Fine costs for Euclid's algorithm on polynomials and Farey maps

Valérie Berthé, Hitoshi Nakada, Rie Natsui, Brigitte Vallée

FINE COSTS FOR THE EUCLID ALGORITHM ON POLYNOMIALS AND FAREY MAPS

VALÉRIE BERTHÉ, HITOSHI NAKADA, RIE NATSUI, AND BRIGITTE VALLÉE

Abstract. This paper studies digit-cost functions for the Euclid algorithm on polynomials with coefficients in a finite field, in terms of the number of operations performed on the finite field $\mathbb{F}_q$. The usual bit-complexity is defined with respect to the degree of the quotients; we focus here on a notion of 'fine' complexity (and on associated costs) which relies on the number of their non-zero coefficients. It also considers and compares the ergodic behavior of the corresponding costs for truncated trajectories under the action of the Gauss map acting on the set of formal power series with coefficients in a finite field. The present paper is thus mainly interested in the study of the probabilistic behavior of the corresponding random variables: average estimates (expectation and variance) are obtained in a purely combinatorial way thanks to classical methods in combinatorial analysis (more precisely, bivariate generating functions); some of our costs are even proved to satisfy an asymptotic Gaussian law.

We also relate this study with a Farey algorithm which is a refinement of the continued fraction algorithm for the set of formal power series with coefficients in a finite field: this algorithm discovers 'step by step' each non-zero monomial of the quotient, so its number of steps is closely related to the number of non-zero coefficients. In particular, this map is shown to admit a finite invariant measure in contrast with the real case. This version of the Farey map also produces mediant convergents in the continued fraction expansion of formal power series with coefficients in a finite field.

Keywords. Laurent formal power series, finite field, continued fractions, Farey map, bit-complexity, cost function, combinatorial analysis, bivariate generating functions

1. Introduction

We fix a positive integer q which is a power of a prime number p, and we consider the field $\mathbb{F}_q$ of cardinality q. It is well-known that the theory of continued fractions extends in a natural way the classical real framework to polynomials and formal power series with coefficients in the finite field $\mathbb{F}_q$. See for instance the survey [2]. Similarly as in the real case, we have in this framework an intimate correspondence between the Euclidean algorithm and continued fraction expansions. We study and compare here digit-cost functions for the Euclidean algorithm, on the one hand, and for truncated trajectories for the Gauss map acting on the set of formal power series, on the other hand.

1.1. **Euclid's algorithm on polynomials.** Let us first recall the Euclidean algorithm for polynomials in $\mathbb{F}_q[X]$. For P and $Q \in \mathbb{F}_q[X]$ with $\deg Q > \deg P \geq 0$, the Euclidean division computes a pair (A, R) with $R = 0$ or $\deg R < \deg P$ for which $Q = AP + R$. The Euclidean algorithm is a sequence of Euclidean divisions; by setting $R_0 := Q,\ R_1 := P$, one gets

$$R_0 = A_1 R_1 + R_2, \qquad R_2 = 0 \quad \text{or} \quad \deg R_2 < \deg R_1.$$

If $R_2 \neq 0$, then we can find, again, a pair of polynomials (A_2, R_3) such that

$$R_1 = A_2 R_2 + R_3, \quad R_3 = 0 \quad \text{or} \quad \deg R_3 < \deg R_2.$$

We can continue this procedure of divisions $R_{k-1} = A_k R_k + R_{k+1}$ until the ℓ-th step where we obtain a remainder $R_{\ell+1} = 0$. The last non-zero remainder R_ℓ is a largest common divisor (polynomial) of R_0 and R_1. In particular, R_0 and R_1 are coprime when $\deg R_\ell = 0$ (i.e., $R_\ell \in \mathbb{F}_q$

The research of the second author was supported in part by Grant-in Aid for Scientific research (No.24340020) of Japan Society for the Promotion of Science. The research of the third author was supported in part by Grant-in Aid for Scientific research (No.23740088) of Japan Society for the Promotion of Science.

with $R_\ell \neq 0$). The Euclidean algorithm builds the continued fraction expansion of the fraction R_1/R_0, that is,

$$\frac{R_1}{R_0} = \frac{1}{\big| A_1} + \frac{1}{\big| A_2} + \cdots + \frac{1}{\big| A_\ell}.$$

Remark that the fraction R_{k+1}/R_k is defined by the ending part of the continued fraction expansion, namely

$$\frac{R_{k+1}}{R_k} = \frac{1}{\big| A_{k+1}} + \frac{1}{\big| A_{k+2}} + \cdots + \frac{1}{\big| A_\ell}.$$

We will use the notation $L(P,Q) = L(R_1,R_0) = \ell$ for the length (i.e., the number of polynomial divisions) of the Euclidean algorithm. We also set $L(0,Q) := 0$.

Extended gcd and Bezout's coefficients. We similarly recall basic facts concerning the extended Euclidean algorithm. Let P and Q in $\mathbb{F}_q[X]$, with $0 \leq \deg P < \deg Q$. Let $\ell := L(P,Q)$. The extended Euclidean algorithm produces a pair of polynomials (S,T) such that

$$\gcd(P,Q) = SQ - TP \tag{1}$$

with the help of the sequences (P_k, Q_k) defined as

$$P_{-1} = 1,\ P_0 = 0, \quad P_{k+1} = A_{k+1}P_k + P_{k-1}, \qquad Q_{-1} = 0,\ Q_0 = 1,\ Q_{k+1} = A_{k+1}Q_k + Q_{k-1}. \tag{2}$$

Indeed, since the sequence $(R_k)_{0\leq k\leq \ell}$ produced by the Euclidean algorithm satisfies

$$R_0 = Q, \quad R_1 = P, \quad R_{k+2} = R_k - A_{k+1}\cdot R_{k+1}, \quad \text{for } 0 \leq k \leq \ell,$$

the equality $(-1)^k R_k = P_{k-1}Q - Q_{k-1}P$ holds for any k with $0 \leq k \leq \ell$ and yields (1) for $k = \ell$, with $S = (-1)^\ell P_{\ell-1}, T = (-1)^\ell Q_{\ell-1}$.

Then, the computation (2) of the Bezout pair (S,T) follows exactly the same lines as the computation of the fraction $P_{\ell-1}/Q_{\ell-1}$, which defines the $(\ell-1)$-th convergent of P/Q, that is,

$$\frac{P_{\ell-1}}{Q_{\ell-1}} = \frac{1}{\big| A_1} + \frac{1}{\big| A_2} + \cdots + \frac{1}{\big| A_{\ell-1}}.$$

Cost of a division. We are interested in the cost of the Euclidean algorithm, where the cost is the total number of operations performed in $\mathbb{F}_q$. Since the algorithm is a sequence of divisions, we first focus on the cost of a single division on the pair (P,Q) with $\deg P < \deg Q$ of the form $Q = AP + R$, with $R = 0$ or $\deg R < \deg P$. One has $\deg Q = \deg A + \deg P$. Such a division is performed with various operations on the field $\mathbb{F}_q$ (divisions, products, subtractions, shifts). The number of most of the operations needed depends on the number of monomials which are present in the divisor P and the quotient Q. For any non-zero polynomial P, $\nu(P)$ stands for the number of non-zero coefficients of P, i.e., the number of non-zero monomials in P. Of course, one has $\nu(P) \leq 1 + \deg P$, but, we wish to evaluate more precisely the number of operations over $\mathbb{F}_q$ which are performed during the division $Q = AP + R$, as summarized in the following table.

Number of divisions in $\mathbb{F}_q$	$\nu(A)$
Number of products in $\mathbb{F}_q$	$\nu(A)\cdot\nu(P)$
Number of subtractions in $\mathbb{F}_q$	$\nu(A)\cdot\nu(P)$
Upper bound for the number of shifts	$\nu(A)\cdot(\deg Q + 1)$
Total number of operations in the field $\mathbb{F}_q$	$O(\nu(A)\cdot(\deg Q + 1))$

The realistic bit-complexity of the Euclidean division would completely take into account the sparse representation of polynomials and would be related to the product $\nu(A)\cdot\nu(P)$. Nevertheless, we have not succeeded to deal with this quantity in our cost estimates, as detailed in Remark 1 below.

Costs in the polynomial case. When the set of inputs is

$$\Omega = \{(P,Q) \in \mathbb{F}_q[X]^2 \,:\, Q \,\text{monic},\, P = 0 \text{ or } \deg P < \deg Q\},$$

the execution of the (extended) Euclid Algorithm on the input pair $(P,Q) \in \Omega$ is defined by the number of steps $\ell := L(P,Q)$, and the three finite sequences of quotients $(A_k)_{1\le k\le \ell}$, remainders $(R_k)_{0\le k\le \ell}$ and denominators $(Q_k)_{1\le k\le \ell}$, with

$$Q_k := \operatorname{den}\left(\frac{1}{|}\,A_1 + \frac{1}{|}\,A_2 + \ldots + \frac{1}{|}\,A_k\right), \qquad \deg Q_k = \sum_{j=1}^{k} \deg A_j,$$

$$R_k = \operatorname{den}\left(\frac{1}{|}\,A_{k+1} + \frac{1}{|}\,A_{k+2} + \cdots + \frac{1}{|}\,A_{\ell}\right) \cdot \gcd(P,Q),$$

$$\deg R_k = \sum_{j=k+1}^{\ell} \deg A_j + \deg \gcd(P,Q), \quad 0 \le k \le \ell - 1,\ R_\ell = \gcd(P,Q).$$

We have now gathered all the required material in order to define our costs for both the Euclidean and the extended Euclidean algorithm on the input (P,Q).

Definition 1 (Costs in the polynomial case)**.**

(*i*) *The total number of non-zero monomials in the set of the quotients is*

$$N(P,Q) = \sum_{k=1}^{\ell} \nu(A_k).$$

(*ii*) *The* usual bit–complexity B *(as defined e.g. in* [13]*) and the* fine bit-complexity ϕ *of the Euclid algorithm on the input* (P,Q) *are*

$$B(P,Q) = \sum_{k=1}^{\ell} (1+\deg A_k)\cdot(1+\deg R_k), \qquad \phi(P,Q) = \sum_{k=1}^{\ell} \nu(A_k)\cdot(1+\deg R_k).$$

(*iii*) *The costs* $\underline{B}$ *and* $\underline{\phi}$ *of the extended Euclid algorithm correspond to the the extra bit–complexity for computing Bezout's coefficients, in their usual or fine versions*

$$\underline{B}(P,Q) = \sum_{k=1}^{\ell-1} (1+\deg A_k)\cdot(1+\deg Q_{k-1}), \qquad \underline{\phi}(P,Q) = \sum_{k=1}^{\ell-1} \nu(A_k)\cdot(1+\deg Q_{k-1}).$$

(*iv*) *The costs* $B + \underline{B}$*, and* $\phi + \underline{\phi}$ *are the costs of the extended Euclidean algorithm, in their usual or fine version. They are called* total costs*.*

1.2. **Continued fractions.** We let denote by

$$\mathbb{F}_q(X), \quad \mathbb{F}_q((X^{-1})), \quad \mathbb{L}$$

the set of rational fractions, the set of Laurent formal series of the variable $1/X$, and the subset of $\mathbb{F}_q((X^{-1}))$ of series of negative degree, respectively. Here the degree of a non-zero element $f \in \mathbb{F}_q((X^{-1}))$ with

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots, \qquad a_n \neq 0$$

is defined as $\deg f = n$. We also define the degree of $0 \in \mathbb{F}_q$ by $\deg 0 = -\infty$ as usual. The norm of f is then defined as $|f| = q^{\deg f}$.

The analog of the Gauss map T on $\mathbb{L}$ is defined as

$$T(f) = \frac{1}{f} - \left[\frac{1}{f}\right] \quad \text{for } f \neq 0, \qquad T(0) = 0,$$

where $[\,\cdot\,]$ stands for the polynomial part for formal power series. In all that follows, the map T will be referred to as the Gauss map, by abuse of language. Then, the Gauss map builds the continued fraction expansion of f, that is,

$$f = \frac{1}{\big|A_1} + \frac{1}{\big|A_2} + \cdots \qquad \text{with} \quad A_k = \left[\frac{1}{T^{k-1}(f)}\right], \qquad k \geq 1.$$

The analog of the Gauss measure is the Haar measure $\mu_{\mathbb{L}}$ (normalized to 1 on $\mathbb{L}$): it is ergodic and T-invariant.

Total costs on $\mathbb{L}$. When f is a rational fraction P/Q of $\mathbb{F}_q(X)$ with $\deg P < \deg Q$, it can be viewed as an element of $\mathbb{L}$, and the iteration of the Gauss map on P/Q exactly coincides with the Euclid Algorithm on (P, Q): the trajectory of P/Q under the action of T arrives at 0 in a finite number of steps and stops there. In the general case of an element f, the trajectory is infinite, but we are interested by the *truncated trajectories* which are stopped at depth n, i.e., after n steps:

$$\mathcal{T}_n(f) := (f, T(f), \dots T^n(f)).$$

The truncated continued fraction at depth n leads to a finite continued fraction expansion and produces a fraction equal to the n-th convergent of f, that is,

$$\frac{P_n}{Q_n} = \frac{1}{\big|A_1} + \frac{1}{\big|A_2} + \cdots \frac{1}{\big|A_n}.$$

The computation of the pair (P_n, Q_n) follows the general recurrence already seen in (2), and we are interested in evaluating the cost of this computation in $\mathbb{L}$ (assuming that the sequence of partial quotients (A_k) has already been computed).

We thus let denote by $N_n(f)$ the total number of non-zero monomials in the sequence of partial quotients $(A_1, A_2, \dots, A_n)$, and we also consider the bit-complexity costs needed for computing the n-th convergent, in their two versions. These costs are to be compared respectively to the costs introduced in (i) and (iii) above for the polynomial case.

Definition 2 (Costs in the continued fraction case)**.**

(*i*) *The total number of non-zero monomials in the sequence of partial quotients* $(A_1, A_2, \dots, A_n)$ *is*

$$N_n(f) := \sum_{k=1}^{n} \nu(A_k).$$

(*ii*) *The usual bit-complexity* $\underline{B}_n$ *and the fine bit complexity* $\underline{\phi}_n$ *are*

$$\underline{B}_n(f) = \sum_{k=1}^{n} (1 + \deg A_k) \cdot (1 + \deg Q_{k-1}), \qquad \underline{\phi}_n(f) = \sum_{k=1}^{n} \nu(A_k) \cdot (1 + \deg Q_{k-1}).$$

1.3. **Probabilistic models.** We deal within two models, namely a discrete and a continuous one.

- The *discrete model* is defined by the sequence of finite sets Ω_m of polynomials, with

$$\Omega_m = \{(P, Q) \in \mathbb{F}_q[X]^2 \,:\, P = 0 \text{ or } 0 \leq \deg P < \deg Q = m,\ Q \,:\, \text{monic}\}, \tag{3}$$

  endowed with the uniform probability denoted as $\mathbb{P}_m$. The expectation and the variance in this model are respectively denoted as $\mathbb{E}_m$ and $\mathbb{V}_m$. We are interested there by the probabilistic behavior of costs $N, B, \phi, \underline{B}, \underline{\phi}$, in the finite set Ω_m, for m tending to infinity.
- The *continuous model* deals with the set $\mathbb{L}$ endowed with its Haar measure $\mu_{\mathbb{L}}$. We study some costs which are relative to the truncated trajectory of $f \in \mathbb{L}$ at depth n, i.e., the costs N_n, B_n and ϕ_n. We consider in this case almost everywhere behavior when the truncation degree n tends to infinity.

Methodology. In the discrete model, the study of the fine costs uses classical methods from analytic combinatorics developed in [13] (such as recalled in Section 2). In the continuous model (see Section 4), we use the ergodic theorem, together with a suitable extension of the function ν (that counts the number of non-zero monomials) to the set $\mathbb{L}$. Note that the ergodic theorem, which is well-suited for the study of truncated trajectories, does not provide any error term. We introduce in this paper (Section 5) an additive (also said subtractive in the continued fraction literature) version of the Gauss map, called here *Farey map* by analogy with the real case, which discovers the non-zero monomials of each quotient one by one. Then, this map can be used to study the function ν. The main difficulty relies in the fact that we need a transformation that gives a particular role to the constant term of the polynomial. We stress the fact that the definition of this map is not canonical, and there are indeed two natural definitions. We provide an explicit expression of an invariant measure for this map (see Theorem 8) which is absolutely continuous with respect to the Haar measure, and we show that it is a finite measure, in contrast to the original Farey map, which has an infinite absolutely continuous invariant measure with respect to Lebesgue measure. We then deduce metric results that can be applied to the study of the cost functions we are considering here. This map is also interesting *per se* because it gives rise to a notion of mediant convergents for $\mathbb{F}_q((X))$ (see Section 6).

A brief overview of the literature. Many costs describing the execution of the Euclidean algorithm (in the discrete model), and of the continued fraction algorithm (in the continuous model), have been widely studied, in the classic number case, and also in the polynomial case. The reader can find an historical account of the literature on the number case, both for the average and distributional analysis of costs, in [13] or [20, 21, 17] and in the references therein. It is in particular known since [3, 4, 8] that the average length of the Euclidean algorithm is linear with respect to the logarithm of the numbers taken as input, with the multiplicative constant being equal to the inverse of the entropy of the Gauss map multiplied by 2, with the factor 2 corresponding to the dimension, i.e., the number of parameters under consideration. For results in distribution concerning the length (i.e., for an asymptotic Gaussian law), see [9], and also [1, 13, 20, 21] for a detailed distributional analysis, also involving more general cost functions.

We focus here on the polynomial case, where the study is simpler. Indeed there are no carries and the topology is ultrametric. Over $\mathbb{F}_q[X]$, the length L of the Euclidean algorithm for polynomials is very precisely studied: on the set of polynomials with degree at most m, its mean and its variance are linear with respect to the degree m (see for instance [6, 14, 15] and [13]). Its distribution is discussed in [12, 7], where it is proven to be binomial. Note in particular that the mean of L is exactly $(q-1)/q \cdot m$ on the set of polynomials with degree less than m; the constant $(q-1)/q$ equals $2/h$ where h is the entropy of the Gauss map, that is, $2q/(q-1)$. Furthermore, the usual bit-complexities $B, \underline{B}, B+\underline{B}$ are studied in [13], where they are proven to obey an asymptotic Gaussian law. In particular,

$$\mathbb{E}_m[B] = m^2\,\frac{2q-1}{2q} + O(m),\ \mathbb{V}_m[B] = m^3\frac{q-1}{3q^2} + O(m^2),\ \mathbb{P}_m\left[\left|\frac{1}{m^2}B - \frac{2q-1}{2q}\right| \geq 1/\varepsilon\right] = O\left(\frac{\varepsilon^2}{m}\right).$$

However, the fine bit-complexity ϕ has not been previously handled.

The results in the polynomial case are obtained via analytic combinatorics (see [6]), with the direct study of bivariate generating functions. In the integer case, the non-ultrametricity of the topology prevents the direct use of generating functions, which are replaced by Dirichlet series. However there is a strong parallelism between the two studies. It is indeed observed in [13] that results in the polynomial case could be obtained via the use of transfer operators (as in the integer case) within the framework of dynamical analysis, which is the central tool in the number case. This is due to the common framework between the integer and the polynomial case, given by the underlying dynamical system, namely the Gauss map, with the branches of the dynamical systems being affine for the polynomial case leading to a dynamical system without memory. For a detailed discussion on the parallelism between the integer and the polynomial case, both for the results and the methods, see Section 6 in [13].

There is a further parallelism that occurs, both in the integer and in the polynomial case, between the probabilistic behavior for costs in the discrete model and in the continuous model, that is, for orbits of rational entries and for truncated trajectories under the action of the Gauss map. As highlighted in [1, 21], executions of the Euclidean algorithm behave on average similarly to the way truncated real trajectories behave on average (this also extends to distributions), and the probabilistic behavior of gcd algorithms related to rational trajectories is quite similar to the behavior of their continuous counterparts, related to generic trajectories.

We stress the fact that concerning the ultrametric version of the Farey map, its invariant measure is finite, unlike in the usual real case.

Description of the results. Here, we wish to study the costs $N, \phi, \underline{\phi}$ in the discrete model, and $N_n, \underline{\phi}_n$ in the continuous model.

As in the previously described studies, we deal in the discrete model with the probabilistic behavior of finite trajectories on the set of pairs of polynomials Ω_m (see (3)), and in the continuous model, we deal with truncated trajectories and obtain results which hold almost everywhere.

For finite trajectories in the discrete model, we obtain (namely in Theorems 1, 3, below), first for the cost N,

$$\mathbb{E}_m[N] = m \cdot \frac{2(q-1)}{q},\ \mathbb{V}_m[N] = m\,\frac{2(q-1)}{q^2} + O(1),\ \mathbb{P}_m\left[\left|\frac{1}{m}N - 2\frac{q-1}{q}\right| \geq 1/\varepsilon\right] = O\left(\frac{\varepsilon^2}{m}\right)$$

and both for costs ϕ or $\underline{\phi}$,

$$\mathbb{E}_m[\phi] = m^2\,\frac{q-1}{q} + O(m),\ \mathbb{V}_m[\phi] = m^3\,\frac{2(q-1)}{3q^2} + O(m^2),\ \mathbb{P}_m\left[\left|\frac{1}{m^2}\phi - \frac{q-1}{q}\right| \geq 1/\varepsilon\right] = O\left(\frac{\varepsilon^2}{m}\right).$$

We obtain also asymptotic Gaussian laws for the costs L, D, N and $\phi + \underline{\phi}$ (namely in Theorems 2, 4, below).

For truncated trajectories, we obtain the following results that hold for a.e. $f \in \mathbb{L}$:

$$\lim_{n\to\infty} \frac{N_n}{\deg Q_n}(f) = 2 \cdot \frac{q-1}{q} \quad \text{and} \quad \lim_{n\to\infty} \frac{1}{\deg^2 Q_n}\underline{\phi}_n(f) = \frac{q-1}{q},$$

which correspond respectively to Theorem 5 and 6 below.

There results confirm the fact that the probabilistic behavior of gcd algorithms related to rational trajectories is quite similar to the behavior of their continuous counterparts, related to generic trajectories, which was already observed for the bit-complexity [13].

Remark 1. A more realistic bit-complexity of the Euclidean division would be provided by the study of the product $\nu(A) \cdot \nu(P)$. Nevertheless, we have not succeeded to deal with this quantity in our cost estimates. Indeed, we know how to handle each factor $\nu(A_k)$, or $\deg A_k$. However, we do not know how to handle $\nu(R_k)$ or $\nu(Q_k)$, whereas it is easy to deal with their degrees, equal to the sum of the degrees of A_j. Our fine complexity ϕ can be considered as an intermediate complexity, between the usual bit complexity and the complexity $\sum_{k=1}^{\ell} \nu(A_k) \cdot \nu(R_k)$, that is,

$$\sum_{k=1}^{\ell} (\deg A_k + 1)(\deg R_k + 1) \leq \phi(P, Q) \leq \sum_{k=1}^{\ell} \nu(A_k) \cdot \nu(R_k).$$

Contents. Let us briefly describe the contents of the paper. We first consider the discrete model associated with polynomials in Section 2 by recalling the methods of analytic combinatorics based on generating functions. Elementary costs are considered (the cost N in particular) as a warm-up. We then discuss in more details the average behavior of the fine-bit complexity costs ϕ and $\phi + \underline{\phi}$ in Section 3. Section 4 is devoted to the continuous model. We obtain, via the ergodic theorem, the almost everywhere behavior of the total number of non-zero coefficients $N_n(f)$ and of the fine bit-complexity $\underline{\phi}_n(f)$. In Section 5 we introduce and discuss two versions for a Farey map, and we show how to apply the corresponding metric results to recover the statistical study of cost functions. The Farey map is lastly seen to produce mediant convergents in the continued fraction expansion in the Appendix (Section 6).

2. Probabilistic estimates of cost functions via analytic combinatorics methodology

In this section, we show how to deduce information concerning the probabilistic behavior of cost functions in the discrete model. Here, we use classical methods in analytic combinatorics. We first recall in Section 2.1, 2.2 and 2.3 the basic approach used for the study of additive costs, such as developed e.g. in [6, 13, 21]. Then, Section 2.4 is devoted to the study of some basic costs defined on polynomials, whereas Section 2.5 and 2.6 analyse the corresponding simple additive costs related to the execution of the Euclidean algorithm for pairs of polynomials.

2.1. **Basic generating functions.** Recall that

$$\Omega = \{(P,Q) \in \mathbb{F}_q[X]^2 \,:\, Q \,\text{monic},\, P = 0 \text{ or } \deg P < \deg Q \,\}.$$

The size of a pair $(P,Q) \in \Omega$ is equal by definition to $\deg Q$, and the subset Ω_m formed by the elements of Ω of size m (with $m \geq 0$) has cardinality $|\Omega_m| = q^{2m}$. Then, the generating function $T_\Omega(z)$ of Ω is

$$T_\Omega(z) := \sum_{m \geq 0} |\Omega_m| z^m = \frac{1}{1-q^2 z}.$$

As it is well known (see for instance [6], Example IX.15), an element (P,Q) of Ω is uniquely determined, through Euclid's algorithm, by the finite sequence of the quotients $(A_1, \cdots, A_\ell)$ (where each A_i is of degree at least one), together with its gcd (which is here monic). (If $P = 0$, then the sequence $(A_1, \cdots, A_\ell)$ is empty.) We thus introduce the sets

$$\mathcal{G} = \{P \in \mathbb{F}_q[X] \,:\, \deg P \geq 1\} \text{ and } \mathcal{U} = \{P \in \mathbb{F}_q[X] \,:\, P \text{ is monic}\},$$

where $\mathcal{G}$ is the set of possible quotients, and $\mathcal{U}$ is the set of possible gcd's. Euclid's algorithm thus provides the following bijection

$$\Omega = \mathtt{Seq}(\mathcal{G}) \cdot \mathcal{U}, \tag{4}$$

where $\mathtt{Seq}(\mathcal{G})$ stands for the set of finite sequences of elements of $\mathcal{G}$.
The generating functions of the sets $\mathcal{G}$ and $\mathcal{U}$ are easily determined, namely

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

Note that

$$\frac{1}{1-G(z)} = \frac{1-qz}{1-q^2 z}.$$

We thus check the indentity

$$T_\Omega(z) = \frac{1}{1-G(z)} \cdot U(z) \tag{5}$$

which 'copies' the bijection (4).

2.2. **The general approach.** Our general approach follows the main following lines, that are classical in analytic combinatorics. For more details, see also [6, 13, 21].

Let c be a cost defined on the set $\mathcal{G} \subset \mathbb{F}_q[X]$, and define the following *additive* cost C relative to the execution of the Euclidean algorithm on the input $(P,Q) \in \Omega$

$$C(P,Q) := \sum_{i=1}^{L(P,Q)} c(A_i), \tag{6}$$

where $A_i = A_i(P,Q)$ are the quotients and $L(P,Q)$ is the number of steps of Euclid's algorithm.

We wish to obtain probabilistic estimates for the cost C on the set Ω, for instance evaluate its expectation $\mathbb{E}_m[C]$ and its variance $\mathbb{V}_m[C]$ on the subset Ω_m, or else, determine its asymptotic distribution on Ω_m when $m \to \infty$. Then, we aim at relating the behavior of cost C on Ω to the behavior of the basic cost c on $\mathcal{G}$. Let us note that, by abuse of notation, we use the same notation $\mathbb{E}_m[\,.\,]$ and $\mathbb{V}_m[\,.\,]$, both for costs c and C defined respectively on $\mathcal{G}_m$ and Ω_m. It is natural for instance to compare the expectation $\mathbb{E}_m[C]$ and its variance $\mathbb{V}_m[C]$ on the subset Ω_m

with their counterparts on the subset $\mathcal{G}_m$ of $\mathcal{G}$ made of the polynomials with degree m, namely the expectation $\mathbb{E}_m[c]$ and the variance $\mathbb{V}_m[c]$ of the cost c on the subset $\mathcal{G}_m$.

We introduce the bivariate generating functions $S_c(z,u), T_C(z,u)$ respectively relative to the cost c on the set $\mathcal{G}$, and to the cost C on the set Ω. Their general terms are

$$[z^m u^k] S_c(z,u) = |\{P \in \mathcal{G} \,:\, \deg P = m \text{ and } c(P) = k\}|\,,$$

$$[z^m u^k] T_C(z,u) = |\{(P,Q) \in \Omega \,:\, \deg Q = m \text{ and } C(P,Q) = k\}|\,.$$

As the cost C is an additive cost associated with the cost c defined on the set $\mathcal{G}$, we then deduce from (5) a relation between these generating functions, namely

$$T_C(z,u) = \frac{1}{1 - S_c(z,u)} \cdot U(z). \tag{7}$$

We are interested in three costs of type C, namely the cost L, the cost D and the cost N respectively related to the following costs c equal to

$$1, \quad d := 1 + \deg, \quad \nu. \tag{8}$$

Section 2.4 provides a simple expression of the generating functions of type S_c associated with these three costs, then we will handle the costs $C = L, C = D, C = N$, via their generating functions of type T_C, in Section 2.5 and 2.6, where their asymptotic Gaussian law will be established. But before handling these cases, we will recall in the next section how to deduce estimates for the expectation and the variance from the generating functions.

2.3. **Cumulative generating functions.** We now deal with the *cumulative generating functions*. The first one, denoted by $S_{(c)}(z)$, is relative to the cost c on the set $\mathcal{G}$, and the second one, denoted by $T_{(C)}(z)$, is relative to the cost C on the set Ω. Their general terms are respectively equal to

$$\sum_{\substack{P \in \mathcal{G}, \\ \deg P = m}} c(P), \qquad \sum_{\substack{(P,Q) \in \Omega, \\ \deg Q = m}} C(P,Q).$$

The series $S_{(c)}(z), T_{(C)}(z)$ are obtained by taking the derivative of $S_c(z,u), T_C(z,u)$ with respect to u, at $u = 1$, i.e.,

$$S_{(c)}(z) = \frac{\partial}{\partial u} S_c(z,u)|_{u=1}, \qquad T_{(C)}(z) = \frac{\partial}{\partial u} T_C(z,u)|_{u=1}. \tag{9}$$

We thus deduce from (7) that

$$T_{(C)}(z) = S_{(c)}(z) \cdot \left(\frac{1}{1 - G(z)}\right)^2 \cdot U(z). \tag{10}$$

The expectations $\mathbb{E}_m[c]$, $\mathbb{E}_m[C]$ are now obtained via the extraction of the coefficient of z^m in the generating functions $S_{(c)}$ and $T_{(C)}$, that is,

$$\mathbb{E}_m[c] = \frac{[z^m] S_{(c)}(z)}{(q-1)q^m}, \qquad \mathbb{E}_m[C] = \frac{[z^m] T_{(c)}(z)}{q^{2m}}.$$

In the same vein, the series $S_{(c^2)}(z), T_{(C^2)}(z)$ are related to the second derivative, via the equalities

$$S_{(c^2)}(z) - S_{(c)}(z) = \frac{\partial^2}{\partial^2 u} S_c(z,u)|_{u=1}, \qquad T_{(C^2)}(z) - T_{(C)}(z) = \frac{\partial^2}{\partial^2 u} T_C(z,u)|_{u=1}. \tag{11}$$

The expectations $\mathbb{E}_m[c^2]$, $\mathbb{E}_m[C^2]$ are now obtained via the extraction of the coefficient of z^m in the generating functions $S_{(c^2)}$ and $T_{(C^2)}$.

2.4. **Costs c on $\mathcal{G}$.** We now consider the three costs c defined in (8).

Lemma 1. *The generating functions $S_c(z,u)$ for the three costs of interest are*

$$S_1(z,u) = u\,G(z), \qquad S_d(z,u) = u\;G(zu), \qquad S_\nu(z,u) = u\,G\left(z\left(u\frac{q-1}{q}+\frac{1}{q}\right)\right).$$

The cumulative generating functions are

$$S_{(1)}(z) = G(z), \qquad S_{(d)}(z) = G(z) + zG'(z) \qquad S_{(\nu)}(z) = G(z) + \frac{q-1}{q}zG'(z).$$

Proof. Let us recall that $[z^m u^k]S_c(z,u) = |\{P \in \mathcal{G} \,:\, \deg P = m \text{ and } c(P) = k\}|$. The variable u in $S_1(z,u)$ occurs with power 1 for every polynomial of $\mathcal{G}$, which yields $S_1(z,u) = uG(z)$. For the cost $d = 1 + \deg$, one gets $S_d(z,u) = uG(zu)$, where the multiplication of the term $G(zu)$ by u corresponds to 1, and the mutiplication by u in $G(uz)$ corresponds to the degree. Lastly, for the cost ν that counts the number of non-zero monomials, the multiplication of the G term by u corresponds to the leading term (which is non-zero), whereas the multipication of z by $\left(u\frac{q-1}{q}+\frac{1}{q}\right)$ in the G term takes into account the remaining monomials. Recall that $G(z) = (q-1)\cdot(\frac{1}{1-qz}-1)$. For each polynomial of a given degree, there are $(q-1)/q$ choices for the non-zero terms, and one choice over q for the zero terms. □

We then deduce from (9) and (11) the following on $\mathcal{G}_m$:

$$\mathbb{E}_m[1] = 1,\ \mathbb{E}_m[d] = m+1,\ \mathbb{E}_m[\nu] = 1 + \frac{q-1}{q}\cdot m, \qquad \mathbb{V}_m[\nu] = \frac{q-1}{q^2}\cdot m.$$

Note that these costs are easy to study in a direct way. For instance, the variable $\nu - 1$ is the sum of m Bernoulli variables of parameter $(q-1)/q$, that is, the distribution of $\nu - 1$ is binomial.

2.5. **Expectation and variance for costs C on Ω.** Here, the costs of interest are of the form

$$C(P,Q) = \sum_{i=1}^{\ell(P,Q)} c(A_i),$$

and involve the value of the cost c on the quotients $A_i = A_i(P,Q)$ of the Euclidean algorithm. The following theorem is a direct application of (10) and (11).

Theorem 1. *On the set Ω_m, the expectation and the variance of the costs L, D, N satisfy*

$$\begin{aligned}
&\mathbb{E}_m[L] = m\left(\tfrac{q-1}{q}\right), && \mathbb{V}_m[L] = m\left(\tfrac{q-1}{q^2}\right)\\
&\mathbb{E}_m[D] = m\left(\tfrac{2q-1}{q}\right) + O(1), && \mathbb{V}_m[D] = m\left(\tfrac{q-1}{q^2}\right) + O(1)\\
&\mathbb{E}_m[N] = 2m\left(\tfrac{q-1}{q}\right) + O(1), && \mathbb{V}_m[N] = 2m\left(\tfrac{q-1}{q^2}\right) + O(1).
\end{aligned}$$

Furthermore, for $C \in \{L, D, N\}$

$$\mathbb{P}_m\left[\left|\frac{1}{m}(C - \mathbb{E}_m[C])\right| \geq 1/\varepsilon\right] = O\left(\frac{\varepsilon^2}{m}\right). \tag{12}$$

Proof. We deduce (12) from a direct application of Chebyshev inequality. □

2.6. **Asymptotic normal laws for costs C on Ω.** We follow here Definition 1 of [13].

Definition 3 (Asymptotic Gaussian law)**.** *Let R be a cost defined on Ω. The cost R is said to follow an asymptotic Gaussian law if there exist two sequences of real numbers $(a_m)_m$, $(b_m)_m$, and a sequence $(r_m)_m$ of functions $r_m \colon \mathbb{R} \to \mathbb{R}$, with $\lim_{m\to\infty} \sup\{r_m(y) \,:\, y \in \mathbb{R}\} = 0$, for which*

$$\mathbb{P}_m\left[(P,Q) \in \Omega_m \,:\, \frac{R(P,Q) - a_m}{\sqrt{b_m}} \leq y\right] = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{y} e^{-t^2/2}dt + r_m(y).$$

The expectation $\mathbb{E}_m[R]$ and the variance $\mathbb{V}_m[R]$ then satisfy

$$\mathbb{E}_m[R] \sim a_m, \quad \mathbb{V}_m[R] \sim b_m.$$

Theorem 2. *The three costs L, D, N follow an asymptotically Gaussian law on Ω.*

Proof. We consider here a cost $C \in \{L, D, N\}$. The expectation of the random variable u^C (for u a complex number close to 1) on the set Ω_m satisfies

$$\mathbb{E}_m[u^C] = \frac{[z^m]T_C(z,u)}{[z^m]T_C(z,1)} = \frac{1}{q^{2m}}[z^m]T_C(z,u) \qquad \text{with} \quad T_C(z,u) = \frac{U(z)}{1 - S_c(z,u)}.$$

By Lemma 1, we know that, for any of the three costs c, the generating function $S_c(z,u)$ is always of the form $S_c(z,u) = uG(z\rho)$, with

$$\rho = 1 \ \ (\text{for } c = 1), \quad \rho = u \ \ (\text{for } c = d = 1 + \deg), \quad \rho = u \cdot \frac{q-1}{q} + \frac{1}{q} \ \ (\text{for } c = \nu).$$

One then checks that $T_C(z,u)$ can be written in the form

$$T_C(z,u) = \frac{U(z)}{1 - uG(z\rho)} = \frac{1 - qz\rho}{(1-qz)\,(1 - qz\rho(u(q-1)+1))}.$$

Then, in each case, as a function of the variable z, the generating function $T_C(z,u)$ has two poles, namely

$$z_c = \frac{1}{q\rho(u(q-1)+1)}, \qquad \text{and } z = \frac{1}{q}.$$

When u is close to 1, the first pole z_c (which depends on the cost c via the value of ρ) is close to $1/q^2$: it is thus the dominant one, and

$$[z^m]T_C(z,u) = (q\rho(u(q-1)+1))^m \cdot \left(\frac{1 - qz_c\rho}{1 - qz_c}\right) \cdot \left(1 + O\left((qz_c)^m\right)\right).$$

Then, uniformly on a complex neighborhood of $u = 1$, one has

$$\mathbb{E}_m[u^C] = A_c(u) \cdot B_c(u)^m \left(1 + O\left(\frac{1}{\kappa_c^m}\right)\right)$$

where $A(u)$, $B(u)$ are analytic at $u = 1$, and

$$B_c(u) = \rho\left(u\frac{q-1}{q} + \frac{1}{q}\right), \qquad \kappa_c \sim \frac{1}{q}.$$

It remains to apply the quasi-power theorem (see [10] and Theorem IX-8 in [6]) which gives a central limit theorem with speed of convergence for random variables whose moment generating function has a 'quasi-power' structure. It thus applies to each random variable C provided that the coefficient of the variance $\mathbb{V}_m[C]$ is not zero, which is true for the three cases under consideration. □

3. Study of the fine-bit complexity in the discrete model

3.1. **Expectation and variance of the fine bit-complexity.** Now we consider the average and the variance of the fine bit-complexity.

Theorem 3. *On the set Ω_m, the expectation and the variance of the fine complexity ϕ satisfy*

$$\mathbb{E}_m[\phi] = \left(\frac{q-1}{q}\right) \cdot m^2 + O(m) \qquad \mathbb{V}_m[\phi] = \frac{2}{3}\left(\frac{q-1}{q^2}\right) \cdot m^3 + O(m^2).$$

Furthermore

$$\mathbb{P}_m\left[\left|\frac{1}{m^2}\phi - \frac{q-1}{q}\right| \geq 1/\varepsilon\right] = O\left(\frac{\varepsilon^2}{m}\right). \tag{13}$$

The same estimates hold for the fine complexity $\underline{\phi}$.

We recall the similar results which have been previously obtained in [13] for the classical bit complexity B

$$\mathbb{E}_m[B] = \left(\frac{2q-1}{2q}\right) \cdot m^2 + O(m) \qquad \mathbb{V}_m[B] = \left(\frac{q-1}{3q^2}\right) \cdot m^3 + O(m^2).$$

Proof. Remark first that the estimates of Theorem 3 also hold for ϕ and for $\underline{\phi}$ since the two fractions

$$\frac{1}{|A_1} + \frac{1}{|A_2} + \cdots + \frac{1}{|A_\ell} \quad \text{and} \quad \frac{1}{|A_\ell} + \frac{1}{|A_2} + \cdots + \frac{1}{|A_1}$$

have the same denominator.

For a general additive cost C (associated with the cost c as in (6)), we can adopt a viewpoint that is different from the one developed in Section 2, first in order to recover (10).

We first fix a length L, that is, we work with finite sequences of L quotients in $\mathcal{G}^L$. We consider the cost $C_i := c(A_i)$, defined on the set $\mathcal{G}^L$, for a given i with $1 \leq i \leq L$. The cumulative generating function of the cost C_i on the class $\Omega^{[L]} := \mathcal{G}^L \times \mathcal{U}$ is

$$G^{i-1}(z) \cdot S_{(c)}(z) \cdot G^{L-i}(z) \cdot U(z),$$

by recalling that $S_{(c)}(z)$ is the cumulative generating function of cost c on the set $\mathcal{G}$. Finally, the cumulative generating function $T_{(C)}(z)$ of the cost C on the class Ω is obtained by taking the sum over all the indices (i, L) with $i \leq L$, which yields

$$T_{(C)}(z) = \frac{1}{1 - G(z)} \cdot S_{(c)}(z) \cdot \frac{1}{1 - G(z)} \cdot U(z), \tag{14}$$

and we recover (10). This will be the viewpoint we now adopt in the present proof.

Recall that

$$\phi(P, Q) = \sum_{i=1}^{L(P,Q)} \nu(A_i) \cdot (1 + \deg R_i), \qquad \deg R_i = \sum_{j=i+1}^{L(P,Q)} \deg A_j + \deg \gcd(P, Q).$$

For a given integer i with $1 \leq i \leq L$, the generating function of the cost $\nu(A_i) \cdot u^{1+\deg R_i}$ on the class $\mathcal{G}^L \times \mathcal{U}$ is as previously (compare with (14))

$$G^{i-1}(z) \cdot S_{(\nu)}(z) \cdot u \cdot G^{L-i}(uz) \cdot U(uz).$$

Then, the generating function of the cost

$$\sum_{i=1}^{L(P,Q)} \nu(A_i) \cdot u^{1+\deg R_i}$$

on the class Ω is obtained by taking the sum over all the indices (i, L) with $1 \leq i \leq L$, which yields

$$\frac{1}{1 - G(z)} \cdot S_{(\nu)}(z) \cdot u \cdot \left(\frac{1}{1 - G(uz)} \right) \cdot U(uz).$$

Finally, the cumulative generating function $T_{(\phi)}(z)$ of the cost ϕ on Ω is obtained by taking the derivative with respect to u at $u = 1$, which yields

$$\mathbb{E}_m[\phi] = \frac{1}{q^{2m}} [z^m] T_{(\phi)}(z) = \frac{q-1}{q} \cdot m^2 + \frac{q-2}{q} \cdot m + O(1).$$

For the variance, we follow an extension of the previous approach which is proposed for instance in [13, 21] in the framework of the study of additive costs associated with Euclidean algorithms for integers, when handling the expectation $\mathbb{E}_m[\phi^2]$ in order to produce an estimate concerning the variance. The cost ϕ^2 is written as

$$\phi^2 = 2 \sum_{i<j\leq L} \nu(A_i)(1 + \deg R_i) \cdot \nu(A_j)(1 + \deg R_j) + \sum_{i \leq L} \nu(A_i)^2 (1 + \deg R_i)^2.$$

We will distinguish two cases, namely pairs $i < j$, then pairs $i = j$.

Non-diagonal terms. We first fix a length L and consider for any pair $i < j \leq L$ an intermediate cost of the form

$$\nu(A_i) \cdot u^{1+\deg R_i} \cdot \nu(A_j) \cdot v^{1+\deg R_j},$$

whose generating function on the class $\Omega^{[L]} = \mathcal{G}^L \times \mathcal{U}$ is equal to

$$G^{i-1}(z) \cdot S_{(\nu)}(z) \cdot u \cdot G^{j-i-1}(uz) \cdot S_{(\nu)}(uz) \cdot v \cdot G^{L-j}(uvz) \cdot U(uvz).$$

Taking the sum over all the indices (i, j, L) with $1 \leq i < j \leq L$ gives

$$\frac{1}{1-G(z)} \cdot S_{(\nu)}(z) \cdot \frac{u}{1-G(uz)} \cdot S_{(\nu)}(uz) \cdot \frac{v}{1-G(uvz)} \cdot U(uvz).$$

Then, the cumulative generating function of the part of the cost ϕ^2 relative to the pairs $i \neq j$ is obtained by taking the derivative with respect to u and v at $u = 1$ and $v = 1$, and then by multiplying by 2. Its general term in $[z^m]$ satisfies

$$\frac{(q-1)^2}{q^2} \cdot q^{2m} m^4 + \frac{2}{3q^2}(q-6)(q-1) \cdot m^3 q^{2m} + O(m^2).$$

Diagonal terms. For the diagonal pairs $i = j$, we consider the cost $\nu^2(A_i) \cdot u^{1+\deg R_i}$ on the class $\Omega^{[L]}$, for $1 \leq i \leq L$, and we take the sum over all the pairs (i, L) with $i \leq L$, that is,

$$\frac{1}{1-G(z)} \cdot S_{(\nu^2)}(z) \cdot u \cdot \frac{1}{1-G(uz)} \cdot U(uz).$$

Then, the cumulative generating function of the part of the cost ϕ^2 relative to the pairs $i = j$ is obtained by taking the sum of the first derivative and the second derivative of the previous expression with respect to u at $u = 1$, and its general term in $[z^m]$ satisfies

$$\frac{2}{3q^2}(2q+1)(q-1) \cdot m^3 q^{2m} + O(m^2 q^{2m}).$$

We deduce that

$$\mathbb{V}_m[\phi] = \frac{2(q-1)}{3q^2} \cdot m^3 + O(m^2).$$

Lastly, (13) is a direct consequence of Chebyshev inequality.

□

3.2. **Asymptotic Gaussian law for the total fine complexity.** The asymptotic normal laws for costs ϕ or $\underline{\phi}$ seem to be more difficult to obtain. Nevertheless the total fine complexity $\phi + \underline{\phi}$ can be proven to be asymptotically Gaussian.

Theorem 4. *On the set Ω, the cost $\phi + \underline{\phi}$ is asymptotically Gaussian.*

We will prove below that the cost $\phi + \underline{\phi}$ decomposes as the sum of several costs. The main part will be provided by the cost $X := N(P, \overline{Q}) \cdot \deg Q$, which is asymptotically Gaussian, according to Theorem 2. We then will prove that the other terms are asymptotically more concentrated, that is, their respective variances are negligible with respect to the variance of X. The proof of Theorem 4 then relies on the following result.

Proposition 1. [13] *Two costs X, Z defined on Ω are said to be variance equivalent with order $1/n$ if $\mathbb{V}_n[X - Z] = 1/n \cdot (\mathbb{V}_n[X])$ when n tends to ∞. We assume furthermore that X admits an asymptotic Gaussian law. Then Z admits also an asymptotic Gaussian law with a variance that satisfies*

$$\mathbb{V}_n[Z] = \mathbb{V}_n[X] \cdot (1 + O(\sqrt{1/n})).$$

Proof. Let us prove now Theorem 4. One has, according to Definition 1,

$$(\phi + \underline{\phi})(P, Q) = \sum_{k=1}^{\ell-1} \nu(A_k) \cdot (2 + \deg Q_{k-1} + \deg R_k) + \nu(A_\ell)(1 + \deg R_\ell),$$

with $\ell = L(P,Q)$. Consequently

$$(\phi + \underline{\phi})(P,Q) = \sum_{k=1}^{\ell} \nu(A_k) \cdot (2 + \deg Q_{k-1} + \deg R_k) - \nu(A_\ell)(1 + \deg Q_{\ell-1}).$$

The equality $\deg Q_{k-1} + \deg R_k = \deg Q - \deg A_k$ entails the relation

$$(\phi + \underline{\phi})(P,Q) = N(P,Q) \cdot \deg Q + 2N(P,Q) - \sum_{k=1}^{\ell} \nu(A_k) \cdot \deg A_k - \nu(A_\ell)(1 + \deg Q_{\ell-1}).$$

The conclusion of the theorem follows from Proposition 1 applied to $X = N(P,Q) \cdot \deg Q$ by noticing that $\mathbb{V}_m[N(P,Q) \cdot \deg Q] = \Omega(m^3)$, and then successively to the terms of

$$Z - X = 2N(P,Q) - \sum_{k=1}^{\ell} \nu(A_k) \cdot \deg A_k - \nu(A_\ell)(1 + \deg Q_{\ell-1}),$$

by proving that their respective variance is in $O(m^2)$ (or even in $O(m)$).

- We first consider the main term which corresponds to the cost $X = N(P,Q) \cdot \deg Q$. The variance of X is equal to $m^2 \mathbb{V}_m(N)$, that is, by Theorem 1
$$\mathbb{V}_m(X) = m^2 \cdot \mathbb{V}_m[N] = m^3 \cdot 2(q-1)/q^2 + O(m^2).$$
Furthermore, the asymptotic Gaussian law holds for N (Theorem 2), which implies the asymptotic Gaussian law for X.
- We recall from Theorem 1 that $\mathbb{V}_m[N] = O(m)$.
- We then consider the additive cost associated with the cost $\nu(A) \cdot \deg A$. By noticing that $\nu(A) \cdot \deg A \leq (1 + \deg A)^2$, we get
$$\begin{aligned} \mathbb{V}_m\left[\textstyle\sum_{k=1}^{\ell} \nu(A_k) \cdot \deg A_k\right] &\leq \mathbb{E}_m\left[\textstyle\sum_{i,j \leq \ell} \nu(A_i) \cdot \deg A_i \cdot \nu(A_j) \cdot \deg A_j\right] \\ &\leq \mathbb{E}_m\left[\textstyle\sum_{i,j \leq \ell} (1 + \deg A_i)^2 \cdot (1 + \deg A_j)^2\right] \\ &= 2\,\mathbb{E}_m\left[\textstyle\sum_{i<j \leq \ell} (1 + \deg A_i)^2 \cdot (1 + \deg A_j)^2\right] + \\ &\quad + \mathbb{E}_m\left[\textstyle\sum_{i \leq \ell} (1 + \deg A_i)^4\right]. \end{aligned}$$
Similarly as in the proof of Theorem 3, if we fix a length $\ell \geq 1$, the generating function corresponding to the pairs $i \neq j$ is
$$G^{i-1} \cdot S_{(d^2)}(z) \cdot G^{j-i-1} \cdot S_{(d^2)}(z) \cdot G^{\ell-j} \cdot U(z).$$
Taking the sum overall the indices $1 \leq i < j \leq \ell$ yields the generating function
$$\left(\frac{1}{1 - G(z)}\right)^3 \cdot (S_{(d^2)}(z))^2 \cdot U(z).$$
Similarly, the cumulative generating function corresponding to the diagonal pairs $i = j$ is
$$\left(\frac{1}{1 - G(z)}\right)^2 \cdot S_{(d^4)}(z) \cdot U(z).$$
In the first case, the expectation is in $O(m^2)$, and in the second case, it is in $O(m)$.
- Finally, it remains to consider the cost $= \nu(A_l)(1 + \deg Q_{l-1})$. One has
$$\mathbb{V}_m[\nu(A_\ell)(1 + \deg Q_{l-1})] \leq \mathbb{E}_m\left[(\nu(A_l)(1 + \deg Q_{l-1}))^2\right] \leq m^2 \cdot \mathbb{E}_m[\nu^2(A_\ell)].$$
Similarly as in the proof of Theorem 3, if we fix a length $\ell \geq 1$, the generating function of the cost $\nu^2(A_\ell)$ is
$$G^{\ell-1} \cdot S_{(\nu^2)}(z) \cdot U(z).$$
Taking the sum over $\ell \geq 1$ yields the generating function
$$\frac{1}{1 - G(z)} \cdot S_{(\nu^2)}(z) \cdot U(z),$$

wich provides $\mathbb{E}_m[\nu^2(A_\ell)] = O(1)$ and $\mathbb{V}_m[\nu(A_\ell)(1+\deg Q_{\ell-1})] = O(m^2)$.

□

4. Study of the main cost functions of interest in the continuous model

We now consider the continuous model, that is, $\mathbb{L}$ endowed with the Haar measure $\mu_{\mathbb{L}}$, together with the costs N_n and $\underline{\phi_n}$ related to truncated trajectories $\mathcal{T}_n(f)$ under the action of the Gauss map, with

$$\mathcal{T}_n(f) = (f, T(f), \cdots, Tn(f)).$$

In particular, we are interested in the behavior of the random variable ν that counts the number of non-zero coefficients in partial quotients.

4.1. The Gauss map and the topology of the set $\mathbb{L}$.

We first need preliminary results concerning the behavior of the Gauss map with respect to cylinders (see Definition 4 below). These results will also be used in Section 5.3.

Recall that, for $f \in \mathbb{F}_q((X^{-1}))$, the degree is equal to the opposite of the valuation of the series f, namely,

$$\deg f = -m \qquad \text{if and only if} \quad f = b_m X^{-m}\left(1 + \frac{1}{X}\cdot g\right) \quad \text{with} \quad b_{-m} \neq 0, \quad \deg g \leq 0.$$

We also recall that the notation $\mathbb{L}$ stands for the subset of $\mathbb{F}_q((X^{-1}))$ formed with elements f with $\deg f < 0$, and, for $m \geq 1$, we set

$$\mathbb{L}_m := \{f \in \mathbb{L} : \deg f = -m\}.$$

We now want to get a simple expression of the Gauss map $T\colon \mathbb{L} \to \mathbb{L}$, $f \mapsto \frac{1}{f} - \left[\frac{1}{f}\right]$ ($[\cdot]$ stands for the polynomial part for formal power series) (see Proposition 2 below). For that purpose, we introduce the following notation.

We fix $\ell \geq 1$. For an element $f \in \mathbb{F}_q((X^{-1}))$, let $\pi = (\pi_0, \pi_1, \dots \pi_{\ell-1})$ be the element of $\mathbb{F}_q^\ell$ which defines, together with the dominant coefficient $\gamma(f)$, the 'beginning' of f (of length ℓ) formed with the part of f with indices $-k \in [\deg f, \deg f + \ell]$. Note that π depends on f and ℓ. More precisely, if $m = -\deg f$ ($m \geq 1$), then f can be written in the form

$$f = \gamma(f) X^{-m}\left(1 + \frac{1}{X}\cdot \underline{\pi}\left(\frac{1}{X}\right)\right) + X^{-(m+\ell+1)} g, \qquad \deg g \leq 0, \tag{15}$$

where $\underline{\pi}$ is the polynomial of degree at most $\ell - 1$ related to π,

$$\underline{\pi}(X) = \pi_0 + \pi_1 X + \dots \pi_{\ell-1} X^{\ell-1}.$$

When f decomposes as in (15), its inverse $1/f$ satisfies

$$\frac{1}{f} = \frac{X^m}{\gamma(f)}\left(\frac{1}{1 + \frac{1}{X}\cdot \underline{\pi}\left(\frac{1}{X}\right)}\right) + X^{m-\ell-1} h, \qquad \text{with} \quad \deg h \leq 0.$$

Then the 'beginning part' of $1/f$ formed with its terms of index $k \in [m, m-\ell]$ only involves the powers $\underline{\pi}^k$ of the polynomial $\underline{\pi}$, with exponents $k \leq \ell$, and more precisely the polynomials $\underline{\pi}^{[k]} := \underline{\pi}^k \mod X^{\ell-k}$, i.e.,

$$\frac{1}{f} = \frac{X^m}{\gamma(f)}\left(1 + \sum_{k=1}^{\ell} (-1)^k X^{-k} \cdot \underline{\pi}^{[k]}(1/X)\right) + X^{m-\ell-1} h.$$

Note that the beginning part of $1/f$ formed with the terms with power $k \in [m, m-\ell]$ only depends on the pair $(\gamma(f), \pi(f))$. Hence, with $\pi \in \mathbb{F}_q^\ell$, we associate $\theta \in \mathbb{F}_q^\ell$ via its polynomial $\underline{\theta}$, which is itself defined as

$$X\underline{\theta}(X) = \sum_{k=1}^{\ell} (-1)^k \; X^k \cdot \underline{\pi}^{[k]}(X).$$

For each ℓ, the map

$$\psi\colon \mathbb{F}_q^\ell \to \mathbb{F}_q^\ell, \quad \pi \mapsto \theta$$

defines an involutive bijection of $\mathbb{F}_q^\ell$ onto itself. In particular, one has $\psi(0^\ell) = 0^\ell$.

There is a precise relation between the polynomial $[1/f]$ and the sequence π defined in (15) for $\ell = m = -\deg f$. When f decomposes as in (15), the integer part $[1/f]$ is completely defined by the sequence $\psi(\pi)$, namely,

$$\left[\frac{1}{f}\right] = \frac{X^m}{\gamma(f)}\left(1 + \left(\frac{1}{X}\right)\psi(\pi)\left(\frac{1}{X}\right)\right).$$

Definition 4 (Cylinders)**.** *For $a \in \mathbb{F}_q^\star$, and for a sequence $\pi \in \mathbb{F}_q^\ell$, we consider the cylinder $E_{[-m,a,\pi]}$ which gathers the elements $f \in \mathbb{L}_m$ which are written as in (15), with $\gamma(f) = a$.*

The set $\mathbb{L}_m$ is the union of all the cylinders $E_{[-m,a,\pi]}$, when a varies in $\mathbb{F}_q^\star$, π describes the set $\mathbb{F}_q^\ell$, and ℓ takes all values larger than or equal to 1. Moreover the measure of each cylinder is equal to $q^{-(m+\ell)}$, and the measure of $\mathbb{L}_m$ equals $(q-1)q^{-m}$.

Proposition 2. *For each $m \geq 1$, the mapping defined on $\mathbb{L}_m$ with values in $\mathbb{F}_q^\star \times \mathbb{F}_q^m$ which associates with f the polynomial $[1/f]$ is a surjection which is constant on each cylinder $E_{[-m,a,\pi]}$ with $\pi \in \mathbb{F}_q^m$ and $a \in \mathbb{F}_q^\star$.*

Proof. It is a direct consequence of the equivalence

$$f \in E_{[-m,a,\pi]} \iff \frac{1}{f} \in E_{[m,1/a,\psi(\pi)]}. \tag{16}$$

□

4.2. **Study of cost N_n.** The cost N_n is defined as $N_n(f) = \sum_{k=1}^n \nu\left(\left[\frac{1}{T^{k-1}(f)}\right]\right)$. If we now define $\underline{\nu}$ on $\mathbb{L}$ by

$$\underline{\nu}(f) := \nu([1/f]), \tag{17}$$

the cost N_n is defined as

$$N_n(f) = \sum_{k=1}^n \underline{\nu}(T^{k-1}f),$$

and this is just the total cost of the truncated trajectory $\mathcal{T}_n(f) = \{f, T(f), \cdots, T^n(f)\}$ related to the basic cost $\underline{\nu}$.

Theorem 5. *For $\mu_{\mathbb{L}}$-a.e. f, one has*

$$\lim_{n\to\infty} \frac{1}{n} N_n(f) = 2, \qquad \lim_{n\to\infty} \frac{1}{n} \deg Q_n(f) = \frac{q}{q-1}, \qquad \lim_{n\to\infty} \frac{N_n}{\deg Q_n}(f) = 2 \cdot \frac{q-1}{q}.$$

Proof. With Proposition 2, and for each $m \geq 1$, the distribution of $\underline{\nu} - 1$ on $\mathbb{L}_m$ is the same as the distribution of ν on $\mathbb{F}_q^m$ which is a binomial distribution. In particular the expectation of ν on $\mathbb{F}_q^m$ equals $m(q-1)/q$. Then, the expectations of $\underline{\nu} - 1$ and $\underline{\nu}$ on $\mathbb{L}$ satisfy

$$\mathbb{E}[\underline{\nu} - 1] = \sum_{m\geq 1} \frac{q-1}{q^m} m \frac{q-1}{q} = 1, \qquad \mathbb{E}[\underline{\nu}] = 2.$$

Remark that the expectation of $-\deg$ on $\mathbb{L}$ equals (see also [2])

$$\mathbb{E}[-\deg] = \sum_{m\geq 1} \frac{q-1}{q^m} m = \frac{q-1}{q}.$$

Then the ergodic theorem applied to the two functions $\nu - 1$ and deg yields the result.

□

4.3. **Fine bit-complexity.** We now consider the fine bit complexity ϕ_n relative to the computation of the n-th convergent of an element of $\mathbb{L}$ defined as

$$\underline{\phi}_n(f) = \sum_{k=1}^{n} \nu(A_k) \cdot (1 + \deg Q_{k-1}).$$

It can also be expressed with the degrees of the quotient A_j as

$$\underline{\phi}_n(f) = \sum_{k=1}^{n} \nu(A_k) \cdot \left(1 + \sum_{j=1}^{k-1} \deg A_j\right) = \sum_{k=1}^{n} \nu(A_k) + \sum_{k=1}^{n} \nu(A_k) \sum_{j=1}^{k-1} \deg A_j.$$

Then, we apply the following result:

Proposition 3. *Let (V_n) and (W_n) be stationary and ergodic sequences of non-negative valued random variables on a probability space $(\Omega, \mathcal{F}, P)$ with finite expectations μ_V and μ_W, respectively. For P-a.e. $\omega \in \Omega$, we have*

$$\lim_{N\to\infty} \frac{1}{N^2} \sum_{k=1}^{N} V_k \sum_{j=k+1}^{N} W_j = \frac{1}{2}\mu_V \mu_W.$$

Proof. Let us fix $\varepsilon > 0$. From the individual ergodic theorem, there exists a positive integer M_0 such that for any integer $M \geq M_0$, the following holds:

$$\left|\frac{1}{M}\sum_{i=1}^{M} V_i - \mu_V\right| < \varepsilon, \qquad \left|\frac{1}{M}\sum_{i=1}^{M} W_i - \mu_W\right| < \varepsilon.$$

Let $N \geq M_0$ be a positive integer. One has

$$\sum_{t=1}^{N} V_t \sum_{s=1}^{t} W_s = \sum_{t=1}^{M_0-1} V_t \sum_{s=1}^{t} W_s + \sum_{t=M_0}^{N} V_t \sum_{s=1}^{t} W_s.$$

We take now N large enough (with $N \geq M_0$) for

$$\left|\frac{1}{N}\sum_{t=1}^{M_0-1} V_t\right| \leq \varepsilon \quad \text{and} \quad \left|\frac{1}{N^2}\sum_{t=1}^{M_0-1} V_t \sum_{s=1}^{t} W_s\right| \leq \varepsilon. \tag{18}$$

For $t \geq M_0$, one has

$$t\,(\mu_W - \varepsilon) \leq \sum_{s=1}^{t} W_s \leq t\,(\mu_W + \varepsilon).$$

Since the random variables take non-negative values, one gets

$$(\sum_{t=M_0}^{N} tV_t)(\mu_W - \varepsilon) \leq \sum_{t=M_0}^{N} V_t \sum_{s=1}^{t} W_s \leq (\sum_{t=M_0}^{N} tV_t)(\mu_W + \varepsilon). \tag{19}$$

By applying Abel's transform, one gets

$$\sum_{t=1}^{N} tV_t = N(\sum_{t=1}^{N} V_t) - \sum_{t=1}^{N-1}\sum_{s=1}^{t} V_s.$$

One has

$$N(\mu_v - \varepsilon) \leq \sum_{t=1}^{N} V_t \leq N(\mu_v + \varepsilon).$$

We also take N large enough (with $N \geq M_0$) for

$$0 \leq \sum_{t=1}^{M_0-1}\sum_{s=0}^{t} V_s \leq N^2\varepsilon \quad \text{and} \quad 0 \leq \sum_{t=1}^{M_0-1} tV_t \leq N^2\varepsilon.$$

Hence we get

$$\frac{(N-1)^2-M_0^2}{2}(\mu_v-\varepsilon)\leq\sum_{t=M_0}^{N-1}\sum_{s=1}^{t}V_s\leq\sum_{t=1}^{N-1}\sum_{s=1}^{t}V_s\leq\frac{N(N-1)}{2}(\mu_v+\varepsilon)-N^2\varepsilon.$$

This yields that

$$N^2\varepsilon-\frac{(N-1)^2-M_0^2}{2}(\mu_v+\varepsilon)+N^2(\mu_v-\varepsilon)\leq\sum_{t=1}^{N}tV_t\leq N^2(\mu_v+\varepsilon)-\frac{(N-1)^2-M_0^2}{2}(\mu_v-\varepsilon).$$

Since $\sum_{t=1}^{N}tV_t-N^2\varepsilon\leq\sum_{t=M_0}^{N}tV_t\leq\sum_{t=1}^{N}tV_t$, this yields, together with (18) and (19), that

$$\lim_{N\to\infty}\frac{1}{N^2}\sum_{t=1}^{N}V_k\sum_{s=1}^{t}W_s=\frac{1}{2}\mu_V\mu_W.$$

We then conclude by noticing that

$$\lim_{N\to\infty}\frac{1}{N^2}\sum_{k=1}^{N}V_k\sum_{j=1}^{k}W_j+\lim_{N\to\infty}\frac{1}{N^2}\sum_{k=1}^{N}V_k\sum_{j=k+1}^{N}W_j=\lim_{N\to\infty}\frac{1}{N^2}\left(\sum_{k=1}^{N}V_k\right)\left(\sum_{j=1}^{N}W_j\right)=\mu_W\mu_V.$$

. □

Applying Proposition 3 to the sequences $V_k=\nu(A_k)$ (of non-zero coefficients of A_n) and $W_k=\deg A_k$ with respective expectations 2 and $q/q-1$ (by Theorem 5) leads to the result:

Theorem 6. *For $\mu_{\mathbb{L}}$-a.e. $f\in\mathbb{L}$, we have*

$$\lim_{n\to\infty}\frac{1}{n^2}\underline{\phi}_n(f)=\frac{q}{q-1},\qquad\lim_{n\to\infty}\frac{1}{(\deg Q_n(f))^2}\cdot\underline{\phi}_n(f)=\frac{q-1}{q}.$$

This result has to be compared to Theorem 3 to confirm the parallelism of the results in the discrete model and in the continuous one. The following corollary is deduced from the fact that a.e. convergence implies convergence in probability:

Corollary 1. *For any $\varepsilon>0$ and $\eta>0$, there exists a positive integer n_0 such that for any $n\geq n_0$ we have*

$$\mu_{\mathbb{L}}\{f\in\mathbb{L}:\left|\frac{1}{(\deg Q_n(f))^2}\cdot\underline{\phi}_n(f)-\frac{q-1}{q}\right|>\varepsilon\}<\eta.$$

The previous results confirm the analogy between the behavior of generic truncated trajectories and rational trajectories. Furthermore, we can also consider the costs applied to the pair of polynomials (P_n,Q_n). More precisely, for $f\in\mathbb{L}$, let $\widehat{P_n}:=\frac{P_n}{\gamma(P_n)}$ and $\widehat{Q_n}:=\frac{Q_n}{\gamma(Q_n)}$ for $n\geq1$. We have $\widehat{Q_n}$ monic and $(\widehat{P_n},\widehat{Q_n})\in\Omega_m$ with $\deg(\widehat{Q_n})=m$. One has

$$\underline{\phi}(\widehat{P_n},\widehat{Q_n})=\underline{\phi_n}(f).$$

One proves similarly as previously the following results concerning $\phi(\widehat{P_n},\widehat{Q_n})$ by noticing that $\widehat{P_n}$ and $\widehat{Q_n}$ are coprime.

Theorem 7. *For $\mu_{\mathbb{L}}$-a.e. $f\in\mathbb{L}$, we have*

$$\lim_{n\to\infty}\frac{1}{n^2}\phi(\widehat{P_n},\widehat{Q_n})=\frac{q}{q-1},\qquad lim_{n\to\infty}\frac{1}{(\deg Q_n(f))^2}\cdot\phi(\widehat{P_n},\widehat{Q_n})=\frac{q-1}{q}.$$

Corollary 2. *For any $\varepsilon>0$ and $\eta>0$, there exists a positive integer n_0 such that for any $n\geq n_0$ we have*

$$\mu\left(\{f\in\mathbb{L}:\left|\frac{1}{(\deg Q_n(f))^2}\cdot\phi(\widehat{P_n},\widehat{Q_n})-\frac{q-1}{q}\right|>\varepsilon\}\right)<1-\eta.$$

Remark 2. The analogy between the discrete and the continuous models can also be illustrated as follows. For any fixed polynomial A in $\mathcal{G}$ and for any fixed $i \geq 1$, one has

$$\frac{1}{q^{2m}} \cdot |\{(P,Q) \in \Omega_m \,:\, A_i(P,Q) = A\}| \to_{m\to\infty} \mu_{\mathbb{L}}(\{f \in \mathbb{L} \,:\, A_i(f) = A\}),$$

that is, for a.e. $f \in \mathbb{L}$,

$$A_i(f) = \lim_{m\to\infty} \mathbb{P}_m[A_i(P,Q) = A].$$

Indeed, $\{f \in \mathbb{L} \,:\, A_i(f) = A\} = T^{-i+1}(\{f \in \mathbb{L} \,:\, A_1(f) = A\})$. By T-invariance of the Haar measure, one has $\mu_{\mathbb{L}}(T^{-i+1}(\{f \in \mathbb{L} \,:\, A_1(f) = A\})) = q^{2\deg(A)}$. Now, we take the cost $c_{i,A}$ defined on Ω as follows: $c_{i,A}(P,Q) = 1$ if and only if $A_i(P,Q) = A$. The corresponding cumulative generating function is

$$\frac{1}{1-G(z)} \cdot z^{\deg(A)} \cdot U(z) = T_\Omega(z) \cdot z^{\deg(A)},$$

which yields that $\mathbb{E}_m[c_{i,A}] = \frac{1}{q^{2m}} \cdot |\{(P,Q) \in \Omega_m \,:\, A_i(P,Q) = A\}| = \frac{1}{q^{2\deg(A)}}$.

5. Farey maps

The aim of this section is to relate the function $\underline{\nu}$ with a Farey type algorithm: this algorithm can be considered as a refinement of the continued fraction algorithm; it discovers step by step each non-zero monomial of partial quotients; its number of steps is thus closely related to the parameter $\underline{\nu}$. More precisely, we will consider two Farey algorithms (see Section 5.2 and 5.3) because of the particular role played by the constant term of polynomial terms.

5.1. **General Farey maps.** In the number case (see e.g. [5]), the Farey map is defined on the unit interval as

$$F_{\mathbb{R}}(x) = \begin{cases} \dfrac{x}{1-x} & 0 \leq x \leq \frac{1}{2} \\ \dfrac{1-x}{x} & \frac{1}{2} < x \leq 1. \end{cases}$$

It satisfies $F_{\mathbb{R}}[0,1/2] = F_{\mathbb{R}}(1/2,1] = [0,1]$: the map $F_{\mathbb{R}}$ is complete on each of its two branches. If we denote, for $x \in (0,\,1)$, by $t(x)$ the first time where x leaves the interval $(\frac{1}{2},1]$ to enter the interval $[0,1/2]$, namely

$$t(x) = \min\{n \geq 1 \,:\, F_{\mathbb{R}}^{n-1}(x) \in (\frac{1}{2},1]\},$$

we obtain

$$F_{\mathbb{R}}^{t(x)}(x) = \frac{1}{x} - \left[\frac{1}{x}\right]$$

which is the Gauss map (in the number case). Furthermore, the equality $j(x) = [1/x]$ holds, and shows that the number of steps $j(x)$ performed by $F_{\mathbb{R}}$ is equal to the partial quotient $[1/x]$: the Farey map $F_{\mathbb{R}}$ goes $[1/x]-1$ times through the first branch defined on $[0,1/2]$, and goes through the second branch only during the last step.

There are two possibilities for defining a Farey map on $\mathbb{F}_q((X^{-1}))$ according to the way the constant term of the polynomial $[1/f]$ is handled (see Section 5.2 and 5.3 below for more details). Note that the set $\mathbb{L}$ on which the Gauss map T is naturally defined does not contain series with non-zero constant terms. We thus will work with the two following subsets of $\mathbb{F}_q((X^{-1}))$

$$\mathbb{J} = \{f \in \mathbb{F}_q((X^{-1})) \,:\, \deg f \leq 0\}, \quad \mathbb{L} = \{f \in \mathbb{F}_q((X^{-1})) \,:\, \deg f < 0\}$$

with their respective normalized Haar measures $\mu_{\mathbb{J}}$ and $\mu_{\mathbb{L}}$ (both sets are compact abelian groups with respect to the addition law '+') which are related by

$$\mu_{\mathbb{L}}(A) = q \cdot \mu_{\mathbb{J}}(A)$$

for any Borel subset A of $\mathbb{L}$. Their difference set $\mathbb{J} \setminus \mathbb{L}$ is the subset $\mathbb{J}^{(0)}$ defined as

$$\mathbb{J}^{(0)} = \{f \in \mathbb{F}_q((X^{-1})) \,:\, \deg f = 0\}$$

which is of positive measure in $\mathbb{J}$.

Remark 3. The situation is different in the real case, since the counterparts of $\mathbb{J}$, namely the interval $[0,1]$, and of $\mathbb{L}$, the interval $[0,1)$, differ from a subset of zero measure. Here, the Gauss map T could be defined on $\mathbb{J}$, but $T(\mathbb{J}) = \mathbb{L}$. This is one of the reasons that makes us work with $\mathbb{J}$ and $\mathbb{L}$.

5.2. **Farey map on $\mathbb{J}$.** We first define a map $F_{\mathbb{J}}$, defined on $\mathbb{J}$, which handles constant monomials as other monomials, and that thus counts them. As its real counterpart $F_{\mathbb{R}}$, it has two branches, defined on two subsets denoted as $\mathbb{J}_1$ and $\mathbb{J}_2$: the choice of the branch depends on whether the number $\underline{\nu}(f) = \mu([1/f])$ of non-zero monomials which remain to be computed in the polynomial $[1/f]$ is yet larger than 1, or equal to 1.

We use here the notation of Section 4.1. The Farey map $F_{\mathbb{J}}$ discovers the monomials of $[1/f]$ one by one. The first one is the monomial $(1/\gamma(f))X^{-\deg f}$, and when we subtract this monomial to $1/f$, we obtain the series

$$G(f) = \frac{1}{f} - \frac{X^{-\deg f}}{\gamma(f)}, \tag{20}$$

with $\gamma(f)$ being the dominant coefficient of f, and there are two possibilities for $\deg G(f)$. Indeed, if $\deg G(f) \geq 0$, the quotient $[1/f]$ is not completely computed, and we continue the computation with $1/G(f)$. In this case, the quotient $[1/f]$ contains at least two monomials, and thus $\underline{\nu}(f) \geq 2$. Otherwise, if $\deg G(f) < 0$, the quotient $[1/f]$ is complete; this means that $\underline{\nu}(f) = 1$, and we apply the map T for computing the following quotient. We thus let:

$$\mathbb{J}_1 := \{f \in \mathbb{J} : \ \underline{\nu}(f) \geq 2\} = \{f \in \mathbb{J} : \ \deg G(f) \geq 0\}$$

$$\mathbb{J}_2 := \{f \in \mathbb{J} : \ \underline{\nu}(f) = 1\} = \{f \in \mathbb{J} : \ \deg G(f) < 0\}$$

$$F(f) = \begin{cases} \dfrac{1}{G(f)} & \text{if} \quad \deg G(f) \geq 0 \\ \dfrac{1}{f} - \left[\dfrac{1}{f}\right] & \text{if} \quad \deg G(f) < 0. \end{cases}$$

Proposition 4. *Let $f \in \mathbb{J}$. We set*

$$t(f) = \min\left\{i \geq 1 \ : \ F_{\mathbb{J}}^{i-1}(f) \in \mathbb{J}_2\right\}$$

the first time when the trajectory of f under the map F leaves the set $\mathbb{J}_1$ to enter the set $\mathbb{J}_2$. Then, $t(f)$ equals the number of non-zero monomials contained in the polynomial $[1/f]$.

5.3. **Farey map on $\mathbb{L}$.** The relation

$$F_{\mathbb{J}}^{t(f)}(f) = T(f) = \frac{1}{f} - \left[\frac{1}{f}\right],$$

together with the fact that T is Haar measure preserving (i.e., $\mu_{\mathbb{L}}$-invariant), prove that $F_{\mathbb{J}}$ has an absolutely continuous invariant measure with respect to $\mu_{\mathbb{J}}$, which is ergodic. This measure will be denoted as $\widehat{\mu}_J$. Indeed, this follows from the fact that an invariant measure for a jump transformation gives an invariant measure for the original transformation, and the ergodicity of these two transformations are equivalent to each other (see [16]). However, this measure is not equal to $\mu_{\mathbb{J}}$ since

$$\mu_{\mathbb{J}}(\mathbb{J}^{(0)}) = \frac{q-1}{q}, \quad F_{\mathbb{J}}^{-1}(\mathbb{J}^{(0)}) \subsetneq \mathbb{L}, \quad \text{and} \quad \mu_{\mathbb{J}}(\mathbb{L}) = \frac{1}{q}.$$

The map $F_{\mathbb{J}}$ is thus not $\mu_{\mathbb{J}}$-preserving. In order to give an explicit expression for the ergodic absolutely continuous invariant measure $\widehat{\mu}_{F_J}$ for $F_{\mathbb{J}}$ (see Theorem 2 below), we now introduce the induced map of $F_{\mathbb{J}}$ on $\mathbb{L}$, denoted as $F_{\mathbb{L}}$, for which $\mu_{\mathbb{L}}$ will be proved to be invariant (see Proposition 5). This will lead us to consider the constant term of the partial quotient in a separate way. Let us recall that that we have initially defined the map F on the set $\mathbb{J}$ (and not on its subset $\mathbb{L}$) because of the need to deal with the constant term (of zero degree) when producing in an additive way the monomials of $[1/f]$.

We now define another Farey map $F_{\mathbb{L}}$ on the set $\mathbb{L}$ as follows

$$F_{\mathbb{L}}(f) = \begin{cases} \dfrac{1}{G(f)} & \text{if} \quad \deg G(f) > 0 \\ \dfrac{1}{f} - \left[\dfrac{1}{f}\right] & \text{if} \quad \deg G(f) \leq 0. \end{cases}$$

Then,

$$F_{\mathbb{L}}(f) = \begin{cases} F_{\mathbb{J}}(f) & \text{if} \quad F_{\mathbb{J}}(f) \in \mathbb{L} \\ F_{\mathbb{J}}^2(f) & \text{if} \quad F_{\mathbb{J}}(f) \in \mathbb{J}^{(0)}. \end{cases}$$

One checks that $F_{\mathbb{L}}$ is the induced transformation of $F_{\mathbb{J}}$ to $\mathbb{L}$. Indeed, if $F_{\mathbb{J}}(f) \in \mathbb{J}^{(0)}$, with $f \in \mathbb{L}$, this implies that $F_{\mathbb{J}}(f) \in \mathbb{J}_2$, and $F_{\mathbb{J}}^2(f) = T(f) \in \mathbb{L}$.

As in the previous section, we then relate this map to the number $\widehat{\underline{\nu}}(f)$ of non-constant monomials in $[1/f]$ (the difference between $\widehat{\underline{\nu}}(f)$ and $\underline{\nu}(f)$ is that $\widehat{\underline{\nu}}(f)$ does not take into account the constant term of $[1/f]$). One has $\deg G(f) \leq 0$ if and only if there exists b in $\mathbb{F}_q$ such that $[1/f] = X^{-\deg f} + b$. This means $\widehat{\underline{\nu}}(f) = 1$. We then set

$$\mathbb{L}_1 := \{f \in \mathbb{L} \,:\, \deg G(f) > 0\} = \{f \in \mathbb{L} \,:\, \widehat{\underline{\nu}}(f) \geq 2\},$$

$$\mathbb{L}_2 := \{f \in \mathbb{L} \,:\, \deg G(f) \leq 0\} = \{f \in \mathbb{L} \,:\, \widehat{\underline{\nu}}(f) = 1\},$$

$$F_{1,\mathbb{L}}(f) = F_{\mathbb{L}}(f) = \frac{1}{G(f)} \quad \text{for} \quad f \in \mathbb{L}_1, \qquad F_{2,\mathbb{L}}(f) = F_{\mathbb{L}}(f) = \frac{1}{f} - \left[\frac{1}{f}\right] \quad \text{for} \quad f \in \mathbb{L}_2.$$

The map $F_{\mathbb{L}}$ is now related to $\widehat{\underline{\nu}}(f)$. We have also:

$$\mathbb{L}_2 = \bigcup_{i \geq 1} \bigcup_{a \in \mathbb{F}_q^*} \bigcup_{b \in \mathbb{F}_q} \{f \in \mathbb{L} \,:\, [1/f] = aX^i + b\}.$$

Proposition 5. *The map $F_{\mathbb{L}}$ is $\mu_{\mathbb{L}}$-preserving.*

To prove this proposition, we need Lemma 2 and 3 below which deal respectively with the two possible types of preimage of a given cylinder set (see Definition 4). We use here the notation of Section 4.1.

Lemma 2. *The measure of the inverse transform of any cylinder $E_{[-k,a,\pi]}$ (with $k \geq 0$) by the first branch $F_{1,\mathbb{L}}$ satisfies*

$$\mu_{\mathbb{L}}(F_{1,\mathbb{L}}^{-1}(E_{[-k,a,\pi]})) = \frac{1}{q+1} \cdot \mu_{\mathbb{L}}(E_{[-k,a,\pi]}), \quad \textit{for } k \geq 1,$$

$$\mu_{\mathbb{L}}(F_{1,\mathbb{L}}^{-1}(E_{[0,a,\pi]})) = \frac{q}{q+1} \cdot \mu_{\mathbb{J}}(E_{[0,a,\pi]}).$$

Proof. Observe first that, here, $E_{[-k,a,\pi]}$ is a cylinder of $\mathbb{L}$ or of $\mathbb{J}^{(0)}$, according to the value k.

Let $f \in \mathbb{L}_m$ with $\gamma(f) = b$ and $1/G(f) \in E_{[-k,a,\pi]}$, with $k \geq 0$ and $\pi \in \mathbb{F}_q^\ell$. Then, by (16), $G(f) \in E_{[k,1/a,\rho]}$ with $\rho = \psi(\pi)$, the inequality $m \geq k+1$ holds and

$$\begin{aligned} \frac{1}{f} &= \frac{X^m}{\gamma(f)} + G(f) = \frac{X^m}{b} + \frac{1}{a} X^k \left[1 + \left(\frac{1}{X}\right) \rho\left(\frac{1}{X}\right)\right] + X^{-(k+\ell+1)} g, \qquad \deg g \leq 0 \\ &= \frac{X^m}{b} \left[1 + \frac{b}{a} \left(\frac{1}{X}\right) \left(\frac{1}{X}\right)^{m-k-1} \left[1 + \left(\frac{1}{X}\right) \rho\left(\frac{1}{X}\right)\right]\right] + X^{-(k+\ell+1)} g. \end{aligned}$$

If we define the sequence θ via its polynomial $\underline{\theta}$ defined as

$$\underline{\theta}(X) = \frac{b}{a} X^{m-k-1} \left(1 + X \underline{\rho}(X)\right),$$

the sequence θ depends on ρ (and then on π) together with (m,b) and it belongs to $\mathbb{F}_q^{m-k+\ell}$. Furthermore, $1/f$ belongs to the cylinder $E_{[m,b,\theta]}$ and f belongs to the cylinder $E_{[-m,1/b,\psi^{-1}(\theta)]}$. Finally, we have proven that

$$F_{1,\mathbb{L}}^{-1}(E_{[-k,a,\pi]}) = \bigcup_{b\in\mathbb{F}_q^\star} \bigcup_{m=k+1}^{\infty} E_{[m,b,\psi^{-1}(\theta)]}$$

is a disjoint union of cylinders where the polynomials $\psi^{-1}(\theta)$ are of degree $m-k-1+\ell$. Since there are $q-1$ possible choices for $b\in\mathbb{F}_q$, we deduce that

$$\mu_{\mathbb{L}}\left(F_{1,\mathbb{L}}^{-1}(E_{[-k,a,\pi]})\right) = (q-1)\sum_{i=1}^{\infty}\frac{1}{q^{k+2i+\ell}} = \frac{q-1}{q^{k+\ell}}\cdot\frac{1}{q^2-1} = \frac{1}{q+1}\cdot\frac{1}{q^{k+\ell}}$$

which yields the assertion of the lemma. □

Remark 4. For any pair (a,π), the equality$F_{\mathbb{L}}^{-1}(E_{[0,a,\pi]}) = F_{1,\mathbb{L}}^{-1}(E_{[0,a\pi]})$ holds.

Lemma 3. *For $k\geq 1$, the measure of the inverse transform of any cylinder $E_{[-k,a,\pi]}$ by the first branch $F_{2,\mathbb{L}}$ satisfies*

$$\mu_{\mathbb{L}}(F_{2,\mathbb{L}}^{-1}(E_{[-k,c,\pi]})) = \frac{q}{q+1}\cdot\mu_{\mathbb{L}}(E_{[-k,c,\pi]}).$$

Proof. Recall that, in this case, there exist $i\geq 1$, $a,b\in\mathbb{F}_q$ with $a\neq 0$ such that $[1/f] = aX^i+b$. Let us fix $a\in\mathbb{F}_q^\star, b\in\mathbb{F}_q$ and $i\geq 1$. Then

$$\begin{aligned}\frac{1}{f} &= (aX^i+b) + \frac{X^{-k}}{c}\left[1+\left(\frac{1}{X}\right)\underline{\pi}\left(\frac{1}{X}\right)\right] + X^{-(k+\ell+1)}g, \qquad \deg g\leq 0\\ &= aX^i\left[1+\left(\frac{1}{X}\right)\left[\frac{b}{a}\left(\frac{1}{X}\right)^{i-1} + \frac{1}{ac}\left(\frac{1}{X}\right)^{k+i-1}\left(1+\left(\frac{1}{X}\right)\underline{\pi}\left(\frac{1}{X}\right)\right)\right]\right] + X^{-(k+\ell+1)}g.\end{aligned}$$

If we define the sequence θ via its polynomiall $\underline{\theta}$ as

$$\underline{\theta}(X) = \frac{b}{a}X^{i-1} + \frac{1}{ca}X^{k+i-1}\left(1+X\underline{\pi}(X)\right),$$

the sequence θ depends on (c,π) together with (i,a,b) and belongs to $\mathbb{F}_q^{k+i+\ell}$. Moreover, when (c,π,i) is fixed, the sequences θ associated with different values of the pair (a,b) are distinct. Furthermore, $1/f$ belongs to the cylinder $E_{[i,a,\theta]}$ and f belongs to the cylinder $E_{[-i,1/a,\psi(\theta)]}$. We thus have

$$F_{2,\mathbb{L}}^{-1}(E_{[-k,a;\pi]}) = \bigcup_{\substack{a\in\mathbb{F}_q^\star,\\ b\in\mathbb{F}_q}} \bigcup_{i=1}^{\infty} E_{[-i,1/a,\psi^{-1}(\theta)]}.$$

This is a disjoint union. Since there are $q-1$ possible choices for a and q possibilities for b, we deduce that

$$\mu_{\mathbb{L}}\left(F_{2,\mathbb{L}}^{-1}(E_{[-k,c,\pi]})\right) = q(q-1)\sum_{i=1}^{\infty}\frac{1}{q^{k+2i+\ell}} = \frac{q(q-1)}{q^{k+\ell}}\cdot\frac{1}{q^2-1} = \frac{q(q-1)}{q^2-1}\mu_{\mathbb{L}}(E_{[-k,c,\pi]})$$

which yields the assertion of the lemma. □

Proof. Let us prove Proposition 5. It is enough to show that

$$\mu_{\mathbb{L}}(F_{\mathbb{L}}^{-1}(E_{[k,a,\pi]})) = \mu_{\mathbb{L}}(E_{[k,a,\pi]})$$

for any cylinder set $E_{[k,a,\pi]}$ of $\mathbb{L}$. According to Lemma 2 and Lemma 3, we get

$$\mu_{\mathbb{L}}(F_{\mathbb{L}}^{-1}(E_{[k,a,\pi]})) = \frac{1}{q+1}\mu_{\mathbb{L}}(E_{[k,a,\pi]}) + \frac{q}{q+1}\mu_{\mathbb{L}}(E_{[k,a,\pi]}) = \mu_{\mathbb{L}}(E_{[k,a,\pi]}),$$

which shows the assertion of Proposition 5. □

5.4. **Metric theory of the Farey map $F_{\mathbb{J}}$.** So far, we have obtained the invariant measure for the induced map $F_{\mathbb{L}}$. We now want to give an explicit expression for the invariant measure of $F_{\mathbb{J}}$.

Remark 5. One has $F_{\mathbb{J}}^{-1}A = F_{\mathbb{L}}^{-1}A$ for any Borel subset A of $\mathbb{J}^{(0)}$. Lemma 2 implies

$$\mu_{\mathbb{L}}(F_{\mathbb{J}}^{-1}A) = q \cdot \mu_{\mathbb{J}}(A) \cdot \frac{1}{q+1}$$

for any Borel subset A of $\mathbb{J}^{(0)}$. In particular, we see that

$$\mu_{\mathbb{L}}(F_{\mathbb{J}}^{-1}\mathbb{J}^{(0)}) = \frac{q}{q+1} \cdot \mu_{\mathbb{J}}(\mathbb{J}^{(0)}) = \frac{q}{q+1}\frac{q-1}{q} = \frac{q-1}{q+1}.$$

Theorem 8. *Let $\widehat{\mu}_{\mathbb{J}}$ be the measure defined on $\mathbb{J}$ by*

$$\widehat{\mu}_{\mathbb{J}}(A) = \frac{q+1}{2q}\left(\mu_{\mathbb{L}}(A \cap \mathbb{L}) + \frac{q}{q+1}\mu_{\mathbb{J}}(A \cap \mathbb{J}^{(0)})\right)$$

for any Borel subset A of $\mathbb{J}$. The measure $\widehat{\mu}_{\mathbb{J}}$ is an invariant probability measure for $F_{\mathbb{J}}$. Furthermore, it is finite and the map $F_{\mathbb{J}}$ is ergodic w.r.t. $\widehat{\mu}_{F_{\mathbb{J}}}$. In particular, $\widehat{\mu}_{\mathbb{J}}(\mathbb{J}_2) = 1/2$.

Proof. Obviously $\frac{q+1}{2q}$ is the normalizing constant. Indeed one checks that

$$\widehat{\mu}_{\mathbb{J}}(\mathbb{J}) = \mu_{\mathbb{L}}(\mathbb{L}) + \frac{q}{q+1}\mu_{\mathbb{J}}(\mathbb{J}^{(0)}) = 1 + \frac{q}{q+1}\frac{q-1}{q} = \frac{2q}{q+1}.$$

It is thus enough to show that

$$\mu_{\mathbb{L}}(F_{\mathbb{J}}^{-1}A \cap \mathbb{L}) + \frac{q}{q+1}\mu_{\mathbb{J}}(F_{\mathbb{J}}^{-1}A \cap \mathbb{J}^{(0)}) = \mu_{\mathbb{L}}(A \cap \mathbb{L}) + \frac{q}{q+1}\mu_{\mathbb{J}}(A \cap \mathbb{J}^{(0)})$$

for any Borel subset A of $\mathbb{J}$.

Assume first $A \subset \mathbb{J}^{(0)}$. One has $F_{\mathbb{J}}^{-1}A = F_{1,\mathbb{J}}^{-1}A \subset \mathbb{L}$. Furthermore, $F_{\mathbb{J}}^{-1}A = F_{\mathbb{L}}^{-1}A$ (since $A \subset \mathbb{J}^{(0)}$). According to Remark 5, one gets $\mu_{\mathbb{L}}(F_{\mathbb{J}}^{-1}A) = q \cdot \mu_{\mathbb{J}}(A) \cdot \frac{1}{q+1}$. Hence

$$\mu_{\mathbb{L}}(F_{\mathbb{J}}^{-1}A \cap \mathbb{L}) + \frac{q}{q+1}\mu_{\mathbb{J}}(F_{\mathbb{J}}^{-1}A \cap \mathbb{J}^{(0)}) = \mu_{\mathbb{L}}(F_{\mathbb{J}}^{-1}A) = \frac{q}{q+1}\mu_{\mathbb{J}}(A) = \mu_{\mathbb{L}}(A \cap \mathbb{L}) + \frac{q}{q+1}\mu_{\mathbb{J}}(A \cap \mathbb{J}^{(0)}).$$

Suppose now that $A \subset \mathbb{L}$. In this case, we have, according to Remark 5

$$\begin{aligned} & \mu_{\mathbb{L}}(F_{\mathbb{J}}^{-1}A \cap \mathbb{L}) + \frac{q}{q+1}\mu_{\mathbb{J}}(F_{\mathbb{J}}^{-1}A \cap \mathbb{J}^{(0)}) \\ = \;& \mu_{\mathbb{L}}(F_{\mathbb{J}}^{-1}A \cap \mathbb{L}) + \mu_{\mathbb{L}}(F_{\mathbb{J}}^{-1}(F_{\mathbb{J}}^{-1}A \cap \mathbb{J}^{(0)})) \\ = \;& \mu_{\mathbb{L}}(F_{\mathbb{J}}^{-1}A \cap \mathbb{L}) + \mu_{\mathbb{L}}(F_{\mathbb{J}}^{-2}A \cap F_{\mathbb{J}}^{-1}\mathbb{J}^{(0)}) \end{aligned}$$

Since $(F_{\mathbb{J}}^{-1}A \cap \mathbb{L}) \cap F_{\mathbb{J}}^{-1}\mathbb{J}^{(0)} = \emptyset$, we have

$$\mu_{\mathbb{L}}(F_{\mathbb{J}}^{-1}A \cap \mathbb{L}) + \mu_{\mathbb{L}}(F_{\mathbb{J}}^{-2}A \cap F_{\mathbb{J}}^{-1}\mathbb{J}^{(0)}) = \mu_{\mathbb{L}}(F_{\mathbb{L}}^{-1}A) = \mu_{\mathbb{L}}(A)$$

which shows the desired assertion concerning the invariance of $\widehat{\mu}_{\mathbb{J}}$.

Let us prove now that $\widehat{\mu}_{\mathbb{J}}(\mathbb{J}_2) = 1/2$. We have

$$\mathbb{J}_2 = \mathbb{J}^{(0)} \cup (\mathbb{J}_2 \setminus \mathbb{J}^{(0)}) \qquad \text{with} \quad \mathbb{J}_2 \setminus \mathbb{J}^{(0)} = \bigcup_{m=1}^{\infty} \{f \in \mathbb{L}_m \,:\, \deg G(f) < 0\},$$

and $\widehat{\mu}_{\mathbb{J}}(\mathbb{J}^{(0)}) = (q-1)/(2q)$.
We now compute the the measure of each set $\{f \in \mathbb{L}_m \,:\, \deg G(f) < 0\}$. If $f \in \mathbb{L}_m$, with $\gamma(f) = a$ and $\deg G(f) < 0$, its inverse $1/f$ satisfies

$$\frac{1}{f} = \frac{X^m}{a} + G(f) \qquad \text{with} \quad \deg G(f) < 0$$

Then $1/f$ belongs to the cylinder $E_{[m,1/a,0^m]}$ whose measure equals q^{-2m}. Hence

$$\widehat{\mu}_{\mathbb{J}}(\mathbb{J}_2 \setminus \mathbb{J}^{(0)}) = \frac{q+1}{2q}\sum_{m=1}^{\infty}\frac{q-1}{q^{2m}} = \frac{1}{2q}.$$

□

Remark 6 (Non-zero coefficients of partial quotients)**.** Observe that we can use the previous results, and in particular the finiteness of the invariant measure $\widehat{\mu}_{\mathbb{J}}$, for recovering the estimate of Theorem 5 concerning the behavior of the total number of non-zero coefficients of partial quotients in the continued fraction expansion of f, that is, for $\mu_{\mathbb{L}}$-a.e. f, one has

$$\lim_{n\to\infty}\frac{1}{n}N_n(f)=2.$$

Indeed, consider the trajectory $\mathcal{Q}(f)$ of f under the action of $F_{\mathbb{J}}$, that is,

$$\mathcal{Q}(f)=(f,F_{\mathbb{J}}(f),F_{\mathbb{J}}^2(f),\dots,F_{\mathbb{J}}^n(f),\dots),$$

and let $\mathcal{Q}_m(f)=(f,F_{\mathbb{J}}(f),F_{\mathbb{J}}^2(f),\dots,F_{\mathbb{J}}^m(f))$.

We let denote by $t_1(f)$ the first time where the trajectory $\mathcal{Q}(f)$ of f under the action of $F_{\mathbb{J}}$ goes out of $\mathbb{J}_2$, that is,

$$t_1(f)=\min\{m\geq 1\,:\,F_{\mathbb{J}}^{m-1}(f)\in\mathbb{J}_2\},$$

and by $t_k(f)$ the k-th time where the trajectory $\mathcal{Q}(f)$ of f goes out of $\mathbb{J}_2$. One has

$$N_n(f)=\sum_{i=1}^{n}t_i(f).$$

Consider a fixed integer n, an integer m which belongs to the interval $[t_n(f),t_{n+1}(f)-1]$. Then, the trajectory $\mathcal{Q}_m(f)$ goes n times through $\mathbb{J}_2$ at times $N_1(f),N_2(f),\dots N_n(f)$, so that

$$n=\sum_{i=1}^{m}\mathbf{1}_{\mathbb{J}_2}({F_{\mathbb{J}}}^i f).$$

Because $F_{\mathbb{J}}$ is ergodic w.r.t. $\widehat{\mu}_{\mathbb{J}}$ and according to Theorem 5, we see that

$$\lim_{m\to\infty}\frac{n}{m}=\lim_{m\to\infty}\frac{1}{m}\sum_{i=1}^{m}\mathbf{1}_{\mathbb{J}_2}(F_{\mathbb{J}}^i f)=\mu_{F_{\mathbb{J}}}(\mathbb{J}_2)=1/2$$

for $\widehat{\mu}_{\mathbb{J}}$-a.e. f, which also means for $\mu_{\mathbb{L}}$-a.e. f. Finally, the inequality $N_n(f)\leq m<N_{n+1}(f)$ entails the equality $\lim_{m\to\infty}(1/n)N_n(f)=2$.

6. Appendix: Mediant convergents of formal power series

The aim of this section is to show that the map $F_{\mathbb{J}}$ produces the mediant convergents in the continued fraction expansion. For connections between the Farey map and mediant convergents in the classical case, see e.g. [11]. Let us first recall what is meant by mediant convergents in the classical case. Let x be an irrational number, $0<x<1$, with simple continued fraction of the form

$$x=\frac{1}{\big|a_1}+\frac{1}{\big|a_2}+\cdots,$$

where a_i, $i\geq 1$, are positive integers. The principal convergents $\frac{p_n}{q_n}$, $n\geq 1$, are defined by

$$\begin{pmatrix}p_{n-1}&p_n\\q_{n-1}&q_n\end{pmatrix}=\begin{pmatrix}0&1\\1&a_1\end{pmatrix}\cdots\begin{pmatrix}0&1\\1&a_n\end{pmatrix},\quad n\geq 1,$$

with

$$\begin{pmatrix}p_{-1}&p_0\\q_{-1}&q_0\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}.$$

One has

$$\frac{p_n}{q_n}=\frac{1}{\big|a_1}+\cdots+\frac{1}{\big|a_n}$$

and

$$\begin{cases} p_{n+1} = a_{n+1}p_n + p_{n-1} \\ q_{n+1} = a_{n+1}q_n + q_{n-1} \end{cases}$$

for $n \geq 1$. The *mediant convergents* (also called *intermediate convergents*) are defined by

$$\begin{cases} u_{n,j} = jp_n + p_{n-1} \\ v_{n,j} = jq_n + q_{n-1} \end{cases}$$

for $1 \leq j < a_{n+1}$. A simple calculation shows

$$\left| x - \frac{u_{n,j}}{v_{n,j}} \right| < \frac{a_{n+1} + 1 - j}{q_{n+1}(j \cdot q_n + q_{n-1})}, \qquad 1 \leq j < a_{n+1}.$$

If we put $j = a_{n+1}$, the above formula gives

$$\left| x - \frac{p_{n+1}}{q_{n+1}} \right| < \frac{1}{q_{n+1}^2}.$$

Mediant convergents thus interpolate $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$.

We now define an analog of the notion of 'mediant convergent' for formal power series. Let $f \in \mathbb{L}$ with continued fraction expansion

$$f = \frac{1}{|\, A_1} + \frac{1}{|\, A_2} + \cdots, \quad A_i \in \mathbb{F}_q[X] \setminus \mathbb{F}_q, \quad i \geq 1.$$

Its principal convergents satisfy:

$$\begin{pmatrix} P_{n-1} & P_n \\ Q_{n-1} & Q_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & A_1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & A_n \end{pmatrix}, \quad n \geq 1,$$

and

$$\begin{cases} P_{n+1} = A_{n+1}P_n + P_{n-1} \\ Q_{n+1} = A_{n+1}Q_n + Q_{n-1}. \end{cases}$$

We write

$$A_{n+1} = b_{t(n+1,1)}X^{t(n+1,1)} + b_{t(n+1,2)}X^{t(n+1,2)} + \cdots + b_{t(n+1,u_{n+1})}X^{t(n+1,u_{n+1})},$$
$$t(n+1,1) > \cdots > t(n+1,u_{n+1}) \geq 0, \quad b_{t(n+1,i)} \neq 0,\ 1 \leq i \leq u_{n+1}.$$

In the process of calculation of A_{n+1}, the coefficients $b_{t(n+1,1)}, \ldots, b_{t(n+1,u_{n+1})}$ are determined step by step in decreasing order of powers. According to this point of view, we define the *mediant convergents* by

$$\begin{cases} U_{n,j} = (b_{t(n+1,1)}X^{t(n+1,1)} + \cdots + b_{t(n+1,j)}X^{t(n+1,j)})P_n + P_{n-1} \\ V_{n,j} = (b_{t(n+1,1)}X^{t(n+1,1)} + \cdots + b_{t(n+1,j)}X^{t(n+1,j)})Q_n + Q_{n-1} \end{cases} \tag{21}$$

for $1 \leq j < u_{n+1}$. Note that

$$\begin{cases} \deg U_{n,j} = \deg P_{n+1} \\ \deg V_{n,j} = \deg Q_{n+1} \end{cases}$$

for $1 \leq j < u_{n+1}$. This definition corresponds to the following matricial decomposition:

$$\begin{pmatrix} 0 & 1 \\ 1 & A_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ b_{t(n+1,1)}X^{t(n+1,1)} & 1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & b_{t(n+1,u_{n+1})}X^{t(n+1,u_{n+1})} \end{pmatrix},$$

which can be compared to the analogous decomposition in the real case:

$$\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{n-1} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Proposition 6. *For all n and for all j with $1 \leq j < u_{n+1}$, one has*

$$\left| f - \frac{U_{n,j}}{V_{n,j}} \right| = \frac{q^{t(n+1,j+1)}}{|Q_{n+1}|^2}.$$

Proof. We put

$$S_{n+1,j} = \sum_{i=1}^{j} b_{t(n+1,i)} X^{t(n+1,i)},$$

and

$$f_{n+1} = \frac{1}{\left| A_{n+2}} + \frac{1}{\left| A_{n+3}} + \cdots .$$

One has $\deg f_{n+1} < 0$. It is easy to see that

$$f = \frac{P_n f_{n+1} + P_{n+1}}{Q_n f_{n+1} + Q_{n+1}}.$$

Hence we have

$$\begin{aligned} \left| f - \tfrac{U_{n,j}}{V_{n,j}} \right| &= \left| \tfrac{P_n f_{n+1} + P_{n+1}}{Q_n f_{n+1} + Q_{n+1}} - \tfrac{U_{n,j}}{V_{n,j}} \right| \\ &= \left| \tfrac{(P_n V_{n,j} - Q_n U_{n,j}) f_{n+1} + (P_{n+1} V_{n,j} - Q_{n+1} U_{n,j})}{(Q_n f_{n+1} + Q_{n+1}) V_{n,j}} \right|. \end{aligned}$$

Since $\deg Q_{n+1} = \deg V_{n,j}$, one has

$$|(Q_n f_{n+1} + Q_{n+1}) V_{n,j}| = |Q_{n+1}|^2.$$

Moreover, the norm of the numerator of the right hand side term is equal to

$$\begin{aligned} & |P_{n+1} V_{n,j} - Q_{n+1} U_{n,j}| \\ = \; & |(A_{n+1} P_n + P_{n-1})(S_{n+1,j} Q_n + Q_{n-1}) - (A_{n+1} Q_n + Q_{n-1})(S_{n+1,j} P_n + P_{n-1})| \\ = \; & |A_{n+1}(P_n Q_{n-1} - Q_n P_{n-1}) + S_{n+1,j}(Q_n P_{n-1} - P_n Q_{n-1})| \\ = \; & q^{t(n+1,j+1)} \end{aligned}$$

since

$$P_n Q_{n-1} - P_{n-1} Q_n = -(P_{n+1} Q_n - P_n Q_{n+1}).$$

This completes the proof of the proposition. □

Remark 7. Since

$$t(n+1,1) > t(n+1,2) > \cdots > t(n+1,u_{n+1}) \geq 0$$

and

$$\deg V_{n,j} = \deg Q_{n+1},$$

we may say that $(\frac{U_{n,j}}{V_{n,j}} : 1 \leq j < u_{n+1})$ interpolate the principal convergents $(\frac{P_n}{Q_n} : n \geq 1)$.

We also introduce the following associated matrices for $f \in \mathbb{J}$

$$M_{\mathbb{J}}(f) = \begin{cases} \begin{pmatrix} 1 & 0 \\ \frac{X^{-\deg f}}{\gamma(f)} & 1 \end{pmatrix} & \text{if} \quad f \in \mathbb{J}_1 \\ \begin{pmatrix} 0 & 1 \\ 1 & \left[\frac{1}{f}\right] \end{pmatrix} & \text{if} \quad f \in \mathbb{J}_2. \end{cases}$$

The following proposition (which is a direct consequence of Proposition 4) states that the map $F_{\mathbb{J}}$ indeed produces the mediant convergents:

Proposition 7. *Let*

$$t_1(f) = \min\left\{i \geq 1 \,:\, F_{\mathbb{J}}^{i-1}(f) \in \mathbb{J}_2\right\}, \qquad t_n(f) = t_1(F_{\mathbb{J}}^{\sum_{i=1}^{n-1} t_i}(f))$$

for $n \geq 1$. *For* $m = \sum_{i=1}^{n} t_i + j$, $0 \leq j < t_{n+1}$,

$$M_{\mathbb{J}}(f)\cdots M_{\mathbb{J}}(F_{\mathbb{J}}^m(f)) = \begin{cases} \begin{pmatrix} U_{n,j} & P_n \\ V_{n,j} & Q_n \end{pmatrix} & \text{if} \quad j \neq 0 \\ \begin{pmatrix} P_{n-1} & P_n \\ Q_{n-1} & Q_n \end{pmatrix} & \text{if} \quad j = 0 \end{cases}$$

for $f \in \mathbb{L}$. *Furthermore, for all* n, $u_n = \nu(A_n)$.

References

[1] V. Baladi, B. Vallée, Euclidean algorithms are Gaussian, Journal of Number Theory **110** (2005), 331?386.

[2] V. Berthé and H. Nakada, On continued fraction expansions in positive characteristic: equivalence relations and some metric properties, Expo. Math. **18** (2000), 257–284.

[3] J.D. Dixon, The number of steps in the Euclidean algorithm, J. Number Theory **2** (1970) 414–422.

[4] J.D. Dixon, A simple estimate for the number of steps in the Euclidean algorithm., Amer. Math. Monthly **78**, (1971), 374–376.

[5] M. J. Feigenbaum, Presentation functions, fixed points, and a theory of scaling function dynamics, J. Statist. Phys. **52** (1988), 527–569.

[6] P. Flajolet and R. Sedgewick, Analytic combinatorics, Cambridge University Press (2009).

[7] C. Friesen and D. Hensley, The statistics of continued fractions for polynomials over a finite field, Proc. Amer. Math. Soc., **124** (1996), 2661–2673.

[8] H. Heilbronn, On the average length of a class of finite continued fractions, Number Theory and Analysis (Papers in Honor of Edmund Landau), Plenum, New York, (1969) 87–96.

[9] D. Hensley, The number of steps in the Euclidean algorithm, J. Number Theory **49** (1994), 142–182.

[10] H.-K. Hwang, On convergence rates in the central limit theorems for combinatorial structures, European Journal of Combinatorics **19** (1998), 329–343.

[11] S. Ito, Algorithms with mediant convergents and their metrical theory, Osaka J. Math. **26** (1989), 557–578.

[12] A. Knopfmacher, J. Knopfmacher, The exact length of the Euclidean algorithm in $\mathbb{F}_q[X]$, Mathematika **35** (1988), 297–304.

[13] L. Lhote and B. Vallée, Gaussian laws for the main parameters of the Euclid algorithms, Algorithmica **50** (2008), 497–554.

[14] K. Ma, J. von zur Gathen, Analysis of Euclidean algorithms for polynomials over finite fields, Journal of Symbolic Computation **9** (1990), 429 – 455.

[15] G. Norton, Precise analyses of the right- and left-shift greatest common divisor algorithms for $GF(q)[x]$, SIAM J. Comput. **18** (1989), 608–624.

[16] F. Schweiger, Ergodic theory of fibred systems and metric number theory, Oxford Science Publications, The Clarendon Press Oxford University Press, New York (1995).

[17] A. V. Ustinov, Asymptotic behaviour of the first and second moments for the number of steps in the Euclidean algorithm, Izv. Math. **72** (2008), 1023–1059.

[18] B. Vallée, Opérateurs de Ruelle–Mayer généralisés et analyse en moyenne des algorithmes d'Euclide et de Gauss, Acta Arith. **81** (1997), 101–144.

[19] B. Vallée, Digits and continuants in Euclidean algorithms. Ergodic versus Tauberian theorems, J. Théorie Nombres Bordeaux **12** (2000), 519–558.

[20] B. Vallée, Dynamical analysis of a class of Euclidean algorithms, Theoret. Comput. Sci. **297** (2003), 447–486.

[21] B. Vallée, Euclidean Dynamics, Discrete Contin. Dyn. Syst. **15** (2006), 281–352.

LIAFA–Univ. Paris Diderot – Paris 7 & CNRS–Case 7014, 75205 Paris Cedex 13, France
E-mail address: berthe@liafa.jussieu.fr

Department of Mathematics, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama 223-8522, Japan
E-mail address: nakada@math.keio.ac.jp

Department of Mathematics, Japan Women's University, 2-8-1 Mejirodai, Bunkyou-ku, Tokyo, 112-8681, Japan
E-mail address: natsui@fc.jwu.ac.jp

GREYC–Université de Caen–Bd. Maréchal Juin, 14032 Caen Cedex, France
E-mail address: Brigitte.Vallee@unicaen.fr