UNIVERSITY OF MELBOURNE

MASTER'S THESIS

Two-dimensional Random Unimodular Complex and Quaternion Lattices

Author:
Jiyuan ZHANG

Supervisor:
Prof. Peter J. FORRESTER

A thesis submitted in fulfillment of the requirements for the degree of Master of Science

in the

School of Mathematics and Statistics

University of Melbourne

Abstract

School of Mathematics and Statistics

Master of Science

Two-dimensional Random Unimodular Complex and Quaternion Lattices

by Jiyuan ZHANG

We discuss lattice reduction in complex and quaternion vector spaces, together with properties of random unimodular lattices that hold statistically, mainly in two dimensions. The computational problem of applying lattice reduction in complex and quaternion lattices is taken up. We give a unified proof of convergence of the appropriate analogue of the Lagrange-Gauss algorithm in the real case to the shortest basis. After specifying a meaning of random lattices, a decomposition of the invariant measure is given it in the coordinates with respect to the shortest basis, and integration over the latter gives rise to probability density functions of certain statistics. Numerical implementation of the lattice reduction algorithms allows for those statistics to be generated by simulation, and excellent agreement with the theory is obtained in all cases.

Acknowledgements

First, I would first like to thank my supervisor Prof. Peter Forrester for the continuous support of my master's study and research, for his patience, motivation, enthusiasm, and immense knowledge. The door to his office was always open whenever I ran into a trouble spot or had a question about my research or writing. I could not have imagined having a better supervisor for my master's study.

I would also like to thank all the mathematics and statistics fellow labmates, for the stimulating discussions and advice on my thesis writing, for the sleepless nights we were working together before deadlines, and for all the fun we have had in the last two years.

Finally, I must express my very profound gratitude to my parents and to my girlfriend, Quan Zhou, for providing me with unfailing support and continuous encouragement throughout my master's degree and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Contents

List of Symbols

$\mathbb{H}$	Set of quaternions
$\mathbb{F}$	Number system $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$, distinguished by the label $\beta = 1, 2, 4$ respectively
$\mathrm{GL}_N(\mathbb{F})$	General linear group over $\mathbb{F}$ of degree N
$\mathrm{SL}_N(\mathbb{F})$	Special linear group over $\mathbb{F}$ of degree N
$\mathrm{U}_N(\mathbb{F})$	Orthogonal group of degree N, unitary group of degree N or simplectic group of degree $2N$ specified by $\mathbb{F}$
$\mathbb{Z}[i]$	Set of Gaussian integers
H	Set of Hurwitz integers
$\mathbb{Z}^{(\beta)}$	$\mathbb{Z}$, $\mathbb{Z}[i]$ or H, distinguished by the label $\beta = 1, 2, 4$ respectively
$(\cdot)^\dagger$	Complex conjugate transpose
$\lceil \cdot \rfloor$	Closest integer function
$D_H(\cdot)$	Lattice quantizer in H
$\Gamma_N^{(\beta)}$	Set of $N \times N$ $\mathbb{F}$-valued lattices
$\zeta(\cdot)$	Riemann zeta function
C	Catalan's constant
χ	Indicator function
$\#\{\cdot\}$	Number of elements in a set
$\mathrm{vol}(\cdot)$	Volume of a measurable set
$\|\cdot\|_{\mathrm{op}}$	matrix operator norm
$\delta(\cdot)$	Dirac delta function

Chapter 1

Introduction

An 2-dimensional unimodular real $lattice$ is an integer span of a basis of $\mathbb{R}^2$, with its determinant having modulus 1, i.e. $\mathbb{Z}\mathbf{b}_1 + \mathbb{Z}\mathbf{b}_2$ and $|\det[\mathbf{b}_1\ \mathbf{b}_2]| = 1$. Such a concept can be generalised to N dimensions. Each lattice is associated with a reduced basis, in the sense that the basis consists of the shortest linearly independent vectors, which can be found by using lattice reduction algorithms. If the lattice is random its basis is a random matrix, following some distributions, and of particular interest is the statistically properties of this random basis such as the length of each basis vector and the angles between each pair of basis vectors. In a recent work [13], the functional forms of such statistical properties of 2-dimensional real random lattices in the sense of Siegel [32] are obtained exactly by integrating over the fundamental domain (set of all reduced lattices). In the same paper a procedure to generate those random lattices is also introduced and by applying a Lagrange-Gauss lattice reduction algorithm (see e.g. [1]), samples of the random basis are obtained and histograms are implemented showing the excellent agreement with the exact PDFs.

Exploring analogous questions in higher dimensional lattices is then a natural problem. However, the problem is complicated, as for example the Lagrange-Gauss algorithm only generates the successive minima up to dimensions $N = 4$ [31, 24], and in higher dimensions this task is costly and complicated. In random matrix theory, matrix groups with entries from any of the three associative normed division algebras $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$ are fundamental [11]. As such, attention is drawn to extending the considerations of [13] to the case of complex and quaternion vector spaces $\mathbb{C}^2$ and $\mathbb{H}^2$. One remarks that lattices in these vector spaces, with scalars equal to the Gaussian integers for $\mathbb{C}^2$, and Hurwitz integers for $\mathbb{H}^2$, received earlier attention for their application to

signal processing in wireless communication [39, 15, 5, 35], and their consequences for lattice packing bounds [37] respectively. The study [23] extends the LLL lattice reduction algorithm to these settings.

This motivates us to undertake a study of the 2-dimensional complex and quaternion lattice reduction problems, with some results applying for general dimensions. In Section 2 it is shown that an N-dimensional quaternion lattice can be viewed as a $2N$-dimensional complex lattice or a $4N$-dimensional real lattice, with some symmetry. In Section 3, we show that the main reason why a greedy reduced basis is that the shortest basis is the "integers" permit a Euclidean algorithm, and 2-dimensional complex and quaternion lattice reduction algorithms with respect to Gaussian and Hurwitz integers is therefore built by imitating the real Lagrange-Gauss algorithm. In the 2-dimensional complex case, the probability density function (PDF) for the lengths of the reduced basis vectors and the scaled inner product $\left| \mathbf{u_1}^{\dagger}\mathbf{u_2}/\|\mathbf{u_1}\|\|\mathbf{u_2}\| \right|$ are computed analytically in Section 4. Analogous considerations are applied to the quaternion lattice, but the corresponding measure is much more complicated to deal with. We find the shortest vector behaviour with length less than 1 by using Siegel's mean value theorem [32], and the asymptotic behaviour of the second shortest linearly independent vector with length tending towards infinity. The exact functional form of the PDF for the scaled inner product of the two basis vectors is also found. In Section 5 a way to sample matrices from $\mathrm{SL}_N(\mathbb{C})$ and $\mathrm{SL}_N(\mathbb{H})$ with a bounded operator norm is found. As for the case of $\mathrm{SL}_N(\mathbb{R})$ discussed in the first paragraph of this chapter, we take the viewpoint that the columns of these matrices specify bases for $\mathbb{C}^N$ and $\mathbb{H}^N$ respectively, and then implement the Lagrange-Gauss algorithm in the complex and quaternion case, obtaining histograms approximating the PDF for the lengths of the reduced basis vectors and the scaled inner product $\left| \mathbf{u_1}^{\dagger}\mathbf{u_2}/\|\mathbf{u_1}\|\|\mathbf{u_2}\| \right|$, and where possible compare against the analytic results. Furthermore, we have found the reason why bounded set gives a good approximation of the whole space in the sense of lattice reduction, and derived that the error produced by the cut-off is bounded by the tail of the PDF of the second shortest basis vector. A few related topics are discussed in Section 6.

Chapter 2

Lattices and reduced basis

Real and complex lattices

Let $N \geq 1$ and $\mathbf{x}_1,\ \mathbf{x}_2,\ ...,\ \mathbf{x}_N$ be a basis of $\mathbb{R}^N$. A (real-valued) lattice with dimension N and *basis* $\mathbf{x}_1,\ \mathbf{x}_2,\ ...,\ \mathbf{x}_N$ is defined as the integer span of the basis vectors:

$$\mathcal{L} = \left\{ \sum_{n=1}^{N} a_n \mathbf{x}_n : \forall \mathbf{x}_n \in \mathbb{R}^N,\ \forall a_n \in \mathbb{Z} \right\}.$$

The basis forms an $N \times N$ matrix $\mathbf{X} = [\mathbf{x}_1, ..., \mathbf{x}_N]$, where the vector $\mathbf{x}_i$ corresponds with the i-th column. The *determinant* of the lattice L with the basis $\mathbf{x}_1,\ \mathbf{x}_2,\ ...,\ \mathbf{x}_N$ is defined to be

$$\det \mathcal{L} = |\det \mathbf{X}|.$$

Proposition 2.1. *Although there are infinitely many basis for a lattice, the determinant of the lattice does not depend on the choice of basis.*

Proof. Follow the prove given from [1, Corollary 1.11]. Suppose $\mathbf{X}$ and $\mathbf{Y}$ are the matrix forms of two basis generating the same lattice, then $\mathbf{X} = \mathbf{BY},\ \mathbf{Y} = \mathbf{CX}$ with $\mathbf{B}$ and $\mathbf{C}$ being $N \times N$ matrices consisting of integer entries, and so $\mathbf{X} = \mathbf{BCX}$. Since $\mathbf{X}$ is a basis, it is invertible and the equation becomes $\mathbf{BC} = \mathbf{I}$, which gives

$$\det(\mathbf{B}) \det(\mathbf{C}) = 1. \tag{2.1}$$

Because $\mathbf{B}$ and $\mathbf{C}$ have only integer entries, it follows either $\det(\mathbf{B}) = \det(\mathbf{C}) = 1$ or $\det(\mathbf{B}) = \det(\mathbf{C}) = -1$. Hence $|\det(\mathbf{Y})| = |\det(\mathbf{CX})| = |\pm\det(\mathbf{X})| = |\det(\mathbf{X})|$. □

This allows us to discuss the volume spanned by basis vectors, sometimes called *covolume*, which has the same value as the absolute determinant of the lattice. Therefore, real lattices can be classified according to their determinants and the *unimodular* lattices, which have determinant 1 are of interests, since for any N dimensional lattice $\mathcal{L}$ with determinant λ, a corresponding lattice $\tilde{\mathcal{L}}$ with determinant 1 can be constructed by scaling each basis vector using a factor $\lambda^{-1/N}$.

This concept can be generalised into a *complex-valued lattice* (or complex lattice), defined as the *Gaussian integer* span of the complex-valued basis vectors:

$$\mathcal{L} = \left\{ \sum_{n=1}^{N} z_n \mathbf{x}_n : \forall z_n \in \mathbb{Z}[i] \right\},$$

where $\mathbf{x}_n \in \mathbb{C}^N$ and the notation $\mathbb{Z}[i]$, defined as $\{a+bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$, denotes the set of all Gaussian integers.

Proposition 2.2. *The determinant of a complex lattice, defined as the modulus of the determinant of one of its basis, does not depend on the choice of basis either.*

Proof. Following the settings of Proposition 2.1 with complex matrices and Gaussian integers replacing real matrices and integers respectively, equation (2.1) is obtained. Taking the modulus of both sides we have $|\det(\mathbf{B})||\det(\mathbf{C})| = 1$, and since the modulus of non-zero Gaussian integers must be greater than 1, $|\det(\mathbf{B})| = |\det(\mathbf{C})| = 1$ also holds and so does the same equality $|\det(\mathbf{Y})| = |\det(\mathbf{CX})| = |\det(\mathbf{C})||\det(\mathbf{X})| = |\det(\mathbf{X})|$. □

A complex number z can be expressed as a pair of real numbers, or a 2×2 block matrix:

$$z = a + bi \Leftrightarrow \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \tag{2.2}$$

where the matrix addition, multiplication, inversion and conjugation coincide with the corresponding operations in the complex field, for example:

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

$$\Leftrightarrow \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \begin{bmatrix} a & b \\ -b & a \end{bmatrix}.$$

Although general matrix multiplication is not commutative, the multiplication of such Hermitian matrices commutes. Then it is natural to think of the equivalence between N-dimensional complex lattices and $2N$-dimensional real lattices. Consider a 4-dimensional real lattice $\mathcal{L}$ whose basis can be written in the following matrix form:

$$\mathbf{A} = \begin{bmatrix} \mathbf{a}_1 & \mathbf{a}_2 & \mathbf{a}_3 & \mathbf{a}_4 \end{bmatrix} = \begin{bmatrix} b_{11}^R & b_{11}^I & b_{12}^R & b_{12}^I \\ -b_{11}^I & b_{11}^R & -b_{12}^I & b_{12}^R \\ b_{21}^R & b_{21}^I & b_{22}^R & b_{22}^I \\ -b_{21}^I & b_{21}^R & -b_{22}^I & b_{22}^R \end{bmatrix}$$

where each column represents a basis vector $\mathbf{a}_i$. For integers $z_1^R, z_2^R, z_1^I, z_2^I$, write

$$\begin{bmatrix} x_1^I \\ x_1^R \\ x_2^I \\ x_2^R \end{bmatrix} = \mathbf{a}_1 z_1^I + \mathbf{a}_2 z_1^R + \mathbf{a}_3 z_2^I + \mathbf{a}_4 z_2^R = \begin{bmatrix} b_{11}^R & b_{11}^I & b_{12}^R & b_{12}^I \\ -b_{11}^I & b_{11}^R & -b_{12}^I & b_{12}^R \\ b_{21}^R & b_{21}^I & b_{22}^R & b_{22}^I \\ -b_{21}^I & b_{21}^R & -b_{22}^I & b_{22}^R \end{bmatrix} \begin{bmatrix} z_1^I \\ z_1^R \\ z_2^I \\ z_2^R \end{bmatrix}. \tag{2.3}$$

The vector $[x_1^I\ x_1^R\ x_2^I\ x_2^R]^\top$ is therefore an element of the lattice $\mathcal{L}$. Denote $x_j = x_j^R + x_j^I i$, $z_j = z_j^R + z_j^I i$ and $b_{j,k} = b_{j,k}^R + b_{j,k}^I i$ for $j, k \in \{1, 2\}$, from the rule of matrix multiplication equation (2.3) is equivalent to:

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = z_1 \begin{bmatrix} b_{11} \\ b_{21} \end{bmatrix} + z_2 \begin{bmatrix} b_{12} \\ b_{22} \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}$$

where the 2×2 matrix represents a basis of $\mathbb{C}^2$, z_1, z_2 are Gaussian integers, and the vector $[x_1\ x_2]^\top$ is an element of a 2-dimensional complex lattice. This can be generalised to N dimensions. For a N-dimensional complex lattice with basis $\mathbf{B}$, the complex mapping $\mathbf{x} = \mathbf{Bz}$ can be equivalently expressed as

$$\begin{bmatrix} \text{Im}(x_1)\ \text{Re}(x_1)\ \text{Im}(x_2)\ \text{Re}(x_2)\ \ldots \end{bmatrix}^\top = \mathbf{A} \begin{bmatrix} \text{Im}(z_1)\ \text{Re}(z_1)\ \text{Im}(z_2)\ \text{Re}(z_2)\ \ldots \end{bmatrix}^\top$$

where $\mathbf{A}$ is a $2N \times 2N$ matrix, obtained from $\mathbf{B}$ by writing each complex entries into a 2×2 block using (2.2). Hence, any N-dimensional complex lattice can be viewed as a special case of a $2N$-dimensional real lattice. Sometimes concepts and results can be formulated directly for complex lattices with minor

modification from the real ones.

Quaternions and quaternion lattices

The idea of using 2 real numbers to represent a complex number is called the Cayley-Dickson construction, with which we can construct new number systems. Define a new imaginary unit j with $j^2 = -1$. Now writing

$$q = z + wj \Leftrightarrow \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix}, \; z, w \in \mathbb{C} \tag{2.4}$$

gives us a definition of $quaternions$. Denote by $\mathbb{H}$ the number system of quaternions. All operations defined in it including addition, multiplication, inversion and conjugation follow the rules of corresponding operations defined in $\mathrm{GL}_2(\mathbb{C})$, the set of 2×2 invertible complex matrices. Multiplication here is not commutative since

$$\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \neq \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

and therefore $\mathbb{H}$ is a non-commutative division ring. Another expression for the quaternions is the Cartesian form $q = a + bi + cj + dk$ where a, b, c, d are real numbers and the three imaginary units i, j, k follow the multiplication rules

$$i^2 = j^2 = k^2 = -1, \; ij = k.$$

These two expressions are equivalent in the setting $z = a + bi$ and $w = c + di$. There is one real part and three distinct imaginary parts of a quaternion:

$$\mathrm{Re}(q) = a, \; \mathrm{Im}_i(q) = b, \; \mathrm{Im}_j(q) = c, \; \mathrm{Im}_k(q) = d.$$

It can also be checked that quaternions inherit the property of complex numbers:

$$q\bar{q} = \bar{q}q = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}$$

and this is defined to be the $modulus$ of a quaternion $|q|$.

Recall the Euclidean space $\mathbb{R}^N$ and its generalisation $\mathbb{C}^N$, which consists of all N-tuples (column vectors) of real or complex numbers respectively. For

any real or complex vectors $\mathbf{u}$ and $\mathbf{v}$, the inner product defined on these spaces can be written into the same form:

$$\mathbf{u}^\dagger \mathbf{v} = \sum_{n=1}^{N} \bar{u}_n v_n. \tag{2.5}$$

We use the physicists' definition, as it is convenient to analyse column vectors. In this definition, the inner product is commutative, linear in the second argument, and positive definite:

$$\mathbf{u}^\dagger \mathbf{v} = \overline{\mathbf{v}^\dagger \mathbf{u}},\ \mathbf{u}^\dagger(\alpha \mathbf{v}_1 + \mathbf{v}_2) = \alpha \mathbf{u}^\dagger \mathbf{v}_1 + \mathbf{u}^\dagger \mathbf{v}_2,\ \mathbf{u}^\dagger \mathbf{u} \geq 0$$

where the last one holds as an equality only for $\mathbf{u} = 0$. The norm induced by this inner product is a real-valued function defined as $\|\mathbf{u}\| = \sqrt{\sum_{n=1}^{N} \bar{u}_n u_n} = \sqrt{\mathbf{u}^\dagger \mathbf{u}}$. Since completeness of the norms hold, those spaces are Hilbert spaces. An important result of vectors in $\mathbb{R}^N$ and $\mathbb{C}^N$ is the Cauchy-Schwarz inequality: $|\mathbf{v}^\dagger \mathbf{u}| \leq \|\mathbf{u}\| \|\mathbf{v}\|$.

Unlike $\mathbb{C}^N$, it is only possible to discuss the $\mathbb{H}$-module instead of a vector space, since $\mathbb{H}$ is not a (commutative) field. Define $\mathbb{H}^N$ as a right $\mathbb{H}$-module consisting of all N-tuples of quaternions, together with addition and right scalar multiplication over $\mathbb{H}$. With $\mathbf{u}$ and $\mathbf{v}$ viewed as $N \times 2$ complex matrices, the inner product can also be defined as (2.5) with commutativity. The linearity here is changed to

$$\mathbf{u}^\dagger(\mathbf{v}_1 \alpha + \mathbf{v}_2) = \mathbf{u}^\dagger \mathbf{v}_1 \alpha + \mathbf{u}^\dagger \mathbf{v}_2$$

as α is a quaternion and the multiplication is not commutative. Also for $\mathbf{u} = (q_1, ..., q_N)^\top$,

$$\mathbf{u}^\dagger \mathbf{u} = \sum_{n=1}^{N} \bar{q_n} q_n = \sum_{n=1}^{N} |q_n|^2 \geq 0$$

where the equality holds only for all $q_n = 0$ and this gives a positive definite inner product. The norm induced by the inner product can be defined in the same way, and the Cauchy-Schwarz inequality also holds since if we let $\lambda = \|\mathbf{v}\|^{-2} \mathbf{v}^\dagger \mathbf{u}$,

$$\begin{aligned} 0 &\leq \|\mathbf{u} - \mathbf{v}\lambda\|^2 \\ &= \|\mathbf{u}\|^2 - \overline{\mathbf{v}^\dagger \mathbf{u}}\lambda - \mathbf{v}^\dagger \mathbf{u}\bar{\lambda} + \|\mathbf{v}\|^2 \lambda\bar{\lambda} \\ &= \|\mathbf{u}\|^2 - \|\mathbf{v}\|^{-2} |\mathbf{v}^\dagger \mathbf{u}|^2 \Rightarrow \mathbf{v}^\dagger \mathbf{u} \geq \|\mathbf{u}\| \|\mathbf{v}\|. \end{aligned}$$

However, since $\mathbb{H}$ is a non-commutative division ring, $\mathbb{H}^N$ is not a Hilbert space.

A $quaternion-valued\ lattice$ (quaternion lattice) can be then defined as the $Hurwitz\ integers$ span of quaternion-valued basis vectors:

$$\mathcal{L} = \left\{ \sum_{n=1}^{N} q_n \mathbf{x}_n : \forall q_n \in H \right\}, \tag{2.6}$$

where $\mathbf{x}_n \in \mathbb{H}^N$ and H defined as $\left\{a+bi+cj+dk \in \mathbb{H} : a,b,c,d \in \mathbb{Z} \text{ or } a,b,c,d \in \mathbb{Z}+\frac{1}{2}\right\}$, denotes the set of all Hurwitz integers. Their distinguishing feature from the obvious $Lipschitz\ integers$, defined as the quaternions with each component an integer, is that they allow for a Euclidean algorithm (see e.g. [22]).

Proposition 2.3. *The determinant of a quaternion lattice, defined as the modulus of the determinant of one of its basis, again does not depend on the choice of basis.*

Proof. Analogous to Propositions 2.1 and 2.2, we follow the same settings in Proposition 2.1 except replacing real matrices and integers with quaternion matrices and Hurwitz integers, and then by the same steps we eventually get (2.1). Since the modulus of a non-zero Hurwitz integer is bigger than 1, the equality

$$|\det(\mathbf{B})| = |\det(\mathbf{C})| = 1$$

holds as well, and using similar discussion one can finish the proof. □

We can show the equivalence between N-dimensional quaternion lattice and $2N$-dimensional complex lattice as above. For an N-dimensional quaternion basis $\mathbf{B}$ and column vector $\mathbf{z}$ with Hurwitz integer entries, $\mathbf{x} = \mathbf{B}\mathbf{z}$ gives all elements in the quaternion lattice. This is equivalent to

$$\begin{bmatrix} \mathrm{Re}(\mathbf{x}_1) + i\mathrm{Im}_i(\mathbf{x}_1) \\ \mathrm{Im}_j(\mathbf{x}_1) + i\mathrm{Im}_k(\mathbf{x}_1) \\ \mathrm{Re}(\mathbf{x}_2) + i\mathrm{Im}_i(\mathbf{x}_2) \\ \mathrm{Im}_j(\mathbf{x}_2) + i\mathrm{Im}_k(\mathbf{x}_2) \\ \vdots \end{bmatrix} = \mathbf{A} \begin{bmatrix} \mathrm{Re}(\mathbf{z}_1) + i\mathrm{Im}_i(\mathbf{z}_1) \\ \mathrm{Im}_j(\mathbf{z}_1) + i\mathrm{Im}_k(\mathbf{z}_1) \\ \mathrm{Re}(\mathbf{z}_2) + i\mathrm{Im}_i(\mathbf{z}_2) \\ \mathrm{Im}_j(\mathbf{z}_2) + i\mathrm{Im}_k(\mathbf{z}_2) \\ \vdots \end{bmatrix}$$

where $\mathbf{A}$ is changed from $\mathbf{B}$ by writing each quaternion entries into a 2×2 block using (2.4), an analogue of (2.2). Here, due to the special structure of Hurwitz integers that it contains two sub-lattices, one of which consists of translated Lipschitz integers, the corresponding "complex integers" should be such that

at the $(2n-1)$-th and $2n$-th places both are Gaussian integers or half Gaussian integers, with $1 \leq n \leq N$.

A convenient notation of real, complex and quaternion number systems is introduced:

$$\mathbb{F} = \begin{cases} \mathbb{R}, \ \beta = 1 \\ \mathbb{C}, \ \beta = 2 \\ \mathbb{H}, \ \beta = 4 \end{cases}$$

where the label β, borrowed from the random matrix theory, denotes the number of independent real parts. Lattices are considered to be $\mathbb{F}$-valued without further description. Units in $\mathbb{F}$ are sometimes uniformly represented by e_r with $0 \leq r \leq \beta - 1$ for consistency, i.e.

$$1 = e_0, \ i = e_1, \ j = e_2, \ k = e_3.$$

Furthermore for the corresponding "integers" in each number system, we use $\mathbb{Z}^{(\beta)}$ to denote $\mathbb{Z}$, $\mathbb{Z}[i]$ or H, specified by the β.

Reduced basis

Denote the set of unimodular lattices $\Gamma_N^{(\beta)}$, where N is the dimension and β denotes the number system. This is also specified by the quotient space $\mathrm{SL}_N(\mathbb{F})/\mathrm{SL}_N(\mathbb{Z}^{(\beta)})$, or the $fundamental\ domain$. Other than a set of discrete points, a concise way to specify a lattice is to consider the collection of "shortest" vectors that generates this lattice, which is also called the $reduced\ basis$, uniquely (up to multiplication by an integer of unit modulus) associated with each lattice. The fundamental domain $\Gamma_N^{(\beta)}$ can be then viewed as the set consisting of all those reduced basis.

Definition 2.1. A basis $\{\mathbf{b}_1, ..., \mathbf{b}_N\}$ of a real lattice $\mathcal{L}$ is said to be ($Minkowski$) $reduced$ if for all $1 \leq i \leq N$, $\mathbf{b}_i$ has the minimal norm among all lattice vectors such that $\{\mathbf{b}_1, ..., \mathbf{b}_i\}$ can be extended to a basis of the lattice $\mathcal{L}$, i.e.

$$\|\mathbf{b}_1\| \leq \|\mathbf{b}_1\| \leq \cdots \leq \|\mathbf{b}_N\|,$$

$$\|\mathbf{b}_i + x_1\mathbf{b}_1 + \cdots + x_{i-1}\mathbf{b}_{i-1}\| \leq \|\mathbf{b}_i\|, \quad \forall x_i \in \mathbb{Z}^{(\beta)}, \quad \forall 2 \leq i \leq N.$$

It is a known theorem that a Minkowski reduced basis corresponds to the shortest linear independent vectors in the lattice for dimensions $N = 2, 3$ and 4 and in fact we will give a proof for $N = 2$ with general $\mathbb{F}$ in the next chapter. However in the case $N = 5$ the shortest linearly independent vectors may not form a basis. This is a classical result due to Korkine and Zolotareffin 1870's. Consider the matrix of basis vectors

$$X = \begin{bmatrix} 2 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

One observe that $(0, 0, 0, 0, 2)$ is a closest vector, but so replacing the last column does not allow the vector $(1, 1, 1, 1, 1)$ to be generated by integer linear combinations.

Given a $\mathrm{SL}_N(\mathbb{F})$ matrix $\mathbf{B}$ (a basis), there must be a unique (up to sign) matrix $\mathbf{V} \in \Gamma_N^{(\beta)}$ (a reduced basis), such that they span the same lattice. This corresponds to multiplying $\mathbf{M}$ to the right of $\mathbf{B}$, where $\mathbf{M} \in \mathrm{SL}_N^{\pm}\left(\mathbb{Z}^{(\beta)}\right)$ i.e. $\mathbf{V} = \mathbf{BM}$, and the choice of $\mathbf{M}$ is also unique. Similar discussion for $\mathbb{F} = \mathbb{R}$ appears in [1, 13]. Finding the unique $\mathbf{M}$ for a given basis is called the *lattice reduction algorithm*, which is discussed later on.

Chapter 3

Two-dimensional Lattice Reduction Algorithms

Our study of lattice reduction in $\mathbb{C}^2$ and $\mathbb{H}^2$ draws heavily on the theory of lattice reduction in $\mathbb{R}^2$. For the logical development of our work we must revise some essential aspects of the latter, presenting in particular theory associated with the Lagrange-Gauss algorithm.

The Lagrange-Gauss algorithm for lattice in $\mathbb{R}^2$

Let $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_0\}$ with $\|\mathbf{b}_1\| \leq \|\mathbf{b}_0\|$ say, be a basis for $\mathbb{R}^2$, and let $\mathcal{L} = \{n_1\mathbf{b}_1 + n_0\mathbf{b}_0 \,|\, n_1, n_0 \in \mathbb{Z}\}$ be the corresponding lattice. The lattice reduction problem in $\mathbb{R}^2$ is to find the shortest nonzero vector in $\mathcal{L}$ (call this $\boldsymbol{\alpha}$), and the shortest nonzero vector linearly independent from $\boldsymbol{\alpha}$ (call this $\boldsymbol{\beta}$) to obtain a new, reduced basis.

Let us suppose that a fundamental cell in $\mathcal{L}$ has unit volume. Then with $\boldsymbol{\alpha}, \boldsymbol{\beta}$ written as column vectors, the matrix $B = [\mathbf{b}_1\ \mathbf{b}_0]$ has unit modulus for its determinant, which we denote $\mathbf{B} \in \mathrm{SL}_2^{\pm}(\mathbb{R})$. Similarly with $\mathbf{V} = [\boldsymbol{\alpha}\,\boldsymbol{\beta}]$ we have $\mathbf{V} \in \mathrm{SL}_2^{\pm}(\mathbb{R})$. The matrices $\mathbf{B}$ and $\mathbf{V}$ are related by

$$\mathbf{V} = \mathbf{B}\mathbf{M}, \quad \mathbf{M} \in \mathrm{SL}_2^{\pm}(\mathbb{Z}). \tag{3.1}$$

The Lagrange-Gauss algorithm finds a sequence of matrices $\mathbf{M}_i \in \mathrm{SL}_2^-(\mathbb{Z})$ $(i = 1, \ldots, r^*)$ such that

$$\mathbf{M} = \mathbf{M}_1\mathbf{M}_2 \cdots \mathbf{M}_{r^*}, \quad \mathbf{M}_i = \begin{bmatrix} -m_i & 1 \\ 1 & 0 \end{bmatrix} \ (m_i \in \mathbb{Z}) \tag{3.2}$$

(in fact for $\mathbf{B}$ chosen with invariant measure, $\mathbf{M}$ samples from $\mathrm{SL}_2^{\pm}(\mathbb{Z})$ uniformly; see [25]). Define

$$\mathbf{B}_{j+1} = \mathbf{B}_j \begin{bmatrix} -m_j & 1 \\ 1 & 0 \end{bmatrix}, \quad \mathbf{B}_1 = \mathbf{B} = [\mathbf{b}_1\, \mathbf{b}_0], \tag{3.3}$$

the first column of $\mathbf{B}_j$ is the second column of $\mathbf{B}_{j+1}$ so that we can now set

$$\mathbf{B}_j = [\mathbf{b}_j\, \mathbf{b}_{j-1}]$$

for some 2×1 columns vectors $\mathbf{b}_j, \mathbf{b}_{j-1}$. Then (3.3) reduces to a single vector recurrence

$$\mathbf{b}_{j+1} = \mathbf{b}_{j-1} - m_j\mathbf{b}_j. \tag{3.4}$$

The integer m_j in (3.4) is chosen to minimise $\|\mathbf{b}_{j+1}\|$ and is given by

$$m_j = \left\lceil \frac{\mathbf{b}_j^\top \mathbf{b}_{j-1}}{\|\mathbf{b}_j\|^2} \right\rfloor, \tag{3.5}$$

where $\lceil \cdot \rfloor$ denotes the closest integer function (boundary case $\lceil \frac{1}{2} \rfloor = 0$), and so

$$\mathbf{b}_{j+1} = \mathbf{b}_{j-1} - \left\lceil \frac{\mathbf{b}_j^\top \mathbf{b}_{j-1}}{\|\mathbf{b}_j\|^2} \right\rfloor \mathbf{b}_j. \tag{3.6}$$

Geometrically, the RHS of (3.6) is recognised as the formula for the component of $\mathbf{b}_{j-1}$ near orthogonal to $\mathbf{b}_j$. The qualification "near" is required because m_j is constrained to be an integer so that $\mathbf{b}_{j+1} \in \mathcal{L}$.

A basic property of (3.4) is that successive vectors are smaller in magnitude whenever $m_{j+1} \neq 0$.

Lemma 3.1. *Suppose $m_{j+1} \neq 0$. We have*

$$\|\mathbf{b}_{j+1}\| < \|\mathbf{b}_j\|. \tag{3.7}$$

Proof. Generally

$$\lceil x \rfloor = x + \epsilon, \quad -\frac{1}{2} \leq \epsilon < \frac{1}{2},$$

and so

$$\lceil x - \lceil x \rfloor \rfloor = 0. \tag{3.8}$$

Now, taking the dot product of both sides of (3.6) with the vector $\mathbf{b}_j$ and dividing both sides by $\|\mathbf{b}_j\|^2$, use of (3.8) with $x = \mathbf{b}_j \cdot \mathbf{b}_{j-1}/\|\mathbf{b}_j\|^2$ implies

$$\left\lceil \frac{\mathbf{b}_j^\top \mathbf{b}_{j+1}}{\|\mathbf{b}_j\|^2} \right\rfloor = 0. \tag{3.9}$$

Comparing the LHS of (3.9) with the definition of m_{j+1} as implied by (3.5) by writing

$$\left\lceil \frac{\mathbf{b}_j^\top \mathbf{b}_{j+1}}{\|\mathbf{b}_j\|^2} \right\rfloor = \left\lceil \frac{\|\mathbf{b}_{j+1}\|^2}{\|\mathbf{b}_j\|^2} \frac{\mathbf{b}_j^\top \mathbf{b}_{j+1}}{\|\mathbf{b}_{j+1}\|^2} \right\rfloor$$

we conclude that if $m_{j+1} \neq 0$ then (3.4) holds, as required. □

Since the vectors in $\mathcal{L}$ with length less than some value R form a finite set, Lemma 3.1 implies that for some $j = r$ we must have $m_r = 0$. Then (3.4) gives $\mathbf{b}_{r+1} = \mathbf{b}_{r-1}$. If at this stage $\|\mathbf{b}_r\| \geq \|\mathbf{b}_{r-1}\|$, the algorithm stops with $r^* = r - 1$ in (3.2), and outputs

$$\boldsymbol{\alpha} = \mathbf{b}_{r-1}, \quad \boldsymbol{\beta} = \mathbf{b}_r \tag{3.10}$$

as the reduced basis. If instead $\|\mathbf{b}_r\| < \|\mathbf{b}_{r-1}\| (= \|\mathbf{b}_{r+1}\|)$ the algorithm stops with $r^* = r$ in (3.2) and outputs

$$\boldsymbol{\alpha} = \mathbf{b}_r, \quad \boldsymbol{\beta} = \mathbf{b}_{r+1} \tag{3.11}$$

as the reduced basis.

For both (3.10) and (3.11) it follows from (3.9) with $j = r, r-1$ respectively, and the relative length of $\mathbf{b}_{r+1}, \mathbf{b}_r$ that

$$\|\boldsymbol{\alpha}\| \leq \|\boldsymbol{\beta}\|, \quad \left\lceil \frac{\boldsymbol{\alpha}^\top \boldsymbol{\beta}}{\|\boldsymbol{\alpha}\|^2} \right\rfloor = 0 \tag{3.12}$$

or equivalently

$$\|\boldsymbol{\alpha}\| \leq \|\boldsymbol{\beta}\|, \quad \left| \frac{\boldsymbol{\alpha}^\top \boldsymbol{\beta}}{\|\boldsymbol{\alpha}\|^2} \right| \leq \frac{1}{2}. \tag{3.13}$$

Proposition 3.2. *The inequalities* (3.12) *are equivalent to*

$$\|\boldsymbol{\beta} + m\boldsymbol{\alpha}\| \geq \|\boldsymbol{\beta}\| \geq \|\boldsymbol{\alpha}\| \quad \forall m \in \mathbb{Z}. \tag{3.14}$$

Proof. Denote $m_* = -\boldsymbol{\alpha}^\top \boldsymbol{\beta}/\|\boldsymbol{\alpha}\|^2$, where we notice that $(\boldsymbol{\beta} + m_*\boldsymbol{\alpha})^\top \boldsymbol{\alpha} = 0$, and thus among all $\boldsymbol{\beta} + m\boldsymbol{\alpha}$ for $m \in \mathbb{R}$, $\boldsymbol{\beta} + m_*\boldsymbol{\alpha}$ has the shortest length. For integers m_1 and m_2 define $\Delta m_1 = m_1 - m_*$ and $\Delta m_2 = m_2 - m_*$ such that $|\Delta m_1| < |\Delta m_2|$. One has

$$\|\boldsymbol{\beta} + m_1\boldsymbol{\alpha}\|^2 = \|\boldsymbol{\beta} + m_*\boldsymbol{\alpha} + \Delta m_1\boldsymbol{\alpha}\|^2 = \|\boldsymbol{\beta} + m_*\boldsymbol{\alpha}\|^2 + |\Delta m_1|\,\|\boldsymbol{\alpha}\|^2$$

and

$$\|\boldsymbol{\beta} + m_2\boldsymbol{\alpha}\|^2 = \|\boldsymbol{\beta} + m_*\boldsymbol{\alpha} + \Delta m_2\boldsymbol{\alpha}\|^2 = \|\boldsymbol{\beta} + m_*\boldsymbol{\alpha}\|^2 + |\Delta m_2|\,\|\boldsymbol{\alpha}\|^2,$$

and therefore $\|\boldsymbol{\beta} + m_2\boldsymbol{\alpha}\| > \|\boldsymbol{\beta} + m_1\boldsymbol{\alpha}\|$. This can also be done backwards to show that for any integers m_1 and m_2 satisfying $\|\boldsymbol{\beta} + m_2\boldsymbol{\alpha}\| > \|\boldsymbol{\beta} + m_1\boldsymbol{\alpha}\|$, one has $|\Delta m_1| < |\Delta m_2|$.

So on the one hand, if $\lceil m_* \rfloor = 0$, the closest integer to m_* is 0 and then $\boldsymbol{\beta}$ is the shortest among all $\boldsymbol{\beta} + m\boldsymbol{\alpha}$ for integer m. On the other hand, if (3.14) holds then $\boldsymbol{\beta}$ is the shortest among all $\boldsymbol{\beta} + m\boldsymbol{\alpha}$ for integer m, and therefore $0 \leq m_* \leq 1 - m_*$ or $0 \geq m_* \geq -1 - m_*$, which imply $|m_*| \leq \frac{1}{2}$. □

A basis satisfying (3.14) is said to be greedy reduced in two dimensions [24]. Of fundamental importance is the classical fact that a greedy reduced basis in two dimensions is a shortest reduced basis (the converse is immediate).
Proposition 3.3. *Let* $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ *be a greedy reduced basis. Then* $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ *is a shortest reduced basis.*

Proof. We follow the proof given in [14], which begins with the greedy reduced basis inequalities (3.14). Let $\mathbf{v} = n_1\boldsymbol{\alpha} + n_2\boldsymbol{\beta}$ be any non-zero element of $\mathcal{L}$. In the case either $n_1, n_2 = 0$ it is immediate that $\|\mathbf{v}\| \geq \|\boldsymbol{\beta}\| \geq \|\boldsymbol{\alpha}\|$. In the case $n_1, n_2 \neq 0$, write $n_1 = qn_2 + r$ with $q, r \in \mathbb{Z}$ such that

$$0 \leq r < |n_2|. \tag{3.15}$$

Then

$$\mathbf{v} = r\boldsymbol{\alpha} + n_2(\boldsymbol{\beta} + q\boldsymbol{\alpha})$$

and thus by the triangle inequality

$$\begin{aligned}\|\mathbf{v}\| &\geq |n_2|\,\|\boldsymbol{\beta}+q\boldsymbol{\alpha}\| - r\|\boldsymbol{\alpha}\| \\ &= (|n_2|-r)\,\|\boldsymbol{\beta}+q\boldsymbol{\alpha}\| + r(\|\boldsymbol{\beta}+q\boldsymbol{\alpha}\| - \|\boldsymbol{\alpha}\|)\end{aligned} \tag{3.16}$$

Now by (3.14), $\|\boldsymbol{\beta}+q\boldsymbol{\alpha}\| - \|\boldsymbol{\alpha}\| \geq 0$ and so

$$\|\mathbf{v}\| \geq (|n_2|-r)\,\|\boldsymbol{\beta}+q\boldsymbol{\alpha}\| \geq \|\boldsymbol{\beta}+q\boldsymbol{\alpha}\|, \tag{3.17}$$

where the second inequality follows from (3.15). Finally, applying (3.14) gives $\|\mathbf{v}\| \geq \|\boldsymbol{\beta}\| \geq \|\boldsymbol{\alpha}\|$ as required. □

Lattice reduction in $\mathbb{C}^2$

Recall that with $B = \{\mathbf{b}_1, \mathbf{b}_2\}$, a basis in $\mathbb{C}^2$ such that $|\det[\mathbf{b_1}, \mathbf{b_2}]| = 1$ restricting the fundamental unit cell to have unit generalised area, the corresponding lattice is defined as

$$\mathcal{L} = \{m_1\mathbf{b_1} + m_2\mathbf{b_2} \,|\, m_1, m_2 \in \mathbb{Z}[i]\},$$

where $\mathbb{Z}[i]$ denotes the Gaussian integers. The complex Lagrange-Gauss algorithm proceeds by generalising the working of the real case as presented above. The equation (3.1) holds with $M \in \mathrm{SL}^{\pm}{}_2(\mathbb{Z}[i])$ and the matrices M_i in (3.2) are now elements of $\mathrm{SL}_2^-(\mathbb{Z}[i])$ with $m_i \in \mathbb{Z}[i]$. To minimise $\|\mathbf{b}_{j+1}\|$ in (3.4) requires

$$m_j = \left\lceil \frac{\mathbf{b}_j^\dagger \mathbf{b}_{j-1}}{\|\mathbf{b}_j\|^2} \right\rfloor \tag{3.18}$$

where $\lceil z \rfloor := \lceil \mathrm{Re}(z) \rfloor + i \lceil \mathrm{Im}(z) \rfloor$, and so the analogue of (3.6) reads

$$\mathbf{b}_{j+1} = \mathbf{b}_{j-1} - \left\lceil \frac{\mathbf{b}_j^\dagger \mathbf{b}_{j-1}}{\|\mathbf{b}_j\|^2} \right\rfloor \mathbf{b}_j. \tag{3.19}$$

Next, we would like to establish the analogue of Lemma 3.1.

Lemma 3.4. *Define* $\mathbf{b}_{j+1}$ *by* (3.19)*, and with* m_j *defined by* (3.18)*, suppose* $m_{j+1} \neq 0$*. Then we have the inequality*

$$\|\mathbf{b}_{j+1}\| < \|\mathbf{b}_j\|.$$

Proof. Analogously

$$\lceil z \rfloor = z + r, \quad |\mathrm{Re}(r)| < \frac{1}{2}, \quad |\mathrm{Im}(r)| < \frac{1}{2}$$

and so

$$\lceil z - \lceil z \rfloor \rfloor = 0. \tag{3.20}$$

Now, taking the dot product of both sides of (3.19) with the vector $\mathbf{b}_j$ and dividing both sides by $\|\mathbf{b}_j\|^2$, use of (3.20) with $z = \mathbf{b}_j^\dagger \mathbf{b}_{j-1}/\|\mathbf{b}_j\|^2$ implies

$$\left\lceil \frac{\|\mathbf{b}_{j+1}\|^2}{\|\mathbf{b}_j\|^2} \frac{\mathbf{b}_{j+1}^\dagger \mathbf{b}_j}{\|\mathbf{b}_{j+1}\|^2} \right\rfloor = \left\lceil \frac{\mathbf{b}_j^\dagger \mathbf{b}_{j+1}}{\|\mathbf{b}_j\|^2} \right\rfloor = 0 \tag{3.21}$$

Comparing the LHS of (3.21) with the definition of m_{j+1} as implied by (3.18) we gain the required conclusion. □

The complex Lagrange-Gauss algorithm terminates with outputs (3.10) or (3.11) depending on the validity of $\|\mathbf{b}_{r+1}\| \geq \|\mathbf{b}_r\|$ as in the real case, and the vectors $\boldsymbol{\alpha}, \boldsymbol{\beta}$ satisfying

$$\|\boldsymbol{\alpha}\| \leq \|\boldsymbol{\beta}\|, \quad \left\lceil \frac{\boldsymbol{\alpha}^\dagger \boldsymbol{\beta}}{\|\boldsymbol{\alpha}\|^2} \right\rfloor = 0, \tag{3.22}$$

or equivalently

$$\|\boldsymbol{\alpha}\| \leq \|\boldsymbol{\beta}\|, \quad \mathrm{Re}\left(\frac{\boldsymbol{\alpha}^\dagger \boldsymbol{\beta}}{\|\boldsymbol{\alpha}\|^2}\right) \leq \frac{1}{2}, \quad \mathrm{Im}\left(\frac{\boldsymbol{\alpha}^\dagger \boldsymbol{\beta}}{\|\boldsymbol{\alpha}\|^2}\right) \leq \frac{1}{2}.$$

Proposition 3.5. *The inequalities* (3.22) *are equivalent to*

$$\|\boldsymbol{\beta} + m\boldsymbol{\alpha}\| \geq \|\boldsymbol{\beta}\| \geq \|\boldsymbol{\alpha}\| \quad \forall m \in \mathbb{Z}[i]. \tag{3.23}$$

Proof. Denote $m_* = -\boldsymbol{\alpha}^\top \boldsymbol{\beta}/\|\boldsymbol{\alpha}\|^2$. We notice that $(\boldsymbol{\beta} + m_*\boldsymbol{\alpha})^\dagger \boldsymbol{\alpha} = 0$, and thus among all $\boldsymbol{\beta} + m\boldsymbol{\alpha}$ for $m \in \mathbb{C}$, $\boldsymbol{\beta} + m_*\boldsymbol{\alpha}$ has the shortest length. For Gaussian integers m_1 and m_2 define $\Delta m_1 = m_1 - m_*$ and $\Delta m_2 = m_2 - m_*$. Then by similar discussion to proposition 3.1, $|\Delta m_1| < |\Delta m_2| \Leftrightarrow \|\boldsymbol{\beta} + m_2\boldsymbol{\alpha}\| > \|\boldsymbol{\beta} + m_1\boldsymbol{\alpha}\|$. So on the one hand, if $\lceil m_* \rfloor = 0$, the closest Gaussian integer to m_* is 0 and then $\boldsymbol{\beta}$ is the shortest among all $\boldsymbol{\beta} + m\boldsymbol{\alpha}$ for Gaussian integer m. On the other hand, if (3.23) holds then $\boldsymbol{\beta}$ is the shortest among all $\boldsymbol{\beta} + m\boldsymbol{\alpha}$ for Gaussian integer m,

which implies m is inside the corresponding Voronoi region of 0 in the complex plane, directly giving $\lceil m \rfloor = 0$. □

The fact that $\mathbb{Z}[i]$ is a Euclidean domain with the absolute value as norm allows to deduce the complex analogue of Proposition 3.3.

Proposition 3.6. *For complex lattice, let $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ be a complex greedy reduced basis, then $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ is a shortest reduced basis.*

Proof. We follow the proof of Proposition 3.3, now setting $\mathbf{v} = n_1\boldsymbol{\alpha} + n_2\boldsymbol{\beta}$, $n_1, n_2 \in \mathbb{Z}[w]$. In the case $n_1 \neq 0$, the fact that $\mathbb{Z}[i]$ is a Euclidean domain with the absolute value as norm allows us to write

$$n_1 = qn_2 + r, \quad q, r \in \mathbb{Z}[i]$$

with

$$0 \leq |r| < |n_2|.$$

Equations (3.16) and (3.17) again hold, with r replaced by $|r|$, implying $\|\mathbf{v}\| \geq \|\boldsymbol{\beta}\| \geq \|\boldsymbol{\alpha}\|$ as required. □

Lattice reduction in $\mathbb{H}^2$

The definition of the quaternion number system was revised (2.6). With $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{H}^2$ and $|\det[\mathbf{b}_1\, \mathbf{b}_2]| = 1$ we make use of the Hurwitz integers to define the quaternion lattice

$$\mathcal{L}_H = \{m_1\mathbf{b_1} + m_2\mathbf{b_2} \,|\, m_1, m_2 \in H\}. \tag{3.24}$$

Around each Hurwitz integer z is its Voronoi region, consisting of all points in $\mathbb{H}$ closer to z than to all the other Hurwitz integer. Associated with this is a quantizer D_H, mapping a given $q \in \mathbb{H}$ to the closest Hurwitz integer (uniquely provided q is not on the boundary of the Voronoi region)

$$D_H(q) = \underset{\lambda \in H}{\operatorname{argmin}} \|\lambda - q\|. \tag{3.25}$$

Since the Hurwitz integer consists of two disjoint unions of rectangular lattices

$$H = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}\}$$

$$\cup \{(a+bi+cj+dk)+\frac{1}{2}(1+i+j+k) : a,b,c,d \in \mathbb{Z}\}$$

Denote them H_1 and H_2 respectively. Then

$$D_{H_1}(z) = \lceil \mathrm{Re}\, z \rfloor + \sum_{\nu=1}^{3} e_\nu \lceil \mathrm{Im}_{e_\nu} z \rfloor \tag{3.26}$$

$$D_{H_2}(z) = \left\lceil \mathrm{Re}(z-\frac{1}{2}) \right\rfloor + \sum_{\nu=1}^{3} e_\nu \left(\left\lceil \mathrm{Im}_{e_\nu}(z-\frac{1}{2}) \right\rfloor \right) + \frac{1}{2}(1+i+j+k) \tag{3.27}$$

and so

$$D_H(q) = \underset{\lambda \in \{D_{H_1}(q), D_{H_2}(q)\}}{\mathrm{argmin}} |\lambda - q|. \tag{3.28}$$

The lattice quantizer is relevant to the formulation of a quaternion Lagrange-Gauss algorithm. Thus the reasoning leading to (3.19) tells us that

$$m_j = D_H \left(\frac{\mathbf{b}_j^\dagger \mathbf{b}_{j-1}}{\|\mathbf{b}_j\|^2} \right), \tag{3.29}$$

$$\mathbf{b}_{j+1} = \mathbf{b}_{j-1} - D_H \left(\frac{\mathbf{b}_j^\dagger \mathbf{b}_{j-1}}{\|\mathbf{b}_j\|^2} \right) \mathbf{b}_j. \tag{3.30}$$

We will see below that the analogues of Lemmas 3.1 and 3.4 remain true. Iteration of (3.30) typically gives smaller vectors, as known in the real and complex cases from Lemmas 3.1 and 3.4.

Lemma 3.7. *Define* $\mathbf{b_{j+1}}$ *by* (3.30)*, and with* m_j *defined by* (3.29)*, suppose* $m_{j+1} \neq 0$*. Then we have the inequality* $\|\mathbf{b}_{j+1}\| < \|\mathbf{b}_j\|$.

Proof. Generally

$$D_H(\zeta) = \zeta + r,$$

where r is an element of the Voronoi region of the origin in H, telling us that

$$D_H\left(\zeta - D_H(\zeta)\right) = 0$$

(cf.(3.8) and (3.20)). Choosing $\zeta = \mathbf{b}_j^\dagger \mathbf{b}_{j-1}/\|\mathbf{b}_j\|^2$, after taking the dot product of both sides of (3.30) with respect to $\mathbf{b}_j^\dagger$ it follows that

$$D_H \left(\frac{\|\mathbf{b}_{j+1}\|^2}{\|\mathbf{b}_j\|^2} \frac{\mathbf{b}_{j+1}^\dagger \mathbf{b}_j}{\|\mathbf{b}_{j+1}\|^2} \right) = D_H \left(\frac{\mathbf{b}_j^\dagger \mathbf{b}_{j+1}}{\|\mathbf{b}_j\|^2} \right) = 0. \tag{3.31}$$

Comparing the definition of m_{j+1} and (3.31) we see that if $m_{j+1} \neq 0$, then we must have $\|\mathbf{b}_{j+1}\| < \|\mathbf{b}_j\|$, as required. □

As in the analogous setting for lattice reduction in $\mathbb{R}^2$ and $\mathbb{C}^2$, it follows from Lemma 3.7 that the quaternion Lagrange-Gauss algorithm terminates, and furthermore that the output vectors $\boldsymbol{\alpha}, \boldsymbol{\beta}$ can be chosen to satisfy

$$||\boldsymbol{\alpha}|| \leq ||\boldsymbol{\beta}||, \qquad D_H\Big(\frac{\boldsymbol{\alpha}^\dagger \boldsymbol{\beta}}{||\boldsymbol{\alpha}||^2}\Big) = 0. \tag{3.32}$$

Proposition 3.8. *The second condition of* (3.32) *is equivalent to requiring that*

$$||\boldsymbol{\beta} + m\boldsymbol{\alpha}|| \geq ||\boldsymbol{\beta}||, \qquad \forall m \in H. \tag{3.33}$$

Proof. Denote $m_* = -\boldsymbol{\alpha}^\dagger \boldsymbol{\beta}/\|\boldsymbol{\alpha}\|^2$, where we notice that $(\boldsymbol{\beta} + m_*\boldsymbol{\alpha})^\dagger \boldsymbol{\alpha} = 0$, and thus among all $\boldsymbol{\beta} + m\boldsymbol{\alpha}$ for $m \in \mathbb{H}$, $\boldsymbol{\beta} + m_*\boldsymbol{\alpha}$ has the shortest length. For Hurwitz integers m_1 and m_2 define $\Delta m_1 = m_1 - m_*$ and $\Delta m_2 = m_2 - m_*$. Then by similar discussion to proposition 3.1, $|\Delta m_1| < |\Delta m_2| \Leftrightarrow \|\boldsymbol{\beta} + m_2\boldsymbol{\alpha}\| > \|\boldsymbol{\beta} + m_1\boldsymbol{\alpha}\|$. So on the one hand, if $D_H(m_*) = 0$, the closest Hurwitz integer to m_* is 0 and then $\boldsymbol{\beta}$ is the shortest among all $\boldsymbol{\beta} + m\boldsymbol{\alpha}$ for Gaussian integer m. On the other hand, if (3.33) holds then $\boldsymbol{\beta}$ is the shortest among all $\boldsymbol{\beta} + m\boldsymbol{\alpha}$ for Hurwitz integer m, which implies m is inside the Voronoi region of 0 in $\mathbb{H}$, directly giving $D_H(m) = 0$. □

Thus $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ is a greedy basis. But we know from the proofs of Propositions 3.3 and 3.6 that subject only to the set of integers — here the Hurwitz integers H — being a Euclidean domain with absolute value for norm, the greedy basis $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ is the shortest reduced basis. It has already been remarked that as distinct from the Lipschitz integers the Hurwitz integers do allow for a Euclidean algorithm, and it furthermore is true that the absolute value function is the norm. Hence we have a quaternion analogue of Propositions 3.3 and 3.6.

Proposition 3.9. *Let $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ be a greedy basis for the Hurwtiz integer quaternion lattice. Then $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ is a shortest reduced basis.*

Proof. We follow the proof of Propositions 3.3 and 3.6, now setting $\mathbf{v} = n_1\boldsymbol{\alpha} + n_2\boldsymbol{\beta}$, $n_1, n_2 \in H$. In the case $n_1 \neq 0$, the assumption that H is a Euclidean domain with the absolute value as norm allows us to write

$$n_1 = qn_2 + r, \quad q, r \in H$$

with

$$0 \leq |r| < |n_2|.$$

Equations (3.16) and (3.17) again hold, with r replaced by $|r|$, implying $\|\mathbf{v}\| \geq \|\boldsymbol{\beta}\| \geq \|\boldsymbol{\alpha}\|$ as required. □

Chapter 4

Random lattices and their statistics

Random matrices and random lattices

Lattices can be represented as a matrix of reduced lattice vectors, so to consider random lattices one is naturally led to the topic of random matrix theory. Recall a random variable is a measurable function $\mathbf{G} : \Omega \to E$ where Ω refers to a probability space and E is a measurable space. If we let $E = \mathrm{Mat}_N(\mathbb{F})$, the set of $N \times N$ $\mathbb{F}$-valued matrix, the random variable becomes a $random\ matrix$. Another equivalent viewpoint is to consider an $\mathbb{F}$-valued random matrix as a matrix with $\mathbb{F}$-valued random variable entries.

A particular measure that is widely used in random matrix theory is the $invariant\ measure$. Generally it is defined as a measure μ on the Borel subsets of a locally compact Hausdorff topological group G, such that for all Borel subsets $S \subset G$ and $g \in G$ one has $\mu(gS) = \mu(Sg) = \mu(S)$. $Haar\ measure$ is the invariant inner regular measure that does not vanish identically (see e.g. [27, 28]). According to Haar's theorem, if G is compact, up to a positive multiplicative constant, there is a unique positive Haar measure. In particular, one can uniquely specify a Haar measure on G by imposing the normalization such that $\mu(G) = 1$, this assuming the measure is normalisable.

As an example let us consider the scalar case first. Let $x = \sum_{r=1}^{\beta} x_r e_r \in \mathbb{F}$, and recall the Lebesgue measure $\mathrm{d}x = \prod_{r=1}^{\beta} \mathrm{d}x_r$ has the property of being unchanged by translation. Thus for a fixed $x^{(0)} \in \mathbb{F}$,

$$\mathrm{d}(x + x^{(0)}) = \prod_{r=1}^{\beta} \mathrm{d}(x_r + x_r^{(0)}) = \prod_{r=1}^{\beta} \mathrm{d}x_r = \mathrm{d}x.$$

The modification of Lebesgue measure needed to have invariance with respect to scalar multiplication is

$$\mathrm{d}\mu(x) = \frac{\mathrm{d}x}{|x|^\beta} \tag{4.1}$$

as one can check that $|\det \frac{\partial(\alpha x)}{\partial x}| = |\alpha|^\beta$ for any $\alpha \in \mathbb{F}$. Therefore $\mathrm{d}\mu(x)$ is uncharged by replacing x with αx.

Consider the invariant measure of matrices. Let $\mathbf{G} \in \mathrm{GL}_N(\mathbb{F})$. For a fixed $\mathbf{A} \in \mathrm{GL}_N(\mathbb{F})$,

$$(\mathrm{d}\mathbf{AG}) = (\mathrm{d}\mathbf{GA}) = |\det \mathbf{A}|^{\beta N}(\mathrm{d}\mathbf{G})$$

(these follow from e.g. [12, Prop. 3.2.4]). One therefore has that

$$\frac{(\mathrm{d}\mathbf{G})}{|\det \mathbf{G}|^{\beta N}} \tag{4.2}$$

is unchanged by both left and right group multiplication, and is thus the left and right invariant Haar measure for the group. Note that in (4.2) the case $N = 1$ reduces to (4.1), and in the case of $\mathrm{GL}_N(\mathbb{R})$ and thus $\beta = 1$ (4.2) was identified by Siegel [32]. Matrices in $\mathrm{SL}_N(\mathbb{F})$ form a subgroup of $\mathrm{GL}_N(\mathbb{F})$ with unit determinant and using a delta function distribution to implement the constraint the invariant measure is written as

$$\delta(1 - \det \mathbf{G})(\mathrm{d}\mathbf{G}) \tag{4.3}$$

We point out the fact that neither (4.2) nor (4.3) is normalizable. Another matrix group of importance is the unitary group:

$$\mathrm{U}_N(\mathbb{F}) := \{\mathbf{G} \in \mathrm{GL}_N(\mathbb{F}) : \mathbf{G}^\dagger\mathbf{G} = \mathbf{I}\}.$$

We denote the Haar measure of $\mathbf{G} \in \mathrm{U}_N(\mathbb{F})$ as $(\mathbf{G}^\dagger\mathrm{d}\mathbf{G})$. For $\mathbb{F} = \mathbb{R}$ and $\mathbb{C}$ this was first identified by Hurwitz [17]; the extension of Hurwitz's ideas to the case of unitary matrices with quaternion entries is given in [8]. The precise value of its volume $\mathrm{vol}(\mathrm{U}_N(\mathbb{F}))$ depends on the convention used to relate the line element corresponding to the differential $\left(\mathbf{G}^\dagger\mathrm{d}\mathbf{G}\right)$ to the Euclidean line element; see [13, Remark 2.3]. This convention can be uniquely specified by integrating (5.4) against Gaussian weighted matrices – see [13, Remark 2.3] –

with the result [7, Eq. (1) with $m = n$]

$$\operatorname{vol} \mathrm{U}_N(\mathbb{F}) = 2^N \prod_{k=1}^{N} \frac{\pi^{\beta k/2}}{\Gamma(\beta k/2)}. \tag{4.4}$$

Siegel [32] introduced the notion of a random lattice. The construction of Siegel of a random lattice requires first the specification of the unique invariant measure for the matrix group $\mathrm{SL}_N(\mathbb{R})$ as identified in (4.3) above; each such matrix is interpreted as having columns forming a basis $\mathcal{B}$. One also requires the fact that the quotient space $\mathrm{SL}_N(\mathbb{R})/\mathrm{SL}_N(\mathbb{Z})$ can be identified with the lattice $\mathcal{L}$, and that this quotient space has finite volume with respect to the invariant measure.

Such construction can be extended to general $\mathbb{F}$. After applying a lattice reduction algorithm, the domain of the basis is restricted in the quotient space $\mathrm{SL}_N(\mathbb{F})/\mathrm{SL}_N(\mathbb{Z}^{(\beta)})$ and the invariant measure (4.3) holds

$$\chi_{\mathbf{G}\in\Gamma_N^{(\beta)}} \delta(1 - \det \mathbf{G})(\mathrm{d}\mathbf{G}) \tag{4.5}$$

This measure is normalizable [32, 33], and with volume denoted as $\operatorname{vol}\left(\Gamma_N^{(\beta)}\right)$ gives the normalization.

Statistics for the real lattice

As already noted in [12], the Haar measure for $\mathrm{SL}_N(\mathbb{R})$ with $N = 2$ can be parametrised in terms of variables convenient for the computation of statistics. The variables of interest come about by writing $\mathbf{V} \in \mathrm{SL}_2(\mathbb{R})$ in the form $\mathbf{V} = \mathbf{QR}$, where $\mathbf{Q}$ is a real orthogonal matrix with determinant $+1$ and $\mathbf{R}$ is an upper triangular matrix with positive diagonal entries,

$$\mathbf{R} = \begin{bmatrix} r_{11} & r_{12} \\ 0 & r_{22} \end{bmatrix}, \quad r_{22} = 1/r_{11}. \tag{4.6}$$

With $\mathbf{V} = [\boldsymbol{\alpha}\,\boldsymbol{\beta}]$, the matrix $\mathbf{Q}$ can be used to rotate the lattice so that $\boldsymbol{\alpha}$ lies along the positive x-axis. Thus (4.6) gives $\boldsymbol{\alpha} = (r_{11}, 0)$, $\boldsymbol{\beta} = (r_{12}, 1/r_{11})$ and the

inequalities (3.13) read

$$r_{12}^2 + r_{22}^2 \geq r_{11}^2, \quad 2|r_{12}| \leq r_{11}. \tag{4.7}$$

Further, [12, Ex. 3.2 q4 (i)] tells us that applying a QR decomposition on a 2×2 real random matrix $\mathbf{V}$ gives

$$(\mathrm{d}\mathbf{V}) = r_{11}(\mathrm{d}\mathbf{R})(\mathbf{Q}^\top \mathrm{d}\mathbf{Q}). \tag{4.8}$$

Substitute (4.6) and (4.8) to (4.5) and the invariant measure in the coordinates r_{11} and r_{12} is proportional to

$$\chi_{r_{12}^2 \geq r_{11}^2 - 1/r_{11}^2} \chi_{|r_{12}| \leq r_{11}/2} \, \mathrm{d}r_{11}\mathrm{d}r_{12}. \tag{4.9}$$

The factor 2π coming from integrating $(\mathbf{Q}^\top \mathrm{d}\mathbf{Q})$ is not included in this expression as it effectively cancels out by the requirement that the probability density functions be normalised. The value 2π is equal to one half of the value implied by (4.4) due to the requirement that $\det \mathbf{Q} = +1$. In [13], volume and probability density functions for the length of the basis vectors of 2-dimensional real lattice are discussed, as well as the angle between basis vectors.

Proposition 4.1. *Let the volume associated with (4.9) be denoted* $\mathrm{vol}\,\Gamma_2^{(1)}$. *We have*

$$\mathrm{vol}\,\Gamma_2^{(1)} = \frac{\pi}{6}. \tag{4.10}$$

The probability density function of the length of the shortest basis vector is given by

$$\frac{6}{\pi}\left(\chi_{r<1} r + \chi_{1<r<(4/3)^{1/2}}\left(r - \frac{2}{r}\sqrt{r^4-1}\right)\right). \tag{4.11}$$

The probability density function of the length of the second shortest basis vector is given by

$$\frac{12}{\pi s}\left(\chi_{1<s<(4/3)^{1/2}}\sqrt{s^4-1} + \chi_{s>(4/3)^{1/2}}\left(s^2 - \sqrt{s^4-1}\right)\right). \tag{4.12}$$

The probability function of $\xi := \cos\theta$, *where* θ *is the angle between those two basis vectors, is given by*

$$-\frac{3}{2\pi}\frac{\log(4\xi^2)}{\sqrt{1-\xi^2}}, \quad 0 < |\xi| < 1/2. \tag{4.13}$$

Proof. For notation convenience write $r_{11} = r$ and $r_{12} = x$. The inequalities

(4.7) tells us that the maximum value of r occurs when $(r/2)^2 = r^2 1/r^2 \Rightarrow r = (4/3)^{1/2}$. It follows that the p.d.f for the shortest basis vector is

$$\frac{1}{\mathrm{vol}\,\Gamma_2^{(1)}}\left(2\chi_{0<r<1}\int \chi_{0<x<r/2}\mathrm{d}x + 2\chi_{1<r<(4/3)^{1/2}}\int \chi_{\sqrt{r^2-1/r^2}<x<r/2}\mathrm{d}x\right)$$

and the fact that its integration over r equals 1 gives the volume. Together we obtain (4.11) and (4.10). The length of the second shortest vector is $s := \sqrt{x^2+1/r^2}$, and applying the change of variable $r = 1/\sqrt{s^2-x^2}$ to (4.9) gives

$$\int \frac{1}{\mathrm{vol}\,\Gamma_2^{(1)}}\chi_{x^2\le s^2-1/s^2}\chi_{x^2+1/(4x^2)\ge s^2}\frac{s}{(s^2-x^2)^{3/2}}dx,$$

simplified to (4.12). For the angle $\xi = x/\sqrt{x^2+1/r^2}$, we consider the transform $x = \xi/(r\sqrt{1-\xi^2})$ and (4.9) becomes

$$\frac{1}{\mathrm{vol}\,\Gamma_2^{(1)}(1-\xi^2)^{3/2}}\int \chi_{(4\xi^2/(1-\xi^2))^{1/4}\le r\le(1-\xi^2)^{1/4}}\frac{1}{r}dr,$$

simplified to (4.13). □

Remark 4.2. *Expanding* (4.12) *for large* s *gives*

$$\frac{6}{\pi}\left(\frac{1}{s^3}+\frac{1}{4s^7}+O\left(\frac{1}{s^{11}}\right)\right). \tag{4.14}$$

In the variable $\tilde{s} = 1/s$*, the leading term in the* $\tilde{s}\to 0$ *expansion is thus* $6\tilde{s}/\pi$*, which is precisely that exhibited by the PDF for the shortest vector.*

Statistics of the shortest reduced basis for the Gaussian integers

In the real case the inequalities (3.13) specifying a shortest reduced basis can also be obtained by transforming the basis vectors to a Gram-Schmidt basis. In the complex case this can be achieved by writing $\mathbf{V} = \mathbf{UT}$, where $\mathbf{U} \in \mathrm{SL}_2(\mathbb{C})$ and

$$\mathbf{T} = \begin{bmatrix} t_{11} & t_{12}^{(r)} + it_{12}^{(i)} \\ 0 & t_{22} \end{bmatrix}, \quad t_{11} > 0,\ t_{22} = 1/t_{11}. \tag{4.15}$$

Making use of the known change of variables from the elements of $\mathbf{V}$ to $\{\mathbf{U}, \mathbf{T}\}$ (see e.g. [12, Eq.(3.23)]) the invariant measure (4.5) for $N = 2$ can be written

$$\delta(1 - t_{11}t_{22})t_{11}^3 t_{22}\mathrm{d}t_{11}\mathrm{d}t_{22}(\mathbf{U}^\dagger \mathrm{d}\mathbf{U}). \tag{4.16}$$

Also, with $\boldsymbol{\alpha} = (t_{11}, 0)$, $\boldsymbol{\beta} = (t_{12}^{(r)} + it_{12}^{(i)}, 1/t_{11})$ the inequalities (3.22) read

$$t_{11}^2 \leq (t_{12}^{(r)})^2 + (t_{12}^{(i)})^2 + (1/t_{11})^2, \quad 2|t_{12}^{(r)}| \leq t_{11}, \quad 2|t_{12}^{(i)}| \leq t_{11}. \tag{4.17}$$

Integrating over t_{22} shows that as a function of the variables $\{t_{11}, t_{12}^{(r)}, t_{12}^{(i)}\}$ the invariant measure restricted to the domain of the shortest reduced basis is equal to

$$t_{11}\chi_{t_{11}^2 \leq (t_{12}^{(r)})^2 + (t_{12}^{(i)})^2 + (1/t_{11})^2}\chi_{2|t_{12}^{(r)}| \leq t_{11}}\chi_{2|t_{12}^{(i)}| \leq t_{11}}\mathrm{d}t_{11}\mathrm{d}t_{12}^{(r)}\mathrm{d}t_{12}^{(i)}. \tag{4.18}$$

This does not include the integration over $(\mathbf{U}^\dagger \mathrm{d}\mathbf{U})$, which according to (4.4) evaluates to $2\pi^2$; being a constant this effectively plays no role in subsequent calculations.

The statistics of the corresponding shortest basis vectors are determined by appropriate integration over (4.18) – t_{11} is the length of the shortest vector, $\left((t_{12}^{(r)})^2 + (t_{12}^{(i)})^2 + (1/t_{11})^2\right)^{1/2}$ is the length of the second shortest vector, while for the complex analogue of the cosine of the angle between α and β we have

$$\frac{\boldsymbol{\alpha}^\dagger \boldsymbol{\beta}}{\|\boldsymbol{\alpha}\|\|\boldsymbol{\beta}\|} = \frac{t_{12}^{(r)} + it_{12}^{(i)}}{\sqrt{(t_{12}^{(r)})^2 + (t_{12}^{(i)})^2 + (1/t_{11})^2}}. \tag{4.19}$$

These variables should be held fixed when computing the corresponding PDF. Integrating (4.18) over all variables gives a volume $\mathrm{vol}\,\widehat{\Gamma}_2^{(2)}$, which occurs in the computation of the PDFs as the normalisation. Our first task is to compute this volume.

Proposition 4.3. *Let the volume associated with* (4.18) *be denoted* $\mathrm{vol}\,\Gamma_2^{(2)}$. *We have*

$$\mathrm{vol}\,\Gamma_2^{(2)} = \frac{C}{3}, \tag{4.20}$$

where C denotes Catalan's constant.

Proof. For notational convenience in (4.18) we write $t_{11} = t$, $t_{12}^{(r)} = y_1$, $t_{12}^{(i)} = y_2$. Integrating over y_1 and y_2 gives

$$t\mathrm{d}t \int \chi_{\|\mathbf{y}\|^2 \geq t^2 - 1/t^2} \chi_{|y_1| \leq t/2} \chi_{|y_2| \leq t/2} \mathrm{d}y_1 \mathrm{d}y_2, \tag{4.21}$$

where $\mathbf{y} = (y_1, y_2)$. Geometrically, the integral here corresponds to the area overlap between the outside of a disk of radius $t^2 - 1/t^2$ $(t \geq 1)$ centred at the origin, and a square of side length t centred at the origin. For $t < 1$ the first inequality is always true, and the integral is equal to the area of the square, t^2.

It follows that with $V_2(a, b)$ denoting the area of overlap between a disk of radius a, and square of side length b, both centred at the origin, (4.21) can be written

$$\begin{aligned} &\left(t^3 \chi_{0<t<1} + \chi_{t>1} t \left(t^2 - V_2\left((t^2 - 1/t^2)^{1/2}, t/2\right)\right)\right) \mathrm{d}t \\ &\quad = \left(t^3 \chi_{0<t<1} + \chi_{t>1} t \left(t^2 - (t^2 - 1/t^2) V_2\left(1, \frac{t}{2(t^2 - 1/t^2)^{1/2}}\right)\right)\right) \mathrm{d}t. \end{aligned} \tag{4.22}$$

According to Problem 96-19, SIAM Review 39 p.779-786 (1997), or alternatively by direct calculation

$$V_2(1, a) = \begin{cases} 4a^2, & 0 < a < 1/\sqrt{2} \\ 4a\sqrt{1 - a^2} + 4 \arcsin a - \pi, & 1/\sqrt{2} < a < 1 \\ \pi, & 1 < a \end{cases} \tag{4.23}$$

thus reducing (4.22) to

$$\begin{aligned} &\Big(\chi_{0<t<1} t^3 + \chi_{1<t<(4/3)^{1/4}} t(t^2 - \pi(t^2 - 1/t^2)) \\ &+ \chi_{(4/3)^{1/4}<t<2^{1/4}} t \left(t^2 - (t^2 - 1/t^2)(4a\sqrt{1 - a^2} + 4 \arcsin a - \pi)|_{a = \frac{t}{2(t^2 - 1/t^2)^{1/2}}}\right)\Big) \mathrm{d}t. \end{aligned} \tag{4.24}$$

Elementary integration and/or use of computer algebra gives for the integral over t

$$\int \chi_{0<t<1} t^3 \mathrm{d}t = \frac{1}{4} \tag{4.25}$$

$$\int \chi_{1<t<(4/3)^{1/4}} t(t^2-\pi(t^2-1/t^2))\mathrm{d}t = \frac{1}{12}\left(1+\pi(-1+\log(64/27))\right) \tag{4.26}$$

$$\int \chi_{(4/3)^{1/4}<t<2^{1/4}} t\left(t^2-(t^2-1/t^2)(4a\sqrt{1-a^2}-\pi)|_{a=\frac{t}{2(t^2-1/t^2)^{1/2}}}\right)\mathrm{d}t$$
$$= \frac{1}{12}\left(-4+2\pi-3\pi\log(3/2)-2\sqrt{3}\log(2-\sqrt{3})\right) \tag{4.27}$$

$$\int \chi_{(4/3)^{1/4}<t<2^{1/4}} t^3 4\arcsin\frac{t}{2(t^2-1/t^2)^{1/2}}\mathrm{d}t = \frac{1}{12}\left(-\pi+\sqrt{3}\log(7-4\sqrt{3})\right). \tag{4.28}$$

However the remaining integral

$$\int \chi_{(4/3)^{1/4}<t<2^{1/4}} \frac{4}{t}\arcsin\frac{t}{2(t^2-1/t^2)^{1/2}}\mathrm{d}t$$

does not yield immediately to such an approach. For this integral, to be denoted J, we begin with some simple manipulation and the change of variables $1/t^2 = s$ to obtain

$$J = \int_{1/2}^{3/4} \frac{1}{s}\arcsin\frac{1}{2(1-s)^{1/2}}\mathrm{d}s.$$

Computer algebra now gives

$$J = \frac{C}{3}+\frac{\pi}{4}\log\frac{9}{8}, \tag{4.29}$$

where C denotes Catalan's constant. Adding (4.25)-(4.29) gives (4.20). □

In the proof of Proposition 4.3 the expression (4.24) corresponds to integrating (4.18) over $t_{12}^{(r)}$ and $t_{12}^{(i)}$, and thus after normalisation by dividing by (4.20) and removal of $\mathrm{d}t$ corresponds to the PDF of the length of the shortest basis vector.

Proposition 4.4. *For random complex lattices in $\mathbb{C}^2$, the probability density function for the length of the shortest basis vector is equal to*

$$\frac{3}{C}\Big\{\chi_{0<t<1}t^3+\chi_{1<t<(4/3)^{1/4}}t(t^2-\pi(t^2-1/t^2))$$
$$+\chi_{(4/3)^{1/4}<t<2^{1/4}}\Big(t^3-t^3\sqrt{3-4/t^4}+\pi(t^3-1/t)$$
$$-4(t^3-1/t)\arcsin\frac{t}{2(t^2-1/t^2)^{1/2}}\Big)\Big\}. \tag{4.30}$$

As noted in the second paragraph of this chapter, the length of the second shortest basis vector is given by $r = (y_1^2 + y_2^2 + 1/t^2)^{1/2}$, with y_1, y_2, t as specified above (4.21). Changing variables from t to r and imposing the ordering and sign restriction $t/2 > y_2 > y_1 > 0$ the functional form in (4.18) transforms to

$$\frac{8r}{(r^2 - y_1^2 - y_2^2)^2} \chi_{y_1^2+y_2^2<r^2-1/r^2} \chi_{r^2<y_1^2+y_2^2+1/4y_1^2} \chi_{0<y_1<y_2}. \tag{4.31}$$

Integrating over y_1 and y_2 and normalisation by (4.20) gives the explicit form of the corresponding PDF.

Proposition 4.5. *In the setting of Propositions 4.3 and 4.4, the PDF for the length of the second shortest basis vector is equal to*

$$\begin{aligned}\frac{3}{C}\Bigg\{ & \chi_{1<r<(4/3)^{1/4}\pi} \frac{r^4-1}{r} + \chi_{(4/3)^{1/4}<r<2^{1/4}} \\ & \times \left(\frac{r}{4}\sqrt{3r^4-4} + \frac{r^4-1}{2r}\left(\arctan \frac{r^2}{\sqrt{3r^4-4}} + \arctan \frac{r^2\sqrt{3r^4-4} - 2r^4 + 2}{r^4-2} - \frac{\pi}{2} \right) \right) \\ & + \chi_{r>2^{1/4}} \left(\frac{r}{4}(r^2 - \sqrt{r^4-2}) + \frac{r^4-1}{2r}\left(\arctan \frac{r^2+\sqrt{r^4-2}}{r^2-\sqrt{r^4-2}} - \frac{\pi}{2} \right) \right) \Bigg\}. \end{aligned} \tag{4.32}$$

Proof. Regarding $r > 1$ as a parameter, there are three ranges of r values giving a distinctly shaped region as defined by the three inequalities in (4.31), see Figure 4.1.

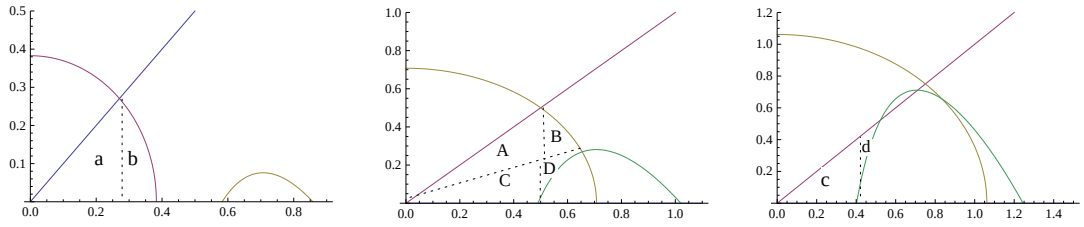

FIGURE 4.1

The latter can then be divided into subregions which allow for explicit parametrisation of the ranges of integration. Thus for $1 < r < (4/3)^{1/4}$,

$$a = \int_0^{\sqrt{(r^2-r^{-2})/2}} \mathrm{d}y_1 \int_0^{y_1} \mathrm{d}y_2\,, \quad b = \int_{\sqrt{(r^2-r^{-2})/2}}^{\sqrt{r^2-r^{-2}}} \mathrm{d}y_1 \int_0^{\sqrt{r^2-r^{-2}-y_1^2}} \mathrm{d}y_2\,;$$

or $(4/3)^{1/4} < r < 2^{1/4}$,

$$A = \int_0^{\sqrt{(r^2-r^{-2})/2}} \mathrm{d}y_1 \int_{(y_1/r^2)\sqrt{3r^4-4}}^{y_1} \mathrm{d}y_2\,, \quad B = \int_{\sqrt{(r^2-r^{-2})/2}}^{r/2} \mathrm{d}y_1 \int_{(y_1/r^2)\sqrt{3r^4-4}}^{\sqrt{r^2-r^{-2}-y_1^2}} \mathrm{d}y_2$$

$$C = \int_0^{\sqrt{(r^2-\sqrt{r^4-1})/2}} \mathrm{d}y_1 \int_0^{(y_1/r^2)\sqrt{3r^4-4}} \mathrm{d}y_2\,, \quad D = \int_{\sqrt{(r^2-r^{-2})/2}}^{r/2} \mathrm{d}y_1 \int_{\sqrt{r^2-y_1^2-1/(4y_1^2)}}^{(y_1/r^2)\sqrt{3r^4-4}} \mathrm{d}y_2\,;$$

and for $r > 2^{1/4}$

$$c = \int_0^{\sqrt{(r^2-\sqrt{r^4-1})/2}} \mathrm{d}y_1 \int_0^{y_1} \mathrm{d}y_2\,, \quad d = \int_{\sqrt{(r^2-\sqrt{r^4-1})/4}}^{\sqrt{(r^2-\sqrt{r^4-1})/2}} \mathrm{d}y_1 \int_{\sqrt{r^2-y_1^2-1/(4y_1^2)}}^{y_1} \mathrm{d}y_2.$$

To compute the PDF of the second shortest basis vector, each of these integrations should be extended to include the function $1/(r^2 - y_1^2 - y_2^2)^2$ for their integrand, as required by (4.31). The resulting integrals can all be computed explicitly. Multiplying the result by $8r$ as also required by (4.31), and normalising by (4.20) we obtain (4.32). □

Remark 4.6. *Expanding (4.32) for large r one obtains*

$$\frac{3}{C}\Big(\frac{1}{r^5} + \frac{2}{3r^9} + \mathrm{O}\Big(\frac{1}{r^{13}}\Big)\Big).$$

In the variable $s = 1/r$, the leading term for the expansion as $s \to 0$ is thus $3s^3/C$. This coincides with the small t behaviour of the PDF for the shortest vector (4.30), and in particular has the same functional dependence on the arithmetic constant C.

The final quantity to be considered is the complex analogue of the cosine of the angle between the shortest reduced basis vectors (4.19). We write

$$\xi_R = \frac{t_{12}^{(r)}}{\sqrt{(t_{12}^{(r)})^2 + (t_{12}^{(i)})^2 + 1/t_{11}^2}}, \quad \xi_I = \frac{t_{12}^{(i)}}{\sqrt{(t_{12}^{(r)})^2 + (t_{12}^{(i)})^2 + 1/t_{11}^2}}. \tag{4.33}$$

Their joint distribution can be calculated according to the following result.

Proposition 4.7. *The variables ξ_R, ξ_I specified by (4.33) have joint distribution with PDF equal to*

$$-\frac{3}{C}\frac{\log 4 \max(|\xi_R|^2, |\xi_I|^2)}{4(1-\xi_R^2-\xi_I^2)^2} \tag{4.34}$$

supported on

$$\max(|\xi_R|^2, |\xi_I|^2) \leq 1/4. \tag{4.35}$$

Proof. It follows from (4.33) that

$$t_{12}^{(r)} = \frac{\xi_R}{t_{11}\sqrt{1-\xi_R^2-\xi_I^2}}, \quad t_{12}^{(i)} = \frac{\xi_I}{t_{11}\sqrt{1-\xi_R^2-\xi_I^2}}.$$

The Jacobian for the change of variables from $(t_{12}^{(r)}, t_{12}^{(i)})$ to (ξ_R, ξ_I) is thus

$$\left| \det \begin{bmatrix} \frac{\partial t_{12}^{(\mathrm{r})}}{\partial \xi_R} & \frac{\partial t_{12}^{(\mathrm{r})}}{\partial \xi_I} \\ \frac{\partial t_{12}^{(\mathrm{i})}}{\partial \xi_R} & \frac{\partial t_{12}^{(\mathrm{i})}}{\partial \xi_I} \end{bmatrix} \right| = \frac{1}{t_{11}^2(1-\xi_R^2-\xi_I^2)^2}.$$

Hence the functional form in (4.18) transforms to

$$\frac{1}{t_{11}(1-\xi_R^2-\xi_I^2)^2} \chi_{t_{11}^4 < \frac{1}{1-\xi_R^2-\xi_I^2}} \chi_{t_{11}^4 > \frac{4\xi_I^2}{1-\xi_R^2-\xi_I^2}} \chi_{t_{11}^4 > \frac{4\xi_R^2}{1-\xi_R^2-\xi_I^2}}.$$

Integration over t_{11} in this expression is elementary, and after dividing by the normalisation (4.20) the PDF (4.34) results. □

Corollary 4.8. *Let $\xi_R = \xi\cos\theta$, $\xi_I = \xi\sin\theta$, $\xi > 0$, $0 < \theta < 2\pi$ so that $\xi = (\xi_R^2+\xi_I^2)^{1/2}$. The PDF of ξ is equal to*

$$-\frac{6\xi}{C(1-\xi^2)^2}\left(\chi_{0<\xi<1/2}\left(\frac{\pi}{2}\log\xi + C\right) + \chi_{1/2<\xi<1/\sqrt{2}}\int_{\arccos(1/2\xi)}^{\pi/4}\log(4\xi^2\cos^2\theta)\mathrm{d}\theta\right). \tag{4.36}$$

Proof. The Jacobian for the change of variable to polar coordinates is $\mathrm{d}\xi_R\mathrm{d}\xi_I = \xi\mathrm{d}\xi\mathrm{d}\theta$. For $0 < \xi < 1/2$, the inequality (4.35) is valid for all $0 < \theta < 2\pi$, and the integral over θ in (4.34) is equal to

$$-\frac{3\xi}{4C(1-\xi^2)^2}8\int_0^{\pi/4}\log(2\xi^2\cos^2\theta)\mathrm{d}\theta$$

which evaluates to the first case in (4.36). For $1/2 < \xi < 1/\sqrt{2}$, and restricting θ to the range $0 < \theta < \pi/4$, the inequality (4.35) is valid for $\arccos(1/2\xi) < \theta < \pi/4$, and this implies the second case in (4.36). □

Statistics of the shortest reduced basis for the Hurwitz integers

As for the real and complex cases, a convenient parametrisation of the shortest basis is obtained by using the Gram–Schmidt basis. Thus one decomposes $\mathbf{V} = \mathbf{UT}$ where $\mathbf{U} \in \mathrm{SL}_2(\mathbb{H})$ and

$$\mathbf{T} = \begin{bmatrix} t_{11} & \sum_{s=1}^{3} e_\nu t_{12}^\nu \\ 0 & t_{22} \end{bmatrix}, \qquad t_{11} > 0, \quad t_{22} = 1/t_{11}.$$

Since in the Gram–Schmidt basis

$$\boldsymbol{\alpha} = (t_{11}, 0), \qquad \boldsymbol{\beta} = \Big(\sum_{\nu=0}^{3} e_\nu t_{12}^\nu, 1/t_{11} \Big),$$

the conditions (3.32) characterising the shortest basis give

$$t_{11}^2 - 1/t_{11}^2 \leq \sum_{s=0}^{3} (t_{12}^\nu)^2, \qquad D_H\Big(\sum_{\nu=0}^{3} e_\nu t_{12}^\nu / t_{11} \Big) = 0.$$

Also, the Jacobian associated with the Gram–Schmidt basis is $t_{11}^6 t_{22}^2$ (see e.g. [12, Ex. 3.2 q.5(i)]). Thus for $\mathbb{F} = \mathbb{H}$ the (normalised) invariant measure (4.5) in the variables $\{t_{11}, t_{22}, \{t_{12}^\nu\}_{\nu=0}^3\}$ after integrating out over t_{22} reads

$$\frac{1}{\operatorname{vol} \Gamma_2^{(4)}} \chi_{t_{11}^2 - 1/t_{11}^2 \leq \sum_{\nu=0}^{3} (t_{12}^\nu)^2} \chi_{D_H\left(\sum_{\nu=0}^{3} e_\nu t_{12}^\nu / t_{11}\right) = 0} t_{11}^3 dt_{11} \prod_{\nu=0}^{3} dt_{12}^\nu, \tag{4.37}$$

where $\operatorname{vol} \Gamma_2^{(4)}$ is the normalisation.

The functional form of the PDF for the length t of the shortest basis vector can be read off from (4.37) in the region $t < 1$.

Proposition 4.9. *Let* $\operatorname{vol} \Gamma_2^{(4)}$ *be as in (4.37). For* $0 < t < 1$ *the PDF for the length of the shortest basis vector is equal to*

$$\frac{1}{\operatorname{vol} \Gamma_2^{(4)}} \frac{t^7}{2}. \tag{4.38}$$

Proof. Rewrite (4.37) as

$$\frac{1}{\operatorname{vol}\Gamma_2^{(4)}}\chi_{1-1/t_{11}^4\le\sum_{s=0}^3 y_\nu^2}\chi_{D_H\left(\sum_{\nu=0}^3 e_\nu y_\nu\right)=0}t_{11}^7 dt_{11}\prod_{\nu=0}^3 dy_\nu, \tag{4.39}$$

with $y_\nu = t_{12}^\nu/t_{11}$. With $t = t_{11}$, for $0 < t < 1$ the first of the two constraints in (4.39) — and the only one involving t, is always valid. Noting that

$$\int \chi_{D_H(\sum_{\nu=0}^3 e_\nu y_\nu)=0}\prod_{\nu=0}^3 dy_\nu = \operatorname{vol} V, \tag{4.40}$$

where V denotes the Voronoi cell, then noting that $\operatorname{vol} V$ is equal to the volume of a fundamental cell for the lattice in $\mathbb{R}^4$ corresponding to the Hurwitz integers, the task is to calculate this latter volume. Since the lattice corresponding to the Hurwtiz integers can be generated by

$$\begin{bmatrix} 1/2 & 0 & 0 & 0 \\ 1/2 & 1 & 0 & 0 \\ 1/2 & 0 & 1 & 0 \\ 1/2 & 0 & 0 & 1 \end{bmatrix}$$

we conclude $\operatorname{vol} V = 1/2$, and (4.38) follows. □

From the definition of the Hurwitz integers and the quantizer D_H, the constraint $D_H(\sum_{\nu=0}^3 e_\nu t_{12}^\nu/t_{11}) = 0$ can be characterised by the inequalities

$$|t_{12}^\nu| < \frac{1}{2}t_{11} \quad (\nu = 0,\dots,3) \quad \text{and} \quad \sum_{\nu=0}^3 |t_{12}^\nu| < t_{11}. \tag{4.41}$$

We have not succeeded in extending the method of the proof of Propositions 4.1 and 4.3 for a direct calculation of

$$\operatorname{vol}\Gamma_{4,H} = \int \chi_{t_{11}^2-1/t_{11}^2\le\sum_{\nu=0}^3 (t_{12}^\nu)^2}\Big(\prod_{\nu=0}^3 \chi_{|t_{12}^\nu|\le t_{11}/2}\Big)\chi_{\sum_{\nu=0}^3|t_{12}^\nu|\le t_{11}} t_{11}^3 dt_{11}\prod_{\nu=0}^3 dt_{12}^\nu, \tag{4.42}$$

where in obtaining this integral we have used the fact $\operatorname{vol}\Gamma_{4,H}$ is the normalisation in (4.37). But we can deduce its value, as we now proceed to demonstrate.

First, we obtain a numerical estimate. A simple change of variables, and use of the fact that (4.42) is even in each t_{12}^{ν} allows (4.42) to be rewritten

$$\operatorname{vol}\Gamma_{4,H} = 4\int \chi_{2>u>0}\chi_{u^{1/2}-u^{-1/2}\leq\sum_{\nu=0}^{3}x_\nu^2} \times\Big(\prod_{\nu=0}^{3}\chi_{2^{1/4}/2>x_\nu>0}\chi_{x_\nu\leq u^{1/4}/2}\Big)\chi_{\sum_{\nu=0}^{3}x_\nu\leq u^{1/4}}du\prod_{\nu=0}^{3}dx_\nu. \tag{4.43}$$

This is well suited to estimation by a Monte Carlo rejection method, which with 10^6 trials gives the estimate 0.105.

In [13, Remark 4.5] it was noted that the PDF for the length of the shortest lattice vector in the real case, which for $0 < s < 1$ was found to equal $6s/\pi$, is consistent with a corollary of Siegel's mean value theorem [32] requiring that the expected number of vectors in a disk of radius R be equal to the area of the disk. Siegel's mean value theorem in [32] applies to the case of real lattices, so to find out the exact value of $\operatorname{vol}\Gamma_2^{(4)}$ using similar method, we first make note of a general statement of the mean value theorem, but without proof.

Theorem 4.10 (Siegel). *$\mathrm{d}\mu_N(\mathcal{L}^{(\beta)})$ denotes the invariant measure of a $\mathbb{F}$-valued lattice $\mathcal{L}^{(\beta)}$ with dimension N and index β. Let $\rho(x):\mathbb{F}^N\to\mathbb{F}$ be a compactly supported and bounded Borel measurable function. Then*

$$\int\sum_{x\in\mathcal{L}^{(\beta)}-\{0\}}\rho(x)\mathrm{d}\mu_N(\mathcal{L}^{(\beta)}) = \int_{\mathbb{R}^{\beta N}}K\rho(x)dx \tag{4.44}$$

where K is a scale factor equal to the dilation implied by the natural embedding of the integers.

Proposition 4.11. *We have*

$$\operatorname{vol}\Gamma_2^{(4)} = \frac{7\zeta(3)}{80}\approx 0.1051799... \tag{4.45}$$

Proof. A similar argument as [13, Remark 4.5] can be given in the quaternion case. Taking $\rho(x)=\chi_{\|x\|\leq R}$ gives

$$\sum_{x\in\mathcal{L}^{(4)}-\{0\}} = \#\left\{x\in\mathcal{L}^{(4)}-\{0\}:\|x\|\leq R\right\}.$$

Consider a 2-dimensional quaternion lattice with shortest basis $\{\mathbf{b}_1,\mathbf{b}_2\}$ ($\|\mathbf{b}_1\|\leq\|\mathbf{b}_2\|$). By restricting $R\leq 1$, only multiples of $\mathbf{b}_1$ appear inside the circle with

radius R. Denote $N(x)$ the number of nonzero Hurwitz integers with length less than or equal to x, then the LHS of Siegel's mean value theorem is

$$\begin{aligned}\text{LHS} &= \int \#\left\{q\mathbf{b}_1 \in \mathcal{L}^{(4)} - \{0\} : \|q\mathbf{b}_1\| \leq R\right\} \mathrm{d}\mu_N(\mathcal{L}^{(4)}) \\ &= \int \#\left\{q \in H - \{0\} : \|q\| \leq R/\|\mathbf{b}_1\|\right\} \mathrm{d}\mu_N(\mathcal{L}^{(4)}) \\ &= \frac{1}{2\mathrm{vol}\,\Gamma_2^{(4)}} \int_0^R N(R/s)s^7 \mathrm{d}s = \frac{R^8}{2\mathrm{vol}\,\Gamma_2^{(4)}} \int_1^\infty \frac{N(t)}{t^9}\mathrm{d}t\end{aligned}$$

where we substitute (4.38) and make a change of variable $t = R/s$. Furthermore let $M(x)$ be the number of Hurwitz integers with length exactly being x. There exists an ordered sequence $0 < t_1 < t_2 < ...$ such that $\forall\, p$, $M(t_p) \neq 0$ and $\forall\, x \neq t_p$, $M(x) = 0$. Notice that $M(t_p) = N(t_p) - N(t_{p-1})$ and $t_1 = 1$. We make a partition of $[1, \infty)$ using such a sequence and

$$\begin{aligned}\text{LHS} &= \frac{R^8}{2\mathrm{vol}\,\Gamma_2^{(4)}} \sum_{p=1}^{\infty} \int_{t_p}^{t_{p+1}} \frac{N(t)\mathrm{d}t}{t^9} = \frac{R^8}{16\mathrm{vol}\,\Gamma_2^{(4)}} \sum_{p=1}^{\infty} N(t_p)\left(\frac{1}{t_p^8} - \frac{1}{t_{p+1}^8}\right) \\ &= \frac{R^8}{16\mathrm{vol}\,\Gamma_2^{(4)}} \sum_{p=1}^{\infty} \frac{M(t_p)}{t_p^8} = \frac{R^8}{16\mathrm{vol}\,\Gamma_2^{(4)}} \sum_{q\in H-\{0\}} \frac{1}{|q|^8}\end{aligned}$$

From [40],

$$\sum_{q\in H-\{0\}} \frac{1}{|q|^8} = T(0,4) + S(0,4) = 21\zeta(3)\zeta(4).$$

Evaluating t he RHS of (4.44) gives $\pi^4 K R^8/24$. Equating them gives (4.45) with $K = 4$, coming from the fact that Hurwitz integers have unit cell of area $\frac{1}{2}$. □

Remark 4.12. *Weil [38] gives a generalisation of Siegel's mean value theorem, and in particular allows the case of a complex lattice to be considered. Again by taking the same $\rho(x)$ and $R < 1$, together with Proposition 4.4 one can write that*

$$LHS = \frac{3R^4}{C} \int_1^\infty \frac{N'(t)}{t^5}\mathrm{d}t$$

where $N'(t)$ denotes the number of nonzero Gaussian integers with length less than or equal to x. Let $M'(x)$ be the number of Gaussian inters with length exactly being x,

and similar sequence $0 < t'_1 < t'_2 < \ldots$ can be constructed. It follows that

$$LHS = \frac{3R^4}{4C} \sum_{p=1}^{\infty} \frac{M'(p)}{t'^4_p} = \frac{3R^4}{4C} \sum_{z \in \mathbb{Z}[i]-\{0\}} \frac{1}{|z|^4}. \tag{4.46}$$

From [40] we have

$$\sum_{z \in \mathbb{Z}[i]-\{0\}} \frac{1}{|z|^4} = 4\zeta_{\mathbb{Z}[i]}(2) = 4\frac{\pi^2}{6}C.$$

which substituted in (4.46) shows LHS $= \frac{\pi^2}{2}R^4 = RHS$,. This agrees with the RHS *of (4.44), which equals the volume of a 4-dimensional ball, multiplied by factor $K = 1$.*

Proposition 4.13. *For $s \to \infty$, the asymptotic behaviour of the PDF for the length of the second shortest basis vector is*

$$\frac{1}{2\mathrm{vol}\,\Gamma_2^{(4)}} \frac{1}{s^9}.$$

Proof. In (4.37), with the quantiser rewritten according to (4.41) and $\mathbf{X} = (X_0, \ldots, X_3) = (t^0_{12}, \ldots, t^3_{12})$, we change variables from t_{11} to $s = (\mathbf{X}^2 + 1/t^2_{11})^{1/2}$ — the length of the second shortest basis vector — to deduce that the PDF of the latter is

$$\frac{1}{\mathrm{vol}\,\Gamma_2^{(4)}} \int \chi_{|\mathbf{X}|^2 \le s^2 - 1/s^2} \Big(\prod_{\nu=0}^{3} \chi_{|\mathbf{X}|^2 + 1/4X_\nu^2 \ge s^2} \Big) \chi_{|\mathbf{X}|^2 + 1/(\sum_{\nu=0}^{3} |X_\nu|)^2 \ge s^2} \frac{s}{(s^2 - |\mathbf{X}|^2)^3} \prod_{\nu=0}^{3} dX_\nu. \tag{4.47}$$

Denote

$$\Gamma_1 = \chi_{|\mathbf{X}|^2 \le s^2 - 1/s^2}, \quad \Gamma_2 = \prod_{\nu=0}^{3} \chi_{|\mathbf{X}|^2 + 1/4X_\nu^2 \ge s^2}, \quad \Gamma_3 = \chi_{|\mathbf{X}|^2 + 1/(\sum_{\nu=0}^{3} |X_\nu|)^2 \ge s^2},$$

and for $\mu = 1, 2$ let

$$D_\mu = \prod_{\alpha=0}^{3} \chi_{|X_\nu|^2 \le (s^2 - \sqrt{s^4-1})/2^{2\mu-1}}, \quad R_\mu = \chi_{(\sum_{\alpha=0}^{3} |X_\nu|)^2 \le 4(s^2 - \sqrt{s^4-1})/2^{2\mu-1}}.$$

We can check that as $s \to \infty$

$$\Gamma_1 \subseteq \Gamma_2, \qquad D_1 \subseteq \Gamma_2 \subseteq D_2, \qquad R_1 \subseteq \Gamma_3 \subseteq R_2.$$

Also, as $s \to \infty$

$$D_1, D_2 \to \prod_{\nu=0}^{3} \chi_{1/(2s)+\mathrm{O}(1/s^5)\geq|X_\nu|}, \qquad R_1, R_2 \to \chi_{1/s+\mathrm{O}(1/s^5)\geq\sum_{\nu=0}^{3}|X_\nu|},$$

so for large s it follows from the above working that the PDF (4.47) has the leading asymptotic form

$$\frac{1}{\mathrm{vol}\,\Gamma_2^{(4)}}\frac{1}{s^5}\int\prod_{\nu=0}^{3}\chi_{|X_\nu|\leq 1/2s}\,\chi_{\sum_{\nu=0}^{3}|X_\nu|\leq 1/s}\prod_{\nu=0}^{3}dX_\nu.$$

Scaling s from the integral, then recognising what remains as (4.40) simplifies this to

$$\frac{1}{2\mathrm{vol}\,\Gamma_2^{(4)}}\frac{1}{s^9}.$$

□

Remark 4.14. *Together with Remark 4.2 and Remark 4.6, one notices that by using a change of variable $s \mapsto 1/s$ the asymptotic behaviour of the second shortest vector is the same as the short behaviour of the shortest vector. To see this one rewrites the part of (4.11), (4.31) and (4.38) from 0 to 1 consistently as $A_\beta x^{2\beta-1}$. Denote the reduced basis $\{\mathbf{b}_1, \mathbf{b}_2\}$ with $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$ and then for $0 < s < 1$,*

$$\mathbb{P}\{\|\mathbf{b}_1\| < s\} = \frac{A_\beta}{2\beta}s^{2\beta}. \tag{4.48}$$

Now consider the height of the parallelogram formed by the basis, which is not bigger than $\|\mathbf{b}_2\|$, the hypotenuse:

$$\|\mathbf{b}_2\| \geq \left\|\mathbf{b}_2 - \frac{\mathbf{b}_1^\dagger\mathbf{b}_2}{\|\mathbf{b}_1\|^2}\mathbf{b}_1\right\|,$$

according to which the inequality

$$\mathbb{P}\{\|\mathbf{b}_2\| > 1/s\} \geq \mathbb{P}\left\{\left\|\mathbf{b}_2 - \frac{\mathbf{b}_1^\dagger\mathbf{b}_2}{\|\mathbf{b}_1\|^2}\mathbf{b}_1\right\| > 1/s\right\} = \mathbb{P}\{\|\mathbf{b}_1\| < s\} \tag{4.49}$$

holds where the last step is due to the fact that the lattice is unimodular and the volume of the parallelogram is 1. The restrictions $\prod_{\nu=0}^{3}\chi_{|t_{12}^\nu|<t_{11}/2}$ implies when $\|\mathbf{b}_2\| > 1/s$,

the height takes its minimum when $|t_{12}^{\nu}| = t_{11}/2$ *for all* ν*, which gives*

$$\mathbb{P}\{\|\mathbf{b}_2\| > 1/s\} \leq \mathbb{P}\left\{\left\|\mathbf{b}_2 - \frac{\mathbf{b}_1^{\dagger}\mathbf{b}_2}{\|\mathbf{b}_1\|^2}\mathbf{b}_1\right\| > \sqrt{\frac{1}{s^2} - \left(\frac{\beta s}{2}\right)^2}\right\}. \tag{4.50}$$

Substituting (4.48) *into* (4.49) *and* (4.50) *and taking* $s \to 0$ *gives*

$$\mathbb{P}\{\|\mathbf{b}_2\| > 1/s\} \to \frac{A_\beta}{2\beta} s^{2\beta}. \tag{4.51}$$

In the quaternion case the analogue of the variables (4.33) are the four variables

$$\xi_\nu = \frac{t_{12}^{\nu}}{\sqrt{\sum_{\nu=0}^{3}(t_{12}^{\nu})^2 + 1/t_{11}^2}} \qquad \nu = 0, \ldots, 3.$$

Proposition 4.15. *The variables* ξ_ν*,* $\nu = 0, 1, 2, 3$ *specified above have joint distribution with PDF equal to*

$$-\frac{1}{\operatorname{vol}\Gamma_2^{(4)}} \cdot \frac{\log \max(\max_\nu(4|\xi_\nu|^2), (\sum_{\nu=0}^{3}|\xi_\nu|)^2)}{4(1-\sum_{\nu=0}^{3}\xi_\nu^2)^3} \tag{4.52}$$

supported on $\max(\max_\nu(4|\xi_\nu|^2), (\sum_{\nu=0}^{3}|\xi_\nu|)^2) \leq 1$.

Proof. Similarly to Proposition 4.7, it follows from (4.33) that

$$t_{12}^{(\nu)} = \frac{\xi_\nu}{t_{11}\sqrt{1-\sum_{\nu=0}^{3}\xi_\nu^2}}, \quad \nu = 0, 1, 2, 3$$

The Jacobian for the change of variables from $(t_{12}^{(0)}, t_{12}^{(1)}, t_{12}^{(2)}, t_{12}^{(3)})$ to $(\xi_0, \xi_1, \xi_2, \xi_3)$ is thus

$$\left|\det \frac{\partial(t_{12}^{(0)}, t_{12}^{(1)}, t_{12}^{(2)}, t_{12}^{(3)})}{\partial(\xi_0, \xi_1, \xi_2, \xi_3)}\right| = \frac{1}{t_{11}^4(1-\sum_{\nu=0}^{3}\xi_\nu^2)^3}.$$

The functional form in (4.18) thus transforms to

$$\frac{1}{t_{11}(1-\sum_{\nu=0}^{3}\xi_\nu^2)^3}\chi_{t_{11}^4 < \frac{1}{1-\sum_{\nu=0}^{3}\xi_\nu^2}}\left(\prod_{\nu=0}^{3}\chi_{t_{11}^4 > \frac{4\xi_\nu^2}{1-\sum_{\nu=0}^{3}\xi_\nu^2}}\right)\chi_{t_{11}^4 > \frac{(\sum_{\nu=0}^{3}|\xi_\nu|)^2}{1-\sum_{\nu=0}^{3}\xi_\nu^2}}.$$

Integration over t_{11} in this expression and the PDF (4.52) results. □

Chapter 5

Numerical computations

Sampling random lattices

For practical purposes, sampling random lattices directly is itself a big challenge, but as mentioned in Chapter 4, it can be achieved by "sampling" $\mathrm{SL}_N(\mathbb{F})$ first and then applying lattice reduction algorithms. As sampling $\mathrm{SL}_N(\mathbb{F})$, a infinite domain, is impossible, sampling an approximation of $\mathrm{SL}_N(\mathbb{F})$ with finite domain may be a solution. A truncated set is suggested by Macbeath and Rogers [21] using the matrix operator norm:

$$D_R^{\|\cdot\|_{\mathrm{op}}}(\mathrm{SL}_N(\mathbb{F})) = \{\mathbf{G} \in \mathrm{SL}_N(\mathbb{F}) \,:\, R > \sigma_1\} \tag{5.1}$$

where σ_1 is the biggest singular value of $\mathbf{G}$. In the sense of sampling uniformly distributed random lattices, we find it works well as the sampled random lattices give convergence in probability as R goes to infinity.

Lemma 5.1. *Let* $\mathbf{X}$ *be a* $N \times N$ *Hermitian matrix and* $\lambda_{\max}$ *be its largest eigenvalue. Then for all complex vector* $\mathbf{u}$ *with length 1,*

$$\lambda_{\max} \geq \mathbf{u}^\dagger \mathbf{X} \mathbf{u}$$

Proof. Spectral decomposition gives $\mathbf{X} = \mathbf{Q}^\dagger \mathbf{D} \mathbf{Q}$ and let $\mathbf{v} = \mathbf{Q}\mathbf{u}$. Then

$$\begin{aligned}\mathbf{u}^\dagger \mathbf{X} \mathbf{u} = \mathbf{v}^\dagger \mathbf{D} \mathbf{v} &= \lambda_{\max} v_1^2 + \lambda_2 v_2^2 + \ldots + \lambda_N v_N^2 \\ &\leq \lambda_{\max}(v_1^2 + v_2^2 + \ldots + v_N^2) = \lambda_{\max} \mathbf{v}^\dagger \mathbf{v} = \lambda_{\max} (\mathbf{u}\mathbf{Q})^\dagger \mathbf{Q}\mathbf{u} = \lambda_{\max}\end{aligned}$$

as $\mathbf{Q}^\dagger \mathbf{Q} = \mathbf{I}$ and $\mathbf{u}^\dagger \mathbf{u} = \|\mathbf{u}\| = 1$. □

Proposition 5.2. *Define $\|\cdot\|_{\mathrm{L}}$ to be a norm of $N \times N$ complex matrices giving the length of its longest column vector, then for any such matrix $\mathbf{A}$, $\|\mathbf{A}\|_{\mathrm{op}} \geq \|\mathbf{A}\|_{\mathrm{L}}$.*

Proof. Let $\mathbf{A} = [\mathbf{a}_1, ..., \mathbf{a}_N]$ and without loss of generality, suppose $\mathbf{a}_1$ is the longest column vector, then

$$\mathbf{A}^\dagger \mathbf{A} = \left[\mathbf{a}_i^\dagger \mathbf{a}_j\right]_{i,j=1}^{N}.$$

Furthermore, let $\mathbf{u} = [1, 0, ..., 0]^\dagger$ and applying Lemma 5.1 gives

$$\|\mathbf{A}\|_{\mathrm{op}}^2 = \lambda_{\max} \geq \mathbf{a}_1^\dagger \mathbf{a}_1 = \|\mathbf{A}\|_{\mathrm{L}}^2$$

which finishes the proof. □

Remark 5.3. *For quaternion matrices, there are (at least) 2 columns has the largest length, and 2 largest singular values for $\mathbf{A}^\dagger\mathbf{A}$. Proposition 4.2 still holds although there is at least 2 choices of the longest $\mathbf{a}_i$.*

Proposition 5.4. *Let $\|\cdot\|$ be a matrix norm such that for any matrix $\mathbf{A}$, $\|\mathbf{A}\| \geq k\|\mathbf{A}\|_{\mathrm{L}}$, where $\|\cdot\|_L$ is defined in Proposition 5.2 and k is a positive constant. Then the volume*

$$\mathrm{vol}\left\{\mathbf{B} \in \Gamma_N^{(\beta)} : \|\mathbf{BM}\| > R,\ \forall \mathbf{M} \in \mathrm{SL}_N(\mathbb{Z}^{(\beta)})\right\} \to 0$$

as $R \to \infty$, where $\Gamma_N^{(\beta)}$ denotes the fundamental domain, i.e. lattice subgroup of $SL_N(\mathbb{F})$.

Proof. It is sufficient to show that

$$\mathrm{vol}\left\{\mathbf{B} \in \Gamma_N^{(\beta)} : \|\mathbf{BM}\|_L > R',\ \forall \mathbf{M} \in \mathrm{SL}_N(\mathbb{Z}^{(\beta)})\right\} \to 0,$$

where $R'k = R$. One notices that among all basis $\mathbf{BM}$ of a lattice, the shortest "longest basis vector" is the longest basis vector in the minimal basis $\mathbf{B}$. Therefore it is sufficient to show

$$\mathrm{vol}\left\{\mathbf{B} \in \Gamma_N^{(\beta)} : \|\mathbf{B}\|_L > R'\right\} \to 0 \tag{5.2}$$

which is the probability that the length of the second shortest vector is bigger than R' goes to 0. This is always true regardless of the choice of the probability density function if it exists. □

Remark 5.5. *Together with proposition 4.2 if we let the norm be* $\|\cdot\|_{\mathrm{op}}$*, it tells us* $\mathcal{F}\left(D_R^{\|\cdot\|_{op}}\mathrm{SL}_N(\mathbb{F})\right)$*, where* $\mathcal{F}$ *denotes the reduction algorithm, converges to* $\Gamma^{(\beta)}$ *in probability corresponding to the uniform invariant measure. This gives us confidence in sampling* $\mathrm{SL}_N(\mathbb{F})$ *using truncated set such as* $D_R^{\|\cdot\|_{\mathrm{op}}}\mathrm{SL}_N(\mathbb{F})$*, which asymptotically preserves the uniform distribution of random lattices.*

Remark 5.6. *Recall (4.51), which gives us a prescription of (5.2) in* $N = 2$*, enabling us to choose the truncation* R *with the error under control by* $O(R^{-2\beta})$*.*

Remark 5.7. *Notice that the Schatten* p*-norm* $\|\cdot\|_p$*, defined as*

$$\|\mathbf{M}\|_p = \left(\sum_{i=1}^{N}\sigma_i^p(\mathbf{M})\right)^{1/p}$$

where $\sigma_i(\mathbf{M})$ *denotes its* i*-th singular value, is equivalent to* $\|\cdot\|_{\mathrm{op}}$*, that is, there exists positive* C_1 *and* C_2 *such that for all matrices* $\mathbf{M} \in \mathrm{SL}_N(\mathbb{F})$*,*

$$C_1\|\mathbf{M}\|_{\mathrm{op}} \geq \|\mathbf{M}\|_p \geq C_2\|\mathbf{M}\|_{\mathrm{op}}.$$

In fact C_1 *can be chosen to be* $N^{1/p}$ *and* C_2 *be 1. Hence they all satisfy the property* $\|\mathbf{M}\|_p \geq C\|\mathbf{M}\|_L$ *for some positive constant* C*, and therefore truncated set can be replaced by* $D_R^{\|\cdot\|_p}(\mathrm{SL}_N(\mathbb{F}))$*. A typical example is a ball of radius* R *with respect to the Frobenius norm (p=2), suggested by [10].*

Uniform sampling from $\mathrm{SL}_2(\mathbb{F})$

In preparation for sampling $\mathrm{SL}_2(\mathbb{F})$, as done in the pioneering work of Jack and Macbeath [18] in the case $\mathbb{F} = \mathbb{R}$, we make use of a singular value decomposition

$$\mathbf{G} = \mathbf{U}^{(\beta)}\mathrm{diag}(\sigma_1, \sigma_2)\mathbf{V}^{(\beta)}, \tag{5.3}$$

where $\mathbf{U}^{(\beta)}, \mathbf{V}^{(\beta)} \in \mathrm{U}_2(\mathbb{F})$ – the set of 2×2 unitary matrices with entries in $\mathbb{F}$. In the case $\beta = 4$ each entry in the diagonal matrix is repeated twice, becoming a 4×4 matrix $\mathrm{diag}(\sigma_1, \sigma_1, \sigma_2, \sigma_2)$. For (5.3) to be one-to-one it is required that the singular values be ordered

$$\sigma_1 \geq \sigma_2 > 0$$

and that the entries in the first row of $V^{(\beta)}$ be real and positive.

Changing variables according to (5.3) gives (see e.g. [7, Prop. 2])

$$(\mathrm{d}\mathbf{G}) = \left(\frac{2\pi^{\beta/2}}{\Gamma(\beta/2)}\right)^{-2} \left(\mathbf{U}^{(\beta)\dagger}\mathrm{d}\mathbf{U}^{(\beta)}\right) \left(\mathbf{V}^{(\beta)\dagger}\mathrm{d}\mathbf{V}^{(\beta)}\right) \sigma_1^{\beta-1}\sigma_2^{\beta-1}(\sigma_1^2-\sigma_2^2)^{\beta}\,\mathrm{d}\sigma_1\mathrm{d}\sigma_2, \tag{5.4}$$

where $\left(\mathbf{U}^{(\beta)\dagger}\mathrm{d}\mathbf{U}^{(\beta)}\right)$ and $\left(\mathbf{V}^{(\beta)\dagger}\mathrm{d}\mathbf{V}^{(\beta)}\right)$ are the invariant measures on $\mathrm{U}_2(\mathbb{F})$ defined in Chapter 4. The factor $\left(\frac{2\pi^{\beta/2}}{\Gamma(\beta/2)}\right)^{-2}$ comes about due to the restriction on the entries in the first row of $\mathbf{V}^{(\beta)}$.

Let us now first restrict the matrices $\mathbf{G} \in \mathrm{GL}_N(\mathbb{F})$ to have positive determinant, then to have determinant unity by imposing the delta function constraint in (4.3). This requires that we multiply (5.4) by

$$\left(\frac{2\pi^{\beta/2}}{\Gamma(\beta/2)}\right)^{-1} \delta\left(1-\sigma_1\sigma_2\right).$$

Consequently, with (5.1) it follows from this modification of (5.4) that

$$\left(\frac{2\pi^{\beta/2}}{\Gamma(\beta/2)}\right)^{-3} \mathrm{vol}(\mathrm{U}_2(\mathbb{F}))^2 \chi_{0<\sigma_2<\sigma_1<R}\,\delta\left(1-\sigma_1\sigma_2\right)\sigma_1^{\beta-1}\sigma_2^{\beta-1}(\sigma_1^2-\sigma_2^2)^{\beta}\,\mathrm{d}\sigma_1\mathrm{d}\sigma_2 \tag{5.5}$$

where the indicator function comes from the truncated set , and the precise value of $\mathrm{vol}(\mathrm{U}_2(\mathbb{F}))^2$ is obtained from (4.4):

$$\mathrm{vol}\,\mathrm{U}_2(\mathbb{F}) = 2^2\,\frac{\pi^{\beta/2}}{\Gamma(\beta/2)}\,\frac{\pi^{\beta}}{\Gamma(\beta)}. \tag{5.6}$$

Proposition 5.8. *Denote*

$$J^{(\beta)}(R) := \int \chi_{0<\sigma_2<\sigma_1<R}\,\delta\left(1-\sigma_1\sigma_2\right)\sigma_1^{\beta-1}\sigma_2^{\beta-1}(\sigma_1^2-\sigma_2^2)^{\beta}\,\mathrm{d}\sigma_1\mathrm{d}\sigma_2. \tag{5.7}$$

Then

$$J^{(1)}(R) = \frac{R^2}{2} + \frac{1}{2R^2} - 1, \tag{5.8}$$

$$J^{(2)}(R) = \frac{R^4}{4} - \frac{1}{4R^4} - 2\log\,R, \tag{5.9}$$

$$J^{(4)}(R) = \frac{R^8}{8} - R^4 + \frac{1}{R^4} - \frac{1}{8R^8} + 6\log\, R. \tag{5.10}$$

Proof. The delta function can be rewritten as $\frac{1}{\sigma_1}\delta(\sigma_2 - \frac{1}{\sigma_1})$, and after integrating over σ_2 the integrand becomes $\frac{1}{\sigma_1}(\sigma_1^2 - \frac{1}{\sigma_1^2})^\beta$. Integrating this from 1 to R for each β gives (5.8), (5.9) and (5.10). □

We now take up the problem of sampling according to Haar measure random matrices from $\mathrm{SL}_2(\mathbb{F})$ with bound R on the operator norm. In the case $\mathbb{F} = \mathbb{R}$ a method based on the singular value decomposition (5.3) has been given and implemented in [13]. A generalisation to $\mathbb{F} = \mathbb{C}$ and $\mathbb{H}$ is straightforward, as we will now proceed to demonstrate.

The unitary matrices in (5.3) are to have entries in $\mathbb{C}$ and $\mathbb{H}$ for $\beta = 2$ and 4 respectively, and to be chosen with Haar measure. A simple way to achieve this is to first generate a pair of 2×1 standard Gaussian vectors with entries from the appropriate number field, then apply the Gram-Schmidt algorithm to obtain an orthonormal basis. Forming a matrix from the latter gives the sought Haar distributed unitary matrix; see e.g. [8, §5.2]. An alternative way to sample these is to consider the Euler parametrization of the unitary matrices also given in [8]. For $\mathbb{F} = \mathbb{R}$, with θ uniformly distributed in $[0, 2\pi)$, the matrix

$$\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$$

is uniformly distributed in $\mathrm{U}_2(\mathbb{R})$. For the complex case, such parametrization is slightly more complicated. Thus

$$e^{i\eta/2} \begin{bmatrix} e^{i\alpha}\cos\phi & e^{i\beta}\sin\phi \\ -e^{-i\beta}\sin\phi & e^{-i\alpha}\cos\phi \end{bmatrix}$$

is uniformly distributed in $\mathrm{U}_2(\mathbb{C})$, with α, β, η uniformly distributed in $[0, 2\pi)$ and $\frac{1}{2}\sin^2\theta$ uniformly distributed in $[0, 1/2)$. Parametrization of quaternion unitary matrices has also been demonstrated. The entries in the first row of $\mathbf{V}$ are required to be real and positive, giving extra constraints on the parameters, and sampling according to the unrestricted parameter consistently gives extra copies of the original sample of random matrices, which does not affect the results.

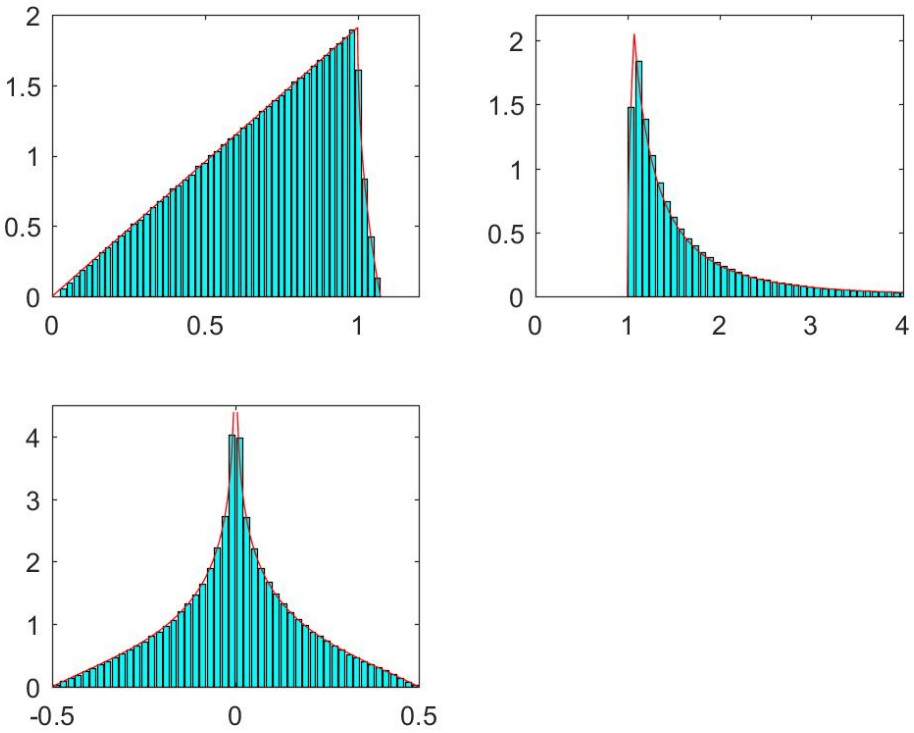

FIGURE 5.1: A total of 10^6 matrices were sampled from $\mathrm{SL}_2(\mathbb{R})$ with invariant measure and cut-off $R = 40$. For each, the Lagrange–Gauss lattice reduction algorithm has been applied to compute the shortest basis vector $\boldsymbol{\alpha}$ and the second shortest basis vector $\boldsymbol{\beta}$. Histograms have been formed for the PDF of the statistics for $||\boldsymbol{\alpha}||$ (top left), $||\boldsymbol{\beta}||$ (top right) and $\boldsymbol{\alpha}^\top \boldsymbol{\beta}/(||\boldsymbol{\alpha}||\,||\boldsymbol{\beta}||)$ (bottom left), and compared against the theoretical predictions.

Due to the constraint in (4.3), for $N = 2$ the remaining task is to compute the distribution of the singular value σ_1 – the second singular value is not independent being given by $\sigma_2 = 1/\sigma_1$. With $\sigma_1 \leq R$, it follows from (5.4) and (5.7) that the cumulative distribution of σ_1 is given by

$$J_2^{(\beta)}(r)/J_2^{(\beta)}(R), \quad 1 < r < R, \tag{5.11}$$

which is made explicit from (5.8), (5.9) and (5.10). Setting (5.11) equal to s, with s chosen uniformly between 0 and 1, then solving for r, samples σ_1 from (5.11).

Now forming the product (5.3) gives a member of $\mathrm{GL}_N(\mathbb{F})$ with modulus

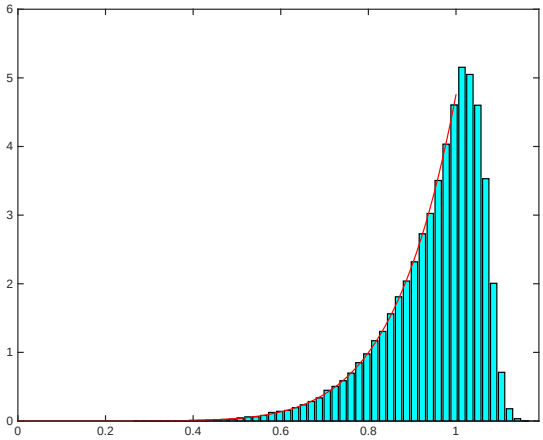

FIGURE 5.2: A total of 10^6 matrices were sampled from $\mathrm{SL}_2(\mathbb{H})$ with invariant measure and cutoff $R = 40$. For each, the quaternion Lagrange–Gauss lattice reduction algorithm with respect to the Hurwitz integers has been applied to compute the shortest basis vector $\boldsymbol{\alpha}$. A histogram has been formed for the PDF of $||\boldsymbol{\alpha}||$. In the range $0 < s < 1$ the theoretical prediction (4.38) with $\Gamma_{4,H}$ specified by (4.45) has been superimposed.

of its determinant equal to 1. Dividing out the phase of the latter gives the sought matrices from $\mathrm{SL}_N(\mathbb{F})$. In fact this last step is unnecessary for present purposes relating to random lattices as only the modulus of the determinant is relevant.

Implementing the Lagrange–Gauss algorithm

For practical purpose to building lattice reduction algorithms, the termination $m_j \neq 0$, $m_{j+1} = 0$ suggested by Lemmas 3.1, 3.4 and 3.7 is not the most convenience one. In fact one notices that by the definitions of m_j and m_{j+1},

$$D_{\mathbb{Z}^{(\beta)}}\left(\frac{\|\mathbf{b}_j\|^2}{\|\mathbf{b}_{j+1}\|^2}\frac{\mathbf{b}_j^\dagger \mathbf{b}_{j+1}}{\|\mathbf{b}_j\|^2}\right) = D_{\mathbb{Z}^{(\beta)}}\left(\frac{\mathbf{b}_j^\dagger \mathbf{b}_{j+1}}{\|\mathbf{b}_{j+1}\|^2}\right) = 0$$

and with

$$D_{\mathbb{Z}^{(\beta)}}\left(\frac{\mathbf{b}_j^\dagger \mathbf{b}_{j+1}}{\|\mathbf{b}_j\|^2}\right) \neq 0$$

one concludes that $\|\mathbf{b}_{j+1}\| \geq \|\mathbf{b}_j\|$. Hence, iterations gives a sequence of vectors $\mathbf{b}_i$ with decreasing length, until $m = 0$ for the first time, where the length of $\mathbf{b}_i$ is no longer decreasing. If the algorithm still runs it gives the last and second last vectors alternately, which form the reduced basis. According to these one can build the 2-dimensional complex and quaternion lattice reduction algorithm as Algorithm 5.1.

Algorithm 5.1 Two-dimensional $\mathbb{F}$-valued lattice reduction algorithm

Input:
A basis $\mathbf{b}_1, \mathbf{b}_2$ of a lattice $\mathcal{L}$ in $\mathbb{F}^2$.
Output:
A minimal basis $\boldsymbol{\alpha}, \boldsymbol{\beta}$ of the lattice $\mathcal{L}$ with $\|\boldsymbol{\alpha}\| \leq \|\boldsymbol{\beta}\|$

1: Set $\boldsymbol{\alpha}, \boldsymbol{\beta}$ be $\mathbf{b}_1, \mathbf{b}_2$ such that $\|\boldsymbol{\alpha}\| \leq \|\boldsymbol{\beta}\|$
2: **while** $\|\boldsymbol{\alpha}\| < \|\boldsymbol{\beta}\|$ **do**
3: Set $temp \leftarrow \boldsymbol{\beta} - \boldsymbol{\alpha} * D_{\mathbb{Z}^{(\beta)}}(\boldsymbol{\alpha}^\dagger \boldsymbol{\beta}/\|\boldsymbol{\alpha}\|^2)$.
4: Set $\boldsymbol{\beta} \leftarrow \boldsymbol{\alpha}$, $\boldsymbol{\alpha} \leftarrow temp$.
5: **end while**
6: Interchange $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ and return.

As for the quantizer $D_{\mathbb{Z}^{(\beta)}}$ in the real and complex cases the closest integer function can be made use of, while in the quaternion case one may refer to (3.26) and (3.28) or alternatively use the closest integer function for the first sub-lattice, and then apply a search for all its neighbours such that (3.25) holds.

In Figure 5.1 we compare the corresponding histograms obtained for $||\boldsymbol{\alpha}||$, $||\boldsymbol{\beta}||$ and $|\boldsymbol{\alpha}^\dagger \boldsymbol{\beta}|/(||\boldsymbol{\alpha}||\,||\boldsymbol{\beta}||)$ of real random lattices against the theoretical predictions of Proposition 4.1. In Figure 5.3, we compare the corresponding histograms obtained for those statistics of complex random lattices against the theoretical predictions of Propositions 4.4, 4.5, 4.7 and Corollary 4.8. We see are all in excellent agreement. Using similar methods the quaternion version of the Lagrange–Gauss algorithm can also be implemented, allowing for the plotting of a histogram approximating the PDF for the shortest basis vector. As shown in Figure 5.2 this exhibits excellent agreement with the theoretical prediction Propositions 4.9 augmented by Proposition 4.11.

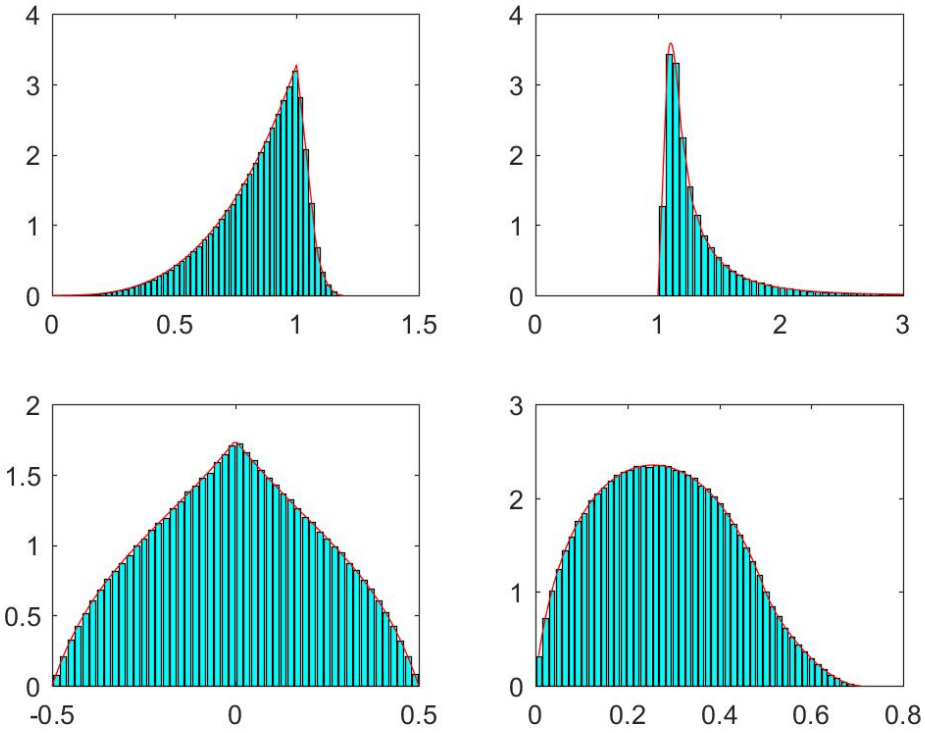

FIGURE 5.3: A total of 10^6 matrices were sampled from $\mathrm{SL}_2(\mathbb{C})$ with invariant measure and cutoff $R = 40$. For each, the complex Lagrange–Gauss lattice reduction algorithm with respect to the Gaussian integers has been applied to compute the shortest basis vector $\boldsymbol{\alpha}$ and the second shortest basis vector $\boldsymbol{\beta}$. Histograms have been formed for the PDF of the statistics for $||\boldsymbol{\alpha}||$ (top left), $||\boldsymbol{\beta}||$ (top right), $\mathrm{Re}(\boldsymbol{\alpha}^\dagger\boldsymbol{\beta})/(||\boldsymbol{\alpha}||\,||\boldsymbol{\beta}||)$ (bottom left) and $|\boldsymbol{\alpha}^\dagger\boldsymbol{\beta}|/(||\boldsymbol{\alpha}||\,||\boldsymbol{\beta}||)$ (bottom right), and compared against the theoretical predictions.

Chapter 6

Related topics

Relationship to hyperbolic geometry

The vector equation (3.6) can also be written in scalar form, albeit involving complex numbers [6]. Thus, set $\mathbf{b}_j = (x_j, y_j)$ and write $b_j = x_j + \mathrm{i}y_j$. The fact that

$$\frac{b_{j-1}}{b_j} = \frac{\mathbf{b}_j \cdot \mathbf{b}_{j-1}}{\|b_j\|^2} + \mathrm{i}\frac{\det B}{\|b_j\|^2}, \quad B = [\mathbf{b}_{j-1}\, \mathbf{b}_j] \tag{6.1}$$

then allows (3.6) to be written

$$b_{j+1} = b_{j-1} - \left\lceil \mathrm{Re}\, \frac{b_{j-1}}{b_j} \right\rfloor b_j,$$

or equivalently, with $z_j = b_j/b_{j-1}$ ($b_{j-1} \neq 0$)

$$z_{j+1} = \frac{1}{z_j} - \left\lceil \mathrm{Re}\, \frac{1}{z_j} \right\rfloor. \tag{6.2}$$

With α and β the complex numbers corresponding to the vectors $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, setting $z = \beta/\alpha$ the conditions (3.13) for a reduced basis read

$$|z| \geq 1, \quad |\mathrm{Re}\, z| \leq \frac{1}{2}. \tag{6.3}$$

The inequalities (6.3) are recognised as specifying the fundamental domain in the upper half plane model of hyperbolic geometry, up to details on the boundary; see e.g. [36]. Starting with $r_1 = b_1/b_0$, $|r_1| < 1$, the recurrence (6.2) is to be iterated until $|r_{j+1}| \geq 1$.

Changing variables in the invariant measure (4.9) gives

$$\pi\chi_{x^2+y^2>1}\chi_{|x|<1/2}\chi_{y>0}\frac{\mathrm{d}x\mathrm{d}y}{y^2}. \tag{6.4}$$

The factor $\mathrm{d}x\mathrm{d}y/y^2$, in keeping with the remark above (6.3), is familiar as the invariant measure in the upper half plane model of hyperbolic geometry [36].

Now we will show how the complex vector equation (3.19) can be written in a quaternion scalar form. Writing a pair of complex basis vectors $\mathbf{b}_l = (w_l, z_l)$, $w_l, z_l \in \mathbb{C}$, define

$$q_l = w_l + jz_l, \quad |q_l|^2 = |w_l|^2 + |z_l|^2, \tag{6.5}$$

where the unit i in w_l, z_l is to be regarded as part of the quarternion algebra (note that we have chosen to have the unit j to the left). With V the 2×2 matrix with complex vectors $\mathbf{b}_{l-1}$ and $\mathbf{b}_l$ as its columns, analogous to (3.11) one can check

$$q_l{}^{-1}q_{l-1} = \frac{\overline{\mathbf{b}}_l \cdot \mathbf{b}_{l-1}}{\|\mathbf{b}_l\|^2} + j\frac{\det V}{\|\mathbf{b}_l\|^2} \tag{6.6}$$

(cf.(6.2)). Another viewpoint on (6.6) is in terms of the so-called Cayley–Dickson doubling formula. Thus for $a, b, c, d \in \mathbb{C}$ define

$$\overline{(a,b)} = (\overline{a}, -b), \qquad (a,b)(c,d) = (ac - d\overline{b}, \overline{a}d + cb). \tag{6.7}$$

Identify $(a, b) = a + jb$. Then these rules together with $q_l^{-1}q_{l-1} = |q_l|^{-2}\overline{q}_l q_{l-1}$ and $\overline{q}_l = (\overline{a}, -b)$, $q_{l-1} = (c, d)$ and the fact that complex numbers commute imply (6.6).

Consequently, the complex vector recurrence (3.19), rearranged so that order of multiplication in the last term is reversed (this is in keeping with the unit j in (6.5) being to the left, and thus purely complex multiplication taking place to the right), can be rewritten as the quaternion scalar recurrence

$$q_j^{-1}q_{j+1} = q_j^{-1}q_{j-1} - D_{\mathbb{Z}[w]}\left((\mathrm{Re} + i\,\mathrm{Im}_i)q_j^{-1}q_{j-1}\right) \tag{6.8}$$

where Im_i denotes the (real) coefficient of i. Now writing $Q_j^{-1} = q_j^{-1}q_{j-1}$ gives the analogue of (6.2),

$$Q_{j+1} = \frac{1}{Q_j} + D_{\mathbb{Z}[w]}\Big(\frac{1}{Q_j}\Big). \tag{6.9}$$

For the measure (4.18), introduce the scaled vector

$$\frac{1}{|\boldsymbol{\alpha}|}\boldsymbol{\beta} = \left((t_{12}^{(r)} + it_{12}^{(i)})/t_{11}, 1/t_{11}^2\right)$$

and set $q = (t_{12}^{(r)} + it_{12}^{(i)})/t_{11} + j/t_{11}^2$. Then

$$x_1 = t_{12}^{(r)}/t_{11}, \quad x_2 = t_{12}^{(i)}/t_{11}, \quad x_3 = 1/t_{11}^2.$$

In these variables the invariant measure (4.18) reads

$$\chi_{x_1^2+x_2^2+x_3^2>1}\chi_{|x_1|\leq\frac{1}{2}}\chi_{|x_2|\leq\frac{1}{2}}\chi_{x_3>0}\frac{\mathrm{d}x_1\mathrm{d}x_2\mathrm{d}x_3}{x_3^3}. \tag{6.10}$$

The factor $\mathrm{d}x_1\mathrm{d}x_2\mathrm{d}x_3/x_3^3$ is recognised as the invariant measure for hyperbolic 3-space.

On the other hand, the rewrite of this quaternion vector equation to a scalar equation using the doubling of the quaternions to the octonions as implied by (6.7) breaks down. This is because to identify the first component of $(\overline{a}, -b)(c, d)$ as specified by (6.7) with a dot product requires that $d\overline{b} = \overline{b}d$ — and this commutivity — which is not true for quaternions.

Other integers

Inspection of the proof of Proposition 3.6 shows it requires that an appropriate generalisation of the integers should permit a Euclidean algorithm with the absolute value function as norm. This requirement permits the choices:

$$\mathbb{Z}[\sqrt{D}] = \{n_1 + n_2\sqrt{D} : n_1, n_2 \in \mathbb{Z}\}, \quad D = -1, -2 \tag{6.11}$$

$$\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{D})\right] = \left\{n_1 + \frac{n_2}{2}(1+\sqrt{D}) : n_1, n_2 \in \mathbb{Z}\right\}, \quad D = -3, -7, -11, \tag{6.12}$$

these being the complex quadratic integers with the desired property [16]. They have been isolated in the context of lattice reduction in the earlier work [23]. The case $D = -1$ gives the Gaussian integers, the case we have discussed, and $D = -3$ the Eisenstein integers. The latter case has been discussed in the context of complex generalisations of the Lagrange-Gauss algorithm in

the previous work [35]. Similar to the discussion of the quaternion case, a lattice quantizer $D_{\mathbb{Z}[w]}$ mapping a given point $z \in \mathbb{C}$ to a closest lattice point (the latter is unique provided z is not on the boundary of the Voronoi region)

$$D_{\mathbb{Z}[w]}(z) = \underset{\lambda \in \mathbb{Z}[w]}{\operatorname{argmin}} \|\lambda - z\| \tag{6.13}$$

should be introduced. The lattice corresponding to (6.11) is rectangular for $D = -2$ and

$$D_{\mathbb{Z}[\sqrt{2}i]}(z) = \lceil \operatorname{Re} z \rfloor + i\sqrt{2} \left\lfloor \operatorname{Im} z/\sqrt{2} \right\rceil . \tag{6.14}$$

Similar to Hurwitz integers, the lattices corresponding to (6.12) consist of the disjoint union of two rectangular lattices

$$\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{D})\right] = \{n_1 + n_2\sqrt{D} \,:\, n_1, n_2 \in \mathbb{Z}\} \cup \{(n_1 + 1/2) + (n_2 + 1/2)\sqrt{D} \,:\, n_1, n_2 \in \mathbb{Z}\}$$

Denoting these E_1, E_2 respectively we have

$$\begin{aligned} D_{E_1}(z) &= \lceil \operatorname{Re} z \rfloor + \sqrt{D} \lceil \operatorname{Im} z/\sqrt{-D} \rfloor \\ D_{E_2}(z) &= \lceil \operatorname{Re}(z - 1/2) \rfloor + \sqrt{D} \left\lfloor \operatorname{Im}\left(z - \frac{\sqrt{D}}{2}\right) /\sqrt{-D} \right\rceil + \frac{1+\sqrt{D}}{2} \end{aligned}$$

and so

$$D_{\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{D})\right]}(z) = \underset{\beta \in \{D_{E_1}(z), D_{E_2}(z)\}}{\operatorname{argmin}} |\beta - z|. \tag{6.15}$$

In the case $D = -3$ – the Eisenstein integers – the formula (6.15) can be found in [35]. Statistics of these complex quadratic integer lattice can also be found by using the same methods.

A generalisation of complex quadratic integer to quaternion is the maximal order of Euclidean quaternion fields [2], which still permits the Euclidean property. As [23] suggests, lattice reduction algorithms can be built over these orders, and again similar analysis of statistics can be done. Hurwitz integers are one of the special cases where the quaternion field is chosen as $\left(\frac{-1,-1}{\mathbb{Q}}\right)$, as

well as other examples such as a maximal order of $\left(\frac{-1,-1}{\mathbb{Q}(\sqrt{2})}\right)$:

$$\{n_1 + n_2\frac{1+i}{\sqrt{2}} + n_3\frac{1+j}{\sqrt{2}} + n_4\frac{1+i+j+k}{2} : \ n_1, n_2, n_3, n_4 \in \mathbb{Z}\}.$$

Further choices are given by [3].

A generalisation of Lipschitz integer to octonions is the Gravesian octonions, whose components are all integers, and it does not permit Euclidean algorithm either. As stated in [4, 9], there are 7 maximal orders containing Gravesian octonions, each of which is isometric to E_8 rescaled by a factor of $1/\sqrt{2}$. The problem of whether a lattice reduction algorithm over 2-dimensional octonion lattices with respect to E_8 is available is of further interest, and so are the statistics of those random octonion lattices.

General N

A generalisation of real lattice reduction algorithm to dimension 3 is given in [31]. Generally a reduced basis of a 3-dimensional $\mathbb{F}$-valued lattice satisfies

$$\begin{gathered}\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \|\mathbf{b}_3\|, \\ \|\mathbf{b}_2 + x_1\mathbf{b}_1\| \geq \|\mathbf{b}_2\|, \quad \|\mathbf{b}_3 + x_1\mathbf{b}_1 + x_2\mathbf{b}_2\| \geq \|\mathbf{b_3}\|, \quad \forall x_1, x_2 \in \mathbb{Z}^{(\beta)}\end{gathered} \tag{6.16}$$

The first two inequalities together give a reduced basis of a 2-dimensional lattice and a longer linearly independent vector $\mathbf{b}_3$. The third inequality tells us the third vector is chosen to have the shortest projection on the plane spanned by $\{\mathbf{b}_1, \mathbf{b}_2\}$. It suffices to consider the eight lattice points around the minimal $\mathbf{b}_3$, and one should make sure that the projection is located within the Voronoi region of 0. This is to say the projection of $\mathbf{b}_3$ in each direction upon taking the $\mathbb{Z}^{(\beta)}$ quantizer gives 0. Hence the inequalities (6.16) are equivalent to:

$$\begin{gathered}\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \|\mathbf{b}_3\|, \\ D_{\mathbb{Z}^{(\beta)}}\left(\frac{\mathbf{b}_1^\dagger\mathbf{b}_2}{\|\mathbf{b}_1\|^2}\right) = D_{\mathbb{Z}^{(\beta)}}\left(\frac{\mathbf{b}_1^\dagger\mathbf{b}_3}{\|\mathbf{b}_1\|^2}\right) = D_{\mathbb{Z}^{(\beta)}}\left(\frac{\mathbf{b}_2^\dagger\mathbf{b}_3}{\|\mathbf{b}_2\|^2}\right) = D_{\mathbb{Z}^{(\beta)}}\left(\frac{(\mathbf{b}_1 \pm \mathbf{b}_2)^\dagger\mathbf{b}_3}{\|\mathbf{b}_1 \pm \mathbf{b}_2\|^2}\right) = 0.\end{gathered} \tag{6.17}$$

Also by posing this reduced condition, one believes that proper complex and quaternion lattice reduction algorithms can be generalised to the 3 dimensional case – this is a topic for further research.

Joint measure of the Gram Schmidt basis can be obtained by rewriting (6.17) into proper variables, and the corresponding statistics can also be computed numerically. In [13], 3-dimensional real random lattices are sampled by sampling within a ball of radius R with respect to the operator norm and applying the 3-dimensional Lagrange-Gauss algorithm. A comparison of theoretical prediction to the simulation is one of the key points to research.

It is also implied in [31] that the Lagrange-Gauss algorithm can be extended to higher dimension, while for dimensions greater than 4 the reduced basis we obtained does not necessarily give the shortest vector. In general high dimensional Lagrange-Gauss algorithm is NP-hard [24] and the LLL algorithm [20] can find a short enough basis in polynomial time with guaranteed worst-case performance. In the LLL algorithm one inserts a reduction parameter $\alpha \in (\frac{1}{4}, 1)$ instead of $\alpha = 1$ in Lagrange-Gauss algorithm, giving tolerance that it does not necessarily produce the shortest basis. Besides, BKZ algorithm [30] and RSR algorithm [29] are introduced recently, and they can be compared in terms of runtime and approximation to an optimal solution, always relative to the dimension of the given lattice. For higher dimensional analysis of random lattices such algorithms may be of interests.

The limit $N \to \infty$ has been studied in the real case, with a number of results given in [26, 19, 34]. A generalisation of those results to complex and quaternion lattice requires to generalise Siegel's mean value theorem and Roger's integration formula, and it s topic for future study.

Bibliography

[1] Murray R Bremner. *Lattice basis reduction: an introduction to the LLL algorithm and its applications*. CRC Press, 2011.

[2] Jean-Paul Cerri, Jérôme Chaubert, and Pierre Lezowski. "Euclidean totally definite quaternion fields over the rational field and over quadratic number fields". In: *International Journal of Number Theory* 9.03 (2013), pp. 653–673.

[3] Jean-Paul Cerri and Pierre Lezowski. "Computation of Euclidean minima in totally definite quaternion fields". In: (2016).

[4] John H Conway and Derek A Smith. "On quaternions and octonions: their geometry, arithmetic, and symmetry". In: *Bulletin of the American Mathematical Society* 42 (2005), pp. 229–243.

[5] J. Jaldén D. Wübben D. Seethaler and G. Matz. "Lattice reduction algorithm for low-complexity full-diversity mimo detection". In: *Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE*. Vol. 28. IEEE Signal Proc. Magazine. 2009, pp. 70–91.

[6] Hervé Daudé, Philippe Flajolet, and Brigitte Vallée. "An average-case analysis of the Gaussian algorithm for lattice reduction". In: *Combinatorics, Probability and Computing* 6.4 (1997), pp. 397–433.

[7] José A Dı, Ramón Gutiérrez-Jáimez, et al. "On Wishart distribution: some extensions". In: *Linear Algebra and its Applications* 435.6 (2011), pp. 1296–1310.

[8] Persi Diaconis and Peter J Forrester. "Hurwitz and the origins of random matrix theory in mathematics". In: *Random Matrices: Theory and Applications* 6.01 (2017), p. 1730001.

[9] Tevian Dray and Corinne A Manogue. *The geometry of the octonions*. World Scientific, 2015.

[10] William Duke, Zeév Rudnick, Peter Sarnak, et al. "Density of integer points on affine homogeneous varieties". In: *Duke mathematical journal* 71.1 (1993), pp. 143–179.

[11] Freeman J Dyson. "The threefold way. Algebraic structure of symmetry groups and ensembles in quantum mechanics". In: *Journal of Mathematical Physics* 3.6 (1962), pp. 1199–1215.

[12] Peter J Forrester. *Log-gases and random matrices (LMS-34)*. Princeton University Press, 2010.

[13] Peter J Forrester. "Volumes for $SL_N(\mathbb{R})$, the Selberg integral and random lattices". In: *arXiv preprint arXiv:1604.07462* (2016).

[14] Steven D Galbraith. *Mathematics of public key cryptography*. Cambridge University Press, 2012.

[15] Ying Hung Gan, Cong Ling, and Wai Ho Mow. "Complex lattice reduction algorithm for low-complexity full-diversity MIMO detection". In: *IEEE Transactions on Signal Processing* 57.7 (2009), pp. 2701–2710.

[16] Godfrey Harold Hardy and Edward Maitland Wright. *An introduction to the theory of numbers*. Oxford University Press, 1979.

[17] A. Hurwitz. "Über die Erzeugung der Invarianten durch Integration". In: *Nachr. Ges. Wiss. Göttingen* (1897), pp. 71–90.

[18] Henry Jack and AM Macbeath. "The volume of a certain set of matrices". In: *Mathematical Proceedings of the Cambridge Philosophical Society*. Vol. 55. 3. Cambridge University Press. 1959, pp. 213–223.

[19] Seungki Kim. "On the distribution of lengths of short vectors in a random lattice". In: *Mathematische Zeitschrift* 282.3-4 (2016), pp. 1117–1126.

[20] Arjen Klaas Lenstra, Hendrik Willem Lenstra, and László Lovász. "Factoring polynomials with rational coefficients". In: *Mathematische Annalen* 261.4 (1982), pp. 515–534.

[21] AM Macbeath and CA Rogers. "A modified form of Siegel's mean-value theorem". In: *Mathematical Proceedings of the Cambridge Philosophical Society*. Vol. 51. 4. Cambridge University Press. 1955, pp. 565–576.

[22] António Machiavelo and Luís Roçadas. "Some Connections Between The Arithmetic and The Geometry of Lipschitz Integers". In: *arXiv preprint arXiv:1201.5817* (2012).

[23] Huguette Napias. "A generalization of the LLL-algorithm over euclidean rings or orders". In: *Journal de théorie des nombres de Bordeaux* 8.2 (1996), pp. 387–396.

[24] Phong Q Nguyen and Damien Stehlé. "Low-dimensional lattice basis reduction revisited". In: *International Algorithmic Number Theory Symposium*. Springer. 2004, pp. 338–357.

[25] I. Rivin. "How to pick a random integer matrix? (and other questions)". In: *Math. Computation* 85 (2016).

[26] Claude Ambrose Rogers. "The moments of the number of points of a lattice in a bounded set". In: *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 248.945 (1955), pp. 225–251.

[27] Walter Rudin. *Functional analysis. International series in pure and applied mathematics*. 1991.

[28] D. Salamon. *Measure and Integration*. EMS textbooks in mathematics. European Mathematical Society, 2016. ISBN: 9783037191590. URL: https://books.google.com.au/books?id=1MjOjwEACAAJ.

[29] Claus-Peter Schnorr. "Lattice reduction by random sampling and birthday methods". In: *STACS*. Vol. 2607. Springer. 2003, pp. 145–156.

[30] Claus-Peter Schnorr and Martin Euchner. "Lattice basis reduction: Improved practical algorithms and solving subset sum problems". In: *Mathematical programming* 66.1-3 (1994), pp. 181–199.

[31] Igor Semaev. "A 3-dimensional lattice reduction algorithm". In: *Cryptography and Lattices*. Springer, 2001, pp. 181–193.

[32] Carl Ludwig Siegel. "A mean value theorem in geometry of numbers". In: *Annals of Mathematics* (1945), pp. 340–347.

[33] Carl Ludwig Siegel. "The volume of the fundamental domain for some infinite groups". In: *Transactions of the American Mathematical Society* 39.2 (1936), pp. 209–218.

[34] Anders Södergren. "On the Poisson distribution of lengths of lattice vectors in a random lattice". In: *Mathematische Zeitschrift* 269.3 (2011), pp. 945–954.

[35] Qifu Tyler Sun et al. "Lattice network codes based on Eisenstein integers". In: *IEEE Transactions on Communications* 61.7 (2013), pp. 2713–2725.

[36] Audrey Terras. *Harmonic analysis on symmetric spaces—Euclidean space, the sphere, and the Poincaré upper half-plane*. Springer Science & Business Media, 2013.

[37] Stephanie Vance. "Improved sphere packing lower bounds from Hurwitz lattices". In: *Advances in Mathematics* 227.5 (2011), pp. 2144–2156.

[38] A. Weil. "Sur quelques resultats de Siegel". In: *Summa Brasil Math* 1 (1946), pp. 21–39.

[39] Huan Yao and Gregory W Wornell. "Lattice-reduction-aided detectors for MIMO communication systems". In: *Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE*. Vol. 1. IEEE. 2002, pp. 424–428.

[40] IJ Zucker. "Exact results for some lattice sums in 2, 4, 6 and 8 dimensions". In: *Journal of Physics A: Mathematical, Nuclear and General* 7.13 (1974), p. 1568.