K\, \mu(n) \qquad \text{with} \quad \mu(n) = a(n) n \log n. \tag{3}$$

In particular, Fürer proved this year (Fürer, 2007) that it is possible to choose $a(n) = 2^{O(\log^\star n)}$, and improves the previous function $a(n) = \log\log n$, due to Schönhage and Strassen.[2]

Such a fast multiplication also leads to a fast division:

There exist two constants A_3, A_4 (larger than A_1, A_2) such that, for any pair of integers u, v whose respective sizes satisfy $\ell(u) = n$ and $\ell(v) = Kn$ for some integer $K > 1$, the bit-cost $D(u, v)$ of the division between two numbers v and u satisfies[3]

$$A_3\, (K-1)\, \mu(n) \le D(v, u) \le A_4\, (K-1)\, \mu(n) \qquad \text{with} \quad \mu(n) = a(n) n \log n. \tag{4}$$

Finally, we obtain the exact average-case complexity of our versions of the two main algorithms of interest, the $\underline{\mathcal{HG}}$ algorithm, and the $\underline{\mathcal{G}}$ algorithm itself. When they use a fast multiplication which satisfies (3) and a fast division which satisfies (4), we prove the following estimates [Theorems 6 and 7] for the average bit-complexity B, G of both algorithms, on the set of random inputs of size n:

$$\mathbb{E}_n[B] = \Theta(1)\, n(\log n)^2\, a(n) \left[1 + O\left(\frac{1}{a(n)}\right)\right],$$

$$\mathbb{E}_n[G] = \Theta(1)\, n\, (\log n)^2\, a(n) \left[1 + O\left(\frac{1}{a(\sqrt{n}\log n)}\right)\right].$$

[1] The notation $f = \Omega(g)$ means that there exists $B > 0$ such that, for n large enough, $f_n \ge B g_n$, and the notation $f = \Theta(g)$ means that $f = \Omega(g)$ and $f = O(g)$.

[2] The function $\log^\star$ denotes the iterated logarithm function, that is $\log^\star(n)$ denotes the number of times the logarithm function must be iteratively applied before the result is less than or equal to 1.

[3] In this case $(K-1)n$ is the size of the quotient.

Author's personal copy

Furthermore, we obtain precise information about the Θ-term, which involves two types of constants: first, the constants A_1, A_2, A_3, A_4, which intervene in the cost of the multiplication and the division [see (3) and (4)], second, together with the density ψ defined in (2), another mysterious "spectral" constant σ (defined in Section 1.3). Our proven average bit-complexity of the $\underline{\mathcal{HG}}$, $\underline{\mathcal{G}}$ algorithms then appears to be of the same order as the usual (heuristic) bound on the worst-case complexity of $\mathcal{HG}$, $\mathcal{G}$ algorithms.

1.3. Methods

Even if our main conclusions obtained here are "expected", and certainly will not surprise the reader, the irruption of the density ψ defined in (2) is unexpected, and an actual proof of this phenomenon is not straightforward. This is due to the fact that there are correlations between successive steps of the Euclid Algorithm. Accordingly, the tools which are usual in analysis of algorithms (Flajolet and Sedgewick, in press), such as generating functions, are not well-suited in this case. All the analyses which will be described here are instances of the dynamical analysis paradigm, where the algorithm is seen as a dynamical system. Then, the analysis uses, together with generating functions, the transfer operator of the underlying dynamical system as a main tool. Here, the transfer operator $\mathbf{H}_s$ relative to the Euclidean dynamical system is

$$\mathbf{H}_s[f](x) := \sum_{m\geq 1} \frac{1}{(m+x)^{2s}} f\left(\frac{1}{m+x}\right), \tag{5}$$

and the Gauss density φ defined in (1) is just the unique density fixed by $\mathbf{H} := \mathbf{H}_1$, whereas one of the main objects of this paper, the density ψ, is proportional to

$$\mathbf{H}'[\varphi], \qquad \text{with} \quad \mathbf{H}' := \frac{\mathrm{d}}{\mathrm{d}s}\mathbf{H}_s|_{s=1}.$$

The present paper mainly uses two previous works, and can be viewed as an extension of them: first, the average-case analysis of the Lehmer–Euclid algorithm performed in Daireaux and Vallée (2004); second, the distributional methods described in Baladi and Vallée (2005) and Lhote and Vallée (2008). First, we again use the general framework that Daireaux and Vallée have developed for the analysis of the Lehmer–Euclid Algorithm, which explains how the Lehmer–Euclid algorithm can be viewed as a sequence of Interrupted Euclidean algorithms $\mathcal{E}_{[\delta,\delta+\gamma]}$. Most of the studies in the Dynamical Analysis framework use well-known properties of the transfer operator $\mathbf{H}_s$ when it acts on the functional space $\mathcal{C}^1(I)$, namely the existence of a unique dominant eigenvalue, separated from the remainder of the spectrum by a spectral gap. But, in the present paper, we also need other properties (deeper ones) which were already crucial in previous distributional analysis (Baladi and Vallée, 2005, 2004; Lhote and Vallée, 2008) – namely, the *US* (Uniform Estimates on Strips) Property for the quasi-inverse $(I-\mathbf{H}_s)^{-1}$ of the transfer operator –. The *US*(α) Property can be summarised in an informal way as follows:

Property *US*(α) (*Uniform Estimates on Strips*). *When* $\mathbf{H}_s$ *acts on the functional space* $\mathcal{C}^1(\mathcal{I})$ *of functions with a continuous derivative on the unit interval* $\mathcal{I} := [0,1]$, *the following holds on the strip* $\mathcal{S}_\alpha := \{s, 1-\alpha \leq \Re s \leq 1+\alpha\}$

(i) *The quasi-inverse* $(I-\mathbf{H}_s)^{-1}$ *has a unique pôle located at* $s=1$.
(ii) *It is of polynomial growth with respect to* $|\Im s|$ *when* $|\Im s|$ *tends to* ∞.

It is known from works of Mayer (1991) and Efrat (1993), that the quasi-inverse $(I-\mathbf{H}_s)^{-1}$, when it acts on a nice space $\mathcal{F}$ of analytic functions, has a unique pôle located at $s=1$ in the half-plane $\Re s > 1/2$. The other singularities of the quasi-inverse are located on the line $\Re s = 1/2$ or at values s for which the Riemann zeta function satisfies $\zeta(2s)=0$. Then, for any $\alpha < 1/2$, the vertical strip $\mathcal{S}_\alpha$ contains only one pôle of the quasi-inverse $(I-\mathbf{H}_s)^{-1}$, located at $s=1$. But this does not mean that the *US*-strip can be chosen as $\mathcal{S}_\alpha$, for two main reasons: first, we do not know if the quasi-inverse (even if it acts on $\mathcal{F}$) has a polynomial growth on $\mathcal{S}_\alpha$ when $|\Im s|$ tends to ∞. Moreover, the quasi-inverse $(I-\mathbf{H}_s)^{-1}$ (when it acts on $\mathcal{C}^1$) may possess many other singularities than when it acts on $\mathcal{F}$.

Author's personal copy

Extending methods due to Dolgopyat, Baladi and Vallée proved that there exists an $\alpha > 0$ for which Property $US(\alpha)$ holds. The arguments which show the existence of such a strip are not completely constructive, and we do not know any explicit strictly positive lower bound on α. In the paper, such a lower bound is denoted by σ, and the parameter $\underline{\sigma} := \min(\sigma, 1/2)$ plays a central rôle in our analyses: This is the mysterious constant which intervenes in the constants of our two main theorems, Theorems 6 and 7. It also intervenes in the exponents of all the remainder terms of Theorems 1–5.

In order to establish our main results, we are led to studying parameters of various type, whose generating functions involve operators $\mathbb{G}_{s,t}$ which depend on two variables s, t. However, for small values of parameter t, all these operators can be viewed as a perturbation of the quasi-inverse $(I-\mathbf{H}_s)^{-1}$ and the *US* Property extends to these perturbated quasi-inverses. In particular, the existence of a strip $\mathcal{S}$ where the *US* property holds uniformly with respect to t is crucial in the analysis.

Plan and notations. Section 2 describes the main algorithms $\mathcal{HG}$ and $\mathcal{G}$. Section 3 presents the main steps towards a proven analysis. Here, we state our main results of general interest, without proofs. In Section 4, we describe the versions $\underline{\mathcal{HG}}$ and $\underline{\mathcal{G}}$ to be analyzed, and, with the results of Section 3, we show the two main results about their average bit-complexity. Section 5 describes the general framework of the Dynamical Analysis paradigm, and Section 6 is devoted to the proof of the main results stated in Section 3. Some technical results are gathered in an Appendix.

We denote the logarithm in base 2 by $\lg x$, and $\ell(x)$ denotes the binary size of integer x, namely $\ell(x) := \lfloor \lg x \rfloor + 1$.

2. Fast and interrupted Euclidean algorithms

We present in this section the main algorithms studied in this paper. We first describe the general structure of the Euclid Algorithm (Section 2.1), then we present the idea of Lehmer, made more precise by Jebelean (Section 2.2). Next, we explain the principles of the Lehmer–Euclid algorithm (Section 2.4), which were used later in the Knuth–Schönhage algorithm. We finally explain how the $\mathcal{HG}$ algorithm, described in Section 2.5 can be seen as a sequence of interrupted Euclidean algorithms (introduced in Section 2.3) where the sequence of divisions is stopped as soon as the integers have lost a fraction of their number of bits.

2.1. Euclid's algorithm

Let (A_1, A_0) be a pair of positive integers with $A_1 \leq A_0$. On input (A_1, A_0), the Euclid algorithm computes the remainder sequence (A_k) with a succession of divisions of the form

$$A_k = Q_{k+1}A_{k+1} + A_{k+2}, \quad \text{with} \quad Q_{k+1} = \left\lfloor \frac{A_k}{A_{k+1}} \right\rfloor, \tag{6}$$

and stops when $A_{p+1} = 0$. The integer Q_k is the k-th quotient and the successive divisions can be written as

$$\mathcal{A}_k = \mathcal{Q}_{k+1}\mathcal{A}_{k+1}, \quad \text{with} \quad \mathcal{A}_k := \begin{pmatrix} A_{k+1} \\ A_k \end{pmatrix} \quad \text{and} \quad \mathcal{Q}_k := \begin{pmatrix} 0 & 1 \\ 1 & Q_k \end{pmatrix},$$

so that

$$\mathcal{A}_0 = \mathcal{M}_{(i)}\mathcal{A}_i \quad \text{with} \quad \mathcal{M}_{(i)} := \mathcal{Q}_1\mathcal{Q}_2\cdots\mathcal{Q}_i. \tag{7}$$

In the following, we consider a part of the plain Euclidean Algorithm $\mathcal{E}$, (which is sometimes called a "slice") between index i and index j, namely the interrupted algorithm $\mathcal{E}_{(i,j)}$ which begins with the pair $\mathcal{A}_i$ as its input and computes the sequence of divisions (6) with $i \leq k \leq j-1$. Its output is the pair $\mathcal{A}_j$ together with the matrix

$$\mathcal{M}_{(i,j)} = \prod_{k=i+1}^{j} \mathcal{Q}_k, \qquad \mathcal{M}_{(1,i)} = \mathcal{M}_{(i)}, \tag{8}$$

Author's personal copy

with matrix $\mathcal{M}_{(i)}$ defined in (7). We define the size of a matrix $\mathcal{M}$ as the maximum of the binary sizes of its coefficients. The size $\ell_{(i,j)}$ of the matrix $\mathcal{M}_{(i,j)}$ satisfies

$$\ell_{(i,j)} \leq 2(j-i) + \sum_{k=i+1}^{j} \ell(Q_k). \tag{9}$$

The (naive) bit-complexity $C_{(i,j)}$ of the algorithm $\mathcal{E}_{(i,j)}$ satisfies

$$C_{(i,j)} := \sum_{k=i+1}^{j} \ell(A_k) \cdot \ell(Q_k) \leq \ell(A_{i+1}) \cdot \sum_{k=i+1}^{j} \ell(Q_k). \tag{10}$$

The Lehmer Algorithm (Lehmer, 1938; Knuth, 1998) replaces large divisions by large multiplications and small divisions. The fast algorithm applies recursively the principles of Lehmer, and using fast FFT multiplications of complexity $\Theta(\mu(n))$ (with $\mu(n) = a(n)n \log n$) replaces the costly computation of the remainder sequence A_i (which requires $O(n^2)$ bit operations), by a sequence of matrix products: it divides the total Euclidean Algorithm into interrupted Euclidean algorithms, of the form $\mathcal{E}_{(i,j)}$ and computes matrices of the form $\mathcal{M}_{(i,j)}$, defined in (8). The recursion, based on Divide and Conquer techniques, is stopped when the integers are small enough, and, at this moment, the algorithm uses small divisions. One finally obtains a subquadratic gcd algorithm.

2.2. How to replace large divisions by small divisions?

Lehmer remarked that, when two pairs (A, B) and (a, b) lead to rationals A/B and a/b that are close enough, the Euclid algorithm on (A, B) or (a, b) produces (at least at the beginning of the execution) the same quotient sequence (Q_i). This is why the following definition is introduced:

Definition (*Set $\Pi_{\langle\gamma\rangle}$*). Consider $\gamma \in]0, 1]$. For an input pair (A, B), we denote by $\Pi_{\langle\gamma\rangle}(A, B)$ the set defined as

$$\Pi_{\langle\gamma\rangle}(A, B) := \left\{(a, b); \quad \ell(b) = \lfloor \gamma \ell(B) \rfloor, \qquad \left|\frac{A}{B} - \frac{a}{b}\right| \leq \frac{1}{b}\right\}.$$

And the criterion (due to Lehmer and made precise by Jebelean (1997, 1995)) is:

Lemma 1 (*Lehmer, Jebelean*). *Consider $\gamma \in]0, 1]$. Associate with a (large) pair (A, B) a small pair $(a, b) \in \Pi_{\langle\gamma\rangle}(A, B)$, together with the sequence of the remainders (a_i) of the Euclid Algorithm on the small input (a, b). Denote by k the first integer k for which a_k satisfies $\ell(a_k) \leq \lceil \gamma \ell(B)/2 \rceil \approx \ell(b)/2$. Then the sequence of the quotients q_i of the Euclid Algorithm on the small input (a, b) coincides with the sequence of the quotients Q_i of the Euclid Algorithm on the large input (A, B) for $i \leq k - 3$.*

Usually, this criterion is used with a particular pair (a, b) of the set $\Pi_{\langle\gamma\rangle}(A, B)$, where the integer b is obtained by the $\lfloor \gamma n \rfloor$-truncation of B, i.e., the suppression of its $(1 - \gamma)n$ least significant bits. Then a is easy to compute since it may be chosen itself as the $\lfloor \gamma n \rfloor$-truncation of A. This special pair is denoted by $T_\gamma(A, B)$. However, the Jebelean criterion holds for any choice of $(a, b) \in \Pi_{\langle\gamma\rangle}(A, B)$, not only for the special pair $T_\gamma(a, b)$, even if the integer a is less easy to compute in the general case: the integer a can be chosen as the integer part of the rational $(Ab)/B$, and its computation needs a product and a division.

2.3. Interrupted algorithms

In Jebelean's property (Lemma 1), the Euclid Algorithm on the small pair (a, b) of binary size m is stopped as soon the remainder a_k has lost $\lceil m/2 \rceil$ bits. This is a particular case of the so-called Interrupted Euclidean Algorithm of parameter δ (with $0 < \delta < 1$), which stops as soon as the current remainder has lost δm bits (with respect to the input which has m bits). This (general) interrupted Algorithm denoted by $\mathcal{E}_\delta$, and described in Fig. 2, is defined as follows: on the input (A, B) of size n, this algorithm begins at the beginning of the Euclid Algorithm, and stops as soon as the remainder A_i

Author's personal copy

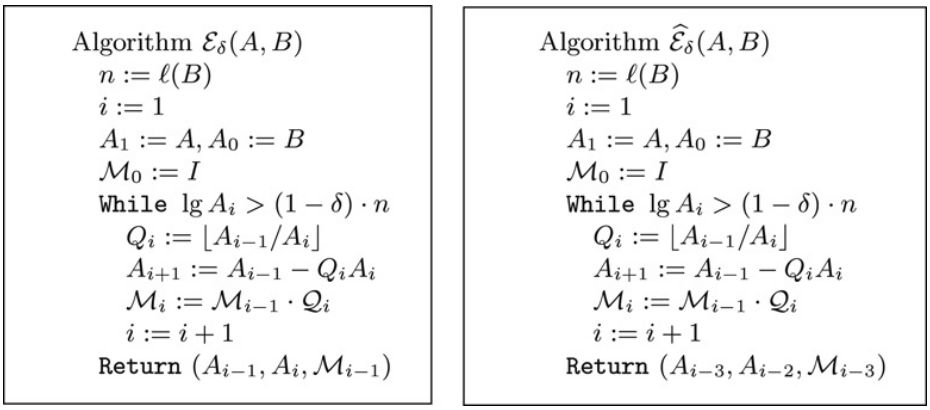


Fig. 2. The $\mathcal{E}_\delta$ Algorithm, and the $\widehat{\mathcal{E}}_\delta$ algorithm, which is a slight modification of the $\mathcal{E}_\delta$ Algorithm.

Algorithm $\mathcal{LE}_{[\delta,\delta+\gamma]}(A,B)$

Input. The pair (A',B') obtained after P_δ iterations of the $\mathcal{E}$ Algorithm on the input pair (A,B).
Output. The pair (C',D') which would be obtained after $P_{\delta+\gamma}$ iterations of the $\mathcal{E}$ Algorithm on the input pair (A,B).

(*i*) Truncate the input (A',B'), and consider the small pair $(a,b) := T_{2\gamma}(A',B')$.
(*ii*) Perform the $\widehat{\mathcal{E}}_{1/2}$ algorithm on the pair (a,b), which produces a pair (c,d) and a matrix $\mathcal{M}$.
(*iii*) Perform the product $\left(\begin{smallmatrix} C \\ D \end{smallmatrix}\right) := \mathcal{M}^{-1}\left(\begin{smallmatrix} A' \\ B' \end{smallmatrix}\right)$.
(*iv*) Use the Adjust function, which performs some steps of the Euclid Algorithm from the pair (C,D) and stops as soon the current remainder pair (C',D') has a size less than $(1-\delta-\gamma)n$.

Fig. 3. An implementation of the $\mathcal{LE}_{[\delta,\delta+\gamma]}$ Algorithm using the $\mathcal{HG}$ algorithm (in the case where $2\gamma < 1-\delta$).

has lost $\delta\, n$ bits (with respect to the input B). Then, with the notations defined in Section 2.1, one has $\mathcal{E}_\delta = \mathcal{E}_{(1,P_\delta)}$, with

$$P_\delta := \min\{k;\, \lg A_k \le (1-\delta)n\}\,. \tag{11}$$

Fig. 2 also describes the $\widehat{\mathcal{E}}_\delta$ Algorithm, which is just a slight modification of the $\mathcal{E}_\delta$ Algorithm, where the last three steps are suppressed (in view of applications of Lemma 1), and $\widehat{P}_\delta$ denotes the variable $P_\delta - 3$. Then, P_δ is just the number of iterations of the $\mathcal{E}_\delta$ algorithm and $P_1 = P$ is just the number of iterations of the Euclid Algorithm. The variable $\widehat{P}_\delta$ denotes the number of steps of the plain Euclid Algorithm which would be used to obtain the output of the $\widehat{\mathcal{E}}_\delta$ algorithm.

In the following, it will be convenient to consider more general interrupted algorithms, of the form $\mathcal{E}_{[\delta,\delta+\gamma]}$. The Algorithm $\mathcal{E}_{[\delta,\delta+\gamma]}$ is defined as follows: on the input (A, B) of size n, this algorithm begins at the P_δ-th iteration of the Euclid Algorithm, as soon as the remainder A_k has lost $\delta\, n$ bits (with respect to the input B) and stops when the remainder A_i has lost $\gamma\, n$ additional bits (with respect to the input B). Then, $\mathcal{E}_{[0,\delta]} = \mathcal{E}_\delta = \mathcal{E}_{(0,P_\delta)}$ and $\mathcal{E}_{[\delta,\gamma+\delta]} = \mathcal{E}_{(P_\delta,P_{\delta+\gamma})}$, where P_δ is defined in (11). Of course, we can also design the variants with a hat, where the last three steps are suppressed: this is the $\widehat{\mathcal{E}}_{1/2}$ algorithm which is used in Jebelean's Lemma.

2.4. Implementing the interrupted algorithms with the help of the $\widehat{\mathcal{E}}_{1/2}$ Algorithm. Principles of the Lehmer–Euclid Algorithm

With Jebelean's lemma, it is possible to use the $\widehat{\mathcal{E}}_{1/2}$ algorithm inside the $\mathcal{E}_{[\delta,\delta+\gamma]}$ algorithm. This is the main idea due to Lehmer, which gives rise to the $\mathcal{LE}_{[\delta,\delta+\gamma]}$ described in Fig. 3. We now comment this figure.

Author's personal copy

Suppose that the Euclid Algorithm, on an input (A, B) of length n, has already performed P_δ iterations. Now, the current pair, denoted by (A', B') has a binary size close to $(1-\delta)n$. We may use the Jebelean Property to continue. Then, we choose a degree 2γ of truncation (with $2\gamma < 1-\delta$) and consider the small pair $(a, b) = T_{2\gamma}(A', B')$ with $T_{2\gamma}$ defined in Section 2.2. The $\mathcal{HG}$ algorithm on this pair (a, b) (of size $m \approx 2\gamma n$) will produce a matrix $\mathcal{M}$ which would have been produced by the Euclid algorithm on the pair (A', B'). Then, the pair (C, D) computed as $\binom{C}{D} = \mathcal{M}^{-1}\binom{A'}{B'}$ is a remainder pair of the Euclid algorithm on the input (A, B). The size of the matrix $\mathcal{M}$ is approximately $m/2$, but smaller than $m/2$ (due to the three backward steps of Lemma 1), and thus of the form $(m/2) - r(A, B)$, where $r(A, B)$ is the number of bits which are "lost" for the matrix $\mathcal{M}$ during the three backward steps. Then, with (9), $r(A, B)$ satisfies,

$$3 \le r(A, B) \le Q(a, b) \qquad \text{with} \quad Q := \sum_{i=P_{1/2}-2}^{P_{1/2}} \ell(q_i) + 1. \tag{12}$$

Here, q_i are the quotients that occur in the Euclid Algorithm, and P_δ is defined in (11). Since the truncature length m is of the form $m \approx 2\gamma n$, then the size of the pair (C, D) is approximately equal to $[1-\delta-\gamma]n$, but slightly larger. If we wish to obtain a remainder pair (C', D') of length $[1-\delta-\gamma]n$, we have to perform, from the pair (C, D) a certain number of steps of the Euclid Algorithm, in order to cancel the loss due to the backward steps. This is the goal of the Adjust function, whose cost $R(A, B)$ will be estimated with (10) as

$$3(1-\delta)n \le R(A, B) \le (1-\delta)n \cdot Q(a, b). \tag{13}$$

We recall that, in the papers where the worst-case of fast GCD's is studied, the authors suppose that Q is $O(1)$ (in the worst case). We will *prove* that the *mean value* of Q on Ω_n will be indeed asymptotic to a precise constant η, which will be defined later. Then, the mean asymptotic cost of Step (iv) will be of order $O(n)$.

Step (iii) performs a matrix product and uses a fast multiplication of type (3). The integer pair (A', B') has size $\approx (1-\delta)n$, while the coefficients of the matrix $\mathcal{M}^{-1}$ have size $\approx \gamma n$. Then, if there exists an integer K for which $(1-\delta) = K\gamma$, the total cost $S(A, B)$ of Step (iii) is "expected" to satisfy

$$4A_1 \frac{1-\delta}{\gamma}\mu(\gamma n) \le S(A, B) \le 4A_2 \frac{1-\delta}{\gamma}\mu(\gamma n). \tag{14}$$

Finally, we have designed an algorithm $\mathcal{LE}_{[\delta,\delta+\gamma]}$ which produces the same result as the interrupted algorithm $\mathcal{E}_{[\delta,\delta+\gamma]}$, and is described in Fig. 3.

In Section 3.4, we shall state a class of results which prove that these last estimates (14) hold in the average case, as soon as a convenient choice of parameters δ, γ is done. In the same vein, these results will prove that the mean value of parameter R on Ω_n is of order $O(n)$, which will entail, with (12) and (13), that the cost R of the Adjust functions will be negligible with respect to the cost of matrix products.

2.5. The usual designs for the recursive gcd: The $\mathcal{HG}$ and $\mathcal{G}$ algorithms

There are two main ideas: first, the decomposition

$$\mathcal{E}_{[0,1/2]} = \mathcal{E}_{[0,1/4]} \cdot \mathcal{E}_{[1/4,1/2]},$$

is used. Second, each of the two interrupted algorithms $\mathcal{LE}_{[0,1/4]}$ and $\mathcal{LE}_{[1/4,1/2]}$ is designed as previously, but it now calls (in a recursive way) the $\widehat{\mathcal{E}}_{[0,1/2]}$ algorithm on truncated data of size $n/2$. This leads to a recursive version of the $\mathcal{HG}$ algorithm. Then, the first recursive call uses $\gamma = 1/4$, and two values for δ, namely $\delta = 0$ and $\delta = 1/4$. In fact, the precise decomposition used is $\widehat{\mathcal{E}}_{[0,1/2]} = \mathcal{E}_{[0,1/4]} \cdot \widehat{\mathcal{E}}_{[1/4,1/2]}$, which leads to modifying the Adjust function for this step: the second Adjust function may also perform some backward steps in the Euclid Algorithm on large inputs.

The general structure of the algorithm $\mathcal{HG}$ is described in Fig. 4. The recursion is stopped when the naive algorithm $\widehat{\mathcal{E}}_{1/2}$ becomes competitive. This defines a threshold for the binary size denoted by S (remark that $S = S(n)$ is a function of the input size n).

Author's personal copy

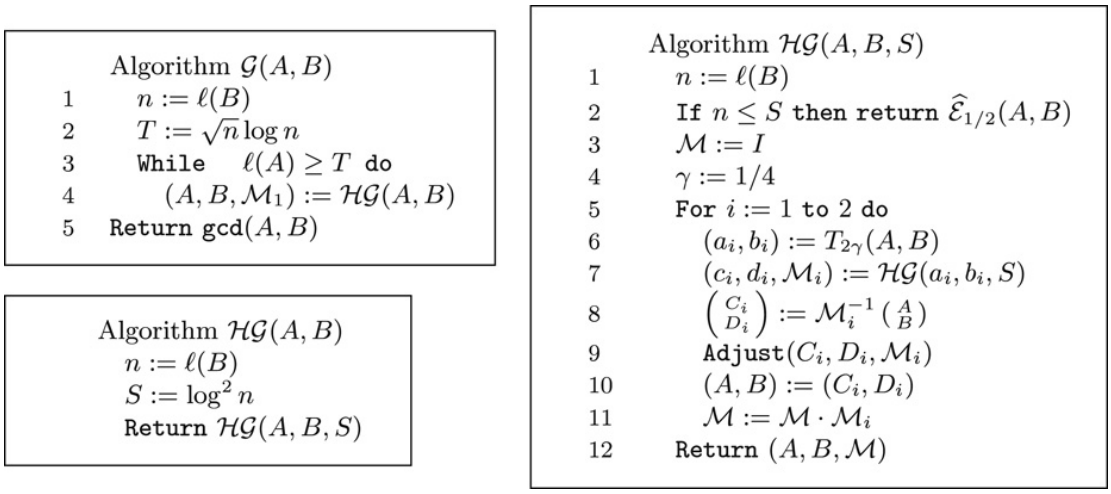


Fig. 4. General structure of the classical algorithms $\mathcal{HG}$ and $\mathcal{G}$.

With this $\mathcal{HG}$ algorithm, we can obtain an algorithm named $\mathcal{G}$ which computes the gcd. The idea for designing such an algorithm is to decompose the total Euclid Algorithm into interrupted algorithms, as

$$\mathcal{E}_{[0,1]} = \mathcal{E}_{[0,1/2]} \cdot \mathcal{E}_{[1/2,3/4]} \cdots \mathcal{E}_{[1-(1/2)^k,1-(1/2)^{k+1}]} \cdots .$$

Then, the $\mathcal{HG}$ algorithm, when running on inputs of size $n/(2^k)$ produced by the $\mathcal{E}_{[0,1-(1/2)^k]}$ algorithm can easily simulate the $\mathcal{E}_{[1-(1/2)^k,1-(1/2)^{k+1}]}$ algorithm.

This decomposition also stops when the naive algorithm gcd becomes competitive. This defines a threshold for the length denoted by T (remark that $T = T(n)$ is also a function of the input size n).

We now consider the $\mathcal{HG}$ Algorithm, where all the products use a FFT multiplication which satisfies (3). In this case, we choose the recursion depth H so that the main cost will be the "internal" cost, of order $\Theta(\mu(n))\log n$, since the cost due to the leaves (where the naive $\widehat{\mathcal{E}}_{1/2}$ is performed) will be of asymptotic smaller order. Then, H satisfies the relation[4]

$$2^H \cdot \left(\frac{n}{2^H}\right)^2 \approx_{\leq} \mu(n)\log n,$$

$$\text{so that} \quad \frac{n}{2^H} \approx_{\leq} S(n) = a(n)\log^2 n, \quad H \approx_{\geq} \lg n - 2\lg\lg n - \lg\lg\lg n.$$

(We use here the fact that $a(n) = O(\log\log n)$.)

This is the "classical" version of the Knuth–Schönhage algorithm. Clearly, the cost of this algorithm comes from three types of operations:

(i) the two recursive calls of line 7;
(ii) the products done at lines 8 and 11: with a clever implementation, it is possible to use in line 8 the pair (c,d) just computed in line 7. If all the matrices and integer pairs have – on average – the expected size, the total expected cost due to the products is

$$[12+8+8]\,\mu(n/4) = 28\,\Theta(1)\mu(n/4),$$

where the constants hidden in the Θ-term are A_1, A_2 defined in (3);
(iii) the two functions Adjust performed at line 9, whose total average cost is $R(n)$.

We consider as the set of all possible inputs of the $\mathcal{HG}$ algorithm the set $\Omega := \{(u,v);\ 0 \leq u \leq v\}$, and the set of all possible inputs of size n,

$$\Omega_n := \{(u,v);\quad 0 \leq u \leq v,\quad \ell(v) = n\} \tag{15}$$

[4] The notation $a(n) \approx_{\leq} b(n)$ means: There exist two constants A, B with $0 < A < B < 1$ for which $Ab(n) \leq a(n) \leq Bb(n)$.

Author's personal copy

is endowed with some probability $\mathbb{P}_n$. We denote by $B(n)$ the average number of bit operations performed by the algorithm $\mathcal{HG}$ on Ω_n. Since each of the two recursive calls is made on data with size $n/2$, it can be "expected" that $B(n)$ asymptotically satisfies

$$B(n) \approx 2B\left(\frac{n}{2}\right) + 28\,\Theta(1)\mu\left(\frac{n}{4}\right) + R(n) \qquad \text{for } n > S. \tag{16}$$

Moreover, the average cost $R(n)$ can be "expected" to be negligible with respect to the multiplication cost $\mu(n)$. If the FFT multiplication is used of type (3), the total average bit-cost is "expected" to be

$$B(n) \approx \Theta(\mu(n)\log n) = \Theta(n(\log n)^2\, a(n)),$$

where the constants hidden in the Θ-terms are $7A_1$, $7A_2$, with A_1, A_2 defined in (3).

With this (heuristic) analysis of the $\mathcal{HG}$ algorithm, it is easy to obtain the (heuristic) average bit-complexity of the $\mathcal{G}$ algorithm which makes a recursive use of the $\mathcal{HG}$ algorithm and stops as soon as the naive algorithm becomes competitive. It then stops at a recursion depth M, when

$$\left(\frac{n}{2^M}\right)^2 \approx_{\leq} \mu(n)\log n,$$

so that

$$\frac{n}{2^M} \approx_{\leq} T(n) = \sqrt{n}\log n, \qquad M \approx_{\geq} \frac{1}{2}\lg n - \lg\lg n.$$

The average bit-cost $G(n)$ of the $\mathcal{G}$ algorithm on data of size n satisfies

$$G(n) \approx \sum_{i=0}^{M-1} B\left(\frac{n}{2^i}\right) \qquad \text{so that} \quad G(n) \approx \Theta(B(n)).$$

3. The main steps towards a proven analysis

The previous analysis is based on the Divide and Conquer equation (16). It is only heuristic because this equality is not a "true" equality. It is not clear why a "true" equality should hold, since each of the two recursive calls is done on data which do not possess a priori the same distribution as the input data. And, of course, the same problem will be asked at each depth of the recursion. If we wish a "Divide and Conquer" probabilistic approach to be possible, we have to make precise *the evolution of the distribution during the Euclid Algorithm, but also the distribution of the associated truncated data.*

We first describe in Section 3.1 the main parameters of interest, together with their probabilistic version. Then, we state our main two results, Theorems 1 and 2, which are of general interest. In particular, Theorem 2 involves the density ψ already defined in (2) which plays a central rôle in our analysis. These theorems are stated here, but not proved. This will be done in Section 6. Then, in Section 3.5, we explain how Theorem 2 can be applied to truncated data and gives rise to Theorem 3, as soon as the truncation is a probabilistic one, defined in Section 3.4. Section 3.6 describes the analysis of the Adjust Functions (Theorem 4), and finally Section 3.7 provides estimates for the mean bit-complexity of the interrupted algorithms described in Section 2.4, in particular the mean-complexity of Steps (iii) and (iv) (Theorem 5).

3.1. Parameters P_δ and $x_{\langle\delta\rangle}$, and their probabilistic variants

Consider a density f on the unit interval $= [0, 1]$, which is "extended" to the set $\Omega := \{0 \leq u < v\}$ via the equality $f(u, v) := f(u/v)$. The set Ω_n formed with the inputs of size n, already defined in (15), namely $\Omega_n := \{0 \leq u < v, \ell(v) = n\}$ is endowed with the restriction of f to Ω_n: for any pair $(u, v) \in \Omega_n$,

$$\mathbb{P}_{n,f}(u, v) := \frac{1}{|\Omega_n|_f} f\left(\frac{u}{v}\right), \qquad \text{where} \quad |\Omega_n|_f := \sum_{(u,v)\in\Omega_n} f\left(\frac{u}{v}\right) \tag{17}$$

Author's personal copy

is the total f-weight of the set Ω_n. Remark that, for $f \equiv 1$, we recover the uniform density on Ω_n. For reasons which will appear later, the subsets $\widetilde{\Omega}$, $\widetilde{\Omega}_n$ formed with coprime inputs

$$\widetilde{\Omega} := \{(u, v) \in \Omega, \quad \gcd(u, v) = 1\}, \tag{18}$$

$$\widetilde{\Omega}_n := \{(u, v) \in \Omega, \quad \gcd(u, v) = 1, \ell(v) = n\}, \tag{19}$$

play an important (intermediate) rôle. We endow $\widetilde{\Omega}_n$ with the probability $\widetilde{\mathbb{P}}_{n,f}$ defined in the same vein as in (17).

For $(u, v) \in \Omega$, the Euclid Algorithm creates a sequence of successive remainders u_k, with $u_0 := v, u_1 := u, \ldots, u_p := \gcd(u, v)$. The corresponding integer pairs are denoted by $U_k := (u_{k+1}, u_k)$, and the corresponding rationals are denoted by $x_k := u_{k+1}/u_k$. For some $\delta \in]0, 1[$, we have already defined (respectively in Sections 1.2 and 2.3) the random variables $x_{\langle\delta\rangle}$ and P_δ. But, we need a generalized framework where the parameter δ possibly depends on the input size n: this means that we now consider a sequence $\delta = (\delta_n)$ of the $]0, 1[$ interval. For $(u, v) \in \Omega_n$, the number of iterations $P_\delta(u, v)$ is the smallest integer k for which $\lg u_k < (1 - \delta_n)n$. We are also interested in describing the density of the pair $U_{\langle\delta\rangle}$ defined as

$$U_{\langle\delta\rangle} := U_k \qquad \text{when} \quad P_\delta(u, v) = k.$$

This integer pair is the input for all interrupted algorithms with a beginning parameter δ. Since the density on Ω_n is defined via the associated rationals, the position of rational

$$x_{\langle\delta\rangle} := x_k \qquad \text{when} \quad P_\delta(u, v) = k$$

inside the interval $[0, 1]$ will be essential.

We do not succeed in directly studying these two variables $P_\delta, x_{\langle\delta\rangle}$, and we replace them by some of their probabilistic variants, as we now explain. Associate, to some sequence $\delta := (\delta_n)$, a sequence $\rho := (\rho_n)$ which depends on sequence δ and satisfies $\rho < (1 - \delta)$. Then, for any n, consider the interval $I_n(\delta)$ as

$$I_n(\delta) := \left[2^{(1-\delta_n)n}\left(1 - (1 - \delta_n)2^{-n\rho_n}\right), 2^{(1-\delta_n)n}\right].$$

Then, $I_n(\delta)$ is an interval of length $(1 - \delta_n)2^{(1-\delta_n-\rho_n)n}$, its right bound being close to the point $2^{(1-\delta_n)n}$. When the input size n varies, this defines a sequence $I(\delta)$ of intervals. We always consider the case where the interval length tends to ∞ with n, which will be the case in our framework when δ_n does not tend to 1 too fast.

For a given input size n, draw an integer W uniformly in the interval $I_n(\delta)$ and denote by $\underline{P}_\delta$ the first integer k for which u_k is less than W, and by $\underline{x}_{\langle\delta\rangle}$ the rational x_k. The two underlined variables define probabilistic variants of the plain variables. Since they depend on the sequence $I(\delta)$, we call them the $I(\delta)$-probabilistic variants. Moreover, as soon as the inequality $\rho_n > 1/n$ holds, the interval $I_n(\delta)$ is contained in an interval $]A/2, A]$ and contains at most two possible rationals x_k (this is due to the fact that $u_{k+2} \leq (1/2)u_k$). This proves, that in the case when $\rho_n > 1/n$, the probabilistic variable $\underline{x}_{\langle\delta\rangle}$ equals $x_{\langle\delta\rangle}$, $x_{\langle\delta\rangle+1}$, or $x_{\langle\delta\rangle+2}$, while the variables P_δ and $\underline{P}_\delta$ satisfy $\left|P_\delta - \underline{P}_\delta\right| \leq 2$.

3.2. An asymptotic Gaussian law for the number of iterations of the interrupted algorithm

Since the rational x loses $\ell(x)$ bits during $P(x)$ iterations, it can be expected that it loses $\delta\ell(x)$ bits during $\delta P(x)$ iterations, which would imply that $P_\delta(x)$ is sufficiently close to $\delta P(x)$. This is what we call the regularity of the algorithm. With techniques close to the renewal methods, we prove a quasi-powers expression for the moment generating function of $\underline{P}_\delta$, from which we deduce an asymptotic Gaussian law for $\underline{P}_\delta$ on Ω, then an asymptotic Gaussian law for the deterministic variable P_δ on Ω. We then obtain an extension of the result of Baladi and Vallée (2005) (which exhibits an asymptotic Gaussian law for $P := P_1$), even if our proof cannot directly apply to $\delta = 1$.

Theorem 1. *Consider the transfer operator* $\mathbf{H}_s$ *defined in* (5) *when it acts on the functional space* $\mathcal{C}^1(I)$, *denote by* $\Lambda(s) := \log\lambda(s)$ *the logarithm of the dominant eigenvalue* $\lambda(s)$, *and by* σ *a strictly positive lower bound on the width of the* US *strip. Let* $\underline{\sigma} := \min(\sigma, 1/2)$. *Consider the set* Ω_n *endowed with*

Author's personal copy

Theorem 1

$$\widetilde{\rho}(\delta) := \underline{\sigma}\min(\frac{1}{4}, 1-\delta) = \begin{cases} 2\delta\underline{\sigma} & \text{for } \delta \in [0, 1/8] \\ \frac{1}{4}\underline{\sigma} & \text{for } \delta \in [1/8, 3/4] \\ 1-\delta)\underline{\sigma} & \text{for } \delta \in [3/4, 1] \end{cases}$$

$$\widetilde{I}_n(\delta) := \left[2^{(1-\delta_n)n}\left(1-(1-\delta_n)2^{-\widetilde{\rho}(\delta_n)n}\right), 2^{(1-\delta_n)n}\right]$$

$$\widetilde{\tau}(\delta) := \underline{\sigma}\min\left(\frac{1}{4}, 1-\delta, 2\delta\right) = \begin{cases} 2\delta\underline{\sigma} & \text{for } \delta \in [0, 1/8] \\ \frac{1}{4}\underline{\sigma} & \text{for } \delta \in [1/8, 3/4] \\ (1-\delta)\underline{\sigma} & \text{for } \delta \in [3/4, 1] \end{cases}$$

Theorems 2, 3, 4, 5

$$\rho(\delta) := \underline{\sigma}\min\left(\frac{1}{2}, 1-\delta\right) = \begin{cases} \frac{1}{2}\underline{\sigma} & \text{for } \delta \in [0, 1/2] \\ (1-\delta)\underline{\sigma} & \text{for } \delta \in [1/2, 1] \end{cases}$$

$$I_n(\delta) := \left[2^{(1-\delta_n)n}\left(1-(1-\delta_n)2^{-\rho(\delta_n)n}\right), 2^{(1-\delta_n)n}\right]$$

$$\tau(\delta) = \underline{\sigma}\min\left(\frac{1}{8}, \frac{1-\delta}{4}, 2\delta\right) = \begin{cases} 2\delta\underline{\sigma} & \text{for } \delta \in [0, 1/16] \\ \frac{1}{8}\underline{\sigma} & \text{for } \delta \in [1/16, 1/2] \\ \frac{1-\delta}{4}\underline{\sigma} & \text{for } \delta \in [1/2, 1] \end{cases}$$

$$\tau(0,\gamma) = 2\gamma, \quad \tau(\delta,\gamma) := \min\left(\frac{\rho(\delta)}{2} - 2\gamma,\ 2\underline{\sigma}\delta,\ 2\gamma\right) \quad \text{for } \delta > 0, \text{ and } \gamma < \tfrac{1}{4}\rho(\delta).$$

Fig. 5. Definition of functions ρ and τ. Functions ρ describe the interval where the probabilistic choice is done, and functions τ quantify the remainder terms. Both define piecewise affine functions of δ.

a probability $\mathbb{P}_{n,f}$ relative to a strictly positive function f of class $\mathcal{C}^1$, together with a sequence $\delta := (\delta_n) \in]0,1[$, and associate to δ the three sequences $\widetilde{\rho}(\delta), \widetilde{\tau}(\delta), \widetilde{I}(\delta)$ as in Fig. 5. Suppose that the sequence $2^{-n\widetilde{\tau}(\delta)}/(1-\delta)$ tends to 0 (for $n \to \infty$). Then, the following holds

(i) *The $\widetilde{I}(\delta)$ probabilistic variant $\underline{P}_\delta$ of P_δ is asymptotically Gaussian, with a speed of convergence*

$$\max\left((\delta_n n)^{-1/2}, \frac{2^{-n\widetilde{\tau}(\delta_n)}}{1-\delta_n}\right).$$

Moreover, the expectation and the variance of the variable $\underline{P}_\delta$ satisfy

$$\mathbb{E}_{n,f}[\underline{P}_\delta] = 2\log 2\frac{1}{|\Lambda'(1)|}\delta_n n + D_1 + O\left(\frac{2^{-n\widetilde{\tau}(\delta_n)}}{1-\delta_n}\right),$$

$$\mathbb{V}_{n,f}[\underline{P}_\delta] = 2\log 2\left|\frac{\Lambda''(1)}{\Lambda'(1)^3}\right|\delta_n n + D_2 + O\left(\frac{2^{-n\widetilde{\tau}(\delta_n)}}{1-\delta_n}\right).$$

The constants D_1, D_2 and the constant in the O-term only depend on the function f.

(ii) *The variable P_δ is asymptotically Gaussian on Ω_n with a speed of convergence of order*

$$\max\left((\delta_n n)^{-1/3}, \frac{2^{-n\widetilde{\tau}(\delta_n)}}{1-\delta_n}\right),$$

and the expectation and the variance of the variable P_δ satisfy

$$\mathbb{E}_{n,f}[P_\delta] = 2\log 2\frac{1}{|\Lambda'(1)|}\delta_n n + O(1) \qquad \mathbb{V}_{n,f}[P_\delta] = 2\log 2\left|\frac{\Lambda''(1)}{\Lambda'(1)^3}\right|\delta_n n + O(1).$$

The main hypothesis on sequence $\widetilde{\tau}(\delta)$ holds as soon as the sequence δ satisfies

$$\delta_n n \to +\infty, \qquad (1-\delta_n)n > \log n.$$

Then, Theorem 1 holds for a quite large class of sequences δ which contains all the constant sequences $\delta \in]0,1[$. For constant sequences δ, the speeds of convergence are of respective order $n^{-1/2}$ and $n^{-1/3}$.

Author's personal copy

3.3. Distribution of the probabilistic variant of the variable $x_{\langle\delta\rangle}$

Our second result is related to the distribution of the probabilistic variant $\underline{x}_{\langle\delta\rangle}$, and, here, it does not seem possible to derive some information for the deterministic variable $x_{\langle\delta\rangle}$. This result shows that, after P_δ iterations, the rational computed by the Euclid Algorithm is approximatively distributed with the density ψ defined in (2), the remainder term being exponential with respect to the size n.

Theorem 2. *Denote by σ a strictly positive lower bound on the width of the* US *strip and let $\underline{\sigma} := \min(\sigma, 1/2)$. Consider a sequence $\delta := (\delta_n) \in]0,1[$, and associate with δ the three sequences $\rho(\delta), \tau(\delta), I(\delta)$ as in Fig. 5. For any $n \geq 1$, consider an interval $J \subset I$ whose length $|J|$ satisfies $|\lg(|J|)| < (n/4)\rho(\delta_n)$. Then, for any strictly positive density f of class $\mathcal{C}^1$, the probability that the $I(\delta)$-probabilistic rational $\underline{x}_{\langle\delta\rangle}$ computed by the Euclid Algorithm belongs to the interval J satisfies*

$$\mathbb{P}_{n,f}[\underline{x}_{\langle\delta\rangle} \in J] = \left(\int_J \psi(t)\mathrm{d}t\right) \cdot \left[1 + O\left(\frac{2^{-n\tau(\delta_n)}}{1-\delta_n}\right)\right].$$

Here, ψ the density defined in (2) and the constant in the O-term only depends on the function f via its norm $\|f\|_1 := \sup|f| + \sup|f'|$.

As previously, the sequence $2^{-n\tau(\delta_n)}/(1-\delta_n)$ tends to zero as soon as the sequence δ satisfies

$$\delta_n n \to +\infty, \qquad (1-\delta_n)n > \log n.$$

Then, Theorem 2 holds for a quite large class of sequences δ which contains all the constant sequences $\delta \in]0,1[$.

3.4. Probabilistic truncations

Finally, we are also interested by the distribution of the truncated pairs. We recall that the truncated pair $T_\gamma(A,B)$ classically used is obtained with truncations of "numerator" A and "denominator" B of pair (A,B). It is not clear how to describe the distribution of such a truncated pair. This is why we define a probabilistic truncation, which randomly chooses an element of the set $\Pi_{\langle\gamma\rangle}$ defined in Section 2.2. This leads to a more regular distribution, and it is always possible to apply Jebelean's Property (Lemma 1).

For $x = (A,B) \in \Omega_n$, and a degree of truncation γ, we define $\pi_{\langle\gamma\rangle}(A,B)$ as follows:

(1) Choose at random a denominator b in the set $\{v, \ell(v) = \lfloor\gamma n\rfloor\}$ of integers of binary size $m := \lfloor\gamma n\rfloor$, with a probability proportional to b. More precisely, we choose a denominator b according to the law

$$\Pr[b = b_0] = \frac{1}{\theta_m} \cdot b_0 \qquad \text{with} \quad \theta_m = \sum_{b;\,\ell(b)=m} b.$$

(2) Compute the integer a which is the integer part of $x \cdot b$. This computation involves the product $A \cdot b$ then the division of the integer $A \cdot b$ by B. This can be done in $O(\mu(n))$ with a O-constant larger than the constant of the multiplication (see Eq. (4)). Of course, this does not give rise to a very efficient algorithm. However, we will see that using this probabilistic truncation does not change the order of the average complexity of the $\mathcal{HG}$ algorithm. We return to this remark in Theorem 5.

(3) Define $\pi_m(A,B)$ as the pair (a,b), and remark that the set $\pi_m^{-1}(a,b)$ gathers the pairs (C,D) of Ω_n for which the associated rational C/D belongs to the interval

$$J\left(\frac{a}{b}\right) := \left[\frac{a}{b}, \frac{a}{b} + \frac{1}{b}\right[, \quad \text{with } \left|J\left(\frac{a}{b}\right)\right| = \frac{1}{b} = \Theta(2^{-m}).$$

This is sufficient for applying Jebelean's criterion (Lemma 1).

Author's personal copy

We start with a strictly positive density f of class $\mathcal{C}^1$ on $[0, 1]$, and for any integer m, the function $g_m = g_m[f]$ defined on Ω_m as

$$g_m[f](u, v) = \frac{1}{|J(y)|} \int_{J(y)} f(t)\mathrm{d}t, \qquad \text{with} \quad y := \frac{u}{v}$$

only depends on the rational u/v and satisfies

$$\mathbb{P}_{n,f}[(A, B); \pi_m(A, B) = (a, b)] = \mathbb{P}_{m,g_m[f]}(a, b).$$

Furthermore, for any $(u, v) \in \Omega_m$, the relation

$$g_m[f](u, v) = f\left(\frac{u}{v}\right) + O\left(\left|J\left(\frac{u}{v}\right)\right| \cdot \|f\|_1\right)$$

involves the norm $\|f\|_1$ of the function f, defined as $\|f\|_1 := \sup|f| + \sup\left|f'\right|$, and proves that the function $g_m[f]$ (viewed as a function defined on $\mathbb{Q}$) is a smoothed version of the initial function f. Furthermore,

$$\frac{\mathbb{P}_{m,g_m[f]}}{\mathbb{P}_{m,f}} = 1 + O(2^{-m}).$$

Since f is a density on $[0, 1]$, the cumulative sum of $g_m[f](x)$ on Ω_m satisfies

$$\sum_{(u,v)\in\Omega_m} g_m[f](u, v) = \sum_{\ell(v)=m} v \left[\sum_{u<v} \left(\int_{J(\frac{u}{v})} f(t)\right)\right] = \theta_m\left(\int_I f(t)\mathrm{d}t\right) = \theta_m.$$

This allows a comparison between two probabilities:

Lemma 2. *Consider $\gamma \in]0, 1]$ and a strictly positive density f of class $\mathcal{C}^1$ on I. For any n, for any $m := \lfloor \gamma n \rfloor$, for any $(a, b) \in \Omega_m$, one has*

$$\mathbb{P}_{n,f}[(A, B); \pi_{\langle\gamma\rangle}(A, B) = (a, b)] = \mathbb{P}_{m,f}(a, b) \cdot [1 + O(2^{-m})],$$

where the constant in the O-term only depends on f via its norm $\|f\|_1 := \sup|f| + \sup\left|f'\right|$.

3.5. Truncations and evolution of densities

We will deal with the probabilistic truncation $\pi_{\langle\gamma\rangle}$ defined in Section 3.4, and, with Theorem 2 and the previous comparison of densities done in Lemma 2, we obtain the following result which will be a central tool in our analysis.

Theorem 3. *Denote by σ a strictly positive lower bound on the width of the* US *strip and let $\underline{\sigma} := \min(\sigma, 1/2)$. Denote by ψ the density defined in (2). Consider a sequence $\delta := (\delta_n) \in]0, 1[$, and associate with δ the two sequences $\rho(\delta), I(\delta)$ as in Fig. 5. For any sequence γ which satisfies $2\gamma < (1/2)\rho(\delta)$, the distribution of the $\langle 2\gamma\rangle$–truncation of the $I(\delta)$-probabilistic rational $\underline{x}_{\langle\delta\rangle}$ computed by the Euclid Algorithm satisfies*

$$\mathbb{P}_{n,\psi}[x; \pi_{\langle 2\gamma\rangle}(\underline{x}_{\langle\delta\rangle}) = y_0] = \mathbb{P}_{\lfloor 2\gamma n\rfloor,\psi}[y_0] \cdot \left[1 + O\left(\frac{2^{-n\tau(\delta_n,\gamma_n)}}{1-\delta_n}\right)\right],$$

where $\tau(\delta, \gamma)$ is the sequence defined in Fig. 5.

As previously, the sequence $2^{-n\tau(\delta_n,\gamma_n)}/(1-\delta_n)$ tends to zero as soon as the sequences δ, γ satisfy $\gamma < (1/4)\rho(\delta)$ and

$$\delta_n n \to +\infty, \qquad \gamma_n n \to +\infty, \qquad (1-\delta_n)n > \log n.$$

Then, Theorem 3 holds for a quite large class of sequences δ, γ which contains all the constant sequences $\gamma, \delta \in]0, 1[$ satisfying $\gamma < (1/4)\rho(\delta)$. Remark also that the best bound which should relate γ and δ should be $2\gamma < 1 - \delta$. Here, the condition is more restrictive since it implies in particular $2\gamma < (1 - \delta)/4$. This extra factor 4 explains the design of our future algorithm $\underline{\mathcal{HG}}$, described in Section 4.

Author's personal copy

3.6. Mean number of bits lost during the backward steps

We wish to study the parameter Q defined in (12). In fact, we study a more general parameter, the parameter Q_δ, which corresponds to the three backwards steps, when the pair (u, v) has already lost a fraction δ of its bits. And, we are indeed interested in the probabilistic version $\underline{Q}_\delta$ of Q_δ, defined as

$$\underline{Q}_\delta := \sum_{i=\underline{P}_\delta - 2}^{\underline{P}_\delta} \ell(q_i),$$

and the (initial) parameter $\underline{Q}$ is obtained for $\delta = 1/2$. A central result is:

Theorem 4. *Consider the set Ω_n endowed with a probability $\mathbb{P}_{n,f}$ relative to a strictly positive function f of class $\mathcal{C}^1$. Then, for sequence $\delta \in]0, 1[$, the mean value of the cost $\underline{Q}_\delta$ is asymptotic to a constant η, which does not depend on δ and density f, and involves the Gauss density φ defined in (1), together with the operators $\mathbf{H}_{s,w,[\ell]}$ and $\mathbf{H}'_s$ defined in (32) and (33), under the form*

$$\mathbb{E}_{n,f}[\underline{Q}_\delta] = \eta \left[1 + O\left(\frac{2^{-n\tau(\delta_n)}}{1-\delta_n}\right)\right]$$
$$\text{with} \quad \eta := \frac{-6\log 2}{\pi^2} \int_I \mathbf{H}'_1 \circ \left(\frac{\mathrm{d}}{\mathrm{d}w} \mathbf{H}^3_{1,w,[\ell]}\right)_{w=0} [\varphi](t)\mathrm{d}t, \tag{20}$$

where $\rho(\delta)$ and $\tau(\delta)$ are the sequences defined in Fig. 5.

3.7. Mean bit-complexity of the interrupted algorithm $\underline{\mathcal{LE}}_{[\delta,\delta+\gamma]}$

We return now to the algorithm $\mathcal{LE}_{[\delta,\delta+\gamma]}$ defined in Fig. 3 and we use the notations of Section 2.4. We will study a probabilistic version of the algorithm $\mathcal{LE}_{[\delta,\delta+\gamma]}$ which will be denoted by $\underline{\mathcal{LE}}_{[\delta,\delta+\gamma]}$. We now describe the main differences between $\mathcal{LE}_{[\delta,\delta+\gamma]}$ and its probabilistic version. In the probabilistic version $\underline{\mathcal{LE}}_{[\delta,\delta+\gamma]}$:

(a) the input pair of the algorithm is the pair $\underline{U}_{\langle\delta\rangle}$ relative to the parameter $\rho(\delta)$;
(b) the output pair of the algorithm is the pair $\underline{U}_{\langle\delta+\gamma\rangle}$ relative to the parameter $\rho(\delta+\gamma)$;
(c) Step (i) uses the probabilistic truncature $\pi_{\langle 2\gamma\rangle}$ defined in Section 3.4;
(d) Step (ii) uses the probabilistic version $\underline{\widehat{\mathcal{E}}}_{1/2}$, defined as the plain Euclid algorithm which stops at the iteration of index $\underline{P}_{1/2} - 3$.

Then, the Adjust function becomes also probabilistic, since it performs steps for adjusting two probabilistic lengths: the (probabilistic) length of the pair (C, D) and the (probabilistic) length of the output (C', D'). It is denoted by $\underline{\texttt{Adj}}$. Due to the nature of probabilistic choices of these length, this is the length due to the three backwards steps which is dominant,

$$R(A, B) \leq (1-\delta)n \cdot Q_\varepsilon(a, b) \left[1 + O\left(\frac{2^{-n\tau(\delta_n)}}{1-\delta_n}\right)\right], \tag{21}$$

for some ε close to $1/2$.

As in the initial $\mathcal{LE}_{[\delta,\delta+\gamma]}$, Step (iii) uses any fast multiplication of type (3).

The following result studies the bit-complexity of the Interrupted Algorithm $\underline{\mathcal{LE}}_{[\delta,\delta+\gamma]}$ and proves two facts: first, the cost of the multiplications performed in Step (iii) is exactly of the same order as this expected. Second, the cost of the function $\underline{\text{Adj}}$ performed in Step (iv) is negligible with respect to costs of Step (iii).

Theorem 5. *Consider two sequences γ, δ satisfying $2\gamma < (1/2)\rho(\delta)$, with the sequences $\rho(\delta), \tau(\delta)$ from Theorem 3. Then, the probabilistic version $\underline{\mathcal{LE}}_{[\delta,\delta+\gamma]}$ of the $\mathcal{LE}_{[\delta,\delta+\gamma]}$ algorithm described in Section 3.4 satisfies the following:*

Author's personal copy

(a) *In the case when the ratio* $(1-\delta_n)/\gamma_n$ *is integer, the mean bit-complexity cost* $\mathbb{E}_{n,\psi}[S]$ *of Step* (iii) *satisfies:*

$$\mathbb{E}_{n,\psi}[S] = \Theta(1)\frac{1-\delta_n}{\gamma_n}\mu(\gamma_n n)\left[1+O\left(\frac{2^{-n\tau(\delta_n)}}{1-\delta_n}\right)\right],$$

where the hidden constants in the Θ*-term are independent on the pair* (γ,δ) *and can be chosen as* $4A_1, 4A_2$ *for constants* A_1, A_2 *relative to the fast multiplication defined in* (3).

(b) *In the case when the ratio* $(1-\delta_n)/\gamma_n$ *is integer, the mean bit-complexity cost* $\mathbb{E}_{n,\psi}[T]$ *of Step* (i) *satisfies*

$$\mathbb{E}_{n,\psi}[T] = \Theta(1)\frac{1-\delta_n}{\gamma_n}\mu(\gamma_n n)\left[1+O\left(\frac{2^{-n\tau(\delta_n)}}{1-\delta_n}\right)\right],$$

where the hidden constants in the Θ*-term are independent on the pair* (γ,δ) *and can be chosen as* $2\min(A_1,A_3),\ 2\max(A_2,A_4)$ *for constants* A_1, A_2 *relative to the fast multiplication defined in* (3)*, and constants* A_3, A_4 *relative to the fast division defined in* (4).

(c) *The mean bit-complexity cost* $\mathbb{E}_{n,\psi}[R]$ *of Step (iv) satisfies:*

$$\mathbb{E}_{n,\psi}[R] \le (1-\delta_n)n\eta\left[1+O\left(\frac{2^{-n\tau(\delta_n)}}{1-\delta_n}\right)\right]$$

and involves the constant η *defined in* (20).

(d) *Suppose that the sequences* $\gamma, \tau(\delta)$ *satisfy*

$$\log(\gamma_n n)\, a(\gamma_n n) \le (1-\delta_n)\, 2^{n\tau(\delta_n)}.$$

Then, the total bit-complexity of Steps (i), (iii) *and* (iv) *is*

$$\mathbb{E}_{n,\psi}[S+R+T] = \Theta(1)\frac{1-\delta_n}{\gamma_n}\mu(\gamma_n n)\left[1+O\left(\frac{1}{\log(\gamma_n n)\, a(\gamma_n n)}\right)\right]$$

and involves the functions $\mu(n)$ *and* $a(n)$ *associated with the fast multiplication. As previously, the hidden constants in the* Θ*-term are independent on the pair* (γ,δ) *and can be chosen as* $4A_1', 4A_2'$,

$$A_1' := \min\left(A_1, \frac{A_3}{2}\right), \qquad A_2' := \max\left(A_2, \frac{A_4}{2}\right) \tag{22}$$

and involve constants A_i *defined in* (3) *and* (4)*. The hidden constant in the O-term is independent on the pair* (γ,δ) *too.*

Remark. A sufficient condition to ensure the condition needed in (d) is that γ and δ satisfy

$$n(1-\delta_n) = \Omega(n^\alpha), \qquad n\gamma_n = \Omega(n^\beta), \qquad \alpha,\beta > 0.$$

4. The algorithms to be analyzed

There are three main differences between the usual $\mathcal{HG}$ and $\mathcal{G}$ Algorithms and our versions to be analysed which are denoted as $\underline{\mathcal{HG}}$ and $\underline{\mathcal{G}}$ (see Fig. 6).

(i) Our algorithm $\underline{\mathcal{HG}}$ has the same effect as the probabilistic algorithm $\widehat{\underline{\mathcal{LE}}}_{[0,1/2]}$, which is defined as the algorithm $\underline{\mathcal{LE}}_{[0,1/2]}$ where the last three steps are suppressed. It is thus randomised.

(ii) It is a recursive version of the $\widehat{\underline{\mathcal{LE}}}_{[0,1/2]}$, as the $\mathcal{HG}$ algorithm is the recursive version of the $\mathcal{LE}_{[0,1/2]}$. They are both based on a Divide and Conquer principle. However, the relation $2\gamma < (1/2)\rho(\delta)$ which relates the two parameters γ, δ with the width $\underline{\sigma}$ of the *US* strip, crucial for applying Theorem 5, leads to a recursive algorithm $\underline{\mathcal{HG}}$ with L recursive calls, where L depends on the width $\underline{\sigma}$ and satisfies $L > 4/\underline{\sigma}$. Then, the $\underline{\mathcal{HG}}$ algorithm is based on the decomposition

$$\underline{\mathcal{E}}_{[0,1/2]} = \underline{\mathcal{E}}_{[0,\gamma]} \cdot \underline{\mathcal{E}}_{[\gamma,2\gamma]} \cdot \cdots \cdot \underline{\mathcal{E}}_{[i\gamma,(i+1)\gamma]} \cdot \cdots \cdot \underline{\mathcal{E}}_{[(L-1)\gamma,L\gamma]}, \qquad \text{with} \quad \gamma = \frac{1}{2L},$$

Author's personal copy

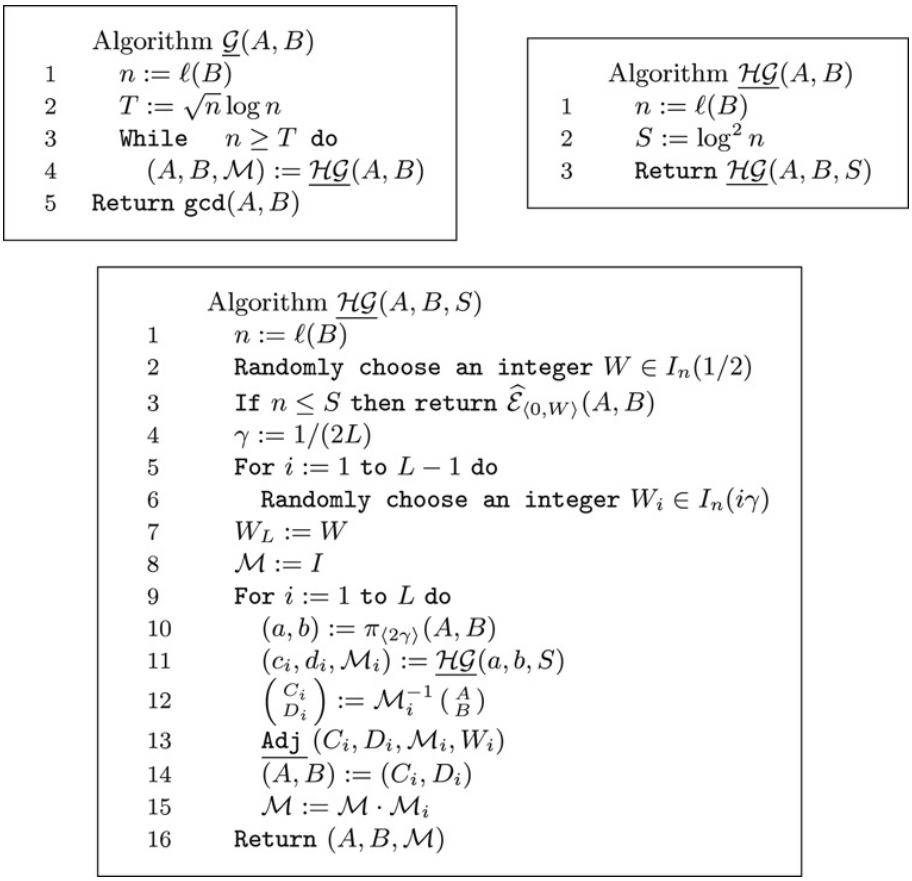


Fig. 6. General structure of the algorithms $\underline{\mathcal{HG}}$ and $\underline{\mathcal{G}}$ to be analysed. The number of recursive calls L satisfies $L > (4/\underline{\sigma})$. For two integers $W_1, W_2 \in [2^n, 1]$, with $W_1 \geq W_2$, the algorithm $\mathcal{E}_{\langle W_1,W_2\rangle}$ is the Euclid algorithm which begins as soon $u_k \leq W_1$ and ends as soon as $u_k \leq W_2$. The $\underline{\mathtt{Adj}}$ function is the probabilistic variant of the Adjust function defined in Section 3.7.

and use truncations of degree 2γ. More precisely, one begins to randomly choose L integers W_i (for $i \in [1..L]$) with $W_i \in I_n(i\gamma)$, and the decomposition used is

$$\underline{\mathcal{E}}_{[0,1/2]} = \mathcal{E}_{\langle 0,W_1\rangle}\cdot\underline{\mathcal{E}}_{\langle W_1,W_2\rangle}\cdot\cdots\cdot\underline{\mathcal{E}}_{\langle W_i,W_{i+1}\rangle}\cdot\cdots\cdot\underline{\mathcal{E}}_{\langle W_{L-1},W_L\rangle},$$

where the algorithm $\mathcal{E}_{\langle W_i,W_{i+1}\rangle}$ is the Euclid algorithm which begins as soon as $u_k \leq W_i$ and ends as soon as $u_\ell \leq W_{i+1}$.

(iii) The study is done when the initial density equals ψ, since it is quasi-invariant under the recursive calls. This choice makes the study of various recursions easier. The constants which appear in Theorems 6 and 7 are relative to this particular case. Since any other strictly positive density f of class $\mathcal{C}^1$ satisfies

$$\frac{\min f}{\max\psi} \leq \frac{\mathbb{E}_{n,f}[C]}{\mathbb{E}_{n,\psi}[C]} \leq \frac{\max f}{\min\psi},$$

Theorems 6 and 7 hold with any strictly positive density of class $\mathcal{C}^1$, with other constants, which depend on f. Remember that ψ is almost constant, with $\min\psi \geq 0.9$ and $\max\psi \leq 1.1$ so that the previous bounds are close to 1 for the choice $f \equiv 1$, that corresponds to the uniform probability.

As before, the recursive calls in the $\underline{\mathcal{HG}}$ Algorithm are stopped when the naive $\widehat{\mathcal{E}}_{1/2}$ Algorithm becomes competitive. The calls of the $\underline{\mathcal{G}}$ Algorithm to the $\underline{\mathcal{HG}}$ algorithm are stopped when the naive gcd algorithm becomes competitive.

Author's personal copy

4.1. The first recursive call

Inside the first recursive call of $\underline{\mathcal{G}}$ to $\underline{\mathcal{HG}}$, the parameter δ belongs to $[0, 1/2]$. We suppose that there are $L \geq 2$ recursive calls of $\underline{\mathcal{HG}}$ to himself. We denote by B_L the bit-complexity of the $\underline{\mathcal{HG}}$ Algorithm when it performs L recursive calls, and we analyse the asymptotic behaviour of the mean value $\mathbb{E}_{n,\psi}[B_L]$ (for $n \to \infty$).

Suppose indeed $L \geq 2$. Then, the possible values for pairs (δ, γ) of the first recursive call satisfy

$$\delta \in \Delta_1 := \left\{ \frac{i}{2L}, \quad \text{with} \quad 0 \leq i \leq L-1 \right\}, \qquad \gamma_1 := \frac{1}{2L}, \tag{23}$$

and the pairs relative to the h-th recursive call are

$$\delta \in \Delta_h := \left\{ \frac{i}{2L^h}, \quad \text{with} \quad 0 \leq i \leq L^h - 1 \right\} \qquad \gamma_h := \frac{1}{2L^h}.$$

We stop the recursion at a level H for which the total bit-cost $P(n)$ of the naive gcd computations is negligible with respect to the total cost of the algorithm. More precisely, if $a(n)$ is the function which intervenes in the multiplication cost, we ask

$$P(n) = \Theta\left(L^H \cdot \left(\frac{n}{L^H}\right)^2\right) = n \log^2 n = \frac{\mu(n) \log n}{a(n)}, \quad H \sim \left(\frac{\log n}{\log L}\right), \quad \frac{n}{L^H} = \Theta(\log^2 n). \tag{24}$$

The parameters δ and γ must satisfy the condition $2\gamma < \frac{1}{2}\rho(\delta)$. Since $\delta \in [0, 1/2]$, this is only possible if

$$\frac{1}{L} = 2\gamma < \frac{1}{2}\rho(\delta) = \frac{1}{4}\underline{\sigma} \qquad \text{or} \quad L > \frac{4}{\underline{\sigma}},$$

and, in this case, the minimum value of $\tau(\delta, \gamma)$ at the h-th recursion level satisfies

$$\exists K > 0, \quad \forall h \geq 1, \quad \min\{\tau(\delta, \gamma_h), \delta \in \Delta_h\} \geq \frac{K}{L^h}. \tag{25}$$

With (25), Theorem 3 entails the following Divide and Conquer probabilistic equation,

$$\mathbb{E}_{n,\psi}[B_L] = \left(\sum_{\delta \in \Delta_1} \mathbb{E}_{\delta n,\psi}[B_L] \right) \cdot \left[1 + O\left(2^{-nK/L}\right)\right] + C_{n,1},$$

where $C_{n,1}$ is the total bit-complexity of steps Steps (i), (iii) and (iv) performed during the executions of the $\underline{\mathcal{E}}_{[\delta,\delta+\gamma]}$ Algorithm, together with the matrix product performed in Line 11, for $\delta \in \Delta_1$ easily estimated with Theorem 5. Expanding the recursion (always with Theorem 3) leads to the estimate

$$\mathbb{E}_{n,\psi}[B_L] = \left(P(n) + \sum_{h=1}^{H} C_{n,h} \right) \left[\prod_{h=1}^{H} 1 + O\left(2^{-nK/L^h}\right) \right],$$

where $P(n)$ is the cost of the "leaves" and $C_{n,h}$ is the total mean cost of all the Steps (i), (iii) and (iv) of the interrupted algorithms at the h-th level, corresponding to $\delta \in \Delta_h$, $\gamma := \gamma_h$. The error term comes from the comparison of the distributions made with Theorem 3, and is of the form, with (24) and (25)

$$1 + O(\varepsilon(n)), \quad \text{with} \quad \varepsilon(n) = \sum_{h=1}^{H} 2^{-\frac{nK}{L^h}} \leq H 2^{-\frac{nK}{L^H}} = \Theta(\log n)\, 2^{-K \log^2 n} = O(n^{-K_1 \log n}).$$

The cost $C_{n,h}$ at the h-th recursion level is easily evaluated with Theorem 5. We let $b(n) := a(n) \log n$. For $h = 1$, Theorem 5 entails the estimate

$$\begin{aligned} C_{n,1} \;&= \Theta(1) \left[\sum_{i=1}^{L} 2L \left(1 - \frac{i}{2L}\right) \right] \mu\left(\frac{n}{2L}\right) \left[1 + O\left(\frac{1}{b(n/L)}\right)\right] \\ &\quad + \Theta(1) \left[\sum_{I=1}^{L} i \right] \mu\left(\frac{n}{2L}\right) \left[1 + O\left(\frac{1}{b(n/L)}\right)\right], \end{aligned}$$

Author's personal copy

where the first term is due to the cost of the interrupted algorithms and the second term to matrix products of Line 11. One has

$$C_{n,1} = \Theta(L^2)\,\mu\left(\frac{n}{2L}\right)\left[1 + O\left(\frac{1}{b(n/L)}\right)\right]$$

where the hidden constants are now respectively $6A'_1 + 8A_1$, $6A'_2 + 8A_2$, with (A'_1, A'_2) defined in (22) and A_1, A_2 defined in (3). In the same vein,

$$C_{n,h} = \Theta(L^{h+1})\mu\left(\frac{n}{2L^h}\right)\left[1 + O\left(\frac{1}{b(n/L^h)}\right)\right],$$

and finally

$$\sum_{h=1}^{H} C_{n,h} = \Theta(1)\frac{L}{2\log L}\mu(n)\log n \cdot \left[1 + O\left(\frac{1}{b(\log^2 n)}\right)\right]$$

where the constants in the Θ-term are always respectively $6A'_1 + 8A_1$, $6A'_2 + 8A_2$. Now, with (24), the error term due to the leaves is of the form $1/a(n)$, and the function $b(\log^2 n)$ is larger than $a(n)$. Finally,

$$\mathbb{E}_{n,\psi}[B_L] = \Theta(1)\frac{L}{2\log L}\mu(n)\log n \cdot \left[1 + O\left(\frac{1}{a(n)}\right)\right]$$

where the constants in the Θ-term are always respectively $6A'_1 + 8A_1$, $6A'_2 + 8A_2$.

Theorem 6. *Consider the $\underline{\mathcal{HG}}$ algorithm defined in Fig. 6, relative to a parameter L which satisfies $L > (2/\underline{\sigma}) - 1$, and involves $\underline{\sigma} := \max(\sigma, 1/2)$, where σ is a strictly positive lower bound for the* US *strip. Suppose that the algorithm uses a fast multiplication of type (3). Then, the mean bit-complexity B_L of this $\underline{\mathcal{HG}}$ algorithm on the set Ω_n endowed with the density ψ defined in (2) satisfies*

$$\mathbb{E}_{n,\psi}[B_L] = \Theta\left(\frac{L}{\log L}\right) n\,(\log n)^2\,a(n) \cdot \left[1 + O\left(\frac{1}{a(n)}\right)\right].$$

Here, the constants in the Θ-term can be chosen as $3A'_1 + 4A_1$, $3A'_2 + 4A_2$, where A'_1, A'_2 defined in (22) are the constants related to the fast multiplication and the fast division. The mean bit-complexity B_L of this $\underline{\mathcal{HG}}$ algorithm on the set Ω_n endowed with any density f of class $\mathcal{C}^1$ satisfies

$$\mathbb{E}_{n,f}[B_L] = \Theta(1)\,n\,(\log n)^2\,a(n) \cdot \left[1 + O\left(\frac{1}{a(n)}\right)\right].$$

Here, the constants in the Θ-term can be chosen as

$$\frac{\min f}{\max \psi}\min\left(7A_1, 4A_1 + \frac{3}{2}A_3\right), \qquad \textit{and} \qquad \frac{\max f}{\min \psi}\max\left(7A_2, 4A_2 + \frac{3}{2}A_4\right),$$

where A_1, A_2 are the constants related to the fast multiplication and A_3, A_4 are the constants related to the fast division.

4.2. The k-th recursive call

The k-th recursive call of $\underline{\mathcal{G}}$ to $\underline{\mathcal{HG}}$ is made on integers with size $n_k = n(1/2)^{k-1}$. It deals with values $\delta^{(k)}$ which belong to the interval $[1 - (1/2)^{k-1}, 1 - (1/2)^k]$, so that the values $(1 - \delta^{(k)})n$ belong to the interval $[n_k, n_k/2]$. If we wish to perform at the k-th level an algorithm $\underline{\mathcal{HG}}$ homothethic to the algorithm of the first level [with a ratio $(1/2)^{k-1}$], we deal with a truncation m_k of the form $m_k = 2\gamma^{(1)}n_k = 2\gamma^{(k)}n$ with $\gamma^{(k)} = 1/(2^{k-1}L)$. Now the parameter $\tau(\delta^{(k)}, \gamma^{(k)})$ relative to values

Author's personal copy

$\delta^{(k)}, \gamma^{(k)}$ used in the kth recursive call of $\underline{\mathcal{G}}$ to $\underline{\mathcal{HG}}$ is related to the parameter $\tau(\delta^{(1)}, \gamma^{(1)})$ relative to values $\delta^{(1)}, \gamma^{(1)}$ used in the first recursive call of $\underline{\mathcal{G}}$ to $\underline{\mathcal{HG}}$, via the inequality

$$n\,\tau(\delta^{(k)}, \gamma^{(k)}) \geq n_k\,\tau(\delta^{(1)}, \gamma^{(1)}).$$

On the other hand, the density $\psi^{(k)}$ of the input pair is close to the initial density, with an approximation factor described in Theorem 2, relative to $\delta = 1 - 2^{-k}$. Then, all the previous study performed for the first recursive call can be applied to the k-th recursive call, as soon as n is replaced by n_k. Then, the bit-complexity $B_{k,L}$ of the k-th recursive call is, with Theorems 2 and 6,

$$\mathbb{E}_{n,\psi}[B_{k,L}] = \Theta\left(\frac{L}{\log L}\right) n_k(\log n_k)^2\, a(n_k) \cdot \left[1 + O\left(\frac{1}{a(n_k)}\right)\right] \cdot \left[1 + O\left(\frac{2^{-n\tau(1-(1/2)^k)}}{2^{-k}}\right)\right] \quad (26)$$

with the same constants involved as in Theorem 6.

4.3. End of the recursion

We stop calling the algorithms $\underline{\mathcal{HG}}$ inside the $\underline{\mathcal{G}}$ algorithm when the naive gcd algorithm becomes competitive, with a complexity $P_1(n) = \Theta(n \log^2 n)$. Then, the level of recursion M is defined by

$$n_M^2 = n \log^2 n \quad \text{so that} \quad n_M = \frac{n}{2^M} = \sqrt{n} \log n, \quad M = (1/2)(\log n).$$

Then, the hypothesis needed in Theorem 5(d) is fulfilled (see the remark after Theorem 5) and the total cost G of the $\underline{\mathcal{G}}$ Algorithm satisfies

$$\mathbb{E}_{n,\psi}[G] = \sum_{k=1}^{M} \mathbb{E}_{n,\psi}[B_{k,L}] = \Theta\left(\frac{L}{\log L}\right) n\,(\log n)^2\, a(n) \cdot \left[1 + O\left(\frac{1}{a(\sqrt{n}\log n)}\right)\right]$$

where the constants in the Θ-term are equal to two times the constants of Theorem 6. Finally, we have proven the following:

Theorem 7. *Consider the $\underline{\mathcal{HG}}$ algorithm defined in Fig. 6, relative to a parameter L which satisfies $L > (2/\underline{\sigma}) - 1$, and involves $\underline{\sigma} := \max(\sigma, 1/2)$, where σ is a strictly positive lower bound for the* US *strip. Suppose that the algorithm uses a fast multiplication of type (3).*

Then, the mean bit-complexity G_L of the $\underline{\mathcal{G}}$ algorithm on the set Ω_n endowed with the density ψ defined in (2) satisfies

$$\mathbb{E}_{n,\psi}[G_L] = \Theta\left(\frac{L}{\log L}\right) n\,(\log n)^2\, a(n) \cdot \left[1 + O\left(\frac{1}{a(\sqrt{n}\log n)}\right)\right].$$

Here, the constants in the Θ-term can be chosen as $\min(14A_1, 8A_1 + 3A_3)$, $\max(14A_2, 8A_2 + 3A_4)$, where A_1, A_2 are the constants related to the fast multiplication and A_3, A_4 are the constants related to the fast division. The mean bit-complexity G_L of the $\underline{\mathcal{G}}$ algorithm on the set Ω_n endowed with any density f of class $\mathcal{C}^1$ satisfies

$$\mathbb{E}_{n,f}[G_L] = \Theta\left(\frac{L}{\log L}\right) n\,(\log n)^2\, a(n) \cdot \left[1 + O\left(\frac{1}{a(\sqrt{n}\log n)}\right)\right].$$

Here, the constants in the Θ-term can be chosen as

$$\frac{\min f}{\max \psi} \min(14A_1, 8A_1 + 3A_3), \qquad \text{and} \qquad \frac{\max f}{\min \psi} \max(14A_2, 8A_2 + 3A_4),$$

where A_1, A_2 are the constants related to the fast multiplication and A_3, A_4 are the constants related to the fast division.

Author's personal copy

5. Description of the dynamical analysis method

Here, we present the main tools which will be used in the proof of Theorems 1 and 2. These tools come from analysis of algorithms (generating functions, here of Dirichlet types, described in 5.1) or dynamical systems theory (mainly transfer operators $\mathbf{H}_s$, described in 5.3 and 5.4). We introduce the main costs C of interest (in 5.2), and their related Dirichlet series, for which we provide an alternative expression with the transfer operator (in 5.5). For obtaining the asymptotic estimates of Theorems 1 and 2, we extract coefficients from these Dirichlet series, in a "uniform way". Then, Property *US* (already described in 1.3) is crucial here for applying with success the Perron Formula, as in previous results of Baladi and Vallée (2005).

5.1. Dirichlet series

For analysing a cost C, we deal with the generating Dirichlet series of the cost C. We recall that we deal with the sets Ω, $\widetilde{\Omega}$ of all possible inputs, and their subsets $\widetilde{\Omega}_n$, Ω_n which gather the inputs (u, v) with $\ell(v) = n$ defined in (18). We will explain later why it is easier and also sufficient to deal with inputs of $\widetilde{\Omega}$ (which is, from the algorithmic point of view, the set of trivial inputs…). We consider these sets endowed with probability $\mathbb{P}_{n,f}$ or $\widetilde{\mathbb{P}}_{n,f}$ defined from a positive function f of the interval $\mathcal{I}$ as

$$\mathbb{P}_{n,f}(u, v) := \frac{1}{|\Omega_n|_f} f\left(\frac{u}{v}\right), \qquad \widetilde{\mathbb{P}}_{n,f}(u, v) := \frac{1}{|\widetilde{\Omega}_n|_f} f\left(\frac{u}{v}\right), \qquad \text{for any } (u, v) \in \Omega_n,$$

where

$$|\Omega_n|_f := \sum_{(u,v)\in\Omega_n} f\left(\frac{u}{v}\right), \qquad |\widetilde{\Omega}_n|_f := \sum_{(u,v)\in\widetilde{\Omega}_n} f\left(\frac{u}{v}\right)$$

are the total f-weights of the sets Ω_n, $\widetilde{\Omega}_n$.

To any cost C, defined on Ω (or $\widetilde{\Omega}$), we associate Dirichlet series

$$F_C(s) = \sum_{(u,v)\in\Omega} \frac{1}{v^{2s}} C(u, v) f\left(\frac{u}{v}\right), \qquad \widetilde{F}_C(s) = \sum_{(u,v)\in\widetilde{\Omega}} \frac{1}{v^{2s}} C(u, v) f\left(\frac{u}{v}\right),$$

whose alternative expressions are

$$F_C(s) = \sum_{v\geq 1} \frac{c_v}{v^{2s}}, \qquad \widetilde{F}_C(s) = \sum_{v\geq 1} \frac{\widetilde{c}_v}{v^{2s}},$$

where $c_v, \widetilde{c}_v$ denote the cumulative costs of C on $\omega_v := \{(u, v) \in \Omega\}, \widetilde{\omega}_v := \{(u, v) \in \widetilde{\Omega}\}$, namely,

$$c_v = \sum_{(u,v)\in\omega_v} C(u, v) f\left(\frac{u}{v}\right), \qquad \widetilde{c}_v = \sum_{(u,v)\in\widetilde{\omega}_v} C(u, v) f\left(\frac{u}{v}\right).$$

For the trivial cost ($C \equiv 1$), the corresponding cumulative costs a_v or $\widetilde{a}_v$ are just the f-weights of subsets ω_v, $\widetilde{\omega}_v$, namely

$$a_v = \sum_{(u,v)\in\omega_v} f\left(\frac{u}{v}\right), \qquad \widetilde{a}_v = \sum_{(u,v)\in\widetilde{\omega}_v} f\left(\frac{u}{v}\right).$$

The mean values of the cost C on Ω_n, $\widetilde{\Omega}_n$ are then given by the ratio of partial sums,

$$\mathbb{E}_{n,f}[C] = \frac{\sum_{\ell(v)=n} c_v}{\sum_{\ell(v)=n} a_v}, \qquad \widetilde{\mathbb{E}}_{n,f}[C] = \frac{\sum_{\ell(v)=n} \widetilde{c}_v}{\sum_{\ell(v)=n} \widetilde{a}_v}. \tag{27}$$

We are mainly interested by some particular costs C.

Author's personal copy

5.2. Costs of interest

We now describe the main costs that intervene in this paper, defined on the set Ω of all the possible inputs. For each theorem, we consider two costs, the deterministic cost that we wish to study and the probabilistic cost (underlined) that we succeed to study. For Theorem 1, we consider the costs $C_1 := P_\delta$, $\underline{C}_1 = \underline{P}_\delta$ for $\delta \in [0, 1]$, defined by the relation (11). This means that

$$P_\delta(u, v) = k \qquad \text{iff} \qquad \lg u_k \le (1-\delta)\ell(u_0) < \lg u_{k-1}.$$

For Theorem 2, we consider the cost C_2 (which depends on the interval J),[5]

$$C_2 = [\![x_{\langle\delta\rangle} \in J]\!] \qquad \text{with} \quad x_{\langle\delta\rangle} := \frac{u_{k+1}}{u_k} \qquad \text{for} \quad k = P_\delta, \qquad \text{and} \quad \underline{C}_2 := [\![\underline{x}_{\langle\delta\rangle} \in J]\!].$$

Finally, for Theorem 4, we consider the cost C_4 (which depends on the interval J),

$$C_4(u, v) = Q_\delta(u, v) = \sum_{i=P_\delta(u,v)-2}^{P_\delta(u,v)} \ell(q_i), \qquad \text{and} \quad \underline{C}_4(u, v) := \sum_{i=\underline{P}_\delta(u,v)-2}^{\underline{P}_\delta(u,v)} \ell(q_i)$$

and, for Theorem 5, the costs $C_5 = \ell(u_{\langle\delta\rangle})$, $\underline{C}_5 := \ell(\underline{u}_{\langle\delta\rangle})$.

We first provide alternative expressions for Dirichlet series $\widetilde{F}_C(s)$, as a function of the transfer operator $\mathbf{H}_s$ relative to the Euclidean dynamical system. We first recall some basic facts about dynamical systems and transfer operators.

5.3. The Euclidean dynamical system

When computing the gcd of the integer-pair (u, v), Euclid's algorithm performs a sequence of divisions. A division $v = uq + r$ replaces the pair (u, v) with the new pair (r, u). If we consider now rationals instead of integer pairs, there exists a map T which replaces the (old) rational u/v by the (new) rational r/u, defined as

$$T(x) = \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor, \qquad T(0) = 0.$$

When extended to the real interval $I = [0, 1]$, the pair (I, T) defines the dynamical system relative to Euclid algorithm. We denote by $\mathcal{H}$ the set of the inverse branches of T,

$$\mathcal{H} = \left\{ h_{[q]} : x \to \frac{1}{q+x}; \quad q \ge 1 \right\},$$

and, more generally, by $\mathcal{H}^p$ the set of inverse branches of depth p (i.e., the set of inverse branches of T^p), namely $\mathcal{H}^p = \{h = h_1 \circ \cdots \circ h_p;\ h_i \in \mathcal{H}, \forall i\}$. With $\mathcal{H}^0 := \{\mathrm{Id}\}$, the set $\mathcal{H}^\star := \cup_{p\ge 0}\mathcal{H}^p$ is the set of all the possible inverse branches of any depth. Then, the Euclid algorithm on the input (u, v) builds a continued fraction

$$\frac{u}{v} = h(0) \qquad \text{with} \quad h = h_1 \circ h_2 \circ \cdots \circ h_p \in \mathcal{H}^p. \tag{28}$$

One then associates with each execution of the algorithm a unique LFT[6] $h \in \mathcal{H}^\star$ whose depth is exactly the number p of divisions performed. Remark that the i-th LFT h_i used by the algorithm is exactly the LFT relative to matrix $\mathcal{Q}_i$ of Section 2.1, so that the LFT $h_1 \circ h_2 \circ \cdots \circ h_i$ is relative to matrix $\mathcal{M}_{(i)}$ of Section 2.1. Then, the *CF*-expansion (28) of u/v, when split at depth i, creates two LFT's $b_i := h_1 \circ h_2 \circ \cdots \circ h_{i-1}$ and $e_i := h_i \circ \cdots \circ h_p$, defining each a rational number: the "beginning"

[5] The symbol $[\![B]\!]$ is known as the Iverson bracket and denotes a Boolean which equals 1 iff B is true.

[6] LFT is a compact notation for linear fractional transformation.

Author's personal copy

rational $b_i(0)$, and the "ending" rational $e_i(0)$. The "ending" rational $e_i(0)$ can be expressed with the remainder sequence (u_i)

$$e_i(0) := h_{i+1} \circ h_{i+2} \circ \cdots \circ h_p(0) = \frac{u_{i+1}}{u_i},$$

while the "beginning" rational $b_i(0)$ can be expressed with the two sequences (p_i), (r_i) related to coefficients of matrix $\mathcal{M}_{(i)}$ defined in (7),

$$b_i(0) := h_1 \circ h_2 \circ \cdots \circ h_{i-1}(0) = \frac{|p_i|}{|r_i|}.$$

The main parameters of interest of the Euclid Algorithm involve the denominators sequences u_i, r_i, which are called the continuants. The continuants are closely related to derivatives of LFT's, as we now explain. For any LFT h, the derivative $h'(x)$ can be expressed with the denominator function D: if the function D is defined by

$$D[g](x) = cx + d, \qquad \text{for } g(x) = \frac{ax+b}{cx+d} \qquad \text{with} \quad \gcd(a, b, c, d) = 1,$$

then

$$h'(x) = \frac{\det h}{D[h](x)^2}, \qquad \text{with} \quad \det h := ad - bc. \tag{29}$$

Finally, since any LFT $h \in \mathcal{H}^\star$ has a determinant of absolute value equal to 1, one has:

$$u_i = |b_i'(0)|^{-1/2}, \qquad r_i = |e_i'(0)|^{-1/2}. \tag{30}$$

5.4. Transfer operators

One of the main tools in dynamical systems theory is the transfer operator (Ruelle, 1978), denoted by $\mathbf{H}_s$. It generalises the density transformer $\mathbf{H}$ that describes the evolution of the density: if $f = f_0$ denotes the initial density on I, and f_1 the density on $\mathcal{I}$ after one iteration of T, then f_1 can be written as $f_1 = \mathbf{H}[f_0]$, where $\mathbf{H}$ is defined by

$$\mathbf{H}[f](x) = \sum_{h \in \mathcal{H}} |h'(x)| f \circ h(x). \tag{31}$$

It is useful to introduce a more general operator that depends on a complex parameter s,

$$\mathbf{H}_s[f](x) = \sum_{h \in \mathcal{H}} |h'(x)|^s f \circ h(x) = \sum_{m \geq 1} \frac{1}{(m+x)^{2s}} f\left(\frac{1}{m+x}\right),$$

and multiplicative properties of derivatives entail that

$$\mathbf{H}_s^p[f](x) = \sum_{h \in \mathcal{H}^p} |h'(x)|^s f \circ h(x), \qquad (I - \mathbf{H}_s)^{-1}[f](x) = \sum_{h \in \mathcal{H}^\star} |h'(x)|^s f \circ h(x).$$

Now, relation (29) between the denominator and the derivative of a LFT, and the fact that any element of $\mathcal{H}^\star$ has a determinant equal to ± 1, entail an alternative expression for the transfer operator,

$$\mathbf{H}_s^p[f](x) = \sum_{h \in \mathcal{H}^p} \frac{1}{D[h](x)^{2s}} f \circ h(x), \quad (I - \mathbf{H}_s)^{-1}[f](x) = \sum_{h \in \mathcal{H}^n} \frac{1}{D[h](x)^{2s}} f \circ h(x),$$

which will show, with (30) that the transfer operator can be viewed as a generating operator for denominator sequences u_i, r_i. This is the main idea on which is based the dynamical analyses. We now explain the relation between Dirichlet series and transfer operators.

Author's personal copy

5.5. The Dirichlet series $F_C(s)$

We describe alternative expression of the Dirichlet series $\widetilde{F}_C(s)$, $\widetilde{F}_C(s)$, as a function of operator $\mathbf{H}_s$. Let us begin with the trivial cost:

Cost $C_0 \equiv 1$. The Euclid algorithm writes each rational $u/v \in \widetilde{\Omega}$ in a unique way as $u/v = h(0)$ with $h \in \mathcal{H}^\star$. Then,

$$\widetilde{F}_0(2s) := \sum_{(u,v)\in\widetilde{\Omega}} \frac{1}{v^{2s}} f\left(\frac{u}{v}\right) = \sum_{k\geq 0} \sum_{h\in\mathcal{H}^k} |h'(0)|^s \cdot f\circ h(0) = (I-\mathbf{H}_s)^{-1}[f](0),$$

from which we deduce an alternative expression of $F_0(2s)$, with the help of the Riemann ζ function:

$$F_0(2s) = \sum_{d\geq 1} \sum_{(u,v)\in\widetilde{\Omega}} \frac{1}{(dv)^{2s}} f\left(\frac{\mathrm{d}u}{\mathrm{d}v}\right) = \zeta(2s)\,\widetilde{F}_0(2s) = \zeta(2s)\,(I-\mathbf{H}_s)^{-1}[f](0).$$

All the studies of the paper are based on refinements of the (simple) equality.

Cost C_1, $\underline{C}_1$ *for Theorem 1.* We will show in Section 6.4 that a main tool for studying the second cost P_δ on Ω, via its moment generating function $\mathbb{E}_{n,f}[\exp(wP_\delta)]$, is the Dirichlet series $G(2s, 2t, w)$ which depends on three parameters s, t, w and is equal to

$$G(2s, 2t, w) = \mathrm{e}^w \zeta(2s+2t)\,(I-\mathbf{H}_{s+t})^{-1} \circ (\mathbf{H}_s - \mathbf{H}_{s+t}) \circ (I-\mathrm{e}^w\mathbf{H}_s)^{-1}[f](0).$$

Cost C_2, $\underline{C}_2$ *for Theorem 2.* We will show in Section 6.1 that a main tool for studying the distribution of $x_{\langle\delta\rangle}$ on Ω (via the estimate of $\mathbb{P}_{n,f}[x_{\langle\delta\rangle} \in J]$) is the Dirichlet series which depends on two parameters s, t, together with the interval J,

$$F(2s, 2t, J) = \zeta(2s+2t)\,(I-\mathbf{H}_{s+t})^{-1}\left[1_J \cdot (\mathbf{H}_s - \mathbf{H}_{s+t}) \circ (I-\mathbf{H}_s)^{-1}[f]\right](0).$$

Cost C_4, $\underline{C}_4$ *for Theorem 4.* We will show in Section 6.7 that a main tool for studying the mean value of Q_δ is the Dirichlet series which depends on two parameters s, t,

$$\zeta(2s+2t)(I-\mathbf{H}_{s+t})^{-1}(\mathbf{H}_s - \mathbf{H}_{s+t}) \circ \left(\frac{\partial}{\partial w}\mathbf{H}^3_{s,w,[\ell]}\right)_{w=0} \circ (I-\mathbf{H}_s)^{-1}[f](0),$$

and involves the weighted transfer operator $\mathbf{H}_{s,w,[\ell]}$ relative to the binary size ℓ and defined as

$$\mathbf{H}_{s,w,[\ell]}[f](x) := \sum_{m\geq 1} \frac{\exp(w\ell(m))}{(m+x)^{2s}} f\left(\frac{1}{m+x}\right). \tag{32}$$

Cost C_5, $\underline{C}_5$ *for Theorem 5.* We will show in Section 6.8 that a main tool for studying the mean value of $\ell(u_{\langle\delta\rangle})$ is the Dirichlet series which depends on two parameters s, t,

$$\zeta(2s+2t)(I-\mathbf{H}_{s+t})^{-1} \circ \mathbf{H}'_{s+t} \circ (I-\mathbf{H}_{s+t})^{-1} \circ (\mathbf{H}_{s+t} - \mathbf{H}_s) \circ (I-\mathbf{H}_s)^{-1}[f](0),$$

and involves the operator $\mathbf{H}'_s := \mathrm{d}/(\mathrm{d}s)\mathbf{H}_s$ defined as

$$\mathbf{H}'_s[f](x) := -2\sum_{m\geq 1} \frac{\log(m+x)}{(m+x)^{2s}} f\left(\frac{1}{m+x}\right). \tag{33}$$

With alternative expressions of these Dirichlet series at hand, we now perform the second step: we find the dominant singularities of these Dirichlet series and their nature, and then transfer this information for obtaining asymptotic expressions of their coefficients. All the expressions previously obtained in this subsection involve the quasi-inverse $(I-\mathbf{H}_s)^{-1}$. This explains why the singularities of the Dirichlet series will be related to the dominant spectral objects of the transfer operator $\mathbf{H}_s$. A precise study of these spectral properties will lead to the asymptotic study of the coefficients of these Dirichlet series.

Author's personal copy

5.6. Spectral properties of the transfer operator $\mathbf{H}_s$

We now recall the main properties of the transfer operator $\mathbf{H}_s$ and its quasi-inverse $(I-\mathbf{H}_s)^{-1}$. These properties depend on the Banach space where the operator acts. Here, the Banach space is $\mathcal{C}^1(\mathcal{I})$, and we recall now the main properties of the operator $\mathbf{H}_s$, when acting on this functional space.

For $\Re(s) > 1/2$, the operator $\mathbf{H}_s$ acts on $\mathcal{C}^1(\mathcal{I})$ and the map $s \to \mathbf{H}_s$ is analytic. For $s = 1$, the operator is quasi-compact: there exists a spectral gap between the unique dominant eigenvalue (that equals 1, since the operator is a density transformer) and the remainder of the spectrum. By perturbation theory, these facts – existence of a dominant eigenvalue $\lambda(s)$ and of a spectral gap – remain true in a complex neighborhood $\mathcal{V}$ of $s = 1$. There, the operator splits into two parts: the part relative to the dominant eigensubspace, denoted $\mathbf{P}_s$, and the part relative to the remainder of the spectrum, denoted $\mathbf{N}_s$, whose spectral radius is strictly less than $\eta|\lambda(s)|$ (with $\eta < 1$). This leads to the following spectral decomposition

$$\mathbf{H}_s[f](x) = \lambda(s)\mathbf{P}_s[f](x) + \mathbf{N}_s[f](x),$$

which extends to the powers $\mathbf{H}_s^n$ of the operator

$$\mathbf{H}_s^n[f](x) = \lambda^n(s)\mathbf{P}_s[f](x) + \mathbf{N}_s^n[f](x), \tag{34}$$

and finally to the quasi-inverse $(\mathbf{I} - \mathbf{H}_s)^{-1}$

$$(I - \mathbf{H}_s)^{-1}[f](x) = \frac{\lambda(s)}{1-\lambda(s)}\mathbf{P}_s[f](x) + (\mathbf{I} - \mathbf{N}_s)^{-1}[f](x). \tag{35}$$

The first term on the right admits a pole (of order 1) at $s = 1$, while the second term is analytic on the half-plane $\{\Re(s) > 1\}$. The dominant eigenvalue $\lambda(s)$ is analytic in a neighborhood of $s = 1$, and the pressure function $\Lambda(s) := \log\lambda(s)$ plays an important rôle. In particular, near $s = 1$, one has

$$(I - \mathbf{H}_s)^{-1}[f](x) \sim \frac{-1}{\lambda'(1)}\varphi(x)\int_I f(t)\mathrm{d}t, \tag{36}$$

where $-\lambda'(1)$ is the entropy of the system, equal to $\pi^2/(6\log 2)$ and φ is the Gauss density, already mentioned in (1).

For Theorem 2, the Dirichlet series $(1/t)F(2s, 2t, J)$ defined in Section 5.5 can be viewed as a perturbation of

$$F_1(2s, J) := -(I - \mathbf{H}_s)^{-1}[\mathbf{1}_J \cdot \mathbf{H}_s' \circ (I - \mathbf{H}_s)^{-1}[f]](0),$$

for small t. This Dirichlet series $F_1(2s, J)$ involves the operator $\mathbf{H}_s' := (\mathrm{d}/\mathrm{d}s)\mathbf{H}_s$, has a pôle of order 2 at $s = 1$, and satisfies for s close to 1, with (36)

$$F_1(2s, J) \sim \frac{-1}{(s-1)^2}\left(\frac{1}{\lambda'(1)}\right)^2\varphi(0)\left(\int_J \mathbf{H}'[\varphi](t)\mathrm{d}t\right),$$

where $\mathbf{H}' := \mathbf{H}_1'$ and φ is the Gauss density defined in (1). This explains why $\psi = \mathbf{H}'[\varphi]$ introduced in (2) plays a central rôle in our analyses.

5.7. US *Property for the Dirichlet series* $F_C(s)$

We have obtained a first information about the singularities of the quasi-inverse $(I - \mathbf{H}_s)^{-1}$ and an alternative expression of $\widetilde{F_C}(s)$ as a function of this quasi-inverse. We now wish to perform the second step and transfer this information for obtaining asymptotic expressions of the coefficients of the Dirichlet series. As a main tool, we rely on convenient "extractors" which express coefficients of series as a function of the series itself. There exist an easy "extractor" for Dirichlet series: the (plain) Tauberian Theorems. However, they do not provide remainder terms, and they are not adapted for our study, since we wish to obtain uniform estimates with respect to auxiliary parameters δ, w, t, J. We then adopt the Perron Formula, which may provide remainder terms, as soon as we have a precise knowledge of $\widetilde{F_C}(s)$ on vertical strips.

Author's personal copy

The Perron Formula of order two (see Ellison and Ellison (1985)) is valid for a Dirichlet series $F(s) = \sum_{n\geq 1} \frac{a_n}{n^{2s}}$ and a vertical line $\Re s = D > 0$ inside the convergence domain of F,

$$\Psi(T) := \sum_{n\leq T} a_n(T-n) = \frac{1}{2i\pi} \int_{D-i\infty}^{D+i\infty} F(s) \frac{T^{2s+1}}{s(2s+1)}\, ds. \tag{37}$$

It is next natural to modify the integration contour $\Re s = D$ into a contour which contains a unique pole of $F(s)$, and it is thus useful to know that the Property *US* [Uniform Estimates on Strips] holds. We have already described this Property in an informal way in Section 1.3. It is now necessary to describe it more precisely.

Theorem A (*US Property for the Euclidean Dynamical System (Dolgopyat, 1998; Baladi and Vallée, 2005)*). *When the transfer operator $\mathbf{H}_s$ relative to the Euclidean dynamical system acts on the functional space $\mathcal{C}^1(\mathcal{I})$ of functions with a continuous derivative on the unit interval $\mathcal{I} := [0, 1]$, there exists $\alpha > 0$ for which the following holds on the strip $\mathcal{S} := \{s, 1-\alpha \leq \Re s \leq 1\}$.*

(i) *The quasi-inverse $(I - \mathbf{H}_s)^{-1}$ has a unique pôle in the vertical strip $\mathcal{S} := \{s, |\Re s - 1| \leq \alpha\}$, located at $s = 1$.*

(ii) *There exist $t_0 > 0, \xi < 1/5, C > 0$, such that, on the truncated strip $\{s, |\Re s - 1| \leq \alpha, |\Im s| \geq t_0\}$, letting $t := \Im s$,*

$$\|(I - \mathbf{H}_s)^{-1}\|_{1,t} = O\left(|\Im s|^{\xi}\right) \qquad \text{with} \quad \|f\|_{1,t} := \sup|f| + (1/t)\sup|f'|.$$

From works of Dolgopyat (1998) and Baladi and Vallée (2005), we know that $(I - \mathbf{H}_s)^{-1}$ satisfies the *US* Property, with a strip of width $\alpha > 0$. With this *US*-Property, we can shift the integration contour in (37). If, for instance

$$F(s) = (1 - \mathbf{H}_{s+t})^{-1}[g](0) := \sum_{n\geq 1} \frac{a_n(t)}{n^{2s}},$$

we obtain

$$\Psi(T) := \sum_{n\leq T} a_n(T-n) = \mathrm{Res}_{s=1-t}\left(\frac{T^{2s+1}}{s(2s+1)}F(s)\right) + \frac{1}{2i\pi}\int_{\Re s=1-t-\alpha} F(s)\frac{T^{2s+1}}{s(2s+1)}\, ds.$$

Finally, if the pole is simple, the residue is not zero, and the following estimate shows the importance of the parameter σ, defined as a lower bound for this width α, since it intervenes in the remainder term, as

$$\Psi(T) = \frac{T^{3-2t}}{(1-t)(3-2t)}\mathrm{Res}_{s=1-t}F(s)\left[1 + O(T^{-2\sigma})\right]. \tag{38}$$

The real σ mentioned in all our Theorems 1–7 is a lower bound for this width α.

6. Proofs of Theorems 1 and 2

Here, we provide the complete proofs of Theorems 1 and 2. We first recall some notations. On an input (u, v), the Euclid algorithm builds a sequence of remainders (u_k) and a sequence of rationals $x_k = u_{k+1}/u_k$.

We recall that $P_\delta(u, v)$ is the smallest integer k for which $\lg u_k$ is less than $(1-\delta)\ell(u_0)$. We are interested in describing the position of the rational

$$x_{\langle\delta\rangle} := x_k \qquad \text{when} \quad P_\delta(u, v) = k.$$

6.1. Proof of Theorem 2 — Step 1. The Dirichlet series of interest

We here provide an estimate of the distribution of the rational $\underline{x}_{\langle\delta\rangle}$, which is a probabilistic version of the rational $x_{\langle\delta\rangle}$.

Author's personal copy

We first deal with intermediate sets $\mathcal{V}^{(k)}_{N,M}(J),\ \mathcal{U}^{(k)}_{N,M}(J)$, defined as

$$\mathcal{V}^{(k)}_{N,M}(J) := \{(u,v)\in\Omega;\quad v=N,\ u_{k+1}=M,\ x_{k+1}\in J\}$$
$$\mathcal{U}^{(k)}_{N,M}(J) := \{(u,v)\in\Omega,\quad v=N, u_k=M,\ x_{k+1}\in J\}$$

and the set[7]

$$\mathcal{A}_N(W,J) := \sum_{k\geq 0}\left[\left(\sum_{M\leq W}\mathcal{V}^{(k)}_{N,M}(J)\right)\setminus\left(\sum_{M\leq W}\mathcal{U}^{(k)}_{N,M}(J)\right)\right] \tag{39}$$

gathers the pairs (u,v) of Ω with $v=N$ for which the following is true: "if k denotes the smallest index for which the remainder u_k has a denominator at most W, the rational x_k belongs to J". This shows that these intermediate sets will be closely related to our problem.

We now observe two facts: The f-weights $\widetilde{u}^{(k)}_{N,M}(J)$, $\widetilde{v}^{(k)}_{N,M}(J)$ of the tilded version of the intermediate sets

$$\widetilde{\mathcal{V}}^{(k)}_{N,M}(J) := \mathcal{V}^{(k)}_{N,M}(J)\cap\widetilde{\Omega},\qquad \widetilde{\mathcal{U}}^{(k)}_{N,M}(J) := \mathcal{U}^{(k)}_{N,M}(J)\cap\widetilde{\Omega}$$

are easily generated by the transfer operator, since the two following equalities hold

$$\widetilde{U}(2s,2t,J,k) := \sum_{N\geq 1}\sum_{M\geq 1}\frac{\widetilde{u}^{(k)}_{N,M}(J)}{N^{2s}M^{2t}} = (I-\mathbf{H}_{s+t})^{-1}\left[1_J\cdot\mathbf{H}_{s+t}\circ\mathbf{H}_s^k[f]\right](0) \tag{40}$$

$$\widetilde{V}(2s,2t,J,k) := \sum_{N\geq 1}\sum_{M\geq 1}\frac{\widetilde{v}^{(k)}_{N,M}(J)}{N^{2s}M^{2t}} = (I-\mathbf{H}_{s+t})^{-1}\left[1_J\cdot\mathbf{H}_s^{k+1}[f]\right](0). \tag{41}$$

On the other hand, there are nice relations between $\mathcal{V}^{(k)}_{N,M}(J),\ \mathcal{U}^{(k)}_{N,M}(J)$ and their tilded versions, as we now explain. Each of these two sets $\mathcal{V}^{(k)}_{N,M}(J),\ \mathcal{U}^{(k)}_{N,M}(J)$ decomposes as a disjoint union

$$\mathcal{V}^{(k)}_{N,M}(J) = \sum_{d\geq 1}\left(\mathcal{V}^{(k)}_{N,M}(J)\cap\Omega_{[d]}\right),\qquad \mathcal{U}^{(k)}_{N,M}(J) = \sum_{d\geq 1}\left(\mathcal{U}^{(k)}_{N,M}(J)\cap\Omega_{[d]}\right),$$

which involves the set $\Omega_{[d]}$ of pairs (u,v) of Ω for which $\gcd(u,v)=d$; the map $(u,v)\mapsto(du,dv)$ defines two bijections which preserve the f-weights,

- first from $\widetilde{\mathcal{V}}^{(k)}_{N,M}(J)$ onto $\left(\mathcal{V}^{(k)}_{dN,dM}(J)\cap\Omega_{[d]}\right)$,
- second from $\widetilde{\mathcal{U}}^{(k)}_{N,M}(J)$ onto $\left(\mathcal{U}^{(k)}_{dN,dM}(J)\cap\Omega_{[d]}\right)$.

Then, the Dirichlet series U, V and their tilded versions $\widetilde{U},\widetilde{V}$ are related via the Riemann ζ function, as follows:

$$U(s,t,J,k) := \sum_{N\geq 1}\sum_{M\geq 1}\frac{u^{(k)}_{N,M}(J)}{N^sM^t} = \zeta(s+t)\,\widetilde{U}(s,t,J,k), \tag{42}$$

$$V(s,t,J,k) := \sum_{N\geq 1}\sum_{M\geq 1}\frac{v^{(k)}_{N,M}(J)}{N^sM^t} = \zeta(s+t)\,\widetilde{V}(s,t,J,k). \tag{43}$$

Finally, the series $F(s,t,J)$ defined as

$$F(s,t,J) := \sum_{k\geq 0}[V(s,t,J,k)-U(s,t,J,k)] \tag{44}$$

[7] The sum $A+B$ between sets A, B replaces the union $A\cup B$ when A and B are disjoint.

Author's personal copy

admits with (42), (43), (40) and (41) the alternative expression which involves the ζ function and the transfer operator $\mathbf{H}_s$

$$F(2s, 2t, J) := \zeta(2s+2t)(I - \mathbf{H}_{s+t})^{-1}\left[1_J \cdot (\mathbf{H}_s - \mathbf{H}_{s+t}) \circ (I - \mathbf{H}_s)^{-1}[f]\right](0). \tag{45}$$

On the other hand, $F(s, t, J)$ is a Dirichlet series of the form

$$F(s, t, J) = \sum_{N\geq 1}\sum_{M\geq 1} \frac{a_{N,M}(J)}{N^s M^t}$$

whose coefficient $a_{N,M}(J)$ satisfies the following, with the definition of F given in (44),

$$\begin{aligned}\sum_{M\leq W} a_{N,M}(J) &= \sum_{M\leq W}\sum_{k\geq 0}\left(v^{(k)}_{N,M}(J) - u^{(k)}_{N,M}(J)\right)\\ &= \sum_{k\geq 0}\left[\left(\sum_{M\leq W} v^{(k)}_{N,M}(J)\right) - \left(\sum_{M\leq W} u^{(k)}_{N,M}(J)\right)\right],\end{aligned}$$

and the last expression is exactly the f-weight of the set $\mathcal{A}_N(W, J)$ defined in (39). Finally, the equality

$$\sum_{N=2^{n-1}}^{2^n} \mathcal{A}_N(2^{(1-\delta)n}, J) = \{(u, v) \in \Omega_n;\, x_{\langle\delta\rangle} \in J\}$$

holds and entails the equality

$$\mathbb{P}_{n,f}[x_{\langle\delta\rangle} \in J] = \frac{1}{|\Omega_n|_f}\sum_{N=2^{n-1}}^{2^n-1}\sum_{M\leq 2^{(1-\delta)n}} a_{N,M}(J),$$

where $|\Omega_n|_f$ is just the f-weight of Ω_n. Comparing the Riemann sum with the integral entails

$$|\Omega_n|_f := \sum_{(u,v)\in\Omega_n} f\left(\frac{u}{v}\right) = \sum_{v=2^{n-1}}^{2^n-1}\sum_{u<v} f\left(\frac{u}{v}\right) = |\Omega_n|\left[1 + 2^{-n}O(\|f\|_1)\right].$$

For studying the $I(\delta)$ probabilistic version $\underline{x}_{\langle\delta\rangle}$, we are led to evaluate the expression

$$\mathbb{P}_{n,f}[\underline{x}_{\langle\delta\rangle} \in J] = \frac{1}{|\Omega_n|_f}\sum_{N=2^{n-1}}^{2^n-1}\frac{1}{|I_n(\delta)|}\sum_{W_1\in I_n(\delta)}\sum_{M\leq W_1} a_{N,M}(J).$$

Since $|\Omega_n| = (3/4)2^{2n}$, we have finally to evaluate

$$\frac{1}{|I_n(\delta)|}\sum_{N=2^{n-1}}^{2^n-1}\sum_{W_1\in I_n(\delta)}\sum_{M\leq W_1} a_{N,M}(J),$$

which is a particular case of

$$E_0(T, W, W_-) := \frac{1}{W - W_-}\sum_{N=T/2}^{T}\sum_{W_1=W_-}^{W}\sum_{M\leq W_1} a_{N,M}(J), \tag{46}$$

where T and W are polynomially related.

It is then sufficient to extract coefficients from the Dirichlet series $F(s, t, J)$ given in (45). However, it is not possible to directly deal with the characteristic function of the interval J, since it does not belong to the "convenient" functional space $\mathcal{C}^1(I)$ where the Property *US* holds. Then, for a function ε

Author's personal copy

positive which satisfies $\varepsilon(x) \le x$, we replace the function $\mathbf{1}_J$ by two functions $\psi^+_{(J,\varepsilon)}$ and $\psi^-_{(J,\varepsilon)}$ of $\mathcal{C}^1(I)$ which are good approximations of $\mathbf{1}_J$, and satisfy $\psi^-_{(J,\varepsilon)} \le \mathbf{1}_J \le \psi^+_{(J,\varepsilon)}$,

$$\left\|\psi^{\pm}_{(J,\varepsilon)}\right\|_1 \le \frac{1}{\varepsilon(|J|)}, \tag{47}$$
$$\int_I \left|\psi^{\pm}_{(J,\varepsilon)}\right|(u)\,\mathrm{d}u \le |J| + \varepsilon(|J|), \quad \int_I \left|\psi^{+}_{(J,\varepsilon)} - \psi^{-}_{(J,\varepsilon)}\right|(u)\,\mathrm{d}u \le \varepsilon(|J|).$$

We replace the Dirichlet series $F(s,t,J)$ by the series $F^+(s,t,J,\varepsilon)$, $F^-(s,t,J,\varepsilon)$ defined as

$$F^{\pm}(2s,2t,J,\varepsilon) = \zeta(2s+2t)(I-\mathbf{H}_{s+t})^{-1}\left[\psi^{\pm}_{(J,\varepsilon)}\cdot(\mathbf{H}_s-\mathbf{H}_{s+t})\circ(I-\mathbf{H}_s)^{-1}[f]\right](0). \tag{48}$$

The coefficients of these series, denoted by $a^{\pm}_{N,M}(J,\varepsilon)$, have the following combinatorial sense: The sum of these coefficients

$$\sum_{M\le W} a^{\pm}_{N,M}(J,\varepsilon) \tag{49}$$

equals the sum, taken over all pairs (u,v) with $v=N$, of the quantities $f(x_k)\cdot\psi^{\pm}_{(J,\varepsilon)}(x_k)$, where x_k is the rational relative to the smallest index k for which u_k is less than W.

We have introduced several objects X for which there exist related objects X^+, X^-, for instance, the Dirichlet series $F(s,t,J)$, the coefficients $a_{N,M}(J,\varepsilon)$, etc. We denote by X^Δ the difference $X^+ - X^-$ and by $X^\diamond$ any element of the set $\{X^+, X^-, X^\Delta\}$. Then, the inequalities

$$\sum_{M\le W} a^-_{N,M}(J,\varepsilon) \le \sum_{M\le W} a_{N,M}(J) \le \sum_{M\le W} a^+_{N,M}(J,\varepsilon) \tag{50}$$

show that our main object of interest $E_0(T,W,W_-)$ defined in (46) can be evaluated with the help of the various $E_0^\diamond(T,W,W_-)$, via the relation

$$E_0(T,W,W_-) = E_0^-(T,W,W_-) + O\left(E_0^\Delta(T,W,W_-)\right). \tag{51}$$

It is then sufficient to deal with the series $F^\diamond(s,t,J,\varepsilon)$, defined in (48).

6.2. Proof of Theorem 2 — Step 2. Extraction via the Perron Formula

The series $F^\diamond$ defined in (48) depends on two complex variables s and t (with J and ε as parameters). We will use the Perron Formula, two times.

First, suppose that the complex s is fixed, satisfies $\Re s > 1$ and consider the Dirichlet series $F^\diamond$ as a function of t, which has an only pôle at $t = 1-s$ in the strip $1-\alpha < \Re(s+t) < 1+\alpha$. Then, with the Perron formula (see Section 5.7)

$$\sum_{W_1\le W}\sum_{M\le W_1}\sum_{N\ge 1}\frac{a^\diamond_{N,M}(J,\varepsilon)}{N^{2s}} = \zeta(2)\frac{W^{2(1-s)+1}}{(3-2s)}\frac{\varphi(0)}{\lambda'(1)}\int_I \psi^\diamond_{(J,\varepsilon)}(u) \times\left[\left(\frac{\mathbf{H}_s-\mathbf{H}_1}{s-1}\right)\circ(1-\mathbf{H}_s)^{-1}[f]\right](u)\mathrm{d}u + \frac{1}{2\mathrm{i}\pi}\int_{\Re(s+t)=1-\alpha}\frac{W^{2t+1}}{t(2t+1)}F^\diamond(2s,2t,J,\varepsilon)\mathrm{d}t.$$

This is now a Dirichlet series with respect to s, which has an only pôle at $s=1$ in the strip $1-\beta < \Re s < 1+\beta$, and using again the Perron Formula for extracting coefficients, we finally obtain four terms for the sum of coefficients

$$E_1^\diamond(T,W) := \sum_{T_1\le T}\sum_{N\le T_1}\sum_{W_1\le W}\sum_{M\le W_1} a^\diamond_{N,M}(J,\varepsilon),$$

Author's personal copy

namely, defining domains $\Gamma_0 = \{s \in \mathbb{C} \mid \Re s = 1-\beta\}$, $\Gamma_1 = \{t \in \mathbb{C} \mid \Re t = -\alpha\}$ and $\Gamma_2 = \{(s,t) \in \mathbb{C}^2 \mid \Re t = \beta - \alpha \text{ and } \Re s = 1-\beta\}$,

$$
\begin{aligned}
&-\zeta(2)\frac{\varphi(0)}{\lambda'(1)^2}\frac{T^3}{3}W\int_I \psi^{\diamond}_{(J,\varepsilon)}(u)\mathbf{H}'[\varphi](u)\mathrm{d}u\\
&-\frac{\zeta(2)\varphi(0)}{2i\pi\lambda'(1)}\int_{\Gamma_0}\frac{T^{2s+1}}{s(2s+1)}\frac{W^{2(1-s)+1}}{(3-2s)(1-s)}\left(\int_I \psi^{\diamond}_{(J,\varepsilon)}(u)\cdot(\mathbf{H}_s-\mathbf{H}_1)\circ(I-\mathbf{H}_s)^{-1}[f](u)\mathrm{d}u\right)\mathrm{d}s\\
&+\frac{1}{2i\pi}\frac{T^3}{3}\int_{\Gamma_1}\zeta(2+2t)\frac{W^{2t+1}}{t(2t+1)}(I-\mathbf{H}_{1+t})^{-1}\left[\psi^{\diamond}_{(J,\varepsilon)}\cdot(\mathbf{H}_1-\mathbf{H}_{1+t})\left[\frac{\varphi}{-\lambda'(1)}\right]\right](0)\,\mathrm{d}t\\
&-\int_{\Gamma_2}\frac{\zeta(2s+2t)}{4\pi^2}\frac{T^{2s+1}}{s(2s+1)}\frac{W^{2t+1}}{t(2t+1)}(I-\mathbf{H}_{s+t})^{-1}\\
&\quad\times\left[\psi^{\diamond}_{(J,\varepsilon)}\cdot(\mathbf{H}_s-\mathbf{H}_{s+t})\circ(I-\mathbf{H}_s)^{-1}[f]\right](0)\mathrm{d}s\,\mathrm{d}t.
\end{aligned}
$$

If we choose $\alpha=\beta$, it seems that the fourth term has a pôle at $t=0$, but this is not a "true" pôle, since there is an occurrence of a secant operator, of the form $(1/t)(\mathbf{H}_{s+t}-\mathbf{H}_s)$ which tends to the operator $\mathbf{H}'_s$ when $t\to 0$. We then choose $\alpha=\beta$, and, for reasons which will appear later, due in particular to possible applications of Proposition A (see Appendix), we choose $\alpha=\beta=\underline{\sigma}:=\min(\sigma,1/2)$.

The first term will provide the main term. For $E_1^{\pm}(T,w)$, it is $\Theta(T^3W)$, more precisely equivalent to

$$
a(J)\frac{T^3}{3}W \qquad \text{with} \quad a(J)=\frac{1}{\lambda'(1)}\int_J \mathbf{H}'[\varphi](t)\mathrm{d}t=\int_J\psi(t)\mathrm{d}t. \tag{52}
$$

(For the computation of the constant $a(J)$, we used the equality $\zeta(2)=-\lambda'(1)\log 2$ which comes from spectral properties at $s=1$ described in Section 5.6). Then Theorem A (Section 5.7) entails estimates for the four terms of $E_1^{\diamond}(T,W)$. Furthermore, the constants involved in the O-terms depend only on J and ε, but not in the same way for all the terms: in the first two terms, the interval J intervenes via the integral of the function $\psi^{\diamond}_{(J,\varepsilon)}$, whereas, in the last two terms, the interval J intervenes via the norm $\|\cdot\|_{1,1}$ of the function $\psi^{\diamond}_{(J,\varepsilon)}$. Finally, with Theorem A, and (47), each $E_1^{\diamond}(T,W)$ can be written as

$$
E_1^{\diamond}(T,W)=a(J)\frac{T^3}{3}W\cdot\left[\sum_{i=1}^{4}A_j^{\diamond}(T,W)\right]
$$

with

$$
\begin{aligned}
&A_1^{\pm}(T,W)=1+O\left(\frac{\varepsilon(|J|)}{|J|}\right), \qquad A_1^{\Delta}(T,W)=O\left(\frac{\varepsilon(|J|)}{|J|}\right),\\
&A_3^{\diamond}(T,W)=O\left(\frac{1}{|J|\varepsilon(|J|)}\right)W^{-2\underline{\sigma}}, \qquad A_4^{\diamond}(T,W)=O\left(\frac{1}{|J|\varepsilon(|J|)}\right)T^{-2\underline{\sigma}},\\
&A_2^{\pm}(T,W)=O\left(1+\frac{\varepsilon(|J|)}{|J|}\right)\left(\frac{T}{W}\right)^{-2\underline{\sigma}}, \qquad A_2^{\Delta}(T,W)=O\left(\frac{\varepsilon(|J|)}{|J|}\right)\left(\frac{T}{W}\right)^{-2\underline{\sigma}}.
\end{aligned} \tag{53}
$$

Remark that $A_1^{\diamond}$ does not depend on (T,W) while $A_2^{\diamond}$ depends only on (T/W) and $A_3^{\diamond}$ only depends on W. Moreover, in view of applying propositions of the Appendix, we remark the following: since there is a polynomial of degree 4 in the denominator of the integral that defines the term $A_2^{\diamond}$, it is possible to take the derivative two times, and this defines a function $(T,W)\mapsto A_2^{\diamond}(T,W)$ of class $\mathcal{C}^2$. Finally, the terms

$$
F_1^{\diamond}(T,W):=\sum_{i=1}^{3}A_j^{\diamond}(T,W), \qquad H_1^{\diamond}(T,W):=\sum_{i=1}^{2}A_j^{\diamond}(T,W)
$$

Author's personal copy

define a function $T \mapsto F_1^{\diamond}(T, W)$ of class $\mathcal{C}^2$, and a function $W \mapsto H_1^{\diamond}(T, W)$ of class $\mathcal{C}^2$. Moreover, if we consider the notion of uniform order given at the beginning of Section 7, it is clear that each term A_i is of uniform order with respect to the convenient variables, and, each of the two derivatives of A_2 is of uniform order.

6.3. Proof of Theorem 2 — Step 3. Final estimates for variable $\underline{x}_{\langle\delta\rangle}$ on Ω

This step can be decomposed into three sub-steps.

Step 3 (a): *The triple (W, J, ε) is fixed, the variable is T.* The sums $\sum_{M\le W} a_{N,M}^{\diamond}(J, \varepsilon)$ are positive, so that the functions

$$T \mapsto E_2^{\diamond}(T, W) := \sum_{N\le T} \sum_{W_1\le W} \sum_{M\le W_1} a_{N,M}^{\diamond}(J, \varepsilon)$$

are increasing. Then, it is possible to transform in $E_1^{\diamond}(T, W)$ the double sum over indices N into a simple sum with Proposition B of the Appendix and deduce from the estimates of $E_1^{\diamond}(T, W)$ estimates for the sums

$$E_2^{\diamond}(T, W) = a(J)\, T^2 W \left[F_2^{\diamond}(T, W) + O(T^{-\underline{\sigma}})\right],$$

with $F_2^{\diamond}(T, W) := F_1^{\diamond}(T, W) + (T/3)(\mathrm{d}/\mathrm{d}T)F_1^{\diamond}(T, W)$. We will be interested in the following by $E^{\diamond}(T, W) := E_2^{\diamond}(T, W) - E_2^{\diamond}(T/2, W)$ for which we get the estimate

$$E^{\diamond}(T, W) = \frac{3}{4}\, a(J)\, T^2 W \left[F^{\diamond}(T, W) + O(T^{-\underline{\sigma}})\right], \tag{54}$$

where $F^{\diamond}(T, W) := (4/3)F_2^{\diamond}(T, W) - (1/3)F_2^{\diamond}(T/2, W)$ defines a function $T \mapsto F^{\diamond}(T, W)$ of class $\mathcal{C}^1$. Applying now Proposition A of Section 7 in case (WB), with the choice $(T - T_-)/T = \Theta(T^{-x})$ (always, for each value of the triple (W, J, ε) fixed) provides the estimate

$$\frac{E^{\diamond}(T, W) - E^{\diamond}(T_-, W)}{T - T_-} = \frac{3}{2}\, a(J)\, TW \times \left[A_1^{\diamond} + O(W^{-2\underline{\sigma}}) + O\left(\left(\frac{T}{W}\right)^{-2\underline{\sigma}}\right) + O(T^{-\underline{\sigma}+x}) + O(T^{-x})\right]. \tag{55}$$

Step 3 (b): *The pair (J, ε) is fixed, T and W are polynomially related.* We let $T = W^{\nu}$. Then, ν and our initial parameter δ are related via the equality $1/\nu = 1-\delta$, and the parameter $\nu \ge 1$ is unbounded for $\delta \in]0, 1]$. We wish to obtain an estimate of our main object of interest $E_0^{\diamond}(W^{\nu}, W, W_-)$, (uniformly with respect to ν),

$$E_0^{\diamond}(W^{\nu}, W, W_-) = \frac{E^{\diamond}(W^{\nu}, W) - E^{\diamond}(W^{\nu}, W_-)}{W - W_-}.$$

First, observe the following decomposition of $E^{\diamond}(W^{\nu}, W) - E^{\diamond}(W^{\nu}, W_-)$ as

$$\left[E^{\diamond}(W^{\nu}, W) - E^{\diamond}(W_-^{\nu}, W_-)\right] - \left[E^{\diamond}(W^{\nu}, W_-) - E^{\diamond}(W_-^{\nu}, W_-)\right]. \tag{56}$$

For the first term of (56), relation (54) entails the estimate

$$E^{\diamond}(W^{\nu}, W) = \frac{3}{4}\, a(J)\, W^{2\nu+1}\left[H^{\diamond}(W) + O(W^{-2\underline{\sigma}}) + O(W^{-\nu\underline{\sigma}})\right],$$

where $H^{\diamond}(W)$ "comes from" $H_1^{\diamond}(W^{\nu}, W)$ after transforming it in the same way which transforms F_1 into F. Then, $W \mapsto H^{\diamond}(W)$ is of class $\mathcal{C}^1$. Applying Proposition A in case (WU) with the choice $(W - W_-)/W := (1/\nu)\Theta(W^{-y})$ provides the estimate

$$\frac{E^{\diamond}(W^{\nu}, W) - E^{\diamond}(W_-^{\nu}, W_-)}{W - W_-} = \frac{3}{4}\,(2\nu + 1)\, a(J)\, W^{2\nu} \times \left[A_1^{\diamond} + O(W^{-2(\nu-1)\underline{\sigma}}) + O\left(W^{-y}\right) + O\left(W^{-2\underline{\sigma}+y}\right) + O(W^{-\nu\underline{\sigma}+y})\right]. \tag{57}$$

Author's personal copy

For the second term of (56), we take the same choice for $(W - W_-)/W$, which leads to the choice

$$\frac{T - T_-}{T_-} = \frac{W^\nu - W_-^\nu}{W_-^\nu} = \nu \frac{W - W_-}{W}[1 + O(W^{-y})] = \Theta\left(W^{-y}\right).$$

Using now (55) with $T^{-x} = W^{-y}$ (i.e., $y = \nu x$) leads to an estimate for

$$\frac{E^\diamondsuit(W^\nu, W_-) - E^\diamondsuit(W_-^\nu, W_-)}{W - W_-}$$

of the form

$$\frac{3}{2} a(J)\, W^{\nu+1}\left[\nu W^{\nu-1}\right]\left[A_1^\diamondsuit + O(W^{-2\underline{\sigma}}) + O(W^{-2(\nu-1)\underline{\sigma}}) + O(W^{-\nu\underline{\sigma}+y}) + O(W^{-y})\right]. \tag{58}$$

Finally, using (56)–(58) and choosing

$$y = \frac{1}{2}\underline{\sigma}\min(\nu, 2), \qquad \frac{W - W_-}{W} = \frac{1}{\nu}\Theta(W^{-y}), \qquad T = W^\nu, \tag{59}$$

together with the precise estimates of terms $A_i^\diamondsuit(T, W)$ given in (53) leads to the final estimates for $E_0^\diamondsuit(T, W, W_-)$, namely

$$E_0^\pm(T, W, W_-) = \frac{3}{4} a(J) W^{2\nu}\left[1 + \nu O\left(R^\pm(W)\right)\right]$$
$$E_0^\Delta(T, W, W_-) = \frac{3\nu}{4}\, a(J) W^{2\nu}\, O\left(R^\Delta(W)\right),$$

with

$$R^\pm(W) = \max\left(\frac{\varepsilon(|J|)}{|J|}, W^{-2(\nu-1)\underline{\sigma}}, \frac{1}{|J|\varepsilon(|J|)} W^{-y}\right)$$
$$R^\Delta(W) = \max\left(\frac{\varepsilon(|J|)}{|J|}, \frac{1}{|J|\varepsilon(|J|)} W^{-y}\right).$$

This entails the final estimate for the "true" $E_0(T, W, W_-)$ for $T = W^\nu$ and $(W - W_-)/W$ as in (59),

$$E_0(T, W, W_-) = \frac{3}{4} a(J) W^{2\nu}\left[1 + \nu O\left(\frac{\varepsilon(|J|)}{|J|}, \frac{1}{|J|\varepsilon(|J|)} W^{-y}, W^{-2(\nu-1)\underline{\sigma}}\right)\right]. \tag{60}$$

Step 3 (c): (T, W, J, ε) *are polynomially related.* We now consider the case when the function ε (which quantifies the approximation of the characteristic function $\mathbf{1}_J$) is a power function, of the form $x \mapsto x^{1+\theta}$. We suppose that all our parameters $X \in \{|J|, \varepsilon(|J|), T, W\}$ have an exponential dependence on n (now J and ε vary), and we fix their exponents $e(X) := n^{-1} \lg X$ as

$$e(T) = 1, \qquad e(W) = (1 - \delta) = \frac{1}{\nu}, \qquad e(|J|) = -2\gamma, \qquad e(\varepsilon(|J|)) = -2\gamma(1 + \theta).$$

Then, the exponents of the three terms in the remainder term of (60) are at least equal to

$$\tau := \min\left(2\gamma\theta,\ \rho(\delta) - 2\gamma(\theta + 2),\ 2\underline{\sigma}\delta\right), \qquad \text{with} \quad \rho(\delta) := \underline{\sigma}\min\left(\frac{1}{2}, 1 - \delta\right).$$

We first choose the exponent of the function $\varepsilon : x \mapsto x^{1+\theta}$ in order to equalise the first two exponents. Since the exponent θ must be strictly positive, this is only possible for $\gamma < (1/4)\rho(\delta)$ and, in this case, the best choice of θ leads to

$$\tau = \tau_1(\delta, \gamma) := \min\left(\frac{1}{2}\rho(\delta) - 2\gamma,\ 2\underline{\sigma}\delta\right).$$

Author's personal copy

Consider now the case when the interval J is large enough (with respect to $\underline{\sigma}$, and the fraction $(1-\delta)$), so that the exponent $-e(|J|)$ satisfies $-e(|J|) = 2\gamma < (1/4)\rho(\delta)$. Then, there is a lower bound $\tau(\delta)$ for $\tau_1(\delta, \gamma)$, which depends only on $\underline{\sigma}$ and δ, with

$$\tau(\delta) := \underline{\sigma} \min\left(\frac{1}{8}, \frac{1-\delta}{4}, 2\delta\right). \tag{61}$$

Step 3 (d): *Conclusion.* We return to our initial problem, and with (60), together with the definition of the interval

$$I_n(\delta) := \left[2^{(1-\delta)n}\left(1-(1-\delta)2^{-\rho(\delta)n}\right), 2^{(1-\delta)n}\right], \qquad \text{with} \quad \rho(\delta) := \underline{\sigma} \min\left(\frac{1}{2}, 1-\delta\right),$$

the definition of $\tau(\delta)$ given in (61) and the expression of $a(J)$ in (52), we obtain an estimate for

$$\sum_{N=2^{n-1}}^{2^n-1} \frac{1}{|I_n(\delta)|} \sum_{W\in I_n(\delta)} \sum_{M\le W} a_{N,M}(J) = \left(\frac{3}{4}2^{2n}\right)\left(\int_J \psi(t)\mathrm{d}t\right)\left[1+\frac{1}{1-\delta}O(2^{-n\tau(\delta)})\right].$$

Since all our estimates are uniform with respect to δ, it is then possible to obtain the same results for a sequence δ_n (which may depend on the size n). Since the first term equals the cardinality of Ω_n, this leads (as we already explained in Section 6.1) to the estimate of the probability

$$\mathbb{P}_{n,f}[\underline{x}_{\langle\delta\rangle} \in J] = \frac{1}{|\Omega_n|_f} \sum_{N=2^{n-1}}^{2^n-1} \frac{1}{|I_n(\delta)|} \sum_{W\in I_n(\delta)} \sum_{M\le W} a_{N,M}(J).$$

Here, the variable $\underline{x}_{\langle\delta\rangle}$ is the $I(\delta)$ probabilistic variant of the variable $x_{\langle\delta\rangle}$, whose definition is now recalled: consider, for a given size n, the interval $I_n(\delta)$ and choose an integer W uniformly in this interval. Denote by $\underline{x}_{\langle\delta\rangle}$ the rational x_k associated to the first index k for which $\lg u_k$ is less than W. Since, in any interval $]A/2, A]$, there are at most two elements of the sequence x_k, then, for n large enough, there are only three possible values for $\underline{x}_{\langle\delta\rangle}$, namely $x_{\langle\delta\rangle+i}$ with $0 \le i \le 2$.

6.4. Proof of Theorem 3

It uses both Theorem 1 and Lemma 2, so that the best choice of the remainder term $\tau(\delta, \gamma)$ is given by

$$\tau(0,\gamma) = 2\gamma, \qquad \tau(\delta,\gamma) = \min(\tau_1(\delta,\gamma), 2\gamma,) = \min\left(2\gamma, \frac{1}{2}\rho(\delta) - 2\gamma, 2\underline{\sigma}\delta\right).$$

6.5. Proof of Theorem 1— Step 1. The Dirichlet series of interest

We study, in the same vein as before, a probabilistic version $\underline{P}_\delta$ of P_δ. We prove that it follows an asymptotic Gaussian law on Ω, from which it will be easy to deduce an asymptotic Gaussian law for the deterministic version P_δ on Ω.

We wish to use the Quasi-Powers Theorem which provides sufficient conditions, which entail an asymptotic Gaussian behaviour.

Theorem B (*Quasi-Powers Theorem (Hwang, 1998)*). *Assume that the moment generating functions* $\mathbb{E}_{n,f}[\exp(wR)]$ *for a cost R are analytic in a complex neighbourhood* $\mathcal{W}$ *of* $w = 0$, *and satisfy*

$$\mathbb{E}_{n,f}[\exp(wR)] = \exp[\beta_n C(w) + D(w)]\left(1 + O(\kappa_n^{-1})\right), \tag{62}$$

with $\beta_n, \kappa_n \to \infty$ *as* $n \to \infty$, $C(w)$, $D(w)$ *analytic on* $\mathcal{W}$ *and the O-term uniform in* $\mathcal{W}$. *Then, the mean and the variance satisfy*

$$\mathbb{E}_{n,f}[R] = C''(0)\cdot\beta_n + D'(0) + O(\kappa_n^{-1}), \qquad \mathbb{V}[R_n] = C''(0)\cdot\beta_n + D''(0) + O(\kappa_n^{-1}).$$

Author's personal copy

Furthermore, if $C''(0) \neq 0$, the distribution of R is asymptotically Gaussian on Ω_n with speed of convergence $O(\kappa_n^{-1} + \beta_n^{-1/2})$,

$$\mathbb{P}_{n,f}\left[x \;\middle|\; \frac{R(x) - C'(0)\beta_n}{\sqrt{C''(0)\beta_n}} \le Y\right] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{Y} \mathrm{e}^{-y^2/2}\, \mathrm{d}y + O(\kappa_n^{-1} + \beta_n^{-1/2}).$$

We shall show that Theorem B can be applied to our framework, with

$$\beta_n = \delta_n\, n, \qquad \kappa_n = \frac{1}{1-\delta_n} 2^{-n\widetilde{\tau}(\delta_n)}, \qquad C(w) = 2\log 2(\xi(w) - 1),$$

where $\widetilde{\tau}(\delta)$ is defined in Fig. 5 and $\xi(w)$ is the solution of the equation $\Lambda(s) = -w$ which involves the pressure function $\Lambda(s) := \log \lambda(s)$. This will entail Theorem 1.

We first wish to estimate the generating function $\mathbb{E}_{n,f}(\exp[w\underline{P}_\delta])$, as a quasi-power. We deal with the function $G(s,t,w) := \zeta(s+t)\,\widetilde{G}(s,t,w)$ with

$$\widetilde{G}(2s, 2t, w) = \mathrm{e}^{w}\,(I - \mathbf{H}_{s+t})^{-1}(\mathbf{H}_s - \mathbf{H}_{s+t}) \circ (I - \mathrm{e}^{w}\mathbf{H}_s)^{-1}[f](0).$$

The series G can be written as a Dirichlet series which depends on two variables s, t, together with a parameter w,

$$G(s,t,w) = \sum_{k\ge 0} \mathrm{e}^{w(k+1)} \sum_{N\ge 1}\sum_{M\ge 1} \frac{b_{N,M}^{(k)}}{N^s M^t} = \sum_{k\ge 0} \mathrm{e}^{wk}[V(s,t,I,k) - U(s,t,I,k)], \tag{63}$$

where the functions U and V are defined in (42) and (43). Here, the coefficient $\sum_{M\le W} b_{N,M}^{(k)}$ equals the f-weight of pairs (u, v) with $v = N$ for which u_{k+1} is at most W, while u_k is greater than W. Then, the quantity

$$\sum_{N=2^{n-1}}^{2^n} \sum_{M\le 2^{(1-\delta)n}} b_{N,M}^{(k)}$$

equals the f-weight of the subset of pairs (u, v) of size n for which P_δ equals $k+1$, and the expression

$$\sum_{N=2^{n-1}}^{2^n} \sum_{M\le 2^{(1-\delta)n}} \sum_{k\ge 0} \mathrm{e}^{w(k+1)} b_{N,M}^{(k)}$$

is the cumulative generating function of parameter P_δ on Ω_n. As previously, it is then sufficient to extract coefficients from the Dirichlet series $G(s,t,w)$.

6.6. *Proof of Theorem 1 — Step 2. Extraction with the Perron Formula*

This series G defined in (63) depends of two complex variables s and t (with w as a parameter). We will use the Perron Formula, two times.

We proceed in two steps, as previously. We first consider the Dirichlet series as a function of t, which has an only pôle at $t = 1 - s$ in the vertical strip in the strip $1 - \alpha < \Re(s+t) < 1 + \alpha$. Then

$$\sum_{W_1\le W} \sum_{M\le W_1} \sum_{N\ge 1} \sum_{k\ge 0} \mathrm{e}^{tk} \frac{b_{N,M}^{(k)}}{N^{2s}} = \zeta(2) \frac{W^{2(1-s)+1}}{(3-2s)} \frac{\varphi(0)}{\lambda'(1)} \int_I \left(\frac{\mathbf{H}_1 - \mathbf{H}_s}{1-s}\right) \circ (I - \mathrm{e}^{w}\mathbf{H}_s)^{-1}[f](u)\mathrm{d}u$$
$$+ \frac{1}{2\mathrm{i}\pi} \int_{\Re(s+t)=1-\alpha} \frac{W^{2t+1}}{t(2t+1)} G(2s, 2t, w)\, \mathrm{d}t.$$

This is now a Dirichlet series with respect to s, which has an only pôle at $s = \xi(w)$ in the vertical strip $1 - \beta < \Re s < 1 + \beta$, where $s = \xi(w)$ is the solution of the equation $\Lambda(s) = -w$. Using again the Perron Formula for extracting coefficients, we obtain finally four terms for this sum of coefficients

$$\mathrm{e}^{-w} D(T, W, w) := \sum_{T_1\le T} \sum_{N\le T_1} \sum_{W_1\le W} \sum_{M\le W_1} \sum_{k\ge 0} \mathrm{e}^{wk} b_{N,M}^{(k)}, \tag{64}$$

Author's personal copy

namely, defining domains $\Gamma_0 = \{s \in \mathbb{C} \mid \Re(s - \xi(w)) = -\beta\}$, $\Gamma_1 = \{t \in \mathbb{C} \mid \Re(\xi(w) + t) = 1 - \alpha\}$ and $\Gamma_2 = \{(s, t) \in \mathbb{C}^2 \mid \Re(t + \xi(w)) = 1 + \beta - \alpha$ and $\Re(s - \xi(w)) = -\beta\}$,

$$\zeta(2)\frac{\nu_{\xi(w)}[f]}{\lambda'(1)\lambda'(\xi(w))}\frac{W^{3-2\xi(w)}}{(3-2\xi(w))}\frac{T^{2\xi(w)+1}}{\xi(w)(2\xi(w)+1)}\int_I\left(\frac{\mathbf{H}_{\xi(w)}-\mathbf{H}_s}{1-\xi(w)}\right)[\varphi_{\xi(w)}](u)\mathrm{d}u$$
$$+\frac{\zeta(2)\varphi(0)}{2i\pi\,\lambda'(1)}\int_{\Gamma_0}\frac{T^{2s+1}}{s(2s+1)}\frac{W^{2(1-s)+1}}{(3-2s)(1-s)}\left(\int_I(\mathbf{H}_s-\mathbf{H}_1)\circ(I-\mathrm{e}^w\mathbf{H}_s)^{-1}[f](u)\mathrm{d}u\right)\mathrm{d}s$$
$$+C_w[f]\,T^{2\xi(w)+1}\int_{\Gamma_1}\frac{W^{2t+1}}{t(2t+1)}(I-\mathbf{H}_{\xi(w)+t})^{-1}\circ\left(\mathbf{H}_{\xi(w)}-\mathbf{H}_{\xi(w)+t}\right)\left[\frac{\varphi_w}{-\lambda'(\xi(w))}\right](0)\,\mathrm{d}t$$
$$-\int_{\Gamma_2}\frac{\zeta(2s+2t)}{4\pi^2}\frac{T^{2s+1}}{s(2s+1)}\frac{W^{2t+1}}{t(2t+1)}(I-\mathbf{H}_{s+t})^{-1}\circ(\mathbf{H}_s-\mathbf{H}_{s+t})\circ(I-\mathrm{e}^w\mathbf{H}_s)^{-1}[f](0)\,\mathrm{d}s\,\mathrm{d}t.$$

Here, the first term involves the dominant eigenfunction φ_s of $\mathbf{H}_s$ and the dominant eigenmeasure ν_s of the dual $\mathbf{H}_s^\star$ at $s = \xi(w)$ and the second term involves

$$C_w[f] := \frac{\zeta(2\xi(w)+2)}{2i\pi\xi(w)(2\xi(w)+1)}\nu_{\xi(w)}[f].$$

We first choose, as in Theorem 2, $\alpha = \beta = \underline{\sigma}$. The first term will provide the main term, which is of the form $A(w)W^{3-2\xi(w)}T^{2\xi(w)+1}$. Applying Theorem A entails estimate for the other three terms, so that $D(T, W, w)$ is written as

$$D(T, W, w) = R(w)\,W^{3-2\xi(w)}\,T^{2\xi(w)+1}\left[1+\sum_{i=2}^{4}A_j(T, W, w)\right].$$

Here, $R(w)$ is analytic and not zero when $w \in \mathcal{W}$ and the following estimates hold

$$A_2(T, W, w) = O\left(\frac{T}{W}\right)^{-2\underline{\sigma}}, \qquad A_3(T, W, w) = O(W^{-2\underline{\sigma}}), \qquad A_4(T, W, w) = O(T^{-2\underline{\sigma}}),$$

where the constants involved in the O-terms are uniform when w is near 0. Moreover, the term A_2 defines a function $(T, W) \mapsto A_2(T, W, w)$ of class $\mathcal{C}^2$ which depends only on T/W (with w as a parameter), whereas the term A_3 depends only on W (with w as a parameter). Finally, the term $F_1(T, W, w) := A_2(T, W, w) + A_3(T, W, w)$ defines a function $T \mapsto F_1(T, W, w)$ of class $\mathcal{C}^2$.

6.7. *Proof of Theorem 1 — Step 3. Final estimates for variable P_δ on Ω*

We now follow the same lines as in the proof of Theorem 2. We first consider W as fixed. For transforming the double sum over indices N into a simple sum, it is possible to apply Proposition D of Appendix, and transform the double sum over indices N into a simple sum. We deduce from the estimate of $D_1(T, W, w)$ in (64) an estimate for the sum

$$D(T, W, w) := \sum_{N=T/2}^{T}\sum_{W_1\le W}\sum_{M\le W_1}\sum_{k\ge 0}\mathrm{e}^{wk}b_{N,M}^{(k)}$$
$$= R_1(w)\,T^{2\xi(w)}\,W^{3-2\xi(w))}\left[1+F(T, W, w)+O(T^{-\underline{\sigma}/2})\right],$$

where $T \mapsto F(T, W, w)$ defines a function of class $\mathcal{C}^1$.

Then, as in Section 6.3, we consider that T and W are polynomially related, and use two times Proposition A as in Section 6.3, in cases (WB) and (WU). Due to the change of the exponent in Proposition C, we slightly change definition for $\rho(\delta)$, $I(\delta)$ and $\tau(\delta)$ and define

$$\widetilde{\rho}(\delta) := \underline{\sigma}\min\left(\frac{1}{4}, 1-\delta\right), \qquad \widetilde{I}_n(\delta) := \left[2^{(1-\delta)n}\left(1-(1-\delta)2^{-\widetilde{\rho}(\delta)n}\right), 2^{(1-\delta)n}\right],$$
$$\widetilde{\tau}(\delta) := \underline{\sigma}\min\left(\frac{1}{4}, 1-\delta, 2\delta\right).$$

Author's personal copy

We then obtain an estimate for the moment generating function of the $\widetilde{I}(\delta)$-probabilistic variant $\underline{P}_\delta$ on Ω_n, namely

$$\mathbb{E}_{n,f}[\exp(w\underline{P}_\delta)] = \frac{1}{|\Omega_n|_f}\sum_{N=2^{n-1}}^{2^n-1}\frac{1}{|\widetilde{I}_n(\delta)|}\sum_{W\in\widetilde{I}_n(\delta)}\sum_{M\le W}\sum_{k\ge 0}\mathrm{e}^{wk}b_{N,M}^{(k)}$$
$$= d(w)2^{2n\delta(\xi(w)-1)}\left[1+\frac{1}{1-\delta}O(2^{-n\widetilde{\tau}(\delta)})\right],$$

with a constant in the O-term uniform with respect to $w\in\mathcal{W}$. As in the proof of Theorem 2, all our estimates are uniform with respect to δ, so that we can consider a sequence δ_n which may depend on the size n. Then, the Quasi-Powers Theorem, applied with

$$C(w) := 2\log 2(\xi(w)-1), \qquad D(w) := \lg d(w)$$

entails an asymptotic Gaussian law for the probabilistic variant $\underline{P}_\delta$ on Ω_n, with a speed of convergence given by

$$\max\left((\delta_n n)^{-1/2}, \frac{2^{-n\widetilde{\rho}(\delta_n)}}{1-\delta_n}\right).$$

Furthermore, we have already remarked that, in any interval $]A/2, A]$, there are at most two elements of the sequence x_k. Then, for n large enough, the two variables – the probabilistic variable $\underline{P}_\delta$ and its deterministic version P_δ – are closely related since they satisfy $|\underline{P}_\delta - P_\delta| \le 2$.

Finally, Proposition 1 of the paper of Lhote and Vallée (2008), together with the inequality $|\underline{P}_\delta - P_\delta| \le 2$ proves that the asymptotic Gaussian law also holds for P_δ on Ω, with a speed of convergence of order

$$\max\left((\delta_n n)^{-1/3}, \frac{2^{-n\widetilde{\rho}(\delta_n)}}{1-\delta_n}\right).$$

6.8. Proof of Theorem 4. Sketch

We study here the parameter Q_δ and introduce the Dirichlet series which depends on two parameters s, t,

$$H(2s,2t) := \zeta(2s+2t)(I-\mathbf{H}_{s+t})^{-1}(\mathbf{H}_{s+t}-\mathbf{H}_s)\circ\left(\frac{\partial}{\partial w}\mathbf{H}_{s,w,[\ell]}^3\right)_{w=0}\circ(I-\mathbf{H}_s)^{-1}[f](0).$$

It involves the weighted transfer operator $\mathbf{H}_{s,w,[\ell]}$ relative to the binary size ℓ and already defined in (32)

$$\mathbf{H}_{s,w,[\ell]}[f](x) := \sum_{m\ge 1}\frac{\exp(w\ell(m))}{(m+x)^{2s}}f\left(\frac{1}{m+x}\right).$$

Applying the same principles as in Sections 6.1 and 6.4 proves that it is well adapted to the study of cost $\underline{Q}_\delta$.

6.9. Proof of Theorem 5. Sketch

We study here the parameter $\ell(U_{\langle\delta\rangle})$ and introduce the Dirichlet series which depends on two parameters s, t,

$$L(2s,2t) := \zeta(2s+2t)(I-\mathbf{H}_{s+t})^{-1}\circ\mathbf{H}'_{s+t}\circ(I-\mathbf{H}_{s+t})^{-1}\circ(\mathbf{H}_{s+t}-\mathbf{H}_s)\circ(I-\mathbf{H}_s)^{-1}[f](0).$$

It involves the derivative of the operator $\mathbf{H}_s$. Applying the same principles as in Sections 6.1 and 6.4 proves that it is well adapted to the study of cost $\ell(\underline{U}_{\langle\delta\rangle})$.

7. Conclusion

This paper provides the first average-case analysis of a subquadratic gcd algorithm. We therefore extend the domain of applicability of dynamical analysis techniques, and show that such methods

Author's personal copy

are also efficient for studying more complex Euclidean algorithms. The type of analysis performed here requires a precise study of the interrupted algorithms, and a precise description of the evolution of the distribution during the execution of the algorithm. This uses heavily the powerful tools of distributional analysis provided by Baladi and Vallée (2005) and Lhote and Vallée (2008).

It would be also interesting to adapt the methodology developed here to other subquadratic gcd algorithms. We have in mind the algorithm recently designed by Stehlé and Zimmermann (2004), based on a division using the least significant bits of the integers. The analysis of the plain gcd algorithm using this division is done in Daireaux et al. (2005). This is clearly a first step in that direction; however, a complete analysis of the SZ Algorithm would use Property *US*, and this Property is not known to hold in the context of the dynamical system related to this gcd using the least significant bits.

Acknowledgments

The authors wish to thank the anonymous referees for their useful and enlightening comments.

Appendix. Propositions A–D

We are interested in finding estimates for partial sums of coefficients, of the form

$$\Phi_w(N) := \sum_{k\le N} c_k(w).$$

However, Perron's formula of order two provide estimates only for double sums,

$$\Psi_w(T) := \sum_{N\le T} \Phi_w(N) = \sum_{N\le T}\sum_{k\le N} c_k(w)$$

in the following general framework where the double sum $\Psi_w(T)$ is of type (P), as it will be defined soon. We first need a definition:

Definition (*Uniform Order*). A function $T \to H_w(T)$ is of uniform order $O(T^{-d})$ for $w \in \mathcal{W}$ if $H_w(\alpha T) = O(T^{-d})$ with a O-term uniform for all $\alpha \in [1/2, 2]$ and $w \in \mathcal{W}$.

We then state our main definition of type (P):

Definition (*Type (P)*). A function $T \mapsto \Psi_w(T)$ is of type (P) if the estimate

$$\Psi_w(T) = F_w(T)\,[G_w(T) + H_w(T)]\,, \quad T \to \infty, \quad w \in \mathcal{W} \tag{65}$$

holds, with

$$F_w(T) = b(w)T^{a(w)}, \quad G_w(T) = c(w) + O(T^{-d}), \qquad H_w(T) = O(T^{-2\sigma}), \qquad \sigma \le 1/2,$$

and O-error terms uniform for $w \in \mathcal{W}$. The four terms $|a(w)|, |b(w)|, |c(w)|, |a(w) - 1|$ admit strictly positive lower bounds on $\mathcal{W}$ and the function H_w is of uniform order $O(T^{-2\sigma})$. Furthermore,

(i) The function $T \mapsto G_w(T)$ satisfies one of the two following properties:
  (W)[Weak Form] G_w is of class $\mathcal{C}^1$ and G'_w is of uniform order $O(T^{-d-1})$.
  (S) [Strong Form] G_w is of class $\mathcal{C}^2$ and G''_w is of uniform order $O(T^{-d-2})$.
(ii) The function $w \mapsto a(w)$ satisfies one of the two following properties:
  (B) [Bounded] $|a(w)|$ admits an upper bound on $\mathcal{W}$.
  (U) [Unbounded] $|a(w)|$ is not bounded on $\mathcal{W}$.

The data of such a function Ψ_w is described by (a, b, c, d, σ) or more precisely by (a, b, G, σ).

Author's personal copy

In such a general framework, the main question is as follows:

From estimates on $\Psi_w(N)$, is it possible to deduce estimates for $\Phi_w(N)$?

It proves useful to introduce intermediate objects: for two indices N_- and N_+ which satisfy $N_- < N < N_+$, consider the two averages

$$\Phi_w^+(N) := \frac{\Psi_w(N_+) - \Psi_w(N)}{N_+ - N} = \frac{1}{N_+ - N} \sum_{k=N+1}^{N_+} \Phi_w(k)$$

$$\Phi_w^-(N) := \frac{\Psi_w(N) - \Psi_w(N_-)}{N - N_-} = \frac{1}{N - N_-} \sum_{k=N_-+1}^{N} \Phi_w(k).$$

The following of the appendix is devoted to the three main steps:

(a) It is always possible to deduce from (65) estimates for $\Phi_w^{\pm}(N)$, as soon as N_- and N_+ are well-chosen. This is the aim of Proposition A.
(b) Then, if the coefficients $c_n(w)$ are positive, these estimates can be transferred into estimates for $\Phi_w(N)$. This is the aim of Proposition B.
(c) Finally, if the coefficients $c_n(w)$ are dominated by $\widehat{c}_n(w)$ (i.e. $|c_n(w)| \le \widehat{c}_n(w)$), and if estimates for $\widehat{\Psi}_w(T)$ of the same vein as $\Psi_w(T)$ hold, then it is possible to obtain estimates for $\Phi_w(N)$. This is the aim of Proposition C. Furthermore, this proposition naturally applies to a "moment generating function" setting described in Proposition D.

A.1. Statements of the propositions

We now describe the three results in a more formal way.

Proposition A (*Basic Versions*). *Consider a function $T \mapsto \Psi_w(T)$ which satisfies (P) on $\mathcal{W}$ with the data (a, b, G, σ), where G is described by the pair (c, d). Then, the following holds for $\Phi_w^{\pm}(N)$ defined by*

$$\Phi_w^+(N) := \frac{\Psi_w(N_+) - \Psi_w(N)}{N_+ - N}, \qquad \Phi_w^-(N) := \frac{\Psi_w(N) - \Psi_w(N_-)}{N - N_-}$$

[Case (WB)] *For $N_- = N - \lfloor N^{1-x} \rfloor$, $N_+ = N + \lfloor N^{1-x} \rfloor$, the sums $\Phi_w^{\pm}(N)$ satisfy*

$$\Phi_w^{\pm}(N) = a(w)\, b(w)\, N^{a(w)-1} \cdot [c(w) + O(N^{-2\sigma+x}) + O(N^{-x}) + O(N^{-d})],$$

where the constants in the O-terms are uniform on $\mathcal{W}$. With the optimal choice $x = \sigma$, one has

$$\Phi_w^{\pm}(N) = a(w)\, b(w)\, N^{a(w)-1} \cdot [c(w) + O(N^{-\sigma}) + O(N^{-d})],$$

where the constants in the O-terms are uniform on $\mathcal{W}$.

[Case (WU)] *For $N_- = N - \lfloor \frac{1}{a(w)} N^{1-x} \rfloor$, $N_+ = N + \lfloor \frac{1}{a(w)} N^{1-x} \rfloor$, the sums $\Phi_w^{\pm}(N)$ satisfy*

$$\Phi_w^{\pm}(N) = a(w)b(w)N^{a(w)-1} \cdot \left[c(w) + O\left(N^{-2\sigma+x}\right) + O(N^{-x}) + O(N^{-d})\right],$$

where the constants in the O-terms are uniform on $\mathcal{W}$. With the optimal choice $x = \sigma$, one has

$$\Phi_w^{\pm}(N) = a(w)b(w)N^{a(w)-1} \cdot \left[c(w) + O(N^{-\sigma}) + O(N^{-d})\right],$$

where the constants in the O-terms are uniform on $\mathcal{W}$.

[Case (SB)] *For $N_- = N - \lfloor N^{1-\sigma} \rfloor$, $N_+ = N + \lfloor N^{1-\sigma} \rfloor$, the sums $\Phi_w^{\pm}(N)$ satisfy*

$$\Phi_w^{\pm}(N) = a(w)\, b(w)\, N^{a(w)-1} \cdot \left[G_w(N) + \frac{N}{a(w)} G'_w(N) + O(N^{-\sigma})\right],$$

where the constant in the O-term is uniform on $\mathcal{W}$.

Author's personal copy

Proposition B (*Positive Coefficients*). *Consider a function $\widehat{\Psi}_w$ related to a sequence of positive functions $\widehat{c}_n : \mathcal{W} \to \mathbb{C}$ which satisfies (P), (SB) on $\mathcal{W}$ with the data $(\widehat{a}, \widehat{b}, \widehat{G}, \widehat{\sigma})$. Then the sum $\widehat{\Phi}_w(N)$ satisfies*

$$\widehat{\Phi}_w(N) := \widehat{a}(w)\,\widehat{b}(w)\,N^{\widehat{a}(w)-1} \cdot \left[\widehat{G}_w(N) + \frac{N}{\widehat{a}(w)}\widehat{G}'_w(N) + O(N^{-\widehat{\sigma}})\right],$$

where the constant in the O-term is uniform on $\mathcal{W}$.

Proposition C (*Domination*). *Consider two functions $\Psi_w, \widehat{\Psi}_w$ related to two sequences of functions $c_n : \mathcal{W} \to \mathbb{C}, \widehat{c}_n : \mathcal{W} \to \mathbb{R}^+$, which satisfy (P)(SB) on $\mathcal{W}$ with the respective data (a, b, G, σ) and $(\widehat{a}, \widehat{b}, \widehat{G}, \widehat{\sigma})$. Suppose furthermore, that the following holds:*

(i) *$\widehat{c}_n$ dominates c_n, i.e., $|c_n(w)| \le \widehat{c}_n(w), \forall w \in \mathcal{W}$.*

(ii) *The two functions $a(w), \widehat{a}(w)$ satisfy : $\exists \alpha < \widehat{\sigma}/2, \forall w \in \mathcal{W}, |\Re a(w) - \Re\widehat{a}(w)| \le \alpha$.*

Then, the sum $\Phi_w(T)$ satisfies, for any $w \in \mathcal{W}$,

$$\Phi_w(T) := \sum_{n \le T} c_n(w) = a(w)\,b(w)\,N^{a(w)-1} \cdot \left[G_w(N) + \frac{N}{a(w)}G'_w(N) + O(N^{-\beta})\right],$$

with $\beta := \min(\sigma, \widehat{\sigma} - 2\alpha)$ and a constant in the O-term uniform on $\mathcal{W}$.

Proposition D (*Particular Case of Proposition C*). *Consider the case when $\mathcal{W}$ is a neighbourhood of 0, $c_n : \mathcal{W} \cap \mathbb{R} \to \mathbb{R}$, and $|c_n(w)| \le c_n(\Re w)$. We let in this case $\widehat{c}_n(w) := c_n(\Re w)$. Then, if Ψ satisfies (P), (SU) with the data (a, b, G, σ), the function $a(w)$ is real as soon as w is real, and $\widehat{\Psi}_w$ satisfies (P), (SU) with the data $(a(\Re w), b(\Re w), G_{\Re w}, \sigma)$. If, moreover, the function $w \mapsto a(w)$ is continuous, then the difference $\Re a(w) - \widehat{a}(w) = \Re a(w) - a(\Re w)$ is less than $\sigma/4$ on a small enough neighbourhood of $w = 0$. And, it is possible to apply Proposition C, with $\beta = \sigma/2$.*

This framework arises in a natural way when we study moment generating functions, since, in this case, the coefficient $c_n(w)$ is a sum of terms of the form $a_{j,n} \exp[w b_{j,n}]$, with reals $a_{j,n} \ge 0$, $b_{j,n}$.

A.2. Proof of Proposition A

For $(T - T_-)/T := T^{-x}$, with $x > 0$, the estimate of $\Psi_w(T)$ entails

$$\Psi_w(T) - \Psi_w(T_-) = (F_w(T) - F_w(T_-))\,G_w(T) + (G_w(T) - G_w(T_-))\,F_w(T) + O\left(F_w(T)T^{-2\sigma}\right).$$

There are two main cases: If $T \mapsto G_w(T)$ is only of class $\mathcal{C}^1$, then

$$\begin{aligned}\frac{1}{T - T_-}[\Psi_w(T) - \Psi_w(T_-)] &= F'_w(T)\left[G_w(T) + G'_w(\widetilde{T})\frac{F_w(T)}{F'_w(T)}\right] \\ &\quad + \frac{T - T_-}{T}O\left(\frac{TF''_w(T)}{F'_w(T)}G_w(T)\right) + \frac{T}{T - T_-}O\left(T^{-2\sigma}\,\frac{F_w(T)}{TF'_w(T)}\right). \quad (66)\end{aligned}$$

If $T \mapsto G_w(T)$ is of class $\mathcal{C}^2$, then

$$\begin{aligned}\frac{1}{T - T_-}[\Psi_w(T) - \Psi_w(T_-)] &= F'_w(T)\left[G_w(T) + G'_w(T)\frac{F_w(T)}{F'_w(T)}\right] \\ &\quad + \frac{T - T_-}{T}O\left(\frac{TF''_w(T)}{F'_w(T)}G_w(T),\ \frac{TF_w(T)}{F'_w(T)}G''_w(T)\right) + \frac{T}{T - T_-}O\left(T^{-2\sigma}\,\frac{F_w(T)}{TF'_w(T)}\right). \quad (67)\end{aligned}$$

In both cases, our assumptions on $F_w(T)$ imply that the two terms in (66) or (67) are both

$$\frac{T - T_-}{T}\,c(w)(a(w) - 1)O(1) = (a(w) - 1)\,O(T^{-x})$$

$$\frac{T}{T - T_-}\,\frac{1}{a(w)}O\left(T^{-2\sigma}\right) = \frac{1}{a(w)}O(T^{-2\sigma+x}).$$

In case (B), the optimal choice is then given by $x = \sigma$. In case (U), the optimal choice is given by the equality $a(w)T^{-x} = [1/a(w)]T^{-2\sigma+x}$. Moreover, if we wish to transfer theses estimates on integer parts, we need the condition $\sigma \le 1/2$.

Author's personal copy

A.3. Proof of Propositions B and C

In the case where (*SB*) holds, we compare $\widehat{\Phi}_w^{\pm}(N)$ and $\widehat{\Phi}_w(N)$. We have

$$\widehat{\Phi}_w(N) = \widehat{\Phi}_w^{-}(N) + \frac{1}{N - N_-} \sum_{k=N_-+1}^{N} (\widehat{\Phi}_w(N) - \widehat{\Phi}_w(k))$$

$$\widehat{\Phi}_w(N) = \widehat{\Phi}_w^{+}(N) + \frac{1}{N_+ - N} \sum_{k=N+1}^{N_+} (\widehat{\Phi}_w(N) - \widehat{\Phi}_w(k)).$$

If the coefficients $\widehat{c}_n(w)$ are real positive, the sequence $k \mapsto \widehat{\Phi}_w(k)$ is increasing, and the inequalities

$$\widehat{\Phi}_w^{-}(N) \le \widehat{\Phi}_w(N) \le \widehat{\Phi}_w^{+}(N)$$

entail that $\widehat{\Phi}_w(N)$ has the same estimate as $\widehat{\Phi}_w^{\pm}(N)$, namely

$$\widehat{\Phi}_w(N) = \widehat{a}(w)\,\widehat{b}(w)\,N^{\widehat{a}(w)-1} \cdot \left[\widehat{G}_w(T) + \frac{N}{\widehat{a}(w)}\widehat{G}'_w(N) + O(N^{-\widehat{\sigma}})\right]$$

$$\left|\widehat{\Phi}_w(N) - \widehat{\Phi}_w^{-}(N)\right| = O(N^{\widehat{a}(w)-1-\widehat{\sigma}}).$$

This provides the proof of Proposition B.

We now prove Proposition C. If the series no longer has positive coefficients, but is dominated, we observe that, for $k \le N$,

$$|\Phi_w(N) - \Phi_w(k)| = \left|\sum_{n=k+1}^{N} c_n(w)\right| \le \sum_{n=k+1}^{N} \widehat{c}_n(w) = \widehat{\Phi}_w(N) - \widehat{\Phi}_w(k),$$

which entails the inequality

$$\left|\Phi_w(N) - \Phi_w^{-}(N)\right| \le \left|\widehat{\Phi}_w(N) - \widehat{\Phi}_w^{-}(N)\right|.$$

We apply the arguments of Proposition B which prove that

$$\left|\widehat{\Phi}_w(N) - \widehat{\Phi}_w^{-}(N)\right| = O(N^{\widehat{a}(w)-1-\widehat{\sigma}}),$$

together with the estimate for $\Phi_w^{-}(N)$ obtained in Proposition A, and finally

$$\begin{aligned}\Phi_w(N) &= a(w)\,b(w)\,N^{a(w)-1} \cdot \left[G_w(N) + \frac{N}{a(w)}G'_w(N) + O(N^{-\sigma}) + O(N^{\widehat{a}(w)-a(w)-\widehat{\sigma}})\right] \\ &= a(w)\,b(w)\,N^{a(w)-1}\left[G_w(N) + \frac{N}{a(w)}G'_w(N) + O\left(N^{-\beta}\right)\right],\end{aligned}$$

with $\beta := \min(\sigma, \widehat{\sigma} - 2\alpha)$. This proves Proposition C.

References

Baladi, V., Vallée, B., 2004. Exponential decay of correlations for surface semi-flows without finite Markov partitions. Proceedings of the American Mathematical Society 133 (3), 865–874.

Baladi, V., Vallée, B., 2005. Euclidean algorithms are Gaussian. Journal of Number Theory 110 (2), 331–386.

Brent, R.P., 1976. Analysis of the binary Euclidean algorithm. In: Traub, J.F. (Ed.), Algorithms and Complexity, New Directions and Recent Results. Academic Press, pp. 321–355.

Cesari, G., 1998. Parallel implementation of Schönhage's integer GCD algorithm. In: Proceedings of ANTS-III. In: LNCS, vol. 1423. pp. 64–76.

Daireaux, B., Maume-Deschamps, V., Vallée, B., 2005. The Lyapounov Tortoise and the dyadic hare. Discrete mathematics and theoretical computer science 2005, In: Proceedings of AofA'05, pp. 71–94.

Daireaux, B., Vallée, B., 2004. Dynamical analysis of the parameterized Lehmer–Euclid Algorithm. Combinatorics, Probability, Computing 499–536.

Dixon, J.D., 1970. The number of steps in the Euclidean algorithm. Journal of Number Theory 2, 414–422.

Dolgopyat, D., 1998. On decay of correlations in Anosov flows. Annals of Mathematics 147, 357–390.

Efrat, I., 1993. Dynamics of the continued fraction map and the spectral theory of $SL(2, \mathbb{Z})$. Inventiones Mathematicae 114, 207–218.

Author's personal copy

Ellison, W., Ellison, F., 1985. Prime Numbers. Hermann, Paris.
Flajolet, P., Sedgewick, R., 2008. Analytic Combinatorics, Cambridge University Press (in press).
Fürer, M., 2007. Faster integer multiplication. In: Proceedings of STOC'07, pp. 57–66.
Heilbronn, H., 1969. On the average length of a class of continued fractions. In: Turan, P. (Ed.), Number Theory and Analysis. Plenum, New-York, pp. 87–96.
Hensley, D., 1994. The number of steps in the Euclidean algorithm. Journal of Number Theory 49 (2), 142–182.
Hwang, H.-K., 1998. On convergence rates in the central limit theorems for combinatorial structures. European Journal of Combinatorics 19, 329–343.
Jebelean, T., 1997. Practical integer division with Karatsuba complexity. In: Proceedings of ISSAC'97.
Jebelean, T., 1995. A double-digit Lehmer–Euclid algorithm for finding the GCD of long integers. Journal of Symbolic Computation 19, 145–157.
Knuth, D.E., 1998. The Art of Computer Programming, 3rd edition. vol. 2. Addison Wesley, Reading, MA.
Knuth, D.E., 1971. The Analysis of Algorithms. In: Actes du Congrès des Mathématiciens, vol. 3. Gauthier-Villars. pp. 269–274.
Lehmer, D.H., 1938. Euclid's algorithm for large numbers. The American Mathematical Monthly 45, 227–233.
Lhote, L., Vallée, B., 2008. Gaussian Laws for the main parameters of the Euclid Algorithm. Algorithmica 50, 497–554. Extended version of Lhote and Vallée (2006).
Lhote, L., Vallée, B., 2006. Sharp estimates for the main parameters of the Euclid algorithm. In: Proceedings of LATIN'06. In: LNCS, vol. 3887, pp. 689–702.
Mayer, D., 1991. A thermodynamic approach to Selberg's zeta function for $PSL(2, \mathbb{Z})$. Bulletin of American Mathematical Society 25 (1), 55–70.
Möller, N., January 2008. On Schönhage's algorithm and subquadratic integer gcd computation. Mathematics of Computation 77 (261), 589–607.
Ruelle, D., 1978. Thermodynamic Formalism. Addison Wesley.
Schönhage, A., 1971. Schnelle Berechnung von Kettenbruchentwicklungen. Acta Informatica 139–144.
Stehlé, D., Zimmermann, P., 2004. A binary recursive gcd algorithm. In: Proceedings of ANTS'04. In: LNCS, vol. 3076. pp. 411–425.
Vallée, B., 2000. Digits and continuants in Euclidean algorithms. Ergodic Versus Tauberian Theorems. Journal de Théorie des Nombres de Bordeaux 12, 531–570.
Vallée, B., 2003. Dynamical analysis of a class of Euclidean algorithms. Theoretical Computer Science 297/1-3, 447–486.
Vallée, B., May 2006. Euclidean dynamics. Discrete and Continuous Dynamical Systems 15 (1), 281–352.
Yap, C.K., 1996. Fundamental Problems in Algorithmic Algebra. Princeton University Press.