LATTICE REDUCTION IN TWO DIMENSIONS: ANALYSES UNDER REALISTIC PROBABILISTIC MODELS

BRIGITTE VALLÉE AND ANTONIO VERA

Abstract. 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.

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 computational mathematics and computer science: for instance, modern cryptanalysis [14], computer algebra [18] integer linear programming [11] and number theory [5].

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 [10] due to Lenstra, Lenstra and Lovàsz, 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, [8], then Vallée [16], who also describes the worst-case input. Then, Daudé, Flajolet and Vallée [6] completed the first work [7] 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 [9] study the geometry of the outputs, and describe the law of some output parameters, when the input model is the previous uniform model.

Date: 10th March 2007.

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 uniformy 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 [17] in a slightly different context, but not actually 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 1].

(*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 2] and provide sharp estimates for the distribution of these output parameters [Theorem 3].

(*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 4 and 5].

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.
We are particularly interested in understanding the results of experiments conducted by Stehlé [15] which are summarized in Figure 1. We return to these experiments and their meanings in Section 2.8. We explain in Section 3.3 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 perform a probabilistic analysis of such parameters: Section 3 is devoted to output parameters, whereas Section 4 focuses on execution parameters.

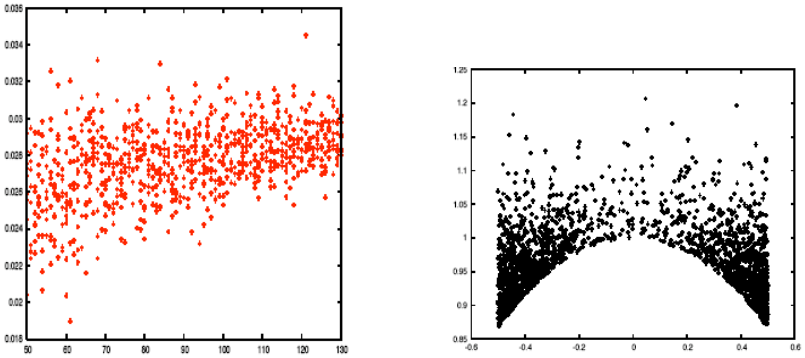

FIGURE 1. On the left: experimental results for the ratio $(1/n)\log\frac{|b_1|}{(\det L)^{1/n}}$ [here, n is the dimension, b_1 is the first vector of the LLL reduced basis and $\det L$ is the determinant of the lattice L]. On the right, the output distribution of "local bases" for the LLL algorithm (see Sections 2.8 and 3.3).

2. Lattice reduction in dimension 2

We present here the two versions of the Gauss algorithms, in their (initial) vectorial framework, then in the complex framework. We present the main parameters of interest, and how they intervene in the analysis of the LLL algorithm.

2.1. Lattices and bases.

A *lattice* of rank 2 in the complex plane $\mathbb{C}$ is the set $\mathcal{L}$ of elements of $\mathbb{C}$ ("vectors") defined by

$$\mathcal{L} = \mathbb{Z}u \oplus \mathbb{Z}v = \{xu + yv; \quad x, y \in \mathbb{Z}\},$$

where (u, v), called a *basis*, is a pair of $\mathbb{R}$–linearly independent elements of $\mathbb{C}$. A lattice is generated by infinitely many bases that are related to each other by integer matrices of determinant ± 1.

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

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

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 vector amongst the shortest 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 miminum. 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., $\det(u, v) \geq 0$]. Such a basis is called positive.

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

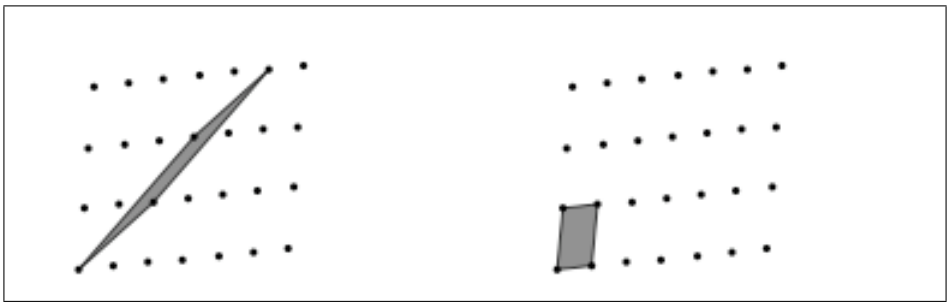

FIGURE 2. A lattice and two of its bases represented by the parallelogram they span. The first basis (on the left) is skew, the second one (on the right) is minimal (reduced).

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:

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

(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:

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

2.2. **The Gaussian reduction schemes.** There are two reduction processes, according as one focuses on positive bases or acute bases.

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:

$$v := v - mu \qquad \text{with} \quad m := \lfloor r(v, u) \rceil, \quad r(v, u) := \Re(\frac{v}{u}) = \frac{(u \cdot v)}{|u|^2},$$

where $\lfloor x \rceil$ represents the integer nearest to the real x.
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

$$v_{i+1} = -v_{i-1} + m_i\, v_i \qquad \text{with} \quad m_i := \lfloor r(v_{i-1}, v_i) \rceil. \tag{2}$$

Here, each quotient m_i is an integer of $\mathbb{Z}$, $p \equiv p(u, v)$ denotes the number of iterations, and the final pair (v_p, v_{p+1}) satisfies the conditions (P) of Proposition

PGauss(u, v)
Input. A positive basis (u, v) of $\mathbb{C}$ with $|v| \leq |u|,\ |r(v, u)| \leq (1/2)$.
Output. A positive minimal basis (u, v) of $\mathcal{L}(u, v)$ with $|v| \geq |u|$.
`While` $|v| \leq |u|$ `do`
$(u, v) := (v, -u)$;
$m := \lfloor r(v, u) \rceil$, with $r(v, u) = \dfrac{(u \cdot v)}{|u|^2}$;
$v := v - mu$;

1. Each step defines a unimodular matrix $\mathcal{M}_i$ with $\det \mathcal{M}_i = 1$,

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

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

$$\begin{pmatrix} v_{p+1} \\ v_p \end{pmatrix} = \mathcal{M} \begin{pmatrix} v_1 \\ v_0 \end{pmatrix} \qquad \text{with} \quad \mathcal{M} := \mathcal{M}_p \cdot \mathcal{M}_{p-1} \cdot \ldots \cdot \mathcal{M}_1. \tag{3}$$

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:

$$v := \epsilon(v - mu) \qquad \text{with} \quad m := \lfloor r(v, u) \rceil\,, \qquad \epsilon = \operatorname{sign}\left(r(v, u) - \lfloor r(v, u) \rceil\right),$$

where $r(v, u)$ is defined as previously.

AGauss(u, v)
Input. A basis (u, v) of $\mathbb{C}$ with $|v| \leq |u|,\ 0 \leq r(v, u) \leq (1/2)$.
Output. An acute minimal basis (u, v) of $\mathcal{L}(u, v)$ with $|v| \geq |u|$.
`While` $|v| \leq |u|$ `do`
$(u, v) := (v, u)$;
$m := \lfloor r(v, u) \rceil\,; \epsilon := \operatorname{sign}[r(v, u) - \lfloor r(v, u) \rceil]$, with $r(v, u) = \dfrac{(u \cdot v)}{|u|^2}$;
$v := \epsilon(v - mu)$;

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

$$\widetilde{m}_i := \lfloor r(w_{i-1}, w_i) \rceil\,, \qquad \epsilon_i = \operatorname{sign}\left(r(w_{i-1}, w_i) - \lfloor r(w_{i-1}, w_i) \rceil\right). \tag{4}$$

Here, each quotient $\widetilde{m}_i$ 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 $\det \mathcal{N}_i = \epsilon_i = \pm 1$,

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

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 [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 Gauss algorithms [defined in (2,4)] satisfy $w_i = \eta_i\, v_i$ for some $\eta_i = \pm 1$ and the quotient $\widetilde{m}_i$ is the absolute value of quotient m_i.

Then, when studying the two kinds of parameters –execution parameters, or output parameters– the two algorithms are essentially the same. 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 length 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 of inputs of size M, endowed with some discrete probability $\mathbb{P}_M$, and study the parameters as 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 takes a quadratic time with respect to the length of the input $\ell(u, v)$. After this, all the computations 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 m_i, followed with the computation of the new coefficients of the Gram matrix $G(v_{i+1}, v_i)$, namely

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

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

$$B(u, v) = \sum_{i=1}^{p(u,v)} \ell(m_i) \cdot \ell(|v_i|^2), \tag{5}$$

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

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 $D(u, v)$, and the approximate difference cost $\underline{D}$:

$$Q(u, v) = \sum_{i=1}^{p(u,v)} \ell(m_i), \qquad D(u, v) = \sum_{i=1}^{p(u,v)} \ell(m_i)\left[\,\ell(|v_i|^2) - \ell(|v_0|^2)\right], \tag{6}$$

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

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

$$B(u, v) = Q(u, v)\,\ell(|u|^2) + \underline{D}(u, v) + [D(u, v) - \underline{D}(u, v)]. \tag{7}$$

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 m_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

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

(b) The length decreases, namely the i-th length decrease d_i and the total length decrease d, defined as

$$d_i := \left|\frac{v_i}{v_0}\right|^2, \qquad d := \left|\frac{v_p}{v_0}\right|^2. \tag{9}$$

Finally, the configuration of the output basis $(\hat{u}, \hat{v})$ is described by three parameters closely related to the minima of the lattice $\mathcal{L}(u, v)$

$$\lambda(u, v) := \lambda_1(\mathcal{L}(u, v)) = |\hat{u}|, \qquad \mu(u, v) := \frac{|\det(u, v)|}{\lambda(u, v)} = |\hat{v}^\star|, \tag{10}$$

$$\gamma(u, v) := \frac{\lambda^2(u, v)}{|\det(u, v)|} = \frac{\lambda(u, v)}{\mu(u, v)} = \frac{|\hat{u}|}{|\hat{v}^\star|}. \tag{11}$$

[Here, $\hat{v}^\star$ is the orthogonal projection of $\hat{v}$ onto the orthogonal of $<u>$]. We come back later to these output parameters and shall explain in Sections 2.8 and 3.3 why they are so important.

2.4. **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 $\lambda \in \mathbb{C} \setminus \{0\}$. An instance is the execution of the Gauss algorithm itself: It should also be observed that exchange operations or translations introduced above only depend on the complex ratio $z = v/u$. Then, the sequence of vectors computed on an input pair $S_\lambda(u, v)$ coincides with the sequence $S_\lambda(v_i)$, where v_i is the sequence computed by the algorithm on the input (u, v). This makes it possible to give a formulation of the Gauss algorithm entirely in terms of complex numbers. A second instance are our execution parameters B, C, d which are also invariant under similarity. A third instance is the characterization of minimal bases given in Proposition 1 that only depends on the ratio $z = v/u$.

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 $z \mapsto T^{-m}z$ with $T(z) = z + 1$, ans a possible sign change $J : z \mapsto -z$.

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

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

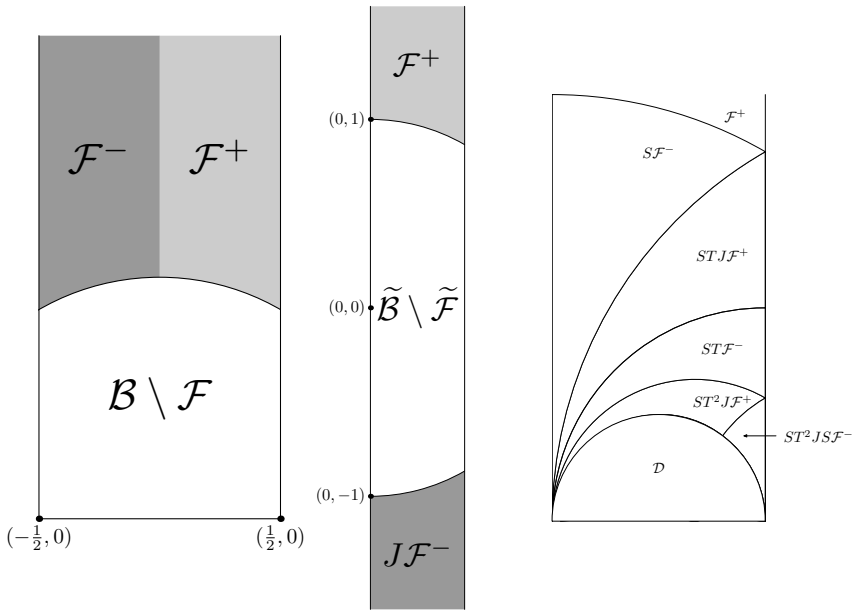

FIGURE 3. On the left and in the middle: the fundamental domains $\mathcal{F}, \widetilde{\mathcal{F}}$ and the strips $\mathcal{B}, \widetilde{\mathcal{B}}$(see Section 2.4). On the right, the six domains which constitute the domain $\mathcal{B}_+ \setminus \mathcal{D}_+$ (see Section 2.6).

In this 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

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

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

$$\mathcal{F} = \left\{ z \in \mathbb{H}; \quad |z| \geq 1, \quad |\Re(z)| \leq \frac{1}{2} \right\}, \qquad \mathcal{F}_+ := \mathcal{F} \cap \mathbb{H}_+, \quad \mathcal{F}_- := \mathcal{F} \cap \mathbb{H}_-. \tag{12}$$

Such a domain, represented in Figure 3, is familiar from the theory of modular forms [13] or the reduction theory of quadratic forms [12].

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

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

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

$$\widetilde{\mathcal{F}} = \left\{ z \in \mathbb{C}; \quad |z| \geq 1 \quad 0 \leq \Re(z) \leq \frac{1}{2} \right\} = \mathcal{F}_+ \cup J\mathcal{F}_-. \tag{13}$$

Each version of the algorithm gives rise to a different set of LFT's. According to the parameters of interest –output parameters or execution parameters– these two sets may be more or less adequate.

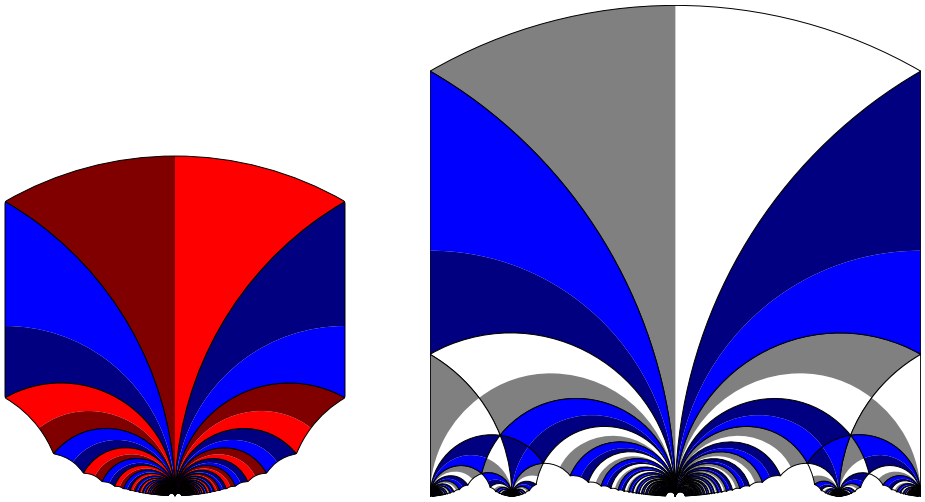

FIGURE 4. On the left, the "central" festoon $\mathcal{F}_{(0,1)}$. On the right, three festoons of the strip $\mathcal{B}$, relative to $(0,1),(1,3),(-1,3)$ and the two half-festoons at $(-1,2)$ and $(1,2)$.

2.5. **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 (2) via the relation $z_i = v_{i+1}/v_i$. They are directly computed by the relation $z_{i+1} := U(z_i)$, 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

$$z_0 = \cfrac{1}{m_1 - \cfrac{1}{m_2 - \cfrac{1}{\ddots \cfrac{}{m_p - z_p}}}} = h(z_p) \qquad \text{with} \quad h := h_{[m_1]} \circ h_{[m_2]} \circ \dots h_{[m_p]},$$

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

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

The set $\mathcal{G}$ of LFTs $h : z \mapsto (az+b)/(cz+d)$ defined with the relation $z = h(\hat{z})$ sends the output domain $\mathcal{F}$ into the input domain $\mathcal{B} \setminus \mathcal{F}$. It 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

$$\mathcal{C} := \{(a,c); \quad \frac{a}{c} \in [-1/2, +1/2],\ c \geq 1; \gcd(a,c) = 1\}, \tag{14}$$

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

$\mathcal{G}_{(a,c)}$ denotes the set of such LFT's, the domain

$$\mathcal{F}_{(a,c)} = \bigcup_{h\in\mathcal{G}_{(a,c)}} h(\mathcal{F}) = h_{(a,c)}\left(\bigcup_{m\in\mathbb{Z}} T^m\mathcal{F}\right) \tag{15}$$

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. In the case when $c = 2$, there are two half-festoons at $1/2$ and $-1/2$. See Figure 4.

2.6. **The LFT's of 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 (4) 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

$$z_{i-1} = h_{<m_i,\epsilon_i>}(z_i) \qquad \text{with} \quad h_{<m,\epsilon>}(z) := \frac{\epsilon}{m+z}.$$

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

$$z_0 = \cfrac{\epsilon_1}{m_1 + \cfrac{\epsilon_2}{m_2 + \cfrac{\epsilon_3}{\ddots \cfrac{}{m_p + z_p}}}} = \widetilde{h}(z_p) \qquad \text{with} \quad \widetilde{h} := h_{<m_1,\epsilon_1>}\circ h_{<m_2,\epsilon_2>}\circ\dots h_{<m_p,\epsilon_p>}.$$

More generally, the i-th complex number z_i satisfies

$$z_i = \widetilde{h}_i(z_p) \qquad \text{with} \quad \widetilde{h}_i := h_{<m_{i+1},\epsilon_{i+1}>}\circ h_{<m_{i+2},\epsilon_{i+2}>}\circ\dots h_{<m_p,\epsilon_p>}. \tag{16}$$

There are two main parts in the execution of the AGauss Algorithm, according to the position of the current complex z_i. While z_i belongs to the disk of diameter $[0, 1/2]$ whose equation is

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

the quotient (m, ϵ) satisfies $(m, \epsilon) \geq (2, +1)$ (wrt the lexicographic order). Then,

$$\mathcal{D} = \bigcup_{h\in\mathcal{H}} h(\widetilde{\mathcal{B}}\setminus\mathcal{D}) \qquad \text{with} \quad \mathcal{H} := \{h_{<m,\epsilon>}; \quad (m,\epsilon) \geq (2,+1)\}.$$

When z_i belongs to $\widetilde{\mathcal{B}}\setminus\mathcal{D}$, there remains at most two iterations. More precisely, (see Figure 3),

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

The subset $\mathcal{K}$ is called the final set of LFT's since it is used only at the end of the algorithm, whereas the subset $\mathcal{H}$ is the core set. Finally, the set $\widetilde{\mathcal{G}}$ decomposes as

$$\widetilde{\mathcal{G}} = \mathcal{H}^\star\cdot\mathcal{K}. \tag{17}$$

2.7. **Probabilistic models.** We recall that our initial motivation consists in studying the probabilistic behaviour of variables defined on discrete subsets. More precisely, we consider as valid inputs the sets

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

or its tilde version, according to the considered algorithm (PGauss or AGauss).

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

$F(u,v) = g(|u|) \cdot f(v/u)$. Moreover, it is sufficient to consider pairs (u,v) of size M with a first vector u of the form $u = (c,0)$ with $\ell(c^2) = M$. Then, the complex $z = v/u$ belongs to $\mathbb{Q}[i]$ and is of the form $(a/c) + i(b/c)$. When the integer c tends 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. A density f on the set $\mathcal{S} \subset \mathbb{C}$ is of valuation r (with $r > -1$) if it is of the form

$$f(z) = y^r \cdot g(z) \qquad \text{where} \quad g(z) \neq 0 \quad \text{for } \Im(z) = 0. \tag{18}$$

We often deal with the standard density of valuation r, denoted by f_r,

$$f_r(z) = \frac{1}{A(r)} y^r \qquad \text{with} \quad A(r) = \iint_{\mathcal{B}\setminus\mathcal{F}} y^r dxdy. \tag{19}$$

Of course, when $r = 0$, we recover the uniform distribution on $\mathcal{B} \setminus \mathcal{F}$ with $A(1) = (1/12)(2\pi + 3\sqrt{3})$. This 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.

2.8. **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 $< b_1, b_2, \ldots, b_{k-1} >$. 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.

3. Output parameters.

This Section describes the probabilistic behaviour of output parameters: we first analyse the output densities, then we focus on the geometry of our three main parameters defined in (10, 11). We then explain how this type of result may be applied in the analysis of the LLL algorithm.

3.1. **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 h with respect to map ϕ, namely $\underline{h} = \phi^{-1} \circ h \circ \phi$, where mappings ϕ, ϕ^{-1} are linear mappings $\mathbb{C}^2 \to \mathbb{C}^2$ defined as

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

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

$$J\underline{h}(x,y) = |h'(z) \cdot h'(\overline{z})| = |h'(z)|^2, \tag{20}$$

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 (20), 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, the output density $\hat{f}$ can be expressed as a function of the input density f,

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

We now analyze an important particular case, where the initial density is the standard density of valuation r defined in (19). Since each element of $\mathcal{G}$ gives rise to a unique pair (c,d) with $c\geq 1, \gcd(c,d)=1$ for which

$$|h'(\hat{z})| = \frac{1}{|c\hat{z}+d|^4}, \qquad f_r\circ\underline{h}(\hat{x},\hat{y}) = \frac{1}{A(r)}\,\frac{\hat{y}^r}{|c\hat{z}+d|^{2r}}, \tag{21}$$

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

We have shown:

Theorem 1. *When the initial density on $\mathcal{B}\setminus\mathcal{F}$ is the standard density of valuation r, denoted by f_r and defined in (19), the output density is closely related to an Eisenstein series E_s of weight $s=2+r$. With respect to the Haar measure μ on $SL_2(\mathbb{Z})$, equal to $d\mu(x,y) = (3/\pi)(1/y^2)dxdy$, the output density $\hat{f}_r$ is expressed as*

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

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

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

The series E_s are Maass forms (see for instance the book [4]): they play an important rôle in the theory of modular forms, because E_s is an eigenfunction for the Laplacian, relative to the eigenvalue $s(1-s)$.

3.2. **Geometry of the output parameters.** The main output parameters defined in (10,11) are closely related to their complex versions, related to basis $(1,z)$,

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

and these last parameters can be expressed with the input–output pair $(z,\hat{z})$.

Proposition 2. *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 (10,11) admit the following expressions*

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

$$\begin{aligned}
\mathtt{Fo}(a,c,\rho) &:= \{(x,y);\quad y>0,\qquad \Big(x-\frac{a}{c}\Big)^2+\Big(y-\frac{\rho}{2c}\Big)^2\le\frac{\rho^2}{4c^2}\quad\}\\
\mathtt{Fa}(a,c,t) &:= \{(x,y);\quad y>0,\qquad \Big(x-\frac{a}{c}\Big)^2+y^2\le\frac{t^2}{c^2}\quad\}\\
\mathtt{Se}(a,c,u) &:= \{(x,y);\quad y>0,\qquad |y|\le\frac{cu}{\sqrt{1-c^2u^2}}\Big|x-\frac{a}{c}\Big|\quad\}.
\end{aligned}$$

FIGURE 5. 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 $\mathtt{Se}(a,c,u)$.

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:

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

Proof. If the initial pair (v_1,v_0) is written as in (3) 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

$$\frac{|v_p|^2}{|v_0|^2}=\frac{|v_p|^2}{|cv_{p+1}+dv_p|^2}=\frac{1}{|c\hat z+d|^2}=|h'(\hat z)|, \tag{22}$$

[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. ■

We now consider the following well-known domains defined in Figure 5. The Ford disk $\mathtt{Fo}(a,c,\rho)$ is a disk of center $(a/c,\rho/(2c))$ and radius $\rho/(2c)$: it is tangent to $y=0$ at point a/c. 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 2. *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 (15) and if the set $\mathcal{C}$ is defined in (14), one has:

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

These "local" definitions 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 triangles (for $\mathcal{M}$) [see Figure 6]. In the

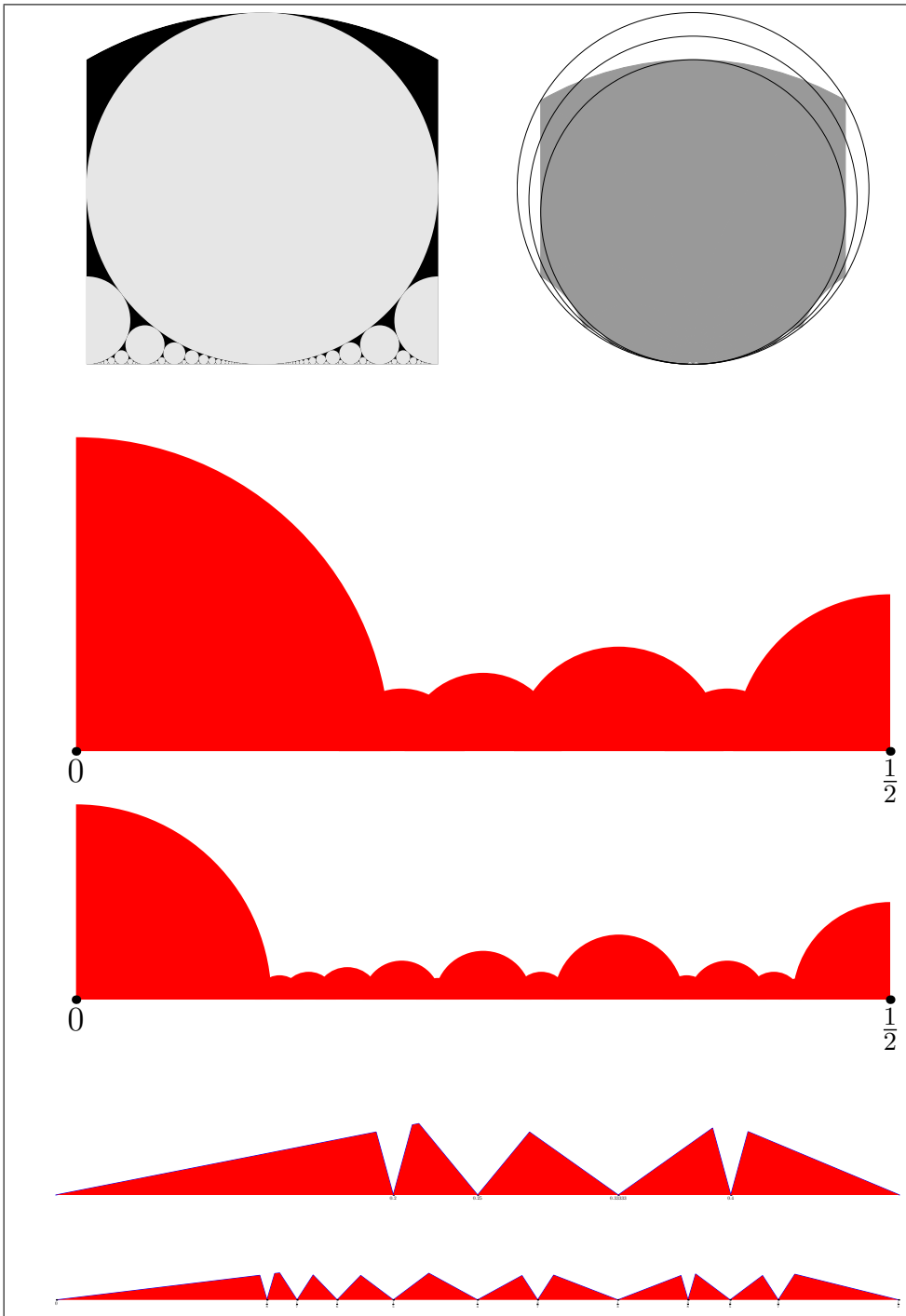

FIGURE 6. On the top: the domain $\Gamma(\rho) := \{z;\ \ \gamma(z) \leq \rho\}$. On the left, $\rho = 1$ (in white). On the right, the domain $\mathcal{F}_{(0,1)} \cap \mathtt{Fo}(0,1,\rho)$ for $\rho = 1, \rho_0 = 2/\sqrt{3}, \rho_1 = (1+\rho_0)/2$. – On the middle, the domain $\Lambda(t) \cap \mathcal{B}_+$, with $\Lambda(t) := \{z;\ \ \lambda(z) \leq t\}$ for $t = 0.193$ and $t = 0.12$. – On the bottom, the domain $M(u) \cap \mathcal{B}_+$ with $M(u) := \{z;\ \ \mu(z) \leq u\}$ for $u = 0.193$ and $u = 0.12$.

case of parameter λ, this "global definition" was already provided in [9]. Computing the measure of disks and angular sectors with respect to a standard density of valuation r lead to the estimate of the main output distributions:

Theorem 3. *When the initial density on $\mathcal{B}\backslash\mathcal{F}$ is the standard density of valuation r, the three main output parameters admit the following distributions:*

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

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

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

The constants $A_i(r)$ involve Euler's Beta function $B(a,b)$ and the measure $A(r)$, in the following way

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

3.3. **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. The LLL algorithm first deals with local bases with even indices. Consider two successive bases B_k and B_{k+2} 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 3 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 a second 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.

4. 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, and length decreases that may be of independent interest.

4.1. **Transfer operators.** The operator $\mathbf{X}_{s,[h]}$, when acting on functions F of two variables, and relative to a mapping h, depends on a (complex) parameter s and is formally defined as

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

More generally, 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 $\mathbf{X}_{s,w,(c),[h]}$ defined as

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

Such operators satisfy a crucial relation of composition: We easily remark that $\mathbf{X}_{s,[h]} \circ \mathbf{X}_{s,[g]} = \mathbf{X}_{s,[g\circ h]}$, and, when the cost c is additive, i.e., $c(g\circ h) = c(g)+c(h)$, the following relation holds:

$$\mathbf{X}_{s,w,(c),[h]} \circ \mathbf{X}_{s,w,(c),[g]} = \mathbf{H}_{s,w,(c),[g\circ h]}. \tag{23}$$

We recall the definition of sets $\widetilde{\mathcal{G}}, \mathcal{H}, \mathcal{K}$ relative to the LFT's used by the AGauss Algorithm, (see Section 2.6), and their fundamental decomposition (17), namely $\widetilde{\mathcal{G}} = \mathcal{H}^\star \cdot \mathcal{K}$. The weighted transfer operators associated to the AGauss Algorithm, namely

$$\mathbf{H}_{s,w,(c)} := \sum_{h\in\mathcal{H}} \mathbf{X}_{s,w,(c),[h]}, \qquad \mathbf{K}_{s,w,(c)} := \sum_{h\in\mathcal{K}} \mathbf{X}_{s,w,(c),[h]} \qquad \mathbf{G}_{s,w} := \sum_{h\in\widetilde{\mathcal{G}}} \mathbf{X}_{s,w,[h]},$$

satisfy, with (23) and (17), the relation

$$\mathbf{G}_{s,w,(c)} = \mathbf{K}_{s,w,(c)} \circ (I - \mathbf{H}_{s,w,(c)})^{-1}. \tag{24}$$

In the same vein, the plain transfer operators (i.e., unweighted) defined as the sum of operators $\mathbf{X}_{s,[h]}$ satisfy the relation

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

When acting on functions of class $\mathcal{C}^1$ and weighted by costs of moderate growth [i.e., $c(h_{[m]} = O(\log m)$], the operator $\mathbf{H}_{s,w,(c)}$ possesses nice spectral properties, and, in particular, for complex numbers s, w close enough to the real axis, a unique dominant eigenvalue, denoted by $\lambda_{(c)}(s,w)$.

4.2. **Additive costs.** For analyzing an additive cost in the continuous model relative to a density f, we use the moment generating function of the cost $C_{(c)}$, denoted by $\mathbb{E}_{(f)}(\exp[wC_{(c)}])$ which satisfies

$$\mathbb{E}_{(f)}(\exp[wC_{(c)}]) = \sum_{h\in\widetilde{\mathcal{G}}} \exp[w(h)] \iint_{h(\widetilde{\mathcal{F}})} \underline{f}(x,y)dxdy.$$

When the density f has a valuation r and is of the form (18), using a change of variables, the expression of the Jacobian, and relation (21) leads to

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

This expression involves the transfer operator $\mathbf{G}_{2+r,w}$ of the algorithm AGauss , and with (24),

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

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_r} for a value of w_r defined by the equation $\lambda_{(c)}(2 + r, w_r) = 1$. Then, with classical methods of analytical combinatorics, we obtained:

Theorem 4. *Consider a step-cost c of moderate growth, namely $c : \mathbb{N} \to \mathbb{R}^+$ with $c(m) = O(\log(m))$ and the relative additive cost $C_{(c)}$. Then, for any density 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 $\mathbf{H}_{s,w,(c)}$, via the relation*

$$\lim_{k\to\infty} \frac{1}{k} \log \mathbb{P}_{(f)}[C_{(c)} = k] = -w_r, \qquad \textit{with} \quad \log \lambda_{(c)}(2 + r, w_r) = 0.$$

This ratio w_r only depends on the valuation r, not on the density itself, and satisfies $w_r = \Theta(r + 1)$ when $r \to -1$.

4.3. **Bit-complexity.** Section 2.3 explains why it is sufficient to study costs $Q, D, \underline{D}$. All these costs are invariant by similarity, i.e., $X(\lambda u, \lambda v) = X(u, v)$ for $X \in \{Q, D, \underline{D}\}$. 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.

In the same vein as in (22), the i-th length decrease can be expressed with the derivative of the LFT h_i defined in (16), as

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

Remark that $\log |h_i'(\hat{z})| \cdot |h_i'(\hat{z})|^s$ is just the derivative of $|h_i'(\hat{z})|^s$ with respect to s. To an operator $\mathbf{X}_{s,w,(c),[h]}$, we associate two operators $W_{(c)}\mathbf{X}_s$ and $\Delta\mathbf{X}_s$ defined as

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

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

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

gives rise to the parallel decomposition of the operators (in the reverse order). If we weight the second factor with the help of W, we obtain the operator

$$\left[\mathbf{K}_s \circ (I - \mathbf{H}_s)^{-1}\right] \circ [W\mathbf{H}_s] \circ (I - \mathbf{H}_s)^{-1}$$

which is the "generating operator" of the cost $Q(z)$. If we weight the second factor with the help of W, and take the derivative Δ of the third one, then we obtain the operator

$$\Delta\left[\mathbf{K}_s \circ (I - \mathbf{H}_s)^{-1}\right] \circ [W\mathbf{H}_s] \circ (I - \mathbf{H}_s)^{-1}$$

which is the "generating operator" of the cost $D(z)$.

Then, for a density of valuation r, of the form (18), one has:

$$\mathbb{E}_{(r)}[Q] = \iint_{\widetilde{\mathcal{F}}} W\mathbf{G}_{2+r}[g](z,\overline{z})dxdy,$$

$$\mathbb{E}_{(r)}[\underline{D}] = \iint_{\widetilde{\mathcal{F}}} \Delta\left[\mathbf{K}_{2+r} \circ (I - \mathbf{H}_{2+r})^{-1}\right] \circ [W\mathbf{H}_{2+r}] \circ (I - \mathbf{H}_{2+r})^{-1}[g](z,\overline{z})dxdy$$

Theorem 5. *On the set Ω_M of inputs of size M endowed with a 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*

$$\mathbb{E}_{M,(r)} = \beta(r)M + \alpha(r) + \epsilon_r(M)$$

$$\text{with} \quad \begin{array}{lcll} \epsilon_r(M) & = & O(M^2 \exp[-(2r+1)M]) & \text{for } -1/2 < r \leq 0, \\ \epsilon_r(M) & = & O(M^2 \exp[-M]) & \text{for } r \geq 0. \end{array}$$

When $r \to -1$, then the two constants $\alpha(r)$ and $\beta(r)$ satisfy

$$\beta(r) =\sim (r+1)^{-1}, \quad \alpha(r) \sim (r+1)^{-2}.$$

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] J. Bourdon, B. Daireaux, B. Vallée. Dynamical analysis of α-Euclidean Algorithms, *Journal of Algorithms* 44 (2002) pp 246–285.

[4] D. Bump. Automorphic Forms and Representations, Cambridge University Press (1996)

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

[6] 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.

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

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

[9] 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

[10] A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen 261* (1982), 513–534.

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

[12] W. Scharlau and H. Opolka. *From Fermat to Minkowski, Lectures on the Theory of Numbers and its Historical Developments*. Undergraduate Texts in Mathematics. Springer-Verlag, 1984.

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

[14] 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.

[15] 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

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

[17] 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.

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

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