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)).