GAUSSIAN LAWS FOR THE MAIN PARAMETERS OF THE EUCLID ALGORITHMS

LOÏCK LHOTE AND BRIGITTE VALLÉE

Abstract. We provide sharp estimates for the probabilistic behaviour of the main parameters of the Euclid Algorithms, both on polynomials and on integer numbers. We study in particular the distribution of the bit-complexity which involves two main parameters : digit–costs and length of remainders. We first show here that an asymptotic gaussian law holds for the length of remainders at a fraction of the execution, which exhibits a deep regularity phenomenon. Then, we study in each framework –polynomials (P) and integer numbers (I)– two gcd algorithms, the standard one (S) which only computes the gcd, and the extended one (E) which also computes the Bezout pair, and is widely used for computing modular inverses.
The extended algorithm is more regular than the standard one, and this explains that our results are more precise for the Extended algorithm: we exhibit an asymptotic gaussian law for the bit–complexity of the extended algorithm, in both cases (P) and (I). We also prove that an asymptotic gaussian law for the bit-complexity of the standard gcd in case (P), but we do not succeed obtaining a similar result in case (I).
The integer study is more involved than the polynomial study, as it is usually the case. In the polynomial case, we deal with the central tools of the distributional analysis of algorithms, namely bivariate generating functions. In the integer case, we are led to dynamical methods, which heavily use the dynamical system underlying the number Euclidean algorithm, and its transfer operator. Baladi and Vallée [2] have recently designed a general framework for "distributional dynamical analysis", where they have exhibited asymptotic gaussian laws for a large family of parameters. However, this family does not contain neither the bit–complexity cost nor the size of remainders, and we have to extend their methods for obtaining our results. Even if these dynamical methods are not necessary in case (P), we explain how the polynomial dynamical system can be also used for proving our results. This provides a common framework for both analyses, which well explains the similarities and the differences between the two cases (P) and (I), for the algorithms themselves, and also for their analysis. An extended abstract of this paper can be found in Proceedings of LATIN'06 [21].

1. Introduction

The Euclid algorithm is one of the most ancient algorithmic scheme. Designed by Euclid himself for computing the greatest common divisor [in shorthand notation, gcd] of two integer numbers, with a sequence of Euclidean divisions, this scheme can also be applied on polynomials with coefficients in a field K. There are two main algorithmic instances of the Euclid Agorithm: the first one works on the ring of polynomials $\mathbb{F}_q[X]$ (whose coefficients belong to the finite field $\mathbb{F}_q$ with q elements), whereas the second one deals with the set $\mathbb{N}$ of positive integers. The Euclid algorithm plays a central rôle in these two algorithmic domains. In polynomial case, this is a main step for factoring polynomials, and, in a sense, factorisation of polynomials can be seen as a sequence of gcd computations. And, polynomial factoring is widely used in computer algebra. Of course, the situation is a priori quite different for integers, since integer factoring is thought to be "difficult", and gcd computations are of no much help here. However, the Euclid algorithm is also central in arithmetics: in the exact rational arithmetics, gcd computations are crucial, in order to keep the size of rationals small. However, the Euclid algorithm is not only useful for computing gcd. Together with the gcd, a second output of the Euclid algorithm is the continued fraction expansion [in both cases]. And it proves often more efficient computing directly with this continued fraction than using the rational itself. And finally, the (extended) Euclidean algorithm computes modular inverses, and this type of computation is central in cryptography, for instance. See the book [30] for nice applications of the Euclidean scheme.

Date: 7th June 2006.

1.1. **The Euclid Algorithms.** In the sequel, the set $\mathbb{A}$ will denote $\mathbb{F}_q[X]$ or $\mathbb{N}$. The degree of a non–zero polynomial u is denoted by $\deg u$. For $u = 0$, we let $\deg u := -\infty$. On positive integers, we consider the usual absolute value $||v|| := v$, while, on polynomials, we consider the ultrametric absolute value, defined by $||v|| := q^{\deg v}$, and $||0|| = 0$. In the integer case, the size of a non–zero integer v, denoted by $\ell(v)$, is the binary length of the integer v; it equals $\lfloor \lg v \rfloor + 1$, where lg denotes the logarithm in base 2. For polynomials, the size $\ell(v)$ of a non-zero polynomial v equals the number of coefficients of the polynomial, i.e., $1 + \deg v$. In summary, for $v \neq 0$,

$$\text{Case } (P): \quad \ell(v) := 1 + \deg v, \qquad \text{Case } (I): \quad \ell(v) := 1 + \lfloor \lg v \rfloor. \tag{1}$$

A polynomial v is monic if its dominant coefficient is equal to 1; in the integer case (by definition), the monic elements are just all the non–zero elements of $\mathbb{N}$. We will consider, as the set of possible inputs for the Euclid Algorithm, the set

$$\Omega := \{(u, v) \in \mathbb{A}^2; \quad 0 \leq ||u|| < ||v||, \quad v \ \text{ monic}\}. \tag{2}$$

For any (u, v) of Ω, and by definition, the size of pair (u, v) is just the size $\ell(v)$ of v and the norm of this pair is just the norm $||v||$ of v.

The Euclid algorithm computes the greatest common divisor (in short gcd) by using Euclidean divisions $v = m \cdot u + r$ with $||r|| < ||u||$. On an input $(u, v) \in \Omega$, it lets $v_0 := v, v_1 := u$, performs a sequence of Euclidean divisions on the form,

$$v_0 = m_1 \cdot v_1 + v_2, \quad v_1 = m_2 \cdot v_2 + v_3, \quad \dots \quad v_i = m_{i+1} \cdot v_{i+1} + v_{i+2} \dots, \tag{3}$$

and stops when the remainder v_{p+1} is zero. The last division performed is just $v_{p-1} = m_p \cdot v_p$. Remark that, in the integer case, the digit m_p satisfies $m_p \neq 1$.
The sequences of the norms $||v_i||$ is strictly decreasing, and the last non-zero remainder v_p is a greatest common divisor of u and v. By definition, the gcd d of (u, v) is the unique monic polynomial d proportional to v_p. The set $\mathcal{G}$ of possible digits in a non final step, the set $\mathcal{F}$ of possible digits in the final step, and the set $\mathcal{U}$ of possible gcd's are

$$\mathcal{G} := \{m \in \mathbb{A}; \ \ ||m|| \geq 1\}, \quad \mathcal{U} := \{d \in \mathbb{A}; \ \ d \ \text{ monic}\}, \quad \mathcal{F}_{\mathcal{I}} := \{m \in \mathbb{N}; m \geq 2\}, \quad \mathcal{F}_{\mathcal{P}} := \mathcal{G}, \tag{4}$$

and the Euclid algorithm builds the fundamental bijection

$$\Omega \sim \mathcal{G}^\star \times \mathcal{U} \quad [\text{Case } (P)] \qquad \Omega \sim [\epsilon + \mathcal{F} \times \mathcal{G}^\star] \times \mathcal{U} \quad [\text{Case } (I)]. \tag{5}$$

1.2. **Bit-complexities.** We wish to study the bit–complexity of the Euclid algorithm; here the bit–complexity means the total number of binary operations for integers, and the total number of operations in the field $\mathbb{F}_q$ for polynomials[1]. The (naive) bit–complexity of the Euclidean division $v = m \cdot u + r$ is $\ell(u) \cdot \ell(m)$ so that, the total bit–complexity of the Euclid Algorithm on (u, v) is

$$B(u, v) = \sum_{i=1}^{p} \ell(m_i) \cdot \ell(v_i). \tag{6}$$

The Extended Euclid algorithm ouputs, at the same time, the Bezout pair (r, s) for which $d = rv + su$. It computes the sequence s_i defined by

$$s_0 = 0, \qquad s_1 = 1, \qquad s_i = s_{i-2} - s_{i-1} \cdot m_{i-1}, \quad 0 \leq i < p.$$

The last element s_p is the Bezout coefficient s. The bit–complexity D of Extended Euclid algorithm is then

$$D(u, v) = \ell(m_p) \cdot \ell(v_p) + \sum_{i=1}^{p-1} \ell(m_i) \cdot [\ell(v_i) + \ell(s_i)]. \tag{7}$$

[1]Since the cardinality q of $\mathbb{F}_q[X]$ is fixed, this is actually a bit–complexity, in the usual meaning

1.3. **Other costs of interest.** We observe that the previous costs of interest B, D can be expressed as a sum of terms, each of them being a product of two factors: the first one involves the size of digits, and the second one involves the size of the so-called continuants, namely v_i and s_i. It is then useful to compare these costs to other costs defined on Ω, namely additive costs, associated to an elementary cost c on digits, under the form

$$C(u,v) := \sum_{i=1}^{p} c(m_i). \tag{8}$$

When $c(m)$ is $O(\log m)$, the cost c, and the cost C are said to be of moderate growth. This class of costs contains quite natural parameters, as the number of steps (for $c = 1$), the number of occurrences of a given digit m_0 (for $c(m) := [[m = m_0]]$), the total encoding length (when c equals the binary length ℓ).
We also consider a cost $N^{(v)}$ which involves the size of remainders, and a cost $N^{(m)}$ which can be seen as a kind of a path-length,

$$N^{(v)}(u,v) := \sum_{i=1}^{p} \ell(v_i), \qquad N^{(m)}(u,v) := \sum_{i=1}^{p+1} i \cdot \ell(m_i). \tag{9}$$

In case (P), these two costs are equal, but this is no longer true in case (I).

We are interested here in precisely studying the probabilistic behaviour of both gcd algorithms, for polynomials and for integers. We consider that inputs (u, v) have a fixed size n, i.e., they belong to the subset

$$\Omega_n := \{(u,v) \in \Omega; \quad \ell(v) = n\}, \tag{10}$$

where Ω is defined in (2). We assume that Ω_n is endowed with the uniform probability $\mathbb{P}_n$. For a random variable R defined on Ω, its restriction to Ω_n is denoted by R_n, and we wish to analyze the asymptotic behaviour of R, i.e., the evolution of variables R_n when n becomes large.

1.4. **Previous results for average-case analysis.** The evolution of the mean values $\mathbb{E}[R_n]$ is of great interest and, more generally, the study of all moments $\mathbb{E}[R_n^\ell]$ provides a first understanding of the probabilistic behaviour of the algorithm: this is the aim of average–case analysis.
In the polynomial case, there are few analyses of this type. The works of Knopfmacher and Knopfmacher [18], or works of Friesen and Hensley [14] directly deal with the distribution. Since the analysis in the number case is more difficult, first analyses began with the study of the average-case, and there are now many well-known results of this type, even if the last ones have been obtained recently. The first results on probabilistic analysis of Euclid's Algorithm are due to Heilbronn and Dixon [8, 15], who have shown, around 1970, that the average number of iterations is linear with respect to the size. During the last ten years, the research team in Caen has designed a complete framework for analyzing an entire class of Euclidean algorithms, with a large class of parameters [26, 27, 28]. It is possible to obtain precise results on the average behaviour of the main parameters of the algorithm : the digits m_i, and the size of continuants v_i and s_i. Akhavi and Vallée have also analyzed the average bit–complexity [1]. These methods consider the underlying dynamical systems, and make a deep use of dynamical tools, like the transfer operator. They form what we now call the dynamical analysis methodology.

1.5. **Distributional analysis and asymptotic gaussian laws.** However, the distributional analysis, which describes the evolution of the distribution of variable R_n, provides a much more precise analysis of the algorithm: this is the ultimate purpose in analysis of algorithms. Very often, variables R_n have a distribution which tends to the Gaussian law: this phenomenon is easily proved as soon as cost R_n is the sum of n elementary costs, which are independent, and possess the same distribution. In the "real algorithmic life", and the "Euclidean world", the elementary costs are not independent, and their distribution may evolve with the evolution of the algorithm. This is why an asymptotic gaussian law, even if it is widely expected, is often difficult to prove, particularly in integer case.

We prove here that many variables R defined on Ω follow asymptotically a gaussian law. We first provide a precise definition of this notion:

Definition 1. [Asymptotic gaussian law.] *Consider a cost R defined on a set Ω and and its restriction R_n to Ω_n. The cost R follows an asymptotic law if there exist three sequences a_n, b_n, r_n, with $r_n \to 0$, for which*

$$\mathbb{P}\left[(u,v)\in\Omega_n \;\middle|\; \frac{R_n(u,v)-a_n}{\sqrt{b_n}} \le y\right] = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{y} e^{-t^2/2}\,dt + r_{n,y}, \qquad r_n := \sup\{r_{n,y};\quad y\in\mathbb{R}\}.$$

The sequence r_n defines the speed of convergence, also denoted by $r[X_n]$. The expectation $\mathbb{E}[R_n]$ and the variance $\mathbb{V}[R_n]$ satisfy $\mathbb{E}[R_n]\sim a_n$, $\mathbb{V}[R_n]\sim b_n$. We say that the pair (a_n, b_n, r_n) is a characteristic triple for the gaussian asymptotic law of R.

1.6. **Previous results for distributional analyses.** All the analyses previously described in 1.3 are "average–case analyses". Knopfmacher and Knopfmacher studied in [18] the exact distribution of number of steps. Then, Friesen and Hensley [14] obtained large deviations in this context. For the number case, there were recently two breakthroughs; the first one, in 1994, when Hensley [16] performed the first distributional analysis, and proved that the number of steps has an asymptotic Gaussian behaviour. However, his proof is not easily extended to other parameters of the algorithm. Then, three years ago, Baladi and Vallée [2] have extended the dynamical analysis method for obtaining limit distributions, for a large class of costs, the so-called additive costs of moderate growth, defined in (8). They deal with the dynamical system underlying the algorithm and make a deep use of the weighted transfer operator, relative to an elementary cost c, which depends on two parameters (s,w) and is defined as

$$\mathbf{G}_{s,w,[c]}[f](x) := \sum_{m\ge 1}\frac{1}{(m+x)^{2s}}\cdot\exp[wc(m)]\cdot f\left(\frac{1}{m+x}\right). \tag{11}$$

For $w=0$, the operator is the plain transfer operator $\mathbf{G}_s$

$$\mathbf{G}_{s}[f](x) := \sum_{m\ge 1}\frac{1}{(m+x)^{2s}}\cdot f\left(\frac{1}{m+x}\right). \tag{12}$$

When c is of moderate growth, for (s,w) near $(1,0)$, the operator $\mathbf{G}_{s,w,[c]}$ acts on $\mathcal{C}^1([0,1])$ and admits a unique dominant eigenvalue denoted by $\lambda(s,w,[c])$. In the same vein, the dominant eigenvalue of $\mathbf{G}_s$ is just denoted by $\lambda(s)$. These dominant eigenvalues play a central work in [2], and also in the present paper. The particular case when c equals the binary length ℓ is crucial in study of bit–complexities.

The result of [2] can be stated as follows.

Theorem *A* (I). [Asymptotic gaussian law for additive costs of moderate growth] (Baladi and Vallée). *Consider an additive cost C relative to an elementary cost c of moderate growth.*
(i) On the set of integer inputs of size n, the cost C asymptotically follows a gaussian law, with mean, variance and speed of convergence given by

$$\mathbb{E}[C_n] = \mu(c)\cdot n + \mu_1(c) + O(2^{-n\gamma}),\quad \mathbb{V}[C_n] = \rho(c)\cdot n + \rho_1(c) + O(2^{-n\gamma}),\quad r[C_n] = O(n^{-1/2}).$$

Here γ is a strictly positive constant which does not depend on cost c.
(ii) The constants $\mu(c)$ and $\rho(c)$ are related to the dominant eigenvalue $\lambda(s,w)$ of the transfer operator $\mathbf{G}_{s,w,[c]}$, defined in (11) and acting on $\mathcal{C}^1([0,1])$. More precisely, they are expressed with the first five derivatives of order 1 and 2 of $\lambda(s,w)$ at $(s,w)=(1,0)$,

$$\mu(c) = \frac{2\log 2}{|\lambda'_s(1,0)|}\cdot\lambda'_w(1,0), \tag{13}$$

$$\rho(c) = \frac{2\log 2}{|\lambda'_s(1,0)|^3}\cdot\left[\lambda'^2_s(1,0)\cdot\lambda''_{w^2}(1,0) - 2\lambda'_w(1,0)\cdot\lambda'_s(1,0)\cdot\lambda''_{sw}(1,0) + \lambda'^2_w(1,0)\cdot\lambda''_{s^2}(1,0)\right]. \tag{14}$$

The computational status of these two constants $\mu(c)$ and $\rho(c)$ is different. Very often, the first derivatives of the pressure admit a closed form at $(1,0)$. For instance, in the case when the cost c is the binary length ℓ,

$$\lambda'_s(1,0) = -\frac{\pi^2}{6\log 2}\qquad \lambda'_w(1,0) = \frac{2}{\log 2}\,\log\prod_{i=0}^{\infty}(1+\frac{1}{2^i}),\qquad \mu(\ell) = \frac{12\log 2}{\pi^2}\log\prod_{i=0}^{\infty}(1+\frac{1}{2^i}). \tag{15}$$

It does not seem to be the same for the constant $\rho(c)$. In [20], Lhote performs a general study for the computational status for this type of "spectral constants" and proves that $\rho(c)$ is polynomial–time computable.

2. Results and outline of the method.

Neither the bit–complexities nor the length of the remainders belong to the class of additive costs. These bit–complexity costs are more difficult to deal with, because they involve both continuants and digits, in a multiplicative way. Here, we aim to study the distribution of the bit–complexity, and we wish to extend both the results of Akhavi and Vallée, about the average bit–complexity, and the general distributional methods of Baladi and Vallée. We wish also to study the evolution of the size of remainders v_i.

2.1. **Extended bit–complexity.** The "extended" cost D defined in (7) is easier to analyze because it is, in a sense, more regular than cost B. We prove here that, on the set of inputs (u, v) of size n, and, in the two cases, polynomial case (P) , and integer case (I), the cost D follows asymptotically a gaussian law.

Theorem 1 (P). [Extended polynomial bit–complexity.] *On the set of polynomial inputs of size n, the bit complexity D of the extended Euclid algorithm follows asymptotically a gaussian law, with mean, variance and speed of convergence given by*

$$\mathbb{E}[D_n] = \frac{2q-1}{q}\cdot n^2\cdot[1+O\left(\frac{1}{n}\right)], \qquad \mathbb{V}[D_n] = \frac{q-1}{q^2}\cdot n^3[1+O\left(\frac{1}{n}\right)], \qquad r[D_n] = O(n^{-1/2}). \tag{16}$$

In fact, it is easy to obtain, in case (P), the exact asymptotic expansion of both $\mathbb{E}[D_n]$ and $\mathbb{V}[D_n]$. In the integer case, the results are of the same spirit; however, the main constants that intervene in the mean and the variance are more involved, and the proven speed of convergence is not optimal.

Theorem 1 (I). [Extended integer bit–complexity.] (i) *On the set of integer inputs of size n, the bit complexity D of the extended Euclid algorithm follows asymptotically a Gaussian law, with mean, variance and speed of convergence given by*

$$\mathbb{E}[D_n] = \mu(\ell)\cdot n^2\cdot[1+O\left(\frac{1}{n}\right)], \qquad \mathbb{V}[D_n] = \rho(\ell)\cdot n^3[1+O\left(\frac{1}{n}\right)], \qquad r[D_n] = O(n^{-1/3}), \tag{17}$$

where $\mu(\ell)$ and $\rho(\ell)$ are the constants which appear in (13,14) of Theorem A*, when the cost c is the binary length ℓ.*

2.2. **Standard bit–complexity.** For the standard bit–cost B, defined in (6), we prove the following:

Theorem 2 (P). [Standard polynomial bit–complexity.] *On the set of polynomial inputs of size n, the bit complexity B of the standard Euclid algorithm follows asymptotically a gaussian law, with mean, variance and speed of convergence given by*

$$\mathbb{E}[B_n] = \frac{2q-1}{2q}\cdot n^2\cdot[1+O\left(\frac{1}{n}\right)], \qquad \mathbb{V}[B_n] = \frac{q-1}{3q^2}\cdot n^3[1+O\left(\frac{1}{n}\right)], \qquad r[B_n] = O(n^{-1/2}). \tag{18}$$

As in Theorem 1(P), it is easy to obtain, in this case, the exact asymptotic expansions of both $\mathbb{E}[B_n]$ and $\mathbb{V}[B_n]$. For the integer case, we have only partial results: we already know from results of Akhavi and Vallée [1] that $\mathbb{V}[B_n]$ is of order $o(n^4)$. Here, we study more precisely the asymptotic behaviour of the variance $\mathbb{V}[B_n]$. Moreover, we will state in Section 4 two conjectures : a conjecture (C) which allows to relate the variance $\mathbb{V}[B_n]$ and the variance $\mathbb{V}[D_n]$, and a conjecture (G) which entails the plausibility of an asymptotic gaussian law for the standard bit-complexity B, even if it does not itself imply this asymptotic behaviour.

Theorem 2 (I). [Standard integer bit–complexity.] *On the set of integer inputs of size n, the mean and the variance of B_n satisfy*

$$\mathbb{E}[B_n] = \mu_0(\ell)\cdot n^2\cdot[1+O\left(\frac{1}{n}\right)], \qquad \mathbb{V}[B_n] = \rho_0(\ell)\cdot n^3[1+O\left(\frac{1}{n}\right)], \tag{19}$$

The constant $\mu_0(\ell)$ is related to constant $\mu(\ell)$ via the equality $\mu_0(\ell) = (1/2)\mu(\ell)$.

Moreover, under the conjecture (C) the constant $\rho_0(\ell)$ is related to constant $\rho(\ell)$ of Theorem 1 (I) via the equality $\rho_0(\ell) = (1/3)\rho(\ell)$.

2.3. **Size of remainders.** We are also interested in describing the evolution of the size of remainders v_i during the execution of the algorithm, and we consider the size of the remainder v_i at "a fraction of the depth". For an input (u, v), we denote by $P(u, v)$ the number of iterations of the Euclid Algorithm on the input (u, v), that is also called the depth of (u, v). Furthermore, for a real $\delta \in]0, 1[$, the random variable $L^{[\delta]}$ is the size of remainder v_i when i equals $\lfloor \delta P \rfloor$. It is defined as

$$L^{[\delta]}(u, v) := \ell(v_{\lfloor \delta P(u,v) \rfloor}). \tag{20}$$

The following result shows that the size of the remainders at a fraction δ of the depth asymptotically follows a gaussian law, at least when δ is rational. This proves that the evolution of the sizes of remainders is very regular during an execution of the algorithm. This result constitutes a "discrete version" of the well-known result of [22] (sharpened by Vallée in [29]) who shows that the n-th continuant of a real $x \in \mathcal{I}$ asymptotically follows a gaussian law, when $\mathcal{I}$ is endowed with any density of class C^1.
This result also plays a central rôle in the analysis of the so–called Interrupted Euclidean Algorithm which stops as soon as the size $\ell(v_i)$ of the remainder v_i is less than $\delta \cdot \ell(v_0)$. An average–case analysis of the Interrupted Algorithm is provided in [5], and the present results are a first [but crucial] step towards the distributional analysis of the algorithm. And the Interrupted Algorithm is itself a basic procedure of the Lehmer Euclid Algorithm [19], or the recursive Euclidean Algorithms [24, 6].

Theorem 3. [Gaussian limit law for sizes of remainders at a fraction of the depth.] *Consider a rational δ of $]0, 1[$. On the set of inputs of size n, the length $L^{[\delta]}$ defined in (20) follows asymptotically a Gaussian law. The speed of convergence is*

$$r_n = O(n^{-1/2}) \quad \text{in case (P)}, \qquad r_n = O(n^{-1/3}) \quad \text{in case (I)},$$

and the following estimates hold for the mean and the variance,

$$\text{Case (I):} \quad \mathbb{E}[L_n^{[\delta]}] = \mu_{[\delta]} \cdot n + O(1), \qquad \mathbb{V}[L_n^{[\delta]}] = \rho_{[\delta]} \cdot n + O(1),$$

$$\text{Case (P):} \quad \mathbb{E}[L_n^{[\delta]}] = \mu_{[\delta]} \cdot n + \mu_1(\delta) + O(2^{-n\gamma}), \qquad \mathbb{V}[L_n^{[\delta]}] = \rho_{[\delta]} \cdot n + \rho_1(\delta) + O(2^{-n\gamma}).$$

Here γ is a strictly positive constant which depends on δ, and the constants $\mu_{[\delta]}$ and $\rho_{[\delta]}$ satisfy

$$\mu_{[\delta]} = (1 - \delta), \qquad \rho_{[\delta]} = \frac{\delta(1-\delta)}{q-1} \quad \text{in case (P)}, \qquad \rho_{[\delta]} = \delta(1-\delta)\frac{|\Lambda''(1)|}{|\Lambda'(1)|} > 0 \quad \text{in case (I)},$$

where $\Lambda(s)$ is the logarithm of the dominant eigenvalue $\lambda(s)$ of the operator $\mathbf{G}_s$ defined in (12).

Remark. Our methods only allow to deal with the case when δ is irrational.

We describe now the main principles of our method.

2.4. **Generating Functions.** We mainly use methods from analytic combinatorics, which deal with generating functions. See the book [12] for a complete treatment of this methodology. Our main tool is, as usual in analysis of algorithms, (bivariate) generating functions which depend on two parameters: the first one "marks" the input size, and the second one "marks" the cost of interest. For reasons which will appear clearer later, and unlike in classical use, we choose generating functions of Dirichlet type with respect to the size parameter s. The (bivariate) generating function of some cost R defined on the input set Ω will be

$$S_R(s, w) := \sum_{(u,v)\in\Omega} \frac{1}{||v||^{2s}} \exp[wR(u, v)] = \sum_{k\geq 1} \frac{1}{k^{2s}} r_k(w) \tag{21}$$

where $r_k(w)$ is the cumulative value of $\exp[wR]$ on inputs for which $||v|| = k$. We recall that $||v|| = v$ in the integer case and $||v|| = q^{\deg v}$ in the polynomial case. Then, in integer case, this series remains a (general) Dirichlet series, while, in polynomial case, this is in fact a power series in $z = q^{-2s}$ which will be alternatively denoted by $T_R(z, w)$,

$$T_R(z, w) := S_R(-\frac{1}{2}\log_q z, w) = \sum_{(u,v)\in\Omega} z^{\deg v} \exp[wR(u, v)]. \tag{22}$$

We recognize in $T_R(z,w)$ the usual bivariate generating function, where variable z marks the degree, quite close to the polynomial input size . These bivariate series are used for analyzing the distribution of cost R.

If we restrict our study to the moment of order k, we deal with a Dirichlet Series $S_R^{[k]}(s)$ with respect to the unique variable s, which is the k-th derivative of $w \mapsto S_R(s,w)$ at $w=0$,

$$S_R^{[k]}(s) := \frac{\partial^k}{\partial w^k} S_R(s,w)|_{w=0} = \sum_{(u,v)\in\Omega} \frac{1}{||v||^{2s}} R^k(u,v). \tag{23}$$

This is also a power series $T_R^{[k]}(z)$ in the polynomial case, namely

$$T_R^{[k]}(z) = \sum_{(u,v)\in\Omega} R^k(u,v) \cdot z^{\deg v}.$$

We first look for an alternative expression for these series $S_R(s,w)$ from which the position and the nature of the dominant singularity of $S_R(s,w)$ become apparent. Then, with taking derivatives, we also obtain alternative expressions for $S_R^{[k]}(s)$. Then, we transfer these informations on the coefficients of $S_R(s,w)$ or $S_R^{[k]}(s)$, which are our prime subject of interest.

How to obtain an alternative expression for series $S_R(s,w)$? In the case of the polynomial gcd, it is possible to directly deal with the bijection (5), because it keeps track of the size; for instance, for an additive cost C related to some step-cost c, we easily obtain an alternative form for $T_C(z,w)$ which involves the quasi inverse $1/(1-G_c(z,w))$ of the generating function $G_c(z,w)$ relative to cost c,

$$G_c(z,w) = \sum_{m\in\mathcal{G}} \exp[wc(m)] \cdot z^{\deg m}. \tag{24}$$

And, now, for integers? The bijection is of no longer use, since it does not deal properly with the integer size, and the series $S_R(s,w)$ cannot be directly expressed with the quasi-inverse of $1/(1-A_c(s,w))$ of the generating function $A_c(s,w)$ relative to cost c,

$$A_c(s,w) = \sum_{m\in\mathcal{G}} \frac{1}{||m||^{2s}} \exp[wc(m)]. \tag{25}$$

We will use the transfer operator $G_{s,w,[c]}$ relative to the underlying dynamical system, defined in (11), as a "generating" operator, and we will deal with the more elaborated bijection (39) : now, the bivariate series $S_C(s,w)$ can be expressed with the quasi-inverse $(I-\mathbf{G}_{s,w,[c]})^{-1}$ of $\mathbf{G}_{s,w,[c]}$ [see for instance Equation (51)].

It will be possible to transfer these informations on the coefficients of series, as soon as we dispose of a convenient "extractor" which expresses coefficients of series as a function of the series itself. Of course, the common extractor is the Cauchy formula. For power series, the usual integration contour is a (compact) circle, whereas it is an (unbounded) vertical line for Dirichlet series; this explains why it is more difficult to deal with Dirichlet series than usual (power) series. The main "extractors" for Dirichlet series are Tauberian Theorems [which do not provide remainder terms], or the Perron Formula [which may provide remainder terms]. Tauberian theorems are well-adapted for average–case analysis, but Perron's formulae are essential in distributional analysis. However, they need a more precise information on the quasi–inverse of $(I-\mathbf{G}_{s,w})^{-1}$, namely the existence of a vertical strip free of poles (as in the Prime Number Theorem...)

2.5. **Decomposition of bit-complexity costs.** Our first step is quite natural. Since the expression of the bit–complexities is quite involved , we "split" each cost of interest [namely the cost B, and the extended cost D] into two parts: a "main" cost X, which will be (asymptotically) gaussian, and a "remainder" cost Y, which will be (asymptotically) more concentrated that the main cost. The following result proves that, in this general framework, the total cost $Z=X+Y$ is (asymptotically) gaussian, and its characteristics –mean value, variance, and speed of convergence– are expressed with characteristics of X and Y.

Definition 2. [Variance-equivalence] *Consider two costs X and Z, defined on Ω and their restrictions X_n, Z_n to Ω_n. We say that X and Z are variance–equivalent if $\mathbb{V}[X_n - Z_n] = o(\mathbb{V}[X_n])$ for*

$n \to \infty$. They are called equivalent with order α_n [with $\alpha_n \to 0$] if $\mathbb{V}[X_n - Z_n] = \alpha_n \cdot \mathbb{V}[X_n]$. We denote by $X \asymp_\alpha Z$ such a situation.

Proposition 1. *Consider two costs X and Z, defined on Ω and their restrictions X_n, Z_n to Ω_n. Suppose that X and Z are variance–equivalent (with order α_n) and that X admits an asymptotic gaussian limit law with a speed of convergence $r[X_n]$. Then Z admits an asymptotic gaussian limit law, with a variance and a speed of convergence which satisfy*

$$\mathbb{V}[Z_n] = \mathbb{V}[X_n] \cdot [1 + O(\alpha_n^{1/2})], \qquad r[Z_n] = r[X_n] + O(\alpha_n^{1/3}).$$

Proof. Consider $Y := Z - X$ and the two variables $\bar{X}_n = (X_n - \mathbb{E}[X_n]) \cdot (\mathbb{V}[X_n])^{-1/2}$ and $\bar{Y}_n = (Y_n - \mathbb{E}[Y_n]) \cdot (\mathbb{V}[X_n])^{-1/2}$. Then, the random variable $\bar{X}_n + \bar{Y}_n$ satisfies

$$\mathbb{P}[\bar{X}_n + \bar{Y}_n \le a] = \mathbb{P}\left[\left[\bar{X}_n + \bar{Y}_n \le a\right] \cap \left[|\bar{Y}_n| \le \epsilon_n\right]\right] + \mathbb{P}\left[\left[\bar{X}_n + \bar{Y}_n \le a\right] \cap \left[|\bar{Y}_n| > \epsilon_n\right]\right].$$

The second term is less than $\mathbb{P}\left[|\bar{Y}_n| > \epsilon_n\right]$, and, with the Markov inequality, it is $O(\alpha_n \cdot \epsilon_n^{-2})$. Now, for the first term, one has

$$\mathbb{P}\left[\bar{X}_n \le a - \epsilon_n\right] \le \mathbb{P}\left[\left[\bar{X}_n + \bar{Y}_n \le a\right] \cap \left[|\bar{Y}_n| \le \epsilon_n\right]\right] \le \mathbb{P}\left[\bar{X}_n \le a + \epsilon_n\right],$$

and both lower and upper bounds are of the form

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{a \pm \epsilon_n} e^{-t^2/2} dt + O(r_n) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{a} e^{-t^2/2} dt + O(r_n + \epsilon_n),$$

with $r_n = r[X_n]$. Finally, the speed of convergence is $O(r_n + \epsilon_n + \alpha_n \cdot \epsilon_n^{-2})$ and the optimal choice $\epsilon_n^3 = \alpha_n$ provides the result. ∎

Remark. In case (P), we deal with an order $\alpha_n = O(n^{-2})$ [which will entail an optimal speed of convergence of order $n^{-1/2}$], whereas we only obtain an order $\alpha_n = O(n^{-1})$ [which will entail a speed of convergence of order $n^{-1/3}$]. In both cases, the variances studied are of order n^3 and are proven to admit an asymptotic expansion, which is polynomial wrt n. Then the estimates about the variances can be improved and become $\mathbb{V}[Z_n] = \mathbb{V}[X_n] + O(n^2)$.

2.6. **Quasi-Powers Theorem.** This theorem provides sufficient conditions on the moment generating function under which the parameter R is proven to follow an asymptotic gaussian law.

Theorem *B*. [Hwang] *Consider a cost R defined on a set Ω and and its restriction R_n to Ω_n, and suppose that the moment generating function $\mathbb{E}[\exp(wR_n)]$ of R_n is an analytic function on a neighborhood $\mathcal{W}$ of $w = 0$ and satisfies on $\mathcal{W}$*

$$\mathbb{E}[\exp(wR_n)] = \exp[\beta_n A(w) + B(w)] \cdot \left(1 + O(\kappa_n^{-1})\right) \qquad (\beta_n, \kappa_n \to \infty),$$

with $A(w)$, $B(w)$ analytic on $\mathcal{W}$ and a O-term uniform on $\mathcal{W}$. Then, the expectation and the variance of R_n satisfy

$$\mathbb{E}[R_n] = A'(0) \cdot \beta_n + B'(0) + O(\kappa_n^{-1}), \quad \mathbb{V}[R_n] = A''(0) \cdot \beta_n + B''(0) + O(\kappa_n^{-1}).$$

Moreover, if $A''(0)$ is not zero, then R_n asymptotically a Gaussian law with speed of convergence $r_n = O(\kappa_n^{-1} + \beta_n^{-1/2})$.

2.7. **Various types of costs.** With the previous decomposition, we are then led to study various costs C, and in particular, the so–called end–costs and additive costs, whose generating functions will be easy to deal with. The behaviour of additive costs C heavily depends on the behaviour of cost c.

Definition 3. [Types of cost] (i) *An elementary cost c and its associated additive cost C are of intermediate growth if $c(m) = O(\ell(m)^\beta)$ with $\beta > 0$. An elementary cost c and its associated additive cost C are of moderate growth if $c(m) = O(\ell(m))$.*
(ii) *An end–cost R is a cost which only depends on gcd $v_p$and last quotient m_p in a polynomial way wrt the sizes $\ell(v_p), \ell(m_p)$. A mixed cost is a cost which is the product of an end cost by an additive cost of an intermediate growth.*

The general philosophy of our work is now summarized by the following theorem, which is one of the basic results of our paper.

Theorem 4. *The following holds:*

(*a*) *In case* (I), *any additive cost* C *of moderate growth is asymptotically gaussian with a characteristic triple of the form* $[O(n), O(n), O(n^{-1/2})]$. *In case* (P), *any additive cost* C *of moderate growth, whose elementary cost is not proportional to* $c = \deg$, *is asymptotically gaussian with a characteristic triple of the form* $[O(n), O(n), O(n^{-1/2})]$.

(*b*) *In case* (P), *the costs* N *defined in (9) are asymptotically gaussian with a characteristic triple of the form* $[O(n^2), O(n^3), O(n^{-1/2})]$.

(*c*) *Any additive cost* C *of intermediate growth satisfies the concentration property, i.e., the expectation* $\mathbb{E}[C_n]$ *and the variance* $\mathbb{V}[C_n]$ *are* $O(n)$.

(*d*) *Any end–cost has all its moments of order* $O(1)$. *Any mixed cost has an expectation of order* $O(n)$.

Remark. We conjecture that Assertion (*b*) also holds in case (I), but we do not know how to prove it. We state this fact as our Conjecture (G).

2.8. **Plan of the paper.** Section 3 is devoted to the polynomial case, and deals with (bivariate) generating functions. Sections 4 and 5 deal with the number case: Section 4 describes the dynamical system underlying the Euclid algorithm, introduces the transfer operator and provides alternative expressions of the generating functions which involve the transfer operator. Then, in Section 5, we perform the analytic study, and obtain the main results in the number case. In Section 6, we describe an unified framework for the two cases (P) and (I).

3. The Euclid algorithm on polynomials.

We perform the analysis of the Euclid algorithm on $\mathbb{F}_q[X]$, and we wish to prove the four Theorems with their (P) version. We first decompose the bit-complexities cost, and show that these decompositions involve the costs which are studied in Theorem 4. Then, the remainder of this Section is devoted to the proof of the version (P) of Theorem 4 and Theorem 3. The main tool here for studying the behaviour of these costs is the generating function, univariate (in the case where only moments are analysed) or bivariate, when we expect a gaussian limit law. When all the assertions of Theorem 4 are proven, we obtain Theorem 1 (P) and Theorem 2 (P) with an application of Proposition 1.

3.1. **Decomposition of costs.** For simplicity, we denote by m_{p+1} the monic gcd v_p. The polynomial case (P) will be easier because both bit-complexities B and D are only expressed with the sequence $\ell(m_i)$ (with $1 \le i \le p+1$). Since the degrees of polynomials v_i and s_i are both related to degrees $\deg m_i$ of quotients m_i, one has, for any i, with $0 \le i \le p$,

$$\deg v_i = \sum_{j=i+1}^{p+1} \deg m_j, \qquad \deg s_i = \sum_{j=1}^{i-1} \deg m_j, \qquad \ell(v_i) + \ell(s_i) = 2 + \ell(v_0) - \ell(m_i). \tag{26}$$

This provides the following decompositions for the bit-complexities:

Proposition 2(P). *On* Ω_n, *the extended bit-complexity* $D = D_n$ *decomposes as*

$$D_n = \left[n \cdot \sum_{i=1}^{p-1} \ell(m_i) \right] + \left[2 \cdot \sum_{i=1}^{p-1} \ell(m_i) - \sum_{i=1}^{p-1} \ell^2(m_i) \right] + [\ell(m_p) \cdot \ell(m_{p+1})]$$

On Ω_n, *the plain bit-complexity* $B = B_n$ *decomposes as*

$$B_n = \left[\frac{1}{2}(n-1)^2 - 1 + \sum_{i=1}^{p+1} i \cdot \deg m_i \right] + \left[\sum_{i=1}^{p+1} (1 - \frac{1}{2} \deg^2 m_i) \right].$$

With Theorem 4 (P), *and Definition 2, the following holds on* Ω_n,

$$D \asymp_{(n^{-2})} n \cdot L, \quad \text{with} \quad L = \sum_{i=1}^{p-1} \ell(m_i) \qquad\qquad B \asymp_{(n^{-2})} N + \frac{n^2}{2}, \quad \text{with} \quad N = \sum_{i=1}^{p+1} i \deg m_i,$$

and the costs $n \cdot L$ *and* N *are both asymptotically gaussian with a characteristic triple of the type* $[O(n^2), O(n^3), O(n^{-1/2})]$.

Proof. Each decomposition exhibits three possible blocks delimited by square brackets. The first block will provide the "main" part, which will be proven to be (asymptotically) gaussian. The

cost L is an additive cost of moderate growth and will be proven to be asymptotically gaussian in Section 3.3. The gaussian behaviour of cost N will be proven in Section 3.5. The possible third block is formed with end costs studied in Section 3.8. The second block is formed with additive costs of intermediate growth, whose variance will be proven of order $O(n)$ in Section 3.7. ■

3.2. **Generating functions.** Here, our main tools are *generating functions*, since it will be easy to transfer operations on the polynomials into operations on the generating functions. We will always deal with generating functions which will be fractional fractions with respect to z and $t = e^w$. The reference size for generating functions is the degree. We recall that the Euclidean algorithm builds a bijection between Ω and the cartesian product $\mathcal{G}^\star \times \mathcal{U}$ with

$$\Omega := \{(u, v); v \text{ monic} \quad \text{and} \quad [u = 0 \quad \text{or} \quad \deg u < \deg v]\},$$

$$\mathcal{G} := \{m \in \mathbb{F}_q[X]; \quad \deg m \geq 1\}, \qquad \mathcal{U} := \{v \in \mathbb{F}_q[X]; \quad v \quad \text{monic}\}.$$

The generating functions $T(z)$ of Ω, $G(z)$ of $\mathcal{G}$, $U(z)$ of $\mathcal{U}$ are then equal to

$$T(z) = \frac{1}{1 - q^2 z} \qquad G(z) = \frac{(q-1)qz}{1 - qz} = (q-1)\left[\frac{1}{1-qz} - 1\right], \qquad U(z) = \frac{1}{1-qz}.$$

The fundamental bijection, which is compatible with the notion of size, can be translated into an equality between generating functions. Since the generating function of $\mathcal{G}^\star$ is just the quasi-inverse $1/(1 - G(z))$, we finally obtain

$$T(z) = \frac{1}{1 - G(z)} \cdot U(z).$$

Of course, this equality is trivial in this case. However, we will see how useful it will be when we refine it when considering some *additive cost*. Flajolet adopts this point of view in [11], and obtains a concise and elegant proof of results previously obtained in [18] [with counting arguments] on the distributional analysis of the number of iterations.

In the remainder of this section, we make a constant use of bivariate generating functions relative to some parameter R, namely the series $T_R(z, w)$ or $\hat{T}_R(z, t)$

$$T_R(z, w) := \sum_{(u,v)\in\Omega} e^{wR(u,v)} \cdot z^{\deg v}, \qquad \hat{T}_R(z, t) := \sum_{(u,v)\in\Omega} t^{R(u,v)} \cdot z^{\deg v}.$$

We first analyse costs for which we expect an asymptotic gaussian law, namely
- additive costs of moderate growth, in 3.3 and 3.4,
- cost N in 3.5,
- degree of the remainder v_i at a fraction of the execution in 3.6.

3.3. **Gaussian law for additive costs of moderate growth.** Consider a cost c defined on $\mathbb{F}_q[X]$. The total cost C relative to c is defined on the set Ω as

$$C(u, v) := \sum_{i=1}^{p} c(m_i).$$

Consider also the bivariate generating functions $G_c(z, w), T_C(z, w)$

$$G_c(z, w) := \sum_{m\in\mathcal{G}} e^{wc(m)} \cdot z^{\deg m}, \qquad T_C(z, w) := \sum_{(u,v)\in\Omega} e^{wR(u,v)} \cdot z^{\deg v}.$$

Now, the bijection (5), together with the additivity of cost (8) provide a relation between the bivariate generating functions $G_c(z, w), U(z), T_C(z, w)$, namely

$$T_C(z, w) = \frac{U(z)}{1 - G_c(z, w)}. \tag{27}$$

The moment generating function $\mathbb{E}[\exp(wC_n)]$ is expressed with coefficients of $T_C(z, w)$ and $T(z) = T_C(z, 0)$ as

$$\mathbb{E}[\exp(wC_n)] = \frac{[z^{n-1}]T_C(z, w)}{[z^{n-1}]T_C(z, 0)}.$$

With the particular form of T_C, it is clear that the dominant singularity is brought by the denominator; it is located at $z = \sigma(w)$, where $\sigma(w)$ is defined by the equation $G(\sigma(w), w) = 1$. At $w = 0$, one has $\sigma(w) = q^{-2}$ and the two derivatives

$$G'_z(q^{-2}, 0) = G'_z(q^{-2}) = \frac{q^3}{q-1}, \qquad G'_w(q^{-2}, 0) = \sum_{m\in\mathcal{G}} c(m) \cdot q^{-2\deg m} = \sum_{m\in\mathcal{G}} \frac{c(m)}{||m||^2},$$

are not zero. From the Implicit Function Theorem, and the moderate growth condition, such a function σ is well–defined and analytic on a neighborhood of $w = 0$ and satisfies $\sigma(0) = 1/q^2$. Since G is analytic, the denominator $1 - G_c(z, w)$ possesses a simple pôle at $s = \sigma(w)$. And finally, on a neighborhood of $w = 0$,

$$[z^n]T_C(z, w) = \exp[-n\Sigma(w) + V(w)] \cdot [1 + O(\theta^n)], \qquad \text{with} \quad \Sigma(w) = \log\sigma(w), \quad \theta < 1.$$

Moreover V is analytic on $\mathcal{W}$, and the O–term is uniform on $\mathcal{W}$. Then, the Quasi-Powers Theorem applies, with

$$A(w) = -\Sigma(w) + \Sigma(0), \qquad B(w) = V(w) - V(0), \quad \kappa_n = \theta^{-n},$$

and provides the estimates for the mean and the variance,

$$\mathbb{E}[C_n] = -\Sigma'(0) \cdot n + V'(0) + O(\theta^n), \qquad \mathbb{V}_n = \Sigma''(0) \cdot n + V''(0) + O(\theta^n).$$

Provided that the condition $\Sigma''(0) \neq 0$ holds, this entails an asymptotic gaussian law with a speed of convergence $r_n = O(n^{-1/2})$.
We now study in the next lemma the condition $\Sigma''(0) \neq 0$.

Lemma 1. *For a cost c defined on $\mathbb{F}_q[X]$, consider the function σ defined on a neighborhood of $w = 0$ by the equality $G(\sigma(w), w) = 1$, and denote by Σ the function defined by $\Sigma = \log\sigma$. Then, the two conditions are equivalent*

(i) $\Sigma''(0) = 0$,

(ii) The cost c is proportional to cost deg.

Proof. At $z = \sigma(w)$, the series $G(z, w)$ satisfies

$$1 = G(\sigma(w), w) = \sum_{m\in\mathcal{G}} e^{f_m(w)} \qquad \text{with} \qquad f_m(w) := wc(m) + \Sigma(w)\deg m.$$

We already know that the two derivatives $G'_z(q^{-2}, 0)$ and $G'_z(q^{-2}, 0)$ are not zero. This implies (with taking the derivative of the equality $G(\sigma(w), w) = 0$) that $\sigma'(0) \neq 0$, and this entails that $\Sigma'(0) \neq 0$. With two derivations wrt w, at $w = 0$, we obtain

$$0 = \sum_{m\in\mathcal{G}} [f''_m(w) + f'^2_m(w)] \cdot e^{f_m(w)}. \tag{28}$$

If $\Sigma''(0) = 0$, then the equality $f''_m(0) = \Sigma''(0) \cdot \deg m = 0$ holds for all $m \in \mathcal{G}$. Then, Relation (28) proves the equality $f'_m(0) = 0 = c(m) + \Sigma'(0) \cdot \deg m$, valid for all $m \in \mathcal{G}$. Since $\Sigma'(0) \neq 0$, this entails that $c(m)$ is a linear function of $\deg m$.
Conversely, if c is of the form $c(m) = d \cdot \deg m$, then $G(z, w)$ can be written as

$$G(z, w) = \frac{(q-1)qze^{dw}}{1 - qze^{dw}} = G(ze^{dw}), \tag{29}$$

and the function $\sigma(w)$ is defined by the relation $\sigma(w) = q^{-2} \cdot e^{-dw}$. Then Σ is a linear function of w and $\Sigma''(0) = 0$. This ends the proof of the lemma. ■

Remark. If we are interested in an additive cost defined by $C(u, v) := \sum_{i=1}^{p} c(m_i) + d(v_p)$, the bivariate series is now

$$T_C(z, w) = \frac{U_d(z, w)}{1 - G_c(z, w)}, \tag{30}$$

and the analysis is almost the same [compare (27) and (30)].

3.4. **Some particular costs of moderate growth.** We consider the cases when c is constant, and then the case when $c = \ell$. The total costs C associated are of main algorithmic interest since the cost relative to $c = 1$ is the number P of iterations and the cost relative to $c = \ell$ is the total space necessary for the sequence of the digits. This is also equal to the total encoding length of the continued fraction relative to the input u/v (see Introduction and Section 6).

Case $c = 1$. Here, the series $G(z, w)$ satisfies $G(z, w) = e^w G(z)$, so that the function σ is defined by the relation

$$\frac{1}{\sigma(w)} = q[1 + (q-1)e^w].$$

Then, the two first derivatives of $\Sigma = \log \sigma$ satisfy : $\quad -\Sigma'(0) = \dfrac{q-1}{q}, \qquad \Sigma''(0) = \dfrac{q-1}{q^2}.$

Case $c = \ell$. Here, the series $G(z, w)$ satisfies

$$G(z, w) = e^w \cdot \sum_{m \in \mathcal{G}} (ze^w)^{\deg m} = \frac{(q-1)qze^{2w}}{1 - qze^w} = e^w G(ze^w)$$

so that the function σ is defined by the relation: $\quad \dfrac{1}{\sigma(w)} = qe^w \cdot [1 + (q-1)e^w].$

Then, the two first derivatives of $\Sigma = \log \sigma$ satisfy: $\quad -\Sigma'(0) = \dfrac{2q-1}{q}, \qquad \Sigma''(0) = \dfrac{q-1}{q^2}.$

This entails that the mean value $\mathbb{E}[L_n]$ of the total encoding length of the continued fraction is asymptotic to $n \cdot [2 - (1/q)]$.

3.5. **Gaussian law for Cost N.** The main cost in the decomposition of the cost B involves the cost N defined as

$$N(u, v) := \sum_{i=1}^{p+1} i \cdot \deg m_i,$$

and we now show that N asymptotically follows a gaussian law. The bivariate generating function $T_N(z, w)$ admits the alternative expression

$$T_N(z, w) = U(z, w) + \sum_{p \geq 1} G(z, w) \cdot G(z, 2w) \cdot \ldots \cdot G(z, pw) \cdot U(z, (p+1)w)$$

which involves the bivariate generating functions $U(z, w)$ et $G(z, w)$ relative to cost $c = \deg$. In this case, letting $t = e^w$, the equalities $G(z, w) = G(zt), U(z, w) = U(zt)$ hold and we deal in this subsection with the bivariate generating function $\hat{T}_N(z, t)$. This series satisfies

$$\hat{T}_N(z, t) = U(zt) + \sum_{p \geq 1} G(zt) \cdot G(zt^2) \cdot \ldots \cdot G(zt^p) \cdot U(zt^{p+1}), \tag{31}$$

and then satisfies the following functional equation

$$\hat{T}_N(z, t) = U(zt) + G(zt) \cdot \hat{T}_N(zt, t), \tag{32}$$

which appears in other studies related to analyses of path-lengths. Using the explicit formulae for G, U, we obtain

$$\hat{T}_N(z, t) = \sum_{p \geq 0} [(q-1)qz]^p \cdot t^{p(p+1)/2} \cdot \prod_{j=1}^{p+1} \frac{1}{1 - qzt^j}$$

The last sum is of the form $\Phi(-(q-1), -qz, t)$ with

$$\Phi(u, \xi, t) := \sum_{p \geq 0} \xi^p u^p \cdot t^{p(p+1)/2} \prod_{j=1}^{p+1} \frac{1}{1 + \xi t^j}.$$

Since Φ satisfies the identity $\Phi(u, \xi, t) = 1 - t\xi(1-u)\Phi(tu, \xi, t)$, the following q-identity, which resorts to q-calculus[2],

$$\Phi(u, \xi, t) = 1 + \sum_{n \geq 1} (-1)^n (t\xi)^n \prod_{j=0}^{n-1} (1 - ut^j)$$

[2]The term q in the q-calculus is without relation with the cardinality q of the field $\mathbb{F}_q$.

entails an alternative expression for $\hat{T}_N(z,t)$, namely

$$\hat{T}_N(z,t) = 1 + \sum_{n\geq 1}(qzt)^n \prod_{j=0}^{n-1}(1+(q-1)t^j)$$

The moment generating function of the cost N on Ω_{n+1} is then equal to

$$\mathbb{E}[\exp(wN_{n+1})] = \frac{[z^n]T_N(z,w)}{|\Omega_{n+1}|} = e^{nw}\prod_{j=0}^{n-1}\left[\frac{1+(q-1)e^{jw}}{q}\right].$$

We now study the parameter $\widetilde{N}$ which is defined by

$$\widetilde{N}(u,v) = \frac{N(u,v)}{\ell(v)-1}, \qquad \text{i.e.,} \quad \widetilde{N}_{n+1} := \frac{N_{n+1}}{n},$$

and we prove that it follows an asymptotic gaussian law. The moment generating function of $\widetilde{N}$ on Ω_{n+1} is of the form $\exp\delta_n(w)$ with

$$\delta_n(w) = w + \sum_{j=0}^{n-1} F_w(\frac{j}{n}), \qquad \text{with} \quad F_w(y) := \log\frac{1+(q-1)e^{wy}}{q}.$$

We remark that the function F_w can be expressed with the function Σ relative to cost $c=1$, via the relation $F_w(y) = \Sigma(0) - \Sigma(wy)$. We transform the previous sum into an integral with the Euler-Mac Laurin formula, and now

$$\delta_n(w) = n\cdot A(w) + B(w) + O(\frac{1}{n}), \qquad \text{with} \quad A(w) = \int_0^1 [\Sigma(0)-\Sigma(wy)]\,dy,$$

with an analytic function B on a complex neighborhood of 0. Then

$$\mathbb{E}_n[\exp(w\widetilde{N}_n)] = \exp[(n-1)\cdot A(w) + B(w)]\cdot(1+O(\frac{1}{n})).$$

Then, the Quasi-Powers Theorem entails the following estimates for the expectation and the variance of parameter $\widetilde{N}$,

$$\mathbb{E}[\widetilde{N}_n] = A'(0)\cdot n + O(1) = \frac{q-1}{2q}\cdot n + O(1), \qquad \mathbb{V}[\widetilde{N}_n] = A''(0)\cdot n + O(1) = \frac{q-1}{3q^2}\cdot n + O(1).$$

Moreover, since $A''(0)\neq 0$, then the cost $\widetilde{N}$ follows an asymptotic normal law, with a speed of convergence $r_n = O(n^{-1/2})$. The parameter N (our prime subject of interest) then follows an asymptotic normal law with parameters

$$\mathbb{E}_n[N] = \frac{q-1}{2q}\cdot n^2 + O(n), \qquad \mathbb{V}_n[N] = \frac{q-1}{3q^2}\cdot n^3 + O(n^2), \qquad r_n = O(n^{-1/2}).$$

Remark. This proof seems to be completely specific to the case where the cost deg intervenes. The cost $N^{[c]}$ associated to another cost c of moderate growth does not seem to be analyzed with the same tool of q-calculus.

3.6. **Gaussian law for $L^{[\delta]}$.** The bivariate generating function for $L^{[\delta]}$ is just denoted by $T_{[\delta]}(z,w)$. With the bijection (5), relation (26), and the special form of the bivariate generating function $G(z,w)$ relative to $c = \deg$ [see (29)], it admits a nice alternative form

$$T_{[\delta]}(z,w) = U(ze^w)\cdot\sum_{p\geq 0} G(z)^{\lfloor\delta p\rfloor}G(ze^w)^{p-\lfloor\delta p\rfloor}. \tag{33}$$

Now, if δ is a rational of the form $\delta = c/(c+d)$, then

$$T_{[\delta]}(z,w) = U(ze^w)\cdot\left[\sum_{j=0}^{c+d-1} G(ze^w)^{j-\lfloor\delta j\rfloor}G(z)^{\lfloor\delta j\rfloor}\right]\cdot\left[\sum_{k\geq 0} G(ze^w)^{dk}\cdot G(z)^{ck}\right],$$

$$T_{[\delta]}(z,w) = U(ze^w)\cdot\left[\sum_{j=0}^{c+d-1} G(ze^w)^{j-\lfloor\delta j\rfloor}G(z)^{\lfloor\delta j\rfloor}\right]\cdot\frac{1}{1-G(z)^c\,G(ze^w)^d} \tag{34}$$

The last expression is a rational fraction wrt two variables $G(z)$ and $G(ze^w)$, and the dominant pôles are only brought by the denominator. The denominator $z \to 1 - [G(z)^\delta G(ze^w)^{1-\delta}]^D$ admits as zeroes all the values of z for which

$$\psi(z,w) := G(z)^\delta G(ze^w)^{1-\delta} = \exp[2iL\pi/D] \qquad \text{with } 0 \le L < D.$$

The Implicit Functions Theorem can be applied: there is a sufficiently small neighborhood of w on which a curve of the form $z = \sigma_L(w)$ is well defined and satisfies $\psi(\sigma_L(w), w) = \exp[2iL\pi/D]$. For $w = 0$, the equality $\psi(z, 0) = G(z)$ entails that the relation $G(\sigma_L(0)) = \exp[2iL\pi/D]$ holds. Then,

$$\sigma_L(0) = \left(\frac{1}{q}\right) \frac{1}{1 + (q-1)\exp[2iL\pi/D]}, \qquad \text{so that, for } 0 < L < D, \quad |\sigma_L(0)| > q^{-2} = |\sigma_0(0)|.$$

There exist a (complex) neighborhood $\mathcal{W}$ of $w = 0$ and a positive number $\theta < 1$ for which $|\sigma_0(w)| \le \theta|\sigma_L(w)|$, for any L, with $0 < L < D$. Furthermore, when $w = 0$, the residue of $T_{[\delta]}(z, w)$ at $z = \sigma_0(w)$ is the residue of $T(z)$ at $z = q^{-2}$. It is non zero, since q^{-2} is actually a simple pôle for T. Then, there exists a small neighborhood of $w = 0$ for which the residue of $T_{[\delta]}(z, w)$ at $z = \sigma_0(w)$ is non zero. Finally, $T_{[\delta]}(z, w)$ admits as dominant singularity an unique (simple) pôle at $z = \sigma_0(w)$, and

$$[z^n]T_{[\delta]}(z,w) = \left(\frac{1}{\sigma_0(w)}\right)^n \cdot V(w) \cdot [1 + O(\theta^n)],$$

with a non-zero analytic function $V(w)$ and a O–term uniform on $\mathcal{W}$. The quasi-powers theorem can be applied with $A(w) = -\log \sigma_0(w) + \log \sigma_0(0)$. Now, il we let $\Lambda(z) := \log G(q^{-2}e^{-z})$, the relation $\psi(\sigma_0(w), w) = 1$ which defines $\sigma_0(w)$ can be written as

$$\delta\Lambda(A(w)) + (1-\delta)\Lambda(A(w) - w) = 0.$$

Now, with two derivations, we obtain:

$$A'(0) = 1 - \delta, \qquad A''(0) = \delta(1-\delta)\frac{\Lambda''(0)}{|\Lambda'(0)|} = \frac{1}{q-1} \cdot \delta(1-\delta) > 0.$$

Remark. It is important to remark that, in the case when δ is not rational, the singularity q^{-2} is no longer a pôle. Consider the case where $z = q^{-2}$. Then

$$T(q^{-2}, w) := U(q^{-2}e^w) \sum_{p \ge 0} G(q^{-2}e^w)^{p - \lfloor \delta p \rfloor}$$

is a power series wrt $G(q^{-2}e^w)$ which possesses integer coefficients and is not a rational fraction. Then, we can apply a Theorem due to Polya:

Theorem C**.** [Polya] *If a power series with integer coefficients converges inside the unit disc, then the function it represents is either a rational function or a function that admits the unit circle as a natural boundary.*

This proves that $w \mapsto T(q^{-2}, w)$ admits as singularities all the points of the curve $\{w \in \mathcal{W};\ G(q^{-2}e^w) = 1\}$.

Now, at the end of this section, we study costs, for which we only expect results on moments, namely, additive costs of intermediate growth, end–costs and mixed costs.

3.7. **Additive costs of intermediate growth.** We recall that the series $T_C(z, w)$ relative to any additive cost C can be expressed as

$$T_C(z,w) = \frac{U(z)}{1 - G(z,w)},$$

where $G(z, w)$ is the bivariate series relative to cost c. Now, if c is of intermediate growth, the generating function $G(z, w)$ is no longer analytic at $w = 0$. However, it admits derivatives of any order, and it is the same for $T_C(z, w)$. The derivative of order k of $T_C(z, w)$ (wrt w, at $w = 0$), denoted by $T_C^{[k]}(z)$, will provide informations on the moment of order k of C, via the relation

$$\mathbb{E}[C_n^k] = \frac{[z^{n-1}]T_C^{[k]}(z)}{[z^{n-1}]T(z)}. \tag{35}$$

The first two series $T_C^{[k]}(z)$ (for $k = 1, 2$) are equal to

$$T_C^{[1]} = \frac{U \cdot G_{[c]}}{(1-G)^2}, \qquad T_C^{[2]} = \frac{U \cdot G_{[c^2]}}{(1-G)^2} + 2\,\frac{U \cdot G_{[c]}^2}{(1-G)^3}$$

where the "weighted" series $G_{[d]}$ relative to some cost d is defined as

$$G_{[d]}(z) = \sum_{m \in \mathcal{G}} d(m) \cdot z^{\deg m}.$$

Since c is of intermediate growth, the two series $G_{[c]}, G_{[c^2]}$ are analytic on a disk of center 0 and radius strictly larger than q^{-2}. The explicit expressions of G and U entail precise expressions for $T_C^{[k]}(z)$ (for $k = 1, 2$), namely

$$T_C^{[1]}(z) = G_{[c]}(z) \cdot \frac{(q-1)qz}{(1-q^2z)^2}, \qquad T_C^{[2]}(z) = G_{[c^2]}(z) \cdot \frac{(q-1)qz}{(1-q^2z)^2} + 2G_{[c]}^2(z) \cdot \frac{(q-1)qz(1-qz)}{(1-q^2z)^3},$$

which show that $T_C^{[1]}$ has a dominant pôle of order 2 at $z = q^{-2}$, $T_C^{[2]}$ has a dominant pôle of order 3 at $z = q^{-2}$. Then, with the Cauchy Formula,

$$[z^n]S_C^{[1]}(z) = q^{2n} \cdot \left[\frac{q-1}{q} \cdot G_{[c]}(q^{-2})\right] \cdot n + O(1),$$

$$[z^n]S_C^{[2]}(z) = q^{2n} \cdot \left[\frac{q-1}{q} G_{[c]}(q^{-2})\right]^2 \cdot n^2 + O(n).$$

Now, the equality $[z^n]T(z) = q^{2n}$ proves that the first two moments of C_n admit the following estimates

$$\mathbb{E}[C_n^i] = \left[\frac{q-1}{q} G_{[c]}(q^{-2})\right]^i \cdot n^i\,(1 + O(\frac{1}{n})).$$

This exhibits a cancellation in the dominant term of the variance, so that $\mathbb{V}[C_n] = \mathbb{E}[C_n^2] - \mathbb{E}[C_n]^2 = O(n)$. This proves the assertion (c) of Theorem 4 (P).

3.8. **End costs and mixed costs.** The end costs are all the costs of the form $O(\ell(m_p) + \ell(v_p))^k$ for some integer fixed k. If E denotes the end-cost defined by $E(u, v) = \ell(m_p) + \ell(v_p)$, it is sufficient to show that all the moments of E_n (of any order k) are $O(1)$. The bivariate generating function T_E of E, can be written, with additivity of cost E, and bijection (5) as

$$T_E(z, w) = U(z, w) \cdot \left(1 + \frac{G(z, w)}{1 - G(z)}\right).$$

Now, the k-th derivative of $T_E(z, w)$ [wrt w, at $w = 0$] is

$$T_E^{[k]}(z) = \frac{\partial^k}{\partial w^k} U(z, w)|_{w=0} + \frac{1}{1 - G(z)} \left(\frac{\partial^k}{\partial w^k}(UG)(z, w)\right)|_{w=0}.$$

Since the function $(UG)(z, w)$, and all its derivatives (wrt w, at $w = 0$), are analytic in a disk of center 0 and radius strictly larger than q^{-2}, the series $T_E^{[k]}(z)$ possess a unique dominant pôle at $z = q-2$, of order 1. Then, with the Cauchy Formula,

$$[z^n]T_E^{[k]}(z) = q^{2n} \cdot \frac{\partial^k}{\partial w^k}(UG)(\frac{1}{q^2}, 0) \cdot (1 + O(n^{-1})).$$

With (35) and relation $[z^n]T(z) = q^{2n}$, this proves the first part of assertion (d) of Theorem 4(P).

A mixed cost is a cost of the form $M^{(k)} = \ell(v_p)^k \cdot C$, where C is of intermediate growth. For studying costs M, we consider a tri-variate generating function

$$T_M(z, w, t) := \sum_{(u,v) \in \Omega} e^{t\ell(v_p)} \cdot e^{wC(u,v)} \cdot z^{\deg v}$$

which can be written as

$$T_M(z, w, t) = \frac{U(z, t)}{1 - G(z, w)},$$

and the derivative $\partial^{k+1}/\partial t^k \partial w$ of the series (at $t=0, w=0$), of the form

$$T_M^{[k]}(z) = U_t^{(k)}(z,0) \cdot G'_w(z,0) \cdot \frac{1}{1-G^2(z)}$$

gives access to the expectation of the cost $M^{(k)}$, Since the function $U(z,t)$, and all its derivatives (wrt t, at $t=0$), the functions $G(z,w), G'_w(z,w)$, are analytic in a disk of center 0 and radius strictly larger than q^{-2}, the series $T_M^{[k]}(z)$ possesses a pôle of order 2 . at $z=q-2$. Then, with the Cauchy Formula,

$$[z^n]T_M^{[k]}(z) = n \cdot q^{2n} \cdot U(k)_t(q^{-2},0) \cdot G'_w(q^{-2},0) \cdot (1+O(n^{-1})),$$

With (35) and relation $[z^n]T(z) = q^{2n}$, this proves the second part of assertion (d) of Theorem $4(P)$.

3.9. **Conclusion of the polynomial study.** This first analysis is now complete, since we have proven all the versions (P) of the main four theorems. We now consider the integer case.

4. The Euclid Algorithm on Integers. Algebraic study

We now perform the analysis of the Euclid algorithm on integers, and we wish to prove the four Theorems with their (I) version. We first decompose the bit-complexities cost, and show that these decompositions involve the costs which are studied in Theorem 4. Since the integer study is more involved, there are two sections devoted to the analysis in case (I). The present section introduces the main tool of the analysis: the transfer operator. Then, it performs an "algebraic" study: it provides, for each cost of interest, an alternative expression of the generating function which involves the transfer operator. These alternative expressions will be used in Section 5 for the analytical study.

4.1. **Continued fraction expansion.** Each division–step of the Euclid algorithm $v = m \cdot u + r$ uses a digit m and changes the old pair (u,v) into a new pair (r,u). Instead of integers, we consider rationals [the old rational $x = u/v$, and the new rational $y = r/u$] which both belong to the unit interval, and we look for a relation between y and x. One has

$$y = \frac{r}{u} = \frac{v-mu}{u} = \frac{v}{u} - \lfloor \frac{v}{u} \rfloor = \frac{1}{x} - \lfloor \frac{1}{x} \rfloor.$$

The map $T : \mathcal{I} \to \mathcal{I}$, defined as

$$T(x) = \frac{1}{x} - \lfloor \frac{1}{x} \rfloor \quad \text{for } x \neq 0, \qquad T(0) = 0, \tag{36}$$

is called the Gauss map and plays a fundamental rôle in the study of the Euclid Algorithm. When the quotient is m, there exists also a linear fractional transformation (LFT) $h_{[m]}$ for which

$$x = h_{[m]}(y) \qquad \text{with} \quad h_{[m]}(y) = \frac{1}{m+y} \ .$$

Of course, the LFT's $h_{[m]}$ are the inverse branches of T. On an input (u,v), the execution (3) creates a (unique) continued fraction of the form

$$\frac{u}{v} = \cfrac{1}{m_1 + \cfrac{1}{m_2 + \cfrac{1}{\ddots \cfrac{}{m_{p-1} + \cfrac{1}{m_p}}}}} = h_{[m_1]} \circ h_{[m_2]} \circ \dots h_{[m_p]} = h(0), \tag{37}$$

and the Euclid algorithm "writes" the result $u/v = h(0)$. We remark that the last step of the Euclid algorithm is particular, since the last digit m_p satisfies $m_p > 1$. Then, with the set $\mathcal{H}, \mathcal{F}$ defined as

$$\mathcal{H} = \{h_{[m]}, m \geq 1\}, \qquad \mathcal{F} = \{h_{[m]}, m \geq 2\}, \qquad \mathcal{U} := \{d \in \mathbb{N}; d \geq 1\}, \tag{38}$$

the Euclid Algorithm builds the bijection

$$\Omega \sim [\epsilon + \mathcal{H}^\star \times \mathcal{F}] \times \mathcal{U}. \tag{39}$$

In fact, any rational admits two $CFE's$, the first one, built by the Euclid Algorithm, is the proper one: its sequence of digits is $(m_1, m_2, \ldots, m_p)$ with $m_p \neq 1$. The second one is the improper one, of the form $(m_1, m_2, \ldots, m_p - 1, 1)$. We consider here these two $CFE's$ which generate together the whole set $\mathcal{H}^\star$, and we do not study exactly costs defined from the actual execution of the algorithm, but a "smoothed" version which takes into account the two possible "executions". Note that the sequences v_i and s_i are the same for these two executions, and the smoothed version $\widetilde{C}$ of an additive cost C is

$$2\widetilde{C}(u,v) := \left(\sum_{i=1}^{p} c(m_i)\right) + \left(\sum_{i=1}^{p-1} c(m_i)\right) + c(m_p - 1) + c(1).$$

For all the costs R which are studied here, of intermediate growth, Theorem 4 (c) proves that the end cost $\widetilde{R} - R$ is negligible. It is then sufficient to study the smoothed version, and we shall denote by S_R the Dirichlet series relative to this smoothed version $\widetilde{R}$. Dealing with these smoothed versions finally leads to the bijection

$$\Omega \sim \mathcal{H}^\star \times \mathcal{U}. \tag{40}$$

4.2. **Expression for continuants.** When the algorithm performs p iterations, it gives rise to a continued fraction of depth p. Here, we show that the main parameters of the Euclid Algorithm on the input (u, v) (quotients m_i, remainders v_i and continuants s_i) can be read on the continued fraction of the rational u/v. When the CFE of u/v is splitted at depth i, the LFT h defines three LFT's, the beginning LFT b_i, the middle LFT h_i and the ending LFT e_i, respectively defined as

$$b_i := h_{[m_1]} \circ h_{[m_2]} \circ \ldots \circ h_{[m_{i-1}]}, \qquad h_i := h_{[m_i]} \qquad e_i := h_{[m_{i+1}]} \circ \ldots \circ h_{[m_p]},$$

so that h decomposes as $h = b_i \circ e_{i-1} = b_i \circ h_i \circ e_i$. The continuant s_i (which intervenes in the extended gcd algorithm) is the denominator of the beginning rational $b_i(0)$, while the remainder v_i is related to the denominator w_i of the ending rational $e_i(0)$ via the equality $v_i = v_p \cdot w_i$. For any LFT h of the form

$$h(x) = (\alpha x + \beta)/(\gamma x + \delta) \qquad \text{with } \alpha, \beta, \gamma, \delta \text{ coprime integers}, \tag{41}$$

there exists a simple (but important) relation between the denominator $D[h]$ of the LFT h, defined by $D[h](x) := |\gamma x + \delta|$, and the derivative $h'(x)$, namely

$$|h'(x)| = \frac{|\det h|}{D[h](x)^2}.$$

Here, all the LFT's h used by the Euclid algorithm have their determinant that satisfy $|\det h| = 1$. Then, $v_0^{-2} = v_p^{-2} \cdot |h'(0)|$, and, more generally, the i-th continuants admit expressions which involve the beginning LFT e_i and the ending LFT b_i under the form

$$s_i^{-2} = |b_i'(0)|, \qquad v_i^{-2} = v_p^{-2} \cdot |e_i'(0)|. \tag{42}$$

We also deal with "approximate" versions w_i, t_i of parameters s_i, v_i,

$$w_i = v_i/v_p, \qquad t_i := |b_i'(e_i(0))^{-1/2}|.$$

Since any LFT h used by the Euclid Algorithm is of the form (41) with $0 < \gamma \leq \delta$, the relation $|h'(x)| \leq 4|h'(y)|$ holds, for all $x, y \in \mathcal{I}$, for any $h \in \mathcal{H}^\star$ and entails that any $d_i := \lg t_i - \lg s_i$ satisfies $0 \leq d_i \leq 1$.

4.3. **Decomposition of the bit-complexities.** We consider the two costs which involve these approximate parameters t_i, w_i,

$$A(u,v) := \sum_{i=1}^{p} \ell(m_i) \cdot \lg w_i, \qquad \bar{A}(u,v) := \sum_{i=1}^{p} \ell(m_i) \cdot \lg t_i,$$

via their logarithms instead of their integer size. These costs will be easily generated by our transfer operators [See Proposition 3, Section 3.11] and they are also closely related to our costs of interest, since Theorem 4 (c) entails the estimates

$$A \asymp_{(n^{-1})} B, \qquad A + \bar{A} \asymp_{(n^{-1})} D.$$

We now aim to obtain decompositions of costs B, D, in the same vein as in polynomial case. The present decompositions will be more involved than in the polynomial case. This is due to the fact that it is no longer possible to express the bit-complexities, with only the parameters $\ell(m_i)$. We then introduce new parameters, the cost

$$r = \lg v_p + \lg v_0 - \ell(v_0) \tag{43}$$

and the sequence θ_i, which we now define. Denote by x_i the rational v_{i+1}/v_i [which is equal to the rational w_{i+1}/w_i]. The relation $w_{i-1} = m_i \cdot w_i + w_{i+1}$ entails that, for any i, with $1 \leq i \leq p$,

$$\lg w_{i-1} - \lg w_i = \lg(m_i + x_i) = \ell(m_i) + \theta_i, \qquad \text{with} \quad \theta_i = \lg \frac{m_i + x_i}{\widetilde{m}_i}, \quad x_i := T^i(\frac{u}{v}), \tag{44}$$

and $\widetilde{m}_i$ the smallest power of two at least equal to m_i. Remark that θ_i satisfies $-1 \leq \theta_i \leq 1$. Relation (44) replaces the polynomial relation $\ell(v_{i-1}) - \ell(v_i) = \ell(m_i) - 1$, and, in the number case, the sequence θ_i plays a similar rôle as the constant sequence equal to -1 in the polynomial case. Then, for any $i, 0 \leq i \leq p-1$, one has

$$\lg w_i = \sum_{j=i+1}^{p} [\ell(m_j) + \theta_j], \tag{45}$$

and, with definition of r, the previous relation for $i = 0$ entails on Ω_n the decomposition:

$$\sum_{i=1}^{p} [\ell(m_i) + \theta_i] = \lg w_0 = n - r. \tag{46}$$

Then, on Ω_n, the cost A can be written as

$$A_n = \sum_{i=1}^{p} \big([\ell(m_i) + \theta_i] - \theta_i\big)\big(\sum_{j>i} [\ell(m_j) + \theta_j]\big) = \frac{1}{2}(n-r)^2 - \frac{1}{2}(n-r) - \sum_{i=1}^{p} \theta_i \lg w_i.$$

In the study of cost $A_n + \bar{A}_n$, the relation $\lg t_i + \lg(m_i + x_i) + \lg w_i = \lg w_0 = n - r$ holds and entails the equality $\lg s_i + \lg w_i + \ell(m_i) = n - r - \theta_i$. Then, the cost $A_n + \bar{A}_n$ can be written as

$$A(u,v) + \bar{A}(u,v) = \sum_{i=1}^{p} \ell(m_i)[n - r - \theta_i - \ell(m_i)] = n \cdot \sum_{i=1}^{p} \ell(m_i) - \sum_{i=1}^{p} \ell^2(m_i) - \sum_{i=1}^{p} \ell(m_i)(r + \theta_i).$$

We have now proven the first assertion of the following proposition.

Proposition 2 (I). *(a) On Ω_n, the approximate bit–complexity cost $A + \bar{A}$ of the Extended Euclidean Algorithm decomposes as*

$$\bar{A} + A = \left[n \cdot \sum_{i=1}^{p} \ell(m_i) \right] - \left[\sum_{i=1}^{p} \ell^2(m_i) \right] - \left[\sum_{i=1}^{p} \ell(m_i)(r + \theta_i) \right].$$

The approximate complexity A of the standard algorithm decomposes as

$$A = \left[\frac{1}{2}(n-r)^2 - \sum_{i=1}^{p} \theta_i \lg w_i \right] - \frac{1}{2}(n-r).$$

(b) With Theorem 4 (I), and Definition 2, the following holds on Ω_n,

$$D \asymp_{(n^{-1})} n \cdot L, \quad \text{with} \quad L = \sum_{i=1}^{p-1} \ell(m_i) \qquad\qquad B \asymp_{(n^{-1})} \frac{n^2}{2} - \underline{N}, \quad \text{with} \quad \underline{N} := \sum_{i=1}^{p} \theta_i \lg w_i.$$

Here $n \cdot L$ is asymptotically Gaussian with a characteristic triple $[O(n^2), O(n^3), O(n^{-1/2}]$, and conjecture ($G$) is related to the gaussian behaviour of N defined in (9).

(c) Furthermore, the cost Θ equal to the sum of the terms of the sequence θ_i satisfies

$$\Theta := \sum_{i=1}^{p} \theta_i, \qquad \Theta \asymp_{(n^{-2})} n - L,$$

and Θ is asymptotically gaussian with characteristic triple $[O(n), O(n), O(n^{-1/2})]$.

(d) The variances $\mathbb{V}[A_n]$ and $\mathbb{V}[\bar{A}_n]$ satisfy $\mathbb{V}[A_n] = \mathbb{V}[\bar{A}_n] + O(n^2)$.

Proof. The variables θ_i and d_i are bounded. The expectation of $\ell(v_p)$ is of order $O(1)$ from Theorem 4 (d). This is the same for variable r defined in (43). The expectation of $L \cdot \lg v_p$ is of order $O(n)$ from Theorem 4 (d). We conclude with Proposition 1. In the same vein, Assertion (c) uses Relation (46) and Proposition 1.
Finally, comparing the variances of A and $\bar{A}$ makes use of cost $\hat{A}$ defined by

$$\hat{A}(u,v) := \sum_{i=1}^{p} \ell(m_i) \cdot \lg s_i.$$

In fact, A and $\hat{A}$ are closely related via the mirror operation, which we now describe: To an element $h = h_1 \circ h_2 \circ \ldots \circ h_p$ of $\mathcal{H}^\star$, we associate its mirror $\hat{h}$, which is formed with the same elements as h, but in the inverse order. Then $h(0)$ and $\hat{h}(0)$ are rationals with the same denominator, and we denote by a hat the mirror operation which is induced on integer pairs. Now, the relation $\hat{A}(u,v) = A(\widehat{u,v})$ implies the equalities $\mathbb{E}[A_n] = \mathbb{E}[\hat{A}_n]$, $\mathbb{V}[A_n] = \mathbb{V}[\hat{A}_n]$.
On the other side, the variables $\bar{A}$ and $\hat{A}$ satisfy $\mathbb{V}[\bar{A}_n - \hat{A}_n] = O(n^2)$. If these variances are actually of order $\Theta(n^3)$, this implies that $\mathbb{V}[\bar{A}_n] = \mathbb{V}[A_n] \cdot (1 + O(n^{-1/2}))$. We will prove in the sequel that all these variances admit expansions which are polynomial with respect to n. And finally, provided that all the variances are of order exactly $\Theta(n^3)$, we deduce that the estimate $\mathbb{V}[A_n] = \mathbb{V}[\bar{A}_n] + O(n^2)$ holds. ■

4.4. **Plain bit-complexity : our conjectures.** Another expression of cost $\underline{N}$,

$$\underline{N} = \sum_{i=1}^{p} (\sum_{j<i} \theta_i) \cdot \lg(m_i + x_i),$$

exhibits the similarity of cost $\underline{N}$ with the cost N defined in (9) which has been studied in case (P): since the cost Θ is gaussian with the characteristic triple $[O(n), O(n), O(n^{-1/2})]$, the factor $(\sum_{j<i} \theta_i)$ in the previous sum is close to its mean, of order i. Then, a first step in order to prove that $\underline{N}$ is gaussian, is to prove that its smoothed versions, obtained when the sequence θ_i is replaced by a constant, namely

$$N^{(v)} = \sum_{i=1}^{p} \lg w_i, \qquad \hat{N}^{(v)} = \sum_{i=1}^{p} \lg v_i \qquad \text{or} \qquad N^{(m)} = \sum_{i=1}^{p} i \cdot \ell(m_i) \tag{47}$$

are asymptotically gaussian. Since Theorem 4 (c) implies that $\hat{N}^{(v)} \asymp_{(n-1)} N^{(v)}$, it is sufficient to study $N^{(v)}$ and $N^{(m)}$. We do not know how prove their (asymptotic) gaussian behaviours, but we have access to an alternative expression for the bivariate generating functions of these costs. Then, our first conjecture (G) is stated as follows:

Conjecture (G)**.** *The costs $N^{(v)}$ and $N^{(m)}$ are asymptotically gaussian.*

Even if this first conjecture is proven, it does not provide a precise estimate for the variance of our actual parameter $\hat{N}$. Our other conjecture (C) directly deals with the dominant constant of $\mathbb{V}[B_n]$ and aims to relate it with $\mathbb{V}[D_n]$. In the polynomial case, we know that $\mathbb{V}[B_n] = (1/3)\mathbb{V}[D_n]$, and we conjecture that the same holds in case (I). The parameter N is not easy to deal with, via our methods. However, as we already said, the costs A and $\bar{A}$ are easier to analyse. The relations

$$\mathbb{V}[B_n] = \mathbb{V}[A_n] + O(n^2), \qquad 2\mathbb{V}[A_n] + 2\mathbb{V}[\bar{A}_n] = 4\mathbb{V}[A_n] = \big(\mathbb{V}[D_n] + \mathbb{V}[A_n - \bar{A}_n]\big) + O(n^2),$$

entail the equality

$$12(\mathbb{V}[B_n] - \frac{1}{3}\mathbb{V}[D_n]) = \mathbb{V}[D_n] - 3\mathbb{V}[A_n - \bar{A}_n] + O(n^2).$$

This motivates our conjecture (C), equivalent to the assertion $\mathbb{V}[B_n] = (1/3)\mathbb{V}[D_n]$.

Conjecture (C)**.** *The variance $\mathbb{V}[A_n]$ is non zero and the two terms $3\mathbb{V}[A_n - \bar{A}_n]$ and $\mathbb{V}[D_n]$ have the same dominant terms of order n^3.*

We now study the main costs of interest. Remind that the bijection (5) is no longer use, since it does not properly deal with the integer size. We mainly use the bijection (40) $\Omega \sim \mathcal{H}^\star \times \mathcal{U}$ and explain how it is possible to generate the set $\mathcal{H}^\star$ with the help of transfer operators.

4.5. **Dynamical systems and transfer operator.** A continuous extension of one step of the Euclid algorithm to real numbers x of $\mathcal{I} := [0,1]$ is provided by the Gauss map $T : \mathcal{I} \to \mathcal{I}$, defined in (36). The pair $(\mathcal{I}, T)$ defines a dynamical system. The set $\mathcal{H}$ defined in (38) is just the set of branches of the inverse function T^{-1} that are also naturally numbered by the digit set $\mathcal{G}$. The set $\mathcal{H}^k$ is the set of the inverse branches of the iterate T^k, and the set $\mathcal{H}^\star := \cup_k \mathcal{H}^k$ is the semi-group generated by $\mathcal{H}$.

The main purpose in Dynamical Systems is the study of trajectories of a point x under the action of T. Here, we are interested in studying particular trajectories, relative to rational numbers x, which meet 0. A priori, they are not at all typical, but we aim to compare them to generic trajectories. The behaviour of generic trajectories of dynamical systems, is more easily explained by examining the flow of densities. The set $\mathcal{I}$ is endowed with some initial density $f = f_0$, and the time evolution governed by the map T modifies the density. The successive densities $f_1, f_2, \ldots, f_n, \ldots$ describe the global evolution of the system at time $t = 0, 1, 2, \ldots$. There exists an operator $\mathbf{G}$ for which $f_1 = \mathbf{G}[f_0]$, $f_2 = \mathbf{G}[f_1]$, and more generally $f_n = \mathbf{G}[f_{n-1}] = \mathbf{G}^n[f_0]$ for all n. This operator, called the density transformer, or the Perron-Frobenius operator, can be defined as

$$\mathbf{G}[f](x) = \sum_{h\in\mathcal{H}} |h'(x)| \cdot f\circ h(x) = \sum_{m\geq 1} \frac{1}{(m+x)^2} \cdot f(\frac{1}{m+x}), \tag{48}$$

and involves the set $\mathcal{H}$ defined in (38). It proves quite useful to add an extra parameter s in order to define the transfer operator $\mathbf{G}_s$ (or Ruelle operator [23]), already defined in (12)

$$\mathbf{G}_s[f](x) = \sum_{h\in\mathcal{H}} |h'(x)|^s \cdot f\circ h(x) = \sum_{m\geq 1} \frac{1}{(m+x)^{2s}} \cdot f(\frac{1}{m+x}). \tag{49}$$

Such an operator is well-defined for $\Re s > 1/2$ and acts on $\mathcal{C}^1(I)$. Note that the n-th iterate $\mathbf{G}_s^n$ of $\mathbf{G}_s$ has exactly the same form as $\mathbf{G}_s$, with a sum now taken over the set $\mathcal{H}^n$. The analog also holds for the quasi-inverse $(I-\mathbf{G}_s)^{-1}$, for which the sum is taken over $\mathcal{H}^\star$. Then, with transfer operator, we have at hand a dictionary which replaces the dictionary on (usual) generating functions. The operator $\mathbf{G}_s$ will play exactly the same rôle as $G(z)$ in Section 3 on polynomials. As in Section 3, we deal with modifications of $\mathbf{G}_s$, where we introduce another parameter w in order to mark our parameters of interest. These transfer operators will provide alternative expressions for the generating functions of interest.

As in Section 3, we begin with studying costs, for which we wish to establish an asymptotic gaussian law, namely

– additive costs of moderate growth (already proven in [2]) for Theorem 4 (a), also used for proving Theorem 1 (I),

– size of the remainder at a fraction of the execution, for Theorem 3 (I),

– parameters $N^{(v)}$ and $N^{(m)}$, in relation with Conjecture (G), useful for Theorem 2 (I).

We consider all the bivariate generating functions $S_R(s,w)$, defined in (21) and we aim expressing them with a convenient transfer operator, which depends also on these two parameters s and w.

4.6. **Additive costs.** Consider an additive cost C relative to a step-cost c. We first define the cost c on $\mathcal{H}$ by letting $c(h_{[m]}) := c(m)$, then we extend cost c on $\mathcal{H}^\star$ by additivity, by letting

$$\text{for} \quad h = h_1 \circ h_2 \circ \ldots \circ h_p, \qquad c(h) := \sum_{i=1}^{p} c(h_i).$$

Then, for any input (u,v) with a CFE of the form $u/v = h(0)$, the cost $C(u,v)$ equals $c(h)$. Consider the weighted transfer operator $\mathbf{G}_{s,w,[c]}$ relative to the digit cost c, already defined in (11),

$$\mathbf{G}_{s,w,[c]}[f](x) = \sum_{h\in\mathcal{H}} \exp[wc(h)] \cdot |h'(x)|^s \cdot f\circ h(x) \ = \sum_{m\geq 1} \exp[wc(m)] \cdot \frac{1}{(m+x)^{2s}} \cdot f(\frac{1}{m+x}). \tag{50}$$

Now, the n–th iterate of $\mathbf{G}_{s,w,[c]}$ has exactly the same expression as $\mathbf{G}_{s,w,[c]}$, with $\mathcal{H}$ replaced by its n–th power $\mathcal{H}^n$. And, the quasi–inverse of the operator, of the form

$$(I - \mathbf{G}_{s,w,[c]})^{-1}[f](x) = \sum_{h\in\mathcal{H}^\star} \exp[wc(h)] \cdot |h'(x)|^s \cdot f\circ h(x) \ ,$$

"generates" the bivariate generating function $S_C(s,w)$ of cost C (relative to coprime inputs). Furthermore, the Zeta function, defined as

$$\zeta(2s) := \sum_{d\geq 1} \frac{1}{d^{2s}},$$

allows to deal with general inputs [not only coprime inputs]. Finally, the complete formula for the series $S_C(s,w)$ is

$$S_C(s,w) = \zeta(2s)\cdot (I - \mathbf{G}_{s,w,[c]})^{-1}[1](0). \tag{51}$$

4.7. **Remainder at a fraction of the depth.** We first study the parameter $\widehat{L}^{[\delta]}$ which equals the logarithm of remainder v_i for $i = \lfloor \delta P \rfloor$, and we denote by $S_{[\delta]}(s,w)$ the bivariate generating function relative to the parameter $2\cdot \widetilde{L}^{[\delta]}$[3]. We will return to the parameter $L^{[\delta]}$ with Proposition 1 and relation $\widehat{L}^{[\delta]} = \widetilde{L}^{[\delta]} + O(1)$.
Consider an input (u,v) of Ω on which the algorithm performs p iterations. There exists a unique LFT h of depth p such that $u/v = h(0)$. We decompose h into two LFT's g and r of depth $\lfloor \delta p \rfloor$ and $p - \lfloor \delta p \rfloor$ such that $h = g\circ r$. With the relations

$$|(g\circ r)'(0)| = v_0^{-2}, \quad |r'(0)| = w_{\lfloor \delta p\rfloor}^{-2} = v_{\lfloor \delta p\rfloor}^{-2}\cdot v_p^2,$$

the general term of the series $S_{[\delta]}(s,w)$ decomposes as

$$\frac{v_{\lfloor \delta p\rfloor}^{2w}}{v_0^{2s}} = v_p^{2w}\cdot |r'(0)|^{-w}\cdot |(g\circ r)'(0)|^s = v_p^{2w}\cdot |r'(0)|^{s-w}\cdot |g'(r(0))|^s.$$

Now, when (u,v) varies in the set of coprime inputs of Ω with a given height p, we obtain

$$\sum_{\substack{(u,v)\in\Omega\\ P(u,v)=p,\,\gcd(u,v)=1}} \frac{v_{\lfloor \delta p\rfloor}^{2w}}{v_0^{2s}} = \mathbf{G}_{s-w}^{p-\lfloor \delta p\rfloor}\circ \mathbf{G}_s^{\lfloor \delta p\rfloor}[1](0), \tag{52}$$

and finally, with all depths, and general inputs [no longer only coprime],

$$S_{[\delta]}(s,w) = \zeta(2s-2w)\cdot \left(\sum_{p\geq 0} \mathbf{G}_{s-w}^{p-\lfloor \delta p\rfloor}\circ \mathbf{G}_s^{\lfloor \delta p\rfloor}\right)[1](0). \tag{53}$$

The central part of the previous formula defines the so–called pseudo–quasi-inverse $\mathbb{G}_{s,w}$, namely

$$\mathbb{G}_{s,w} := \sum_{p\geq 0} \mathbf{G}_{s-w}^{p-\lfloor \delta p\rfloor}\circ \mathbf{G}_s^{\lfloor \delta p\rfloor}. \tag{54}$$

Of course, since $\mathbf{G}_s$ and $\mathbf{G}_{s,w}$ do not commute, this is not a "true" quasi-inverse. However, we study this operator when w is near to 0, and we can hope that the properties of $\mathbb{G}_{s,w}$ will be close to properties of a true quasi-inverse.

4.8. **Costs N.** In case (I), the two parameters defined in (9) are no longer equal, and we consider two bivariate generating functions, $S_{(v)}(s,w)$ [for cost $N^{(v)}$] and $S_{(m)}(s,w)$ [for cost $N^{(m)}$]. We express these series with two operators $\mathbb{S}_{(v)}(s,w)$ and $\mathbb{S}_{(m)}(s,w)$ as

$$S_{(v)}(s,w) = \mathbb{S}_{(v)}(s,w)[1](0) \qquad S_{(m)}(s,w) = \mathbb{S}_{(m)}(s,w)[1](0).$$

With the same principles as previously, the two operators are defined as follows:

$$\mathbb{S}_{(v)}(s,w) = \zeta(2s)\cdot \big(I + \sum_{p\geq 1} \mathbf{G}_{s-pw}\circ \mathbf{G}_{s-(p-1)w}\circ \ldots \circ \mathbf{G}_{s-w}\big), \tag{55}$$

$$\mathbb{S}_{(m)}(s,w) = \zeta(2s)\cdot \big(I + \sum_{p\geq 1} \mathbf{G}_{s,pw}\circ \mathbf{G}_{s,(p-1)w}\circ \ldots \circ \mathbf{G}_{s,w}\big).$$

Here, the weighted operator $\mathbf{G}_{s,w} := \mathbf{G}_{s,w,[\ell]}$ is relative to the binary cost ℓ. Note that the first generating operator satisfies the functional equation

$$\mathbb{S}_{(v)}(s,w) = \zeta(2s)I + \mathbb{S}_{(v)}(s-w,w)\circ \mathbf{G}_{s-w}, \tag{56}$$

whereas a similar equation does not seem to hold for the second generating operator.

[3] the tilde notation refers to the smoothed cost defined in Section 4.1

In both cases, the operators look like quasi-inverses; however, there is is an important difference with our previous pseudo-quasi-inverse (54). Previously, the operator $\mathbb{G}_{s,w}$ can be viewed as a small perturbation of the quasi-inverse $(I-\mathbf{G}_s)^{-1}$, since for a small w, each term of $\mathbb{G}_{s,w}$ is close to the corresponding term of $(I-\mathbf{G}_s)^{-1}$. Here, this is no longer true, since the terms which define $\mathbb{S}(s,w)$ contain operators of the form $\mathbf{G}_{s-iw}$ where i tends to ∞.

We now study other costs R, for which we only expect results for the expectation and the variance. We then deal with univariate generating functions, denoted by $S_R^{[1]}(s)$ for the mean, and $S_R^{[2]}(s)$ for the moment of order 2. We wish to study
– end-costs and mixed costs for Theorem 4 (d),
– additive costs of intermediate growth for Theorem 4 (c),
– costs A, $\bar{A}$ for Theorem 2 (P), whose study is also crucial for Conjecture (C).

4.9. **Square brackets.** We now introduce an object which will be quite useful in the sequel. We first consider the set $\mathcal{T}\subset\mathcal{L}(\mathcal{C}^1(I))$ of operators $\mathbf{H}_s$ of the form

$$\mathbf{H}_s[f](x)=\sum_{m\geq 1}\frac{R_m(x)}{(m+x)^{2s}}\cdot f\left(\frac{1}{m+x}\right),\qquad \text{for } \Re s>1/2,$$

for which there exists a positive number k and a constant K, such that, for any m, one has $|R_m(x)|\leq K\cdot(\log m)^k$. Now, there are two operators which operate on the set $\mathcal{T}$: the derivation with respect to s, denoted by Δ [which multiplies each term $R_m(x)$ by the factor $-\log(m+x)$], and, for a cost c of intermediate growth, the weighting operator $W_{[c]}$ which weights each component R_m by the factor $c(m)$. Of course, our transfer operator $\mathbf{G}_s$ is an element of $\mathcal{T}$. Moreover, the weighted operator $\mathbf{G}_{s,w,[c]}$ (relative to any cost c of intermediate growth), together with its derivatives of any order with respect to s and w (at $w=0$) belongs to the set $\mathcal{T}$.

Definition 4. [Square brackets.] *Consider the algebra $\mathcal{A}$ generated by the operator Δ, and all the weighting operators $W_{[c]}$ relative to costs c of intermediate growth. Consider k elements of $\mathcal{A}$, denoted by $A_1,A_2,\ldots,A_k$. The square bracket $[A_1,A_2,\ldots,A_k](s)$ is the Dirichlet series equal to*

$$\zeta(2s)(I-\mathbf{G}_s)^{-1}\circ A_1\mathbf{G}_s\circ(I-\mathbf{G}_s)^{-1}\circ A_2\mathbf{G}_s\circ\ldots\circ A_k\mathbf{G}_s\circ(I-\mathbf{G}_s)^{-1}[1](0).$$

We now see some examples of the occurrence of this object.

4.10. **Additive costs C of intermediate growth. Mixed costs.** In this case, it will not be possible to deal directly with the transfer operator $\mathbf{G}_{s,w,[c]}$ as previously, since it is no longer analytic at $(1,0)$ [with respect to w]; however, when c is of intermediate growth, $\mathbf{G}_{s,w,[c]}$ admits derivatives at any order with respect to w, at $w=0$, and we work with univariate series $S_C^{[j]}(s)$ [defined in (23)] which admit alternative expressions of the form

$$S_C^{[1]}=[W_{[c]}],\qquad S_C^{[2]}=[W_{[c]}^2]+2[W_{[c]},W_{[c]}]. \tag{57}$$

For studying a mixed cost of the form $M^{(k)}=\ell(v_p)^k\cdot C$, where C is of intermediate growth, we consider the trivariate generating function

$$S_M(s,w,t):=\sum_{(u,v)\in\Omega}\frac{v_p^{2t}}{v^{2s}}\cdot\exp[wC(u,v)],$$

which is expressed with the tri-variate operator, as

$$S_M(s,w,t)=\zeta(2s-2t)\cdot(I-\mathbf{G}_{s,w,[c]})^{-1}[1](0).$$

Then, the derivative $\partial^{k+1}/\partial t^k\partial w$ of the series (at $t=0,w=0$), of the form

$$S_M^{[k]}(s)=\frac{\zeta^{(k)}(2s)}{\zeta(2s)}\cdot[W_{[c]}]$$

gives access to the expectation of the cost $M^{(k)}$.

4.11. **Conjecture** (C)**.** We now deal with conjecture (C), and we obtain a precise expression of the Dirichlet series $S^{[2]}_{A-\bar{A}}$. In this subsection, the reference to the cost c is omitted in W since c is always the binary length ℓ.

Proposition 3. *The part $\widetilde{S}^{[2]}_{A-\bar{A}}$ of the series $S^{[2]}_{A-\bar{A}}$ which only gathers all the square brackets of order at least 3 can be written as the sum of two series, $\Gamma_1(s)$ (which gathers all the square brackets of order 4), and $\Gamma_2(s)$ (which gathers all the square brackets of order 3), namely*

$$\Gamma_1(s) := [\Delta,\Delta,W,W] + [W,W,\Delta,\Delta] - [W,\Delta,\Delta,W] - [\Delta,W,W,\Delta],$$

and

$$2\Gamma_2(s) = [\Delta,\Delta,W^2] + [W^2,\Delta,\Delta] - [\Delta,W^2,\Delta] + [\Delta^2,W,W] + [W,W,\Delta^2] - [W,\Delta^2,W] +$$
$$+[\Delta,\Delta W,W] + [W,\Delta W,\Delta] - [\Delta,W,\Delta W] - [W,\Delta,\Delta W] - [\Delta W,\Delta,W] - [\Delta W,W,\Delta].$$

Proof. We begin with the moments of order 1, then we deal with the moments of order 2.

Moments of order 1. We first deal with the elementary costs $[\ell(m_i)\cdot w_i^{2w}]$, $[\ell(m_i)\cdot t_i^{2w}]$ for some (small) w. The corresponding Dirichlet generating functions are

$$\zeta(2s)\cdot\sum_{p\geq i}\mathbf{G}_{s-w}^{p-i}\circ\mathbf{G}_{s,[\ell]}\circ\mathbf{G}_s^{i-1}[1](0), \qquad \zeta(2s)\cdot\sum_{p\geq i}\mathbf{G}_s^{p-i}\circ\mathbf{G}_{s,[\ell]}\circ\mathbf{G}_{s-w}^{i-1}[1](0).$$

Now, the Dirichlet series $(2\log 2)S^{[1]}_A(s)$, $(2\log 2)S^{[1]}_{\bar{A}}(s)$, are just obtained with taking the sum over all the indices i between 1 and p, and taking the derivative with respect to w (at $w=0$). We obtain, after the first step [i.e., taking the sum over indices i]

$$\zeta(2s)\,(I-\mathbf{G}_{s-w})^{-1}\circ\mathbf{G}_s^{[\ell]}\circ(I-\mathbf{G}_s)^{-1}[1](0), \qquad \zeta(2s)\,(I-\mathbf{G}_s)^{-1}\circ\mathbf{G}_s^{[\ell]}\circ(I-\mathbf{G}_{s-w})^{-1}[1](0),$$

and, after the second step,

$$(2\log 2)\cdot S^{[1]}_A = [\Delta,W], \qquad (2\log 2)\cdot S^{[1]}_{\bar{A}} = [W,\Delta]. \tag{58}$$

Moments of order 2. For the three moments of order 2, namely $\mathbb{E}[A_n^2], \mathbb{E}[\bar{A}_n^2], \mathbb{E}[A_n\cdot\bar{A}_n]$, we first deal with the elementary cost $[\ell(m_i)\cdot\ell(m_j)\cdot u_i^{2w}\cdot {u_j}^{2t}]$, for $u_k\in\{w_k,t_k\}$ and fixed index i,j with $1\leq i,j\leq p$. There are two cases, $i=j$ and $i\neq j$. Then, we take the sum over all the pairs i,j with i,j between 1 and p and any possible p. We first obtain an alternative expression for the corresponding Dirichlet series (first step) and then, we take the derivative with respect to t,w, at $w=0, t=0$ (second step). We obtain the Dirichlet series with a multiplicative factor equal to $(2\log 2)^2$. Since we deal with the two main terms in the asymptotics, we do not need terms which involve only three quasi–inverses. The Dirichlet series which only takes into account square brackets of order at least 3 will be denoted with a tilde.

Cost A^2. We deal with the elementary cost $[\ell(m_i)\cdot\ell(m_j)\cdot w_i^{2w}\cdot {w_j}^{2t}]$, and we obtain for $j>i$

$$\sum_{p\geq j}\mathbf{G}_{s-w-t}^{p-j}\circ\mathbf{G}_{s-w}^{[\ell]}\circ\mathbf{G}_{s-w}^{j-i-1}\circ\mathbf{G}_s^{[\ell]}\circ\mathbf{G}_s^{i-1}[1](0),$$

and after the first step for any $i\neq j$,

$$2(I-\mathbf{G}_{s-w-t})^{-1}\circ\mathbf{G}_{s-w}^{[\ell]}\circ(I-\mathbf{G}_{s-w})^{-1}\circ\mathbf{G}_s^{[\ell]}\circ(I-\mathbf{G}_s)^{-1},$$

and finally after the second step

$$4[\Delta,\Delta,W,W] + 2[\Delta,W,\Delta,W] + 2[\Delta^2,W,W] + 2[\Delta,\Delta W,W].$$

Second, for $i=j$, the same ideas apply with the operator

$$(I-\mathbf{G}_{s-w})^{-1}\circ\mathbf{G}_s^{[\ell^2]}\circ(I-\mathbf{G}_s)^{-1}$$

and two successive derivations with respect to w (at $w=0$). This provides the term $2[\Delta,\Delta,W^2]$. Finally,

$$(2\log^2 2)\cdot\widetilde{S}^{[2]}_A = 2[\Delta,\Delta,W,W] + [\Delta,W,\Delta,W] + [\Delta^2,W,W] + [\Delta,\Delta W,W] + [\Delta,\Delta,W^2].$$

Cost $\bar{A}^2$. We deal with the elementary cost $[\ell(m_i)\cdot\ell(m_j)\cdot t_i^{2w}\cdot {t_j}^{2t}]$, and, for $j>i$, we obtain

$$\sum_{p\geq j}\mathbf{G}_s^{p-j}\circ\mathbf{G}_s^{[\ell]}\circ\mathbf{G}_{s-w}^{j-i-1}\circ\mathbf{G}_s^{[\ell]}\circ\mathbf{G}_{s-w-t}^{i-1}[1](\eta).$$

Then, we take the sum over all the pairs i,j with $i\neq j$ and i,j between 1 and p, and take the derivative with respect to t,w (at $w=0,t=0$). We obtain after the first step [for cost A^2]

$$2(I-\mathbf{G}_s)^{-1}\circ\mathbf{G}_s^{[\ell]}\circ(I-\mathbf{G}_{s-w})^{-1}\circ\mathbf{G}_{s-w}^{[\ell]}\circ(I-\mathbf{G}_{s-w-t})^{-1},$$

and, after the second step,

$$4[W,W,\Delta,\Delta]+2[W,\Delta,W,\Delta]+2[W,W,\Delta^2]+2[W,\Delta W,\Delta].$$

Second, for $i=j$, the same ideas apply with the operator

$$(I-\mathbf{G}_s)^{-1}\circ\mathbf{G}_s^{[\ell^2]}\circ(I-\mathbf{G}_{s-w})^{-1},$$

and two successive derivations with respect to w (at $w=0$). This provides the term $2[W^2,\Delta,\Delta]$. Finally, for cost $\bar{A}^2$,

$$(2\log^2 2)\cdot\widetilde{S}_{\bar{A}}^{[2]}=2[W,W,\Delta,\Delta]+[W,\Delta,W,\Delta]+[W,W,\Delta^2]+[W,\Delta W,\Delta]+[W^2,\Delta,\Delta].$$

Cost $A\bar{A}$. We deal with the elementary cost $[\ell(m_i)\cdot\ell(m_j)\cdot w_i^{2w}\cdot {t_j}^{2t}]$, and there are three different cases $j>i, j<i$ and $j=i$. For $j>i$, we obtain,

$$\sum_{p\geq j}\mathbf{G}_{s-w}^{p-i}\circ\mathbf{G}_{s-w}^{[\ell]}\circ\mathbf{G}_{s-w-t}^{j-i-1}\circ\mathbf{G}_{s-t}^{[\ell]}\circ\mathbf{G}_{s-t}^{j-1}[1](\eta),$$

and after the first step

$$(I-\mathbf{G}_{s-w})^{-1}\circ\mathbf{G}_{s-w}^{[\ell]}\circ(I-\mathbf{G}_{s-w-t})^{-1}\circ\mathbf{G}_{s-t}^{[\ell]}\circ(I-\mathbf{G}_{s-t})^{-1}[1](0).$$

For $j<i$, we obtain,

$$\sum_{p\geq i}\mathbf{G}_{s-w}^{p-i}\circ\mathbf{G}_s^{[\ell]}\circ\mathbf{G}_s^{i-j-1}\circ\mathbf{G}_s^{[\ell]}\circ\mathbf{G}_{s-t}^{i-1}[1](\eta),$$

and after the first step,

$$(I-\mathbf{G}_{s-w})^{-1}\circ\mathbf{G}_s^{[\ell]}\circ(I-\mathbf{G}_s)^{-1}\circ\mathbf{G}_s^{[\ell]}\circ(I-\mathbf{G}_{s-t})^{-1}[1](0).$$

Finally, for $i=j$, the same ideas apply with the operator

$$(I-\mathbf{G}_{s-w})^{-1}\circ\mathbf{G}_s^{[\ell^2]}\circ(I-\mathbf{G}_{s-t})^{-1},$$

and two successive derivations with respect to w and t (at $w=0,t=0$). This provides the term $[\Delta,W^2,\Delta]$. Finally, for cost $A\bar{A}$,

$$(4\log^2 2)\cdot\widetilde{S}_{A\bar{A}}^{[1]}=2[W,\Delta,\Delta,W]+2[\Delta,W,W,\Delta]+[W,\Delta,W,\Delta]+[\Delta,W,\Delta,W]+$$

$$+[W,\Delta^2,W]+[\Delta,W,\Delta W]+[W,\Delta,\Delta W]+[\Delta W,\Delta,W]+[\Delta W,W,\Delta]+[\Delta,W^2,\Delta].$$

With a combination of the three previous series, respectively relative to cost $A^2,\bar{A}^2,A\bar{A}$, we obtain the result. ■

4.12. **Conclusion of this section.** We have obtained an alternative expression for each generating function related to each cost of interest. Each expression involves a "generating operator".

5. The Euclid Algorithm on Integers. Analytic study.

With alternative expressions of Dirichlet series provided in the previous section at hand, it is now possible to perform the second step: we wish to find the dominant singularities of these Dirichlet series and their nature, and then transfer these informations towards coefficients and obtain asymptotic expressions for their coefficients.

5.1. **First spectral properties of the transfer operator.** As we previously saw, all the generating functions (bivariate or univariate) admit alternative expressions which involve the quasi–inverse [or the pseudo quasi–inverse] of a transfer operator (weighted or not). The dominant singularities of this type of operator (QI or PQI) and their nature are closely related to *spectral properties* of the plain operator, on a convenient functional space, which will be here $\mathcal{C}^1(\mathcal{I})$. When w is near 0, and for an elementary cost c, the transfer operator $\mathbf{G}_{s,w,[c]}$ is just a perturbation of the plain operator $\mathbf{G}_s$.

For $\Re(s) > 1/2$, the operator $\mathbf{G}_s$ acts on $\mathcal{C}^1(I)$ and the map $s \mapsto \mathbf{G}_s$ 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 unique 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 projection onto 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

$$\mathbf{G}_s = \lambda(s)\mathbf{P}_s + \mathbf{N}_s,$$

which extends to the powers of the operator

$$\mathbf{G}_s^n = \lambda^n(s)\mathbf{P}_s + \mathbf{N}_s^n, \tag{59}$$

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

$$(I - \mathbf{G}_s)^{-1} = \frac{\lambda(s)}{1 - \lambda(s)}\mathbf{P}_s + (\mathbf{I} - \mathbf{N}_s)^{-1}. \tag{60}$$

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 $\{\Re(s) \geq 1\}$. We further need a precise expression of the expansion of the quasi-inverse near $s = 1$.

Dominant spectral objects at $s = 1$. All the dominant spectral objects of $\mathbf{G}$ are explicit

$$\lambda(1) = 1, \qquad \mathbf{P}[f](x) = \varphi(x) \cdot \int_I f(t)dt, \qquad \text{with} \quad \varphi(x) = \frac{1}{\log 2}\frac{1}{1+x}. \tag{61}$$

Moreover at $s = 1$, the first two derivatives of $\Lambda(s) := \log \lambda(s)$ satisfy

$$B := -\Lambda'(1) > 0, \qquad A := \Lambda''(1) > 0. \tag{62}$$

Finally, the expansion of $(I - \mathbf{G}_s)^{-1}$ at $s = 1$, of the form

$$(I - \mathbf{G}_s)^{-1} = \frac{1}{s-1}\frac{\mathbf{P}}{|\lambda'(1)|} + \mathbf{Q} + O(s-1), \qquad \text{with} \quad \mathbf{Q} = \frac{\Delta\mathbf{P}}{|\lambda'(1)|} - \frac{\lambda''(1)\mathbf{P}}{2|\lambda'(1)|^2} + (I - \mathbf{N})^{-1}, \tag{63}$$

involves the so–called Porter Operator $\mathbf{Q}$, closely related to the Porter constant [see the book [13] for precisions on the Porter constant]. In particular, with (61, 63), for any operator $\mathbf{H} \in \mathcal{L}(\mathcal{C}^1(I))$, one has

$$(I - \mathbf{G}_s)^{-1} \circ \mathbf{H}[\varphi] \sim \frac{1}{s-1} \cdot \frac{1}{|\lambda'(1)|} \cdot \varphi \cdot I[\mathbf{H}], \qquad \text{with} \quad I[\mathbf{H}] := \int_I \mathbf{H}[\varphi](t)dt. \tag{64}$$

This proves:

Proposition 4. *Any Dirichlet series denoted by a square bracket of the form $[A_1, A_2, \dots A_k]$ [see Definition 3] has a pôle of order $k + 1$ at $s = 1$, and it admits an expansion of the form*

$$[A_1, A_2, \dots, A_k](s) = \sum_{p=0}^{k} \frac{a_{k-p}}{\log 2 \cdot |\lambda'(1)|^{p+1}} \cdot \frac{1}{(s-1)^{p+1}} + O(1) \qquad \textit{with} \quad a_0 = \prod_{i=1}^{k} I[A_i\mathbf{G}],$$

where $I[\cdot]$ is defined in (64) and φ is defined in (61).

Remark. Then, the dominant constant a_0 depends only on the subset $\{A_1, A_2, \dots A_k\}$ and does not depend on the order of the sequence $(A_1, A_2, \dots, A_k)$. This will entail a a cancellation in the variance.

5.2. **Various extractors.** We then wish to transfer these informations towards coefficients and obtain asymptotic expressions for these coefficients. We use, as a main tool, convenient "extractors" which express coefficients of series as a function of the series itself. There exist various "extractors", which will be chosen according to the informations that are expected for coefficients. There are three main cases, which are summarized as follows:

Case 1. [Average case analysis] We wish to obtain estimates for all the moments of order k, [obtained from coefficients of univariate series $S_R^{[i]}(s)$], with only the dominant term. This is useful here for proving Theorem 4 (c) : mean for costs of intermediate growth, and mixed costs.

Case 2. [Analysis of the variance] We wish to obtain dominant and subdominant terms for the moments of order 1 and 2 [obtained from coefficients of univariate series $S_R^{[i]}(s)$]. This is useful for the variance of costs of intermediate growth, and study of Conjecture C.

Case 3. [Distributional analysis] We wish to obtain gaussian normal law. Since we use the Quasi-Powers Theorem [see Theorem B, Section 2.6], we need expansions for coefficients of bivariate generating functions $S_R(s,w)$ which must be uniform wrt w. This is useful for proving Theorem 4 $(a),(b)$, and studying Conjecture (G).

For Case 1, Tauberian Theorems are used as our main extractor. When we wish to obtain remainder terms (or uniform terms), we then adopt the Perron Formula, and use it with some success, provided that we have a precise knowledge of the series –univariate series in case 2, or bivariate series in case 3.

5.3. **Study of case 1. Tauberian Theorems.** As we said, Tauberian Theorems [7, 25] are used when we only wish the dominant term of the estimates for the plain moments, as this is the case for mixed costs.

Theorem D**.** [Tauberian Theorem]. [Delange] *Let $F(s)$ be a Dirichlet series with non negative coefficients such that $F(s)$ converges for $\Re(s) > \sigma > 0$. Assume that*
(i) $F(s)$ is analytic on $\Re(s) = \sigma, s \neq \sigma$, and
(ii) for some $\gamma \geq 0$, one has $F(s) = A(s)(s-\sigma)^{-\gamma-1} + C(s)$, where A, C are analytic at σ, with $A(\sigma) \neq 0$.
Then, as $K \to \infty$,

$$\sum_{n \leq K} a_n = \frac{A(\sigma)}{\sigma \Gamma(\gamma+1)}\, K^\sigma \log^\gamma K \quad [1+\epsilon(K)\,], \quad \epsilon(K) \to 0.$$

This Theorem is easy to deal with. The generating function $S^{[k]}(s)$ of Section 4.10 gives access to the mean of cost $M^{(k)}$. The only property which has to be checked is the aperiodicity:

Aperiodicity. *The quasi-inverse $(I - \mathbf{G}_s)^{-1}$ is analytic on $\{\Re s = 1, s \neq 1\}$,*

which can be directly checked. Then Tauberian Theorem can be applied and proves that $\mathbb{E}[M_n^{(k)}]$ is of order $O(n)$.

5.4. **Study of cases 2 and 3. The Perron Formula and the US Properties.** We follow the same lines as described in the work [2]. We consider Dirichlet series, univariate or bivariate, and we wish to obtain estimates for the partial sums of their coefficients. More precisely, we let

$$F(s) := \sum_{n \geq 1} \frac{a_n}{n^{2s}} \qquad \text{or} \qquad F(s,w) := \sum_{n \geq 1} \frac{a_n(w)}{n^{2s}}$$

and we study

$$\Phi(p) = \sum_{n \leq p} a_p \qquad \text{or} \qquad \Phi_w(p) = \sum_{n \leq p} a_p(w). \tag{65}$$

For a Dirichlet series $F(s) = \sum_{n \geq 1} a_n n^{-2s}$, the Perron Formula of order two (see [10]) relates partial sums of the coefficients of F to the integral of F on a vertical line $\Re s = D > 0$ inside the convergence domain of F,

$$\Psi(T) := \sum_{N \leq T} \sum_{n \leq N} a_n = \frac{1}{2i\pi} \int_{D-i\infty}^{D+i\infty} F(s) \frac{T^{2s+1}}{s(2s+1)}\, ds\,. \tag{66}$$

Of course, when the Dirichlet series is of the form $F(s,w) = \sum_{n\geq 1} a_n(w) n^{-2s}$, the Perron formula relates $F(s,w)$ and the analog $\Psi_w(T)$ of $\Psi(T)$ [when a_n is replaced by $a_n(w)$].

There are now two main steps: first apply (with some success) the Perron Formula, then return to themain object of interest, which is not the functions Ψ of (66), but the functions Φ of (65). The second step is easier than the first step: The functions Ψ can be viewed as smoothed versions of functions Φ, and it is sufficient to use the same arguments as in Baladi–Vallée [2], corrected by Cesaratto [4]. We now concentrate on the first step, where we use the Perron Formula.

Univariate case. 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 following Property *US* [Uniform Estimates on Strips] holds for F near $s = 1$.

Property *US(s).* For any small ξ, there is $\alpha > 0$ for which the following is true:

- (i) $F(s)$ admits a unique pole in the strip $|\Re s - 1| \leq \alpha$.
- (ii) On the left vertical line $\Re s = 1 - \alpha$, the Dirichlet series $F(s)$ is $O(\max(1, |\Im s|^{\xi}))$, with a small ξ.

Bivariate case. We need uniform estimates when w is near 0, and it is natural to consider the following Property, which is a uniform perturbation of the previous one.

Property *US(s, w).* For any small ξ, there is $\alpha > 0$ and a neighborhood $\mathcal{W}$ of $w = 0$ for which the following is true:

- (i) $s \mapsto F(s,w)$ admits a unique pole $\sigma(w)$ in the strip $|\Re s - 1| \leq \alpha$.
- (ii) On the left vertical line $\Re s = 1 - \alpha$, the Dirichlet series $F(s)$ is $O(\max(1, |\Im s|^{\xi}))$, with a small ξ, and a O–term uniform wrt w.

Baladi and Vallée [2] have generalized ideas due to Dolgopyat [9] and prove that the *US* Properties hold for Dirichlet series relative to the quasi-inverses: Property $US(s)$ holds for the plain quasi-inverse $(I - \mathbf{G}_s)^{-1}$, and Property $US(s,w)$ holds for the quasi-inverse of the weighted operator $\mathbf{G}_{s,w,[c]}$ used for studying costs C of moderate growth [see Section 4.6]. For proving that Property *US* holds, the strip is split into two regions: a region near the real axis, where s is close to the pole $s = 1$ [or its perturbation $\sigma(w)$defined by relation $\lambda(\sigma(w), w) = 1$], and the region far from the real axis, where the powers of $\mathbf{G}_{s,w}$ are proven to satisfy

$$\exists M, \quad \exists \gamma < 1, \quad \forall n, \forall w \in \mathcal{W}, \quad ||\mathbf{G}^n_{s,w}||_{1,t} \leq M \cdot \gamma^n |t|^{\xi} \tag{67}$$

[here, $t := \Im s$ and the norm $||\cdot||_{1,t}$ is defined by $||f||_{1,t} = ||f||_0 + (1/t)||f||_1$].

In the sequel, we will extend this methodology in order to study

- the variance of a cost of intermediate growth, for proving Theorem 4 (c),
- the variance of the cost $A - \bar{A}$, for dealing with Conjecture (C),
- the moment generating function of cost $\hat{L}^{[\delta]}$, for proving Theorem 3,
- the moment generating function of cost $N^{(v)}$, for dealing with conjecture (G).

We begin with the variance studies, which are related to costs expressed with square brackets.

5.5. **Asymptotic estimates for coefficients of square brackets.** We are now ready to prove the following:

Proposition 5. *Consider any cost R for which the relative Dirichlet series $S_R(s)$ involves square brackets of the form $[A_1, A_2, \ldots, A_k]$. Then, each such square bracket contributes to the expectation $\mathbb{E}_n[R]$ with a term*

$$\mathbb{E}[R_n] = \left(\sum_{p=0}^{k} \frac{(2\log 2)^p}{p! |\lambda'(1)|^p} \cdot a_{k-p} n^p \right) \cdot [1 + O(2^{-n\beta})], \qquad \text{for some } \beta > 0.$$

Proof. We use Property *US*(s) for the quasi-inverse, namely (67) and we obtain for the square bracket $[A_1, A_2, \ldots, A_k]$ in the region far from the real axis,

$$|[A_1, A_2, \ldots, A_k]| \leq \left(\frac{1}{1-\gamma} \right)^{k+1} \cdot M^k \cdot \ |\Im s|^{(k+1)\xi} \cdot \prod_{i=1}^{k} ||A_i \mathbf{G}_s||_{1,t}.$$

so that $[A_1, A_2, \ldots, A_k]$ satisfies the Property *US* in this region.

For the region near the real axis, we use that the square bracket is meromorphic at $s = 1$. We fix α sufficiently small and we consider the strip $\mathcal{S}$ delimited by the vertical lines $|\Re(s)-1| < \alpha$. With $US(s)$, this strip contains 1 as a unique pole of $[A_1, A_2, \dots, A_k]$ (of order $k+1$). Consider now the rectangle $\mathcal{R}$ delimited by $\mathcal{S}$ and the two horizontal lines $|\Im(s)| = U$. With the Cauchy Theorem,

$$\frac{1}{2i\pi}\int_{\mathcal{R}} [A_1, A_2, \dots, A_k](s)\frac{T^{2s+1}}{s(2s+1)}ds = \frac{T^3}{3}\left(\sum_{k=0}^{p}\frac{a_{p-k}}{|\lambda'(1)^{k+1}\log 2}\frac{2^k}{k!}\log^k T\right).$$

We now let U tend to ∞. With Property $US(s)$, the left integral is $O(T^{3-2\alpha})$ and the right integral is exactly the integral of the Perron Formula.
Suppose that near $s = 1$, some generating function relative to some cost R is expressed with square brackets. This entails the following estimates for the partial sums $\Psi_R(T)$

$$\Psi_R(T) = \frac{T^3}{3}\left(\sum_{k=0}^{p}\frac{a_{p-k}}{|\lambda'(1)^{k+1}\log 2}\frac{2^k}{k!}\log^k T\right) + O(T^{3-2\alpha}).$$

Then, with the same principles as in Baladi-Vallée and Cesaratto, we obtain, after some steps of smoothing and de-smoothing, for some $\beta > 0$, the convenient expression for $\mathbb{E}[R_n]$. ■

Variance of costs of moderate growth. With relations (57), Proposition 5 entails the following estimates for $\mathbb{E}[C_n], \mathbb{E}[C_n^2]$,

$$\mathbb{E}[C_n] = I[W\mathbf{G}]\cdot\left(\frac{2\log 2}{|\lambda'(1)|}\right)n + O(1) \qquad \mathbb{E}[C_n^2] = 2\frac{1}{2}\cdot I[W\mathbf{G}]^2\cdot\left(\frac{2\log 2}{|\lambda'(1)|}\right)^2 n^2 + O(n).$$

The dominant term (of order n^2) is the same in $\mathbb{E}[C_n]^2$ and in $\mathbb{E}[C_n^2]$, which proves an estimate for $\mathbb{V}[C_n]$ of the form $\mathbb{V}[C_n] = O(n)$. This proves the "difficult" assertion of Theorem 4 (c).

Variance of $A - \bar{A}$. Proposition 5 entails the following estimates for $\mathbb{E}[A_n], \mathbb{E}[A_n^2]$,

$$(\log 2)\cdot\mathbb{E}[A_n] = \frac{1}{2}I[\Delta\mathbf{G}]\cdot I[W\mathbf{G}]\cdot\left(\frac{2^2}{2!}\cdot\frac{(\log 2)^2}{|\lambda'(1)|^2}\right)n^2 + O(n)$$

$$(\log^2 2)\cdot\mathbb{E}[A_n^2] = \frac{3}{2}I[\Delta\mathbf{G}]^2\cdot I[W\mathbf{G}]^2\cdot\left(\frac{2^4}{4!}\cdot\frac{(\log 2)^4}{|\lambda'(1)|^4}\right)n^4 + O(n^3).$$

We remark that the dominant term (of order n^4) is the same in $\mathbb{E}[A_n]^2$ and in $\mathbb{E}[A_n^2]$, which proves an estimate for $\mathbb{V}[A_n]$ of the form $\mathbb{V}[A_n] = \rho_0(\ell)\cdot n^3 + O(n^2)$. We recall the conjecture (C), about bit costs A and $\bar{A}$,

$$\mathbb{V}[A_n - \bar{A}_n] - \frac{1}{3}\mathbb{V}[A_n + \bar{A}_n] = O(n^2).$$

For proving conjecture (C), we need proving that $\rho_0(\ell) = (1/3)\rho(\ell)$, where $\rho(\ell)$ is the constants which occurs in the dominant term of the variance in Theorem 1(I). We show the following:

Proposition 6. *Denote by $\mathbf{Q}$ the Porter operator defined in (63). Then, Conjecture (C) holds if, for any $X, Y \in \{\Delta, W\}$, one has:*

$$I[X\mathbf{G}\circ\mathbf{Q}\circ Y\mathbf{G}] = \int_I (X\mathbf{G})[Y\varphi](t)dt - I[X\mathbf{G}]\int_I [Y\varphi](t)dt.$$

Proof. With Proposition 4, both series Γ_1 and Γ_2 of Proposition 3 have a pole of order at most four at $s = 1$ and can be written as

$$\Gamma_i(s) = \frac{1}{\log 2\cdot|\lambda'(1)|^4}\frac{1}{(s-1)^4}\gamma_i + O(\frac{1}{(s-1)^3}).$$

Explicit form of constants γ_i. The dominant coefficient γ_2 equals to

$$2\gamma_2 = \sum_{\substack{X,Y\in\{\Delta,W\}\\ X'\neq X, Y'\neq Y}} (-1)^{[X=Y]}\cdot I[X'\mathbf{G}]\cdot I[Y'\mathbf{G}]\cdot I[XY\mathbf{G}]$$

The dominant coefficient γ_1 is expressed with the subdominant terms in the expression of $\Gamma_1(s)$. At $s = 1$, the expansions of the three operators $(I-\mathbf{G}_s)^{-1}, \Delta\mathbf{G}_s, W\mathbf{G}_s$ respectively involve the Porter

operator $\mathbf{Q}$, already defined in (63), together with the operators $\Delta^2\mathbf{G}, \Delta W\mathbf{G}$, which intervene in the expansion of $\Delta\mathbf{G}_s$ and $W\mathbf{G}_s$ at $s = 1$,

$$\Delta\mathbf{G}_s = \Delta\mathbf{G} + (s-1)\Delta^2\mathbf{G} + O((s-1)^2) \qquad W\mathbf{G}_s = W\mathbf{G} + (s-1)\Delta W\mathbf{G} + O((s-1)^2).$$

The subdominant constant of the series Γ_1 is obtained when replacing, in each of the four terms of Γ, one of the nine places[4] (and only one) by its subdominant constant. However, all the terms obtained by replacing $\Delta\mathbf{G}_s$ or $W\mathbf{G}_s$ by their subdominant terms disappear. This is the same for terms which contain the operator $\mathbf{Q}$ at the beginning or at the end. Then, the subdominant constant γ_1 of Γ_1 is expressed via integrals of the form $I[\mathbf{H}]$ defined in (64) as a sum of four main terms, namely,

$$\gamma_1 = \sum_{\substack{X,Y\in\{\Delta,W\}\\ X'\neq X, Y'\neq Y}} (-1)^{[X=Y]} \cdot I[X\mathbf{G}] \cdot I[Y\mathbf{G}] \cdot I[X'\mathbf{G} \circ \mathbf{Q} \circ Y'\mathbf{G}].$$

Finally, the coefficient $\gamma := \gamma_1 + \gamma_2$ satisfies

$$2\gamma = \sum_{\substack{X,Y\in\{\Delta,W\}\\ X'\neq X, Y'\neq Y}} (-1)^{[X=Y]} \cdot I[X'\mathbf{G}] \cdot I[Y'\mathbf{G}] \cdot \left(I[XY\mathbf{G}] + I[X\mathbf{G} \circ \mathbf{Q} \circ Y\mathbf{G}]\right). \tag{68}$$

Then, Proposition 5 entails

$$\mathbb{E}_n[(A - \bar{A})^2] = \frac{2\log 2}{3|\lambda'(1)|^3} \cdot (2\gamma) \cdot n^3 + O(n^2).$$

Explicit form of constant $\rho(\ell)$. For Conjecture (C), we aim comparing the constant 2γ to the constant $\widetilde{\rho}(\ell)$ which appears in the variance of the extended binary cost,via the relation

$$\mathbb{V}[A_n + \bar{A}_n] = \frac{2\log 2}{|\lambda'(1)|^3} \cdot \widetilde{\rho}(\ell) \cdot n^3 + O(n^2).$$

An alternative expression for $\widetilde{\rho}(\ell)$ is obtained in Relation (14) of Theorem A,

$$\widetilde{\rho}(\ell) = \lambda'^2_s(1,0) \cdot \lambda''_{w^2}(1,0) - 2\lambda'_w(1,0) \cdot \lambda'_s(1,0) \cdot \lambda''_{sw}(1,0) + \lambda'^2_w(1,0) \cdot \lambda''_{s^2}(1,0)$$

We consider the weighted operator relative to the binary length cost ℓ , and we omit the reference to cost ℓ. We denote it by $\mathbf{G}_{s,w}$, its dominant eigenvalue by $\lambda(s,w)$, and its dominant eigenfunction by $\varphi(s,w)$. With taking derivatives of the relation $\mathbf{G}_{s,w}[\varphi_{s,w}] = \lambda_{s,w}\varphi_{s,w}$, with respect to s at $s = 1$ [Operation Δ] and wrt w at $w = 0$ [operation W], we obtain the following relations: with first derivatives,

$$I[X\mathbf{G}] = (X\lambda),$$

and with second derivatives,

$$I[XY\mathbf{G}] + \int_I (X\mathbf{G})[Y\varphi](t)dt + \int_I (Y\mathbf{G})[X\varphi](t)dt - I[X\mathbf{G}] \int_I [Y\varphi](t)dt - I[Y\mathbf{G}] \int_I [X\varphi](t)dt = (XY\lambda).$$

Finally the constant $\widetilde{\rho}(\ell)$ has exactly the same structure as γ, namely,

$$\widetilde{\rho}(\ell) = \sum_{\substack{X,Y\in\{\Delta,W\}\\ X'\neq X, Y'\neq Y}} (-1)^{[X=Y]} \cdot I[X'\mathbf{G}] \cdot I[Y'\mathbf{G}] \cdot \left(I[XY\mathbf{G}] + \int_I (X\mathbf{G})[Y\varphi](t)dt - I[X\mathbf{G}] \int_I [Y\varphi](t)dt\right). \tag{69}$$

Then, comparing equalities (69) and (68) proves Proposition 6. ■

We now deal with bivariate series, and we wish to exhibit gaussian laws.

[4]there are nine places in a square bracket of order 4: the four "written" places and the five "implicit" places, where the QI is omitted

5.6. **Gaussian law for $L^{[\delta]}$.** We follow the general lines described in Section 5.4. For the region far from the real axis, it is easy to obtain the estimate $US(s,w)$: using the relation (67), we obtain for the pseudo-quasi-inverse $\mathbb{G}_{s,w}$ defined in (54),

$$||\mathbb{G}_{s,w}||_{1,t} \leq M \cdot (\sum_p \gamma^p)\ |\Im s|^{2\xi},$$

so that $F(s,w) = \mathbb{G}_{s,w}[1](0)$ satisfies $US(s,w)$ on a region "far from" the real axis.
Near the real axis, the study is more intricate for the pseudo-quasi-inverse operator $\mathbb{G}_{s,w}$ than for the plain quasi-inverse. It is clear that $\mathbb{G}_{s,w}$ has a singularity at $(s,w) = (1,0)$. In order to obtain $US(s,w)$, it is then necessary to describe the behaviour of $\mathbb{G}_{s,w}$ when (s,w) is near $(1,0)$.
If (s,w) belongs to a (fixed) neighborhood $\mathcal{V}_1$ of $(1,0)$, the two values s and $s-w$ belong to the previous neighborhood $\mathcal{V}$ of $s=1$. Then, the two operators $\mathbf{G}_s, \mathbf{G}_{s-w}$ are quasi–compact, the dominant eigenvalue $\lambda(s), \lambda(s-w)$ of the operators $\mathbf{G}_s, \mathbf{G}_{s-w}$ are well–defined, and the spectral decomposition (59) of $\mathbf{G}_t$ applies to $t = s, t = s-w$ and extends to the operator $\mathbb{G}_{s,w}$ which decomposes into a sum of four terms, a "dominant" term and three "remainder" terms.

Remainder terms. Each of the three remainder terms is obtained by replacing in the operator $\mathbb{G}_{s,w}$, and for at least one value of $t = s$ or $t = s-w$, the iterates $\mathbf{G}_t^k$ by the corresponding powers of the operator $\mathbf{G}_t$, the other terms being (possibly) replaced by the corresponding term of the dominant operator $\lambda(t) \cdot \mathbf{P}_t$ or $\mathbf{N}_t$. One obtains three operators: one operator which contains only operators of type $\mathbf{N}$, and two operators with exactly one occurrence of type $\mathbf{P}$.
Denote by $\nu(t)$ the spectral radius of the operator $\mathbf{N}_t$, and by $R := \log \nu$. There exists a neighborhood such that $\nu(s)$ and $\nu(s-w)$ are strictly less than some $a < 1$. Then, the series with only operators of type $\mathbf{N}$ is absolutely convergent. Consider now the other two series, whose norms can be easily compared to a geometric sum, whose logarithm of the general term is

$$\delta R(s) + (1-\delta)\Re\Lambda(s-w), \qquad \delta\Re\Lambda(s) + (1-\delta)R(s-w). \tag{70}$$

We now prove that these terms are strictly negative on a neighborhood of $(s,w) = (1,0)$ of the form $|s-1| + |w| < \rho$. First, there exists a complex neighborhood $\mathcal{V}$ of $\tau = 1$ for which

$$R(\tau) < (1/2)R(1) < 0, \quad |\Lambda'(\tau)| \leq 2B,$$

with B defined in (62). Then one has

$$\max(|\Lambda(s)|, |\Lambda(s-w)|) \leq (|s-1| + |w|)\, 2B\rho,$$

and, finally, if $\beta := \inf(\delta, 1-\delta)$, and if $\rho \leq \beta \cdot |R(1)|/(8B)$, both terms in (70) are less than $\beta R(1)/8 < 0$. Finally, for (s,w) near (1, 0), the norm of the remainder operator is bounded by $(1 - \exp[\beta R(1)/8])^{-1}$

The dominant term. The dominant term is obtained when replacing each occurrence of $\mathbf{G}_t$ by the term $\lambda(t)\mathbf{P}_t$, and is of the form $F(s,w) \cdot [\mathbf{P}_{s-w} \circ \mathbf{P}_s[1](0)]$, with

$$F(s,w) = \sum_{p=0}^{+\infty} \lambda(s)^{\lfloor \delta p \rfloor} \cdot \lambda(s-w)^{p - \lfloor \delta p \rfloor}.$$

The properties of $F(s,w)$ will heavily depend on the nature of δ [rational versus irrational]. If δ is rational, the function $F(s,w)$ is a rational fraction wrt two variables $\lambda(s-w)$ and $\lambda(s)$. More precisely, if δ is of the form c/D, with $d = D - c$, one has

$$F(s,w) = \left(\sum_{j=0}^{D-1} \lambda(s-w)^{j - \lfloor \delta j \rfloor} \cdot \lambda(s)^{\lfloor \delta j \rfloor} \right) \left(\sum_{k \geq 0} (\lambda^d(s-w)\lambda^c(s))^k \right).$$

Then, if we let $\psi(s,w) := \lambda(s-w)^{1-\delta}\lambda(s)^{\delta}$, $F(s,w)$ can be written as

$$F(s,w) = \frac{P(s,w)}{1 - \psi(s,w)^D} \qquad \text{with} \quad P(s,w) := \sum_{j=0}^{D-1} \lambda(s-w)^{j - \lfloor \delta j \rfloor} \lambda(s)^{\lfloor \delta j \rfloor}.$$

It is then essential to study the function $\psi(s,w)$. The denominator $s \to 1 - \psi(s,w)^D$ admits as zeroes all the values of s for which

$$\psi(s,w) = \exp[2iL\pi/D] \qquad \text{with } 0 \leq L < D.$$

This means that the function Ψ defined as $\Psi := \log \psi$ satisfies

$$\Psi(s,w) := (1-\delta)\Lambda(s-w) + \delta\Lambda(s) = \frac{2iL\pi}{D}, \qquad \text{avec} \quad L \in \mathbb{Z}.$$

For $w = 0$, one has $\Psi(s,w) = \Lambda(s) = 2iL\pi/D$. Then, for w close to 0, the pôles of $F(s,w)$ are near to the curve $\mathcal{R} := \{s; \Re\Lambda(s) = 0\}$. We now describe this curve $\mathcal{R}$: the expansion of $\Lambda(s)$ near $s = 1$, involves the first derivatives A and B defined in (62) under the form

$$\Lambda(s) = -B(s-1) + A\cdot(s-1)^2 + O(|s-1|^3). \tag{71}$$

This entails that for s close enough to 1, with $s = \rho + it$,

$$\Re\Lambda(s) \sim -B(\rho-1) - At^2, \qquad \Im\Lambda(s) \sim -Bt.$$

Then, the curve $\mathcal{R}$ is close to the curve of equation $B(\rho-1) + At^2 = 0$ and is contained in the right plane $\Re s \leq 1$.

Consider two parts of this curve $\mathcal{R}$. The first part,

$$\mathcal{A} := \{s; \quad \Re\Lambda(s) = 0, \quad |\Im\Lambda(s)| > \frac{3\pi}{2D}\}$$

is strictly contained inside the right plane $\{\Re s < 1 - 4\Delta\}$ for some $\Delta > 0$. By a small perturbation, there exists a neighborhood $\mathcal{W}_A$ of $w = 0$ for which the domain

$$\mathcal{A}_w := \{s; \quad |\Re\Psi(s,w)| \leq \frac{C}{D^2}, \quad |\Im\Psi(s,w)| > \frac{3\pi}{2D}\} \tag{72}$$

is strictly contained inside the right plane $\{\Re s < 1 - 3\Delta\}$, for any $w \in \mathcal{W}_A$.
The second part of the curve is the portion of the curve

$$\mathcal{B} := \{s; \quad \Re\Lambda(s) = 0, \quad |\Im\Lambda(s)| < \frac{\pi}{2D}\},$$

which is contained in the strip $|\Re s - 1| < d$ for some d. By a small perturbation, there exists a neighborhood $\mathcal{W}_B$ of $w = 0$ for which the domain

$$\mathcal{B}_w := \{s; \quad |\Re\Psi(s,w)| \leq \frac{C}{D^2}, \quad |\Im\Psi(s,w)| < \frac{\pi}{2D}\} \tag{73}$$

is strictly contained in the strip $|\Re s - 1| < 2d\}$, for any $w \in \mathcal{W}_B$.

Property $US(s,w)$ for $F(s,w)$. The expansion in (71) entails that $3\Delta > 2d$. We choose $\alpha \in]2d, 3\Delta[$ and we prove that the property $US(s,w)$ holds in the strip $|\Re s - 1| < \alpha$ for $w \in \mathcal{W}_A \cap \mathcal{W}_B$.
First, from (72), the only possible pôle of $F(s,w)$ in the strip $|\Re s - 1| < 3\Delta$ is the pôle $s = \sigma_0(w)$. Since the strip $|\Re s - 1| < \alpha$ is contained in $|\Re s - 1| < 3\Delta$, the only possible pôle of $F(s,w)$ in the strip $|\Re s - 1| < \alpha$ is the pôle $s = \sigma_0(w)$. We prove now that $s = \sigma_0(w)$ is actually a pôle for $F(s,w)$. We now omit the index 0 in σ_0. The numerator $P(\sigma(w), w)$ satisfies at $w = 0$ the relation $P(\sigma(w), w) = P(1,0) = D$. Then, there exists a neighborhood of $w = 0$ for which $P(\sigma(w), w)$ is not zero. Moreover, at $w = 0$, the derivative $\Psi'(\rho(w), w)$ equals $\Psi'(1,0) = \Lambda'(1) \neq 0$. Then , for w close enough to 0, the derivative $\Psi'(\rho(w), w)$ is non zero.
Second, with (72) and (73), there are only two possibilities on the line $\Re s = 1 - \alpha$, namely,

$$|\Re\Psi(s,w)| > \frac{C}{D^2} \qquad \text{or} \qquad \frac{\pi}{2D} \leq |\Im\Psi(s,w)| \leq \frac{3\pi}{2D}.$$

This entails that the denominator $1 - \psi(s,w)^D$ of $F(s,w)$ admits a lower bound, either

$$|\psi(s,w)^D - 1| \geq \exp[C/D] - 1 \geq C/D \qquad \text{or} \quad |\psi(s,w)^D - 1| \geq 1.$$

On the other hand, since the numerator $P(s,w)$ satisfies

$$|P(s,w)| \leq \sum_{j=0}^{D-1} |\lambda(s-w)|^{j-\lfloor \delta j \rfloor} \cdot |\lambda(s)|^{\lfloor \delta j \rfloor},$$

it is (uniformly) bounded. Finally, on the line $\Re s = 1 - \alpha$, the dominant term admits a uniform bound wrt w.

End of the proof of Theorem 3. We end the proof with the same principles as described in 5.4. We then obtain a uniform estimate for the moment generating function of $\hat{L}^{[\delta]}$

$$\mathbb{E}[\exp(2w\hat{L}_n^{[\delta]})] = \exp[nA(w) + B(w)] \cdot [1 + O(2^{-n\gamma})].$$

Here $A(w) = -\sigma_0(w) + \sigma_0(0)$ is defined by the implicit equation $\psi(\sigma_0(w), w) = 1$. The expression of $\sigma_0(w)$ is then given by

$$\delta\Lambda(\sigma_0(w)) + (1-\delta)\Lambda(\sigma_0(w) - w) = 0.$$

With two derivations, the dominant coefficients of the mean and the variance are obtained. With the Quasi-Powers Theorem, the speed of convergence is $O(n^{-1/2})$. We have obtained an asymptotic gaussian law for the parameter $\hat{L}^{[\delta]}$ which is the logarithm of the remainder at the fraction δ of the execution. The algorithmic parameter of interest is the size of the remainder. As we already said it in Section 4.7, the relation $L^{[\delta]} = \hat{L}^{[\delta]} + O(1)$, together with Proposition 1 entails Theorem 3.

Remark. In the case when δ is not rational, the property $US(s, w)$ does not hold for $F(s, w)$. See remarks for the polynomial case at the end of 3.6.

5.7. **About the conjecture** (G)**.** The cost of interest is the cost $N^{(v)}$ defined in (47), whose bivariate generating function is $S_{(v)}(s, w) = \mathbb{S}_{(v)}(s, w)[1](0]$, where the operator $\mathbb{S}_{(v)}(s, w)$ satisfies

$$\mathbb{S}_{(v)}(s, w) = \zeta(2s) \cdot \big(I + \sum_{p\geq 1} \mathbf{G}_{s-pw} \circ \mathbf{G}_{s-(p-1)w} \circ \ldots \circ \mathbf{G}_{s-w}\big).$$

There exists a functional equation satisfied by $\mathbb{S}_{(v)}(s, w)$,

$$\mathbb{S}_{(v)}(s, w) = \zeta(2s)I + \mathbb{S}_{(v)}(s - w, w) \circ \mathbf{G}_{s-w}.$$

Comparing to the polynomial case shows that we loose many properties in the integer case. Since operators do not commute, it is no longer possible to obtain an exact expression as in (31). We perhaps may obtain informations on $S(s, w)$ when s is near 1, directly with the functional equation. However, even if we succeed in this first task, we do not see how to prove that the Property $US(s, w)$ holds for $S(s, w)$.

6. A common framework for polynomials and integers.

Our analyses are now complete. Even these analyses were led in a sequential form –polynomials, then integers–, there is clearly a close connection between them, and we have tried to insist on these similarities by using "parallel" notations. This section aims to now describe our analyses in parallel, then provides a common framework, which will also explains the differences and the difficulties of the integer study.

6.1. **Similarities.** The similarities are obvious, since this is the *same* algorithm! The bijection (5) is the same[5], and the decompositions of Proposition 2 (P) and Proposition 2 (I) quite similar. There is a clear analogy between the generating function $G(z)$, and its bivariate extensions, on the one hand, and the operator $\mathbf{G}_s$, and its bivariate extension on the other hand.
The reader must compare

– For additive costs of moderate growth: Relations (27) of Section 3.3 and (51) of Section 4.6.

– For the size of remainders at a fraction of the excution: Relations (33) of Section 3.6 and (53) of Section 4.7

– For the cost N, the same functional equation in (32) of Section 3.5 and in (56) of Section 4.8.

However, even if these objects are similar, they are not the same. In the integer case, we need a dynamical system and a transfer operator, which are of no use in the polynomial case... Of no use, is it true?

6.2. **The polynomial dynamical system.** We recall that the gcd algorithm on $\mathbf{F}_q[X]$ is based on the Euclidean division: on a pair (u, v) of polynomials with $\deg v > \deg u$,

$$v = m \cdot u + r, \qquad \text{with } r = 0 \text{ or } \deg r < \deg u.$$

As we did it in Sections 4.1 and 4.5 in case (I), it is possible to define a continuous extension of this division. This construction is due to Artin. The analogue of the ring $\mathbb{Z}$ is the ring $\mathbf{F}_q[Z]$ of polynomials, and the field $\mathbf{F}_q(Z)$ (the field of rational fractions) plays the same rôle as the field $\mathbb{Q}$ of rational numbers. We work on the completion of $\mathbf{F}_q[Z]$ with respect to the (ultrametric) absolute

[5]forget the particularities of the last step in case(I)!

value $||.||$ defined as $||u|| := q^{\deg u}$: this is the field of Laurent formal power series $\mathbf{F}_q((1/Z))$ where each element f has a Hensel expansion

$$f = \sum_{n \geq n_0} f_n \, (1/Z)^n, \quad \text{with } f_n \in \mathbf{F}_q \text{ and } n_0 \in \mathbb{Z}. \tag{74}$$

This expansion is parallel to the binary expansion of a real [replace Z by 2]. From the Hensel expansion (74), it is possible to define the function integer part, denoted by $\lfloor . \rfloor$, and the function fractional part, denoted with $\{.\}$, with

$$\lfloor f \rfloor := \sum_{n=n_0}^{0} f_n \, (1/Z)^n \qquad \{f\} := \sum_{n \geq 1} f_n \, (1/Z)^n.$$

The analog of the unit interval $[0, 1]$ is the unit open ball $\mathcal{X}_q$ of $\mathbf{F}_q((1/Z))$, which is also the set of elements with zero integer part. The shift $T : \mathcal{X}_q \to \mathcal{X}_q$ is defined by

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

The set $\mathcal{G}$ of possible quotients is

$$\mathcal{G} := \{m \in \mathbf{F}_q[Z]; \quad ||m|| \geq 1\} = \{m \in \mathbf{F}_q[Z]; \quad \deg m > 0\},$$

and the set of the inverse branches of T is just the set

$$\mathcal{H} := \{h_{[m]} : x \mapsto \frac{1}{m + x}; \quad m \in \mathcal{G}\}.$$

This dynamical systems is precisely described for instance in [3].

This dynamical system possesses very particular properties. The density transformer, and its extension the transfer operator, are defined as usual as

$$\mathbf{G}_s[f](x) = \sum_{m \in \mathcal{G}} \frac{1}{||m + x||^{2s}} \cdot f\left(\frac{1}{m + x}\right),$$

and acts on $\mathcal{C}^1(\mathcal{X}_q)$. Thanks to the ultrametric topology on $\mathcal{X}_q$, the absolute value $||m + x||$ is constant on $\mathcal{X}_q$ and equals to $||m||$. Then, the operator $\mathbf{G}_s$ is equal to

$$\mathbf{G}_s[f](x) = \sum_{m \in \mathcal{G}} \frac{1}{||m||^{2s}} \cdot f\left(\frac{1}{m + x}\right).$$

When applied to the uniform density $f_0 = 1$, the transfer operator $\mathbf{G}_s$ transforms it into a constant function

$$\mathbf{G}_s[1] = \sum_{m \in \mathcal{G}} \frac{1}{||m||^{2s}} = \sum_{m \in \mathcal{D}} \frac{1}{q^{2s \deg m}}.$$

This means that the complex number $\mathbf{G}_s[1]$ is the eigenvalue relative to the eigenfunction equal to 1. On a convenient functional space, this is the dominant eigenvalue. This number $\mathbf{G}_s[1]$ is also a Dirichlet series, but this is also a power series wrt $z = q^{-2s}$. With this change of variables, it coincides with the (usual) generating function $G(z)$ of the set $\mathcal{G}$, which gathers all the non constant polynomials of $\mathbf{F}_q(Z)$,

$$\mathbf{G}_s[1] = G(z) = \sum_{m \in \mathcal{G}} z^{\deg m} = (q-1) \sum_{n \geq 1} q^n z^n = \frac{q(q-1)z}{1 - qz} = \frac{(q-1)}{q^{2s-1} - 1}.$$

This allows a better understanding of the relation between the operator $\mathbf{G}_s$ and the generating function $G(z)$. But, it is not yet clear why it is possible to replace the polynomial transfer operator by its dominant eigenvalue. This is due to the fact that the branches of the polynomial dynamical system are affine, namely, the (ultrametric) norm of their derivatives is constant.
For a dynamical system with affine branches, the transfer operator admits 1 as an eigenfunction, for any value of parameter s. This will be also the case for any weighted transfer operator. Then, Section 3 is completely useless. We could have chosen to perform only one analysis, common to case (P) and (I). Section 4 provides all the results of Section 3: we forget the $\circ$ of composition, the last function 1, and the last point 0. This allows to transform a non commutative framework

into a commutative one. Then, we perform the change of variables $z := q^{-2s}$. We obtain in this way all the expressions of the generating functions of Section 3 with this syntactic transformation.

6.3. **Analytical differences.** Then, there is a common framework, given by the underlying dynamical system, and it would be possible to eliminate the algebraic part of Section 3, with a rewriting of Section 4. However, the analytic part of Section 3 is not a rewriting of Section 5: The analytical studies are very different, in the sense that the analytical study in case (P) is much more easier. The change of variables $z := q^{-2s}$ transforms (unbounded) vertical strips into compact crowns. For instance, the property equivalent to the US Property is very often much more easier to check in the power series. This explains why the Riemann Hypothesis is proven in $\mathbb{F}_q[X]$ (and not yet for numbers...)
Finally, the explanation of the difference is simple: there are no carries for polynomials, then the degree (quite close to the size) is an additive morphism wrt to the multiplication. This gives rise to an ultrametric topology, where it is possible to work with power series.
The existence of carries for integer leads to the usual topology, and it is no longer possible to use power series. Dirichlet series are then used, but, at the same time, the branches of the dynamical systems are no longer affine for the usual topology. This leads to a dynamical system with memory, for which the transfer operator cannot be reduced to its dominant eigenvalue.

References

[1] Akhavi, A., Vallée, B. Average bit–complexity of Euclidean Algorithms, Proceedings of ICALP'2000, Lecture Notes in Computer Science 1853, pp 373–387, Springer.
[2] Baladi, V., and Vallée, B., Euclidean Algorithms are Gaussian, Journal of Number Theory, Volume 110, Issue 2 (2005) pp 331–386
[3] Berthé, V. and Nakada, H. On Continued Fraction Expansions in Positive Characteristic: Equivalence Relations and some metric properties. *Expositiones Mathematicae* 18 (2000) pp 257–284.
[4] Cesaratto, E. Remarks and extensions on the paper "Euclidean Algorithms are gaussian" by V. Baladi and B. Vallée, personal communication.
[5] Daireaux, B. and Vallée, B. Dynamical analysis of the parameterized Lehmer-Euclid Algorithm, Combinatorics, Probability, Computing, pp 499–536 (2004).
[6] Daireaux, B, Lhote, L, Maume-Deschamps, V. and Vallée, B. Analysis of fast versions of the Euclid Algorithm, see web page: `www.info.unicaen.fr/~brigitte`
[7] Delange, H. Généralisation du Théorème d'Ikehara, *Ann. Sc. ENS, (1954) 71, pp 213–242.*
[8] Dixon, J. D. The number of steps in the Euclidean algorithm, *Journal of Number Theory 2* (1970), 414–422.
[9] Dolgopyat, D., On decay of correlations in Anosov flows, *Ann. of Math.* 147 (1998) 357–390.
[10] Ellison, W. and Ellison, F. *Prime Numbers,* Hermann, Paris, 1985.
[11] Flajolet, P. Notes de DEA, personal communication
[12] Flajolet, P. and Sedgewick, R. Analytic Combinatorics, Book in preparation (1999), see also INRIA Research Reports 1888, 2026, 2376, 2956.
[13] Finch, S. R. *Mathematical Constants*, Cambridge University Press, 2003.
[14] Friesen, C., and Hensley, D. The statistics of continued fractions for polynomials over a finite field, *Proceedings of the American Mathematical Society*, 124, (1996) 9, pp 2661–2673,
[15] Heilbronn, H. On the average length of a class of continued fractions, Number Theory and Analysis, ed. by P. Turan, New-York, Plenum, 1969, pp 87-96.
[16] Hensley, D. The number of steps in the Euclidean algorithm, Journal of Number Theory, 49, 2 (1994), 142-182
[17] Hwang, H.-K., *Théorèmes limite pour les structures combinatoires et les fonctions arithmétiques,* PhD thesis, Ecole Polytechnique, Dec. 1994.
[18] Knopfmacher, J. and Knopfmacher, A. The exact length of the Euclidean algorithm in $F_q[X]$, *Mathematika*, 35, (1988), pp 297-304
[19] Lehmer, D. H. Euclid's algorithm for large numbers. Am. Math. Mon. (1938) 45 pp 227–233.
[20] Lhote, L. Computation of a Class of Continued Fraction Constants Proceedings of Alenex–ANALCO04, pp 199–210
[21] Lhote, L. and Vallée, B. *Sharp estimates for the main parameters of the Euclid Algorithm*, Proceedings of LATIN'06, LNCS 3887, pp 689-702.
[22] Philipp, W. Some metrical theorems in number theory II, Duke Math. J. 37 (1970) pp 447–488. Errata, ibid, 788.
[23] Ruelle, D. *Thermodynamic formalism,* Addison Wesley (1978)
[24] Schonhage, A. Schnelle Berechnung von Kettenbruchentwicklungen, Acta Informatica pp 139–144 (1971)
[25] Tenenbaum, G. *Introduction à la théorie analytique des nombres*, vol. 13. Institut Élie Cartan, Nancy, France, 1990.
[26] Vallée, B. Euclidean Dynamics, Discrete and Continuous Dynamical Systems, 15 (1) May 2006, pp 281-352.
[27] Vallée, B. Dynamical Analysis of a Class of Euclidean Algorithms, Theoretical Computer Science, vol 297/1-3 (2003) pp 447-486.

[28] Vallée, B. Digits and Continuants in Euclidean Algorithms. Ergodic Versus Tauberian Theorems, Journal de Théorie des Nombres de Bordeaux, JTNB 12 (2000) pp 531-570.
[29] Vallée, B. Opérateurs de Ruelle-Mayer généralisés et analyse en moyenne des algorithmes de Gauss et d'Euclide, Acta Arithmetica 81.2 (1997), pp 101–144
[30] Von Zur Gathen, J. and Gerhard, J. Modern Computer Algebra, Cambridge University Press (1999)