Probalistic analyses of lattice reductions algorithms

Brigitte Vallée, Antonio Vera

PROBABILISTIC ANALYSES OF LATTICE REDUCTIONS ALGORITHMS

BRIGITTE VALLÉE AND ANTONIO VERA

Résumé. The general behaviour of lattice reduction algorithms is far from being well understood. Indeed, many experimental observations, regarding the execution of the algorithms and the geometry of their ouputs, pose challenging questions, which remain unanswered and lead to natural conjectures yet to be settled. This survey describes complementary approaches, which can be adopted for analysing these algorithms, namely, dedicated modelling, probabilistic methods, and a dynamical systems approach. We explain how a mixed methodology has already proved fruitful for small dimensions p, corresponding to the variety of Euclidean algorithms ($p = 1$) and to the Gauss algorithm ($p = 2$). Such small dimensions constitute an important step in the analysis of lattice reduction in any (high) dimension, since the celebrated LLL algorithm, due to Lenstra, Lenstra and Lovász, precisely involves a sequence of Gauss reduction steps on sublattices of a large lattice.

1. General Context.

The present study surveys the main works aimed at understanding, both from a theoretical and an experimental viewpoint, how the celebrated LLL algorithm designed by Lenstra, Lenstra and Lovász performs in practice. The goal is to precisely quantify the probabilistic behaviour of lattice reduction and attain a justification of many of the experimental facts observed. Beyond its intrinsic theoretical interest, such a justification is important since a fine understanding of the lattice reduction process conditions algorithmic improvements in major application areas, like cryptography, computational number theory, integer programming, and computational group theory. The results obtained in this perspective may then be applied for developing a *general algorithmic strategy* for lattice reduction.

Varied approaches. We briefly describe now three different points of view : dedicated modelling, probabilistic methods, dynamical systems approach.

Dedicated modelling. Probabilistic models are problem-specific in the various applications of lattice reduction. For each particular area, special types of lattice bases are used as input models, which induce rather different quantitative behaviours. An analysis of the lattice reduction algorithms, under such probabilistic models aims at characterizing the behaviour of the main parameters, — principally, the number of iterations, the geometry of reduced bases, and the evolution of densities during an execution.

Probabilistic methods. The probabilistic line of investigation has already led to tangible results under the (somewhat unrealistic) models where vectors of the input basis are independently chosen according to a distribution that is rotationally invariant. In particular, the following question has been answered : what is the probability for a basis to be reduced ? A possible extension of this study to realistic models and to the complete algorithm (not just its input distribution) is here discussed.

Dynamical systems approach. Thanks to earlier results, the dynamics of Euclid's algorithm is now well-understood—many results describe the probabilistic behaviour of that algorithm, based on *dynamical systems theory* as well as related tools, like transfer operators. These techniques are then extended to dimension $p = 2$ (Gauss' algorithm). We examine here possible extensions of the "dynamical analysis methodology" to higher dimensions. The first step in such an endeavour should describe the dynamical system for the LLL algorithm, which is probably a complex object, for $p > 2$.

Date: 29 septembre 2007.

Historical and bibliographic notes. Over the past twenty years, there have been several parallel studies dedicated to the probabilistic behaviour of lattice reduction algorithms, in the two–dimensional case as well as in the general case.

The two dimensional case. The history of the analysis of lattice reduction algorithms starts ... before 1982, when Lagarias [21] performs in 1980 a first (worst–case) analysis of the Gauss algorithms in two and three dimensions. In 1990, Vallée [33] exhibits the exact worst–case complexity of the Gauss algorithm. In the same year, Flajolet and Vallée [15] perform the first probabilistic analysis of the Gauss algorithm : they study the mean value of the number of iterations in the uniform model. Then, in 1994, Daudé, Flajolet and Vallée [13] obtain a complete probabilistic analysis of the Gauss algorithm, with a "dynamical approach", but still under the uniform model. The same year, Laville and Vallée [22] study the main output parameters of the algorithm (the first minimum, Hermite's defect), under the uniform model, still. In 1997, Vallée [34] introduces the model "with valuation" for the Sign Algorithm : this is an algorithm for comparing rationals, whose behaviour is similar to the Gauss algorithm. In 2000, Flajolet and Vallée [16] precisely study all the constants which appear in the analysis of the Sign Algorithm. Finally, in 2007, Vallée and Vera [39] study all the main parameters of the Gauss algorithm (execution parameters and output parameters) in the general model "with valuation".

The dynamical analysis methodology. From 1995, Vallée has built a general method for analyzing a whole class of gcd algorithms. These algorithms are all based on the similar principles as the Euclid algorithms (divisions and exchanges), but they perform divisions of different type. This method, summarized for instance in [32], views an algorithm as a dynamical system and uses a variety of tools, some of them coming from analysis of algorithms (generating functions, singularity analysis, etc...) and other ones being central in dynamical systems, like transfer operators. The interest of such an analysis becomes apparent in the work about the Gauss Algorithm, already described [13], which is in fact the first beginning of dynamical analysis. The dynamical systems that underly the Gauss algorithms are just extensions of systems associated to the (centered) Euclid algorithms which first need a sharp understanding. This is why Vallée returns to the one-dimensional case, first performs average–case analysis for a large variety of Euclidean algorithms and related parameters of interest : number of iterations [36], bit–complexity (with Akhavi) [4], bit–complexity of the fast variants of the Euclid algorithms (with the Caen team) [9]. From 2003, Baladi, Lhote and Vallée [5, 25] also obtain distributional results on the main parameters of the Euclid algorithms –number of iterations, size of the remainder at a fraction of the execution, bit-complexity– and show that they all follow asymptotic normal laws.
It is now natural to expect that most of the principles of the dynamical analysis can be applied to the Gauss algorithm. The first work in this direction is actually done by Vallée and Vera, quite recently (2007), and completes the first work [13].

The general case. The first probabilistic analysis of the LLL algorithm is performed by Daudé and Vallée en 1994 [14] under the "random ball model". These authors obtain an upper–bound for the mean number of iterations of the algorithm. Then, in 2002, Akhavi [2] studies the probabilistic behaviour of a random basis (again, under the random ball model) and he detects two different regimes, according to the dimension of the basis relative to the dimension of the ambient space. In 2006, Akhavi, Marckert and Rouault [3] improve on the previous study, while generalizing it to other randomness models (the so–called spherical models) : they exhibit a limit model, when the ambient dimension becomes large. These studies illustrate the importance of the model "with valuation" for the local bases associated to the input.
In 2003, Ajtai [1] exhibits a randomness model of input bases (which is called the Ajtai model in this paper), under which the probabilistic behaviour of the LLL algorithm is close to the worst-case behaviour. In 2006, Nguyen and others [17] study random lattices and their parameters relevant to lattice reduction algorithms. In 2006, Nguyen and Stehlé [27] conduct many experiments for the LLL algorithms under several randomness models. They exhibit interesting experimental phenomena and provide conjectures that would explain them.

The two–dimensional case as a main tool for the general case. This paper describes a first attempt to apply the dynamical analysis methodology to the LLL algorithm : the LLL algorithm is now viewed as a whole dynamical system which runs in parallel many two dimensional dynamical systems, and "gathers" all the dynamics of these small systems. This (perhaps) makes possible to use the precise

results obtained on the Gauss algorithm –probabilistic, and dynamic– as a main tool for describing the probabilistic behaviour of the LLL algorithm, and its whole dynamics.

Plan of the survey. Section 2 explains why the two dimensional–case is central, introduces the lattice reduction in this particular case, and presents the Gauss algorithm which is our main object of study. Section 3 is devoted to a precise description of the LLL algorithm in general dimension ; it introduces the main parameters of interest : the output parameters which describe the geometry of the output bases, and the execution parameters, which describe the behaviour of the algorithm itself. The results of the main experiments conducted regarding these parameters on "useful" classes of lattices are also reported there. Finally, we introduce variants of the LLL algorithm, where the rôle of the Gauss algorithm becomes more apparent than in standard versions. Section 4 describes the main probabilistic models of interest which appear in "real life" applications—some of them are given because of their naturalness, whereas other ones are related to actual applications of the LLL algorithm. Section 5 is devoted to a particular class of models, the so–called spherical models, which are the most natural models (even though they do not often surface in actual applications). We describe the main results obtained under this model : the distribution of the "local bases", the probability of an initial reduction, and mean value estimates of the number of iterations and of the first minimum.
A first step towards a precise study of other, more "useful", models is a fine understanding of the two dimensional case, where the mixed methodology is employed. In Section 6, we describe the dynamical systems that underly the (two) versions of the Gauss algorithms, together with two (realistic) input probabilistic models of use : the model "with valuation", and the model "with fixed determinant". Sections 7 and 8 focus on the precise study of the main parameters of interest –either output parameters or execution parameters— under the model "with valuation". Finally, Section 9 returns to the LLL algorithm and explains how the results of Sections 6, 7, and 8 could (should ?) be used and/or extended to higher dimensions.

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 $B := (b_1, b_2, \dots b_p)$ 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 [23] 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 section : it 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.

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

$$\mathcal{L} = \mathbb{Z}u \oplus \mathbb{Z}v = \{au + bv; \quad a, b \in \mathbb{Z}\},$$

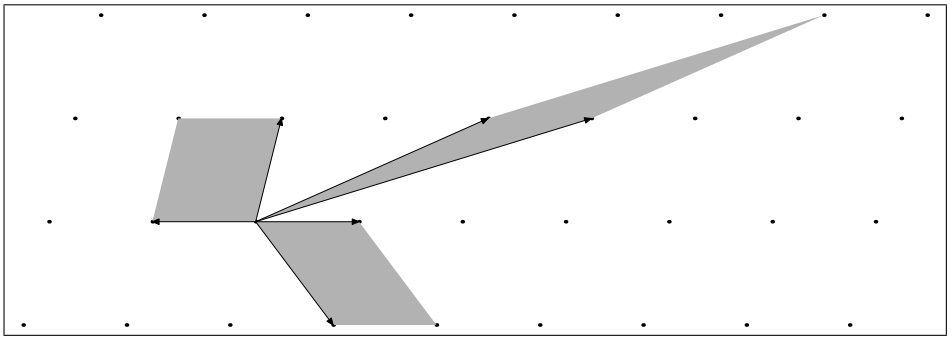

FIG. 1. A lattice and three of its bases represented by the parallelogram they span. The basis on the left is minimal (reduced), whereas the two other ones are skew.

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 1). 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 2.1. [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 acute framework, and, for the second case, the positive 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 2.1. 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[1] to the real x. After this translation, the new coefficient $\tau(v,u)$ satisfies $0 \le |\tau(v,u)| \le (1/2)$.

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

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

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 $\mathbb{Z}$, the final pair (v_p, v_{p+1}) satisfies the conditions (P) of Proposition 2.1. and $P(u,v) := p$ denotes the number of iterations. 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 2.1. The condition (A_1) is simply satisfied by an exchange, and the condition (A_2) is met by an integer translation of the type :

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

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

AGauss(u,v)
Input. An acute basis (u,v) of $\mathbb{C}$ with $|v| \le |u|,\ 0 \le \tau(v,u) \le (1/2)$.
Output. An acute minimal basis (u,v) of $\mathcal{L}(u,v)$ with $|v| \ge |u|$.

```
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 $w_{i+1} = \epsilon_i(w_{i-1} - \widetilde{q}_i\, w_i)$ with

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

[1]The function $\lfloor x \rceil$ is extended to the negative numbers with the relation $\lfloor x \rceil = -\lfloor -x \rceil$.

Here, each quotient $\widetilde{q}_i$ is a positive integer, $p \equiv P(u,v)$ denotes the number of iterations [this equals the previous one], and the final pair (w_p, w_{p+1}) satisfies the conditions (A) of Proposition 2.1. Each step defines a unimodular matrix $\mathcal{N}_i$ with $\det \mathcal{N}_i = \epsilon_i = \pm 1$,

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

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 [6]. We shall come back to this fact in Section 6.3. 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*[2] 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.

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 :

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

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

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

which satisfy $D(u,v) - \underline{D}(u,v) = \Theta(Q(u,v))$ 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 and shall explain in Section 3.5 why they are so important in the study of the LLL algorithm. We now return to the general case of lattice reduction.

3. The LLL algorithm.

We provide a description of the LLL algorithm, introduce the parameters of interest, and explain the bounds obtained in the worst-case analysis. Then, we describe the results of the main experiments conducted for classes of "useful" lattices. Finally, this section presents a variant of the LLL algorithm, where the Gauss algorithm plays a more apparent rôle : it appears to be well-adapted to (further) analyses.

3.1. Description of the algorithm.

We recall that the LLL algorithm considers a Euclidean lattice given by a system B formed of p linearly independent vectors in the ambient space $\mathbb{R}^n$. It aims at finding a reduced basis, denoted by $\hat{B}$ formed with vectors almost orthogonal and short enough. The algorithm deals with the matrix $\mathcal{P}$ which expresses the system B as a function of the Gram–Schmidt orthogonalized system B^* ; the coefficient $m_{i,j}$ of matrix $\mathcal{P}$ is equal to $\tau(b_i, b_j^\star)$ with τ defined in (2). The algorithm performs two main types of operations :

(i) *Size–reduction of vectors.* The vector b_i is size–reduced if all the coefficients $m_{i,j}$ of the i-th row of matrix $\mathcal{P}$ satisfy $|m_{i,j}| \leq (1/2)$ for all $j \in [1..i-1]$. Size-reduction of vector b_i is performed by integer translations of b_i with respect to vectors b_j for all $j \in [1..i-1]$.

Since subdiagonal coefficients play a particular rôle (as we shall see later), the total operation `Size-reduction` (b_i) is subdivided into two main operations :

`Diagonal size-reduction` (b_i) ;
$b_i := b_i - \lfloor m_{i,i-1} \rceil b_{i-1}$;

followed with

`Other-size-reduction` (b_i) ;

$$\texttt{For } j := i-2 \texttt{ downto } 1 \text{ do } b_i := b_i - \lfloor m_{i,j} \rceil b_j \,;$$

(*ii*) *Gauss–reduction of the local bases.* The i-th local basis U_i is formed with the two vectors u_i, v_i, defined as the orthogonal projections of b_i, b_{i+1} on the orthogonal of the subspace $\langle b_1, b_2, \ldots, b_{i-1}\rangle$. The LLL algorithm performs the PGauss algorithm [integer translations and exchanges] on local bases U_i, but there are three differences with the PGauss algorithm previously described :

(*a*) The output test is *weaker* and depends on a parameter $t > 1$: the classical Gauss output test $|v_i| > |u_i|$ is replaced by the output test $|v_i| > (1/t)|u_i|$.

(*b*) The operations that are performed during the PGauss algorithm on the local basis U_i are then *reflected* on the system (b_i, b_{i+1}) : if $\mathcal{M}$ is the matrix built by the PGauss algorithm on (u_i, v_i) then it is applied to the system (b_i, b_{i+1}) in order to find the new system (b_i, b_{i+1}).

(*c*) The PGauss algorithm is performed on the local basis U_i *step by step*. The index i of the local basis visited begins at $i = 1$, ends at $i = p$, and is incremented (when the test in Step 2 is positive) or decremented (when the test in Step 2 is negative and the index i does not equal 1) at each step. This defines a random walk. The length K of the random walk is the number of iterations, and the number of steps K^- where the test in step 2 is negative satisfies

$$K \leq (p-1) + 2K^- . \tag{13}$$

$$\mathcal{P} := \begin{array}{c} \\ b_1 \\ b_2 \\ \vdots \\ b_i \\ b_{i+1} \\ \vdots \\ b_p \end{array} \begin{array}{c} \begin{array}{ccccccc} b_1^\star & b_2^\star & \ldots & b_i^\star & b_{i+1}^\star & \ldots & b_p^\star \end{array} \\ \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & 0 & 0 \\ m_{2,1} & 1 & \ldots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ m_{i,1} & m_{i,2} & \ldots & 1 & 0 & 0 & 0 \\ m_{i+1,1} & m_{i+1,2} & \ldots & m_{i+1,i} & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ m_{p,1} & m_{p,2} & \ldots & m_{p,i} & m_{p,i+1} & \ldots & 1 \end{pmatrix} \end{array} \qquad U_k := \begin{array}{c} \\ u_k \\ v_k \end{array} \begin{array}{c} \begin{array}{cc} b_k^\star & b_{k+1}^\star \end{array} \\ \begin{pmatrix} 1 & 0 \\ m_{k+1,k} & 1 \end{pmatrix} \end{array}$$

LLL (t) $\quad [t > 1]$

Input. A basis B of a lattice L of dimension p.
Output. A reduced basis $\hat{B}$ of L.

`Gram` computes the basis $B^\star$ and the matrix $\mathcal{P}$.
$i := 1$;
`While` $i < p$ `do`
1– `Diagonal Size-Reduction` (b_{i+1})
2– **Test** if local basis U_i is `reduced` : Is $|v_i| > (1/t)|u_i|$?
if yes : `Other-size-reduction` (b_{i+1})
$i := i + 1$;
if not : `Exchange` b_i and b_{i+1}
`Recompute` $(B^\star, \mathcal{P})$;
`If` $i \neq 1$ `then` $i := i - 1$;

FIG. 2. The LLL algorithm, the matrix $\mathcal{P}$, and the local bases U_k.

The LLL algorithm considers the sequence ℓ_i formed with the lengths of the vectors of the Gram orthogonalized basis $B^\star$ and deals with the ratios r_i's between successive Gram orthogonalized vectors, namely

$$r_i := \frac{\ell_{i+1}}{\ell_i}, \qquad \text{with} \quad \ell_i := |b_i^\star|. \tag{14}$$

The steps of Gauss reduction aim at obtaining lower bounds on these ratios. In this way, the interval $[a, A]$ with

$$a := \min\{\ell_i; \quad 1 \leq i \leq p\}, \qquad A := \max\{\ell_i; \quad 1 \leq i \leq p\}, \tag{15}$$

tends to be narrowed since, all along the algorithm, the minimum a is increasing and the maximum A is decreasing. This interval $[a, A]$ plays an important rôle because it provides an approximation for the first minimum $\lambda(\mathcal{L})$ of the lattice (i.e., the length of a shortest non zero vector of the lattice), namely

$$\lambda(\mathcal{L}) \leq A\sqrt{p}, \qquad \lambda(\mathcal{L}) \geq a. \tag{16}$$

At the end of the algorithm, all the local bases are reduced in the t–Gauss meaning. They satisfy conditions that involve the subdiagonal matrix coefficients $m_{i+1,i}$ together with the sequence ℓ_i, namely the t–Lovasz conditions, for any $i, 1 \leq i \leq p-1$,

$$|\hat{m}_{i+1,i}| \leq \frac{1}{2}, \qquad t^2\,(\hat{m}_{i+1,i}^2\,\hat{\ell}_i^2 \,+\, \hat{\ell}_{i+1}^2) \geq \hat{\ell}_i^2, \tag{17}$$

which *imply* the s–Siegel conditions, for any $i, 1 \leq i \leq p-1$,

$$|\hat{m}_{i+1,i}| \leq \frac{1}{2}, \qquad \hat{r}_i := \frac{\hat{\ell}_{i+1}}{\hat{\ell}_i} \geq \frac{1}{s}, \qquad \text{with} \quad s^2 = \frac{4t^2}{4-t^2} \quad \text{and} \quad s = \frac{2}{\sqrt{3}} \quad \text{for } t = 1. \tag{18}$$

A basis for which conditions (18) are fulfilled is called s–Siegel reduced.

There are two kinds of parameters of interest for describing the behaviour of the algorithm : the output parameters and the execution parameters.

3.2. **Output parameters.** The geometry of the output basis is described with three main parameters —the Hermite defect $\gamma(B)$, the length defect $\theta(B)$ or the orthogonality defect $\rho(B)$—. They satisfy the following (worst-case) bounds that are functions of parameter s, namely

(19)
$$\gamma(B) := \frac{|\hat{b}_1|^2}{(\det \mathcal{L})^{2/p}} \leq s^{p-1}, \qquad \theta(B) := \frac{|\hat{b}_1|}{\lambda(\mathcal{L})} \leq s^{p-1}, \qquad \rho(B) := \frac{\prod_{i=1}^{d} |\hat{b}_i|}{\det \mathcal{L}} \leq s^{p(p-1)/2}.$$

This proves that the output satisfies good Euclidean properties. In particular, the length of the first vector of $\hat{B}$ is an approximation of the first minimum $\lambda(\mathcal{L})$ –up to a factor which exponentially depends on dimension p– .

3.3. **Execution parameters.** The execution parameters are related to the execution of the algorithm itself : the length of the random walk (equal to the number of iterations K), the size of the integer translations, the size of the rationals $m_{i,j}$ along the execution.

The product D of the determinants D_j of beginning lattices $\mathcal{L}_j := \langle b_1, b_2, \ldots, b_j \rangle$, defined as

$$D_j := \prod_{i=1}^{j} \ell_i, \qquad D = \prod_{j=1}^{p-1} D_j = \prod_{j=1}^{p-1} \prod_{i=1}^{j} \ell_i,$$

is never increasing all along the algorithm and is strictly decreasing, with a factor of $(1/t)$, for each step of the algorithm when the test in 2 is negative. In this case, the exchange modifies the length of ℓ_i and ℓ_{i+1} —without modifying their product, equal to the determinant of the basis U_i–. The new ℓ_i, denoted by $\check{\ell}_i$ is the old $|v_i|$, which is at most $(1/t)|u_i| = (1/t)\ell_i$. Then the new determinant $\check{D}_i$ satisfies $\check{D}_i \leq (1/t)D_i$, and the others D_j are not modified.

Then the final $\hat{D}$ satisfies $\hat{D} \leq (1/t)^{K^-} D$ where K^- denotes the number of indices of the random walk when the test in 2 is negative (see Section 3.1). With the following bounds on the initial D and the final $\hat{D}$, as a function of variables a, A, defined in (15),

$$D \leq A^{p(p-1)/2}, \qquad \hat{D} \geq a^{p(p-1)/2},$$

together with the expression of K as a function of K^- given in (13), the following bound on K is derived,

$$K \leq (p-1) + p(p-1)\log_t \frac{A}{a}. \tag{20}$$

In the same vein, another kind of bound involves $N := \max |b_i|^2$ and the first minimum $\lambda(\mathcal{L})$, (see [14]),

$$K \leq \frac{p^2}{2} \log_t \frac{N\sqrt{p}}{\lambda(\mathcal{L})}.$$

In the case when the lattice is integer (namely $\mathcal{L} \subset \mathbb{Z}^n$), this bound is slightly better and becomes $K \leq (p-1) + p(p-1)\frac{M}{\lg t}$, where M is the binary size of B, namely $M := \max \ell(|b_i|^2)$, where $\ell(x)$ is the binary size of integer x.

All the previous bounds are *proven upper bounds* on the main parameters. It is interesting to compare these bounds to *experimental mean values* obtained on a variety of lattice bases that actually occur in applications of lattice reduction.

3.4. **Experiments for the LLL algorithm.** In [27], Nguyen and Stehlé have made a great use of their efficient version of the LLL algorithm [26] and conducted for the first time extensive experiments on the two major types of useful lattice bases : the Ajtai bases, and the knapsack–shape bases which will be defined in the next section. Figures 3 and 4 show some of the main experimental results. These experimental results are also described in the survey written by D. Stehlé in these proceedings [31].

Main parameters.	$\hat{r}_i$	γ	θ	ρ	K
Worst-case (Proven upper bounds)	$1/s$	s^{p-1}	s^{p-1}	$s^{p(p-1)/2}$	$\Theta(Mp^2)$
Random Ajtai bases (Experimental mean values)	$1/\alpha$	α^{p-1}	$\alpha^{(p-1)/2}$	$\alpha^{p(p-1)/2}$	$\Theta(Mp^2)$
Random knapsack–shape bases (Experimental mean values)	$1/\alpha$	α^{p-1}	$\alpha^{(p-1)/2}$	$\alpha^{p(p-1)/2}$	$\Theta(Mp)$

FIG. 3. Comparison between proven upper bounds and experimental mean values for the main parameters of interest. Here p is the dimension of the input (integer) basis, and M is the binary size of the input (integer) basis : $M := \Theta(\log N)$ where $N := \max |b_i|^2$.

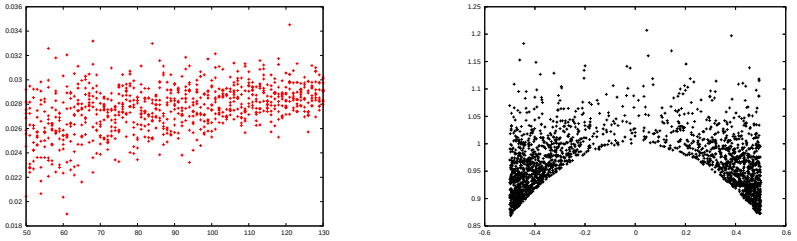

FIG. 4. On the left : experimental results for $\log_2 \gamma$. The experimental value of parameter $[1/(2p)]\,\mathbb{E}[\log_2 \gamma]$ is close to 0.03, so that α is close to 1.04. On the right, the output distribution of "local bases" .

Output geometry. The geometry of the output local basis $\hat{U}_k$ seems to depend neither on the class of lattice bases nor on index k of the local basis (along the diagonal of $\mathcal{P}$), except for very extreme values of k. We consider the complex number $\hat{z}_k$ that is related to the output local basis $\hat{U}_k := (\hat{u}_k, \hat{v}_k)$ via the equality $\hat{z}_k := \hat{m}_{k,k+1} + i\hat{r}_k$. Due to the t–Lovasz conditions on $\hat{U}_k$, described in (17), the complex number $\hat{z}_k$ belongs to the domain

$$\mathcal{F}_t := \{z \in \mathbb{C}; \quad |z| \geq 1/t, \ |\Re(z)| \leq 1/2\},$$

and the geometry of the output local basis $\hat{U}_k$ is characterized by a distribution which much "weights" the "corners" of $\mathcal{F}_t$ defined by $\mathcal{F}_t \cap \{z; \Im z \leq 1/t\}$ [See Figure 4 (right)]. The (experimental) mean values of the output Siegel ratios $\hat{r}_k := \Im(\hat{z}_k)$ appear to be of the same form as the (proven) upper bounds, with a ratio α (close to 1.04) which replaces the ratio s_0 close to 1.15 when

t_0 is close to 1. As a consequence, the (experimental) mean values of parameters $\gamma(B)$ and $\rho(B)$ appear to be of the same form as the (proven) upper bounds, with a ratio α (close to 1.04) which replaces the ratio s_0 close to 1.15.

For parameter $\theta(B)$, the situation is slightly different. Remark that the estimates on parameter θ are not only a consequence of the estimates on the Siegel ratios, but they also depend on estimates which relate the first minimum and the determinant. Most of the lattices are (probably) *regular* : this means that the average value of the ratio between the first minimum $\lambda(\mathcal{L})$ and $\det(\mathcal{L})^{1/p}$ is of polynomial order with respect to dimension p. This regularity property should imply that the experimental mean value of parameter θ is of the same form as the (proven) upper bound, but now with a ratio $\alpha^{1/2}$ (close to 1.02) which replaces the ratio s_0 close to 1.15.

Open question. Does this constant α admit a mathematical definition, related for instance to the underlying dynamical system [see Section 6] ?

Execution parameters. Regarding the number of iterations, the situation differs according to the types of bases considered. For the Ajtai bases, the number of iterations K exhibits experimentally a mean value of the same order as the proven upper bound, whereas, in the case of the knapsack-shape bases, the number of iterations K has an experimental mean value of smaller order than the proven upper bound.

Open question. Is it true for the "actual" knapsack bases that come from cryptographic applications ? [See Section 4.4]

All the remainder of this survey is devoted to presenting a variety of methods that could (should ?) lead to explaining these experiments. One of our main ideas is to use the Gauss algorithm as a central tool for this purpose. This is why we now present a variant of the LLL algorithm where the Gauss algorithm plays a more apparent rôle.

3.5. **A variation for the LLL algorithm : the Odd-Even algorithm.** The original LLL algorithm performs the Gauss Algorithm *step by step*, but does not perform the *whole* Gauss algorithm on local bases. This is due to the definition of the random walk of the indices on the local bases (See Section 3.1). However, this is not the only strategy for reducing all the local bases. There exists for instance a variant of the LLL algorithm, introduced by Villard [41] 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 we shall explain in Section 6 that it has a better "dynamical" structure.

During one even (resp. odd) phase, the *whole* AGauss algorithm is performed on all local bases U_i 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. Here, we will use this algorithm in Section 9, when we shall explain the main principles for a dynamical study of the LLL algorithm.

Consider, for an odd index k, two successive bases $U_k := (u_k, v_k)$ and $U_{k+2} := (u_{k+2}, v_{k+2})$. Then, the Odd Phase of the Odd-Even LLL algorithm (completely) reduces these two local bases (in the t–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

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

where parameters λ, μ are defined in (11). During the Even phase, the LLL algorithm considers (in parallel) all the local bases with an even index. Now, at the beginning of the following Even Phase, the (input) basis U_{k+1} is formed (up to a similarity) from the two previous output bases, as : $u_{k+1} = \hat{v}_k^\star$, $v_{k+1} = \nu \hat{v}_k^\star + \hat{u}_{k+2}$, where ν is a real number of the interval $[-1/2, +1/2]$. Then, the initial Siegel ratio r_{k+1} of the Even Phase can be expressed with the output lengths of the Odd Phase, as

$$r_{k+1} = \frac{\lambda(u_{k+2}, v_{k+2})}{\mu(u_k, v_k)}.$$

This explains the important rôle which is played by these parameters λ, μ. We study these parameters in Section 7.

Odd–Even LLL (t) $\quad [t > 1]$

Input. A basis B of a lattice L of dimension p.
Output. A reduced basis $\hat{B}$ of L.

`Gram` computes the basis $B^\star$ and the matrix $\mathcal{P}$.
`While` B is not reduced `do`
  `Odd Phase` (B) :
    `For` $i = 1$ to $\lfloor n/2 \rfloor$ `do`
      `Diagonal-size-reduction` (b_{2i}) ;
      $\mathcal{M}_i := t$–AGauss (U_{2i-1}) ;
      $(b_{2i-1}, b_{2i}) := (b_{2i-1}, b_{2i})^t \mathcal{M}_i$;
    `For` $i = 1$ to n `do Other-size-reduction` (b_i) ;
    `Recompute` $B^\star, \mathcal{P}$;
  `Even Phase` (B) :
    `For` $i = 1$ to $\lfloor (n-1)/2 \rfloor$ `do`
      `Diagonal-size-reduction` (b_{2i+1}) ;
      $\mathcal{M}_i := t$–AGauss (U_{2i}) ;
      $(b_{2i}, b_{2i+1}) := (b_{2i}, b_{2i+1})^t \mathcal{M}_i$;
    `For` $i = 1$ to n `do Other-size-reduction` (b_i) ;
    `Recompute` $B^\star, \mathcal{P}$;

FIG. 5. The Odd-Even variant of the LLL algorithm.

4. What is a random (basis of a) lattice ?

We now describe the main probabilistic models, addressing the various applications of lattice reduction. For each particular area, there are special types of input lattice bases that are used and this leads to different probabilistic models dependent upon the specific application area considered. Cryptology is a main application area, and it is crucial to describe the major "cryptographic" lattices, but there also exist other important applications.

There are various types of "interesting" lattice bases. Some of them are also described in the survey of D. Stehlé in these proceedings [31].

4.1. **Spherical Models.** The most natural way is to choose independently p vectors in the n-dimensional unit ball, under a distribution that is invariant by rotation. This is the spherical model introduced for the first time in [14], then studied in [2, 3] (See Section 5). This model does not seem to have surfaced in practical applications (except perhaps in integer linear programming), but it constitutes a reference model, to which it is interesting to compare the realistic models of use.

We consider distributions $\nu_{(n)}$ on $\mathbb{R}^n$ that are invariant by rotation, and satisfy $\nu_{(n)}(0) = 0$, which we call "simple spherical distributions". For a simple spherical distribution, the angular part $\theta_{(n)} := b_{(n)}/|b_{(n)}|$ is uniformly distributed on the unit sphere $\mathbb{S}_{(n)} := \{x \in \mathbb{R}^n : \|x\| = 1\}$. Moreover, the radial part $|b_{(n)}|^2$ and the angular part are independent. Then, a spherical distribution is completely determined by the distribution of its radial part, denoted by $\rho_{(n)}$.

Here, the beta and gamma distribution play an important rôle. Let us recall that, for strictly positive real numbers $a, b \in \mathbb{R}^{+\star}$, the beta distribution of parameters (a, b) denoted by $\beta(a, b)$ and the gamma distribution of parameter a denoted by $\gamma(a)$ admit densities of the form

$$\beta_{a,b}(x) = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} x^{a-1}(1-x)^{b-1}\ \mathbf{1}_{(0,1)}(x), \qquad \gamma_a(x) = \frac{e^{-x}x^{a-1}}{\Gamma(a)}\ \mathbf{1}_{[0,\infty)}(x).$$

We now describe three natural instances of simple spherical distributions.

(i) The first instance of a simple spherical distribution is the uniform distribution in the unit ball $\mathcal{B}_{(n)} := \{x \in \mathbb{R}^n : \|x\| \leq 1\}$. In this case, the radial distribution $\rho_{(n)}$ equals the beta distribution $\beta(n/2, 1)$.

(ii) A second instance is the uniform distribution on the unit sphere $\mathbb{S}_{(n)}$, where the radial distribution $\rho_{(n)}$ is the Dirac measure at $x = 1$.

(*iii*) A third instance occurs when all the n coordinates of the vector $b_{(n)}$ are independent and distributed with the standard normal law $\mathcal{N}(0,1)$. In this case, the radial distribution $\rho_{(n)}$ has a density equal to $2\gamma_{n/2}(2t)$.

When the system $B_{p,(n)}$ is formed with p vectors (with $p \leq n$) which are picked up randomly from $\mathbb{R}^n$, independently, and with the same simple spherical distribution $\nu_{(n)}$, we say that the system $B_{p,(n)}$ is distributed under a "spherical model". Under this model, the system $B_{p,(n)}$ (for $p \leq n$) is almost surely linearly independent.

4.2. **The Ajtai bases.** Consider an integer sequence $a_{i,p}$ defined for $1 \leq i \leq p$, which satisfies the conditions

$$\text{For any } i, \quad \frac{a_{i+1,p}}{a_{i,p}} \to 0 \qquad \text{when } p \to \infty.$$

A sequence of Ajtai bases $B := (B_p)$ relative to the sequence $a = (a_{i,p})$ is defined as follows : The basis B_p is of dimension p and is formed by vectors $b_{i,p} \in \mathbb{Z}^p$ of the form

$$b_{i,p} = a_{i,p}\, e_i + \sum_{j=1}^{i-1} a_{i,j,p}\, e_j \qquad \text{with} \quad a_{i,j,p} = \text{rand}\left(-\frac{a_{j,p}}{2}, \frac{a_{j,p}}{2}\right) \quad \text{for} \quad j < i.$$

[Here, (e_j) (with $1 \leq j \leq p$) is the canonical basis of $\mathbb{R}^p$]. Remark that these bases are already size-reduced, since the coefficient $m_{i,j}$ equals $a_{i,j,p}/a_{j,p}$. However, all the input ratios r_i, equal to $a_{i+1,p}/a_{i,p}$, tend to 0 when p tends to ∞. All this explains why similar bases have been used by Ajtai in [1] to show the tightness of worst-case bounds of [28].

4.3. **Variations around knapsack bases and their transposes.** This last type gathers various shapes of bases, which are all formed by "bordered identity matrices". See Figure 6.

(*i*) The knapsack bases themselves are the rows of the $p \times (p+1)$ matrices of the form of Figure 6 (*a*), where I_p is the identity matrix of order p and the components $(a_1, a_2, \ldots a_p)$ of vector A are sampled independently and uniformly in $[-N, N]$, for some given bound N. Such bases often occur in cryptanalyses of knapsack-based cryptosystems, or in number theory (reconstructions of minimal polynomials and detections of integer relations between real numbers).

(*ii*) The bases relative to the transposes of matrices described in Figure 6 (*b*) arise in searching for simultaneous diophantine approximations (with $q \in \mathbb{Z}$) or in discrete geometry (with $q = 1$).

(*iii*) The NTRU cryptosystem was first described in terms of polynomials over finite fields, but the public-key can be seen [11] as the lattice basis given by the rows of the matrix $(2p \times 2p)$ described in Figure 6 (*c*) where q is a small power of 2 and H_p is a circulant matrix whose line coefficients are integers of the interval $]-q/2, q/2]$.

4.4. **Random lattices.** There is a natural notion of random lattice, introduced by Siegel [30] in 1945. The space of (full-rank) lattices in $\mathbb{R}^n$ modulo scale can be identified with the quotient $X_n = SL_n(\mathbb{R})/SL_n(\mathbb{Z})$. The group $G_n = SL_n(\mathbb{R})$ possesses a unique (up to scale) bi-invariant Haar measure, which projects to a finite measure on the space X_n. This measure ν_n (which can be normalized to have total volume 1) is by definition the unique probability on X_n which is invariant under the action of G_n : if $A \subseteq X_n$ is measurable and $g \in G_n$, then $\nu_n(A) = \nu_n(gA)$. This gives rise to a natural notion of random lattices. We come back to this notion in the two–dimensional case in Section 7.2.

$$\left(\begin{array}{c|c} A & I_p \end{array}\right) \quad \left(\begin{array}{c|c} y & 0 \\ \hline x & qI_p \end{array}\right) \quad \left(\begin{array}{c|c} I_p & H_p \\ \hline 0_p & qI_p \end{array}\right) \quad \left(\begin{array}{c|c} q & 0 \\ \hline x & I_{n-1} \end{array}\right)$$

$$(a) \qquad (b) \qquad (c) \qquad (d)$$

FIG. 6. Different kinds of lattices useful in applications

4.5. **Probabilistic models –continuous or discrete–.** Except two models – the spherical model, or the model of random lattices – that are *continuous* models, all the other ones (the Ajtai model or the various knapsack–shape models) are discrete models. In these cases, it is natural to build probabilistic models which preserve the "shape" of matrices and replace discrete coefficients by continuous ones. This allows to use in the probabilistic studies all the continuous tools of (real and complex) analysis.

(*i*) A first instance is the Ajtai model relative to sequence $a := (a_{i,p})$, for which the continuous version of dimension p is as follows :

$$b_{i,p} = a_{i,p}\, e_i + \sum_{j=1}^{i-1} x_{i,j,p}\, a_{j,p}\, e_j \qquad \text{with } x_{i,j,p} = \mathrm{rand}\,(-1/2, 1/2) \quad \text{for all } j < i \le p.$$

(*ii*) We also may replace the discrete model associated to knapsack bases of Figure 6(*a*) by the continuous model where A is replaced by a real vector x uniformly chosen in the ball $\|x\|_\infty \le 1$ and I_p is replaced by ρI_p, with a small positive constant $0 < \rho < 1$. Generally speaking, choosing continuous random matrices independently and uniformly in their "shape" class leads to a class of "knapsack–shape" lattices.

Remark. It is very unlikely that such knapsack–shape lattices share all the same properties as the knapsack lattices that come from the actual applications –for instance, the existence of an unusually short vector (significantly shorter than expected from Minkowski's theorem)–.

Conversely, we can associate to any continuous model, a discrete one : consider a domain $\mathcal{B} \subset \mathbb{R}^n$ with a "smooth" frontier. For any integer N, we can "replace" a (continuous) distribution in the domain $\mathcal{B}$ relative to some density f of class $\mathcal{C}^1$ by the distribution in the discrete domain

$$\mathcal{B}_N := \mathcal{B} \cap \frac{\mathbb{Z}^n}{N},$$

defined by the restriction f_N of f to $\mathcal{B}_N$. When $N \to \infty$, the distribution relative to density f_N tends to the distribution relative to f, due to the Gauss principle, which relates the volume of a domain $\mathcal{A} \subset \mathcal{B}$ (with a smooth frontier $\partial\mathcal{A}$) and the number of points in the domain $\mathcal{A}_N := \mathcal{A} \cap \mathcal{B}_N$,

$$\frac{1}{N^n}\mathrm{card}(\mathcal{A}_N) = \mathrm{Vol}(\mathcal{A}) + O\left(\frac{1}{N}\right) \mathrm{Area}(\partial\mathcal{A}).$$

We can apply this framework to any (simple) spherical model, and also to the models that are introduced for the two dimensional case.

In the same vein, we can consider a discrete version of the notion of a random lattice : Consider the set $\mathcal{L}(n, N)$ of the n-dimensional integer lattices of determinant N. Any lattice of $\mathcal{L}(n, N)$ can be transformed into a lattice of X_n (defined in 4.4) by the homothethy Ψ_N of ratio $N^{-1/n}$. Goldstein and Mayer [20] show that for large N, the following is true : given any measurable subset $A_n \subseteq X_n$ whose boundary has zero measure with respect to ν_n, the fraction of lattices of $\mathcal{L}(n, N)$ whose image by Ψ_N lies in A_n tends to $\nu_n(A)$ as N tends to infinity. In other words, the image by Ψ_N of the uniform probability on $\mathcal{L}(n, N)$ tends to the measure ν_n.
Thus, to generate lattices that are random in a natural sense, it suffices to generate uniformly at random a lattice in $\mathcal{L}(n, N)$ for large N. This is particularly easy when $N = q$ is prime. Indeed, when q is a large prime, the vast majority of lattices in $\mathcal{L}(n, q)$ are lattices spanned by rows of the matrices described in Figure 6(*d*), where the components x_i (with $i \in [1..n-1]$) of the vector x are chosen independently and uniformly in $\{0, \ldots, q-1\}$.

5. Probabilistic analyses of the LLL algorithm in the spherical model.

In this Section, the dimension of the ambient space is denoted by n, and the dimension of the lattice is denoted by p, and a basis of dimension p in $\mathbb{R}^n$ is denoted by $B_{p,(n)}$. The codimension g, equal by definition to $n - p$, plays a fundamental rôle here. We consider the case where n tends to ∞ while $g := g(n)$ is a fixed function of n (with $g(n) \le n$). We are interested in the following questions :

(*i*) Consider a real $s > 1$. What is the probability $\pi_{p,(n),s}$ that a random basis $B_{p,(n)}$ was already s–reduced in the Siegel sense [i.e., satisfy the relations (18)] ?

(*ii*) Consider a real $t > 1$. What is the average number of iterations of the LLL(t) algorithm on a random basis $B_{p,(n)}$?
(*iii*) What is the mean value of the first minimum of the lattice generated by a random basis $B_{p,(n)}$?
This section answers these questions in the case when $B_{p,(n)}$ is randomly chosen under a spherical model, and shows that there are two main cases according to the codimension $g := n - p$.

5.1. **Main parameters of interest.** Let $B_{p,(n)}$ be a linearly independent system of vectors of $\mathbb{R}^n$ whose codimension is $g = n - p$. Let $B^{\star}_{p,(n)}$ be the associated Gram-Schmidt orthogonalized system. We are interested by comparing the lengths of two successive vectors of the orthogonalized system, and we introduce several parameters related to the Siegel reduction of the system $B_{p,(n)}$.

Definition 5.1. *To a system $B_{p,(n)}$ of p vectors in $\mathbb{R}^n$, we associate the Gram-Schmidt orthogonalized system $B^{\star}_{p,(n)}$ and the sequence $\underline{r}_{j,(n)}$ of Siegel ratios, defined as*

$$\underline{r}_{j,(n)} := \frac{\ell_{n-j+1,(n)}}{\ell_{n-j,(n)}}, \qquad \text{for } g+1 \leq j \leq n-1,$$

together with two other parameters

$$\mathcal{M}_{g,(n)} := \min\{\underline{r}^2_{j,(n)}; \quad g+1 \leq j \leq n-1\} \qquad \mathcal{I}_{g,(n)} := \min\left\{j : \underline{r}^2_{j,(n)} = \mathcal{M}_{g,(n)}\right\}.$$

The parameter $\mathcal{M}_{g,(n)}$ is the reduction level, *and the parameter $\mathcal{I}_{g,(n)}$ is the* index of worst local reduction.

Remarks. The ratio $\underline{r}_{j,(n)}$ is closely related to the ratio r_i defined in Section 3.1 [see Equation (14)]. There are two differences : The rôle of the ambient dimension n is made apparent, and the indices i and j are related via $\underline{r}_j := r_{n-j}$. The rôle of this "time inversion" will be explained later. The variable $\mathcal{M}_{g,(n)}$ is the supremum of the set of those $1/s^2$ for which the basis $B_{n-g,(n)}$ is s–reduced in the Siegel sense. In other words $1/\mathcal{M}_{g,(n)}$ denotes the infimum of values of s^2 for which the basis $B_{n-g,(n)}$ is s–reduced in the Siegel sense. This variable is related to our initial problem, due to the equality

$$\pi_{n-g,(n),s} := \mathbb{P}[B_{n-g,(n)} \text{is } s\text{–reduced}] = \mathbb{P}[\mathcal{M}_{g,(n)} \geq \frac{1}{s^2}],$$

and we wish to evaluate the limit distribution (if it exists) of $\mathcal{M}_{g,(n)}$ when $n \to \infty$. The second variable $\mathcal{I}_{g,(n)}$ denotes the smallest index j for which the Siegel condition relative to the index $n-j$ is the weakest. Then $n - \mathcal{I}_{g,(n)}$ denotes the largest index i for which the Siegel condition relative to index i is the weakest. This index indicates where the limitation of the reduction comes from.

When the system $B_{p,(n)}$ is chosen at random, the Siegel ratios, the reduction level and the index of worst local reduction are random variables, well–defined whenever $B_{p,(n)}$ is a linearly independent system. We wish to study the asymptotic behaviour of these random variables (with respect to the dimension n of the ambient space), when the system $B_{p,(n)}$ is distributed under a so-called (concentrated) spherical model, where the radial distribution $\rho_{(n)}$ fulfills the following *Concentration Property* $\mathcal{C}$.

Concentration Property $\mathcal{C}$. *There exist a sequence $(a_n)_n$ and constants $d_1, d_2, \alpha > 0$, $\theta_0 \in (0,1)$ such that, for every n and $\theta \in (0, \theta_0)$, the distribution function $\rho_{(n)}$ satisfies*

$$\rho_{(n)}\left(a_n(1+\theta)\right) - \rho_{(n)}\left(a_n(1-\theta)\right) \geq 1 - d_1 e^{-n d_2 \theta^{\alpha}}. \tag{21}$$

In this case, it is possible to transfer results concerning the uniform distribution on $\mathbb{S}_{(n)}$ [where the radial distribution is Dirac] to more general spherical distributions, provided that the radial distribution be concentrated enough. This *Concentration Property* $\mathcal{C}$ holds in the three main instances previously described of simple spherical distributions.

We first recall some definitions of probability theory, and define some notations :

A sequence (X_n) of real random variables converges in distribution towards the real random variable X iff the distribution function F_n of X_n is pointwise convergent to the distribution function F of X on the set of continuity points of F. A sequence (X_n) of real random variables converges in

probability to a constant a if, for any $\epsilon > 0$, the sequence $\mathbb{P}[|X_n - a| > \epsilon]$ tends to 0. The two situations are respectively denoted as

$$X_n \xrightarrow[n]{(d)} X, \qquad\qquad X_n \xrightarrow[n]{proba.} a.$$

We now state the main results of this section, and provide some hints for the proof.

Theorem 5.2. (Akhavi, Marckert, Rouault [3] 2005) *Let $B_{p,(n)}$ be a random basis with codimension $g := n - p$ under a concentrated spherical model. Let $s > 1$ be a real parameter, and suppose that the dimension n of the ambient space tends to ∞.*
(i) If $g := n - p$ tends to infinity, then the probability $\pi_{p,(n),s}$ that $B_{p,(n)}$ is already s–reduced tends to 1.
(ii) If $g := n-p$ is constant, then the probability $\pi_{p,(n),s}$ that $B_{p,(n)}$ is already s–reduced converges to a constant in $(0, 1)$ (depending on s and g). Furthermore, the index of worst local reduction $\mathcal{I}_{g,(n)}$ converges in distribution.

5.2. **The irruption of β and γ laws.** When dealing with the Gram-Schmidt orthogonalization process, beta and gamma distributions are encountered in an extensive way. We begin to study the variables $Y_{j,(n)}$ defined as

$$Y_{j,(n)} := \frac{\ell^2_{j,(n)}}{|b_{j,(n)}|^2} \qquad \text{for } j \in [2..n].$$

and we show that they admit beta distributions.

Proposition 5.3. (Akhavi, Marckert, Rouault [3] 2005) (i) *Under any spherical model, the variables $\ell^2_{j,(n)}$ are independent.*
Moreover, the variable $Y_{j,(n)}$ follows the beta distribution $\beta((n-j+1)/2, (j-1)/2)$, for $j \in [2..n]$, and the set $\{Y_{j,(n)}, |b_{k,(n)}|^2;\ \ (j,k) \in [2..n] \times [1..n]\}$ is formed with independent variables.
(ii) *Under the random ball model $\mathbb{U}_n$, the variable $\ell^2_{j,(n)}$ follows the beta distribution $\beta((n-j+1)/2, (j+1)/2)$*

Proposition 5.3 is now used for showing that, under a concentrated spherical model, the beta and gamma distributions will play a central rôle in the analysis of the main parameters of interest introduced in Definition 5.1.
Denote by $(\eta_i)_{i\geq 1}$ a sequence of independent random variables where η_i follows a Gamma distribution $\gamma(i/2)$ and consider, for $k \geq 1$, the following random variables

$$\mathcal{R}_k = \eta_k/\eta_{k+1}, \qquad \mathcal{M}_k = \min\{\mathcal{R}_j;\quad j \geq k+1\}, \qquad \mathcal{I}_k = \min\{j \geq k+1;\quad \mathcal{R}_j = \mathcal{M}_k\}.$$

We will show in the sequel that they intervene as the limits of variables (of the same name) defined in Definition 5.1. There are different arguments in the proof of this fact.

(a) Remark first that, for the indices of the form $n - i$ with i fixed, the variable $\underline{r}^2_{n-i,(n)}$ tends to 1 when $n \to \infty$. It is then convenient to extend the tuple $(\underline{r}_{j,(n)})$ (only defined for $j \leq n-1$) into an infinite sequence by setting $\underline{r}_{k,(n)} := 1$ for any $k \geq n$.

(b) Second, the convergence

$$\mathcal{R}_j \xrightarrow[j]{a.s.} 1, \qquad\qquad \sqrt{k}(\mathcal{R}_k - 1) \xrightarrow[k]{(d)} \mathcal{N}(0, 4),$$

leads to consider the sequence $(\mathcal{R}_k - 1)_{k\geq 1}$ as an element of the space $\mathcal{L}_q$, for $q > 2$. We recall that

$$\mathcal{L}_q := \{x, \|x\|_q < +\infty\}, \qquad \text{with} \quad \|x\|_q := \big(\sum_{i\geq 1} |x_i|^q\big)^{1/q}, \qquad \text{for} \quad x = (x_i)_{i\geq 1}.$$

(c) Finally, classical results about independent gamma and beta distributed random variables, together with the weak law of large numbers and previous Proposition 5.3, prove that

$$\text{For each } j \geq 1, \quad \underline{r}^2_{j,(n)} \xrightarrow[n]{(d)} \mathcal{R}_j. \tag{22}$$

This suggests that the minimum $\mathcal{M}_{g,(n)}$ is reached by the $\underline{r}^2_{j,(n)}$ corresponding to smallest indices j and motivates the "time inversion" done in Definition 3.1.

5.3. **The limit process.** It is then possible to prove that the processes $R_{(n)} := (\underline{r}_{k,(n)} - 1)_{k\geq 1}$ converge (in distribution) to the process $R := (\mathcal{R}_k - 1)_{k\geq 1}$ inside the space $\mathcal{L}_q$, when the dimension n of the ambient space tends to ∞. Since $\mathcal{M}_{g,(n)}$ and $\mathcal{I}_{g,(n)}$ are continuous functionals of the process $R_{(n)}$, they also converge in distribution respectively to $\mathcal{M}_g$ and $\mathcal{I}_g$.

Theorem 5.4. (Akhavi, Marckert, Rouault [3] 2005) *For any concentrated spherical distribution, the following holds :*

(i) The convergence $(\underline{r}^2_{k,(n)} - 1)_{k\geq 1} \xrightarrow[n]{(d)} (\mathcal{R}_k - 1)_{k\geq 1}$ *holds in any space* $\mathcal{L}_q$, *with* $q > 2$.

(ii) For any fixed k, *one has :* $\mathcal{M}_{k,(n)} \xrightarrow[n]{(d)} \mathcal{M}_k, \qquad \mathcal{I}_{k,(n)} \xrightarrow[n]{(d)} \mathcal{I}_k$.

(iii) For any sequence $n \mapsto g(n)$ *with* $g(n) \leq n$ *and* $g(n) \to \infty$, *one has :* $\mathcal{M}_{g(n),(n)} \xrightarrow[n]{proba.} 1$.

This result solves our problem and proves Theorem 5.2. We now give some precisions on the limit processes $\sqrt{\mathcal{R}_k}, \sqrt{\mathcal{M}_k}$, and describe some properties of the distribution function F_k of $\sqrt{\mathcal{M}_k}$, which is of particular interest, due to the equality $\lim_{n\to\infty} \pi_{n-k,(n),s} = 1 - F_k(1/s)$.

Proposition 5.5. (Akhavi, Marckert, Rouault [3] 2005) *The limit processes* $\sqrt{\mathcal{R}_k}, \sqrt{\mathcal{M}_k}$ *admit densities which satisfy the following :*
(i) For each k, *the density* φ_k *of* $\sqrt{\mathcal{R}_k}$ *is*

$$\varphi_k(x) = 2B\left(\frac{k}{2}, \frac{k+1}{2}\right) \frac{x^{k-1}}{(1+x^2)^{k+(1/2)}}\, \mathbf{1}_{[0,\infty[}(x), \qquad \text{with} \quad B(a,b) := \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)}. \tag{23}$$

(ii) For each k, *the random variables* $\sqrt{\mathcal{M}_k}, \mathcal{M}_k$ *have densities, which are positive on* $(0,1)$ *and zero outside. The distribution functions* F_k, G_k *satisfy for* x *near* 0, *and for each* k,

$$\Gamma\left(\frac{k+2}{2}\right) F_k(x) \sim x^{k+1}, \qquad G_k(x) = F_k(\sqrt{x}).$$

There exists τ *such that, for each* k, *and for* $x \in [0,1]$ *satisfying* $|x^2 - 1| \leq (1/\sqrt{k})$

$$0 \leq 1 - F_k(x) \leq \exp\left[-\left(\frac{\tau}{1-x^2}\right)^2\right].$$

(iii) For each k, *the cardinality of the set* $\{j \geq k+1; \quad \mathcal{R}_j = \mathcal{M}_k\}$ *is almost surely equal to 1.*

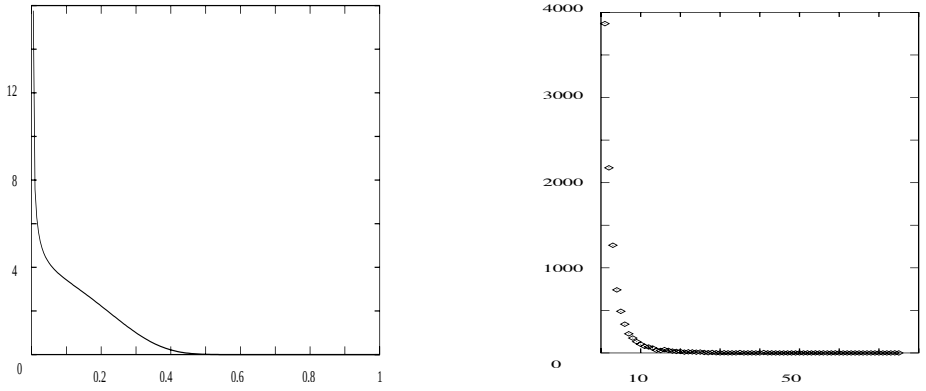

FIG. 7. On the left : simulation of the density of $\mathcal{M}_0$ with 10^8 experiments.–On the right : the histogram of $\mathcal{I}_0$ provided by 10^4 simulations. For any g, the sequence $k \mapsto \mathcal{P}[\mathcal{I}_g = k]$ seems to be rapidly decreasing

In particular, for a full–dimensional lattice

$$\lim_{n\to\infty} \pi_{n,(n),s} \sim_{s\to\infty} 1 - \frac{1}{s}, \qquad \lim_{n\to\infty} \pi_{n,(n),s} \leq \exp\left[-\left(\frac{\tau s^2}{s^2-1}\right)^2\right] \qquad \text{when } s \to 1$$

Figure 7 shows some experiments in the case of a full–dimensional lattice ($g = 0$). In this case, the density g_0 of $\mathcal{M}_0$ is proven to be $\Theta(1/\sqrt{x})$ when $x \to 0$ and tends rapidly to 0 when $x \to 1$. Moreover, the same figure shows that the worst reduction level for a full–dimensional lattice is almost always very small : that means that the first index i where the test in step 2. of the LLL algorithm (see Section 3.1) is negative is very close to n.

These (probabilistic) methods do not provide any information about the speed of convergence of $\pi_{n-g,(n)}$ towards 1 when n and g tend to ∞. In the case of the random ball model, Akhavi directly deals with the beta law of the variables ℓ_i and observes that

$$1 - \pi_{p,(n),s} \leq \sum_{i=1}^{p-1} \mathbb{P}[\ell_{i+1} \leq \frac{1}{s}\ell_i] \leq \sum_{i=1}^{p-1} \mathbb{P}[\ell_{i+1} \leq \frac{1}{s}] \leq \sum_{i=1}^{p-1} \exp\left[\frac{n}{2} H(\frac{i}{n})\right] \left(\frac{1}{s}\right)^{n-i},$$

where H is the entropy function defined as $H(x) = -x \log x - (1-x)\log(1-x)$, for $x \in [0,1]$, which satisfies $0 \leq H(x) \leq \log 2$. This proves :

Proposition 5.6. (Akhavi [2] 2000) *Under the random ball model, the probability that a basis $B_{p,(n)}$ be reduced satisfies, for any n, for any $p \leq n$, for any $s > 1$,*

$$1 - \pi_{p,(n),s} \leq \frac{1}{s-1}\ (\sqrt{2})^n \left(\frac{1}{s}\right)^{n-p}.$$

In particular, for any $s > \sqrt{2}$, the probability that $B_{cn,(n)}$ be s–reduced tends exponentially to 1, provided $1 - c$ is larger than $1/(2 \lg s)$.

5.4. **A first probabilistic analysis of the LLL algorithm.** In the case of the random ball model, Daudé and Vallée directly deal with the beta law of the variables ℓ_i and obtain estimates for the average number of iterations K and the first minimum $\lambda(\mathcal{L})$. They consider the case of the full dimensional lattices, namely the case when $p = n$. However, their proof can be extended to the case of a basis $B_{p,(n)}$ in the random ball model with $p \leq n$.

Using properties of the beta function, they first obtain a simple estimate for the distribution for the parameter ℓ_i,

$$\mathbb{P}[\ell_i \leq u] \leq (u\sqrt{n})^{n-i+1}$$

and deduce that the random variable $a := \min \ell_i$ satisfies

$$\mathbb{P}[a \leq u] \leq \sum_{i=1}^{p} \mathbb{P}[\ell_i \leq u] \leq (2\sqrt{n})u^{n-p+1}, \qquad \mathbb{E}\left[\log\left(\frac{1}{a}\right)\right] \leq \frac{1}{n-p+1}\left[\frac{1}{2}\log n + 2\right].$$

The result then follows from (16) and (20). It shows that, as previously, there are two regimes according to the dimension p of the basis relative to the dimension n of the ambient space.

Theorem 5.7. (Daudé and Vallée [14] 1994) *Under the random ball model, the number of iterations K of the LLL algorithm on $B_{p,(n)}$ has a mean value satisfying*

$$\mathbb{E}_{p,(n)}[K] \leq p - 1 + \frac{p(p-1)}{n-p+1}\left(\frac{1}{\log t}\right)\left[\frac{1}{2}\log n + 2\right],$$

Furthermore, the first minimum of the lattice generated by $B_{p,(n)}$ satisfies

$$\mathbb{E}_{p,(n)}[\lambda(\mathcal{L})] \geq \frac{n-p+1}{n-p+2}\left(\frac{1}{2\sqrt{n}}\right)^{1/(n-p+1)}$$

In the case when $p = cn$, with $c < 1$,

$$\mathbb{E}_{cn,(n)}[K] \leq \frac{cn}{1-c}\left(\frac{1}{\log t}\right)\left[\frac{1}{2}\log n + 2\right], \qquad \mathbb{E}_{cn,(n)}[\lambda(\mathcal{L})] \geq \exp\left[\frac{1}{2(1-c)n}\log\frac{1}{4n}\right].$$

5.5. **Conclusion of the probabilistic study in the spherical model.** In the spherical model, and when the ambient dimension n tends to ∞, all the local bases (except perhaps the "last" ones) are s–Siegel reduced. For the last ones, at indices $i := n-k$, for fixed k, the distribution of the ratio r_i admits a density φ_k which is given by Proposition 5.5. Both when $x \to 0$ and when $x \to \infty$, the density φ_k has a behaviour of power type, $\varphi_k(x) = \Theta(x^{k-1})$ for $x \to 0$, and $\varphi_k(x) = \Theta(x^{-k-2})$ for $x \to \infty$. It is clear that the potential degree of reduction of the local basis of index k is decreasing when k is decreasing. It will be interesting in the sequel to consider local bases with an initial density of this power type. However, the exponent of the density and the index of the local basis may be chosen independent, and the exponent is no longer integer. This type of choice provides a class of input local bases with different potential degree of reduction and leads to the so–called model "with valuation" which will be introduced in the two dimensional–case in Section 6.8 and studied in Sections 7 and 8.

6. Returning to the Gauss Algorithm.

We return to the two–dimensional case, and describe a complex version for each of the two versions of the Gauss algorithm. 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.

6.1. **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 2.1 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

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

6.2. **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

$$U(z) = -\frac{1}{z} + \left\lfloor \Re\left(\frac{1}{z}\right)\right\rceil = -\left(\frac{1}{z} - \left\lfloor \Re\left(\frac{1}{z}\right)\right\rceil\right) \tag{24}$$

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

$$\mathcal{F} = \left\{ z \in \mathbb{H}; \quad |z| \geq 1, \quad |\Re(z)| \leq \frac{1}{2} \right\}, \qquad \mathcal{F}_+ := \mathcal{F} \cap \mathbb{H}_+, \quad \mathcal{F}_- := \mathcal{F} \cap \mathbb{H}_-. \tag{25}$$

Such a domain, represented in Figure 8, is familiar from the theory of modular forms or the reduction theory of quadratic forms [29].

Consider the pair $(\mathcal{B}, U)$ where the map $U : \mathcal{B} \to \mathcal{B}$ is defined in (24) 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 $PSL_2(\mathbb{Z})$[3], 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 $\mathcal{F}$.

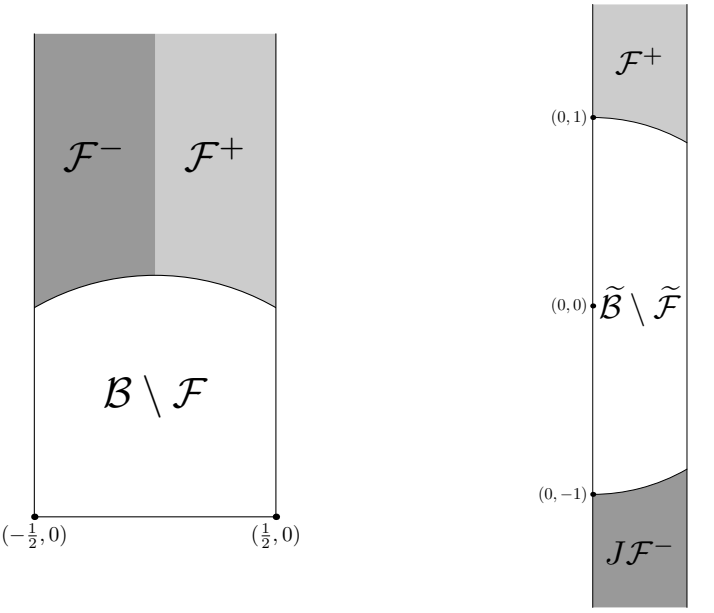

Fig. 8. The fundamental domains $\mathcal{F}, \widetilde{\mathcal{F}}$ and the strips $\mathcal{B}, \widetilde{\mathcal{B}}$ (see Section 6.2).

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

$$\widetilde{U}(z) = \epsilon\left(\frac{1}{z}\right)\left(\frac{1}{z} - \left\lfloor \Re\left(\frac{1}{z}\right)\right\rceil\right) \qquad \text{with} \quad \epsilon(z) := \operatorname{sign}(\Re(z) - \lfloor \Re(z) \rceil), \tag{26}$$

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

$$\widetilde{\mathcal{F}} = \left\{ z \in \mathbb{C}; \quad |z| \geq 1 \; 0 \leq \Re(z) \leq \frac{1}{2} \right\} = \mathcal{F}_+ \cup J\mathcal{F}_-. \tag{27}$$

Consider the pair $(\widetilde{\mathcal{B}}, \widetilde{U})$ where the map $\widetilde{U} : \widetilde{\mathcal{B}} \to \widetilde{\mathcal{B}}$ is defined in (26) 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]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 $ad - bc = 1$.

6.3. **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 :
– for the PGauss algorithm, it is related to the Euclidean division of the form $v = qu + r$ with $|r| \in [0, +u/2]$
– for the AGauss algorithm, it is based on the Euclidean division of the form $v = qu + \epsilon r$ with $\epsilon := \pm 1, r \in [0, +u/2]$.
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 $\mathcal{I} := [-1/2, +1/2]$ and $\widetilde{\mathcal{I}} := [0, 1/2]$, the maps $V : \mathcal{I} \to \mathcal{I}$ or $\widetilde{V} : \widetilde{\mathcal{I}} \to \widetilde{\mathcal{I}}$ are defined as follows

$$V(x) := \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rceil, \quad \text{for } x \neq 0, \qquad V(0) = 0, \tag{28}$$

$$\widetilde{V}(x) = \epsilon \left(\frac{1}{x}\right) \left(\frac{1}{x} - \left\lfloor \frac{1}{x} \right\rceil\right), \quad \text{for } x \neq 0, \qquad \widetilde{V}(0) = 0. \tag{29}$$

[Here, $\epsilon(x) := \text{sign}(x - \lfloor x \rceil)$]. This leads to two (real) dynamical systems $(\mathcal{I}, V)$ and $(\widetilde{\mathcal{I}}, \widetilde{V})$ whose graphs are represented in Figure 9. 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 [6]. The first system is called the F-Euclid system (or algorithm), whereas the second one is called the U-Euclid system (or algorithm).

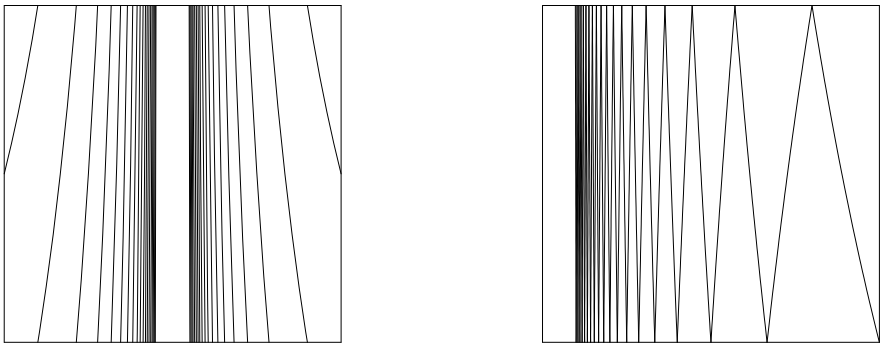

Fig. 9. The two dynamical systems underlying the centered Euclidean algorithms

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 $(\mathcal{I}, -V)$ and $(\widetilde{\mathcal{I}}, \widetilde{V})$ 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 $i\infty$.

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

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

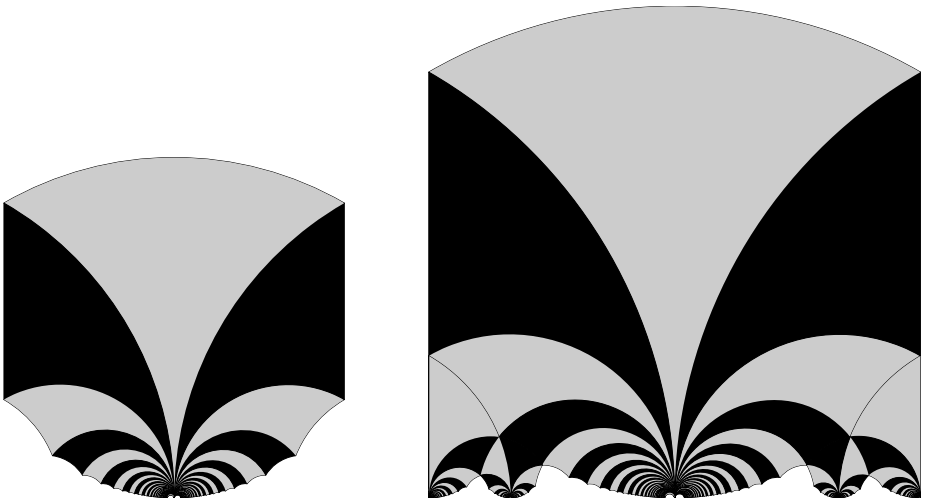

FIG. 10. On the left, the "central" festoon $\mathcal{F}_{(0,1)}$. On the right, three festoons of the strip $\mathcal{B}$, relative to $(0,1),(1,3),(-1,3)$ and the two half-festoons at $(-1,2)$ and $(1,2)$.

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

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

Proposition 6.1. (Folklore) *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

$$\mathcal{C} := \{(a,c); \quad \frac{a}{c} \in [-1/2, +1/2],\ c \geq 1; \gcd(a,c) = 1\}, \tag{30}$$

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 $|b_0| \leq |a/2|, |d_0| \leq |c/2|$.

Definition 6.1. [Festoons] *If $\mathcal{G}_{(a,c)}$ denotes the set of LFT's of $\mathcal{G}$ which admit (a,c) as coefficients, the domain*

$$\mathcal{F}_{(a,c)} = \bigcup_{h \in \mathcal{G}_{(a,c)}} h(\mathcal{F}) = h_{(a,c)} \left(\bigcup_{q \in \mathbb{Z}} T^q \mathcal{F} \right) \tag{31}$$

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 10).

6.5. **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

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

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

$$z_0 = \cfrac{1}{m_1 + \cfrac{\epsilon_1}{m_2 + \cfrac{\epsilon_2}{\ddots \cfrac{}{m_p + \epsilon_p z_p}}}} = \widetilde{h}(z_p) \qquad \text{with} \quad \widetilde{h} := h_{\langle m_1,\epsilon_1\rangle} \circ h_{\langle m_2,\epsilon_2\rangle} \circ \dots h_{\langle m_p,\epsilon_p\rangle}.$$

More generally, the i-th complex number z_i satisfies

$$z_i = \widetilde{h}_i(z_p) \qquad \text{with} \quad \widetilde{h}_i := h_{\langle m_{i+1},\epsilon_{i+1}\rangle} \circ h_{\langle m_{i+2},\epsilon_{i+2}\rangle} \circ \dots h_{\langle m_p,\epsilon_p\rangle}. \tag{32}$$

We now explain the particular rôle which is played by the disk $\mathcal{D}$ of diameter $\widetilde{\mathcal{I}} = [0, 1/2]$. Figure 11 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

$$\widetilde{\mathcal{B}} \setminus \widetilde{\mathcal{D}} = \bigcup_{h\in\mathcal{K}} h(\widetilde{\mathcal{F}}) \qquad \text{with} \quad \mathcal{K} := \{I, S, STJ, ST, ST^2J, ST^2JS\}. \tag{33}$$

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 11).

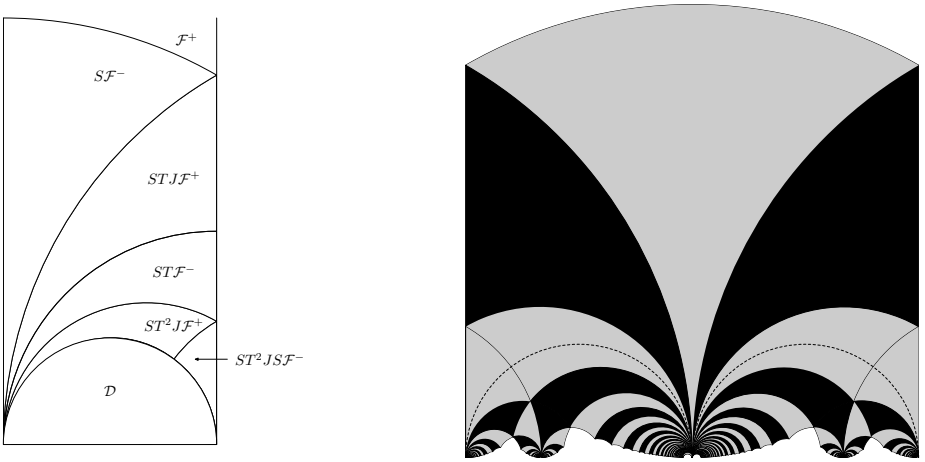

FIG. 11. On the left, the six domains which constitute the domain $\mathcal{B}_+ \setminus \mathcal{D}_+$. On the right, the disk $\mathcal{D}$ is not compatible with the geometry of transforms of the fundamental domains $\mathcal{F}$.

As Figure 12 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 $\mathcal{D}$ of diameter $[0, 1/2]$ whose alternative 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 $(m_i, \epsilon_i) \geq (2, +1)$ (wrt the lexicographic order), and the algorithm uses at each step the set

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

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

$$\mathcal{D} = \bigcup_{h\in\mathcal{H}^+} h(\widetilde{\mathcal{B}} \setminus \mathcal{D}) \qquad \text{with} \quad \mathcal{H}^+ := \sum_{k\geq 1} \mathcal{H}^k. \tag{34}$$

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 (33) and Figure 11), that constitutes the FinalGauss algorithm, which uses the set $\mathcal{K}$ of LFT's, called the final set of LFT's and described in (33). Finally, we have proven :

Proposition 6.2. (Daudé, Flajolet, Vallée [13, 15, 16] 1990–1999) *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*

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

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) ;

Fig. 12. The decomposition of the AGauss Algorithm.

6.6. **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 (29). 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 8 why it can be seen as an exact generalization of the F-Euclid algorithm.
For instance, if R denotes the number of iterations of the CoreGauss algorithm, 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

$$[R \geq k+1] = \bigcup_{h\in\mathcal{H}^k} h(\mathcal{D}), \tag{35}$$

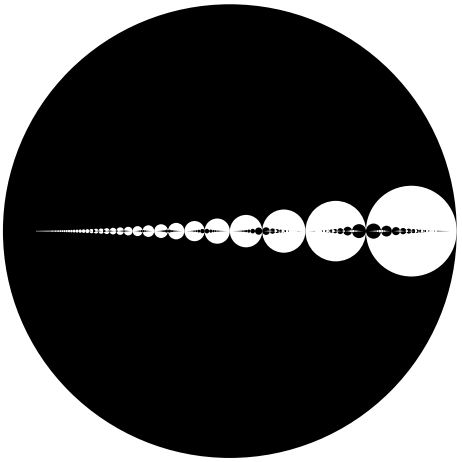

FIG. 13. The domains $[R = k]$ alternatively in black and white.

which is represented in Figure 11. The disk $h(\mathcal{D})$ for $h \in \mathcal{H}^+$ is the disk whose diameter is the interval $[h(0), h(1/2)] = h(\widetilde{\mathcal{I}})$. Inside the F-EUCLID dynamical system, the interval $h(\widetilde{\mathcal{I}})$ (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 $\widetilde{\mathcal{I}}$ 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 ? We return to these questions in Section 8.

6.7. **Worst-case analysis of the Gauss algorithm.** 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,

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

according to the considered algorithm (PGAUSS or AGAUSS). We begin by recalling the worst–case behaviour of execution parameters and give a proof in the complex framework.

Proposition 6.3. (Vallée [33] 1991) *On the set $\widetilde{\Omega}_M$, the maximum number of iterations P of the* AGAUSS *algorithm, and the maximum value of any additive cost C of moderate growth*[4] *are $\Theta(M)$. In particular, the maximal value B_M of the bit–complexity B on $\widetilde{\Omega}_M$ is $\Theta(M^2)$ and the maximal value P_M of the number of iterations P on $\widetilde{\Omega}_M$ satisfies*

$$P_M \sim \frac{1}{2} \frac{\log 2}{\log(1+\sqrt{2})} M.$$

Proof. We here use the complex framework of the AGAUSS algorithm, and the study of the maximum number of iterations is the complex version of Vallée's result, initially performed in the vectorial framework [33].

Number of iterations. It is sufficient to study the number R of iterations of the COREGAUSS Algorithm since it is related to the total number of iterations P via the inequality $P \leq R + 2$. The inclusion

$$[R \geq k+1] \subset \left\{ z; \quad |\Im(z)| \leq \frac{1}{2} \left(\frac{1}{1+\sqrt{2}} \right)^{2k-1} \right\} \tag{36}$$

[4]This means that the elementary cost c satisfies $c(q) = O(\log q)$ (see Section 2.3).

will lead to the result : since any non real complex $z = v/u$ relative to an integer pair (u, v) has an imaginary part at least equal to $1/|u|^2$, then z belongs to the domain $[R \leq k]$ as soon as $|u|^2 \leq 2(1+\sqrt{2})^{2k-1}$.
We now prove Relation (36) : Indeed, we know from (35) that the domain $[R \geq k+1]$ is the union of transforms $h(\mathcal{D})$ for $h \in \mathcal{H}^k$, where $\mathcal{D}$ and $\mathcal{H}$ are defined in Proposition 6.2. The largest such disk $h(\mathcal{D})$ is obtained when all the quotients (m, ϵ) are the smallest ones, i.e., when all $(m, \epsilon) = (2, +1)$. In this case, the coefficients (c, d) of h are the terms A_k, A_{k+1} of the sequence defined by $A_0 = 0, A_1 = 1$ and the recurrence $A_{k+1} = 2A_k + A_{k-1}$, which satisfy $A_k \geq (1+\sqrt{2})^{k-2}$. Then, the largest such disk has a radius at most equal to $(1/2)(1+\sqrt{2})^{1-2k}$.

Additive costs. Since we restrict ourselves to costs c of moderate growth, it is sufficient to study the cost C relative to the step cost $c(q) := \log q$.
Consider the sequence of vectors $w_0 = u, w_1 = v, \ldots, w_{k+1}$ computed by the AGauss algorithm on the input (u, v) with $M := \ell(|u|^2)$. We consider the last step as a special case, and we use for it the (trivial) upper bound $|m_{k+1}| \leq |u|^2$; for the other steps, we consider the associated complex numbers z_i defined by $z_{i-1} = h_i(z_i)$ [where the LFT h_i has a digit q_i at least equal to 2] and the complex $\check{z} := z_k$ before the last iteration which belongs to $\widetilde{\mathcal{B}} \setminus \widetilde{\mathcal{F}}$. Then the expression $z = z_0 = h(\check{z})$ involves the LFT $h := h_1 \circ h_2 \ldots \circ h_k$ which corresponds to the algorithm except its last step. Since any complex $z = v/u$ relative to an integer pair (u, v) has an imaginary part at least equal to $1/|u|^2$, one has

$$\frac{1}{|u|^2} \leq |\Im h(\check{z})| = |\Im(\check{z})| \cdot |h'(\check{z})| \leq \prod_{i=1}^{k} |h_i'(z_i)| \leq \prod_{i=1}^{k} \frac{1}{|q_i - (1/2)|^2} \leq 2^k \prod_{i=1}^{k} \frac{1}{q_i^2}.$$

This proves that the cost $C(u, v)$ relative to $c(q) = \log q$ satisfies $C(u, v) = O(M)$.

Bit-complexity. The result is obtained thanks to Eq. (8). ■

6.8. **Probabilistic models for two dimensions.** We now return to our initial motivation, and begin our probabilistic studies. 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 (as we already explained in Section 4.4), 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. In our asymptotic framework, where the size M becomes large, 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.

The model with "valuation". In Section 5, it is shown that each input local basis U_{n-k} in the spherical model with ambient dimension n admits (for $n \to \infty$) a distribution with a density φ_k defined in (23). 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 [34] 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

$$f(z) = |\Im(z)|^r \cdot g(z) \qquad \text{where} \quad g(z) \neq 0 \quad \text{for } \Im(z) = 0. \tag{37}$$

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

$$f_r(z) = \frac{1}{A(r)} |\Im(z)|^r \qquad \text{with} \quad A(r) = \iint_{\mathcal{B}\setminus\mathcal{F}} y^r \, dx dy. \tag{38}$$

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.

The Ajtai model in two dimensions. This model (described in the general case in Section 4.2) corresponds to bases (u, v) for which the determinant $\det(u, v)$ satisfies

$$\frac{|\det(u, v)|}{\max(|u|, |v|)^2} = y_0 \qquad \text{for some } y_0 \in]0, 1].$$

In the complex framework, this leads to densities $f(z)$ on $\mathcal{B} \setminus \mathcal{F}$ (or on the tilde corresponding domain) of the form $f(z) = \texttt{Dirac}(y_0)$ for some $y_0 \in]0, 1]$. When y_0 tends to 0, then the model also tends to the "one dimensional model" (where u and v are colinear) and the Gauss Algorithm also "tends" to the Euclidean Algorithm. As in the model "with valuation", it is important to precisely describe this transition and compare to the result of Goldstein and Mayer [20].

7. Analysis of lattice reduction in two dimensions : 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.

7.1. Output densities.

For studying the evolution of distributions (on complex numbers), we are led to study the LFT's h used in the Gauss algorithm [Section 6], whose set is $\mathcal{G}$ for the PGauss Algorithm [Section 6.4]. We 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 $(h, h) : (u, v) \mapsto (h(u), h(v))$ 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

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

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

$$J\underline{h}(x, y) = |h'(z) \cdot h'(\overline{z})| = |h'(z)|^2, \tag{39}$$

since h has real coefficients. Let us consider any measurable set $\mathcal{A} \subset \mathcal{F}$, and study the final density $\hat{f}$ on $\mathcal{A}$. It 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 (39), 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 7.1. (Vallée and Vera [39] 2007) (*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 6.1.*
(*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 6.2.*
(*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 each step of the CoreGauss *algorithm defined in Proposition 6.2. and $\mathcal{H}^+ := \cup_{k\geq 1}\mathcal{H}^k$.*

7.2. **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 (38). Since each element of $\mathcal{G}$ gives rise to a unique pair (c,d) with $c\geq 1, \gcd(c,d)=1$ [see Section 6.4] for which

$$|h'(\hat{z})| = \frac{1}{|c\hat{z}+d|^4}, \qquad f_r\circ \underline{h}(\hat{x},\hat{y}) = \frac{1}{A(r)}\, \frac{\hat{y}^r}{|c\hat{z}+d|^{2r}}, \tag{40}$$

$$\text{the output density on } \mathcal{F} \text{ is} \quad \hat{f}_r(\hat{x},\hat{y}) = \frac{1}{A(r)} \sum_{\substack{(c,d)=1\\ c\geq 1}} \frac{\hat{y}^r}{|c\hat{z}+d|^{4+2r}}\,. \tag{41}$$

It is natural to compare this density to the density relative to the measure relative to "random lattices" defined in Section 4.4. In the particular case of two dimensions, the set $X_2 = SL_2(\mathbb{R})/SL_2(\mathbb{Z})$ is exactly[5] the fundamental domain $\mathcal{F}$. Moreover, the measure of density $f(z) = \Im(z)^{-2}$ 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 defined in Section 4.4 is exactly the measure on $\mathcal{F}$ of density

$$\eta(x,y) := \frac{3}{\pi}\frac{1}{y^2} \qquad \text{since} \quad \iint_{\mathcal{F}} \frac{1}{y^2} dxdy = \frac{\pi}{3}. \tag{42}$$

If we make apparent this density η inside the expression of $\hat{f}_r$ provided in (41), we obtain :

Theorem 7.2. (Vallée and Vera [39] 2007) *When the initial density on $\mathcal{B}\setminus\mathcal{F}$ is the standard density of valuation r, denoted by f_r and defined in (38), the output density of the* PGauss *algorithm on $\mathcal{F}$ involves the Eisenstein series E_s of weight $s = 2+r$: With respect to the Haar measure ν_2 on $\mathcal{F}$, whose density η is defined in (42), the output density $\hat{f}_r$ is expressed as*

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

[5]Not exactly : up to a convenient definition of $\mathcal{F}$ on its frontier.

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

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

and the output distribution relative to the input distribution of valuation r tends to the distribution ν_2 relative to random lattices when r tends to -1.

The series E_s are Maass forms (see for instance the book [7]) : 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 is unexpected, and, at the moment, it is not clear how to use the (other) classical well-known properties of the Eisenstein series E_s for studying the output densities.

7.3. **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 7.3. *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*

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

The following inclusions hold :

$$[\lambda(z) = t] \subset \left[\Im(z) \geq \frac{\sqrt{3}}{2}t^2\right], \qquad [\mu(z) = u] \subset \left[\Im(z) \leq \frac{2}{\sqrt{3}}u^2\right]. \tag{43}$$

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 (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

$$\frac{|v_p|^2}{|v_0|^2} = \frac{|v_p|^2}{|cv_{p+1}+dv_p|^2} = \frac{1}{|c\hat{z}+d|^2} = |h'(\hat{z})|, \tag{44}$$

[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. ■

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

FIG. 14. The three main domains of interest : the Ford disks $\texttt{Fo}(a,c,\rho)$, the Farey disks $\texttt{Fa}(a,c,t)$, the angular sectors $\texttt{Se}(a,c,u)$.

7.4. **Domains relative to the output parameters.** We now consider the following well-known domains defined in Figure 14. The Ford disk $\texttt{Fo}(a,c,\rho)$ 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 $\texttt{Fa}(a,c,t)$ is a disk of center $(a/c,0)$ and radius t/c. Finally, the angular sector $\texttt{Se}(a,c,u)$ 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 7.4. (Laville, Vallée, Vera, [22, 39] 1994–2007) *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 $\texttt{Fo}(a,c,\rho)$*, Farey disks* $\texttt{Fa}(a,c,t)$*, and angular sectors* $\texttt{Se}(a,c,u)$*. More precisely, if* $\mathcal{F}_{(a,c)}$ *denotes the Festoon relative to pair* (a,c) *defined in (31) and if the set* $\mathcal{C}$ *is defined as in (30), one has :*

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

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 15]. In the case of domain $\Lambda(t)$, this "global definition" is provided in [22], and for $M(u)$, it is provided in [39].

Define the subset $\mathcal{P}(t)$ of set $\mathcal{P}$ defined in Section 6.4 as

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

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 $\{(a/c)\le x\le(b/d)\}$.

The global definition of domain $\Lambda(t)$ is provided in [22] : 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

$$\Lambda(t)\cap\mathcal{S}(a/c,b/d) = \texttt{Fa}_+(a,c,t)\cup\texttt{Fa}_-(b,d,t)\cup\texttt{Fa}(a+b,c+d,t). \tag{45}$$

Here $\texttt{Fa}_+(a,c,t),\texttt{Fa}_-(b,d,t)$ are the half Farey disks formed with the intersections of $\texttt{Fa}(a,c,t)$, $\texttt{Fa}(b,d,t)$ with the strip $\mathcal{S}(a/c,b/d)$. The domain of (45) is exactly the union of the two disks $\texttt{Fa}_+(a,c,t)$ and $\texttt{Fa}_-(b,d,t)$ if and only if the condition $(c^2+d^2+cd)t^2\ge 1$ holds, but, the Farey disk relative to the median $(a+b)/(c+d)$ plays a rôle otherwise. This condition $(c^2+d^2+cd)t^2\le 1$ is satisfied in particular if $\max(ct,dt)$ is smaller than $1/\sqrt{3}$. This occurs in the interval $[a/c,b/d]$ when c,d both belong to the interval $[0,(1/\sqrt{3})(1/t)]$. When $t\to 0$, the proportion of pairs $(a/c,b/d)$ for which the intersection of Eqn (47) is formed with three disks tends to $1/6$.

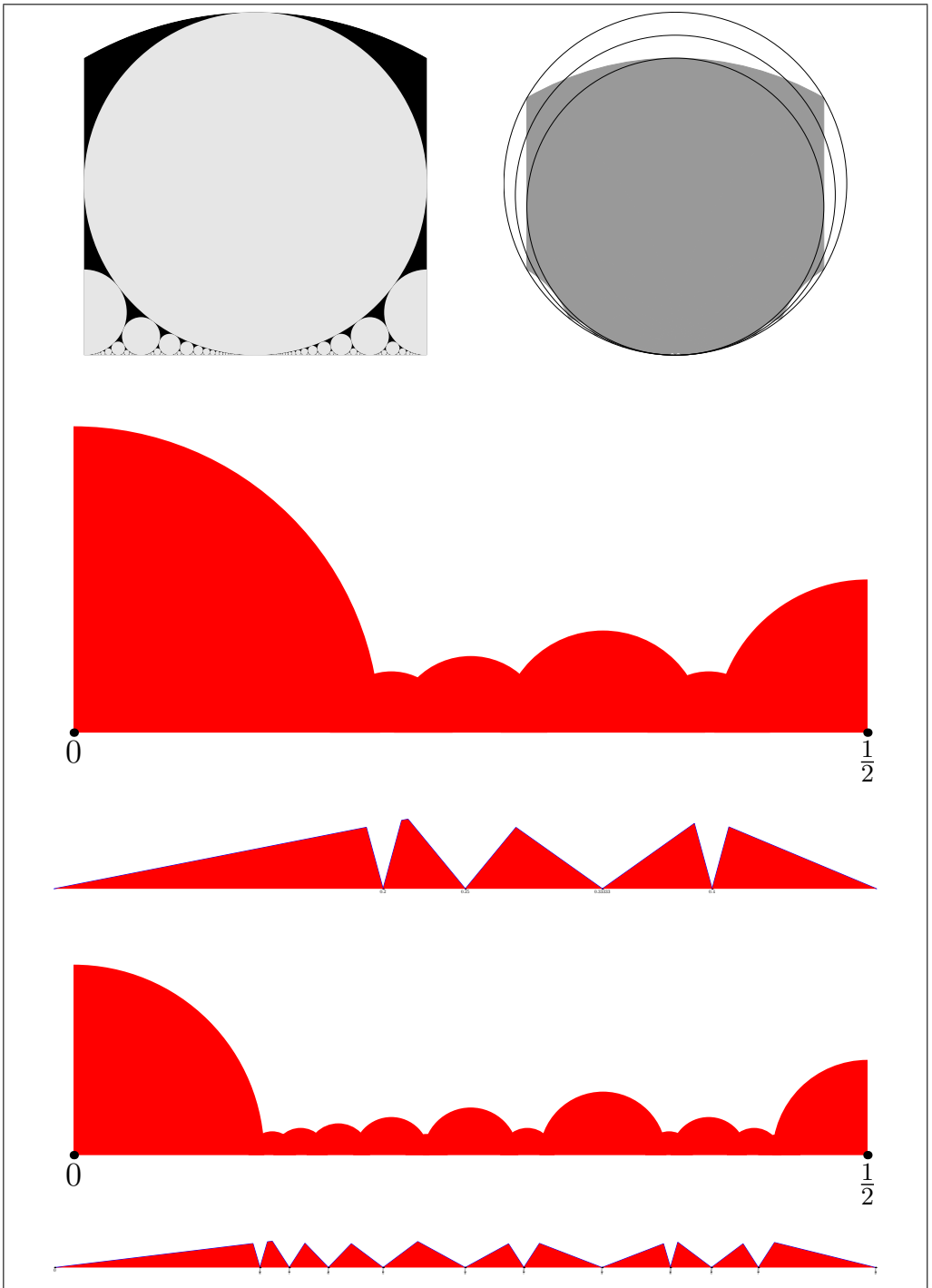

FIG. 15. On the top : the domain $\Gamma(\rho) := \{z; \quad \gamma(z) \leq \rho\}$. On the left, $\rho = 1$ (in white). On the right, the domain $\mathcal{F}_{(0,1)} \cap \mathtt{Fo}(0,1,\rho)$ for $\rho = 1, \rho_0 = 2/\sqrt{3}, \rho_1 = (1+\rho_0)/2$. – On the middle, the domain $\Lambda(t) \cap \mathcal{B}_+$, with $\Lambda(t) := \{z; \quad \lambda(z) \leq t\}$ and the domain $M(u) \cap \mathcal{B}_+$ with $M(u) := \{z; \quad \mu(z) \leq u\}$ for $u = t = 0.193$.– On the bottom, the same domains for $u = t = 0.12$.

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

$$\bigcup_{\substack{(a,c)\in\mathcal{C}\\ c\le 1/t}} \mathtt{Fa}(a,c,t) \subset \Lambda(t) \subset \bigcup_{\substack{(a,c)\in\mathcal{C}\\ c\le 2/(\sqrt{3}t)}} \mathtt{Fa}(a,c,t). \tag{46}$$

The global definition of domain $M(u)$ is provided in [39] : consider a pair $(a/c, b/d)$ of rationals satisfying $ad - bc = -1$ whose denominator pair (c, d) belongs to $\mathcal{P}(u)$. There exists a local characterization of $M(u) \cap \mathcal{S}(a/c, b/d)$ which does not depend any longer on the festoons, namely

$$M(u) \cap \mathcal{S}(a/c, b/d) = \mathtt{Se}(a, c, u) \cap \mathtt{Se}(b, d, u) \cap \mathtt{Se}(b - a, d - c, u). \tag{47}$$

The domain of (47) is exactly the triangle $\mathtt{Se}(a, c, u) \cap \mathtt{Se}(b, d, u)$ if and only if the condition $(c^2 + d^2 - cd)u^2 \le (3/4)$ holds, but, this is a "true" quadrilateral otherwise. This condition $(c^2 + d^2 - cd)u^2 \ge (3/4)$ is satisfied in particular if $\min(cu, du)$ is larger than $\sqrt{3}/2$. This occurs in the interval $[a/c, b/d]$ when c, d both belong to the interval $[(\sqrt{3}/2)(1/u), 1/u]$. When $u \to 0$, the proportion of pairs $(a/c, b/d)$ for which the intersection of Eqn (47) is a "true" quadrilateral tends to $2[1 - (\sqrt{3}/2)]^2$.

7.5. **Distribution functions of output parameters : case of densities with valuations.** 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 7.5. (Vallée and Vera [39] 2007) *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 :*

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

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

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

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

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

The constants $A_i(r)$ involve Euler's Gamma function and the measure $A(r)$ defined in (38) 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

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

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 (46) 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 (43) leads to the inequality. ■

Interpretation of the results. We provide a first interpretation of the main results described in Theorem 7.5.

(*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 7.2, 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 (42), which is associated to the Haar measure ν_2 defined in 4.4 and 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 describe the distribution function of parameter γ for $\rho > 1$? Figure 15 [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 Section 3.4.

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 9.1).

The corners of the fundamental domain. With Theorem 7.5, 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 4[right].

Proposition 7.6. *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*

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

where $A_1(r)$ is defined in Theorem 7.5. There are three main cases of interest for $1 - C(r)$, namely

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

7.6. **Distribution functions of output parameters : case of fixed determinant.** Computing the measure of disks and angular sectors with respect to the measure concentrated on the line $y = y_0$ leads to the estimates of the main output distributions. We here focus on the parameter γ.

The intersection of the disk $\mathtt{Fo}(a, c, \rho)$ with the line $y = y_0$ is non empty as soon as y_0 is less than ρ/c^2. The intersection $\Gamma(\rho) \cap [y = y_0]$ is just "brought" by the Ford disks for which the integer c is less than $x_0 = \sqrt{\rho/y_0}$. Then, for $\rho < 1$, the Ford disks $\mathtt{Fo}(a, c, \rho)$ are disjoint and

$$\mathbb{P}_{[y_0]}[\gamma(z) \leq \rho] = 2\rho\, S_g(x_0) \qquad \text{with} \quad S_g(x_0) = \frac{1}{x_0} \sum_{c \leq x_0} \frac{\varphi(c)}{c}\, g\left(\frac{c}{x_0}\right), \qquad \text{and} \quad g(t) = \sqrt{1 - t^2}.$$

For any function g smooth enough, one has

$$\lim_{x \to \infty} S_g(x) = \frac{1}{\zeta(2)} \int_0^1 g(t) dt,$$

This proves that when y_0 tends to 0, the probability $\mathbb{P}_{[y_0]}[\gamma(z) \leq \rho]$ tends to $(3/\pi)\rho$. We recover the result of [20] in the two–dimensional case.

7.7. **A related result which also deals with Farey disks.** For analyzing integer factoring algorithms, Vallée was led in 1988 to study the set

$$\mathcal{B} = \mathcal{B}(N, h, h') := \{x \in [1..N]; \quad x^2 \bmod N \in [h, h']\}, \qquad \text{for} \quad h' - h = 8N^{2/3},$$

and its distribution in $[1..N]$. She described in [38, 37] a polynomial–time algorithm, called the Two–Thirds Algorithm which draws elements from $\mathcal{B}$ in a quasi–uniform way[6]. This was (for her) a main tool for obtaining a *provable* complexity bound for integer factoring algorithms based on congruences of squares. Fifteen years later, Coron in [12], then Gentry in [19] discovered that such an algorithm also plays a central rôle in cryptography, more precisely in security proofs (see the survey of Gentry [18] in these proceedings). Furthermore, Gentry in [19] modified Vallée's algorithm and obtained an algorithm which draws elements from $\mathcal{B}$ in an exact uniform way. This constitutes a main step in the security proof of Rabin partial-domain-hash signatures.

The main idea of Vallée, which has been later adapted by Gentry, is to perform a local study of the set $\mathcal{B}$. In this way, she refines ideas of the work done in [40]. This last work is one of the first works which relates general small modular equations to lattices, and will be further generalized ten years later by Coppersmith [10]. Consider an integer x_0, for which the rational $2x_0/N$ is close to a rational a/c with a small denominator c. Then, the set of elements of $\mathcal{B}$ near x_0 can be easily described with the help of the lattice $\underline{L}(x_0)$ generated by the pair of vectors $(2x_0, 1), (N, 0)$. More precisely, the two conditions are equivalent

(i) $x = x_0 + u$ belongs to $\mathcal{B}$

(ii) There exists w such that the point (w, u) belongs to $\underline{L}(x_0)$ and lies between two parabolas with respective equations

$$w + u^2 + x_0^2 = h, \qquad w + u^2 + x_0^2 = h'.$$

[6] We use the term quasi–uniform to mean that the probability that $x \in \mathcal{B}$ is drawn is between $\ell_1/|\mathcal{B}|$ and $\ell_2/|\mathcal{B}|$, for constants independent on x and N.

This equivalence is easy to obtain (just expand x^2 as $(x_0+u)^2 = x_0^2 + 2x_0u + u^2$) and gives rise to an efficient drawing algorithm of $\mathcal{B}$ near x_0, *provided that* the lattice $\underline{L}(x_0)$ has a sufficiently short vector in comparison to the gap $h' - h$ between the two parabolas. Vallée proved that this happens when the complex $z_0 = 2x_0/N + i/N$ relative to the input basis of $\underline{L}(x_0)$ belongs to a Farey disk $\mathtt{Fa}(a, c, t)$ with $t = (h' - h)/N = 4N^{-1/3}$. In 1988, the rôle played by Farey disks (or Farey intervals) was surprising, but, now, from previous studies performed in Sections 7.4 and 7.5, we know that these objects are central in such a result.

8. Analysis of the execution parameters of the Gauss Algorithm.

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 based on tools that come both from dynamical system theory and analysis of algorithms. We shall use here the AGauss algorithm, with the decomposition provided in Proposition 6.2.

8.1. **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 of class $\mathcal{C}^2$ 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 $t = 0$, $t = 1$, $t = 2$, ...

We will study here two dynamical systems, respectively related to the F-Euclid algorithm and to CoreGauss algorithm, and defined in Section 6.

8.2. **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 $\mathbf{X}_{s,[h]}$, relative to a mapping h, which acts on functions f of one variable, depends on some parameter s and is formally defined as

$$\mathbf{X}_{s,[h]}[f](x) = |h'(x)|^s \cdot f \circ h(x). \tag{48}$$

The operator $\mathbf{X}_{1,[h]}$ expresses the part of the new density which is brought when the algorithm uses the branch h, and the operator which takes into account all the inverse branches of the set $\mathcal{H}$, defined as

$$\mathbf{H}_s := \sum_{h\in\mathcal{H}} \mathbf{H}_{s,[h]}, \tag{49}$$

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 [see Section 6.3], due to the precise expression of the set $\mathcal{H}$, one has, for any $x \in \widetilde{\mathcal{I}} = [0, 1/2]$

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

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 8.4.

8.3. **Case of the** AGauss **algorithm.** Theorem 7.1 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 Section 7.1 that the Jacobian of the transformation $(x,y) \mapsto \underline{h}(x,y) = (\Re h(x+iy), \Im h(x+iy))$ 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 $\mathbf{Y}_{s,[h]}$, of the form

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

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 does not possess "good" properties, because the modulus $|h'(z)|$ does not define an analytic function of variable z. 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 $\widetilde{\mathcal{I}} := [0, 1/2]$. Such an operator acts on analytic functions, and the equalities

$$\underline{\mathbf{X}}_{s,[h]}[F](z,\overline{z}) = \mathbf{Y}_{s,[h]}[f](z), \quad \underline{\mathbf{X}}_{s,[h]}[F](x,x) = \mathbf{X}_{s,[h]}[f](x) \quad \text{for} \quad f(z) := F(z,\overline{z}), \tag{50}$$

prove that the elementary operators $\underline{\mathbf{X}}_{s,[h]}$ are extensions of the operators $\mathbf{X}_{s,[h]}$ 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 $f(z) = F(z,\overline{z})$, 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

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

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 6.2, defined as

$$\underline{\mathbf{H}}_s := \sum_{h\in\mathcal{H}} \underline{\mathbf{X}}_{s,[h]}, \qquad \mathbf{K}_s := \sum_{h\in\mathcal{K}} \underline{\mathbf{X}}_{s,[h]} \qquad \mathbf{G}_s := \sum_{h\in\widetilde{\mathcal{G}}} \underline{\mathbf{X}}_{s,[h]}, \tag{51}$$

satisfy with Proposition 6.2,

$$\mathbf{G}_s = \mathbf{K}_s \circ (I - \underline{\mathbf{H}}_s)^{-1} - I \tag{52}$$

Remark that the operator $\underline{\mathbf{H}}_s$ admits a nice expression

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

Due to (50), this is an extension of the operator $\mathbf{H}_s$, defined in (49), which satisfies relation $\underline{\mathbf{H}}_s[F](x,x) = \mathbf{H}_s[f](x)$ when f is the diagonal map of F. Furthermore, assertions (ii) and (iii) of Theorem 7.1 can be re–written as :

Theorem 7.1 [Dynamical version] *Consider the densities (the input density f and the output density $\hat{f}$) as functions of two complex variables $z, \overline{z}$, namely $f(x,y) = F(z,\overline{z})$, $\hat{f}(x,y) = \hat{F}(z,\overline{z})$. Then*

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

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 (51) 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 $\mathbf{X}_{s,[h]}$ in analysis of algorithms ; for this aim, we modify them in such a way that they become "generating operators" that generate themselves generating functions related to algorithms. 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

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

entails, with Proposition 6.2, an extension of (52) as

$$\mathbf{G}_{s,w,(c)} = \mathbf{K}_{s,w,(c)} \circ (I - \underline{\mathbf{H}}_{s,w,(c)})^{-1} - I, \tag{53}$$

when the operators $\mathbf{G}_{s,w,(c)}, \mathbf{K}_{s,w,(c)}, \underline{\mathbf{H}}_{s,w,(c)}$ are defined in the same vein as in (51).

8.4. **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 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 [35], [8]), 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 $\lambda_{(c)}(s, w_{(c)}(s)) = 1$. More precisely, when $w = 0$, one has :

$$(I - \underline{\mathbf{H}}_s)^{-1}[F](z,u) = \frac{1}{s-1} \frac{6 \log \phi}{\pi^2} \underline{\psi}(z,u) \int_{\widetilde{\mathcal{I}}} F(x,x)dx, \tag{54}$$

where $\underline{\psi}(x)$ is an extension of the invariant density ψ of the F-Euclid Algorithm, and satisfies $\underline{\psi}(x,x) = \psi(x)$. An exact expression for $\underline{\psi}$ is provided in [35],

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

8.5. **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 $c(h_{\langle q,\epsilon\rangle}) := c(q)$, and 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 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[7] model relative to a density f of type (r, g) defined in (37), 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 (37), using a change of variables, the expression of the Jacobian, and relation (40) leads to

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

This expression involves the transfer operator $\mathbf{G}_{2+r,w,(c)}$ of the algorithm AGauss, and with (53),

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

The probability $\mathbb{P}[C_{(c)} = k]$ is obtained by extracting the coefficient of $\exp[kw]$ in the moment generating function. Then the asymptotic behaviour of $\mathbb{P}[C_{(c)} = k]$ is related to singularities of $\mathbb{E}_{\langle f\rangle}(\exp[wC_{(c)}])$. This series has a pôle at $e^{w_{r,(c)}}$ where $w = w_{r,(c)}$ is defined by the spectral equation $\lambda_{(c)}(2 + r, w) = 1$ 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 8.1. (Daudé, Flajolet, Vallée, Vera, [13, 39] 1994–2007) *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*

$$\mathbb{P}_{\langle f\rangle}[C_{(c)} = k] \sim a(r) \exp[-kw_{r,(c)}], \qquad \text{for } k \to \infty, \tag{55}$$

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

In the particular case of a constant step-cost $c = 1$, the operator $\underline{\mathbf{H}}_{s,w,(1)}$ reduces to $e^w \cdot \underline{\mathbf{H}}_s$, and the ratio $w_{r,(1)}$ in (55) is just equal to $\lambda(2 + r)$.

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 6.2). Furthermore, the probability of the event $[R \geq k + 1]$ can be expressed in an easier way using (35), as

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

[7] It is also possible to transfer this continuous model to the discrete one with principles described in Section 4.4. This is done for instance in [13], but this will not be done here.

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

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

$$A_4(r) = \frac{\sqrt{\pi}}{4^{r+2}} \frac{\Gamma((r+1)/2)}{\Gamma(r/2+2)}. \tag{56}$$

This leads to the following result :

Theorem 8.2. (Daudé, Flajolet, Vallée, [13, 35] 1994–1996) *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*

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

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 [24]. In [16], numerical values are computed in the case of the uniform density, i.e., for $\lambda(2)$ and $\mathbb{E}_{(0)}[R]$,

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

For $r \to -1$, the dominant eigenvalue $\lambda(2+r)$ tends to $\lambda(1) = 1$ and $\lambda(2+r) - 1 \sim \lambda'(1)(1+r)$. This explains the evolution of the behaviour of the Gauss Algorithm when the data become more and more concentrated near the real axis.

8.6. **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 (44), the i-th length decrease can be expressed with the derivative of the LFT h_i defined in (32), 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 8.3. 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 $W := W_{(\ell)}$, we obtain the operator

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

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

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

which is the "generating operator" of the cost $D(z)$. These functionals W, Δ are also central in the analysis of the bit–complexity of the Euclid Algorithm [25], [4].

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

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

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

and involve the measure $A_4(r)$ of disk $\mathcal{D}$ wrt to the standard density of valuation r, whose expression is given in (56). Remark that $A_4(r)\sim(r+1)^{-1}$ when $r\to-1$. With (54), 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 defined in Section 6.7, with the Gauss principle recalled in Section 4.4. We have have then described the main ingredients of the proof for the following result :

Theorem 8.3. (Vallée and Vera [39] 2007) *On the set Ω_M of inputs of size M endowed with a density f of valuation r, the central execution[8] 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*

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

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

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.

9. First steps in the probabilistic analysis of the LLL algorithm.

We return now to the LLL algorithm and explain how the previous approaches can be applied for analyzing the algorithm.

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

9.1. **Evolution of densities of the local bases.** The LLL algorithm aims at reducing all the local bases U_k (defined in Section 3.1) 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 variant OddEven described in Section 3.5 is well–adapted to this purpose.

In the first Odd Phase, the LLL algorithm first deals with local bases with odd indices. Consider two successive bases U_k and U_{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[9] 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, Theorem 7.5 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 (see Section 6.8), we obtain a precise information on the distribution of the norms $|\hat{v}_k^\star|, |\hat{u}_{k+2}|$.

In the first Even Phase, the LLL algorithm considers the local bases with an even index. Now, the basis U_{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 (quasi–)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 U_{k+1}. We then hope to "follow" the evolution of densities of local bases along the whole execution of the LLL algorithm.

Open question : Is this approach robust enough to "follow" the evolution of densities of local bases along the whole execution of the LLL algorithm ? Of course, in the "middle" of the algorithm, the two variables $\hat{v}_k^\star, \hat{u}_{k+2}$ are no longer independent. Are they not too dependent, so that we can apply the previous method ? Is it true that the variables ν at the *beginning* of the phase are almost uniformly distributed on $[-1/2, +1/2]$? Here, some experiments will be of great use.

9.2. **The dynamical system underlying the** Odd-Even-LLL **algorithm.** We consider 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 9.1 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 !

Références

[1] M. Ajtai. The worst-case behavior of Schnorr's algorithm approximating the shortest nonzero vector in a lattice, Proceedings of the 35th Symposium on the Theory of Computing (STOC 2003), ACM, 2003, 396–406

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

[3] A. Akhavi, J.-F. Marckert and A. Rouault. On the Reduction of a Random Basis, *Proceedings of SIAM-ALENEX/ANALCO'07.* New-Orleans, january 07

[4] 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.

[5] V. Baladi and B. Vallée. Euclidean Algorithms are Gaussian, *Journal of Number Theory*, Volume 110, Issue 2 (2005) pp 331–386

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

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

[9] The notation * refers to the Gram–Schmidt process as in Sections 2 and 3.

[8] 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).

[9] E. Cesaratto, J. Clément, B. Daireaux, L. Lhote, V. Maume-Deschamps, B. Vallée. Analysis of fast versions of the Euclid Algorithm, *Proceedings of SIAM-ALENEX/ANALCO'07.*

[10] D. Coppersmith. Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities, *Journal of Cryptology*, vol 10(4), 1997,233–260

[11] D. Coppersmith and A. Shamir. Lattice Attacks on NTRU, *Proceedings of Eurocrypt 1997*, Springer, LNCS, 1233 (1997) 52-61,

[12] J-S. Coron. Security Proof for Partial-Domain Hash Signature Schemes In *Proceedings of Crypto 2002*, LNCS 2442, 613–626, Springer-Verlag (2002)

[13] 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.

[14] H. Daudé, B. Vallée. An upper bound on the average number of iterations of the LLL algorithm. *Theoretical Computer Science 123*, 1 (1994), 95–115.

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

[16] 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

[17] N. Gama, N. Howgrave-Graham, H. Koy, and P.Nguyen. Rankin's Constant and Blockwise Lattice Reduction, *Proceedings of Crypto 2006*, Springer LNCS 4117, (2006) 112–130

[18] C. Gentry. The Geometry of Provable Security : some proofs of Security in which Lattices make a Surprise Appearance, *These proceedings*

[19] C. Gentry. How to compress Rabin Ciphertexts and Signatures (and more), *Proceedings of Crypto'04*, 179–200, Springer Verlag (2004)

[20] D. Goldstein and A. Mayer. On the equidistribution of Hecke points, *Forum Mathematicum*, 15, (2003), 165–189

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

[22] 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

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

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

[25] L. Lhote and B. Vallée. Sharp estimates for the main parameters of the Euclid Algorithm, *Proceedings of LATIN 2006*, pages 689–702, Lecture Notes in Computer Science, 3887, Springer

[26] P. Nguyen, P. and D. Stehlé. Floating-Point LLL Revisited, *Proceedings of Eurocrypt 2005*, Springer, LNCS 2005, vol 3494, 215–233.

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

[28] C. P.Schnorr. A Hierarchy of Polynomial Lattice Basis Reduction Algorithms, *Theoretical Computer Science*, vol 53, (1987), 201–224

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

[30] C.L. Siegel. A mean value theorem in geometry of numbers, *Annals in Mathematics*, 46(2) 340–347, 1945.

[31] D. Stehlé. Floating Point LLL : Theoretical and Practical aspects, *These proceedings.*

[32] B. Vallée. Euclidean Dynamics, *Discrete and Continuous Dynamical Systems*, 15 (1) May 2006, pp 281-352.

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

[34] 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.

[35] 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

[36] B. Vallée. Dynamical Analysis of a Class of Euclidean Algorithms, *Theoretical Computer Science* 297 1-3, 2003, 447–486

[37] B. Vallée. Generation of elements with small modular squares and provably fast integer factoring algorithms, *Mathematics of Computation*, vol 56, 194, 823–849, 1991.

[38] B. Vallée. Provably fast integer factoring algorithm with quasi-uniform quadratic residues, *Proceedings of ACM-STOC-89*, Seattle, 98–106.

[39] B. Vallée, A. Vera. Lattice Reduction in two dimensions : analyses under realistic probabilistic models, to appear in Proceedings of AofA'07, *Discrete Mathematics and Theoretical Computer Science*.

[40] B. Vallée, M. Girault, P. Toffin. How to guess ℓ-th roots modulo n by reducing lattices bases, *Proceedings of AAECC-88*, Rome, Lectures Notes in Computer Science (357), 427–442.

[41] G. Villard. Parallel lattice basis reduction. *Proceedings of International Symposium on Symbolic and Algebraic Computation*, Berkeley California USA . ACM Press, July 1992.

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