

# MEAN VALUE FORMULAS ON SUBLATTICES AND FLAGS OF THE RANDOM LATTICE

SEUNGKI KIM

**ABSTRACT.** We present extensions of the Siegel integral formula ([13]), which counts the vectors of the random lattice, to the context of counting its sublattices and flags. Perhaps surprisingly, it turns out that many quantities of interest diverge to infinity.

## 1. INTRODUCTION

We start by recalling the celebrated Siegel integral formula ([13]), one of the cornerstones of geometry of numbers. Let  $X_n = \mathrm{SL}(n, \mathbb{Z}) \backslash \mathrm{SL}(n, \mathbb{R})$  be the space of lattices of determinant 1, and equip  $X_n$  with the measure  $\mu_n$  (defined up to a constant, which is to be determined by Theorem 1 below) that is inherited from the Haar measure of  $\mathrm{SL}(n, \mathbb{R})$ ; in particular,  $\mu_n$  is invariant under the right  $\mathrm{SL}(n, \mathbb{R})$ -action on  $X_n$ . In this setting, Siegel proved the following theorem.

**Theorem 1** (Siegel [13]).  *$\mu_n(X_n) < \infty$ , so upon normalizing we may suppose  $\mu_n(X_n) = 1$ . Also, for  $f : \mathbb{R}^n \rightarrow \mathbb{R}$  a compactly supported and bounded Borel measurable function, we have*

$$\int_{X_n} \sum_{\substack{x \in L \\ x \neq 0}} f(x) d\mu_n(L) = \int_{\mathbb{R}^n} f(x) dx.$$

There are many other useful variations of Theorem 1. For instance, Rogers proved the following, known as the Rogers integral formula.

**Theorem 2** (Rogers [7]). *Let  $1 \leq k \leq n - 1$ . Then for  $f : (\mathbb{R}^n)^k \rightarrow \mathbb{R}$  a compactly supported and bounded Borel measurable function, we have*

$$\int_{X_n} \sum_{\substack{x_1, \dots, x_k \in L \\ \mathrm{rk} \langle x_1, \dots, x_k \rangle = k}} f(x_1, \dots, x_k) d\mu_n(L) = \int_{\mathbb{R}^n} \dots \int_{\mathbb{R}^n} f(x_1, \dots, x_k) dx_1 \dots dx_k.$$

Rogers also proved explicit formulas of this kind for the cases  $\mathrm{rk} \langle x_1, \dots, x_k \rangle = l$  for any  $1 \leq l < k$  — see ([7]) for the precise statement. This result, called the Rogers integral formula, is the essential tool for the study of random lattice vectors, since it makes possible to study the higher moments of the lattice vector-counting function  $\sum_{x \in L \setminus \{0\}} f(x)$ . See Schmidt ([9]) for yet more variants of the Siegel integral formula, and Kim ([4]), Shapira and Weiss ([11]), and Södergren and Strömbergsson ([15]) for some of the recent applications of these mean value theorems.

The motivation of the present paper is to explore the extensions of these results from the counting of lattice vectors to that of rank  $d < n$  sublattices and of flags. In other words, we ask whether they too demonstrate any interesting statistical behavior, like the lattice vectors do.

On the practical side, we hope that such extensions will find applications in lattice-based cryptography. One of the basic implications of Theorem 1, that a ball of volume  $V$  contains  $V$  nonzero lattice vectors on average, is already a fundamental tool for predicting and fine-tuning the decryption process. More recent results, such as the Poissonian behavior of short lattice vectors ([14]), have also found applications in cryptanalysis ([1]). It is therefore natural to expect that analogous results on sublattices would be useful too, since those are what the BKZ algorithm (stands for Block Korkine-Zolotarev, originally proposed by Schnorr and Euchner [10]), the standard decryption algorithm for lattice-based systems, operates on.

Our first result is the following generalization of Theorem 2. For a lattice  $L \in X_n$  and  $1 \leq d < n$ , write  $\text{Gr}(L, d)$  for the set of primitive rank  $d$  sublattices of  $L$ . For an element  $A \in \text{Gr}(L, d)$ , define  $\det A$  as follows: choose any basis  $\{v_1, \dots, v_d\}$  of  $A$ , and we set  $\det A = \|v_1 \wedge \dots \wedge v_d\|$ , where  $\|\cdot\|$  here is the standard Euclidean norm in  $\wedge^d \mathbb{R}^n$ . This definition is independent of the basis choice. Throughout this paper, for  $A \in \text{Gr}(L, d)$  and  $H \geq 0$  we write

$$f_H(A) = \begin{cases} 1 & \text{if } \det A \leq H \\ 0 & \text{otherwise.} \end{cases}$$

We also define

$$a(n, d) = \frac{1}{n} \binom{n}{d} \prod_{i=1}^d \frac{V(n-i+1)\zeta(i)}{V(i)\zeta(n-i+1)},$$

where  $V(i) = \pi^{i/2}/\Gamma(1+i/2)$  is the volume of the unit ball in  $\mathbb{R}^i$ , and  $\zeta(i)$  is the Riemann zeta function evaluated at the positive integer  $i$ , except that we pretend  $\zeta(1) = 1$  for notational convenience. Then we prove the following, the first main result of the present paper.

**Theorem 3.** *Suppose  $1 \leq k \leq n-1$ ,  $1 \leq d_1, \dots, d_k \leq n-1$  with  $d_1 + \dots + d_k \leq n-1$ . Then*

$$\int_{X_n} \sum_{\substack{A_1 \in \text{Gr}(L, d_1) \\ A_1, \dots, A_k \text{ independent}}} \dots \sum_{\substack{A_k \in \text{Gr}(L, d_k)}} f_{H_1}(A_1) \dots f_{H_k}(A_k) d\mu_n(L) = \prod_{i=1}^k a(n, d_i) H_i^n.$$

*Remark.* (i) We point out that the  $k=1$  case of this theorem is proved by Thunder ([17]) in the more general context of number fields.

(ii) If one wants a formula that counts non-primitive sublattices as well, by a standard Möbius inversion argument (see [8], or Section 7.1 of [5]) one can show that we could simply replace all the  $a(n, d)$  by

$$c(n, d) = a(n, d) \prod_{i=1}^d \zeta(n-i+1).$$

The same applies to our other results introduced below.

It is natural to ask what happens if the sublattices  $A_1, \dots, A_k$  are not independent. In fact, if  $A_i \cap A_j \neq A_i, A_j, 0$  for some  $i, j$ , the corresponding integral diverges, as can be seen from the next statement that we prove.

**Theorem 4.** *Let  $1 \leq r < d_1, d_2$ , so that  $d_1 + d_2 < n + r$ . Then*

$$\int_{X_n} \sum_{A \in \text{Gr}(L, d_1)} \sum_{\substack{B \in \text{Gr}(L, d_2) \\ \text{rk } A \cap B = r}} f_{H_1}(A) f_{H_2}(B) d\mu_n(L) = \infty.$$

Because

$$(1) \quad \int_{X_n} \left( \sum_{A \in \text{Gr}(L, d)} f_H(A) \right)^2 d\mu_n(L) = \sum_{r=0}^d \int_{X_n} \sum_{A \in \text{Gr}(L, d)} \sum_{\substack{B \in \text{Gr}(L, d) \\ \text{rk } A \cap B = r}} f_H(A) f_H(B) d\mu_n(L),$$

Theorem 4 has the following consequence.

**Corollary.** *The  $L^2$ -norm of  $\sum_{A \in \text{Gr}(L, d)} f_H(A)$  diverges.*

Thus, unfortunately, it would be difficult to study  $\text{Gr}(L, d)$  via the standard methods. At least we learn that the statistics of rank  $d$  sublattices is radically different from that of lattice vectors. In particular, the various Poissonian properties enjoyed by random lattice vectors (see e.g. [4]) fail spectacularly for rank  $d$  sublattices. It may be possible to tweak the left-hand side of (1), for example by restricting to counting certain pairs of elements of  $\text{Gr}(L, d)$ , to extract some useful information, but I have been unable to do so.

At the other extreme is the case in which  $A_1 \subseteq \dots \subseteq A_k$ , and we would be counting *flags*. For  $L \in X_n$  and  $d_0 = 0 < d_1 < \dots < d_k < d_{k+1} = n$ , a flag of type  $\mathfrak{d} = (d_1, \dots, d_k)$  (rational with respect to  $L$ ) is a sequence of sublattices

$$A_1 \subseteq A_2 \subseteq \dots \subseteq A_k \subseteq L$$

such that  $\dim A_i = d_i$ . Define

$$a(n, \mathfrak{d}) = a(n, d_1) \prod_{i=1}^{k-1} \frac{n - d_{i-1}}{d_{i+1} - d_{i-1}} a(n - d_i, d_{i+1} - d_i).$$

(This coincides with  $a(\alpha)$  in Thunder ([16]).) Then we have the following formula for counting rational flags.

**Theorem 5.** *The  $\mu_n$ -average of the number of flags  $A_1 \subseteq \dots \subseteq A_k$  of type  $\mathfrak{d} = (d_1, \dots, d_k)$  such that  $\det A_i \leq H_i$  for  $i = 1, \dots, k$  is equal to*

$$a(n, \mathfrak{d}) \prod_{i=1}^k H_i^{d_{i+1} - d_{i-1}}.$$

Theorem 5 has the following corollary.

**Corollary.** *The  $\mu_n$ -average number of flags of height  $\leq H$  is equal to  $\infty$ .*

Here, the *height* of a flag  $A_1 \subseteq \dots \subseteq A_k$  is defined as the quantity

$$\prod_{i=1}^k (\det A_i)^{d_{i+1} - d_{i-1}}.$$

(See e.g. [3] or [16].) Therefore, the average number of flags of height  $\leq H$  equals

$$a(n, \mathfrak{d}) \int_{\substack{x_i > 0 \\ x_1 \dots x_k \leq H}} dx_1 \dots dx_k,$$

but this is  $\infty$  for  $k \geq 2$ . It may be interesting to compare this result with Theorem 5 in Thunder ([16]).

We end the introduction with a few words on the method of proof. It is a product of a reflection on the phenomenon in which the mean of a counting function over  $X_n$  coincides with its main term for a fixed individual lattice. For instance, Theorem 1 implies

$$\int_{X_n} |B(V) \cap L \setminus \{0\}| d\mu_n(L) = V,$$

which is the expected main term of an estimate of  $|B(V) \cap L \setminus \{0\}|$  for a fixed  $L$ . Among several possible approaches to mean value formulas, we chose the one that transparently shows how this happens. A discrete analogue of Theorem 1 of Rogers ([7]), which bears some semblance to the Hecke equidistribution (Lemma 7 below), reduces the problem of averaging over  $X_n$  to that of counting over a fixed lattice; and the author's recent work ([5]) solves this counting problem. This argument also serves to fix a recently found error in Rogers' proof of the formula named after him ([7]); see Section 2 below for details. For Theorems 4 and 5, we also need the standard unfolding trick for the Eisenstein series.

If so desired, an appropriate combination of these techniques allows one to handle many other integrals in which the sublattices  $A_1, \dots, A_k$  interact in different ways, e.g. something like

$$\int_{X_n} \sum_{\substack{A_1 \in \text{Gr}(L, d_1) \\ A_1, A_2 \text{ independent}}} \sum_{\substack{A_2 \in \text{Gr}(L, d_2) \\ A_1, A_2 \text{ independent}}} \sum_{B \in \text{Gr}(A_1 \oplus A_2, r)} f_{H_1}(A_1) f_{H_2}(A_2) f_{H_3}(B) d\mu_n(L).$$

**1.1. Acknowledgments.** This work was supported by NSF grant CNS-2034176. The author thanks the referee for the careful review of the original manuscript.

## 2. SOME BACKGROUND

Fix a positive integer  $n$ . For a prime  $p$  and  $c \in \{1, \dots, n\}$ , let  $\mathcal{M}_p^{(c)}$  be the set of  $n \times n$  integral matrices  $M = (m_{ij})_{1 \leq i, j \leq n}$  such that  $m_{ij} = \delta_{ij}$  for  $j \neq c$ , and  $0 \leq m_{ic} \leq p-1$  for  $i < c$ ,  $m_{cc} = p$ , and  $m_{ic} = 0$  for  $i > c$ . To illustrate,  $M$  is a matrix of the form

$$\begin{pmatrix} 1 & & & x_1 & & \\ & \ddots & & \vdots & & \\ & & 1 & x_{c-1} & & \\ & & & p & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}.$$

Also let  $\mathcal{M}_p = \bigcup_{c=1}^n \mathcal{M}_p^{(c)}$ . It is clear that  $|\mathcal{M}_p^{(c)}| = p^{c-1}$ , so  $|\mathcal{M}_p| = 1 + p + \dots + p^{n-1}$ . For the  $n \times n$  diagonal matrix

$$\alpha_p = \text{diag}(1, \dots, 1, p) = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & p \end{pmatrix},$$

$\mathcal{M}_p$  serves as a set of all distinct representatives of the right cosets of  $\Gamma$  in the double coset  $\Gamma \alpha_p \Gamma$ , where  $\Gamma = \text{SL}(n, \mathbb{Z})$  — see Chapter 3 of Shimura ([12]). The Hecke operator on the functions on  $X_n$  with respect to  $\alpha_p$ , which we denote by  $T_p$ , is defined as

$$\begin{aligned} T_p \rho(L) &= \frac{1}{|\Gamma \backslash \Gamma \alpha_p \Gamma|} \sum_{M \in \Gamma \backslash \Gamma \alpha_p \Gamma} \rho(p^{-1/n} ML) \\ &= \frac{1}{|\mathcal{M}_p|} \sum_{M \in \mathcal{M}_p} \rho(p^{-1/n} ML). \end{aligned}$$

Throughout this paper, we will also write  $L$  for any representative of the coset  $L \in X_n$  when it is harmless to do so, as we have done above. In other words, we write  $L$  for both an element of  $\mathrm{SL}(n, \mathbb{R})$  and the lattice spanned by the row vectors of  $L$ , to keep the notations simple.

Lemma 7 below, which is a discrete analogue of Theorem 1 of Rogers ([7]), is crucial to the present paper. However, the author (thanks to Kevin Schmitt) recently found that Rogers's argument contains an error: in p. 256 of [7], he claims  $\int_{X_n} \rho(\gamma L) d\mu_n = \int_{X_n} \rho(L) d\mu_n$  for any  $\gamma \in \mathrm{SL}(n, \mathbb{R})$ , saying that it follows "from the known properties of the fundamental domain," but offering no justification otherwise. This equality is in fact not true, which can be seen by taking  $n = 2$ ,  $\rho$  any function on  $X_n$  vanishing in a neighborhood of the cusp, and

$$\gamma = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

for large  $a > 0$ , for example. Fortunately, in our discrete context, the needed relation follows from the basic properties of the Hecke operators.

**Lemma 6.** *Let  $\rho(L)$  be an integrable function on  $X_n$ . Then*

$$\int_{X_n} T_p \rho(L) d\mu_n(L) = \int_{X_n} \rho(L) d\mu_n(L).$$

*Proof.* The argument is very similar to the proof of Proposition 3.39 in [12]. Write  $\Gamma = \mathrm{SL}(n, \mathbb{Z})$  as before, and let

$$\widetilde{\mathcal{M}}_p^{(c)} = \{E_{cn}M : M \in \mathcal{M}_p^{(c)}\},$$

where  $E_{cn}$  is the permutation matrix obtained by swapping the  $c$ -th and  $n$ -th rows of the  $n \times n$  identity matrix and then changing the sign of the  $n$ -th row (so that  $\det E_{cn} = 1$ ). Observe that  $\widetilde{\mathcal{M}}_p := \bigcup_{c=1}^n \widetilde{\mathcal{M}}_p^{(c)}$  is also a set of all representatives of the right cosets of  $\Gamma$  in  $\Gamma \alpha_p \Gamma$ . Moreover,  $\alpha_p^{-1}M \in \Gamma$  for all  $M \in \widetilde{\mathcal{M}}_p$ . Therefore

$$\Gamma = \Gamma \cap \alpha_p^{-1} \Gamma \alpha_p \Gamma = \bigcup_{M \in \widetilde{\mathcal{M}}_p} (\Gamma \cap \alpha_p^{-1} \Gamma \alpha_p \alpha_p^{-1} M) = \bigcup_{M \in \widetilde{\mathcal{M}}_p} (\Gamma \cap \alpha_p^{-1} \Gamma \alpha_p) \alpha_p^{-1} M.$$

This shows that the elements  $\alpha_p^{-1}M$ ,  $M \in \widetilde{\mathcal{M}}_p$ , serve as the coset representatives of  $\Gamma \cap \alpha_p^{-1} \Gamma \alpha_p$  in  $\Gamma$ . Hence we can reinterpret  $T_p$  as

$$T_p \rho(L) = \frac{1}{|\mathcal{M}_p|} \sum_{N \in (\Gamma \cap \alpha_p^{-1} \Gamma \alpha_p) \backslash \Gamma} \rho(p^{-1/n} \alpha_p N L).$$

For a choice of the fundamental domain  $P$  with respect to  $\Gamma \cap \alpha_p^{-1} \Gamma \alpha_p$ , we have

$$\begin{aligned} & \int_{X_n} T_p \rho(L) d\mu_n(L) \\ &= \frac{1}{|\mathcal{M}_p|} \int_{X_n} \sum_{N \in (\Gamma \cap \alpha_p^{-1} \Gamma \alpha_p) \backslash \Gamma} \rho(p^{-1/n} \alpha_p N L) d\mu_n(L) \\ &= \frac{1}{|\mathcal{M}_p|} \int_P \rho(p^{-1/n} \alpha_p L) d\mu_n(L) \\ &= \frac{1}{|\mathcal{M}_p|} \int_{p^{-1/n} \alpha_p P} \rho(L) d\mu_n(L). \end{aligned}$$

However,  $p^{-1/n}\alpha_p P$  is a fundamental domain with respect to  $\alpha_p\Gamma\alpha_p^{-1}\cap\Gamma$ . Since  $|\mathcal{M}_p| = [\Gamma : \Gamma \cap \alpha_p^{-1}\Gamma\alpha_p] = [\Gamma : \alpha_p\Gamma\alpha_p^{-1} \cap \Gamma]$  (see e.g. Proposition 3.6 of [12]), this completes the proof.  $\square$

**Lemma 7.** *Let  $\rho(L)$  be a non-negative integrable function on  $X_n$ . Suppose  $\lim_{p \rightarrow \infty} T_p \rho(L)$  exists and have the same (finite) value  $I$  for all  $L \in X_n$ . Then  $I = \int_{X_n} \rho d\mu_n$ .*

*Proof.* For any function  $F$  and  $h \in \mathbb{R}$ , write  $[F]_h := \min(F, h)$ . For any  $h > I$ , the dominated convergence theorem implies

$$\int_{X_n} [T_p \rho]_h(L) d\mu_n(L) \rightarrow I$$

as  $p \rightarrow \infty$ . Also by Lemma 6, we have

$$\int_{X_n} [\rho]_h(L) d\mu_n(L) = \int_{X_n} T_p[\rho]_h(L) d\mu_n(L) \leq \int_{X_n} [T_p \rho]_h(L) d\mu_n(L).$$

Taking  $p \rightarrow \infty$  and then  $h \rightarrow \infty$  here, by the monotone convergence theorem we obtain the upper bound

$$\int_{X_n} \rho(L) d\mu_n(L) \leq I.$$

On the other hand, consider the integral

$$\begin{aligned} & \int_{X_n} T_p \rho(L) d\mu_n(L) \\ &= \int_{X_n} \frac{1}{|\mathcal{M}_p|} \sum_{M \in \mathcal{M}_p} \rho(p^{-1/n} ML) d\mu_n(L) \\ &= \frac{1}{|\mathcal{M}_p|} \sum_{M \in \mathcal{M}_p} \int_{X_n} \rho(p^{-1/n} ML) d\mu_n(L). \end{aligned}$$

Combined with Fatou's lemma, this implies that

$$I = \int_{X_n} \lim_{p \rightarrow \infty} T_p \rho(L) d\mu_n(L) \leq \lim_{p \rightarrow \infty} \int_{X_n} T_p \rho(L) d\mu_n(L) = \int_{X_n} \rho(L) d\mu_n(L),$$

again by Lemma 6. This completes the proof.  $\square$

*Remark.* Lemma 7 may remind one of the Hecke equidistribution ([2]). Of course, the latter is a much deeper statement, but Lemma 7 has the advantage that it applies to functions that are neither compactly supported nor bounded, which is the situation we are in.

To confirm the rather strong condition for Lemma 7, we need the following theorem recently established by the author ([5]). Here we only state the parts that we need.

**Theorem 8** (Kim [5]). *For a (full-rank) lattice  $L \in \mathbb{R}^n$ , define  $P(L, d, H)$  to be the number of primitive rank  $d < n$  sublattices of  $L$  of determinant less than or equal to  $H$ . Also let*

$$b(n, d) = \max \left( \frac{1}{d}, \frac{1}{n-d} \right).$$

Then

$$(2) \quad P(L, d, H) = a(n, d) \frac{H^n}{(\det L)^d} + O \left( \sum_{\substack{\gamma \in \mathbb{Q} \\ 0 \leq \gamma \leq n-b(n, d)}} b_\gamma(L) H^\gamma \right),$$

where the implied constant depends only on  $n$  and  $d$ , the sum on the right is finite, and every  $b_\gamma$  is a reciprocal of a product of the successive minima of  $L$ , so that the right-hand side of (2) is invariant under rescaling  $L$  to  $\alpha L$  and  $H$  to  $\alpha^d H$ .

Furthermore, for a sublattice  $S \subseteq L$  of rank  $\leq n - d$ , define  $P_S(L, d, H)$  to be the number of primitive rank  $d$  sublattices of  $L$  of determinant  $\leq H$  that intersect trivially with  $S$ . Then  $P_S(L, d, H)$  also satisfies the estimate (2); in particular, the error term is independent of  $S$ . The sublattices that do intersect  $S$  contribute at most  $O(\sum_{\gamma \leq n-1} b_\gamma H^\gamma)$ .

For a  $d \times n$  matrix  $A = (a_{ij})_{d \times n}$  and  $c \in \{1, \dots, n\}$ , write  $A^{(c)} = (a_{ij})_{d \times (c-1)}$  for the “first”  $d \times (c-1)$  submatrix of  $A$ . We also define  $\det A = (\det A A^T)^{1/2}$ . As with  $L$ , let us use the same letter  $A$  to refer to the rank  $d$  lattice generated by the row vectors of  $A$ . With this convention, the definition of  $\det A$  just given for the matrix  $A$  is consistent with the definition of  $\det A$  for  $A \in \text{Gr}(L, d)$  in the introduction. For  $A \in \text{Gr}(L, d)$ , we also sometimes write  $\det_L A$  when the extra clarification might be helpful.

**Proposition 9.** *We continue with the notations of the preceding discussion. In addition, choose a basis  $\{v_1, \dots, v_n\}$  of  $L \in X_n$ , and also write  $L$  for the matrix whose  $i$ -th row is  $v_i$ . Let  $A$  be an integral  $d \times n$  matrix,  $c \in \{d+1, \dots, n\}$ , and let  $\bar{L}^{(c)}$  be the  $(c-1) \times n$  matrix whose  $i$ -th row vector  $\bar{v}_i$  is the projection of  $v_i$  onto  $\text{span}\{v_c, \dots, v_n\}^\perp$ . Then, provided  $\det A^{(c)} \neq 0$ ,  $\det AL \geq \det A^{(c)} \bar{L}^{(c)}$ .*

*Proof.* We first present the proof for the case  $c = n$ . Write  $A = (A^{(n)}; a)$ , with  $a = (a_{1n}, \dots, a_{dn})^T$ . Similarly, write

$$L = \begin{pmatrix} 1 & & \mu_1 \\ & \ddots & \vdots \\ & & 1 & \mu_{n-1} \\ & & & 1 \end{pmatrix} \cdot \begin{pmatrix} \bar{L}^{(n)} \\ v_n \end{pmatrix}$$

for some  $\mu_1, \dots, \mu_{n-1} \in \mathbb{R}$ . Write  $\mu = (\mu_1, \dots, \mu_{n-1})^T$ . Then

$$AL = A^{(n)} \bar{L}^{(n)} + (A^{(n)} \mu + a) v_n.$$

Temporarily write  $\mathcal{A} = A^{(n)} \bar{L}^{(n)}$ ,  $\mathcal{B} = (A^{(n)} \mu + a) v_n$ . Then

$$(AL)(AL)^T = (\mathcal{A} + \mathcal{B})(\mathcal{A}^T + \mathcal{B}^T) = \mathcal{A}\mathcal{A}^T + \mathcal{B}\mathcal{B}^T,$$

because  $\mathcal{A}\mathcal{B}^T = \mathcal{B}\mathcal{A}^T = 0$ . Also observe that

$$\mathcal{B}\mathcal{B}^T = \|v_n\|^2 (A^{(n)} \mu + a)(A^{(n)} \mu + a)^T.$$

The matrix-determinant lemma now gives

$$(\det AL)^2 = (\det \mathcal{A})^2 (1 + \|v_n\|^2 (A^{(n)} \mu + a)^T (\mathcal{A}\mathcal{A}^T)^{-1} (A^{(n)} \mu + a)) \geq (\det \mathcal{A})^2,$$

which yields the desired conclusion.

To prove the  $c = n - 1$  case, for example, observe that we can write

$$\bar{L}^{(n)} = \begin{pmatrix} 1 & & \mu'_1 \\ & \ddots & \vdots \\ & & 1 & \mu'_{n-2} \\ & & & 1 \end{pmatrix} \cdot \begin{pmatrix} \bar{L}^{(n-1)} \\ \bar{v}_{n-1} \end{pmatrix}$$

for some  $\mu'_1, \dots, \mu'_{n-2} \in \mathbb{R}$ , where  $\bar{v}_{n-1}$  is the last row of  $\bar{L}^{(n)}$ . By repeating the argument above, we obtain  $\det A^{(n)} \bar{L}^{(n)} \geq \det A^{(n-1)} \bar{L}^{(n-1)}$ . The remaining cases follow by further repetitions.  $\square$

### 3. PROOF OF THEOREM 3

Recall that we wish to evaluate the integral

$$(3) \quad \int_{X_n} \sum_{A_1 \in \text{Gr}(L, d_1)} \cdots \sum_{\substack{A_k \in \text{Gr}(L, d_k) \\ A_1, \dots, A_k \text{ independent}}} f_{H_1}(A_1) \cdots f_{H_k}(A_k) d\mu_n(L),$$

where we have  $d_1 + \dots + d_k := d < n$ . The plan is to instead estimate the sum

$$(4) \quad \frac{1}{|\mathcal{M}_p|} \sum_{M \in \mathcal{M}_p} \sum_{A_1 \in \text{Gr}(\mathbb{Z}^n, d_1)} \cdots \sum_{\substack{A_k \in \text{Gr}(\mathbb{Z}^n, d_k) \\ A_1, \dots, A_k \text{ independent}}} f_{p^{d_1/n} H_1}(A_1 ML) \cdots f_{p^{d_k/n} H_k}(A_k ML)$$

for a fixed  $L \in X_n$  in the  $p$  limit, and then use Lemma 7 to prove Theorem 3. More precisely, we rewrite (4) as

$$\frac{1}{|\mathcal{M}_p|} \sum_{c=1}^n \sum_{M \in \mathcal{M}_p^{(c)}} \sum_{\substack{A_1 \in \text{Gr}(\mathbb{Z}^n, d_1) \\ A_1, \dots, A_k \text{ independent}}} \cdots \sum_{A_k \in \text{Gr}(\mathbb{Z}^n, d_k)} f_{p^{d_1/n} H_1}(A_1 ML) \cdots f_{p^{d_k/n} H_k}(A_k ML),$$

and study the inner sum for each  $c$ , to show that this approaches  $\prod_{i=1}^k a(n, d_i) H_i^n$  as  $p \rightarrow \infty$ . This is independent of  $L$ , and hence Lemma 7 applies.

Throughout this section, we fix a representative of  $L$  in  $\text{SL}(n, \mathbb{R})$ , also denoted by  $L$ . It will also be helpful for us to identify each  $A_l \in \text{Gr}(\mathbb{Z}^n, d_l)$  with a choice of its matrix representative, e.g. its Hermite normal form (HNF), for explicit computations. Let  $c \in \{1, \dots, n\}$ , and

$$M = \begin{pmatrix} 1 & & x_1 \\ & \ddots & \vdots \\ & & 1 & x_{c-1} \\ & & & p \\ & & & & 1 \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix} \in \mathcal{M}_p^{(c)}.$$

If we write  $A_l = (a_{ij}^l)_{d_l \times n}$  as a matrix, then for each  $l$

$$A_l ML = \begin{pmatrix} a_{11}^l & a_{12}^l & \cdots & \sum_{j=1}^{c-1} a_{1j}^l x_j + p a_{1c}^l & \cdots & a_{1n}^l \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{d_l 1}^l & a_{d_l 2}^l & \cdots & \sum_{j=1}^{c-1} a_{d_l j}^l x_j + p a_{d_l c}^l & \cdots & a_{d_l n}^l \end{pmatrix} L.$$



Denote by  $A_l^{(c)} = (a_{ij}^l)_{d_l \times (c-1)}$  the first  $d_l \times (c-1)$  submatrix of  $A_l$ , and write

$$A = (a_{ij})_{d \times n} = \begin{pmatrix} A_1 \\ \vdots \\ A_k \end{pmatrix}, A^{(c)} = (a_{ij})_{d \times (c-1)} = \begin{pmatrix} A_1^{(c)} \\ \vdots \\ A_k^{(c)} \end{pmatrix},$$

which are  $d \times n$  and  $d \times (c-1)$  matrices, respectively.

**3.1. The main term.** The main term of (4) comes from the terms with  $c = n$ , namely

$$(5) \quad \frac{1}{|\mathcal{M}_p|} \sum_{M \in \mathcal{M}_p^{(n)}} \sum_{\substack{A_1 \in \text{Gr}(\mathbb{Z}^n, d_1) \\ A_1, \dots, A_k \text{ independent}}} \dots \sum_{A_k \in \text{Gr}(\mathbb{Z}^n, d_k)} f_{p^{d_1/n} H_1}(A_1 ML) \dots f_{p^{d_k/n} H_k}(A_k ML).$$

Consider the map  $A^{(n)} : \mathbb{F}_p^{n-1} \rightarrow \mathbb{F}_p^d$  induced by the matrix  $A^{(n)}$  as above. We claim that the contribution to the above sum from the  $A_l$ 's for which  $A^{(n)}$  is not surjective is negligible. There are two cases:

(i)  $\det A^{(n)} \geq p$  over  $\mathbb{Q}$ . Then

$$p \leq \det A^{(n)} \leq \prod_{l=1}^k \det A_l^{(n)},$$

so there exists an  $l$  such that  $\det A_l^{(n)} \geq p^{d_l/n+1/nk}$ , and hence  $\det A_l^{(n)} \bar{L} \gg_L p^{d_l/n+1/nk}$ , where  $\bar{L}$  here is  $\bar{L}^{(n)}$  in the statement of Proposition 9. Proposition 9 implies  $\det A_l ML \gg_L p^{d_l/n+1/nk}$ . For  $p$  sufficiently large, this is greater than  $p^{d_l/n} H_l$ , and so does not contribute to the sum.

(ii)  $\det A^{(n)} = 0$  over  $\mathbb{Q}$ . Row-reduce  $A$  so that the last row equals  $(0, \dots, 0, C)$  with  $C \neq 0$  — possible by assumption  $\text{rk } A = d$  — which shows that  $\det AM \geq p$ . This again implies  $\det A_l ML \gg_L p^{d_l/n+1/nk}$  for some  $l$ .

Now if  $A^{(n)}$  did induce a surjective map onto  $\mathbb{F}_p^d$ , then the vectors

$$\left( \sum_{j=1}^{n-1} a_{1j} x_j, \dots, \sum_{j=1}^{n-1} a_{dj} x_j \right)$$

are equidistributed mod  $p$ . Therefore computing (5) is equivalent to computing

$$\frac{p^{n-1}}{p^d |\mathcal{M}_p|} \sum_{\substack{A_1 \in \text{Gr}(\mathbb{Z}^n, d_1) \\ \text{rk}_p A^{(n)} = d}} \dots \sum_{A_k \in \text{Gr}(\mathbb{Z}^n, d_k)} f_{p^{d_1/n} H_1}(A_1 L) \dots f_{p^{d_k/n} H_k}(A_k L)$$

(here  $\text{rk}_p$  means the rank modulo  $p$ ). This is equal to

$$(6) \quad \frac{p^{n-1}}{p^d |\mathcal{M}_p|} \sum_{\substack{A_1 \in \text{Gr}(\mathbb{Z}^n, d_1) \\ \text{rk } A^{(n)} = d}} \dots \sum_{A_k \in \text{Gr}(\mathbb{Z}^n, d_k)} f_{p^{d_1/n} H_1}(A_1 L) \dots f_{p^{d_k/n} H_k}(A_k L)$$

because  $\text{rk}_p A^{(n)} = d \Leftrightarrow \text{rk } A^{(n)} = d$  and  $p \nmid \det A^{(n)}$ , and we already showed that if  $p \mid \det A^{(n)}$  the corresponding sets of  $A_l$ 's do not contribute to the sum.

The summation in (6) requires that  $A_k$  is independent of  $A_1, \dots, A_{k-1}$  and  $(0, \dots, 0, 1)$ , since otherwise,  $A_1 \oplus \dots \oplus A_k$  contains a nonzero multiple of  $(0, \dots, 0, 1)$ , which implies

$\text{rk } A^{(n)} < d$ . Thus, by applying Theorem 8 with  $S = A_1 \oplus \dots \oplus A_{k-1} \oplus \text{span}_{\mathbb{Z}}\{(0, \dots, 0, 1)\}$ , we can rewrite (6) as

$$\frac{p^{n-1}}{p^d |\mathcal{M}_p|} \left( a(n, d_k) H_k^n p^{d_k} + o_L(H_k^n p^{d_k}) \right) \cdot \sum_{\substack{A_1 \in \text{Gr}(\mathbb{Z}^n, d_1) \\ \vdots \\ A_{k-1} \in \text{Gr}(\mathbb{Z}^n, d_{k-1}) \\ \text{rk } A^{(n)} = d - d_k}} \dots \sum_{A_{k-1} \in \text{Gr}(\mathbb{Z}^n, d_{k-1})} f_{p^{d_1/n} H_1}(A_1 L) \dots f_{p^{d_{k-1}/n} H_{k-1}}(A_{k-1} L),$$

where  $A^{(n)}$  here now means

$$A^{(n)} = \begin{pmatrix} A_1^{(n)} \\ \vdots \\ A_{k-1}^{(n)} \end{pmatrix}.$$

Repeating the same argument with other  $A_i$ 's, we find that (6) equals

$$\frac{p^{n-1}}{|\mathcal{M}_p|} \left( \prod_{i=1}^k a(n, d_i) H_i^n + o_{L, H_1, \dots, H_k}(1) \right).$$

Recalling  $|\mathcal{M}_p| = \sum_{i=0}^{n-1} p^i$ , and taking  $p \rightarrow \infty$ , this gives the intended main term  $\prod_{i=1}^k a(n, d_i) H_i^n$  for (4).

**3.2. Error terms, part 1.** In the rest of this section, we show that, for  $c \in \{1, \dots, n-1\}$ ,

$$(7) \quad \frac{1}{|\mathcal{M}_p|} \sum_{M \in \mathcal{M}_p^{(c)}} \sum_{\substack{A_1 \in \text{Gr}(\mathbb{Z}^n, d_1) \\ \vdots \\ A_k \in \text{Gr}(\mathbb{Z}^n, d_k) \\ A_1, \dots, A_k \text{ independent}}} \dots \sum_{A_k \in \text{Gr}(\mathbb{Z}^n, d_k)} f_{p^{d_1/n} H_1}(A_1 M L) \dots f_{p^{d_k/n} H_k}(A_k M L)$$

vanishes as  $p \rightarrow \infty$ . This will complete the proof of Theorem 3.

We first assume  $c > d$ , and consider the contributions from those  $A_1, \dots, A_k$  such that  $\text{rk}_p A^{(c)} = d$ . By a similar argument to the  $c = n$  case, the surjection of the linear map  $A^{(c)} : \mathbb{F}_p^{c-1} \rightarrow \mathbb{F}_p^d$  implies that their contributions amount to

$$\frac{p^{c-1}}{p^d |\mathcal{M}_p|} \sum_{A_1 \in \text{Gr}(\mathbb{Z}^n, d_1)} \dots \sum_{\substack{A_k \in \text{Gr}(\mathbb{Z}^n, d_k) \\ \text{rk}_p A^{(c)} = d}} f_{p^{d_1/n} H_1}(A_1 L) \dots f_{p^{d_k/n} H_k}(A_k L).$$

We simply drop the rank condition and bound this by

$$\frac{p^{c-1}}{|\mathcal{M}_p|} \left( \prod_{i=1}^k a(n, d_i) H_i^n + o_{L, H_1, \dots, H_k}(1) \right),$$

which clearly vanishes as  $p \rightarrow \infty$ .

Continue with the assumption  $c > d$ , but this time suppose  $\text{rk}_p A^{(c)} < d$ . If  $\det A^{(c)} \geq p$  (over  $\mathbb{Q}$ ), then we can argue exactly as in (i) in Section 3.1 above and show it does not contribute to (7). The case  $\det A^{(c)} = 0$  will be handled below.

**3.3. Error terms, part 2.** We now assume that either  $c > d$  and  $\det A^{(c)} = 0$ , or  $c \leq d$ , in which case  $\det A^{(c)} = 0$  necessarily. Write  $\text{rk}_p A^{(c)} = c' < \min(c, d)$ . We claim that we may assume  $\text{rk } A^{(c)} = c'$  as well. If not, then  $\text{rk } A^{(c)} > \text{rk}_p A^{(c)}$ , and thus the HNF of  $A^{(c)}$  has a leading coefficient (also called a pivot) that is a nonzero multiple of  $p$ . But this implies that  $\det A \geq p$  by the Cauchy-Binet formula, and we can again argue as in (i) in Section 3.1 to show that this  $A$  contributes zero to (7).

Suppose in addition that  $\text{rk } A^{(c+1)} = c' + 1$ . Then the HNF of  $A$  has a pivot in column  $c$ , and it follows that the HNF of  $AM$  has a pivot in column  $c$  that is a multiple of  $p$ . This implies  $\det AM \geq p$ , and again we argue as in (i) in Section 3.1.

Summarizing our argument so far, it remains to consider the case in which  $\det A^{(c)} = 0$ , and  $\text{rk}_p A^{(c)} = \text{rk } A^{(c)} = \text{rk } A^{(c+1)} = c' < \min(c, d)$ . For integers  $1 \leq r_1 < r_2 < \dots < r_{c'} \leq d$ , let  $r = (r_1, \dots, r_{c'})$ , and for a matrix  $B$  with  $d$  rows, denote by  $B|_r$  the matrix with  $c'$  rows whose  $i$ -th row is the  $r_i$ -th row of  $B$ . For each  $r$ , let us restrict (7) to those  $A$  for which the rows of  $A^{(c)}|_r$  are linearly independent. Thus, we are considering the following restriction of (7):

$$\frac{1}{|\mathcal{M}_p|} \sum_{M \in \mathcal{M}_p^{(c)}} \sum_{\substack{A_1 \in \text{Gr}(\mathbb{Z}^n, d_1) \\ \text{rk } A = d, \text{rk } A^{(c)}|_r = \text{rk}_p A^{(c)} = \text{rk } A^{(c)} = \text{rk } A^{(c+1)} = c'}} \dots \sum_{A_k \in \text{Gr}(\mathbb{Z}^n, d_k)} f_{p^{d_1/n} H_1}(A_1 ML) \dots f_{p^{d_k/n} H_k}(A_k ML).$$

For each  $A$  appearing in this sum, there exists a rational  $d \times c'$  matrix  $R$  such that  $A^{(c)} = RA^{(c)}|_r$ . Due to the rank condition  $\text{rk } A^{(c)} = \text{rk } A^{(c+1)}$ , we also must have  $A^{(c+1)} = RA^{(c+1)}|_r$ . In other words,  $R$  and  $A^{(c+1)}|_r$  determine  $A^{(c+1)}$  under our current assumptions. With this understanding, we can rewrite the above sum as

$$\frac{1}{|\mathcal{M}_p|} \sum_R \sum_{M \in \mathcal{M}_p^{(c)}} \sum_{\substack{A_1 \in \text{Gr}(\mathbb{Z}^n, d_1) \\ \text{rk } A = d, A^{(c)} = RA^{(c)}|_r, \\ \text{rk } A^{(c)}|_r = \text{rk}_p A^{(c)} = \text{rk } A^{(c)} = \text{rk } A^{(c+1)} = c'}} \dots \sum_{A_k \in \text{Gr}(\mathbb{Z}^n, d_k)} f_{p^{d_1/n} H_1}(A_1 ML) \dots f_{p^{d_k/n} H_k}(A_k ML),$$

where the sum over  $R$  is over all  $d \times c'$  matrices such that the inner sum is nontrivial. Similarly to the argument in Section 3.1, for each  $A$  appearing in the sum, as  $M$  ranges over  $\mathcal{M}_p^{(c)}$ , the  $c$ -th column of  $A|_r M$

$$\left( \sum_{j=1}^{c-1} a_{r_1 j} x_j + p a_{r_1 c}, \dots, \sum_{j=1}^{c-1} a_{r_{c'} j} x_j + p a_{r_{c'} c} \right)^T$$

becomes equidistributed mod  $p$ . Also, multiplying by  $M$  from the right keeps all the rank conditions invariant. Thus the above sum becomes

$$\begin{aligned} & \frac{p^{c-1}}{p^{c'} |\mathcal{M}_p|} \sum_R \sum_{\substack{A_1 \in \text{Gr}(\mathbb{Z}^n, d_1) \\ \text{rk } A = d, A^{(c)} = RA^{(c)}|_r, \\ \text{rk } A^{(c)}|_r = \text{rk}_p A^{(c)} = \text{rk } A^{(c)} = \text{rk } A^{(c+1)} = c'}} \dots \sum_{A_k \in \text{Gr}(\mathbb{Z}^n, d_k)} f_{p^{d_1/n} H_1}(A_1 L) \dots f_{p^{d_k/n} H_k}(A_k L) \\ (8) \quad & = \frac{p^{c-1}}{p^{c'} |\mathcal{M}_p|} \sum_{\substack{A_1 \in \text{Gr}(\mathbb{Z}^n, d_1) \\ \text{rk } A = d, \text{rk } A^{(c)}|_r = \text{rk } A^{(c)} = \text{rk } A^{(c+1)} = c'}} \dots \sum_{A_k \in \text{Gr}(\mathbb{Z}^n, d_k)} f_{p^{d_1/n} H_1}(A_1 L) \dots f_{p^{d_k/n} H_k}(A_k L). \end{aligned}$$

It remains to estimate this sum (8). By dropping the rank conditions and applying Theorem 8, (8) is at most

$$\frac{p^{c-c'+d-1}}{|\mathcal{M}_p|} \left( \prod_{i=1}^k a(n, d_i) H_i^n + o_{L, H_1, \dots, H_k}(1) \right),$$

which approaches 0 as  $p \rightarrow \infty$  provided  $n - c > d - c'$  (note that  $n - c \geq d - c'$  always). If  $n - c = d - c'$ , note that the HNF of  $A$  is of the form

$$\begin{pmatrix} P & * \\ 0 & Q \end{pmatrix},$$

where  $P$  is a  $c' \times c$  matrix, and  $Q$  is a  $(d - c') \times (n - c)$  matrix, where  $P$  and  $Q$  are themselves HNFs and must be of full rank. Now since  $n - c = d - c'$  by assumption,  $Q$  is a square matrix, and therefore  $Q$  must be an upper triangular matrix with no nonzero diagonal entries. This implies that  $A_1 \oplus \dots \oplus A_k$  intersects nontrivially with  $\text{span}_{\mathbb{Z}}\{(0, \dots, 0, 1)\}$ . Therefore, one of the  $A_l$ 's intersects nontrivially with the lattice  $S_l := A_1 \oplus \dots \oplus \hat{A}_l \oplus \dots \oplus A_k \oplus \text{span}_{\mathbb{Z}}\{(0, \dots, 0, 1)\}$  — where  $\hat{A}_l$  here indicates that  $A_l$  does *not* appear in the sum — of dimension at most  $d - d_l + 1$ . But Theorem 8 implies

$$\sum_{\substack{A_l \in \text{Gr}(\mathbb{Z}^n, d_l) \\ A_l \cap S_l \neq \emptyset}} f_{p^{d_l/n} H_l}(A_l L) = o_{L, H_1, \dots, H_k}(p^{d_l}),$$

which implies that (8) is bounded by

$$o_{L, H_1, \dots, H_k} \left( \frac{p^{c - c' + d - 1}}{|\mathcal{M}_p|} \right) = o_{L, H_1, \dots, H_k}(1),$$

as desired.

#### 4. THE CASE OF PARTIALLY OVERLAPPING SUBLATTICES

In this section we prove Theorem 4. Recall that we are considering the integral

$$(9) \quad \int_{X_n} \sum_{A \in \text{Gr}(L, d_1)} \sum_{\substack{B \in \text{Gr}(L, d_2) \\ \text{rk } A \cap B = r}} f_{H_1}(A) f_{H_2}(B) d\mu_n(L)$$

for  $1 \leq r < d_1, d_2$ , so that  $d_1 + d_2 < n + r$ .

Let  $L \in X_n$ . For a primitive sublattice  $C \subseteq L$  of rank  $r < n$ , we identify the quotient lattice  $L/C$  with the projection of  $L$  onto the  $n - r$ -dimensional subspace of  $\mathbb{R}^n$  orthogonal to  $C$ , and assign the metric induced by this projection from the metric on  $L$ . If  $A \in \text{Gr}(L, d)$  satisfies  $C \subseteq A$ , then it is easy to see that  $A/C \in \text{Gr}(L/C, d - r)$ , and that it satisfies

$$\det_L(A) = \det_L(C) \det_{L/C}(A/C).$$

Using this relation, we rewrite the inner sum of (9) as

$$\sum_{C \in \text{Gr}(L, r)} \sum_{\substack{\bar{A} \in \text{Gr}(L/C, d_1 - r) \\ \bar{B} \in \text{Gr}(L/C, d_2 - r) \\ \text{indep}}} f_{H_1/\det_L C}(\bar{A}) f_{H_2/\det_L C}(\bar{B}).$$

We will interpret this expression as a pseudo-Eisenstein series, i.e. a function on  $X_n$  of form  $\sum_{\gamma \in P \cap \Gamma \backslash \Gamma} f(\gamma L)$  where  $\Gamma = \text{SL}(n, \mathbb{Z})$  and  $P$  is a parabolic subgroup of  $\text{SL}(n, \mathbb{R})$ , and then use the unfolding trick. Fix a representative of  $L \in X_n$  in  $\text{SL}(n, \mathbb{R})$ , again denoted by  $L$ . In this context, a choice of  $C \in \text{Gr}(L, r)$  corresponds to two choices of  $\gamma \in P(n - r, r, \mathbb{Z}) \backslash \text{SL}(n, \mathbb{Z})$ , where

$$P(a, b, F) = \left\{ \begin{pmatrix} G_a & * \\ & G_b \end{pmatrix} : G_a \in \text{SL}(a, F), G_b \in \text{SL}(b, F) \right\}$$

for any ring  $F$ .  $C$  and  $\gamma$  are related by  $C = (\text{sublattice generated by last } r \text{ rows of } \gamma L)$ , and this correspondence is one-to-two due to the two possible orientations for the last  $r$  rows of  $\gamma L$ .

Next, fixing a representative of  $\gamma$ , we can uniquely decompose  $\gamma L$  in the form

$$(10) \quad \begin{pmatrix} G_{n-r} & U \\ & G_r \end{pmatrix} \begin{pmatrix} \alpha^{-\frac{1}{n-r}} I_{n-r} & \\ & \alpha^{\frac{1}{r}} I_r \end{pmatrix} K',$$

for some  $G_{n-r} \in \text{SL}(n-r, \mathbb{R})$ ,  $G_r \in \text{SL}(r, \mathbb{R})$ ,  $U \in \text{Mat}_{(n-r) \times r}(\mathbb{R})$ , and  $K'$  an element of a fundamental domain of  $(\text{SO}(n-r, \mathbb{R}) \times \text{SO}(r, \mathbb{R})) \backslash \text{SO}(n, \mathbb{R})$ , which we fix in advance. In this context, a choice of an independent pair  $\bar{A} \in \text{Gr}(L/C, d_1-r)$  and  $\bar{B} \in \text{Gr}(L/C, d_2-r)$  corresponds to four choices — again due to the four possibilities for the orientations — of  $\delta \in P'(n-d_1-d_2+r, d_2-r, d_1-r, \mathbb{Z}) \backslash \text{SL}(n-r, \mathbb{Z})$ , where

$$P'(a, b, c, F) = \left\{ \begin{pmatrix} G_a & * & * \\ & G_b & 0 \\ & & G_c \end{pmatrix} : G_a \in \text{SL}(a, F), G_b \in \text{SL}(b, F), G_c \in \text{SL}(c, F) \right\}$$

for any ring  $F$ . Indeed,  $\bar{A}$  is the sublattice generated by the last  $d_1-r$  rows of

$$(11) \quad \delta \cdot G_{n-r} \cdot \alpha^{-\frac{1}{n-r}} I_{n-r} \cdot (\text{first } n-r \text{ rows of } K');$$

this expression is independent of  $U$  because  $\bar{A}$  is orthogonal to  $C$ , and equivalently also to the last  $r$  rows of  $K'$ . Similarly,  $\bar{B}$  is the sublattice generated by the next last  $d_2-r$  rows of (11). But since we are only interested in the determinants of  $\bar{A}$  and  $\bar{B}$ , in what follows we can regard them as the sublattices generated by the corresponding rows of  $\delta \cdot \alpha^{-\frac{1}{n-r}} G_{n-r}$ .

The considerations so far allows us to rewrite (9) as

$$\frac{1}{8} \int_{P(n-r, r, \mathbb{Z}) \backslash \text{SL}(n, \mathbb{R})} \sum_{\delta} f_{H_1/\alpha}(\bar{A}) f_{H_2/\alpha}(\bar{B}) d\mu_n,$$

where  $\delta$  is summed over  $P'(n-d_1-d_2+r, d_2-r, d_1-r, \mathbb{Z}) \backslash \text{SL}(n-r, \mathbb{Z})$ .

Lemma 10 below, which gives a decomposition of  $d\mu_n$  compatible with (10), implies that this equals

$$(\text{const}) \int_0^\infty \int_{X_{n-r}} \sum_{\substack{\bar{A} \in \text{Gr}(\alpha^{-\frac{1}{n-r}} G_{n-r}, d_1-r) \\ \bar{B} \in \text{Gr}(\alpha^{-\frac{1}{n-r}} G_{n-r}, d_2-r) \\ \text{indep}}} f_{H_1/\alpha}(\bar{A}) f_{H_2/\alpha}(\bar{B}) d\mu_{n-r}(G_{n-r}) \cdot \alpha^{n-1} d\alpha,$$

which, by Theorem 3 (notice that  $\det \alpha^{-\frac{1}{n-r}} G_{n-r} = \alpha^{-1}$ , so we normalize accordingly), equals

$$(\text{const}) \int_0^\infty H_1^{n-r} H_2^{n-r} \alpha^{-n+d_1+d_2-1} d\alpha,$$

which is divergent, proving Theorem 4. One way to understand this phenomenon is that, if  $L \in X_n$  is heavily skewed i.e. its successive minima have a huge gap, there may exist too many possibilities for  $C = A \cap B$ . Indeed, if we additionally required that  $\alpha = \det C \geq 1$ , say, then we would have instead obtained

$$(\text{const}) \int_1^\infty H_1^{n-r} H_2^{n-r} \alpha^{-n+d_1+d_2-1} d\alpha,$$

which converges, at least when  $d_1 + d_2 < n$ .

Before we prove the needed lemma, we fix our notations related to  $d\mu_n$ . Recall the standard fact (see e.g. [6]) that, with respect to the  $NAK$  decomposition of  $\mathrm{SL}(n, \mathbb{R})$ , we can write  $d\mu_n$  as

$$d\mu_n = \tau(n) dN \cdot dA \cdot dK,$$

where  $\tau(n)$  is some constant,  $dN = \prod_{i < j} dn_{ij}$ ,  $dA = \prod_i \alpha_i^{-i(n-i)} d\alpha_i / \alpha_i$  upon writing  $A = \mathrm{diag}(a_1, \dots, a_n)$  and  $\alpha_i = a_i / a_{i+1}$ , and  $dK$  is the Haar measure on  $\mathrm{SO}(n, \mathbb{R})$  so that

$$\int_{\mathrm{SO}(n, \mathbb{R})} dK = \prod_{i=2}^n iV(i).$$

To make  $\int_{X_n} d\mu_n = 1$ , we set

$$\tau(n) = \frac{1}{n} \prod_{i=2}^n \zeta^{-1}(i).$$

**Lemma 10.** *With respect to the decomposition (10) of  $\mathrm{SL}(n, \mathbb{R})$ , we have*

$$d\mu_n = \frac{n}{r(n-r)} \cdot \frac{\tau(n)}{\tau(r)\tau(n-r)} dU d\mu_r(G_r) d\mu_{n-r}(G_{n-r}) \alpha^{n-1} d\alpha dK',$$

where  $dU = \prod_{\substack{1 \leq i \leq n-r \\ 1 \leq j \leq r}} du_{ij}$  on writing  $U = (u_{ij})_{\substack{1 \leq i \leq n-r \\ 1 \leq j \leq r}}$ , and  $dK'$  is the natural measure on  $(\mathrm{SO}(n-r, \mathbb{R}) \times \mathrm{SO}(r, \mathbb{R})) \backslash \mathrm{SO}(n, \mathbb{R})$  descended from the measure  $dK$  on  $\mathrm{SO}(n, \mathbb{R})$ .

*Proof.* The only nontrivial part of the proof consists of comparing the diagonal parts, or the “ $A$  parts”, of the measures  $d\mu_n, d\mu_{n-r}, d\mu_r$ . We can decompose

$$\begin{pmatrix} a_1 & & & & \\ & \ddots & & & \\ & & a_{n-r} & & \\ & & & \ddots & \\ & & & & a_r \end{pmatrix} = \begin{pmatrix} b'_1 & & & & \\ & \ddots & & & \\ & & b'_{n-r} & & \\ & & & b''_1 & \\ & & & & \ddots \\ & & & & & b''_r \end{pmatrix} \begin{pmatrix} \alpha^{\frac{-1}{n-r}} & & & & \\ & \ddots & & & \\ & & \alpha^{\frac{-1}{n-r}} & & \\ & & & \alpha^{\frac{1}{r}} & \\ & & & & \ddots \\ & & & & & \alpha^{\frac{1}{r}} \end{pmatrix},$$

where there is the relation  $\prod a_i = \prod b'_i = \prod b''_i = 1$  among the entries. Write  $\alpha_i = a_i / a_{i+1}, \beta'_i = b'_i / b'_{i+1}, \beta''_i = b''_i / b''_{i+1}$ . Then the measures on the “ $A$  parts” of the groups  $G_n, G_{n-r}, G_r$  are, respectively,

$$dA := \prod_i \alpha_i^{-i(n-i)} \frac{d\alpha_i}{\alpha_i}, dB' = \prod_i \beta'_i{}^{-i(n-r-i)} \frac{d\beta'_i}{\beta'_i}, dB'' = \prod_i \beta''_i{}^{-i(r-i)} \frac{d\beta''_i}{\beta''_i}.$$

It remains to perform the change of coordinates from the  $\alpha_i$ -coordinates to the  $\beta'_i, \beta''_i, \alpha$ -coordinates. We have  $\alpha_i = \beta'_i$  for  $1 \leq i \leq n-r-1$  and  $\alpha_{n-r+i} = \beta''_i$  for  $1 \leq i \leq r-1$ , and the single nontrivial relation

$$\alpha_{n-r} = \frac{b'_{n-r}}{b''_1} \alpha^{-\frac{n}{r(n-r)}}.$$

At this point, we can compute and find that

$$(12) \quad dA = dB' dB'' \cdot \prod_{i=1}^{n-r-1} \beta'_i{}^{-r-i} \prod_{i=1}^{r-1} \beta''_i{}^{-(n-r)(r-i)} \cdot \alpha_{n-r}^{-r(n-r)} \frac{d\alpha_{n-r}}{\alpha_{n-r}}.$$

On the other hand, from the shape of the Jacobian matrix

$$\begin{pmatrix} - & \frac{\partial \alpha_i}{\partial \beta'_1} & - \\ & \vdots & \\ - & \frac{\partial \alpha_i}{\partial \alpha} & - \\ & \frac{\partial \alpha_i}{\partial \beta''_1} & \\ - & \vdots & - \end{pmatrix} = \begin{pmatrix} 1 & & * \\ & \ddots & \vdots \\ & & 1 & * \\ & & \frac{\partial \alpha_{n-r}}{\partial \alpha} & \\ & & * & 1 & \ddots \\ & & \vdots & & \\ & & * & & 1 \end{pmatrix}$$

and the fact that

$$\frac{\partial \alpha_{n-r}}{\partial \alpha} = -\frac{n}{r(n-r)} \alpha_{n-r} \alpha^{-1},$$

we have

$$-\frac{d\alpha_{n-r}}{\alpha_{n-r}} = \frac{n}{r(n-r)} \frac{d\alpha}{\alpha} + (\text{terms in } d\beta' \text{ and } d\beta''),$$

and the  $d\beta'$  and  $d\beta''$  parts here do not affect the outcome of the computation. Thus we can pretend that we have

$$\begin{aligned} & \alpha_{n-r}^{-r(n-r)} \frac{d\alpha_{n-r}}{\alpha_{n-r}} \\ &= \frac{-n}{r(n-r)} \left( \frac{b'_{n-r}}{b''_1} \alpha^{-\frac{n}{r(n-r)}} \right)^{-r(n-r)} \frac{d\alpha}{\alpha} \\ &= \frac{-n}{r(n-r)} \frac{\prod_{i=1}^{n-r-1} \beta_i^{r_i}}{\prod_{i=1}^{r-1} \beta_i^{r-(n-r)(r-i)}} \alpha^n \frac{d\alpha}{\alpha}. \end{aligned}$$

Substituting this into (12), we obtain

$$dA = \frac{-n}{r(n-r)} dB' dB'' \alpha^n \frac{d\alpha}{\alpha},$$

which completes the proof. By reorienting  $\alpha$  (which moves in the opposite direction to  $\alpha_{n-r}$ ) we can eliminate the negative sign.  $\square$

## 5. AVERAGE NUMBER OF FLAGS

The same technique as in the previous section can be applied to compute the  $\mu_n$ -average number of flags bounded by certain constraints, even though such a formula for a fixed lattice is not known and is probably difficult to find. In this section, we compute the average number of flags such that  $\det A_i \leq H_i$  for  $i = 1, \dots, k$ , i.e. the quantity

$$\int_{X_n} \sum_{\substack{A_1 \subseteq \dots \subseteq A_k \subseteq L \\ \dim A_i = d_i}} \prod_{i=1}^k f_{H_i}(A_i) d\mu_n,$$

or equivalently

$$\int_{X_n} \sum_{A_1 \in \text{Gr}(L, d_1)} \sum_{\bar{A}_2 \in \text{Gr}(L/A_1, d_2-d_1)} \dots \sum_{\bar{A}_k \in \text{Gr}(L/A_{k-1}, d_k-d_{k-1})} f_{H_1}(A_1) f_{H_2/\det A_1}(A_2) \dots d\mu_n,$$

thereby proving Theorem 5.

First consider the case  $k = 2$ , in which we are computing

$$\int_{X^n} \sum_{A_1 \in \text{Gr}(L, d_1)} \sum_{\bar{A}_2 \in \text{Gr}(L/A_1, d_2 - d_1)} f_{H_1}(A_1) f_{H_2/\det A_1}(A_2) d\mu_n.$$

By the same argument as in the previous section, and Lemma 10, this equals

$$\frac{n}{d_1(n-d_1)} \cdot \frac{\tau(n)}{\tau(d_1)\tau(n-d_1)} \cdot \frac{1}{2} \text{vol} \left( \frac{\text{SO}(n, \mathbb{R})}{\text{SO}(n-d_1, \mathbb{R}) \times \text{SO}(d_1, \mathbb{R})} \right) \cdot \int \int_{X_{d_1}} d\mu_{d_1} \int_{X_{n-d_1}} \sum_{\bar{A}_2} f_{H_2/\alpha}(\bar{A}_2) d\mu_{n-d_1} f_{H_1}(\alpha) \alpha^{n-1} d\alpha.$$

Using the fact that  $\text{vol}(\text{SO}(n, \mathbb{R})) = \prod_{i=2}^n iV(i)$ , one finds that the product of the terms on the first line here equals  $na(n, d_1)$ . By Theorem 3, the integral part is equal to

$$\begin{aligned} & a(n-d_1, d_2-d_1) \int_0^{H_1} \alpha^{n-1} \cdot \alpha^{d_2-d_1} \left( \frac{H_2}{\alpha} \right)^{n-d_1} d\alpha \\ &= a(n-d_1, d_2-d_1) H_2^{n-d_1} \int_0^{H_1} \alpha^{d_2-1} d\alpha \\ &= \frac{a(n-d_1, d_2-d_1)}{d_2} H_1^{d_2} H_2^{n-d_1}. \end{aligned}$$

This proves the  $k = 2$  case. For general  $k$ , we proceed by induction: we have

$$\begin{aligned} & \frac{n}{d_1(n-d_1)} \cdot \frac{\tau(n)}{\tau(d_1)\tau(n-d_1)} \cdot \frac{1}{2} \text{vol} \left( \frac{\text{SO}(n, \mathbb{R})}{\text{SO}(n-d_1, \mathbb{R}) \times \text{SO}(d_1, \mathbb{R})} \right) \cdot \\ & \int \int_{X_{d_1}} d\mu_{d_1} \int_{X_{n-d_1}} \sum_{\bar{A}_2, \dots, \bar{A}_k} f_{H_2/\alpha}(\bar{A}_2) \dots f_{H_k/\det A_{k-1}\alpha}(\bar{A}_k) d\mu_{n-d_1} f_{H_1}(\alpha) \alpha^{n-1} d\alpha. \end{aligned}$$

The first line is exactly the same as in the  $k = 2$  case. As for the integral, writing  $\mathfrak{d}' = (d_2 - d_1, \dots, d_k - d_1)$ , and using the induction hypothesis, we find that it is equal to

$$\begin{aligned} & a(n-d_1, \mathfrak{d}') \int_0^{H_1} \alpha^{n-1} \cdot \alpha^{d_k-d_1} \prod_{i=2}^k \left( \frac{H_i}{\alpha} \right)^{d_{i+1}-d_{i-1}} d\alpha \\ &= a(n-d_1, \mathfrak{d}') \prod_{i=2}^k H_i^{d_{i+1}-d_{i-1}} \int_0^{H_1} \alpha^{d_2-1} d\alpha \\ &= \frac{a(n-d_1, \mathfrak{d}')}{d_2} \prod_{i=1}^k H_i^{d_{i+1}-d_{i-1}}. \end{aligned}$$

Since

$$a(n-d_1, \mathfrak{d}') = a(n-d_1, d_2-d_1) \prod_{i=2}^{k-1} \frac{n-d_{i-1}}{d_{i+1}-d_{i-1}} a(n-d_i, d_{i+1}-d_i),$$

this gives the desired result.

## REFERENCES

- [1] S. Bai, D. Stehlé, W. Wen. Measuring, simulating and exploiting the head concavity phenomenon in BKZ. *Advances in cryptology — ASIACRYPT 2018*. Part I, 369-404, Lecture Notes in Comput. Sci., 11272, Springer, Cham, 2018.
- [2] S. G. Dani and G. Margulis. Limit distribution of orbits of unipotent flows and values of quadratic forms. *Advances in Soviet Math.*, Vol 16, 1993, pp. 91-137.



- [3] J. Franke, Y. Manin, and Y. Tschinkel. Rational points of bounded height on Fano varieties. *Invent. Math.* 95 (1989), no. 2, 421-435.
- [4] S. Kim. Random lattice vectors in a set of size  $O(n)$ . *Int. Math. Res. Not.* (2020), 2020(5): 1385-1416.
- [5] S. Kim. Counting rational points of a Grassmannian. *arXiv*: 1908.01245
- [6] S. Kim and A. Venkatesh. The behavior of random reduced bases. *Int. Math. Res. Not.* (2018), 2018(20): 6442-6480.
- [7] C. A. Rogers, Mean values over the space of lattices. *Acta Math.* 94 (1955), 249-287.
- [8] W. M. Schmidt. Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height. *Duke Math. J.* 35 (1968), 327-339.
- [9] W. M. Schmidt. Masstheorie in der Geometrie der Zahlen. *Acta Math.* 102, no. 3-4 (1959): 159-224.
- [10] P. Schnorr and M. Euchner. Lattice basis reduction: improved practical algorithms and solving subset sum problems. *Math. Programming* 66 (1994), no. 2, Ser. A, 181-199.
- [11] U. Shapira and B. Weiss. A volume estimate for the set of stable lattices. *Comptes Rendus Mathématique* 352, no.11 (2014), pp.875-879.
- [12] G. Shimura. Introduction to the arithmetic theory of automorphic functions. Princeton University Press, Princeton, N.J., 1971.
- [13] C. L. Siegel. A mean value theorem in geometry of numbers. *Ann. of Math.* (2) 46, (1945). 340-347.
- [14] A. Södergren, On the Poisson distribution of lengths of lattice vectors in a random lattice. *Math. Z.* 269 (2011), 945-954.
- [15] A. Södergren and A. Strömbergsson. On the generalized circle problem for a random lattice in large dimension. *Adv. Math.* 345 (2019), 1042-1074.
- [16] J. L. Thunder. Asymptotic estimates for rational points of bounded height on flag varieties. *Compositio Math.* 88 (1993), no. 2, 155-186.
- [17] J. L. Thunder. Higher-dimensional analogs of Hermite's constant. *Michigan Mathematics Journal* 45, no. 2 (1998): 301-314.