Lattice reduction in two dimensions : analyses under realistic probabilistic models

Brigitte Vallée, Antonio Vera

Lattice reduction in two dimensions: analyses under realistic probabilistic models

Brigitte Vallée and Antonio Vera

CNRS UMR 6072, GREYC, Université de Caen, F-14032 Caen, France

The Gaussian algorithm for lattice reduction in dimension 2 is precisely analysed under a class of realistic probabilistic models, which are of interest when applying the Gauss algorithm "inside" the LLL algorithm. The proofs deal with the underlying dynamical systems and transfer operators. All the main parameters are studied: execution parameters which describe the behaviour of the algorithm itself as well as output parameters, which describe the geometry of reduced bases.

Keywords: Lattice Reduction, Gauss' algorithm, LLL algorithm, Euclid's algorithm, probabilistic analysis of algorithms, Dynamical Systems, Dynamical analysis of Algorithms.

1 Introduction

The lattice reduction problem consists in finding a short basis of a lattice of Euclidean space given an initially skew basis. This reduction problem plays a primary rôle in many areas of computer science and computational mathematics: for instance, modern cryptanalysis [18], computer algebra [24], integer linear programming [14], and number theory [7].

In the two-dimensional case, there exists an algorithm due to Lagrange and Gauss which computes in linear time a minimal basis of a lattice. This algorithm is in a sense optimal, from both points of view of the time-complexity and the quality of the output. It can be viewed as a generalization of the Euclidean Algorithm to the two dimensional-case. For $n \geq 3$, the LLL algorithm [13] due to Lenstra, Lenstra and Lovász, computes a reduced basis of an n-dimensional lattice in polynomial time. However, the notion of reduction is weaker than in the case $n = 2$, and the exact complexity of the algorithm (even in the worst-case, and for small dimensions) is not precisely known. The LLL algorithm uses as a main procedure the Gauss Algorithm.

This is why it is so important to have a precise understanding of the Gauss Algorithm. First, because this is a central algorithm, but also because it plays a primary rôle inside the LLL algorithm. The geometry of the n-dimensional case is involved, and it is easier to well understand the (hyperbolic) geometry of the complex plane which appears in a natural way when studying the Gauss Algorithm.

The previous results. Gauss' algorithm has been analyzed in the worst case by Lagarias, [11], then Vallée [20], who also describes the worst-case input. Then, Daudé, Flajolet and Vallée [8] completed the first work [9] and provided a detailed average-case analysis of the algorithm, in a natural probabilistic model which can be called a uniform model. They study the mean number of iterations, and prove that it is asymptotic to a constant, and thus essentially independent of the length of the input. Moreover, they show that the number of iterations follows an asymptotic geometric law, and determine the ratio of this law. On the other side, Laville and Vallée [12] study the geometry of the outputs, and describe the law of some output parameters, when the input model is the previous uniform model.
The previous analyses only deal with uniform-distributed inputs and it is not possible to apply these results "inside" the LLL algorithm, because the distribution of "local bases" which occur along the execution of the LLL algorithm is far from uniform. Akhavi, Marckert and Rouault [2] showed that, even in the uniform model where all the vectors of the input bases are independently and uniformly drawn in the unit ball, the skewness of "local bases" may vary a lot. It is then important to analyse the Gauss algorithm in a model where the skewness of the input bases may vary. Furthermore, it is natural from the works of Akhavi [1] to deal with a probabilistic model where, with a high probability, the modulus of the determinant $\det(u,v)$ of a basis (u,v) is much smaller than the product of the lengths $|u|\cdot|v|$. More precisely, a natural model is the so–called model of valuation r, where

$$\mathbb{P}\left[(u,v);\quad \frac{|\det(u,v)|}{\max(|u|,|v|)^2}\leq y\right]=\Theta(y^{r+1}),\qquad \text{with}\quad (r>-1).$$

Remark that, when r tends to -1, this model tends to the "one dimensional model", where u and v are colinear. In this case, the Gauss Algorithm "tends" to the Euclidean Algorithm, and it is important to precisely describe this transition. This model "with valuation" was already presented in [21, 22] in a slightly different context, but not deeply studied.

Our results. In this paper, we perform an exhaustive study of the main parameters of Gauss algorithm, in this scale of distributions, and obtain the following results:

(i) We first relate the output density of the algorithm to a classical object of the theory of modular forms, namely the Eisenstein series, which are eigenfunctions of the hyperbolic Laplacian [Theorem 2].

(ii) We also focus on the properties of the output basis, and we study three main parameters: the first minimum, the Hermite constant, and the orthogonal projection of a second minimum onto the orthogonal of the first one. They all play a fundamental rôle in a detailed analysis of the LLL algorithm. We relate their "contour lines" with classical curves of the hyperbolic complex plane [Theorem 3] and provide sharp estimates for the distribution of these output parameters [Theorem 4].

(iii) We finally consider various parameters which describe the execution of the algorithm (in a more precise way than the number of iterations), namely the so–called additive costs, the bit-complexity, the length decreases, and we analyze their probabilistic behaviour [Theorems 5 and 6].

Along the paper, we explain the rôle of the valuation r, and the transition phenomena between the Gauss Algorithm and the Euclidean algorithms which occur when $r\to -1$.

Towards an analysis of the LLL algorithm. The present work thus fits as a component of a more global enterprise whose aim is to understand theoretically how the LLL algorithm performs in practice, and to quantify precisely the probabilistic behaviour of lattice reduction in higher dimensions.

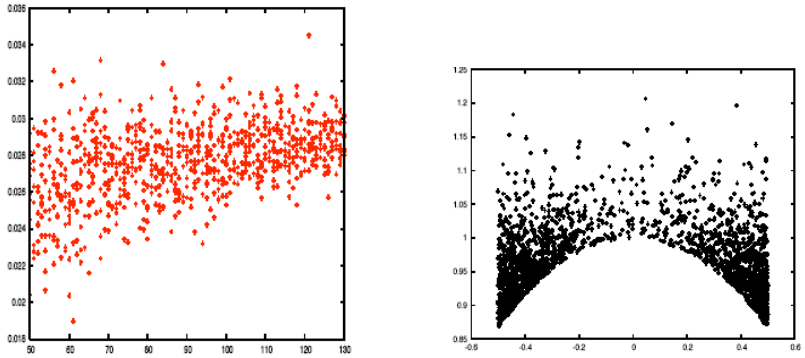

Figure 1: On the left: experimental results for the ratio $(1/n)\log\frac{|b_1|}{(\det L)^{1/n}}$ [here, n is the dimension, b_1 is the first vector of the LLL reduced basis and $\det L$ is the determinant of the lattice L]. On the right, the output distribution of "local bases" for the LLL algorithm (see Sections 3.8 and 4.7).

We are particularly interested in understanding the results of experiments conducted by Stehlé [19] which are summarized in Figure 1. We return to these experiments and their meanings in Section 3.8. We explain in Section 4.7 how our present results may explain such phenomena and constitute a first (important) step in the probabilistic analysis of the LLL algorithm.

Plan of the paper. We first present in Section 2 the algorithms to be analyzed and their main parameters. Then, we present a complex version of these algorithms, which leads to view each algorithm as a dynamical system. Finally, we perform a probabilistic analysis of such parameters: Section 4 is devoted to output parameters, whereas Section 5 focuses on execution parameters.

2 The lattice reduction algorithm in the two dimensional-case.

A lattice $\mathcal{L} \subset \mathbb{R}^n$ of dimension p is a discrete additive subgroup of $\mathbb{R}^n$. Such a lattice is generated by integral linear combinations of vectors from a family $B := (b_1, b_2, \ldots b_p)$ of $p \leq n$ linearly independent vectors of $\mathbb{R}^n$, which is called a basis of the lattice $\mathcal{L}$. A lattice is generated by infinitely many bases that are related to each other by integer matrices of determinant ± 1. Lattice reduction algorithms consider a Euclidean lattice of dimension p in the ambient space $\mathbb{R}^n$ and aim at finding a "reduced" basis of this lattice, formed with vectors almost orthogonal and short enough.

The LLL algorithm designed in [13] uses as a sub–algorithm the lattice reduction algorithm for two dimensions (which is called the Gauss algorithm) : it performs a succession of steps of the Gauss algorithm on the "local bases", and it stops when all the local bases are reduced (in the Gauss sense). This is why it is important to precisely describe and study the two–dimensional case. This is the purpose of this paper. The present section describes the particularities of the lattices in two dimensions, provides two versions of the two–dimensional lattice reduction algorithm, namely the Gauss algorithm, and introduces its main parameters of interest.

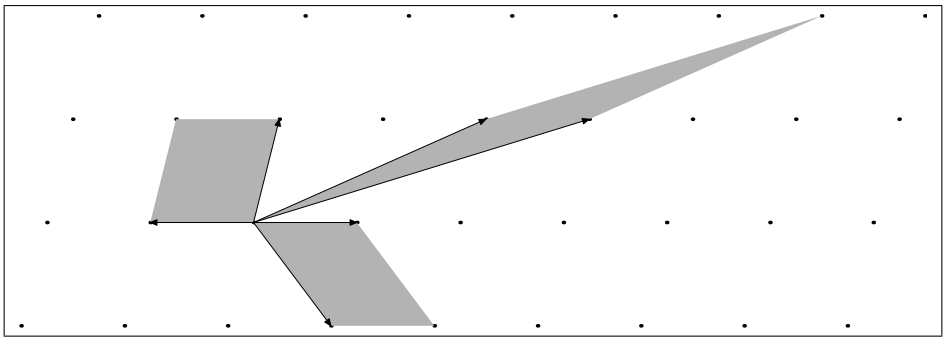

Figure 2: A lattice and three of its bases represented by the parallelogram they span. The basis on the left is minimal (reduced), whereas the two other ones are skew.

2.1 Lattices in two dimensions.

Up to a possible isometry, a two–dimensional lattice may always be considered as a subset of $\mathbb{R}^2$. With a small abuse of language, we use the same notation for denoting a complex number $z \in \mathbb{C}$ and the vector of $\mathbb{R}^2$ whose components are $(\Re z, \Im z)$. For a complex z, we denote by $|z|$ both the modulus of the complex z and the Euclidean norm of the vector z; for two complex numbers u, v, we denote by $(u \cdot v)$ the scalar product between the two vectors u and v. The following relation between two complex numbers u, v will be very useful in the sequel

$$\frac{v}{u} = \frac{(u \cdot v)}{|u|^2} + i\frac{\det(u,v)}{|u|^2}. \tag{1}$$

A *lattice* of two dimensions in the complex plane $\mathbb{C}$ is the set $\mathcal{L}$ of elements of $\mathbb{C}$ (also called vectors) defined by $\mathcal{L} = \mathbb{Z}u \oplus \mathbb{Z}v = \{au + bv; \quad a, b \in \mathbb{Z}\}$, where (u, v), called a *basis*, is a pair of $\mathbb{R}$–linearly independent elements of $\mathbb{C}$. Remark that in this case, due to (1), one has $\Im(v/u) \neq 0$.

Amongst all the bases of a lattice $\mathcal{L}$, some that are called reduced enjoy the property of being formed with "short" vectors. In dimension 2, the best reduced bases are *minimal* bases that satisfy optimality properties: define u to be a first minimum of a lattice $\mathcal{L}$ if it is a nonzero vector of $\mathcal{L}$ that has smallest Euclidean norm; the length of a first minimum of $\mathcal{L}$ is denoted by $\lambda_1(\mathcal{L})$. A second minimum v is any shortest vector amongst the vectors of the lattice that are linearly independent of u; the Euclidean length of a second minimum is denoted by $\lambda_2(\mathcal{L})$. Then a basis is *minimal* if it comprises a first and a second mininum (See Figure 2). In the sequel, we focus on particular bases which satisfy one of the two following properties:

(P) it has a positive determinant [i.e., $\det(u,v) \geq 0$ or $\Im(v/u) \geq 0$]. Such a basis is called *positive*.

(A) it has a positive scalar product [i.e., $(u \cdot v) \geq 0$ or $\Re(v/u) \geq 0$]. Such a basis is called *acute*.

Without loss of generality, we may always suppose that a basis is acute (resp. positive), since one of (u, v) and $(u, -v)$ is.

The following result gives characterizations of minimal bases. Its proof is omitted.

Proposition 1. [Characterizations of minimal bases.]
(P) [Positive bases.] *Let (u, v) be a positive basis. Then the following two conditions (a) and (b) are equivalent:*

(*a*) *the basis* (u,v) *is minimal;*
(*b*) *the pair* (u,v) *satisfies the three simultaneous inequalities:*

$$(P_1):\ |\frac{v}{u}|\geq 1,\quad (P_2):\ |\Re(\frac{v}{u})|\leq \frac{1}{2}\qquad \textit{and}\quad (P_3):\ \Im(\frac{v}{u})\geq 0$$

(*A*) [Acute bases.] *Let* (u,v) *be an acute basis. Then the following two conditions* (*a*) *and* (*b*) *are equivalent:*
(*a*) *the basis* (u,v) *is minimal;*
(*b*) *the pair* (u,v) *satisfies the two simultaneous inequalities:*

$$(A_1):\ |\frac{v}{u}|\geq 1,\qquad \textit{and}\qquad (A_2):\ 0\leq \Re(\frac{v}{u})\leq \frac{1}{2}.$$

2.2 The Gaussian reduction schemes.

There are two reduction processes, according as one focuses on positive bases or acute bases. According as we study the behaviour of the algorithm itself, or the geometric characteristics of the output, it will be easier to deal with one version than with the other one: for the first case, we will choose the positive framework, and, for the second case, the acute framework.

The positive Gauss Algorithm. The positive lattice reduction algorithm takes as input a positive arbitrary basis and produces as output a positive minimal basis. The positive Gauss algorithm aims at satisfying simultaneously the conditions (P) of Proposition 1. The conditions (P_1) and (P_3) are simply satisfied by an exchange between vectors followed by a sign change $v:=-v$. The condition (P_2) is met by an integer translation of the type:

$$v:=v-qu\qquad \text{with}\quad q:=\lfloor\tau(v,u)\rceil,\quad \tau(v,u):=\Re(\frac{v}{u})=\frac{(u\cdot v)}{|u|^2},\tag{2}$$

where $\lfloor x\rceil$ represents the integer nearest to the real x[†]. After this translation, the new coefficient $\tau(v,u)$ satisfies $0\leq\tau(v,u)\leq(1/2)$.

PGAUSS(u,v)
Input. A positive basis (u,v) of $\mathbb{C}$ with $|v|\leq|u|$, $|\tau(v,u)|\leq(1/2)$.
Output. A positive minimal basis (u,v) of $\mathcal{L}(u,v)$ with $|v|\geq|u|$.

```
While |v| ≤ |u| do
      (u,v) := (v,−u);
      q := ⌊τ(v,u)⌉,
      v := v − qu;
```

[†] The function $\lfloor x\rceil$ is defined as $\lfloor x+1/2\rfloor$ for $x\geq 0$ and $\lfloor x\rceil=-\lfloor -x\rceil$ for $x<0$.

On the input pair $(u,v)=(v_0,v_1)$, the positive Gauss Algorithm computes a sequence of vectors v_i defined by the relations

$$v_{i+1} = -v_{i-1} + q_i v_i \qquad \text{with} \quad q_i := \lfloor \tau(v_{i-1}, v_i) \rceil \,. \tag{3}$$

Here, each quotient q_i is an integer of $\mathbb{Z}$, $P(u,v)=p$ denotes the number of iterations, and the final pair (v_p, v_{p+1}) satisfies the conditions (P) of Proposition 1. Each step defines a unimodular matrix $\mathcal{M}_i$ with $\det \mathcal{M}_i = 1$,

$$\mathcal{M}_i = \begin{pmatrix} q_i & -1 \\ 1 & 0 \end{pmatrix}, \qquad \text{with} \quad \begin{pmatrix} v_{i+1} \\ v_i \end{pmatrix} = \mathcal{M}_i \begin{pmatrix} v_i \\ v_{i-1} \end{pmatrix},$$

so that the Algorithm produces a matrix $\mathcal{M}$ for which

$$\begin{pmatrix} v_{p+1} \\ v_p \end{pmatrix} = \mathcal{M} \begin{pmatrix} v_1 \\ v_0 \end{pmatrix} \qquad \text{with} \quad \mathcal{M} := \mathcal{M}_p \cdot \mathcal{M}_{p-1} \cdot \ldots \cdot \mathcal{M}_1. \tag{4}$$

The acute Gauss Algorithm. The acute reduction algorithm takes as input an arbitrary acute basis and produces as output an acute minimal basis. This AGAUSS algorithm aims at satisfying simultaneously the conditions (A) of Proposition 1. The condition (A_1) is simply satisfied by an exchange, and the condition (A_2) is met by an integer translation of the type:

$$v := \varepsilon(v - qu) \qquad \text{with} \quad q := \lfloor \tau(v,u) \rceil \,, \qquad \varepsilon = \operatorname{sign}\left(\tau(v,u) - \lfloor \tau(v,u) \rceil\right),$$

where $\tau(v,u)$ is defined as in (2). After this transformation, the new coefficient $\tau(v,u)$ satisfies $0 \leq \tau(v,u)| \leq (1/2)$.

AGAUSS(u,v)

Input. An acute basis (u,v) of $\mathbb{C}$ with $|v| \leq |u|$, $0 \leq \tau(v,u) \leq (1/2)$.

Output. An acute minimal basis (u,v) of $\mathcal{L}(u,v)$ with $|v| \geq |u|$.

```
While |v| ≤ |u| do
      (u,v) := (v,u);
      q := ⌊τ(v,u)⌉ ; ε := sign(τ(v,u) − ⌊τ(v,u)⌉),
      v := ε(v − qu);
```

On the input pair $(u,v)=(w_0,w_1)$, the Gauss Algorithm computes a sequence of vectors w_i defined by the relations $\quad w_{i+1} = \varepsilon_i(w_{i-1} - \widetilde{q}_i w_i) \quad$ with

$$\widetilde{q}_i := \lfloor \tau(w_{i-1}, w_i) \rceil \,, \qquad \varepsilon_i = \operatorname{sign}\left(\tau(w_{i-1}, w_i) - \lfloor \tau(w_{i-1}, w_i) \rceil\right). \tag{5}$$

Here, each quotient $\widetilde{q}_i$ is a positive integer, $p \equiv p(u,v)$ denotes the number of iterations [this will be the same as the previous one], and the final pair (w_p, w_{p+1}) satisfies the conditions (A) of Proposition 1. Each step defines a unimodular matrix $\mathcal{N}_i$ with $\det \mathcal{N}_i = \varepsilon_i = \pm 1$,

$$\mathcal{N}_i = \begin{pmatrix} -\varepsilon_i \widetilde{q}_i & \varepsilon_i \\ 1 & 0 \end{pmatrix}, \qquad \text{with} \quad \begin{pmatrix} w_{i+1} \\ w_i \end{pmatrix} = \mathcal{N}_i \begin{pmatrix} w_i \\ w_{i-1} \end{pmatrix},$$

so that the algorithm produces a matrix $\mathcal{N}$ for which

$$\begin{pmatrix} w_{p+1} \\ w_p \end{pmatrix} = \mathcal{N} \begin{pmatrix} w_1 \\ w_0 \end{pmatrix} \qquad \text{with} \quad \mathcal{N} := \mathcal{N}_p \cdot \mathcal{N}_{p-1} \cdot \ldots \cdot \mathcal{N}_1.$$

Comparison between the two algorithms. These algorithms are closely related, but different. The AGAUSS Algorithm can be viewed as a folded version of the PGAUSS Algorithm, in the sense defined in [4]. We shall come back to this fact in Section 3.3. And the following is true:

Consider two bases: a positive basis (v_0, v_1)*, and an acute basis* (w_0, w_1) *that satisfy* $w_0 = v_0$ *and* $w_1 = \eta_1 v_1$ *with* $\eta_1 = \pm 1$*. Then the sequences of vectors* (v_i) *and* (w_i) *computed by the two versions of the Gauss algorithm (defined in Eq.(3),(5)) satisfy* $w_i = \eta_i v_i$ *for some* $\eta_i = \pm 1$ *and the quotient* $\widetilde{q}_i$ *is the absolute value of quotient* q_i*.*

Then, when studying the two kinds of parameters –execution parameters, or output parameters– the two algorithms are essentially the same. As already said, we shall use the PGAUSS Algorithm for studying the output parameters, and the AGAUSS Algorithm for the execution parameters.

2.3 Main parameters of interest.

The size of a pair $(u, v) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ is

$$\ell(u, v) := \max\{\ell(|u|^2), \ell(|v|^2)\} = \ell\left(\max\{|u|^2, |v|^2\}\right),$$

where $\ell(x)$ is the binary length of the integer x. The Gram matrix $G(u, v)$ is defined as

$$G(u, v) = \begin{pmatrix} |u|^2 & (u \cdot v) \\ (u \cdot v) & |v|^2 \end{pmatrix}.$$

In the following, we consider subsets Ω_M which gather all the (valid) inputs of size M relative to each version of the algorithm. They will be endowed with some discrete probability $\mathbb{P}_M$, and the main parameters become random variables defined on these sets.

All the computations of the Gauss algorithm are done on the Gram matrices $G(v_i, v_{i+1})$ of the pair (v_i, v_{i+1}). The *initialization* of the Gauss algorithm *computes* the Gram Matrix of the initial basis: it computes three scalar products, which takes a *quadratic time*[‡] with respect to the length of the input $\ell(u, v)$. After this, all the computations of the *central part* of the algorithm *are directly done* on these matrices; more precisely, each step of the process is a Euclidean division between the two coefficients of the first line of the Gram matrix $G(v_i, v_{i-1})$ of the pair (v_i, v_{i-1}) for obtaining the quotient q_i, followed with the computation of the new coefficients of the Gram matrix $G(v_{i+1}, v_i)$, namely

$$|v_{i+1}|^2 := |v_{i-1}|^2 - 2q_i\,(v_i \cdot v_{i-1}) + q_i^2 |v_i|^2, \qquad (v_{i+1} \cdot v_i) := q_i\,|v_i|^2 - (v_{i-1} \cdot v_i).$$

Then the cost of the i-th step is proportional to $\ell(|q_i|) \cdot \ell(|v_i|^2)$, and the bit-complexity of the central part of the Gauss Algorithm is expressed as a function of

$$B(u, v) = \sum_{i=1}^{p(u,v)} \ell(|q_i|) \cdot \ell(|v_i|^2), \tag{6}$$

where $p(u, v)$ is the number of iterations of the Gauss Algorithm. In the sequel, B will be called the bit-complexity.

[‡] we consider the naive multiplication between integers of size M, whose bit-complexity is $O(M^2)$.

The bit-complexity $B(u,v)$ is one of our parameters of interest, and we compare it to other simpler costs. Define three new costs, the quotient bit-cost $Q(u,v)$, the difference cost $\underline{D}(u,v)$, and the approximate difference cost D:

$$Q(u,v)=\sum_{i=1}^{p(u,v)}\ell(|q_i|),\qquad \underline{D}(u,v)=\sum_{i=1}^{p(u,v)}\ell(|q_i|)\left[\,\ell(|v_i|^2)-\ell(|v_0|^2)\right], \tag{7}$$

$$D(u,v):=2\sum_{i=1}^{p(u,v)}\ell(|q_i|)\lg\left|\frac{v_i}{v}\right|,$$

which satisfy $D(u,v)-\underline{D}(u,v)=O(Q(u,v))$ and

$$B(u,v)=Q(u,v)\,\ell(|u|^2)+D(u,v)+[\underline{D}(u,v)-D(u,v)]\,. \tag{8}$$

We are then led to study two main parameters related to the bit-cost, that may be of independent interest:

(a) The so-called additive costs, which provide a generalization of cost Q. They are defined as the sum of elementary costs, which only depend on the quotients q_i. More precisely, from a positive elementary cost c defined on $\mathbb{N}$, we consider the total cost on the input (u,v) defined as

$$C_{(c)}(u,v)=\sum_{i=1}^{p(u,v)}c(|q_i|)\,. \tag{9}$$

When the elementary cost c satisfies $c(m)=O(\log m)$, the cost C is said to be of moderate growth.

(b) The sequence of the i-th length decreases d_i (for $i\in[1..p]$) and the total length decrease $d:=d_p$, defined as

$$d_i:=\left|\frac{v_i}{v_0}\right|^2,\qquad d:=\left|\frac{v_p}{v_0}\right|^2. \tag{10}$$

Finally, the configuration of the output basis $(\hat{u},\hat{v})$ is described via its Gram–Schmidt orthogonalized basis, that is the system $(\hat{u}^\star,\hat{v}^\star)$ where $\hat{u}^\star:=\hat{u}$ and $\hat{v}^\star$ is the orthogonal projection of $\hat{v}$ onto the orthogonal of $<\hat{u}>$. There are three main output parameters closely related to the minima of the lattice $\mathcal{L}(u,v)$,

$$\lambda(u,v):=\lambda_1(\mathcal{L}(u,v))=|\hat{u}|,\qquad \mu(u,v):=\frac{|\det(u,v)|}{\lambda(u,v)}=|\hat{v}^\star|, \tag{11}$$

$$\gamma(u,v):=\frac{\lambda^2(u,v)}{|\det(u,v)|}=\frac{\lambda(u,v)}{\mu(u,v)}=\frac{|\hat{u}|}{|\hat{v}^\star|}. \tag{12}$$

We come back later to these output parameters.

3 The Gauss Algorithm in the complex plane.

We now describe a complex version for each of the two versions of the Gauss algorithms. This leads to view each algorithm as a dynamical system, which can be seen as a (complex) extension of (real) dynamical systems relative to the centered Euclidean algorithms. We provide a precise description of linear fractional transformations (LFTs) used by each algorithm. We finally describe the (two) classes of probabilistic models of interest.

3.1 The complex framework.

Many structural characteristics of lattices and bases are invariant under linear transformations —similarity transformations in geometric terms— of the form $S_\lambda : u \mapsto \lambda u$ with $\lambda \in \mathbb{C} \setminus \{0\}$.

(*a*) A first instance is the execution of the Gauss algorithm itself: it should be observed that translations performed by the Gauss algorithms only depend on the quantity $\tau(v,u)$ defined in (2), which equals $\Re(v/u)$. Furthermore, exchanges depend on $|v/u|$. Then, if v_i (or w_i) is the sequence computed by the algorithm on the input (u,v), defined in Eq. (3), (5), the sequence of vectors computed on an input pair $S_\lambda(u,v)$ coincides with the sequence $S_\lambda(v_i)$ (or $S_\lambda(w_i)$). This makes it possible to give a formulation of the Gauss algorithm entirely in terms of complex numbers.

(*b*) A second instance is the characterization of minimal bases given in Proposition 1 that only depends on the ratio $z = v/u$.

(*c*) A third instance are the main parameters of interest: the execution parameters D,C,d defined in (7,9,10) and the output parameters λ,μ,γ defined in (11,12). All these parameters admit also complex versions: For $X \in \{\lambda,\mu,\gamma,D,C,d\}$, we denote by $X(z)$ the value of X on basis $(1,z)$. Then, there are close relations between $X(u,v)$ and $X(z)$ for $z = v/u$:

$$X(z) = \frac{X(u,v)}{|u|}, \quad \text{for} \quad X \in \{\lambda,\mu\}, \qquad X(z) = X(u,v), \quad \text{for} \quad X \in \{D,C,d,\gamma\}.$$

It is thus natural to consider lattice bases taken up to equivalence under similarity, and it is sufficient to restrict attention to lattice bases of the form $(1,z)$. We denote by $L(z)$ the lattice $\mathcal{L}(1,z)$. In the complex framework, the geometric transformation effected by each step of the algorithm consists of an inversion-symmetry $S : z \mapsto 1/z$, followed by a translation $z \mapsto T^{-q}z$ with $T(z) = z+1$, ans a possible sign change $J : z \mapsto -z$.

The upper half plane $\mathbb{H} := \{z \in \mathbb{C};\ \Im(z) > 0\}$ plays a central rôle for the PGAUSS Algorithm, while the right half plane $\{z \in \mathbb{C};\quad \Re(z) \geq 0, \Im(z) \neq 0\}$ plays a central rôle in the AGAUSS algorithm. Remark just that the right half plane is the union $\mathbb{H}_+ \cup J\mathbb{H}_-$ where $J : z \mapsto -z$ is the sign change and

$$\mathbb{H}_+ := \{z \in \mathbb{C};\quad \Im(z) > 0, \Re(z) \geq 0\}, \qquad \mathbb{H}_- := \{z \in \mathbb{C};\quad \Im(z) > 0, \Re(z) \leq 0\}.$$

3.2 The dynamical systems for the GAUSS *algorithms.*

In this complex context, the PGAUSS algorithm brings z into the vertical strip $\mathcal{B}_+ \cup \mathcal{B}_-$ with

$$\mathcal{B} = \left\{ z \in \mathbb{H};\quad |\Re(z)| \leq \frac{1}{2} \right\}, \qquad \mathcal{B}_+ := \mathcal{B} \cap \mathbb{H}_+, \quad \mathcal{B}_- := \mathcal{B} \cap \mathbb{H}_-,$$

reduces to the iteration of the mapping

$$U(z) = -\frac{1}{z} + \left\lfloor \Re\left(\frac{1}{z}\right) \right\rfloor = -\frac{1}{z} - \left\lfloor \Re\left(-\frac{1}{z}\right) \right\rfloor \tag{13}$$

and stops as soon as z belongs to the domain $\mathcal{F} = \mathcal{F}_+ \cup \mathcal{F}_-$ with

$$\mathcal{F} = \left\{ z \in \mathbb{H};\quad |z| \geq 1, \quad |\Re(z)| \leq \frac{1}{2} \right\}, \qquad \mathcal{F}_+ := \mathcal{F} \cap \mathbb{H}_+, \quad \mathcal{F}_- := \mathcal{F} \cap \mathbb{H}_-. \tag{14}$$

Such a domain, represented in Figure 3, is familiar from the theory of modular forms or the reduction theory of quadratic forms [17].

Consider the pair $(\mathcal{B},U)$ where the map $U:\mathcal{B}\to\mathcal{B}$ is defined in (13) for $z\in\mathcal{B}\setminus\mathcal{F}$ and extended to $\mathcal{F}$ with $U(z)=z$ for $z\in\mathcal{F}$. This pair $(\mathcal{B},U)$ defines a dynamical system, and $\mathcal{F}$ can be seen as a "hole": since the PGAUSS algorithm terminates, there exists an index $p\geq 0$ which is the first index for which $U^p(z)$ belongs to $\mathcal{F}$. Then, any complex number of $\mathcal{B}$ gives rise to a trajectory $z,U(z),U^2(z),\ldots,U^p(z)$ which "falls" in the hole $\mathcal{F}$, and stays inside $\mathcal{F}$ as soon it attains $\mathcal{F}$. Moreover, since $\mathcal{F}$ is a fundamental domain of the upper half plane $\mathbb{H}$ under the action of $PSL_2(\mathbb{Z})$[§], there exists a tesselation of $\mathbb{H}$ with transforms of $\mathcal{F}$ of the form $h(\mathcal{F})$ with $h\in PSL_2(\mathbb{Z})$. We will see later that the geometry of $\mathcal{B}\setminus\mathcal{F}$ is compatible with the geometry of $\mathcal{F}$.

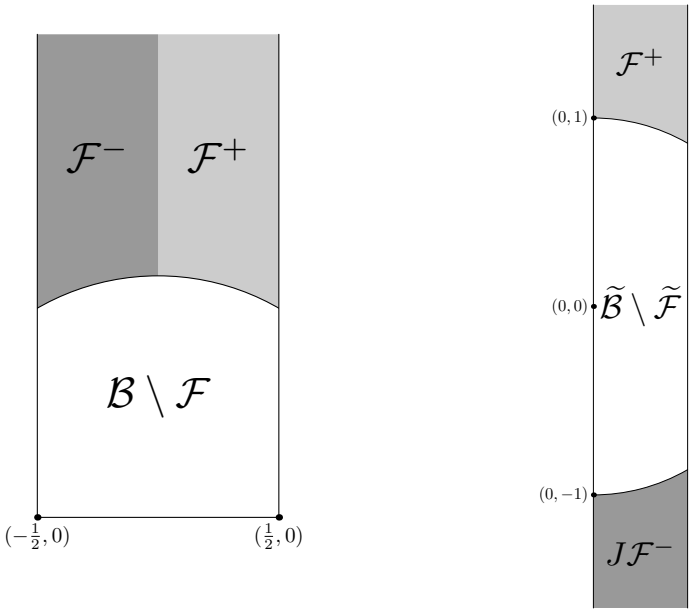

Figure 3: The fundamental domains $\mathcal{F},\widetilde{\mathcal{F}}$ and the strips $\mathcal{B},\widetilde{\mathcal{B}}$.

In the same vein, the AGAUSS algorithm brings z into the vertical strip

$$\widetilde{\mathcal{B}}=\left\{z\in\mathbb{C};\quad \Im(z)\neq 0,\quad 0\leq\Re(z)\leq\frac{1}{2}\right\}=\mathcal{B}_+\cup J\mathcal{B}_-,$$

reduces to the iteration of the mapping

$$\widetilde{U}(z)=\varepsilon\left(\frac{1}{z}\right)\left(\frac{1}{z}-\left\lfloor\Re\left(\frac{1}{z}\right)\right\rceil\right)\qquad\text{with}\quad\varepsilon(z):=\operatorname{sign}(\Re(z)-\lfloor\Re(z)\rceil),\tag{15}$$

[§] We recall that $PSL_2(\mathbb{Z})$ is the set of LFT's of the form $(az+b)/(cz+d)$ with $a,b,c,d\in\mathbb{Z}$ and $ad-bc=1$.

and stops as soon as z belongs to the domain $\widetilde{\mathcal{F}}$

$$\widetilde{\mathcal{F}} = \left\{ z \in \mathbb{C}; \quad |z| \geq 1 \quad 0 \leq \Re(z) \leq \frac{1}{2} \right\} = \mathcal{F}_+ \cup J\mathcal{F}_-. \tag{16}$$

Consider the pair $(\widetilde{\mathcal{B}}, \widetilde{U})$ where the map $\widetilde{U} : \widetilde{\mathcal{B}} \to \widetilde{\mathcal{B}}$ is defined in (15) for $z \in \widetilde{\mathcal{B}} \setminus \widetilde{\mathcal{F}}$ and extended to $\widetilde{\mathcal{F}}$ with $\widetilde{U}(z) = z$ for $z \in \widetilde{\mathcal{F}}$. This pair $(\widetilde{\mathcal{B}}, \widetilde{U})$ also defines a dynamical system, and $\widetilde{\mathcal{F}}$ can also be seen as a "hole".

3.3 Relation with the centered Euclid Algorithm.

It is clear (at least in an informal way) that each version of Gauss algorithm is an extension of the (centered) Euclid algorithm:

(i) for the PGAUSS algorithm, it is related to the Euclidean division of the form $v = qu + r$ with $|r| \in [0, +u/2]$

(ii) for the AGAUSS algorithm, it is based on the Euclidean division of the form $v = qu + \varepsilon r$ with $\varepsilon := \pm 1, r \in [0, +u/2]$.

If, instead of pairs, that are the old pair (u, v) and the new pair (r, u), one considers rationals, namely the old rational $x = u/v$ or the new rational $y = r/u$, each Euclidean division can be written with a map that expresses the new rational y as a function of the old rational x, as $y = V(x)$ (in the first case) or $y = \widetilde{V}(x)$ (in the second case). With $I := [-1/2, +1/2]$ and $\widetilde{I} := [0, 1/2]$, the maps $V : I \to I$ or $\widetilde{V} : \widetilde{I} \to \widetilde{I}$ are defined as follows

$$V(x) := \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rceil, \quad \text{for } x \neq 0, \qquad V(0) = 0, \tag{17}$$

$$\widetilde{V}(x) = \varepsilon\left(\frac{1}{x}\right) \left(\frac{1}{x} - \left\lfloor \frac{1}{x} \right\rceil \right), \quad \text{for } x \neq 0, \qquad \widetilde{V}(0) = 0. \tag{18}$$

[Here, $\varepsilon(x) := \text{sign}(x - \lfloor x \rceil)$]. This leads to two (real) dynamical systems (I, V) and $(\widetilde{I}, \widetilde{V})$ whose graphs are represented in Figure 4. Remark that the tilded system is obtained by a folding of the untilded one (or unfolded one), (first along the x axis, then along the y axis), as it is explained in [4]. The folded system is called the F-EUCLID system (or algorithm), whereas the unfolded one is called the U-EUCLID system (or algorithm).

Of course, there are close connections between U and $-V$ on the one hand, and $\widetilde{U}$ and $\widetilde{V}$ on the other hand: Even if the complex systems $(\mathcal{B}, U)$ and $(\widetilde{\mathcal{B}}, \widetilde{U})$ are defined on strips formed with complex numbers z that are not real (i.e., $\Im z \neq 0$), they can be extended to real inputs "by continuity": This defines two new dynamical systems $(\underline{\mathcal{B}}, \underline{U})$ and $\underline{\widetilde{\mathcal{B}}}, \underline{\widetilde{U}})$, and the real systems $(I, -V)$ and $(\widetilde{I}, \widetilde{V})$ are just the restriction of the extended complex systems to real inputs. Remark now that the fundamental domains $\mathcal{F}, \widetilde{\mathcal{F}}$ are no longer "holes" since any real irrational input stays inside the real interval and never "falls" in them. On the contrary, the trajectories of rational numbers end at 0, and finally each rational is mapped to $i\infty$.

3.4 The LFT's used by the PGAUSS algorithm.

The complex numbers which intervene in the PGAUSS algorithm on the input $z_0 = v_1/v_0$ are related to the vectors (v_i) defined in (3) via the relation $z_i = v_{i+1}/v_i$. They are directly computed by the relation

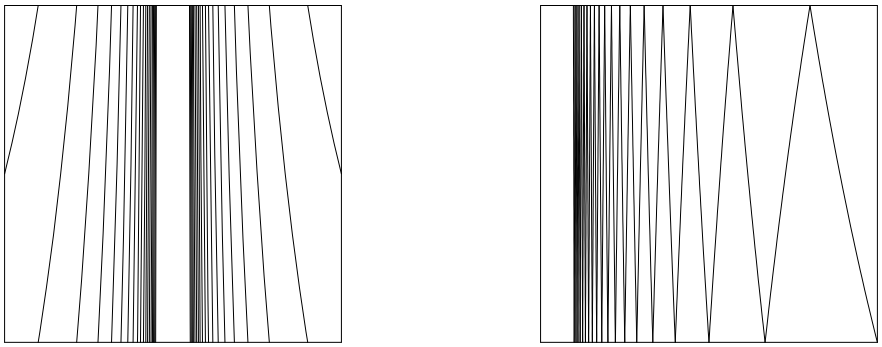

Figure 4: The two dynamical systems underlying the centered Euclidean algorithms: on the left, the unfolded one (U-EUCLID); on the right, the folded one (F-EUCLID)

$z_{i+1} := U(z_i)$, so that the old z_{i-1} is expressed with the new one z_i as

$$z_{i-1} = h_{[m_i]}(z_i), \qquad \text{with} \quad h_{[m]}(z) := \frac{1}{m-z}.$$

This creates a continued fraction expansion for the initial complex z_0, of the form

$$z_0 = h(z_p) \qquad \text{with} \quad h := h_{[m_1]} \circ h_{[m_2]} \circ \dots h_{[m_p]},$$

which expresses the input $z = z_0$ as a function of the output $\hat{z} = z_p$. More generally, the i-th complex number z_i satisfies

$$z_i = h_i(z_p) \qquad \text{with} \quad h_i := h_{[m_{i+1}]} \circ h_{[m_{i+2}]} \circ \dots h_{[m_p]}.$$

Proposition 2. *The set $\mathcal{G}$ of LFTs $h : z \mapsto (az+b)/(cz+d)$ defined with the relation $z = h(\hat{z})$ which sends the output domain $\mathcal{F}$ into the input domain $\mathcal{B} \setminus \mathcal{F}$ is characterized by the set $\mathcal{Q}$ of possible quadruples (a,b,c,d). A quadruple $(a,b,c,d) \in \mathbb{Z}^4$ with $ad-bc = 1$ belongs to $\mathcal{Q}$ if and only if one of the three conditions is fulfilled*

(i) ($c = 1$ or $c \geq 3$) and ($|a| \leq c/2$);
(ii) $c = 2, a = 1, b \geq 0, d \geq 0$;
(iii) $c = 2, a = -1, b < 0, d < 0$.

There exists a bijection between $\mathcal{Q}$ and the set $\mathcal{P} = \{(c,d); \quad c \geq 1, \gcd(c,d) = 1\}$. On the other hand, for each pair (a,c) in the set

$$\mathcal{C} := \{(a,c); \quad \frac{a}{c} \in [-1/2, +1/2],\ c \geq 1; \gcd(a,c) = 1\}, \tag{19}$$

any LFT of $\mathcal{G}$ which admits (a,c) as coefficients can be written as $h = h_{(a,c)} \circ T^q$ with $q \in \mathbb{Z}$ and $h_{(a,c)}(z) = (az+b_0)/(cz+d_0)$, with $|b_0| \leq |a/2|, |d_0| \leq |c/2|$.

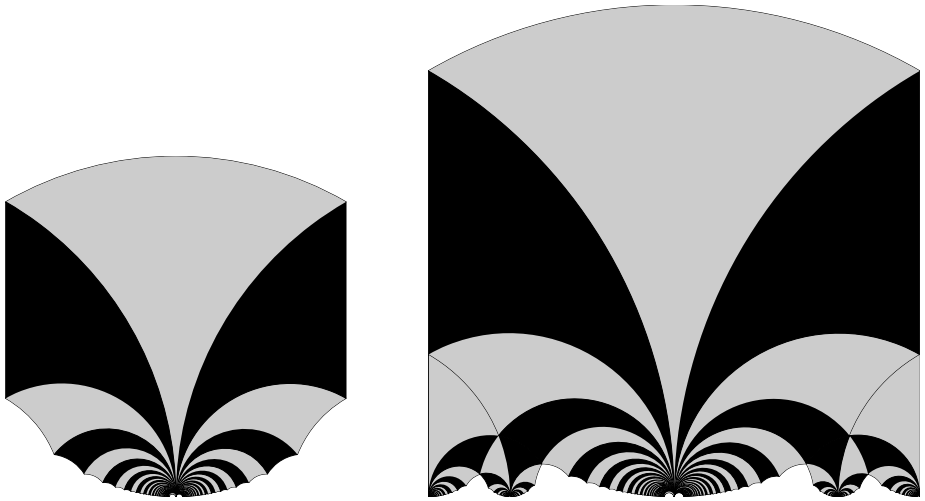

Figure 5: On the left, the "central" festoon $\mathcal{F}_{(0,1)}$. On the right, three festoons of the strip $\mathcal{B}$, relative to $(0,1),(1,3),(-1,3)$ and the two half-festoons at $(-1,2)$ and $(1,2)$.

Definition. [Festoons] *If $\mathcal{G}_{(a,c)}$ denotes the set of LFT's of $\mathcal{G}$ which admit (a,c) as coefficients, the domain*

$$\mathcal{F}_{(a,c)} = \bigcup_{h\in\mathcal{G}_{(a,c)}} h(\mathcal{F}) = h_{(a,c)}\left(\bigcup_{q\in\mathbb{Z}} T^q\mathcal{F}\right) \tag{20}$$

gathers all the transforms of $h(\mathcal{F})$ which belong to $\mathcal{B}\setminus\mathcal{F}$ for which $h(i\infty)=a/c$. It is called the festoon of a/c.

Remark that, in the case when $c=2$, there are two half-festoons at $1/2$ and $-1/2$ (See Figure 5).

3.5 The LFT's used by the AGAUSS algorithm.

In the same vein, the complex numbers which intervene in the AGAUSS algorithm on the input $z_0 = w_1/w_0$ are related to the vectors (w_i) defined in (5) via the relation $z_i = w_{i+1}/w_i$. They are computed by the relation $z_{i+1} := \widetilde{U}(z_i)$, so that the old z_{i-1} is expressed with the new one z_i as

$$z_{i-1} = h_{\langle m_i,\varepsilon_i\rangle}(z_i) \qquad \text{with} \quad h_{\langle m,\varepsilon\rangle}(z) := \frac{1}{m+\varepsilon z}.$$

This creates a continued fraction expansion for the initial complex z_0, of the form

$$z_0 = \widetilde{h}(z_p) \qquad \text{with} \quad \widetilde{h} := h_{\langle m_1,\varepsilon_1\rangle}\circ h_{\langle m_2,\varepsilon_2\rangle}\circ\ldots h_{\langle m_p,\varepsilon_p\rangle}.$$

More generally, the i-th complex number z_i satisfies

$$z_i = \widetilde{h}_i(z_p) \qquad \text{with} \quad \widetilde{h}_i := h_{\langle m_{i+1},\varepsilon_{i+1}\rangle}\circ h_{\langle m_{i+2},\varepsilon_{i+2}\rangle}\circ\ldots h_{\langle m_p,\varepsilon_p\rangle}. \tag{21}$$

We now explain the particular rôle which is played by the disk $\mathcal{D}$ of diameter $\widetilde{I} = [0, 1/2]$. Figure 6 shows that the domain $\widetilde{\mathcal{B}} \setminus \mathcal{D}$ decomposes as the union of six transforms of the fundamental domain $\widetilde{\mathcal{F}}$, namely

$$\widetilde{\mathcal{B}} \setminus \widetilde{\mathcal{D}} = \bigcup_{h \in \mathcal{K}} h(\widetilde{\mathcal{F}}) \qquad \text{with} \quad \mathcal{K} := \{I, S, STJ, ST, ST^2J, ST^2JS\}. \tag{22}$$

This shows that the disk $\mathcal{D}$ itself is also a union of transforms of the fundamental domain $\widetilde{\mathcal{F}}$. Remark that the situation is different for the PGAUSS algorithm, since the frontier of $\mathcal{D}$ lies "in the middle" of transforms of the fundamental domain $\mathcal{F}$ (see Figure 6).

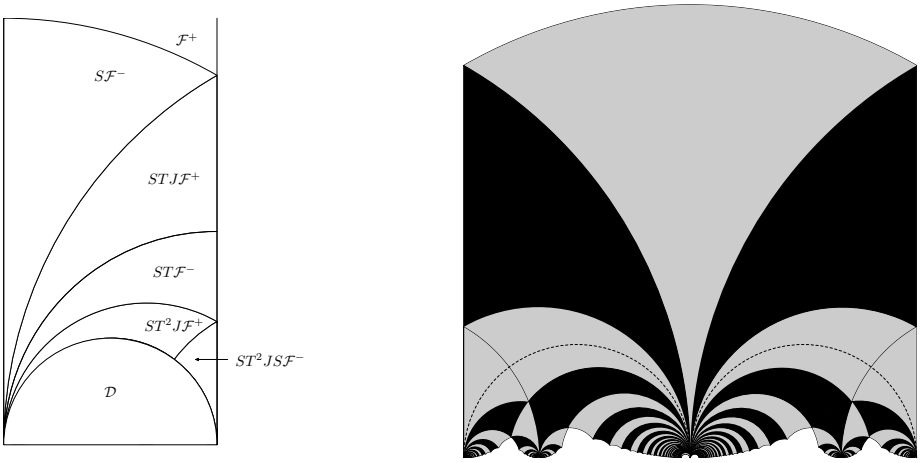

Figure 6: On the left, the six domains which constitute the domain $\mathcal{B}_+ \setminus \mathcal{D}_+$. On the right, the disk $\mathcal{D}$ is not compatible with the geometry of transforms of the fundamental domains $\mathcal{F}$.

As Figure 7 shows it, there are two main parts in the execution of the AGAUSS Algorithm, according to the position of the current complex z_i with respect to the disk $\mathcal{D}$ whose equation is

$$\mathcal{D} := \{z; \qquad \Re\left(\frac{1}{z}\right) \geq 2\}.$$

While z_i belongs to $\mathcal{D}$, the quotient (m_i, ε_i) satisfies $(m_i, \varepsilon_i) \geq (2, +1)$ (wrt the lexicographic order), and the algorithm uses at each step the set

$$\mathcal{H} := \{h_{\langle m,\varepsilon\rangle}; \quad (m, \varepsilon) \geq (2, +1)\}$$

so that $\mathcal{D}$ can be written as

$$\mathcal{D} = \bigcup_{h \in \mathcal{H}^+} h(\widetilde{\mathcal{B}} \setminus \mathcal{D}) \qquad \text{with} \quad \mathcal{H}^+ := \sum_{k \geq 1} \mathcal{H}^k. \tag{23}$$

The part of the AGAUSS algorithm performed when z_i belongs to $\mathcal{D}$ is called the COREGAUSS algorithm. The total set of LFT's used by the COREGAUSS algorithm is then the set $\mathcal{H}^+ = \cup_{k \geq 1} \mathcal{H}^k$. As soon as z_i

does not any longer belong to $\mathcal{D}$, there are two cases. If z_i belongs to $\widetilde{\mathcal{F}}$, then the algorithm ends. If z_i belongs to $\widetilde{\mathcal{B}} \setminus (\widetilde{\mathcal{F}} \cup \mathcal{D})$, there remains at most two iterations (due to (22) and Figure 6), that constitutes the FINALGAUSS algorithm, which uses the set $\mathcal{K}$ of LFT's, called the final set of LFT's. Finally, we have proven:

Proposition 3. *The set $\widetilde{\mathcal{G}}$ formed by the LFT's which map the fundamental domain $\widetilde{\mathcal{F}}$ into the set $\widetilde{\mathcal{B}} \setminus \widetilde{\mathcal{F}}$ decomposes as $\widetilde{\mathcal{G}} = (\mathcal{H}^\star \cdot \mathcal{K}) \setminus \{I\}$ where*

$$\mathcal{H}^\star := \sum_{k \geq 0} \mathcal{H}^k, \qquad \mathcal{H} := \{h_{\langle m,\varepsilon\rangle}; \quad (m,\varepsilon) \geq (2,+1)\}, \qquad \mathcal{K} := \{I, S, STJ, ST, ST^2J, ST^2JS\}.$$

Here, if $\mathcal{D}$ denotes the disk of diameter $[0,1/2]$, then $\mathcal{H}^+$ is the set formed by the LFT's which map $\widetilde{\mathcal{B}} \setminus \mathcal{D}$ into $\mathcal{D}$ and $\mathcal{K}$ is the final set formed by the LFT's which map $\widetilde{\mathcal{F}}$ into $\widetilde{\mathcal{B}} \setminus \mathcal{D}$. Furthermore, there is a characterization of $\mathcal{H}^+$ due to Hurwitz which involves the golden ratio $\phi = (1+\sqrt{5})/2$:

$$\mathcal{H}^+ := \{h(z) = \frac{az+b}{cz+d}; \quad (a,b,c,d) \in \mathbb{Z}^4, b, d \geq 1, ac \geq 0, \\ |ad-bc| = 1, |a| \leq \frac{|c|}{2}, b \leq \frac{d}{2}, -\frac{1}{\phi^2} \leq \frac{c}{d} \leq \frac{1}{\phi}\}.$$

COREGAUSS(z)
Input. A complex number in $\mathcal{D}$.
Output. A complex number in $\widetilde{\mathcal{B}} \setminus \mathcal{D}$.
`While` $z \in \mathcal{D}$ `do` $z := \widetilde{U}(z)$;

FINALGAUSS(z)
Input. A complex number in $\widetilde{\mathcal{B}} \setminus \mathcal{D}$.
Output. A complex number in $\widetilde{\mathcal{F}}$.
`While` $z \notin \widetilde{\mathcal{F}}$ `do` $z := \widetilde{U}(z)$;

AGAUSS(z)
Input. A complex number in $\widetilde{\mathcal{B}} \setminus \widetilde{\mathcal{F}}$.
Output. A complex number in $\widetilde{\mathcal{F}}$.
COREGAUSS (z);
FINALGAUSS (z);

Figure 7: The decomposition of the AGAUSS Algorithm.

3.6 Comparing the CoreGauss *algorithm and the* F-Euclid *algorithm.*

The COREGAUSS algorithm has a nice structure since it uses at each step the same set $\mathcal{H}$. This set is exactly the set of LFT's which is used by the F-EUCLID Algorithm relative to the dynamical system defined in (18). Then, the COREGAUSS algorithm is just a lifting of this F-EUCLID Algorithm, whereas the final steps of the AGAUSS algorithm use different LFT's, and are not similar to a lifting of a Euclidean Algorithm. This is why the COREGAUSS algorithm is interesting to study: we will see in Section 5.3 why it can be seen as an exact generalization of the F-EUCLID algorithm.

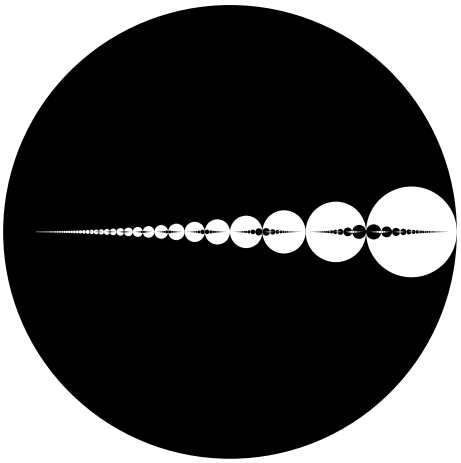

Figure 8: The domains $[R = k]$ alternatively in black and white.

Consider, for instance, the number R of iterations of the CoreGauss algorithm. Then, the domain $[R \geq k+1]$ gathers the complex numbers z for which $\widetilde{U}^k(z)$ are in $\mathcal{D}$. Such a domain admits a nice characterization, as a union of disjoint disks, namely

$$[R \geq k+1] = \bigcup_{h \in \mathcal{H}^k} h(\mathcal{D}), \tag{24}$$

which is represented in Figure 6. The disk $h(\mathcal{D})$ for $h \in \mathcal{H}^+$ is the disk whose diameter is the interval $[h(0), h(1/2)] = h(I)$. Inside the F-Euclid dynamical system, the interval $h(\widetilde{I})$ (relative to a LFT $h \in \mathcal{H}^k$) is called a fundamental interval (or a cylinder) of depth k: it gathers all the real numbers of the interval $\widetilde{I}$ which have the same continued fraction expansion of depth k. This is why the disk $h(\mathcal{D})$ is called a fundamental disk.

This figure shows in a striking way the efficiency of the algorithm, and asks natural questions: Is it possible to estimate the probability of the event $[R \geq k+1]$? Is it true that it is geometrically decreasing? With which ratio? These questions are asked (and answered) in [8], at least in the "uniform" model. We return to these questions in Section 5.5.

3.7 Probabilistic models for two dimensions.

Since we focus on the invariance of algorithm executions under similarity transformations, we assume that the two random variables $|u|$ and $z = v/u$ are independent and consider densities F on pairs of vectors (u,v) which are of the form $F(u,v) = f_1(|u|) \cdot f(v/u)$. Moreover, it is sufficient to consider pairs (u,v) of size M with a first vector u of the form $u = (c,0)$ with $\ell(c^2) = M$. Finally, we define the discrete models of size M as

$$\Omega_M := \{(u,v) \in \mathbb{Z}^4; \quad \frac{v}{u} \in \mathcal{B} \setminus \mathcal{F}, \quad u = (c,0) \quad \ell(c^2) = M\},$$

$$\widetilde{\Omega}_M := \{(u,v) \in \mathbb{Z}^4; \quad \frac{v}{u} \in \widetilde{\mathcal{B}} \setminus \widetilde{\mathcal{F}}, \quad u = (c,0) \quad \ell(c^2) = M\}.$$

In both cases, the complex $z = v/u$ belongs to $\mathbb{Q}[i]$ and is of the form $(a/c) + i(b/c)$. When the integers c and M tend to ∞, this discrete model "tends" to a continuous model, and the density f is defined on a subset of $\mathbb{C}$. It is sometimes more convenient to view this density as a function defined on $\mathbb{R}^2$, and we denote by $\underline{f}$ the function f viewed as a function of two real variables x, y. It is clear that the rôles of two variables x, y are not of the same importance: the variable $y = \Im(z)$ plays the crucial rôle, whereas the variable $x = \Re(z)$ plays an auxiliary rôle. This is why the two main models that are now presented involve densities $\underline{f}(x,y)$ which only depend on y.

Results of Akhavi [1] and Akhavi, Marckert, Rouault [2] show that densities "with valuation" play a natural rôle in lattice reduction algorithms. We are then led to consider the 2–dimensional bases (u,v) which follow the so–called model of valuation r (with $r > -1$), for which

$$\mathbb{P}\left[(u,v); \quad \frac{|\det(u,v)|}{\max(|u|,|v|)^2} \leq y\right] = \Theta(y^{r+1}), \qquad \text{when} \quad y \to 0.$$

We note that, when the valuation r tends to -1, this model tends to the "one dimensional model", where u and v are colinear. In this case, the Gauss Algorithm "tends" to the Euclidean Algorithm, and it is important to precisely describe the transition. This model "with valuation" was already presented in [21] in a slightly different context, but not actually studied there.

The model with valuation defines a scale of densities, for which the weight of skew bases may vary. When r tends to -1, almost all the input bases are formed of vectors which form a very small angle, and, with a high probability, they represent hard instances for reducing the lattice.

In the complex framework, a density f on the set $\mathcal{S} \subset \mathbb{C} \setminus \mathbb{R}$ is of valuation r (with $r > -1$) if it is of the form

$$f(z) = |\Im(z)|^r \cdot g(z) \qquad \text{where} \quad g(z) \neq 0 \quad \text{for } \Im(z) = 0. \tag{25}$$

Such a density is called of type (r,g). We often deal with the standard density of valuation r,

$$f_r(z) = \frac{1}{A(r)} |\Im(z)|^r \qquad \text{with} \quad A(r) = \iint_{\mathcal{B}\setminus\mathcal{F}} y^r dxdy. \tag{26}$$

Of course, when $r = 0$, we recover the uniform distribution on $\mathcal{B} \setminus \mathcal{F}$ with $A(0) = (1/12)(2\pi + 3\sqrt{3})$. When $r \to -1$, then $A(r)$ is $\Theta[(r+1)^{-1}]$. More precisely

$$A(r) - \frac{1}{r+1}\left(\frac{\sqrt{3}}{2}\right)^{r+1} = \log\frac{4}{3}.$$

Notations. The (continuous) model relative to a density f is denoted with an index of the form $\langle f \rangle$, and when the valuation is the standard density of valuation r, the model is denoted with an index of the form (r). The discrete models are denoted by two indices, the integer size M and the index which describes the function f, as previously.

3.8 The LLL algorithm and the complex framework.

Consider a lattice of $\mathbb{R}^n$ generated by a set $B := \{b_1, b_2, \ldots, b_n\}$ of n independent vectors. The LLL algorithm "reduces" the basis B by successively dealing with two-dimensional lattices $\mathcal{L}_k$ generated by

the so-called local bases B_k: The k-th local basis B_k is formed with the two vectors u_k, v_k, defined as the orthogonal projection of b_k, b_{k+1} on the orthogonal of the subspace $\langle b_1, b_2, \ldots, b_{k-1}\rangle$. The LLL algorithm is a succession of calls to the Gauss algorithm on these local bases, and it stops when all the local bases are reduced (in the Gauss meaning). Then, the complex output $\hat{z}_k$ defined from $(\hat{u}_k, \hat{v}_k)$ as in (1) is an element of the fundamental domain $\mathcal{F}$. Figure 1 (on the right) shows the experimental distribution of outputs $\hat{z}_k$, which does not seem to depend on index $k \in [1..n]$. There is an accumulation of points in the "corners" of $\mathcal{F}$, and the mean value of parameter γ is close to 1.04.

4 Analysis of the output parameters.

This section describes the probabilistic behaviour of output parameters: we first analyze the output densities, then we focus on the geometry of our three main parameters defined in (11, 12). We shall use the PGAUSS Algorithm for studying the output parameters.

4.1 Output densities.

For studying the evolution of distributions (on complex numbers), we are led to consider the 2–variables function $\underline{h}$ that corresponds to the complex mapping $z \mapsto h(z)$. More precisely, we consider the function $\underline{h}$ which is conjugated to $(v,w) \mapsto (h(v), h(w))$ with respect to map Φ, namely $\underline{h} = \Phi^{-1} \circ (h,h) \circ \Phi$, where mappings Φ, Φ^{-1} are linear mappings $\mathbb{C}^2 \to \mathbb{C}^2$ defined as

$$\Phi(x,y) = (z = x + iy, \bar{z} = x - iy), \qquad \Phi^{-1}(z,\bar{z}) = \left(\frac{z+\bar{z}}{2}, \frac{z+\bar{z}}{2i}\right).$$

Since Φ and Φ^{-1} are linear mappings, the Jacobian $J\underline{h}$ of the mapping $\underline{h}$ satisfies

$$J\underline{h}(x,y) = |h'(z) \cdot h'(\bar{z})| = |h'(z)|^2, \tag{27}$$

since h has real coefficients. Consider any measurable set $\mathcal{A} \subset \mathcal{F}$. The final density $\hat{f}$ on $\mathcal{A}$ is brought by all the antecedents $h(\mathcal{A})$ for $h \in \mathcal{G}$, which form disjoints subsets of $\mathcal{B} \setminus \mathcal{F}$. Then,

$$\iint_{\mathcal{A}} \hat{f}(\hat{x},\hat{y})\, d\hat{x}\, d\hat{y} = \sum_{h \in \mathcal{G}} \iint_{\underline{h}(\mathcal{A})} f(x,y)\, dx\, dy.$$

Using the expression of the Jacobian (27), and interverting integral and sum lead to

$$\sum_{h \in \mathcal{G}} \iint_{\mathcal{A}} |h'(\hat{z})|^2 f \circ \underline{h}(\hat{x},\hat{y}) d\hat{x} d\hat{y} = \iint_{\mathcal{A}} \left(\sum_{h \in \mathcal{G}} |h'(\hat{z})|^2 f \circ \underline{h}(\hat{x},\hat{y}) \right) d\hat{x} d\hat{y}.$$

Finally, we have proven:

Theorem 1. (i) *The output density $\hat{f}$ on the fundamental domain $\mathcal{F}$ can be expressed as a function of the input density f on $\mathcal{B} \setminus \mathcal{F}$ as*

$$\hat{f}(\hat{x},\hat{y}) = \sum_{h \in \mathcal{G}} |h'(\hat{z})|^2 f \circ \underline{h}(\hat{x},\hat{y}),$$

where $\mathcal{G}$ is the set of LFTs used by the PGAUSS *algorithm defined in Proposition 2.*

(*ii*) *In the same vein, the output density* $\hat{f}$ *on the fundamental domain* $\widetilde{\mathcal{F}}$ *can be expressed as a function of the input density* f *on* $\widetilde{\mathcal{B}} \setminus \widetilde{\mathcal{F}}$ *as*

$$\hat{f}(\hat{x},\hat{y}) = \sum_{h \in \widetilde{\mathcal{G}}} |h'(\hat{z})|^2 f \circ \underline{h}(\hat{x},\hat{y}),$$

where $\widetilde{\mathcal{G}}$ *is the set of LFTs used by the* AGAUSS *algorithm defined in Proposition 3.*
(*iii*) *Finally, the output density* $\hat{f}$ *on the domain* $\widetilde{\mathcal{B}} \setminus \mathcal{D}$ *can be expressed as a function of the input density* f *on* $\mathcal{D}$ *as*

$$\hat{f}(\hat{x},\hat{y}) = \sum_{h \in \mathcal{H}^+} |h'(\hat{z})|^2 f \circ \underline{h}(\hat{x},\hat{y}),$$

where $\mathcal{H}$ *is the set of LFTs used by the* COREGAUSS *algorithm defined in Proposition 3.*

4.2 The irruption of Eisenstein series.

We now analyze an important particular case, where the initial density is the standard density of valuation r defined in (26). Since each element of $\mathcal{G}$ gives rise to a unique pair (c,d) with $c \geq 1, \gcd(c,d) = 1$ for which

$$|h'(\hat{z})| = \frac{1}{|c\hat{z}+d|^4}, \qquad f_r \circ \underline{h}(\hat{x},\hat{y}) = \frac{1}{A(r)} \frac{\hat{y}^r}{|c\hat{z}+d|^{2r}}, \tag{28}$$

$$\text{the output density on } \mathcal{F} \text{ is} \quad \hat{f}_r(\hat{x},\hat{y}) = \frac{1}{A(r)} \sum_{\substack{(c,d)=1 \\ c \geq 1}} \frac{\hat{y}^r}{|c\hat{z}+d|^{4+2r}}\,. \tag{29}$$

It is natural to compare this density to the density relative to the measure relative to "random lattices": in the particular case of two dimensions, the set $X_2 = SL_2(\mathbb{R})/SL_2(\mathbb{Z})$ is exactly[¶] the fundamental domain $\mathcal{F}$. Moreover, the measure of density $\Im(z)^{-2}$ is invariant under the action of $PSL_2(\mathbb{Z})$: indeed, for any LFT h with $\det h = \pm 1$, one has

$$|\Im(h(z))| = |\Im(z)| \cdot |h'(z)|, \qquad \text{so that} \quad \iint_{h(\mathcal{A})} \frac{1}{y^2} dxdy = \iint_{\mathcal{A}} |h'(z)|^2 \frac{1}{\Im(h(z))^2} dxdy = \iint_{\mathcal{A}} \frac{1}{y^2} dxdy.$$

Then, the probability ν_2 on $\mathcal{F}$ of density[‖]

$$\eta(x,y) := \frac{3}{\pi} \frac{1}{y^2} \tag{30}$$

is invariant under the action of $PSL_2(\mathbb{Z})$. If we make apparent this density η inside the expression of $\hat{f}_r$ provided in (29), we obtain:

Theorem 2. *When the initial density on* $\mathcal{B} \setminus \mathcal{F}$ *is the standard density of valuation* r*, denoted by* f_r *and defined in (26), the output density of the* PGAUSS *algorithm on* $\mathcal{F}$ *involves the Eisenstein series* E_s *of*

[¶] Not exactly: up to a convenient definition of $\mathcal{F}$ on its frontier.
[‖] the integral $\iint_{\mathcal{F}} \eta(x,y)dxdy = 1$.

weight $s = 2+r$: With respect to the Haar measure μ on $\mathcal{F}$, whose density η is defined in (30), the output density $\hat{f}_r$ is expressed as

$$\hat{f}_r(x,y)\,dxdy = \frac{\pi}{3A(r)} F_{2+r}(x,y)\,\eta(x,y)dxdy, \quad \text{where} \quad F_s(x,y) = \sum_{\substack{(c,d)=1\\ c\geq 1}} \frac{y^s}{|cz+d|^{2s}}.$$

is closely related to the classical Eisenstein series E_s of weight s, defined as

$$E_s(x,y) := \frac{1}{2} \sum_{\substack{(c,d)\in\mathbb{Z}^2\\ (c,d)\neq(0,0)}} \frac{y^s}{|cz+d|^{2s}} = \zeta(2s)\cdot[F_s(x,y)+y^s].$$

When $r \to -1$, classical results about Eisenstein series prove that

$$E_s(x,y) \sim_{s\to 1} \frac{1}{2(s-1)} \qquad \text{so that} \quad \lim_{r\to -1} \frac{\pi}{3A(r)} F_{2+r}(x,y) = 1,$$

which imply that the ouput distribution relative to the input distribution of valuation r tends to the distribution ν_2 relative to random lattices when $r \to -1$.

The series E_s are Maass forms (see for instance the book [5]): they play an important rôle in the theory of modular forms, because E_s is an eigenfunction for the Laplacian, relative to the eigenvalue $s(1-s)$. The irruption of Eisenstein series in the lattice reduction framework was unexpected, and, at the moment, it is not clear how to use the classical well-known properties of the Eisenstein series E_s for studying the output densities.

4.3 Geometry of the output parameters.

The main output parameters are defined in (11,12). For $X \in \{\lambda,\mu,\gamma\}$, we denote by $X(z)$ the value of X on basis $(1,z)$, and there are close relations between $X(u,v)$ and $X(z)$ for $z = v/u$:

$$\lambda(u,v) = |u|\cdot\lambda(z), \qquad \mu(u,v) = |u|\cdot\mu(z), \qquad \gamma(u,v) = \gamma(z).$$

Moreover, the complex versions of parameters λ,μ,γ can be expressed with the input–output pair $(z,\hat{z})$.

Proposition 4. *If $z = x+iy$ is an initial complex number of $\mathcal{B}\setminus\mathcal{F}$ leading to a final complex $\hat{z} = \hat{x}+i\hat{y}$ of $\mathcal{F}$, then the three main output parameters defined in (11,12) admit the following expressions*

$$\det L(z) = y, \qquad \lambda^2(z) = \frac{y}{\hat{y}}, \qquad \mu^2(z) = y\hat{y}, \qquad \gamma(z) = \frac{1}{\hat{y}}.$$

Then, the following inclusions hold:

$$[\lambda(z) = t] \subset \left[\Im(z) \geq \frac{\sqrt{3}}{2}t^2\right], \qquad [\mu(z) = u] \subset \left[\Im(z) \leq \frac{2}{\sqrt{3}}u^2\right]. \tag{31}$$

If z leads to $\hat{z}$ by using the LFT $h \in \mathcal{G}$ with $z = h(\hat{z}) = (a\hat{z}+b)/(c\hat{z}+d)$, then:

$$\lambda(z) = |cz-a|, \qquad \gamma(z) = \frac{|cz-a|^2}{y}, \qquad \mu(z) = \frac{y}{|cz-a|}.$$

$$\begin{array}{lcll}
\mathtt{Fo}(a,c,\rho) & := & \{(x,y);\quad y>0, & \left(x-\dfrac{a}{c}\right)^2+\left(y-\dfrac{\rho}{2c^2}\right)^2\le\dfrac{\rho^2}{4c^4}\} \\
\mathtt{Fa}(a,c,t) & := & \{(x,y);\quad y>0, & \left(x-\dfrac{a}{c}\right)^2+y^2\le\dfrac{t^2}{c^2}\} \\
\mathtt{Se}(a,c,u) & := & \{(x,y);\quad y>0, & |y|\le\dfrac{cu}{\sqrt{1-c^2u^2}}\left|x-\dfrac{a}{c}\right|\} \qquad \text{for } cu\le 1 \\
\mathtt{Se}(a,c,u) & := & \{(x,y);\quad y>0,\} & \qquad \text{for } cu\ge 1
\end{array}$$

Figure 9: The three main domains of interest: the Ford disks $\mathtt{Fo}(a,c,\rho)$, the Farey disks $\mathtt{Fa}(a,c,t)$, the angular sectors $\mathtt{Se}(a,c,u)$.

Proof. If the initial pair (v_1,v_0) is written as in (4) as

$$\begin{pmatrix} v_1 \\ v_0 \end{pmatrix} = \mathcal{M}^{-1}\begin{pmatrix} v_{p+1} \\ v_p \end{pmatrix}, \qquad \text{with} \quad \mathcal{M}^{-1} := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{and} \quad z=h(\hat z)=\frac{a\hat z+b}{c\hat z+d},$$

then the total length decrease satisfies

$$\frac{|v_p|^2}{|v_0|^2}=\frac{|v_p|^2}{|cv_{p+1}+dv_p|^2}=\frac{1}{|c\hat z+d|^2}=|h'(\hat z)|, \tag{32}$$

[we have used the fact that $\det\mathcal{M}=1$.] This proves that $\lambda^2(z)$ equals $|h'(\hat z)|$ as soon as $z=h(\hat z)$. Now, for $z=h(\hat z)$, the relations

$$y=\frac{\hat y}{|c\hat z+d|^2}, \qquad \hat y=\frac{y}{|cz-a|^2},$$

easily lead to the end of the proof. ■

4.4 Domains relative to the output parameters.

We now consider the following well-known domains defined in Figure 9. The Ford disk $\mathtt{Fo}(a,c,\rho)$ is a disk of center $(a/c,\rho/(2c^2))$ and radius $\rho/(2c^2)$: it is tangent to $y=0$ at point $(a/c,0)$. The Farey disk $\mathtt{Fa}(a,c,t)$ is a disk of center $(a/c,0)$ and radius t/c. Finally, the angular sector $\mathtt{Se}(a,c,u)$ is delimited by two lines which intersect at a/c, and form with the line $y=0$ angles equal to $\pm\arcsin(cu)$. These domains intervene for defining the three main domains of interest.

Theorem 3. *The domains relative to the main output parameters, defined as*

$$\Gamma(\rho):=\{z\in\mathcal{B}\setminus\mathcal{F};\quad \gamma(z)\le\rho\}, \qquad \Lambda(t):=\{z\in\mathcal{B}\setminus\mathcal{F};\quad \lambda(z)\ \le t\},$$

$$M(u):=\{z\in\mathcal{B}\setminus\mathcal{F};\quad \mu(z)\ \le u\}$$

are described with Ford disks $\mathtt{Fo}(a,c,\rho)$*, Farey disks* $\mathtt{Fa}(a,c,t)$*, and angular sectors* $\mathtt{Se}(a,c,u)$*. More precisely, if* $\mathcal{F}_{(a,c)}$ *denotes the Festoon relative to pair* (a,c) *defined in (20) and if the set* $\mathcal{C}$ *is defined as in (19), one has:*

$$\Gamma(\rho) = \bigcup_{(a,c)\in\mathcal{C}} \mathtt{Fo}(a,c,\rho)\cap\mathcal{F}_{(a,c)}, \qquad \Lambda(t) = \bigcup_{(a,c)\in\mathcal{C}} \mathtt{Fa}(a,c,t)\cap\mathcal{F}_{(a,c)},$$

$$M(u) = \bigcup_{(a,c)\in\mathcal{C}} \mathtt{Se}(a,c,u)\cap\mathcal{F}_{(a,c)}.$$

Each "local" definition of sets Λ,Γ,M can be transformed in a "global definition" which no more involves the festoons. It involves, for instance, a subfamily of complete (intersecting) Farey disks (for Λ), or quadrilaterals (for M) [see Figure 10].
Define the subset $\mathcal{P}(t)$ of set $\mathcal{P}$ defined in Section 3.4 as

$$\mathcal{P}(t) := \{(c,d);\quad c,d\geq 1, ct\leq 1, dt\leq 1, (c+d)t>1, (c,d)=1\},$$

and, for a pair $(a/c,b/d)$ of rationals satisfying $ad-bc=-1$, denote by $\mathcal{S}(a/c,b/d)$ the intersection of $\mathcal{B}\setminus\mathcal{F}$ with the vertical strip $\{(a/c)\leq x\leq(b/d)\}$.

The "global" definition of domain $\Lambda(t)$ is provided in [12]: consider a pair $(a/c,b/d)$ of rationals satisfying $ad-bc=-1$ whose denominator pair (c,d) belongs to $\mathcal{P}(t)$. There exists a local characterization of $\Lambda(t)\cap\mathcal{S}(a/c,b/d)$ which does not depend any longer on the festoons, namely

$$\Lambda(t)\cap\mathcal{S}(a/c,b/d) = \mathtt{Fa}_+(a,c,t)\cup\mathtt{Fa}_-(b,d,t)\cup\mathtt{Fa}(a+b,c+d,t). \tag{33}$$

Here $\mathtt{Fa}_+(a,c,t),\mathtt{Fa}_-(b,d,t)$ are the half Farey disks formed with the intersections of $\mathtt{Fa}(a,c,t)$, $\mathtt{Fa}(b,d,t)$ with the strip $\mathcal{S}(a/c,b/d)$. The domain of (33) is exactly the union of the two disks $\mathtt{Fa}_+(a,c,t)$ and $\mathtt{Fa}_-(b,d,t)$ if and only if the condition $(c^2+d^2+cd)t^2>1$ holds. The Farey disk relative to the median $(a+b)/(c+d)$ only plays a rôle when $(c^2+d^2+cd)t^2\leq 1$. This last condition is satisfied in particular if $\max(ct,dt)$ is smaller than $1/\sqrt{3}$, or, equivalently, when both c and d belong to the interval $[0,1/(t\sqrt{3})]$. When $t\to 0$, the proportion of pairs $(a/c,b/d)$ for which the intersection of Eqn (33) is formed with three disks tends to $1/6$.

Then the following inclusions hold (where the "left" union is a disjoint union)

$$\bigcup_{\substack{(a,c)\in\mathcal{C}\\ c\leq 1/t}} \mathtt{Fa}(a,c,t) \subset \Lambda(t) \subset \bigcup_{\substack{(a,c)\in\mathcal{C}\\ c\leq 2/(\sqrt{3}t)}} \mathtt{Fa}(a,c,t). \tag{34}$$

We now deal with the domain $M(u)$: consider a pair $(a/c,b/d)$ of rationals satisfying $ad-bc=-1$ whose denominator pair (c,d) belongs to $\mathcal{P}(u)$. Then, the denominator f of any rational e/f of the interval $]a/c,b/d[$ satisfies $fu\geq(c+d)u>1$, and the domain $\mathtt{Se}(e,f,u)\cap\mathcal{F}_{(e,f)}$ equals the whole festoon $\mathcal{F}_{(e,f)}$. We obtain a characterization of $M(u)$ which does not depend any longer on the festoons, namely

$$M(u)\cap\mathcal{S}(a/c,b/d) = \mathtt{Se}(a,c,u)\cap\mathtt{Se}(b,d,u)\cap\mathtt{Se}(b-a,d-c,u). \tag{35}$$

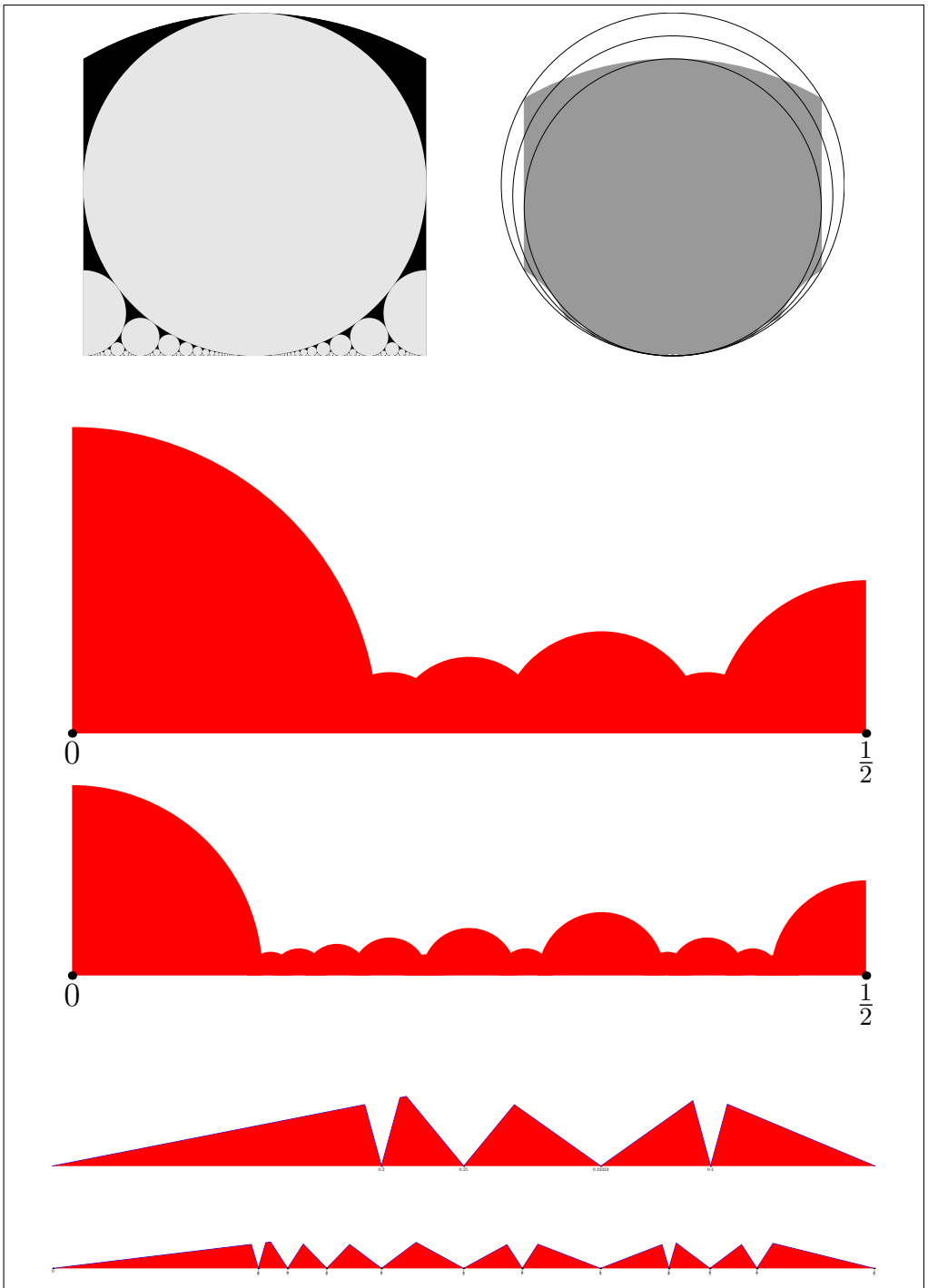

Figure 10: On the top: the domain $\Gamma(\rho) := \{z;\ \gamma(z) \le \rho\}$. On the left, $\rho = 1$ (in white). On the right, the festoon $\mathcal{F}_{(0,1)}$ together with $\mathtt{Fo}(0,1,\rho)$ for $\rho = 1, \rho_0 = 2/\sqrt{3}, \rho_1 = (1+\rho_0)/2$. – On the middle, the domain $\Lambda(t) \cap \mathcal{B}_+$, with $\Lambda(t) := \{z;\ \lambda(z) \le t\}$ for $t = 0.193$ and $t = 0.12$. – On the bottom, the domain $M(u) \cap \mathcal{B}_+$ with $M(u) := \{z;\quad \mu(z) \le u\}$ for $u = 0.193$ and $u = 0.12$.

The domain of (35) may coincide with the triangle $\mathtt{Se}(a,c,u) \cap \mathtt{Se}(b,d,u)$ when the two sides of the triangle intersect on the frontier $\mathcal{F}_{(a,c)} \cap \mathcal{F}_{(b,d)}$. But, this is not always the case since the two sides of the triangle may intersect inside the festoon $\mathcal{F}_{(b-a,d-c)}$. In this case, the domain of (35) is a "true" quadrilateral. This last case occurs if and only if the condition $(c^2+d^2-cd)u^2 \geq (3/4)$ holds. This condition is satisfied in particular if $\min(cu,du)$ is larger than $\sqrt{3}/2$. This occurs in the interval $[a/c, b/d]$ when both c and d belong to $[(\sqrt{3}/2)(1/u), 1/u]$. When $u \to 0$, the proportion of pairs $(a/c, b/d)$ for which the intersection of Eqn (35) is a "true" quadrilateral tends to $2[1-(\sqrt{3}/2)]^2$.

4.5 Distribution functions of output parameters.

Computing the measure of disks and angular sectors with respect to a standard density of valuation r leads to the estimates of the main output distributions:

Theorem 4. *When the initial density on $\mathcal{B} \setminus \mathcal{F}$ is the standard density of valuation r, the three main output parameters admit the following distributions:*

$$\begin{array}{lcll} \mathbb{P}_{(r)}[\gamma(z) \leq \rho] & = & A_1(r) \cdot \dfrac{\zeta(2r+3)}{\zeta(2r+4)} \cdot \rho^{r+2} & \text{for} \quad \rho \leq 1, \\ \\ \mathbb{P}_{(r)}[\lambda(z) \leq t] & = & \Theta(t^{r+2}) & \text{for} \quad r > 0, \\ \mathbb{P}_{(r)}[\lambda(z) \leq t] & = & \Theta(t^2 |\log t|) & \text{for} \quad r = 0, \\ \mathbb{P}_{(r)}[\lambda(z) \leq t] & = & \Theta(t^{2r+2}) & \text{for} \quad r < 0, \\ \\ \mathbb{P}_{(r)}[\mu(z) \leq u] & = & \Theta(u^{2r+2}). & \end{array}$$

In the case when $r \geq 0$, there are precise estimates for parameter λ, when $t \to 0$:

$$\begin{array}{lcll} \mathbb{P}_{(r)}[\lambda(z) \leq t] & \sim_{t\to 0} & A_2(r) \dfrac{\zeta(r+1)}{\zeta(r+2)} \cdot t^{r+2} & \text{for} \quad r > 0, \\ \\ \mathbb{P}_{(r)}[\lambda(z) \leq t] & \sim_{t\to 0} & A_2(0) \dfrac{1}{\zeta(2)} t^2 |\log t| & \text{for} \quad r = 0. \end{array}$$

For any valuation $r > -1$, the following inequalities hold

$$\mathbb{P}_{(r)}[\lambda(z) \leq t] \geq \frac{1}{A(r)} \frac{1}{r+1} \left(\frac{\sqrt{3}}{2}\right)^{r+1} t^{2r+2}, \qquad \mathbb{P}_{(r)}[\mu(z) \leq u] \leq A_3(r) \left(\frac{2}{\sqrt{3}}\right)^{r+1} u^{2r+2}.$$

The constants $A_i(r)$ involve Euler's Gamma function and the measure $A(r)$ defined in (26) in the following way

$$A_1(r) := \frac{\sqrt{\pi}}{A(r)} \frac{\Gamma(r+3/2)}{\Gamma(r+3)}, \qquad A_2(r) = \frac{\sqrt{\pi}}{2A(r)} \frac{\Gamma((r+1)/2)}{\Gamma(r/2+2)}, \qquad A_3(r) = \frac{1}{A(r)} \frac{1}{(r+2)(r+1)}.$$

Proof. [Sketch] First, the measure (wrt the standard density of valuation r) of each basic domain (disks of Farey or Ford type, triangles) is easy to compute. For a disk of radius ρ, centered on the real axis (resp

tangent to the real axis), this measure equals $2A_2(r)\rho^{r+2}$ (resp. $A_1(r)(2\rho)^{r+2}$), and involves constants $A_i(r)$ defined in the theorem. Furthermore, if φ denotes the Euler totient function, there are exactly $\varphi(c)$ basic disks of the same radius in each domain. Then, the identity

$$\sum_{c\geq 1}\frac{\varphi(c)}{c^s}=\frac{\zeta(s-1)}{\zeta(s)},\qquad \text{for}\quad \Re s\geq 2$$

explains the occurrence of the function $\zeta(s-1)/\zeta(s)$ in our estimates. Consider two examples:

(a) For $\rho\leq 1$, the domain $\Gamma(\rho)$ is made with disjoint Ford disks of radius $\rho/(2c^2)$. An easy application of previous principles leads to the result.

(b) For $\Lambda(t)$, these same principles, together with relation (34) entail the following inequalities

$$t^{r+2}\sum_{c\leq 1/t}\frac{\varphi(c)}{c^{r+2}}\leq\frac{1}{A_2(r)}\mathbb{P}_{(r)}[\lambda(z)\leq t]\leq t^{r+2}\sum_{c\leq 2/(\sqrt{3}t)}\frac{\varphi(c)}{c^{r+2}},$$

and there are several cases when $t\to 0$ according the sign of r. For $r>0$, the Dirichlet series involved are convergent. For $r\leq 0$, we consider the series

$$\sum_{c\geq 1}\frac{\varphi(c)}{c^{r+2+s}}=\frac{\zeta(s+r+1)}{\zeta(s+r+2)},$$

(which has a pôle at $s=-r$), and Tauberian theorems (or Perron's formula for $r=0$) provide an estimate for

$$\sum_{c\leq N}\frac{\varphi(c)}{c^{r+2}}\sim_{N\to\infty}\frac{1}{\zeta(2)}N^{r+1},\quad (\text{for } r>0),\quad\text{and}\quad\sum_{c\leq N}\frac{\varphi(c)}{c^2}\sim_{N\to\infty}\frac{1}{\zeta(2)}N\log N.$$

For domain $M(u)$, the study of quadrilaterals can be performed in a similar way. The measure (wrt standard density of valuation r) of a triangle of horizontal basis a and height h is of the form $A_3(r)\,a\,h^{r+1}$, and involves the constant $A_3(r)$ defined in the theorem. Furthermore, the height of each quadrilateral of $M(u)$ is $\Theta(u^2)$, and the sum of the bases a equal 1. Then $\mathbb{P}_{(r)}[\mu(z)\leq u]=\Theta(u^{2r+2})$. Furthermore, using the inclusions of (31) leads to the inequality. ■

Interpretation of the results. We provide a first interpretation of the main results described in the previous theorem.

(i) For any $y_0\geq 1$, the probability of the event $[\hat{y}\geq y_0]$ is

$$\mathbb{P}_{(r)}[\hat{y}\geq y_0]=\mathbb{P}_{(r)}[\gamma(z)\leq\frac{1}{y_0}]=A_1(r)\frac{\zeta(2r+3)}{\zeta(2r+4)}\frac{1}{y_0^{r+2}}.$$

This defines a function of the variable $y_0\mapsto\psi_r(y_0)$, whose derivative is a power function of variable y_0, of the form $\Theta({y_0}^{-r-3})$. This derivative is closely related to the output density $\hat{f}_r$ of Theorem 2, via the equality

$$\psi_r'(y_0):=\int_{-1/2}^{+1/2}\hat{f}_r(x,y_0)dx.$$

Now, when $r \to -1$, the function $\psi'_r(y)$ has a limit which is exactly the density η, defined in (30), which is associated to the Haar measure μ_2 defined in 7.2.

(ii) The regime of the distribution function of parameter λ changes when the sign of valuation r changes. There are two parts in the domain $\Lambda(t)$: the lower part, which is the horizontal strip $[0 \leq \Im(z) \leq (2/\sqrt{3})t^2]$, and the upper part defined as the intersection of $\Lambda(t)$ with the horizontal strip $[(2/\sqrt{3})t^2 \leq \Im(z) \leq t]$. For negative values of r, the measure of the lower part is dominant, while, for positive values of r, this is the upper part which has a dominant measure. For $r = 0$, there is a phase transition between the two regimes: this occurs in particular in the usual case of a uniform density.

(iii) In contrast, the distribution function of parameter μ has always the same regime. In particular, for negative values of valuation r, the distribution functions of the two parameters, λ and μ are of the same form.

Open questions. Is it possible to get information on the constants hidden in the Θ's for parameter μ (in case of any valuation) and for λ (in case of a negative valuation)? This will be important in the study of the LLL algorithm (See Section 4.7).

Is it possible to describe the distribution function of parameter ρ for $\rho > 1$? Figure 10 [top] shows that its regime changes at $\rho = 1$. This will be important for obtaining a precise estimate of the mean value $\mathbb{E}_{(r)}[\gamma]$ as a function of r and comparing this value to experiments reported in the Introduction.

4.6 The corners of the fundamental domain

With Theorem 4, it is possible to compute the probability that an output basis lies in the corners of the fundamental domain, and to observe its evolution as a function of valuation r. This is a first step for a sharp understanding of Figure 1[right].

Proposition 5. *When the initial density on $\mathcal{B} \setminus \mathcal{F}$ is the standard density of valuation r, the probability for an output basis to lie on the corners of the fundamental domain is equal to*

$$C(r) := 1 - A_1(r) \cdot \frac{\zeta(2r+3)}{\zeta(2r+4)}.$$

There are three main cases of interest for $1 - C(r)$

$$[r \to -1]: \quad \frac{3}{\pi} \qquad [r = 0]: \quad \frac{3\pi}{2\pi + 3\sqrt{3}} \frac{\zeta(3)}{\zeta(4)} \qquad [r \to \infty]: \quad \sqrt{\frac{\pi}{r}} e^{-3/2}.$$

4.7 Returning to the LLL Algorithm.

The LLL algorithm aims at reducing all the local bases B_k in the Gauss meaning. For obtaining the output density at the end of the algorithm, it is interesting to describe the evolution of the distribution of the local bases along the execution of the algorithm.

There exists for instance a variant of the LLL algorithm, introduced by Villard [23] which performs a succession of phases of two types, the odd ones, and the even ones. We adapt this variant and choose to perform the AGAUSS algorithm, because, as we shall explain in Section 6, it has a better structure. During one even (resp. odd) phase, the *whole* AGAUSS algorithm is performed on all local bases B_k with even

(resp. odd) indices. Since local bases with odd (resp. even) indices are "disjoint", it is possible to perform these Gauss algorithms *in parallel*. This is why Villard has introduced this algorithm.
Consider the Odd phase, and two successive bases B_k and B_{k+2} with odd indices, respectively endowed with some initial densities F_k and F_{k+2}. Denote by z_k and z_{k+2} the complex numbers associated to local bases (u_k, v_k) and (u_{k+2}, v_{k+2}) via relation (1). Then, the LLL algorithm reduces these two local bases (in the Gauss meaning) and computes two reduced local bases denoted by $(\hat{u}_k, \hat{v}_k)$ and $(\hat{u}_{k+2}, \hat{v}_{k+2})$, which satisfy in particular

$$|\hat{v}_k^\star| = |u_k| \cdot \mu(z_k), \qquad |\hat{u}_{k+2}| = |u_{k+2}| \cdot \lambda(z_{k+2}).$$

Then our Theorem 4 provides insights on the distribution of $\mu(z_k), \lambda(z_{k+2})$. Since, in our model, the random variables $|u_k|$ and z_k (resp. $|u_{k+2}|$ and z_{k+2}) are independent, we obtain a precise information on the distribution of the norms $|\hat{v}_k^\star|, |\hat{u}_{k+2}|$.
In the Even phase, the LLL algorithm considers the local bases with an odd index. Now, the basis B_{k+1} is formed (up to a similarity) from the two previous output bases, as:

$$u_{k+1} = |\hat{v}_k^\star|, \qquad v_{k+1} = \nu |\hat{v}_k^\star| + i |\hat{u}_{k+2}|,$$

where ν can be assumed to follow a uniform law on $[-1/2, +1/2]$. Moreover, at least at the beginning of the algorithm, the two variables $|\hat{v}_k^\star|, |\hat{u}_{k+2}|$ are independent. All this allows to obtain precise informations on the new input density F_{k+1} of the local basis B_{k+1}. We then hope to "follow" the evolution of densities of local bases along the execution of the LLL algorithm.

5 Analysis of the execution parameters.

We finally focus on parameters which describe the execution of the algorithm: we are mainly interested in the bit–complexity, but we also study additive costs that may be of independent interest. We here use an approach both based on tools that come from dynamical system theory and analysis of algorithms. We shall use here the AGAUSS algorithm, with the decomposition provided in Proposition 3.

5.1 Dynamical systems and transfer operators.

Recall that a dynamical system is a pair formed by a compact set X and a mapping $W : X \to X$ for which there exists a (finite or denumerable) set $\mathcal{Q}$, (whose elements are called digits), and a topological partition $\{X_q\}_{q \in \mathcal{Q}}$ of the set X in subsets X_q such that the restriction of W to each element X_q of the partition is C^2 and invertible. Here, we are led to so–called complete dynamical systems, where the restriction of $W|_{X_q} : X_q \to X$ is surjective. A special rôle is played by the set $\mathcal{H}$ of branches of the inverse function W^{-1} of W that are also naturally numbered by the index set $\mathcal{Q}$: we denote by $h_{\langle q \rangle}$ the inverse of the restriction $W|_{X_q}$, so that X_q is exactly the image $h_{\langle q \rangle}(X)$. The set $\mathcal{H}^k$ is the set of the inverse branches of the iterate W^k; its elements are of the form $h_{\langle q_1 \rangle} \circ h_{\langle q_2 \rangle} \circ \cdots \circ h_{\langle q_k \rangle}$ and are called the inverse branches of depth k. The set $\mathcal{H}^\star := \cup_{k \geq 0} \mathcal{H}^k$ is the semi-group generated by $\mathcal{H}$.

Given an initial point x in X, the sequence $\mathcal{W}(x) := (x, Wx, W^2x, \ldots)$ of iterates of x under the action of W forms the trajectory of the initial point x. We say that the system has a hole Y if any point of X eventually falls in Y: for any x, there exists $p \in \mathbb{N}$ such that $W^p(x) \in Y$.

The main study in dynamical systems concerns itself with the interplay between properties of the transformation W and properties of trajectories under iteration of the transformation. The behaviour of typical

trajectories of dynamical systems is more easily explained by examining the flow of densities. The time evolution governed by the map W modifies the density, and the successive densities $f_1, f_2, \ldots, f_n, \ldots$ describe the global evolution of the system at time $t = 0, t = 1, t = 2, \ldots$.
We will study here two dynamical systems, respectively related to the F-EUCLID algorithm and to CORE-GAUSS algorithm, and defined in Sections 3.3 and 3.5.

5.2 Case of the F-EUCLID system.

We first focus on the case when X is a compact interval of the real line. Consider the (elementary) operator $\mathbf{X}_{2s,[h]}$, relative to a mapping h, which acts on functions f of one variable, depends on some parameter s and is formally defined as

$$\mathbf{X}_{s,[h]}[f](x) = |h'(x)|^s \cdot f \circ h(x). \tag{36}$$

The operator $\mathbf{X}_{1,[h]}$ expresses the part of the new density which is brought when one uses the branch h, and the operator

$$\mathbf{H}_s := \sum_{h \in \mathcal{H}} \mathbf{H}_{s,[h]} \tag{37}$$

is called the transfer operator. For $s = 1$, the operator $\mathbf{H}_1 = \mathbf{H}$ is the density transformer, (or the Perron-Frobenius operator) which expresses the new density f_1 as a function of the old density f_0 via the relation $f_1 = \mathbf{H}[f_0]$. In the case of the F-EUCLID algorithm, due to the precise expression of the set $\mathcal{H}$, one has, for any $x \in \widetilde{I} = [0, 1/2]$

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

The density transformer $\mathbf{H}$ admits a unique invariant density $\psi(x)$ which involves the golden ratio $\phi = (1+\sqrt{5})/2$,

$$\psi(x) = \frac{1}{\log \phi} \left(\frac{1}{\phi + x} + \frac{1}{\phi^2 - x} \right).$$

This is the analog (for the F-EUCLID algorithm) of the celebrated Gauss density associated to the standard Euclid algorithm and equal to $(1/\log 2)1/(1+x)$.

The main properties of the F-EUCLID algorithm are closely related to spectral properties of the transfer operator $\mathbf{H}_s$, when it acts on a convenient functional space. We return to this fact in Section 5.4.

5.3 Case of the AGAUSS algorithm.

Theorem 1 describes the output density $\hat{f}$ as a function of the initial density f. The output density $\hat{f}(\hat{z})$ is written as a sum of all the portions of the density which are brought by all the antecedents $h(\hat{z})$, when $h \in \widetilde{\mathcal{G}}$. We have seen in the proof of this theorem that the Jacobian of the transformation $(x,y) \mapsto \underline{h}(x,y) = h(x+iy)$ intervenes in the expression of $\hat{f}$ as a function of f. Furthermore, the Jacobian $J\underline{h}(x,y)$ is equal to $|h'(z)|^2$. It would be natural to consider an (elementary) operator $\mathbf{Y}_{2s,[h]}$, of the form

$$\mathbf{Y}_{2s,[h]}[f](z) = |h'(z)|^{2s} \cdot f(h(z)).$$

In this case, the sum of such operators, taken over all the LFT's which intervene in one step of the AGAUSS algorithm, and viewed at $s = 1$, describes the new density which is brought at each point $z \in \widetilde{\mathcal{F}}$ during

this step, when the density on $\widetilde{\mathcal{B}} \setminus \widetilde{\mathcal{F}}$ is f. However, such an operator has not good properties, because the modulus $|h'(z)|$ does not define an analytic function. It is more convenient to introduce another elementary operator which acts on functions F of two variables, namely

$$\underline{\mathbf{X}}_{2s,[h]}[F](z,u) = \check{h}(z)^s \cdot \check{h}(u)^s \cdot F(h(z),h(u)),$$

where $\check{h}$ is the analytic extension of $|h'|$ to a complex neighborhood of $[0,1/2]$. Such an operator acts on analytic functions, and the equalities

$$\underline{\mathbf{X}}_{2s,[h]}[F](z,\bar{z}) = \mathbf{Y}_{2s,[h]}[f](z), \qquad \underline{\mathbf{X}}_{2s,[h]}[F](x,x) = \mathbf{X}_{2s,[h]}[f](x) \qquad \text{for} \quad f(z) := F(z,\bar{z}), \tag{38}$$

prove that the elementary operators $\underline{\mathbf{X}}_{2s,[h]}$ are extensions of the operators $\mathbf{X}_{2s,[h]}$ that are well-adapted to our purpose. Furthermore, they are also well-adapted to deal with densities with valuation. Indeed, when applied to a density f of valuation r, of the form $f(z) = F(z,\bar{z})$, when $F(z,u) = |z-u|^r L(z,u)$ involves an analytic function L which is non zero on the diagonal $z = u$, one has

$$\underline{\mathbf{X}}_{2s}[F](z,\bar{z}) = |y|^r \underline{\mathbf{X}}_{2s+r}[L](z,\bar{z}).$$

Such operators satisfy a crucial relation of composition: with multiplicative properties of the derivative of $g \circ h$, we easily remark that

$$\underline{\mathbf{X}}_{s,[h]} \circ \underline{\mathbf{X}}_{s,[g]} = \underline{\mathbf{X}}_{s,[g\circ h]}.$$

Then, the operators relative to the main set of LFT's $\widetilde{\mathcal{G}}, \mathcal{K}, \mathcal{H}$ associated to the AGAUSS algorithm via Proposition 3, defined as

$$\underline{\mathbf{H}}_s := \sum_{h\in\mathcal{H}} \underline{\mathbf{X}}_{s,[h]}, \qquad \mathbf{K}_s := \sum_{h\in\mathcal{K}} \underline{\mathbf{X}}_{s,[h]} \qquad \mathbf{G}_s := \sum_{h\in\widetilde{\mathcal{G}}} \underline{\mathbf{X}}_{s,[h]}, \tag{39}$$

satisfy with Proposition 3,

$$\mathbf{G}_s = \mathbf{K}_s \circ (I - \underline{\mathbf{H}}_s)^{-1} - I\,. \tag{40}$$

Remark that the operator $\underline{\mathbf{H}}_{2s}$ admits the nice expression

$$\underline{\mathbf{H}}_{2s}[F](z,u) = \sum_{(m,\varepsilon)\geq(2,1)} \left(\frac{1}{(m+\varepsilon z)(m+\varepsilon u)}\right)^{2s} \cdot F\left(\frac{1}{m+\varepsilon z}, \frac{1}{m+\varepsilon u}\right).$$

Due to (38), this is an extension of $\mathbf{H}_{2s}$ (defined in (37), which satisfies relation $\underline{\mathbf{H}}_{2s}[F](x,x) = \mathbf{H}_{2s}[f](x)$ when f is the diagonal map of F. Furthermore, assertions (ii) and (iii) of Theorem 1 can be re–written as: *Consider the densities (the input density f and the output density $\hat{f}$) as functions of two complex variables $z,\bar{z}$, namely $f(x,y) = F(z,\bar{z})$, $\hat{f}(x,y) = \hat{F}(z,\bar{z})$. Then*

$$\textit{(Assertion } (ii)\textit{)}: \quad \hat{F} = \mathbf{G}_2[F], \qquad \textit{(Assertion } (iii)\textit{)}: \quad \hat{F} = \underline{\mathbf{H}}_2 \circ (I - \underline{\mathbf{H}}_2)^{-1}[F]$$

and the operators $\mathbf{G}_2, \underline{\mathbf{H}}_2 \circ (I - \underline{\mathbf{H}}_2)^{-1}$ can be viewed as (total) "density transformers" of the algorithms (the AGAUSS *algorithm or the* COREGAUSS *algorithm) since they describe how the final density $\hat{F}$ can be expressed as a function of the initial density F.*

The operators defined in (39) are called transfer operators. For $s=1$, they coincide with density transformers, and, for other values of s, they can be wiewed as extensions of density transformers. They play a central rôle in studies of dynamical systems. The main idea in "dynamical analysis" methodology is to use these operators $\mathbf{X}_{2s,[h]}$ and to modify them in such a way that they become "generating operators" that generate themselves generating functions of interest. For instance, if a cost $c(h)$ is defined for the mapping h, it is natural to add a new parameter w for marking the cost, and consider the weighted operator $\underline{\mathbf{X}}_{s,w,(c),[h]}$ defined as

$$\underline{\mathbf{X}}_{2s,w,(c),[h]}[F](z,u) = \exp[wc(h)] \cdot \check{h}(z)^s \cdot \check{h}(u)^s \cdot F(h(z),h(u)).$$

Of course, when $w=0$, we recover the operator $\underline{\mathbf{X}}_{2s,[h]}$. When the cost c is additive, i.e., $c(g\circ h) = c(g)+c(h)$, the composition relation

$$\underline{\mathbf{X}}_{s,w,(c),[h]} \circ \underline{\mathbf{X}}_{s,w,(c),[g]} = \underline{\mathbf{H}}_{s,w,(c),[g\circ h]}$$

entails, with Proposition 3, an extension of (40) as

$$\mathbf{G}_{s,w,(c)} = \mathbf{K}_{s,w,(c)} \circ (I - \underline{\mathbf{H}}_{s,w,(c)})^{-1} - I \tag{41}$$

5.4 Functional analysis.

It is first needed to find a convenient functional space where the operator $\underline{\mathbf{H}}_s$ and its variants $\underline{\mathbf{H}}_{s,w,(c)}$ will possess good spectral properties : Consider the open disk $\mathcal{V}$ of diameter $[-1/2,1]$ and the functional space $B_\infty(\mathcal{V})$ of all functions F (of two variables) that are holomorphic in the domain $\mathcal{V}\times\mathcal{V}$ and continuous on the closure $\overline{\mathcal{V}}\times\overline{\mathcal{V}}$. Endowed with the sup-norm,

$$||F|| = \sup\{|F(z,u)|;\ (z,u)\in\mathcal{V}\times\mathcal{V}\},$$

$B_\infty(\mathcal{V})$ is a Banach space and the transfer operator $\underline{\mathbf{H}}_s$ acts on $\mathcal{B}_\infty(\mathcal{M})$ for $\Re(s)>(1/2)$ and is compact. Furthermore, when weighted by a cost of moderate growth [i.e., $c(h_{\langle q\rangle}) = O(\log q)$], for w close enough to 0, and $\Re s>(1/2)$, the operator $\underline{\mathbf{H}}_{s,w,(c)}$ also acts on $\mathcal{B}_\infty(\mathcal{V})$. Moreover, (see [22], [6]), for a complex number s close enough to the real axis, with $\Re s>(1/2)$, it possesses nice spectral properties; in particular, in such a situation, the operator $\underline{\mathbf{H}}_{s,w,(c)}$ has a unique dominant eigenvalue *(UDE)*, denoted by $\lambda_{(c)}(s,w)$, which is separated from the remainder of the spectrum by a spectral gap *(SG)*. This implies the following: for any fixed s close enough to the real axis, the quasi–inverse $w\mapsto (I-\underline{\mathbf{H}}_{s,w,(c)})^{-1}$ has a dominant pôle located at $w=w_{(c)}(s)$ defined by the implicit equation $\lambda_{(c)}(s,w_{(c)}(s))=1$. In particular, when $w=0$, one has:

$$(I-\underline{\mathbf{H}}_s)^{-1}[F](z,u) = \frac{1}{s-1}\frac{6\log\phi}{\pi^2}\underline{\psi}(z,u)\int_{\widetilde{I}} F(x,x)dx, \tag{42}$$

where $\underline{\psi}(x)$ is an extension of the invariant density ψ, and satisfies $\underline{\psi}(x,x)=\psi(x)$. An exact expression for $\underline{\psi}$ is provided in [22],

$$\underline{\psi}(z,u) = \frac{1}{\log\phi}\frac{1}{u-z}\left(\log\frac{\phi+u}{\phi+z}+\log\frac{\phi^2-u}{\phi^2-z}\right) \qquad \text{for } z\neq u, \text{ and} \qquad \underline{\psi}(z,z)=\psi(z).$$

5.5 Additive costs.

We recall that we wish to analyze the additive costs described in Section 2.3. and defined more precisely in (9). Such a cost $C_{(c)}$ is defined via an elementary cost c defined on quotients q_i, and we are interested by elementary costs of moderate growth, for which $c(|q|) = O(\log|q|)$. Such costs will intervene in the study of the bit–complexity cost, and will be relative in this case to the elementary cost $c(|q|) := \ell(|q|)$ where $\ell(x)$ denotes the binary length of the integer cost. There is another important case of such an additive cost: the number of iterations, relative to an elementary cost $c = 1$.

We first note that c can be defined on LFT's h corresponding to one step of the algorithm, via the relation $c(h_{\langle q,\varepsilon\rangle}) := c(q)$; and then it can be extended to the total set of LFT's in a linear way: for $h = h_1 \circ h_2 \circ \ldots \circ h_p$, we define $c(h)$ as $c(h) := c(h_1) + c(h_2) + \ldots + c(h_p)$. This gives rise to another definition for the complex version of the cost defined by $C(z) := C(1,z)$. If $z \in \widetilde{\mathcal{B}} \setminus \widetilde{\mathcal{F}}$ leads to $\hat{z} \in \widetilde{\mathcal{F}}$ by using the LFT $h \in \widetilde{\mathcal{G}}$ with $z = h(\hat{z})$, then $C(z)$ equals (by definition) $c(h)$.

We study cost $C_{(c)}$ in the continuous** model relative to a density f of type (r,g) defined in (25), and we wish to prove that $k \mapsto \mathbb{P}_{\langle f\rangle}[C_{(c)} = k]$ has a geometrical decreasing, with an estimate of the ratio. For this purpose, we use the moment generating function of the cost $C_{(c)}$, denoted by $\mathbb{E}_{\langle f\rangle}(\exp[wC_{(c)}])$ which satisfies

$$\mathbb{E}_{\langle f\rangle}(\exp[wC_{(c)}]) := \sum_{k\geq 0} \exp[wk]\cdot\mathbb{P}[C_{(c)} = k] = \sum_{h\in\widetilde{\mathcal{G}}} \exp[wc(h)] \iint_{h(\widetilde{\mathcal{F}})} \underline{f}(x,y)dxdy.$$

When the density is of the form (25), using a change of variables, the expression of the Jacobian, and relation (28) leads to

$$\mathbb{E}_{\langle f\rangle}(\exp[wC_{(c)}]) = \sum_{h\in\widetilde{\mathcal{G}}} \exp[wc(h)] \iint_{\widetilde{\mathcal{F}}} y^r\,|h'(z)|^{2+r} g(h(z),h(\bar{z}))dxdy.$$

This expression involves the transfer operator $\mathbf{G}_{2+r,w,(c)}$ of the algorithm AGAUSS, and with (41),

$$\mathbb{E}_{\langle f\rangle}(\exp[wC_{(c)}]) = \iint_{\widetilde{\mathcal{F}}} y^r \left[\mathbf{K}_{2+r,w}\circ(I-\underline{\mathbf{H}}_{2+r,w})^{-1} - I\right][g](z,\bar{z})dxdy.$$

The asymptotic behaviour of $\mathbb{P}[C_{(c)} = k]$ is obtained by extracting the coefficient of $\exp[kw]$ in the moment generating function. This series has a pôle at $e^{w(2+r)}$ for the value $w(2+r)$ of w defined by the spectral equation $\lambda_{(c)}(2+r, w(2+r)) = 1$ that involves the dominant eigenvalue of the core operator $\underline{\mathbf{H}}_{s,w,(c)}$. Then, with classical methods of analytical combinatorics, we obtain:

Theorem 5. *Consider a step-cost c of moderate growth, namely $c : \mathbb{N} \to \mathbb{R}^+$ with $c(q) = O(\log(q))$ and the relative additive cost $C_{(c)}$ defined in (9). Then, for any density f of valuation r, the cost $C_{(c)}$ follows an asymptotic geometric law. Moreover, the ratio of this law is closely related to the dominant eigenvalue of the core transfer operator $\underline{\mathbf{H}}_{s,w,(c)}$, via the relation*

$$\mathbb{P}_{\langle f\rangle}[C_{(c)} = k] \sim a(r)\exp[-kw_{(c)}(2+r)], \qquad \text{for } k\to\infty, \tag{43}$$

** It is also possible to transfer this continuous model to the discrete one. This is done for instance in [8].

where $a(r)$ is some strictly positive constant which depends on density f and cost c. The ratio $w_{(c)}(2+r)$ is defined by the spectral relation $\lambda_{(c)}(2+r, w(2+r)) = 1$; it only depends on cost c and the valuation r, not on the density itself, and satisfies $w_{(c)}(2+r) = \Theta(r+1)$ when $r \to -1$.

In the particular case of a constant step-cost c equal to 1, the operator $\underline{\mathbf{H}}_{s,w,(1)}$ is simply $e^w \cdot \underline{\mathbf{H}}_s$, and the value $w_{(1)}(s)$ is defined by the the relation $e^w \lambda(s) = 1$: this entails that the ratio in (43) is just equal to $\lambda(2+r)$. We recover in this case the main results of [8, 22].
In this case, there exists an alternative expression for the mean number of iterations of the CoreGauss algorithm which uses the characterization of Hurwitz (recalled in Proposition 3). Furthermore, the probability of the event $[R \geq k+1]$ can be expressed in an easier way using (24), as

$$\mathbb{P}[R \geq k+1] = \frac{1}{A_3(r)} \sum_{h \in \mathcal{H}^k} \iint_{h(\mathcal{D})} y^r dxdy = \frac{1}{A_3(r)} \iint_{\mathcal{D}} \Big(\sum_{h \in \mathcal{H}^k} |h'(z)|^{2+r} \Big) y^r dxdy$$

$$= \frac{1}{A_4(r)} \iint_{\mathcal{D}} y^r \, \underline{\mathbf{H}}^k_{2+r}[1](z)\, dxdy,$$

where $A_4(r)$ is the measure of $\mathcal{D}$ with respect to the standard density of valuation r,

$$A_4(r) = \frac{\sqrt{\pi}}{4^{r+2}} \frac{\Gamma((r+1)/2)}{\Gamma(r/2+2)}. \tag{44}$$

This leads to the following result:

Theorem. [Daudé, Flajolet, Vallée] *Consider the continuous model with the standard density of valuation r. Then, the expectation of the number of iterations R of the* CoreGauss *algorithm admits the following expression*

$$\mathbb{E}_{(r)}[R] = \frac{1}{A_4(r)} \iint_{\mathcal{D}} y^r (I - \underline{\mathbf{H}}_{2+r})^{-1}[1](z,\bar{z}) dxdy = \frac{2^{2+r}}{\zeta(2r+4)} \sum_{\substack{(c,d) \\ d\phi < c < d\phi^2}} \frac{1}{(cd)^{2+r}}.$$

Furthermore, for any fixed valuation $r > -1$, the number of iterations follows a geometric law

$$\mathbb{P}_{(r)}[R \geq k+1] \sim_{k \to \infty} \widetilde{a}(r)\, \lambda(2+r)^k$$

where $\lambda(s)$ is the dominant eigenvalue of the core transfer operator $\underline{\mathbf{H}}_s$ and $a(r)$ involves the dominant projector $\mathbf{P}_s$ relative to the dominant eigenvalue $\lambda(s)$ under the form

$$\widetilde{a}(r) = \frac{1}{A_4(r)} \iint_{\mathcal{D}} y^r \, \mathbf{P}_{2+r}[1](z) dxdy.$$

It seems that there does not exist any close expression for the dominant eigenvalue $\lambda(s)$. However, this dominant eigenvalue is polynomial–time computable, as it is proven by Lhote [15]. In [10], numerical values are computed in the case of the uniform density, i.e., for $\lambda(2)$ and $\mathbb{E}_{(0)}[R]$,

$$\mathbb{E}_{(0)}[R] \sim 1.3511315744, \qquad \lambda(2) \sim 0.0773853773.$$

5.6 Bit-complexity

We are interested in the study of the bit–complexity B defined in Section 2.3, and it is explained there why it is sufficient to study costs Q, D defined by

$$Q(u,v) = \sum_{i=1}^{P(u,v)} \ell(|q_i|), \qquad D(u,v) := 2 \sum_{i=1}^{P(u,v)} \ell(|q_i|) \lg \left| \frac{v_i}{v} \right|.$$

These costs are invariant by similarity, i.e., $X(\lambda u, \lambda v) = X(u,v)$ for $X \in \{Q, D, P\}$. If, with a small abuse of notation, we let $X(z) := X(1,z)$, we are led to study the main costs of interest in the complex framework. It is possible to study the mean value of the bit–complexity of the AGAUSS algorithm, but, here, we restrict the study to the case of the COREGAUSS algorithm, for which the computations are nicer.

In the same vein as in (32), the i-th length decrease can be expressed with the derivative of the LFT h_i defined in (21), as

$$\frac{|v_i|^2}{|v_0|^2} = |h_i'(\hat{z})| \qquad \text{so that} \quad 2 \lg \left(\frac{|v_i|}{|v_0|} \right) = \lg |h_i'(\hat{z})|.$$

Finally, the complex versions of costs Q, D are

$$Q(z) = \sum_{i=1}^{P(z)} \ell(|q_i|), \qquad D(z) := \sum_{i=1}^{P(z)} \ell(|q_i|) \lg |h_i'(\hat{z})|.$$

Remark that $\lg |h_i'(\hat{z})| \cdot |h_i'(\hat{z})|^s$ is just the derivative of $(1/\log 2)|h_i'(\hat{z})|^s$ with respect to s. The cost Q is just an additive cost relative to cost $c = \ell$ which was already studied in Section 5.5. But, we here adopt a slightly different point of view: we restrict ourselves to the COREGAUSS algorithm, and focus on the study of the expectation.

To an operator $\underline{\mathbf{X}}_{s,w,(c),[h]}$, we associate two operators $W_{(c)}\underline{\mathbf{X}}_{s,[h]}$ and $\Delta\underline{\mathbf{X}}_{s,[h]}$ defined as

$$W_{(c)}\underline{\mathbf{X}}_{s,[h]} = \frac{d}{dw}\underline{\mathbf{X}}_{s,w,(c),[h]}|_{w=0}, \qquad \Delta\underline{\mathbf{X}}_{s,[h]} = \frac{1}{\log 2}\frac{d}{ds}\underline{\mathbf{X}}_{s,0,(c),[h]}.$$

The operator $W_{(c)}$ is using for weighting with cost c, while Δ weights with $\lg |h'(\hat{z})|$. The refinement of the decomposition of the set $\mathcal{H}^+$ as

$$\mathcal{H}^+ := [\mathcal{H}^\star] \cdot \mathcal{H} \cdot [\mathcal{H}^\star]$$

gives rise to the parallel decomposition of the operators (in the reverse order). If we weight the second factor with the help of $W_{(\ell)}$, we obtain the operator

$$\left[(I - \underline{\mathbf{H}}_s)^{-1}\right] \circ \left[W_{(\ell)}\underline{\mathbf{H}}_s\right] \circ (I - \underline{\mathbf{H}}_s)^{-1} = W_{(\ell)}[(I - \underline{\mathbf{H}}_s)^{-1}],$$

which is the "generating operator" of the cost $Q(z)$. If, in addition of weighting the second factor with the help of $W_{(\ell)}$, we take the derivative Δ of the third one, then we obtain the operator

$$\Delta\left[(I - \underline{\mathbf{H}}_s)^{-1}\right] \circ \left[W_{(\ell)}\underline{\mathbf{H}}_s\right] \circ (I - \underline{\mathbf{H}}_s)^{-1}$$

which is the "generating operator" of the cost $D(z)$. These functionals $W_{(c)}, \Delta$ are also central in the analysis of the bit–complexity of the Euclid Algorithm [16], [3].

For the standard density f of valuation r, the mean values of parameters Q, D satisfy

$$q(r) := \mathbb{E}_{(r)}[Q] = \frac{1}{A_4(r)} \iint_{\widetilde{\mathcal{B}}\setminus\mathcal{D}} y^r W_{(\ell)}[(I-\underline{\mathbf{H}}_{2+r})^{-1}][1](z,\bar{z})\, dxdy,$$

$$d(r) := \mathbb{E}_{(r)}[D] = \frac{1}{A_4(r)} \iint_{\widetilde{\mathcal{B}}\setminus\mathcal{D}} y^r \Delta\left[(I-\underline{\mathbf{H}}_{2+r})^{-1}\right] \circ \left[W_{(\ell)}\underline{\mathbf{H}}_{2+r}\right] \circ (I-\underline{\mathbf{H}}_{2+r})^{-1}[1](z,\bar{z})\, dxdy,$$

and involve the measure $A_4(r)$ of disk $\mathcal{D}$ wrt to the standard density of valuation r, whose expression is given in (44). Remark that $A_4(r) \sim (r+1)^{-1}$ when $r \to -1$. With (42), this proves that

$$q(r) = \Theta[(r+1)^{-1}], \qquad d(r) = \Theta[(r+1)^{-2}], \qquad (r \to -1).$$

We have provided an average–case analysis of parameters Q, D in the continuous model. It is possible to adapt this analysis to the discrete model. We have proven:

Theorem 6. *On the set Ω_M of inputs of size M endowed with a density f of valuation r, the central execution[††] of the Gauss algorithm has a mean bit–complexity which is linear with respect to the size M. More precisely, for an initial standard density of valuation r, one has*

$$\mathbb{E}_{M,(r)}[B] = q(r)M + d(r) + \Theta[q(r)] + \varepsilon_r(M)$$

$$\text{with} \quad \begin{array}{rcll} \varepsilon_r(M) & = & O(M^2)(r+1)M\exp[-(r+1)M] & \text{for } -1 < r \le 0, \\ \varepsilon_r(M) & = & O(M^3\exp[-M]) & \text{for } r \ge 0. \end{array}$$

The two constants $q(r)$ and $d(r)$ are the mean values of parameters Q, D with the (continuous) standard density of valuation r. They do not depend on M, and satisfy

$$q(r) = \Theta[(r+1)^{-1}], \qquad d(r) = \Theta[(r+1)^{-2}], \qquad (r \to -1).$$

For $r \to -1$ and $M \to \infty$ with $(r+1)M \to 1$, then $\mathbb{E}_{M,(r)}[B]$ is $O(M^2)$.

Open question. Provide a precise description of the phase transition for the behaviour of the bit-complexity between the Gauss algorithm for a valuation $r \to -1$ and the Euclid algorithm.

6 Conclusion

In the version of the LLL algorithm previously described in Section 4.7, there are two dynamical systems, the Odd dynamical system (relative to the Odd phases) and the Even dynamical system (relative to the Even phases). The Odd (resp. Even) dynamical system performs (in parallel) the dynamical system relative to the AGAUSS on all the complex numbers z_i of odd (resp. even) indices. Between the end of one phase and the beginning of the following phase, computations in the vein of Section 4.7 take place.
The dynamics of each system, Odd or Even, is easily deduced from the dynamics of the AGAUSS system. In particular, there is an Even Hole and an Odd Hole, which can be described as a function of the hole of the AGAUSS system. But the main difficulty for analyzing the ODD-EVEN Algorithm will come from the difference on the geometry of the two holes –the Odd one and the Even one... This is a work in progress!

[††] This is, by definition (see Section 2.3), the execution of the algorithm, EXCEPT the initialization process where the Gram matrix is computed.

References

[1] A. AKHAVI. Random lattices, threshold phenomena and efficient reduction algorithms, *Theoretical Computer Science*, 287 (2002) 359–385

[2] A. AKHAVI, J.-F. MARCKERT ET A. ROUAULT. On the Reduction of a Random Basis, *Proceedings of SIAM-ALENEX/ANALCO'07*. New-Orleans, january 07

[3] A. AKHAVI and B. VALLÉE. Average bit-complexity of Euclidean algorithms, in *Proceedings of ICALP'2000* - Genève, 14 pages, Lecture Notes in Computer Science 1853, pp 373–387.

[4] J. BOURDON, B. DAIREAUX, B. VALLÉE. Dynamical analysis of α-Euclidean Algorithms, *Journal of Algorithms* 44 (2002) pp 246–285.

[5] D. BUMP. Automorphic Forms and Representations, Cambridge University Press (1996)

[6] F. CHAZAL, V. MAUME-DESCHAMPS, B. VALLÉE Erratum to "Dynamical sources in information theory: fundamental intervals and word prefixes", Algorithmica 38 pp 591–596 (2004).

[7] H. COHEN. A course in Computational Algebraic Number Theory, GTM 138, Springer Verlag, 4th Edition (2000).

[8] H. DAUDÉ, P. FLAJOLET, B. VALLÉE. An average-case analysis of the Gaussian algorithm for lattice Reduction, *Combinatorics, Probability and Computing* (1997) 6, pp 397–433.

[9] P. FLAJOLET, B. VALLÉE. *Gauss' reduction Algorithm : an average case analysis, Proceedings of IEEE-FOCS 90*, St-Louis, Missouri, volume 2, pp 830-39.

[10] P. FLAJOLET, B. VALLÉE. Continued fractions, Comparison algorithms and fine structure constants Constructive, Experimental et Non-Linear Analysis, Michel Thera, Editor, Proceedings of Canadian Mathematical Society, Vol 27 (2000), pages 53-82

[11] J. C. LAGARIAS. Worst–case complexity bounds for algorithms in the theory of integral quadratic forms. *Journal of Algorithms 1*, 2 (1980), 142–186.

[12] H. LAVILLE, B. VALLÉE. Distribution de la constante d'Hermite et du plus court vecteur dans les réseaux de dimension 2, *Journal de Théorie des nombres de Bordeaux* 6 (1994) pp 135-159

[13] A. K. LENSTRA, H. W. LENSTRA, AND L. LOVÁSZ. Factoring polynomials with rational coefficients. *Mathematische Annalen 261* (1982), 513–534.

[14] H. W. LENSTRA. Integer programming with a fixed number of variables, *Mathematics of Operations Research*, vol. 8, 4, (1983), 538–548

[15] L. LHOTE Computation of a class of Continued Fraction constants. *Proceedings of Alenex-ANALCO'04*, 199–210

[16] L. LHOTE and B. VALLÉE. Sharp estimates for the main parameters of the Euclid Algorithm, in LATIN 2006, pages 689–702, Lecture Notes in Computer Science, 3887, Springer

[17] J.-P. SERRE. *A Course in Arithmetic*. Graduate Texts in Mathematics. Springer Verlag, 1973.

[18] P. NGUYEN, J. STERN. The Two Faces of Lattices in Cryptology, *Proceedings of the 2001 Cryptography and Lattices Conference (CALC'01)*, Springer, LNCS, volume 2146, (2001), 146–180.

[19] P. NGUYEN, D. STEHLÉ. LLL on the average, *Proceedings of the 7th Algorithmic Number Theory Symposium (ANTS VII)*, Springer, LNCS vol. 4076, (2006), 238–256

[20] B. VALLÉE. Gauss' algorithm revisited. *Journal of Algorithms 12* (1991), 556–572.

[21] B. VALLÉE. Algorithms for computing signs of 2×2 determinants: dynamics and average–case analysis, *Proceedings of ESA'97* (5th Annual European Symposium on Algorithms) (Graz, Septembre 97), LNCS 1284, pp 486–499.

[22] B. VALLÉE. Opérateurs de Ruelle-Mayer généralisés et analyse en moyenne des algorithmes de Gauss et d'Euclide, Acta Arithmetica 81.2 (1997), pp 101–144

[23] G. VILLARD. Parallel lattice basis reduction. In International Symposium on Symbolic and Algebraic Computation, Berkeley California USA . ACM Press, July 1992.

[24] C.K. YAP. Fundamental Problems in Algorithmic Algebra, Princeton University Press (1996)