

Moments of the number of points in a bounded set for number field lattices

Nihar Gargava, Vlad Serban and Maryna Viazovska

Abstract

We examine the moments of the number of lattice points in a fixed ball of volume V for lattices in Euclidean space which are modules over the ring of integers of a number field K . In particular, denoting by ω_K the number of roots of unity in K , we show that for lattices of large enough dimension the moments of the number of ω_K -tuples of lattice points converge to those of a Poisson distribution of mean V/ω_K . This extends work of Rogers for \mathbb{Z} -lattices. What is more, we show that this convergence can also be achieved by increasing the degree of the number field K as long as K varies within a set of number fields with uniform lower bounds on the absolute Weil height of non-torsion elements.

Contents

1	Introduction	1
1.1	Outline of paper and proof	4
2	Lattices from number fields and integral formula for lifts	5
2.1	Effective higher moment results from lifts of codes	6
2.2	Lattices from reductions	6
3	Convergence of the higher moment formula	10
3.1	Heights of subspaces	11
3.2	Relating the two types of heights	12
3.3	Rational points of bounded height in Grassmannian varieties over number fields	13
4	Towards Poisson distribution	14
4.1	Matrices of type A_m^1	15
5	Upper bounds on moments using Weil heights	18
5.1	Mahler measures and the Bogomolov property	18
5.2	Bounds for contributions from projective space	20
5.3	Summing over ideals	24
5.4	General error estimates for A_m^2 -type terms	27
5.5	General moments using the Bogomolov property	35
6	Odds and ends	38
6.1	No limiting Poisson moments	38
6.2	More general bodies	38
A	Proof of Lemma 15	40
B	Convex combinations lemma	43

1 Introduction

A classical result in the geometry of numbers due to C.L. Siegel [1] establishes a mean value theorem for lattice sum functions $F_f(\Lambda) = \sum_{\lambda \in \Lambda \setminus \{0\}} f(\lambda)$, where $f : \mathbb{R}^t \rightarrow \mathbb{C}$ is integrable and decays sufficiently fast.

More precisely, the space $\mathrm{SL}_t(\mathbb{R})/\mathrm{SL}_t(\mathbb{Z})$ of unimodular lattices in \mathbb{R}^t carries a canonical Haar measure of total mass one. Viewing $F_f(\Lambda)$ as a random variable on that space, Siegel [1] proved the mean value theorem

$$\mathbb{E}[F_f(\Lambda)] = \int_{\mathbb{R}^t} f(x) dx.$$

In particular, when f is the indicator function of a bounded convex body $F_f(\Lambda)$ counts non-trivial lattice points and the famous Minkowski–Hlawka theorem [2] can be deduced in this way. Various refinements of this approach imposing extra structure have since appeared, in particular for lattices coming from maximal orders in number fields or \mathbb{Q} -division rings [3, 4, 5]. The additional structure can often be leveraged for suitable applications; for instance A. Venkatesh in [4] deduces the currently best asymptotic lower bounds on the sphere packing density in high dimensions by working with cyclotomic integers.

In a series of papers [6, 7, 8], C.A. Rogers established roughly a decade after Siegel formulas for the higher moments of \mathbb{Z} -lattices and explicitly evaluated those formulas when the lattice sum function is counting non-trivial lattice points in a bounded convex set. More precisely, Rogers obtains in [8, Theorem 3]:

Theorem. (Rogers, 1956) *Let $\Lambda \subseteq \mathbb{R}^t$ be a random unit covolume lattice and let S be a centrally symmetric Borel set of volume V . Consider the random variable*

$$\rho(\Lambda) := F_{\mathbf{1}_S}(\Lambda) = \#(S \cap (\Lambda \setminus \{0\})).$$

Then, provided the \mathbb{Z} -rank t of the lattices satisfies $t \geq \lceil \frac{1}{4}n^2 + 3 \rceil$, it follows that the n -th moment of the number of non-zero lattice points in S satisfies

$$2^n \cdot m_n\left(\frac{V}{2}\right) \leq \mathbb{E}[\rho(\Lambda)^n] \leq 2^n \cdot m_n\left(\frac{V}{2}\right) + E_{n,t} \cdot (V+1)^{n-1},$$

where

$$m_n(\lambda) = e^{-\lambda} \sum_{r=0}^{\infty} \frac{\lambda^r}{r!} r^n = \mathbb{E}_{X \sim \mathcal{P}(\lambda)}(X^n) \quad (1)$$

is the n th moment of a Poisson distribution with parameter λ and where $E_{n,t}$ is an error term decaying exponentially as t increases:

$$E_{n,t} \leq 2 \cdot 3^{\lceil \frac{n^2}{4} \rceil} \cdot \left(\frac{\sqrt{3}}{2}\right)^t + 21 \cdot 5^{\lceil \frac{n^2}{4} \rceil} \cdot \left(\frac{1}{2}\right)^t.$$

In other words, Rogers showed that the number of pairs of non-trivial lattice points in S has a distribution which approaches a Poisson distribution with mean $\frac{1}{2}V$ for large values of t . In particular, we obtain for large rank t essentially $2\sqrt{t}$ point count estimates

$$\begin{aligned} \mathbb{E}\left(\frac{1}{2}\rho(\Lambda)\right) &= \frac{1}{2} \mathrm{vol}(S), \\ \mathbb{E}\left(\left(\frac{1}{2}\rho(\Lambda)\right)^2\right) &= \left(\frac{1}{2} \mathrm{vol}(S)\right)^2 + \left(\frac{1}{2} \mathrm{vol}(S)\right) + o(1), \\ \mathbb{E}\left(\left(\frac{1}{2}\rho(\Lambda)\right)^3\right) &= \left(\frac{1}{2} \mathrm{vol}(S)\right)^3 + 3\left(\frac{1}{2} \mathrm{vol}(S)\right)^2 + \left(\frac{1}{2} \mathrm{vol}(S)\right) + o(1), \\ &\vdots \end{aligned}$$

which are valid independently of $\mathrm{vol}(S)$. Note that the polynomials appearing on the right hand side are Touchard polynomials¹ in $\frac{1}{2} \mathrm{vol}(S)$ and that the appearance of the fraction $\frac{1}{2}$ on either side of the estimates results from the symmetries of ± 1 acting on all lattice vectors.

It seems natural to ask whether similar higher moment results hold for lattices with additional structure, or whether the behaviour is qualitatively different. For a number field K the ring of integers \mathcal{O}_K can be seen via the Minkowski embedding as a lattice in $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{[K:\mathbb{Q}]}$. Thus, any \mathcal{O}_K -module of finite rank t produces (after possible scaling) a unimodular lattice in the space $\mathrm{SL}_t(K \otimes_{\mathbb{Q}} \mathbb{R})/\mathrm{SL}_t(\mathcal{O}_K)$, which also comes equipped with a canonical probability measure. We study higher moments of the number of points in a bounded convex set for such \mathcal{O}_K -lattices.

A first observation is that, assuming that S is symmetric about the origin, the finite order units in \mathcal{O}_K act freely on the lattice points in S and thus lattice points should come in ω_K -tuples instead of pairs, where ω_K denotes the root number of K . As a consequence of our main theorems, we are indeed able to show that for balls S the number of ω_K -tuples of \mathcal{O}_K -lattice points in S have a distribution asymptotic to a Poisson distribution with mean $\frac{1}{\omega_K}V$:

¹For the first moment, Siegel's theorem tells us that the error term is exactly zero.

Theorem 1. *Let K be any number field and let n be fixed. Then there is an explicit constant $t_0(K, n) = O_K(n^3 \log \log n)$ such that the n -th moment $\mathbb{E}[\rho(\Lambda)^n]$ of the number of nonzero lattice points lying in an origin-centered ball of volume V and a random unit covolume \mathcal{O}_K -lattice of rank t satisfies*

$$\omega_K^n \cdot m_n\left(\frac{V}{\omega_K}\right) \leq \mathbb{E}[\rho(\Lambda)^n] \leq \omega_K^n \cdot m_n\left(\frac{V}{\omega_K}\right) + E_{n,t,K} \cdot (V+1)^{n-1}$$

with the error term

$$E_{n,t,K} \leq C_K \cdot t^{(n-2)/2} \cdot e^{-\varepsilon_K \cdot (t-t_0)}$$

provided that $t > t_0(K, n)$. Here m_n is as defined in Equation (1) and the ball of volume V is with respect to the Euclidean norm given in Equation (3). The constants $C_K, \varepsilon_K > 0$ are uniform in the rank t of the \mathcal{O}_K -lattices and can also be explicitly described.

An expression for the explicit constants $t_0(K, n)$ and ε_K in terms of n and the geometry of the unit lattice of K can be found in Corollary 58.

Rogers' results rely on his integral formula for the n -th moments. Such a result is also available in the context of \mathcal{O}_K -lattices and implicit in the literature. For instance, S. Kim [9] establishes an integral formula in the adelic language and deduces convergence of the second moment. See also, e.g., [10] and [11, Theorem 1]. However, one of the main challenges arising for general number fields is dealing with infinite unit groups in \mathcal{O}_K and bounding their contributions (see 4 for the integral formula). We remedy this by employing lower bounds on the Weil height of units \mathcal{O}_K^\times . In fact, height considerations allow us to prove stronger asymptotic results by increasing not just the \mathcal{O}_K -rank of the lattices, but also the degree of the number field.

More precisely, we show:

Theorem 2. *Let \mathcal{S} denote any set of number fields K such that the absolute Weil height of elements in $K^\times \setminus \mu_K$ has a strictly positive uniform lower bound on \mathcal{S} . There are then for a given n explicit constants $t_0(n, \mathcal{S}) = O_{\mathcal{S}}(n^3 \log \log n)$ as well as explicit constants $C, \varepsilon > 0$, all uniform in \mathcal{S} , such that for any $t > t_0$ and for any $K \in \mathcal{S}$ of degree d the n -th moment $\mathbb{E}[\rho(\Lambda)^n]$ of the number of nonzero \mathcal{O}_K -lattice points in an origin-centered ball of volume V and Λ in the space of unit covolume \mathcal{O}_K -lattices of rank t satisfies:*

$$\omega_K^n \cdot m_n\left(\frac{V}{\omega_K}\right) \leq \mathbb{E}[\rho(\Lambda)^n] \leq \omega_K^n \cdot m_n\left(\frac{V}{\omega_K}\right) + E_{n,t,K} \cdot (V+1)^{n-1}.$$

where the error term satisfies

$$E_{n,t,K} \leq C \cdot (td)^{(n-2)/2} \cdot \omega_K^{n^2/4} \cdot Z(K, t, n) \cdot e^{-\varepsilon \cdot d(t-t_0)}.$$

Here ω_K are the number of roots of unity in K , $Z(K, t, n)$ denotes a finite product of Dedekind zeta values ζ_K at certain real values > 1 and m_n is as in Equation (1).

See the more detailed Theorem 57 for explicit values of the constant $t_0(n, \mathcal{S})$, of the zeta factor $Z(K, t, n)$ and of the constants C, ε . Note that the terms $(td)^{(n-2)/2} \cdot \omega_K^{n^2/4}$ grow polynomially in t, d since $\omega_K = O(d \log \log d)$ and the error term indeed decays exponentially in the dimension of the lattices.

The height bound assumption on $\bigcup_{K \in \mathcal{S}} K$ in Theorem 2 is in the literature referred to as the *Bogomolov property*. A prototypical example of an infinite tower satisfying the Bogomolov property are the cyclotomic numbers $\mathbb{Q}^{cyc} = \bigcup_{i \geq 2} \mathbb{Q}(\zeta_i)$, so that the limiting results of Theorem 2 in particular apply to lattices over cyclotomic integers of increasing degree for fixed large enough rank. In this case we can also bound the zeta factor uniformly-see Corollary 60. For the reader's convenience and as an illustration, we record here an entirely explicit ensuing second moment result over cyclotomic fields:

Corollary 3. *Consider a sequence of cyclotomic number fields given by $K_i = \mathbb{Q}(\zeta_{k_i})$ of degree $d_i = \varphi(k_i)$ and let $t_0 = \frac{267}{10}$. There then exist uniformly bounded constants $C, \varepsilon > 0$ such that for any $t \geq 27$ and for any degree d_i the second moment $\mathbb{E}[\rho(\Lambda)^2]$ of the number of nonzero \mathcal{O}_K -lattice points in an origin-centered ball of volume V over the space of \mathcal{O}_K -lattices of rank t and unit covolume satisfies:*

$$V^2 + V \cdot \omega_{K_i} \leq \mathbb{E}[\rho(\Lambda)^2] \leq V^2 + V \cdot \omega_{K_i} \cdot (1 + C \cdot e^{-\varepsilon \cdot d_i(t-t_0)}).$$

Moreover, the inequality holds for $\varepsilon = \frac{1}{400}$ and $C = (3 + \frac{3}{1 - e^{-d_i(t-t_0)/1124}}) \cdot \zeta_{K_i}(\frac{37t}{52}) \cdot \zeta_{K_i}(\frac{t}{25})$ for any given $t \geq 27$ and $d_i \geq 2$. In particular, $C \leq 5625 \cdot \max_i(\zeta_{K_i}(\frac{37t}{52}) \cdot \zeta_{K_i}(\frac{t}{25}))$ holds for all such t, d_i .

We refer the reader unfamiliar with heights and the Bogomolov property to the discussion in Section 5 for details and other examples of infinite extensions with this property. We also partially prove in Proposition 62 the necessity of the height bound assumption in Theorem 2, showing that for any fixed rank t there exist number fields K_i of arbitrarily large degree with moments strictly larger than Poisson of mean V/ω_{K_i} . Finally, we remark that similar results apply to more general convex sets S beyond balls (see 64), however in pinning down the asymptotic distribution one needs to take into account the symmetry properties of the body S .

In conclusion, we observe not just a limiting Poisson behaviour for the finer moduli space of \mathcal{O}_K -lattices of fixed covolume, but also uncover additional flexibility in choosing the parameters of the Poisson distribution by varying the number of roots of unity in K . We therefore expect applications to the geometry of numbers and in particular hope to address the lattice packing and covering problems in the vein of [4],[6],[12],[13]. Beyond that, integral formulas and higher moments have been employed among others in dynamics in the context of logarithm laws for flows on homogeneous spaces and Diophantine approximation (see e.g., [14, 15], [16, Section 5] and [17]).

Furthermore, \mathcal{O}_K -lattices have emerged as interesting candidates for lattice-based cryptography (see e.g., [18, 19, 20]). The setup in these works often resembles our line of investigation, even considering lattices of fixed \mathcal{O}_K -rank and varying cyclotomic number field K . In analysing the hardness of problems such as the shortest vector problem (SVP) on these restricted lattices, our results indicate a Poisson-like behaviour similar to the full probability space of random lattices, albeit with a different Poisson parameter.

1.1 Outline of paper and proof

The paper is organized as follows: Section 2 establishes an effective version of the Rogers integral formula for \mathcal{O}_K -lattices, showing in particular that the expected moments can be attained up to arbitrarily high precision from lattices lifted from suitable finite sets of linear codes. This is of independent interest, expanding on the literature showing lattices attaining the expected mean values can be achieved in this way (see, e.g., [21, 22, 23, 24, 25, 26]). We also cover some preliminaries in this section.

Section 3 then establishes convergence of the higher moments and includes some preparatory lemmas. Convergence can be deduced by relating moments to values of height zeta functions on suitable Grassmannians. These converge by work of W. Schmidt [27] on asymptotic counts for points of bounded height in such varieties. Section 4 then deals with the main Poisson terms and some first estimates.

Section 5 tackles the general term and contains the main results. In order to go beyond just convergence of the moments, asymptotic estimates for points of bounded height are not sufficient, and one needs to have good control of the error terms for small heights as well. In order to illustrate how the results were achieved, we sketch our proof for the simple case of the second moment. In this case, via the integral formula the second moment computation for a fixed ball S in t copies of Euclidean space $K \otimes_{\mathbb{Q}} \mathbb{R}$ amounts to:

$$\text{vol}(S)^2 + \sum_{\alpha \in K^\times} [\mathcal{O}_K : (\alpha)^{-1} \cap \mathcal{O}_K]^{-t} \cdot \text{vol}(S \cap \alpha S).$$

To arrive at a result as in Corollary 3 it suffices to prove exponential decay of the sum

$$\sum_{\alpha \in (K^\times \setminus \mu_K) / \mu_K} [\mathcal{O}_K : (\alpha)^{-1} \cap \mathcal{O}_K]^{-t} \cdot \frac{\text{vol}(S \cap \alpha S)}{\text{vol}(S)}, \quad (2)$$

where μ_K denotes the roots of unity in K . In order to do so, we first bound for a fixed $\beta \in K^\times$ the shifted sum over units: $S_\beta = \sum_{\alpha \in (\mathcal{O}_K^\times \setminus \mu_K) / \mu_K} \frac{\text{vol}(S \cap \alpha \beta S)}{\text{vol}(S)}$. The full result for (2) is then deduced by summing over principal ideals (β) the quantity $[\mathcal{O}_K : (\beta)^{-1} \cap \mathcal{O}_K]^{-t} \cdot S_\beta$ and relating its decay to the decay of S_β up to some Dedekind zeta values of K (see e.g., Proposition 47). In order to bound S_β , we use a geometric convex combination Lemma to show that the volume ratio $\frac{\text{vol}(S \cap \alpha \beta S)}{\text{vol}(S)}$ decays exponentially with the Weil height of $\alpha\beta$, see Lemma 39 as well as Lemmas 53, 54, and 55 for the more general case. The final ingredient is then a count of the number of units $\alpha \in \mathcal{O}_K^\times$ such that $\alpha\beta$ has bounded Weil height. This is achieved in Lemma 41 using properties of heights and the unit lattice. Note that here it is really the points of *small height* which have the weightiest contributions to S_β and therefore we need genuine upper bounds on such counts as opposed to the classical asymptotic formulae for increasing height. We hope this also illustrates for the reader why height lower bounds for algebraic integers play an important role in our work.

For the n -th moment when $n > 2$, there are additional complications. We must evaluate the sum

$$\sum_{m=1}^{n-1} \sum_{\substack{D \in M_{m \times n}(K) \\ \text{rank}(D)=m \\ D \text{ is row reduced echelon}}} \mathfrak{D}(D)^{-t} \int_{x \in K \otimes_{\mathbb{Q}} \mathbb{R}^{t \times m}} \mathbf{1}_{S^m}(xD) dx,$$

where $\mathfrak{D}(D)$ is a measure of the denominators in D extending $[\mathcal{O}_K : (\alpha)^{-1} \cap \mathcal{O}_K]$ for $(n, m) = (2, 1)$. The main Poisson terms come from matrices D with a single non-zero entry in μ_K per column (we denote this set by A_m). While our overarching approach in estimating the error terms generalizing (2) is similar to the second moment, we now needed to distinguish several cases depending on the shape of D - see Section 5.4 for details. The trickiest case are matrices D close to A_m , in that D having entries of Weil height larger than some threshold $h_0 \approx \frac{1}{2} \log n$ or having many non-vanishing $m \times m$ minors makes estimates easier. However, the remaining cases then constitute a finite set of matrices D with entries of height bounded by h_0 and having at least one column which differs from columns in the main terms A_m . This is just enough to push through our results (see Proposition 56) and obtain suitable exponential decay of each error term.

Finally, Section 6.2 adds some concluding remarks on height assumptions and more general bodies.

Acknowledgements

We would like to thank Matthew DeCourcy-Ireland, Gabrielle De Micheli, Gauthier Leterrier and Philippe Michel for helpful conversations on topics related to this paper. We also thank Alexander Gorodnik for insights around equidistribution of Hecke points and Barak Weiss for discussions about lattice coverings. Finally, we thank Danylo Radchenko for supplying a major part of the argument in Lemma 59.

This research was majorly funded by the Swiss National Science Foundation (SNSF), Project funding (Div. I-III), "Optimal configurations in multidimensional spaces", 184927. Part of this research was carried out by the first named author during their stay at Quantinuum Ltd, Cambridge, UK.

2 Lattices from number fields and integral formula for lifts

Let K be a number field and let \mathcal{O}_K denote its ring of integers. Let $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$ denote the $[K : \mathbb{Q}]$ -dimensional Euclidean space associated to K and let $\overline{(\cdot)} : K_{\mathbb{R}} \rightarrow K_{\mathbb{R}}$ be a positive-definite involution² on $K_{\mathbb{R}}$ such that the following is a positive-definite real quadratic form on $K_{\mathbb{R}}$:

$$\langle x, y \rangle = \Delta_K^{-\frac{2}{[K:\mathbb{Q}]}} \text{tr}(x\overline{y}). \quad (3)$$

Here Δ_K is the absolute value of the discriminant of the number field K . Note that the quadratic form makes \mathcal{O}_K into a lattice in $K_{\mathbb{R}}$ and the normalization in Equation (3) ensures it has unit covolume. When multiple copies $K_{\mathbb{R}}$ are considered, we will assume that the quadratic form is the sum of the quadratic forms from Equation (3) on each copy. This quadratic form therefore defines a Lebesgue measure on any number of copies of $K_{\mathbb{R}}$.

As pointed out in the introduction, integral formulas for higher moments over number fields can be found in the literature. A. Weil vastly generalized Siegel's mean value theorem [10]. One may recover a n th moment formula from Weil's work by considering the algebraic group $G = \text{SL}_t(K)$ acting on the left on the affine variety $M_{t \times n}(K)$ in Weil's setup as described in §5-12 of [10]. We record the higher moment formulas which form the starting point for our work here:

Theorem 4. [9, 10, 11]

For any number t of copies of $K_{\mathbb{R}}$ let $g : K_{\mathbb{R}}^{t \times n} \rightarrow \mathbb{R}$ be a compactly supported Riemann-integrable function and equip $K_{\mathbb{R}}^t$ with the measure as discussed around Equation (3). Then, putting the Haar probability measure on $\text{SL}_t(K_{\mathbb{R}})/\text{SL}_t(\mathcal{O}_K)$, we have that

$$\int_{\text{SL}_t(K_{\mathbb{R}})/\text{SL}_t(\mathcal{O}_K)} \left(\sum_{v \in \gamma \mathcal{O}_K^{t \times n}} g(v) \right) d\gamma = \sum_{m=0}^n \sum_{\substack{D \in M_{m \times n}(K) \\ \text{rank}(D)=m \\ D \text{ is row reduced echelon}}} \mathfrak{D}(D)^{-t} \int_{x \in K_{\mathbb{R}}^{t \times m}} g(xD) dx,$$

²The standard choice is to consider the involution $\overline{(\cdot)}$ given by identifying $K_{\mathbb{R}} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ and defining $\overline{(\cdot)}$ to be the identity on the real places and complex conjugation otherwise.

where $\mathfrak{D}(D)$ is the index of the sublattice $\{C \in M_{1 \times m}(\mathcal{O}_K) \mid C \cdot D \in M_{1 \times n}(\mathcal{O}_K)\}$ in $M_{1 \times m}(\mathcal{O}_K)$. Here the right hand side could diverge (however, see Corollary 21), and the term at $m = 0$ is understood to be $g(0)$.

Remark 5. In the same setting as Theorem 4, we have

$$\int_{\mathrm{SL}_t(K_{\mathbb{R}})/\mathrm{SL}_t(\mathcal{O}_K)} \left(\sum_{v \in \gamma \mathcal{O}_K^{t \times n} \setminus \{0\}} g(v) \right) d\gamma = \sum_{m=1}^n \sum_{\substack{D \in M_{m \times n}(K) \\ \mathrm{rank}(D)=m \\ D \text{ is row reduced echelon} \\ D \text{ has no zero columns}}} \mathfrak{D}(D)^{-t} \int_{x \in K_{\mathbb{R}}^{t \times m}} g(xD) dx.$$

2.1 Effective higher moment results from lifts of codes

The existential results for the continuous and non-compact space of lattices $\mathrm{SL}_t(K_{\mathbb{R}})/\mathrm{SL}_t(\mathcal{O}_K)$ discussed in the introduction do not yield a way to arrive at explicit constructions for applications to coding theory, cryptography or the geometry of numbers. To that end, in this section we will produce a growing family of explicit lattices that equidistribute with respect to Siegel transforms. That is, we find a collection of unit covolume lattices $\{\Lambda_{i,j}\}_i$ such that as $j \rightarrow \infty$, we get $\#\{\Lambda_{i,j}\}_i \rightarrow \infty$ and

$$\frac{1}{\#\{\Lambda_{i,j}\}_i} \sum_i \left(\sum_{v \in \Lambda_{i,j}} f(v) \right)^n \rightarrow \int_{\mathrm{SL}_t(K_{\mathbb{R}})/\mathrm{SL}_t(\mathcal{O}_K)} \left(\sum_{v \in \gamma \mathcal{O}_K^t} f(v) \right)^n d\gamma.$$

This can be thought of as an analogue of the following result, which could be attributed to Rogers [28], seemingly the first to consider an effective version of Siegel's mean value theorem.

Theorem 6. (Rogers, 1947)

Let p be an arbitrary prime, \mathbb{F}_p be the field with p elements and let $\pi_p : \mathbb{Z}^d \rightarrow \mathbb{F}_p^d$ be the natural coordinate-wise projection map. Let \mathcal{L}_p be the set of sub-lattices of \mathbb{Z}^d that are pre-images of one-dimensional subspaces in this projection map scaled to become unit covolume, i.e.

$$\mathcal{L}_p = \{C_p \pi_p^{-1}(\mathbb{F}_p v) \mid v \in \mathbb{F}_p^d \setminus \{0\}\}, C_p = p^{-(1-\frac{1}{d})}.$$

Consider a compactly supported continuous function $f : \mathbb{R}^d \rightarrow \mathbb{R}$. Then the following holds:

$$\lim_{p \rightarrow \infty} \left[\frac{1}{\#\mathcal{L}_p} \sum_{\Lambda \in \mathcal{L}_p} \sum_{v \in \Lambda \setminus \{0\}} f(v) \right] = \int_{\mathbb{R}^d} f(x) dx.$$

Theorem 6 can for instance be used to effectively generate lattices that attain the Minkowski lower bound on the sphere packing density. Results along the line of Theorem 6 have appeared [25, 26] for mean values of lattices with additional structure and with applications in mind.

Remark 7. The set of lattices in Theorem 6 are Hecke points for the homogeneous space $\mathrm{SL}_t(\mathbb{R})/\mathrm{SL}_t(\mathbb{Z})$. These Hecke points are a growing collection of points parametrized by a primes p as $p \rightarrow \infty$. Rogers' Theorem 6 can be thought of as saying that these Hecke points equidistribute with respect to Siegel transforms. But more is true, in fact they equidistribute with respect to all test functions $\mathcal{C}_c(\mathrm{SL}_t(\mathbb{R})/\mathrm{SL}_t(\mathbb{Z}))$.

Equidistribution of Hecke points is a very well-studied topic [29, 30]. Using the general methods of [29], it should follow that the set of lattices $\mathcal{L}(\mathcal{P}, s)$ defined in (4) equidistribute as $N(\mathcal{P}) \rightarrow \infty$. In this paper we only focus on showing equidistribution with respect to Siegel transforms for the Hecke points considered below. Using that $\mathcal{L}(\mathcal{P}, s)$ equidistribute on the moduli space of \mathcal{O}_K -modules, one can arrive at another proof of Theorem 4. We skip these details.

2.2 Lattices from reductions

Let $f : K_{\mathbb{R}}^t \rightarrow \mathbb{R}$ be a compactly supported Riemann-integrable function on the real Euclidean space formed by taking t copies of $K_{\mathbb{R}}$. This space contains \mathcal{O}_K^t as a unit-covolume lattice. We consider unramified prime ideals $\mathcal{P} \subseteq \mathcal{O}_K$ and fix a number $s \in \{1, \dots, d-1\}$. If $\pi_{\mathcal{P}} : \mathcal{O}_K \rightarrow k_{\mathcal{P}}$ is the projection map to the residue field $k_{\mathcal{P}}$, we want to consider the following set of unit covolume lattices:

$$\mathcal{L}(\mathcal{P}, s) = \{\beta\pi_{\mathcal{P}}^{-1}(S) \mid S \subseteq k_{\mathcal{P}}^t \text{ is a } s\text{-dimensional } k_{\mathcal{P}}\text{-subspace}\} \quad (4)$$

where ³

$$\beta = \beta(\mathcal{P}, s) = \mathbf{N}(\mathcal{P})^{-(1-\frac{s}{t})\frac{1}{[K:\mathbb{Q}]}}.$$

Indeed, this scaling factor β ensures that the lattice $\beta\pi_{\mathcal{P}}^{-1}(S)$ has the same covolume as $\mathcal{O}_K^t \subseteq K_{\mathbb{R}}^t$.

What we are interested in is the following average:

$$\frac{1}{\#\mathcal{L}(\mathcal{P}, s)} \sum_{\Lambda \in \mathcal{L}(\mathcal{P}, s)} \left(\sum_{v \in \Lambda} f(v) \right)^n. \quad (5)$$

We will in fact consider the slightly more general setup: let $g : K_{\mathbb{R}}^{t \times n} \rightarrow \mathbb{R}$ be a compactly supported Riemann-integrable function on $[K : \mathbb{Q}] \cdot t \cdot n$ real variables. We evaluate the average

$$\frac{1}{\#\mathcal{L}(\mathcal{P}, s)} \sum_{\Lambda \in \mathcal{L}(\mathcal{P}, s)} \left(\sum_{v \in \Lambda^n} g(v) \right).$$

This sum reduces to Equation (5) under the substitution of $g(v_1, \dots, v_n) = f(v_1)f(v_2)\dots f(v_n)$. We perform some manipulations on this sum. Letting $\mathbf{1}(P)$ denote the indicator function of a proposition P , we have that

$$\begin{aligned} & \frac{1}{\#\mathcal{L}(\mathcal{P}, s)} \sum_{\Lambda \in \mathcal{L}(\mathcal{P}, s)} \left(\sum_{v \in \Lambda^n} g(v) \right) \\ &= \frac{1}{\#\mathcal{L}(\mathcal{P}, s)} \sum_{\substack{S \subseteq k_{\mathcal{P}}^t \\ S \simeq k_{\mathcal{P}}^s}} \left(\sum_{x \in (\pi_{\mathcal{P}}^{-1}(S))^n} g(\beta x) \right) \\ &= \frac{1}{\#\mathcal{L}(\mathcal{P}, s)} \sum_{\substack{S \subseteq k_{\mathcal{P}}^t \\ S \simeq k_{\mathcal{P}}^s}} \left(\sum_{x \in \mathcal{O}_K^{t \times n}} g(\beta x) \mathbf{1}(\pi_{\mathcal{P}}(x) \in S^n) \right) \\ &= \sum_{x \in \mathcal{O}_K^{t \times n}} g(\beta x) \left(\frac{1}{\#\mathcal{L}(\mathcal{P}, s)} \sum_{\substack{S \subseteq k_{\mathcal{P}}^t \\ S \simeq k_{\mathcal{P}}^s}} \mathbf{1}(\pi_{\mathcal{P}}(x) \in S^n) \right) \\ &= \sum_{x \in \mathcal{O}_K^{t \times n}} g(\beta x) \left(\frac{1}{\#\mathcal{L}(\mathcal{P}, s)} \sum_{\substack{S \subseteq k_{\mathcal{P}}^t \\ S \simeq k_{\mathcal{P}}^s}} \mathbf{1}(\text{span}(\pi_{\mathcal{P}}(x_1), \dots, \pi_{\mathcal{P}}(x_n)) \subseteq S) \right). \end{aligned}$$

The inner sum is just the probability of a random subspace $S \subseteq k_{\mathcal{P}}^t$ of fixed dimension s containing some given set of points $x_1, x_2, \dots, x_n \in k_{\mathcal{P}}^t$. This probability, other than depending on \mathcal{P}, s , depends only on the $k_{\mathcal{P}}$ -dimension of the subspace generated by $\pi_{\mathcal{P}}(x_1), \dots, \pi_{\mathcal{P}}(x_n)$. This dimension equals the rank of $\pi_{\mathcal{P}}(x) \in M_{t \times n}(k_{\mathcal{P}})$ which is certainly less than the rank of $x \in M_{t \times n}(\mathcal{O}_K) \subseteq M_{t \times n}(K)$. So we can split our sum into

$$= \sum_{m=0}^{\min(n, t)} \sum_{\substack{x \in M_{t \times n}(\mathcal{O}_K) \\ \text{rank}(x)=m}} \frac{g(\beta x)}{\#\mathcal{L}(\mathcal{P}, s)} \left(\sum_{\substack{S \subseteq k_{\mathcal{P}}^t \\ S \simeq k_{\mathcal{P}}^s}} \mathbf{1}(\text{span}(\pi_{\mathcal{P}}(x_1), \dots, \pi_{\mathcal{P}}(x_n)) \subseteq S) \right). \quad (6)$$

³There is an abuse of notation in Equation (4) as $\pi_{\mathcal{P}}$ denotes a map on $\mathcal{O}_K^t \rightarrow k_{\mathcal{P}}^t$. Henceforth, this map is to be understood as “applying the mod \mathcal{P} operation at each coordinate”.

Given $x \in M_{t \times n}(\mathcal{O}_K)$, we might for some \mathcal{P} encounter a “rank-drop” phenomenon, that is $\text{rank}(\pi_{\mathcal{P}}(x)) < \text{rank}(x)$. However, the good news is that the matrices x where this rank-drop happens can be “pushed away” from the support of g by taking $N(\mathcal{P})$ to be large enough. The following lemma captures this idea.

Lemma 8. *Suppose that $x \in M_{t \times n}(\mathcal{O}_K)$ is a matrix with $\text{rank}(x) = m > 0$ and \mathcal{P} is a prime ideal in \mathcal{O}_K such that $\text{rank}(\pi_{\mathcal{P}}(x)) < m$. Then, for any Euclidean norm $\|\bullet\| : M_{t \times n}(K_{\mathbb{R}}) \rightarrow \mathbb{R}_{\geq 0}$, we can find a constant $C > 0$ depending on $K, \|\bullet\|, t, n$ and independent of m, \mathcal{P} such that*

$$\|x\| \geq C N(\mathcal{P})^{\frac{1}{m[K:\mathbb{Q}]}}$$

Proof. By choosing a \mathbb{Z} -basis of \mathcal{O}_K , we can embed $\iota : \mathcal{O}_K \hookrightarrow M_{[K:\mathbb{Q}]}(\mathbb{Z})$ as a subring of the square integer matrices of size $[K:\mathbb{Q}]$. Without loss of generality, we assume that the norm $\|\bullet\|$ is the Euclidean norm via the embedding

$$\iota : M_{t \times n}(\mathcal{O}_K) \hookrightarrow M_{t[K:\mathbb{Q}] \times n[K:\mathbb{Q}]}(\mathbb{Z}) \subseteq \mathbb{R}^{tn[K:\mathbb{Q}]^2}.$$

Since $\text{rank}(x) = m$, we know that there exists a non-singular $m \times m$ minor $a \in M_m(\mathcal{O}_K)$ appearing as a submatrix in x . It is clear that $0 \neq \det a \in \mathcal{P}$ otherwise there is no rank-drop modulo \mathcal{P} . Therefore, we get that

$$N(\mathcal{P}) \mid N(\det a).$$

Observe also that via the map $\iota : M_m(\mathcal{O}_K) \rightarrow M_{m[K:\mathbb{Q}]}(\mathbb{Z})$ we have the determinant relation $\det(\iota(a)) = N(\det(a))$. Since we know that $0 \neq |\det(\iota(a))| \geq N(\mathcal{P})$, at least one non-zero integer appearing in the matrix entries of $\iota(a)$ would have absolute value bigger than $\frac{1}{m[K:\mathbb{Q}]} N(\mathcal{P})^{\frac{1}{m[K:\mathbb{Q}]}}$. This produces the same lower bound on the Euclidean norm of $\iota(a)$ up to a constant, and similarly also for $\iota(x)$.

This finishes our proof. \square

Lemma 9. *Suppose $y_1, y_2, \dots, y_m \in k_{\mathcal{P}}^t$ are linearly independent vectors (over $k_{\mathcal{P}}$). Then the following holds:*

$$\frac{1}{\#\mathcal{L}(\mathcal{P}, s)} \left(\sum_{\substack{S \subseteq k_{\mathcal{P}}^t \\ S \simeq k_{\mathcal{P}}^s}} \mathbf{1}(\text{span}(y_1, y_2, \dots, y_m) \subseteq S) \right) = \begin{cases} 0 & \text{if } s < m \\ N(\mathcal{P})^{-s(t-s)} & \text{if } s = m \\ N(\mathcal{P})^{-m(t-s)} \cdot (1 + o(1)) & \text{if } s > m. \end{cases}$$

Here the error term $o(1)$ is with respect to growing norm $N(\mathcal{P})$.

Proof. The case with $s < m$ is clear. In general for a finite field of size q , the number of s -dimensional subspaces in a t -dimensional vector space is the cardinality of the Grassmannian $\mathbf{Gr}(s, \mathbb{F}_q^t)$ given by

$$\frac{(q^t - 1)(q^t - q) \cdots (q^t - q^{s-1})}{(q^s - 1)(q^s - q) \cdots (q^s - q^{s-1})} = q^{s(t-s)} \cdot (1 + o(1)).$$

In our case, $\#k_{\mathcal{P}} = N(\mathcal{P})$. Up to some change of variables, the numerator is actually counting the number of $(s-m)$ -dimensional subspaces in a $(t-m)$ -dimensional space and therefore has cardinality $\#\mathbf{Gr}(s-m, \mathbb{F}_q^{t-m})$. This is sufficient to get our result. \square

Theorem 10. *Take $t \geq 2$, $n \in \{1, \dots, t-1\}$ and choose s as either $t-1$, or any number in $\{n, n+1, \dots, t-1\}$ that satisfies*

$$1 - \frac{s}{t} < \frac{1}{n}.$$

Let $g : K_{\mathbb{R}}^{t \times n} \rightarrow \mathbb{R}$ be a compactly supported Riemann integrable function. With $\mathcal{L}(\mathcal{P}, s)$ defined as in Equation (4), we have that as $N(\mathcal{P}) \rightarrow \infty$

$$\frac{1}{\#\mathcal{L}(\mathcal{P}, s)} \sum_{\Lambda \in \mathcal{L}(\mathcal{P}, s)} \left(\sum_{v \in \Lambda^n} g(v) \right) \rightarrow \sum_{m=0}^n \sum_{\substack{D \in M_{m \times n}(K) \\ \text{rank}(D)=m \\ D \text{ is row reduced echelon}}} \mathfrak{D}(D)^{-t} \int_{x \in K_{\mathbb{R}}^{t \times m}} g(xD) dx, \quad (7)$$

where $\mathfrak{D}(D)$ is the index of the sublattice $\{C \in M_{1 \times m}(\mathcal{O}_K) \mid C \cdot D \in M_{1 \times n}(\mathcal{O}_K)\}$ in $M_{1 \times m}(\mathcal{O}_K)$. Here the right hand side could diverge (however, see Corollary 21), and the term at $m = 0$ is understood to be $g(0)$.

Proof. From the discussion above, we arrive at Equation (6), and it remains to consider

$$\sum_{m=0}^n \sum_{\substack{x \in M_{t \times n}(\mathcal{O}_K) \\ \text{rank}(x)=m}} \frac{g(\beta x)}{\#\mathcal{L}(\mathcal{P}, s)} \left(\sum_{\substack{S \subseteq k_{\mathcal{P}}^t \\ S \simeq k_{\mathcal{P}}^s}} \mathbf{1}(\text{span}(\pi_{\mathcal{P}}(x_1), \dots, \pi_{\mathcal{P}}(x_n)) \subseteq S) \right).$$

Note that here $\beta = \beta(\mathcal{P}, s) = \mathbf{N}(\mathcal{P})^{-\left(1 - \frac{s}{t}\right) \frac{1}{[K:\mathbb{Q}]}}$. The rank m ranges within $\{0, 1, \dots, n\}$ since $\min(n, t) = n$. Also, since $s \geq n$, we expect the quantity in parentheses to be nonzero.

We recall that $M_{t \times n}(K_{\mathbb{R}})$ has the Euclidean measure given by $t \cdot n$ copies of the quadratic form coming from Equation (3). When $m > 1$, we know from Lemma 8 that we will encounter a rank-drop mod \mathcal{P} only if for some predetermined constant $C > 0$

$$\begin{aligned} \|x\| &\geq C \mathbf{N}(\mathcal{P})^{\frac{1}{m[K:\mathbb{Q}]}} \\ \Rightarrow \|\beta x\| &\geq C \mathbf{N}(\mathcal{P})^{\frac{1}{[K:\mathbb{Q}]} \cdot \left(\frac{1}{m} - \left(1 - \frac{s}{t}\right)\right)}. \end{aligned}$$

Since

$$\frac{1}{m} - \left(1 - \frac{s}{t}\right) \geq \frac{1}{n} - \left(1 - \frac{s}{t}\right) > 0,$$

for a large enough value of $\mathbf{N}(\mathcal{P})$ we have that all the matrices of $x \in M_{t \times n}(\mathcal{O}_K)$ where rank-drop could happen are outside the support of g . Let us assume that $\mathbf{N}(\mathcal{P})$ is large enough for this to hold. Hence whenever $g(\beta x)$ is non-zero, the span of $\pi_{\mathcal{P}}(x_1), \pi_{\mathcal{P}}(x_2), \dots, \pi_{\mathcal{P}}(x_n)$ is of the same $k_{\mathcal{P}}$ -dimension as the rank of x . Using Lemma 9, we can rewrite our sum as

$$\sum_{m=0}^n \sum_{\substack{x \in M_{t \times n}(\mathcal{O}_K) \\ \text{rank}(x)=m}} \frac{g(\beta x)}{\mathbf{N}(\mathcal{P})^{m(t-s)}} \cdot (1 + o(1)) = \sum_{m=0}^n \sum_{\substack{x \in M_{t \times n}(\mathcal{O}_K) \\ \text{rank}(x)=m}} g(\beta x) \beta^{mt[K:\mathbb{Q}]} \cdot (1 + o(1)).$$

In order to arrive at the row reduced echelon matrix formulation, observe that the following K -subspaces of K^t

$$\begin{aligned} V_0 &= 0 \\ V_1 &= Kx_1 \\ V_2 &= Kx_1 + Kx_2 \\ V_3 &= Kx_1 + Kx_2 + Kx_3 \\ &\vdots \end{aligned}$$

satisfy that

$$\dim_K V_i - \dim_K V_{i-1} \in \{0, 1\} \text{ for } i \in \{1, 2, \dots, n\}.$$

Define $I \subseteq \{1, \dots, n\}$ as those indices such that $\dim_K V_i - \dim_K V_{i-1} = 1$. Then the vectors $\{x_i\}_{i \in I}$ are a basis of the K -span of $\{x_i\}_{i=1}^n$ and we conclude that $\#I = m$. Furthermore for $i \notin I$ we can uniquely find coefficients $\{a_{ij}\}_{j=1}^n \subseteq K$ such that

$$x_i = \sum_{j \in I \cap \{1, 2, \dots, j-1\}} a_{ij} x_j, \quad a_{ij} = 0 \text{ for } j \notin I \cap \{1, 2, \dots, j-1\}.$$

For $i \in I$, we may simply define $a_{ij} = \delta_{ij}$ using the Kronecker-delta symbol.

This setup leads us to the rank factorization of $x \in M_{t \times n}(K)$: the columns $\{x_i\}_{i \in I}$ form a matrix $C \in M_{t \times m}(K)$ and the coefficients $\{a_{ij}\}_{i \in \{1, \dots, n\}, j \in I}$ form the transpose of $D \in M_{m \times n}(K)$ such that

$$x = CD.$$

Observe that D is in row reduced echelon form. The matrices C and D are uniquely determined among all such decompositions. So we really obtain a bijection

$$\left\{ \begin{array}{l} x \in M_{t \times n}(\mathcal{O}_K), \\ \text{rank}(x)=m \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} D \in M_{m \times n}(K), \\ D \text{ is row reduced echelon,} \\ \text{rank}(D) = m \end{array} \right\} \times \left\{ \begin{array}{l} C \in M_{t \times m}(\mathcal{O}_K), \\ C \cdot D \in M_{t \times n}(\mathcal{O}_K) \end{array} \right\}.$$

With this in hand, we can rewrite our sum as

$$\sum_{m=0}^n \sum_{\substack{D \in M_{m \times n}(K) \\ \text{rank}(D)=m \\ D \text{ is row reduced echelon}}} \left(\sum_{\substack{C \in M_{t \times m}(\mathcal{O}_K) \\ C \cdot D \in M_{t \times n}(\mathcal{O}_K)}} g(\beta \cdot CD) \cdot \beta^{mt[K:\mathbb{Q}]} \cdot (1 + o(1)) \right).$$

We now observe that the condition $C \cdot D \in M_{t \times n}(\mathcal{O}_K)$ defines a sublattice of $M_{t \times m}(\mathcal{O}_K)$ of index $\mathfrak{D}(D)^t$. Therefore, as $N(\mathcal{P})$ increases, the inner sum converges to the Riemann integral of $x \mapsto g(xD)$ scaled by a factor of $\mathfrak{D}(D)^{-t}$ and we arrive at our result. \square

The following reformulation of Theorem 10 will also be quite useful for us.

Corollary 11. *In the same setting as Theorem 10, we have that as $N(\mathcal{P}) \rightarrow \infty$,*

$$\frac{1}{\#\mathcal{L}(\mathcal{P}, s)} \sum_{\Lambda \in \mathcal{L}(\mathcal{P}, s)} \left(\sum_{v \in (\Lambda \setminus \{0\})^n} g(v) \right) \rightarrow \sum_{m=1}^n \sum_{\substack{D \in M_{m \times n}(K) \\ \text{rank}(D)=m \\ D \text{ is row reduced echelon} \\ D \text{ has no zero columns}}} \mathfrak{D}(D)^{-t} \int_{x \in K_{\mathbb{R}}^{t \times m}} g(xD) dx.$$

3 Convergence of the higher moment formula

In this section, we explain how to establish convergence of the expression in the integral formula of Theorem 4 and thus convergence of the moments.

For this purpose, it is sufficient to consider the case when g is the indicator function of a unit ball in $K_{\mathbb{R}}^{t \times n}$, since if the integral is bounded in this case then it should be bounded for all $g \in \mathcal{C}_c(K_{\mathbb{R}}^t)$. The formula can then be related to height zeta functions of Grassmannians and convergence follows from estimates of W. Schmidt on points of bounded height in Grassmannians [27]. Of course, the more crucial case for us is when $g(x_1, x_2, \dots, x_n) = \mathbf{1}_B(x_1) \mathbf{1}_B(x_2) \dots$, where each $\mathbf{1}_B$ is the indicator function of some ball $B \subseteq K_{\mathbb{R}}^t$, however we postpone this discussion for now.

Lemma 12. *Let g be the indicator function as described in the preceding paragraph and let $V(d)$ denote the volume of a d -dimensional unit ball. If $D \in M_{m \times n}(K)$ is a full-rank matrix, then we have that*

$$\int_{K_{\mathbb{R}}^{t \times m}} g(xD) dx = \det(D; M_{t \times m}(\mathcal{O}_K))^{-1} V(mt[K:\mathbb{Q}]).$$

Here, we define $\det(D; M_{t \times m}(\mathcal{O}_K))$ as the volume of the fundamental domain of the $mt[K:\mathbb{Q}]$ -dimensional \mathbb{Z} -lattice $M_{t \times n}(\mathcal{O}_K) \cdot D$.

Remark 13. *Equivalently, $\det(D; M_{t \times m}(\mathcal{O}_K))$ is the $(mt[K:\mathbb{Q}])$ -dimensional volume of the image of a unit cube in $K_{\mathbb{R}}^{t \times m}$ via $x \mapsto xD$. This image is a parallelepiped in $K_{\mathbb{R}}^{t \times n} \simeq \mathbb{R}^{tn[K:\mathbb{Q}]}$.*

Proof. (of Lemma 12)

Observe that by the definition of the Riemann integral

$$\int_{K_{\mathbb{R}}^{t \times m}} g(xD) dx = \lim_{\varepsilon \rightarrow 0} \varepsilon^{mt[K:\mathbb{Q}]} \left(\sum_{x \in M_{t \times m}(\mathcal{O}_K)} g(\varepsilon \cdot xD) \right).$$

The sum is now counting the number of lattice points of $\varepsilon M_{t \times m}(\mathcal{O}_K)$ in the ball. \square

Lemma 14. *Suppose $D \in M_{m \times n}(K)$. Then*

$$\det(D; M_{t \times m}(\mathcal{O}_K)) = \det(D; M_{1 \times m}(\mathcal{O}_K))^t.$$

Here the left-hand side is the quantity described above and the right hand side is the analogous quantity computing the volume of the fundamental domain of $M_{1 \times m}(\mathcal{O}_K) \cdot D \subseteq M_{1 \times n}(K_{\mathbb{R}}) \simeq K_{\mathbb{R}}^n$.

3.1 Heights of subspaces

Let us recreate the height functions on K -subspaces of K^t as given in [27]. Consider the standard Plücker embedding

$$\begin{aligned} \iota : \mathbf{Gr}(m, K^n) &\rightarrow \mathbf{P}(\wedge^m K^n) \\ \text{span}_K(w_1, w_2, \dots, w_m) &\mapsto [w_1 \wedge w_2 \wedge \dots \wedge w_m]. \end{aligned}$$

Here $\mathbf{P}(\wedge^m K^n) = \mathbf{Gr}(1, \wedge^m K^n)$ is the m th exterior product (over K) of the vector space K^n and w_1, \dots, w_m are some K -linearly independent vectors inside K^n . A constructive way to see this map is that if $S \in \mathbf{Gr}(m, K^n)$ is generated by w_1, \dots, w_m then $\iota(S)$ is the one-dimensional subspace generated by the $m \times m$ minors of the $n \times m$ matrix whose columns are w_1, \dots, w_m . We shall denote the norm of the fractional \mathcal{O}_K -ideal generated by $x_1, \dots, x_N \in K$ by:

$$N(\langle x_1, x_2, \dots, x_N \rangle) := N(\mathcal{O}_K x_1 + \dots + \mathcal{O}_K x_N). \quad (8)$$

Let $\sigma_1, \sigma_2, \dots, \sigma_{[K:\mathbb{Q}]} : K \rightarrow \mathbb{C}$ be all the complex embeddings of K . We can apply them coordinate-wise and lift them as $\sigma_1, \dots, \sigma_N : K^N \rightarrow \mathbb{C}^N$ for any $N \geq 1$. Now, for any projective space $\mathbf{P}(K^N)$, we can define the l^2 -height function as

$$\begin{aligned} H : \mathbf{P}(K^N) &\rightarrow \mathbb{R}_{\geq 0} \\ [x_1, \dots, x_N] &\mapsto \frac{1}{N(\langle x_1, x_2, \dots, x_N \rangle)} \prod_{i=1}^{[K:\mathbb{Q}]} \sqrt{\sum_{j=1}^N |\sigma_i(x_j)|^2}. \end{aligned} \quad (9)$$

We similarly define the l^∞ -height function:

$$\begin{aligned} H_W : \mathbf{P}(K^N) &\rightarrow \mathbb{R}_{\geq 0} \\ [x_1, \dots, x_N] &\mapsto \frac{1}{N(\langle x_1, x_2, \dots, x_N \rangle)} \prod_{i=1}^{[K:\mathbb{Q}]} \max_{j=1 \dots N} |\sigma_i(x_j)| \end{aligned} \quad (10)$$

Observe that both the heights defined above are well-defined functions on $\mathbf{P}(K^N)$.

Enumerating the size- m subsets of $\{1, 2, \dots, n\}$, we get an obvious identification $\mathbf{P}(\wedge^m K^n) \leftrightarrow \mathbf{P}(K^{\binom{n}{m}})$. Using this, we can define the height of a subspace in $\mathbf{Gr}(m, K^n)$ to be

$$\begin{aligned} H : \mathbf{Gr}(m, K^n) &\rightarrow \mathbb{R}_{\geq 0} \\ S &\mapsto H(\iota(S)) \end{aligned} \quad (11)$$

and similarly,

$$\begin{aligned} H_W : \mathbf{Gr}(m, K^n) &\rightarrow \mathbb{R}_{\geq 0} \\ S &\mapsto H_W(\iota(S)) \end{aligned}$$

Now, we are ready to state an important lemma, which is essentially Theorem 1 from [27].

Lemma 15. *Suppose $m \leq n$. Let $D \in M_{m \times n}(K)$ be a full-rank row reduced matrix and let $S = D^T K^m \in \mathbf{Gr}(m, K^n)$ be the m -dimensional subspace spanned by its rows. The height function H from Equation (11) satisfies*

$$H(S) = \det(D; M_{1 \times m}(\mathcal{O}_K)) \cdot \mathfrak{D}(D).$$

Here $\det(D; M_{1 \times m}(\mathcal{O}_K))$ is as defined in Lemma 14 and $\mathfrak{D}(D)$ is as defined in Theorem 10.

Proof. A proof is given for the reader's convenience in Appendix A. □

3.2 Relating the two types of heights

The following gives a relationship between the two types of heights defined in this section. This will be useful for proving Poisson estimates later on in the paper.

Lemma 16. *Let $x = [x_1, x_2, \dots, x_N] \in \mathbf{P}(K^N)$. Then the following relation exists between heights defined in Equation (9) and (10):*

$$H(x)^2 \geq \left(H_W(x)^{\frac{2}{[K:\mathbb{Q}]}} + (N-1) \frac{M(x)^{\frac{2}{[K:\mathbb{Q}](N-1)}}}{H_W(x)^{\frac{2}{[K:\mathbb{Q}](N-1)}}} \right)^{[K:\mathbb{Q}]},$$

where

$$M(x) = \frac{N(x_1)N(x_2)\dots N(x_N)}{N(\langle x_1, x_2, \dots, x_N \rangle)^N}. \quad (12)$$

Here $N(x_i)$ denotes the norm of the ideal generated by x_i and N is any strictly positive integer.

Proof. Observe that the following is a convex function on \mathbb{R}^N :

$$(x_1, \dots, x_N) \rightarrow \log(e^{x_1} + e^{x_2} + \dots + e^{x_N}),$$

and hence we get that for $x_{ij} \geq 0$

$$\prod_{j=1}^r \left(\sum_{i=1}^N x_{ij} \right) \geq \left(\sum_{i=1}^N \left(\prod_{j=1}^r x_{ij} \right)^{\frac{1}{r}} \right)^r.$$

For maximum efficacy, before applying the above inequality, one should rearrange the inner sums in the decreasing order. So we add the assumption that for each j , $x_{1j} \geq x_{2j} \geq \dots \geq x_{rj}$. Now, using the arithmetic-mean-geometric-mean inequality on the last $N-1$ terms on each of the r multiplicands, we get:

$$\begin{aligned} \prod_{j=1}^r \left(\sum_{i=1}^N x_{ij} \right) &\geq \left(\sum_{i=1}^N \left(\prod_{j=1}^r x_{ij} \right)^{\frac{1}{r}} \right)^r \geq \left(\left(\prod_{j=1}^r x_{1j} \right)^{\frac{1}{r}} + (N-1) \left(\prod_{i=2}^N \prod_{j=1}^r x_{ij} \right)^{\frac{1}{r(N-1)}} \right)^r \\ &= \left(\left(\prod_{j=1}^r x_{1j} \right)^{\frac{1}{r}} + (N-1) \frac{\left(\prod_{i=1}^N \prod_{j=1}^r x_{ij} \right)^{\frac{1}{r(N-1)}}}{\left(\prod_{j=1}^r x_{1j} \right)^{\frac{1}{r(N-1)}}} \right)^r. \end{aligned}$$

Now set $r = [K:\mathbb{Q}]$ and for each r let $\{x_{i1}, x_{i2}, \dots\}$ be the numbers $\{|\sigma(x_1)|^2, |\sigma(x_2)|^2, \dots\}$ written down in the decreasing order, with $\sigma: K \rightarrow \mathbb{C}$ being the i th embedding with respect to some enumeration. This way, we have that

$$\prod_{j=1}^r x_{1j} = \prod_{\sigma: K \rightarrow \mathbb{C}} \max_{i=1 \dots N} |\sigma(x_i)|^2 = H_W(x)^2 N(\langle x_1, x_2, \dots, x_N \rangle)^2.$$

So we reach the conclusion that

$$H(x)^2 \geq \left(H_W(x)^{\frac{2}{[K:\mathbb{Q}]}} + (N-1) \frac{M(x)^{\frac{2}{[K:\mathbb{Q}](N-1)}}}{H_W(x)^{\frac{2}{[K:\mathbb{Q}](N-1)}}} \right)^{[K:\mathbb{Q}]}. \quad \square$$

Concerning the quantity $M(x)$ we have:

Lemma 17. Let $x = [x_1, \dots, x_N] \in \mathbf{P}(K^N)$. The quantity $M(x)$ defined in Equation (12) is an integer at least 1 if and only if $x_1 \cdots x_N \neq 0$ and zero otherwise. Moreover, $M(x) = 1$ implies that $x_i \in \mathcal{O}_K^\times$ for all i (up to scaling, i.e. as an element of $\mathbf{P}(K^N)$) and if $M(x) > 1$ it equals the norm of a non-trivial ideal in \mathcal{O}_K .

Proof. For a prime ideal $\mathcal{P} \subseteq \mathcal{O}_K$, let $\nu_{\mathcal{P}}(x) \in \mathbb{Z}$ be the \mathcal{P} -adic valuation of $x \in K$. Then, we observe that

$$N(\langle x_1, \dots, x_N \rangle) = \prod_{\substack{\mathcal{P} \subseteq \mathcal{O}_K \\ \mathcal{P} \text{ is prime}}} N(\mathcal{P})^{\min_{i=1 \dots N} \nu_{\mathcal{P}}(x_i)}.$$

Note that the product is supported on finitely many primes. On the other hand

$$N(x_1 \dots x_N) = \prod_{\substack{\mathcal{P} \subseteq \mathcal{O}_K \\ \mathcal{P} \text{ is prime}}} N(\mathcal{P})^{\sum_{i=1 \dots N} \nu_{\mathcal{P}}(x_i)}.$$

So we get that

$$M(x) = \prod_{\substack{\mathcal{P} \subseteq \mathcal{O}_K \\ \mathcal{P} \text{ is prime}}} N(\mathcal{P})^{\sum_{i=1 \dots N} \nu_{\mathcal{P}}(x_i) - N \min_{i=1 \dots N} \nu_{\mathcal{P}}(x_i)}.$$

All the exponents are positive integers. They are zero only when all the $\nu_{\mathcal{P}}(x_i)$ are equal to each other and this is only possible if they differ at most by units. \square

3.3 Rational points of bounded height in Grassmannian varieties over number fields

Lemma 12, Lemma 14, Lemma 15 and Theorem 10 yield the following.

Lemma 18. Let g be the indicator function $\mathbf{1}_{B_R}$, where B_R is a ball in $K_{\mathbb{R}}^{t \times n}$ of radius R . Then, we have that

$$\begin{aligned} & \sum_{m=1}^n \sum_{\substack{D \in M_{m \times n}(K) \\ \text{rank}(D)=m \\ D \text{ is row reduced echelon} \\ D \text{ has no zero columns}}} \mathfrak{D}(D)^{-t} \int_{x \in K_{\mathbb{R}}^{t \times m}} g(xD) dx \\ &= 1 + \sum_{m=1}^n Z(t; \mathbf{Gr}(m, K^n), H) \cdot V(mt[K : \mathbb{Q}]) R^{mt}. \end{aligned}$$

Here $Z(t; \mathbf{Gr}(m, K^n), H)$ is the height zeta function defined as

$$Z(t; \mathbf{Gr}(m, K^n), H) = \sum_{S \in \mathbf{Gr}(m, K^n)} \frac{1}{H(S)^t}.$$

To show the convergence of the right hand side in Theorem 10, it is sufficient to show that all the height zeta functions in Lemma 18 converge. The asymptotic growth of points of bounded height on these varieties has been established by Schmidt and we have from [27, Theorem 3]:

Theorem 19. (Schmidt, 1967) There exist constants $C_1, C_2 > 0$ depending only on n, m, K such that

$$C_1 T^n \leq \#\{S \in \mathbf{Gr}(m, K^n) \mid H(S) \leq T\} \leq C_2 T^n$$

Corollary 20. The height zeta functions $Z(t; \mathbf{Gr}(m, K^n), H)$ converge when $t \geq n + 1$.

Proof. Define for $n \geq 1$

$$a_l = \#\{S \in \mathbf{Gr}(m, K^n) \mid H(S) \in [l - 1, l)\}.$$

Then Theorem 19 and Abel's summation formula gives us that

$$\begin{aligned} \sum_{l=1}^T \frac{a_l}{l^t} &= \left(\sum_{l=1}^T a_l \right) T^{-t} + \int_1^T \left(\sum_{l=1}^{\lfloor x \rfloor} a_l \right) \frac{t}{x^{t+1}} dx \\ &\leq C_2 T^{n-t} + t C_2 \int_1^T x^{n-t-1} dx \end{aligned}$$

Here, the first term converges as $T \rightarrow \infty$ since $n - t \leq -1$ and the second term also converges since $n - t - 1 \leq -2$ \square

Corollary 21. *The higher moment formula as given in Theorem 4 converges for $t \geq n + 1$. In particular, as $N(\mathcal{P}) \rightarrow \infty$ in Theorem 10, the right side of (7) is a finite quantity.*

4 Towards Poisson distribution

Going beyond convergence, we now turn towards establishing the limiting Poisson distribution. Let $V(n)$ henceforth denote the volume of the unit ball in dimension $n \geq 1$. The following identifies the main Poisson term and is an adaptation of [8, Lemma 4]:

Lemma 22. *Let μ_K denote the cyclic group of roots of unity in \mathcal{O}_K . Let $\omega_K = \#\mu_K$. Consider the set A_m for $m \in \{1, \dots, n\}$ given by*

$$A_m = \left\{ D \in M_{m \times n}(K) \mid \begin{array}{l} D_{ij} \in \mu_K \cup \{0\}, \\ D \text{ is in row-reduced echelon form of rank}(D)=m \\ D \text{ has exactly one non-zero entry in each column} \end{array} \right\}.$$

Let $B \subseteq K_{\mathbb{R}}^t$ denote a ball with respect to the norm given in Equation 3. Let $g = \mathbf{1}_B \otimes \dots \otimes \mathbf{1}_B : K_{\mathbb{R}}^{t \times n} \rightarrow \mathbb{R}$ be the n -fold indicator function of the ball in each coordinate. Restricting the higher moment formula as in Theorems 4 or 10 to matrices in A_m , we obtain that

$$\sum_{m=1}^n \sum_{D \in A_m} \mathfrak{D}(D)^{-t} \int_{x \in K_{\mathbb{R}}^{t \times m}} g(xD) dx = \omega_K^n \exp\left(-\frac{1}{\omega_K} \cdot V(t[K : \mathbb{Q}])\right) \sum_{r=0}^{\infty} \frac{r^n}{r!} \left(\frac{1}{\omega_K} \cdot V(t[K : \mathbb{Q}])\right)^r.$$

Proof. Observe that for $D \in A_m$, we have $\mathfrak{D}(D) = 1$. Next, observe that B is invariant under the diagonal action of μ_K on $K_{\mathbb{R}}^t$ due to the choice of the quadratic form defining the ball. Therefore, for any units $\alpha_1, \alpha_2, \dots, \alpha_n \in \mu_K$ we have that

$$g(\alpha_1 x_1, \alpha_2 x_2, \dots, \alpha_n x_n) = g(x_1, x_2, \dots, x_n),$$

where μ_K acts diagonally on $K_{\mathbb{R}}^t$ viewed as t copies of $K_{\mathbb{R}}$. This implies that for any $D \in A_m$, we must have

$$\int_{x \in K_{\mathbb{R}}^{t \times m}} g(xD) dx = \text{vol}(B)^m.$$

The combinatorial problem of counting $\#A_m$ is, up to multiplication by a power of ω_K , the same as that of partitioning n columns into m sets. Therefore, we have that

$$\#A_m = \omega_K^{n-m} \left\{ \begin{matrix} n \\ m \end{matrix} \right\},$$

where $\left\{ \begin{matrix} n \\ m \end{matrix} \right\}$ is the Stirling number of the second kind. Hence, setting $V = V(t[K : \mathbb{Q}])$ gives

$$\sum_{m=1}^n \sum_{D \in A_m} \int_{x \in K_{\mathbb{R}}^{t \times m}} g(xD) dx = \sum_{m=1}^n V^m \omega_K^{n-m} \left\{ \begin{matrix} n \\ m \end{matrix} \right\} = \omega_K^n \sum_{m=1}^n \left\{ \begin{matrix} n \\ m \end{matrix} \right\} \frac{V^m}{\omega_K^m}.$$

Now we invoke the following identity about Touchard polynomials and we are done:

$$\sum_{m=1}^n \left\{ \begin{matrix} n \\ m \end{matrix} \right\} x^m = e^{-x} \sum_{r=0}^{\infty} \frac{r^n}{r!} x^r.$$

\square

We now turn to studying and bounding the contributions of the rest of the terms. To that end, we introduce the following notations for the remainder of the paper:

$$A_m^1 = \left\{ D \in M_{m \times n}(K) \mid \begin{array}{l} D_{ij} \in K, \\ D \text{ is in row-reduced echelon form with } \text{rank}(D)=m \\ \text{All the matrix entries are in } \mu_K \cup \{0\} \end{array} \right\} \setminus A_m.$$

$$A_m^2 = \left\{ D \in M_{m \times n}(K) \mid \begin{array}{l} D_{ij} \in K, \\ D \text{ is in row-reduced echelon form of } \text{rank}(D)=m \end{array} \right\} \setminus (A_m^1 \sqcup A_m).$$

Note that for $m = 1$ we have that $A_m = A_m^1$. For $m \geq 2$ we record here a standard estimate on volume ratios:

Lemma 23. *We have the estimates on volume ratios:*

$$\frac{V(mt[K : \mathbb{Q}])}{V(t[K : \mathbb{Q}])^m} = \frac{\Gamma\left(\frac{t[K:\mathbb{Q}]}{2} + 1\right)^m}{\Gamma\left(\frac{mt[K:\mathbb{Q}]}{2} + 1\right)} < \frac{(t[K : \mathbb{Q}]\pi)^{\frac{m-1}{2}}}{m^{\frac{1}{2}mt[K:\mathbb{Q}] + \frac{1}{2}}} \cdot e^{\frac{m}{6t[K:\mathbb{Q}]}}.$$

Proof. Straightforward by using honest upper and lower bounds in Stirling approximation. \square

4.1 Matrices of type A_m^1

In this subsection we obtain the following bound on the contribution of A_m^1 -type terms. These are the terms for which the geometrical methods utilized by Rogers [8] generalize without much difficulty. The more delicate terms, involving contributions from unit entries of infinite order, will be dealt with in Section 5.

Theorem 24. *Consider the setup of Lemma 22. Let K be a number field and let $n < t$. We then have that*

$$V(t[K : \mathbb{Q}])^{-m} \sum_{m=1}^n \sum_{D \in A_m^1} \mathfrak{D}(D)^{-t} \int_{K_{\mathbb{R}}^{t \times m}} g(xD) dx \leq C \left(\frac{\sqrt{3}}{2}\right)^{t[K:\mathbb{Q}]},$$

where the constant does not depend on n, m, K . If the number field K is also changing with n, m fixed, the constant C grows at most polynomially in $[K : \mathbb{Q}]$.

We record a trivial count which reduces the proof to bounding the contribution of each individual matrix:

Lemma 25. *We have that*

$$\sum_{m=1}^n \# A_m^1 \leq \sum_{m=1}^n \binom{n}{m} (1 + \omega_K)^{(n-m)m}.$$

The following result, an adaptation of [8, Lemma 5], suffices for our purposes:

Lemma 26. *Let $f : K_{\mathbb{R}}^t \rightarrow \mathbb{R}$ be the indicator function of a ball B of radius $R > 0$. Then, for any $\alpha_1, \alpha_2 \in \mu_K$ and $a \in K_{\mathbb{R}}^t$, we have that*

$$\frac{1}{V(t[K : \mathbb{Q}])^2 R^{2t[K:\mathbb{Q}]}} \int_{K_{\mathbb{R}}^{2 \times t}} f(x)f(y)f(\alpha_1 x + \alpha_2 y) dx dy \leq 2 \left(\frac{\sqrt{3}}{2}\right)^{t[K:\mathbb{Q}]}.$$

Proof. Since f is invariant under μ_K , we can assume that the integral is

$$\int_{K_{\mathbb{R}}^{t \times 2}} f(x)f(y)f(\alpha y - x) dx dy, \text{ for some } \alpha \in \mu_K.$$

We can rewrite the above as

$$\int_{K_{\mathbb{R}}^t} f(y) \left(\int_{K_{\mathbb{R}}^t} f(x)f(\alpha y - x) dx \right) dy.$$

The inner term is the intersectional volume of two translates of B , one centered at the origin and the other at αy . By doing some elementary geometry (see Figure 1), one can see that

$$\int_{K_{\mathbb{R}}^t} f(x)f(\alpha y - x)dx = 2V(N-1)R^N \int_{\frac{1}{2}\frac{\|\alpha y\|}{R}}^1 (1-\rho^2)^{\frac{N-1}{2}} d\rho,$$

where $N = t[K : \mathbb{Q}]$ and ρ is an integration parameter (see Figure 1). We understand the right hand side to be 0 if $\|\alpha y\| > 2R$.

Substituting this in our expression gives

$$\begin{aligned} & \left(2V(N-1)R^{t[K:\mathbb{Q}]}\right) \int_{K_{\mathbb{R}}^t} f(y) \left(\int_{\frac{1}{2}\frac{\|y\|}{R}}^1 (1-\rho^2)^{\frac{N-1}{2}} d\rho \right) dy \\ &= 2V(N-1)V(N)R^{2N}N \int_0^1 \xi^{N-1} \left(\int_{\frac{1}{2}\xi}^1 (1-\rho^2)^{\frac{N-1}{2}} d\rho \right) d\xi. \end{aligned}$$

Performing explicit computations as in [8, Lemma 5], we find that this expression is bounded by

$$\leq 2V(N)^2 R^{2N} \left(\frac{\sqrt{3}}{2}\right)^N.$$

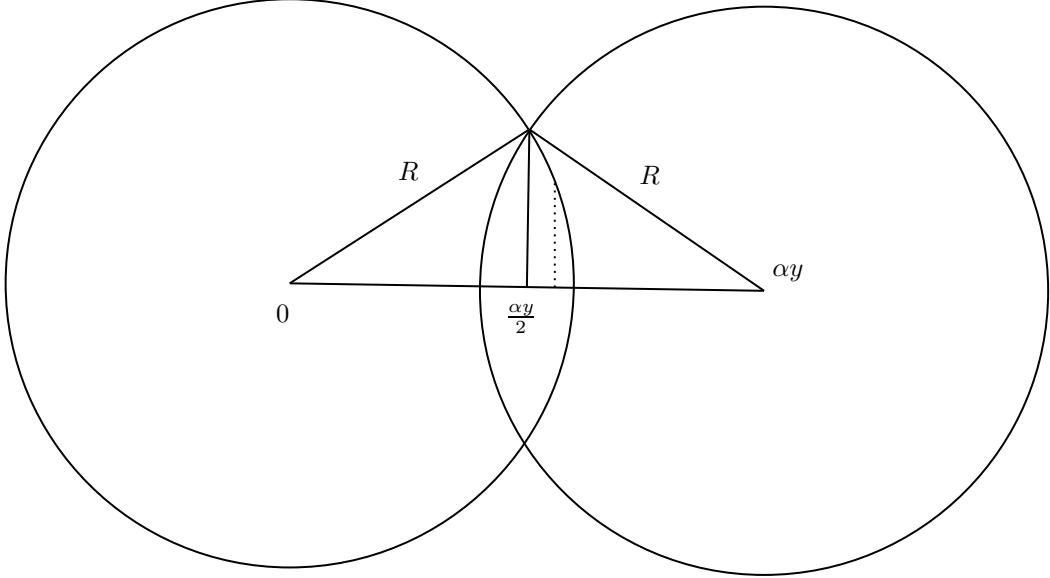


Figure 1: Intersection of two balls. The base of the dotted line is at a distance of $R\rho$ from the origin. Cutting the intersection along the dotted line gives a ball in one dimension less and has radius $R\sqrt{1-\rho^2}$. We integrate on the parameter ρ .

□

Lemma 27. For any $z \in K_{\mathbb{R}}^t$ and with the same setting as Lemma 26, we have

$$\int_{K_{\mathbb{R}}^{t \times 2}} f(x)f(y)f(\alpha_1 x + \alpha_2 y + z)dx dy \leq \int_{K_{\mathbb{R}}^{t \times 2}} f(x)f(y)f(\alpha_1 x + \alpha_2 y)dx dy.$$

Proof. Let $z = (z_1, z_2, \dots, z_t) \in K_{\mathbb{R}}^t$ and let $z' = (z'_1, z_2, \dots, z_t)$, where $z'_1 \in K_{\mathbb{R}} \simeq \mathbb{R}^{\oplus r_1} \oplus \mathbb{C}^{\oplus r_2}$ is equal to z_1 at all embeddings except one embedding $\sigma : K \rightarrow \mathbb{R}$ or $\sigma : K \rightarrow \mathbb{C}$ where it is equal to 0.

Thus we can write $z = \pi(z)e_{1,\sigma} + z'$ where $\pi : K_{\mathbb{R}}^t \rightarrow \mathbb{R}$ is the \mathbb{R} -coordinate of z_1 along σ and $e_{1,\sigma}$ is an appropriate vector.

For the statement, we will prove the following inequality and the rest will follow suit:

$$\int_{K_{\mathbb{R}}^{t \times 2}} f(x)f(y)f(\alpha_1 x + \alpha_2 y + z)dx dy \leq \int_{K_{\mathbb{R}}^{t \times 2}} f(x)f(y)f(\alpha_1 x + \alpha_2 y + z')dx dy. \quad (13)$$

For x, y we analogously define $x' = x - \pi(x)e_{1,\sigma}$ and $y' = y - \pi(y)e_{1,\sigma}$. Then the claim above will follow from the claim that for any $x, y \in K_{\mathbb{R}}^t$

$$\begin{aligned} & \int_{\mathbb{R}^2} f(x' + se_{1,\sigma})f(y' + te_{1,\sigma})f(\alpha_1(x' + se_{1,\sigma}) + \alpha_2(y' + te_{1,\sigma}) + z) dsdt \\ & \leq \int_{\mathbb{R}^2} f(x' + se_{1,\sigma})f(y' + te_{1,\sigma})f(\alpha_1(x' + se_{1,\sigma}) + \alpha_2(y' + te_{1,\sigma}) + z') dsdt. \end{aligned} \quad (14)$$

Indeed, we can obtain (13) from (14) by integrating along x', y' .

To prove the last inequality, observe that if $B \subseteq K_{\mathbb{R}}^t$ is the ball whose indicator function is f and if $P \subseteq K_{\mathbb{R}}^{t \times 2}$ is 2-dimensional plane spanned by $(e_{1,\sigma}, 0)$ and $(0, e_{1,\sigma})$ then

$$(B \times B) \cap ((x', y') + P) \subseteq K_{\mathbb{R}}^{t \times 2}$$

is the area within a square centered at the point x', y' since

$$\|x' + se_{1,\sigma}\|^2 = \|x'\|^2 + s^2 \text{ and } \|y' + te_{1,\sigma}\|^2 = \|y'\|^2 + t^2.$$

Furthermore, if $E_z \subseteq K_{\mathbb{R}}^{t \times 2}$ is the set whose indicator function is $(x, y) \mapsto f(\alpha_1 x + \alpha_2 y + z)$, then

$$E_z \cap ((x', y') + P) \text{ and } E_{z'} \cap ((x', y') + P)$$

are both 2-dimensional areas between two parallel lines and one is a translate of the other. Since the latter area is symmetrical around (x', y') and the former may not be, we can conclude geometrically

$$\text{vol}((B \times B) \cap E_z \cap ((x', y') + P)) \leq \text{vol}((B \times B) \cap E_{z'} \cap ((x', y') + P))$$

This shows that (14) must hold. □

Proof of Theorem 24. Set $N = t[K : \mathbb{Q}]$ as before. By Lemma 25 it is enough to consider the contribution of any $D \in A_m^1$.

For such matrices D , we claim that

$$V(N)^{-m} \frac{1}{\mathfrak{D}(D)^t} \int_{x \in M_{t \times m}(K_{\mathbb{R}})} g(xD) dx \leq 2\left(\frac{\sqrt{3}}{2}\right)^N.$$

Indeed, recall that D is an $m \times n$ matrix with entries in $\mu_K \cup \{0\}$ such that it has at least one column with more than one entry. Hence, without loss of generality we can assume that D looks like

$$\begin{bmatrix} 1 & & & \mu_1 & \dots & * \\ & 1 & & \mu_2 & \dots & * \\ & & 1 & * & \dots & * \\ & & & \ddots & & \vdots \\ & & & & 1 & * & \dots & * \end{bmatrix}.$$

So if f is the indicator function of the ball as in the statement of Lemma 26, then we can write that for $x \in K_{\mathbb{R}}^{t \times n}$

$$\begin{aligned} f(xD) &= f(x_1)f(x_2)\dots f(x_m)f(\mu_1 x_1 + \mu_2 x_2 + \dots)\dots \\ &\leq f(x_1)\dots f(x_m)f(\mu_1 x + \mu_2 x + \dots) \end{aligned}$$

Then, we can invoke Lemma 27 to get that

$$\begin{aligned} \int_{x \in K_{\mathbb{R}}^{t \times m}} f(xD) &\leq \int_{x \in K_{\mathbb{R}}^{t \times m}} f(x_1)\dots f(x_m)f(\mu_1 x_1 + \mu_2 x_2 + \dots) dx \\ &\leq \int_{x \in K_{\mathbb{R}}^{t \times m}} f(x_1)\dots f(x_m)f(\mu_1 x_1 + \mu_2 x_2) dx \end{aligned}$$

The claim is therefore a consequence of Lemma 26. The contribution from these terms decays exponentially as a result. The statement of the theorem then follows, given that $\#A_m^1$ grows at most polynomially in the degree $d = [K : \mathbb{Q}]$, whereas the term $(\frac{\sqrt{3}}{2})^N$ decays exponentially with d . □

5 Upper bounds on moments using Weil heights

We now turn to bounding the remaining terms in order to establish explicit formulas for moments of \mathcal{O}_K -lattices. Our aim is to establish such formulas while allowing the degree $d = [K : \mathbb{Q}]$ to vary as well. Our results will involve lower bounds on the Weil height for algebraic numbers. Such bounds are closely related to Lehmer's problem-which is still open-however suitable bounds for our purposes are known in many interesting and important cases.

5.1 Mahler measures and the Bogomolov property

For an algebraic number $\alpha \in K^\times$, recall that the Mahler measure (or unnormalised exponential Weil height) is given by the product over the set of places M_K of K :

$$H_W(\alpha) := \prod_{v \in M_K} \max\{1, |\alpha|_v\}.$$

We also define, keeping only the infinite places, the closely related

$$H_\infty(\alpha) = \prod_{\sigma: K \rightarrow \mathbb{C}} \max\{1, |\sigma(\alpha)|\}$$

which will be more directly relevant for estimates in the Euclidean space associated to K . The two coincide for algebraic integers and in general differ by a denominator. We also recall that the **absolute** Mahler measure (or exponential Weil height) of an algebraic number α is given by $H_W(\alpha)^{1/\deg(\alpha)}$ and we shall denote by

$$h(\alpha) = \log(H_W(\alpha)^{1/\deg(\alpha)})$$

the **Weil height** of an algebraic number. For non-integers, we shall also write $h_\infty(\alpha)$ for $\log(H_\infty(\alpha)^{1/\deg(\alpha)})$.

Remark 28. *Note that the absolute Mahler measure and Weil heights are independent of the subfield over which one is considering an algebraic integer. That is, if $\beta \in K$ we have $\deg \beta = \#\{\sigma : \mathbb{Q}(\beta) \rightarrow \mathbb{C}\}$ and*

$$\frac{\log\left(\prod_{\sigma: K \rightarrow \mathbb{C}} \max\{1, |\sigma(\beta)|\}\right)}{[K : \mathbb{Q}]} = \frac{\log\left(\prod_{\sigma: \mathbb{Q}(\beta) \rightarrow \mathbb{C}} \max\{1, |\sigma(\beta)|\}\right)}{[\mathbb{Q}(\beta) : \mathbb{Q}]}.$$

Lehmer's famous problem asks for a uniform lower bound for $h(\alpha) \deg(\alpha)$. We shall consider algebraic numbers related to the stronger property:

Definition 29. *A subset $S \subset \overline{\mathbb{Q}}$ is said to satisfy the **Bogomolov property** if there exists a constant $C > 0$ such that*

$$h(\alpha) \geq C$$

provided $\alpha \in S$ has infinite multiplicative order.

Throughout this section, we will therefore consider \mathcal{O}_K -lattices for towers of number fields inside a subset of $\overline{\mathbb{Q}}$ satisfying the Bogomolov property. In other words, we formulate the assumption:

Hypothesis 30. *As K varies among the number fields considered, there exist uniform constants $c_0 \geq c_1 > 0$ such that the absolute (logarithmic) Weil heights satisfy*

$$h(\alpha) > c_1 \text{ for } \alpha \in K^\times \setminus \mu_K$$

and

$$h_\infty(\alpha) = h(\alpha) > c_0 \text{ for } \alpha \in \mathcal{O}_K \setminus \{\mu_K, 0\},$$

where μ_K denotes the group of roots of unity contained in K .

We now recall some important examples from the literature when the Bogomolov property is satisfied. The first result is a bound due to Schinzel [31]:

Theorem 31. *Assume that an algebraic number α of infinite multiplicative order is contained in a totally real field. Then, denoting by $\varphi = \frac{1+\sqrt{5}}{2}$ the golden ratio, we have*

$$h(\alpha) \geq \frac{1}{2} \log \varphi \approx 0.2406 \dots$$

Moreover, the same is true for α in a CM field provided one (and equivalently, all) of its Archimedean embeddings satisfy $|\alpha| \neq 1$.

We therefore get that Theorem 31 also applies to algebraic integers in CM fields, however there exist algebraic numbers which are not roots of unity but all of whose conjugates lie on the unit circle—in fact the bound is violated for such numbers. We do, however, have for abelian extensions the bound due to Amoroso–Dvornicich [32]:

Theorem 32. *Assume that an algebraic number α of infinite multiplicative order is contained in an abelian extension of \mathbb{Q} . Then we have*

$$h(\alpha) \geq \frac{\log 5}{12} \approx 0.1341 \dots$$

We may therefore record as a special case:

Corollary 33. *Any tower of cyclotomic fields satisfies Hypothesis 30 with constants $c_0 = \frac{1}{2} \log \varphi \approx 0.2406$ and $c_1 = \frac{\log 5}{12} \approx 0.1341$.*

Even in the special case of cyclotomic fields these bounds are reasonably sharp, for instance in the field $\mathbb{Q}(\zeta_{21})$ there is an algebraic number of height $\log(7)/12$. Concerning Schinzel’s result, we already have exceptions in the following range (see [33, Theorem 5.39]):

Theorem 34. *Suppose that β is a cyclotomic integer. Then the only values for $h_\infty(\beta)$ inside the interval $(0, 0.27132]$ occur for $\beta = 2 \cos(2\pi/5)$, $2 \cos(2\pi/7)$, $2 \cos(2\pi/60)$.*

Beyond these results, the Bogomolov property is itself well-studied and we list a number of subsets of $\overline{\mathbb{Q}}$ satisfying it and leading to towers of number fields verifying Hypothesis 30. We refer the reader to [33, Chapter 11] and [34] for more details.

- Generalizing the totally real case, Langevin [35] showed that the property holds for closed subsets of \mathbb{C} which do not contain the unit circle.
- Totally p -adic numbers or (infinite) Galois extensions with bounded local degree at some rational prime p satisfy Bogomolov’s property (see [36] and [37, Theorem 2]).
- Generalizing the abelian case, Habegger [38] shows that fields obtained adjoining torsion points of elliptic curves over \mathbb{Q} have the Bogomolov property. Amoroso–David–Zannier show [34, Theorem 1.5.] among others that infinite Galois extensions of a fixed number field with Galois group G have the Bogomolov property provided that G has finite exponent modulo center.

We end our discussion with some height bounds that work for every number field, in particular we state E. Dobrowolski’s asymptotic result [39, Theorem 1]:

Theorem 35. *Let α be an algebraic integer of degree d , not zero or a root of unity, and let $\varepsilon > 0$. Then for $d \geq d(\varepsilon)$ we have that*

$$h(\alpha) \geq \frac{1 - \varepsilon}{d} \cdot \left(\frac{\log \log d}{\log d} \right)^3.$$

Moreover, P. Voutier [40] showed that for any $d \geq 2$ we may take

$$h(\alpha) \geq \frac{1}{4d} \cdot \left(\frac{\log \log d}{\log d} \right)^3.$$

We therefore record the obvious but important remark:

Remark 36. *Any fixed number field K satisfies Hypothesis 30 for suitable constants.*

In particular, this will imply our limiting moment formulas established in this section are valid for any fixed number field and large enough rank.

5.2 Bounds for contributions from projective space

Throughout this section, $M \geq 1$ is a fixed integer and we write $\alpha = (\alpha_1, \dots, \alpha_M) \in K^M \setminus \{0\}$ as well as the height:

$$H_\infty(\alpha) = \prod_{\sigma: K \rightarrow \mathbb{C}} \max_{1 \leq j \leq M} \max(1, |\sigma(\alpha_j)|)$$

which specializes to the (exponential) Weil height when $M = 1$ and $\alpha \in \mathcal{O}_K^M$. We also write

$$h_\infty(\alpha) = \frac{1}{d} \log H_\infty(\alpha)$$

and denote the norm ⁴ of the denominator ideal generated by α by

$$D(\alpha) := N(\mathcal{O}_K + \alpha_1 \mathcal{O}_K + \dots + \alpha_M \mathcal{O}_K)^{-1}. \quad (15)$$

Observe that the inequalities:

$$D(\alpha)^{-1} \leq N(\alpha_1 \cdots \alpha_M)^{\frac{1}{M}} \leq H_\infty(\alpha)$$

follow from the definitions when the $\alpha_i \neq 0$ and that we have the relation

$$D(\alpha) \cdot N(\langle 1, \alpha_1, \dots, \alpha_M \rangle) = 1$$

with the norm defined under (8).

Our main goal in this subsection is to examine for $t > M \geq 1$ the sum

$$S_{M,t} := \sum_{\alpha \in (K^\times)^M} D(\alpha)^{-t} \text{vol}(B \cap \alpha_1^{-1} B \cap \dots \cap \alpha_M^{-1} B).$$

This will yield upper bounds on the A_m^2 -terms when $m = 1$ or can be viewed as bounding height zeta functions for projective spaces instead of the full Grassmannian variety $\mathbf{Gr}(m, K^n)$.

Lemma 37. *The quantity $N(\langle \alpha_0, \dots, \alpha_M \rangle)^t \text{vol}(\alpha_0^{-1} B \cap \alpha_1^{-1} B \cap \dots \cap \alpha_M^{-1} B)$ only depends on the class $[\alpha_0 : \dots : \alpha_M]$ in projective space $\mathbf{P}^M(K)$ modulo permutation of coordinates.*

Proof. Multiplying by a scalar $\lambda \in K^\times$ scales the volume by $N(\lambda)^{-t}$ whereas the index is scaled by $N(\lambda)$. \square

In particular, scaling by α_i of maximal norm this implies that we may restrict our computations for $S_{M,t}$ to the case where $N(\alpha_i^{-1}) \geq 1 \forall i$. We shall use the following convex combination lemma to bound volumes of intersections of scaled balls:

Lemma 38. *Let $M \geq 1$ and suppose $\alpha_0, \alpha_1, \dots, \alpha_M \in K^*$. Let B be an origin-centered ball of radius R in the space $K_{\mathbb{R}}^t$ with respect to the norm in Equation (3). Given that K^* acts on $K_{\mathbb{R}}^t$ diagonally, we have*

$$\text{vol}(\alpha_0 B \cap \alpha_1 B \cap \dots \cap \alpha_M B) \leq \text{vol}(B) \cdot \min_{\substack{c_i \geq 0 \\ \sum_i c_i = 1}} \left\{ \prod_{\sigma: K \rightarrow \mathbb{C}} \left(\sum_{i=0}^M c_i |\sigma(\alpha_i)|^2 \right)^{-\frac{t}{2}} \right\},$$

where the minimum is over any real convex combination of the α_i .

Proof. We are calculating the volume of the intersections of the following ellipsoids (see Equation (3)):

$$\left\{ x \in K_{\mathbb{R}}^t \mid \Delta_K^{-\frac{2}{[K:\mathbb{Q}]}} \sum_{j=1}^t \text{tr}(\alpha_i x_j \overline{\alpha_i x_j}) \leq R^2 \right\}, \text{ as } i \in \{0, 1, \dots, M\}$$

Observe that for any $\{c_0, \dots, c_M\} \in \mathbb{R}_{\geq 0}$ such that $\sum_i c_i = 1$, we have that

$$\bigcap_{i=0}^M \left\{ x \in K_{\mathbb{R}}^t \mid \Delta_K^{-\frac{2}{[K:\mathbb{Q}]}} \sum_{j=1}^t \text{tr}(\alpha_i x_j \overline{\alpha_i x_j}) \leq R^2 \right\} \subseteq \left\{ x \in K_{\mathbb{R}}^t \mid \Delta_K^{-\frac{2}{[K:\mathbb{Q}]}} \sum_{j=1}^t \text{tr} \left(\left(\sum_{i=0}^M c_i \alpha_i \overline{\alpha_i} \right) x_j \overline{x_j} \right) \leq R^2 \right\}$$

⁴We slightly abuse notations by decreeing our norms of algebraic numbers are positive, ergo the norms of the ideal they generate.

The ellipsoid defined on the right side has volume given by

$$\text{vol}(B) \prod_{\sigma: K \rightarrow \mathbb{C}} \left(\sum_i c_i |\sigma(\alpha_i)|^2 \right)^{-t/2}.$$

□

We are now in a position to connect the intersection volumes to Weil heights:

Lemma 39. *Let $\alpha_1, \dots, \alpha_M \in K^\times$. We have the bound:*

$$\frac{\text{vol}(B \cap \alpha_1 B \cap \dots \cap \alpha_M B)}{\text{vol}(B)} \leq \left(\frac{H_\infty(\alpha)^{\frac{2}{d}} + M \cdot H_\infty(\alpha)^{-\frac{2}{dM}} \cdot \text{N}(\alpha_1 \dots \alpha_M)^{\frac{2}{dM}}}{M+1} \right)^{-dt/2}.$$

Moreover, under the assumption that $\text{N}(\alpha_1 \dots \alpha_M) \geq 1$ we have for any $k \geq 2$:

$$\frac{\text{vol}(B \cap \alpha_1 B \cap \dots \cap \alpha_M B)}{\text{vol}(B)} \leq \text{N}(\alpha_1 \dots \alpha_M)^{\frac{t}{kM}} \cdot \left(\frac{H_\infty(\alpha)^{\frac{2(k-1)}{kd}} + M \cdot H_\infty(\alpha)^{-\frac{2(k-1)}{kMd}}}{M+1} \right)^{-dt/2}$$

Proof. Lemma 38 together with Lemma 16 comparing heights yields the inequality

$$\frac{\text{vol}(B \cap \alpha_1 B \cap \dots \cap \alpha_M B)}{\text{vol}(B)} \leq \left(\frac{H_\infty(\alpha)^{\frac{2}{d}} + M \cdot H_\infty(\alpha)^{-\frac{2}{dM}} \cdot \text{N}(\alpha_1 \dots \alpha_M)^{\frac{2}{dM}}}{M+1} \right)^{-\frac{1}{2}dt},$$

where we also applied the bound in Lemma 17. To obtain the second formulation we now factor out $\text{N}(\alpha_1 \dots \alpha_M)^{\frac{2}{kdM}}$ and writing

$$g_M(x) = \frac{x + Mx^{-\frac{1}{M}}}{M+1}$$

we have the bound

$$\begin{aligned} \text{N}(\alpha_1 \dots \alpha_M)^{\frac{t}{kM}} \cdot \left(\frac{H_\infty(\alpha)^{\frac{2}{d}} + M \cdot H_\infty(\alpha)^{-\frac{2}{dM}} \cdot \text{N}(\alpha_1 \dots \alpha_M)^{\frac{2}{d(M+1)}}}{M+1} \right)^{-dt/2} \\ \leq g_M \left(\frac{H_\infty(\alpha)^{\frac{2}{d}}}{\text{N}(\alpha_1 \dots \alpha_M)^{\frac{2}{kdM}}} \right)^{-dt/2}, \end{aligned}$$

using that $\text{N}(\alpha_1 \dots \alpha_M) \geq 1$. Now observe that $g_M(x)$ is increasing for $x, M \geq 1$ so that using the inequality $\text{N}(\alpha_1 \dots \alpha_M)^{1/M} \leq H_\infty(\alpha)$ we can bound

$$g_M \left(\frac{H_\infty(\alpha)^{\frac{2}{d}}}{\text{N}(\alpha_1 \dots \alpha_M)^{\frac{2}{kdM}}} \right) \geq g_M(H_\infty(\alpha)^{\frac{2(k-1)}{kd}}).$$

The claim follows. □

Remark 40. *The role of k in Lemma 39 and ensuing results is slightly artificial, but it allows us in later results to take k large enough so that we can control the sum of volume ratios over units for small t while the additional factor $\text{N}(\alpha)^{\frac{t}{kM}}$ allows us to relate the sum $S_{M,t}$ to a Dedekind zeta value. This leads to slightly better results for small moments.*

The following lemmas provide upper bounds for point counts in the unit lattice:

Lemma 41. *Assume Hypothesis 30 and its notations. Consider the canonical log embedding: $L : K^\times \rightarrow \mathbb{R}^{r_1+r_2}$ defined by mapping*

$$\alpha \mapsto (\log |\sigma_1(\alpha)|, \dots, 2 \log |\sigma_{r_1+r_2}(\alpha)|),$$

as well as the function

$$h : \mathbb{R}^{r_1+r_2} \rightarrow \mathbb{R}_{\geq 0}$$

$$x \mapsto \frac{1}{[K:\mathbb{Q}]} \cdot \sum_{j=1}^{r_1+r_2} \max(0, x_j).$$

Then for any $\eta \in \mathbb{R}^{r_1+r_2}$ with $\sum_{j=1}^{r_1+r_2} \eta_j = Y$ and any $B \geq 0$ we have that

$$\#\{\beta \in \mathcal{O}_K^\times \mid h(\eta + L(\beta)) \leq B\} \leq \omega_K \cdot \left(\frac{B + c_0/2 + \max(0, -\frac{Y}{d})}{c_0/2} \right)^{r_1+r_2-1}.$$

Proof. Note that the factor of 2 at complex places in the definition of L ensures that $L(\mathcal{O}_K^\times)$ is contained in the hyperplane $H := \{x \in \mathbb{R}^{r_1+r_2} : \sum_{j=1}^{r_1+r_2} x_j = 0\}$. Observe that h satisfies the triangle inequality and in fact satisfies the properties of a semi-norm on H . Now by Hypothesis 30 we obtain for any $\beta \in \mathcal{O}_K^\times \setminus \mu_K$ that

$$h(L(\beta)) = h_\infty(\beta) \geq c_0.$$

Let now $P = \{\xi \in H : h(\xi) \leq c_0/2\}$. We claim that for $\eta \in \mathbb{R}^{r_1+r_2}$ and $\beta_1, \beta_2 \in \mathcal{O}_K^\times$:

$$(L(\beta_1) + \eta + P) \cap (L(\beta_2) + \eta + P) = \begin{cases} L(\beta_1) + \eta + P & \text{if } \beta_1\beta_2^{-1} \in \mu_K \\ \emptyset & \text{else.} \end{cases}$$

To prove the claim, let y be in the intersection. Then by the triangle inequality we have that

$$h(L(\beta_1^{-1}\beta_2)) \leq h(y - L(\beta_1) - \eta) + h(L(\beta_2) + \eta - y) \leq c_0$$

and therefore $\beta_1\beta_2^{-1} \in \mu_K$. Since L is a homomorphism to the additive group whose kernel is μ_K the claim follows.

Moreover, if for $\beta \in \mathcal{O}_K^\times$ we have that $h(\eta + L(\beta)) \leq B$, then $L(\beta) + \eta + P$ is contained in the set

$$Q = \{\xi \in \mathbb{R}^{r_1+r_2} : \sum_{j=1}^{r_1+r_2} \xi_j = Y, h(\xi) \leq B + c_0/2\}.$$

For any fixed η , we thus obtain by the claim that

$$\#\{\beta \in \mathcal{O}_K^\times \mid h(\eta + L(\beta)) \leq B\} \leq \omega_K \cdot \frac{\text{vol}(Q)}{\text{vol}(P)},$$

where the volumes are computed with respect to the natural measure identifying the hyperspaces P and Q are in with $\mathbb{R}^{r_1+r_2-1}$.

For η such that $Y = \sum_{j=1}^{r_1+r_2} \eta_j \geq 0$, it is easy to see that the volume of Q is bounded by the volume of $P_B = \{\xi \in H : h(\xi) \leq c_0/2 + B\}$. Thus we bound the desired unit count by

$$\omega_K \cdot \frac{\text{vol}(P_B)}{\text{vol}(P)} = \omega_K^M \cdot \frac{\text{vol}(\{\xi \in H : h(\xi) \leq c_0/2 + B\})}{\text{vol}(\{\xi \in H : h(\xi) \leq c_0/2\})}.$$

Since H is an \mathbb{R} -vector space of dimension $r_1 + r_2 - 1$ and h a semi-norm on that vector space, the result follows for $Y \geq 0$.

When $Y < 0$, observe that $\tilde{\eta}$ defined by $\tilde{\eta}_j = \eta_j - \frac{Y}{r_1+r_2}$ satisfies

$$\sum_{j=1}^{r_1+r_2} \tilde{\eta}_j = 0 \text{ and } h(\tilde{\eta}) \leq h(\eta) + h\left(-\frac{Y}{r_1+r_2}\right).$$

Therefore, given that $h(\eta + L(\beta)) \leq B$ implies $h(\tilde{\eta} + L(\beta)) \leq B + h\left(-\frac{Y}{r_1+r_2}\right)$, we may obtain an upper bound by running the same argument as in the first part of the proof with $\tilde{\eta}$ instead of η and $B + h\left(-\frac{Y}{r_1+r_2}\right)$ instead of B . This settles the case of $Y < 0$ since $h\left(-\frac{Y}{r_1+r_2}\right) = -Y/d$. \square

Note that we also have the following inequality by definition:

Lemma 42. *Let $\alpha \in (\overline{K}^\times)^M$ be an M -tuple of algebraic numbers. Then $h_\infty(\alpha) \geq \max_{1 \leq i \leq M} h_\infty(\alpha_i)$.*

Lemma 43. *Assume Hypothesis 30 and its notations. Let $\alpha \in (K^\times)^M$ and $B \geq 0$. Then*

$$\#\{\beta \in (\mathcal{O}_K^\times)^M \mid h_\infty(\alpha\beta) \leq B\} \leq \omega_K^M \cdot \prod_{1 \leq i \leq M} \left(\frac{B + c_0/2 + \max(0, -\frac{\log N(\alpha_i)}{d})}{c_0/2} \right)^{(r_1+r_2-1)}.$$

Proof. By Lemma 42, we have that

$$\#\{\beta \in (\mathcal{O}_K^\times)^M \mid h_\infty(\alpha\beta) \leq B\} \leq \prod_{1 \leq i \leq M} \#\{\beta \in \mathcal{O}_K^\times \mid h_\infty(\alpha_i\beta) \leq B\}$$

We conclude by Lemma 41. \square

Proposition 44. *Assume Hypothesis 30 and its notations and fix $k \geq 2$. There exist positive constants $C, \varepsilon_1 > 0$ uniformly bounded in d, t such that for all $\alpha \in (K^\times)^M \setminus \mu_K^M$ with $N(\alpha_i) \geq 1$ for $i \in [1, \dots, M]$ the following holds: write*

$$t_0 = \frac{2r_K \cdot M}{d} \cdot \frac{\log(2 + \frac{1}{2k})}{\log(f_M(c_0(1 - \frac{1}{k})))},$$

where $f_M(x) := \frac{\exp(x) + M \exp(-\frac{x}{M})}{M+1}$ and r_K is the rank of the unit group. Then we have for any $t > t_0$ and any $d \geq 1$ that

$$\sum_{\substack{\beta \in (\mathcal{O}_K^\times)^M \\ \alpha\beta \notin \mu_K^M}} \frac{\text{vol}(B \cap (\alpha_1\beta_1)^{-1}B \cap \dots \cap (\alpha_M\beta_M)^{-1}B)}{\text{vol}(B)} \leq C \cdot \omega_K^M \cdot N(\alpha)^{\frac{-t}{kM}} \cdot D(\alpha)^{\frac{t}{4}} \cdot e^{-\varepsilon_1 \cdot d \cdot (t-t_0)}.$$

Moreover, the constants can be made explicit. We may for instance take

$$\varepsilon_1 = \frac{1}{2} \min \left\{ \frac{c_1}{8}, \log(f_M(\frac{3}{4}c_1)), \alpha_M \cdot \frac{c_0(k-1)}{k} \right\}$$

and $C = 1 + \frac{1}{1 - e^{-\alpha_M \cdot c_0 \cdot d \cdot (t-t_0) \cdot (k-1)/(4k^2)}}$, where $\alpha_M > 0$ is small enough so that $f_M(x) \geq e^{\alpha_M \cdot x}$ for $x \geq c_0/2$.

Proof. We consider the function $f_M(x) := \frac{\exp(x) + M \exp(-x/M)}{M+1}$ satisfying $f_1(x) = \cosh(x)$, $f_M(0) = 1$ and increasing exponentially for $x > 0$. We also abbreviate $N(\alpha) = \prod_i N(\alpha_i)$. Then by Lemma 39 our task is reduced to bounding for suitably chosen $k \geq 2$:

$$\sum_{\substack{\beta \in (\mathcal{O}_K^\times)^M \\ \alpha\beta \notin (\mu_K)^M}} N(\alpha)^{\frac{-t}{kM}} \cdot f_M(h_\infty(\alpha\beta) \cdot (2(1 - \frac{1}{k})))^{-dt/2},$$

where $h_\infty(\alpha\beta) = \frac{1}{d} \cdot \log(H_\infty(\alpha\beta))$ reduces to the log Weil height for $M = 1$. Recall the c_0 defined in Hypothesis 30. Since f_M is increasing it suffices to bound, for any $S \in \mathbb{Z}_{>0}$, the sum

$$\Sigma_{M,k}^\infty := \sum_{n=S}^\infty \#\left\{ \beta \in (\mathcal{O}_K^\times)^M \mid h_\infty(\alpha\beta) \in \left[\frac{nc_0}{2S}, \frac{(n+1)c_0}{2S} \right] \right\} \cdot f_M\left(\frac{nc_0(1 - \frac{1}{k})}{S}\right)^{-dt/2}$$

together with the term with the contribution of the remaining units satisfying $h_\infty(\alpha\beta) < c_0/2$:

$$\Sigma_{M,k}^{c_0} := \sum_{\substack{\beta \in (\mathcal{O}_K^\times)^M \\ h_\infty(\alpha\beta) < \frac{c_0}{2}}} f_M(h_\infty(\alpha\beta) \cdot 2(1 - \frac{1}{k}))^{-dt/2}.$$

So our goal is to show for appropriate constants C, ε_1 that

$$\Sigma_{M,k}^{c_0} + \Sigma_{M,k}^\infty \leq C \cdot D(\alpha)^{\frac{t}{4}} \cdot e^{-\varepsilon_1 \cdot d \cdot (t-t_0)}.$$

Let us examine the term $\Sigma_{M,k}^{c_0}$ first. We have the bound on the number of units

$$\#\{\beta \in (\mathcal{O}_K^\times)^M \mid h_\infty(\alpha\beta) < c_0/2\} \leq \omega_K^M.$$

Indeed, let $\beta_1 = (\beta_{11}, \dots, \beta_{1M})$ and $\beta_2 = (\beta_{21}, \dots, \beta_{2M})$ be in $(\mathcal{O}_K^\times)^M$. Then, for we know that for each $j = 1, 2$ and each $i = 1, \dots, M$ we have $h_\infty(\alpha_i \beta_{ji}) < \frac{c_0}{2}$. Then by the triangle inequality (c.f. Lemma 41), we can show that $h_\infty(\beta_{1j}^{-1} \beta_{2j}) < c_0$ so that $\beta_1 \beta_2^{-1} \in (\mu_K)^M$.

By assumption, since $\alpha\beta \notin (\mu_K)^M$ there exists a constant c_1 such that

$$h(\alpha\beta) = h_\infty(\alpha\beta) + \frac{1}{d} \cdot \log D(\alpha) \geq c_1 > 0.$$

Let us first assume that $D(\alpha) < \exp(dc_1/4)$. Then $\Sigma_{M,k}^{c_0}$ is bounded by

$$\omega_K^M \cdot f_M \left(2\left(1 - \frac{1}{k}\right) \cdot \left(c_1 - \frac{1}{d} \cdot \log D(\alpha)\right)\right)^{-dt/2} \leq \omega_K^M \cdot f_M \left(2\left(1 - \frac{1}{k}\right) \cdot \frac{3}{4}c_1\right)^{-dt/2} \leq \omega_K^M \cdot f_M \left(\frac{3}{4}c_1\right)^{-dt/2}.$$

In the case when $D(\alpha) \geq \exp(dc_1/4)$, we simply bound the contribution $\Sigma_{M,k}^{c_0}$ by observing that $D(\alpha)^{-\frac{t}{4}} \leq e^{-\frac{dtc_1}{16}}$, so that these terms satisfy the bound claimed in the proposition.

We may now therefore turn to the remaining terms $\Sigma_{M,k}^\infty$. Since, we assumed that $N(\alpha_i) \geq 0$, we know that $\max(0, -\frac{1}{d} \log N(\alpha_i)) = 0$. Lemma 43 therefore yields:

$$\begin{aligned} \Sigma_{M,k}^\infty &\leq \omega_K^M \cdot \sum_{n=S}^{\infty} \left(\frac{n+S+1}{S}\right)^{(r_1+r_2-1)M} \cdot f_M\left(\frac{n}{S} \cdot c_0\left(1 - \frac{1}{k}\right)\right)^{-dt/2} \\ &= \omega_K^M \cdot \sum_{n=1}^{\infty} \left(\frac{n}{S} + 2\right)^{(r_1+r_2-1)M} \cdot f_M\left(\frac{n+S-1}{S} \cdot c_0\left(1 - \frac{1}{k}\right)\right)^{-dt/2} \\ &\leq \omega_K^M \cdot \sum_{n=1}^{\infty} f_M\left(\frac{S+n-1}{S} \cdot c_0\left(1 - \frac{1}{k}\right)\right)^{-\frac{d(t-t_0)}{2}} \\ &\leq \omega_K^M \cdot \sum_{n=S}^{\infty} \exp\left(-n \cdot \frac{\alpha_M \cdot c_0(k-1) \cdot d(t-t_0)}{2kS}\right) \end{aligned} \tag{16}$$

where $\alpha_M > 0$ is a constant small enough so that $f_M(x) \geq e^{\alpha_M \cdot x}$ if $x \geq c_0/2$ and where

$$t_0 \geq \frac{2(r_1 + r_2 - 1)M}{d} \sup_{n \in \mathbb{N}_{\geq 1}} \frac{\log\left(\frac{n}{S} + 2\right)}{\log\left(f_M\left(\frac{S+n-1}{S} \cdot c_0 \cdot \left(1 - \frac{1}{k}\right)\right)\right)}$$

for suitable k . The logarithm ratio decays as n increases and therefore it suffices to take

$$t_0 \geq \frac{2(r_1 + r_2 - 1)M}{d} \cdot \frac{\log\left(\frac{1}{S} + 2\right)}{\log\left(f_M\left(c_0\left(1 - \frac{1}{k}\right)\right)\right)}.$$

Summing up the geometric series in (16) gives us

$$\Sigma_{M,k}^\infty \leq \omega_K^M \cdot \frac{\exp\left(-\frac{\alpha_M \cdot c_0(k-1) \cdot d(t-t_0)}{2k}\right)}{1 - \exp\left(-\frac{\alpha_M \cdot c_0(k-1) \cdot d(t-t_0)}{2kS}\right)}.$$

We chose to present the results for the choice of $S = 2k$.

□

5.3 Summing over ideals

It remains to sum the contributions in Proposition 44 over principal ideals. To that end, we have:

Lemma 45. *Let $\mathcal{J} \subset \mathcal{O}_K$ be an integral ideal. Then for any real $t > 1$ we have:*

$$\sum_{\substack{\mathcal{I} \subset \mathcal{J} \\ \text{integral ideal}}} N(\mathcal{I})^{-t} = N(\mathcal{J})^{-t} \cdot \zeta_K(t)$$

Proof. The proof follows from the definitions since we are in a Dedekind domain: for instance writing the prime decomposition $\mathcal{J} = \prod_i \mathcal{P}_i$, the left hand side becomes

$$\sum_{\substack{\mathcal{I} \subset \mathcal{O}_K \\ \mathcal{I} \text{ integral ideal}}} N(\mathcal{I} \cdot \prod_i \mathcal{P}_i)^{-t} = N(\prod_i \mathcal{P}_i)^{-t} \cdot \sum_{\substack{\mathcal{I} \subset \mathcal{O}_K \\ \mathcal{I} \text{ integral ideal}}} N(\mathcal{I}).$$

□

We can now reformulate the $m = 1$ term for the n -th moment:

Proposition 46. *Let $\alpha_1, \dots, \alpha_M \in K^\times$. Then the $m = 1$ term in Theorem 10 is given for indicator functions of balls by*

$$\sum_{\alpha_1, \dots, \alpha_M \in K^\times} D(\alpha)^{-t} \cdot \text{vol}(B \cap \alpha_1 B \cap \dots \cap \alpha_M B),$$

where $D(\alpha)$ is as defined in (15). Moreover, for any function $f_M : K^{\times, M} \rightarrow \mathbb{R}$ and any $T \in \mathbb{R}_{>1}$, the sum

$$\sum_{\alpha_1, \dots, \alpha_M \in K^\times} D(\alpha)^{-T} \cdot \text{vol}(B \cap \alpha_1 B \cap \dots \cap \alpha_M B) \cdot f_M(\alpha_1, \dots, \alpha_M)$$

equals:

$$\zeta_K(T)^{-1} \cdot \sum_{\substack{\mathcal{I} \subset \mathcal{O}_K \\ \mathcal{I} \text{ integral ideal}}} N(\mathcal{I})^{-T} \sum_{\alpha_1, \dots, \alpha_M \in \mathcal{I}^{-1} \setminus \{0\}} \text{vol}(B \cap \alpha_1 B \cap \dots \cap \alpha_M B) \cdot f_M(\alpha_1, \dots, \alpha_M).$$

Proof. For the first expression, it suffices to see that the index of $\{c \in \mathcal{O}_K : c \cdot \alpha_i \in \mathcal{O}_K \forall i\}$ in \mathcal{O}_K is equivalent to the index of $(\alpha_1, \dots, \alpha_M)^{-1} \cap \mathcal{O}_K$ in \mathcal{O}_K , where $(\alpha_1, \dots, \alpha_M)$ denotes the fractional ideal generated by the α_i . Let now \mathcal{J} denote the integral ideal $(\alpha_1, \dots, \alpha_M)^{-1} \cap \mathcal{O}_K$. To establish the equivalence of the second expression, observe that for an integral ideal $\mathcal{I} \subset \mathcal{O}_K$ we have

$$\alpha_1, \dots, \alpha_M \in \mathcal{I}^{-1} \Leftrightarrow \mathcal{I} \subset (\alpha_1, \dots, \alpha_M)^{-1} \cap \mathcal{O}_K = \mathcal{J}.$$

Thus in the second expression every tuple $\alpha_1, \dots, \alpha_M$ contributes

$$\zeta_K(T)^{-1} \cdot \sum_{\substack{\mathcal{I} \subset \mathcal{J} \\ \mathcal{I} \text{ integral ideal}}} N(\mathcal{I})^{-T} \cdot \text{vol}(B \cap \alpha_1 B \cap \dots \cap \alpha_M B) \cdot f_M(\alpha_1, \dots, \alpha_M).$$

In the first expression the contribution is $N(\mathcal{J})^{-T} \cdot \text{vol}(B \cap \alpha_1 B \cap \dots \cap \alpha_M B) \cdot f_M(\alpha_1, \dots, \alpha_M)$. We conclude by Lemma 45 that the two expressions are equal. □

We can now put everything together:

Proposition 47. *Assume Hypothesis 30 and its notations and fix $k \geq 2$. There exist positive constants $C_M, \varepsilon_M > 0$ uniformly bounded in d, t such that the following holds: write*

$$t_0 = \sup_{K \in \mathcal{S}} \left\{ kM + \frac{1}{2}, \frac{2r_K \cdot M}{d} \cdot \frac{\log(2 + \frac{1}{2k})}{\log(f_M(c_0(1 - \frac{1}{k})))} \right\},$$

where $f_M(x) := \frac{\exp(x) + M \exp(-\frac{x}{M})}{M+1}$ and r_K is the rank of the unit group. For any $t > t_0$ we then have:

$$\sum_{\alpha \in (K^\times)^M \setminus \mu_K^M} D(\alpha)^{-t} \text{vol}(B \cap \alpha_1^{-1} B \cap \dots \cap \alpha_M^{-1} B) \leq C_M \cdot \omega_K^M \cdot \frac{\zeta_K(t(\frac{3}{4} - \frac{1}{k})) \cdot \zeta_K(\frac{t}{kM})^M}{\zeta_K(\frac{3t}{4})} \cdot e^{-\varepsilon_M \cdot d \cdot (t-t_0)} \cdot \text{vol}(B).$$

We may moreover take

$$\varepsilon_M = \frac{1}{2} \min \left\{ \frac{c_1}{8}, \log(f_M(\frac{3}{4}c_1)), \alpha_M \cdot \frac{c_0(k-1)}{k} \right\}$$

and $C_M = (2M+1)(1 + \frac{1}{1 - e^{-\alpha_M \cdot c_0 \cdot d \cdot (t-t_0)(k-1)/(4k^2)}})$, where $\alpha_M > 0$ is small enough so that $f_M(x) \geq e^{\alpha_M \cdot x}$ for $x \geq c_0/2$.

Proof. After multiplying by a constant $2M$, we may in addition assume that $N(\alpha_i) \geq 1$. Indeed we may cover $(K^\times)^M \setminus \mu_K^M$ by M sets on which $N(\alpha_i)$ is smallest for some fixed $1 \leq i \leq M$. By Lemma 37 and the ensuing remark, for each such set the contribution is bounded by twice the contribution of $\{\alpha \in (K^\times)^M \setminus \mu_K^M : N(\alpha_i) \geq 1 \forall i\}$. Using Proposition 44, we immediately obtain (constants C, ε_1 as in 44):

$$\sum_{\alpha \in (\mathcal{O}_K^\times)^M \setminus (\mu_K^\times)^M} D(\alpha)^{-t} \text{vol}(B \cap \alpha_1^{-1}B \cap \dots \cap \alpha_M^{-1}B) \cdot \text{vol}(B)^{-1} \leq C \cdot \omega_K^M \cdot e^{-\varepsilon_1 \cdot d \cdot (t-t_0)}.$$

It remains to bound:

$$\sum_{\substack{\alpha \in (K^\times)^M \setminus (\mathcal{O}_K^\times)^M \\ N(\alpha_i) \geq 1}} D(\alpha)^{-t} \text{vol}(B \cap \alpha_1^{-1}B \cap \dots \cap \alpha_M^{-1}B) \cdot \text{vol}(B)^{-1}.$$

We apply Proposition 44 and deal with bounding (constants C, ε_1 as in 44) the sum

$$\sum_{\substack{\alpha \in (K^\times)^M \setminus (\mathcal{O}_K^\times)^M \\ N(\alpha_i) \geq 1}} C \cdot D(\alpha)^{-t} N(\alpha)^{\frac{-t}{kM}} \cdot D(\alpha)^{\frac{t}{4}} \cdot e^{-\varepsilon_1 \cdot d \cdot (t-t_0)}.$$

Using the Proposition 46 with $T = \frac{3}{4}t$, it therefore suffices to bound

$$\zeta_K\left(\frac{3t}{4}\right)^{-1} \cdot \sum_{\substack{\mathcal{I} \subset \mathcal{O}_K \\ \mathcal{I} \text{ integral ideal}}} N(\mathcal{I})^{\frac{3t}{4}} \sum_{\substack{\alpha_i \in (\mathcal{I}^{-1} \setminus \{0\}) / \mathcal{O}_K^\times \\ N(\alpha_i) \geq 1}} N(\alpha)^{\frac{-t}{kM}} \cdot e^{-\varepsilon_1 \cdot d \cdot (t-t_0)}.$$

Now observe that the map $\alpha_i \mapsto (\alpha_i) \cdot \mathcal{I}$ gives a bijection between $(\mathcal{I}^{-1} \setminus \{0\}) / \mathcal{O}_K^\times$ and integral ideals $\mathcal{J} \subset \mathcal{O}_K$ in the ideal class of \mathcal{I} . We may therefore bound this expression by:

$$\zeta_K\left(\frac{3t}{4}\right)^{-1} \cdot \sum_{\substack{\mathcal{I} \subset \mathcal{O}_K \\ \mathcal{I} \text{ integral ideal}}} N(\mathcal{I})^{\frac{3t}{4}} \prod_{1 \leq i \leq M} \sum_{\substack{\mathcal{J} \subset \mathcal{O}_K \\ N(\mathcal{I}) \leq N(\mathcal{J})}} N(\mathcal{J}\mathcal{I}^{-1})^{-\frac{t}{kM}} \cdot e^{-\varepsilon_1 \cdot d \cdot (t-t_0+1)}$$

and therefore as claimed by

$$\frac{\zeta_K\left(t\left(\frac{3}{4} - \frac{1}{k}\right)\right) \cdot \zeta_K\left(\frac{t}{kM}\right)^M}{\zeta_K\left(\frac{3t}{4}\right)} \cdot e^{-\varepsilon_1 \cdot d \cdot (t-t_0)}.$$

We see that in particular taking $k \geq 2$ and $t \geq kM + 1/2$ suffices for convergence of the zeta factors for any given d and we obtain the explicit constants by setting $C_M = (2M + 1) \cdot C$ and $\varepsilon_M = \varepsilon_1$. \square

We therefore find:

Theorem 48. *Let \mathcal{S} denote any set of number fields satisfying Hypothesis 30 and let c_0, c_1 denote the resulting uniform constants. For any choice of $k \geq 2$ there exist positive constants $C_M, \varepsilon_M > 0$ uniformly bounded in d, t such that the following holds: write*

$$t_0 = \sup_{K \in \mathcal{S}} \left(kM + \frac{1}{2}, \frac{2r_K \cdot M}{d} \cdot \frac{\log\left(2 + \frac{1}{2k}\right)}{\log\left(f_M(c_0(1 - \frac{1}{k}))\right)} \right),$$

where

$$f_M(x) = \frac{\exp(x) + M \exp(-x/M)}{M+1}$$

and r_K is the rank of the unit group. We then have for any $t > t_0$ and for any $K \in \mathcal{S}$ of degree d :

$$\sum_{\alpha \in (K^\times)^M} D(\alpha)^{-t} \text{vol}(B \cap \alpha_1^{-1}B \cap \dots \cap \alpha_M^{-1}B) = \text{vol}(B) \cdot \omega_K^M \left(1 + C_M \cdot Z(K, t, M, k) \cdot e^{-\varepsilon_M \cdot d \cdot (t-t_0)} \right),$$

where

$$0 \leq Z(K, t, M, k) \leq \zeta_K\left(t\left(\frac{3}{4} - \frac{1}{k}\right)\right) \cdot \zeta_K\left(\frac{t}{kM}\right)^M \cdot \zeta_K\left(\frac{3t}{4}\right)^{-1}.$$

We may moreover take ε_M and C_M as in Proposition 47.

Proof. This follows from the previous proposition and the fact that $\text{vol}(B \cap \alpha^{-1}B) = \text{vol}(B)$ if $\alpha \in \mu_K$. \square

Remark 49. If we consider cyclotomic fields of increasing degree, we may take $c_0 = 0.24$ and for $M = 1$ the condition on t is satisfied for $t_0 < 27, k = 26$. For $M = 2, 3, 4, 5$ we get $t_0 < 97, 213, 372, 576$ and $k = 48, 70, 92, 115$. As a function of M , a calculation shows that we have $t_0 \leq CM^2$ for $C \approx 22.18 \dots$ as M grows.

Note that $\omega_K^M = o(d^{M+1})$ so that we indeed obtain exponential decay of the error term and in particular deduce a result for the second moment:

Corollary 50. Let \mathcal{S} denote any set of number fields satisfying Hypothesis 30 and let c_0, c_1 denote the resulting uniform constant. Then for any choice of $k \geq 2$ there exist positive uniformly bounded constants $C, \varepsilon > 0$ such that the following holds: write

$$t_0 = \sup_{K \in \mathcal{S}} \left\{ k + \frac{1}{2}, \frac{2r_K}{d} \cdot \frac{\log(2 + \frac{1}{2k})}{\log(\cosh(c_0(1 - \frac{1}{k})))} \right\},$$

where r_K is the rank of the unit group. We then have for any $t > t_0$ and for any $K \in \mathcal{S}$ of degree d that the second moment $\mathbb{E}[\rho(\Lambda)^2]$ of the number of nonzero \mathcal{O}_K -lattice points in a fixed origin-centered ball of volume V in $K_{\mathbb{R}}^t$ satisfies:

$$\begin{aligned} V^2 + \omega_K \cdot V &\leq \mathbb{E}[\rho(\Lambda)^2] \\ &\leq V^2 + \omega_K \cdot V + \omega_K^2 \cdot C \cdot Z(K, t, k) \cdot e^{-\varepsilon \cdot d \cdot (t - t_0)} \cdot V, \end{aligned}$$

where $0 \leq Z(K, t, k) \leq \zeta_K(t(\frac{3}{4} - \frac{1}{k})) \cdot \zeta_K(\frac{t}{k}) \cdot \zeta_K(\frac{3t}{4})^{-1}$.

We may moreover take $\varepsilon = \frac{1}{2} \min(\frac{c_1}{8}, \log(\cosh(3c_1/4))), \frac{2c_0(k-1)}{5k})$ and $C = 3 + \frac{3}{1 - e^{-c_0 \cdot d(t-t_0)(k-1)/(10k^2)}}$.

Proof. This follows from Theorem 48 for $M = 1$. The explicit constants can be obtained by bounding $\cosh(x) > e^{\frac{2}{5} \min(x, x^2)}$. \square

See Corollary 3 for the ensuing second moment result for cyclotomic fields. To go beyond the second and third moments we shall extend this approach in the next section.

5.4 General error estimates for A_m^2 -type terms

In this section, we estimate the contributions of more general subspaces of dimension m to the integral formula by reducing to our previous considerations for projective space. Recall from Section 4 the set of matrices

$$A_m^2 = \left\{ D \in M_{m \times n}(K) \mid \begin{array}{l} D_{ij} \in K, \\ D \text{ is in row-reduced echelon form of rank}(D)=m \\ D \text{ has at least one entry } \notin \mu_K \cup \{0\} \end{array} \right\}.$$

The main result of this section is the following:

Theorem 51. Let \mathcal{S} denote any set of number fields satisfying Hypothesis 30 and let c_0, c_1 denote the resulting uniform constants. Fix n and $2 \leq m < n$. There exist explicit positive uniform constants $C_{\mathcal{S}}, \varepsilon_{\mathcal{S}} > 0$ such that the following holds: write t_0 for

$$2(n-m) \cdot \sup_{K \in \mathcal{S}} \left\{ m^2 + m, \frac{r_K(m^2 + m)}{d} \cdot \frac{\log(2 + 12c_0^{-1} + 2 \log(n-m) \cdot c_0^{-1})}{\log(\min\{\frac{64}{27}, e^{\frac{1}{3}c_1}, \cosh^3(c_1)\})}, \frac{r_K}{d} \cdot \log_2^{-1}(f_{n-m}(\frac{3}{4}c_0)) \right\},$$

where r_K is the rank of the unit group and $f_{n-m}(x) = \frac{e^x + (n-m)e^{-\frac{x}{n-m}}}{1+n-m}$. We then have for any $t > t_0$ and for any $K \in \mathcal{S}$:

$$\frac{1}{V(td)^m R^{mtd}} \sum_{D \in A_m^2} \frac{1}{\mathfrak{D}(D)^t} \int_{K_{\mathbb{R}}^{m \times t}} f(xD) dx \leq C_{\mathcal{S}} \cdot \omega_K^{m(n-m)}(td)^{\frac{m-1}{2}} \cdot Z(K, t, n, m) \cdot e^{-\varepsilon_{\mathcal{S}} \cdot d \cdot (t - t_0)},$$

with the zeta factor

$$Z(K, t, n, m) = \frac{\zeta_K\left(\frac{1}{2(m+1)}t - \frac{1}{e}m(n-m)\right) \cdot \zeta_K\left(\frac{t}{4m(n-m)}\right)^{m(n-m)}}{\zeta_K(t-1)}.$$

Moreover, we may take

$$\varepsilon_S = \frac{1}{2} \log(\min\{\frac{4}{3}, e^{\frac{c_1}{3(m+1)}}, f_{n-m}(3c_1/4)\}).$$

The constant C_S may also be chased down as a function depending only m, n, c_0, c_1 .

Remark 52. Note that despite the relatively ugly expression for the minimal rank t_0 , we have that $t_0(n) = O(n^3 \log \log n)$ as the moment n increases with a constant only depending on the choice of number fields \mathcal{S} .

In order to prove the theorem, we will actually subdivide the A_m^2 -terms as follows: write

$$\begin{aligned} A_m^{2,0} &= \left\{ D \in M_{m \times n}(K) \mid \begin{array}{l} D_{ij} \in K, \\ D \text{ is in row-reduced echelon form of rank}(D)=m \\ D \text{ has exactly one non-zero entry per column} \\ D \text{ has at least one entry } \notin \mu_K \cup \{0\}. \end{array} \right\}, \\ A_m^{2,h_0} &= \left\{ D \in M_{m \times n}(K) \mid \begin{array}{l} D_{ij} \in K, \\ D \text{ is in row-reduced echelon form of rank}(D)=m \\ D \text{ has all entries of Weil height less than } h_0 \\ D \text{ has at least one entry } \notin \mu_K \cup \{0\}. \end{array} \right\} \setminus A_m^{2,0}, \\ A_m^{2,\infty} &= \left\{ D \in M_{m \times n}(K) \mid \begin{array}{l} D_{ij} \in K, \\ D \text{ is in row-reduced echelon form of rank}(D)=m \\ D \text{ has at least one entry of Weil height larger than } h_0 \end{array} \right\} \setminus A_m^{2,0} \end{aligned}$$

for a suitable choice of threshold height $h_0 > 0$. These sets clearly cover A_m^2 and we show that the contribution of each term decays exponentially.

Consider first the $A_m^{2,0}$ -type terms. In this case, the contributions can via a separation of variables be reduced to products of intersections of shifted balls as in subsection 5.2. We have thus already done all the work and the results follow from Theorem 48. This in turn allows us to assume that D in A_m^{2,h_0} has at least one column with multiple entries. We prove the contributions of such terms decay similarly to Lemma 26 even for relatively small height by cherry-picking a particular column of D to which to apply estimates (see Lemma 54). Finally, h_0 is chosen large enough so that the terms in $A_m^{2,\infty}$ have exponentially decaying contributions purely for height reasons.

The following convex combination lemmas will allow us to handle the A_m^{2,h_0} and $A_m^{2,\infty}$ -type terms.

Lemma 53. Let $f : K_{\mathbb{R}}^t \rightarrow \mathbb{R}$ be the indicator function of a ball of radius $R > 0$ and assume $n > m \geq 2$. Then, for any $(\alpha_{i,j}) \in M_{(n-m) \times m}(K)$, we have that

$$\begin{aligned} & \frac{\int_{K_{\mathbb{R}}^{m \times t}} f(x_1) \cdots f(x_m) \prod_{j=1}^{n-m} f\left(\sum_{i=1}^m \alpha_{i,j} x_i\right) dx_1 \cdots dx_m}{V(mt[K : \mathbb{Q}]) R^{mt[K : \mathbb{Q}]}} \\ & \leq (m+1)^{mtd/2} \cdot \min_{1 \leq k \leq n-m} \min_{J \in \binom{[n-m]}{k}} \prod_{\sigma : K \rightarrow \mathbb{C}} \left(1 + \frac{1}{k} \sum_{j \in J} \sum_{i=1}^m |\sigma(\alpha_{i,j})|^2 \right)^{-\frac{t}{2}}. \end{aligned}$$

Proof. We will again use the idea of convex combinations, see Lemma 68 of the appendix for a slightly more general result and an alternative derivation. Let $c_k \in [0, 1]$ for $1 \leq k \leq n$ be any coefficients satisfying $\sum_{k=1}^n c_k = 1$. Then for $(x_1, \dots, x_m) \in K_{\mathbb{R}}^{t \times m}$ the conditions $\|x_1\| \leq R, \dots, \|x_m\| \leq R$ and $\|\sum_{i=1}^m \alpha_{i,j} x_i\| \leq R$ for $1 \leq j \leq n-m$ imply that

$$c_1 \|x_1\|^2 + \cdots + c_m \|x_m\|^2 + \sum_{j=1}^{n-m} c_{j+m} \cdot \left\| \sum_{i=1}^m \alpha_{i,j} x_i \right\|^2 \leq R^2. \quad (17)$$

Equation (17) then defines an ellipsoid in $K_{\mathbb{R}}^{t \times m}$. The relevant quadratic form is scaled by a symmetric matrix that in each copy of \mathbb{R}^m looks like (after fixing one of the t copies and an embedding $\sigma : K \rightarrow \mathbb{C}$):

$$A_{\sigma} := \begin{bmatrix} c_1 + \sum_{j=1}^{n-m} c_{j+m} \sigma(\alpha_{1,j}) \overline{\sigma(\alpha_{1,j})} & \cdots & \sum_{j=1}^{n-m} c_{j+m} \sigma(\alpha_{1,j}) \overline{\sigma(\alpha_{m,j})} \\ \vdots & \ddots & \vdots \\ \sum_{j=1}^{n-m} c_{i+m} \sigma(\alpha_{i,j}) \overline{\sigma(\alpha_{i,1})} & \cdots & c_m + \sum_{j=1}^{n-m} c_{j+m} \sigma(\alpha_{m,j}) \overline{\sigma(\alpha_{m,j})} \end{bmatrix}$$

It therefore suffices to give a lower bound on $\det(A_\sigma)$, since the volume ratio equals

$$\prod_{\sigma:K \rightarrow \mathbb{C}} \sqrt{\det(A_\sigma)}^{-t}.$$

We now make the choice of $c_1 = \dots = c_m = \frac{1}{m+1}$ and may for $j \in J$ set $c_{m+j} = \frac{1}{k(m+1)}$ and take the remaining convex coefficients to be zero. A bound on $\det(A_\sigma)$ may now be deduced from combinatorics. For instance, it is known that the coefficient of z^{m-k} in $\det(z \cdot \text{Id} + X)$ is the sum of the $k \times k$ principal minors of a square matrix X . Writing $A_\sigma = z \cdot \text{Id} + X$ for $z = 1/(m+1)$ we see that X is a positive semidefinite Hermitian matrix and therefore its principal minors are nonnegative. We thus obtain a lower bound by keeping the terms in z^m and z^{m-1} resulting in the bound

$$\det(A_\sigma) \geq (m+1)^{-m} \left(1 + \frac{1}{k} \sum_{j \in J} \sum_{i=1}^m |\sigma(\alpha_{i,j})|^2\right).$$

The result follows since this is valid for any choice of k non-pivot columns J . \square

Recall now that we write for nonzero $\alpha \in (K^\times)^M$ and for some integer $M > 0$ the height:

$$H_\infty(\alpha) = \prod_{\sigma:K \rightarrow \mathbb{C}} \max_{1 \leq j \leq M} \max(1, |\sigma(\alpha_j)|).$$

Lemma 54. *Let $D \in M_{m \times n}(K)$ be a row-echelon matrix of rank m written as $D = (\text{Id}_m \mid \alpha)$ for entries $\alpha_{i,j} \in K$. Let $f : K_{\mathbb{R}}^t \rightarrow \mathbb{R}$ be the indicator function of a ball of unit radius and assume $n > m \geq 1$. For any fixed column of $(\alpha)_{ij}$ with $\alpha_1, \dots, \alpha_M \in K^\times$ denoting its non-zero entries we have the bound:*

$$\begin{aligned} & \frac{\int_{K_{\mathbb{R}}^{m \times t}} f(x_1) \cdots f(x_m) \prod_{j=1}^{n-m} f(\sum_{i=1}^m \alpha_{i,j} x_i) dx_1 \cdots dx_m}{V(t[K : \mathbb{Q}])^m} \\ & \leq (M+1)^{Mtd/2} \cdot \frac{V(t[K : \mathbb{Q}]M)}{V(t[K : \mathbb{Q}])^M} \left(H_\infty(\alpha)^{\frac{2}{d}} + M N(\alpha)^{2/(dM)} \cdot H_\infty(\alpha)^{\frac{-2}{dM}} \right)^{-\frac{dt}{2}}, \end{aligned}$$

where we abbreviate $N(\alpha)$ for $N(\alpha_1 \cdots \alpha_M)$.

Proof. We induct on m . For any column j of $(\alpha)_{ij}$, first observe that we have the trivial bound

$$\int_{K_{\mathbb{R}}^{m \times t}} f(x_1) \cdots f(x_m) \prod_{j=1}^{n-m} f(\sum_{i=1}^m \alpha_{i,j} x_i) dx_1 \cdots dx_m \leq \int_{K_{\mathbb{R}}^{m \times t}} f(x_1) \cdots f(x_m) f(\sum_{i=1}^m \alpha_{i,j} x_i) dx_1 \cdots dx_m.$$

We shall prove by induction that the right hand side is bounded. When $m = M = 1$, the claimed bound is a special case of Lemma 39. Let now $m \geq 2$ arbitrary. If $M = m$ we apply Lemma 53 and reduce to a term that looks like the height of the class $(1 : \alpha_1 : \dots : \alpha_m)$ in projective space. Comparing heights as in Lemma 16 we then obtain the claimed bound. Finally, if $M < m$, writing x_1, \dots, x_M for the variables corresponding to rows with non-zero entries in the j -th column we have:

$$\frac{\int_{K_{\mathbb{R}}^{m \times t}} f(x_1) \cdots f(x_m) f(\sum_{i=1}^m \alpha_{i,j} x_i) dx_1 \cdots dx_m}{V(t[K : \mathbb{Q}])^m} = \frac{\int_{K_{\mathbb{R}}^{m \times t}} f(x_1) \cdots f(x_M) f(\sum_{i=1}^M \alpha_i x_i) dx_1 \cdots dx_M}{V(t[K : \mathbb{Q}])^M}$$

by separating variables. But the latter is bounded by exactly the desired term by induction. \square

We also record the result taking into account all of the columns:

Lemma 55. *Let $D \in M_{m \times n}(K)$ be a row-echelon matrix of rank m written as $D = (\text{Id}_m \mid \alpha)$ for entries $\alpha_{i,j} \in K$, exactly M entries $\alpha_1, \dots, \alpha_M$ of them non-zero. Let $f : K_{\mathbb{R}}^t \rightarrow \mathbb{R}$ be the indicator function of a ball of unit radius and assume $n > m \geq 1$. Then*

$$\begin{aligned} & \frac{\int_{K_{\mathbb{R}}^{m \times t}} f(x_1) \cdots f(x_m) \prod_{j=1}^{n-m} f(\sum_{i=1}^m \alpha_{i,j} x_i) dx_1 \cdots dx_m}{V(t[K : \mathbb{Q}])^m} \\ & \leq (m+1)^{mtd/2} \cdot \frac{V(t[K : \mathbb{Q}]m)}{V(t[K : \mathbb{Q}])^m} \left(e^{2 \cdot h_\infty(\sqrt{\frac{1}{n-m}} \alpha)} + \frac{M}{n-m} N(\sqrt{\frac{1}{n-m}} \alpha)^{2/(dM)} \cdot e^{\frac{-2}{M} \cdot h_\infty(\sqrt{\frac{1}{n-m}} \alpha)} \right)^{-\frac{dt}{2}}, \end{aligned}$$

where we abbreviate $N(\alpha)$ for $N(\alpha_1 \cdots \alpha_M)$.

Note that we use absolute heights in the statement to obtain the right result independently of whether $\sqrt{n-m} \in K$.

Proof. We apply Lemma 53 for the full number of columns. This yields a term that looks like the height of the class $(1 : \sqrt{\frac{1}{n-m}}\alpha_1 : \cdots : \sqrt{\frac{1}{n-m}}\alpha_M)$ in projective space. Comparing heights as in Lemma 16 we then obtain the claimed bound. \square

We may now sum up these contributions over units to obtain similarly to Proposition 44:

Proposition 56. *Assume Hypothesis 30 and its notations. Assume $n > m \geq 2$. There exist explicit positive constants $C, \varepsilon_1 > 0$ uniform in d, t such that for all $D = (\text{Id}_m \mid \alpha_{ij})$ in $A_m^2 \setminus A_m^{2,0}$ the following holds: write*

$$t_0 = \frac{2r_K \cdot m(m+1)(n-m) \cdot \log(2 + 12c_0^{-1} + 2 \log(n-m) \cdot c_0^{-1})}{d \log(s)},$$

where r_K is the rank of the unit group and $s = \min(\frac{64}{27}, e^{\frac{c_1}{3}}, \cosh^3(c_1)) > 1$ is a constant depending only on the choice of number fields. Let f denote the indicator function of a ball of radius R and let $\alpha_1, \dots, \alpha_M$ for $n-m+1 \leq M \leq m(n-m)$ denote the nonzero entries of $(\alpha)_{ij}$. Write $D_\beta = (\text{Id}_m \mid \beta\alpha)$ for $\beta \in (\mathcal{O}_K^\times)^M$, where we scale the nonzero entries $\alpha_i \mapsto \beta_i \alpha_i$ and $D(\alpha)$ is as defined in 15. Then for any $t > t_0$ we have the bound:

$$\begin{aligned} & \frac{1}{V(td)^m R^{mtd}} \sum_{\beta \in (\mathcal{O}_K^\times)^M} \int_{K_{\mathbb{R}}^{m \times t}} f(xD_\beta) dx_1 \cdots dx_m \\ & \leq C \cdot \omega_K^M \cdot (td\pi)^{m/2} \cdot \max(N(\alpha)^{\frac{-t}{4M}}, N(\alpha)^{\frac{-tm}{(m+1)M}}) \cdot D(\alpha)^{\frac{t}{2(m+1)} + \frac{r_K M}{ed}} \cdot e^{-\varepsilon_1 \cdot d \cdot (t-t_0)}. \end{aligned}$$

Moreover, we may e.g. choose $\varepsilon_1 = \frac{1}{2} \log(\min\{\frac{4}{3}, e^{\frac{c_1}{3(m+1)}}, \cosh(c_1)\})$ and $C = \frac{4}{1 - e^{d(t_0-t)/2}}$.

Proof. The proof proceeds similar to Proposition 44 and uses Lemmas 54 and 55. We first record a count of unit M -tuples β with bounded height after scaling by α . Note that $D(\alpha) \in \mathbb{Z}_{\geq 1}$ by definition and moreover for any $1 \leq i \leq M$ we have that

$$\max(1, N(\alpha_i)^{-1}) \leq D(\alpha_i) \leq D(\alpha).$$

We may therefore apply Lemma 43 and bound

$$\begin{aligned} & \#\{\beta \in (\mathcal{O}_K^\times)^M \mid \frac{1}{d} \log H_\infty(\alpha\beta) \leq B\} \\ & \leq \omega_K^M \cdot \prod_{i=1}^M \left(\frac{B + \max(0, \log(N(\alpha_i)^{\frac{-1}{d}})) + \frac{c_0}{2}}{\frac{c_0}{2}} \right)^{r_K} \\ & \leq \omega_K^M \cdot \left(\frac{B + \log(D(\alpha)^{\frac{1}{d}}) + \frac{c_0}{2}}{\frac{c_0}{2}} \right)^{r_K M}. \end{aligned}$$

Note also that we will systematically use the bounds on the volume ratios involving unit balls in Lemma 23 when applying Lemma 54. The approximation $\frac{V(ktd)}{V(td)^k} \approx k^{-ktd/2}$ will be factored into our estimates for $1 \leq k \leq m$ whereas the error term bound in the Stirling approximation $p_k(t, d) := \frac{(td\pi)^{(k-1)/2}}{\sqrt{k}} \cdot e^{k/(6td)}$ ultimately yields the factor $(td\pi)^{m/2}$ in the statement of the proposition.

Type $A_m^{2, \text{ho}}$ terms. We first estimate the sum for terms $D_\beta \in A_m^{2, \text{ho}}$. We claim that since $D \in A_m^2 \setminus A_m^{2,0}$, there exists a column of D with k non-zero entries $\alpha_j = (\alpha_{j1}, \dots, \alpha_{jk})$ satisfying

$$N(\alpha_j) \geq N(\alpha)^{\frac{k}{M}} \text{ and } (\alpha_j \notin (\mathcal{O}_K^\times)^k \text{ or } k \geq 2.)$$

Indeed, consider the nonempty set $J \subset \{1, \dots, n\}$ of columns with multiple non-zero entries. If all non-zero entries of D outside of J are units, then we are done since \mathcal{O}_K^\times -entries have unit norm and thus the norm condition is also satisfied for one of the columns of J . It remains to deal with the case when all the columns in J fail the norm condition. But then the set $J' \subseteq \{1, \dots, n\} \setminus J$ of columns of D with exactly one non-unit

entry must be non-empty. Since at least one column in all of $\{1, \dots, n\}$ must have the norm condition, in this case it will be a column in J' . Hence we get a column with the desired property.

Let $\alpha_j = (\alpha_{j1}, \dots, \alpha_{jk})$ henceforth denote such a column with its k non-zero entries. Among the M nonzero entries of D , the indices $\{j1, \dots, jk\}$ pick out a k -element subset of $\{1, \dots, M\}$. Given $\beta \in (\mathcal{O}_K^\times)^M$, we shall therefore in what follows write $\alpha_j \beta$ for the k -tuple of algebraic numbers $\alpha_j \beta = (\alpha_{j1} \beta_{j1}, \dots, \alpha_{jk} \beta_{jk})$. We apply Lemma 54 to the column α_j in order to establish the proposition for terms in \mathbf{A}_m^{2, h_0} .

This yields, incorporating the unit counts and Stirling approximation terms above:

$$\begin{aligned} & \sum_{\beta \in (\mathcal{O}_K^\times)^M} \frac{\int_{K_{\mathbb{R}}^{m \times t}} f(xD_\beta) dx_1 \cdots dx_m}{V(td)^m R^{mtd}} \\ & \leq (1 + \frac{1}{k})^{ktd/2} \cdot p_k(t, d) \cdot \sum_{\substack{\beta \in (\mathcal{O}_K^\times)^M \\ D_\beta \in A_m^{2, h_0}}} \left(H_\infty(\alpha_j \beta)^{\frac{2}{d}} + k N(\alpha_j)^{\frac{2}{dk}} \cdot H_\infty(\alpha_j \beta)^{\frac{-2}{dk}} \right)^{-\frac{dt}{2}} \\ & \leq (1 + \frac{1}{k})^{ktd/2} \cdot p_k(t, d) \cdot \#\{\beta \in (\mathcal{O}_K^\times)^M \mid \frac{1}{d} \log H_\infty(\alpha_j \beta) \leq h_0\} \cdot f_k(\alpha_j)^{-\frac{dt}{2}} \\ & \leq (1 + \frac{1}{k})^{ktd/2} \cdot p_k(t, d) \cdot \omega_K^M \cdot \left(\frac{h_0 + \log(D(\alpha)^{\frac{1}{d}}) + \frac{c_0}{2}}{\frac{c_0}{2}} \right)^{r_K M} \cdot f_k(\alpha_j)^{-\frac{dt}{2}}, \end{aligned}$$

writing $p_k(t, d) = \frac{(td\pi)^{(k-1)/2}}{\sqrt{k}} \cdot e^{k/(6td)}$ and setting

$$f_k(\alpha_j) := \min_{\substack{\beta \in (\mathcal{O}_K^\times)^M \\ D_\beta \in A_m^{2, h_0}}} H_\infty(\alpha_j \beta)^{\frac{2}{d}} + k N(\alpha_j)^{\frac{2}{dk}} \cdot H_\infty(\alpha_j \beta)^{\frac{-2}{dk}}.$$

We wish to give a lower bound on $f_k(\alpha_j)$. To that end, recall that by Hypothesis 30 there is a lower bound

$$H_\infty(\alpha_j \beta) \cdot D(\alpha_j) = H_\infty(\alpha_j \beta) \cdot D(\alpha_j \beta) \geq e^{dc_1} \quad (18)$$

for some $c_1 > 0$ as long as $\alpha_j \beta \notin \mu_K^k$. Moreover we remark that by definition $D(\alpha_j) \leq D(\alpha)$. We distinguish two cases:

Case 1: The denominators are large so that $D(\alpha_j) \geq e^{\frac{1}{3}dc_1}$ or we have at least $k \geq 2$ non-zero entries $(\alpha_{j1}, \dots, \alpha_{jk})$. We then simply bound $f_k(\alpha_j)$ by taking its minimum as a function of the Weil height. It occurs when the equality

$$H_\infty(\alpha_j \beta)^{\frac{2}{d}} = N(\alpha_j)^{\frac{2}{d(k+1)}}$$

is satisfied and we obtain that

$$f_k(\alpha_j)^{-\frac{dt}{2}} \leq N(\alpha_j)^{-\frac{t}{k+1}} \cdot (1+k)^{-\frac{1}{2}dt} \text{ together with } \left(D(\alpha_j) \geq e^{\frac{1}{3}dc_1} \text{ or } k \geq 2 \right).$$

We therefore have in the case where $D(\alpha_j) \geq e^{\frac{1}{3}dc_1}$ that

$$(1 + \frac{1}{k})^{ktd/2} \cdot f_k(\alpha_j)^{-\frac{dt}{2}} \cdot D(\alpha)^{-\frac{t}{2(m+1)}} \leq N(\alpha_j)^{-\frac{t}{k+1}} \cdot e^{-\frac{td}{2} \cdot (\frac{c_1}{3(m+1)})} \cdot \left(\frac{(k+1)^{(k-1)}}{k^k} \right)^{\frac{td}{2}}.$$

If $k = 1$, this gives us

$$(1 + \frac{1}{k})^{ktd/2} \cdot f_k(\alpha_j)^{-\frac{dt}{2}} \cdot D(\alpha)^{-\frac{t}{2(m+1)}} \leq N(\alpha_j)^{-\frac{t}{k+1}} \cdot e^{-\frac{td}{2} \cdot (\frac{c_1}{3(m+1)})},$$

otherwise we know that

$$\frac{(k+1)^{(k-1)}}{k^k} \leq \frac{3}{4} \text{ for } k \geq 2$$

and therefore under the assumption that either $D(\alpha_j) \geq e^{\frac{1}{3}dc_1}$ or $k \geq 2$, we can conclude

$$(1 + \frac{1}{k})^{ktd/2} \cdot f_k(\alpha_j)^{-\frac{dt}{2}} \cdot D(\alpha)^{-\frac{t}{2(m+1)}} \leq N(\alpha_j)^{-\frac{t}{k+1}} \cdot e^{-\frac{td}{2} \cdot \min(\log(\frac{4}{3}), \frac{c_1}{3(m+1)})}.$$

Thus, taking into account that $N(\alpha_j) \geq N(\alpha)^{\frac{k}{M}}$, we get that for any $k \geq 1$

$$N(\alpha_j)^{\frac{1}{k+1}} \geq N(\alpha)^{\frac{k}{M(k+1)}} \geq \min(N(\alpha)^{\frac{m}{(m+1)M}}, N(\alpha)^{\frac{1}{2M}}),$$

where we upper or lower bound the exponent depending on whether $N(\alpha) \leq 1$ or not. So we have

$$(1 + \frac{1}{k})^{ktd/2} \cdot f_k(\alpha_j)^{-\frac{dt}{2}} \cdot D(\alpha)^{-\frac{t}{2(m+1)}} \leq \max(N(\alpha)^{\frac{-t}{2M}}, N(\alpha)^{\frac{-tm}{(m+1)M}}) \cdot e^{-\frac{td}{2} \cdot \min(\log(\frac{4}{3}), \frac{c_1}{3(m+1)})}.$$

Case 2: The denominators satisfy $D(\alpha_j) < e^{\frac{1}{3}dc_1}$ and $k = 1$. Then note that by our assumptions $\alpha_j \notin \mathcal{O}_K^\times$ and therefore for any $\beta \in \mathcal{O}_K^\times$ we have that $\alpha_j\beta \notin \mu_K$. Hence we deduce via (18) that $H_\infty(\alpha_j\beta) \geq e^{2dc_1/3}$. Moreover, we may rewrite

$$f_k(\alpha_j) \geq \min_{\substack{\beta \in (\mathcal{O}_K^\times)^M \\ D_\beta \in A_m^{2, h_0}}} \left(N(\alpha_j)^{\frac{1}{2d}} \cdot g\left(\frac{H_\infty(\alpha_j\beta)}{N(\alpha_j\beta)^{1/4}}\right) \right) \text{ for } g(x) = x^{\frac{2}{d}} + x^{-\frac{2}{d}}$$

and given that g is increasing in the range $[1, \infty[$ and $H_\infty(\alpha_j\beta) \geq N(\alpha_j\beta)$ we get

$$g\left(\frac{H_\infty(\alpha_j\beta)}{N(\alpha_j\beta)^{\frac{3}{4}}}\right) \geq g\left(H_\infty(\alpha_j\beta)^{\frac{3}{4}}\right)$$

so that we can bound

$$(1 + \frac{1}{k})^{ktd/2} \cdot f_k(\alpha_j)^{-\frac{dt}{2}} \leq N(\alpha_j)^{-\frac{t}{4}} \cdot (1 + \frac{1}{k})^{ktd/2} \cdot g(e^{\frac{1}{2}dc_1})^{-dt/2} \\ \leq N(\alpha_j)^{-\frac{t}{4}} \cdot \cosh(c_1)^{-dt/2}.$$

Taking into account that $N(\alpha_j) \geq N(\alpha)^{\frac{k}{M}}$ and $k = 1$, we can write

$$(1 + \frac{1}{k})^{ktd/2} \cdot f_k(\alpha_j)^{-\frac{dt}{2}} \leq N(\alpha)^{-\frac{t}{4M}} \cdot \cosh(c_1)^{-dt/2}.$$

Putting all of these cases and bounds together, we obtain the upper bound on the volume ratio

$$\sum_{\substack{\beta \in (\mathcal{O}_K^\times)^M \\ D_\beta \in A_m^{2, h_0}}} \frac{\int_{K_{\mathbb{R}}^{m \times t}} f(xD_\beta) dx_1 \cdots dx_m}{V(td)^m R^{mtd}} \\ \leq 3 \cdot p_m(t, d) \cdot \max(N(\alpha)^{\frac{-t}{4M}}, N(\alpha)^{\frac{-tm}{(m+1)M}}) \cdot D(\alpha)^{\frac{t}{2(m+1)}} \cdot \omega_K^M \cdot \left(\frac{h_0 + \log(D(\alpha)^{\frac{1}{d}}) + \frac{c_0}{2}}{\frac{c_0}{2}}\right)^{r_K M} \cdot S^{-dt/2},$$

where $p_m(t, d) = \frac{(td\pi)^{(m-1)/2}}{\sqrt{m}} \cdot e^{m/(6td)}$ and $S > 1$ is given by

$$S = \min\left\{\frac{4}{3}, e^{\frac{c_1}{3(m+1)}}, \cosh(c_1)\right\}.$$

Note that the various values of S correspond to the cases when $k \geq 2$, $D(\alpha_j) \geq e^{\frac{1}{3}dc_1}$ or the remaining case. It now suffices to find t_0 large enough so that

$$\left(\frac{h_0 + \log(D(\alpha)^{\frac{1}{d}}) + \frac{c_0}{2}}{\frac{c_0}{2}}\right)^{r_K M} \cdot S^{-dt/2} \leq e^{-\varepsilon_1 \cdot d \cdot (t-t_0)} \cdot D(\alpha)^{\frac{r_K M}{\varepsilon d}},$$

with ε_1 as in the statement of the proposition. By Jensen's inequality we may bound

$$\left(\frac{h_0 + \log(D(\alpha)^{\frac{1}{d}}) + \frac{c_0}{2}}{\frac{c_0}{2}}\right)^{r_K M} \leq 2^{r_K M - 1} \left(\left(1 + \frac{2h_0}{c_0}\right)^{r_K M} + \left(\frac{2}{dc_0} \log D(\alpha)\right)^{r_K M} \right)$$

and we examine how each individual term behaves with growing d, t . Viewed as a function in $d \geq 1$, we may estimate $\left(\frac{\log D(\alpha_j)}{d}\right)^d \leq e^{\frac{\log D(\alpha_j)}{e}}$ and therefore obtain

$$\left(\frac{4 \log D(\alpha_j)}{dc_0}\right)^{r_K M} \leq \left(\frac{4}{c_0}\right)^{r_K M} \cdot D(\alpha_j)^{\frac{r_K M}{ed}}. \quad (19)$$

The upper bound on $\sum_{\substack{\beta \in (\mathcal{O}_K^\times)^M \\ D_\beta \in A_m^{2, h_0}}} \frac{\int_{K_{\mathbb{R}}^{m \times t}} f(x D_\beta) dx_1 \cdots dx_m}{V(td)^m R^{mtd}}$ therefore holds as claimed in the proposition provided that

$$t_0 \geq \frac{2r_K \cdot M}{d \log S} \cdot \max \left\{ \log \left(\frac{4}{c_0} \right), \log \left(2 + 4 \frac{h_0}{c_0} \right) \right\}.$$

Note that for $t \geq t_0$ we also have $3 \cdot p_m(t, d) \leq (td\pi)^{m/2}$. This concludes our dealings with the A_m^{2, h_0} -type terms.

Type $\mathbf{A}_m^{2, \infty}$ terms. By Lemma 55, the sum

$$\begin{aligned} \Sigma_{n, m}^\infty &:= \sum_{\substack{\beta \in (\mathcal{O}_K^\times)^M \\ D_\beta \in A_m^{2, \infty}}} \binom{m+1}{m}^{mtd/2} \left(e^{2 \cdot h_\infty(\sqrt{\frac{1}{n-m}} \alpha \beta)} + \frac{M}{(n-m)^2} N(\alpha)^{2/(dM)} \cdot e^{\frac{-2}{M} \cdot h_\infty(\sqrt{\frac{1}{n-m}} \alpha \beta)} \right)^{-\frac{dt}{2}} \\ &\geq \sum_{\substack{\beta \in (\mathcal{O}_K^\times)^M \\ D_\beta \in A_m^{2, \infty}}} \frac{\int_{K_{\mathbb{R}}^{m \times t}} f(x D_\beta) dx_1 \cdots dx_m}{V(td)^m R^{mtd}} \end{aligned}$$

provides an upper bound and it suffices to estimate $\Sigma_{n, m}^\infty$. For $D_\beta \in \mathbf{A}_m^{2, \infty}$ we have by assumption that the heights are bounded below by

$$h_\infty(\alpha \beta) \geq \max_{1 \leq i \leq M} h_\infty(\alpha_i \beta_i) \geq h_0.$$

Abbreviating $f_m(x) = e^{2x} + \frac{M}{(n-m)^2} N(\alpha)^{\frac{2}{dM}} e^{-2\frac{x}{M}}$, we may rewrite

$$\Sigma_{n, m}^\infty = \sum_{\substack{\beta \in (\mathcal{O}_K^\times)^M \\ D_\beta \in A_m^{2, \infty}}} \binom{m+1}{m}^{mtd/2} f_m \left(h_\infty \left(\sqrt{\frac{1}{n-m}} \alpha \beta \right) \right).$$

Now observe that

$$\log(\sqrt{n-m}) + h_\infty \left(\frac{1}{\sqrt{n-m}} \alpha \beta \right) = \frac{1}{[K(\sqrt{n-m}):\mathbb{Q}]} \cdot \sum_{\sigma: K(\sqrt{n-m}) \rightarrow \mathbb{C}} \max_{1 \leq j \leq M} \max(\log \sqrt{n-m}, \log(|\sigma(\alpha_j \beta_j)|)) \geq h_\infty(\alpha \beta).$$

Hence, we know that for any $B \geq 1$

$$h_\infty \left(\frac{1}{\sqrt{n-m}} \alpha \beta \right) \leq B \Rightarrow h_\infty(\alpha \beta) \leq B + \frac{1}{2} \log(n-m)$$

and therefore we have the inclusion of sets

$$\begin{aligned} &\left\{ \beta \in (\mathcal{O}_K^\times)^M \mid D_\beta \in A_m^{2, \infty}, h_\infty \left(\frac{1}{\sqrt{n-m}} \alpha \beta \right) \leq B \right\} \\ &\subseteq \left\{ \beta \in (\mathcal{O}_K^\times)^M \mid h_0 \leq \frac{1}{d} \log(H_\infty(\alpha \beta)) \leq B + \frac{1}{2} \log(n-m) \right\}. \end{aligned}$$

We may therefore bound the sum $\Sigma_{n, m}^\infty$ by

$$\begin{aligned} &\left(1 + \frac{1}{m}\right)^{td/2} \cdot \sum_{i=1}^{\infty} \#\{\beta \in (\mathcal{O}_K^\times)^M \mid h_0 \leq \frac{1}{d} \log H_\infty(\alpha \beta) \leq h_0 + i\} \cdot f_m(h_0 + i - 1 - \frac{1}{2} \log(n-m))^{-\frac{dt}{2}} \\ &\leq e^{td/2} \cdot \omega_K^M \cdot \sum_{i=1}^{\infty} \left(\frac{h_0 + i + \log(D(\alpha)^{\frac{1}{d}}) + \frac{c_0}{2}}{\frac{c_0}{2}} \right)^{r_K M} \cdot f_m(h_0 + i - 1 - \frac{1}{2} \log(n-m))^{-\frac{dt}{2}}, \end{aligned}$$

where for the second inequality we count units via Lemma 43 as before. The inequality

$$H_\infty\left(\sqrt{\frac{1}{n-m}}\alpha\beta\right) \geq N\left(\sqrt{\frac{1}{n-m}}\alpha\right)^{\frac{1}{M}}$$

allows us to simply estimate

$$f_m(x) \geq N(\alpha)^{\frac{1}{4M}} \cdot e^x \text{ for } x = h_0 + i - 1 - \frac{1}{2} \log(n-m) \text{ and } i \in \mathbb{N}.$$

Using Jensen's inequality and bounding the contribution of $D(\alpha)$ to unit counts as in Equation (19), we therefore obtain

$$\Sigma_{n,m}^\infty \leq \omega_K^M \cdot N(\alpha)^{\frac{-t}{2M}} \cdot \sum_{i=1}^{\infty} \exp\left(-\frac{d(t-t_0)}{2} \cdot (h_0 + i - 2 - \frac{1}{2} \log(n-m))\right)$$

where we have chosen

$$t_0 \geq \frac{2r_K \cdot M}{d} \cdot \sup_{i \in \mathbb{Z}_{\geq 1}} \frac{\max\left\{\log\left(2 + \frac{4}{c_0}(h_0 + i)\right), \log\left(\frac{4}{c_0}\right)\right\}}{h_0 + i - 2 - \frac{1}{2} \log(n-m)}.$$

Observe that the term in $i = 1$ attains the maximum. We may now make a choice of threshold height

$$h_0 = 2 + \frac{1}{2} \log(n-m).$$

This yields the condition

$$t_0 \geq \frac{2r_K \cdot M}{d} \cdot \log\left(2 + 12c_0^{-1} + 2 \log(n-m) \cdot c_0^{-1}\right).$$

The result follows by bookkeeping of all the bounds obtained, noting that we may bound $\log(S)^{-1} \leq (m+1) \log(s)^{-1}$ for any $m \geq 2$. Similarly the explicit constants can be chased through the arguments. \square

With this in hand, we are ready to tackle:

Proof of Theorem 51. First, note that it suffices to prove the statement fixing pivot columns and some number M of nonzero entries in the last $n-m$ columns of D . We have $M \geq n-m$ and the contributions for matrices in $A_m^{2,0}$ when $M = n-m$ are dealt with in Proposition 47 (we apply it with $M = n-m$ and $k = 4$). All of these contributions must be taken into account when expliciting the constants in the asymptotic.

Second, we claim that

$$\mathfrak{D}(D) \geq D(\alpha) = N(\langle 1, \alpha_1, \dots, \alpha_M \rangle)^{-1},$$

where $(\alpha_1, \dots, \alpha_M)$ are the non-zero entries of D in the non-pivot columns. Note that a sharper result can be obtained by taking all of the Plücker coordinates of D into account, see Part 2. of Proposition 66, but the claim suffices for our purposes. To prove the claim, observe that $\mathfrak{D}(D)$ is by definition the index as a sublattice of \mathcal{O}_K^m of the set of $(c_1, \dots, c_m) \in \mathcal{O}_K^m$ such that for each column $1 \leq i \leq n$ we have $\sum_{j=1}^m c_j D_{ij} \in \mathcal{O}_K$. This amounts to a linear condition modulo the integral ideal $I_i = (\alpha_{i1}, \dots, \alpha_{is})^{-1}$ where $i1, \dots, is$ are the indices of the subset of $(\alpha_1, \dots, \alpha_M)$ in the i -th column of D . Considering multiple columns, (c_1, \dots, c_m) must lie in an intersection of hyperplanes modulo $J = \sum_{i=m+1}^{n-m} I_i \subset \mathcal{O}_K$. For every prime $\mathfrak{p} \mid J$, we then get that by construction the c_i satisfy at least one linear equation

$$\sum_{j=1}^m c_j D_j \equiv 0 \pmod{\mathfrak{p}^{\text{ord}_{\mathfrak{p}}(J)}}$$

with at least one $c_j \not\equiv 0 \pmod{\mathfrak{p}^{\text{ord}_{\mathfrak{p}}(J)}}$. In other words, this forces (c_1, \dots, c_m) into the pre-image of a hyperplane under the reduction map $\mathcal{O}_K^m \rightarrow (\mathcal{O}_K/\mathfrak{p}^{\text{ord}_{\mathfrak{p}}(J)})^m$, which then has index $\mathfrak{p}^{\text{ord}_{\mathfrak{p}}(J)}$. By the Chinese remainder theorem, we therefore get that $\mathfrak{D}(D) \geq N(J)$. But we have that $D(\alpha) = N(J)$ and the claim follows.

By the claim and Proposition 56, the proof of the theorem thus reduces to establishing convergence of the sum

$$\sum_{\alpha \in (K^\times)^M \setminus (\mathcal{O}_K^\times)^M} \max\left(N(\alpha)^{\frac{-t}{4M}}, N(\alpha)^{\frac{-tm}{(m+1)M}}\right) \cdot D(\alpha)^{\frac{t}{2(m+1)} + \frac{r_k M}{ed}} \cdot D(\alpha)^{-t}.$$

Summing over ideals as in Proposition 47, it therefore suffices to bound

$$\zeta_K\left(t - \frac{t}{2(m+1)} - \frac{r_k M}{ed}\right)^{-1} \cdot \sum_{\substack{I \subset \mathcal{O}_K \\ I \text{ integral ideal}}} \mathbf{N}(I)^{-t + \frac{t}{2(m+1)} + \frac{r_k M}{ed}} \prod_{1 \leq i \leq M} \sum_{J \subset \mathcal{O}_K} \mathbf{N}(J)^{-\frac{t}{4M}} \mathbf{N}(I)^{\frac{tm}{(m+1)M}}.$$

We see that this is bounded by $Z(K, t, n, m)$ as claimed, and we record the additional condition on t to ensure convergence of the zeta values. The rest is keeping track of bounds on t and explicit exponents for the various cases. \square

5.5 General moments using the Bogomolov property

Summarizing the results of this section, we obtain the following main theorem:

Theorem 57. *Let \mathcal{S} denote any set of number fields satisfying Hypothesis 30 and let c_0, c_1 denote the resulting uniform constants. Fix a moment $n \geq 2$. There exist constants $0 < C_{\mathcal{S}}, \varepsilon_{\mathcal{S}} < \infty$ uniform in d, t such that the following holds: let t_0 denote*

$$\sup_{K \in \mathcal{S}} \left(\frac{r_K n(n+1)^2}{d} \cdot \frac{\log(2 + 12c_0^{-1} + 2 \log(n-1) \cdot c_0^{-1})}{\log\left(\min\left\{\frac{64}{27}, e^{\frac{1}{3}c_1}, \cosh^3(c_1)\right\}\right)}, \frac{2r_K(n-1)}{d} \cdot \frac{\log(17/8)}{\log(f_{n-1}(\frac{3}{4}c_0))} \right),$$

where $f_m(x) := \frac{\exp(x) + m \exp(-\frac{x}{m})}{m+1}$ and r_K is the rank of the unit group. We then have for any $t > t_0$ and for any $K \in \mathcal{S}$ of degree d that the n -th moment $\mathbb{E}[\rho(\Lambda)^n]$ of the number of nonzero \mathcal{O}_K -lattice points in an origin-centered ball of volume V in $K_{\mathbb{R}}^t$ satisfies:

$$\begin{aligned} \omega_K^n e^{-V/\omega_K} \sum_{r=0}^{\infty} \frac{r^n}{r!} \left(\frac{V}{\omega_K}\right)^r &\leq \mathbb{E}[\rho(\Lambda)^n] \\ &\leq \omega_K^n e^{-V/\omega_K} \sum_{r=0}^{\infty} \frac{r^n}{r!} \left(\frac{V}{\omega_K}\right)^r + C_{\mathcal{S}} \cdot \omega_K^{\frac{n^2}{4}} (td)^{\frac{n-2}{2}} \cdot e^{-\varepsilon_{\mathcal{S}} d(t-t_0)} \cdot (V+1)^{n-1} \cdot Z(K, t, n), \end{aligned}$$

where $0 \leq Z(K, t, n) = \frac{\zeta_K(\frac{1}{2(m+1)}t - \frac{1}{e}m(n-m)) \cdot \zeta_K(\frac{t}{n^2})^{\frac{1}{4}n^2}}{\zeta_K(t-1)}$. Moreover, it suffices to take

$$\varepsilon_{\mathcal{S}} = \frac{1}{2} \log(\min\left\{\frac{4}{3}, e^{\frac{c_1}{3n+2}}, f_{n-1}(\frac{3}{4}c_1)\right\}).$$

The constant $C_{\mathcal{S}}$ may as well be chased down explicitly in terms of $n, \varepsilon_{\mathcal{S}}$.

Proof. This follows from our previous results, namely the terms with $m = 1$ are dealt with in Theorem 48 (we simply put $k = 4$). The error terms in A_m^2 for $m \geq 2$ are bounded via Theorem 51, keeping the values of $2 \leq m \leq n$ that give the worst bound on t_0 . The zeta factors from A_m^2 are the larger ones. The contributions of terms in A_m^1 for $m \geq 2$ decay exponentially by Theorem 24 and they are thus easily handled error terms. Finally, the main term contributions for $2 \leq m \leq n-1$ are computed in Lemma 22. The explicit exponent $\varepsilon_{\mathcal{S}}$ is found by taking the smallest over all the different terms and the constant $C_{\mathcal{S}}$ can be chased down similarly as an enumeration of cases as well as geometric sums bounded in terms of $\varepsilon_{\mathcal{S}}$ and several counts, such as Stirling numbers, which depend only on the moment. \square

A few comments on Theorem 57 are in order. First, the bound on t is $t_0 = O(n^3 \log \log n)$ as n increases with an implicit constant only depending on the number fields. For specific setups, especially for small moments where the contributions are covered in Theorem 48, the bound as well as the zeta factor can be sharpened slightly. Similarly, the explicit exponent may be optimised; Theorem 57 emphasizes a general result for reasonable and explicit bounds, and we make no claim as to optimality of these. Recall also that $\omega_K = O(d \log \log d)$ so that the theorem indeed exhibits exponential decay in d, t of the non-Poisson terms provided the zeta factors do not grow exponentially in d .

Second, one may trivially take \mathcal{S} to be a constant number field K . Hypothesis 30 is then satisfied and we obtain convergence of the moments of the number of ω_K -tuples of lattice points inside a ball of volume V towards the moments of a Poisson distribution of mean V/ω_K for any number field K and large enough number of copies t . We record a version of this statement:

Corollary 58. *Let K be any number field of fixed degree d . Let c_0, c_1 denote the constants bounding the Weil height on \mathcal{O}_K and K as in 30 and fix a moment $n \geq 2$. Let t_0 be as in Theorem 57. We then have for any $t > t_0$ that the n -th moment $\mathbb{E}[\rho(\Lambda)^n]$ of the number of nonzero \mathcal{O}_K -lattice points in an origin-centered ball of volume V in $K_{\mathbb{R}}^t$ satisfies:*

$$\begin{aligned} \omega_K^n e^{-V/\omega_K} \sum_{r=0}^{\infty} \frac{r^n}{r!} (V/\omega_K)^r &\leq \mathbb{E}[\rho(\Lambda)^n] \\ &\leq \omega_K^n e^{-V/\omega_K} \sum_{r=0}^{\infty} \frac{r^n}{r!} (V/\omega_K)^r + C_K \cdot t^{(n-2)/2} \cdot e^{-\varepsilon_K(t-t_0)} \cdot (V+1)^{n-1}, \end{aligned}$$

for constants $C_K, \varepsilon_K > 0$ uniform in t . Moreover, we may take

$$\varepsilon_K = \frac{1}{2} \log(\min\{\frac{4}{3}, e^{\frac{c_1}{3n+2}}, f_{n-1}(\frac{3}{4}c_1)\}).$$

The constant C_K may as well be chased down explicitly in terms of $n, \varepsilon_K, \omega_K$ and Dedekind zeta values of K .

Third, it is not entirely trivial that for appropriately large fixed t, k the error term in Theorem 57 decays exponentially in d due to the dependence on K of the zeta factor error terms $Z(K, t, n, k)$ in Theorem 57, which a priori could grow exponentially in d . Proving bounds in d for the growth does not appear trivial for general number fields. For instance, using lattice-point estimate based methods such as the Dedekind-Weber theorem to count ideals of bounded norm does not appear like a promising approach due to the fact that the best known bounds on the error term for counts of ideals of bounded norm grows exponentially in d (see, e.g., [41, Corollaire 1.3.]). Nevertheless, for specific towers of number fields one should be able to prove the desired boundedness (or at least subexponential growth in d) for Dedekind zeta values. For instance we have:

Lemma 59. *Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic field of degree $d = \varphi(n)$. Let $s > 1$ be a real number. Then we have that*

$$\zeta_K(s) \leq C(s)$$

for some constants $C(s) > 0$ uniform in d .

Proof. We first claim that the Dedekind zeta function of cyclotomic fields $\mathbb{Q}(\zeta_n)$ may be written as

$$\zeta_K(s) = \prod_{p \in \mathbb{P}} \frac{1}{\left(1 - \frac{1}{p^{s \cdot \text{ord}_{n_p} p}}\right)^{\frac{\varphi(n_p)}{\text{ord}_{n_p} p}}},$$

where $n_p = n \cdot p^{-v_p(n)}$ denotes the prime-to- p part of n .

The claim follows from examining for each Euler factor the splitting behaviour of primes above p based on the factorization of the cyclotomic polynomial $\Phi_n(x)$ modulo p . For instance, if $p \nmid n$, the number of roots of a factor of $\Phi_n(x)$ modulo p coincides with the size of the orbit of Frobenius acting via multiplication-by- p on $(\mathbb{Z}/n\mathbb{Z})^\times$, and hence the result follows in this case. When $p \mid n$, the same applies to the subextension $\mathbb{Q}(\zeta_{n_p})$ unramified at p , and then the remaining extension $K/\mathbb{Q}(\zeta_{n_p})$ is totally ramified at p , and the claim follows.

Using the claim, we have the following argument due to Danylo Radchenko: write $\zeta_K(s) = T_1 T_2$ where

$$T_1 = \prod_{p \mid n} \frac{1}{\left(1 - \frac{1}{p^{s \cdot \text{ord}_{n_p} p}}\right)^{\frac{\varphi(n_p)}{\text{ord}_{n_p} p}}},$$

and

$$T_2 = \prod_{p \nmid n} \frac{1}{\left(1 - \frac{1}{p^{s \cdot \text{ord}_n p}}\right)^{\frac{\varphi(n)}{\text{ord}_n p}}}.$$

For T_2 , we have that

$$\log T_2 \ll \sum_{p|n} \frac{\varphi(n)}{(\text{ord}_n p) p^{s \cdot \text{ord}_n p}}.$$

We write $\varphi(n) \leq n$, $\text{ord}_n p \geq 1$ and observe that the set $\{p^{\text{ord}_n p}\}_{p \in \mathbb{P}}$ lies in $\{n+1, 2n+1, \dots\}$. Since they are simply different prime powers, there are no repetitions.

So we have

$$\log T_2 \ll n \left(\frac{1}{(n+1)^s} + \frac{1}{(2n+1)^s} + \dots \right) \ll \frac{1}{n^{s-1}} \ll 1.$$

Now for T_1 ,

$$\log T_1 \ll \sum_{p|n} \frac{\varphi(n_p)}{(\text{ord}_{n_p} p) p^{s \cdot \text{ord}_{n_p} p}},$$

we again write $\varphi(n_p) \leq n_p$, $\text{ord}_{n_p} p \geq 1$ and use that $p^{\text{ord}_{n_p} p} \geq n_p$ so this gives us

$$\log T_1 \ll \sum_{p|n} \frac{1}{n_p^{s-1}} = \frac{1}{n^{s-1}} \sum_{p|n} p^{\nu_p(n) \cdot (s-1)}$$

Let k be the number of primes in n . Then the largest prime factor of n can be at most $\frac{n}{p_1 p_2 \dots p_{k-1}} \leq \frac{n}{(k-1)!}$. So we write

$$\log T_1 \ll \frac{k}{n^{s-1}} \left(\frac{n}{(k-1)!} \right)^{s-1}.$$

This tends to 0 as $k \rightarrow \infty$ so it must be bounded. \square

Finally, we make Theorem 57 more explicit for towers of cyclotomic fields:

Corollary 60. *Consider a sequence of cyclotomic number fields given by $K_i = \mathbb{Q}(\zeta_{k_i})$ of degree $d_i = \varphi(k_i)$ and let $n \geq 2$. Moreover let*

$$t_0 = \max \left\{ 19n(n+1)^2 \log(52 + \frac{25}{3} \log(n-1)), \frac{(n-1) \log(\frac{17}{8})}{\log(f_{n-1}(\frac{9}{50}))} \right\}.$$

where $f_{n-1}(x) := \frac{\exp(x) + (n-1) \exp(-\frac{x}{n-1})}{n}$. There exists constants $C_n, \varepsilon_n > 0$ uniform in d_i, t such that for any $t > t_0$ and any degree d_i the n -th moment $\mathbb{E}[\rho(\Lambda)^n]$ of the number of nonzero \mathcal{O}_K -lattice points in an origin-centered ball of volume V in $K_{\mathbb{R}}^t$ satisfies

$$\begin{aligned} \omega_{K_i}^n e^{-V/\omega_{K_i}} \sum_{r=0}^{\infty} \frac{r^n}{r!} \left(\frac{V}{\omega_{K_i}} \right)^r &\leq \mathbb{E}[\rho(\Lambda)^n] \\ &\leq \omega_{K_i}^n e^{-V/\omega_{K_i}} \sum_{r=0}^{\infty} \frac{r^n}{r!} \left(\frac{V}{\omega_{K_i}} \right)^r + C_n \cdot \omega_{K_i}^{\frac{n^2}{4}} (td_i)^{\frac{n-2}{2}} \cdot e^{-\varepsilon_n \cdot d_i(t-t_0)} \cdot (V+1)^{n-1}, \end{aligned}$$

ergo the moments of the number of ω_{K_i} -tuples of nonzero lattice points approach the moments of a Poisson distribution of mean V/ω_{K_i} as $d_i t \rightarrow \infty$. Moreover, we may take

$$\varepsilon_n = \frac{1}{2} \log(\min\{5^{\frac{1}{36n+24}}, f_{n-1}(\frac{\log 5}{16})\}).$$

The constant C_n may as well be chased down explicitly in terms of n, ε_K and Dedekind zeta values of K .

Proof. The result follows from Theorem 57 using Corollary 33 and the resulting constants. With these choices, some of the conditions on t_0 in Theorem 57 simplify. We bound the zeta factors in Theorem 57 uniformly in $\varphi(k_i)$ by Lemma 59. \square

Again we note that for low moments such as $n = 2, 3$ better bounds can be achieved, in particular because we can reduce to contributions from projective space heights and Theorem 48. Moreover, as n becomes large, $\frac{(n-1) \log(17/8)}{\log(f_{n-1}(9/50))} \leq 45n^2$ and it suffices to take $t_0 \geq 19n(n+1)^2 \log(52 + \frac{25}{3} \log(n-1))$ in Corollary 60.

6 Odds and ends

This section is devoted to a couple results and remarks complementing the results established in Section 5.

6.1 No limiting Poisson moments

Section 5 establishes that under some assumptions on height lower bounds, the n -th moments approach the moments of a Poisson distribution even when varying the number fields for a fixed large enough number of copies. We now show that in order to obtain such a behaviour, some assumption on the heights is necessary by exhibiting sequences of number fields K for which moments do not converge to Poisson moments of the expected parameters V/ω_K .

Lemma 61. *Let B denote the unit ball in $K_{\mathbb{R}}^t$ and for $\alpha \in K^\times$ denote by $H_W(\alpha)$ its Mahler measure. Then*

$$D(\alpha)^{-t} \cdot \sum_{\alpha \in \mathcal{O}_K^\times} \frac{\text{vol}(B \cap \alpha^{-1}B)}{\text{vol}(B)} \geq \sum_{\alpha \in K^\times} H_W(\alpha)^{-t}.$$

Proof. We may without loss of generality assume $\alpha \in \mathcal{O}_K$. In each of the t copies of $K_{\mathbb{R}}$ and for each nonzero $\alpha \in \mathcal{O}_K$, the origin-centered ellipsoid of lengths

$$\min(1, |\sigma_1(\alpha)|), \dots, \min(1, |\sigma_d(\alpha)|),$$

where $\sigma_1, \dots, \sigma_d$ are the embeddings $K \rightarrow \mathbb{C}$, is contained inside of $B \cap \alpha^{-1}B$. \square

Note that this provides a lower bound for the second moment in termst of the height zeta function of $\mathbb{P}^1(K)$. We deduce:

Proposition 62. *Let f_n be a sequence of irreducible polynomials of degree n such that their Mahler measures are uniformly bounded $\forall n$. Let $K_n := \mathbb{Q}(f_n)$ be the resulting sequence of number fields. Then for any fixed number of copies $t > 2$ there exists $C_t > 0$ such that over any number field K_n the second moment satisfies*

$$\mathbb{E}[\rho(\Lambda)^2] \geq C_t + \omega_{K_n}^2 e^{-V/\omega_{K_n}} \sum_{r=0}^{\infty} \frac{r^2}{r!} (V/\omega_{K_n})^r.$$

Proof. From the integral formula, it suffices to show that $\sum_{\alpha \in \mathcal{O}_K^\times} \frac{\text{vol}(B \cap \alpha^{-1}B)}{\text{vol}(B)} \geq C_t + \omega_{K_n}$ for some $C_t > 0$ not depending on n . But this is clear from Lemma 61 and our assumptions on heights in K_n . \square

Needless to say that similar results hold for higher moments as well. We also note that there are many sequences satisfying the assumptions of Proposition 62. For example, one has limiting results for Mahler measures such as (see [42]):

$$\lim_{n \rightarrow \infty} H_\infty(\alpha_n) = 1.3815 \dots, \text{ where } \alpha_n^n - \alpha_n + 1 = 0,$$

so where α_n is a root of $f_n(x) = x^n - x + 1$.

6.2 More general bodies

Although the bounds are more easily derived for indicator functions of balls, we can use spherical symmetrization to obtain results for more general bodies. The quantities appearing in the integral formula will be largest in the spherical case, so that the upper bounds on moments are valid more generally. The same methods as in Rogers' work [8, Theorem 1,2] carry through, so we simply restate:

Theorem 63. *Let g be a non-negative compactly supported Riemann integrable function on $K_{\mathbb{R}}^{t \times n}$ and let g^* denote the function obtained by spherical symmetrization. Let $g(\Lambda)$ and $g^*(\Lambda)$ denote the corresponding lattice sum functions over non-trivial lattice points. Then the moments over the space of unimodular \mathcal{O}_K -lattices or over the smaller sets satisfying mean value formulas as in Theorem 10 satisfy:*

$$\begin{aligned} \mathbb{E}[g(\Lambda)] &= \mathbb{E}[g^*(\Lambda)] \\ \mathbb{E}[g(\Lambda)^2] &\leq \mathbb{E}[g^*(\Lambda)^2] \\ \mathbb{E}[g(\Lambda)^3] &\leq \mathbb{E}[g^*(\Lambda)^3] \end{aligned}$$

and moreover if for each constant $c > 0$ the set of points with $g(x) > c$ is convex we have that

$$\mathbb{E}[g(\Lambda)^k] \leq \mathbb{E}[g^*(\Lambda)^k]$$

for all $k \geq 4$ as well.

Proof. Given the integral formula as in Theorems 4 and 10, this reduces to integral inequalities in Euclidean space, and thus follows from the inequalities in [43] in the same way as [8, Theorems 1,2]. \square

This yields the following version of the main theorem.

Theorem 64. *Let \mathcal{S} denote any set of number fields satisfying Hypothesis 30 and let c_0, c_1 denote the resulting uniform constants. Fix a moment $n \geq 2$. Let g be the characteristic function of a bounded, convex set S in $K_{\mathbb{R}}^d$ of volume V , with the origin as centre and assume that S is fixed by the coordinate-wise action of a cyclic group $\mu_{N_K} \subseteq \mu_K$ of order N_K . There exist explicit constants $C_S, \varepsilon_S > 0$ uniform in d, t such that the following holds: for $t_0(\mathcal{S}, n)$ as defined in Theorem 57 and for all $t > t_0(\mathcal{S}, n)$, we have*

$$N_K^n \cdot m_n\left(\frac{1}{N_K}V\right) \leq \mathbb{E}[g(\Lambda)^n] \leq \omega_K^n \cdot m_n\left(\frac{1}{\omega_K}V\right) + C_S \cdot \omega_K^{\frac{n^2}{4}} (td)^{\frac{n-2}{2}} \cdot e^{-\varepsilon_S d(t-t_0)} \cdot (V+1)^{n-1} \cdot Z(K, t, n).$$

Here m_n is as defined in (1) and $Z(K, t, n), C_S, \varepsilon_S$ are as in Theorem 57.

Proof. The upper bound follows from Theorem 63 and from our results for the spherical case in Theorem 57. The lower bound follows by symmetry under μ_{N_K} in the same way as Lemma 22 establishes the lower bound when S is a ball and invariant under the whole μ_K -action. \square

Remark 65. *The lower bound in Theorem 64 can be tightened for general bounded convex bodies. For instance, for any chain of subgroups $\{\pm 1\} = G_1 < \dots < G_k = \mu_K$ and bounded convex set S , we may stratify $S = \sqcup_{i=1}^k S_i$ by setting*

$$S_k = \bigcap_{g \in G_k} gS \text{ and } S_{i-1} = \bigcap_{g \in G_{i-1}} gS \setminus S_i$$

for $1 \leq i \leq k$. The lower bound can then be improved (in the notations of Theorem 64) to

$$\sum_{i=1}^k (\#G_i)^n \cdot m_n\left(\frac{\text{vol}(S_i)}{\#G_i}\right) \leq \mathbb{E}[g(\Lambda)^n]$$

by applying Theorem 64 to the G_i -symmetrized and measurable sets $S_k \sqcup \dots \sqcup S_i$ and inclusion-exclusion.

A Proof of Lemma 15

It is clear what $\det(D)\mathfrak{D}(D)$ on the right-hand side is measuring. Indeed, first note that

$$\mathfrak{D}(D) = \# \frac{\mathcal{O}_K^m}{\{v \in \mathcal{O}_K^m \mid D^T v \in \mathcal{O}_K^n\}} = \# \frac{D^T \mathcal{O}_K^m}{D^T \mathcal{O}_K^m \cap \mathcal{O}_K^n}$$

So we have that

$$\mathfrak{D}(D) \det(D) = \# \frac{D^T \mathcal{O}_K^m}{D^T \mathcal{O}_K^m \cap \mathcal{O}_K^n} \det(D; M_{1 \times m}(\mathcal{O}_K))$$

is simply the volume of a parallelepiped spanning a \mathbb{Z} -basis of the lattice $\Lambda = D^T \mathcal{O}_K^m \cap \mathcal{O}_K^n = D^T K^n \cap \mathcal{O}_K^m$ (this equality holds since D^T is column reduced and $m \leq n$). The following tells us that the height $H(S)$ is also calculating this volume.

Proposition 66. *Suppose that $w_1, \dots, w_m \in K^n$ are a set of K -linearly independent vectors spanning a subspace S . Let $\Lambda = \mathcal{O}_K^n \cap K$. If we consider the lattice $\Lambda' = \mathcal{O}_K w_1 + \mathcal{O}_K w_2 + \dots + \mathcal{O}_K w_m$, then $[\Lambda : \Lambda' \cap \Lambda] < \infty$ and $[\Lambda' : \Lambda' \cap \Lambda] < \infty$. So we have that*

$$[\Lambda : \Lambda' \cap \Lambda] \det \Lambda = [\Lambda' : \Lambda' \cap \Lambda] \det \Lambda'.$$

We claim:

1. Set $N = \binom{n}{m}$ and $[x_1, \dots, x_N] = \iota(S)$ (as defined in §3.1). Then

$$\det \Lambda' = \prod_{i=1}^{[K:\mathbb{Q}]} \sqrt{\sum_{j=1}^N |\sigma_i(x_j)|^2}.$$

- 2.

$$\frac{[\Lambda : \Lambda' \cap \Lambda]}{[\Lambda' : \Lambda' \cap \Lambda]} = N((x_1, \dots, x_N)). \quad (20)$$

Here the right hand side denotes the norm of the fractional ideal $\mathcal{O}_K x_1 + \dots + \mathcal{O}_K x_N$.

Proof of Claim 1:

Let us evaluate $\det \Lambda'$. Fix a \mathbb{Z} -basis a_1, a_2, \dots, a_r of \mathcal{O}_K , where $r = [K : \mathbb{Q}]$. A \mathbb{Z} -basis of Λ' is given by $a_1 w_1, a_2 w_1, \dots, a_r w_1, a_1 w_2, a_2 w_2, \dots, a_r w_2, \dots, a_1 w_m, a_2 w_m, \dots, a_r w_m$. We will calculate the volume of the parallelepiped spanned by these vectors with respect to the quadratic form in Equation 3. Observe that for $x, y \in K_{\mathbb{R}}$

$$\mathrm{tr}(x\bar{y}) = \sum_{i=1}^r \sigma_i(x) \overline{\sigma_i(y)}.$$

Let $w_i = (w_{i1}, w_{i2}, \dots, w_{in}) \in K^n$. If we define the $rn \times rm$ matrix

$$A = \begin{bmatrix} \sigma_1(a_1 w_{11}) & \dots & \sigma_1(a_r w_{11}) & \dots & \sigma_1(a_1 w_{m1}) & \dots & \sigma_1(a_r w_{m1}) \\ & & \vdots & & \vdots & & \vdots \\ \sigma_r(a_1 w_{11}) & \dots & \sigma_r(a_r w_{11}) & \dots & \sigma_r(a_1 w_{m1}) & \dots & \sigma_r(a_r w_{m1}) \\ & & \vdots & & \vdots & & \vdots \\ \sigma_1(a_1 w_{1n}) & \dots & \sigma_1(a_r w_{1n}) & \dots & \sigma_1(a_1 w_{mn}) & \dots & \sigma_1(a_r w_{mn}) \\ & & \vdots & & \vdots & & \vdots \\ \sigma_r(a_1 w_{1n}) & \dots & \sigma_r(a_r w_{1n}) & \dots & \sigma_r(a_1 w_{mn}) & \dots & \sigma_r(a_r w_{mn}) \end{bmatrix}$$

then it follows that

$$(\det \Lambda')^2 = \Delta_K^{-2m} \det A^* A.$$

We can expand the right hand side using the Cauchy-Binet theorem, obtaining that

$$\det A^* A = \sum_{\substack{I \subseteq \{1 \dots rm\} \\ \# I = rm}} |\det(A_I)|^2,$$

where A_I is the $rm \times rm$ minor of A with rows in I .

Each row of A is a complex embedding of the vector

$$(a_i w_{jk})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq m}} \text{ for some } k \in \{1, \dots, n\}.$$

We claim that the only I for which $\det(A_I)^2$ could be non-zero are the ones where each embedding σ_i appears exactly m times applied to various m -subsets of these n possible rows. That is, $I \subseteq \{1 \dots rn\}$ should be of the form

$$I = \bigsqcup_{i \in \{1, \dots, m\}} \bigcup_{k \in J_i} \{kr - r + i\}, \text{ for some } J_1, J_2, \dots, J_r \subseteq \{1, \dots, n\}, \#J_1 = \#J_2 = \dots = \#J_r = m. \quad (21)$$

To observe this, note that if $m' > m$ then the following row-vectors are K -linearly dependent.

$$\begin{aligned} & (w_{1k_1}, w_{2k_1}, \dots, w_{mk_1}), \\ & (w_{1k_2}, w_{2k_2}, \dots, w_{mk_2}), \\ & \vdots \\ & (w_{1k_{m'}}, w_{2k_{m'}}, \dots, w_{mk_{m'}}). \end{aligned}$$

This implies that the following rows are \mathbb{Q} -linearly dependent

$$\begin{aligned} & (a_1 w_{1k_1}, \dots, a_r w_{1k_1}, \dots, a_1 w_{mk_1}, \dots, a_r w_{mk_1}), \\ & (a_1 w_{1k_2}, \dots, a_r w_{1k_2}, \dots, a_1 w_{mk_2}, \dots, a_r w_{mk_2}), \\ & \vdots \\ & (a_1 w_{1k_{m'}}, \dots, a_r w_{1k_{m'}}, \dots, a_1 w_{mk_{m'}}, \dots, a_r w_{mk_{m'}}), \end{aligned}$$

and therefore if we apply invertible \mathbb{Q} -linear maps in each coordinate of these rows then they remain \mathbb{Q} -linearly dependent. Hence, each σ_i will appear in no more than m rows associated to each and as a result I can only be of the form in Equation (21).

Suppose therefore that I is of the form in Equation (21) where the $J_i = \{k_{i1}, k_{i2}, \dots, k_{im}\} \subseteq \{1, \dots, n\}$. Then up to permutation of rows, the matrix A_I is given by

$$A_I = \begin{bmatrix} \sigma_1(a_1)\sigma_1(w_{1k_{11}}) & \dots & \sigma_1(a_r)\sigma_1(w_{1k_{11}}) & \dots & \sigma_1(a_1)\sigma_1(w_{mk_{11}}) & \dots & \sigma_1(a_r)\sigma_1(w_{mk_{11}}) \\ \sigma_1(a_1)\sigma_1(w_{1k_{12}}) & \dots & \sigma_1(a_r)\sigma_1(w_{1k_{12}}) & \dots & \sigma_1(a_1)\sigma_1(w_{mk_{12}}) & \dots & \sigma_1(a_r)\sigma_1(w_{mk_{12}}) \\ & & & \vdots & & & \\ \sigma_1(a_1)\sigma_1(w_{1k_{1m}}) & \dots & \sigma_1(a_r)\sigma_1(w_{1k_{1m}}) & \dots & \sigma_1(a_1)\sigma_1(w_{mk_{1m}}) & \dots & \sigma_1(a_r)\sigma_1(w_{mk_{1m}}) \\ & & & \vdots & & & \\ \sigma_r(a_1)\sigma_r(w_{1k_{r1}}) & \dots & \sigma_r(a_r)\sigma_r(w_{1k_{r1}}) & \dots & \sigma_r(a_1)\sigma_r(w_{mk_{r1}}) & \dots & \sigma_r(a_r)\sigma_r(w_{mk_{r1}}) \\ \sigma_r(a_1)\sigma_r(w_{1k_{r2}}) & \dots & \sigma_r(a_r)\sigma_r(w_{1k_{r2}}) & \dots & \sigma_r(a_1)\sigma_r(w_{mk_{r2}}) & \dots & \sigma_r(a_r)\sigma_r(w_{mk_{r2}}) \\ & & & \vdots & & & \\ \sigma_r(a_1)\sigma_r(w_{1k_{rm}}) & \dots & \sigma_r(a_r)\sigma_r(w_{1k_{rm}}) & \dots & \sigma_r(a_1)\sigma_r(w_{mk_{rm}}) & \dots & \sigma_r(a_r)\sigma_r(w_{mk_{rm}}) \end{bmatrix}.$$

Upon inspection, one can conclude that actually $A_I = WB$ where W and B are $rm \times rm$ matrices given

by

$$W = \begin{bmatrix} \sigma_1(w_{1k_{11}}) & \cdots & \sigma_1(w_{mk_{11}}) & & & \\ & & \vdots & & & \\ \sigma_1(w_{1k_{1m}}) & \cdots & \sigma_1(w_{mk_{1m}}) & & & \\ & & & \ddots & & \\ & & & & \sigma_r(w_{1k_{r1}}) & \cdots & \sigma_r(w_{mk_{r1}}) \\ & & & & & & \vdots \\ & & & & \sigma_r(w_{1k_{rm}}) & \cdots & \sigma_r(w_{mk_{rm}}) \end{bmatrix},$$

$$B = \begin{bmatrix} \sigma_1(a_1) & \cdots & \sigma_1(a_r) & & & & \\ & & & \sigma_1(a_1) & \cdots & \sigma_1(a_r) & \\ & & & & & & \cdots \\ & & & & & & \sigma_1(a_1) & \cdots & \sigma_1(a_r) \\ \sigma_2(a_1) & \cdots & \sigma_2(a_r) & & & & \\ & & & \sigma_2(a_1) & \cdots & \sigma_2(a_r) & \\ & & & & & & \cdots \\ & & & & & & \sigma_2(a_1) & \cdots & \sigma_2(a_r) \\ & & & & & & \vdots \\ \sigma_r(a_1) & \cdots & \sigma_r(a_r) & & & & \\ & & & \sigma_r(a_1) & \cdots & \sigma_r(a_r) & \\ & & & & & & \cdots \\ & & & & & & \sigma_r(a_1) & \cdots & \sigma_r(a_r) \end{bmatrix}.$$

It then follows that $|\det B| = \Delta_K^m$ and thus as J_1, J_2, \dots, J_r go through all the possible m -subsets of $\{1, \dots, n\}$

$$\sum_{\substack{I \subseteq \{1, \dots, rn\} \\ \#I=m}} |\det A_I|^2 = \Delta_K^{2m} \prod_{l=1}^r \left(\sum_{\{k_1, \dots, k_m\} \subseteq \{1, \dots, n\}} \left| \det_{1 \leq i, j \leq m} [\sigma_l(w_{ik_j})] \right|^2 \right).$$

This settles the claim.

Proof of Claim 2:

We are given $\{(w_{i1}, w_{i2}, \dots, w_{in})\}_{i=1}^m \in K^n$. Define $W \in M_{n \times m}(\mathcal{O}_K)$ as

$$W = \begin{bmatrix} w_{11} & w_{21} & \cdots & w_{m1} \\ w_{21} & w_{22} & \cdots & w_{m2} \\ & & \vdots & \\ w_{m1} & w_{m2} & \cdots & w_{mn} \end{bmatrix}.$$

Then $\Lambda' = W\mathcal{O}_K^m$ and $\Lambda = WK^m \cap \mathcal{O}_K^n$.

To prove this claim, it is sufficient to prove it for the case when $\{w_{ij}\} \subseteq \mathcal{O}_K$. Indeed, let us multiply W by an integer $\kappa \in \mathcal{O}_K$ that can cancel all the denominators (i.e. $\kappa \cdot w_{ij} \in \mathcal{O}_K$). Then note that $\kappa\Lambda' \subseteq \Lambda' \cap \Lambda$ and

$$[\Lambda' : \kappa\Lambda'] = N(\kappa)^m,$$

so we have

$$\frac{[\Lambda : \Lambda \cap \Lambda']}{[\Lambda' : \Lambda \cap \Lambda']} = \frac{[\Lambda : \Lambda \cap \Lambda'] [\Lambda' \cap \Lambda : \kappa\Lambda']}{[\Lambda' : \Lambda \cap \Lambda'] [\Lambda' \cap \Lambda : \kappa\Lambda']} = \frac{[\Lambda : \kappa\Lambda']}{[\Lambda' : \kappa\Lambda']} = [\Lambda : \kappa\Lambda'] N(\kappa)^{-m}.$$

This establishing the identity $[\Lambda : \kappa\Lambda'] = N(\langle \kappa^m x_1, \dots, \kappa^m x_N \rangle)$ would finish the proof.

Therefore, let us now assume without loss of generality that we have $\{w_{ij}\} \subseteq \mathcal{O}_K$ and hence $\Lambda' \subseteq \Lambda$. We want to show that

$$N(\langle x_1, \dots, x_N \rangle) = [\Lambda : \Lambda'] = [W^{-1}\mathcal{O}_K^n : \mathcal{O}_K^m],$$

where $W^{-1}\mathcal{O}_K^n = \{\alpha = (\alpha_1, \dots, \alpha_m) \in K^m \mid W\alpha \in \mathcal{O}_K^n\}$, which is an \mathcal{O}_K -module in K^m . Let W_J be the $m \times m$ minor of W by selecting a subset of rows $J \subseteq \{1, \dots, m\}$ with $\#J = m$. Then by multiplying by adjoint matrices, it is clear that for $\alpha \in K^m$

$$W \cdot \alpha \in \mathcal{O}_K^n \Rightarrow W_J \cdot \alpha \in \mathcal{O}_K^m \Rightarrow \det(W_J) \cdot \alpha \in \mathcal{O}_K^m.$$

Define $\mathcal{I} = \langle \rho \rangle \subseteq \mathcal{O}_K$ to be the ideal generated by

$$\rho = \prod_{J \in \binom{[n]}{m}} \det W_J.$$

We see that if $\alpha \in \langle \frac{1}{\rho} \rangle = \mathcal{I}^{-1}$, then we have

$$\mathcal{O}_K^m \subseteq W^{-1} \mathcal{O}_K^n \subseteq (\mathcal{I}^{-1})^m,$$

since \mathcal{I}^{-1} is the fractional ideal “inverse” of \mathcal{I} defined as $\mathcal{I}^{-1} = \{\kappa \in \mathcal{O}_K \mid \kappa \mathcal{I} \subseteq \mathcal{O}_K\}$. Note that \mathcal{I}^{-1} is an \mathcal{O}_K -module and so is $\mathcal{I}^{-1}/\mathcal{O}_K$. We are thus interested in simply calculating the number of solutions of

$$W \cdot \alpha = 0 \pmod{\mathcal{O}_K}, \quad \alpha \in (\mathcal{I}^{-1}/\mathcal{O}_K)^m.$$

In particular, we want to show that the number of solutions to this is equal, as in Equation (20), to

$$N(\langle \det W_J \rangle_{J \subseteq \{1, \dots, m\}}).$$

This calculation can be done locally, with respect to each prime ideal \mathcal{P} dividing \mathcal{I} . Since \mathcal{I} is a principal ideal, multiplication by the generator ρ gives us an isomorphism of \mathcal{O}_K -modules as

$$\frac{\mathcal{I}^{-1}}{\mathcal{O}_K} \simeq \frac{\mathcal{O}_K}{\mathcal{I}}.$$

Factoring $\mathcal{I} = \mathcal{P}_1^{f_1} \mathcal{P}_2^{f_2} \dots \mathcal{P}_s^{f_s}$ and writing the sum of ideals generated by the $\det W_J$ as $\mathcal{P}_1^{e_1} \mathcal{P}_2^{e_2} \dots \mathcal{P}_s^{e_s}$, we have that $0 \leq e_i \leq f_i$ for each $i \in \{1, \dots, s\}$ and

$$\frac{\mathcal{I}^{-1}}{\mathcal{O}_K} \simeq \frac{\mathcal{O}_K}{\mathcal{I}} = N(\mathcal{P}_1)^{e_1} N(\mathcal{P}_2)^{e_2} \dots N(\mathcal{P}_s)^{e_s}.$$

Hence, the problem is reduced to showing that the number of solutions of the following is $N(\mathcal{P})^{e_i}$ for each $i \in \{1, \dots, s\}$.

$$W \cdot \alpha = 0 \pmod{\mathcal{P}_i^{f_i}}, \quad \alpha \in (\mathcal{O}_K/\mathcal{P}_i^{f_i})^m.$$

This can be proved via induction as explained in [27, Lemma 4.5].

Remark 67. Observe that for any $x_1, \dots, x_N \in K$, we get that the norm of the principal ideal generated by x_1, \dots, x_N is

$$N(\langle x_1, \dots, x_N \rangle)^{-1} = \prod_{\substack{v \in M_K \\ v \nmid \infty}} \max_{1 \leq i \leq N} |x_i|_v$$

B Convex combinations lemma

We record here a general lemma that was used in some special instances in the paper. We hope that future literature around this topic could benefit from this idea.

Lemma 68. Let $D \in M_{m \times n}(K)$ (not necessarily reduced) be a matrix given as

$$D = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ & \vdots & & \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} \end{bmatrix}. \quad (22)$$

Let $f : K_{\mathbb{R}}^t \rightarrow \mathbb{R}$ be the indicator function of a unit ball. Then, we have that for any $c_1, \dots, c_n \in [0, 1]$ such that $\sum c_i = 1$

$$\frac{1}{V(\text{mtd})} \int_{K_{\mathbb{R}}^{t \times m}} \prod_{j=1}^n f\left(\sum_{i=1}^m \alpha_{ij} x_i\right) dx \leq \prod_{\sigma: K \rightarrow \mathbb{C}} \left(\sum_{J \in \binom{[n]}{m}} (\prod_{j \in J} c_j) |\sigma(\det(D_J))|^2 \right)^{-\frac{t}{2}}.$$

Here the product on the right is over $d = r_1 + 2r_2$ embeddings of K into \mathbb{C} .

Proof. Let $x = (x_1, \dots, x_m) \in (K_{\mathbb{R}}^t)^m$. The integral is computing the volume of the set in $(K_{\mathbb{R}}^t)^m$ satisfying

$$\begin{aligned} \|\alpha_{11}x_1 + \dots + \alpha_{1m}x_m\|^2 &\leq 1, \\ \|\alpha_{12}x_1 + \dots + \alpha_{2m}x_m\|^2 &\leq 1, \\ &\vdots \\ \|\alpha_{1n}x_1 + \dots + \alpha_{mn}x_m\|^2 &\leq 1. \end{aligned}$$

Adding all of these together with a weight of c_i assigned to each respective condition, we get

$$\sum_{j=1}^n c_j \|\alpha_{1j}x_1 + \dots + \alpha_{mj}x_m\|^2 \leq 1. \quad (23)$$

This means that the set whose volume we are estimating is contained in the set of points satisfying inequality (23). The latter defines an ellipsoid whose volume is given by

$$\frac{V(mtd)}{\text{vol}\left(\frac{K_{\mathbb{R}}^{t \times m}}{\mathcal{O}_K \sqrt{c_1} \omega_1 + \dots + \mathcal{O}_K \sqrt{c_n} \omega_n}\right)},$$

where $\omega_1, \dots, \omega_n \in K_{\mathbb{R}}^t$ are the columns of D .

Note that writing $K_{\mathbb{R}}^{t \times m} \simeq K_{\mathbb{R}}^{m \times t}$ the quadratic form defined by (23) is actually t copies of the quadratic form in $K_{\mathbb{R}}^m$ defined by the same equation but with $x_1, \dots, x_m \in K_{\mathbb{R}}^m$ instead. The result now follows from Lemma 69. \square

Lemma 69. *Let $D \in M_{m \times n}(K)$ be a full-rank matrix, for example, the one given in Equation (22). Let $\Lambda \subseteq K_{\mathbb{R}}^m$ be the \mathcal{O}_K -module generated by the columns of D . Then, the covolume of this lattice is*

$$\prod_{\sigma: K \rightarrow \mathbb{C}} \left(\sum_{J \in \binom{[n]}{m}} |\sigma(\det(D_J))|^2 \right)^{\frac{1}{2}}.$$

Here the product is $d = r_1 + 2r_2$ embeddings of $K \rightarrow \mathbb{C}$ and the inner sum is over all $m \times m$ minors of D .

Proof. Follows from Proposition 66, Part 1. \square

References

- [1] Carl L. Siegel. A mean value theorem in geometry of numbers. *Ann. of Math. (2)*, 46(2):340–347, 1945.
- [2] Edmund Hlawka. Zur Geometrie der Zahlen. *Math. Z.*, 49(1):285–312, 1943.
- [3] Stephanie Vance. Improved sphere packing lower bounds from Hurwitz lattices. *Adv. Math.*, 227(5):2144–2156, 2011.
- [4] Akshay Venkatesh. A note on sphere packings in high dimension. *Int. Math. Res. Not. IMRN*, 2013(7):1628–1642, 2013.
- [5] Nihar P. Gargava. Lattice packings through division algebras. *Math. Z.*, 303(1):1–32, 2023.
- [6] Claude A. Rogers. The moments of the number of points of a lattice in a bounded set. *Philos. Trans. Roy. Soc. A*, 248(945):225–251, 1955.
- [7] Claude A. Rogers. Mean values over the space of lattices. *Acta Math.*, 94:249–287, 1955.
- [8] Claude A. Rogers. The number of lattice points in a set. *Proc. Lond. Math. Soc. (3)*, 6(2):305–320, 1956.
- [9] Seungki Kim. Adelic Rogers integral formula. *arXiv:2205.03138*, 2022.
- [10] André Weil. Sur la formule de Siegel dans la théorie des groupes classiques. *Acta Math.*, 113:1–87, 1965.

- [11] Nathan Hughes. Mean values over lattices in number fields and effective Diophantine approximation. *arXiv:2306.02499*, 2023.
- [12] Claude A. Rogers. Lattice coverings of space: the Minkowski–Hlawka theorem. *Proc. Lond. Math. Soc. (3)*, 8(3):447–465, 1958.
- [13] Or Ordentlich, Oded Regev, and Barak Weiss. New bounds on the density of lattice coverings. *J. Amer. Math. Soc.*, 35(1):295–308, 2022.
- [14] Dmitry Kleinbock and Grigory A. Margulis. Logarithm laws for flows on homogeneous spaces. *Invent. Math.*, 138:451–494, 1998.
- [15] Jayadev S. Athreya and Grigory A. Margulis. Logarithm laws for unipotent flows, I. *J. Mod. Dyn.*, 3(3):359–378, 2009.
- [16] Michael Björklund and Alexander Gorodnik. Poisson approximation and Weibull asymptotics in the geometry of numbers. *Trans. Amer. Math. Soc.*, 376(3):2155–2180, 2023.
- [17] Gaurav Aggarwal and Anish Ghosh. Two central limit theorems in Diophantine approximation. *arXiv:2306.02304*, 2023.
- [18] Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-LWE for any ring and modulus. In *STOC’17—Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 461–473. ACM, New York, 2017.
- [19] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Mildly short vectors in cyclotomic ideal lattices in quantum polynomial time. *J. ACM*, 68(2):1–26, 2021.
- [20] Gabrielle De Micheli and Daniele Micciancio. A fully classical LLL algorithm for modules. Cryptology ePrint Archive, Paper 2022/1356, 2022. <https://eprint.iacr.org/2022/1356>.
- [21] Jason Rush and Neil Sloane. An improvement to the Minkowski–Hlawka bound for packing superballs. *Mathematika*, 34:8–18, 1987.
- [22] Jason Rush. A lower bound on packing density. *Invent. Math.*, 98(3):499–510, 1989.
- [23] Hans-Andrea Loeliger. Averaging bounds for lattices and linear codes. *IEEE Trans. Inform. Theory*, 43(6):1767–1773, 1997.
- [24] Philippe Gaborit and Gilles Zémor. On the construction of dense lattices with a given automorphisms group. *Ann. Inst. Fourier*, 57(4):1051–1062, 2007.
- [25] Philippe Moustrou. On the density of cyclotomic lattices constructed from codes. *Int. J. Number Theory*, 13(05):1261–1274, 2017.
- [26] Nihar Gargava and Vlad Serban. Dense packings via lifts of codes to division rings. *IEEE Trans. Inform. Theory.*, 69(5), 2022.
- [27] Wolfgang M. Schmidt. On heights of algebraic subspaces and Diophantine approximations. *Ann. of Math. (2)*, 85(3):430–472, 1967.
- [28] Claude A. Rogers. Existence theorems in the geometry of numbers. *Ann. of Math. (2)*, 48(4):994–1002, 1947.
- [29] Laurent Clozel, Hee Oh, and Emmanuel Ullmo. Hecke operators and equidistribution of Hecke points. *Invent. Math.*, 144(2):327–351, 2001.
- [30] Alex Gorodnik, François Maucourant, and Hee Oh. Manin’s and Peyre’s conjectures on rational points and adelic mixing. *Annales Sci. Éc. Norm. Supér. (4)*, 41(3):385–437, 2008.
- [31] Andrzej Schinzel. On the product of the conjugates outside the unit circle of an algebraic number. *Acta Arith.*, 24(4):385–399, 1973.

- [32] Francesco Amoroso and Roberto Dvornicich. A lower bound for the height in abelian extensions. *J. Number Theory*, 80(2):260–272, 2000.
- [33] James McKee and Chris Smyth. *Around the Unit Circle: Mahler Measure, Integer Matrices and Roots of Unity*. Universitext. Springer International Publishing, 2021.
- [34] Francesco Amoroso, Sinnou David, and Umberto Zannier. On fields with Property (B). *Proc. Amer. Math. Soc.*, 142(6):1893–1910, 2014.
- [35] Michel Langevin. Minorations de la maison et de la mesure de Mahler de certains entiers algébriques. *C. R. Acad. Sci. Paris Sér. I Math.*, 303(12):523–526, 1986.
- [36] Lukas Pottmeyer. Small totally p -adic algebraic numbers. *Int. J. Number Theory*, 14(10):2687–2697, 2018.
- [37] Enrico Bombieri and Umberto Zannier. A note on heights in certain infinite extensions of \mathbb{Q} . *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.*, 12(1):5–14, 2001.
- [38] Philipp Habegger. Small height and infinite nonabelian extensions. *Duke Math. J.*, 162(11):2027–2076, 2013.
- [39] Edward Dobrowolski. On a question of Lehmer and the number of irreducible factors of a polynomial. *Acta Arith.*, 34(4):391–401, 1979.
- [40] Paul Voutier. An effective lower bound for the height of algebraic numbers. *Acta Arith.*, 74(1):81–95, 1996.
- [41] Thomas Ange. Le théorème de Schanuel dans les fibrés adéliques Hermitiens. *Manuscripta Math.*, 144(3-4):565–608, 2014.
- [42] David W. Boyd. Variations on a theme of Kronecker. *Canad. Math. Bull.*, 21(2):129–133, 1978.
- [43] Claude A. Rogers. Two integral inequalities. *J. Lond. Math. Soc.*, 31(2):235–238, 1956.

N. Gargava, ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE, VAUD, SWITZERLAND
E-mail address: `nihar.gargava@epfl.ch`

V. Serban, ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE, VAUD, SWITZERLAND
E-mail address: `vlad.serban@epfl.ch`

M. Viazovska, ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE, VAUD, SWITZERLAND
E-mail address: `maryna.viazovska@epfl.ch`