Probabilistic behaviour of lattice reduction algorithms

Brigitte Vallée, Antonio Vera

Chapter 3
Probabilistic Analyses of Lattice Reduction Algorithms

Brigitte Vallée and Antonio Vera

Abstract The general behavior 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 outputs, 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 analyzing these algorithms, namely, dedicated modeling, 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.

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 behavior of lattice reduction and attain a justification of many of the experimental facts observed. Beyond its intrinsic theoretical interest, such a justification is important as a fine understanding of the lattice reduction process conditions algorithmic improvements in major application areas, most of them being described in this book: cryptography (see [28, 31]), computational number theory (see [21, 22, 35]), integer programming (see [1]), etc. The results obtained in this perspective may then be applied for developing a *general algorithmic strategy* for lattice reduction.

B. Vallée (✉) · Antonio Vera
Laboratoire GREYC, CNRS UMR 6072, Université de Caen and ENSICAEN,
F-14032 Caen, France,
e-mail: brigitte.vallee@info.unicaen.fr

Varied Approaches

We briefly describe now three different points of view: dedicated modeling, probabilistic methods, and dynamical systems approach.

Dedicated Modeling. 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 behaviors. An analysis of the lattice reduction algorithms under such probabilistic models aims at characterizing the behavior 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 an input basis to be already reduced? A possible extension of this study to realistic models and to the complete algorithm (not just its input distribution) is discussed here.

Dynamical Systems Approach. Thanks to earlier results, the dynamics of Euclid's algorithm is now well-understood – many results describe the probabilistic behavior 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 the possible extensions of the "dynamical analysis methodology" to higher dimensions. The first step in such an endeavor should describe the dynamical system for the LLL algorithm, which is probably a complex object, for $p > 2$.

Historical and Bibliographic Notes

Over the past 20 years, there have been several parallel studies dedicated to the probabilistic behavior 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 [23] performs in 1980 a first (worst–case) analysis of the Gauss algorithms in two and three dimensions. In 1990, Vallée [38] exhibits the exact worst–case complexity of the Gauss algorithm. In the same year, Flajolet and Vallée [16] 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 et al. [14] 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 [24] study the main output parameters of the algorithm (the first minimum, Hermite's defect), under the uniform model, still. In 1997,

Vallée [39] introduces the model "with valuation" for the Sign Algorithm: this is an algorithm for comparing rationals, whose behavior is similar to the Gauss algorithm. In 2000, Flajolet and Vallée [17] precisely study all the constants that appear in the analysis of the Sign Algorithm. Finally, in 2007, Vallée and Vera [45, 47] 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 same principles as the Euclid algorithms (divisions and exchanges), but they differ on the kind of division performed. This method, summarized for instance in [37], 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 [14], previously described, which is in fact the first beginning of dynamical analysis. The dynamical systems underlying 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 [41], bit-complexity (with Akhavi) [5], and bit-complexity of the fast variants of the Euclid algorithms (with the CAEN group) [10]. From 2003, Baladi et al. [6, 27] 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, and bit-complexity – and show that they all follow asymptotic normal laws.

It is now natural to expect that most of the principles of 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 [14].

The General Case. The first probabilistic analysis of the LLL algorithm is performed by Daudé and Vallée on 1994 [15] under the "random ball model." These authors obtain an upper bound for the mean number of iterations of the algorithm. Then, in 2002, Akhavi [3] studies the probabilistic behavior 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 et al. [4] 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 [2] exhibits a randomness model of input bases (which is called the Ajtai model in this paper), under which the probabilistic behavior of the LLL algorithm is close to the worst-case behavior. In 2006, Nguyen et al. [30] study random lattices together with their parameters relevant to lattice reduction algorithms. In 2006, Nguyen and Stehlé [30] 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 that 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 behavior of the LLL algorithm and its whole dynamics.

Plan of the Survey

Section "The Lattice Reduction Algorithm in the Two-Dimensional Case" 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 "The LLL Algorithm" 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 behavior 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 role of the Gauss algorithm becomes more apparent than in standard versions. Section "What is a Random (Basis of a) Lattice?" describes the main probabilistic models of interest that appear in "real life" applications – some of them are given because of their naturalness, while other ones are related to actual applications of the LLL algorithm. Section "Probabilistic Analyses of the LLL Algorithm in the Spherical Model" 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.

The 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 "Returning to the Gauss Algorithm", we describe the dynamical systems that underlie 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 "Analysis of Lattice Reduction in Two-Dimensions: The Output Parameters" and "Analysis of the Execution Parameters of the Gauss Algorithm" on the precise study of the main parameters of interest – either output parameters or execution parameters – under the model "with valuation." Finally, Section "First Steps in the Probabilistic Analysis of the LLL Algorithm" returns to the LLL algorithm and explains how the results of Sections "Returning to the Gauss Algorithm – Analysis of the Execution Parameters of the Gauss Algorithm" could (should?) be used and/or extended to higher dimensions.

The Lattice Reduction Algorithm in the Two-Dimensional Case

A lattice $\mathcal{L} \subset \mathbb{R}^n$ of dimension p is a discrete additive subgroup of $\mathbb{R}^n$. Such a lattice is generated by integral linear combinations of vectors from a family $B := (b_1, b_2, \ldots b_p)$ of $p \leq n$ linearly independent vectors of $\mathbb{R}^n$, which is called a basis of the lattice $\mathcal{L}$. A lattice is generated by infinitely many bases that are related to each other by integer matrices of determinant ± 1. Lattice reduction algorithms consider a Euclidean lattice of dimension p in the ambient space $\mathbb{R}^n$ and aim at finding a "reduced" basis of this lattice, formed with vectors almost orthogonal and short enough. The LLL algorithm designed in [25] uses as a sub-algorithm the lattice reduction algorithm for two dimensions (which is called the Gauss algorithm):[1] 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.

We also see in this article that the Gauss algorithm solves the reduction problem in an optimal sense: it returns a minimal basis, after a number of iterations, which is at most linear with respect to the input size. This type of algorithms can be generalized in small dimensions. For instance, in the three-dimensional case, Vallée in 1987 [42] or Semaev more recently [33] provide optimal algorithms, which directly find a minimal basis, after a linear number of iterations. However, algorithms of this quality no longer exist in higher dimensions, and the LLL algorithm can be viewed as an approximation algorithm that finds a good basis (not optimal generally speaking) after a polynomial number of iterations (not linear generally speaking).

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

$$\frac{v}{u} = \frac{(u \cdot v)}{|u|^2} + \mathrm{i}\frac{\det(u, v)}{|u|^2}. \tag{3.1}$$

[1] It seems that the Gauss algorithm, as it is described here, is not actually due to Gauss, but due to Lagrange.

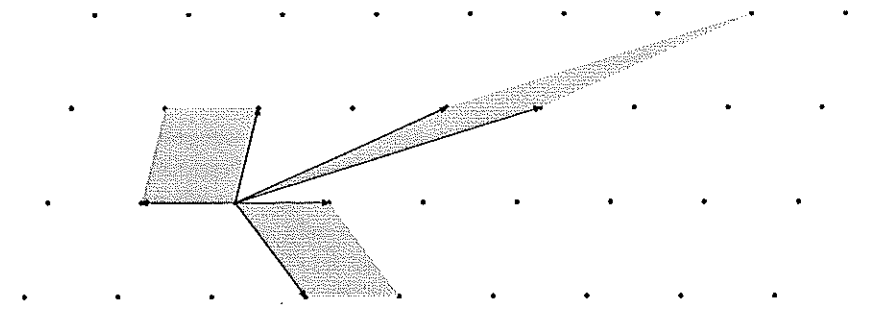

Fig. 3.1 A lattice and three of its bases represented by the parallelogram they span. The basis on the *left* is minimal (reduced), while the two other ones are skew

A *lattice* of two-dimensions in the complex plane $\mathbb{C}$ is the set $\mathcal{L}$ of elements of $\mathbb{C}$ (also called vectors) defined by

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

where (u, v), called a *basis*, is a pair of $\mathbb{R}$-linearly independent elements of $\mathbb{C}$. Remark that in this case, due to (3.1), 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 one of the first minimum 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 minimum (See Fig. 3.1). In the sequel, we focus on particular bases that satisfy one of the two following properties:

- (P) It has a positive determinant [i.e., $\det(u, v) > 0$ or $\Im(v/u) > 0$]. 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), as one of (u, v) and $(u, -v)$ is.
The following result gives characterizations of minimal bases. Its proof is omitted.

Proposition 1. [Characterizations of minimal bases.]

- (P) [Positive bases.] *Let (u, v) be a positive basis. Then the following two conditions (a) and (b) are equivalent:*
- (a) *The basis (u, v) is minimal*
- (b) *The pair (u, v) satisfies the three simultaneous inequalities:*

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

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

PGAUSS(u, v)
Input. A positive basis (u, v) of $\mathbb{C}$ with $|v| \leq |u|$, $|\tau(v, u)| \leq (1/2)$.
Output. A positive minimal basis (u, v) of $\mathcal{L}(u, v)$ with $|v| \geq |u|$.
`While` $|v| < |u|$ `do`
$(u, v) := (v, -u)$;
$q := \lfloor \tau(v, u) \rceil$;
$v := v - qu$;

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

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

The Gaussian Reduction Schemes

There are two reduction processes, according as one focuses on positive bases or acute bases. Accordingly, as we study the behavior 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 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

$$v := v - qu \qquad \text{with} \quad q := \lfloor \tau(v, u) \rceil, \quad \tau(v, u) := \Re\left(\frac{v}{u}\right) = \frac{(u \cdot v)}{|u|^2}, \tag{3.2}$$

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

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

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

$$v_{i+1} = -v_{i-1} + q_i\, v_i \qquad \text{with} \quad q_i := \lfloor \tau(v_{i-1}, v_i) \rceil\,. \tag{3.3}$$

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 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

$$\begin{pmatrix} v_{p+1} \\ v_p \end{pmatrix} = \mathcal{M} \begin{pmatrix} v_1 \\ v_0 \end{pmatrix} \qquad \text{with} \quad \mathcal{M} := \mathcal{M}_p \cdot \mathcal{M}_{p-1} \cdot \ldots \cdot \mathcal{M}_1. \tag{3.4}$$

The Acute Gauss Algorithm

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

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

where $\tau(v, u)$ is defined as in (3.2). 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`
$(u, v) := (v, u)$;
$q := \lfloor \tau(v, u) \rceil$; $\varepsilon := \operatorname{sign}\left(\tau(v, u) - \lfloor \tau(v, u) \rceil\right)$;
$v := \varepsilon(v - qu)$;

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

$$\widetilde{q}_i := \lfloor \tau(w_{i-1}, w_i) \rceil\,, \qquad \varepsilon_i = \operatorname{sign}\left(\tau(w_{i-1}, w_i) - \lfloor \tau(w_{i-1}, w_i) \rceil\right). \tag{3.5}$$

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 1. Each step defines a unimodular matrix $\mathcal{N}_i$ with $\det \mathcal{N}_i = -\varepsilon_i = \pm 1$,

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

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

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

Comparison Between the Two Algorithms

These algorithms are closely related, but different. The AGAUSS Algorithm can be viewed as a folded version of the PGAUSS Algorithm, in the sense defined in [7]. We shall come back to this fact in Section "Relation with the Centered Euclid Algorithm", and the following is true.

Consider two bases: a positive basis (v_0, v_1) *and an acute basis* (w_0, w_1)*, which 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 (3.3) and (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.

Main Parameters of Interest

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

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

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*[3] 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 an 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 ith step is proportional to $\ell(|q_i|) \cdot \ell(|v_{i-1}|^2)$, and the bit-complexity of the central part of the Gauss Algorithm is expressed as a function of

$$B(u, v) = \sum_{i=1}^{P(u,v)} \ell(|q_i|) \cdot \ell(|v_{i-1}|^2), \tag{3.6}$$

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 main 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:

$$Q(u, v) = \sum_{i=1}^{P(u,v)} \ell(|q_i|), \qquad \underline{D}(u, v) = \sum_{i=1}^{P(u,v)} \ell(|q_i|)\left[\,\ell(|v_{i-1}|^2) - \ell(|v_0|^2)\right],$$
$$D(u, v) := \sum_{i=1}^{P(u,v)} \ell(|q_i|) \lg \left|\frac{v_{i-1}}{v}\right|^2, \tag{3.7}$$

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

$$B(u, v) = Q(u, v)\,\ell(|u|^2) + D(u, v) + [\underline{D}(u, v) - D(u, v)]. \tag{3.8}$$

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

(a) The additive costs, which provide a generalization of costs P and Q. They are defined as the sum of elementary costs, which depend only 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

$$C_{(c)}(u, v) = \sum_{i=1}^{P(u,v)} c(|q_i|). \tag{3.9}$$

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

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 ith length decreases d_i for $i \in [1..p]$ (with $p := P(u, v)$]) and the total length decrease $d := d_p$, defined as

$$d_i := \left|\frac{v_i}{v_0}\right|^2, \qquad d := \left|\frac{v_p}{v_0}\right|^2. \tag{3.10}$$

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

$$\lambda(u, v) := \lambda_1(\mathcal{L}(u, v)) = |\widehat{u}|, \qquad \mu(u, v) := \frac{|\det(u, v)|}{\lambda(u, v)} = |\widehat{v}^\star|, \tag{3.11}$$

$$\gamma(u, v) := \frac{\lambda^2(u, v)}{|\det(u, v)|} = \frac{\lambda(u, v)}{\mu(u, v)} = \frac{|\widehat{u}|}{|\widehat{v}^\star|}. \tag{3.12}$$

We return later to these output parameters and shall explain in Section "A Variation for the LLL Algorithm: The Odd-Even Algorithm" why they are so important in the study of the LLL algorithm. We now return to the general case of lattice reduction.

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.

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 $\widehat{B}$ formed with vectors almost orthogonal and short enough. The algorithm (see Figure 3.2) 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 $\tau(b_i, b_j^*)$, with τ defined in (3.2). The algorithm performs two main types of operations (see Figure 3.2):

$$\mathcal{P} := \begin{array}{c} \\ b_1 \\ b_2 \\ \vdots \\ b_i \\ b_{i+1} \\ \vdots \\ b_p \end{array} \begin{array}{c} \begin{array}{ccccccc} b_1^\star & b_2^\star & \dots & b_i^\star & b_{i+1}^\star & \dots & b_p^\star \end{array} \\ \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ m_{2,1} & 1 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ m_{i,1} & m_{i,2} & \dots & 1 & 0 & 0 & 0 \\ m_{i+1,1} & m_{i+1,2} & \dots & m_{i+1,i} & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ m_{p,1} & m_{p,2} & \dots & m_{p,i} & m_{p,i+1} & \dots & 1 \end{pmatrix} \end{array}$$

$$U_k := \begin{array}{c} \\ u_k \\ v_k \end{array} \begin{array}{c} \begin{array}{cc} b_k^\star & b_{k+1}^\star \end{array} \\ \begin{pmatrix} 1 & 0 \\ m_{k+1,k} & 1 \end{pmatrix} \end{array}$$

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

Input. A basis B of a lattice L of dimension p.
Output. A reduced basis $\widehat{B}$ 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. 3.2 The LLL algorithm: the matrix $\mathcal{P}$, the local bases U_k, and the algorithm itself

1. *Size-reduction of vectors.* The vector b_i is size-reduced if all the coefficients $m_{i,j}$ of the ith 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 $j \in [1..i-1]$.
   As subdiagonal coefficients play a particular rôle (as we shall see later), the 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);
   `For` $j := i - 2$ `downto` 1 `do` $b_i := b_i - \lfloor m_{i,j} \rceil b_j$.
2. *Gauss-reduction of the local bases.* The ith 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 $\langle b_1, b_2, \dots, b_{i-1} \rangle$. 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

$$K \leq (p-1) + 2K^-. \tag{3.13}$$

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 Siegel ratios r_i's between successive Gram orthogonalized vectors, namely

$$r_i := \frac{\ell_{i+1}}{\ell_i}, \qquad \text{with} \quad \ell_i := |b_i^\star|. \tag{3.14}$$

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

$$a := \min\{\ell_i; \quad 1 \leq i \leq p\}, \qquad A := \max\{\ell_i; \quad 1 \leq i \leq p\}, \tag{3.15}$$

tends to be narrowed as, 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 nonzero vector of the lattice), namely

$$\lambda(\mathcal{L}) \leq A\sqrt{p}, \qquad \lambda(\mathcal{L}) \geq a. \tag{3.16}$$

At the end of the algorithm, the basis $\widehat{B}$ satisfies the following:[4] each local bases is reduced in the t-Gauss meaning. It satisfies conditions that involve the subdiagonal matrix coefficients $\widehat{m}_{i+1,i}$ together with the sequence $\widehat{\ell}_i$, namely the t-Lovász conditions, for any $i, 1 \leq i \leq p-1$,

[4] All the parameters relative to the output basis $\widehat{B}$ are denoted with a hat.

$$|\widehat{m}_{i+1,i}| \leq \frac{1}{2}, \qquad t^2\,(\widehat{m}_{i+1,i}^2\,\widehat{\ell}_i^2 + \widehat{\ell}_{i+1}^2) \geq \widehat{\ell}_i^2, \tag{3.17}$$

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

$$|\widehat{m}_{i+1,i}| \leq \frac{1}{2}, \quad \widehat{r}_i := \frac{\widehat{\ell}_{i+1}}{\widehat{\ell}_i} \geq \frac{1}{s}, \quad \text{with } s^2 = \frac{4t^2}{4-t^2} \quad \text{and} \quad s = \frac{2}{\sqrt{3}} \quad \text{for } t = 1. \tag{3.18}$$

A basis fulfilling conditions (3.18) is called s-Siegel reduced .

Main Parameters of Interest

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

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

$$\gamma(B) := \frac{|\widehat{b}_1|^2}{(\det \mathcal{L})^{2/p}} \leq s^{p-1}, \qquad \theta(B) := \frac{|\widehat{b}_1|}{\lambda(\mathcal{L})} \leq s^{p-1}, \tag{3.19}$$

$$\rho(B) := \frac{\prod_{i=1}^{d} |\widehat{b}_i|}{\det \mathcal{L}} \leq s^{p(p-1)/2}.$$

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

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 ratio between the new determinant $\check{D}_i$ and the old one satisfies $\check{D}_i/D_i \leq (1/t)$, while the other D_j are not modified.

Then, the ratio between the final $\widehat{D}$ and the initial D satisfies $(\widehat{D}/D) \leq (1/t)^{K^-}$, where K^- denotes the number of indices of the random walk when the test in 2 is negative (see Section "Description of the Algorithm"). With the following bounds on the initial D and the final $\widehat{D}$, as a function of variables a, A, defined in (3.15),

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

together with the expression of K as a function of K^- given in (3.13), the following bound on K is derived,

$$K \leq (p-1) + p(p-1)\log_t \frac{A}{a}. \tag{3.20}$$

In the same vein, another kind of bound involves $N := \max |b_i|^2$ and the first minimum $\lambda(\mathcal{L})$, (see [15]),

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

In the case when the lattice is integer (namely $\mathcal{L} \subset \mathbb{Z}^n$), this bound is slightly better and becomes

$$K \leq (p-1) + p(p-1)\frac{M}{\lg t}.$$

It involves $\lg t := \log_2 t$ and the binary size M of B, defined as $M := \max \ell(|b_i|^2)$, 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.

Experiments for the LLL Algorithm

In [30], Nguyen and Stehlé have made a great use of their efficient version of the LLL algorithm [29] 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 3.3 and 3.4 show some of the main experimental results. These experimental results are also described in the survey written by D. Stehlé in these proceedings [36].

Main parameters.	$\widehat{r}_i$	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. 3.3 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 $N := \max |b_i|^2$

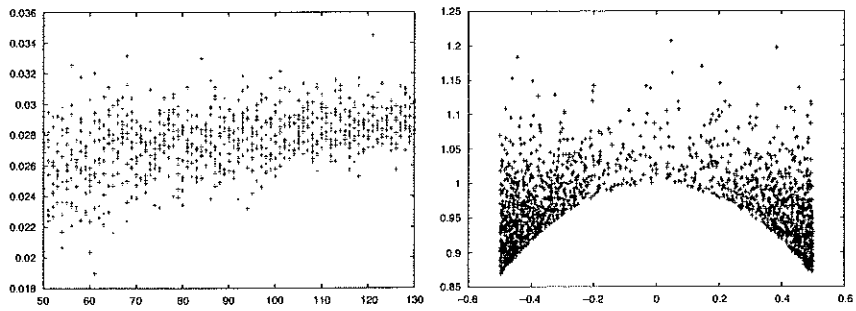

Fig. 3.4 *Left*: experimental results for $\log_2 \gamma$. The experimental value of parameter $[1/(2p)]\,\mathbb{E}[\log_2 \gamma]$ is close to 0.03, so that α is close to 1.04. *Right*: the output distribution of "local bases"

Output geometry. The geometry of the output local basis $\widehat{U}_k$ 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 $\widehat{z}_k$ that is related to the output local basis $\widehat{U}_k := (\widehat{u}_k, \widehat{v}_k)$ via the equality $\widehat{z}_k := \widehat{m}_{k,k+1} + i\widehat{r}_k$. Because of the t-Lovász conditions on $\widehat{U}_k$, described in (3.17), the complex number $\widehat{z}_k$ 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 $\widehat{U}_k$ 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 Fig. 3.4 (right)]. The (experimental) mean values of the output Siegel ratios $\widehat{r}_k := \Im(\widehat{z}_k)$ 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) that 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 that 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 Sections "Returning to the Gauss Algorithm and First Steps in the Probabilistic Analysis of the LLL Algorithm"?

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 "Probabilistic Models: Continuous or Discrete"]

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.

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 "Description of the Algorithm"). 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 [48], 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 "Returning to the Gauss Algorithm" that it has a better "dynamical" structure.

During one even (respectively, odd) phase (see Figure 3.5), the *whole* AGAUSS algorithm is performed on all local bases U_i with even (respectively, odd) indices. Since local bases with odd (respectively, 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 "First Steps in the Probabilistic Analysis of the LLL Algorithm", when we shall explain the main principles for a dynamical study of the LLL algorithm.

Odd–Even LLL (t) $\quad [t > 1]$

Input. A basis B of a lattice L of dimension p.
Output. A reduced basis $\widehat{B}$ 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. 3.5 Description of the Odd–Even variant of the LLL algorithm, with its two phases, the Odd Phase and the Even Phase

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 $(\widehat{u}_k, \widehat{v}_k)$ and $(\widehat{u}_{k+2}, \widehat{v}_{k+2})$, which satisfy in particular

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

where parameters λ, μ are defined in (3.11). 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 $u_{k+1} = \widehat{v}_k^\star$, $v_{k+1} = \nu \widehat{v}_k^\star + \widehat{u}_{k+2}$, 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 that is played by these parameters λ, μ. We study these parameters in Section "Analysis of Lattice Reduction in Two-Dimensions: The Output Parameters".

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 Stehlé in this book [36].

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 [15], then studied in [3,4] (See Section "Probabilistic Analyses of the LLL Algorithm in the Spherical Model"). 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 $\mathcal{S}_{(n)} := \{x \in \mathbb{R}^n : \|x\| = 1\}$. 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

$$\beta_{a,b}(x) = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} x^{a-1}(1-x)^{b-1}\, \mathbf{1}_{(0,1)}(x), \qquad \gamma_a(x) = \frac{e^{-x}x^{a-1}}{\Gamma(a)}\, \mathbf{1}_{[0,\infty)}(x). \tag{3.21}$$

We now describe three natural instances of simple spherical distributions.

1. 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 $\beta(n/2, 1)$.
2. 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 $x = 1$.
3. 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.

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

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

[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, as the coefficient $m_{i,j}$ equals $a_{i,j,p}/a_{j,p}$. However, all the input Siegel ratios r_i, defined in (3.14) and here equal to $a_{i+1,p}/a_{i,p}$, tend to 0 when p tends to ∞. Then, such bases are not reduced "at all," and this explains why similar bases have been used by Ajtai in [2] to show the tightness of worst-case bounds of [32].

Variations Around Knapsack Bases and Their Transposes

This last type gathers various shapes of bases, which are all formed by "bordered identity matrices"; see Fig. 3.6.

1. The knapsack bases themselves are the rows of the $p \times (p+1)$ matrices of the form of Fig. 3.6a, 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).
2. The bases relative to the transposes of matrices described in Fig. 3.6b arise in searching for simultaneous Diophantine approximations (with $q \in \mathbb{Z}$) or in discrete geometry (with $q = 1$).

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

(a) (b) (c) (d)

Fig. 3.6 Different kinds of lattice bases useful in applications. Type (**a**) Knapsack bases; Type (**b**) bases used for factoring polynomials, for solving Diophantine equations; Type (**c**) Bases for NTRU; Type (**d**) bases related to random lattices

3. The NTRU cryptosystem was first described in terms of polynomials over finite fields, but the public-key can be seen [12] as the lattice basis given by the rows of the matrix $(2p \times 2p)$ described in Fig. 3.6c, where q is a small power of 2 and H_p is a circulant matrix whose line coefficients are integers of the interval $]-q/2, q/2]$.

Random Lattices

There is a natural notion of random lattice, introduced by Siegel [34] in 1945. The space of (full-rank) lattices in $\mathbb{R}^n$ modulo scale can be identified with the quotient $\mathbb{X}_n = SL_n(\mathbb{R})/SL_n(\mathbb{Z})$. 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 $\mathbb{X}_n$. This measure ν_n (which can be normalized to have total volume 1) is by definition the unique probability on $\mathbb{X}_n$, which is invariant under the action of G_n: if $A \subseteq \mathbb{X}_n$ 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 "Relation with Eisenstein Series".

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 that 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.

1. 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:

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

2. We may also replace the discrete model associated to knapsack bases of Fig. 3.6a by the continuous model, where A is replaced by a real vector x uniformly chosen in the ball $\|x\|_\infty \leq 1$ 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 1. 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 $\mathcal{X} \subset \mathbb{R}^n$ with a "smooth" frontier. For any integer N, we can "replace" a (continuous) distribution in the domain $\mathcal{X}$ relative to some density f of class $\mathcal{C}^1$ by the distribution in the discrete domain

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

defined by the restriction f_N of f to $\mathcal{X}_N$. 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 $\mathcal{A} \subset \mathcal{X}$ (with a smooth frontier $\partial\mathcal{A}$) and the number of points in the domain $\mathcal{A}_N := \mathcal{A} \cap \mathcal{X}_N$,

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

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 $\mathbb{X}_n$ (defined in 4.4) by the homothecy Ψ_N of ratio $N^{-1/n}$. Goldstein and Mayer [20] show that for large N, the following is true: given any measurable subset $A_n \subseteq \mathbb{X}_n$ whose boundary has zero measure with respect to ν_n, the proportion 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 Fig. 3.6d, where the components x_i (with $i \in [1..n-1]$) of the vector x are chosen independently and uniformly in $\{0, \ldots, q-1\}$.

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 $g(n) \leq n$). We are interested in the following questions:

1. 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 (3.18)]?
2. Consider a real $t > 1$. What is the average number of iterations of the LLL(t) algorithm on a random basis $B_{p,(n)}$?
3. 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 $g := n-p$.

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 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*

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

together with two other parameters

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

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

Remark 2. The ratio $\underline{r}_{j,(n)}$ is closely related to the ratio r_i defined in Section "Description of the Algorithm" [see (3.14)]. 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

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

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 behavior 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 C*.

Concentration Property *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*

$$\rho_{(n)}\left(a_n(1+\theta)\right) - \rho_{(n)}\left(a_n(1-\theta)\right) \geq 1 - d_1\, \mathrm{e}^{-n d_2 \theta^\alpha}. \tag{3.22}$$

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 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* $\varepsilon > 0$, *the sequence* $\mathbb{P}[|X_n - a| > \varepsilon]$ *tends to 0. The two situations are respectively denoted as*

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

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

Theorem 1. (Akhavi et al. [4] 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.

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 2. (Akhavi et al. [4] 2005)

1. 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.
2. 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 2 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 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

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

We will show in the sequel that they intervene as the limits of variables (of the same name) defined in Definition 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

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

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

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

(c) Finally, classical results about independent gamma and beta distributed random variables, together with the weak law of large numbers and previous Proposition 2, prove that

$$\text{For each } j \geq 1, \ \underline{r}^2_{j,(n)} \xrightarrow[n]{(d)} \mathcal{R}_j. \tag{3.23}$$

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 1.

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 ∞. As $\mathcal{M}_{g,(n)}$ 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 2. (Akhavi et al. [4] 2005) *For any concentrated spherical distribution, the following holds:*

1. *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* $q > 2$.
2. *For any fixed* k, *one has* $\mathcal{M}_{k,(n)} \xrightarrow[n]{(d)} \mathcal{M}_k, \mathcal{I}_{k,(n)} \xrightarrow[n]{(d)} \mathcal{I}_k$.
3. *For any sequence* $n \mapsto g(n)$ *with* $g(n) \leq n$ *and* $g(n) \to \infty$, *the convergence* $\mathcal{M}_{g(n),(n)} \xrightarrow[n]{proba.} 1$ *holds.*

This result solves our problem and proves Theorem 1. 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 3. (Akhavi et al. [4] 2005) *The limit processes* $\sqrt{\mathcal{R}_k}, \sqrt{\mathcal{M}_k}$ *admit densities that satisfy the following:*

1. *For each* k, *the density* φ_k *of* $\sqrt{\mathcal{R}_k}$ *is*

$$\varphi_k(x) = 2B\left(\frac{k}{2}, \frac{k+1}{2}\right) \frac{x^{k-1}\mathbf{1}_{[0,\infty[}(x)}{(1+x^2)^{k+(1/2)}}, \quad \text{with } B(a,b) := \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}. \tag{3.24}$$

2. *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* $|x^2 - 1| \leq (1/\sqrt{k})$,

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

3. *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.*

In particular, for a full-dimensional lattice,

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

Figure 3.7 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 "Description of the Algorithm") 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

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

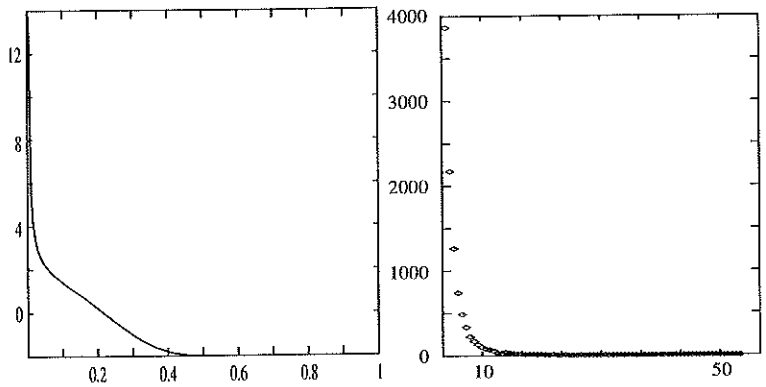

Fig. 3.7 *Left*: simulation of the density of $\mathcal{M}_0$ with 10^8 experiments. *Right*: the histogram of $\mathcal{I}_0$ provided by 10^4 simulations. For any g, the sequence $k \mapsto \P[\mathcal{I}_g = k]$ seems to be rapidly decreasing

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 4. (Akhavi [3] 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 $1/(2 \lg s)$.

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

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

The result then follows from (3.16) and (3.20). 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 3. (Daudé and Vallée [15] 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 $c < 1$,

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

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 behavior 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 "Probabilistic Models for Two-Dimensions" and studied in Sections "Analysis of Lattice Reduction in Two-Dimensions: The Output Parameters" and "Analysis of the Execution Parameters of the Gauss Algorithm".

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 consider each algorithm as a dynamical system, which can be seen as a (complex) extension of a (real) dynamical system relative to a centered Euclidean algorithm. We provide a precise description of the linear fractional transformations (LFTs) used by each algorithm. We finally describe the (two) classes of probabilistic models of interest.

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 depend only on the quantity $\tau(v,u)$ defined in (3.2), which equals $\mathfrak{R}(v/u)$. 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 (3.3) and (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 (3.7), (3.9), and (3.10) and the output parameters λ, μ, γ defined in (3.11) and (3.12). 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 $z = v/u$:

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

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 $T(z) = z + 1$, and 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 $\{z \in \mathbb{C};\ \ \Re(z) \geq 0, \Im(z) \neq 0\}$ 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

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

The Complex Versions for the GAUSS *Algorithms*

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

$$U(z) = -\frac{1}{z} + \left\lfloor \Re\left(\frac{1}{z}\right) \right\rceil = -\left(\frac{1}{z} - \left\lfloor \Re\left(\frac{1}{z}\right) \right\rceil\right), \tag{3.25}$$

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

$$\mathcal{F} = \left\{ z \in \mathbb{H};\quad |z| \geq 1, |\Re z| \leq \frac{1}{2} \right\}, \quad \mathcal{F}_+ := \mathcal{F} \cap \mathbb{H}_+,\ \mathcal{F}_- := \mathcal{F} \cap \mathbb{H}_-. \tag{3.26}$$

Such a domain, represented in Fig. 3.8, is closely related to the classical fundamental domain $\widehat{\mathcal{F}}$ of the upper half plane $\mathbb{H}$ under the action of the group

$$PSL_2(\mathbb{Z}) := \{h : z \mapsto h(z);\quad h(z) = \frac{az+b}{cz+d},\quad a,b,c,d \in \mathbb{Z},\quad ad - bc = 1\}.$$

More precisely, the difference $\mathcal{F} \setminus \widehat{\mathcal{F}}$ is contained in the frontier of $\mathcal{F}$.

Consider the pair $(\mathcal{B}, U)$, where the map $U : \mathcal{B} \to \mathcal{B}$ is defined in (3.25) 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,[5] and $\mathcal{F}$ can be seen as a "hole": as 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 as it attains $\mathcal{F}$. Moreover, as $\mathcal{F}$ is, up to its frontier, a fundamental domain of the

[5] We will see a formal definition of a dynamical system in Section "Analysis of the Execution Parameters of the Gauss Algorithm".

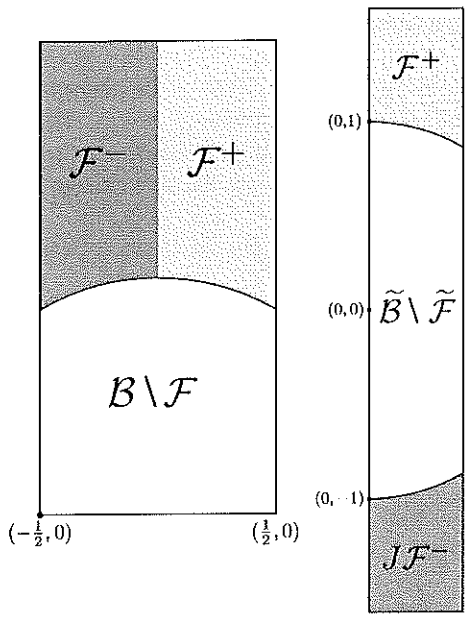

Fig. 3.8 The fundamental domains $\mathcal{F}, \widetilde{\mathcal{F}}$ and the strips $\mathcal{B}, \widetilde{\mathcal{B}}$ defined in Section "The Complex Versions for the GAUSS Algorithms"

upper half plane $\mathbb{H}$ under the action of $PSL_2(\mathbb{Z})$, there exists a topological tessellation 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 in Section "The LFTs Used by the AGAUSS Algorithm. The COREGAUSS Algorithm" that the geometry of $\mathcal{B} \setminus \mathcal{F}$ is compatible with this tessellation.

In the same vein (see Figure 3.8), the AGAUSS algorithm brings z into the vertical strip

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

reduces to the iteration of the mapping

$$\widetilde{U}(z) = \varepsilon\left(\frac{1}{z}\right)\left(\frac{1}{z} - \left\lfloor \Re\left(\frac{1}{z}\right)\right\rceil\right), \qquad \text{with} \quad \varepsilon(z) := \operatorname{sign}(\Re(z) - \lfloor \Re(z) \rceil), \tag{3.27}$$

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

$$\widetilde{\mathcal{F}} = \left\{ z \in \mathbb{C}; \quad |z| \geq 1, \quad 0 \leq \Re(z) \leq \frac{1}{2} \right\} = \mathcal{F}_+ \cup J\mathcal{F}_-. \tag{3.28}$$

Consider the pair $(\widetilde{\mathcal{B}}, \widetilde{U})$, where the map $\widetilde{U} : \widetilde{\mathcal{B}} \to \widetilde{\mathcal{B}}$ is defined in (3.27) 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."

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 a Euclidean division of the form
$$v = qu + r \text{ with } |r| \in [0, +u/2]$$
- For the AGAUSS algorithm, it is based on a Euclidean division of the form
$$v = qu + \varepsilon r \text{ with } \varepsilon := \pm 1, r \in [0, +u/2]$$

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

$$V(x) := \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rceil, \quad \text{for } x \neq 0, \qquad V(0) = 0, \tag{3.29}$$

$$\widetilde{V}(x) = \varepsilon\left(\frac{1}{x}\right)\left(\frac{1}{x} - \left\lfloor \frac{1}{x} \right\rceil\right), \quad \text{for } x \neq 0, \qquad \widetilde{V}(0) = 0. \tag{3.30}$$

[Here, $\varepsilon(x) := \text{sign}(x - \lfloor x \rceil)$].

This leads to two (real) dynamical systems $(\mathcal{I}, V)$ and $(\widetilde{\mathcal{I}}, \widetilde{V})$ whose graphs are represented in Fig. 3.9. 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 [7]. The first system is called the F-EUCLID system (or algorithm), while the second one is called the U-EUCLID system (or algorithm).

Of course, there are close connections between U and $-V$, on the one hand, and $\widetilde{U}$ and $\widetilde{V}$, on the other hand: even if the complex systems $(\mathcal{B}, U)$ and $(\widetilde{\mathcal{B}}, \widetilde{U})$ are

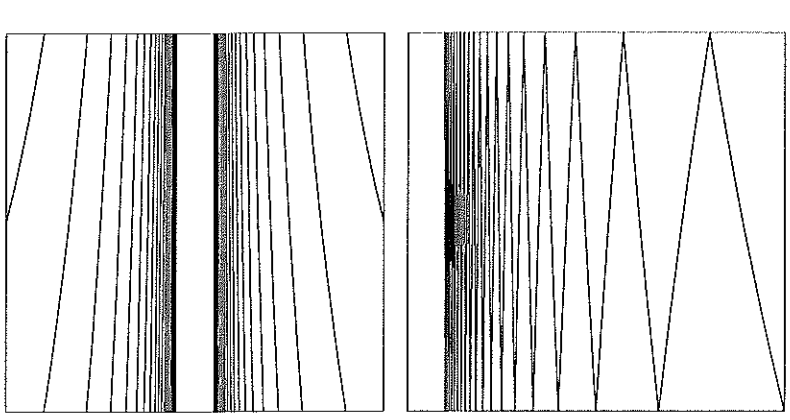

Fig. 3.9 The two dynamical systems underlying the centered Euclidean algorithms

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 $(\widetilde{\mathcal{B}}, \widetilde{U})$, 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" as 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 $i\infty$.

The LFTs Used by the PGAUSS *Algorithm*

The complex numbers that intervene in the PGAUSS algorithm on the input $z_0 = v_1/v_0$ are related to the vectors (v_i) defined in (3.3) 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

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

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 $\widehat{z} = z_p$. More generally, the ith complex number z_i satisfies

$$z_0 = h_i(z_i), \qquad \text{with} \quad h_i := h_{[m_1]} \circ h_{[m_2]} \circ \dots h_{[m_i]}.$$

Proposition 5. (Folklore) *The set $\mathcal{G}$ of LFTs $h : z \mapsto (az + b)/(cz + d)$ defined with the relation $z = h(\widehat{z})$, 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*

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

There exists a bijection between $\mathcal{Q}$ and the set $\mathcal{P} = \{(c, d) \in \mathbb{Z}^2;\ c \geq 1,\ \gcd(c, d) = 1\}$. On the other hand, for each pair (a, c) in the set

$$\mathcal{C} := \{(a, c);\quad \frac{a}{c} \in [-1/2, +1/2],\ c \geq 1; \gcd(a, c) = 1\}, \tag{3.31}$$

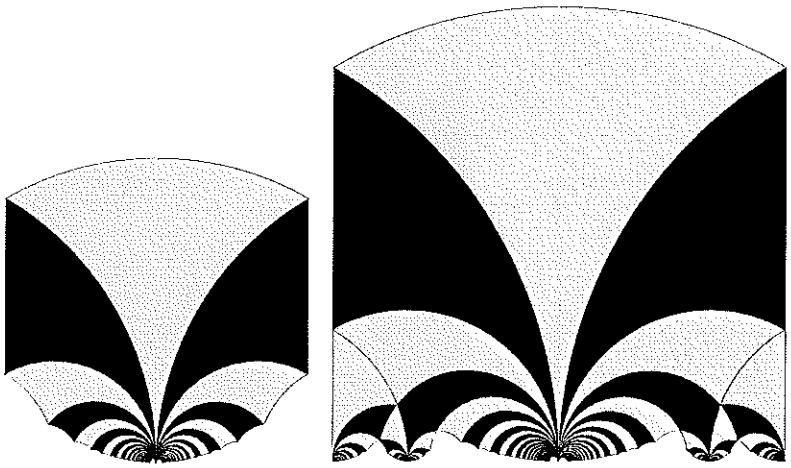

Fig. 3.10 *Left*: the "central" festoon $\mathcal{F}_{(0,1)}$. *Right*: three festoons of the strip $\mathcal{B}$, relative to $(0, 1)$, $(1, 3)$, $(-1, 3)$ and the two half-festoons at $(-1, 2)$ and $(1, 2)$

each 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 2. [Festoons] *If $\mathcal{G}_{(a,c)}$ denotes the set of LFTs of $\mathcal{G}$, which admit (a, c) as coefficients, the domain*

$$\mathcal{F}_{(a,c)} = \bigcup_{h \in \mathcal{G}_{(a,c)}} h(\mathcal{F}) = h_{(a,c)} \left(\bigcup_{q \in \mathbb{Z}} T^q \mathcal{F} \right) \tag{3.32}$$

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 Fig. 3.10).

The LFTs Used by the AGAUSS *Algorithm. The* COREGAUSS *Algorithm*

In the same vein, the complex numbers that intervene in the AGAUSS algorithm on the input $z_0 = w_1/w_0$ are related to the vectors (w_i) defined in (3.5) 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

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

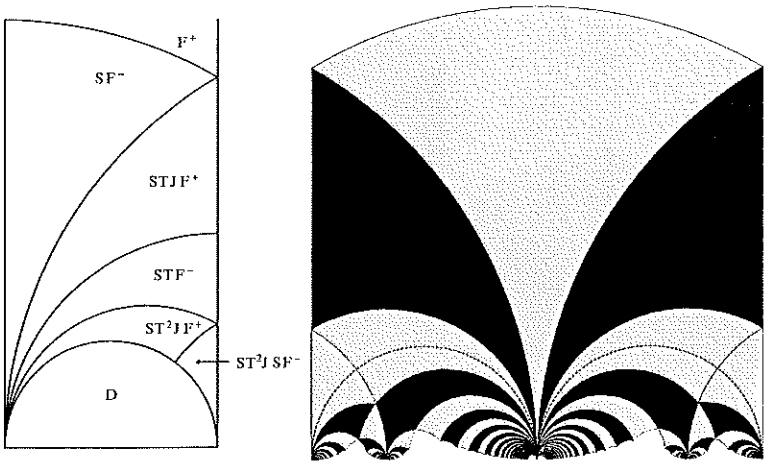

Fig. 3.11 *Left*: the six domains which constitute the domain $\mathcal{B}_+ \setminus \mathcal{D}_+$. *Right*: the disk $\mathcal{D}$ is not compatible with the geometry of transforms of the fundamental domains $\mathcal{F}$

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

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

More generally, the ith complex number z_i satisfies

$$z_0 = \widetilde{h}_i(z_i) \qquad \text{with} \quad \widetilde{h}_i := h_{(m_1,\varepsilon_1)} \circ h_{(m_2,\varepsilon_2)} \circ \dots h_{(m_i,\varepsilon_i)}. \tag{3.33}$$

We now explain the particular rôle that is played by the disk $\mathcal{D}$ of diameter $\widetilde{\mathcal{I}} = [0, 1/2]$. Figure 3.11 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

$$\widetilde{\mathcal{B}} \setminus \mathcal{D} = \bigcup_{h \in \mathcal{K}} h(\widetilde{\mathcal{F}}), \qquad \text{with} \quad \mathcal{K} := \{I, S, STJ, ST, ST^2J, ST^2JS\}. \tag{3.34}$$

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, as the frontier of $\mathcal{D}$ lies "in the middle" of transforms of the fundamental domain $\mathcal{F}$ (see Fig. 3.11).

As Fig. 3.12 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

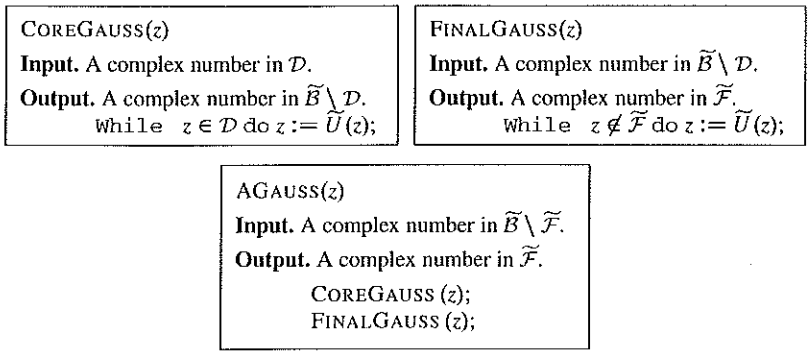

Fig. 3.12 The decomposition of the AGauss Algorithm into two parts: its core part (the CoreGauss Algorithm) and its final part (the FinalGauss Algorithm)

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

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

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

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

$$\mathcal{D} = \bigcup_{h \in \mathcal{H}^+} h(\widetilde{\mathcal{B}} \setminus \mathcal{D}) \qquad \text{with} \quad \mathcal{H}^+ := \sum_{k \geq 1} \mathcal{H}^k. \tag{3.35}$$

The part of the AGauss algorithm performed when z_i belongs to $\mathcal{D}$ is called the CoreGauss algorithm. The total set of LFTs 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 (3.34) and Fig. 3.11), that constitutes the FinalGauss algorithm, which uses the set $\mathcal{K}$ of LFTs, called the final set of LFTs and described in (3.34). Finally, we have proven the decomposition of the AGauss Algorithm, as is described in Fig. 3.12, and summarized in the following proposition:

Proposition 6. (Daudé et al. [14] (1994), Flajolet and Vallée [16, 17] (1990–1999)) *The set $\widetilde{\mathcal{G}}$ formed by the LFTs that 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*

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

Here, if $\mathcal{D}$ denotes the disk of diameter $[0, 1/2]$, then $\mathcal{H}^+$ is the set formed by the LFTs that map $\widetilde{\mathcal{B}} \setminus \mathcal{D}$ into $\mathcal{D}$ and $\mathcal{K}$ is the final set formed by the LFTs that 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 $\phi = (1 + \sqrt{5})/2$:

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

Comparing the CoreGauss *Algorithm and the* F-Euclid *Algorithm*

The CoreGauss algorithm has a nice structure as it uses ateach step the same set $\mathcal{H}$. This set is exactly the set of LFTs that are used by the F-Euclid Algorithm, closely related to the dynamical system defined in (3.30). Then, the CoreGauss algorithm is just a lifting of this F-Euclid Algorithm, while 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 "Analysis of the Execution Parameters of the Gauss Algorithm" 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

$$[R \geq k+1] = \bigcup_{h \in \mathcal{H}^k} h(\mathcal{D}), \tag{3.36}$$

which is represented in Figure 3.13. 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 $\widetilde{\mathcal{I}}$ that 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 "Analysis of the Execution Parameters of the Gauss Algorithm".

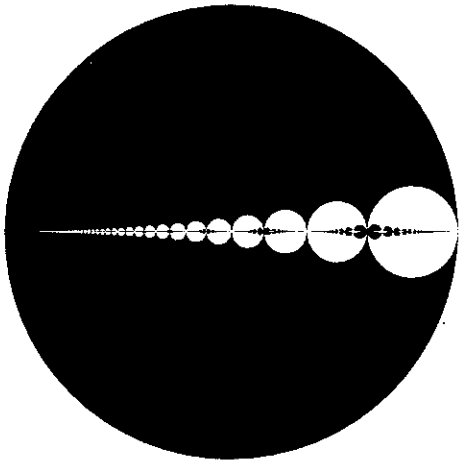

Fig. 3.13 The domains $[R = k]$ alternatively in *black* and *white*. The figure suggests that reduction of almost-collinear bases is likely to require a large number of iterations

Worst-Case Analysis of the Gauss Algorithm

Before beginning our probabilistic studies, we recall the worst-case behavior of execution parameters and give a proof in the complex framework.

Theorem 4. (Vallée [38] 1991) *Consider the* AGAUSS *Algorithm, with an input* (u, v) *of length* $\max(|u|, |v|)$ *at most equal to* N. *Then, the maximum number of iterations* P_N, *and the maximum value* C_N *of any additive cost* C *of moderate growth*[6] *are* $\Theta(\log N)$, *while the maximal value* B_N *of the bit-complexity* B *is* $\Theta(\log^2 N)$. *More precisely, the maximal value* P_N *of the number of iterations* P *satisfies*

$$P_N \sim_{N\to\infty} \frac{1}{\log(1+\sqrt{2})} \log N.$$

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 [38].

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

$$[R \geq k+1] \subset \left\{ z; \quad |\Im(z)| \leq \frac{1}{2} \left(\frac{1}{1+\sqrt{2}} \right)^{2k-1} \right\} \tag{3.37}$$

[6] This means that the elementary cost c satisfies $c(q) = O(\log q)$ (see Section "Main Parameters of Interest").

will lead to the result: as any nonreal 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 (3.37): Indeed, we know from (3.36) 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. The largest such disk $h(\mathcal{D})$ is obtained when all the quotients (m, ε) are the smallest ones, that is, when all $(m, \varepsilon) = (2, +1)$. In this case, the coefficients (c, d) of h are the terms A_k, A_{k+1} of the sequence defined by

$$A_0 = 0, \quad A_1 = 1, \qquad \text{and} \quad A_{k+1} = 2A_k + A_{k-1} \quad \text{for } k \geq 1,$$

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. As 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 that 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. As 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 (3.8). ■

Probabilistic Models for Two-Dimensions

We now return to our initial motivation, and begin our probabilistic studies. As 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 only depend on the ratio $z = v/u$, of the form $F(u, v) = f(v/u)$. Moreover, it is sufficient to consider pairs (u, v) with a first vector u of the form $u = (N, 0)$. Finally, we define in a generic way the discrete model Ω_N as

$$\Omega_N := \left\{ z = \frac{v}{u}; \quad u = (N, 0), v = (a, b), \ (a, b, N) \in \mathbb{Z}^3, \ z \in \mathcal{X} \right\},$$

and there are three main cases, according to the algorithm of interest, namely $\mathcal{X} = \mathcal{B} \setminus \mathcal{F}$ for PGAUSS, $\mathcal{X} = \widetilde{\mathcal{B}} \setminus \widetilde{\mathcal{F}}$ for AGAUSS, or $\mathcal{X} = \mathcal{D}$ for COREGAUSS.

In each case, the complex $z = v/u$ belongs to $\mathbb{Q}[i] \cap \mathcal{X}$ and is of the form $(a/N) + i(b/N)$. Our discrete probabilistic models are defined as the restrictions to Ω_N of a continuous model defined on $\mathcal{X}$. More precisely, we choose a density f on $\mathcal{X}$, and consider its restriction on Ω_N. Normalized by the cardinality $|\Omega_N|$, this gives rise to a density f_N on Ω_N, which we extend on $\mathcal{X}$ as follows: $f_N(x) := f_N(\omega)$ as soon as x belongs to the square of center $\omega \in \Omega_N$ and edge $1/N$. We obtain, in such a way, a family of functions f_N defined on $\mathcal{X}$. When the integer N tends to ∞, this discrete model "tends" to the continuous model relative to the density f (as we already explained in Section "Probabilistic Models: Continuous or Discrete").

It is sometimes more convenient to view these densities as functions defined on $\mathbb{R}^2$, and we will denote by the same symbol 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, while 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 depend only on y.

The Model with "Valuation"

In Section "Probabilistic Analyses of the LLL Algorithm in the Spherical Model", 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 (3.24). We are then led to consider the two-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 collinear. 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 [39] 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

$$f(z) = |\Im(z)|^r \cdot g(z), \qquad \text{where} \quad g(z) \neq 0 \quad \text{for } \Im(z) = 0. \tag{3.38}$$

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

$$f_r(z) = \frac{1}{A(r)}|\Im(z)|^r, \qquad \text{with} \quad A(r) = \iint_{\mathcal{B}\setminus\mathcal{F}} y^r \, dxdy. \tag{3.39}$$

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

$$A(r) \sim \frac{1}{r+1}, \qquad r \to -1.$$

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 that describes the function f, as previously.

The Ajtai Model in Two-Dimensions

This model (described in the general case in Section "Ajtai Bases") 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 collinear) 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].

Analysis of Lattice Reduction in Two-Dimensions: The Output Parameters

This section describes the probabilistic behavior of output parameters: we first analyze the output densities, then we focus on the geometry of our three main parameters defined in (3.11) and (3.12). We shall use the PGAUSS Algorithm for studying the output parameters.

Output Densities

For studying the evolution of distributions (on complex numbers), we are led to study the LFTs h used in the Gauss algorithm [Section "Returning to the Gauss Algorithm"], whose set is $\mathcal{G}$ for the PGAUSS Algorithm [Section "The LFTs Used by the PGAUSS Algorithm"]. We consider the two-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

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

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

$$J\underline{h}(x,y) = |h'(z) \cdot h'(\bar{z})| = |h'(z)|^2, \tag{3.40}$$

as h has real coefficients. Let us consider any measurable set $\mathcal{A} \subset \mathcal{F}$, and study the final density $\widehat{f}$ 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,

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

Using the expression of the Jacobian (3.40), and interchanging integral and sum lead to the equality

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

Finally, we have proven:

Theorem 5. (Vallée and Vera [45, 47] 2007) *The output density $\widehat{f}$ of each of the three algorithms satisfies the following:*

i. The output density $\widehat{f}$ of the PGAUSS *Algorithm on the fundamental domain $\mathcal{F}$ is expressed as a function of the input density f on $\mathcal{B} \setminus \mathcal{F}$ as*

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

where $\mathcal{G}$ is the set of LFTs used by the PGAUSS *algorithm described in Proposition 5.*

ii. The output density $\widehat{f}$ of the AGAUSS *Algorithm on the fundamental domain $\widetilde{\mathcal{F}}$ is expressed as a function of the input density f on $\widetilde{\mathcal{B}} \setminus \widetilde{\mathcal{F}}$ as*

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

where $\widetilde{\mathcal{G}}$ is the set of LFTs used by the AGAUSS *algorithm defined in Proposition 6.*

iii. The output density $\widehat{f}$ of the COREGAUSS *Algorithm on the domain $\widetilde{\mathcal{B}} \setminus \mathcal{D}$ can be expressed as a function of the input density f on $\mathcal{D}$ as*

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

where $\mathcal{H}$ is the set of LFTs used by each step of the COREGAUSS *algorithm defined in Proposition 6. and $\mathcal{H}^+ := \cup_{k \geq 1} \mathcal{H}^k$.*

Relation with Eisenstein Series

We now analyze an important particular case, where the initial density is the standard density of valuation r defined in (3.39). As each element of $\mathcal{G}$ gives rise to a unique pair (c, d) with $c \geq 1, \gcd(c, d) = 1$ [see Section "The LFTs Used by the PGAUSS Algorithm"] for which

$$|h'(\widehat{z})| = \frac{1}{|c\widehat{z} + d|^4}, \qquad f_r \circ \underline{h}(\widehat{x}, \widehat{y}) = \frac{1}{A(r)} \frac{\widehat{y}^r}{|c\widehat{z} + d|^{2r}}, \tag{3.41}$$

$$\text{the output density on } \mathcal{F} \text{ is } \quad \widehat{f}_r(\widehat{x}, \widehat{y}) = \frac{1}{A(r)} \sum_{\substack{(c,d)=1 \\ c \geq 1}} \frac{\widehat{y}^r}{|c\widehat{z} + d|^{4+2r}}. \tag{3.42}$$

It is natural to compare this density with the density relative to the measure relative to "random lattices" defined in Section "Random Lattices". In the particular case of two-dimensions, the fundamental domain for the action of $PSL_2(\mathbb{Z})$ on $\mathbb{H}$ equals $\mathcal{F}$ up to its frontier. 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 $|\Im(h(z))| = |\Im(z)| \cdot |h'(z)|$, so that

$$\iint_{h(\mathcal{A})} \frac{1}{y^2} \, \mathrm{d}x\mathrm{d}y = \iint_{\mathcal{A}} |h'(z)|^2 \frac{1}{\Im(h(z))^2} \, \mathrm{d}x\mathrm{d}y = \iint_{\mathcal{A}} \frac{1}{y^2} \, \mathrm{d}x\mathrm{d}y.$$

Then, the probability ν_2 defined in Section "Random Lattices" is exactly the measure on $\mathcal{F}$ of density

$$\eta(x,y) := \frac{3}{\pi}\frac{1}{y^2} \qquad \text{as} \qquad \iint_{\mathcal{F}} \frac{1}{y^2}\,\mathrm{d}x\mathrm{d}y = \frac{\pi}{3}. \tag{3.43}$$

If we make apparent this density η inside the expression of $\widehat{f_r}$ provided in (3.42), we obtain:

Theorem 6. (Vallée and Vera [45,47] 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 (3.39), 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 (3.43), the output density $\widehat{f_r}$ is expressed as*

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

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

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

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

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

Then, when r tends to -1, the output distribution relative to an input distribution, which is standard and of valuation r, tends to the distribution ν_2 relative to random lattices.

The series E_s are Mass forms (see for instance the book [8]): 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.

Geometry of the Output Parameters

The main output parameters are defined in (3.11,3.12). 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 $(z, \widehat{z})$.

Proposition 7. *If $z = x + iy$ is an initial complex number of $\mathcal{B} \setminus \mathcal{F}$ leading to a final complex $\widehat{z} = \widehat{x} + i\widehat{y}$ of $\mathcal{F}$, then the three main output parameters defined in (3.11) and (3.12) admit the following expressions:*

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

The following inclusions hold:

$$[\lambda(z) = t] \subset \left[\Im(z) \geq \frac{\sqrt{3}}{2}t^2\right], \qquad [\mu(z) = u] \subset \left[\Im(z) \leq \frac{2}{\sqrt{3}}u^2\right]. \tag{3.44}$$

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

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

Proof. If the initial pair (v_1, v_0) is written as in (3.4) as

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

then the total length decrease satisfies

$$\frac{|v_p|^2}{|v_0|^2} = \frac{|v_p|^2}{|cv_{p+1} + dv_p|^2} = \frac{1}{|c\widehat{z} + d|^2} = |h'(\widehat{z}), \tag{3.45}$$

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

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

easily lead to the result. ■

Domains Relative to the Output Parameters

We now consider the following well-known domains defined in Fig. 3.14. The Ford disk $\mathtt{Fo}(a,c,\rho)$ is a disk of center $(a/c, \rho/(2c^2))$ and radius $\rho/(2c^2)$: it is tangent to $y = 0$ at point $(a/c, 0)$. The Farey disk $\mathtt{Fa}(a,c,t)$ is a disk of center $(a/c, 0)$ and radius t/c. Finally, the angular sector $\mathtt{Se}(a,c,u)$ is delimited by two lines that 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. (Laville and Vallée [24] (1990), Vallée and Vera [45] (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 $\mathtt{Fo}(a,c,\rho)$, *Farey disks* $\mathtt{Fa}(a,c,t)$, *and angular sectors* $\mathtt{Se}(a,c,u)$. *More precisely, if* $\mathcal{F}_{(a,c)}$ *denotes the Festoon relative to pair* (a,c) *defined in (3.32) and if the set* $\mathcal{C}$ *is defined as in (3.31), one has:*

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

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

$$\mathtt{Fo}(a,c,\rho) := \left\{(x,y);\quad y>0,\quad \left(x-\frac{a}{c}\right)^2 + \left(y-\frac{\rho}{2c^2}\right)^2 \le \left(\frac{\rho}{2c^2}\right)^2\right\}$$

$$\mathtt{Fa}(a,c,t) := \left\{(x,y);\quad y>0,\quad \left(x-\frac{a}{c}\right)^2 + y^2 \le \left(\frac{t}{c}\right)^2\right\}$$

$$\mathtt{Se}(a,c,u) := \left\{(x,y);\quad y>0,\quad y \le \frac{|c|u}{\sqrt{1-c^2u^2}}\left|x-\frac{a}{c}\right|\right\} \qquad \text{for } |c|u<1$$

$$\mathtt{Se}(a,c,u) := \{(x,y);\quad y>0,\} \qquad \text{for } |c|u \ge 1$$

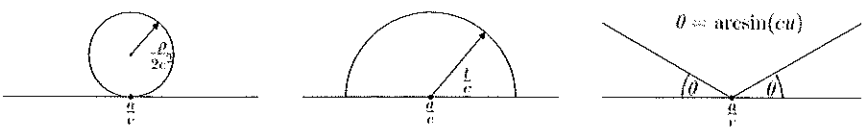

Fig. 3.14 The three main domains of interest: the Ford disks $\mathtt{Fo}(a,c,\rho)$, the Farey disks $\mathtt{Fa}(a,c,t)$, and the angular sectors $\mathtt{Se}(a,c,u)$

Each of these descriptions of Λ, Γ, M can be transformed in a description that no more involves the festoons. It involves, for instance, a subfamily of Farey disks (for Λ), or a subfamily of angular sectors (for M) [see Fig. 3.15].

Consider the set $\mathcal{P} := \{(c,d);\ \ c,d \geq 1, (c,d) = 1\}$, already used in Section "The LFTs Used by the PGAUSS Algorithm", and its subset $\mathcal{P}(t)$ defined as

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

Consider a pair $(c,d) \in \mathcal{P}(t)$. There exists a unique pair (a,b) for which the rationals a/c and b/d belong to $[-1/2, +1/2]$ and satisfy $ad - bc = 1$. We then associate to the pair (c,d) the intersection of the vertical strip $\{(x,y);\ \ (a/c) \leq x \leq (b/d)\}$ with $\mathcal{B} \setminus \mathcal{F}$, and we denote it by $\mathcal{S}(c,d)$. Remark that the definition of $\mathcal{P}(t)$ implies that the only rationals of the strip $\mathcal{S}(c,d)$ with a denominator at most $(1/t)$ are a/c and b/d.

Domain $\Lambda(t)$. For any $t > 0$ and any pair $(c,d) \in \mathcal{P}(t)$, there exists a characterization of the intersection of the domain $\Lambda(t)$ with the vertical strip $\mathcal{S}(c,d)$, provided in [24], which does not depend any longer on the festoons, namely

$$\Lambda(t) \cap \mathcal{S}(c,d) = \underline{\mathtt{Fa}}(a,c,t) \cup \underline{\mathtt{Fa}}(b,d,t) \cup \mathtt{Fa}(a+b, c+d, t). \tag{3.46}$$

Here, the pair (a,b) is the pair associated to (c,d), the domains $\underline{\mathtt{Fa}}(a,c,t)$, $\underline{\mathtt{Fa}}(b,d,t)$ are the intersections of Farey disks $\mathtt{Fa}(a,c,t)$, $\mathtt{Fa}(b,d,t)$ with the strip $\mathcal{S}(c,d)$. The domain in (3.46) is exactly the union of the two disks $\underline{\mathtt{Fa}}(a,c,t)$ and $\underline{\mathtt{Fa}}(b,d,t)$ if and only if the condition $(c^2+d^2+cd)t^2 \geq 1$ holds, but the Farey disk relative to the median $(a+b)/(c+d)$ plays a rôle otherwise. The proportion of pairs $(c,d) \in \mathcal{P}(t)$ for which the condition $(c^2+d^2+cd)t^2 \geq 1$ holds tends to $2 - (2\pi)/(3\sqrt{3}) \approx 0.7908$ when $t \to 0$.

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

$$\bigcup_{\substack{(a,c)\in\mathcal{C}\\ c\leq 1/(2t)}} \mathtt{Fa}(a,c,t) \subset \Lambda(t) \subset \bigcup_{\substack{(a,c)\in\mathcal{C}\\ c\leq 2/(\sqrt{3}t)}} \mathtt{Fa}(a,c,t). \tag{3.47}$$

Domain $M(u)$. For any $u > 0$ and any pair $(c,d) \in \mathcal{P}(u)$, there exists a characterization of the intersection of the domain $M(u)$ with the vertical strip $\mathcal{S}(c,d)$, provided in [47], which does not depend any longer on the festoons, namely

$$M(u) \cap \mathcal{S}(c,d) = \underline{\mathtt{Se}}(a,c,u) \cap \underline{\mathtt{Se}}(b,d,u) \cap \mathtt{Se}(b-a, d-c, u). \tag{3.48}$$

Here, the pair (a,b) is the pair associated to (c,d), the domains $\underline{\mathtt{Se}}(a,c,u)$, $\underline{\mathtt{Se}}(b,d,u)$ are the intersections of $\mathtt{Se}(a,c,u)$, $\mathtt{Se}(b,d,u)$ with the strip $\mathcal{S}(c,d)$. The domain in (3.48) is exactly the triangle $\underline{\mathtt{Se}}(a,c,u) \cap \underline{\mathtt{Se}}(b,d,u)$ if and only if one of the two conditions $(c^2+d^2-cd)u^2 \leq (3/4)$ or $cd\,u^2 \leq (1/2)$ holds, but this is a "true" quadrilateral otherwise. The proportion of pairs $(c,d) \in \mathcal{P}(u)$ for

which the condition $[(c^2 + d^2 - cd)u^2 \leq (3/4) \text{ or } cd\,u^2 \leq (1/2)]$ holds tends to $(1/2) + (\pi\sqrt{3}/12) \approx 0.9534$ when $u \to 0$.

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. We first present the main constants that will intervene in our results.

Constants of the Analysis

The measure of a disk of radius ρ centered on the real axis equals $2A_2(r)\,\rho^{r+2}$. The measure of a disk of radius ρ tangent to the real axis equals $A_1(r)\,(2\rho)^{r+2}$. Such measures involve constants $A_1(r)$, $A_2(r)$, which are expressed with the β law, already defined in (3.21) as

$$A_1(r) := \frac{\sqrt{\pi}}{A(r)}\frac{\Gamma(r+3/2)}{\Gamma(r+3)}, \qquad A_2(r) := \frac{\sqrt{\pi}}{2A(r)}\frac{\Gamma((r+1)/2)}{\Gamma(r/2+2)}. \tag{3.49}$$

For a triangle with basis a on the real axis and height h, this measure equals $A_3(r)\,a\,h^{r+1}$, and involves the constant

$$A_3(r) := \frac{1}{A(r)}\frac{1}{(r+2)(r+1)}. \tag{3.50}$$

For (α, β) that belongs to the triangle $\mathcal{T} := \{(\alpha,\beta); 0 < \alpha, \beta < 1, \alpha + \beta > 1\}$, we consider the continuous analogs of the configurations previously described:

Disks. We consider the figure obtained with three disks D_α, D_β, $D_{\alpha+\beta}$ when these disks satisfy the following: For any $\delta, \eta \in \{\alpha, \beta, \alpha + \beta\}$, the center x_δ is on the real axis, the distance between x_δ and x_η equals $1/(\delta\eta)$ and the radius of D_δ equals $1/\delta$. We can suppose $x_\alpha < x_{\alpha+\beta} < x_\beta$. Then, the configuration $D(\alpha, \beta)$ is defined by the intersection of the union $\cup_\delta D_\delta$ with the vertical strip $\langle x_\alpha, x_\beta\rangle$. The constant $A_4(r)$ is defined as the integral

$$A_4(r) = \frac{1}{A(r)}\iint_{\mathcal{T}} \mathrm{d}\alpha\mathrm{d}\beta \left(\iint_{D(\alpha,\beta)} y^r\,\mathrm{d}x\mathrm{d}y\right). \tag{3.51}$$

Sectors. In the same vein, we consider the figure obtained with three sectors $S_\alpha, S_\beta, S_{\beta-\alpha}$ when these sectors satisfy the following:[7] for any $\delta \in \{\alpha, \beta, \beta-\alpha\}$, the sector S_δ is delimited by two half lines, the real axis (with a positive orientation) and another half-line, that intersect at the point x_δ of the real axis. For any $\delta, \eta \in \{\alpha, \beta, \beta-\alpha\}$, the distance between x_δ and x_η equals $1/(\delta\eta)$. We can suppose $x_{\beta-\alpha} < x_\alpha < x_\beta$; in this case, the angle of the sector S_δ equals $\arcsin\delta$ for $\delta \in \{\beta-\alpha, \alpha\}$ and equals $\pi - \arcsin\delta$ for $\delta = \beta$. The configuration $S(\alpha, \beta)$ is defined by the intersection of the intersection $\cap_\delta S_\delta$ with the vertical strip $\{x_\alpha, x_\beta\}$. The constant $A_5(r)$ is defined as the integral

$$A_5(r) = \frac{1}{A(r)} \iint_{\mathcal{T}} \mathrm{d}\alpha\mathrm{d}\beta \left(\iint_{S(\alpha,\beta)} y^r \, \mathrm{d}x\mathrm{d}y \right). \tag{3.52}$$

Theorem 8. (Vallée and Vera [45,47] 2007) *When the initial density on $\mathcal{B} \setminus \mathcal{F}$ is the standard density of valuation r, the distribution of the three main output parameters involves the constants $A_i(r)$ defined in (3.49), (3.50), (3.51), and (3.52) and satisfies the following:*

1. *For parameter γ, there is an exact formula for any valuation r and any $\rho \leq 1$,*

$$\mathbb{P}_{(r)}[\gamma(z) \leq \rho] = A_1(r) \cdot \frac{\zeta(2r+3)}{\zeta(2r+4)} \cdot \rho^{r+2} \quad \textit{for} \quad \rho \leq 1$$

2. *For parameter λ, there are precise estimates for any fixed valuation $r > -1$, when $t \to 0$,*

$$\mathbb{P}_{(r)}[\lambda(z) \leq t] \sim_{t\to 0} \frac{\zeta(r+1)}{\zeta(r+2)} A_2(r) \cdot t^{r+2} \textit{ for} \quad r > 0,$$

$$\mathbb{P}_{(r)}[\lambda(z) \leq t] \sim_{t\to 0} \frac{1}{\zeta(2)} A_2(0) \cdot t^2 |\log t| \textit{ for} \quad r = 0,$$

$$\mathbb{P}_{(r)}[\lambda(z) \leq t] \sim_{t\to 0} \frac{1}{\zeta(2)} A_4(r) \cdot t^{2r+2} \quad \textit{for} \quad r < 0.$$

Moreover, for any fixed valuation $r > -1$ and any $t > 0$, the following inequality holds

$$\mathbb{P}_{(r)}[\lambda(z) \leq t] \geq \frac{1}{A(r)} \frac{1}{r+1} \left(\frac{\sqrt{3}}{2} \right)^{r+1} t^{2r+2}. \tag{3.53}$$

3. *For parameter μ, there is a precise estimate for any fixed valuation $r > -1$, when $u \to 0$,*

[7] The description is given in the case when $\beta > \alpha$.

$$\mathbb{P}_{(r)}[\mu(z) \le u] \sim_{u\to 0} \frac{1}{\zeta(2)} A_5(r) \cdot u^{2r+2}.$$

Moreover, for any fixed valuation $r > -1$ and any $u > 0$, the following inequalities hold:

$$A_3(r) \left(\frac{\sqrt{3}}{2}\right)^{r+1} \cdot u^{2r+2} \le \mathbb{P}_{(r)}[\mu(z) \le u] \le A_3(r) \cdot u^{2r+2}. \tag{3.54}$$

Proof. [Sketch] If φ denotes the Euler quotient function, there are exactly $\varphi(c)$ coprime pairs (a, c) with $a/c \in]-1/2, +1/2]$. Then, the identity

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

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

(*a*) For $\rho \le 1$, 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 (3.47) entail the following inequalities

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

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

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

(which has a pôle at $s = -r$), and classical estimates entail an estimate for

$$\sum_{c\le N} \frac{\varphi(c)}{c^{r+2}} \sim_{N\to\infty} \frac{1}{\zeta(2)} \frac{N^{-r}}{|r|}, \text{ (for } r < 0), \text{ and } \sum_{c\le N} \frac{\varphi(c)}{c^2} \sim_{N\to\infty} \frac{1}{\zeta(2)} \log N.$$

For domain $M(u)$, the study of quadrilaterals can be performed in a similar way. Furthermore, the height of each quadrilateral of $M(u)$ is $\Theta(u^2)$, and the sum of the bases a equal 1. Then $\mathbb{P}_{(r)}[\mu(z) \le u] = \Theta(u^{2r+2})$. Furthermore, using the inclusions of (3.44) leads to the inequality. ■

Interpretation of the Results

We provide a first interpretation of the main results described in Theorem 8.

1. For any $y_0 \geq 1$, the probability of the event $[\widehat{y} \geq y_0]$ is

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

   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 $\widehat{f_r}$ of Theorem 6 via the equality

$$\psi_r'(y_0) := \int_{-1/2}^{+1/2} \widehat{f_r}(x, y_0)\, \mathrm{d}x.$$

   Now, when $r \to -1$, the function $\psi_r'(y)$ has a limit, which is exactly the density η, defined in (3.43), which is associated to the Haar measure ν_2 defined in Sections "Random Lattices and Relation with Eisenstein Series".
2. The regime of the distribution function of parameter λ changes when the sign of valuation r changes. There are two parts in the domain $A(t)$: 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 $A(t)$ 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, it is the upper part that 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.
3. 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.
4. The bounds (3.53, 3.54) prove that for any $u, t \in [0, 1]$, the probabilities $\mathbb{P}[\lambda(z) \leq t]$, $\mathbb{P}[\mu(z) \leq u]$ tend to 1, when the valuation r tends to -1. This shows that the limit distributions of λ and μ are associated to the Dirac measure at 0.
5. It is also possible to conduct these studies in the discrete model defined in Section "Probabilistic Models for Two-Dimensions". It is not done here, but this type of analysis will be performed in the following section.

Open question. Is it possible to describe the distribution function of parameter γ for $\rho > 1$? Figure 3.15 [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 "A Variation for the LLL Algorithm: The Odd-Even Algorithm".

The corners of the fundamental domain. With Theorem 8, 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 Fig. 3.4 [right].

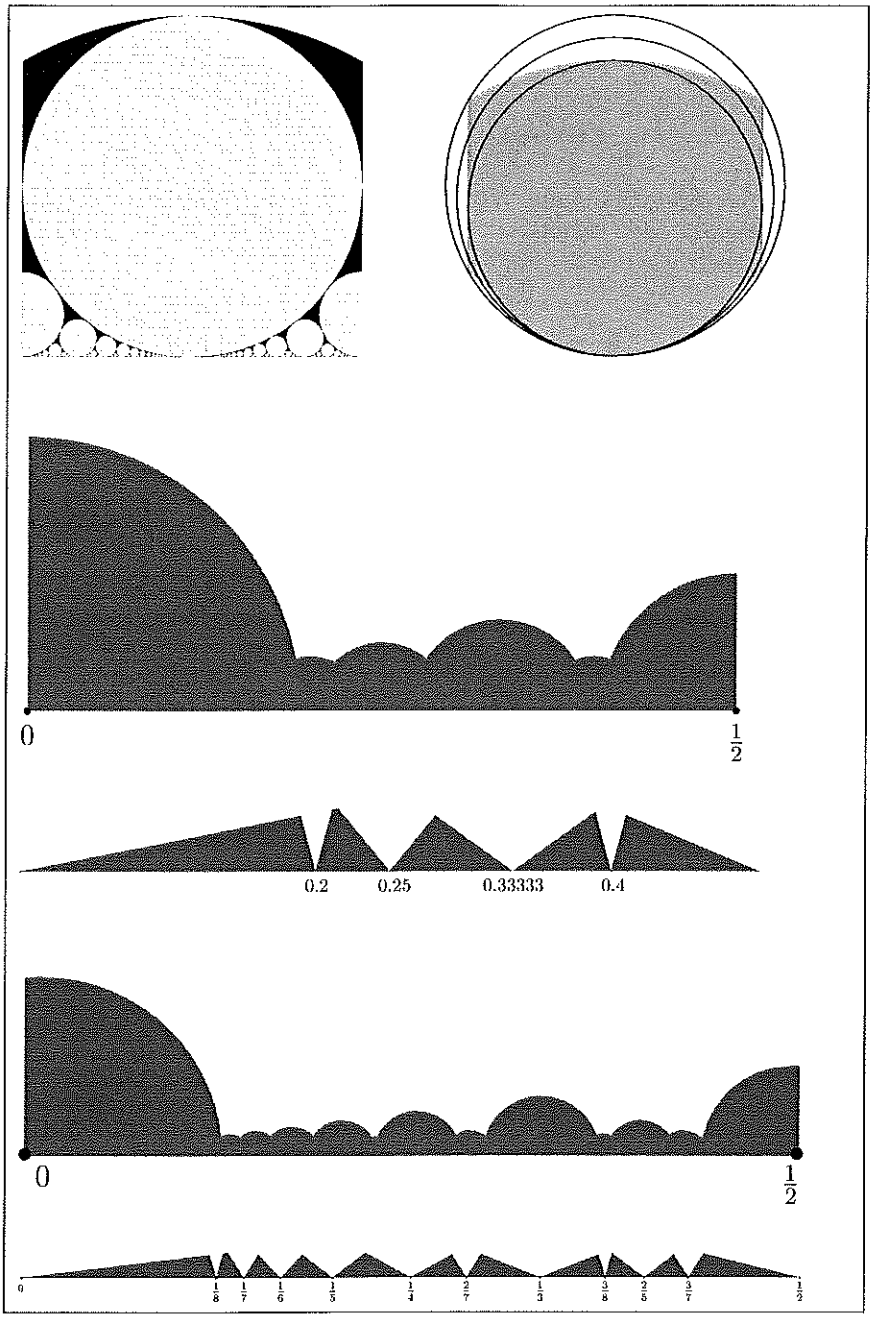

Fig. 3.15 Above: the domain $\Gamma(\rho) := \{z;\ \gamma(z) \leq \rho\}$. On the *left*, $\rho = 1$ (in *white*). On the *right*, the domain $\mathcal{F}_{(0,1)} \cap \mathrm{Fo}(0, 1, \rho)$ for $\rho = 1, \rho_0 = 2/\sqrt{3}, \rho_1 = (1 + \rho_0)/2$. – In the *middle*: the domain $\Lambda(t) \cap \mathcal{B}_+$, with $\Lambda(t) := \{z;\ \lambda(z) \leq t\}$ and the domain $M(u) \cap \mathcal{B}_+$ with $M(u) := \{z;\ \mu(z) \leq u\}$ for $u = t = 0.193$.– Below: the same domains for $u = t = 0.12$

Proposition 8. *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 Section "Distribution Functions of Output Parameters: Case of Densities with Valuations". There are three main cases of interest for $1 - C(r)$, namely

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

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 $\mathrm{Fo}(a, c, \rho)$ with the line $y = y_0$ is nonempty 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 $\mathrm{Fo}(a, c, \rho)$ are disjoint and

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

and $g(t) = \sqrt{1 - t^2}$. For any function g smooth enough, one has

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

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

A Related Result which also Deals with Farey Disks

For analyzing integer factoring algorithms, Vallée was led in 1988 to study the set of "small quadratic residues" defined as

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

and its distribution in $[1..N]$. She described in [43,44] a polynomial–time algorithm, called the Two-Thirds Algorithm, which draws elements from $\mathcal{B}$ in a quasi-uniform way.[8] 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 [13], 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 that 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 and made more precise by Gentry, is to perform a local study of the set $\mathcal{B}$. In this way, she refines ideas of the work done in [46]. This last work was one of the first works that relates general small modular equations to lattices, and was further generalized ten years later by Coppersmith [11]. 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 following two conditions are equivalent:

1. $x = x_0 + u$ belongs to $\mathcal{B}$
2. There exists w such that the point (w, u) belongs to $\underline{L}(x_0)$ and lies between two parabolas with respective equations

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

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 Section "Domains Relative to the Output Parameters", we know that these objects are central in such a result.

Analysis of the Execution Parameters of the Gauss Algorithm

We finally focus on parameters that 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 deal here with the

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

COREGAUSS algorithm, using the decomposition provided in Section "Returning to the Gauss Algorithm" Proposition 6.

Dynamical Systems

A dynamical system is a pair formed by a 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 deal with the 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 $W^p(x) \in Y$.

We will study here two dynamical systems, respectively, related to the F-EUCLID algorithm and to the COREGAUSS algorithm, previously defined (in an informal way) in Section "Returning to the Gauss Algorithm".

Case of the F-EUCLID Algorithm. Here, X is the interval $\widetilde{\mathcal{I}} = [0, 1/2]$. The map W is the map $\widetilde{V}$ defined in Section "Relation with the Centered Euclid Algorithm". The set $\mathcal{Q}$ of digits is the set of pairs $q = (m, \varepsilon)$ with the condition $(m, \varepsilon) \geq (2, +1)$ (with respect to the lexicographic order). The inverse branch $h_{\langle m,\varepsilon\rangle}$ is a LFT, defined as $h_{\langle m,\varepsilon\rangle}(z) = 1/(m + \varepsilon z)$. The topological partition is defined by $X_{\langle m,\varepsilon\rangle} = h_{\langle m,\varepsilon\rangle}(\widetilde{\mathcal{I}})$.

Case of the COREGAUSS Algorithm. Here, X is the vertical strip $\widetilde{\mathcal{B}}$. The map W is equal to the identity on $\widetilde{\mathcal{B}} \setminus \mathcal{D}$ and coincides with the map $\widetilde{U}$ defined in Section "The Complex Versions for the GAUSS Algorithms" otherwise. The set $\mathcal{Q}$ of digits is the set of pairs $q = (m, \varepsilon)$ with the condition $(m, \varepsilon) \geq (2, +1)$ (with respect to the lexicographic order). The inverse branch $h_{\langle m,\varepsilon\rangle}$ is a LFT defined as $h_{\langle m,\varepsilon\rangle}(z) = 1/(m + \varepsilon z)$. The topological partition is defined by $X_{\langle m,\varepsilon\rangle} = h_{\langle m,\varepsilon\rangle}(\widetilde{\mathcal{B}})$ and drawn in Fig. 16. The system has a hole, namely $\widetilde{\mathcal{B}} \setminus \mathcal{D}$.

Transfer Operators

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 behavior of typical trajectories of dynamical systems

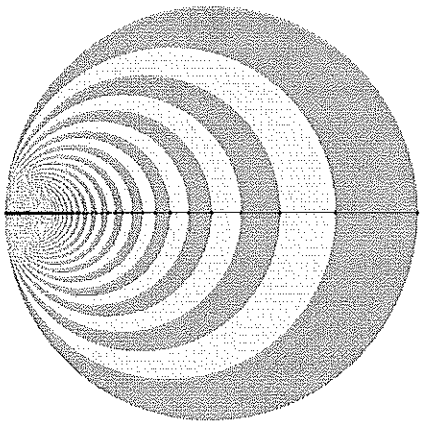

Fig. 3.16 The topological partitions of the CoreGauss dynamical system. The intersection of this partition with the real axis gives rise to the topological partition of the F-Euclid dynamical system

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 $f_0, f_1, f_2, \ldots, f_n, \ldots$ describe the global evolution of the system at discrete times $t = 0$, $t = 1$, $t = 2$, ...

Consider the (elementary) operator $\mathbf{X}_{s,[h]}$, relative to an inverse branch $h \in \mathcal{H}$, which acts on functions $f : X \to \mathbb{R}$, depends on some parameter s, and is formally defined as

$$\mathbf{X}_{s,[h]}[f](x) = J(h)(x)^s \cdot f \circ h(x), \quad \text{where } J(h) \text{ is the Jacobian of branch } h. \tag{3.55}$$

The operator $\mathbf{X}_{1,[h]}$ expresses the part of the new density f_1, which is brought when the algorithm uses the branch h, and the operator that takes into account all the inverse branches of the set $\mathcal{H}$, defined as

$$\mathbf{H}_s := \sum_{h \in \mathcal{H}} \mathbf{X}_{s,[h]}, \tag{3.56}$$

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 $f_1 = \mathbf{H}[f_0]$. The operators defined in (3.56) are called transfer operators. For $s = 1$, they coincide with density transformers, and for other values of s, they can be viewed as extensions of density transformers. They play a central rôle in studies of dynamical systems.

We will explain how transfer operators are a convenient tool for studying the evolution of the densities, in the two systems of interest.

Case of the F-EUCLID **system.** This system is defined on an interval, and the Jacobian $J(h)(x)$ is just equal to $|h'(x)|$. Moreover, because of the precise expression of the set $\mathcal{H}$, one has, for any $x \in \widetilde{\mathcal{I}} = [0, 1/2]$,

$$\mathbf{H}_s[f](x) = \sum_{(m,\varepsilon)\geq(2,1)} \left(\frac{1}{m+\varepsilon x}\right)^{2s} \cdot f\left(\frac{1}{m+\varepsilon x}\right). \tag{3.57}$$

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 "Functional Analysis".

Case of the COREGAUSS **algorithm.** We have seen in Section "Output Densities" that the Jacobian of the transformation $(x, y) \mapsto \underline{h}(x, y) = (\Re h(x + iy), \Im h(x + iy))$ equals $|h'(x + iy)|^2$. It would be natural to consider an (elementary) transfer 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 LFTs that intervene in one step of the COREGAUSS algorithm, and viewed at $s = 2$, describes the new density that is brought at each point $z \in \widetilde{\mathcal{B}} \setminus \mathcal{D}$ during this step, when the density on $\mathcal{D}$ is f.

However, such an operator does not possess "good" properties, because the map $z \mapsto |h'(z)|$ is not analytic. It is more convenient to introduce another elementary operator $\underline{\mathbf{X}}_{s,[h]}$, which acts on functions F of two variables, and is defined as

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

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, which relate $F(z, u)$ and its diagonal f defined by $f(z) := F(z, \bar{z})$,

$$\underline{\mathbf{X}}_{s,[h]}[F](z, \bar{z}) = \mathbf{Y}_{s,[h]}[f](z), \quad \underline{\mathbf{X}}_{s,[h]}[F](x, x) = \mathbf{X}_{s,[h]}[f](x) \tag{3.58}$$

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 $f(z) = F(z, \bar{z})$, where $F(z, u) = |z - u|^r L(z, u)$ involves an analytic function L, which is nonzero on the diagonal $z = u$, one has

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

Finally, for the COREGAUSS Algorithm, we shall deal with the operator $\underline{\mathbf{H}}_s$ defined as $\underline{\mathbf{H}}_s = \sum_{h\in\mathcal{H}} \underline{\mathbf{X}}_{s,[h]}$, which, in this case, admits a nice expression

$$\underline{\mathbf{H}}_s[F](z,u) = \sum_{(m,\varepsilon)\geq(2,1)} \left(\frac{1}{m+\varepsilon z}\right)^s \left(\frac{1}{m+\varepsilon u}\right)^s \cdot F\left(\frac{1}{m+\varepsilon z}, \frac{1}{m+\varepsilon u}\right). \tag{3.59}$$

Because of (3.58), this is an extension of the operator $\mathbf{H}_s$, defined in (3.57), which satisfies the equality

$$\underline{\mathbf{H}}_s[F](x,x) = \mathbf{H}_s[f](x), \qquad \text{when } f \text{ is the diagonal map of } F.$$

The operators $\mathbf{X}_{s,[h]}$, underlined or not, satisfy a crucial relation of composition due to multiplicative properties of the derivative of $g \circ h$. We easily remark that

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

We recall that the set $\mathcal{H}^+ = \cup_{k>0}\mathcal{H}^k$ is the set of the transformations describing the whole executions of our two algorithms of interest. Then, the transfer operator relative to $\mathcal{H}^+$, denoted by $\mathbf{G}_s$ (for the EUCLID Algorithm) or $\underline{\mathbf{G}}_s$ (for the COREGAUSS Algorithm), satisfies

$$\mathbf{G}_s = \mathbf{H}_s \circ (I - \mathbf{H}_s)^{-1} \qquad \text{or} \qquad \underline{\mathbf{G}}_s = \underline{\mathbf{H}}_s \circ (I - \underline{\mathbf{H}}_s)^{-1}, \tag{3.60}$$

and the assertion (3) of Theorem 6 can be re-written as

Theorem 9. [Dynamical version of Theorem 6]. *Consider the* COREGAUSS *algorithm, with its input density f on $\mathcal{D}$ and its output density $\widehat{f}$ on $\widetilde{\mathcal{B}} \setminus \mathcal{D}$, viewed as functions of two complex variables $z, \bar{z}$, namely $f(x,y) = F(z,\bar{z})$, $\widehat{f}(x,y) = \widehat{F}(z,\bar{z})$.*
Then, one has $\widehat{F} = \underline{\mathbf{G}}_2[F]$, where the operator $\underline{\mathbf{G}}_2$ is the "total" density transformer of the COREGAUSS *algorithm, which is related to the density transformer $\underline{\mathbf{H}}_2$ via the equality $\underline{\mathbf{G}}_2 = \underline{\mathbf{H}}_2 \circ (I - \underline{\mathbf{H}}_2)^{-1}$. When the input density F is of type (r, L), then the equality $\widehat{F}(z,\bar{z}) = y^r \underline{\mathbf{G}}_{2+r}[L]$ holds.*

Consider the COREGAUSS algorithm with an initial density, standard of valuation r. Such a density is defined on the input disk $\mathcal{D}$ and involves constant $A_0(r)$ [related with constant $A_2(r)$ defined in (3.49)] under the form

$$\frac{y^r}{A_0(r)} \qquad \text{with} \quad A_0(r) = \frac{1}{4^{r+2}} A_2(r) = \frac{\sqrt{\pi}}{4^{r+2}} \frac{\Gamma((r+1)/2)}{\Gamma(r/2+2)}. \tag{3.61}$$

Remark that $A_0(r) \sim 1/(r+1)$ when $r \to -1$. Then, the Hurwitz characterization provided in Proposition 6 gives rise to a nice expression for the output density $\widehat{F}$ in the case of a standard input density of valuation r, namely

$$\widehat{F}_r(z,\bar{z}) = \frac{1}{A_0(r)} \frac{1}{\zeta(2r+4)} \sum_{\substack{c,d\geq 1 \\ d\phi<c<d\phi^2}} \frac{y^r}{|cz+d|^{2r+4}}.$$

Execution Parameters in the Complex Framework

We are now interested in the study of the following costs:

1. Any additive cost $C_{(c)}$, defined in (3.9), relative to a cost c of moderate growth. There are two particular cases of interest: the number of iterations P, relative to $c = 1$, and the length Q of the continued fraction, relative to the case when c is the binary length ℓ,
$$Q(u, v) = \sum_{i=1}^{P(u,v)} \ell(|q_i|).$$

2. The bit-complexity B defined in Section "Main Parameters of Interest". It is explained (see 3.8) that the cost B decomposes as
$$B(u, v) = Q(u, v)\, \ell(|u|^2) + D(u, v) + \Theta\left(Q(u, v)\right), \tag{3.62}$$
where Q is the length of the continued fraction, already studied in (1), and cost D is defined by
$$D(u, v) = 2 \sum_{i=1}^{P(u,v)} \ell(|q_i|) \lg \left| \frac{v_{i-1}}{v} \right|.$$
It is then sufficient to study costs Q and D.

All these costs are invariant by similarity, that is, $X(\lambda u, \lambda v) = X(u, v)$ for $X \in \{Q, D, P\}$ and $\lambda \in \mathbb{C}^*$. 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. We first provide precise expressions for all these costs in the complex framework.

An additive cost $C_{(c)}$, defined more precisely in (3.9), is related to an elementary cost c defined on quotients q. Such a cost can be defined on $\mathcal{H}$ via the equality $c(h) = c(q)$ for $h = h_{\langle q \rangle}$, and is extended to the total set of LFTs 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 an input $z \in \mathcal{D}$ leads to an output $\widehat{z} \in \widetilde{\mathcal{B}} \setminus \mathcal{D}$ by using the LFT $h \in \mathcal{G}$ with $z = h(\widehat{z})$, then $C(z)$ equals $c(h)$.

In the same vein as in (3.45), the ith length decrease can be expressed with the derivative of the LFT $g_i := h_i^{-1}$ (with h_i defined in (3.33)) as

$$\frac{|v_i|^2}{|v_0|^2} = \frac{1}{|g_i'(z)|} = |c_i z - a_i|^2 \text{ so that } 2 \lg \left(\frac{|v_i|}{|v_0|} \right) = -\lg |g_i'(z)| = -\lg |c_i z - a_i|^2,$$

where a_i, c_i are coefficients of the LFT h_i. Finally, the complex versions of cost D is

$$D(z) = \sum_{i=1}^{P(z)} \ell(|q_i|) \lg |h_{i-1}'(z_{i-1})| = -2 \sum_{i=1}^{P(z)} \ell(|q_i|) \lg |c_{i-1} z - a_{i-1}|. \tag{3.63}$$

The main idea of the dynamical analysis methodology is to use the transfer operators (introduced for studying dynamical systems) in the analysis of algorithms; for this aim, we modify the operators $\underline{\mathbf{X}}_{s,[h]}$ defined in Section "Transfer Operators" in such a way that they become "generating operators" that play the same role as generating functions in analytic combinatorics. In fact, these operators generate themselves... generating functions of the main costs of interest.

Generating Operators for Additive Costs C and Cost D

We now explain how to modify transfer operator in the two main cases: additive cost C and cost D.

Case of additive costs. It is natural to add a new parameter w inside the transfer operator $\underline{\mathbf{X}}_{s,[h]}$ for "marking" the cost: we consider the two-parameters 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 $w = 0$ or $c = 0$, we recover the operator $\underline{\mathbf{X}}_{2s,[h]}$. When the cost c is additive, that is, $c(g \circ h) = c(g) + c(h)$, 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, an extension of (3.60) as

$$\underline{\mathbf{G}}_{s,w,(c)} = \underline{\mathbf{H}}_{s,w,(c)} \circ (I - \underline{\mathbf{H}}_{s,w,(c)})^{-1}, \tag{3.64}$$

where the operators $\underline{\mathbf{G}}_{s,w,(c)}, \underline{\mathbf{H}}_{s,w,(c)}$ are defined in the same vein as in (3.56). In particular,

$$\underline{\mathbf{H}}_{s,w,(c)}[F](z,u) = \sum_{(m,\varepsilon)\geq(2,1)} \exp[wc(m,\varepsilon)] \left(\frac{1}{m+\varepsilon z}\right)^s \left(\frac{1}{m+\varepsilon u}\right)^s \tag{3.65}$$

$$\cdot F\left(\frac{1}{m+\varepsilon z}, \frac{1}{m+\varepsilon u}\right). \tag{3.66}$$

The operator $\underline{\mathbf{G}}_{s,w,(c)}$ generates the moment generating function of the cost $C_{(c)}$, as we will see now. The moment generating function $\mathbb{E}_{(f)}(\exp[wC_{(c)}])$ is defined as

$$\mathbb{E}_{(f)}(\exp[wC_{(c)}]) := \sum_{h\in\mathcal{H}^+} \exp[wc(h)] \cdot \mathbb{P}_{(f)}[C = c(h)]$$

$$= \sum_{h\in\mathcal{H}^+} \exp[wc(h)] \iint_{h(\widetilde{\mathcal{B}}\setminus\mathcal{D})} \underline{f}(x,y)\,\mathrm{d}x\mathrm{d}y.$$

Using a change of variables and the expression of the Jacobian leads to

$$\mathbb{E}_{(f)}(\exp[wC_{(c)}]) = \sum_{h\in\mathcal{H}^+} \exp[wc(h)] \iint_{\widetilde{\mathcal{B}}\setminus\mathcal{D}} |h'(z)|^2 f(h(z), h(\bar{z}))\,\mathrm{d}x\mathrm{d}y$$

$$= \iint_{\widetilde{\mathcal{B}}\setminus\mathcal{D}} \underline{\mathbf{G}}_{2,w,(c)}[f](z,\bar{z})\,\mathrm{d}x\mathrm{d}y.$$

Now, when the density F is of type (r, L), using relation (3.41) leads to

$$\mathbb{E}_{(f)}(\exp[wC_{(c)}]) = \iint_{\widetilde{\mathcal{B}}\setminus\mathcal{D}} y^r\, \underline{\mathbf{G}}_{2+r,w,(c)}[L](z,\bar{z})\,\mathrm{d}x\mathrm{d}y. \tag{3.67}$$

The expectation $\mathbb{E}_{(f)}[C_{(c)}]$ is just obtained by taking the derivative with respect to w (at $w = 0$). This is why we introduce the functional $W_{(c)}$, which takes the derivative with respect to w, at $w = 0$. It then "weights" the operator $\underline{\mathbf{X}}_{s,[h]}$ with the cost $c(h)$, as

$$W_{(c)}\mathbf{X}_{s,[h]} := \frac{\partial}{\partial w}\underline{\mathbf{X}}_{s,w,(c),[h]}|_{w=0} = c(h)\mathbf{X}_{s,[h]}.$$

When extended via linearity, it defines the generating operator of cost C as

$$\underline{\mathbf{G}}_{s,C} := W_{(c)}[\underline{\mathbf{G}}_s] = W_{(c)}\left[\underline{\mathbf{H}}_s \circ (I - \underline{\mathbf{H}}_s)^{-1}\right]. \tag{3.68}$$

This provides an alternative expression for the expectation of any additive cost:

$$\mathbb{E}_{(f)}[C_{(c)}] = \iint_{\widetilde{\mathcal{B}}\setminus\mathcal{D}} \underline{\mathbf{G}}_{2,C}[F](z,\bar{z})\,\mathrm{d}x\mathrm{d}y = \iint_{\widetilde{\mathcal{B}}\setminus\mathcal{D}} y^r\, \underline{\mathbf{G}}_{2+r,C}[L](z,\bar{z})\,\mathrm{d}x\mathrm{d}y, \tag{3.69}$$

the last equality holding for a density F of type (r, L).

Case of Cost D. Remark that, in (3.63), the quantity $\lg|h_i'(z_i)|\cdot|h_i'(z)|^s$ is just the derivative of $(1/\log 2)|h_i'(z)|^s$ with respect to s. This is why we introduce another functional Δ, in the same vein as previously, where the functional W relative to the cost was introduced. To an operator $\underline{\mathbf{X}}_{s,[h]}$, we associate an operator $\Delta\underline{\mathbf{X}}_{s,[h]}$ defined as

$$\Delta\underline{\mathbf{X}}_{s,[h]} = \frac{1}{\log 2}\frac{\partial}{\partial s}\underline{\mathbf{X}}_{s,[h]}.$$

The functional Δ weights the operator $\underline{\mathbf{X}}_{s,[h]}$ with the weight $-\lg|h'|$.

Now, with the help of these two functionals $W := W_{(\ell)}$ and Δ, we can build the generating operator for D. 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

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

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

$$\underline{\mathbf{G}}_{s,D} := (I - \underline{\mathbf{H}}_s)^{-1} \circ W\,[\underline{\mathbf{H}}_s] \circ \Delta\left[(I - \underline{\mathbf{H}}_s)^{-1}\right],$$

$$\underline{\mathbf{G}}_{s,D} = (I - \underline{\mathbf{H}}_s)^{-1} \circ W\,[\underline{\mathbf{H}}_s] \circ (I - \underline{\mathbf{H}}_s)^{-1} \circ \Delta\,[\underline{\mathbf{H}}_s] \circ (I - \underline{\mathbf{H}}_s)^{-1}, \tag{3.70}$$

which is the "generating operator" of the cost $D(z)$, as the equalities hold,

$$\mathbb{E}_{(f)}[D] := \iint_{\mathcal{D}} D(z)\, F(z,\bar{z})\, \mathrm{d}x\mathrm{d}y,$$

$$= \iint_{\widetilde{\mathcal{B}}\setminus\mathcal{D}} \underline{\mathbf{G}}_{2,D}[F](z,\bar{z})\, \mathrm{d}x\mathrm{d}y = \iint_{\widetilde{\mathcal{B}}\setminus\mathcal{D}} y^r\, \underline{\mathbf{G}}_{2+r,D}[L](z,\bar{z})\, \mathrm{d}x\mathrm{d}y, \tag{3.71}$$

the last equality holding for a density F of type (r, L).

Case of costs C, B in the Euclid Algorithm. These functionals W, Δ are also central in the analysis of the bit-complexity of the Euclid Algorithm [5,27]. One deals in this case with the Dirichlet series relative to cost X, for $X \in \{\mathrm{Id}, C_{(c)}, B\}$, defined as

$$F_X(s) := \sum_{\substack{(u,v)\in\mathbb{Z}^2 \\ v/u\in\mathcal{T},\gcd(u,v)=1}} \frac{X(u,v)}{v^{2s}}.$$

These series admit alternative expressions that involve the quasi-inverse $(I - \mathbf{H}_s)^{-1}$ of the plain operator $\mathbf{H}_s$, together with functionals $W_{(c)}$ and Δ. Finally, the following equalities

$$F_{\mathrm{Id}}(s) = \mathbf{G}_s[1](0), \qquad F_C(s) = \mathbf{G}_{s,C}[1](0), \qquad F_B(s) = -\mathbf{G}_{s,D}[1](0). \tag{3.72}$$

hold, and involve the non-underlined[9] versions $\mathbf{G}_s, \mathbf{G}_{s,C}, \mathbf{G}_{s,D}$ of the generating operators $\underline{\mathbf{G}}_s, \underline{\mathbf{G}}_{s,C}, \underline{\mathbf{G}}_{s,D}$ defined in (3.68, 3.70).

Functional Analysis

We need precise information on the quasi-inverse $(I - \underline{\mathbf{H}}_s)^{-1}$, which is omnipresent in the expressions of our probabilistic studies (see 3.67, 3.69, 3), as the quasi-inverse $(I - \underline{\mathbf{H}}_s)^{-1}$ was already omnipresent in the probabilistic analyses of the F-EUCLID Algorithm.

[9] These operators are defined in the same vein as underlined versions, replacing each occurrence of the underlined operator $\underline{\mathbf{H}}_s$ by the plain operator $\mathbf{H}_s$.

It is first needed to find convenient functional spaces where the operators $\mathbf{H}_s$, $\underline{\mathbf{H}}_s$ 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 spaces $A_\infty(\mathcal{V})$, $B_\infty(\mathcal{V})$ of all functions f (of one variable) or F (of two variables) that are holomorphic and continuous on the frontier: $A_\infty(\mathcal{V})$ is the space of functions f holomorphic in the domain $\mathcal{V}$ and continuous on the closure $\bar{\mathcal{V}}$, while $B_\infty(\mathcal{V})$ is the space of functions F holomorphic in the domain $\mathcal{V}\times\mathcal{V}$ and continuous on the closure $\bar{\mathcal{V}}\times\bar{\mathcal{V}}$. Endowed with the sup-norm, these are Banach spaces; for $\Re(s) > (1/2)$, the transfer operator $\mathbf{H}_s$ acts on $A_\infty(\mathcal{V})$, the transfer operator $\underline{\mathbf{H}}_s$ acts on $B_\infty(\mathcal{V})$, and these are compact operators. Furthermore, when weighted by a cost of moderate growth [i.e., $c(h_{(q)}) = O(\log q)$], for w close enough to 0, and $\Re s > (1/2)$, the operator $\underline{\mathbf{H}}_{s,w,(c)}$ also acts on $B_\infty(\mathcal{V})$, and is also compact.

In the case of the F-EUCLID Algorithm, the spectral properties of the transfer operator defined in (3.57) play a central rôle in the analysis of the algorithm. For real s, the transfer operator $\mathbf{H}_s$ has a unique dominant eigenvalue $\lambda(s)$, which is real and separated from the remainder of the spectrum by a spectral gap. For $s = 1$, the dominant eigenvalue of the density transformer $\mathbf{H}$ satisfies $\lambda(1) = 1$, and the dominant eigenfunction $\psi(x)$ (which is then invariant under the action of $\mathbf{H}$) admits a closed form that 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 with the standard Euclid algorithm and equal to $(1/\log 2)1/(1+x)$.

Moreover, the quasi-inverse $(I - \mathbf{H}_s)^{-1}$ has a pôle at $s = 1$, and satisfies

$$(I - \mathbf{H}_s)^{-1}[f](z) \sim_{s\to 1} \frac{1}{s-1}\frac{1}{h(\mathcal{E})}\psi(z)\int_{\widetilde{\mathcal{I}}} f(x)\,\mathrm{d}x, \tag{3.73}$$

where the constant $h(\mathcal{E})$ is the entropy of the F-EUCLID dynamical system, and satisfies

$$h(\mathcal{E}) = |\lambda'(1)| = \frac{\pi^2}{6\log\phi} \approx 3.41831. \tag{3.74}$$

The operator $\underline{\mathbf{H}}_{s,w,(c)}$ also possesses nice spectral properties (see [40], [9]): for a complex number s close enough to the real axis, with $\Re s > (1/2)$, it has a unique dominant eigenvalue, denoted by $\lambda_{(c)}(s,w)$, which is separated from the remainder of the spectrum by a spectral gap. 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 recovers the plain operator $\underline{\mathbf{H}}_s$, which has the same dominant eigenvalue $\lambda(s)$ as the operator $\mathbf{H}_s$. For $s = 1$, it has a dominant eigenvalue $\lambda(1) = 1$ with a dominant eigenfunction $\underline{\psi}$, which 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 [40],

$$\underline{\psi}(z,u) = \frac{1}{\log\phi}\frac{1}{u-z}\left(\log\frac{\phi+u}{\phi+z} + \log\frac{\phi^2-u}{\phi^2-z}\right) \quad \text{for } z \neq u, \text{ and } \underline{\psi}(z,z) = \psi(z). \tag{3.75}$$

Near $s = 1$, the quasi-inverse satisfies

$$(I - \underline{\mathbf{H}}_s)^{-1}[F](z,u) \sim_{s\to 1} \frac{1}{s-1}\frac{1}{h(\mathcal{E})}\, I[F]\, \underline{\psi}(z,u), \quad \text{with } I[F] := \int_{\widetilde{\mathcal{I}}} F(x,x)\,\mathrm{d}x. \tag{3.76}$$

We consider, in the sequel of this section, the COREGAUSS algorithm with an initial density, standard of valuation r. Such a density is defined as $y^r/A_0(r)$, with $A_0(r)$ defined in (3.61). In this case, there are nice expressions for the moment generating functions $\mathbb{E}_{(r)}[\exp(wC)]$, for the expectations $E_{(r)}[C], \mathbb{E}_{(r)}[D]$, described in (3.67, 3.69, 3), where we let $L = 1$.

Probabilistic Analysis of the F-EUCLID *Algorithm*

We wish to compare the behavior of the two algorithms, the COREGAUSS Algorithm and the F-EUCLID Algorithm, and we first recall here the main facts about the probabilistic behavior of the F-EUCLID Algorithm.

Theorem 10. (Akhavi and Vallée [5] (1998), Vallée [37, 41] (2003-2007)) *On the set ω_N formed with input pairs (u,v) for which $u/v \in \widetilde{\mathcal{I}}$ and $|v| \leq N$, the mean number of iterations P, the mean value of a cost C of moderate growth, the mean value of the bit-complexity B satisfy, when $M \to \infty$,*

$$\mathbb{E}_N[P] \sim \frac{2\log 2}{h(\mathcal{E})}\lg N,\ \mathbb{E}_M[C_{(c)}] \sim \frac{2\log 2}{h(\mathcal{E})}\mathbb{E}[c]\lg N,\ \mathbb{E}_M[B] \sim \frac{\log 2}{h(\mathcal{E})}\mathbb{E}[\ell]\lg^2 N.$$

Here, $h(\mathcal{E})$ denotes the entropy of the F-EUCLID *dynamical system, described in (3.74), and $\mathbb{E}[c]$ denotes the mean value of the step-cost c with respect to the invariant density ψ. This is a constant of Khinchin's type, of the form*

$$\mathbb{E}[c] := \sum_{h\in\mathcal{H}} \int_{h(\widetilde{\mathcal{I}})} \ell(h)\psi(x)\,\mathrm{d}x.$$

In particular, when c is the binary length ℓ, there is a nice formula for $\mathbb{E}[\ell]$, namely

$$\mathbb{E}[\ell] = \frac{1}{\log\phi}\log\prod_{k\geq 1}\frac{2^k\phi^2+\phi}{2^k\phi^2-1} \approx 2.02197.$$

Proof (Sketch). One deals with the Dirichlet series $F_X(s)$ relative to cost X, defined in (3.72). Using the spectral relation (3.73) together with Tauberian Theorems leads to the asymptotic study of the coefficients of the series and provides the result. ■

Moreover, there exist also more precise distributional results [6, 27] which show that all these costs $P, C_{(c)}$, together with a regularized version of B, admit asymptotic Gaussian laws for $M \to \infty$.

What can be expected about the probabilistic behavior of the CoreGauss Algorithm? On the one hand, there is a strong formal similarity between the two algorithms, as the CoreGauss Algorithm can be viewed as a lifting of the F-Euclid Algorithm. On the other hand, important differences appear when we consider algorithms: the F-Euclid algorithm never terminates, except on rational inputs that fall in the hole $\{0\}$, while the CoreGauss Algorithm always terminates, except for irrational real inputs. However, it is clear that these differences disappear when we restrict to rational inputs, real or complex ones. In this case, both algorithms terminate, and it is quite interesting to determine if there exists a precise transition between these two (discrete) algorithms.

Distribution of Additive Costs

We wish to prove that $k \mapsto \mathbb{P}_{(r)}[C_{(c)} = k]$ has a geometrical decreasing, with a precise estimate for the ratio. For this purpose, we use the moment generating function $\mathbb{E}_{(r)}(\exp[wC_{(c)}])$ of the cost $C_{(c)}$, for which we have provided an alternative expression in (3.67). We first study any additive cost, then we focus on the number of iterations.

General additive cost. The asymptotic behavior of the probability $\mathbb{P}_{(r)}[C_{(c)} = k]$ (for $k \to \infty$) is obtained by extracting the coefficient of $\exp[kw]$ in the moment generating function. Then the asymptotic behavior of $\mathbb{P}_{(r)}[C_{(c)} = k]$ is related to singularities of $\mathbb{E}_{(r)}(\exp[wC_{(c)}])$. This series has a pôle at $e^{w_{(c)}(r+2)}$, where $w = w_{(c)}(s)$ is defined by the spectral equation $\lambda_{(c)}(s, w) = 1$ that involves the dominant eigenvalue $\lambda_{(c)}(s, w)$ of the operator $\underline{\mathbf{H}}_{s,w,(c)}$, which is described in (3.65). Then, with classical methods of analytic combinatorics, we obtain:

Theorem 11. (Daudé et al. [14] (1994), Vallée and Vera [45] (2007)) *Consider the* CoreGauss *algorithm, when its inputs are distributed inside the disk $\mathcal{D}$ with the continuous standard density of valuation r. Then, any additive cost $C_{(c)}$ defined in (3.9), associated to a step-cost c of moderate growth asymptotically, follows a geometric law.*

The ratio of this law, equal to $\exp[-w_{(c)}(r+2)]$, *is related to the solution $w_{(c)}(s)$ of the spectral relation $\lambda_{(c)}(s, w) = 1$, which involves the dominant eigenvalue of the transfer operator $\underline{\mathbf{H}}_{s,w,(c)}$. It satisfies, for any cost c of moderate growth, $w_{(c)}(r+2) = \Theta(r+1)$ when $r \to -1$. More precisely, one has*

$$\mathbb{P}_{(r)}[C_{(c)} = k] \sim_{k\to\infty} a(r) \exp[-kw_{(c)}(r+2)], \qquad \text{for } k \to \infty, \tag{3.77}$$

where $a(r)$ is a strictly positive constant that depends on cost c and valuation r.

Number of iterations. In the particular case of a constant step-cost $c = 1$, the cost $C_{(c)}$ is just the number R of iterations and the operator $\underline{\mathbf{H}}_{s,w,(1)}$ reduces to $e^w \cdot \underline{\mathbf{H}}_s$. In this case, there exists a nice 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 (3.36), as

$$\mathbb{P}_{(r)}[R \geq k+1] = \frac{1}{A_0(r)} \sum_{h \in \mathcal{H}^k} \iint_{h(\mathcal{D})} y^r \mathrm{d}x\mathrm{d}y = \frac{1}{A_0(r)} \iint_{\mathcal{D}} y^r \, \underline{\mathbf{H}}^k_{2+r}[1](z)\, \mathrm{d}x\mathrm{d}y,$$

where $A_0(r)$ is defined in (3.61). This leads to the following result:

Theorem 12. (Daudé et al. [14] (1994), Vallée [40] (1996)) *Consider the* CoreGauss *algorithm, when its inputs are distributed inside the disk $\mathcal{D}$ with the continuous standard density of valuation r. Then, the expectation of the number R of iterations admits the following expression:*

$$\mathbb{E}_{(r)}[R] = \frac{2^{2r+4}}{\zeta(2r+4)} \sum_{\substack{c,d \geq 1 \\ d\phi < c < d\phi^2}} \frac{1}{(cd)^{2+r}}.$$

Furthermore, for any fixed valuation $r > -1$, the number R of iterations asymptotically 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 transfer operator $\underline{\mathbf{H}}_s$ and $\widetilde{a}(r)$ is a strictly positive constant that depends on the valuation r.

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 [26]. In [17], numerical values are computed in the case of the uniform density, that is, for $\lambda(2)$ and $\mathbb{E}_{(0)}[R]$,

$$\mathbb{E}_{(0)}[R] \approx 1.08922, \qquad \lambda(2) \approx 0.0773853773.$$

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 behavior of the Gauss Algorithm when the data become more and more concentrated near the real axis.

Mean Bit-Complexity

We are now interested in the study of the bit-complexity B,[10] and we focus on a standard density of valuation r. We start with the relation between B, and costs C, D

[10] We study the central part of the bit-complexity, and do not consider the initialization process, where the Gram matrix is computed; see Section "Main Parameters of Interest".

recalled in Section "Execution Parameters in the Complex Framework", together with the expressions of the mean values of parameters C, D obtained in (3.69, 3). We state three main results: the first one describes the evolution in the continuous model when the valuation r tends to -1; the second one describes the evolution of the discrete model when the integer size M tends to ∞, the valuation being fixed; finally, the third one describes the evolution of the discrete model when the valuation r tends to -1 *and* the integer size M tends to ∞.

Theorem 13. (Vallée and Vera [45, 47], 2007) *Consider the* CoreGauss *Algorithm, where its inputs are distributed inside the input disk $\mathcal{D}$ with the standard density of valuation $r > -1$. Then, the mean value $\mathbb{E}(r)[C]$ of any additive cost C of moderate growth, and the mean value $E_{(r)}[D]$ of cost D are well-defined and satisfy when $r \to -1$,*

$$\mathbb{E}_{(r)}[C] \sim \frac{1}{r+1}\frac{\mathbb{E}[c]}{h(\mathcal{E})}, \qquad \mathbb{E}_{(r)}[D] \sim -\frac{1}{(r+1)^2}\frac{1}{\log 2}\frac{\mathbb{E}[\ell]}{h(\mathcal{E})}.$$

When r tends to -1, the output density, associated with an initial density of valuation r, tends to $\frac{1}{h(\mathcal{E})}\frac{1}{y}\underline{\psi}$, where $\underline{\psi}$ is the invariant density for $\underline{\mathbf{H}}_1$ described in (3.75).

Remark that the constants that appear here are closely related to those which appear in the analysis of the Euclid algorithm (Theorem 10). More precisely, the asymptotics are almost the same when we replace $1/(r+1)$ (in Theorem 13) by $\log N$ (in Theorem 10). Later, Theorem 15 will make precise this observation.

Proof. For any valuation r, the variables C, D are integrable on the disk $\mathcal{D}$: this is due to the fact that, for $X \in \{\mathrm{Id}, C, D\}$, the integrals taken over the horizontal strip $\mathcal{H}_N := \mathcal{D} \cap \{z;\ |\Im z| \leq (1/N)\}$ satisfy, with $M = \log N$,

$$\frac{1}{A_0(r)} \iint_{\mathcal{H}_N} y^r\, X(z)\, \mathrm{d}x\mathrm{d}y = \frac{M^{e(X)}}{N^{r+1}}\, O\left(1 + (r+1)M\right),$$

where the exponent $e(X)$ depends on cost X; one has $e(\mathrm{Id}) = 0, e(C) = 1, e(D) = 2$. This proves that cost X is integrable on $\mathcal{D}$. Furthermore, when $r \to -1$, relations (3.76, 3.73) prove the following behaviors:

$$\underline{\mathbf{G}}_{2+r,\mathrm{Id}}[F] \sim \frac{1}{r+1}\frac{1}{h(\mathcal{E})}\, I[F]\, \underline{\psi},$$

$$\underline{\mathbf{G}}_{2+r,C_{(c)}}[F] \sim \frac{1}{(r+1)^2}\frac{\mathbb{E}[c]}{h(\mathcal{E})^2}\, I[F]\, \underline{\psi}, \quad \underline{\mathbf{G}}_{2+r,D}[F] \sim -\frac{1}{(r+1)^3}\frac{\mathbb{E}[\ell]}{h(\mathcal{E})^2}\, I[F]\, \underline{\psi},$$

where the integral $I[F]$ is defined in (3.76) and $\underline{\psi}$ is described in (3.75). The first equality, together with the definition of $A_0(r)$ and the fact that $A_0(r) \sim (r+1)^{-1}$

for $r \to -1$, implies the equality

$$\iint_{\widetilde{\mathcal{B}}\setminus\mathcal{D}} \frac{1}{y}\,\Psi(z,\bar{z})\,\mathrm{d}x\mathrm{d}y = h(\mathcal{E}).$$

Using a nice relation between $I[\Psi]$ and $h(\mathcal{E})$ finally leads to the result. ■

It is now possible to transfer this analysis to the discrete model defined in Section "Probabilistic Models for Two-Dimensions", with the Gauss principle recalled in Section "Probabilistic Models: Continuous or Discrete".

Theorem 14. (Vallée and Vera [45, 47], 2007) *Consider the* CoreGauss *Algorithm, where its integer inputs (u,v) of length $M := \max\{\ell(|u|^2, \ell(|v|^2\}$ are distributed inside the input disk $\mathcal{D}$ with the standard density of valuation $r > -1$. Then, the mean value $\mathbb{E}_{(r,M)}[X]$ of cost X – where X is any additive cost C of moderate growth, or cost D – tends to the mean value $\mathbb{E}_{(r)}[X]$ of cost X, when $M \to \infty$. More precisely,*

$$\mathbb{E}_{(r,M)}[X] = \mathbb{E}_{(r)}[X] + \frac{M^{e(X)}}{N^{r+1}}\, O\left(\max\{1,(r+1)M\}\right),$$

where the exponent $e(X)$ depends on cost X and satisfies $e(C) = 1, e(D) = 2$. The mean value $\mathbb{E}_{(r,M)}[B]$ of the bit-complexity B satisfies, for any fixed $r > -1$, when $M \to \infty$,

$$\mathbb{E}_{(r,M)}[B] \sim \mathbb{E}_{(r)}[Q] \cdot M.$$

In particular, the mean bit-complexity is linear with respect to M.

Finally, the last result describes the transition between the CoreGauss algorithm and the F-Euclid Algorithm, obtained when the valuation r tends to -1, and the integer size M tends to $= \infty$:

Theorem 15. (Vallée and Vera [45, 47], 2007) *Consider the* CoreGauss *Algorithm, where its integer inputs (u,v) of length $M := \max\{\ell(|u|^2, \ell(|v|^2\}$ are distributed inside the input disk $\mathcal{D}$ with the standard density of valuation $r > -1$. When the integer size M tends to ∞ and the valuation r tends to -1, with $(r+1)M = \Omega(1)$, the mean value $\mathbb{E}_{(r,M)}[X]$ of cost X, where X can be any additive cost C of moderate growth, or cost D, satisfies*

$$\mathbb{E}_{(r,M)}[X] = \mathbb{E}_{(r)}[X]\left[1 + O\left(\frac{(M(r+1))^{e(X)+1}}{N^{r+1}}\right)\right]\left[\frac{1}{1-N^{-(r+1)}}\right],$$

where the exponent $e(X)$ depends on cost X and satisfies $e(C) = 1, e(D) = 2$.

Then, if we let $(r+1)M =: M^{\alpha} \to \infty$ *(with* $0 < \alpha < 1$*), then the mean values satisfy*

$$\mathbb{E}_{(r,M)}[C] \sim \frac{\mathbb{E}[c]}{h(\mathcal{E})} M^{1-\alpha}, \qquad \mathbb{E}_{(r,M)}[D] \sim -\frac{\mathbb{E}[\ell]}{h(\mathcal{E})} \frac{1}{\log 2} M^{2-2\alpha}$$

$$\mathbb{E}_{(r,M)}[B] \sim \frac{\mathbb{E}[\ell]}{h(\mathcal{E})} M^{2-\alpha}.$$

If now $(r+1)M$ *is* $\Theta(1)$*, then*

$$\mathbb{E}_{(r,M)}[C] = \Theta(M), \qquad \mathbb{E}_{(r,M)}[D] = \Theta(M^2), \qquad \mathbb{E}_{(r,M)}[B] = \Theta(M^2).$$

Open question. Provide a precise description of the phase transition for the behavior of the bit-complexity between the Gauss algorithm for a valuation $r \to -1$ and the Euclid algorithm: determine the constant hidden in the Θ term as a function of $(r+1)M$.

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.

Evolution of Densities of the Local Bases

The LLL algorithm aims at reducing all the local bases U_k (defined in Section "Description of the Algorithm") 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 "A Variation for the LLL Algorithm: The Odd-Even Algorithm" 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 with local bases (u_k, v_k) and (u_{k+2}, v_{k+2}) via relation (3.1). Then, the LLL algorithm reduces these two local bases (in the Gauss meaning) and computes two reduced local bases denoted by $(\widehat{u}_k, \widehat{v}_k)$ and $(\widehat{u}_{k+2}, \widehat{v}_{k+2})$, which satisfy[11] in particular

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

[11] The notation * refers to the Gram–Schmidt process as in Sections "The Lattice Reduction Algorithm in the Two-Dimensional Case and The LLL Algorithm".

Then, Theorem 8 provides insights on the distribution of $\mu(z_k), \lambda(z_{k+2})$. As, in our model, the random variables $|u_k|$ and z_k (respectively, $|u_{k+2}|$ and z_{k+2}) are independent (see Section "Probabilistic Models for Two-Dimensions"), we obtain a precise information on the distribution of the norms $|\widehat{v}_k^\star|, |\widehat{u}_{k+2}|$.

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

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

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 $|\widehat{v}_k^\star|, |\widehat{u}_{k+2}|$ are independent. All this allows to obtain precise information 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 $\widehat{v}_k^\star, \widehat{u}_{k+2}$ are no longer independent. Are they independent enough, 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.

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 (respectively, Even) dynamical system performs (in parallel) the same operations as the AGAUSS dynamical system, on each complex number z_i of odd (respectively, even) indices. Between the end of one phase and the beginning of the following phase, computations in the vein of Section "Evolution of Densities of the Local Bases" 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!

References

1. K. AARDAL AND F. EISENBRAND. The LLL algorithm and integer programming, *This book*
2. M. AJTAI. Optimal lower bounds for the Korkine-Zolotareff parameters of a lattice and for Schnorr's algorithm for the shortest vector problem. Theory of Computing 4(1): 21–51 (2008)

3. A. AKHAVI. Random lattices, threshold phenomena and efficient reduction algorithms, *Theoretical Computer Science*, 287, (2002), 359–385
4. 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, long version to appear in *ESAIM Probability and Statistics*
5. A. AKHAVI AND B. VALLÉE. Average bit-complexity of Euclidean algorithms, In *Proceedings of ICALP'2000* – Genève, 14 pages, LNCS, 373–387, (1853)
6. V. BALADI AND B. VALLÉE. Euclidean algorithms are Gaussian, *Journal of Number Theory*, 110(2), (2005), 331–386
7. J. BOURDON, B. DAIREAUX, AND B. VALLÉE. Dynamical analysis of α-Euclidean algorithms, *Journal of Algorithms*, 44, (2002), 246–285
8. D. BUMP. *Automorphic Forms and Representations*, Cambridge University Press, Cambridge, (1996)
9. F. CHAZAL, V. MAUME-DESCHAMPS, AND B. VALLÉE. Erratum to "Dynamical sources in information theory: fundamental intervals and word prefixes", *Algorithmica*, 38, (2004), 591–596
10. E. CESARATTO, J. CLÉMENT, B. DAIREAUX, L. LHOTE, V. MAUME-DESCHAMPS AND B. VALLÉE. Analysis of fast versions of the Euclid algorithm, Journal of Symbolic Computation, 44 (2009) pp 726-767
11. D. COPPERSMITH. Small solutions to polynomial equations, and low exponent RSA vulnerabilities, *Journal of Cryptology*, 10(4), (1997), 233–260
12. D. COPPERSMITH AND A. SHAMIR. Lattice attacks on NTRU, *Proceedings of Eurocrypt 1997*, LNCS, 1233, 52–61, Springer, Berlin, (1997)
13. J.-S. CORON. Security proof for partial-domain hash signature schemes. In *Proceedings of Crypto 2002*, LNCS, 2442, 613–626, Springer, Berlin, (2002)
14. H. DAUDÉ, P. FLAJOLET, AND B. VALLÉE. An average-case analysis of the Gaussian algorithm for lattice reduction, *Combinatorics, Probability and Computing* 6, (1997), 397–433
15. H. DAUDÉ AND B. VALLÉE. An upper bound on the average number of iterations of the LLL algorithm. *Theoretical Computer Science* 123(1), (1994), 95–115
16. P. FLAJOLET AND B. VALLÉE. Gauss' reduction algorithm : an average case analysis, *Proceedings of IEEE-FOCS 90*, St-Louis, Missouri, 2, 830–39
17. P. FLAJOLET AND B. VALLÉE. Continued fractions, comparison algorithms and fine structure constants *Constructive, Experimental and Non-Linear Analysis*, Michel Thera, Editor, Proceedings of Canadian Mathematical Society, 27, 53–82, (2000)
18. C. GENTRY. The geometry of provable security: some proofs of security in which lattices make a surprise appearance, *This book*
19. C. GENTRY. How to compress rabin ciphertexts and signatures (and more), *Proceedings of Crypto'04*, 179–200, Springer, Berlin, (2004)
20. D. GOLDSTEIN AND A. MAYER. On the equidistribution of Hecke points, *Forum Mathematicum*, 15, (2003), 165–189
21. G. HANROT. LLL: a tool for effective diophantine approximation, *This book*
22. J. KLÜNERS. The van Hoeij algorithm for factoring polynomials, *This book*
23. J. C. LAGARIAS. Worst-case complexity bounds for algorithms in the theory of integral quadratic forms. *Journal of Algorithms* 1(2), (1980), 142–186
24. H. LAVILLE AND 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), 135–159
25. A. K. LENSTRA, H. W. LENSTRA, AND L. LOVÁSZ. Factoring polynomials with rational coefficients. *Mathematische Annalen* 261, (1982), 513–534
26. L. LHOTE. Computation of a class of continued fraction constants. *Proceedings of ALENEX-ANALCO'04*, 199–210
27. L. LHOTE AND B. VALLÉE. Gaussian laws for the main parameters of the Euclid algorithm, *Algorithmica* (2008), 497–554
28. A. MAY. Using LLL reduction for solving RSA and factorization problems, *This book*

29. P. NGUYEN AND D. STEHLÉ. Floating-point LLL revisited, *Proceedings of Eurocrypt 2005* , LNCS, 3494, 215–233, Springer, Berlin, (2005)
30. P. NGUYEN AND D. STEHLÉ. LLL on the average, *Proceedings of the 7th Algorithmic Number Theory Symposium (ANTS VII)*, LNCS, 4076, 238–256, Springer, Berlin, (2006)
31. J. HOFFSTEIN, N. HOWGRAVE-GRAHAM, J. PIPHER, AND W. WHYTE. NTRUEncrypt and NTRUSign, *This book.*
32. C. P. SCHNORR. A hierarchy of polynomial lattice basis reduction algorithms, *Theoretical Computer Science*, 53, (1987), 201–224
33. I. SEMAEV. A 3-dimensional lattice reduction algorithm, *Proceedings of the 2001 Cryptography and Lattices Conference (CALC'01)*, LNCS, 2146, 181–193, Springer, Berlin, (2001)
34. C. L. SIEGEL. A mean value theorem in geometry of numbers, *Annals in Mathematics*, 46(2), (1945), 340–347
35. D. SIMON. Selected applications of LLL in number theory, *This book*
36. D. STEHLÉ. Floating point LLL: theoretical and practical aspects, *This book.*
37. B. VALLÉE. Euclidean Dynamics, *Discrete and Continuous Dynamical Systems*, 15(1), (2006), 281–352
38. B. VALLÉE. Gauss' algorithm revisited. *Journal of Algorithms* 12, (1991), 556–572
39. 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, September 97), LNCS, 1284, 486–499
40. B. VALLÉE. Opérateurs de Ruelle-Mayer généralisés et analyse en moyenne des algorithmes de Gauss et d'Euclide, *Acta Arithmetica* 81.2, (1997), 101–144
41. B. VALLÉE. Dynamical analysis of a class of Euclidean algorithms, *Theoretical Computer Science* 297(1–3), (2003), 447–486
42. B. VALLÉE. An affine point of view on minima finding in integer lattices of lower dimensions. *Proceedings of EUROCAL'87*, LNCS, 378, 376–378, Springer, Berlin, (1987)
43. B. VALLÉE. Generation of elements with small modular squares and provably fast integer factoring algorithms, *Mathematics of Computation*, 56(194), (1991), 823–849
44. B. VALLÉE. Provably fast integer factoring algorithm with quasi-uniform quadratic residues, *Proceedings of ACM-STOC-89*, Seattle, 98–106
45. B. VALLÉE AND A. VERA. Lattice reduction in two-dimensions: analyses under realistic probabilistic models, Proceedings of the AofA'07 conference, *Discrete Mathematics and Theoretical Computer Science*, Proc. AH, (2007), 181–216
46. B. VALLÉE, M. GIRAULT, AND P. TOFFIN. How to guess ℓ-th roots modulo n by reducing lattices bases, *Proceedings of AAECC-88*, Rome, LNCS, (357), 427–442
47. A. VERA. Analyses de l'algorithme de Gauss. Applications à l'analyse de l'algorithme LLL, PhD Thesis, University of Caen, (July 2009)
48. G. VILLARD. Parallel lattice basis reduction. *Proceedings of International Symposium on Symbolic and Algebraic Computation*, Berkeley, ACM, (1992)