Journal of Number Theory 190 (2018) 1–39

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Volumes and distributions for random unimodular complex and quaternion lattices

Peter J. Forrester [a,*], Jiyuan Zhang [b]

[a] *School of Mathematics and Statistics, ARC Centre of Excellence for Mathematical & Statistical Frontiers, University of Melbourne, Victoria 3010, Australia*
[b] *School of Mathematics and Statistics, University of Melbourne, Victoria 3010, Australia*

ARTICLE INFO

Article history:
Received 29 October 2017
Received in revised form 14 March 2018
Accepted 26 March 2018
Available online 22 April 2018
Communicated by B. Conrey

Keywords:
Lattice reduction
Geometry of numbers
Random matrices

ABSTRACT

Two themes associated with invariant measures on the matrix groups $\mathrm{SL}_N(\mathbb{F})$, with $\mathbb{F} = \mathbb{R}, \mathbb{C}$ or $\mathbb{H}$, and their corresponding lattices parametrised by $\mathrm{SL}_N(\mathbb{F})/\mathrm{SL}_N(\mathcal{O})$, $\mathcal{O}$ being an appropriate Euclidean ring of integers, are considered. The first is the computation of the volume of the subset of $\mathrm{SL}_N(\mathbb{F})$ with bounded 2-norm or Frobenius norm. Key here is the decomposition of measure in terms of the singular values. The form of the volume, for large values of the bound, is relevant to asymptotic counting problems in $\mathrm{SL}_N(\mathcal{O})$. The second is the problem of lattice reduction in the case $N = 2$. A unified proof of the validity of the appropriate analogue of the Lagrange–Gauss algorithm for computing the shortest basis is given. A decomposition of measure corresponding to the QR decomposition is used to specify the invariant measure in the coordinates of the shortest basis vectors. With $\mathbb{F} = \mathbb{C}$ this allows for the exact computation of the PDF of the first minimum (for $\mathcal{O} = \mathbb{Z}[i]$ and $\mathbb{Z}[(1 + \sqrt{-3})/2]$), and the PDF of the second minimum and that of the angle between the minimal basis vectors (for $\mathcal{O} = \mathbb{Z}[i]$). It also encodes the specification of fundamental domains of the corresponding quotient spaces. Integration over the latter gives rise to certain number theoretic constants, which are also present in the asymptotic forms of the PDFs of the lengths of the shortest basis vectors. Siegel's mean value gives an alternative method to compute the arithmetic

* Corresponding author.
E-mail addresses: pjforr@unimelb.edu.au (P.J. Forrester), jiyuanz@student.unimelb.edu.au (J. Zhang).

https://doi.org/10.1016/j.jnt.2018.03.010

constants, allowing in particular the computation of the leading form of the PDF of the first minimum for $\mathbb{F} = \mathbb{H}$ and $\mathcal{O}$ the Hurwitz integers, for which direct integration was not possible.

1. Introduction

Let $\mathcal{B} = \{\mathbf{b}_0, \mathbf{b}_1, \dots, \mathbf{b}_{d-1}\}$ be a basis of $\mathbb{R}^d$, and require that the corresponding parallelotope have unit volume. Let

$$\mathcal{L} = \{m_0\mathbf{b}_0 + \cdots + m_{d-1}\mathbf{b}_{d-1} \,|\, m_0, \dots, m_{d-1} \in \mathbb{Z}\} \tag{1.1}$$

denote the corresponding lattice. The Minkowski–Hlawka theorem tells us that for large d, there exists lattices such that the shortest vectors have length proportional to $\sqrt{d}$. By the Minkowski convex body theorem this is also the maximum possible order of magnitude of the shortest vectors; see e.g. [3]. Siegel [34] introduced the notion of a random lattice, and was able to show that for large dimension d, a random lattice will typically achieve the Minkowski–Hlawka bound.

The construction of Siegel of a random lattice requires first the specification of the unique invariant measure for the matrix group $\mathrm{SL}_N(\mathbb{R})$; 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 set of lattices, and that this quotient space has finite volume with respect to the invariant measure.

In a recent work [14] by one of the present authors, a viewpoint from random matrix theory was taken on the computation of volumes associated with $\mathrm{SL}_N(\mathbb{R})$, and this led to a Monte Carlo procedure to generate random lattices in the sense of Siegel. In low dimensions $d = 2$, 3 and 4 there are fast exact lattice reduction algorithms to find the shortest lattice vectors [31,27] – the case $d = 2$ is classical being due to Lagrange and Gauss; see e.g. [2]. These were implemented in dimensions two and three to obtain histograms of the lengths and their mutual angles; in dimension two the exact functional forms were obtained by integration over the fundamental domain. For general d, it was shown how a mean value theorem derived by Siegel in [34] implies the exact functional form of the distribution $P_{\mathrm{short}}(t)$ of the length of the shortest vector for general d,

$$P_{\mathrm{short}}(t) \underset{t\to 0}{\sim} \frac{dv_d}{2\zeta(d)} t^{d-1}, \tag{1.2}$$

where $\zeta(x)$ denotes the Riemann zeta function, and v_d the volume of the unit ball in dimension d (actually only the case $d = 3$ was presented, but the derivation applies for general d to give (1.2)).

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 [9] (dropping the requirement of associativity permits the octonions $\mathbb{O}$ to be added to the list; see the recent work [13] for spectral properties of various ensembles of 2×2 and 3×3 Hermitian matrices with entries in $\mathbb{O}$). As such, attention is drawn to extending the considerations of [14] to the case of complex and quaternion vector spaces $\mathbb{C}^n$ and $\mathbb{H}^n$. One remarks that lattices in these vector spaces, with scalars equal to the Gaussian integers and Eisenstein integers for $\mathbb{C}^2$, and Hurwitz integers for $\mathbb{H}^n$, received earlier attention for their application to signal processing in wireless communication [41,17,40,36], and their consequences for lattice packing bounds [38] respectively. The study [26] extends the LLL lattice reduction algorithm to these settings.

Of particular interest from the viewpoint of [14] are the invariant measure for $\mathrm{SL}_N(\mathbb{C})$ and $\mathrm{SL}_N(\mathbb{H})$, the associated volumes, and the corresponding lattice reduction problems. Following the work of Jack and Macbeath in the case of $\mathrm{SL}_N(\mathbb{R})$, we begin in §2 by using the singular value factorisation to decompose the invariant measures. To obtain a finite volume, a certain truncation must be introduced, most naturally by restricting the norm $\|M\|$ to be bounded by a value R. We do this in the case of the 2-norm $\|M\|_2 := \mu_1$, where μ_1 is the largest singular value of M, and the Frobenius norm $\|M\|_F := \left(\sum_{j=1}^N \mu_j^2\right)^{1/2}$, where μ_j is the jth largest singular value. The large R form of the volume is of particular relevance due to counting formulas of the type [8]

$$\#\{\gamma \,:\, \gamma \in \mathrm{SL}_N(\mathbb{Z}),\, \|\gamma\| \leqslant R\} \underset{R\to\infty}{\sim} \frac{1}{\operatorname{vol}\Gamma} \int\limits_{\|G\|\leqslant R} (\mathrm{d}G). \tag{1.3}$$

Here $(\mathrm{d}G)$ is the Haar measure on $\mathrm{SL}_N(\mathbb{R})$, and vol Γ the volume of the corresponding fundamental domain. A generalisation of (1.3) applying to lattice subgroups of topological groups, and in particular

$$\#\{\gamma : \gamma \in \mathrm{SL}_N(\mathbb{Z}[i]), \|\gamma\| \leqslant R\}, \tag{1.4}$$

is given in [19, Th. 1.5], and has the same structure as (1.3). As an application of our evaluation of the volume of a ball in $\mathrm{SL}_N(\mathbb{C})$ we are able to compute the leading large R form of (1.4), up to the value of vol Γ; in the case $N = 2$ this can be determined and we obtain the explicit asymptotic expression (4.35) below.

For lattices in $\mathbb{C}^2$ with scalars from particular rings of complex quadratic integers, there is a generalisation of the Lagrange–Gauss algorithm that allows for the determination of a reduced basis $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ with the shortest possible lengths. For the Gaussian and Eisenstein integers this has been noted previously [41,36], although our proofs given in §4.1 are different and apply to all cases at once. They are motivated by known theory in the real case, which we revise in §3. Another point covered in §3 is the observation in [5] that the original Lagrange–Gauss algorithm is equivalent to a simple mapping in the complex plane, related to the Gauss map for continued fractions. We show in §4.2

that in the case of lattices in $\mathbb{C}^2$, the generalisation of the Lagrange–Gauss algorithm for lattice reduction can be written as a scalar mappings of quaternions.

In the Gaussian case, the PDF for the lengths of the reduced basis vectors and the scaled inner product $|\overline{\boldsymbol{\alpha}} \cdot \boldsymbol{\beta}/\|\boldsymbol{\alpha}\|\|\boldsymbol{\beta}\|\,|$ are computed analytically in Section 4.4. For values of s less than 1, it is found $P_{\rm short}(s) = cs^3$ for a particular c, thus relating to (1.2) with $d = 4$. This latter result is found too in the case of the Eisenstein integers, for a different value of c, upon the exact calculation of the functional form of the PDF of the length of the shortest vector carried out in Section 4.5. Siegel's mean value theorem [34] is used to give an independent computation of c in the two cases.

Analogous considerations are applied to lattices formed from vectors in $\mathbb{H}^2$ with scalars the integer Hurwitz quaternions in Section 5; now $P_{\rm short}(s) \underset{s\to 0}{\sim} ks^7$ for a particular k, thus relating to (1.2) with $d = 8$. Here the direct computation of k as done for the case of the Gaussian and Eisenstein integers appears not to be tractable, but the exact value can be found indirectly by use of Siegel's mean value theorem.

2. Invariant measure and volumes for $\mathbf{SL}_N(\mathbb{C})$ and $\mathbf{SL}_N(\mathbb{H})$

2.1. Invariant measure

By way of preliminaries, one recalls that the quaternions $\mathbb{H}$ are a non-commutative algebra with elements of the form

$$a_0 + a_1\mathrm{i} + a_2\mathrm{j} + a_3\mathrm{k}, \tag{2.1}$$

where $a_0, \dots, a_3 \in \mathbb{R}$, $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1$, $\mathrm{ijk} = -1$, and each distinct pair of $\{\mathrm{i}, \mathrm{j}, \mathrm{k}\}$ anti-commutes. However, matrix groups with elements from $\mathbb{H}$ typically make use of the representation of quaternions as 2×2 complex matrices

$$\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix}, \quad z = a_0 + a_i\mathrm{i},\ w = a_2 + a_3\mathrm{i}. \tag{2.2}$$

Thus for example matrices from $\mathrm{GL}_N(\mathbb{H})$ and $\mathrm{SL}_N(\mathbb{H})$ are then $N \times N$ block matrices with each entry a 2×2 block of the form (2.2), and hence $2N \times 2N$ complex matrices.

Let $G \in \mathrm{GL}_N(\mathbb{F})$, where $\mathbb{F} = \mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$. Label by $\beta = 1, 2, 4$ respectively according to the number of independent real parts in an element of $\mathbb{F}$. The symbol $(\mathrm{d}G)$ denotes the product of differentials of all the real and imaginary parts of G. Since for fixed $A \in \mathrm{GL}_N(\mathbb{F})$

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

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

$$\frac{(\mathrm{d}G)}{|\det G|^{\beta N}} \tag{2.3}$$

is unchanged by both left and right group multiplication, and is thus the left and right invariant Haar measure for the group. In the case of $\mathrm{GL}_N(\mathbb{R})$ and thus $\beta = 1$ (2.3) was identified by Siegel [34]. Matrices in $\mathrm{SL}_N(\mathbb{F})$ form the subgroup of $\mathrm{GL}_N(\mathbb{F})$ with unit determinant. Using a delta function distribution to implement this constraint, (2.3) becomes

$$\delta(1 - \det G)\,(\mathrm{d}G). \tag{2.4}$$

In preparation for computing volumes associated with (2.4), as done in the pioneering work of Jack and Macbeath [22] in the case $\mathbb{F} = \mathbb{R}$, we make use of a singular value decomposition

$$G = U^{(\beta)}\mathrm{diag}(\sigma_1, \dots, \sigma_N)V^{(\beta)}, \tag{2.5}$$

where $U^{(\beta)}, V^{(\beta)} \in \mathrm{U}_N(\mathbb{F})$ – the set of $N \times N$ unitary matrices with entries in $\mathbb{F}$. In the case $\beta = 4$ each entry in $\mathrm{diag}(\sigma_1, \dots, \sigma_N)$ is a 2×2 block matrix, so viewed as a $2N \times 2N$ matrix each σ_i is repeated twice along the diagonal. For (2.5) to be one-to-one it is required that the singular values be ordered

$$\sigma_1 \geqslant \sigma_2 \geqslant \cdots \geqslant \sigma_N \geqslant 0$$

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

Changing variables according to (2.5) gives (see e.g. [7, Prop. 2])

$$\begin{aligned}(\mathrm{d}G) = \left(\frac{2\pi^{\beta/2}}{\Gamma(\beta/2)}\right)^{-N} \left(U^{(\beta)\dagger}\mathrm{d}U^{(\beta)}\right)\left(V^{(\beta)\dagger}\mathrm{d}V^{(\beta)}\right) \\ \times \prod_{l=1}^{N} \sigma_l^{\beta-1} \prod_{1 \leqslant j < k \leqslant N} (\sigma_j^2 - \sigma_k^2)^\beta \,\mathrm{d}\sigma_1 \cdots \mathrm{d}\sigma_N,\end{aligned} \tag{2.6}$$

where $\left(U^{(\beta)\dagger}\mathrm{d}U^{(\beta)}\right)$ and $\left(V^{(\beta)\dagger}\mathrm{d}V^{(\beta)}\right)$ are the invariant measure on $\mathrm{U}_N(\mathbb{F})$. For $\mathbb{F} = \mathbb{R}$ and $\mathbb{C}$ this was first identified by Hurwitz [21]; the extension of Hurwitz's ideas to the case of unitary matrices with quaternion entries is given in [6]. The factor $\left(\frac{2\pi^{\beta/2}}{\Gamma(\beta/2)}\right)^{-N}$ comes about due to the restriction on the entries in the first row of $V^{(\beta)}$.

Let us now first restrict the matrices $G \in \mathrm{GL}_N(\mathbb{F})$ to have positive determinant, then to have determinant unity by imposing the delta function constraint in (2.4). This requires that we multiply (2.6) by

$$\left(\frac{2\pi^{\beta/2}}{\Gamma(\beta/2)}\right)^{-1} \delta\left(1 - \prod_{l=1}^{N} \sigma_l\right), \tag{2.7}$$

where the first factor corresponds to the reduction in volume due to the restriction to positive determinant. Consequently, with

$$D_R^{\|\cdot\|_2}(\mathrm{SL}_N(\mathbb{F})) = \{M \in \mathrm{SL}_N(\mathbb{F}) : \sigma_1 \leqslant R\} \tag{2.8}$$

it follows from this modification of (2.6) that

$$\mathrm{vol}\left(D_R^{\|\cdot\|_2}(\mathrm{SL}_N(\mathbb{F}))\right) = \left(\frac{2\pi^{\beta/2}}{\Gamma(\beta/2)}\right)^{-(N+1)} (\mathrm{vol}\,\mathrm{U}_N(\mathbb{F}))^2$$
$$\times \int_{0<\sigma_N<\cdots<\sigma_1<R} \delta(1-\sigma_1\cdots\sigma_N)\prod_{l=1}^N \sigma_l^{\beta-1} \prod_{1\leqslant j<k\leqslant N}(\sigma_j^2-\sigma_k^2)^\beta \,\mathrm{d}\sigma_1\cdots\mathrm{d}\sigma_N. \tag{2.9}$$

The precise value of $\mathrm{vol}\,\mathrm{U}_N(\mathbb{F})$ depends on the convention used to relate the line element corresponding to the differential $U^{(\beta)\dagger}\mathrm{d}U^{(\beta)}$ to the Euclidean line element; see [14, Remark 2.3]. This convention can be uniquely specified by integrating (2.6) against Gaussian weighted matrices G – see [14, Remark 2.3] – with the result [7, Eq. (1) with $m=n$]

$$\mathrm{vol}\,\mathrm{U}_N(\mathbb{F}) = 2^N \prod_{k=1}^N \frac{\pi^{\beta k/2}}{\Gamma(\beta k/2)}. \tag{2.10}$$

In the case $\beta = 1$ the multiple integral in (2.9) was first evaluated by Jack and Macbeath [22]. In the recent work [14] a simplified derivation was given by making use of the Selberg integral [30,15,12]. This strategy can be extended to general β.

Proposition 1. *Define*

$$J_N^{(\beta)}(R) := \int_{R>\sigma_1>\cdots>\sigma_N>0} \delta\left(1-\prod_{l=1}^N \sigma_l\right)\prod_{l=1}^N \sigma_l^{\beta-1} \prod_{1\leqslant j<k\leqslant N}(\sigma_j^2-\sigma_k^2)^\beta \,\mathrm{d}\sigma_1\cdots\mathrm{d}\sigma_N \tag{2.11}$$

and set

$$A_N^{(\beta)}(R) = \frac{2^{-N}}{N!} R^{N(\beta-1)+\beta N(N-1)} \prod_{j=0}^{N-1} \frac{\Gamma(1+j\beta/2)\Gamma\left(1+(j+1)\beta/2\right)}{\Gamma(1+\beta/2)}. \tag{2.12}$$

For $c>0$ we have

$$J_N^{(\beta)}(R) = \frac{A_N^{(\beta)}(R)}{2\pi\mathrm{i}} \int_{c-\mathrm{i}\infty}^{c+\mathrm{i}\infty} R^{Ns} \prod_{j=0}^{N-1} \frac{\Gamma\left(\left(s-1+(j+1)\beta\right)/2\right)}{\Gamma\left(\left(s+1+(N+j)\beta\right)/2\right)}\,\mathrm{d}s. \tag{2.13}$$

Proof. Replace the delta function factor $\delta\left(1-\prod_{j=1}^N \sigma_l\right)$ by $\delta\left(t-\prod_{l=1}^N \sigma_l\right)$ and denote (2.11) in this setting by $J_N^{(\beta)}(R;t)$. Making the change of variables $\sigma_l^2 = x_l$ and taking the Mellin transform of both sides shows

$$\int_0^\infty J_N^{(\beta)}(R;t)t^{s-1}\,\mathrm{d}t = \frac{2^{-N}}{N!}\int_0^{R^2}\mathrm{d}x_1\cdots\int_0^{R^2}\mathrm{d}x_N\prod_{l=1}^N x_l^{(s+\beta)/2-3/2}\prod_{1\leqslant j<k\leqslant N}|x_k-x_j|^\beta$$
$$= \frac{2^{-N}}{N!}R^{N(s+\beta)}R^{\beta N(N-1)-N}S_N\left((s+\beta-3)/2,0,\beta/2\right).$$

Here $S_N(a,b,c)$ is the Selberg integral in the notation of [12, Ch. 4]. Making use of the gamma function evaluation of the Selberg integral [30], [12, Eq. (4.3)], and the notation (2.12) reduces this to

$$A_N^{(\beta)}(R)R^{Ns}\prod_{j=0}^{N-1}\frac{\Gamma\left((s-1+(j+1)\beta)/2\right)}{\Gamma\left((s+1+(N+j)\beta)/2\right)}.$$

As a function of s, this is analytic in the right half plane, and uniformly bounded. The standard formula for the inverse Mellin transform can therefore be applied, giving (2.13). □

Remark 2. For future reference we note from (2.13), as an application of the residue theorem, or alternatively by direct computation from (2.11), that for $N=2$

$$J_N^{(2)}(R) = R^4 - \frac{1}{R^4} - 8\log R, \tag{2.14}$$

$$J_N^{(4)}(R) = \frac{R^8}{8} - R^4 + \frac{1}{R^4} - \frac{1}{8R^8} + 6\log R. \tag{2.15}$$

Consideration of the direct computation of (2.11) shows that for general N and $\beta = 1, 2$ or 4, the function $J_N^{(\beta)}(R)$ is a finite series in power functions and logarithms of R, which vanishes when $R=1$.

Remark 3. The delta function constraint in (2.11) implies that the factor $\prod_{l=1}^N \sigma_l^{\beta-1}$ can be replaced by $\prod_{l=1}^N \sigma_l^\mu$ for any $\mu > -1$. The independence of μ manifests itself in (2.13) by $c>0$ being arbitrary.

Corollary 4. *As $R\to\infty$, for $(N,\beta)\neq(2,2)$,*

$$J_N^{(\beta)}(R) = C_{N,\beta}R^{\beta N(N-1)} + \mathrm{O}\left(\begin{cases} R^{\beta N(N-2)}, & \beta = 1,2 \\ R^{\beta N(N-3/2)}, & \beta = 4 \end{cases}\right) \tag{2.16}$$

where

$$C_{N,\beta} = \frac{2\beta^N}{2^{2N}\Gamma(N\beta/2)}\prod_{j=0}^{N-1}\frac{\Gamma(1+j\beta/2)\Gamma^2\left((j+1)\beta/2\right)}{\Gamma(1+\beta/2)\Gamma\left(1+(N+j-1)\beta/2\right)} \tag{2.17}$$

and

$$\operatorname{vol}\left(D_R^{\|\cdot\|_2}(\mathrm{SL}_N(\mathbb{F}))\right) = \frac{\pi^{\beta N^2/2}\Gamma(\beta/2)}{\Gamma(N\beta/2)\pi^{\beta/2}} \prod_{j=0}^{N-1} \frac{\Gamma(1+j\beta/2)}{\Gamma\left(1+(N+j-1)\beta/2\right)} R^{\beta N(N-1)} + \mathrm{O}\left(\begin{cases} R^{\beta N(N-2)}, & \beta = 1,2 \\ R^{\beta N(N-3/2)}, & \beta = 4 \end{cases}\right). \tag{2.18}$$

In the case $(N,\beta) = (2,2)$*, the bound on the correction term is* $\mathrm{O}(\log R)$.

Proof. Standard estimates of the gamma function imply that the integrand decays fast enough in the left half plane that the contour can be closed in the region without changing its value, by Cauchy's theorem. This allows the integral to be computed in terms of a sum over its residues. The poles of the integrand occur at $s = 1-(j+1)\beta$ $(j = 0,\dots,N-1)$ in the cases $\beta = 1,2$; for $\beta = 4$ there are a further set of poles at $s = 1-(j+3/2)\beta$ $(j = 0,\dots,N-1)$. The leading contribution to the large R expansion results from pole closest to the origin. This occurs at $s = 1-\beta$. Evaluating the residue at this point gives (2.16) and (2.17). The residue of the pole second closest to the origin gives the next term in the large R expansion; the order of this term is also a bound since the number of residues is finite. Note that the case $(N,\beta) = (2,2)$because the pole at $s = 1-\beta$ goes from being first to second order. □

Also of interest is the analogue of (2.8) for the Frobenius-norm

$$D_R^{\|\cdot\|_F}(\mathrm{SL}_N(\mathbb{F})) = \left\{ M \in \mathrm{SL}_N(\mathbb{F}) \,:\, \sum_{j=1}^N \sigma_j^2 \leqslant R^2 \right\},$$

for which the analogue of (2.9) reads

$$\operatorname{vol}\left(D_R^{\|\cdot\|_F}(\mathrm{SL}_N(\mathbb{F}))\right) = \left(\frac{2\pi^{\beta/2}}{\Gamma(\beta/2)}\right)^{-(N+1)} (\operatorname{vol}\mathrm{U}_N(\mathbb{F}))^2\, \widehat{I}_N^{(\beta)}(R), \tag{2.19}$$

where

$$\widehat{I}_N^{(\beta)}(R) = \frac{1}{N!} \int\limits_{\sigma_l>0\,:\,\sum_{j=1}^N \sigma_j^2 \leqslant R^2} \delta\left(1-\prod_{l=1}^N \sigma_l\right) \prod_{1\leqslant j<k\leqslant N} |\sigma_j^2-\sigma_k^2|^\beta \,\mathrm{d}\sigma_1\cdots\mathrm{d}\sigma_N. \tag{2.20}$$

The integral $\widehat{I}_N^{(\beta)}(R)$ was evaluated in [12, Prop. 2.9] for $\beta = 1$, according to a strategy that extends to general β.

Proposition 5. *For* $c > 0$ *we have*

$$\widehat{I}_N^{(\beta)}(R) = \frac{R^{\beta N(N-1)}}{2^N N!} \prod_{j=1}^N \frac{\Gamma(1+\beta j/2)}{\Gamma(1+\beta/2)} \frac{1}{2\pi\mathrm{i}} \int\limits_{c-\mathrm{i}\infty}^{c+\mathrm{i}\infty} \frac{\prod_{j=1}^N \Gamma\left(s/2+\beta(N-j)/2\right)}{\Gamma\left(sN/2+\beta N(N-1)/2+1\right)} R^{sN}\,\mathrm{d}s. \tag{2.21}$$

Proof. First introduce

$$K_N^{(\beta)}(r,t) = \frac{1}{N!}\int_0^\infty \mathrm{d}\sigma_1 \cdots \int_0^\infty \mathrm{d}\sigma_N\, \delta\left(r^2 - \sum_{p=1}^N \sigma_p^2\right) \delta\left(t - \prod_{l=1}^N \sigma_l\right) \prod_{1\leqslant j<k\leqslant N} |\sigma_j^2 - \sigma_k^2|^\beta$$

so that

$$\widehat{I}_N^{(\beta)}(R) = 2\int_0^R K_N^{(\beta)}(r,t)\Big|_{t=1}\, r\,\mathrm{d}r. \tag{2.22}$$

Forming the Mellin transform with respect to t shows, after minor manipulation including the change of variables $\sigma_l^2 = x_l$, that

$$\begin{aligned}&\int_0^\infty K_N^{(\beta)}(r,t)t^{s-1}\,\mathrm{d}t \\ &\quad = \frac{r^{\beta N(N-1)+sN-2}}{2^N N!}\int_{\mathbb{R}_+^N} \delta\left(1 - \sum_{p=1}^N x_p\right)\prod_{l=1}^N x_l^{s/2-1} \prod_{1\leqslant j<k\leqslant N} |x_k - x_j|^\beta\,\mathrm{d}x_1\cdots\mathrm{d}x_N.\end{aligned}$$

The multidimensional integral in this expression is closely related to the Selberg integral, and has the known evaluation in terms of gamma functions [43], [12, Eq. (4.154)]. Substituting this, then integrating both sides over $r \in (0,R)$ shows

$$\begin{aligned}&\int_0^\infty \left(2\int_0^R K_N^{(\beta)}(r,t) r\,\mathrm{d}r\right) t^{s-1}\,\mathrm{d}t \\ &\quad = \frac{R^{sN+\beta N(N-1)}}{2^N N!\Gamma\left(sN/2+\beta N(N-1)/2+1\right)}\prod_{j=1}^N \frac{\Gamma\left(s/2+\beta(N-j)/2\right)\Gamma(1+\beta j/2)}{\Gamma(1+\beta/2)}.\end{aligned}$$

The stated result (2.21) now follows by taking the inverse Mellin transform and setting $t=1$. □

Corollary 6. *As* $R\to\infty$

$$\widehat{I}_N^{(\beta)}(R) = \widehat{C}_N^{(\beta)} R^{\beta N(N-1)} + \mathrm{O}\left(\begin{cases} R^{N(N-2)}, & \beta = 1 \\ R^{2N(N-2)}\log R, & \beta = 2 \\ R^{4N(N-1)-2N}, & \beta = 4, \end{cases}\right), \tag{2.23}$$

where

$$\widehat{C}_N^{(\beta)}(R) = \frac{2}{2^N\Gamma\left(\beta N(N-1)/2+1\right)}\frac{1}{\Gamma(\beta N/2)}\prod_{j=1}^N \frac{\Gamma^2(\beta j/2)}{\Gamma(\beta/2)}, \tag{2.24}$$

and

$$\operatorname{vol} D_R^{\|\cdot\|_F}(\mathrm{SL}_N(\mathbb{F})) = \frac{\pi^{\beta(N^2-1)/2}\Gamma(\beta/2)}{\Gamma(\beta N/2)\Gamma\left(\beta N(N-1)/2+1\right)} R^{\beta N(N-1)} + \mathrm{O}\left(\begin{cases} R^{N(N-2)}, & \beta = 1 \\ R^{2N(N-2)}\log R, & \beta = 2 \\ R^{4N(N-1)-2N}, & \beta = 4. \end{cases}\right). \tag{2.25}$$

Proof. We proceed in an analogous way to the proof of Corollary 3, and begin by shifting the contour to the line parallel to the imaginary axis with $c = -c_\beta - \epsilon$, $\epsilon > 0$ with $c_\beta = 1$ for $\beta = 1$ and $c_\beta = 2$ for $\beta = 2$ and 4. According to the residue theorem, this changes the value of the integral by $2\pi i$ times the sum of the residue at $s = 0$ and $s = -c_\beta$. The residue at $s = 0$ gives the leading terms, and that at $s = -c_\beta$ the leading correction. The large R form of the integrand along the shifted contour shows that the order of the leading correction is a bound on the error term. This establishes (2.23); (2.25) then follows from (2.19). □

Remark 7. The leading terms in (2.18) and (2.25) are equal for $N = 2$, giving in the case $\beta = 2$ for example

$$\operatorname{vol} D_R^{\|\cdot\|}(\mathrm{SL}_2(\mathbb{F})) = \frac{\pi^3}{2} R^4 + \mathrm{O}(\log R), \tag{2.26}$$

but for $N > 2$ (2.25) is smaller, in keeping with the truncation of the integration domain in going from (2.11) to (2.20).

As commented in the Introduction, one interest in the asymptotic volume formulas (2.18) and (2.23) lies in asymptotic counting formulas of the type (1.3). For example, as a natural extension of (1.3), one might expect[1] that

$$\#\{\gamma : \gamma \in \mathrm{SL}_N(\mathbb{Z}[i]),\ \|\gamma\| \leqslant R\} \underset{R\to\infty}{\sim} \frac{1}{\operatorname{vol}\left(\mathrm{SL}_N(\mathbb{C})/\mathrm{SL}_N(\mathbb{Z}[i])\right)} \int\limits_{G\in \mathrm{SL}_N(\mathbb{C}):\|G\|\leqslant R} (\mathrm{d}G), \tag{2.27}$$

where $\mathbb{Z}[i]$ denotes the Gaussian integers. In fact a general asymptotic counting theorem for lattice subgroups of topological groups, implying (2.27), can be found in [19, Th. 1.5], as cited in the recent work [10]. The leading asymptotics of the integral over G is given by (2.18) with $\beta = 2$ for $\|\cdot\| = \|\cdot\|_{\mathrm{Op}}$ and by (2.23) with $\beta = 2$ for $\|\cdot\| = \|\cdot\|_F$.

[1] F. Calegari (private correspondence) remarks that in the context of [8], or also Eskin–McMullen, [11, Theorem 1.4], the basic point is that the $\mathbb{Z}[i]$ points of a semi-simple group G (like SL_n) are the $\mathbb{Z}$ points of another group $G' = \mathrm{Res}_{\mathbb{Q}(i)/\mathbb{Q}}(G)$ (the Weil restriction of scalars), so one can apply these theorems to G' to show that counting problem in G in the ring of integers of some (any) number field reduces to a volume calculation.

It remains then to compute $\mathrm{vol}\,(\mathrm{SL}_N(\mathbb{C})/\mathrm{SL}_N(\mathbb{Z}[i])$ in the same normalisation as that used to compute $\int_{G\in \mathrm{SL}_N(\mathbb{C}):\|G\|\leqslant R}(\mathrm{d}G)$. In relation to (1.3) it was shown in [8] that

$$\mathrm{vol}\,(\mathrm{SL}_N(\mathbb{R})/\mathrm{SL}_N(\mathbb{Z})) = \zeta(2)\zeta(3)\cdots\zeta(N), \tag{2.28}$$

where $\zeta(s)$ denotes the Riemann zeta function (see also [18]). A result of Siegel [33] gives that for a certain non-arithmetic constant A, depending on the normalisation of the measure,

$$\mathrm{vol}\,(\mathrm{SL}_N(\mathbb{C})/\mathrm{SL}_N(\mathbb{Z}[i]) = A\zeta_{\mathbb{Z}[i]}(2)\,\zeta_{\mathbb{Z}[i]}(3)\,\cdots\,\zeta_{\mathbb{Z}[i]}(N). \tag{2.29}$$

Here $\zeta_{\mathbb{Z}[i]}(s)$ denotes the Dedekind zeta function for the Gaussian integers,

$$\zeta_{\mathbb{Z}[i]}(s) = \frac{1}{4}\sum_{(m,n)\neq(0,0)}\frac{1}{(m^2+n^2)^s} = \zeta(s)\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{(2n-1)^s}, \tag{2.30}$$

where the second equality is a well known factorisation; see e.g. [1]. For future reference we note that for $s=2$ this gives

$$\zeta_{\mathbb{Z}[i]}(2) = \zeta(2)\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{(2n-1)^2} = \frac{\pi^2}{6}C, \tag{2.31}$$

where

$$C = \sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{(2n-1)^2}$$

denotes Catalan's constant. In Remark 13 below, we will show that in the same normalisation as used to compute the integral over $G\in \mathrm{SL}_N(\mathbb{C})$, for $N=2$ (2.29) holds with $A=1$.

3. The Lagrange–Gauss algorithm – the real case

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.

3.1. Vector recurrence and shortest reduced basis

Let $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_0\}$ with $\|\mathbf{b}_1\| \leqslant \|\mathbf{b}_0\|$ 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 $B \in \mathrm{SL}_2^{\pm}(\mathbb{R})$. Similarly with $V = [\boldsymbol{\alpha}\, \boldsymbol{\beta}]$ we have $V \in \mathrm{SL}_2^{\pm}(\mathbb{R})$. The matrices B and V are related by

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

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

$$M = M_1 M_2 \cdots M_{r^*}, \quad M_i = \begin{bmatrix} -m_i & 1 \\ 1 & 0 \end{bmatrix} (m_i \in \mathbb{Z}) \tag{3.2}$$

(in fact for B chosen with invariant measure, M samples from $\mathrm{SL}_2^{\pm}(\mathbb{Z})$, with a restriction on the size of the matrix norm, uniformly; see [28]). Defining

$$B_{j+1} = B_j \begin{bmatrix} -m_j & 1 \\ 1 & 0 \end{bmatrix}, \quad B_1 = B = [\mathbf{b}_1\, \mathbf{b}_0], \tag{3.3}$$

the first column of B_j is the second column of B_{j+1} so that we can now set

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

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

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

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

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

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 $m_{j+1} \neq 0$; see e.g. [2].

Lemma 8. *Suppose $m_{j+1} \neq 0$. We have*

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

Proof. Generally

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

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

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

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

$$\left\lceil \frac{\mathbf{b}_j \cdot \mathbf{b}_{j+1}}{\|\mathbf{b}_j\|^2} \right\rfloor = \left\lceil \frac{\|\mathbf{b}_{j+1}\|^2}{\|\mathbf{b}_j\|^2} \frac{\mathbf{b}_j \cdot \mathbf{b}_{j+1}}{\|\mathbf{b}_{j+1}\|^2} \right\rfloor, \tag{3.10}$$

we conclude that if $m_{j+1} \neq 0$ then (3.7) holds, as required. □

Since the vectors in $\mathcal{L}$ with length less than some value R form a finite set, Lemma 8 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 $\|\mathbf{b}_r\| \geqslant \|\mathbf{b}_{r-1}\|$, the algorithm stops with $r^* = r - 1$ in (3.2), and outputs

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

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

$$\boldsymbol{\alpha} = \mathbf{b}_r, \quad \boldsymbol{\beta} = \mathbf{b}_{r+1} \tag{3.12}$$

as the reduced basis. Equivalently, the recurrence (3.2) is iterated until for some $j = r^*$, $\|\boldsymbol{b}_{r^*+1}\| \geq \|\boldsymbol{b}_{r^*}\|$, and the output is the shortest basis $\boldsymbol{\alpha} = \mathbf{b}_{r^*}$ and $\boldsymbol{\beta} = \mathbf{b}_{r^*+1}$.

For both (3.11) and (3.12) it follows from (3.9) with $j = r, r-1$ respectively, and the relative length of $\mathbf{b}_{r+1}, \mathbf{b}_r$ that

$$\|\boldsymbol{\alpha}\| \leqslant \|\boldsymbol{\beta}\|, \quad \left\lceil \frac{\boldsymbol{\alpha} \cdot \boldsymbol{\beta}}{\|\boldsymbol{\alpha}\|^2} \right\rfloor = 0$$

or equivalently

$$\|\boldsymbol{\alpha}\| \leqslant \|\boldsymbol{\beta}\|, \quad \left|\frac{\boldsymbol{\alpha}\cdot\boldsymbol{\beta}}{\|\boldsymbol{\alpha}\|^2}\right| \leqslant \tfrac{1}{2}. \tag{3.13}$$

One observes that the final inequality is equivalent to requiring that

$$\|\boldsymbol{\beta} + n\boldsymbol{\alpha}\| \geqslant \|\boldsymbol{\beta}\|, \quad \forall n \in \mathbb{Z}. \tag{3.14}$$

An alternative way to see (3.14) is to recall that the integer value m_j which minimises (3.4) is given by (3.5), and to apply this with $\mathbf{b}_{j-1} = \boldsymbol{\beta}$, $\mathbf{b}_j = \boldsymbol{\alpha}$, for which $m_j = 0$. Basis vectors which satisfy (3.14), together with the first inequality in (3.13), are said to be greedy reduced in two dimensions [27]. 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 9. *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 [16], which begins with the greedy reduced basis inequalities

$$\|\boldsymbol{\beta} + m\boldsymbol{\alpha}\| \geqslant \|\boldsymbol{\beta}\| \geqslant \|\boldsymbol{\alpha}\|, \quad \forall m \in \mathbb{Z}. \tag{3.15}$$

Let $\mathbf{v} = n_1\boldsymbol{\alpha} + n_2\boldsymbol{\beta}$ be any nonzero element of $\mathcal{L}$. In the case $n_2 = 0$ we have that $\mathbf{v}$ and $\boldsymbol{\alpha}$ are linearly dependent and it is immediate that $\|\mathbf{v}\| \geqslant \|\boldsymbol{\alpha}\|$. In the case $n_2 \neq 0$, write $n_1 = qn_2 + r$ with $q, r \in \mathbb{Z}$ such that

$$0 \leqslant r < |n_2|. \tag{3.16}$$

Then

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

and thus by the triangle inequality

$$\begin{aligned} \|\mathbf{v}\| &\geqslant |n_2|\|\boldsymbol{\beta} + q\boldsymbol{\alpha}\| - r\|\boldsymbol{\alpha}\| \\ &= (|n_2| - r)\|\boldsymbol{\beta} + q\boldsymbol{\alpha}\| + r(\|\boldsymbol{\beta} + q\boldsymbol{\alpha}\| - \|\boldsymbol{\alpha}\|). \end{aligned} \tag{3.17}$$

Now by (3.15), $\|\boldsymbol{\beta} + q\boldsymbol{\alpha}\| - \|\boldsymbol{\alpha}\| \geqslant 0$ and so

$$\|\mathbf{v}\| \geqslant (|n_2| - r)\,\|\boldsymbol{\beta} + q\boldsymbol{\alpha}\| \geqslant \|\boldsymbol{\beta} + q\boldsymbol{\alpha}\|, \tag{3.18}$$

where the second inequality follows from (3.16). Finally, applying (3.15) gives $\|\mathbf{v}\| \geqslant \|\boldsymbol{\beta}\| \geqslant \|\boldsymbol{\alpha}\|$ as required. □

3.2. Complex scalar recurrence

The vector equation (3.6) can also be written in scalar form, albeit involving complex numbers [5]. Thus, set $\mathbf{b}_j = (x_j, y_j)$ and write $b_j = x_j + \mathrm{i}y_j$. The fact that

$$\frac{b_{j-1}}{b_j} = \frac{\mathbf{b}_j \cdot \mathbf{b}_{j-1}}{\|b_j\|^2} + \mathrm{i}\frac{\det B}{\|b_j\|^2}, \quad B = [\mathbf{b}_j\, \mathbf{b}_{j-1}] \tag{3.19}$$

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

$$z_{j+1} = \frac{1}{z_j} - \left\lceil \mathrm{Re}\, \frac{1}{z_j} \right\rfloor. \tag{3.20}$$

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

$$|z| \geqslant 1, \quad |\mathrm{Re}\, z| \leqslant \tfrac{1}{2}. \tag{3.21}$$

The inequalities (3.21) 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. [37]. Starting with $r_1 = b_1/b_0$, $|r_1| < 1$, the recurrence (3.20) is to be iterated until $|r_{j+1}| \geqslant 1$.

As already noted in [14], the Haar measure for $\mathrm{SL}_N(\mathbb{R})$ with $N = 2$ can be parametrised in terms of variables which allow for a seemingly different simplification of the inequalities (3.13), which can in fact be identified with (3.21). The variables of interest come about by writing $V \in \mathrm{SL}_2(\mathbb{R})$ in the form $V = QR$, where Q is a real orthogonal matrix with determinant $+1$ and R is an upper triangular matrix with positive diagonal entries,

$$R = \begin{bmatrix} r_{11} & r_{12} \\ 0 & r_{22} \end{bmatrix}, \quad r_{22} = 1/r_{11}. \tag{3.22}$$

With $V = [\boldsymbol{\alpha}\, \boldsymbol{\beta}]$, the matrix Q can be used to rotate the lattice so that $\boldsymbol{\alpha}$ lies along the positive x-axis. Thus (3.22) gives $\boldsymbol{\alpha} = (r_{11}, 0)$, $\boldsymbol{\beta} = (r_{12}, 1/r_{11})$ and the inequalities (3.13) read

$$r_{12}^2 + r_{22}^2 \geqslant r_{11}^2, \quad 2|r_{12}| \leqslant r_{11}. \tag{3.23}$$

Further, [14, Eq. (4.13)] tells us that the invariant measure, restricted to the fundamental domain of the shortest basis vectors, in the coordinates r_{11} and r_{12} is equal to

$$2\pi\chi_{r_{11}/2\geqslant|r_{12}|\geqslant A_{r_{11}}(r_{11}^2-1/r_{11}^2)^{1/2}}\,\mathrm{d}r_{11}\mathrm{d}r_{12}, \tag{3.24}$$

where $A_r = 1$ for $r \geqslant 1$, $A_r = 0$ otherwise. In relation to (3.20) and (3.21), we should introduce the scaled vector $\frac{1}{|\boldsymbol{\alpha}|}\boldsymbol{\beta} = (r_{12}/r_{11}, 1/r_{11}^2)$ and thus identify $z = r_{12}/r_{11} + \mathrm{i}/r_{11}^2$. The inequalities (3.23) then reduce to (3.21), while changing variables in the invariant measure (3.24) gives

$$\pi\chi_{x^2+y^2>1}\chi_{|x|<1/2}\chi_{y>0}\frac{\mathrm{d}x\mathrm{d}y}{y^2}. \tag{3.25}$$

The factor $\mathrm{d}x\mathrm{d}y/y^2$, in keeping with the remark below (3.21), is familiar as the invariant measure in the upper half plane model of hyperbolic geometry [37].

Distributions for the lengths of $||\boldsymbol{\alpha}||$ and $||\boldsymbol{\beta}||$ can be computed by appropriate integrations over (3.24) and (3.25) [14]. In the present context, the first calculation of this type appears to have been carried out by Shlosman and Tsfasman [32], who computed the distribution of the random variable $\pi/(4y) = \pi r_{11}^2/4$ – this has the interpretation as the sphere (disk) packing density. Integrations with respect to (3.24) are also a feature of exact calculations for the distribution of certain scaled diameters for random $2k$-regular circulant graphs with $k = 2$ [24]; of the study of kinetic transport in the two-dimensional periodic Lorenz gas [23]; and of calculations relating to the asymptotics of certain random linear congruences $\mod p$, as $p \to \infty$ [35], amongst other recent examples.

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

4.1. The complex Lagrange–Gauss algorithm

We seek a generalisation of the Lagrange–Gauss lattice reduction algorithm to the case of lattices in $\mathbb{C}^2$. As a first task, an appropriate generalisation of the integers in the complex plane must be identified. As well as closure under addition and multiplication, inspection of the proof of Proposition 9 tells us that these complex integers should permit a Euclidean algorithm with the absolute value function as norm. This requirement permits the choices

$$\mathbb{Z}[\sqrt{D}] = \{n_1 + n_2\sqrt{D} : n_1, n_2 \in \mathbb{Z}\}, \quad D = -1, -2 \tag{4.1}$$

$$\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{D})\right] = \left\{n_1 + \frac{n_2}{2}(1+\sqrt{D}) : n_1, n_2 \in \mathbb{Z}\right\}, \quad D = -3, -7, -11, \tag{4.2}$$

these being the complex quadratic integers with the desired property [20]. They have been identified in the context of lattice reduction in the earlier work [26]. The case $D = -1$ gives the Gaussian integers, and $D = -3$ the Eisenstein integers. These two cases have been discussed in the context of complex generalisations of the Lagrange–Gauss algorithm in [41,36]. With the complex integers chosen as in (4.1) or (4.2), and $B = \{\mathbf{b}_0, \mathbf{b}_1\}$ a basis in $\mathbb{C}^2$ such that $|\det[\mathbf{b}_0, \mathbf{b}_1]| = 1$ – this requirement restricting the

fundamental unit cell to have unit generalised area, analogous to (1.1) the corresponding lattice is defined as

$$\mathcal{L} = \{m_0\mathbf{b}_0 + m_1\mathbf{b}_1 \,|\, m_0, m_1 \in \mathbb{Z}[w]\}. \tag{4.3}$$

The set $\mathbb{Z}[w]$ with w as in (4.1) and (4.2) forms a lattice in $\mathbb{C}$. Around each lattice point $l \in \mathbb{C}$ is its Voronoi region, consisting of all points in $\mathbb{C}$ closer to l than to the other lattice points. A lattice quantiser $D_{\mathbb{Z}[w]}$ maps 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)

$$D_{\mathbb{Z}[w]}(z) = \operatorname*{argmin}_{\lambda\in\mathbb{Z}[w]} \|\lambda - z\|. \tag{4.4}$$

The lattice corresponding to (4.1) is square for $D = -1$ and rectangular for $D = -2$. The Voronoi region is correspondingly square and rectangular. Because of this

$$D_{\mathbb{Z}[i]}(z) = \lceil \mathrm{Re}\ z \rfloor + \mathrm{i}\lceil \mathrm{Im}\ z \rfloor \tag{4.5}$$

and

$$D_{\mathbb{Z}[\sqrt{2}i]}(z) = \lceil \mathrm{Re}\ z \rfloor + \mathrm{i}\sqrt{2}\left\lceil \mathrm{Im}\ z/\sqrt{2} \right\rfloor. \tag{4.6}$$

The lattices corresponding to (4.2) consist of the disjoint union of two rectangular lattices

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

Denoting these $\mathcal{L}_1, \mathcal{L}_2$ respectively we have

$$\begin{aligned} D_{\mathcal{L}_1}(z) &= \lceil \mathrm{Re}\ z \rfloor + \sqrt{D}\lceil \mathrm{Im}\ z/\sqrt{-D} \rfloor \\ D_{\mathcal{L}_2}(z) &= \lceil \mathrm{Re}(z - 1/2) \rfloor + \sqrt{D}\left\lceil \mathrm{Im}\left(z - \frac{\sqrt{D}}{2}\right)/\sqrt{-D} \right\rfloor + \frac{1+\sqrt{D}}{2} \end{aligned}$$

and so

$$D_{\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{D})\right]}(z) = \operatorname*{argmin}_{\beta\in\{D_{\mathcal{L}_1}(z), D_{\mathcal{L}_2}(z)\}} |\beta - z|. \tag{4.7}$$

In the case $D = -3$ – the Eisenstein integers – the formula (4.7) can be found in [36].

The complex Lagrange–Gauss algorithm proceeds by generalising the working of the real case as presented in Section 3. The equation (3.1) holds with $M \in \mathrm{SL}^{\pm}{}_2(\mathbb{Z}[w])$ and the matrices M_i in (3.2) are now elements of $\mathrm{SL}_2^-(\mathbb{Z}[w])$ with $m_i \in \mathbb{Z}[w]$. To minimise $\|\mathbf{b}_{j+1}\|$ in (3.4) requires

$$m_j = D_{\mathbb{Z}[w]}\left(\frac{\overline{\mathbf{b}}_j \cdot \mathbf{b}_{j-1}}{\|\mathbf{b}_j\|^2}\right) \tag{4.8}$$

and so the analogue of (3.6) reads

$$\mathbf{b}_{j+1} = \mathbf{b}_{j-1} - D_{\mathbb{Z}[w]}\left(\frac{\overline{\mathbf{b}}_j \cdot \mathbf{b}_{j-1}}{\|\mathbf{b}_j\|^2}\right)\mathbf{b}_j. \tag{4.9}$$

Next, we would like to establish the analogue of Lemma 8.

Lemma 10. *Define* $\mathbf{b}_{j+1}$ *by* (4.9)*, and with* m_j *defined by* (4.8)*, suppose* $m_{j+1} \neq 0$*. Then we have the inequality* (3.7)*,* $\|\mathbf{b}_{j+1}\| < \|\mathbf{b}_j\|$*.*

Proof. Generally

$$D_{\mathbb{Z}[w]}(\zeta) = \zeta + r,$$

where r is an element of the Voronoi region of the origin in $\mathbb{Z}[w]$, telling us that

$$D_{\mathbb{Z}[w]}\left(\zeta - D_{\mathbb{Z}[w]}(\zeta)\right) = 0$$

(cf.(3.8)). Choosing $\zeta = \overline{\mathbf{b_j}} \cdot \mathbf{b}_{j-1}/\|\mathbf{b}_j\|^2$, after taking the dot product of both sides of (4.9) with respect to $\overline{\mathbf{b_j}}$ it follows that

$$D_{\mathbb{Z}[w]}\left(\frac{\overline{\mathbf{b}}_j \cdot \mathbf{b}_{j+1}}{\|\mathbf{b}_j\|^2}\right) = 0, \text{ or equivalently } D_{\mathbb{Z}[w]}\left(\frac{\mathbf{b}_j \cdot \overline{\mathbf{b}}_{j+1}}{\|\mathbf{b}_j\|^2}\right) = 0 \tag{4.10}$$

(cf.(3.9)). But from (4.8)

$$m_{j+1} = D_{\mathbb{Z}[w]}\left(\frac{\overline{\mathbf{b}}_{j+1} \cdot \mathbf{b}_j}{\|\mathbf{b}_{j+1}\|^2}\right) = D_{\mathbb{Z}[w]}\left(\frac{\|\mathbf{b}_j\|^2}{\|\mathbf{b}_{j+1}\|^2}\frac{\overline{\mathbf{b}}_{j+1} \cdot \mathbf{b}_j}{\|\mathbf{b}_j\|^2}\right) \tag{4.11}$$

(cf. (3.10)). Comparing (4.11) and (4.10) we see that if $m_{j+1} \neq 0$, then we must have the stated inequality. □

The complex Lagrange–Gauss algorithm terminates with outputs (3.8) or (3.9) depending on the validity of $\|\mathbf{b}_{r+1}\| \geqslant \|\mathbf{b}_r\|$ as in the real case, and the vectors $\boldsymbol{\alpha}, \boldsymbol{\beta}$ satisfying

$$\|\boldsymbol{\alpha}\| \leqslant \|\boldsymbol{\beta}\|, \quad D_{\mathbb{Z}[w]}\left(\frac{\overline{\boldsymbol{\alpha}} \cdot \boldsymbol{\beta}}{\|\boldsymbol{\alpha}\|^2}\right) = 0. \tag{4.12}$$

From the complex analogue of the text below (3.14) we see that the second equation is equivalent to

$$\|\boldsymbol{\beta} + n\boldsymbol{\alpha}\| \geqslant \|\boldsymbol{\beta}\|, \quad \forall n \in \mathbb{Z}[w], \tag{4.13}$$

telling us that $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ is a greedy reduced basis, as in the real case.

The assumption that $\mathbb{Z}[w]$ is a Euclidean domain with the absolute value as norm allows to deduce the complex analogue of Proposition 9.

Proposition 11. *Let $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ be a complex greedy reduced basis, and let $\mathbb{Z}[w]$ be one of (4.1), (4.2). Then $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ is a shortest reduced basis.*

Proof. We follow the proof of Proposition 9, now setting $\mathbf{v} = n_1\boldsymbol{\alpha} + n_2\boldsymbol{\beta}$, $n_1, n_2 \in \mathbb{Z}[w]$. In the case $n_2 \neq 0$, the assumption that $\mathbb{Z}[w]$ is a Euclidean domain with the absolute value as norm allows us to write

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

with

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

Equations (3.17) and (3.18) again hold, with r replaced by $|r|$, implying $\|\mathbf{v}\| \geqslant \|\boldsymbol{\beta}\| \geqslant \|\boldsymbol{\alpha}\|$ as required. □

4.2. Quaternion scalar recurrence

We saw how the real vector equation (3.4) could also be written in the complex scalar form (3.12). Here we will show how the complex vector equation (4.9) can be written in a quaternion scalar form; for the latter recall the definitions at the beginning of §2.1.

Writing a pair of complex basis vectors $\mathbf{b}_l = (w_l, z_l)$, $w_l, z_l \in \mathbb{C}$, define

$$q_l = w_l + \mathrm{j}z_l, \quad |q_l|^2 = |w_l|^2 + |z_l|^2, \tag{4.14}$$

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 (3.12) one can check

$${q_l}^{-1} q_{l-1} = \frac{\overline{\mathbf{b}}_l \cdot \mathbf{b}_{l-1}}{\|\mathbf{b}_l\|^2} + \mathrm{j}\frac{\det V}{\|\mathbf{b}_l\|^2} \tag{4.15}$$

(cf.(3.20)). Another viewpoint on (4.15) is in terms of the so-called Cayley–Dickson doubling formula. Thus for $a, b, c, d \in \mathbb{C}$ define

$$\overline{(a, b)} = (\overline{a}, -b), \qquad (a, b)(c, d) = (ac - d\overline{b}, \overline{a}d + cb). \tag{4.16}$$

Identify $(a, b) = a + \mathrm{j}b$. Then these rules together with $q_l^{-1} q_{l-1} = |q_l|^{-2}\overline{q}_l q_{l-1}$ and $\overline{q}_l = (\overline{a}, -b)$, $q_{l-1} = (c, d)$ together with the fact that complex numbers commute imply (4.15).

Consequently, the complex vector recurrence (4.9), rearranged so that order of multiplication in the last term is reversed (this is in keeping with the unit j in (4.14) being to the left, and thus purely complex multiplication taking place to the right), can be rewritten as the quaternion scalar recurrence

$$q_j^{-1}q_{j+1} = q_j^{-1}q_{j-1} - D_{\mathbb{Z}[w]}\left((\mathrm{Re} + \mathrm{i}\,\mathrm{Im}_i)q_j^{-1}q_{j-1}\right) \tag{4.17}$$

where Im_i denotes the (real) coefficient of i. Now writing $Q_j^{-1} = q_j^{-1}q_{j-1}$ gives the analogue of (3.20),

$$Q_{j+1} = \frac{1}{Q_j} + D_{\mathbb{Z}[w]}\Big((\mathrm{Re} + \mathrm{i}\,\mathrm{Im}_i)\frac{1}{Q_j}\Big). \tag{4.18}$$

4.3. The Gram–Schmidt 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 $V = UT$, where $U \in \mathrm{SU}(2)$ and

$$T = \begin{bmatrix} t_{11} & t_{12}^{(r)} + \mathrm{i}t_{12}^{(i)} \\ 0 & t_{22} \end{bmatrix}, \quad t_{11} > 0,\ t_{22} = 1/t_{11}. \tag{4.19}$$

Recalling the text above (2.7), and making use of the known change of variables from the elements of V to $\{U, T\}$ (see e.g. [12, Prop. 3.2.5]) the invariant measure (2.4) for $N = 2$ can be written

$$\left(\frac{1}{2\pi}\right)\delta(1 - t_{11}t_{22})t_{11}^3 t_{22}\mathrm{d}t_{11}\mathrm{d}t_{22}\mathrm{d}t_{12}^{(r)}\mathrm{d}t_{12}^{(i)}(U^\dagger \mathrm{d}U). \tag{4.20}$$

Also, with $\boldsymbol{\alpha} = (t_{11}, 0)$, $\boldsymbol{\beta} = (t_{12}^{(r)} + \mathrm{i}t_{12}^{(i)}, 1/t_{11})$ the inequalities implied by (4.12) for $w = \mathrm{i}$ read

$$t_{11}^2 \leqslant (t_{12}^{(r)})^2 + (t_{12}^{(i)})^2 + (1/t_{11})^2, \quad 2|t_{12}^{(r)}| \leqslant t_{11}, \quad 2|t_{12}^{(i)}| \leqslant t_{11}. \tag{4.21}$$

Integrating over U using (2.10), and 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

$$(2\pi^2)t_{11}\chi_{t_{11}^2 \leqslant (t_{12}^{(r)})^2 + (t_{12}^{(i)})^2 + (1/t_{11})^2}\chi_{2|t_{12}^{(r)}| \leqslant t_{11}}\chi_{2|t_{12}^{(i)}| \leqslant t_{11}}\mathrm{d}t_{11}\mathrm{d}t_{12}^{(r)}\mathrm{d}t_{12}^{(i)}. \tag{4.22}$$

Now introduce the scaled vector

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

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

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

In these variables the invariant measure (4.22) reads

$$\pi^2 \chi_{x_1^2+x_2^2+x_3^2>1} \chi_{|x_1|\leqslant \frac{1}{2}} \chi_{|x_2|\leqslant \frac{1}{2}} \chi_{x_3>0} \frac{\mathrm{d}x_1 \mathrm{d}x_2 \mathrm{d}x_3}{x_3^3}. \tag{4.23}$$

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.

4.4. Statistics of the shortest reduced basis for the Gaussian integers

In the case of the Gaussian integers, the statistics of the corresponding shortest basis vectors are determined by appropriate integration over (4.22) – 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 $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ we have

$$\frac{\overline{\boldsymbol{\alpha}} \cdot \boldsymbol{\beta}}{\|\boldsymbol{\alpha}\|\|\boldsymbol{\beta}\|} = \frac{t_{12}^{(r)} + \mathrm{i}t_{12}^{(i)}}{\sqrt{(t_{12}^{(r)})^2 + (t_{12}^{(i)})^2 + (1/t_{11})^2}} \tag{4.24}$$

so these variables should be held fixed when computing the corresponding PDF. Integrating (4.22) over all variables gives the volume of the invariant measure (4.20) restricted to the domain (4.21) which occurs in the computation of the PDFs as the normalisation. Our first task is to compute this volume.

Proposition 12. *Let the volume associated with* (4.22) *be denoted* $\mathrm{vol}\,\widehat{\Gamma}$. *We have*

$$\mathrm{vol}\,\widehat{\Gamma} = \frac{2\pi^2}{3} C, \tag{4.25}$$

where C *denotes Catalan's constant as defined above* (2.31).

Proof. For notational convenience in (4.22) we write $t_{11} = t$, $t_{12}^{(r)} = y_1$, $t_{12}^{(i)} = y_2$. Integrating over y_1 and y_2 gives

$$(2\pi^2) t \mathrm{d}t \int \chi_{\|\mathbf{y}\|^2 \geqslant t^2 - 1/t^2} \chi_{|y_1|\leqslant t/2} \chi_{|y_2|\leqslant t/2} \mathrm{d}y_1 \mathrm{d}y_2, \tag{4.26}$$

where $\mathbf{y} = (y_1, y_2)$. Geometrically, the integral here corresponds to the area overlap between the outside of a disk of radius $\sqrt{t^2 - 1/t^2}$ $(t \geqslant 1)$ 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 $2b$, both centred at the origin, (4.26) can be written

$$(2\pi^2)\left(t^3\chi_{0<t<1}+\chi_{t>1}t\left(t^2-V_2\left((t^2-1/t^2)^{1/2},t/2\right)\right)\right)\mathrm{d}t$$
$$=(2\pi^2)\left(t^3\chi_{0<t<1}+\chi_{t>1}t\left(t^2-(t^2-1/t^2)V_2\left(1,\frac{t}{2(t^2-1/t^2)^{1/2}}\right)\right)\right)\mathrm{d}t. \quad (4.27)$$

An elementary exact calculation gives

$$V_2(1,a)=\begin{cases}4a^2, & 0<a<1/\sqrt{2}\\ 4a\sqrt{1-a^2}+4\arcsin a-\pi, & 1/\sqrt{2}<a<1\\ \pi, & 1<a\end{cases} \quad (4.28)$$

(see [29] for an n-dimensional generalisation of this result) thus reducing (4.27) to

$$(2\pi^2)\Big(\chi_{0<t<1}t^3+\chi_{1<t<(4/3)^{1/4}}t(t^2-\pi(t^2-1/t^2))$$
$$+\chi_{(4/3)^{1/4}<t<2^{1/4}}t\left(t^2-(t^2-1/t^2)(4a\sqrt{1-a^2}+4\arcsin a-\pi)|_{a=\frac{t}{2(t^2-1/t^2)^{1/2}}}\right)\Big)\mathrm{d}t. \quad (4.29)$$

Elementary integration and/or use of computer algebra (we used Mathematica) gives for the integral over t

$$\int\chi_{0<t<1}t^3\mathrm{d}t=\frac{1}{4} \quad (4.30)$$
$$\int\chi_{1<t<(4/3)^{1/4}}t(t^2-\pi(t^2-1/t^2))\mathrm{d}t=\frac{1}{12}\left(1+\pi(-1+\log(64/27))\right) \quad (4.31)$$
$$\int\chi_{(4/3)^{1/4}<t<2^{1/4}}t\left(t^2-(t^2-1/t^2)(4a\sqrt{1-a^2}-\pi)|_{a=\frac{t}{2(t^2-1/t^2)^{1/2}}}\right)\mathrm{d}t$$
$$=\frac{1}{12}\left(-4+2\pi-3\pi\log(3/2)-2\sqrt{3}\log(2-\sqrt{3})\right) \quad (4.32)$$
$$\int\chi_{(4/3)^{1/4}<t<2^{1/4}}t^3 4\arcsin\frac{t}{2(t^2-1/t^2)^{1/2}}\mathrm{d}t=\frac{1}{12}\left(-\pi+\sqrt{3}\log(7-4\sqrt{3})\right). \quad (4.33)$$

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

$$J = \frac{C}{3} + \frac{\pi}{4} \log \frac{9}{8}, \tag{4.34}$$

where C denotes Catalan's constant. Adding (4.30)–(4.34) gives $C/3$. Multiplying by $2\pi^2$ as required by (4.26) then gives (4.25). □

Remark 13. In [14] it was shown that the analogue of $\mathrm{vol}\,\hat{\Gamma}$ for lattice reduction in $\mathbb{R}^2$ equals $\pi^2/3$, which is twice the value of $\mathrm{vol}\,\mathrm{SL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{Z})$ as given by (2.28) with $N = 2$. This can be understood since the space of reduced vectors contains the involution $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\} \mapsto \{-\boldsymbol{\alpha}, -\boldsymbol{\beta}\}$, and so maps two-to-one to the fundamental domain of $\mathrm{SL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{Z})$. For the present lattice reduction problem, the mapping from the space of reduced lattice vectors to $\mathrm{SL}_2(\mathbb{C})/\mathrm{SL}_2(\mathbb{Z}[i])$ is four-to-one due to the involutions $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\} \mapsto \{-\boldsymbol{\alpha}, -\boldsymbol{\beta}\}$, $\{\mathrm{i}\boldsymbol{\alpha}, -\mathrm{i}\boldsymbol{\beta}\}$, $\{-\mathrm{i}\boldsymbol{\alpha}, \mathrm{i}\boldsymbol{\beta}\}$. Hence $\mathrm{vol}\,\mathrm{SL}_2(\mathbb{C})/\mathrm{SL}_2(\mathbb{Z}[i]) = \frac{\pi^2}{6} C = \zeta_{\mathbb{Z}[i]}(2)$, where the final equality uses (2.31). It thus follows from (2.26) and (2.27) that

$$\#\{\gamma : \gamma \in \mathrm{SL}_2(\mathbb{Z}[i]),\ ||\gamma|| \le R\} \underset{R\to\infty}{\sim} \frac{3}{\pi C} R^4. \tag{4.35}$$

In the proof of Proposition 12 the expression (4.29) corresponds to integrating (4.22) over $t_{12}^{(r)}$ and $t_{12}^{(i)}$, and thus after normalisation by dividing by (4.25) and removal of $\mathrm{d}t$ corresponds to the PDF of the length of the shortest basis vector.

Proposition 14. *For random complex lattices in $\mathbb{C}^2$, with the defining basis vectors chosen with invariant measure and spanned using the Gaussian integers, the probability density function for the length of the shortest basis vector is equal to*

$$\begin{aligned} \frac{3}{C} \Big\{ & \chi_{0<t<1} t^3 + \chi_{1<t<(4/3)^{1/4}} t(t^2 - \pi(t^2 - 1/t^2)) \\ & + \chi_{(4/3)^{1/4}<t<2^{1/4}} \Big(t^3 - t^3 \sqrt{3 - 4/t^4} + \pi(t^3 - 1/t) \\ & - 4(t^3 - 1/t) \arcsin \frac{t}{2(t^2 - 1/t^2)^{1/2}} \Big) \Big\}. \end{aligned} \tag{4.36}$$

As noted in the opening paragraph of this section, 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 (4.26). Changing variables from t to r and imposing the ordering and sign restriction $t/2 > y_2 > y_1 > 0$ the functional form in (4.22) transform to

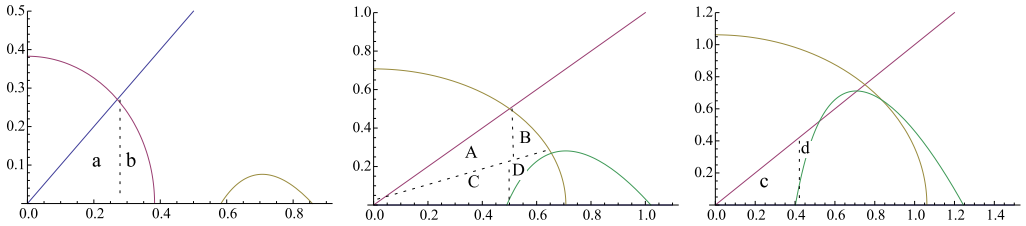

Fig. 4.1. This is a plot in the positive y_1y_2-plane of the regions implied by the inequalities in (4.37) for fixed values of r in the ranges $< r < (4/3)^{1/4}$, $(4/3)^{1/4} < r < 2^{1/4}$ and $r > 2^{1/4}$ respectively. The common intersection of the inequalities corresponds to the labelled regions in each case.

$$(16\pi^2)\frac{r}{(r^2-y_1^2-y_2^2)^2}\chi_{y_1^2+y_2^2<r^2-1/r^2}\chi_{r^2<y_1^2+y_2^2+1/4y_1^2}\chi_{0<y_1<y_2}\,\mathrm{d}r\mathrm{d}y_1\mathrm{d}y_2. \tag{4.37}$$

Integrating over y_1 and y_2 and normalisation by (4.25) gives the explicit form of the corresponding PDF.

Proposition 15. *In the setting of Propositions 12 and 14, the PDF for the length of the second shortest basis vector is equal to*

$$\begin{aligned}
&\frac{3}{C}\Bigg\{\chi_{1<r<(4/3)^{1/4}}\pi\frac{r^4-1}{r}+\chi_{(4/3)^{1/4}<r<2^{1/4}}\\
&\quad\times\left(2r\sqrt{3r^4-4}+\frac{4(r^4-1)}{r}\left(\arctan\frac{r^2}{\sqrt{3r^4-4}}\right.\right.\\
&\quad\left.\left.+\arctan\frac{r^2\sqrt{3r^4-4}-2r^4+2}{r^4-2}-\frac{\pi}{2}\right)\right)\\
&\quad+\chi_{r>2^{1/4}}\left(2r(r^2-\sqrt{r^4-2})+\frac{4(r^4-1)}{r}\left(\arctan\frac{r^2+\sqrt{r^4-2}}{r^2-\sqrt{r^4-2}}-\frac{\pi}{2}\right)\right)\Bigg\}.
\end{aligned} \tag{4.38}$$

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 (4.37); see Fig. 4.1.

The regions satisfying all the inequalities have been divided into subregions $a,\dots,d$, $A,\dots,D$, 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 $r > 2^{1/4}$

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

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 (4.37). The resulting integrals can all be computed explicitly. Multiplying the result by $16\pi^2 r$ as also required by (4.37), and normalising by (4.25) we obtain (4.38). □

Remark 16. Expanding (4.38) for large r one obtains with the help of computer algebra

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

Multiplying by $\mathrm{d}r$ to obtain the corresponding probability measure, then changing variables $s = 1/r$, the resulting PDF thus has for its leading term in the small s expansion $3s^3/C$. This coincides with the small t behaviour of the PDF for the shortest vector (4.36), and in particular has the same functional dependence on the arithmetic constant C.

In the case of lattice reduction applied to bases chosen with invariant measure from $\mathrm{SL}_2(\mathbb{R})$, one can deduce from [14, Eq. (4.16)] that for large s the PDF for the distribution of the second shortest basis vector has the large s expansion $(12/(\pi s))(1/(2s^2)+1/(8s^6)+\cdots)$. In the variable $\tilde{s} = 1/s$, the leading term in the $\tilde{s} \to 0$ expansion of the transformed PDF is thus $6\tilde{s}/\pi$. This is precisely the form of the PDF of the shortest lattice vector in the range $0 < s < 1$ [14, Eq. (4.15)], analogous to what was just exhibited in relation to (4.38) and (4.36). Such a property to be expected, as the volume of the unit cell must be unity, and in the case of one very short vector, and one very long vector, the volume to leading order will just be the product of the lengths, telling us that such vectors are equal in number.

The final quantity to be considered is the complex analogue of the cosine of the angle between the shortest reduced basis vectors (4.24). We write

$$\xi_R = \frac{t_{12}^{(r)}}{\sqrt{(t_{12}^{(r)})^2 + (t_{12}^{(i)})^2 + 1/t_{11}^2}}, \quad \xi_I = \frac{t_{12}^{(i)}}{\sqrt{(t_{12}^{(r)})^2 + (t_{12}^{(i)})^2 + 1/t_{11}^2}}. \tag{4.39}$$

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

Proposition 17. *The variables ξ_R, ξ_I specified by (4.39) have joint distribution with PDF equal to*

$$-\frac{3}{C}\frac{\log 4\max(|\xi_R|^2, |\xi_I|^2)}{4(1-\xi_R^2-\xi_I^2)^2} \tag{4.40}$$

supported on

$$\max(|\xi_R|^2, |\xi_I|^2) \leqslant 1/4. \tag{4.41}$$

Proof. It follows from (4.39) 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 $(t_{12}^{(r)}, t_{12}^{(i)}) =: (t_{12}, s_{12})$ to (ξ_R, ξ_I) is thus

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

The functional form in (4.22) thus transforms to

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

Integration over t_{11} in this expression is elementary, and after dividing by the normalisation (4.25) the PDF (4.40) results. □

Corollary 18. *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*

$$-\frac{6\xi}{C(1-\xi^2)^2}\left(\chi_{0<\xi<1/2}\left(\frac{\pi}{2}\log\xi + C\right) + \chi_{1/2<\xi<1/\sqrt{2}}\int_{\arccos(1/2\xi)}^{\pi/4}\log(4\xi^2\cos^2\theta)\mathrm{d}\theta\right). \tag{4.42}$$

Proof. The Jacobian for the change of variables to polar coordinates is $d\xi_R d\xi_I = \xi d\xi d\theta$. For $0 < \xi < 1/2$, the inequality (4.41) is valid for all $0 < \theta < 2\pi$, and the integral over θ in (4.40) is equal to

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

which after multiplication by ξ evaluates to the first case in (4.42). For $1/2 < \xi < 1/\sqrt{2}$, and restricting θ to the range $0 < \theta < \pi/4$, the inequality (4.41) is valid for $\arccos(1/2\xi) < \theta < \pi/4$, and this implies the second case in (4.42). □

In [14, 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 [34] 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 [34] applies to the case of real lattices, but the more general statement of the mean value theorem by Weil [39] (for a clear statement of the latter, see [25, Th. 3]) removes this requirement, and in particular allows the case of a complex lattice to be considered.

The corollary of the mean value theorem of interest is the requirement that the expected number of vectors in the punctured complex disk of radius R, $\Omega(R)$, be equal to the volume of the disk. The latter, corresponding to the set $|w|^2 + |z|^2 < R^2$, $w, z, \in \mathbb{C}$ is equal to the volume of a ball of radius R in $\mathbb{R}^4$, which has value $\frac{\pi^2}{2} R^4$, so as a consequence of the mean value theorem we must have

$$\Omega(R) = \frac{\pi^2}{2} R^4. \tag{4.43}$$

On the other hand, in light of Propositions 14 and 17 together, for $R < 1$ the punctured complex disk of radius R will only contain certain Gaussian integer multiples of the shortest lattice vector $\boldsymbol{\alpha}$: $m\boldsymbol{\alpha}$, $m \in \mathbb{Z}[i]$ with $|m|\,||\boldsymbol{\alpha}|| < R$, $(m \neq 0)$. Define $||\boldsymbol{\alpha}||/R = s$, and define $N_{\mathbb{Z}[i]}(p)$ to be the number of Gaussian integers with *square* norm less than or equal to p. Use of (4.36) for $t < 1$ shows that for $R < 1$

$$\begin{aligned} \Omega(R) &= \frac{3}{C} R^4 \sum_{p=1}^{\infty} N_{\mathbb{Z}[i]}(p) \int_{(1/(p+1))^{1/2}}^{(1/p)^{1/2}} s^3 \, ds \\ &= \frac{3R^4}{4C} \sum_{p=1}^{\infty} N_{\mathbb{Z}[i]}(p) \Big(\frac{1}{p^2} - \frac{1}{(p+1)^2} \Big) = \frac{3R^4}{4C} \sum_{p=1}^{\infty} \frac{M_{\mathbb{Z}[i]}(p)}{p^2}, \end{aligned} \tag{4.44}$$

where $M_{\mathbb{Z}[i]}(p) := N_{\mathbb{Z}[i]}(p) - N_{\mathbb{Z}[i]}(p-1)$ specifies the number of Gaussian integers with square norm equal to p. In the notation (2.31) we have

$$\sum_{p=1}^{\infty} \frac{M_{\mathbb{Z}[i]}(p)}{p^2} = 4\zeta_{\mathbb{Z}[i]}(2) = 4\frac{\pi^2}{6} C,$$

which substituted in (4.44) reclaims (4.43).

4.5. The case of Eisenstein integers

For the choices of w as equal to $\frac{1}{2}(1+\sqrt{D})$ for $D=-3,-7,-11$ as in (4.2) the domain specified by the second condition in (4.12) is a hexagon rather than a square ($D=-1$), or rectangle ($D=-2$) in the coordinates $X=t_{12}^{(r)}/t_{11}$, $Y=t_{12}^{(i)}/t_{11}$. Specifically, for $D=-3$ the hexagon has vertices at

$$\left(0,\frac{1}{\sqrt{3}}\right),\left(\frac{1}{2},\frac{1}{2\sqrt{3}}\right),\left(\frac{1}{2},-\frac{1}{2\sqrt{3}}\right),\left(0,-\frac{1}{\sqrt{3}}\right),\left(-\frac{1}{2},-\frac{1}{2\sqrt{3}}\right),\left(-\frac{1}{2},\frac{1}{2\sqrt{3}}\right) \tag{4.45}$$

and is thus a regular hexagon with side length $1/\sqrt{3}$, centred at the origin and with two sides parallel to the y-axis. In terms of inequalities, this hexagon is specified by the requirements that

$$|X|<\frac{1}{2},\qquad \sqrt{3}|Y|+|X|<1. \tag{4.46}$$

Using the variables $\{t_{11},X,Y\}$ the analogue of (4.22) for the invariant measure restricted to the domain of the shortest reduced basis is the expression

$$(2\pi^2)t_{11}^3\chi_{1-1/t_{11}^4\leqslant X^2+Y^2}\chi_{(X,Y)\in\mathcal{H}}\mathrm{d}t_{11}\mathrm{d}X\mathrm{d}Y, \tag{4.47}$$

where $\mathcal{H}$ denotes the above specified regular hexagon.

Analogous to the computation of (4.36), the statistics of the shortest reduced basis can be obtained by appropriate integration over (4.47). We begin with the normalisation, obtained by integrating (4.47).

Proposition 19. *Let the volume associated with* (4.47) *be denoted* $\mathrm{vol}\,\widehat{\Gamma}_{\mathcal{H}}$. *We have*

$$\mathrm{vol}\,\widehat{\Gamma}_{\mathcal{H}}=\frac{\pi}{2}\log 2-\frac{3\pi}{8}\log 3+\frac{3}{2}\left(\mathrm{Im}\,L_2\left(\frac{3-i\sqrt{3}}{6}\right)+\mathrm{Im}\,L_2\left(\frac{3+i\sqrt{3}}{4}\right)\right), \tag{4.48}$$

where

$$L_2(z)=\sum_{n=1}^{\infty}\frac{z^n}{n^2} \tag{4.49}$$

is the dilogarithm function.

Proof. For $t_{11}>1$ the inequalities in (4.47) correspond to the overlap between the regular hexagon $\mathcal{H}$ with vertices (4.45) and the outside of a circle of radius $1-1/t_{11}^4$. For $0<t_{11}<1$ the first inequality is always valid, and the remaining factor $\chi_{(X,Y)\in\mathcal{H}}$ is the indicator function of the hexagon. Noting that $\mathcal{H}$ has area $\sqrt{3}/2$ shows that integration over X and Y in (4.47) gives the function of t

$$\chi_{0<t<1} t^3 \frac{\sqrt{3}}{2} + \chi_{t>1} t^3 \left(\frac{\sqrt{3}}{2} - V^{\mathcal{H}d}\left((1 - 1/t^4)^{1/2} \right) \right), \tag{4.50}$$

where $V^{\mathcal{H}d}(a)$ is the area of overlap between the hexagon $\mathcal{H}$ and a disk of radius a centred at the origin.

Elementary considerations give

$$V^{\mathcal{H}d}(a) = \begin{cases} \pi a^2, & 0 < a < 1/2, \\ \pi a^2 - 6a^2 \arctan(4a^2 - 1)^{1/2} + \frac{3}{2}(4a^2 - 1)^{1/2}, & 1/2 < a < 1/\sqrt{3}, \\ \frac{\sqrt{3}}{2}, & a > 1/\sqrt{3}. \end{cases} \tag{4.51}$$

If we write

$$\operatorname{vol} \widehat{\Gamma}_{\mathcal{H}} = V_1 + V_2, \quad V_2 = -6 \int_{(4/3)^{1/4}}^{(3/2)^{1/4}} \frac{1}{t} \arctan \left(3 - \frac{4}{t^4} \right)^{1/2} \mathrm{d}t$$

then the integral over t specifying V_1 as implied by (4.50) and (4.51) can either be done by elementary computation or the use of computer algebra and gives

$$V_1 = \frac{\pi}{4} \log \frac{3}{2}. \tag{4.52}$$

For the integral defining V_2 straightforward changes of variables give

$$\begin{aligned} V_2 &= -\frac{3}{2} \int_0^{1/\sqrt{3}} \frac{2s}{3 - s^2} \arctan s \, \mathrm{d}s \\ &= \frac{\pi}{4} \log \frac{8}{3} - \frac{3}{2} \int_0^{1/\sqrt{3}} \frac{\log(3 - s^2)}{1 + s^2} \, \mathrm{d}s \\ &= 3\pi \log 2 - \frac{5\pi}{8} \log 3 + \frac{3}{2} \left(\operatorname{Im} L_2 \left(\frac{3 - i\sqrt{3}}{6} \right) + \operatorname{Im} L_2 \left(\frac{3 + i\sqrt{3}}{4} \right) \right), \end{aligned} \tag{4.53}$$

where the second equality uses integration by parts, and the third computer algebra; in the latter $L_2(z)$ is the dilogarithm function. Adding (4.52) and (4.53) gives the first line on (4.48). □

The volume (4.48), obtained by direct integration, can be written in a simpler form by adopting instead an indirect approach using Siegel's mean value theorem.

Proposition 20. *An alternative evaluation of the volume in Proposition 19 is*

$$\operatorname{vol}\widehat{\Gamma}_{\mathcal{H}} = \frac{1}{4}\operatorname{Im} L_2\left(\frac{1+i\sqrt{3}}{2}\right). \tag{4.54}$$

Proof. According to (4.50), for $0 < t < 1$ the PDF of the shortest vector is $\frac{1}{\operatorname{vol}\widehat{\Gamma}_{\mathcal{H}}}\frac{\sqrt{3}}{2}t^3$. Siegel's mean value theorem [34], generalised by Weil [39] to apply in the present setting, has the consequence that the expected number of lattice points in a (complex) disk of radius R is equal to the area of that disk (this assumes a unit normalisation of the volume associated with the integers; see below).

Repeating the considerations which led to (4.44) we obtain

$$\Omega(R) = \frac{R^4}{\operatorname{vol}\widehat{\Gamma}_{\mathcal{H}}}\Big(\frac{\sqrt{3}}{2}\Big)\frac{1}{4}\sum_{\substack{(m,n)\in\mathbb{Z}^2\\(m,n)\neq(0,0)}}\frac{1}{((m+n/2)^2+n^2(3/4))^2}.$$

As an analytic function in s one has (see e.g. [1, Eq. (1.4.16)])

$$\sum_{\substack{(m,n)\in\mathbb{Z}^2\\(m,n)\neq(0,0)}}\frac{1}{((m+n/2)^2+n^2(3/4))^s} = \sum_{\substack{(m,n)\in\mathbb{Z}^2\\(m,n)\neq(0,0)}}\frac{1}{(m^2+mn+n^2)^s} = 6\zeta(s)g(s),$$

where $\zeta(s)$ denotes the Riemann zeta function and

$$g(s) = 1 - 2^{-s} + 4^{-s} - 5^{-s} + 7^{-s} - \cdots = \frac{2}{\sqrt{3}}\operatorname{Im}\operatorname{Li}_s(e^{2\pi i/3}),$$

Li_s denoting the polylogarithm function. For $s = 2$ (dilogarithm case) the duplication formula $\operatorname{Li}_2(z^2) = 2(\operatorname{Li}_2(z) + \operatorname{Li}_2(-z))$ implies $\operatorname{Im}\operatorname{Li}_s(e^{2\pi i/3}) = \frac{2}{3}\operatorname{Im}\operatorname{Li}_s(e^{\pi i/3})$ and so substituting (4.54) we see the latter is valid provided

$$\Omega(R) = \Big(\frac{4}{3}\Big)\Big(\frac{\pi^2R^4}{2}\Big). \tag{4.55}$$

This is a factor $\frac{4}{3}$ bigger than (4.43). To understand this, we note that as a lattice in $\mathbb{R}^2$, $\mathbb{Z}[i]$ has unit cells of area 1, while $\mathbb{Z}(\frac{1}{2}+i\sqrt{3})$ has unit cells of area $\frac{\sqrt{3}}{2}$. The latter creates a scale factor which when raised to the power of d (the (complex) dimension of the lattice; here $d = 2$) should be included in the meaning of $\Omega(R)$ (for a real lattice, choosing even integers rather than integers best illustrates this point), thus implying (4.55). □

The (un-normalised) PDF for the length of the shortest basis vector is given by (4.50). Normalising by (4.54) and substituting (4.51) allows us to specify the analogue of Proposition 14 in the case of the Eisenstein integers.

Proposition 21. *For random complex lattices in $\mathbb{C}^2$, with the defining basis vectors chosen with invariant measure and the lattice formed using the Eisenstein integers, the PDF for the length of the shortest basis vector is equal to*

$$\frac{1}{\operatorname{vol}\widehat{\Gamma}_{\mathcal{H}}}\Big\{\chi_{0<t<1}t^3\frac{\sqrt{3}}{2}+\chi_{1<t<(4/3)^{1/4}}t^3\left(\frac{\sqrt{3}}{2}-\pi\left(1-\frac{1}{t^4}\right)\right)$$
$$+\chi_{(4/3)^{1/4}<t<(3/2)^{1/4}}t^3\Big(\frac{\sqrt{3}}{2}-\pi\left(1-\frac{1}{t^4}\right)+6\left(1-\frac{1}{t^4}\right)\arctan\left(3-\frac{4}{t^4}\right)^{1/2}$$
$$-\frac{3}{2}\left(3-\frac{4}{t^4}\right)^{1/2}\Big)\Big\}, \tag{4.56}$$

where $\operatorname{vol}\widehat{\Gamma}_{\mathcal{H}}$ *is given by* (4.54).

We have not attempted to compute the PDF of the second shortest basis vector, due to the complexity of the calculation as evident from the proof of Proposition 14. However, the computation of the joint distribution of

$$\xi_R=\frac{X}{\sqrt{X^2+Y^2+1/t_{11}^4}},\qquad \xi_I=\frac{Y}{\sqrt{X^2+Y^2+1/t_{11}^4}} \tag{4.57}$$

and thus the analogue of Proposition 17 is straightforward.

Proposition 22. *The joint distribution of the variables ξ_R, ξ_I as specified by (4.57) has PDF*

$$-\frac{1}{\operatorname{Im}L_2((1+i\sqrt{3})/2)}\frac{\log\max\left(4|\xi_R|^2,(|\xi_R|+\sqrt{3}|\xi_I|)^2\right)}{(1-\xi_R^2-\xi_I^2)^2}$$

supported on $\max\left(4|\xi_R|^2,(|\xi_R|+\sqrt{3}|\xi_I|^2)\right)\le 1$.

5. The quaternion Lagrange–Gauss algorithm

The definition of the quaternion number system was revised at the beginning of Section 4.2. The Hurwitz integers H are the quaternions (2.1) with each a_i either all integers, or all half integers. Their distinguishing feature from the obvious Lipschitz integers, defined as the quaternions (2.1) with each a_i an integer, is that they allow for a Euclidean algorithm [4]. With $\mathbf{b}_0,\mathbf{b}_1\in\mathbb{H}^2$ we make use of the Hurwitz integers to define the quaternion lattice

$$\mathcal{L}_H=\{m_0\mathbf{b}_0+m_1\mathbf{b}_1\,|\,m_0,m_1\in H\}. \tag{5.1}$$

For notational convenience let us rewrite (2.1) as $a=\sum_{j=0}^3 a_je_j$, $a_j\in\mathbb{R}$, and denote $\operatorname{Re}q=a_0$, $\operatorname{Im}_{e_j}q=a_j$ $(j=1,2,3)$. For $z\in H$ define the lattice quantiser

$$D_H(z) = \operatorname*{argmin}_{\lambda \in H} \|\lambda - z\|. \tag{5.2}$$

We see that analogous to (4.7)

$$D_H(z) = \operatorname*{argmin}_{\beta \in \{D_{H_1}(z), D_{H_2}(z)\}} |\beta - z|$$

where

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

$$D_{H_2}(z) = \lceil \operatorname{Re}(z - 1/2) \rfloor + \frac{1}{2} + \sum_{\nu=1}^{3} e_\nu \left(\lceil \operatorname{Im}_{e_\nu}(z - 1/2) \rfloor + \frac{1}{2} \right).$$

The lattice quantiser is relevant to the formulation of a quaternion Lagrange–Gauss algorithm. Thus the reasoning leading to (4.9) tells us that

$$\mathbf{b}_{j+1} = \mathbf{b}_{j-1} - \mathbf{b}_j \, D_H \left(\frac{\overline{\mathbf{b}}_j \cdot \mathbf{b}_{j-1}}{\|\mathbf{b_j}\|^2} \right) \tag{5.3}$$

(note the order of the multiplication in the final term). We will see below that the analogues of Lemma 8 and Proposition 9 remain true. 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 (4.16) breaks down. This is because to identify the first component of $(\overline{a}, -b)(c, d)$ as specified by (4.16) with a dot product requires that $d\overline{b} = \overline{b}d$ – and thus commutivity – which is not true in general for quaternions.

Iteration of (5.3) typically gives smaller vectors, as known in the real and complex cases from Lemmas 8 and 10.

Lemma 23. *Define m_j by (4.8) with $\mathbb{Z}[w]$ replaced by H. Define $\mathbf{b}_{j+1}$ by (5.3) and suppose the resulting value of m_{j+1} is nonzero. Then*

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

Proof. The same proof as for Lemma 8 suffices. □

As in the analogous setting for lattice reduction in $\mathbb{R}^2$ and $\mathbb{C}^2$, it follows from Lemma 23 that the quaternion Lagrange–Gauss algorithm terminates, and furthermore that the output vectors $\boldsymbol{\alpha}, \boldsymbol{\beta}$ can be chosen to satisfy

$$||\boldsymbol{\alpha}|| \le ||\boldsymbol{\beta}||, \qquad D_H\Big(\frac{\overline{\boldsymbol{\alpha}} \cdot \boldsymbol{\beta}}{||\boldsymbol{\alpha}||^2} \Big) = 0. \tag{5.4}$$

The second of these conditions is equivalent to requiring that

$$||\boldsymbol{\beta} + n\boldsymbol{\alpha}|| \geq ||\boldsymbol{\beta}||, \qquad \forall n \in H$$

(cf. going from (4.12) to (4.13)) and thus $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ is a greedy basis. But we know from the proofs of Propositions 9 and 11 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 9 and 11.

Proposition 24. *Let $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ be a greedy basis for the Hurwitz integer quaternion lattice (5.1). Then $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ is a shortest reduced basis.*

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 $V = UT$ where $U \in \mathrm{SL}_2(\mathbb{H})$ and

$$T = \begin{bmatrix} t_{11}e_0 & t_{12}^0 e_0 + \sum_{l=1}^3 e_l t_{12}^l \\ 0 & t_{22}e_0 \end{bmatrix}, \qquad t_{11} > 0, \quad t_{22} = 1/t_{11}.$$

Since in the Gram–Schmidt basis

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

the conditions (5.4) characterising the shortest basis give

$$1 - 1/t_{11}^4 \leq \sum_{l=0}^3 X_l^2, \qquad D_H\Big(\sum_{l=0}^3 e_l X_l \Big) = 0,$$

where $X_l = t_{12}^l/t_{11}$.

Also, the Jacobian associated with the change of variables to the Gram–Schmidt basis is $t_{11}^7 t_{22}^3$ (see e.g. [12, Ex. 3.2 q.5(i)]). Thus for $\mathbb{F} = \mathbb{H}$ the (normalised) invariant measure (2.4) in the variables $\{t_{11}, t_{22}, \{X_l\}_{l=0}^3\}$ after integrating out over t_{22} reads

$$\frac{1}{\mathrm{vol}\, \Gamma_{4,H}} \chi_{1-1/t_{11}^4 \leq \sum_{l=0}^3 X_l^2} \chi_{D_H(\sum_{l=0}^3 e_l X_l)=0} t_{11}^7 \mathrm{d}t_{11} \prod_{l=0}^3 \mathrm{d}X_l, \tag{5.5}$$

where $\mathrm{vol}\, \Gamma_{4,H}$ is the normalisation.

The functional form of the PDF for the length t say of the shortest basis vector can be read off from (5.5) in the region $t < 1$.

Proposition 25. *Let* $\operatorname{vol}\Gamma_{4,H}$ *be as in (5.5). For* $0 < t < 1$ *the PDF for the length of the shortest basis vector is equal to*

$$\frac{1}{\operatorname{vol}\Gamma_{4,H}}\frac{t^7}{2}. \tag{5.6}$$

Proof. With $t = t_{11}$, for $0 < t < 1$ the first of the two constraints in (5.5) – and the only one involving t, is always valid. Noting that

$$\int \chi_{D_H(\sum_{l=0}^3 e_l X_l)=0} \prod_{l=0}^3 \mathrm{d}X_l = \operatorname{vol} V, \tag{5.7}$$

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 Hurwitz 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 (5.6) follows. □

From the definition of the Hurwitz integers, and the quantiser D_H, the constraint $D_H(\sum_{l=0}^3 e_l X_l) = 0$ can be characterised by the inequalities

$$|X_l| < \frac{1}{2} \quad (l = 0, \dots, 3) \quad \text{and} \quad \sum_{l=0}^3 |X_l| < 1. \tag{5.8}$$

We have not succeeded in extending the method of the proof of Propositions 12 and 19 for a direct calculation of

$$\operatorname{vol}\Gamma_{4,H} = \int \chi_{2^{1/4}>t_{11}>0} \chi_{1-1/t_{11}^4 \le \sum_{l=0}^3 X_l^2} \Big(\prod_{l=0}^3 \chi_{|X_l|\le 1/2} \Big) \chi_{\sum_{l=0}^3 |X_l| \le 1} t_{11}^7 \mathrm{d}t_{11} \prod_{l=0}^3 \mathrm{d}X_l, \tag{5.9}$$

where in obtaining this integral we have used the fact $\operatorname{vol}\Gamma_{4,H}$ is the normalisation in (5.5), and that t_{11} is positive and can be no bigger than $2^{1/4}$. But we can deduce its value, as we now proceed to demonstrate.

First, we remark that the integrand in (5.9) is even in the X_l, and so can be restricted to positive values of these variables provided we multiply by 2^4. Doing this, the change of variables $X_l = x_l/t_{11}$, $t_{11} = u^{1/4}$ shows

$$\operatorname{vol}\Gamma_{4,H} = 4\int \chi_{2>u>0}\chi_{u^{1/2}-u^{-1/2}\le\sum_{l=0}^3 x_l^2}\Big(\prod_{l=0}^3 \chi_{2^{1/4}/2>x_l>0}\chi_{x_l\le u^{1/4}/2}\Big) \times \chi_{\sum_{l=0}^3 x_l\le u^{1/4}}\mathrm{d}u\prod_{l=0}^3 \mathrm{d}x_l. \quad (5.10)$$

This is well suited to approximate numerical evaluation by a Monte Carlo rejection method, which with 10^6 trials gives the estimate 0.105. In fact Siegel's mean value theorem can be used to indirectly compute the exact value.

Proposition 26. *The exact value of the normalisation is*

$$\Gamma_{4,H} = \frac{7\zeta(3)}{80} \approx 0.1051799\cdots \quad (5.11)$$

Proof. Let $\Omega(R)$ denote the expected number of vectors in the punctured quaternion disk of radius R. The fact that as a lattice in $\mathbb{R}^4$, the Hurwitz integers have unit cell of area $\frac{1}{2}$ (recall the proof of Proposition 25) tells us that the appropriate version of Siegel's mean value theorem as generalised by Weil [39] is the statement that

$$\Omega(R) = 2^2\frac{\pi^4 R^8}{24}, \quad (5.12)$$

where $\pi^4R^8/24$ is the volume of the ball of radius R in $\mathbb{R}^8$. The factor of 2^2 is due to the area of the unit cell corresponding to the Hurwitz integers being $1/2$; recall the discussion below (4.55).

On the other hand, starting with (5.6), the considerations which led to (4.44) give

$$\Omega(R) = \frac{R^8}{16\operatorname{vol}\Gamma_{4,H}}\sum_{\mathbf{q}\in H\setminus\{\mathbf{0}\}}\frac{1}{|\mathbf{q}|^8}.$$

With $\zeta(s)$ denoting the Riemann zeta function, results contained in [42] tell us that

$$\sum_{\mathbf{q}\in H\setminus\{\mathbf{0}\}}\frac{1}{|\mathbf{q}|^8} = 21\zeta(3)\zeta(4) = \frac{21\pi^4}{90}\zeta(3)$$

and thus

$$\Omega(R) = \frac{7\pi^4R^8\zeta(3)}{2^5\cdot 3\cdot 5\cdot \operatorname{vol}\Gamma_{4,H}} \quad (5.13)$$

Equating with (5.12) gives (5.11). □

Remark 27. For the PDF of the second shortest basis vector in the real and complex cases, it has been demonstrated in Remark 16 that the asymptotic form for large length s, after the change of variables $s \mapsto 1/s$, is precisely the same as the small-s form of the PDF of the shortest basis vector. Here we will demonstrate this same property for the quaternion case. In (5.5), with the quantiser rewritten according to (5.8), and the change of variables $X_l \mapsto t_{11} X_l$, we set and $\mathbf{X} = (X_0, \dots, X_3)$, and further change variables from t_{11} to $s = (|\mathbf{X}|^2 + 1/t_{11}^2)^{1/2}$ – the length of the second shortest basis vector – to deduce that the PDF of the latter is

$$\frac{1}{\operatorname{vol} \Gamma_{4,H}} \int \chi_{|\mathbf{X}|^2 \le s^2 - 1/s^2} \Big(\prod_{l=0}^{3} \chi_{|\mathbf{X}|^2 + 1/4X_l^2 \ge s^2} \Big) \chi_{|\mathbf{X}|^2 + 1/(\sum_{l=0}^{3} |X_l|)^2 \ge s^2} \frac{s}{(s^2 - |\mathbf{X}|^2)^3} \times \prod_{l=0}^{3} \mathrm{d}X_l. \tag{5.14}$$

Denote

$$\Gamma_1 = \{\mathbf{X} : |\mathbf{X}|^2 \le s^2 - 1/s^2\}, \ \Gamma_2 = \cup_{l=0}^{3} \{\mathbf{X} : |\mathbf{X}|^2 + 1/4X_l^2 \ge s^2\},$$
$$\Gamma_3 = \{\mathbf{X} : |\mathbf{X}|^2 + 1/(\sum_{l=0}^{3} |X_l|)^2 \ge s^2\},$$

and for $\mu = 1, 2$ let

$$D_\mu = \cup_{l=0}^{3} \{\mathbf{X} : |X_l|^2 \le (s^2 - \sqrt{s^4 - 2^{\mu-1}})/2^{2\mu-1}\},$$
$$R_\mu = \{\mathbf{X} : (\sum_{l=0}^{3} |X_l|)^2 \le 4(s^2 - \sqrt{s^4 - 2^{\mu-1}})/2^{2\mu-1}\}.$$

Here D_1 (D_2) results from replacing $|\mathbf{X}|^2$ by $|X_l|^2$ ($2|X_l|^2$) in Γ_2, then solving for $|X_l|^2$. Similarly, R_1 (R_2) results from replacing $|\mathbf{X}|^2$ by $\frac{1}{2}(\sum_{l=0}^{3} |X_l|)^2$ ($(\sum_{l=0}^{3} |X_l|)^2$) respectively. By construction

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

Also, as $s \to \infty$, $\Gamma_2 \subseteq \Gamma_1$ and

$$D_1, D_2 \to \cup_{l=0}^{3} \{X_l : 1/(2s) + \mathrm{O}(1/s^5) \ge |X_l|\}, R_1, R_2 \to \{\mathbf{X} : 1/s + \mathrm{O}(1/s^5) \ge \sum_{l=0}^{3} |X_l|\}.$$

It follows from the above working that for large s the PDF (5.14) has the leading asymptotic form

$$\frac{1}{\operatorname{vol} \Gamma_{4,H}} \frac{1}{s^5} \int \prod_{l=0}^{3} \chi_{|X_l| \le 1/2s} \, \chi_{\sum_{l=0}^{3} |X_l| \le 1/s} \prod_{l=0}^{3} \mathrm{d}X_l.$$

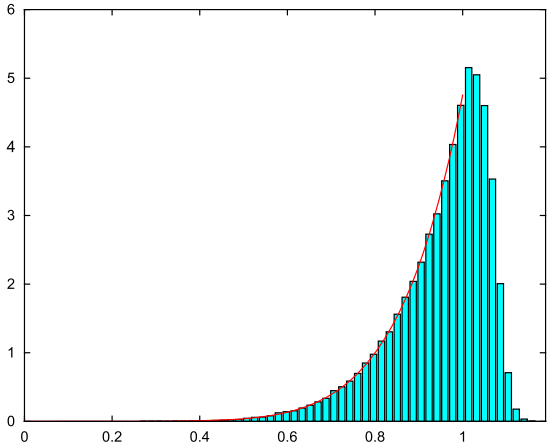

Fig. 5.2. A total of 10^6 matrices were sampled from $\mathrm{SL}_2(\mathbb{H})$ with invariant measure and bound $R = 40$ on the 2-norm. For each, the quaternion Lagrange–Gauss lattice reduction algorithm with respect to the Hurwitz integers has been applied to compute the shortest basis vector $\boldsymbol{\alpha}$. A histogram has been formed for the PDF of $||\boldsymbol{\alpha}||$. In the range $0 < s < 1$ the theoretical prediction (5.6) with $\Gamma_{4,H}$ specified by (5.11) has been superimposed.

Scaling s from the integral, then recognising what remains as (5.7) simplifies this to

$$\frac{1}{2\mathrm{vol}\,\Gamma_{4,H}} \frac{1}{s^9}.$$

Associating this with a measure and thus multiplying by ds, changing variables $s \mapsto 1/s$ we obtain (5.6), which was our claim. As discussed in Remark 16, this can be anticipated from the fact that the area of a unit cell is unity.

In the quaternion case the analogue of the variables (4.39) and (4.57) are the four variables

$$\xi_l = \frac{X_l}{\sqrt{|\mathbf{X}|^2 + 1/t_{11}^4}} \qquad l = 0, \dots, 3.$$

Although we don't give the details, we remark that the joint distribution of these variables can be computed to obtain a PDF analogous to those in Propositions 17 and 22.

Using an extension of the numerical method detailed in [14] the quaternion version of the Lagrange–Gauss algorithm as detailed above has been implemented, allowing for the plotting of a histogram approximating the PDF for the shortest basis vector. As shown in Fig. 5.2 this exhibits excellent agreement with the theoretical prediction (5.6) augmented by (5.11). The numerical methods of [14] have also been appropriately generalised to provide realisations by way of histograms of the PDFs (4.36), (4.38), (4.42) and (4.56). Although we refrain from displaying the results, we remark that again the agreement is excellent.

Acknowledgments

This research project is part of the program of study supported by the ARC Centre of Excellence for Mathematical & Statistical Frontiers. We thank F. Calegari for the footnote made in relation to (2.27). We thank too the referee for a very thorough reading.

References

[1] J.M. Borwein, M.L. Glasser, R.C. McPhedran, J.G. Wan, I.J. Zucker, Lattice Sums Then and Now, Cambridge University Press, Cambridge, 2013.
[2] M.R. Bremner, Lattice Basis Reduction: An Introduction to the LLL Algorithm and Its Applications, CRC Press, Boca Raton, FL, 2012.
[3] J.H. Conway, N.J.A. Sloane, Sphere Packing, Lattices and Groups, 3rd ed., Springer-Verlag, Berlin, New York, 1999.
[4] J.H. Conway, D.A. Smith, On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry, AK Peters Ltd., 2003.
[5] H. Daudé, P. Flajolet, B. Vallée, An average-case analysis of the Gaussian algorithm for lattice reduction, Combin. Probab. Comput. 6 (1997) 397–433.
[6] P. Diaconis, P.J. Forrester, Hurwitz and the origin of random matrix theory in mathematics, Random Matrices Theory Appl. 6 (2017) 1730001.
[7] J.A. Díaz-García, R. Gutiérrex-Jáimez, On Wishart distribution: some extensions, Linear Algebra Appl. 435 (2011) 1296–1310.
[8] W. Duke, Z. Rudnick, P. Sarnak, Density of integer points on affine homogeneous varieties, Duke Math. J. 81 (1993) 143–179.
[9] F.J. Dyson, The three fold way. Algebraic structure of symmetry groups and ensembles in quantum mechanics, J. Math. Phys. 3 (1962) 1199–1215.
[10] D. El-Baz, Spherical equidistribution in adelic lattices and applications, arXiv:1710.07944.
[11] A. Eskin, C. McMullen, Mixing, counting, and equidistribution in Lie groups, Duke Math. J. 71 (1993) 181–209.
[12] P.J. Forrester, Log-Gases and Random Matrices, Princeton University Press, Princeton, NJ, 2010.
[13] P.J. Forrester, Octonions in random matrix theory, Proc. R. Soc. A 473 (2017) 20160800.
[14] P.J. Forrester, Volumes for $\mathrm{SL}_n(\mathbb{R})$, the Selberg integral and random lattices, Found. Comput. Math. (2018), https://doi.org/10.1007/s10208-018-9376-1.
[15] P.J. Forrester, S.O. Warnaar, The importance of the Selberg integral, Bull. Amer. Math. Soc. 45 (2008) 489–534.
[16] S. Galbraith, Mathematics of Public Key Cryptography, Cambridge University Press, Cambridge, 2012.
[17] Y.H. Gan, C. Ling, W.H. Mow, Complex lattice reduction algorithm for low-complexity full-diversity MIMO detection, IEEE Trans. Signal Process. 47 (2009) 2701–2710.
[18] P. Garrett, Volume of $\mathrm{SL}_n(\mathbb{Z})\backslash\mathrm{SL}_n(\mathbb{R})$ and $\mathrm{Sp}_n(\mathbb{Z})\backslash\mathrm{Sp}_n(\mathbb{R})$, web resource http://www-users.math.umn.edu/~garrett/m/v/volumes.pdf.
[19] A. Gorodnik, A. Nevo, The Ergodic Theory of Lattice Subgroups, Ann. of Math. Stud., vol. 172, PUP, Princeton, NJ, 2010.
[20] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, 5th ed., Oxford Science Publications, Oxford, 1979.
[21] A. Hurwitz, Über die Erzeugung der Invarianten durch Integration, Nachr. Ges. Wiss. Gött. (1897) 71–90.
[22] H. Jack, A.M. Macbeath, The volume of a certain set of matrices, Math. Proc. Cambridge Philos. Soc. 55 (1959) 213–223.
[23] J. Marklof, A. Strömbergsson, Kinetic transport in the two-dimensional periodic Lorentz gas, Nonlinearity 21 (2008) 1413–1422.
[24] J. Marklof, A. Strömbergsson, Diameters of random circulant graphs, Combinatorica 33 (2013) 429–466.
[25] M. Morishita, A mean value theorem in adele geometry, Sürikaisekikenkyšho Kökyüroku (1996) 1–11.

[26] H. Napias, A generalization of the LLL-algorithm over Euclidean rings or orders, J. Théor. Nombres Bordeaux 8 (1996) 387–396.
[27] P.Q. Nguyen, D. Stehlé, Low-dimensional lattice basis reduction revisited, in: Algorithmic Number Theory, in: Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, Heidelberg, 2001, pp. 338–357.
[28] I. Rivin, How to pick a random integer matrix? (and other questions), Math. Comput. 85 (2016) 783–797.
[29] C.C. Rousseau, O.G. Ruehr, Problems and solutions, Subsection: The volume of the intersection of a cube and a ball in N-space. Two solutions by Bernd Tibken and Denis Constales, SIAM Rev. 39 (1997) 779–786.
[30] A. Selberg, Bemerkninger om et multipelt integral, Norsk. Mat. Tidsskr. 24 (1944) 71–78.
[31] I. Semaev, A 3-dimensional lattice reduction algorithm, in: P. Huber, M. Rosenblatt (Eds.), Proc. of CALC '01, in: Lecture Notes in Comput. Sci., vol. 2146, Springer-Verlag, 2001, pp. 183–193.
[32] S. Shlosman, M.A. Tsfasman, Random lattices and random sphere packings: typical properties, Mosc. Math. J. 1 (2001) 73–89.
[33] C.L. Siegel, The volume of the fundamental domain for some infinite groups, Trans. Amer. Math. Soc. 39 (1936) 209–218.
[34] C.L. Siegel, A mean value theorem in geometry of numbers, Ann. Math. 46 (1945) 340–347.
[35] A. Strömbergsson, A. Venkatesh, Small solutions to linear congruences and Hecke equidistribution, Acta Arith. 118 (2005) 41–78.
[36] Q.T. Sun, J. Yuan, T. Huang, K.W. Shum, Lattice network codes based on Eisenstein integers, IEEE Signal Process. Mag. 61 (2013) 2713–2725.
[37] A. Terras, Harmonic Analysis on Symmetric Spaces – Euclidean Space, the Sphere, and the Poincaré Upper Half Plane, Springer Science+Business Media, New York, 2013.
[38] S. Vance, Improved sphere packing lower bounds from Hurwitz lattices, Adv. Math. 46 (2011) 340–347.
[39] A. Weil, Sur quelques resultats de Siegel, Summa Bras. Math. 1 (1946) 21–39.
[40] D. Wübben, D. Seethaler, J. Jaldén, G. Matz, Lattice reduction algorithm for low-complexity full-diversity mimo detection, IEEE Signal Process. Mag. 28 (2009) 70–91.
[41] H. Yao, G.W. Wornell, Lattice-reduction-aided detectors for mimo communication systems, in: Proc. IEEE Global Communications Conf., GLOBE-COM, Taipei, Taiwan, Nov. 2002.
[42] I.J. Zucker, Lattice sums in $2, 4, 6$ and 8 dimensions, J. Phys. A 7 (1976) 1568–1575.
[43] K. Zyczkowski, H.-J. Sommers, Induced measures in the space of mixed quantum states, J. Phys. A 34 (2001) 7111–7125.