University of Zurich
Institute of Mathematics

An Analysis of the Number of Reduction Steps for Special Two-Dimensional Lattices

---

Master's Thesis in Mathematics

Author: Julia Würsch, 21-716-618
Supervisor: Prof. Dr. Joachim Rosenthal
Co-Supervisors: Sina Schaeffler, Giacomo Borin, Dr. Luca De Feo
Submission: August 2026

Abstract

The Gaussian algorithm for lattice reduction in two dimensions is analyzed for special input lattices arising from ideals in imaginary quadratic fields. In particular, we examine the distribution of the number of reduction steps. For this, we examine the tail probability $\Pr[L \geq k+1]$, which quantifies the probability that the reduction algorithm requires more than k reduction steps.

We analyze the geometric properties of such lattices arising from ideals and construct a probabilistic model for their initial distribution in a fundamental domain. Based on the transfer operator framework introduced by Daudé, Flajolet, and Vallée [DFV96], we derive numerical estimates for the reduction step probability of these special lattices. We further introduce a geometric line-intersection model that exploits the geometric properties observed in the initial distribution of the lattices. A numerical comparison with experimental data shows that this method provides a more accurate prediction of the observed probabilities.

Contents

1 Introduction **4**

2 Preliminaries **7**
2.1 Lattices and Reduction 7
2.2 Number-theoretic Background 9
2.3 Transfer Operators 11
2.4 Spectral Theory 11
2.5 General Mathematical Background 12

3 Probabilistic Framework **13**
3.1 Tail probability of Reduction steps 13
3.2 From Algorithm to dynamical system 13
3.3 Lattices with uniform input density 16
3.3.1 Transfer Operator representation for uniform input density 16
3.4 Lattices with general input density 18
3.4.1 General Transfer Operator 18
3.5 Spectral Analysis of the Transfer Operator 20
3.5.1 Uniform transfer operator 20
3.5.2 General transfer operator 23

4 Ideal Lattices **26**
4.1 Lattices from Ideals 26
4.2 Geometry of these lattices 30
4.3 Model their distribution 34
4.4 Generation of Experimental Data 35

5 Applying probability models for computations **37**
5.1 The transfer operator method 37
5.1.1 Choosing probability density function ρ 37
5.1.2 Truncated operator for computations 39
5.1.3 Estimation of the probability 42
5.1.4 Numerical Verification in the uniform case 49
5.2 The Line-Disk intersection method 50
5.3 Extension to band area 53

Bibliography **55**

1 Introduction

Motivation. The development of quantum computers poses a significant threat to many of the cryptographic protocols in use today. Indeed, several widely deployed cryptographic protocols are expected to become insecure once sufficiently powerful quantum computers are available. To address this challenge, researchers are developing new cryptographic protocols that will remain secure against classical and quantum computers. This field of research, known as post-quantum cryptography (PQC), is focused on ensuring long-term security in the presence of quantum computer development. Among the proposed post-quantum approaches, lattice-based and isogeny-based cryptography have received considerable attention. Although lattices are most commonly associated with lattice-based cryptography, they also arise in certain isogeny-based constructions.

In lattice-based cryptography, security is directly based on the computational difficulty of solving certain lattice problems, such as the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP). The SVP asks for a non-zero lattice vector of the shortest norm, while the CVP asks for a lattice vector closest to a prescribed target point. These problems are believed to be computationally hard even for quantum computers.

Isogeny-based cryptography relies on the computational difficulty of finding isogenies between elliptic curves. Although lattices do not form the underlying security assumption in this setting, lattice reduction plays an important algorithmic role. In particular, in the *SQIsign* signature scheme [Feo+20], the *Qlapoti* algorithm [Bor+], which is based on the *Clapoti* framework, uses lattice reduction to find short integer solutions to modular equations. Lattice reduction also appears in group-action-based schemes, such as *Qt-Pegasis* [Dar+25], which make use of lattice reduction to compute reduced representatives of ideals arising from ideal classes of quadratic fields. The lattices studied in this thesis originate from such problems in isogeny-based cryptography. Understanding the behavior of lattice reduction algorithms on these lattices is therefore of both practical and theoretical interest.

Background. A lattice is a discrete subset of an Euclidean space generated by integer linear combinations of a basis. Equivalently, it is an additive subgroup of $\mathbb{R}^n$, which means that the sum and difference of two lattice points is again a lattice point.

The same lattice can be represented by many different bases. Some bases consist of short, nearly orthogonal vectors, while others consist of long, highly skew vectors.

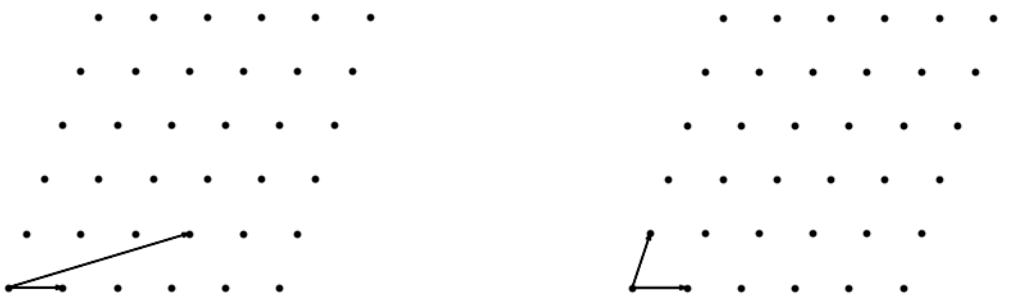

Figure 1.1: The same lattice represented by two different bases. The left basis is skew, and the right basis is reduced.

Many computational problems on lattices, such as the SVP and CVP, become significantly easier when the lattice is represented by a basis consisting of short vectors. This motivates the lattice reduction problem: given a basis of a lattice, find another basis of the same lattice whose vectors

are shorter and closer to being orthogonal. Lattice reduction algorithms achieve this through a sequence of reduction steps, each transforming the current basis into a more reduced one. The process ends once a reduced basis is obtained. Efficient lattice reduction algorithms are fundamental tools in computational number theory, optimization, and cryptography. In dimension two, lattice reduction can be performed by the Standard Gaussian Algorithm (SGA), which is closely related to the Euclidean GCD Algorithm and to continued fraction expansions. In higher dimensions, the most widely used reduction algorithm is the Lenstra-Lenstra-Lovász (LLL) algorithm.

Topic. The running time of the Gaussian reduction algorithm strongly depends on the input lattice. For cryptographic applications, a predictable running time is essential, since variation in execution time may leak information about the input. To obtain guarantees that hold for all inputs, one often resorts to worst-case bounds on the number of reduction steps. However, lattices that achieve this worst-case behavior are expected to be extremely rare.

Despite the simplicity of the Gaussian Algorithm, its behavior is not yet fully understood from a probabilistic perspective. Lagarias showed that the Gaussian algorithm has a logarithmic worst-case complexity in the size of the input lattice [Lag80]. On the other hand, Daudé, Flajolet, and Vallée [DFV96] proved that the average-case complexity is asymptotically constant. Beyond the worst- and average-cases, relatively little is known about the probability that the algorithm requires an unusually large number of reduction steps.

To obtain practically relevant bounds on the running time, it is necessary to understand the tail behavior of the distribution of reduction steps. More precisely, if L denotes the number of reduction steps performed by the algorithm, then we are interested in the tail probability

$$\Pr[L \geq k + 1],$$

which describes the probability that more than k reduction steps are required. Understanding the decay of this probability makes it possible to determine thresholds beyond which the occurrence of additional reduction steps becomes cryptographically negligible.

Daudé, Flajolet, and Vallée [DFV96] showed that the distribution of the number of reduction steps decays geometrically. Their analysis exploits deep connections between lattice reduction, continued fractions, and transfer operators. However, these results are restricted by the assumption that the input lattices are uniformly distributed. To move beyond this setting, Vallée [Val97] developed a transfer-operator framework that applies to a broad class of input densities.

In this thesis, we study the tail probability of the number of reduction steps for lattice distributions arising from isogeny-based cryptography. Since these distributions are derived from ideal classes of quadratic fields, the results are also relevant to class-group-based cryptographic constructions. We further investigate methods for estimating these probabilities.

Contribution. This thesis extends the transfer operator approach of Daudé, Flajolet, and Vallée [DFV96] to the lattices arising from ideals of quadratic fields which are used in isogeny-based cryptography.

For this purpose, we study lattices arising from ideals in quadratic fields and investigate their geometric properties. Based on this analysis, we identify a suitable input density function that allows the transfer operator framework to be applied in this setting. Using this framework, we compute numerical estimates of the tail probabilities of the number of reduction steps and compare the resulting predictions with experimentally generated data.

Furthermore, we develop a geometric approach, called the line-intersection method, which more accurately predicts the true reduction-step probabilities. The method exploits both the geometric properties of the considered lattices and the geometric decay of the distribution under repeated applications of the reduction map. We explain how the method can be implemented computationally and provide numerical results obtained from it. These results are compared again with the experimental data. Finally, we analyze the observed discrepancies between the theoretical predictions and the experimental results and discuss possible explanations for their occurrence.

Thesis Outline. Chapter 2 introduces the necessary background on lattices and lattice reduction, together with the number-theoretic, dynamical, and spectral-theoretic tools used throughout the thesis. In particular, we present the Standard Gaussian Algorithm and introduce its complex

formulation, explaining how lattice reduction in dimension two can be interpreted within a complex framework and how this viewpoint leads to the Complex Gaussian Algorithm. We then introduce transfer operators and the associated spectral theory, which provide a main analytic tool used throughout the thesis.

In Chapter 3 we explain the probabilistic framework for the Complex Gaussian Algorithm. We first relate the reduction map to a dynamical system through the close connection between lattice reduction and continued fractions (Section 3.2). We then derive the corresponding transfer operators for lattices with uniform input density (Section 3.3) and for lattices with general input density (Section 3.4). Finally, We analyze the spectral properties for these transfer operators, deriving asymptotical estimates of the probability of reduction steps (Section 3.5).

Chapter 4 focuses on lattices arising from the isogeny-based motivation, namely lattices associated with ideals. We describe the correspondence between such ideals and lattices and present an algorithm for sampling these lattices. We then investigate their geometric properties (Section 4.2), and develop a probabilistic model for their distribution (Section 4.3). In addition, We generate experimental data that will later serve as a basis for comparison with the theoretical predictions (Section 4.4).

Finally, Chapter 5 applies both the transfer operator method and the line intersection method to compute the probabilities of the reduction steps. Section 5.1 presents the transfer operator method and its computational results, while Section 5.2 covers the line intersection method together with its numerical results, compares its predictions with the experimental data and discusses possible explanations for the observed discrepancies.

Acknowledgments. I am deeply grateful to Sina Schaeffler, Giacomo Borin and Dr. Luca De Feo for their continuous support throughout this thesis. Their valuable discussions, insightful feedback, and careful reviews greatly improved my work. I would like to thank Prof. Dr. Joachim Rosenthal for supervising this thesis and for sharing his enthusiasm for cryptography through his lectures. Furthermore, I would like to thank the entire IBM team for their warm welcome and for making me feel included from the very beginning. In particular, I would like to thank Eliot Collombet for the enjoyable conversations in our shared office and during lunch breaks.

2 Preliminaries

In this chapter, we introduce the background material and notation required throughout the thesis.

2.1 Lattices and Reduction

Before studying lattice reduction algorithms, we first introduce the notion of a lattice and recall several basic properties that will be used throughout this thesis. The presentation follows [DFV96].

Definition 2.1 (Lattice in $\mathbb{R}^2$)**.** A 2-dimensional lattice in $\mathbb{R}^2$ is a set of the form

$$\Lambda = \mathbb{Z}u + \mathbb{Z}v = \{au + bv \mid a, b \in \mathbb{Z}\} ,$$

where $u, v \in \mathbb{R}^2$ are linearly independent. The pair (u, v) is called a basis of Λ.

Definition 2.2 (Acute Basis)**.** An ordered basis (u, v) of a lattice is called acute if the angle between u and v is at most $\pi/2$, that is,

$$\langle u, v\rangle \geq 0.$$

To describe reduced lattice bases, we first introduce the notion of a minimal basis.

Definition 2.3 (Minimal Basis)**.** [DFV96] Define u as the first minimum of a lattice Λ if it is a non-zero vector of Λ with smallest Euclidean norm, and define a second minimum v any vector among the shortest vectors of the lattice that are linearly independent of u. A basis is *minimal* if it consists of a first and a second minimum.

Remark 2.4. [DFV96] Without loss of generality, one can always assume that a minimal basis is acute, since (u, v) or $(u, -v)$ is acute.

It is often convenient to use the slightly weaker notion of a quasi-minimal basis.

Definition 2.5 (Quasi-Minimal Basis)**.** [DFV96] A basis is said to be *quasi-minimal* if the triangle $\langle u, v, u - v\rangle$, which it defines, contains two minima of the lattice. Then there is one among the six following pairs

$$(u, v), (v, u), (u, u - v), (v, v - u), (u - v, u), (v - u, v),$$

that defines a minimal basis of the lattice.

Since $\mathbb{R}^2$ and $\mathbb{C}$ are isomorphic as real vector spaces, every lattice in $\mathbb{R}^2$ can be represented in complex coordinates. Under the identification

$$\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} \longleftrightarrow u_1 + iu_2,$$

the lattice basis vectors $u, v \in \mathbb{R}^2$ may be viewed as complex numbers.

Definition 2.6 (Lattice in $\mathbb{C}$)**.** [DFV96] A 2-dimensional lattice in the complex plane $\mathbb{C}$ is the set

$$\Lambda = \mathbb{Z}u \oplus \mathbb{Z}v = \{au + bv \mid a, b \in \mathbb{Z}\} ,$$

where (u, v) is a tuple of two $\mathbb{R}$-linearly independent elements of $\mathbb{C}$ and is called the basis of Λ.

Given an ordered basis (u, v) with $u \neq 0$, we associate the complex parameter

$$z = \frac{v}{u}. \tag{2.1}$$

The ratio z is invariant under simultaneous multiplication of the basis vectors by a nonzero complex number.

The geometric properties of a basis can be expressed directly in terms of the associated complex parameter $z = v/u$. In particular, minimal and quasi-minimal bases admit the following characterization.

Proposition 2.7 (Acute Minimal Basis)**.** *[DFV96] For an acute basis (u, v) the following conditions are equivalent:*

1. *(u, v) is a minimal basis;*
2. *(u, v) satisfies the following inequalities:*

$$\left|\frac{u}{v}\right| \geq 1;\ 0 \leq \left|\Re(\frac{v}{u})\right| \leq \frac{1}{2}.$$

For an acute basis (u, v) the following conditions are equivalent:

1. *(u, v) is a quasi-minimal basis;*
2. *(u, v) satisfies the following inequalities:*

$$0 \leq \Re\left(\frac{v}{u}\right) \leq 1\ ;\ 0 \leq \Re\left(\frac{u}{v}\right) \leq 1.$$

The goal of lattice reduction is to transform an arbitrary basis into a minimal or quasi-minimal basis. The Standard Gaussian Algorithm produces a quasi-minimal basis by repeatedly replacing the longer basis vector by its difference with a suitable integer multiple of the shorter basis vector. The integer multiple is exactly how many times the smaller basis vector fits into the larger basis vector:

$$q := \left\lfloor \frac{\langle v, u\rangle}{\|u\|^2} \right\rceil.$$

Algorithm 1 Standard Gaussian Algorithm [SGA]

Input: Basis (u, v) of a Lattice, without loss of generality assume $\|v\| \leq \|u\|$.
Output: Reduced basis such that $\left|\frac{\langle v,u\rangle}{\|u\|^2}\right| \leq \frac{1}{2}$ and $\|u\| \leq \|v\|$.
while $\|v\| \leq \|u\|$ **do**
  $q := \left\lfloor \frac{\langle v,u\rangle}{\|v\|^2} \right\rceil$ ▷ Round to nearest integer
  $(u, v) := (v, u - qv)$
end while

Properties of Proposition 2.7 can be interpreted using the parameter $z = v/u$. A minimal basis is represented by z if $|z| \geq 1$ and $0 \leq \Re(z) \leq \frac{1}{2}$. Similarly, a quasi-minimal basis is represented by z if $0 \leq \Re(z) \leq 1$ and $0 \leq \Re(\frac{1}{z}) \leq 1$. We can rewrite the last conditions as follows: z represents an acute and quasi-minimal basis if and only if

$$z \in \mathcal{B} = \{z \mid 0 \leq \Re(z) \leq 1\}, \text{ and } z \notin \mathcal{D} = \{z \mid \Re(\frac{1}{z}) \geq 1\}.$$

With this representation of a quasi-minimal basis, we can rewrite the SGA 1 using the complex framework.

Algorithm 2 SGA in complex framework [DFV96]

Input: $z \in \mathbb{C}$ such that $z \in \mathcal{D}$
Output: $z \notin \mathcal{D}$
while $z \in \mathcal{D}$ **do**
  $z := U(z) = \frac{1}{z} - \lfloor \Re(\frac{1}{z}) \rfloor$
end while

Notice that the stopping condition of Algorithm 1 and Algorithm 2 coincides since

$$\|u\| \leq \|v\| \iff |z| = \left|\frac{v}{u}\right| \geq 1 \iff z \notin \mathcal{D}.$$

Two lattices that differ by multiplication by a nonzero complex scalar determine the same parameter $z = v/u$. This motivates the following notion of equivalence.

Definition 2.8. [Sta21, p. 1] Two lattices Λ and Λ' are called *homothetic* if one is obtained from the other by scaling by a complex number. In this case, we write $\Lambda \sim \Lambda'$.

2.2 Number-theoretic Background

The dynamical description of lattice reduction is expressed most naturally in terms of continued fractions. We therefore introduce continued fractions and the associated continuants.

Definition 2.9 (Continued Fraction)**.** A finite continued fraction is an expression of the form

$$m_0 + \cfrac{1}{m_1 + \cfrac{1}{m_2 + \cfrac{1}{\ddots + \cfrac{1}{m_k}}}},$$

where $m_0 \in \mathbb{Z}$ and $m_1, \ldots, m_k \in \mathbb{Z}_{>0}$.

Throughout this thesis, we will primarily work with generalized continued fractions that include a complex remainder and are of the form

$$\cfrac{1}{m_1 + \cfrac{1}{m_2 + \cfrac{1}{\ddots + \cfrac{1}{m_k + z_k}}}}, \tag{2.2}$$

where $m_1, \ldots, m_k \in \mathbb{Z}_{>0}$ and $z_k \in \mathbb{C}$.

Each finite truncation of a continued fraction can be rewritten as a single rational expression:

$$\begin{aligned} \frac{p_0}{q_0} &:= m_0 \\ \frac{p_1}{q_1} &:= \frac{m_1 m_0 + 1}{m_1} \\ \frac{p_2}{q_2} &:= \frac{m_2(m_1 m_0 + 1) + m_0}{m_2 m_1 + 1}, \\ &\vdots \end{aligned}$$

where p_k/q_k is called the k-th convergent of the continued fraction.

The numerators and denominators arising in this process satisfy simple recurrence relations. In particular, both can be expressed using continuants.

Definition 2.10 (Continuant)**.** The k-th continuant $Q_k(x_1, x_2, \ldots, x_k)$ is defined recursively by

$$\begin{aligned} &Q_0 = 1, \\ &Q_1(x_1) = x_1, \\ &Q_k(x_1, x_2, \ldots, x_k) = x_k Q_{k-1}(x_1, \ldots, x_{k-1}) + Q_{k-2}(x_1, \ldots, x_{k-2}). \end{aligned}$$

If p_k/q_k denotes the k-th convergent of a continued fraction, then

$$q_k = Q_k(m_1, \ldots, m_k), \qquad p_k = Q_{k+1}(m_0, \ldots, m_k).$$

An important property of continuants is their symmetry:

$$Q_k(x_1, \ldots, x_k) = Q_k(x_k, \ldots, x_1). \tag{2.3}$$

Chapter 4 studies lattices arising from ideals in imaginary quadratic fields. To describe these lattices, we first introduce quadratic fields and their rings of integers, which provide the fundamental arithmetic structure.

Definition 2.11 (Number Field)**.** A subfield K of $\mathbb{C}$ is called a number field if it has finite degree over $\mathbb{Q}$.

Definition 2.12 (Quadratic Field)**.** A quadratic field is defined as $\mathbb{Q}(\sqrt{\Delta})$ where Δ is not a perfect square.

Throughout this thesis, our focus will lie on imaginary quadratic fields, that is, quadratic fields of the form $\mathbb{Q}(\sqrt{\Delta})$ with $\Delta < 0$.

Every quadratic field admits a unique representation of the form $\mathbb{Q}(\sqrt{\Delta})$, where Δ is a square-free integer.

Definition 2.13 (Algebraic Integer)**.** [Ste12, Def. 2.3.3] Let K be a number field, then $x \in K$ is an algebraic integer if it is a root of a monic polynomial with coefficients in $\mathbb{Z}$.

The algebraic integers of a number field form a ring, known as its ring of integers.

Definition 2.14 (Ring of Integers)**.** Let K be a number field, the ring of integers of K is defined as all algebraic integers of K.

$$\mathcal{O}_K = \{\alpha \mid \alpha \in K,\ \alpha \text{ is an algebraic integer}\}.$$

Proposition 2.15. *Let K be a number field, the set $\mathcal{O}_K = \{\alpha \mid \alpha \in K,\ \alpha$ is an algebraic integer$\}$ is a commutative ring with unity.*

As $\mathcal{O}_K$ is a ring, it is logical to consider the lattices that lie in it.

Definition 2.16. [Sta21, Def. 1] A complex lattice $\Lambda = \alpha\mathbb{Z} + \beta\mathbb{Z}$ is called a K-lattice if $\beta/\alpha \in K$, where K is an imaginary quadratic field.

Any K-lattice can be scaled to lie as a sublattice in the ring of integers $\mathcal{O}_K$ [Sta21, p. 3].

Definition 2.17. [Sta21, Def. 2] The order of a K-lattice Λ is defined as

$$\mathrm{ord}(\Lambda) = \{x \in \mathbb{C} \mid x\Lambda \subseteq \Lambda\}.$$

Proposition 2.18. *[Sta21, Prop. 2] The* $\mathrm{ord}(\Lambda)$ *is a subring of $\mathcal{O}_K$ with unity.*

K-lattices are closely related to binary quadratic forms, which will be discussed in detail in Chapter 4.

Definition 2.19 (Binary Quadratic Form)**.** [Bue89] A binary quadratic form (BQF) is a function f in two variables $f(x, y) = ax^2 + bxy + cy^2$ with integer coefficients a, b and c. We denote a binary quadratic form by $f = (a, b, c)$.

Definition 2.20. [Joh07] The discriminant of binary quadratic form $f = (a, b, c)$ is defined as $\Delta = b^2 - 4ac$.

The discriminant is the fundamental invariant of a binary quadratic form and determines many of its properties.

Proposition 2.21. *The binary quadratic form $f = (a, b, c)$ is called*

1. *positive definite, iff $\Delta < 0$ and $a > 0$.*
2. *primitive, iff* $\gcd(a, b, c) = 1$.

2.3 Transfer Operators

To study how the distribution of lattices evolves under successive reduction steps, we introduce the transfer operator, which naturally describes the pushforward of distributions under the induced dynamical system.

Definition 2.22 (Transfer Operator)**.** [Rue02] The transfer operator $\mathcal{L}$ acting on functions $\Phi : \Lambda \to \mathbb{C}$ is defined as

$$(\mathcal{L}\Phi)(x) = \sum_{y \in F^{-1}(x)} g(y)\Phi(y),$$

where $F : \Lambda \to \Lambda$ and $g : \Lambda \to \mathbb{C}$ are maps.

Here, F describes the underlying dynamical system, while g is a weight function. The function Φ typically represents a density or distribution.

Remark 2.23. [Rue02] A particularly important choice of the weight function is

$$g = \frac{1}{|J|},$$

where $|J|$ denotes the Jacobian determinant of F, whenever it exists. In this setting, the image of the measure $\Phi(x)dx$ under F is given by

$$(\mathcal{L}\Phi)(x)dx.$$

Thus, the transfer operator exactly describes the pushforward of densities in a dynamical system.

2.4 Spectral Theory

One of the primary focuses of this thesis is the long-term growth of the transfer operator. To analyze this asymptotic behavior we use tools from functional analysis, in particular from spectral theory.

Definition 2.24. Let T be a bounded linear operator on a Banach space. Then the spectrum of T is defined as

$$\sigma(T) = \{\lambda \in \mathbb{C} \mid T - \lambda I \text{ is not bijective}\}.$$

Definition 2.25. The spectral radius of the same operator T as above is defined as

$$r(T) = \sup_{\lambda \in \sigma(T)} |\lambda|.$$

The spectral radius is closely related to the asymptotic growth of the iterates of an operator, as shown by Gelfand's spectral radius formula.

Theorem 2.26 (Gelfand's Spectral Radius Formula)**.** *Let T be a bounded linear operator in a Banach space. Then:*

$$r(T) = \lim_{n \to \infty} \|T^n\|^{1/n}.$$

This theorem is especially useful for compact operators, since the spectral radius is attained by an eigenvalue whenever it is nonzero.

Theorem 2.27. *Let X be a Banach space, and C a compact operator acting on X. Then every non-zero $\lambda \in \sigma(C)$ is an eigenvalue of C.*

Since determining the entire spectrum of an operator is often unnecessary and difficult in practice, it is useful to focus on the eigenvalues of largest modulus. The spectral gap and the spectral ratio measure the relationship between the two largest eigenvalues and provide information about the asymptotic behavior of the operator.

Definition 2.28. Assume that the eigenvalues of T can be ordered by decreasing modulus as $|\lambda_1| \geq |\lambda_2| \geq \ldots$, where the eigenvalue λ_1 is called the dominant eigenvalue, while λ_2 is called the subdominant eigenvalue. The spectral gap is defined as

$$|\lambda_1| - |\lambda_2|,$$

and the spectral ratio is defined as

$$\frac{|\lambda_2|}{|\lambda_1|}.$$

2.5 General Mathematical Background

In addition to the main conceptual framework introduced above, we recall several standard notions from analysis and measure theory that will be used throughout the thesis.

We begin with the definition of a norm, since it is a fundamental concept that appears repeatedly in the analysis of the lattice bases.

Definition 2.29. Given a Vector space X, a norm in X is a real-valued function $\|\cdot\| : X \to \mathbb{R}$ with the following properties.

1. Positive definiteness: $\|x\| \geq 0 \quad \text{and} \quad \|x\| = 0 \iff x = 0 \quad \forall x \in X.$
2. Absolute homogeneity: $\|ax\| = |a|\|x\| \quad \forall x \in X, a \in \mathbb{R}.$
3. Triangle equation: $\|x + y\| \leq \|x\| + \|y\| \quad \forall x, y \in X.$

A commonly used norm in functional analysis is the supremum norm.

Example 2.30. An example of a norm is the supremum norm. Let $f : X \to Y$ be a function, then the supremum norm is defined as

$$\|f\|_\infty = \sup_{x \in X} \|f\|_Y,$$

where $(Y, \|\cdot\|_Y)$ is a normed space.

To apply functional-analytic techniques to the transfer operator, we work in a suitable Banach space, which provides the structure required for proving the operator properties introduced in Chapter 3.

Definition 2.31 (Banach Space)**.** A normed linear space $(X, \|\cdot\|)$ is said to be a Banach space if it is a complete Metric space.

A key part of this thesis is to describe the distribution of the studied lattices, which requires introducing the notion of a probability density function.

Definition 2.32 (Probability Density Function)**.** Let $(X, \mathcal{A})$ be a measurable space with a reference measure μ. A probability measure Pr on $(X, \mathcal{A})$ is absolutely continuous if

$$\Pr[A] = \int_A \rho \; d\mu, \quad \forall A \in \mathcal{A},$$

for some measurable function $\rho : X \to [0, \infty)$. This function is called the probability density function [PDF] of Pr with respect to μ. Additionally,

$$\int_X \rho \; d\mu = 1.$$

Finally, we recall a classical compactness criterion in Euclidean spaces, which will be used to show the nuclearity property of the transfer operator.

Theorem 2.33 (Heine-Borel)**.** *Any subset of a Euclidean space is compact if and only if it is closed and bounded.*

3 Probabilistic Framework

3.1 Tail probability of Reduction steps

Let L denote the number of reduction steps required by the reduction algorithm. To understand how likely long reductions are, we study the tail probability

$$\Pr[L \geq k+1], \tag{3.1}$$

which is the probability that more than k reduction steps are required. Estimating this probability allows us to evaluate how frequently large numbers of reduction steps occur and provides a way to determine potential upper bounds on L. First, we consider lattices distributed uniformly and then we extend the analysis to lattices that come from an arbitrary input density.

3.2 From Algorithm to dynamical system

This section follows the complex dynamical framework introduced in [DFV96]. For the entirety of this thesis we will use the complex Algorithm 2 to analyze. We can rewrite the reduction step $U(z)$ of Algorithm 2 in the following way:

$$z_{k+1} = -m_{k+1} + \frac{1}{z_k}, \text{ where } m_{k+1} := \lfloor \Re(\frac{1}{z_k}) \rfloor \implies z_k = \frac{1}{m_{k+1} + z_{k+1}},$$

where z_k denotes the complex lattice obtained after k reduction steps.

We now notice that the reversed reduction step is exactly of the form of a generalized continued fraction with depth k, as introduced in equation (2.2). This defines a homography $h_{\mathbf{m}} = h_{m_1,m_2,\ldots,m_k}$ by

$$h_{\mathbf{m}}(x) = \cfrac{1}{m_1 + \cfrac{1}{m_2 + \cfrac{1}{\ddots + \cfrac{1}{m_k + x}}}},$$

with all m_i being strictly positive integers. Hence,

$$z_0 = h_{\mathbf{m}}(z_k).$$

We denote the depth of a homography h by $|h|$. We say that the homography $h_{m_1,\ldots,m_k}$ corresponds to a word $\mathbf{m} = [m_1, \ldots, m_k]$.

Recall that the reduction algorithm runs on z in the fundamental disk $\mathcal{D} = \{z \mid \mathrm{Re}(\frac{1}{z}) \geq 1\}$ and stops as soon as z is no longer in $\mathcal{D}$. With this in mind, one can describe the event $[L \geq k+1]$ as a set of all z such that all $k+1$ iterations of its reduction step $U(z)$ are still in $\mathcal{D}$.

$$[L \geq k+1] = \{z \mid U^j(z) \in \mathcal{D}\ \forall j \in \{0, \ldots, k\}\}. \tag{3.2}$$

As soon as one iteration $U^j(z)$ is no longer inside $\mathcal{D}$ all the next iterations are also outside $\mathcal{D}$. In other words, once a lattice is reduced, it will stay so, even after applying further reduction steps. With this property, we can define a decreasing chain of domains $\mathcal{D}_k = \{z \mid U^j(z) \in \mathcal{D}\ \forall j \in \{0, \ldots, k\}\}$, and for $k = 0$ we define $\mathcal{D}_0 = \mathcal{D}$ as the fundamental disk.

Proposition 3.1. *Each domain $\mathcal{D}_k$ describes the event that at least $k+1$ reduction steps are required, that is,*

$$[L \geq k+1] = \mathcal{D}_k.$$

Proof. First, we prove the inclusion $[L \geq k+1] \subseteq \mathcal{D}_k$.

$$\begin{aligned} z \in [L \geq k+1] &\implies U^j(z) \in \mathcal{D}\ \ \forall j \in \{0, \ldots, k\} \implies z \in U^{(-j)}(\mathcal{D})\ \ \forall j \in \{0, \ldots, k\} \\ &\implies z \in U^{(-k)}(\mathcal{D}) = \mathcal{D}_k. \end{aligned}$$

Secondly, we prove the contrary inclusion $\mathcal{D}_k \subseteq [L \geq k+1]$.

$$\begin{aligned} z \in \mathcal{D}_k = U^{(-k)}(\mathcal{D}) &\implies U^k(z) \in \mathcal{D} \implies U^j(z) \in \mathcal{D} \ \ \forall j \in \{0, \dots, k\} \\ &\implies z \in [L \geq k+1]. \end{aligned}$$

Both inclusions together prove the set equality $[L \geq k+1] = \mathcal{D}_k$. □

The domains can now be represented using the homographies h.

Proposition 3.2. *Each domain $\mathcal{D}_k$ is the following disjoint union up to measure 0 boundary terms.*

$$\mathcal{D}_k = \bigsqcup_{|h|=k} h(\mathcal{D}) \ . \tag{3.3}$$

Proof. If $z \in \mathcal{D}_k$, then this implies $U^k(z) \in \mathcal{D}$, which is exactly the same as saying there exists a word $[m_1, \dots, m_k]$ such that $h_{m_1,\dots,m_k}(z) \in \mathcal{D}$. That is exactly the same as $z \in \bigcup_{|h|=k} h(\mathcal{D})$. The other implication uses similar arguments. Given $h_{\mathbf{m}}(z) \in \mathcal{D}$ for an arbitrary h with depth $|h| = k$, we know that $U^k(z) \in \mathcal{D}$ because that is exactly how we defined the homography h. The disjointness holds since every finite continued fraction corresponds to a unique number, which means there cannot be two different words that lead to the same result. That is, $\nexists\, \mathbf{m} \neq \mathbf{m}'$ such that $h_{\mathbf{m}}(z) = h_{\mathbf{m}'}(z)$. □

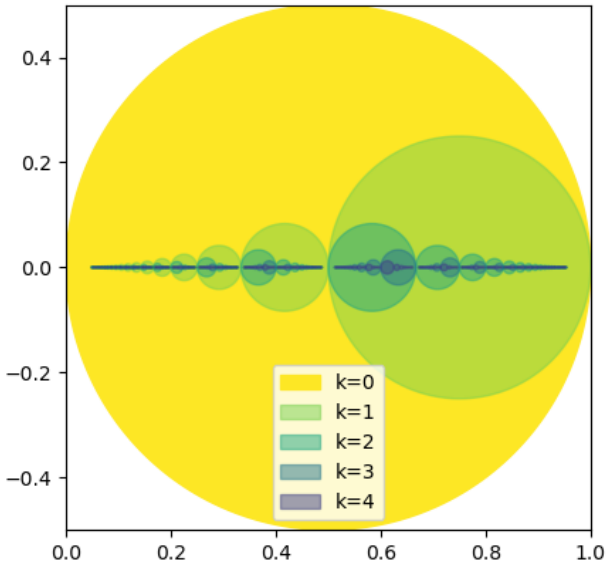

Figure 3.1: The domains D_k for $k \in \{0, 1, 2, 3, 4\}$.

Since homographies h are möbius transformations, they map disks into disks. Consequently, each set $h(\mathcal{D})$ appearing in the decomposition of Proposition 3.2 is again a disk. This is clearly visible in Figure 3.1 as one can see that each domain consists of an union of disks which decrease in size.

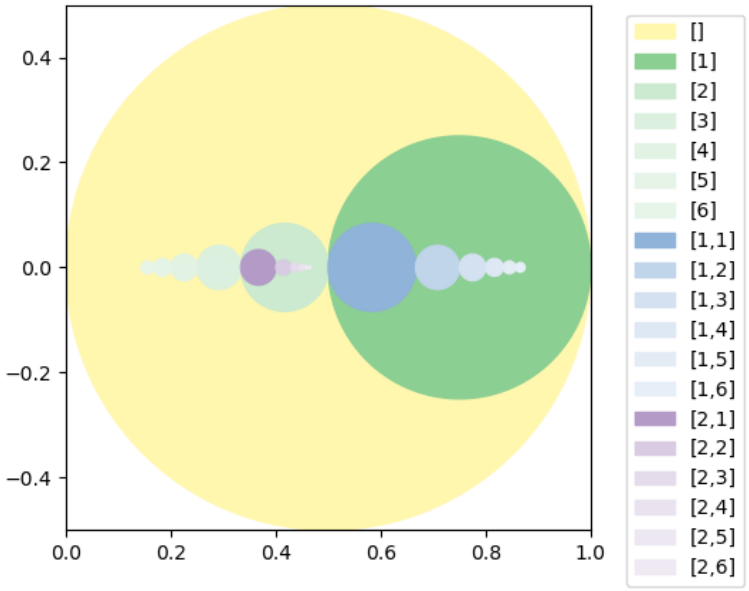

Figure 3.2: The Disks and their corresponding words, computed as explained in Section 5.2.

Depth k	Word $\mathbf{m}$	Homography $h_{\mathbf{m}}$	Disk
0	$\emptyset$	id	$\mathcal{D}$
1	$[m_1]$	$h_{m_1}(z) = \dfrac{1}{m_1 + z}$	$h_{m_1}(\mathcal{D})$
2	$[m_1, m_2]$	$h_{m_1,m_2}(z) = \dfrac{1}{m_1 + \dfrac{1}{m_2 + z}}$	$h_{m_1,m_2}(\mathcal{D})$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
k	$[m_1, \ldots, m_k]$	$h_{m_1,\ldots,m_k}(z)$	$h_{m_1,\ldots,m_k}(\mathcal{D})$

Table 3.1: Correspondence between words, homographies and disks.

In Table 3.1 the m_i are strictly positive integers, and since each homography $h_{\mathbf{m}}$ is defined using a word $\mathbf{m}$, the disk $h_{\mathbf{m}}(\mathcal{D})$ corresponds to the same word, which is visualized in Figure 3.2. With this relation in mind, we can better understand what the domains D_k really are.

$$\begin{aligned} k = 0 \quad &: \quad \mathcal{D} \\ k = 1 \quad &: \quad \mathcal{D}_1 = \bigsqcup_{m_1} h_{m_1}(\mathcal{D}) \\ k = 2 \quad &: \quad \mathcal{D}_2 = \bigsqcup_{m_1,m_2} h_{m_1,m_2}(\mathcal{D}) \\ &\vdots \\ k \quad &: \quad \mathcal{D}_k = \bigsqcup_{|\mathbf{m}|=k} h_{\mathbf{m}}(\mathcal{D}). \end{aligned}$$

We can express homographies of depth k using continuants (Definition 2.10):

$$h_{\mathbf{m}}(z) = \frac{P_k + zP_{k-1}}{Q_k + zQ_{k-1}}, \tag{3.4}$$

where

$$Q_k(h) = Q_k(m_1, \ldots, m_k), \quad Q_{k-1}(h) = Q_{k-1}(m_1, \ldots, m_{k-1}),$$

$$P_k(h) = Q_{k-1}(m_2, \ldots, m_k), \quad P_{k-1}(h) = Q_{k-2}(m_2, \ldots, m_{k-1}).$$

And note that the following determinant identity holds

$$Q_k P_{k-1} - Q_{k-1} P_k = (-1)^k. \tag{3.5}$$

This representation then leads to equation [DFV96]

$$\Pr[L \geq k+1] = \sum_{|h|=k} \frac{1}{Q_k^2 (Q_k + Q_{k-1})^2}.$$

3.3 Lattices with uniform input density

Let us first consider the case where the lattices z are uniformly distributed in $\mathcal{D}$. We are talking about a continuous distribution where the probabilities are determined by areas rather than by counting points. We therefore denote the area of a set by $\|\cdot\|$. The set $\mathcal{D}_k$ consists of all complex lattices $z \in \mathcal{D}_k$ that are not yet reduced after k reduction steps. Hence, the probability that more than k reduction steps are required is given by

$$\Pr[L \geq k+1] = \frac{\|\mathcal{D}_k\|}{\|\mathcal{D}\|}. \tag{3.6}$$

Using the decomposition

$$\mathcal{D}_k = \bigsqcup_{|h|=k} h(\mathcal{D}),$$

the area of $\mathcal{D}_k$ can be expressed as the sum of the areas of its disjoint components. Consequently, as shown in [DFV96],

$$\Pr[L \geq k+1] = \frac{\|\mathcal{D}_k\|}{\|\mathcal{D}\|} \overset{(2)}{=} \frac{4}{\pi} \sum_{|h|=k} \|h(\mathcal{D})\| \tag{3.7}$$

$$\overset{(3)}{=} \frac{4}{\pi} \sum_{|h|=k} \left| \frac{h(0) - h(1)}{2} \right|^2 \pi = \sum_{|h|=k} |h(0) - h(1)|^2 . \tag{3.8}$$

For the equality marked by (2), we use that $\mathcal{D}$ is a disk of radius $1/2$, so that

$$\|\mathcal{D}\| = \frac{\pi}{4}.$$

For the equality marked by (3), we use the fact that the homographies h have real coefficients and, therefore, map the real axis to itself. Since 0 and 1 are the endpoints of a diameter of $\mathcal{D}$, their images $h(0)$ and $h(1)$ are the endpoints of a diameter of the disk $h(\mathcal{D})$. Consequently, $h(\mathcal{D})$ has radius

$$\left| \frac{h(0) - h(1)}{2} \right|,$$

and therefore area

$$\|h(\mathcal{D})\| = \pi \left| \frac{h(0) - h(1)}{2} \right|^2 .$$

3.3.1 Transfer Operator representation for uniform input density

To get an estimate of the probability, we can use a transfer operator, as it naturally describes the evolution of a distribution after each iteration. And our goal is to understand how the initial probability density behaves under the iteration of the $U(z)$ map.

Following the Definition 2.22, we define the transfer operator for the uniform case.

In our case the dynamical system is represented by $F = U$ and the distribution by $\phi = f$. Hence, the condition of the sum can be rewritten in terms of homographies of depth 1:

$$y \in U^{-1}(x) \iff U(y) = x \iff \frac{1}{y} - m = x \iff y = \frac{1}{m+x} = h(x),$$

with $|h| = 1$. Thus, the transfer operator can be written as

$$(\mathcal{L}f)(z) = \sum_{y=h(z),|h|=1} g(y)f(y),$$

with $g = 1/|J|$, where $|J|$ is the determinant of the Jacobian matrix of U.

To determine the weight function g, we compute the Jacobian determinant of the map U. Writing $z = x + iy$, we express $U = 1/z - m$ in terms of the real variables x and y. Using

$$\frac{1}{z} = \frac{1}{x+iy} = \frac{x-iy}{(x^2+y^2)},$$

we obtain

$$U(x+iy) = \frac{x}{x^2+y^2} - m + i\frac{-y}{x^2+y^2} \implies U(x,y) = (U_1(x,y), U_2(x,y)),$$

where $U_1(x,y) = \frac{x}{x^2+y^2} - m$ and $U_2(x,y) = \frac{-y}{x^2+y^2}$. Then we get the following Jacobian matrix:

$$J(U) = \begin{bmatrix} \partial_x U_1 & \partial_y U_1 \\ \partial_x U_2 & \partial_y U_2 \end{bmatrix} = \frac{1}{M^2}\begin{bmatrix} y^2-x^2 & -2yx \\ 2yx & y^2-x^2 \end{bmatrix},$$

where $M = (x^2+y^2)$. The determinant is given by

$$\begin{aligned} |J(U)| &= \frac{1}{M^4}[(y^2-x^2)^2 + 4x^2y^2] = \frac{1}{M^4}[y^4 - 2y^2x^2 + x^4 + 4x^2y^2] \\ &= \frac{(y^2+x^2)^2}{(x^2+y^2)^4} = \frac{1}{(x^2+y^2)^2} = \frac{1}{|z|^4}. \end{aligned}$$

Since

$$g(z) = \frac{1}{|J(U)(z)|} = |z|^4,$$

the transfer operator becomes

$$\begin{aligned} (\mathcal{L}f)(z) &= \sum_{y=h(z),|h|=1} g(y)f(y) = \sum_{|h|=1} g(h(z))f(h(z)) \\ &= \sum_{|h|=1} \frac{1}{|m+z|^4} f\Big(\frac{1}{m+z}\Big) = \sum_{m\geq 1} \frac{1}{|m+z|^4} f\Big(\frac{1}{m+z}\Big). \end{aligned}$$

To prepare for the functional-analytic setting in Section 3.5, we slightly enlarge the fundamental interval $[0,1]$ and choose a bounded open interval J satisfying $[0,1] \subsetneq J$. From now on, we will refer to the transfer operator for a uniform input density by $\mathcal{G}_s$.

For each inverse branch h, let $\widetilde{h}$ be the holomorphic function that coincides with $\sqrt{|h'|}$ on J. Using the identity

$$|h'(z)|^{s/2} = \widetilde{h}(z)^s,$$

the transfer operator can be written as

$$\mathcal{G}_s[f](z) = \sum_{|h|=1} \frac{1}{|m+z|^s} f\Big(\frac{1}{m+z}\Big) = \sum_{m\geq 1} \frac{1}{|m+z|^s} f\Big(\frac{1}{m+z}\Big) = \sum_{|h|=k} \tilde{h}(z)^s \; f\circ h(z). \tag{3.9}$$

And we see that its iteration is

$$\mathcal{G}_s^k[f](z) = \sum_{|h|=k} \frac{1}{|m+z|^s} f\Big(\frac{1}{m+z}\Big).$$

Using the above mentioned relation $h(z) = \frac{1}{m+z} = \frac{P_k+zP_{k-1}}{Q_k+zQ_{k-1}}$, the scalar appearing in each summand can be rewritten as

$$\begin{aligned}\frac{1}{(m+z)^s} = \tilde{h}(z)^s &= \sqrt{\Big|\Big(\frac{P_k+zP_{k-1}}{Q_k+zQ_{k-1}}\Big)'\Big|^s} \\ &= \sqrt{\Big|\frac{P_{k-1}(Q_k+zQ_{k-1}) - Q_{k-1}(P_k+zP_{k-1})}{(Q_k+zQ_{k-1})^2}\Big|^s} = \sqrt{\Big|\frac{Q_kP_{k-1}-Q_{k-1}P_k}{(Q_k+zQ_{k-1})^2}\Big|^s} \\ &\overset{3.5}{=} \sqrt{\Big|\frac{(-1)^k}{(Q_k+zQ_{k-1})^2}\Big|^s} = \frac{1}{(Q_k+zQ_{k-1})^s}\ .\end{aligned}$$

Hence,

$$\mathcal{G}_s^k[f](z) = \sum_{|h|=k} \frac{1}{(Q_k+Q_{k-1}z)^s} f\Big(\frac{P_k+zP_{k-1}}{Q_k+zQ_{k-1}}\Big).$$

For $z = 0$: using the symmetry property (2.3) and the equality $P_k(h) = Q_{k-1}(\hat{h})$, where h corresponds to the word $[m_1, \ldots, m_k]$ and $\hat{h}$ to $[m_k, \ldots, m_1]$, we get

$$\mathcal{G}_s^k[f](0) = \sum_{|h|=k} \frac{1}{Q_k^s} f\Big(\frac{Q_{k-1}}{Q_k}\Big).$$

And therefore we get the relation [DFV96]

$$\Pr[L \geq k+1] = \sum_{|h|=k} \frac{1}{Q_k^2(Q_k+Q_{k-1})^2} = \mathcal{G}_4^k[u(t)](0), \text{ where } u(t) = \frac{1}{(1+t)^2}.$$

This is important because it allows us to estimate the probability $\Pr[L \geq k+1]$ by analyzing the transfer operator $\mathcal{G}$.

3.4 Lattices with general input density

In the case of a general input density, the probability can no longer be expressed solely in terms of the areas of $\mathcal{D}_k$ as in (3.6). Instead, the density of the input distribution must be taken into account. Let ρ denote the input density. Then, with respect to the area measure $dA(z) = dx\,dy$ for $z = x + iy$, we have

$$\Pr[L \geq k+1] = \int_{\mathcal{D}_k} \rho(z)\ dA(z).$$

3.4.1 General Transfer Operator

In Chapter 3.3, we looked only at a uniform input density, which leads to the single-variable transfer operator $\mathcal{G}$, if we were to work with a single-variable transfer operator for any input density, an additional weight factor depending on the input density would be required. To avoid this dependence, we introduce the general transfer operator with two variables, which arises naturally when rewriting probability $\Pr[L \geq k+1]$.

Let ρ be the probability density function (PDF) that describes the input distribution of the lattices, and denote the probability coming from this PDF as $\Pr_\rho$. We use the measure for complex numbers $d\mu = dA(z)$, which is just $dxdy$ for $z = x + iy$.

$$\Pr_\rho[L \geq k+1] = \int_{\mathcal{D}_k} \rho(z)\ dA(z) \overset{3.2}{=} \sum_{|h|=k} \int_{h(\mathcal{D})} \rho(z) dA(z) \tag{3.10}$$

$$= \sum_{|h|=k} \int_{\mathcal{D}} \rho(h(w))\ |J(h(w))|\ dA(w), \tag{3.11}$$

where the last equation comes from a change of variable $z = h(w)$, and $|J(h(w))|$ is the determinant of the Jacobian matrix. The next step is to find the Jacobian determinant, and for this, we rewrite the function h as a function of two real variables instead of one complex variable.

$$h(w) = \frac{1}{m+w}, \quad w = x + iy \in \mathbb{C}\,,$$

$$h(x+iy) = \frac{m+x}{(m+x)^2+y^2} + i\frac{-y}{(m+x)^2+y^2}.$$

This gives the following Jacobian matrix.

$$J(h(x+iy)) = \frac{1}{M^2}\begin{bmatrix} y^2-(x+m)^2 & -2y(x+m) \\ 2y(x+m) & y^2-(x+m)^2 \end{bmatrix},$$

where $M = (m+x)^2 + y^2$.

Hence, the Jacobian determinant is

$$\begin{aligned}
|J(h(w))| &= \left| \frac{1}{M^4}\left[(y^2-(x+m)^2)^2 + (2y(x+m))^2\right] \right| \\
&= \left| \frac{y^4 - 2y^2(x+m)^2 + (x+m)^4 + 4y^2(x+m)^2}{((m+x)^2+y^2)^4} \right| \\
&= \left| \frac{((m+x)^2+y^2)^2 - 2y^2(x+m)^2 + 2y^2(m+x)^2}{((m+x)^2+y^2)^4} \right| \\
&= \frac{1}{((m+x)^2+y^2)^2} = \frac{1}{|m+w|^4} = \frac{1}{(m+w)^2(m+\overline{w})^2} = |h'(w)|^2.
\end{aligned}$$

This leads to the following representation of the probability coming from the equation (3.11).

$$\begin{aligned}
\Pr_{\rho}[L \geq k+1] &= \sum_{|h|=k} \int_{\mathcal{D}} \rho(h(w))\ |h'(w)|^2\ dA(w) \\
&= \sum_{|h|=k} \int_{\mathcal{D}} \rho(h(w))\ \frac{1}{(m+w)^2(m+\overline{w})^2}\ dA(w).
\end{aligned}$$

Definition 3.3 (General transfer operator)**.** [Val97] The general transfer operator is defined by

$$\mathbf{G}_{s,t}[F](u,v) = \sum_{m\geq 1} \frac{1}{(m+u)^s(m+v)^t} F\Big(\frac{1}{m+u}, \frac{1}{m+v}\Big).$$

And its iteration

$$\mathbf{G}^k_{s,t}[F](u,v) = \sum_{|h|=k} \tilde{h}(u)^s \tilde{h}(v)^t F(h(u),h(v)) = \sum_{|h|=k} \mathbf{C}^{(h)}_{s,t}, \tag{3.12}$$

where the holomorphic function $\tilde{h}(u)$ coincides with $\sqrt{h'(u)}$ on the interval J.

We can use this operator to rewrite the probability.

$$\Pr_{\rho}[L \geq k+1] = \int_{\mathcal{D}} \mathbf{G}^k_{2,2}[F](u,\overline{u})\ dA(u). \tag{3.13}$$

For a function F such that $F(x+iy, x-iy) = \rho(x,y)$ or in complex notation $F(u,\overline{u}) = \rho(u)$.

Notice that the general transfer operator $\mathbf{G}$ is again independent of the input density, as is the usual transfer operator $\mathcal{G}$ for the uniform input density.

3.5 Spectral Analysis of the Transfer Operator

3.5.1 Uniform transfer operator

To get an estimation on the transfer operator, we want to use the dominant eigenvalue since by the Gelfand's formula (Theorem 2.26) the dominant eigenvalue controls the growth rate of the operator.

$$r(\mathcal{G}_s) := \lambda_s = \lim_{k\to\infty} \|\mathcal{G}_s^k\|^{1/k},$$

where $r(\mathcal{G}_s)$ denotes the spectral radius of $\mathcal{G}_s$.

We want to apply the Perron-Frobenius theorem to show that $\mathcal{G}$ has a positive dominant eigenvalue. We use the Krasnosel'skii theorem [Kra64], so we need the transfer operator $\mathcal{G}_s$ to be compact and u_0-positive. We introduce the notion *nuclear of order 0* which implies compactness.

Definition 3.4 (Nuclear of order 0)**.** [DFV96] Let B be a Banach space and B^* its dual space. An operator $M : B \to B$ is called *nuclear of order* 0 if it admits the representation

$$M[f] \;=\; \sum_{i\in I} \mu_i e_i^*(f) e_i \quad \text{for all } f \in B,$$

with $e_i \in B$, $e_i^* \in B^*$ such that $\|e_i\| = \|e_i^*\| = 1$ and $\sum |\mu_i|^p < \infty \,\forall p > 0$.

Proposition 3.5. *If $\mathcal{G}_s$ is nuclear of order 0, then $\mathcal{G}_s$ is compact.*

Proof. Let us assume that the operator $\mathcal{G}_s : A_\infty(\mathcal{V}) \to A_\infty(\mathcal{V})$ is nuclear of order 0. That is, we have the representation

$$\mathcal{G}_s[f] = \sum_{i\in I} \mu_i \; e_i^*(f) \; e_i,$$

where $\|e_i\| = \|e_i^*\| = 1$ and for all $p > 0 \quad \sum |\mu_i|^p < \infty$. Defining $T_i[f] := \mu_i e_i^*(f) e_i$, we observe that the rank of T_i is 1, since for fixed i we have that $e_i^*(f)$ is just a complex constant. So, taking the partial sum $\sum_i^n T_i[f] =: \mathcal{G}_{s,n}$, we know that this operator is of finite rank. Using functional analysis knowledge, we know that $\mathcal{G}_{s,n}$ is compact. Lastly, we show that the operator $\mathcal{G}_s$ is actually the norm limit of these partial operators $\mathcal{G}_{s,n}$.

$$\|(\mathcal{G}_s - \mathcal{G}_{s,n})[f]\| = \left\| \sum_{i=n+1}^{\infty} \mu_i \; e_i^*(f) \; e_i \right\| \le \sum_{i=n+1}^{\infty} |\mu_i| \; |e_i^*(f)| \; \|e_i\| \le \sum_{i=n+1}^{\infty} |\mu_i| \; \|f\|$$

$$\implies \|\mathcal{G}_s - \mathcal{G}_{s,n}\| \le \sum_{i=n+1}^{\infty} |\mu_i|.$$

And since we know that $\sum |\mu_i|^p < \infty$ is especially true for $p = 1$, we know that the tail $\sum_{i=n+1}^{\infty} |\mu_i| \longrightarrow 0$ as $n \to \infty$. This concludes that the operator $\mathcal{G}_s$ is compact when it is nuclear of order 0. □

As mentioned before, J is a bounded open interval that strictly contains the interval $[0, 1]$ and let $\mathcal{V}$ be an open disk with diameter J. In addition, we need $h(\overline{\mathcal{V}}) \subsetneq \mathcal{V}$ for each homography of depth 1.

Remark 3.6. [DFV96] The interval J is usually chosen in the form $(-\delta, 1+3\delta)$, where $0 < \delta \le 1/2$. A good choice is for example $\delta = 1/2$, that is the open disk with center 1 and radius 3/2.

We choose the suitable Banach space

$$\mathcal{A}_\infty(\mathcal{V}) = \left\{ f : \mathcal{V} \to \mathbb{C} \;\middle|\; f \text{ holomorphic on } \mathcal{V} \text{ and continuous on } \overline{\mathcal{V}} \right\}. \tag{3.14}$$

In this space, each bounded operator is *nuclear of order 0*. For the following proposition it is important to introduce the following notation of the transfer operator.

$$\mathcal{G}_s^k = \sum_{|h|=k} \mathcal{C}_s^{(h)}, \quad \mathcal{C}_s^{(h)}[f](z) = \tilde{h}(z)^s f \circ h(z).$$

Proposition 3.7. *The transfer operator $\mathcal{G}_s$ is nuclear of order 0 on the Banach space $\mathcal{A}_\infty(\mathcal{V})$.*

Proof. As stated above, it is only necessary to prove boundedness to show nuclearity of order 0. We will use the argument that since $\mathcal{G}$ is a convergent sum of bounded operators, it is also bounded. So, the only thing we need to prove, is that the operators $\mathcal{C}_s^{(h)}$ are bounded. For this, notice that by Heine-Borel $\overline{\mathcal{V}}$ is compact since it is bounded and closed in $\mathbb{R}^2$ (2.33). We have that $h'(z) = -\frac{1}{(m+z)^2}$ is continuous if and only if $z = -m$ is not in $\mathcal{V}$, that is, it is not possible to attain. Since $m > 1$ we have $-m < -1/2$. Therefore, $-m$ is not in $\mathcal{V}$ by Remark 3.6. Therefore, we find that h' is continuous in the compact set $\overline{\mathcal{V}}$ and this implies that its supremum and infimum exist. Let $M_h := \sup_z |h'(z)| < \infty$ be this supremum. So we now find that $h' < M_h$ is bounded, and hence $\tilde{h}$ is bounded. f is a function in $\mathcal{A}_\infty(\mathcal{V})$, which means that f is continuous on $\overline{\mathcal{V}}$ and therefore also bounded by its supremum $\|f\| < \infty$. As a last step, we use the condition $h(\overline{\mathcal{V}}) \subsetneq \mathcal{V}$ to show that the composition with h is still bounded. $|f(h(z))| < \sup_{w\in h(\mathcal{V})} |f(w)| = \sup_{w\in\mathcal{V}} |f(w)| = \|f\| < \infty$. Putting everything together, we exactly get that each $\mathcal{C}_s^{(h)}$ is bounded. □

By Proposition 3.7 we now know that the transfer operator $\mathcal{G}_s$ is compact in the Banach space $\mathcal{A}_\infty(\mathcal{V})$.

We will show the positivity of the transfer operator $\mathcal{G}_s$ using the notion of u_0-positive with respect to a cone.

Definition 3.8 (Proper Reproducing Cone)**.** [DFV96] A proper cone in a real space B is a set K such that

1. for every positive p and for every element f in K the product pf is again an element of K;
2. the only element of K whose negative also belongs to K is the zero element.

A proper cone is called *reproducing* if every element of B can be written as the difference of two elements of K, that is, if $B = K - K$.

Definition 3.9 (u_0-positivity with respect to a cone)**.** [DFV96] Let K be a proper reproducing cone with a non-empty interior K°. An operator $M : B \to B$ is positive with respect to a cone K if

$$M(K) \subset K.$$

Let $u_0 \in K^\circ$. A positive operator M is called u_0-positive with respect to a cone K if, for every non-zero element $f \in K$, there exists a positive integer p and positive real numbers α and β such that

$$\beta u_0 \leq M^p[f] \leq \alpha u_0.$$

Proposition 3.10. *The transfer operator $\mathcal{G}_s$ restricted to the real Banach space $R_\infty(\mathcal{V}) = \{f \in A_\infty(\mathcal{V}) \mid f(x) \in \mathbb{R}$ for all $x \in J\}$ is u_0-positive with respect to the proper reproducing cone $K = \{f \in R_\infty(\mathcal{V}) \mid f(x) \geq 0$ for all $x \in J\}$.*

Proof. First, we check that K is a proper reproducing cone. Let $p > 0$ be an arbitrary positive real number and $f \in K$ then $pf(x) \geq 0$ since both elements are positive and therefore $pf \in K$. Second, let $f \in K$ and $-f \in K$ then we have that $f(x) \geq 0$ and $-f(x) \geq 0 \implies f(x) \leq 0$ which can only hold if $f(x) = 0$. This shows $K \cap -K = \{0\}$. Last, we need to prove the reproducing property. Let $f \in R_\infty(\mathcal{V})$, define the positive and negative part as $f^+ = \max_x\{f(x), 0\}$ and $f^- = \max_x\{-f(x), 0\}$. Note that we can write $f = f^+ - f^-$ and both f^+ and f^- are positive functions and therefore in K. This concludes $R_\infty(\mathcal{V}) = K - K$.

Now we have a proper reproducing cone K. Let $u_0 = 1$, then u_0 is an element in the interior $K^\circ = \{f \in R_\infty(\mathcal{V}) \mid f(x) > 0$ for all $x \in J\}$.

With the restriction to the Banach space $R_\infty(\mathcal{V})$ the transfer operator $\mathcal{G}_s$ is u_0-positive with respect to K. For the upper bound α we define $M := \|f\|$ and $A_p = \sup_x\{\sum_{|h|=p} \tilde{h}(x)^s\}$ both exist because of the boundedness of $\mathcal{V}$ and the convergence of the sum. Then we can use the upper bound $\mathcal{G}_s^p[f] \leq M \sum_{|h|=p} \tilde{h}(x)^s \leq M A_p =: \alpha$. For the lower bound β, we use the fact that $f \neq 0$ and $f \geq 0$, which means $\exists\ x_0 \in J$ such that $f(x_0) > 0$ and by the continuity of the function

f we actually have a subinterval $J_0 \subset J$ where $f \geq c$ for some constant $c > 0$. Then we get $\mathcal{G}_s^p[f](x) \geq c \sum_{|h|=p, h(x)\in J_0} \tilde{h}(x)^s$.

Using the continuants representative (3.4) for $h(x)$ we get the following continuants expression for $\tilde{h}$.

$$\tilde{h}(x)^s = \frac{1}{(Q_k + xQ_{k-1})^s} \ , \quad |h| = k.$$

Let $b = \sup_x\{x \in J\}$ be the upper bound of the interval J. Then we get that for each h with depth p, $\tilde{h}(x)^s \geq \frac{1}{(Q_p + bQ_{p-1})^s}$ for all $x \in J$. Finally, we can take the homography h such that this term is the smallest, that is, $H = \min_{|h|=p} \frac{1}{(Q_p(h)+bQ_{p-1}(h))^s}$. This minimum exists and is strictly larger than zero since there are only finitely many words of length p. Therefore,

$$\mathcal{G}_s^p[f](x) \geq c \sum_{|h|=p, h(x)\in J_0} H > 0.$$

For the last inequality, we need to ensure that there exists at least one h such that $h(x) \in J_0$ for every $x \in J$. Since rationals are dense in $\mathbb{R}$ we find that there exists at least one rational number $q \in J_0$. And each rational number can be uniquely represented by a finite continued fraction. There exist p and a word $\mathbf{m} = [m_1, \ldots, m_p]$ such that $h_{\mathbf{m}}(0) = q \in J_0$. We observe that the image $h_{\mathbf{m}}(J)$ is again an interval. Since the intervals $h_{\mathbf{m}}(J)$ shrink as depth p increases, we can choose p to be sufficiently large and extend, respectively, the word $\mathbf{m}$ such that $h_{\mathbf{m}}(J) \subset J_0$. This concludes the proof. □

Now we can apply Krasnosel'skii theorems [Kra64, Thm. 2.5, 2.10 and 2.13] to the transfer operator $\mathcal{G}_s$, which shows that a compact and u_0-positive operator satisfies a Perron-Frobenius property. Note that Krasnosel'skii uses the term *completely continuous*, which means a continuous operator that maps every bounded set into a compact set [Kra64, p. 67]. This term is exactly what we call compact today for a linear operator.

Since the spectrum of $\mathcal{G}_s$ is real for real s [DFV96, p. 14], the spectrum is the same as the spectrum of the operator restricted to the real Banach space $R_\infty(\mathcal{V})$.

As in [DFV96, p. 14] stated, we have the following spectral decomposition: $\mathcal{G}_s^k[f] = \sum_i \lambda_{i,s}^k f_{i,s}^*[f] f_{i,s}$. So in our case, we have the following Perron-Frobenius properties.

Theorem 3.11 (Perron-Frobenius)**.** *[[DFV96, Thm. 8]; see also [May]] For real $s > 1$, $\mathcal{G}_s$ has a simple positive dominant eigenvalue $\lambda_s := \lambda_{1,s}$. With its corresponding eigenfunction f_s strictly positive on $\mathcal{J}$ and normalized by $f_s(0) = 1$. The adjoint operator $\mathcal{G}_s^*$ has a positive eigenfunctional f_s^* with eigenvalue λ_s such that $f_s^*[f] > 0$ if $f > 0$ on $\mathcal{J}$.*
If $\mathcal{P}_s$ denotes the projection on the dominant eigensubspace, $\mathcal{P}_s = f_s^* \otimes f_s$, then

$$\mathcal{G}_s = \lambda_s \mathcal{P}_s + \mathcal{N}_s, \text{ with } \mathcal{P}_s \circ \mathcal{N}_s = \mathcal{N}_s \circ \mathcal{P}_s = 0.$$

Coming from

$$\mathcal{G}_s[f] = \sum_i \lambda_{i,s} f_{i,s}^*[f] f_{i,s} = \lambda_s f_s^*[f] f_s + \sum_{i\leq 2} \lambda_{i,s} f_{i,s}^*[f] f_{i,s}.$$

And with iterating

$$\mathcal{G}_s^k[f](t) = \lambda_s^k f_s^*[f] f_s(t) + \mathcal{N}_s^k.$$

Now we want to estimate what $\mathcal{N}_s^k$ is

$$\left|\frac{\mathcal{N}_s^k[f](t)}{\lambda_s^k}\right| = \left|\frac{G_s^k[f](t)}{\lambda_s^k} - f_s^*[f] f_s(t)\right| \leq \frac{\|\mathcal{N}_s^k\|\|f\|}{\lambda_s^k} \leq \frac{C\rho_s^k\|f\|}{\lambda_s^k} \longrightarrow_{k\to\infty} 0 \ ,$$

where ρ_s is the spectral radius of $\mathcal{N}_s$, which is defined as the $max\{|\mu_s|$ eigenvalues smaller than $\lambda_s\} = |\mu_s|$ called the subdominant eigenvalue. This implies

$$\left|\mathcal{G}_s^k[f](t) - \lambda_s^k f_s^*[f] f_s(t)\right| \leq C(\frac{\rho_s}{\lambda_s})^k \|f\|.$$

So we get

$$\mathcal{G}_s^k[f](t) = \lambda_s^k f_s^*[f] f_s(t) \left(1 + \mathcal{O}\left(\left|\frac{\mu_s}{\lambda_s}\right|^k\right)\right)$$

for $k \to \infty$.

Combining what we have, we get

$$\Pr[L \geq k+1] = \mathcal{G}_4^k[u(t)](0) = \sum_i \lambda_{i,4}^k f_{i,4}^*[u] f_{i,4}(0) = \sum_i \lambda_{i,4}^k c_i, \tag{3.15}$$

where $c_i = f_{i,4}^*[u]$.

Now we can take out the dominant eigenvalue and get the following estimate

$$\Pr[L \geq k+1] = c\lambda_4^k \left[1 + \mathcal{O}\left(\left|\frac{\mu_4}{\lambda_4}\right|^k\right)\right], \tag{3.16}$$

where $\lambda_4 = \lambda_{1,4}$ is the dominant eigenvalue, μ_4 is the subdominant eigenvalue, and c is $f_{1,4}^*[u]$.

From this result, we can use an approximation of the dominant eigenvalue (and the subdominant eigenvalue) to get an asymptotical estimate of the probability $\Pr[L \geq k+1]$.

3.5.2 General transfer operator

Now we use the relation between the usual transfer operator $\mathcal{G}_s$ and the general transfer operator $\mathbf{G}_{s,t}$ to make similar use of the spectral properties. In this section, we will mostly follow the paper [Val97].

Similarly as for the uniform input density, we want to apply Perron-Frobenius. However, proving *nuclear of order 0* and u_0-positive is not as straightforward as for the single-variable transfer operator.

Let $\mathcal{V}$ be the open disk whose diameter is the interval $(-\delta, 2+\delta)$, where we choose $\delta = \frac{1}{4}$, so that $\mathcal{V}$ is the disk centered at 1 with radius $\frac{5}{4}$. We then define a suitable Banach space.

$$B_\infty(\mathcal{V}) = \{F \text{ holomorphic on } \mathcal{V} \times \mathcal{V} \text{ and continuous on } \overline{\mathcal{V}} \times \overline{\mathcal{V}}\},$$

equipped with the sup-norm

$$\|F\| = \sup\{|F(u,v)| \mid (u,v) \in \mathcal{V} \times \mathcal{V}\}.$$

Since we already know the exact parameters (s,t) of $\mathbf{G}_{s,t}^k$, that is, $s,t = 2$, we will follow the paper [Val97] and therefore restrict the operator to the same conditions:

$$(s+t) \in \mathbb{R}, \quad \Re(s+t) > 1, \quad \Re(s) \geq 1, \quad \Re(t) > -1.$$

In this case, the dominant spectral properties of $\mathbf{G}_{s,t}$ are mostly the same as those of $\mathcal{G}_{s+t}$ [Val97, p. 124]. We show that $\mathbf{G}_{s,t}$ is nuclear of order 0 and u_0 positive with respect to a cone, such that we can apply the Perron-Frobenius theorem.

Proposition 3.12. *[Val97] The general transfer operator* $\mathbf{G}_{s,t}$ *is nuclear of order 0.*

Proof. [Val97] The general transfer operator can be expressed as a convergent sum of operators $\mathbf{C}_{s,t}^{(h)}$ (see 3.12). Each of these operators is bounded on $B_\infty(\mathcal{V})$ and is therefore nuclear of order 0. Therefore, the general transfer operator $\mathbf{G}_{s,t}$ is also nuclear of order 0. □

Proposition 3.13. *[Val97] Let* $u_0 = 1$ *be the constant function equal to* 1*. Then for* $s+t \in \mathbb{R}$ *such that* $s+t > 1$*, the operator* $\mathbf{G}_{s,t}$ *restricted to the space* $B_\infty^{\mathbb{R}}(\mathcal{V}) = \{F \in B_\infty \mid f(u) = F(u,u) \in \mathbb{R}\ \forall u \in J\}$ *is* u_0*-positive with respect to the cone* $K' = \{F \in B_\infty^{\mathbb{R}} \mid f(u) = F(u,u) > 0\ \forall u \in J\} \cup \{f \equiv 0\}$.

The proof can be found in [Val97, p. 125].

Now we have a similar theorem as for the uniform input density transfer operator (3.11).

Theorem 3.14. *[Val97] Let $s,t \in \mathbb{C}$ be such that*

$$s+t \in \mathbb{R}, \;\; s+t > 1, \;\; \Re(s) \geq 1, \;\; \Re(t) > -1.$$

Then

1. *the operator $\mathbf{G}_{s,t} : \mathcal{B}_\infty \to \mathcal{B}_\infty$ has a unique simple dominant eigenvalue equal to the dominant eigenvalue λ_{s+t} of the operator $\mathcal{G}_{s+t}$. The dominant eigenvector $F_{s,t}$ of $\mathbf{G}_{s,t}$ and the dominant eigenvector f_{s+t} of $\mathcal{G}_{s+t}$ have the following relation*

$$F_{s,t}(u,v) = \int_0^1 \beta_{t,s}(y) f_{s+t}(u + (v-u)y) dy,$$

where

$$\beta_{t,s}(y) = \frac{\Gamma(s+t)}{\Gamma(s)\Gamma(t)} y^{t-1}(1-y)^{s-1} \;,$$

and $F_{s,t}(u,u) = f_{s+t}(u)$.

2. *If $\mathbf{P_{s,t}}$ is the projection on the dominant eigensubspace defined as $\mathbf{P_{s,t}} = f^*_{s+t} \otimes F_{s,t}$ then we have the representation*

$$\mathbf{G}_{s,t} = \lambda(s+t)\mathbf{P}_{s,t} + \mathbf{N}_{s,t},$$

where $\mathbf{P}_{s,t} \circ \mathbf{N}_{s,t} = \mathbf{N}_{s,t} \circ \mathbf{P}_{s,t} = 0$. For $F \in \mathcal{B}_\infty(\mathcal{V})$ we then have

$$\mathbf{G}^k_{s,t}[F](u,v) = \lambda^k_{s+t} f^*_{s+t}[f] F_{s,t}(u,v) + \mathbf{N}^k_{s,t}[F](u,v),$$

for all $k \geq 1$ and all $(u,v) \in \mathcal{V} \times \mathcal{V}$.

3. *The spectral gap is equal to the spectral radius of $\mathbf{N}_{s,t}$ divided by the spectral radius of $\mathbf{G}_{s,t}$.*

$$\nu_{s+t} = \frac{1}{\lambda_{s+t}} \max(\lambda_{s+t+2}, \mu_{s+t}),$$

where μ_{s+t} is the spectral radius of $\mathcal{N}_{s+t}$.

4. *For each constant $\nu_{s+t} < \alpha < 1$ we have*

$$\mathbf{G}^k_{s,t}[F](u,v) = \lambda^k_{s+t} f^*_{s+t}[f] F_{s,t}(u,v)(1 + \mathcal{O}(\|F\|\alpha^k)),$$

for all k and all functions F in $B_\infty(\mathcal{V})$ which are strictly positive on the diagonal.

Now we apply the spectral decomposition as in the above Theorem 3.14 (4.). Notice that we need that the function $F(w,\overline{w}) = \rho(w)$ is holomorphic for the spectral decomposition.

$$\begin{aligned}
\Pr_\rho[L \geq k+1] &= \int_{\mathcal{D}} \mathbf{G}^k_{2,2}[F](w,\overline{w}) \, dA(w) \\
&= \int_{\mathcal{D}} \lambda^k_4 f^*_4[\rho] F_{2,2}(w,\overline{w}) \left(1 + \mathcal{O}\left(\|F\|\alpha^k\right)\right) dA(w) \\
&= \lambda^k_4 f^*_4[\rho] \int_{\mathcal{D}} F_{2,2}(w,\overline{w}) \left(1 + \mathcal{O}\left(\|F\|\alpha^k\right)\right) dA(w) \\
&= \lambda^k_4 f^*_4[\rho] C_4 \left(1 + \mathcal{O}\left(\|F\|\alpha^k\right)\right),
\end{aligned}$$

where $C_4 := \int_{\mathcal{D}} F_{2,2}(w,\overline{w}) \, dA(w)$ is a constant.

To compute the constant C_4 we apply Theorem 3.14 (1.):

$$C_4 = \int_{\mathcal{D}} F_{2,2}(w,\overline{w}) \, dA(w) = \int_{\mathcal{D}} \int_0^1 \beta_{2,2}(y) f_4(w + (\overline{w}-w)y) \, dy dA(w) \tag{3.17}$$

$$= \int_{\mathcal{D}} \int_0^1 \frac{\Gamma(4)}{\Gamma(2)\Gamma(2)} y(1-y) f_4\left(w + (\overline{w}-w)\, y\right) \, dy dA(w) \tag{3.18}$$

$$= \frac{\Gamma(4)}{\Gamma(2)\Gamma(2)} \int_{\mathcal{D}} \int_0^1 (y - y^2) f_4(w + (\overline{w}-w)y) \, dy \, dA(w) \tag{3.19}$$

$$= 6 \int_{\mathcal{D}} \int_0^1 (y - y^2) f_4(w + (\overline{w}-w)y) \, dy \, dA(w). \tag{3.20}$$

Since we know that for each $n \in \mathbb{N}$ the Gamma function can be calculated by $\Gamma(n) = (n-1)!$ [Wei], we easily compute $\frac{\Gamma(4)}{\Gamma(2)\Gamma(2)} = 6$.

For readability, we restate the full equation:

$$\Pr_{\rho}[L \geq k+1] = \lambda_4^k f_4^*[\rho]\, C_4 \, \left(1 + \mathcal{O}\left(\|F\|\alpha^k\right)\right), \tag{3.21}$$

for $\nu_4 < \alpha < 1$.

This expression shows that, for suitable input densities ρ, the tail probability decays asymptotically at a geometric rate determined by the dominant eigenvalue λ_4. More precisely, the leading-order behavior is given by

$$\Pr_{\rho}[L \geq k+1] \sim \lambda_4^k \, f_4^*[\rho]\, C_4,$$

while the remaining terms decay exponentially faster.

4 Ideal Lattices

In the classical average-case analysis of Lagrange's algorithm, the input basis is sampled uniformly from a bounded region. However, in practice the lattice bases are not sampled uniformly at random. The lattices this thesis focuses on come from ideals in the ideal class group and are widely used among cryptography. The discussion begins with the definition of the ideal class group, followed by the correspondence between ideal classes, lattices, and binary quadratic forms. For a more detailed discussion of these concepts, see [Sta21].

Definition 4.1 (Ideal)**.** Given a commutative ring R, an ideal $I \subseteq R$ is an additive subgroup of R such that for $x, y \in I$ and $r \in R$ the following holds:

1. $x + y \in I$,
2. $rx \in I$.

An ideal I is called *principal* if there exists an element $a \in R$ such that

$$I = (a) := \{ra \mid r \in R\} = aR.$$

Definition 4.2 (Fractional Ideal)**.** Let $K = \mathbb{Q}(\sqrt{\Delta})$ be a quadratic field and let $\mathcal{O}_K$ be its ring of integers. A fractional ideal of $\mathcal{O}_K$ is an $\mathcal{O}_K$-submodule $I \subseteq K$ such that there exists a nonzero element $d \in \mathcal{O}_K$ satisfying

$$dI \subseteq \mathcal{O}_K.$$

Equivalently, $I = d^{-1}J$ for some nonzero $d \in \mathcal{O}_K$ and some ideal J of $\mathcal{O}_K$.

A principal fractional ideal is generated by a single non-zero element of $\mathcal{O}_K$.

Definition 4.3 (Ideal Class Group)**.** Let $K = \mathbb{Q}(\sqrt{\Delta})$ be a quadratic field and $\mathcal{O}_K$ its ring of integers. The ideal class group $\mathrm{Cl}(K)$ is the group of equivalence classes of non-zero fractional ideals of $\mathcal{O}_K$ under the equivalence relation

$$I \sim J \iff \exists\, \alpha, \beta \neq 0 \in \mathcal{O}_K : \ \alpha I = \beta J.$$

Multiplication is defined by $[I] \cdot [J] := [I \cdot J]$ and the identity element is the ideal class of the principal fractional ideals.

Corollary 4.4. *[Sta21, Corollary 1] The Ideal classes of $\mathcal{O}_K$ are in bijection with K-lattices of order $\mathcal{O}_K$, up to homothety. The identification is obtained by considering an ideal class as a complex lattice under a fixed embedding of K in $\mathbb{C}$.*

Definition 4.5 (Fundamental Discriminant)**.** [Sta21, Def. 5] A discriminant Δ is fundamental if it is of the form $\Delta = 4m$ for $m \equiv 2$ or $3 \mod 4$ and square-free. Or of the form $\Delta = m$ for $m \equiv 1 \mod 4$ and square-free.

Corollary 4.6. *[Sta21, Corollary 2] Let Δ be a negative fundamental discriminant associated to quadratic imaginary field K. There is a bijection between proper equivalence classes of integral binary quadratic forms of discriminant Δ and homothety classes of K-lattices of order $\mathcal{O}_K$.*

Using these corollaries, each ideal lattice can be associated with a binary quadratic form.

4.1 Lattices from Ideals

Let $\Delta < 0$ be a square-free integer and consider the quadratic field $\mathbb{Q}[\sqrt{\Delta}]$. To sample an ideal, we make use of the fact that we can sample a binary quadratic form of discriminant Δ and then construct the corresponding ideal. Algorithm 3 implements this procedure.

The Algorithm 3 loops over the primes p until a suitable binary quadratic form is found. To ensure that the resulting binary quadratic form has discriminant Δ, the third coefficient c of the binary quadratic form $f(p, \pm b, c)$ is chosen as

$$c = \frac{b^2 - \Delta}{4p}.$$

Algorithm 3 Sampling a class group element

[SBK24, p. 11]

Input: The discriminant Δ of the group.
Output: A class group element represented by (p, b).

r = $\log_2(|\Delta|)/2 - 1$
while True **do**
  p ← random prime of maximal bit-length r
  if $\left(\frac{\Delta}{p}\right) = 1$ **then**
    b = $\sqrt{\Delta}$ mod p
    if $b^2 - \Delta \bmod 4\text{p} \neq 0$ **then**
      continue
    end if
    if $\frac{b^2-\Delta}{4p} = 0$ or $\Delta \neq b^2 - 4p\frac{b^2-\Delta}{4p}$ **then**
      continue
    end if
    break
  end if
end while
sign ← random 1 or -1
return $(p, \text{sign} \cdot b)$

With this choice, the discriminant of $f(p, b, c)$ is

$$b^2 - 4pc = b^2 - 4p\frac{b^2 - \Delta}{4p} = b^2 - (b^2 - \Delta) = \Delta.$$

Since $\sqrt{\Delta} \mod p$ has two solutions, namely $\pm b$, the algorithm chooses a random possible class group element represented by the binary quadratic form (p, b) or $(p, -b)$. In practical cryptographic applications, a cryptographically secure hash function would be used to select one of the two square root solutions. However, in this thesis, the elements are chosen uniformly at random.

Note 4.7. The tuple (p, b) uniquely defines a binary quadratic form $f(p, b, c)$ with $c = \frac{b^2-\Delta}{4p}$.

To obtain a lattice basis that corresponds to (p, b) we use the following theorem.

Theorem 4.8. *[Sta21, Thm. 1] We have bijections $Cl(K) \leftrightarrow \{K - $ lattices of order $\mathcal{O}_K / \sim\} \leftrightarrow \{$BQF with discriminant $\Delta\}$ given by (left to right),*

$$\mathfrak{a} \mapsto \mathcal{L} = \alpha\mathbb{Z} + \beta\mathbb{Z} \mapsto N(\alpha x - \beta y)/N(\mathfrak{a})$$

and by (right to left),

$$ax^2 + bxy + cy^2 \mapsto \mathcal{L} = \mathbb{Z} + \frac{-b + \sqrt{\Delta}}{2a}\mathbb{Z} \mapsto \left(a, \frac{-b + \sqrt{\Delta}}{2}\right).$$

Applied to the BQF $f(p, b, c)$ with $c = \frac{b^2-\Delta}{4p}$, we get the following lattice and ideal.

$$\Lambda_f = \mathbb{Z} + \frac{-b + \sqrt{\Delta}}{2p}\mathbb{Z} \sim p\mathbb{Z} + \frac{-b + \sqrt{\Delta}}{2}\mathbb{Z}, \text{ by homothety equivalence.} \tag{4.1}$$

$$\mathfrak{a}_f = \langle p, \frac{-b + \sqrt{\Delta}}{2} \rangle. \tag{4.2}$$

Now for a negative discriminant $\Delta < 0$ we can use the representation in $\mathbb{R}^2$ rather than in $\mathbb{C}$. We use the equality $\sqrt{\Delta} = i\sqrt{|\Delta|}$.

$$p = p + 0 \cdot i \mapsto \begin{pmatrix} p \\ 0 \end{pmatrix} , \tag{4.3}$$

$$\frac{-b + \sqrt{\Delta}}{2} = -\frac{b}{2} + i\frac{\sqrt{|\Delta|}}{2} \mapsto \begin{pmatrix} -\frac{b}{2} \\ \frac{\sqrt{|\Delta|}}{2} \end{pmatrix} . \tag{4.4}$$

Currently, these two vectors live on the standard basis $(1, i)$ of $\mathbb{C}$ over $\mathbb{R}$. Since $\sqrt{|\Delta|}$ is generally irrational, computations involving these vectors require floating-point arithmetic and are therefore only approximate due to limited memory space. For computational purposes, it is preferable to work with vectors in $\mathbb{Q}^2$, where arithmetic can be performed exactly. To obtain such a representation, we change from the standard basis

$$(1, i)$$

to the basis

$$(1, \sqrt{\Delta}) = (1, i\sqrt{|\Delta|}).$$

With respect to this new basis, the lattice basis is represented by the vectors

$$\begin{pmatrix} p \\ 0 \end{pmatrix}, \qquad \begin{pmatrix} -\frac{b}{2} \\ \frac{1}{2} \end{pmatrix}. \tag{4.5}$$

Notice that with the basis change the inner product also changes:

$$\langle v, u \rangle = v_1 u_1 + \sqrt{\Delta}\, v_2 u_2, \text{ where } v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \text{ and } u = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}. \tag{4.6}$$

This is important since the norm and inner product are used in the lattice reduction algorithm and therefore need to be adapted to this new definition.

Finally, we have the two lattice basis vectors with respect to the basis $(1, \sqrt{\Delta})$:

$$v = \begin{pmatrix} p \\ 0 \end{pmatrix}, \; u = \begin{pmatrix} -\frac{b}{2} \\ \frac{1}{2} \end{pmatrix}. \tag{4.7}$$

The Algorithm 3 restricts the primes p to satisfy

$$p \leq \sqrt{\frac{|\Delta|}{4}}. \tag{4.8}$$

The following theorem shows that this condition ensures that the resulting basis is reduced.

Theorem 4.9. *The basis $v = (p, 0)^\top, u = (-b/2, 1/2)^\top$ with respect to the basis $(1, \sqrt{\Delta})$ is reduced for $p \in [0, \sqrt{|\Delta|/4}]$.*

Proof. We consider two cases for our reduction.

Case 1: $\|v\|^2 \leq \|u\|^2$**:** We have $|\langle v, u \rangle| = \frac{p|b|}{2} \leq \frac{p^2}{2} = \frac{\|v\|^2}{2}$, since $|b| < p$.

Case 2: $\|u\|^2 \leq \|v\|^2$**:** We have $b^2 + |\Delta| \leq 4p^2$.

$$\begin{aligned} |\langle u, v \rangle| \leq \frac{\|u\|^2}{2} &\iff \frac{p|b|}{2} \leq \frac{b^2 + |\Delta|}{8} \iff 4p|b| \leq b^2 + |\Delta| \\ &\iff 0 \leq b^2 - 4p|b| + |\Delta| =: f(|b|). \end{aligned}$$

The quadratic polynomial $f(x) = x^2 - 4px + |\Delta|$ has a positive leading coefficient and is therefore positive everywhere except in the interval (x_1, x_2) where x_1, x_2 are its roots. So to determine if $f(|b|) \geq 0$ we need to check that $|b| \notin (x_1, x_2)$. The quadratic polynomial $f(x)$ has zeros $x_{1,2} = 2p \pm \sqrt{4p^2 - |\Delta|}$. Without loss of generality, we assume that $4p^2 - |\Delta| > 0$, since otherwise $f(x)$ has at most one root implying that f is non-negative.

We get

$$\begin{aligned} f(|b|) \geq 0 &\iff |b| \notin \left(2p - \sqrt{4p^2 - |\Delta|}, 2p + \sqrt{4p^2 - |\Delta|}\right) \\ &\iff |b| \leq 2p - \sqrt{4p^2 - |\Delta|} \text{ or } |b| \geq 2p + \sqrt{4p^2 - |\Delta|}. \end{aligned}$$

Since we know that $|b| < p$, we proof the first inequality $|b| \leq 2p - \sqrt{4p^2 - |\Delta|}$. Because $b^2 = \Delta \mod p$, there exists a non-negative integer k such that $b^2 = \Delta + kp$.

$$|b| \leq 2p - \sqrt{4p^2 - |\Delta|} \iff \sqrt{\Delta + kp} \leq 2p - \sqrt{4p^2 - |\Delta|}.$$

Notice that $\sqrt{4p^2 - |\Delta|} \leq \sqrt{4p^2} = 2p$ implies that both sides of the inequality are nonnegative and therefore we can square them and use the fact that Δ is negative and therefore $\Delta = -|\Delta|$.

$$\begin{aligned} kp - |\Delta| \leq (2p - \sqrt{4p^2 - |\Delta|})^2 &\iff kp - |\Delta| \leq 8p^2 - 4p\sqrt{4p^2 - |\Delta|} - |\Delta| \\ &\iff kp \leq 8p^2 - 4p\sqrt{4p^2 - |\Delta|} \iff k \leq 8p - 4\sqrt{4p^2 - |\Delta|} \\ &\iff \sqrt{4p^2 - |\Delta|} \leq 2p - \frac{k}{4}. \end{aligned}$$

Since $\sqrt{4p^2 - |\Delta|} \geq 0$, we know from the above inequality that $k \leq 8p$, which implies that

$$2p - \frac{k}{4} \geq \frac{2p^2 - 2}{p} \geq 0.$$

Again since both sides are non-negative we can square them.

$$\begin{aligned} &\iff 4p^2 - |\Delta| \leq 4p^2 - pk + \frac{k^2}{16} \iff -|\Delta| \leq -pk + \frac{k^2}{16} \\ &\iff pk - \frac{k^2}{16} \leq |\Delta| \iff p \leq \frac{|\Delta| + \frac{k^2}{16}}{k}. \end{aligned}$$

So with the above arguments we have shown that the basis is minimal exactly if

$$|b| \notin \left(2p - \sqrt{4p^2 - |\Delta|}, 2p + \sqrt{4p^2 - |\Delta|}\right) \iff p \leq \frac{|\Delta|}{k} + \frac{k}{16}.$$

So it is left to show that the right part is true. For this we define the function $g(k) = \frac{|\Delta|}{k} + \frac{k}{16}$ and find a uniform lower bound for it. To get a uniform lower bound of $g(k)$ we search for extremum, especially a minimum. An extremum appears when the first derivative is zero. Differentiating yields

$$g'(k) = -\frac{|\Delta|}{k^2} + \frac{1}{16}.$$

Hence

$$g'(k) = 0 \iff -\frac{|\Delta|}{k^2} + \frac{1}{16} = 0 \iff k^2 = 16|\Delta| \iff k = 4\sqrt{|\Delta|}.$$

Thus g has an extremum at $k = 4\sqrt{|\Delta|}$. Since

$$g''(k) = \frac{|\Delta|}{k^3} > 0,$$

this extremum is a minimum. Therefore

$$g(k) \geq g(4\sqrt{|\Delta|}) = \frac{\sqrt{|\Delta|}}{2}.$$

Using the assumption $p \in [0, \sqrt{|\Delta|/4}]$, we obtain

$$p \leq \sqrt{|\Delta|/4} = \frac{\sqrt{|\Delta|}}{2} \leq g(k) = \frac{|\Delta|}{k} + \frac{k}{16}.$$

This is exactly the condition required above and therefore the basis is reduced. □

Having established the reducedness for primes $p \leq \sqrt{|\Delta|/4}$, we now consider the more interesting case of larger primes.

4.2 Geometry of these lattices

We use Algorithm 3 to sample lattices arising from ideals in quadratic fields $\mathbb{Q}[\sqrt{\Delta}]$, as these are precisely the lattices encountered in the isogeny-based cryptographic setting motivating this work. Understanding their distribution is therefore important for assessing the practical behavior of lattice reduction. In Algorithm 3 the prime p is sampled with bit-length

$$r = \frac{\log_2(|\Delta)|}{2} - 1,$$

which corresponds approximately to the condition

$$p \leq \sqrt{\frac{|\Delta|}{4}}. \tag{4.9}$$

By Theorem 4.9, lattices obtained from primes satisfying (4.9) are already reduced. To investigate the distribution for larger primes, for which Algorithm 3 may return unreduced lattices, we extend the sampling range and consider primes up to

$$p \leq \sqrt{\left(\frac{|\Delta|}{4}\right)^n}, \quad n > 0. \tag{4.10}$$

Equivalently, instead of sampling primes with bit-length r, we sample primes with bit-length nr. Thus, increasing n allows us to study the behavior of the resulting lattices for progressively larger primes.

The imaginary part of the lattices z is very small and decreases as n increases. Consequently, larger values of n lead to smaller y-coordinates and require more reduction steps.

Figure 4.1 illustrates this behavior experimentally. As n increases, the distribution of the number of reduction steps shifts to the right, confirming that lattices closer to the real axis typically require a larger number of reduction steps.

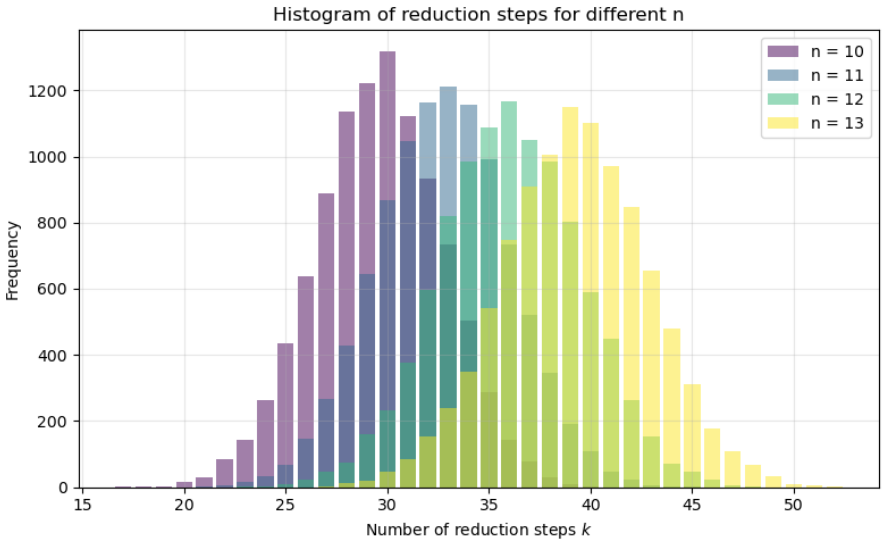

Figure 4.1: Sampled Lattices with different n and $\Delta = -(5 \cdot 2^{32} - 1)$.

Recall that the lattices are represented by points in the complex disk $\mathcal{D}$ introduced in Section 3.2. We use this disk model to study the distribution of lattices. As shown in Figure 4.2, the sampled lattices are concentrated within an extremely narrow band, almost forming a horizontal line near the x-axis ($y = 0$). Since the variation of the imaginary part is not visible on this scale, Figure 4.3 displays the same data using a logarithmic scale for $\Im(z)$. The figure shows that the imaginary parts scatter while remaining extremely small. Moreover, the points appear to be bounded below by a nearly horizontal line, suggesting the existence of a lower bound on $\Im(z)$.

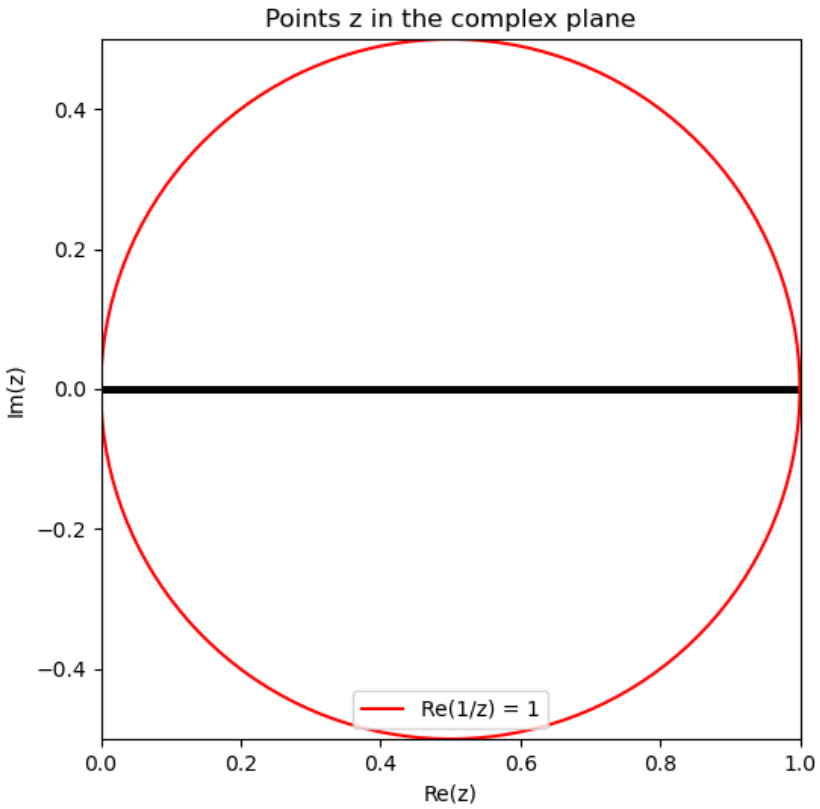

Figure 4.2: Sampled lattices with $n = 3$ and $\Delta = -(5 \cdot 2^{32} - 1)$ obtained from 10 000 samples.

To determine the imaginary part of the lattice, we express the lattice basis with respect to the complex basis $(1, i)$, as in (4.3):

$$\begin{pmatrix} -b/2 & p \\ \sqrt{|\Delta|}/2 & 0 \end{pmatrix}. \tag{4.11}$$

Recall that the complex representation of the lattice is given by

$$z = \frac{v}{u},$$

where $u, v \in \mathbb{C}$ satisfy $\|v\| \leq \|u\|$. Writing

$$v = v_1 + i \cdot v_2, \qquad u = u_1 + i \cdot u_2,$$

the vectors

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}, \qquad \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$$

form a basis of the lattice.

Since the complex representation of the lattice includes an ordered basis $\|v\| \leq \|u\|$, it remains to determine which basis vector has the smaller norm. For the basis

$$\begin{pmatrix} p \\ 0 \end{pmatrix}, \qquad \begin{pmatrix} -\frac{b}{2} \\ \frac{\sqrt{|\Delta|}}{2} \end{pmatrix}, \tag{4.12}$$

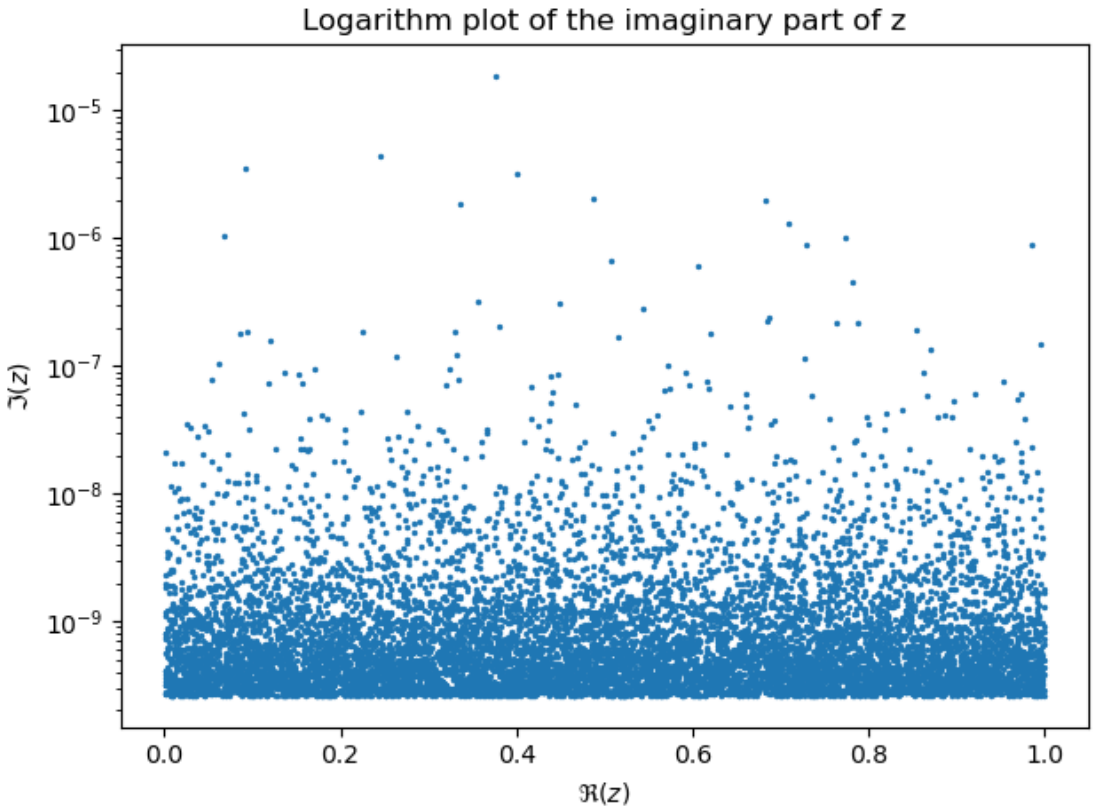

Figure 4.3: Plot of $\log_{10}(\Im(z))$ for the same 10 000 sampled lattices with $n = 3$ and $\Delta = -(5 \cdot 2^{32} - 1)$.

their squared norms are

$$\left\| \begin{pmatrix} p \\ 0 \end{pmatrix} \right\|^2 = p^2, \qquad \left\| \begin{pmatrix} -\frac{b}{2} \\ \frac{\sqrt{|\Delta|}}{2} \end{pmatrix} \right\|^2 = \frac{b^2}{4} + \frac{|\Delta|}{4}.$$

Proposition 4.10. *For the lattice obtained by Algorithm 3, we always have* $p^2 > b^2/4 + |\Delta|/4$, *for* $n > 1$.

Proof.

$$p^2 - \frac{b^2}{4} \geq p^2 - \frac{p^2}{16} = \frac{15}{16} p^2 > \frac{|\Delta|}{4}.$$

The last inequality is true because when sampling p it will be approximately $\sqrt{(|\Delta|/4)^n}$ and $n > 1$. We used the fact that one can choose the solution $b = \sqrt{|\Delta|} \mod p$ to be larger than $p/2$. □

Proposition 4.10 determines the ordering of the basis vectors and shows that

$$\left\| \begin{pmatrix} p \\ 0 \end{pmatrix} \right\|^2 > \left\| \begin{pmatrix} -\frac{b}{2} \\ \frac{\sqrt{|\Delta|}}{2} \end{pmatrix} \right\|^2.$$

Consequently, the corresponding complex lattice is

$$z = \frac{\frac{-b}{2} + \frac{\sqrt{|\Delta|}}{2} i}{p}.$$

Its imaginary part is therefore given by

$$\Im(z) = \frac{\sqrt{|\Delta|}}{2p} .$$

Using the sampling condition

$$p \leq \sqrt{\left(\frac{|\Delta|}{4}\right)^n} ,$$

we obtain

$$\frac{1}{p} \geq \sqrt{\left(\frac{4}{|\Delta|}\right)^n} .$$

Thus, we obtain the following lower bound on $\Im(z)$

$$\Im(z) = \frac{\sqrt{|\Delta|}}{2p} \geq \sqrt{|\Delta|}\frac{1}{2}\sqrt{(\frac{4}{|\Delta|})^n} = \sqrt{(\frac{4}{|\Delta|})^{n-1}} . \tag{4.13}$$

To obtain a meaningful upper bound on $\Im(z)$, we need to study lower bounds on the primes p. Such a lower bound on p could be imposed directly by modifying Algorithm 3. Alternatively, one could seek a probabilistic lower bound on the output primes.

To derive a probabilistic lower bound, one must understand the distribution of the primes returned by Algorithm 3. The algorithm repeatedly samples candidate primes satisfying

$$p \leq X := \sqrt{\left(\frac{|\Delta|}{4}\right)^n} ,$$

until a valid class group element is obtained. Thus, the key question is how many candidates are expected to be sampled before a prime that satisfies the required conditions is found. More precisely, the output prime p must satisfy

$$\left(\frac{\Delta}{p}\right) = 1, \qquad b^2 - \Delta \equiv 0 \pmod{4p}, \qquad \frac{b^2 - \Delta}{4p} \neq 0,$$

where b is the square root of Δ modulo p.

Let

$$q := \Pr\left[\left(\frac{\Delta}{p}\right) = 1,\, b^2 - \Delta \equiv 0 \pmod{4p},\, \frac{b^2 - \Delta}{4p} \neq 0\right].$$

Assuming that successive candidate primes are sampled independently, the number of candidate primes sampled before a valid prime is found, follows a geometric distribution with parameter q. Let N denote the number of sampled candidate primes before a valid prime is returned. Then,

$$\Pr[N > k] = (1 - q)^k,$$

since the first k trials must all fail. As a simple heuristic, suppose that the only condition imposed on a sampled prime is

$$\left(\frac{\Delta}{p}\right) = 1.$$

For a fixed discriminant Δ, one expects approximately half of the primes to satisfy this condition. Thus, the acceptance probability would be

$$q \approx \frac{1}{2}.$$

Thus,

$$\Pr[N > k] \approx \left(\frac{1}{2}\right)^k .$$

In this simplified model,

$$\Pr[N > 128] \approx 2^{-128},$$

so, with probability at least $1-2^{-128}$ a valid prime is found within 128 samples. A rigorous analysis would require incorporating the remaining acceptance conditions, which we leave for future work.

4.3 Model their distribution

As discussed in Section 4.2 and visualized in Figure 4.2, the sampled input lattices appear to be concentrated near a horizontal line. Motivated by this observation, we model the initial lattice distribution on the fundamental disk $\mathcal{D}$ by a uniform distribution on the segment

$$l : y = d$$

contained in the fundamental disk $\mathcal{D}$, where $d \in \mathbb{R}$ is a parameter.

Since this model is only an approximation of the true distribution, the resulting probability $\Pr[L \geq k+1]$ should be regarded as an estimate.

Using the domains $\mathcal{D}_k$, illustrated in Figure 3.1, we can estimate the tail probabilities $\Pr[L \geq k+1]$. By Proposition 3.1,

$$\mathcal{D}_k = [L \geq k+1].$$

Under this line model, probabilities are determined by relative lengths on l rather than by the areas of the domains $\mathcal{D}_k$. Therefore, the problem reduces to computing the lengths of the intersections

$$l \cap \mathcal{D}_k \ .$$

Since

$$\mathcal{D}_{k+1} \subseteq \mathcal{D}_k,$$

the sets

$$\mathcal{D}_k \setminus \mathcal{D}_{k+1}$$

consist precisely of those lattices that require exactly $k+1$ reduction steps. Furthermore, the domains are composed of disks $h(\mathcal{D})$ with $|h| = k$, whose sizes decrease as k increases. Consequently, for a fixed line $l : y = d$ with $d \neq 0$ only finitely many domains $\mathcal{D}_k$ intersect the line l.

Finally, the domains $\mathcal{D}_k$ are symmetric with respect to the real axis. Therefore, it suffices to consider the lines l in the upper half-plane.

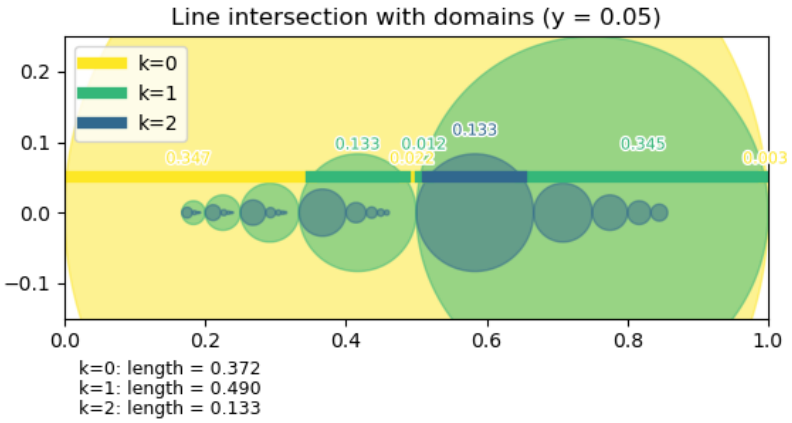

Figure 4.4: Intersection of the domains with the horizontal line $y = 0.05$.

The choice of height d is crucial for obtaining a meaningful estimate. A natural candidate is the mean of the imaginary parts of the sampled lattices. Another possibility is to use the smallest observed value (minimum). We also consider an empirical lower bound that is slightly below all

observed values. However, these approaches depend on a finite sample of lattices and therefore do not take into consideration all of the possible lattices. In addition, we use the theoretical lower bound (4.13). Every lower bound on the y-values yields an upper bound on the probability $\Pr[L \geq k+1]$. Indeed, a decrease in height d leads to an increase in length resulting from the intersection with domains $\mathcal{D}_k$ for larger k. This relation is visualized between Figures 4.4 and 4.5.

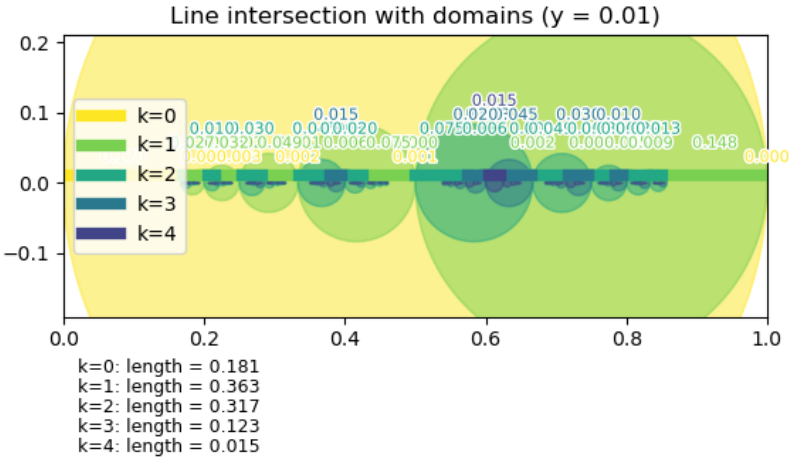

Figure 4.5: Intersection of the domains with the horizontal line $y = 0.01$.

4.4 Generation of Experimental Data

We use SageMath [Dev25] to perform all the calculations described in this chapter and the previous ones. The source code can be found in the repository [Wür26].

Before we actually use the described models we need to have comparison data. For that we use the sampling Algorithm 3 with the following parameters.

Parameter	Value
Δ	$-(5 \cdot 2^{32} - 1)$
n	3
N	10000

Where n is such that primes $p \leq \sqrt{(|\Delta|/4)^n}$ and N denotes the number of sampled elements.

For sampling, we just run the reduction algorithm and count how many reduction steps are needed. Notice that since we use a different inner product (4.6) the reduction algorithm is adjusted to this inner product. The results on the count of the reduction steps are shown in Figure 4.6.

In addition, we can now compute the relevant d values and estimate the location of the line $l : y = d$.

In Table 4.1 we observe a gap between the observed lower bound and the proved lower bound. The observed lower bound is approximately 5.7 times larger than the theoretical bound. The reason for this gap is the proved lower bound is attained in the extreme case where the prime p is as large as allowed, namely $p = \sqrt{(|\Delta|/4)^n}$. Since $\Im(z) = \sqrt{|\Delta|}/(2p)$, larger values of p correspond to smaller values of $\Im(z)$. Therefore, the fact that we observed the minimum to be larger than the theoretical bound means that none of the sampled primes were sufficiently close to this maximal value.

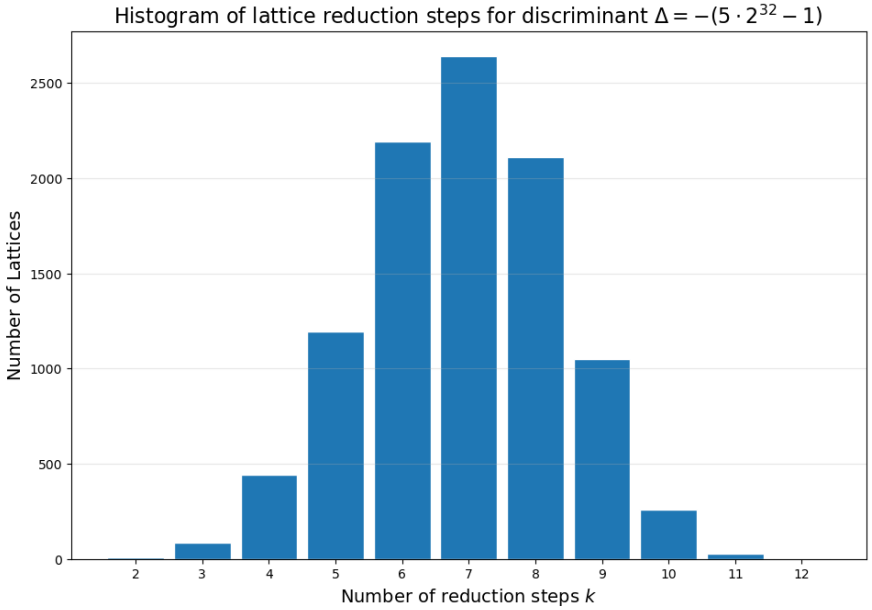

Figure 4.6: Histogram on number of reduction steps of sampled lattices.

d value	Description
$2.50 \cdot 10^{-5}$	Mean of $\Im(z)$ from sampling
$1.06 \cdot 10^{-9}$	Minimum of $\Im(z)$ from sampling
$1.00 \cdot 10^{-9}$	Observed lower bound of $\Im(z)$ from sampling
$1.86 \cdot 10^{-10}$	Proved lower bound (see 4.13)

Table 4.1: Different d values to consider.

The experimental data obtained in this chapter will later serve as a basis for comparison with the theoretical predictions.

5 Applying probability models for computations

In this chapter, we apply the probabilistic models developed in the previous chapters to estimate the reduction-step probabilities of lattices arising from ideals in quadratic fields. We compute numerical predictions using both the transfer operator method and the line-intersection method and compare the resulting estimates with experimentally generated data.

5.1 The transfer operator method

5.1.1 Choosing probability density function ρ

An important part in estimating the tail probability $\Pr[L \geq k+1]$ of the number of reduction steps L by the transfer operator method is an accurate approximation of the probability density function describing the distribution of the input lattices.

As a first model, we consider a density that is concentrated near the real axis (see Figure 5.1), reflecting the behavior observed for the lattice distribution arising from ideals of quadratic fields (see Section 4.2). Specifically, we define

$$\rho(z) = \exp(-\Im(z)^2/2\sigma^2). \tag{5.1}$$

The function ρ is not a probability density function on $\mathbb{R}^2$, since its integral over $\mathbb{R}^2$ is infinite. However, the fundamental disk $\mathcal{D}$ is bounded and therefore

$$\int_{\mathcal{D}} \rho(z)\, dA(z) < \infty.$$

After normalization, ρ thus defines a probability density function on $\mathcal{D}$.

This first model of the distribution of the input lattices can be improved by introducing a vertical shift parameter d. As discussed in Section 4.3, the imaginary parts observed in practice are concentrated near a positive value rather than near the real axis. The parameter d allows us to model this behavior by shifting the center of the density to the line

$$l : y = d.$$

The parameter d determines the location of the concentration and allows us to model distributions centered away from the x-axis. We therefore consider the density

$$\rho(z) = \frac{1}{Z_d} \exp\Big(- \frac{(\Im(z) - d)^2}{2\sigma^2}\Big), \tag{5.2}$$

which is concentrated near the line $y = d$. Here,

$$Z_d = \int_{\mathcal{D}} \exp\Big(-\frac{(\Im(z) - d)^2}{2\sigma^2}\Big)\, dA(z)$$

is the normalization constant. Consequently,

$$\int_{\mathcal{D}} \rho(z)\, dA(z) = 1,$$

and ρ defines a probability density function on $\mathcal{D}$.

To simplify the normalization constant Z_d into a single integral, we have the following proposition.

Proposition 5.1. *The normalization constant* $Z_d = \int_{\mathcal{D}} \exp\Big(- \frac{(\Im(z)-d)^2}{2\sigma^2}\Big)\, dA(z)$ *can be written as*

$$Z_d = 2\int_{-1/2}^{1/2} \sqrt{\frac{1}{4} - y^2} \exp\Big(- \frac{(y-d)^2}{2\sigma^2}\Big)\, dy.$$

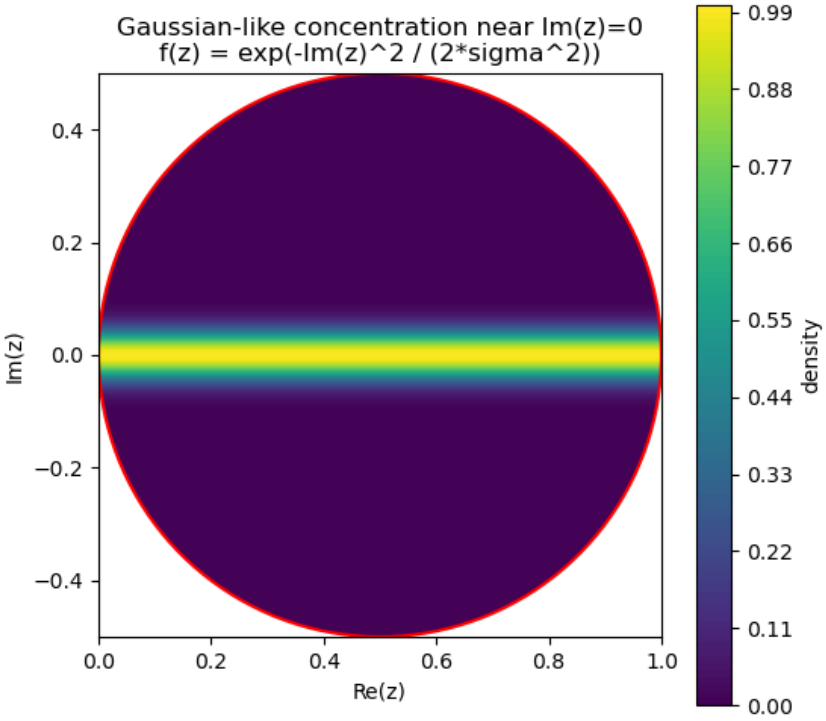

Figure 5.1: $\rho = \exp(-\Im(z)^2/2\sigma^2)$ concentrated at $y = 0$.

Proof. Let $z = x + iy$ and recall that $\mathcal{D}$ is the disk with diameter $[0, 1]$, that is, $\mathcal{D} = \{x + iy \mid (x - 1/2)^2 + y^2 \leq 1/4\}$. This leads to the integral bound $x \in [1/2 - \sqrt{1/4 - y^2}, 1/2 + \sqrt{1/4 - y^2}]$. Using this we can reduce the double integral to a singular integral in the following way.

$$Z_d = \int_{\mathcal{D}} \exp\left(-\frac{(\Im(z) - d)^2}{2\sigma^2}\right) dA(z) \tag{5.3}$$

$$= \int_{-1/2}^{1/2} \int_{1/2-\sqrt{1/4-y^2}}^{1/2+\sqrt{1/4-y^2}} \exp\left(-\frac{(y-d)^2}{2\sigma^2}\right) dxdy \tag{5.4}$$

$$= 2\int_{-1/2}^{1/2} \sqrt{\frac{1}{4} - y^2} \exp\left(-\frac{(y-d)^2}{2\sigma^2}\right) dy. \tag{5.5}$$

□

The probability estimate in Theorem 3.14 requires a holomorphic extension F of the density ρ satisfying

$$F(z, \overline{z}) = \rho(z).$$

We therefore express the function ρ in terms of z and its complex conjugate $\overline{z}$ via the identity

$$\Im(z) = \frac{z - \overline{z}}{2i}.$$

We obtain

$$\rho(z) = \frac{1}{Z_d} \exp\left(-\left(\frac{z - \overline{z}}{2i} - d\right)^2 \frac{1}{2\sigma^2}\right). \tag{5.6}$$

This representation naturally leads to the holomorphic extension

$$F(u,v) = \frac{1}{Z_d} \exp\left(-\left(\frac{u-v}{2\cdot i} - d \right)^2 \frac{1}{2\sigma^2} \right), \tag{5.7}$$

which satisfies $F(z,\overline{z}) = \rho(z)$.

The function F is holomorphic on $\mathbb{C}^2$, since it is obtained by composing holomorphic functions and depends only on the independent complex variables u and v, and not their complex conjugates.

5.1.2 Truncated operator for computations

Since the transfer operator is defined by an infinite sum, it cannot be represented exactly in numerical computations. We therefore introduce a finite-dimensional approximation obtained by truncation. In this subsection, we follow [DFV96] and derive the corresponding truncated operator matrix with respect to the basis $\{(x-a)^i\}$.

The motivation for this construction comes from the problem of estimating the dominant eigenvalue λ_4. The following proposition shows that suitable positive test functions yield an upper and lower bound on the dominant eigenvalue λ_4.

Proposition 5.2. *[DFV96, Prop. 16] Let f be an analytic function and strictly positive on [0,1]. Then if there exist constants α, β such that*

$$\alpha \le \frac{\mathcal{G}[f](x)}{f(x)} \le \beta,$$

the following holds for the dominant eigenvalue

$$\alpha \le \lambda_4 \le \beta.$$

A natural question is how to construct test functions that give a tight bound on λ_4. For this, we focus on analytic functions and study the action of the transfer operator $\mathcal{G}_s$ on their Taylor expansion. Let

$$\sum_j c_j (x-a)^j, \qquad c_j = \frac{f^{(j)}(a)}{j!},$$

be the Taylor expansion of an analytic function at a point $a \in [0,1]$ (see [DFV96]). Since the operator $\mathcal{G}$ is linear, it suffices to analyze the action on the basis elements $(x-a)^j$:

$$\mathcal{G}_s[(x-a)^j](x) = \sum_{m=1}^{\infty} \frac{1}{(m+x)^s} \Big(\frac{1}{m+x} - a \Big)^j = \sum_{l=0}^{j} \binom{j}{l} (-a)^{j-l} \zeta(s+l, x+1), \tag{5.8}$$

where $\zeta(s,w) = \sum_{n=0}^{\infty} (n+w)^{-s}$ is the Hurwitz zeta function.

To express the formula again in the basis $(x-a)^i$ we use the expansion

$$\zeta(s, x+1) = \sum_{i=0}^{\infty} (-1)^i \binom{s+i-1}{i} \zeta(s+i, 1+a)(x-a)^i,$$

which is proved in [DFV96]. Substituting this into the previous formula gives

$$\mathcal{G}_s[(x-a)^j](x) = \sum_{i=0}^{\infty} M_{i,j} (x-a)^i,$$

where

$$M_{i,j} = \sum_{l=0}^{j} \binom{j}{l} (-a)^{j-l} (-1)^i \binom{s+l+i-1}{i} \zeta(s+l+i, 1+a)(x-a)^i. \tag{5.9}$$

We consider the operator $\mathcal{G}_4$ with $s = 4$, which gives

$$M_{i,j} = (-1)^i \sum_{l=0}^{j} \binom{j}{l} (-a)^{j-l} \binom{l+i+3}{i} \zeta(4+l+i, 1+a)(x-a)^i. \tag{5.10}$$

The operator $\mathcal{G}_4$ can therefore be represented by the infinite matrix

$$M = (M_{i,j})_{i,j \geq 0}$$

with respect to the basis $\{(x-a)^i\}_{i \geq 0}$.

For numerical computations, it is not possible to work with the infinite matrix M. We therefore consider its finite truncation T_m, defined as a $m \times m$ matrix consisting of the entries $M_{i,j}$ with $0 \leq i, j < m$.

Consider an analytic function

$$f(x) = \sum_{j}^{m-1} c_j (x-a)^j \ ,$$

with coefficient vector

$$[f]_m = (c_0, \ldots, c_{m-1})^\top \ .$$

We obtain

$$\mathcal{G}[f](x) = (T_m [f]_m)^\top \mathbf{b}_m(x) + \mathcal{O}((x-a)^m) \ ,$$

where

$$\mathbf{b}_m(x) = \begin{pmatrix} (x-a)^0 \\ (x-a)^1 \\ \vdots \\ (x-a)^{m-1} \end{pmatrix}$$

denotes the truncated basis vector.

The matrix T_m then provides finite-dimensional approximations of $\mathcal{G}$, making numerical computations possible. In particular, we compute the dominant eigenvalue $\lambda_4^{[m]}$ of T_m together with a corresponding right eigenvector $v_4^{[m]}$.

Since T_m represents the action of $\mathcal{G}$ with respect to the basis $\{(x-a)^i\}$, the entries of $v_4^{[m]}$ can be interpreted as coefficients of an approximate eigenfunction. This leads to the polynomial

$$p_m(x) = \sum_{i=0}^{m-1} v_4^{[m]}(i)(x-a)^i, \tag{5.11}$$

which serves as an approximation of the dominant eigenfunction $f_{1,4}$ of $\mathcal{G}_4$.

For the exact dominant eigenfunction of the operator $\mathcal{G}$ we have

$$\frac{\mathcal{G}[f_{1,4}](x)}{f_{1,4}(x)} = \lambda_4,$$

for all $x \in [0,1]$. Since p_m is only an approximation of $f_{1,4}$, the ratio

$$\frac{\mathcal{G}x}{p_m(x)}$$

is generally not constant. However, it is nearly constant on a subinterval of $[0,1]$. This plateau provides an estimate of the dominant eigenvalue λ_4 [DFV96], since the values on the plateau are close to the constant ratio associated with the exact dominant eigenvalue λ_4.

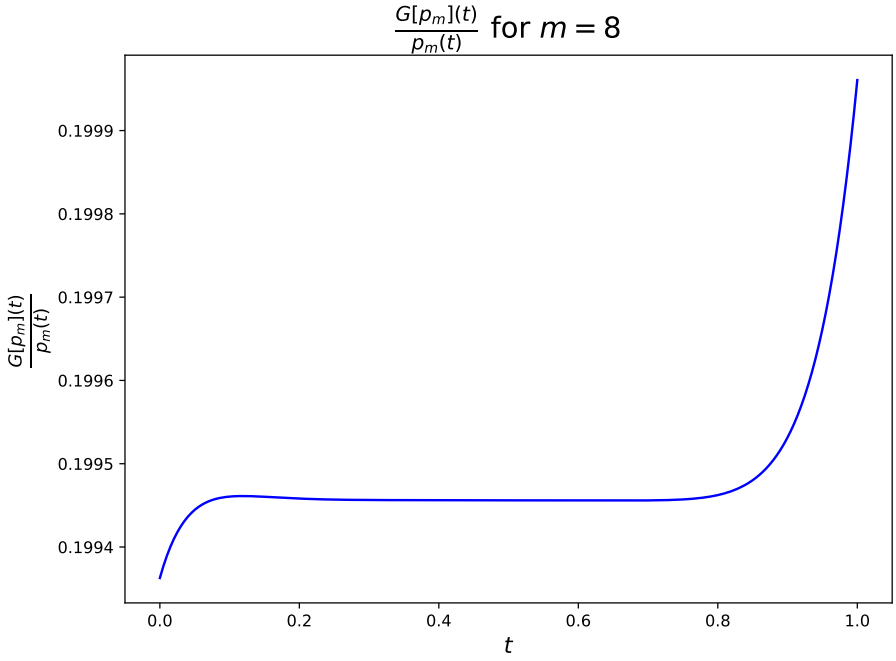

Figure 5.2: Function $\frac{\mathcal{G}[p_m](x)}{p_m(x)}$ for $m = 8$ with noticeable plateau.

In practice, the quotient

$$\frac{\mathcal{G}x}{p_m(x)}$$

is most stable on the interval $[0.1, 0.8]$. We therefore focus on this region when estimating the dominant eigenvalue. Applying Proposition 5.2 gives

$$\inf_{x\in[0.1,0.8]} \frac{\mathcal{G}[p_m](x)}{p_m(x)} \leq \lambda_4 \leq \sup_{x\in[0.1,0.8]} \frac{\mathcal{G}[p_m](x)}{p_m(x)}.$$

Increasing the truncation parameter m improves the approximation of the dominant eigenvalue λ_4, since the error introduced by truncating the infinite matrix becomes smaller.

This approach allows us to compute approximations of the dominant eigenvalue for arbitrary values of s. Having established a method for approximating the dominant eigenvalue λ_4, we focus on the subdominant eigenvalue, denoted by μ_4.

We first derive a formula for the trace of the transfer operator which will allow us to compute a bound for the subdominant eigenvalue μ_4.

Theorem 5.3. *[DFV96, Thm. 15]*

$$\mathrm{Tr}(\mathcal{G}_s^k) = \sum_{|h|=k} \frac{\tau(h)^{-s}}{1-(-1)^k\tau(h)^{-2}}, \quad \textit{with} \quad \tau(h) = \frac{(Q_k + P_{k-1}) + \sqrt{(Q_k + P_{k-1})^2 - 4(-1)^k}}{2} \ .$$

For completeness, we note that the proof is given in [DFV96, p. 24].

One has [Alk12]

$$\mathrm{Tr}(\mathcal{G}_s) = \sum_{n=1}^{\infty} \lambda_{n,s} \ .$$

Since some eigenvalues may be negative, cancellations can occur in this sum. To obtain a bound on the subdominant eigenvalue $\mu_4 = \lambda_{2,4}$ it is convenient to consider

$$\mathrm{Tr}(\mathcal{G}_s^2) = \sum_{n=1}^{\infty} \lambda_{n,s}^2 \ .$$

Using this trace formula, one obtains the following bound for μ_4 [DFV96]:

$$|\mu_4| < (\mathrm{Tr}(\mathcal{G}_4^2) - \lambda_4^2)^{1/2}. \tag{5.12}$$

We recall that for uniformly distributed lattices, the probability

$$\Pr[L \geq k+1]$$

is given by (see (3.15))

$$\Pr[L \geq k+1] = \sum_i \lambda_{i,4}^k c_i, \tag{5.13}$$

where

$$c_i = f_{i,4}^*[u], \qquad u(t) = \frac{1}{(1+t)^2}.$$

Thus, it remains to compute the constants c_i. In particular, for the dominant term, we need the value

$$c = f_{1,4}^*[u].$$

To compute this constant, we use the previous introduced finite-dimensional approximation. The dual eigenfunctional $f_4^* := f_{1,4}^*$ is approximated by the left eigenvector $w_4^{[m]}$ of the truncated operator matrix T_m corresponding to the dominant eigenvalue $\lambda_4^{[m]}$.

For the computation, it is important that both the eigenfunction f_4 and the dual eigenfunctional f_4^* are normalized correctly. That is, we ensure that $f_4[0] = 1$ and that f_4 and f_4^* form a dual pair, that is,

$$\langle f_4^*, f_4 \rangle = f_4^*[f_4] = 1.$$

Lastly, we need the function u to be represented as a coefficient vector $v_u^{[m]}$ with respect to the same basis $\{(x-a)^i\}$ as the dual eigenfunctional f_4^*.

Then we compute

$$c = f_{1,4}^*[u] \approx w_4^{[m]} \cdot v_u^{[m]}.$$

5.1.3 Estimation of the probability

As described in the previous section, we first need to compute the entries M_{ij} of the truncated matrix T_m. For this we use the `hurwitz_zeta` and the `binomial` functions of the SageMath [Dev25] library. Then we use the `eigenvectors_right` function to get all the right eigenvectors of T_m, we filter them and only use the one corresponding to the dominant eigenvalue λ_4.

Since there is no exact way to compute infimum and supremum in SageMath [Dev25] we make grid points in the interval and calculate the value of $\frac{\mathcal{G}[p_m](z)}{p_m(z)}$ at the grid points and take the minimum and maximum value. This gives us upper and lower bounds α and β for the dominant eigenvalue λ_4.

$$\alpha \leq \lambda_4 \leq \beta.$$

In addition, we use a truncated operator $\mathcal{G}$ to compute the value of $\frac{\mathcal{G}[p_m](z)}{p_m(z)}$.

$$\mathcal{G}[f](z) = \sum_{m=1}^{M} \frac{1}{|m+z|^4} f\Big(\frac{1}{m+z}\Big).$$

In Table 5.1 we vary the values of m, which is the size of the matrix T_m and, therefore, the precision. For $m = 4, 8, 16$ we used $M = 1000$. For $m = 32, 64$ we used $M = 10000$.

We notice that even though we have greatly increased the precision, the value of λ_4 is not yet as precise as mentioned in [DFV96]:

$$\lambda_4 = 0.199458818343767 \pm 10^{-15}. \tag{5.14}$$

m	α	β	λ_4	precision (bits)
4	0.194555499821996	0.225736617535107	0.	100
8	0.199363100535324	0.199962493435125	0.199	100
16	0.199458801920642	0.199458911432295	0.199458	100
32	0.199458818341768	0.199458818343433	0.19945881834	500
64	0.199458818341766	0.199458818343434	0.19945881834	500

Table 5.1: Computed values of α, β, and dominant eigenvalue λ for varying m.

m	Approximation of λ_4	Stable digits	precision (bits)
4	0.19901597627733025927843747231635528 2	-	200
8	0.19945693661866914574421664500518515 2	0.199	200
16	0.19945881828605244067425174088658223 2	0.19945	200
32	0.19945881834376725999010690488010943	0.199458818	200
64	0.19945881834376726019184568597987906 5	0.1994588183437672	300
128	0.19945881834376726019184568597987908	0.19945881834376726019184568597987908	600

Table 5.2: Computed values of the dominant eigenvalue λ_4 of the matrix T_m.

So, the next idea is that instead of using the bounds α and β we can directly use the dominant eigenvalue of the truncated operator matrix T_m. Here we examine which digits of the dominant eigenvalue do not change when we go to a better precision m. This leads to a much better idea of what the dominant eigenvalue λ_4 really looks like.

$$\lambda_4 \approx 0.19945881834376726019184568597987908.$$

Similarly, we compute the dominant eigenvalue λ_6, which determines the error term in Theorem 3.14. All computations were performed with 200-bit floating point precision.

m	Approximation of λ_6	Stable digits
4	0.06324502610149	-
8	0.06340210088498	0.063
16	0.06340264977888	0.063402
32	0.06340264978828	0.0634026497

Table 5.3: Computed values of the dominant eigenvalue λ_6 of the matrix T_m.

From Table 5.3 we obtain

$$\lambda_6 \approx 0.0634026497.$$

To compute the subdominant eigenvalue μ_4, we use Theorem 5.3, and because again we cannot compute infinite sums, we use a finite sum instead.

$$\operatorname{Tr} \mathcal{G}_4^2 = \sum_{m_1,m_2 \geq 1}^{M} \frac{\tau_{m_1,m_2}^{-4}}{1-\tau_{m_1,m_2}^{-2}}.$$

Using the approximation

$$\lambda_4 = 0.199458818343767,$$

we evaluate the trace formula with 500-bit floating point precision and obtain

$$\operatorname{Tr}(\mathcal{G}^2) \approx 0.0464718249263114.$$

Applying (5.12) yields

$$|\mu_4| < 0.0817802220051986. \tag{5.15}$$

With these values, we can now compute $\nu_4 = \frac{1}{\lambda_4} \max(\lambda_6, \mu_4)$. We use the upper bound on the subdominant eigenvalue μ_4 so that we get an upper bound on the probability.

$$\nu_4 \approx 0.4100105609983631.$$

In this next part, we compute the constant $f_4^*[\rho]$ using the probability density function

$$\rho(z) = \frac{1}{Z_d} \exp\left(-\frac{(\Im(z) - d)^2}{2 \cdot 0.05^2}\right)$$

introduced in Subsection 5.1.1. Similar as in the computation for the right eigenvector, we use the eigenvector function `eigenvectors_left` from SageMath [Dev25] to compute the left eigenvector representing the eigenfunctional f_4^*. Before applying the dominant left eigenvector, we normalize the left and right eigenvectors so that $f_4^*[f_4] = 1$. First we normalize the right eigenvector by dividing it by its value at zero. Next, we scale the left eigenvector by dividing it by its inner product with the right eigenvector,

`ev_left.dot_product(ev_right)`,

so that $f_4^*[f_4] = 1$.

Since we compute the eigenvectors from the matrix T_m, they naturally inherit the representation in the basis $\{(x - 1/2)^i\}$ (see 5.11). Therefore, before computing $f_4^*[\rho]$, we approximate the probability density function ρ by a polynomial in the same basis, representing this polynomial by its coefficient vector.

$$\rho(z) = \sum_{i=0}^{m-1} c_i (z - 1/2)^i \ .$$

So we can now compute the constant $f_4^*[\rho]$ for different sizes m of the matrix T_m, where ρ is the density concentrated around the horizontal line

$$l : \Im(z) = d,$$

with height parameter d.

m	d	$f_4^*[\rho]$	precision (bits)
16	0	5.18840234258243	300
32	0	5.17148844265055	300
64	0	5.18049632411606	300
128	0	5.18049632291824	600
16	$2.50 \cdot 10^{-5}$	5.19021140860001	300
32	$2.50 \cdot 10^{-5}$	5.17335058120537	300
64	$2.50 \cdot 10^{-5}$	5.18235263879674	300
128	$2.50 \cdot 10^{-5}$	5.18235263760008	600
32	$1.06 \cdot 10^{-9}$	5.17148852167475	300
64	$1.06 \cdot 10^{-9}$	5.18049640289318	300
128	$1.06 \cdot 10^{-9}$	5.18049640169553	600

Table 5.4: Computed value of the constant $f_4^*[\rho]$ for different d and m.

We observe that the constant $f_4^*[\rho]$ remains essentially unchanged as the height parameter d varies. Consequently,

$$f_4^*[\rho] \approx 5.18,$$

independent of the choice of d.

In the next part, we compute the constant C_4 given by (3.20):

$$C_4 = 6 \int_{\mathcal{D}} \int_0^1 (y - y^2) f_4(w + (\overline{w} - w)y)\, dy\, dA(w).$$

To compute the constant C_4, we approximate the double integral using Riemann sums.

$$C_4 \approx 6 \sum_{i,j}^{M} \sum_{y \in Y} f_4^{(m)}(X_{i,j} + \mathbf{i}(1-2y)T_{i,j}) \cdot (y - y^2) \cdot dy \cdot dx \cdot dt. \tag{5.16}$$

Here, $\{X_{i,j}\}$ and $\{T_{i,j}\}$ denote the cartesian grid points used to discretize the disk $\mathcal{D}$ and Y is the uniform grid on $[0, 1]$. The quantities dx, dt, dy are the widths of the corresponding mesh grids. Furthermore, $\mathbf{i} = \sqrt{-1}$ denotes the imaginary unit. The Riemann sums are computed using

$$M = 400,$$

that is, a uniform 400×400 grid $\{(X_{i,j}, T_{i,j})\}$ for variables (x, t) and a uniform grid Y consisting of 400 points for variable y.

m	C_4	precision (bits)
16	0.31291943571713854	200
32	0.3129193380642448	200
64	0.3129193380642424	300

Table 5.5: Computed approximations of the constant C_4 for different values of m.

Table 5.5 shows that the computed values stabilize as m increases. We therefore obtain the approximation

$$C_4 \approx 0.31291933806424.$$

The final parameter required to compute the asymptotic estimate of $\Pr[L \geq k + 1]$ is the norm of the function F (see 5.7). The following proposition gives the supremum norm of the function F.

Proposition 5.4. *For $\sigma = 0.05$ the norm of F is*

$$\|F\| = \frac{1}{Z_d} \exp\Big(\frac{25^2}{2} - 100d^2\Big).$$

Proof. Recall that the function F is defined by

$$F(u, v) = \frac{1}{Z_d} \exp\left(-\left(\frac{u - v}{2i} - d\right)^2 \cdot \frac{1}{2\sigma^2}\right),$$

and its norm by $\|F\| = \sup\{|F(u, v)| \mid (u, v) \in \mathcal{V} \times \mathcal{V}\}$. Let $u = a + ib$ and $v = c + id_v$, we substitute with complex number

$$w = \frac{v - u}{2i} + d = \Big(\frac{d_v - b}{2} + d\Big) + i\Big(-\frac{c - a}{2}\Big) =: x + iy. \tag{5.17}$$

Giving us

$$|F(w)| = \frac{1}{Z_d}\Big|\exp\Big(-\frac{w^2}{2\sigma^2}\Big)\Big| = \frac{1}{Z_d}\exp\Big(-\frac{\Re(w^2)}{2\sigma^2}\Big) = \frac{1}{Z_d}\exp\Big(-\frac{x^2 - y^2}{2\sigma^2}\Big). \tag{5.18}$$

Thus, maximizing $|F(w)|$ is equivalent to minimizing $\Re(w^2) = x^2 - y^2$.

$$\frac{\partial}{\partial x}\Re(w^2) = 2x, \qquad \frac{\partial}{\partial y}\Re(w^2) = -2y. \tag{5.19}$$

Hence, the only critical point is $(x, y) = (0, 0)$. To determine the possible values of (x, y), we parameterize the boundary circle by

$$a - 1 = \frac{5}{4}\cos(\alpha), \quad b = \frac{5}{4}\sin(\alpha),$$
$$c - 1 = \frac{5}{4}\cos(\beta), \quad d_v = \frac{5}{4}\sin(\beta).$$

This gives the exact disk equation for $\mathcal{V}$

$$(a-1)^2 + b^2 = \left(\frac{5}{4}\right)^2,$$

using the fact that $\cos^2 + \sin^2 = 1$. Therefore, the values x and y can be represented by

$$x = d + \frac{5}{8}(\sin\beta - \sin\alpha), \qquad y = \frac{5}{8}(\cos\beta - \cos\alpha),$$

with $\alpha, \beta \in [0, 2\pi]$.

We now determine the set of all possible values of (x, y). We will show that it is exaclty the disk

$$(x-d)^2 + y^2 \le \left(\frac{5}{4}\right)^2.$$

First, we prove that every admissible point (x, y) lies in this disk.

$$\begin{aligned}
(x-d)^2 + y^2 &= \left(\frac{5}{8}(\sin\beta - \sin\alpha)\right)^2 + \left(\frac{5}{8}(\cos\beta - \cos\alpha)\right)^2 \\
&= \left(\frac{5}{8}\right)^2\Big[(\sin\beta - \sin\alpha)^2 + (\cos\beta - \cos\alpha)^2\Big] \\
&= \left(\frac{5}{8}\right)^2\Big[2 - 2\cos(\alpha - \beta)\Big] \\
&= \frac{25}{32}(1 - \cos(\alpha - \beta)) \\
&= \frac{25}{32}2\sin^2\left(\frac{\alpha - \beta}{2}\right) \\
&\le \frac{25}{16} = \left(\frac{5}{4}\right)^2.
\end{aligned}$$

Conversely, for any point of the disk, write

$$x - d = r\cos\varphi, \qquad y = r\sin\varphi, \qquad 0 \le r \le \frac{5}{4}.$$

Choose δ such that

$$r = \frac{5}{4}\sin\delta.$$

Setting

$$\frac{\alpha - \beta}{2} = \delta, \qquad \frac{\alpha + \beta}{2} = \varphi + \frac{\pi}{2},$$

the formulas for x and y are satisfied. Hence every point of the disk occurs, and therefore the admissible set is exactly

$$\{(x, y) : (x-d)^2 + y^2 \le (5/4)^2\}.$$

Hence, the problem is reduced to finding

$$\min_{(x-d)^2 + y^2 \le (\frac{5}{4})^2} (x^2 - y^2).$$

The boundary of this disk can be parameterized by

$$x = d + \frac{5}{4}\cos\theta, \qquad y = \frac{5}{4}\sin\theta,$$

substituting into $x^2 - y^2$ gives

$$f(\theta) := (d + \frac{5}{4}\cos\theta)^2 - (\frac{5}{4}\sin\theta)^2 = d^2 + \frac{5}{2}d\cos\theta + \frac{25}{16}(\cos^2\theta - \sin^2\theta)$$
$$= d^2 + \frac{5}{2}d\cos\theta + \frac{25}{16}\cos(2\theta).$$

Let $t = \cos\theta$ then,

$$f(t) = d^2 + \frac{5}{2}d \cdot t + \frac{25}{16}(-1 + 2t^2) = d^2 + \frac{5}{2}dt + \frac{25}{8}t^2 - \frac{25}{16}, \quad t \in [-1, 1].$$

This is a quadratic function in t and its derivative is

$$f'(t) = \frac{5}{2}d + \frac{25}{4}t,$$

setting it to zero gives $t = -\frac{2d}{5}$. Since $0 \leq d \leq 1/2$,

$$-\frac{1}{5} \leq t \leq 0,$$

which lies indeed in $[-1, 1]$ and is therefore a valid minimum.

$$\min_{(x-d)^2+y^2 \leq (\frac{5}{4})^2} (x^2 - y^2) = f(-\frac{2d}{5}) = \frac{d^2}{2} - \frac{25}{16}. \tag{5.20}$$

Thus,

$$\|F\| = \frac{1}{Z_d}\exp\Big(-\frac{\frac{d^2}{2} - \frac{25}{16}}{2\sigma^2}\Big) = \frac{1}{Z_d}\exp\Big(\frac{25}{32\sigma^2} - \frac{d^2}{4\sigma^2}\Big). \tag{5.21}$$

□

The holomorphic extension F of the density ρ depends on the shift parameter d, therefore we compute the norm for all the different values d established in Table 4.1.

d	$\frac{1}{Z_d}$	$\|F\|$
0	8.068220096219514	$4.2053614741860104 \cdot 10^{136}$
$2.50 \cdot 10^{-5}$	8.068220101579838	$4.2053612135634113 \cdot 10^{136}$
$1.06 \cdot 10^{-9}$	8.068220096219514	$4.2053614741860104 \cdot 10^{136}$
$1.00 \cdot 10^{-9}$	8.068220096219518	$4.205361474186012 \cdot 10^{136}$
$1.86 \cdot 10^{-10}$	8.068220096219516	$4.205361474186011 \cdot 10^{136}$

Table 5.6: Computed values of $\|F\|$ for different d.

The numerical computation suggests that for such small changes in the value of d the norm stays essentially the same, giving us an approximation independent of d.

$$\|F\| \approx 4.20536147418601 \cdot 10^{136}. \tag{5.22}$$

Now we have each component computed separately, so it is time to combine and compute the probability (3.21)

$$\Pr_{\rho}[L \geq k+1] = \lambda_4^k f_4^*[\rho]\; C_4\; \big(1 + \mathcal{O}(\|F\|\alpha^k)\big), \tag{5.23}$$

for $\nu_4 < \alpha < 1$.

We now have numerical approximations for all quantities appearing in (3.21). Before computing the probability $\Pr_\rho[L \geq k+1]$, these values are summarized in Table 5.7.

variable	value
λ_4	0.19945881834376726019184568597987 90
$f_4^*[\rho]$	5.18
C_4	0.31291933806424
$\|F\|$	$4.20536147418601 \cdot 10^{136}$
ν_4	0.4100105609983631

Table 5.7: Summary of the computed results for each component.

k	$\lambda_4^k f_4^*[\rho]\ C_4$	absolute error	$\|F\|\alpha^k$
10	1.615453943400404e-07	9.12112371177787e+125	-
20	1.6100041628524104e-14	1.220481492161273e+115	-
50	1.5937648832811815e-35	2.924016058473051e+82	-
100	1.5670625945861946e-70	1.2542785995364171e+28	-
110	1.5617760636514353e-77	1.6783280932495677e+17	-
150	1.5408076819308166e-105	5.3803220426791475e-27	-
200	1.4896101285713706e-175	9.900036355496615e-136	-
300	1.4646528716300584e-210	4.2466947810869394e-190	2.8994547877823496e+20
352	5.729322668164439e-247	1.218321414296922e-246	2.126466748096853
353	1.1427639293022386e-247	9.963459573488985e-248	0.8718738243315558
355	4.54635147116523e-249	6.663566456754009e-250	0.14656954041096468
400	1.4159857703248659e-280	7.814110826444745e-299	5.518495305678089e-19

Table 5.8: Computed probability $\Pr[L \geq k+1]$

Here, the absolute error is $\lambda_4^k f_4^*[\rho] C_4 \|F\| \alpha^k$, where we take α slightly larger than ν_4 to satisfy its condition $\nu_4 < \alpha < 1$, namely $\alpha = 0.4100105609983632$. And the relative error $\|F\|\alpha^k$ is only observed for the part where it gets more interesting.

We observe that the initial error is very large due to the large value of $\|F\|$. Consequently, the asymptotic estimate is not very informative for small values of k, since the error term dominates the leading term. It is only possible to make numerical statements about the probability once the relative error, that is, $\|F\|\alpha^k$ is sufficiently small. Equivalently, this occurs when the absolute error is much smaller than the leading term $\lambda_4^k f^*[\rho] C_4$. In our computations, this occurs at approximately $k = 353$, the point at which the absolute error becomes smaller than the computed probability value. By $k = 400$, the error is several orders of magnitude smaller than the leading term, indicating that the asymptotic approximation provides a highly accurate estimate of the probability.

$$\Pr[L \geq 401] \approx 1.4159857703248659 \cdot 10^{-280}. \tag{5.24}$$

Although the asymptotic estimate was expected to be inaccurate for small k, the observed error was surprisingly large. This is explained by the extremely large norm of the holomorphic extension F, which appears in the error term. The numerical experiments in Table 5.6 indicate that the norm remains essentially unchanged for small vertical shifts d of the density. Instead the dominant contribution comes from the choice of the complex neighborhood $\mathcal{V}$, since the dominant term $\exp\left(\frac{25}{32\sigma^2}\right)$ of

$$\|F\| = \frac{1}{Z_d} \exp\left(\frac{25}{32\sigma^2} - \frac{d^2}{4\sigma^2}\right)$$

comes from the radius of the chosen disk $\mathcal{V}$. Consequently, the large error term is primarily due to the analytic extension and the choice of $\mathcal{V}$, rather than the location of the line $y = d$. We recall that the disk $\mathcal{V}$ was introduced to create a suitable Banach space to prove the Perron-Frobenius properties of the transfer operator $\mathbf{G}_{s,t}$. This suggests that using different methods other than analyzing the spectrum properties of the transfer operator may produce more accurate results.

5.1.4 Numerical Verification in the uniform case

To check if the transfer operator method implemented is somewhat accurate, we compute the probability for the uniform case, since for low k (for example $k = 3$) we can compute the exact probability with

$$\Pr[L \geq k+1] = \sum_{|h|=k} \frac{1}{Q_k^2 (Q_k + Q_{k-1})^2}.$$

This formula comes from (3.8) using the fact that when representing h with the continuants we get

$$|h(0) - h(1)| = \frac{1}{Q_k (Q_k - Q_{k-1})}.$$

For small values of k, exact expressions are available; see [DFV96, Thm. 13]. For example,

$$\Pr[L \geq 2] = \frac{\pi^2}{3} - 3,$$
$$\Pr[L \geq 3] = -5 + \frac{2\pi^2}{3} - 2\zeta(3) + 2\sum_{n=0}^{\infty} (-1)^n (n+1)\zeta(n+4)(\zeta(n+2) - 1).$$

Evaluating these expressions numerically yields values with high numerical accuracy.

k	$\Pr[L \geq k+1]$
1	0.28986 81336 96452 87294
2	0.04848 08014 49463 63270
3	0.01027 81647 79066 59643

Table 5.9: High-precision numerical approximations of $\Pr[L \geq k+1]$ for $k = 1, 2, 3$.

Using the asymptotic estimate from (3.16),

$$\Pr[L \geq k+1] = \lambda_4^k \cdot f^*[u] \cdot (1 + \mathcal{O}(|\mu_4/\lambda_4|^k)), \quad u(t) = \frac{1}{(1+t)^2},$$

we obtain the approximations listed in the Table 5.10.

k	$\Pr[L \geq k+1]$
1	$0.0911463890628775 \cdot (1 + \mathcal{O}(0.4100105609983631))$
2	$0.01817995105878282 \cdot (1 + \mathcal{O}(0.1681086601301924))$
3	$0.0036261515557323414 \cdot (1 + \mathcal{O}(0.0689263260486633 5))$

Table 5.10: Numerical results using the transfer operator.

The parameters used in the computation are summarized in the Table 5.11.

variable	value
λ_4	0.19945881834376726019184568597987 90
μ_4	0.0817802220051986
$f^*[u]$	0.45696846005468011703662271333860073843744831574
m	64
M	1000

Table 5.11: Summary of the computed values used in the probability computation

Here, m denotes the size of the truncated operator matrix T_m, and M is the truncation bound used in the trace computation to obtain an upper bound for the subdominant eigenvalue μ_4.

Similarly, although not as extreme as for the general input density (5.8), there is a significant difference between the expected probability values and the calculated ones. Again, it was expected that the asymptotically estimated probability will not be accurate for such small values of k.

5.2 The Line-Disk intersection method

To obtain a more accurate approximation of the probability $\Pr[L \geq k+1]$ than that provided by the asymptotic estimate from the transfer operator method, we exploit the fact that the input lattices are concentrated around a horizontal line $l : y = d$. Using this geometric model, together with the geometry of the reduction domains, we derive an alternative approximation method.

As in Figure 3.1 visualized, each domain $\mathcal{D}_k$ consists of a row of decreasing disks. And each of these disks corresponds to a homography $h_{\mathbf{m}}$ of word $\mathbf{m} = [m_1, \ldots, m_k]$. We can go even further and determine the radius and center of a specific disk.

Let $a := h_{\mathbf{m}}(0), b := h_{\mathbf{m}}(1)$, depending on whether the depth k is even or odd, the value of either a or b is higher. Therefore, in general, the disk corresponding to $h_{\mathbf{m}}$ has a diameter $[\min(a,b), \max(a,b)]$. This allows us to uniquely identify each disk by its radius and center.

$$\text{radius} = \frac{|a-b|}{2}, \ \text{center} = \frac{a+b}{2} \ .$$

This is important because it enables us to determine whether the line $l : y = d$ intersects the disk, that is, if $d <$ radius. Note that we use the strict inequality because the measure of a single point is zero and therefore irrelevant to the result. The largest disk in a domain $\mathcal{D}_k$ always corresponds to $h_{\mathbf{m}}$, where $\mathbf{m} = [1, \ldots, 1]$, with k entries equal to 1. It is quick to determine which domains the line l intersects. We can then loop over the words to compute the intersection of the disks corresponding to these words and the line l. To improve understanding, the disk can be represented via the corresponding words as a tree, and depth-first search can then be used to iterate over them.

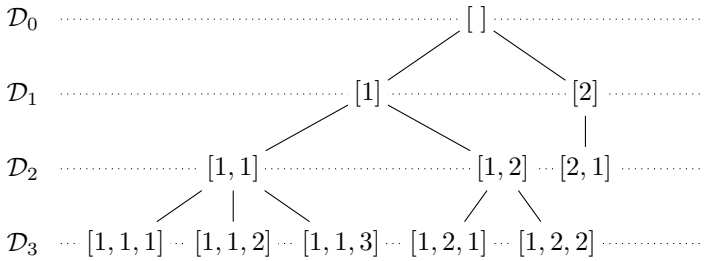

Figure 5.3: An example for a tree representation of the disks

As the domains $\mathcal{D}_k$ form a decreasing chain, we know that if a point z is in $\mathcal{D}_k$, then it is also in $\mathcal{D}_{k-1}$. This means that, with this depth-first search, we count the points multiple times. Therefore, to obtain the final result, we need to subtract the length of the domain $\mathcal{D}_k$ from the length of the domain $\mathcal{D}_{k-1}$, and so on.

k	length of $l \cap \mathcal{D}_k$
0	0.008
1	0.045
2	0.125
3	0.215
4	0.248
5	0.198
6	0.109
7	0.041
8	0.010
9	0.001
10	5.99e-05

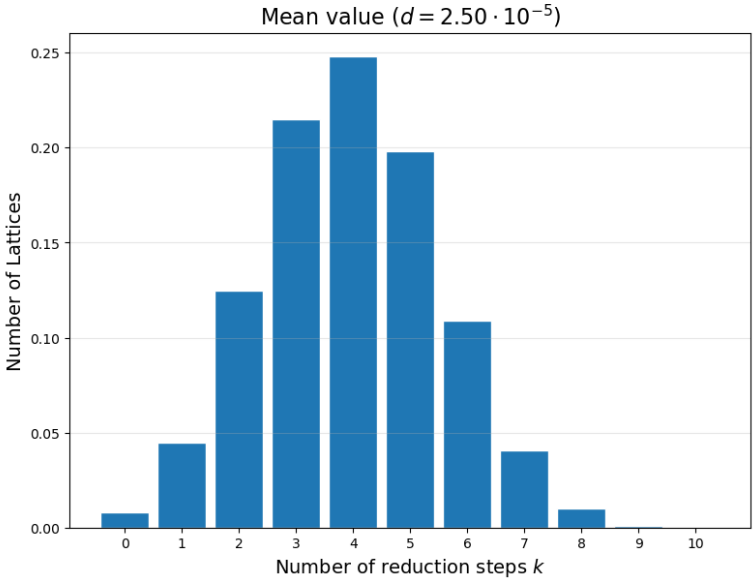

Figure 5.4: Total length with respect to k for line $l : y = 2.50e - 05$ (mean value) for $n = 3$.

k	length of $l \cap \mathcal{D}_k$
0	5.52e-05
1	0.001
2	0.003
3	0.012
4	0.032
5	0.067
6	0.113
7	0.155
8	0.175
9	0.163
10	0.127
11	0.081
12	0.043
13	0.019
14	0.007
15	0.002
16	4.00e-04
17	6.58e-05
18	7.14e-06
19	5.41e-07
20	2.84e-08

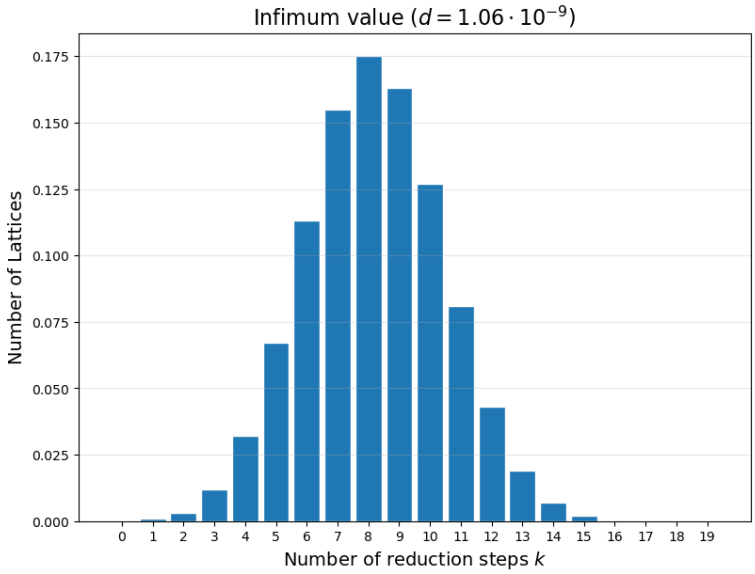

Table 5.12: Total length with respect to k for line $l : y = 1.06e - 09$ (infimum value) for $n = 3$.

k	length of $l \cap \mathcal{D}_k$
0	2.31e-05
1	2.60e-04
2	0.002
3	0.006
4	0.019
5	0.043
6	0.081
7	0.124
8	0.158
9	0.168
10	0.151
11	0.114
12	0.072
13	0.038
14	0.017
15	0.006
16	0.002
17	4.36e-04
18	8.08e-05
19	1.09e-05
20	1.01e-06
21	7.47e-08
22	7.82e-10

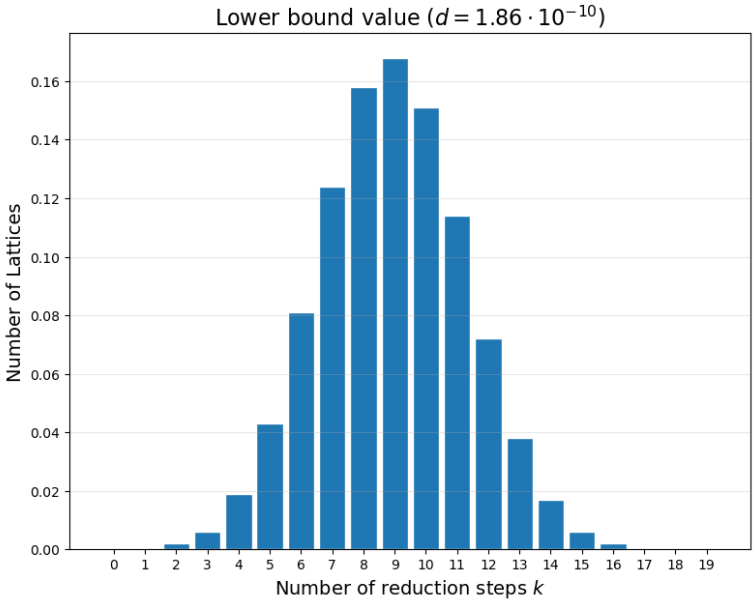

Table 5.13: Total length with respect to k for line $l : y = 1.86e - 10$ (lower bound) for $n = 3$.

All computations are created with $n = 3$, that is, the primes satisfy the bound

$$p \leq \sqrt{\left(\frac{|\Delta|}{4}\right)^n}.$$

We now compare these predicted results with those obtained from lattice sampling shown in Figure 4.6. The histogram of the number of reduction steps in Figure 5.13 is shifted to the right compared to the experimental data (see Figure 5.5). A possible explanation is the choice of the parameter d. In the prediction shown in Figure 5.13 d is chosen as a lower bound on the imaginary part of the lattices. Consequently, the modeled distribution (by the line $y = d$) is closer to the x-axis than the actual lattice samples. Since lattices closer to the x-axis tend to require more reduction steps, the model predicts more higher values for the reduction steps.

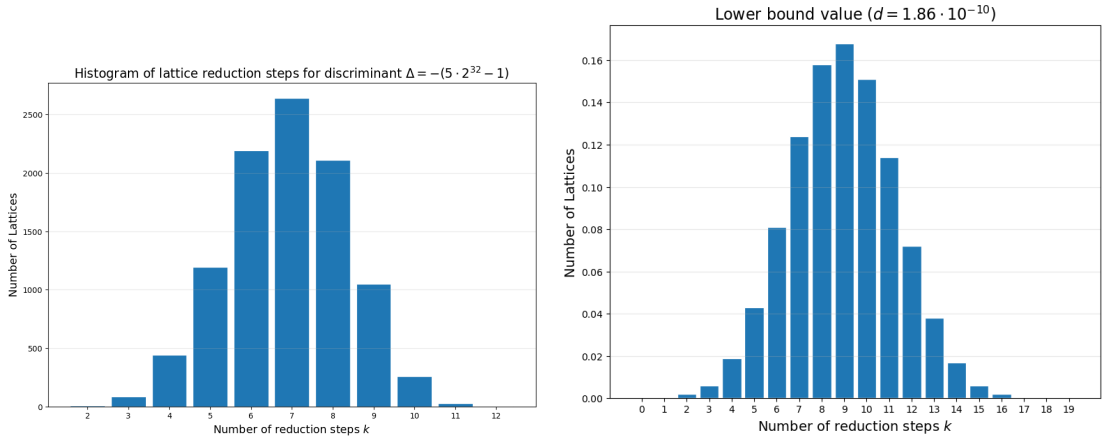

Figure 5.5: Comparison of the reduction-step distributions for sampled lattices (left) and the lower-bound model (right).

On the other hand, when d is chosen as the mean value of the imaginary part of the sampled lattices, the prediction shown in Figure 5.12 is shifted slightly to the left compared to the expected result (see Figure 5.6). Therefore, it tends to underestimate the number of reduction steps. We observe that the expected histogram lies between these predictions. This suggests that the Line-Intersection method provides a good approximation of the reduction step distribution. In particular, the prediction obtained by choosing d as the lower bound is preferable, as it yields an upper bound on the actual number of reduction steps. This is preferable since our primary interest lies in obtaining an upper bound on the probability $\Pr[L \geq k + 1]$.

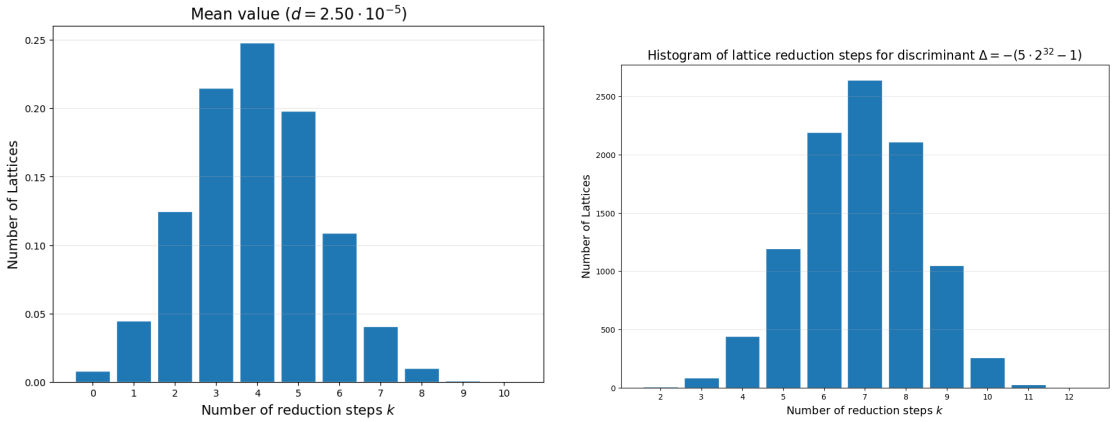

Figure 5.6: Comparison of the reduction-step distributions obtained from the mean-value model (left) and from sampled lattices (right).

5.3 Extension to band area

A possible direction for future work is to replace the line model by a thin horizontal band. Figure 4.3 suggests that the line model does not accurately represent the distribution of the input lattices. While the points are concentrated near a horizontal line, they also exhibit significant vertical scatter. This observation motivates replacing the line model with a thin horizontal band, and studying the area where it intersection with the domains $\mathcal{D}_k$.

The lower boundary of the band can be chosen using the proven lower bound (4.13),

$$\Im(z) \geq \sqrt{\left(\frac{4}{|\Delta|}\right)^{n-1}} \,.$$

For the upper boundary, one could extend the probabilistic analysis outlined at the end of Section 4.2. There, we briefly discussed how probabilistic lower bounds on the output primes might be obtained from the distribution of valid primes returned by Algorithm 3. A rigorous analysis would require taking all acceptance conditions into account and obtaining quantitative bounds on the resulting prime distribution, which was beyond the scope of this thesis.

Bibliography

[Alk12] Giedrius Alkauskas. "Transfer operator for the Gauss' continued fraction map. I. Structure of the eigenvalues and trace formulas". In: *arXiv preprint arXiv:1210.4083* (2012).

[Bor+] Giacomo Borin, Maria Corte-Real Santos, Jonathan Komada Eriksen, Riccardo Invernizzi, Marzio Mula, Sina Schaeffler, and Frederik Vercauteren. *Qlapoti: Simple and Efficient Translation of Quaternion Ideals to Isogenies*.

[Bue89] D. A. Buell. *Binary Quadratic Forms*. Springer-Verlag, 1989.

[Dar+25] Pierrick Dartois, Jonathan Komada Eriksen, Riccardo Invernizzi, and Frederik Vercauteren. *qt-Pegasis: Simpler and Faster Effective Class Group Actions*. 2025. HAL: `hal-05404059`. URL: `https://hal.science/hal-05404059v1`.

[Dev25] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.7)*. `https://www.sagemath.org`. 2025.

[DFV96] Hèléne Daudé, Philippe Flajolet, and Brigitte Vallée. *An Average-case Analysis of the Gaussian Algorithm for Lattice Reduction*. Research Report 2798. INRIA, 1996.

[Feo+20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. *SQISign: compact post-quantum signatures from quaternions and isogenies*. Cryptology ePrint Archive, Paper 2020/1240. 2020. URL: `https://eprint.iacr.org/2020/1240`.

[Joh07] Ulrich Vollmer Johannes Buchmann. *Binary Quadratic Forms - An Algorithmic Approach*. Springer, 2007.

[Kra64] M.A. Krasnosel'skii. *Positive Solutions of Operator Equations*. P. Noordhoff LTD, Groningen, the Netherlands, 1964.

[Lag80] Jeff C Lagarias. "Worst-case complexity bounds for algorithms in the theory of integral quadratic forms". In: *Journal of Algorithms* 1.2 (1980), pp. 142–186.

[May] Dieter H. Mayer. *Continued Fractions and Related Transformations*. Tech. rep. MPI/89-73. Bonn, Germany: Max-Planck-Institut für Mathematik. URL: `https://archive.mpim-bonn.mpg.de/id/eprint/1282/1/preprint_1989_73.pdf`.

[Rue02] David Ruelle. "Dynamical Zeta Functions and Transfer Operators". In: *Notices of the AMS* (2002), pp. 887–895.

[SBK24] István András Seres, Péter Burcsi, and Péter Kutas. *How (not) to hash into class groups of imaginary quadratic fields*. Oct. 2024.

[Sta21] Katherine E. Stange. *Quadratic forms, lattices, and ideal classes*. Teaching notes, University of Colorado. March 1, 2021. URL: `https://math.colorado.edu/~kstange/teaching-resources/numthy/quad-forms-class-gp.pdf`.

[Ste12] William Stein. *Algebraic Number Theory, A Computational Approach*. 14. November 2012.

[Val97] Brigitte Vallée. "Opérateurs de Ruelle–Mayer généralisés et analyse en moyenne des algorithmes d'Euclide et de Gauss". In: *Acta Arithmetica* 81.2 (1997), pp. 101–144.

[Wei] Eric W. Weisstein. *Gamma Function*. From MathWorld—A Wolfram Resource. Accessed: 24 April 2026. URL: `https://mathworld.wolfram.com/GammaFunction.html`.

[Wür26] Julia Würsch. *Lattice reduction*. GitHub repository. 2026. URL: `https://github.com/monolino/lattice_reduction`.

Declaration on the use of generative AI. Microsoft Copilot (Microsoft, 2026) and DeepL Write (DeepL, 2026) were used as auxiliary tools to improve the clarity and readability of the text, discuss mathematical concepts, and assist with Python and Sage programming tasks. The author retains full responsibility for the validity and authenticity of their work.