GEOMETRY-OF-NUMBERS METHODS IN THE CUSP AND APPLICATIONS TO CLASS GROUPS

ARUL SHANKAR, ARTANE SIAD, ASHVIN A. SWAMINATHAN, ILA VARMA

Abstract. In this article, we compute the mean number of 2-torsion elements in class groups of monogenized cubic orders, when such orders are enumerated by height. In particular, we show that the average size of the 2-torsion subgroup in the class group increases when one ranges over all monogenized cubic orders instead of restricting to the family of monogenized cubic fields (or equivalently, monogenized maximal cubic orders) as determined in [8]. In addition, for each fixed odd integer $n \geq 3$, we bound the mean number of 2-torsion elements in the class groups of monogenized degree-n orders, when such orders are enumerated by height.

To obtain such results, we develop a new method for counting integral orbits having bounded invariants and satisfying congruence conditions that lie inside the *cusps* of fundamental domains for coregular representations — i.e., representations of semisimple groups for which the ring of invariants is a polynomial ring. We illustrate this method for the representation of the split orthogonal group on self-adjoint operators for the symmetric bilinear form $\sum_{i=1}^{n} x_i y_{n+1-i}$, the orbits of which naturally parametrize 2-torsion ideal classes of monogenized degree-n orders.

Contents

Date: October 18, 2021.

1. Introduction

Over the past two decades, many breakthroughs have been achieved in the field of arithmetic statistics by means of a general approach that involves arithmetic invariant theory, geometry-of-numbers techniques, averaging methods, and sieve theory. Most notably, this approach has been applied to determine asymptotics for number fields of small fixed degree (see [4, 6, 24, 28]), compute average sizes of p-class groups in certain families of number fields for small primes p (see [4, 8, 24, 29, 39, 40, 42]), calculate average n-Selmer ranks of elliptic curves and hyperelliptic Jacobians for small n (see [7, 9, 10, 11, 12, 37]), and more. The statements that have been tractable through this approach typically concern distributions of arithmetic objects that can be parametrized by *irreducible integral orbits of coregular representations*.

In certain special cases (see [1, 15]), this approach has been generalized using situation-specific techniques to study objects parametrized by *reducible* orbits. The purpose of this article is to develop a systematic method for determining asymptotics for the number of *reducible integral orbits of coregular representations*. As a first new application of this method, we bound the average 2-torsion in the class groups of monogenized orders of fixed odd degree n, computing it exactly when $n = 3$.

1.1. Main results on class group statistics.

In this paper, we study the distributions of 2-class groups of monogenized orders enumerated by height. A *monogenized order* comprises the data $(\mathcal{O}, \alpha)$ of a monogenic order $\mathcal{O} = \mathbb{Z}[\alpha]$ in a number field together with a choice of monogenizer $\alpha \in \mathcal{O}$.[1] Two monogenized orders $(\mathcal{O}, \alpha)$ and $(\mathcal{O}', \alpha')$ are declared isomorphic if there exists a ring isomorphism from $\mathcal{O}$ to $\mathcal{O}'$ taking α to $\pm\alpha' + m$ for some $m \in \mathbb{Z}$. If $(\mathcal{O}, \alpha)$ is a monogenized order, its isomorphism class contains a unique representative $(\mathcal{O}, \alpha_0)$ such that $\mathrm{Tr}(\alpha_0) \in \{0, \dots, n-1\}$. Letting $F(x, z) = x^n + \sum_{i=2}^{n} f_i x^{n-i} z^i$ be the binary form such that $F(x, 1)$ is the minimal polynomial of α_0, we define the *height* of (the isomorphism class of) the monogenized order $(\mathcal{O}, \alpha)$ to be

$$\mathrm{H}(\mathcal{O}, \alpha) := \max_{2 \le i \le n} \{|f_i|^{1/i}\}.$$

With these definitions behind us, we are now in position to state our main results on class group statistics. Our new method for counting reducible integral orbits of coregular representations yields the following theorem for the family of monogenized *cubic* orders:

Theorem 1. *When monogenized cubic orders are enumerated by height, the average size of the 2-torsion subgroups in the class groups of such orders is given by:*

(a) $\dfrac{5}{4} + \dfrac{\zeta(2)}{4\zeta(3)}$ *for the family of totally real monogenized cubic orders, and*

(b) $\dfrac{3}{2} + \dfrac{\zeta(2)}{2\zeta(3)}$ *for the family of complex monogenized cubic orders.*

In previous work of Bhargava, Hanke, and the first-named author (see [8, Theorem 4]), the analogue of Theorem 1 was proven for the subfamily of monogenized *maximal* cubic orders (i.e., monogenized orders that are rings of integers of cubic fields). The key obstacle to generalizing [8, Theorem 4] to the full family is that a non-maximal order $\mathcal{O}$ can have nontrivial torsion in its ideal group $\mathcal{I}(\mathcal{O})$, and 2-torsion ideals can contribute to the 2-torsion subgroup of its class group $\mathrm{Cl}(\mathcal{O})$. The dichotomy between 2-torsion ideal classes that come from 2-torsion ideals of cubic orders and those that do not is beautifully captured in an orbit parametrization discovered by Bhargava (see [3]). As shown by Bhargava and the fourth-named author in [14], if $\mathcal{O}$ is a cubic order and $I \in \mathcal{I}(\mathcal{O})[2]$ (resp., $I \notin \mathcal{I}(\mathcal{O})[2]$) is an ideal of $\mathcal{O}$ whose class in $\mathrm{Cl}(\mathcal{O})$ is

[1] When the choice of monogenizer α is implicit, we abuse notation by writing $\mathcal{O}$ for the monogenized order $(\mathcal{O}, \alpha)$.

2-torsion, then I corresponds via Bhargava's parametrization to a *reducible* (resp., *irreducible*) integral orbit of a certain coregular representation.[2]

In [39, Theorem 9], the second-named author applied a higher-degree generalization of Bhargava's parametrization due to Wood (see §2.2) in conjunction with the aforementioned general approach for counting *irreducible* integral orbits to determine the average size of the quantity

$$\#\operatorname{Cl}(\mathcal{O})[2] - 2^{1-\frac{n+r_1}{2}} \cdot \#\mathcal{I}(\mathcal{O})[2], \tag{1}$$

where $\mathcal{O}$ runs over monogenized degree-n orders with r_1 real embeddings ordered by height. Proving Theorem 1 therefore amounts to determining the average size of $\mathcal{I}(\mathcal{O})[2]$ over monogenized cubic orders. Via the parametrization, this is equivalent to counting *reducible* integral orbits of the relevant coregular representation, which turns out to be the representation of the split orthogonal group $\mathcal{G}_3$ acting on the space W_3 of self-adjoint operators for the symmetric bilinear form $\sum_{i=1}^{3} x_i y_{4-i}$ (see §1.3.1 for the definitions of $\mathcal{G}_3$ and W_3, as well as their higher-dimensional generalizations $\mathcal{G}_n$ and W_n). By applying our method for counting reducible orbits to the representation of $\mathcal{G}_3$ on W_3, we obtain the following result:

Theorem 2. *When monogenized cubic orders are enumerated by height, the average size of the 2-torsion subgroups in the ideal groups of such orders is equal to* $\frac{\zeta(2)}{\zeta(3)}$.

Remark. Strikingly, the average size in Theorem 2 is exactly the same as the value determined by Bhargava and the fourth-named author [15, Theorem 6] for the average size of the 3-torsion subgroups in the ideal groups of (monogenic) quadratic orders!

Our method for counting reducible orbits applies quite generally; in particular, it also works for the representation of $\mathcal{G}_n$ on W_n for every $n > 3$. This allows us to prove the following generalization of Theorem 2 for monogenized orders of *arbitrary* odd degree $n > 3$:

Theorem 3. *Let $n > 3$ be an odd integer. When monogenized degree-n orders are enumerated by height, the mean size of the 2-torsion subgroups in the ideal groups of such orders is bounded by*

$$\prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \zeta(2i) \leq 1.82102.$$

In particular, the average sizes of the 2-torsion subgroups in the class groups and ideal groups of monogenized orders of odd degree n enumerated by height are bounded, independently of n.

Remark. Since the torsion subgroup of the ideal group of a maximal order is trivial, and since the proportion of monogenized degree-n orders that are maximal is equal to $\frac{1}{\zeta(2)} < 100\%$ (see [13, Theorem 1.2]), it follows from Theorem 3 that the average size of the 2-torsion in the ideal groups of *non-maximal* monogenized degree-n orders is bounded. We note, however, that these upper bounds are not optimal: to determine exact asymptotics would require us to compute certain local integrals (see Theorem 5 and §6.2), and these computations remain open for degrees $n > 3$.

The Cohen-Lenstra heuristics (see [18], along with the extensions made by Cohen–Martinet [19], and Malle [30]) constitute a series of conjectures on the distributions of p-parts of class groups in families of number fields of fixed degree and Galois group. Unfortunately, predicting analogous distributions for families of non-maximal orders is beyond the scope of the original conjectures, and it remains to be determined how the heuristics change for families of orders defined by nontrivial global conditions, such as that of being monogenized. Taken together with the results of [8, 39], Theorems 1–3 constitute a first step toward posing more general conjectures about class group distributions. Furthermore, our results give evidence toward the idea that if one seeks to formulate

[2]See also the work [15], where Bhargava and the fourth-named author prove an analogous dichotomy for 3-torsion classes of quadratic orders.

a uniform set of heuristics that apply to all orders in number fields, rather than just maximal orders, it may be more natural to separately study the distributions of the quantities $\mathcal{I}(\mathcal{O})[p^n]$ and

$$\#\operatorname{Cl}(\mathcal{O})[p^n] - p^{c(\mathfrak{F})} \cdot \#\mathcal{I}(\mathcal{O})[p^n],$$

where $c(\mathfrak{F})$ denotes a constant depending on the family $\mathfrak{F} = \{\mathcal{O}\}$ of orders under consideration.

1.2. **Background on geometry-of-numbers methods.** In this section, we summarize the geometry-of-numbers methods that feature in the literature on arithmetic statistics leading up to the present article, and we describe the context for our method of counting reducible orbits.

A *coregular representation* $(\mathcal{G}, W)$ consists of a semisimple algebraic group $\mathcal{G}$, defined over $\mathbb{Z}$, and a finite-dimensional representation W of $\mathcal{G}$, also defined over $\mathbb{Z}$, having a free ring of $\mathcal{G}$-invariants. Suppose that a family of arithmetic objects can be parametrized in terms of certain — usually *irreducible* — $\mathcal{G}(\mathbb{Z})$-orbits on $W(\mathbb{Z})$. Further suppose that these orbits can be equipped with a natural notion of *height* — usually arising from a height function on the family of arithmetic objects being parametrized — and also that this height function can be extended to $W(\mathbb{R})$.

Under the above assumptions, the problem of counting arithmetic objects in the family with bounded height can be translated into the problem of counting lattice points of bounded height in a fundamental domain $\mathcal{D}$ for the action of $\mathcal{G}(\mathbb{Z})$ on $W(\mathbb{R})$. However, such fundamental domains $\mathcal{D}$ are usually not compact, even for the subset $\mathcal{D}_X$ of points in $\mathcal{D}$ that have height less than X. Indeed, the height-bounded fundamental domain $\mathcal{D}_X$ typically consists of a compact *main body* and one or more *cusps*, which are long tentacle-like regions going off to infinity.

One can determine an asymptotic for the number of irreducible lattice points in the main body using geometry-of-numbers methods. If it so happens that the arithmetic objects in question correspond to irreducible $\mathcal{G}(\mathbb{Z})$-orbits of $W(\mathbb{Z})$, and if the number of irreducible lattice points in the cusp can be shown to be negligible relative to the number of points in the main body, then the main-body count gives an asymptotic for the number of arithmetic objects of bounded height in the family.

The development and use of this strategy goes back centuries. Mertens [31] and Siegel [41] developed geometry-of-numbers methods to count the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits on integral binary quadratic forms with bounded discriminant, thereby resolving conjectures of Gauss on the average sizes of class numbers of quadratic orders. In the series of papers [21, 22, 23], Davenport obtained asymptotics for the number of irreducible $\mathrm{GL}_2(\mathbb{Z})$-orbits on integral binary cubic forms having bounded discriminant. Combining these asymptotics with results from class field theory and sieving methods, Davenport and Heilbronn determined the density of discriminants of cubic fields [24].

The primary obstruction to generalizing the work of Mertens, Siegel, and Davenport–Heilbronn to other coregular representations is demonstrating that the number of irreducible points in the cusps is negligible. In the aforementioned works, *ad hoc* geometry-of-numbers techniques were used to *bound* the number of irreducible $\mathrm{GL}_2(\mathbb{Z})$-orbits that lie in cusps of the fundamental domains of binary quadratic and cubic forms. A pioneering advance was made by Bhargava (see [6]), who introduced an averaging technique that has the effect of "thickening" the cusps and that applies to general coregular representations. Bhargava's averaging technique gives a systematic way to bound the number of points in cuspidal regions and thus opened the door to study the distributions of a wide variety of arithmetic objects, particularly those parametrized by irreducible integral orbits of coregular representations. However, these techniques only yield upper bounds on the number of lattice points in the cusps and do not suffice to obtain precise asymptotics.

The purpose of the present article is to develop a general method for determining asymptotics for the number of lattice points in the cuspidal regions of $\mathcal{D}_X$. These regions overwhelmingly contain *reducible* integral orbits of $\mathcal{G}$ on W. We illustrate this method for a representation of particular interest in number theory, namely the action of the split orthogonal group $\mathcal{G}_n$ on the space W_n of self-adjoint operators for the symmetric bilinear form $\sum_{i=1}^{n} x_i y_{n+1-i}$. The irreducible orbits of this representation have been studied extensively in the literature. For example, see [7, Theorem 10.1]

(resp., [37, Theorem 20]), where Bhargava and Gross (resp., the first-named author and Wang) obtained asymptotics for the number of *irreducible* orbits of $\mathcal{G}_n(\mathbb{Z})$ on $W_n(\mathbb{Z})$ having bounded height when n is odd (resp., when n is even) and applied these asymptotics to determine the average sizes of the 2-Selmer groups of monic hyperelliptic Jacobians of any given dimension.

Prior to our work, asymptotics for reducible orbits have been determined in only a few special cases. Firstly, the case of $\mathrm{SL}_2(\mathbb{Z})$ acting on integer-matrix binary cubic forms was handled by Shintani using ζ-function techniques (see [38, Chapter 2, §7, Remark 2]). Shintani's result was later recovered using an elementary geometry-of-numbers argument by Bhargava and the fourth-named author (see [15, §4.1.2]), who applied it to determine the average size of the 3-torsion in class groups of quadratic orders. Secondly, in [1], Altug, the first- and fourth-named authors, and Wilson used both L-function techniques and geometry-of-numbers methods to prove an asymptotic for the number of D_4-reducible orbits of $\mathrm{GL}_2 \times \mathrm{SL}_3$ acting on pairs of integer-matrix ternary quadratic forms.[3] However, all of these works rely crucially on situation-specific techniques and on the fact that the representations under consideration are of relatively small dimension.

In general, since reducible orbits of coregular representations often contain rich arithmetic information (in addition to the works referenced above, see also [13, 34]), we expect that our methods will have applications far beyond the results of this paper. For instance, we note that D_5-quintic rings, as well as elements in ideal groups of cubic orders, correspond to reducible orbits via the relevant parametrizations (see [3, 5, 44]).

1.3. **Summary of the proof.** Fix an integer $n \geq 3$. In this section, we introduce the representation of the split orthogonal group on self-adjoint operators for the symmetric bilinear form $\sum_{i=1}^{n} x_i y_{n+1-i}$. After defining the necessary notation, we illustrate how our method for counting points in cusps of fundamental domains applies to count reducible orbits of this representation, and hence to prove Theorems 1–3.

1.3.1. *Notation and setup.* Let A_0 denote the anti-diagonal $n \times n$ matrix with all anti-diagonal entries equal to 1; viewed as a symmetric bilinear form, notice that A_0 is split (i.e., the symmetric bilinear form associated to A_0 has a maximal isotropic space over $\mathbb{Q}$) and unimodular.

The representation. Let $\mathcal{G}_n$ denote the split orthogonal group scheme over $\mathbb{Z}$ whose R-points are given by

$$\mathcal{G}_n(R) = \begin{cases} \mathrm{SO}_{A_0}(R) := \{g \in \mathrm{SL}_n(R) : g^T A_0 g = A_0\}, & \text{if } n \text{ is odd,} \\ \mathrm{O}_{A_0}(R) := \{g \in \mathrm{SL}_n^{\pm}(R) : g^T A_0 g = A_0\}, & \text{if } n \text{ is even,} \end{cases} \tag{2}$$

for any $\mathbb{Z}$-algebra R. Let W_n denote the affine $\mathbb{Z}$-scheme whose R-points consist of self-adjoint operators for A_0 over R. Then W_n has a natural structure of $\mathcal{G}_n$-representation, given by $g \cdot T = g \cdot T \cdot g^{-1}$ for any $g \in \mathcal{G}_n(R)$ and $T \in W_n(R)$. We typically find it more convenient to work not with $T \in W_n(R)$ but with $B = -A_0 T$, which is an $n \times n$ symmetric matrix with entries in R (see §2.3). Thus, we often abuse notation by writing $B \in W_n(R)$ to mean "the $n \times n$ symmetric matrix arising from the self-adjoint operator $-A_0 B \in W_n(R)$." In this language, the action of an element $g \in \mathcal{G}_n(R)$ on $T \in W_n(R)$ is written as $B \mapsto (g^{-1})^T \cdot B \cdot g^{-1}$.

The invariants. Let U_n denote the affine $\mathbb{Z}$-scheme whose R-points consist of monic degree-n binary forms with coefficients in R. For any $B \in W_n(R)$, the monic degree-n binary form

$$\mathrm{inv}(x \cdot A_0 + z \cdot B) := (-1)^{\lfloor \frac{n}{2} \rfloor} \cdot \det(x \cdot A_0 + z \cdot B) \in U_n(R) \tag{3}$$

is evidently invariant under the action of $\mathcal{G}_n(R)$; in fact, the coefficients of the form $\mathrm{inv}(x \cdot A_0 + z \cdot B)$ freely generate the ring of polynomial invariants for the action of $\mathcal{G}_n$ on W_n. Given $F \in U_n(R)$, we write $\mathrm{inv}^{-1}(F) := \{B \in W_n(R) : \mathrm{inv}(x \cdot A_0 + z \cdot B) = F(x, z)\}$.

[3] We say that an orbit of this representation is *D_4-reducible* if it corresponds to a D_4-quartic number field.

Let N denote the lower triangular unipotent subgroup of SL_2. Then $N(\mathbb{Z})$ acts on $U_n(\mathbb{Z})$ via $(\gamma \cdot F)(x,z) = F((x,z)\cdot\gamma)$ for any $\gamma \in N(\mathbb{Z})$ and $F \in U_n(\mathbb{Z})$; moreover, $N(\mathbb{Z})$ acts on $W_n(\mathbb{Z})$ by sending $B \mapsto u \cdot A_0 + B$ for any $\left[\begin{smallmatrix} 1 & 0 \\ u & 1 \end{smallmatrix}\right] \in N(\mathbb{Z})$ and $B \in W_n(\mathbb{Z})$. For $F \in U_n(\mathbb{R})$, we define its *height* $\mathrm{H}(F)$ to be the height of the isomorphism class of the monogenized order defined by F.

If n is odd, let r_1 be any odd positive integer less or than equal to n, and if n is even, let r_1 be an even nonnegative integer less than or equal to n. Define

$$U_n^{(r_1)}(\mathbb{Z}) := \{F \in U_n(\mathbb{Z}) : F \text{ has nonzero disc. and } r_1 \text{ real roots}\}$$
$$W_n^{(r_1)}(\mathbb{Z}) := \{B \in W_n(\mathbb{Z}) : \mathrm{inv}(x\cdot A_0 + z\cdot B) \in U_n^{(r_1)}(\mathbb{Z})\}.$$

For a real number $X > 0$, let $N_n^{(r_1)}(X)$ be the number of $F \in N(\mathbb{Z})\backslash U_n^{(r_1)}(\mathbb{Z})$ of height up to X.

The notion of reducibility. When $R = \mathbb{Z}$, we say that (the $\mathcal{G}_n(\mathbb{Z})$-orbit of) $B \in W_n(\mathbb{Z})$ is *reducible* if

- (the symmetric bilinear forms associated to) A_0 and B share a maximal isotropic subspace defined over $\mathbb{Q}$ when n is odd, or
- (the symmetric bilinear forms associated to) B has an isotropic subspace of dimension $\frac{n-2}{2}$ defined over $\mathbb{Q}$ contained within a maximal isotropic subspace for (the symmetric bilinear forms associated to) A_0 defined over $\mathbb{Q}$ when n is even.

We say that $B \in W_n(\mathbb{Z})$ is *irreducible* if it is not reducible.

Let R be a $\mathbb{Z}$-algebra. For any subset $S \subset W_n(R)$, let $S_0 \subset S$ be the subset consisting of elements $B = [b_{ij}]$ such that $b_{ij} = 0$ for all pairs (i,j) such that $i + j \le n-1$. Observe that every element of $W_n(\mathbb{Z})_0$ is reducible. Moreover, letting $\mathcal{P} \subset \mathcal{G}_n$ denote the lower-triangular subgroup, observe the action of $\mathcal{G}_n(R)$ on $W_n(R)$ restricts to a well-defined action of $\mathcal{P}(R)$ on $W_n(R)_0$.

1.3.2. *Main results on counting in cusps.* We prove the following asymptotic formula for the count of reducible $\mathcal{G}_n(\mathbb{Z})$-orbits on all of $W^{(r_1)}(\mathbb{Z})$:

Theorem 4. *The number of reducible $\mathcal{G}_n(\mathbb{Z})$-orbits on $W^{(r_1)}(\mathbb{Z})$ having height up to X is given by*

$$\left(\prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \zeta(2i)\right) \cdot N_n^{(r_1)}(X) + o\big(X^{\frac{n^2+n-2}{2}}\big)$$

if n is odd, and is given by

$$\left(\zeta(\tfrac{n}{2}) \prod_{i=1}^{\frac{n-2}{2}} \zeta(2i)\right) \cdot \frac{N_n^{(r_1)}(X)}{2^{\frac{n}{2}}} + o\big(X^{\frac{n^2+n-2}{2}}\big)$$

if n is even.

Remark. We make two observations regarding the form of the asymptotics obtained in Theorem 4. Firstly, the product of ζ-values is the fundamental volume of $\mathcal{G}_n$. Secondly, the additional factor of $2^{-\frac{n}{2}}$ that occurs in the asymptotic for even n in Theorem 4 accounts for the fact that for any $B \in W_n(\mathbb{Z})$, the $x^{n-i}z^i$-coefficient of $\mathrm{inv}(x\cdot A_0 + z\cdot B)$ is divisible by 2 for every odd number $i \in \{1,3,\dots,n-1\}$ (see [40, Theorem 80]).

We now outline the proof of Theorem 4, which occupies §3–§5, and also part of §6. We begin in §3 by constructing fundamental sets for the action of $\mathcal{G}_n(\mathbb{Z})$ on $W_n(\mathbb{R})$. As we show in §3.3, this amounts to constructing a fundamental domain $\mathcal{F}$ for the action of $\mathcal{G}_n(\mathbb{Z})$ on $\mathcal{G}_n(\mathbb{R})$. For the purpose of proving Theorem 4, it is *not* enough to simply invoke the work of Borel and Harish-Chandra (see [16, 17]), who constructed fundamental domains for general semisimple groups. Indeed, our argument in §4.2 requires that the fundamental domain $\mathcal{F}$ be *box-shaped at infinity*, meaning that $\mathcal{F}$ looks like a Siegel domain in a neighborhood of infinity. In §3.1–3.2, we define what it means

for a fundamental domain to be box-shaped at infinity and prove that such fundamental domains exist for the group $\mathcal{G}_n$ (see Theorem 12).

In §4, we prove an intermediate result (see Theorem 18) that expresses the count of reducible orbits of height up to X in terms of an integral C_X, which gives the volume of a certain subset of $W_n(\mathbb{R})_0$ with respect to a certain measure, which we denote by λ. To prove this, we start in §4.1 by applying Bhargava's technique of averaging over translates of the domain $\mathcal{F}$ constructed in §3 to thicken the region in which we are counting lattice points. In this thickened region, all but a negligible number of reducible integral elements lie on the hyperplane $W_n(\mathbb{R})_0 \subset W_n(\mathbb{R})$. This reduces the problem of counting reducible orbits of $\mathcal{G}_n(\mathbb{Z})$ on $W_n(\mathbb{Z})$ to that of counting lattice points lying in the cusp of our fundamental domain for the action of $\mathcal{G}_n(\mathbb{Z})$ on $W_n(\mathbb{R})$. Indeed, the cusp is a narrow region consisting of elements $B = [b_{ij}]$ for which b_{ij} is tiny for all (i, j) such that $i + j \leq n - 1$, so lattice points in the cusp necessarily lie in $W_n(\mathbb{R})_0$.

As it happens, the thickened cusp is still too narrow for us to be able to use standard geometry-of-numbers methods to count lattice points in it. In §4.2, we overcome this difficulty by slicing the thickened cusp into ball-like regions, within each of which it is easier to count lattice points. Summing the count of lattice points over all slices yields Theorem 18. Then, up to a technicality concerning orbits with big integral stabilizer that we resolve in §6.1 (see Proposition 32), all that remains to deduce Theorem 4 from Theorem 18 is to compute the integral C_X. We achieve this in §5 by proving a Jacobian change-of-variables formula that transforms the measure $d\lambda$ on $W_n(\mathbb{R})_0$ into the product of the Euclidean measure on $U_n(\mathbb{R})$ with the Haar measure on the lower-triangular subgroup $\mathcal{P} \subset \mathcal{G}_n$ (see Proposition 24). Such change-of-variable results have previously been proven when the group under consideration is unimodular (see, e.g., [11, §3.4] for the prototypical example), but the fact that the group $\mathcal{P}$ *fails* to be unimodular presents significant new challenges.

In §6.1, we show how the proof of Theorem 4 in §4–5 can be retrofitted to count reducible orbits in subsets $S \subset W_n^{(r_1)}(\mathbb{Z})$ defined by congruence conditions (see Theorem 31). For those subsets S that consist of elements $B \in W^{(r_1)}(\mathbb{Z})$ such that the coefficients of the binary form $\mathrm{inv}(x \cdot A_0 + z \cdot B)$ satisfy finite sets of congruence conditions, Theorem 31 specializes to the following result:

Theorem 5. *Let $\Sigma = U_n^{(r_1)}(\mathbb{Z}) \cap \bigcap_p \Sigma_p$ be a family of monic binary forms defined by finitely many congruence conditions. Then the number of reducible $\mathcal{G}_n(\mathbb{Z})$-orbits of elements $B \in W_n^{(r_1)}(\mathbb{Z})$ such that $\mathrm{inv}(x \cdot A_0 + z \cdot B) \in \Sigma$ of height up to X is given by*

$$N_n^{(r_1)}(X) \cdot \prod_p \int_{F \in \Sigma_p} \# \left(\frac{\mathrm{inv}^{-1}(F)_0}{\mathcal{P}(\mathbb{Z}_p)} \right) dF + o\big(X^{\frac{n^2+n-2}{2}}\big) \tag{4}$$

where dF denotes the Euclidean measure on $U_n(\mathbb{Z}_p)$, normalized so that $U_n(\mathbb{Z}_p)$ has volume 1.

Remark. The occurrence of the lower-triangular subgroup $\mathcal{P}$ in the proof of Theorem 4 and in the statement of Theorem 5 is no accident: indeed, Theorems 4 and 5 may be reinterpreted as providing asymptotics for the number of orbits of $\mathcal{P}(\mathbb{Z})$ on $W_n^{(r_1)}(\mathbb{Z})_0$ having bounded height. This is significant, because there are obstacles to using the geometry-of-numbers methods outlined in §1.2 to count integral orbits for representations of groups, like $\mathcal{P}$, that are not unimodular.

We conclude this section by discussing how our results on counting in cusps can be applied to deduce our main results on class group statistics, namely Theorems 1–3. In §2, we describe how 2-torsion ideal classes in monogenized orders of odd degree n can be parametrized in terms of orbits of $\mathcal{G}_n(\mathbb{Z})$ on $W_n(Z)$, and we demonstrate that 2-torsion *ideals* correspond to reducible orbits under this parametrization. As explained in §2.2, the orbits that correspond to 2-torsion ideals satisfy an additional property known as *projectivity*, which entails a set of congruence conditions at each prime p (see Proposition 8). For elements of $W_3(\mathbb{Z})$, these congruence conditions are sufficiently concrete that we can apply Theorem 31 to count the orbits satisfying them, thus yielding Theorem 2, and hence also Theorem 1. However, the conditions become computationally intractable for elements of

W_n as soon as $n > 3$, rendering it difficult to prove a direct analogue of Theorems 1 and 2 for orders of larger degree. Nonetheless, the asymptotic in Theorem 4 suffices to give the upper bound in Theorem 3 on the average size of the 2-torsion in the ideal groups of monogenized degree-n orders.

We expect that an analogue of Theorem 3 can be obtained for monogenized orders arising from even-degree binary forms, although this would require applying our methods to a different integral form of the group $\mathcal{G}_n$ (see [40, §8]). We further expect that, by combining the methods of this paper with the results of [42], one can bound the average size of the 2-torsion in the ideal groups of orders associated to even-degree binary forms having any fixed leading coefficient (not just 1).

2. Parametrizing 2-torsion ideal classes in monogenized orders

Let G_n be the group scheme over $\mathbb{Z}$ whose S-points are given by

$$G_n(S) = \begin{cases} \mathrm{SL}_n(S), & \text{if } n \text{ is odd,} \\ \mathrm{SL}_n^{\pm}(S), & \text{if } n \text{ is even} \end{cases} \tag{5}$$

for any $\mathbb{Z}$-algebra S. Let $R = \mathbb{Z}$ or $\mathbb{R}$. In this section, we recall a parametrization from the literature that relates certain orbits of $G_n(R)$ on the space $R^2 \otimes_R \mathrm{Sym}_2 R^n$ of pairs of symmetric $n \times n$ matrices over R with 2-torsion ideal classes in monogenized orders over R. We then explain how the orbits of $\mathcal{G}_n(R)$ on $W_n(R)$ can be characterized in terms of this parametrization.

2.1. **Notation for monogenized orders.** Let R be as above, and let K be the fraction field of R. Let $n \geq 3$, and let

$$F(x, z) = x^n + \sum_{i=1}^{n} f_i x^{n-i} z^i \in R[x, z]$$

be a monic binary form of degree n that is separable over K. When it is convenient, we write f_0 for the leading coefficient of F, which will always be equal to 1.

Consider the étale K-algebra $K_F := K[x]/(F(x, 1))$, and let θ denote the image of x in K_F. When $R = \mathbb{Z}$, the monogenized order associated to F is defined to be the pair (R_F, θ), where $R_F := R[\theta] \subset K_F$. If $F' = \gamma \cdot F$ for some $\gamma \in N(\mathbb{Z})$, then γ induces an isomorphism $K_F \simeq K_{F'}$, under which the monogenized orders associated to F and F' are identified.

Given a based fractional ideal I of R_F, the *norm* of I, denoted by $\mathrm{N}(I)$, is the determinant of the K-linear transformation taking the basis of I to the power basis $R\langle 1, \theta, \ldots, \theta^{n-1}\rangle$. The norm of $\kappa \in K_f^{\times}$ is the determinant of the K-linear transformation taking the basis $R\langle 1, \theta, \ldots, \theta^{n-1}\rangle$ to the basis $R\langle \kappa, \kappa \cdot \theta, \ldots, \kappa \cdot \theta^{n-1}\rangle$.

2.2. **The parametrization.** Retain the notation from §2.1. Let I be a based fractional ideal of R_F and let $\alpha \in K_F^{\times}$ be such that

$$I^2 \subset (\alpha) \quad \text{and} \quad \mathrm{N}(I)^2 = \mathrm{N}(\alpha). \tag{6}$$

Consider the symmetric bilinear form

$$\langle -, - \rangle \colon I \times I \to R_F, \quad (\beta, \gamma) \mapsto \langle \beta, \gamma \rangle = \alpha^{-1} \cdot \beta\gamma. \tag{7}$$

Let $\pi_{n-2}, \pi_{n-1} \in \mathrm{Hom}_R(R_F, R)$ be the maps defined as follows:

$$\pi_{n-2}(\theta^{n-2}) - 1 = \pi_{n-2}(\theta^{n-1} + f_1\theta^{n-2}) = \pi_{n-2}(\theta^i) = 0 \quad \text{for each } i \in \{0, \ldots, n-3\}, \text{ and}$$
$$\pi_{n-1}(\theta^{n-2}) = \pi_{n-1}(\theta^{n-1} + f_1\theta^{n-2}) + 1 = \pi_{n-1}(\theta^i) = 0 \quad \text{for each } i \in \{0, \ldots, n-3\}.$$

Let $A_{(I,\alpha)}$ and $B_{(I,\alpha)}$ respectively denote the symmetric $n \times n$ matrices over R representing the two symmetric bilinear forms $\pi_{n-1} \circ \langle -, - \rangle \colon I \times I \to R$ and $\pi_{n-2} \circ \langle -, - \rangle \colon I \times I \to R$ with respect to the chosen basis of I. Then the data of the symmetric bilinear forms $\pi_{n-1} \circ \langle -, - \rangle, \pi_{n-2} \circ \langle -, - \rangle$ is encoded by the pair

$$(A_{(I,\alpha)}, B_{(I,\alpha)}) \in R^2 \otimes_R \mathrm{Sym}_2 R^n.$$

If we change the basis of I by means of an element $g \in G_n(R)$, then the pair $(A_{(I,\alpha)}, B_{(I,\alpha)})$ transforms as $(A_{(I,\alpha)}, B_{(I,\alpha)}) \mapsto \big(g \cdot A_{(I,\alpha)} \cdot g^T, g \cdot B_{(I,\alpha)} \cdot g^T\big)$. It is evident that the binary form

$$\mathrm{inv}\left(x \cdot A_{(I,\alpha)} + z \cdot B_{(I,\alpha)}\right) := (-1)^{\lfloor \frac{n}{2} \rfloor} \cdot \det\left(x \cdot A_{(I,\alpha)} + z \cdot B_{(I,\alpha)}\right)$$

is preserved under the action of $G_n(R)$.

Remark. When n is odd, the action of $-\mathrm{id} \in \mathrm{SL}_n^{\pm}(R)$ centralizes elements of $R^2 \otimes_R \mathrm{Sym}_2 R^n$, so it suffices to work with $\mathrm{SL}_n(R)$ instead of $\mathrm{SL}_n^{\pm}(R)$.

We declare two pairs $(I,\alpha), (I',\alpha')$ satisfying the properties (6) to be equivalent if for some $g \in G_n(R)$ and $\kappa \in K_F^\times$ we have $(I',\alpha') = \big(g\cdot(\kappa\cdot I), \kappa^3 \cdot \alpha\big)$. One readily verifies that if $(I,\alpha), (I',\alpha')$ are equivalent, then $(A_{(I,\alpha)}, B_{(I,\alpha)}), (A_{(I',\alpha')}, B_{(I',\alpha')})$ belong to the same $G_n(R)$-orbit. Given this setup, we have the following fundamental parametrization result:

Theorem 6 ([45, Theorem 3.1])**.** *The map sending the equivalence class of a pair (I,α) satisfying the properties* (6) *to the $G_n(R)$-orbit of the pair $(A_{(I,\alpha)}, B_{(I,\alpha)}) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$ is one-to-one and has image equal to the set of $G_n(R)$-orbits of pairs $(A,B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$ such that $\mathrm{inv}(x \cdot A + z \cdot B) = F(x,z)$. The stabilizer in $G_n(R)$ of the orbit corresponding to a pair (I,α) via this bijection is isomorphic to $\mathrm{End}_{R_F}(I)^\times[2]_{\mathrm{N}\equiv 1} := \{\phi \in \mathrm{End}_{R_F}(I) : \phi^2 = \mathrm{id}, \mathrm{N}(\phi) \in K^{\times 2}\}$ if n is odd and $\mathrm{End}_{R_F}(I)^\times[2]$ if n is even.*[4]

We say that (the $G_n(R)$-orbit of) a pair $(A,B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$ is *reducible* if, when n is odd, the (symmetric bilinear forms associated to) A, B share a maximal isotropic subspace defined over K, and, when n is even, B has an isotropic subspace of dimension $\frac{n-2}{2}$ defined over K contained within a maximal isotropic subspace for A defined over K.

Take n to be odd in the rest of this subsection. The following proposition tells us when the orbit arising from a pair (I,α) is reducible:

Proposition 7 ([29, Theorem 2.6])**.** *The $G_n(R)$-orbit arising from a pair (I,α) satisfying the properties* (6) *via Theorem 6 is reducible if and only if $\alpha \in K_F^{\times 2}$.*

It follows from Proposition 7 that every pair (I,α) giving rise to a reducible orbit is equivalent to a pair of the form $(I',1)$ for some based fractional ideal I'. When R_F is the maximal order in K_F (e.g., when $R = \mathbb{R}$), any such ideal I' must be the unit ideal, so there is a unique reducible pair $(A,B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$ up to the action of $G_n(R)$ with $\mathrm{inv}(x \cdot A + z \cdot B) = F(x,z)$ in this case.

Now take $R = \mathbb{Z}$. To prove Theorems 1–3, we must characterize the pairs in $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ that arise from 2-torsion ideals.[5] Any such ideal $I \in \mathcal{I}(R_F)[2]$ must be invertible; this is a nontrivial condition, for a based fractional ideal I satisfying the properties (6) for some $\alpha \in K_F^\times$ need *not* be invertible when R_F is not the maximal order in K_F. We say that (the $G_n(\mathbb{Z})$-orbit of) a pair $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ such that $\mathrm{inv}(x\cdot A + z\cdot B) = F(x,z)$ is *projective* if $(A,B) = (A_{(I,\alpha)}, B_{(I,\alpha)})$ for some pair (I,α) satisfying the properties (6) such that I is invertible. The following proposition identifies which elements of $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ are projective:

[4]Since F is separable, every R_F-module endomorphism of I is given by multiplication by an element of K_F. Thus, we may take the norms of elements of $\mathrm{End}_{R_F}(I)^\times$.

[5]The characterization of orbits arising from 2-torsion ideals presented in this section holds for any odd n. We restrict our consideration in Theorem 2 to the case where $n = 3$ because the determinantal condition for projectivity in Proposition 8 grows rapidly more complicated for larger values of n.

Proposition 8. *Let $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2\mathbb{Z}^n$ with $\mathrm{inv}(x \cdot A + z \cdot B) = F(x,z)$, where F is as in §2.1. For each $k \in \{0,\dots,n-1\}$, let $C^{(k)}$ be the $n \times n$ matrix over R defined as follows:*

$$C^{(k)} = \begin{cases} A, & \text{if } k = n-1, \\ B, & \text{if } k = n-2, \\ \left(\sum_{i=0}^{n-k-3} f_i \cdot (BA^{-1})^{n-k-2-i}\right) \cdot B, & \text{if } k \in \{1,\dots,n-3\}, \\ \left(\sum_{i=0}^{n-1} f_i \cdot (BA^{-1})^{n-1-i}\right) \cdot A, & \text{if } k = 0. \end{cases} \tag{8}$$

Let M denote the $n \times \binom{n^2+n}{2}$ matrix over R whose k^{th} row consists of the entries of $C^{(k)}$ lying on or above the diagonal, written as a list in some order that is uniform over k. Then the pair (A,B) is projective if and only if the greatest common divisor of the $n \times n$ minors of M is equal to 1.

Proof. Let (I,α) be a pair satisfying the properties (6) corresponding to the pair (A,B) via Theorem 6. By [29, §2.2], the matrices $C^{(k)}$ are symmetric, and the matrix M represents the map of R-modules $I \times I \to R_F$ in (7) with respect to the basis of $I \times I$ obtained by taking pairwise products of the basis elements of I. The fractional ideal I is invertible if and only if $I^2 = (\alpha)$ (as opposed to just having a containment $I^2 \subset (\alpha)$), and this occurs if and only if the map $I \times I \to R_F$ is surjective, which in turn happens if and only if the $n \times n$ minors of M have no common divisor. □

In particular, it follows from Proposition 8 that the locus of projective pairs in $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2\mathbb{Z}^n$ is cut out by congruence conditions modulo p for every prime number p.

A 2-torsion ideal $I \in \mathcal{I}(R_F)[2]$ must also satisfy $\mathrm{N}(I) \in \{\pm 1\}$ with respect to any basis of I. Thus, if we take $\alpha = 1$, then the pair (I,α) satisfies the properties (6). We thus obtain a well-defined map

$$\mathcal{I}(R_F)[2] \to G_n(\mathbb{Z})\backslash(\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2\mathbb{Z}^n) \tag{9}$$

that takes $I \in \mathcal{I}(R_F)[2]$, gives it some basis, and produces the pair $(A_{(I,1)}, B_{(I,1)})$. The following corollary of Theorem 6 characterizes the map (9):

Corollary 9 ([29, Proposition 2.12])**.** *The map* (9) *defines a bijection between ideals in $\mathcal{I}(R_F)[2]$ and $G_n(R)$-orbits of projective reducible pairs $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2\mathbb{Z}^n$ with $\mathrm{inv}(x \cdot A + z \cdot B) = F(x,z)$.*

2.3. **A linearization trick.** We now explain a linearization trick introduced in [7, §3] and [37, §2] that allows us to characterize the orbits of $\mathcal{G}_n(R)$ on $W_n(R)$ in terms of the parametrization described in §2.2. The trick relies on the following two observations:

- If $(A,B) \in R^2 \otimes_R \mathrm{Sym}_2 R^n$ is such that $\det A = (-1)^{\lfloor \frac{n}{2} \rfloor}$, then the matrix $T = -A^{-1}B$ has entries in R is self-adjoint with respect to A (i.e., $T^T A = AT$), and $\mathrm{ch}_T(x) = \mathrm{inv}(x \cdot A + B)$.
- If an $n \times n$ matrix T over R is self-adjoint with respect to a symmetric $n \times n$ matrix A over R such that $\det A = (-1)^{\lfloor \frac{n}{2} \rfloor}$, then $-AT$ is symmetric, and $\mathrm{ch}_T(x) = \mathrm{inv}(x \cdot A - AT)$.

If we further assume that A is split over K and that A is even when n is even and $R = \mathbb{Z}$, then it follows from [36, Chapter V, §2.2] that A belongs to the $G_n(R)$-orbit of A_0. Combining the two observations above with Theorem 6 yields the following result for any nondegenerate $F \in U_n(R)$:

Proposition 10. *The map $T \mapsto (A_0, -A_0^{-1}T)$ induces a reducibility-preserving bijection between the orbits of $\mathcal{G}_n(R)$ on self-adjoint operators $T \in W_n(R)$ with $\mathrm{ch}_T(x) = F(x,1)$ and the $G_n(R)$-orbits of pairs $(A,B) \in R^2 \otimes_R \mathrm{Sym}^2 R^n$ with $\mathrm{inv}(x \cdot A + z \cdot B) = F(x,z)$ such that A is split over K and such that A is even when n is even and $R = \mathbb{Z}$. The stabilizer $\mathrm{Stab}_{\mathcal{G}_n(R)}(T)$ of such an operator T is isomorphic to $\mathrm{End}_{R_F}(I)^\times[2]_{\mathrm{N}\equiv 1}$ if n is odd and $\mathrm{End}_{R_F}(I)^\times[2]$ if n is even.*

In what follows, it is often convenient to work with the symmetric matrix $B = -A_0T$ as opposed to the self-adjoint operator T; thus, we abuse notation by writing "$B \in W_n(R)$" to denote the element $T = -A_0B \in W_n(R)$.

The bijection in Proposition 10 preserves reducibility. When $A = A_0$, the reducibility criterion for $G_n(R)$-orbits takes on the following more convenient form:

Proposition 11 ([7, Proposition 4.4] and [37, Proposition 7])**.** *An element $B \in W_n(R)$ is reducible if and only if for some $\mathcal{G}_n(K)$-translate $B' = [b'_{ij}] \in W_n(K)$ of B we have that $b'_{ij} = 0$ for all pairs (i, j) such that $i + j \leq n - 1$.*

3. Reduction theory

To study monogenized orders, we must work with monic integral binary forms up to the action of $N(\mathbb{Z})$. This, together with the results of §2.2, imply that to count 2-torsion ideal classes of monogenized orders, we must count orbits of $(N \times \mathcal{G}_n)(\mathbb{Z})$ on $W_n(\mathbb{Z})$. The first step toward counting these orbits is to realize them as lattice points in fundamental sets for the action of $(N \times \mathcal{G}_n)(\mathbb{Z})$ on $W_n(\mathbb{R})$. The purpose of this section is to construct these fundamental sets.

Let $f_1 \in \{0, 1, \ldots, n-1\}$ when n is odd and $f_1 \in \{0, 2, \ldots, n-2\}$ when n is even, and consider the affine subspaces $W_{n,f_1} \subset W_n$ and $U_{n,f_1} \subset U_n$ defined by

$$W_{n,f_1}(R) := \left\{B \in V(R) : \mathrm{inv}(x \cdot A_0 + z \cdot B) = x^n + \textstyle\sum_{i=1}^{n} f_i x^{n-i} z^i \text{ for some } f_2, \ldots, f_n \in R\right\},$$
$$U_{n,f_1}(R) := \{F \in U_n(R) : x^{n-1}z\text{-coefficient of } F \text{ equals } f_1\}.$$

Since the $x^{n-1}z$-coefficient of a monic binary n-ic form has only finitely many possibilities up to the action of $N(\mathbb{Z})$, it suffices to construct fundamental sets for the action of $\mathcal{G}_n(\mathbb{Z})$ on $W_{n,f_1}(\mathbb{R})$ for each choice of f_1. We achieve this by means of a two-step process: we first construct a fundamental domain for $\mathcal{G}_n(\mathbb{Z})$ on $\mathcal{G}_n(\mathbb{R})$, and we subsequently combine this fundamental domain with fundamental sets for the action of $\mathcal{G}_n(\mathbb{R})$ on $W_{n,f_1}(\mathbb{R})$.

3.1. **A box-shaped fundamental domain for $\mathcal{G}_n(\mathbb{Z}) \curvearrowright \mathcal{G}_n(\mathbb{R})$.** A fundamental domain $\mathcal{F}$ is said to be *box-shaped at infinity* if it can be sandwiched as $\mathcal{S}_1 \subset \mathcal{F} \subset \mathcal{S}_2$, where $\mathcal{S}_1 \subset \mathcal{S}_2$ are nested generalized Siegel sets for the action of $\mathcal{G}_n(\mathbb{Z})$ on $\mathcal{G}_n(\mathbb{R})$ satisfying the following three conditions:

- There exists an open subset $\mathcal{U}_1 \subset \mathcal{S}_1$ of full measure such that every orbit of $\mathcal{G}_n(\mathbb{Z})$ on $\mathcal{G}_n(\mathbb{R})$ meets $\mathcal{U}_1$ at most once;
- Every orbit of $\mathcal{G}_n(\mathbb{Z})$ on $\mathcal{G}_n(\mathbb{R})$ meets $\mathcal{S}_2$ at least once; and
- The set $\mathcal{S}_2 \smallsetminus \mathcal{S}_1$ is absolutely bounded.

It is crucial for the proof of Theorem 4 (see §4.2) that we use a fundamental domain for the action of $\mathcal{G}_n(\mathbb{Z})$ on $\mathcal{G}_n(\mathbb{R})$ that is box-shaped at infinity. In this subsection and the next, we prove that such a fundamental domain exists:

Theorem 12. *There exists a fundamental domain for the action of $\mathcal{G}_n(\mathbb{Z})$ on $\mathcal{G}_n(\mathbb{R})$ that is box-shaped at infinity.*

Remark. Box-shaped fundamental domains are of considerable value in number theory, because they make it possible to perform a variety of explicit computations, such as the count of reducible orbits featured in this paper. For another example, see [26,27], where Grenier proves the analogue of Theorem 12 for the group SL_n and remarks that having a box-shaped fundamental domain for the action of $\mathrm{SL}_n(\mathbb{Z})$ on $\mathrm{SL}_n(\mathbb{R})$ would facilitate the computation of certain integrals of Eisenstein series that arise when generalizing Selberg's trace formula to the group $\mathrm{SL}_n(\mathbb{Z})$. Grenier's construction has had a number of interesting applications in the literature (see, e.g., [25,35,43]), and as explained in §3.2 (to follow), it plays a central role in our proof of Theorem 12.

The construction of nested generalized Siegel sets $\mathcal{S}_1 \subset \mathcal{S}_2$ satisfying the three conditions itemized above is deferred to §3.2. Once $\mathcal{S}_1$ and $\mathcal{S}_2$ have been constructed, Theorem 12 then follows from the next lemma, which shows that there exists a fundamental domain sandwiched between them:

Lemma 13. *Let Λ be a discrete subgroup of a Lie group $\mathcal{G}$ and denote by $\mathcal{B}(\mathcal{G})$ the Borel σ-algebra of $\mathcal{G}$. Suppose that $\mathcal{S}_1$ and $\mathcal{S}_2$ are sets in $\mathcal{B}(\mathcal{G})$ with the property that the maps $\mathcal{S}_1 \to \mathcal{G}/\Lambda$ and $\mathcal{S}_2 \to \mathcal{G}/\Lambda$ induced by $s \mapsto s\Lambda$ are, respectively, injective and surjective. Then there is a strict fundamental domain $\mathcal{F}$ in $\mathcal{B}(\mathcal{G})$ for the action of Λ on $\mathcal{G}$ such that $\mathcal{S}_1 \subset \mathcal{F} \subset \mathcal{S}_2$.*

Proof. The argument is analogous to the proof of [32, Lemma 4.1.1]. Since Λ is discrete, we can find a non-empty open subset $U \subset \mathcal{G}$ such that $U^{-1}U \cap \Lambda = \{\mathrm{id}\}$. Since $\mathcal{G}$ is second countable, we can find a sequence $\{g_n\} \subset \mathcal{G}$ such that $\mathcal{G} = \bigcup_{n=1}^{\infty} g_n U$. Let $\mathcal{S}'' = \mathcal{S}_2 \smallsetminus \mathcal{S}_1\Lambda$ and set:

$$\mathcal{F}' = \bigcup_{n=1}^{\infty} \left(g_n U \cap \mathcal{S}'' \smallsetminus \bigcup_{i<n} (g_i U \cap \mathcal{S}'')\Lambda \right).$$

Lastly, define $\mathcal{F} = \mathcal{S} \cup \mathcal{F}'$ and note that this union is disjoint. Then $\mathcal{F} \in \mathcal{B}(\mathcal{G})$ since all the operations used in its construction keep us in the σ-algebra. It is easy to check that the induced map $\mathcal{F} \to \mathcal{G}/\Lambda$ sending $x \mapsto x\Lambda$ is bijective. We conclude that $\mathcal{F}$ is a strict fundamental domain. □

3.2. **A pair of nested Siegel sets for $\mathcal{G}_n(\mathbb{Z}) \curvearrowright \mathcal{G}_n(\mathbb{R})$.** In this section, we complete the proof of Theorem 12 by constructing the nested generalized Siegel sets $\mathcal{S}_1 \subset \mathcal{S}_2$ referred to in §3.1.

To begin with, observe that it suffices to construct the Siegel sets $\mathcal{S}_i$ for the action of $\mathrm{SO}_{A_0}(\mathbb{Z})$ on $\mathrm{SO}_{A_0}(\mathbb{R})$, because when n is even, there exist elements in $\mathcal{G}_n(\mathbb{Z})$ having determinant -1. We therefore work with the group SO_{A_0} throughout the rest of this subsubsection.

The construction of $\mathcal{S}_2$ is, in essence, due to Borel and Harish-Chandra (see [7, §9.2] and [37, §4.1], which specialize the results of [16] and [17] for semisimple groups to the case of the group SO_{A_0}). Let $\mathcal{N} \subset \mathrm{SO}_{A_0}(\mathbb{R})$ denote the subgroup of lower-triangular unipotent matrices. A calculation shows that the elements of $\mathcal{N}$ are parametrized as follows:

$$\begin{bmatrix}
1 & & & & & & & & & & & \\
u_{21} & 1 & & & & & & & & & & \\
u_{31} & u_{32} & 1 & & & & & & & & & \\
\vdots & \vdots & \vdots & \ddots & & & & & & & & \\
u_{(\lceil \frac{n}{2} \rceil - 1)1} & u_{(\lceil \frac{n}{2} \rceil - 1)2} & u_{(\lceil \frac{n}{2} \rceil - 1)3} & \cdots & 1 & & & & & & & \\
u_{\lceil \frac{n}{2} \rceil 1} & u_{\lceil \frac{n}{2} \rceil 2} & u_{\lceil \frac{n}{2} \rceil 3} & \cdots & u_{\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor} & 1 & & & & & & \\
u_{(\lceil \frac{n}{2} \rceil + 1)1} & u_{(\lceil \frac{n}{2} \rceil + 1)2} & u_{(\lceil \frac{n}{2} \rceil + 1)3} & \cdots & -\frac{1}{2}u^2_{\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor} + * & -u_{\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor} & 1 & & & & & \\
\vdots & \vdots & \vdots & \iddots & \vdots & \vdots & \vdots & \ddots & & & & \\
u_{(n-2)1} & u_{(n-2)2} & -\frac{1}{2}u^2_{\lceil \frac{n}{2} \rceil 3} + * & \cdots & * & * & * & \cdots & 1 & & & \\
u_{(n-1)1} & -\frac{1}{2}u^2_{\lceil \frac{n}{2} \rceil 2} + * & * & \cdots & * & * & * & \cdots & -u_{32} & 1 & & \\
-\frac{1}{2}u^2_{\lceil \frac{n}{2} \rceil 1} + * & * & * & \cdots & * & * & * & \cdots & * & -u_{21} & 1
\end{bmatrix} \tag{10}$$

when n is odd, and

$$\begin{bmatrix}
1 & & & & & & & & & & & \\
u_{21} & 1 & & & & & & & & & & \\
u_{31} & u_{32} & 1 & & & & & & & & & \\
\vdots & \vdots & \vdots & \ddots & & & & & & & & \\
u_{(\frac{n-2}{2})1} & u_{(\frac{n-2}{2})2} & u_{(\frac{n-2}{2})3} & \cdots & 1 & & & & & & & \\
u_{\frac{n}{2}1} & u_{\frac{n}{2}2} & u_{\frac{n}{2}3} & \cdots & u_{\frac{n}{2}(\frac{n-2}{2})} & 1 & & & & & & \\
u_{(\frac{n+2}{2})1} & u_{(\frac{n+2}{2})2} & u_{(\frac{n+2}{2})3} & \cdots & u_{(\frac{n+2}{2})(\frac{n-2}{2})} & 0 & 1 & & & & & \\
u_{(\frac{n+4}{2})1} & u_{(\frac{n+4}{2})2} & u_{(\frac{n+4}{2})3} & \cdots & * & * & -u_{\frac{n}{2}(\frac{n-2}{2})} & 1 & & & & \\
\vdots & \vdots & \vdots & \iddots & \vdots & \vdots & \vdots & \vdots & \ddots & & & \\
u_{(n-2)1} & u_{(n-2)2} & * & \cdots & * & * & * & * & \cdots & 1 & & \\
u_{(n-1)1} & * & * & \cdots & * & * & * & * & \cdots & -u_{32} & 1 & \\
* & * & * & \cdots & * & * & * & * & \cdots & * & -u_{21} & 1
\end{bmatrix} \tag{11}$$

when n is even, where the $u_{ij} \in \mathbb{R}$ for $i \in \{2, \dots, n-1\}$ and $j \in \{1, \dots, \min\{i-1, n-i\}\}$ are free parameters, and where the symbol "$*$" is shorthand and should be read as follows: if the "$*$"

occurs in the row-i, column-j entry, then it denotes "some polynomial of positive degree in the variables $\{u_{i'j'} : i'-j' \le i-j\}$ with integer coefficients having no constant term" (the polynomial being abbreviated depends on the matrix entry in which it occurs). We often abbreviate the tuple $\big(u_{ij} : i \in \{2,\dots,n-1\},\ j \in \{1,\dots,\min\{i-1,n-i\}\}\big)$ by u, and we often abuse notation by writing u for the corresponding element of $\mathcal{N}$.

Let $\mathcal{A}$ denote the subgroup of diagonal matrices in $\mathrm{SO}_{A_0}(\mathbb{R})$, all of whose entries are positive. The elements of $\mathcal{A}$, which is a maximal torus of $\mathrm{SO}_{A_0}(\mathbb{R})$ normalizing the unipotent subgroup $\mathcal{N}$, admit the following explicit parametrization: the i^{th} diagonal entry is the reciprocal of the $(n-i)^{\text{th}}$, and the first $\lceil \frac{n}{2} \rceil$ diagonal entries can be expressed in the form

$$\prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} s_i^{-1},\ \prod_{i=2}^{\lfloor \frac{n}{2} \rfloor} s_i^{-1},\ \dots,\ s_{\lfloor \frac{n}{2} \rfloor}^{-1},\ 1, \qquad \text{if } n \text{ is odd}, \tag{12}$$

$$\sqrt{s_{\frac{n-2}{2}}^{-1} s_{\frac{n}{2}}^{-1}} \cdot \prod_{i=1}^{\frac{n-4}{2}} s_i^{-1},\ \sqrt{s_{\frac{n-2}{2}}^{-1} s_{\frac{n}{2}}^{-1}} \cdot \prod_{i=2}^{\frac{n-4}{2}} s_i^{-1},\ \dots,\ \sqrt{s_{\frac{n-2}{2}}^{-1} s_{\frac{n}{2}}^{-1}},\ \sqrt{s_{\frac{n-2}{2}} s_{\frac{n}{2}}^{-1}}, \qquad \text{if } n \text{ is even}, \tag{13}$$

where $s_i > 0$ for each i. For a given choice of $s_1,\dots,s_{\lfloor \frac{n}{2} \rfloor} > 0$, we often abbreviate the tuple $(s_1,\dots,s_{\lfloor \frac{n}{2} \rfloor})$ by s, and we often abuse notation by writing s for the corresponding element of $\mathcal{A}$.

Let K denote a maximal compact subgroup of $\mathrm{SO}_{A_0}(\mathbb{R})$; we denote elements of K by θ. Then, by [16, Théorème 2.4 and Exemple 2.5], there exists a constant $c_2 > 0$ and a compact set $\mathcal{N}' \subset \mathcal{N}$ such that if we take $\mathcal{A}' := \{s = (s_1,\dots,s_{\lfloor \frac{n}{2} \rfloor}) \in \mathcal{A} : s_i > c_2 \text{ for all } i\}$, then the set

$$\mathcal{S}_2 := \mathcal{N}' \cdot \mathcal{A}' \cdot \big((K \cap \{\pm \mathrm{id}\})\backslash K\big) \tag{14}$$

meets every orbit of $\mathrm{SO}_{A_0}(\mathbb{Z})$ on $\mathrm{SO}_{A_0}(\mathbb{R})$ (and hence every orbit of $\mathcal{G}_n(\mathbb{Z})$ on $\mathcal{G}_n(\mathbb{R})$) at least once, where $(K \cap \{\pm \mathrm{id}\})\backslash K$ denotes some strict fundamental domain for the action of the group $K \cap \{\pm \mathrm{id}\}$ by left-multiplication on K (where by "strict," we mean that every coset of $K \cap \{\pm \mathrm{id}\}$ has a unique representative).[6] We take the quotient of K by the subgroup $K \cap \{\pm \mathrm{id}\}$ because $\pm \mathrm{id}$ stabilizes every element of $\mathrm{SO}_{A_0}(\mathbb{R})/K$. The following lemma computes the stabilizer of a generic element of $\mathrm{SO}_{A_0}(\mathbb{R})/K$:

Lemma 14. *There exists an open subset $\mathcal{U}_2 \subset \mathrm{SO}_{A_0}(\mathbb{R})/K$ of full measure such that the stabilizer in $\mathrm{SO}_{A_0}(\mathbb{Z})$ of any $g \in \mathcal{U}_2$ is given by $K \cap \{\pm \mathrm{id}\}$.*

Proof. Let $\overline{\mathcal{F}}$ be any fundamental domain for the action of $\mathrm{SO}_{A_0}(\mathbb{Z})$ on $\mathrm{SO}_{A_0}(\mathbb{R})/K$, and let g be an element of the interior of $\overline{\mathcal{F}}$. If $\gamma \in \mathrm{SO}_{A_0}(\mathbb{Z})$ stabilizes g, then there is an open neighborhood $U \ni g$ contained in the interior of $\overline{\mathcal{F}}$ such that $\gamma \cdot U$ is contained in the interior of $\overline{\mathcal{F}}$, implying in fact that γ stabilizes every element of U. Since left-multiplication by γ defines a real-analytic function on $\mathrm{SO}_{A_0}(\mathbb{R})/K$, and since $\mathrm{SO}_{A_0}(\mathbb{R})/K$ is connected (as K meets both of the two connected components of $\mathrm{SO}_{A_0}(\mathbb{R})$), it follows that γ stabilizes all of $\mathrm{SO}_{A_0}(\mathbb{R})/K$.

Now, the stabilizer in $\mathrm{SO}_{A_0}(\mathbb{R})$ of any element $h \in \mathrm{SO}_{A_0}(\mathbb{R})/K$ is given by hKh^{-1}. Since γ stabilizes all of $\mathrm{SO}_{A_0}(\mathbb{R})/K$, it follows that $\gamma \in \mathcal{K} := \bigcap_{h \in \mathrm{SO}_{A_0}(\mathbb{R})} hKh^{-1}$. But because $\mathcal{K}$ is a compact normal subgroup of $\mathrm{SO}_{A_0}(\mathbb{R})$, it follows that $\mathcal{K}$ is discrete. Let $\mathcal{K}^+$ denote the intersection of $\mathcal{K}$ with the identity component $\mathrm{SO}_{A_0}(\mathbb{R})^+$ of $\mathrm{SO}_{A_0}(\mathbb{R})$. Then $\mathcal{K}^+$ is a discrete normal subgroup of the connected group $\mathrm{SO}_{A_0}(\mathbb{R})^+$, and so $\mathcal{K}^+$ is central in $\mathrm{SO}_{A_0}(\mathbb{R})^+$. It follows that $\mathcal{K}^+ \subset \{\pm \mathrm{id}\}$, and hence that $\mathcal{K}^+$ is central in $\mathrm{SO}_{A_0}(\mathbb{R})$. If $\gamma' \in \mathcal{K} \smallsetminus \mathcal{K}^+$, then γ' commutes with elements of both connected components of $\mathrm{SO}_{A_0}(\mathbb{R})$, so γ' is central in $\mathrm{SO}_{A_0}(\mathbb{R})$ since $\mathcal{K}$ is normal. Thus, we have that $\mathcal{K} \subset \{\pm \mathrm{id}\}$, and so $\gamma = \pm \mathrm{id}$.

[6] *A priori*, [16, Théorème 2.4] states that a finite number σ of translates of Siegel sets can be found such that their union meets every orbit of $\mathrm{SO}_{A_0}(\mathbb{Z})$ on $\mathrm{SO}_{A_0}(\mathbb{R})/K$ at least once; here, $\sigma = \#\big(\mathrm{SO}_{A_0}(\mathbb{Z})\backslash \mathrm{SO}_{A_0}(\mathbb{Q})/\mathcal{P}(\mathbb{Q})\big)$, where $\mathcal{P}(\mathbb{Q}) = (\mathcal{N}\cdot\mathcal{A}) \cap \mathrm{SO}_{A_0}(\mathbb{Q})$. But since the algebraic group SO_{A_0} has class number 1, it follows from [33, Propositions 5.4 and 5.10] that $\sigma = 1$.

Finally, let $\mathcal{U}_2$ to be the union of all $\mathrm{SO}_{A_0}(\mathbb{Z})$-translates of the interior of $\overline{\mathcal{F}}$. Then $\mathcal{U}_2$ is an open subset of full measure, and we have shown above that the stabilizer in $\mathrm{SO}_{A_0}(\mathbb{Z})$ of any $g \in \mathcal{U}_2$ is contained in $\{\pm \mathrm{id}\}$, as desired. □

We now make a convenient explicit choice of the compact set $\mathcal{N}'$. Let $\overline{\mathcal{N}} \subset \mathcal{N}$ be the subset defined as follows:

$$\overline{\mathcal{N}} := \begin{cases} \{u \in \mathcal{N} : |u_{ij}| \leq 1 \text{ for } i = \lceil \frac{n}{2} \rceil,\ |u_{ij}| \leq \frac{1}{2} \text{ for } i \neq \lceil \frac{n}{2} \rceil\}, & \text{if } n \text{ is odd,} \\ \{u \in \mathcal{N} : |u_{ij}| \leq \frac{1}{2} \text{ for all } i, j\}, & \text{if } n \text{ is even.} \end{cases}$$

The following result implies that by chopping $\mathcal{N}'$ into pieces and translating them via elements of $\mathcal{N} \cap \mathrm{SO}_{A_0}(\mathbb{Z})$, we can replace $\mathcal{N}'$ with a subset of $\overline{\mathcal{N}}$:

Lemma 15. *Let $u \in \mathcal{N}$. Then there exists $\overline{u} \in \mathcal{N} \cap \mathrm{SO}_{A_0}(\mathbb{Z})$ such that $\overline{u}u \in \overline{\mathcal{N}}$. Moreover, there exists an open subset $\mathcal{U}_3 \subset \mathcal{N}$ of full measure such that for any $u \in \mathcal{U}_3$, there is precisely one element $\overline{u} \in \mathcal{N} \cap \mathrm{SO}_{A_0}(\mathbb{Z})$ such that $\overline{u}u \in \overline{\mathcal{N}}$.*

Proof. We construct $\overline{u}$ inductively. Upon inspecting the characterization of elements of $\mathcal{N}$ provided earlier in this section, we arrive at the following observation: if $k \in \{0, \dots, n-3\}$ is an integer and $u' \in \mathcal{N}$ is an element such that $u'_{ij} = 0$ for all i, j such that $i - j \leq k$, then $(u'u)_{ij} = u'_{ij} + u_{ij}$ for all i, j such that $i - j = k + 1$. By the observation, we may choose $u_1 \in \mathcal{N} \cap \mathrm{SO}_{A_0}(\mathbb{Z})$ such that $\left|(u_1)_{i(i-1)} + u_{i(i-1)}\right| \leq \frac{1}{2}$ for each $i \in \{2, \dots, \lfloor \frac{n}{2} \rfloor\}$ and such that, for n odd, we have $\left|(u_1)_{\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor} + u_{\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor}\right| \leq 1$. Suppose for some $k \in \{0, \dots, n-4\}$ we have chosen $u_\ell \in \mathcal{N} \cap \mathrm{SO}_{A_0}(\mathbb{Z})$ for each $\ell \in \{1, \dots, k+1\}$; then, by the observation, we may choose $u_{k+2} \in \mathcal{N} \cap \mathrm{SO}_{A_0}(\mathbb{Z})$ such that $\left|(u_1)_{i(i-k-2)} + u_{i(i-k-2)}\right| \leq \frac{1}{2}$ for each $i \in \{k+3, \dots, \lfloor \frac{n+k+2}{2} \rfloor\}$, unless n is odd and $i = \lceil \frac{n}{2} \rceil$, in which case we can only arrange for $\left|(u_1)_{\lceil \frac{n}{2} \rceil (\lceil \frac{n}{2} \rceil - k - 2)} + u_{\lceil \frac{n}{2} \rceil (\lceil \frac{n}{2} \rceil - k - 2)}\right| \leq 1$. Having constructed u_ℓ for each $\ell \in \{1, \dots, n-2\}$, we then take $\overline{u} = \prod_{\ell=1}^{n-2} u_{n-2-\ell}$.

As for uniqueness on an open subset of full measure, it suffices to show that $\overline{u}$ is unique when u lies in the interior of $\overline{\mathcal{N}}$, for then we can take $\mathcal{U}_3$ to be the union of all $(\mathcal{N} \cap \mathrm{SO}_{A_0}(\mathbb{Z}))$-translates of the interior of $\overline{\mathcal{N}}$. So take $u \in \overline{\mathcal{N}}$. If $\overline{u}u \in \overline{\mathcal{N}}$ for some $\overline{u} \in \mathcal{N} \cap \mathrm{SO}_{A_0}(\mathbb{Z})$, then the aforementioned observation, together with the fact that u lies in the interior of $\overline{\mathcal{N}}$, implies that $\overline{u}_{i(i-1)} = 0$ for each i. Proceeding inductively as we did to prove existence, we find that $\overline{u} = \mathrm{id}$. □

By Lemma 15, we may assume that $\mathcal{N}' \subset \overline{\mathcal{N}}$. We next show that $\mathcal{N}'$ can be chosen to lie within an even smaller subset of $\overline{\mathcal{N}}$. Let $G \subset \mathrm{SO}_{A_0}(\mathbb{Z})$ denote the subgroup of diagonal matrices with integer entries. One readily verifies that G satisfies the following properties:

- G is a subgroup of K of order $2^{\lfloor \frac{n}{2} \rfloor}$ centralizing the maximal torus $\mathcal{A}$;
- Conjugation by elements of G defines a group action on $\overline{\mathcal{N}}$ with the property that for any $\rho \in G$ and $u \in \overline{\mathcal{N}}$, we have $|(\rho \cdot u)_{ij}| = |u_{ij}|$ for all i, j; and
- The orbit of every element of $\overline{\mathcal{N}}$ under the action of G has a representative u such that for every n we have $u_{i(i-1)} \in [0, \frac{1}{2}]$ for each $i \in \{2, \dots, \lfloor \frac{n}{2} \rfloor\}$ and such that for odd n we have $u_{\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor} \in [-1, -\frac{1}{2}] \cup [0, \frac{1}{2}]$. The representative u is unique if each u_{ij} lies in the interior of the corresponding interval or union of intervals.

It follows that we can take $\mathcal{N}'$ to lie within the subset

$$\widetilde{\mathcal{N}} := \{u \in \overline{\mathcal{N}} : u_{i(i-1)} \in [0, \tfrac{1}{2}] \text{ for each } i \in \{2, \dots, \lfloor \tfrac{n}{2} \rfloor\};\ u_{\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor} \in [-1, -\tfrac{1}{2}] \cup [0, \tfrac{1}{2}] \text{ for odd } n\}.$$

By possibly expanding $\mathcal{N}'$, we may in fact choose $\mathcal{N}'$ to be equal to $\widetilde{\mathcal{N}}$.

We now construct $\mathcal{S}_1$. Let $\mathcal{A}'' := \{s \in \mathcal{A} : s_i > c_1 \text{ for all } i\}$, where the constant $c_1 > 0$ is to be chosen shortly. We then take

$$\mathcal{S}_1 = \mathcal{N}' \cdot \mathcal{A}'' \cdot \big((K \cap \{\pm \mathrm{id}\}) \backslash K\big).$$

It is evident that $\mathcal{S}_1$ and $\mathcal{S}_2$ differ on an absolutely bounded set. The following proposition states that we can choose c_1 so that $\mathcal{S}_1$ satisfies the remaining desired properties:

Proposition 16. *There exists a constant $c_1 > 0$ for which (1) $\mathcal{S}_1 \subset \mathcal{S}_2$ and (2) there exists an open subset $\mathcal{U}_1 \subset \mathcal{S}_1$ of full measure such that every orbit of $\mathrm{SO}_{A_0}(\mathbb{Z})$ on $\mathrm{SO}_{A_0}(\mathbb{R})$ meets $\mathcal{U}_1$ at most once.*

Proof. In [27], Grenier constructs an explicit fundamental domain $\mathscr{F}$ for the action of $\mathrm{SL}_n^{\pm}(\mathbb{Z})$ on $\mathrm{SL}_n^{\pm}(\mathbb{R})$ that has a so-called "box shape" at infinity, meaning that, in a neighborhood of infinity, $\mathscr{F}$ is nothing but a Siegel set. We shall deduce Proposition 16 from a slight reformulation of Grenier's result. To state this reformulation, we must introduce some notation. Let $\mathscr{N} \subset \mathrm{SL}_n^{\pm}(\mathbb{R})$ denote the subgroup of lower-triangular unipotent matrices; for an element $u \in \mathscr{N}$, we denote by u_{ij} the row-i, column-j entry of u. Let $\overline{\mathscr{N}}$ be the set defined by

$$\overline{\mathscr{N}} := \{u \in \mathscr{N} : |u_{ij}| \leq \tfrac{1}{2} \text{ for all } i, j\}$$

Let $\mathscr{A} \subset \mathrm{SL}_n^{\pm}(\mathbb{R})$ denote the subgroup of diagonal matrices with positive entries; for an element $s \in \mathscr{A}$, we denote by s_i the quotient of the row-$(i+1)$, column-$(i+1)$ entry of s by the row-i, column-i entry. Let $\mathscr{K} \subset \mathrm{SL}_n^{\pm}(\mathbb{R})$ denote a maximal compact subgroup containing K.

Consider the subset $\mathscr{N}' \subset \overline{\mathscr{N}}$ defined as follows:

$$\mathscr{N}' := \left\{ u \in \overline{\mathscr{N}} : \begin{array}{c} u_{i(i-1)} \in [0, \frac{1}{2}] \text{ for each } i \in \{2, \dots, \lceil \frac{n}{2} \rceil\}; \\ u_{i(i-1)} \in [-\frac{1}{2}, 0] \text{ for each } i \in \{\lceil \frac{n}{2} \rceil + 2, \dots, n\}; \\ u_{(\lceil \frac{n}{2} \rceil + 1)\lceil \frac{n}{2} \rceil} \in [-\frac{1}{2}, 0] \text{ if } n \text{ is odd, } u_{(\frac{n+2}{2})\frac{n}{2}} \in [-\frac{1}{2}, \frac{1}{2}] \text{ if } n \text{ is even} \end{array} \right\}$$

Let $\mathscr{A}' := \{s \in \mathscr{A} : s_i > c_1 \text{ for all } i\}$ for a sufficiently large constant $c_1 > c_2$. Let $\varepsilon_n \in \mathscr{K}$ denote the identity matrix when n is odd, and the diagonal matrix whose diagonal entries are given by $\frac{n}{2}$ copies of -1 followed by $\frac{n}{2}$ copies of 1 when n is even, and let $\{\pm \mathrm{id}, \pm\varepsilon_n\}\backslash\mathscr{K}$ denote some strict fundamental domain for the action of the group $\{\pm \mathrm{id}, \pm\varepsilon_n\}$ by left-multiplication on K.

We are now in position to state our reformulation of Grenier's result:

Lemma 17. *For every sufficiently large $c_1 > 0$, the following property holds: If*

$$us\theta, u's'\theta' \in \mathscr{N}' \cdot \mathscr{A}' \cdot (\{\pm \mathrm{id}, \pm\varepsilon_n\}\backslash\mathscr{K})$$

are $\mathrm{SL}_n^{\pm}(\mathbb{Z})$-equivalent elements such that $s_i, s_i' > c_1$ for all i and such that u, u' lie in the interior of $\mathscr{N}'$, then $us\theta = u's'\theta'$.

Proof of Lemma 17. In [26], Grenier constructs a fundamental domain $\overline{\mathscr{F}} \subset \mathscr{N} \cdot \mathscr{A}$ for the action of $\mathrm{SL}_n^{\pm}(\mathbb{Z})$ on $\mathrm{SL}_n^{\pm}(\mathbb{R})/\mathscr{K}$. The domain $\overline{\mathscr{F}}$ has the property that no two points in its interior are $\mathrm{SL}_n^{\pm}(\mathbb{Z})$-equivalent. In [27, Theorem 1], Grenier establishes that, for every sufficiently large $c_1 > 0$, we have $\mathscr{N}'' \cdot \mathscr{A}' \subset \overline{\mathscr{F}}$, where $\mathscr{N}'' = \{u \in \mathscr{N}' : u_{(\frac{n+2}{2})\frac{n}{2}} \in [0, \frac{1}{2}]\}$. Consequently, the set $\overline{\mathscr{F}} \cdot (\{\pm \mathrm{id}\}\backslash\mathscr{K})$ is a fundamental domain for the action of $\mathrm{SL}_n^{\pm}(\mathbb{Z})$ on $\mathrm{SL}_n^{\pm}(\mathbb{R})$ containing $\mathscr{N}'' \cdot \mathscr{A}' \cdot (\{\pm \mathrm{id}\}\backslash\mathscr{K})$. Since $\varepsilon_n \cdot \mathscr{N}'' \cdot \varepsilon_n = \mathscr{N}'$, it follows that there is a fundamental domain for the action of $\mathrm{SL}_n^{\pm}(\mathbb{Z})$ on $\mathrm{SL}_n^{\pm}(\mathbb{R})$ containing $\mathscr{N}' \cdot \mathscr{A}' \cdot (\{\pm \mathrm{id}, \pm\varepsilon_n\}\backslash\mathscr{K})$. If we have two distinct $\mathrm{SL}_n^{\pm}(\mathbb{Z})$-equivalent elements $us\theta, u's'\theta' \in \mathscr{N}' \cdot \mathscr{A}' \cdot (\{\pm \mathrm{id}, \pm\varepsilon_n\}\backslash\mathscr{K})$ such that u, u' lie in the interior of $\mathscr{N}'$, then one can find two distinct elements of the interior of $\overline{\mathscr{F}}$ that are $\mathrm{SL}_n^{\pm}(\mathbb{Z})$-equivalent, which is a contradiction. □

We now deduce Proposition 16 from Lemma 17. Let $\mathcal{U}_1$ be an open subset of full measure contained in the interior of $\mathcal{S}_1$ consisting of elements $us\theta$ satisfying the following two properties:

- The image of $us\theta$ in $\mathrm{SO}_{A_0}(\mathbb{R})/K$ lies in $\mathcal{U}_2$; and
- There exists a unique element $u_0 \in \mathscr{N} \cap \mathrm{SL}_n^{\pm}(\mathbb{Z})$ such that $u_0 u$ lies in the interior of $\mathscr{N}'$.

To see why we can arrange for the second property above to hold on a open subset of full measure, observe that by the definitions of $\mathcal{N}'$ and $\mathscr{N}'$, the desired element u_0 must be such that $(u_0)_{i(i-1)} = 0$ for each i. Then, by proving the analogue of Lemma 15 for the group $\mathrm{SL}_n^{\pm}$, one finds that there

exists at least one $u_0 \in \mathscr{N} \cap \mathrm{SL}_n^{\pm}(\mathbb{Z})$ such that $u_0 u \in \mathscr{N}'$. By our explicit characterization of the elements of $\mathcal{N}$ (see (10) and (11)), the row-i, column-j entry of u is a non-constant polynomial in the unipotent coordinates for every pair (i,j) with $i > j+1$. Thus, there exists an open subset $\mathcal{U}_3 \subset \mathcal{N}$ of full measure such that for any $u \in \mathcal{U}_3$ and $u_0 \in \mathscr{N} \cap \mathrm{SL}_n^{\pm}(\mathbb{Z})$, the row-$i$, column-$j$ entry of $u_0 u$ is not an integer multiple of $\frac{1}{2}$ for every pair (i,j) with $i > j$, unless $i+1 = j = \frac{n}{2}$, in which case $u_{ij} = 0$. In particular, if for $u \in \mathcal{U}_3$ and $u_0 \in \mathscr{N} \cap \mathrm{SL}_n^{\pm}(\mathbb{Z})$ we have $u_0 u \in \mathscr{N}'$, then $u_0 u$ must in fact lie in the interior of $\mathscr{N}'$, and imitating the proof of uniqueness in Lemma 15 yields that u_0 must be unique.

Having defined $\mathcal{U}_1$, take any $us\theta, u's'\theta' \in \mathcal{U}_1$ such that $g \cdot us\theta = u's'\theta'$ for some $g \in \mathrm{SO}_{A_0}(\mathbb{Z})$. Let $\varepsilon, \varepsilon' \in \{\pm \mathrm{id}, \pm\varepsilon_n\}$ be such that $\varepsilon\theta, \varepsilon'\theta' \in \{\pm \mathrm{id}, \pm\varepsilon_n\} \backslash \mathscr{K}$. Let $u_0, u_0' \in \mathscr{N} \cap \mathrm{SL}_n^{\pm}(\mathbb{Z})$ be the unique elements such that $u_0(\varepsilon u \varepsilon), u_0'(\varepsilon' u' \varepsilon')$ lie in the interior of $\mathscr{N}'$. Since $s_i, s_i' > c_1$ for all i, it follows from Lemma 17 that $u_0(\varepsilon u \varepsilon) s(\varepsilon\theta) = u_0'(\varepsilon' u' \varepsilon') s'(\varepsilon'\theta')$. By the uniqueness of the Iwasawa decomposition, we must have

$$u_0(\varepsilon u \varepsilon) = u_0'(\varepsilon' u' \varepsilon'), \quad s = s', \quad \varepsilon\theta = \varepsilon'\theta'. \tag{15}$$

The third equality in (15) implies that $\varepsilon\varepsilon' \in K$, so since $\varepsilon_n \notin K$ when n is even, it follows that $\varepsilon\varepsilon' = \pm\mathrm{id}$. But $(K \cap \{\pm\mathrm{id}\}) \backslash K$ contains either θ of $-\theta$ and not both, meaning that $\varepsilon\varepsilon' = \mathrm{id}$. Combining this with the first equality in (15) yields that u is a translate of u' by an element of $\mathscr{N} \cap \mathrm{SL}_n^{\pm}(\mathbb{Z})$, and hence by an element of $\mathcal{N} \cap \mathrm{SO}_{A_0}(\mathbb{Z})$. The uniqueness statement in Lemma 15 then implies that $u = u'$. We conclude that $us\theta = us'\theta'$.

This completes the proof of Proposition 16. □

3.3. **Fundamental sets for $\mathcal{G}_n(\mathbb{R}) \curvearrowright W_{n,f_1}(\mathbb{R})$ and $\mathcal{G}_n(\mathbb{Z}) \curvearrowright W_{n,f_1}(\mathbb{R})$.** From §2.2–2.3, we know that there is one reducible $B \in W_{n,f_1}(\mathbb{R})$ up to the action of $\mathcal{G}_n(\mathbb{R})$ with $\mathrm{inv}(x \cdot A_0 + z \cdot B) = F(x,z)$ for each nondegenerate $F \in U_n(\mathbb{R})$. An explicit representative of this orbit is given as follows. Take any $f = (f_2, \dots, f_n) \in \mathbb{R}^{n-1}$, let $F(x,z) = x^n + \sum_{i=1}^n f_i x^{n-i} z^i$, and let

$$\widetilde{F}(x,z) = x^n + \sum_{i=2}^{n} \widetilde{f}_i x^{n-i} z^i \in \mathbb{R}[x,z] \tag{16}$$

denote the unique $N(\mathbb{R})$-translate of F with $x^{n-1}z$-coefficient equal to 0. If we define a function $\sigma_0 \colon \mathbb{R}^{n-1} \to W_{n,f_1}(\mathbb{R})$ by

$$\sigma_0(f) := \frac{f_1}{n} \cdot A_0 + \begin{bmatrix} & & & & & & & 1 & 0 \\ & & & & & & \iddots & 0 & \\ & & & & & 1 & & & \\ & & & & 1 & 0 & & & \\ & & & 1 & 0 & -\frac{\widetilde{f}_2}{2} & & & \\ & & 1 & 0 & -\frac{\widetilde{f}_2}{2} & -\widetilde{f}_3 & \ddots & & \\ & \iddots & & & & \ddots & \ddots & -\frac{\widetilde{f}_{n-3}}{2} & \\ 1 & 0 & & & & & -\frac{\widetilde{f}_{n-3}}{2} & -\widetilde{f}_{n-2} & -\frac{\widetilde{f}_{n-1}}{2} \\ 0 & & & & & & & -\frac{\widetilde{f}_{n-1}}{2} & -\widetilde{f}_n \end{bmatrix}$$

if n is odd, and by

$$\sigma_0(f) := \frac{f_1}{n}\cdot A_0 + \begin{bmatrix} & & & & & & & & 1 & 0 \\ & & & & & & & \iddots & 0 & \\ & & & & & & 1 & & & \\ & & & & & 1 & 0 & & & \\ & & & & 1 & 0 & & & & \\ & & & 1 & 0 & -\widetilde{f}_2 & -\frac{\widetilde{f}_3}{2} & & & \\ & & 1 & 0 & & -\frac{\widetilde{f}_3}{2} & -\widetilde{f}_4 & \ddots & & \\ & \iddots & & & & & \ddots & \ddots & -\frac{\widetilde{f}_{n-3}}{2} & \\ 1 & 0 & & & & & & -\frac{\widetilde{f}_{n-3}}{2} & -\widetilde{f}_{n-2} & -\frac{\widetilde{f}_{n-1}}{2} \\ 0 & & & & & & & & -\frac{\widetilde{f}_{n-1}}{2} & -\widetilde{f}_n \end{bmatrix}$$

if n is even, then $\mathrm{inv}(x\cdot A_0 + z\cdot\sigma_0(f)) = F(x,z)$. The explicit section σ_0 is useful in the proof of Proposition 24 (to follow) because its image consists of matrices whose entries are polynomials in the f_i. However, in Lemma 20 (also to follow), we shall require a section σ with image consisting of matrices whose entries are $O(X)$ if $\mathrm{H}(F) \ll X$. To this end, let $f \in \mathbb{R}^{n-1}$ be as above, and let $j \in \{2,\dots,n\}$ be any index such that $\max\{|\widetilde{f}_i|^{\frac{1}{i}} : i \in \{2,\dots,n\}\} = |\widetilde{f}_j|^{\frac{1}{j}}$. If we define

$$\sigma(f_2,\dots,f_n) := \frac{f_1}{n}\cdot A_0 + |\widetilde{f}_j|^{\frac{1}{j}}\cdot\sigma_0\big(\widetilde{f}_2\cdot|\widetilde{f}_j|^{-\frac{2}{j}},\dots,\widetilde{f}_n\cdot|\widetilde{f}_j|^{-\frac{n}{j}}\big),$$

then $\mathrm{inv}(x\cdot A_0 + z\cdot\sigma(f_2,\dots,f_n)) = F(x,z)$.

For each $r_1 \in \{1,3,\dots,n\}$ if n is odd and $r_1 \in \{0,2,\dots,n\}$ if n is even, write

$$W_{n,f_1}^{(r_1)}(\mathbb{R}) := \big\{B \in W_{n,f_1}(\mathbb{R}) :\ \mathrm{inv}(x\cdot A_0 + z\cdot B) \text{ has nonzero disc. and } r_1 \text{ real roots}\big\}$$

and let $W_{n,f_1}^{(r_1)}(\mathbb{Z}) := W_n(\mathbb{Z}) \cap W_{n,f_1}^{(r_1)}(\mathbb{R})$. Let $L_{f_1}^{(r_1)}$ be the fundamental set for the action of $\mathcal{G}_n(\mathbb{R})$ on $W_{n,f_1}^{(r_1)}(\mathbb{R})$ defined by

$$L_{f_1}^{(r_1)} := \left\{\sigma(f) : f = (f_2,\dots,f_n) \in \mathbb{R}^{n-1},\ x^n + \sum_{i=1}^{n} f_i x^{n-i}z^i \text{ has nonzero disc. and } r_1 \text{ real roots}\right\}$$

From the stabilizer statement in Theorem 6, it follows that $\#\,\mathrm{Stab}_{\mathcal{G}_n(\mathbb{R})}(B)$ is independent of the choice of $B \in W_{n,f_1}^{(r_1)}(\mathbb{R})$; letting $n_{r_1} := \#\,\mathrm{Stab}_{\mathcal{G}_n(\mathbb{R})}(B)$ for any $B \in W_{n,f_1}^{(r_1)}(\mathbb{R})$, one readily verifies that $n_{r_1} = 2^{\frac{n+r_1-2}{2}}$ if n is odd and $n_{r_1} = 2^{\frac{n+r_1}{2}}$ if n is even.

We are finally in position to construct a fundamental set for the action of $\mathcal{G}_n(\mathbb{Z})$ on $W_{n,f_1}(\mathbb{R})$. For each possible value of r_1 and f_1, we simply take our fundamental set to be the multiset $\mathcal{F}\cdot L_{f_1}^{(r_1)}$. Note that if $B \in (\mathcal{F}\cdot L_{f_1}^{(r_1)}) \cap W_{n,f_1}(\mathbb{Z})$, then B occurs with multiplicity $n_{r_1}/\#\,\mathrm{Stab}_{\mathcal{G}_n(\mathbb{Z})}(B)$.

4. Counting reducible $\mathcal{G}_n(\mathbb{Z})$-orbits on $W_n(\mathbb{Z})$

Let $n \geq 3$, and fix positive integers f_1 and r_1.[7] In this section, we obtain asymptotics for the number of reducible orbits of $\mathcal{G}_n(\mathbb{Z})$ on $W_{n,f_1}^{(r_1)}(\mathbb{Z})$ of bounded height. We express these asymptotics in terms of a weighted volume of sets in $W_n(\mathbb{R})$. To state the main result of this section, and to simplify the exposition in the rest of the paper, we introduce the following pieces of notation:

- For any $\mathcal{G}_n(\mathbb{Z})$-invariant subset $S \subset W_n^{(r_1)}(\mathbb{Z})$, let $S_{\mathrm{red}} \subset S$ denote the subset of reducible elements of S, and for a real number $X > 0$, let $S_X := \{B \in S : \mathrm{H}(B) < X\}$.

[7]Note that definitions of quantities introduced in the rest of the paper may implicitly depend on r_1.

- Let $S_0 \subset S_{\mathrm{red}}$ denote the subset of reducible elements $B = [b_{ij}]$ satisfying the criterion for reducibility given in Proposition 11 — i.e., that $b_{ij} = 0$ for all (i,j) with $i + j \leq n-1$.
- Let dB denote Euclidean measure on $W_n(\mathbb{R})_0$, and we define $\lambda(B)$ by

$$\lambda(B) := \begin{cases} \displaystyle\prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} |b_{i(n-i)}(B)|^{2i-1}, & \text{if } n \text{ is odd,} \\ \displaystyle |b_{\frac{n}{2}\frac{n}{2}}(B)|^{\frac{n-2}{2}} \prod_{i=1}^{\frac{n-2}{2}} |b_{i(n-i)}(B)|^{2i-1}, & \text{if } n \text{ is even.} \end{cases}$$

- Let $H \subset \mathcal{G}_n(\mathbb{R})$ be any left-K-invariant set that is the closure of a nonempty open bounded set (so that in particular, H is compact). Define the set $\mathcal{B}$ by

$$\mathcal{B} := \big\{ B \in H \cdot L_{f_1}^{(r_1)} \cap W_n(\mathbb{R})_0 : b_{i(n-i)} > 0 \text{ for each } i \in \{1, \dots, \lfloor \tfrac{n}{2} \rfloor\} \big\}.$$

- Choose the following Haar measure on $\mathcal{G}_n(\mathbb{R})$:

$$dg = d\theta du(\delta(s)ds), \text{ where } du := \prod_{i=1}^{\lceil \frac{n}{2} \rceil} \prod_{j=1}^{i-1} du_{ij}, \ ds := \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} ds_i, \text{ and} \tag{17}$$

$$\delta(s) := \begin{cases} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} s_i^{\,i^2 - 2i\lfloor \frac{n}{2} \rfloor - 1}, & \text{if } n \text{ is odd,} \\ \big(s_{\frac{n-2}{2}} s_{\frac{n}{2}}\big)^{-\frac{n^2-2n+8}{8}} \prod_{i=1}^{\frac{n-4}{2}} s_i^{\,i^2 - i(n-1) - 1}, & \text{if } n \text{ is even,} \end{cases}$$

  where $d\theta$ is normalized so that $\int_{\theta \in (K \cap \{\pm \mathrm{id}\}) \backslash K} d\theta = 1$.
- Let dh denote the restriction of dg to H. We define the quantity C_X by

$$C_X := \frac{1}{\int_{h \in H} dh} \cdot \int_{B \in \mathcal{B}_X} \lambda(B) dB,$$

- For a finite set Σ of $(N \times \mathcal{G}_n)(\mathbb{Z})$-orbits (or $\mathcal{G}_n(\mathbb{Z})$-orbits) on $W_n(\mathbb{Z})$, let $\sharp\Sigma$ be the number of elements of Σ, where each $B \in \Sigma$ is counted with weight $1/\#\operatorname{Stab}_{\mathcal{G}_n(\mathbb{Z})}(B)$ if n is odd and with weight $2/\#\operatorname{Stab}_{\mathcal{G}_n(\mathbb{Z})}(B)$ if n is even.

Then, over the course of the next two subsections, we prove the following result:

Theorem 18. *We have that*

$$\sharp\left(\frac{(W_{n,f_1}^{(r_1)}(\mathbb{Z})_{\mathrm{red}})_X}{\mathcal{G}_n(\mathbb{Z})} \right) = \frac{1}{n_{r_1}} \cdot \left\{ \begin{array}{l} 2^{\lfloor \frac{n}{2} \rfloor} \displaystyle\prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \zeta(2i), \quad \textit{if } n \textit{ is odd,} \\ 4\zeta(\frac{n}{2}) \displaystyle\prod_{i=1}^{\frac{n-2}{2}} \zeta(2i), \ \textit{if } n \textit{ is even} \end{array} \right\} \cdot C_X + o\big(X^{\frac{n^2+n-2}{2}}\big). \tag{18}$$

4.1. **Averaging over fundamental domains.** In this section, we apply Bhargava's technique for averaging over fundamental domains to put the left-hand side of (18) into a more convenient form.

Let $\mathcal{F}$ be a fundamental domain for the action of $\mathcal{G}_n(\mathbb{Z})$ on $\mathcal{G}_n(\mathbb{R})$ that is box-shaped at infinity (recall that such an $\mathcal{F}$ exists by Theorem 12). For any given $h \in H$, we have that

$$\sharp\left(\frac{(W_{n,f_1}^{(r_1)}(\mathbb{Z})_{\mathrm{red}})_X}{\mathcal{G}_n(\mathbb{Z})} \right) = \begin{cases} \frac{1}{n_{r_1}} \cdot \#\big(\mathcal{F}h \cdot L_{f_1}^{(r_1)} \cap (W_n(\mathbb{Z})_{\mathrm{red}})_X\big), & \text{if } n \text{ is odd,} \\ \frac{2}{n_{r_1}} \cdot \#\big(\mathcal{F}h \cdot L_{f_1}^{(r_1)} \cap (W_n(\mathbb{Z})_{\mathrm{red}})_X\big), & \text{if } n \text{ is even.} \end{cases} \tag{19}$$

Letting $C_H = n_{r_1}\int_{h\in H} dh$ if n is odd and $C_H = \frac{n_{r_1}}{2}\int_{h\in H} dh$ if n is even, and averaging (19) over $h \in H$, we find that

$$\sharp\left(\frac{(W_{n,f_1}^{(r_1)}(\mathbb{Z})_{\mathrm{red}})_X}{\mathcal{G}_n(\mathbb{Z})}\right) = \frac{1}{C_H}\int_{h\in H} \#\big(\mathcal{F}h\cdot L_{f_1}^{(r_1)} \cap (W_n(\mathbb{Z})_{\mathrm{red}})_X\big)dh. \tag{20}$$

By [7, Proposition 10.7] when n is odd and [37, Proposition 23] when n is even,[8] the expected value of $\#\big(\mathcal{F}h\cdot L_{f_1}^{(r_1)} \cap (W_n(\mathbb{Z})_{\mathrm{red}} \smallsetminus W_n(\mathbb{Z})_0)_X\big)$ as $h \in H$ is drawn uniformly at random with respect to the measure dh is $o(X^{\frac{n^2+n-2}{2}})$.[9] Consequently, up to a negligible error, we may replace $W_n(\mathbb{Z})_{\mathrm{red}}$ in (20) with $W_n(\mathbb{Z})_0$. Then, using a now-standard change-of-variables argument due to Bhargava (see, e.g., [7, §10.1]), it follows that

$$\sharp\left(\frac{(W_{n,f_1}^{(r_1)}(\mathbb{Z})_{\mathrm{red}})_X}{\mathcal{G}_n(\mathbb{Z})}\right) = \frac{1}{C_H}\int_{g\in\mathcal{F}} \#\big(gH\cdot L_{f_1}^{(r_1)} \cap (W_n(\mathbb{Z})_0)_X\big)dg + o(X^{\frac{n^2+n-2}{2}}). \tag{21}$$

For $\bullet \in \{\mathcal{N}, \mathcal{A}\}$, consider the map $\pi_\bullet\colon \mathcal{G}_n(\mathbb{R}) \to \mathcal{A}$ obtained by post-composing the diffeomorphism $\mathcal{G}_n(\mathbb{R}) \to \mathcal{N}\times\mathcal{A}\times\mathcal{K}$ given by the Iwasawa decomposition with the projection map $\mathcal{N}\times\mathcal{A}\times\mathcal{K} \to \bullet$. Let $\mathcal{A}^\star := \pi_{\mathcal{A}}(\mathcal{F})$, and for each $s \in \mathcal{A}^\star$, let $\mathcal{N}^\star(s) := \pi_{\mathcal{N}}(\pi_{\mathcal{A}}^{-1}(s)\cap\mathcal{F})$; observe that $\mathcal{N}^\star(s)$ is bounded by construction. Then, setting $\mathcal{B}(u,s) := usH\cdot L_{f_1}^{(r_1)} \cap W_n(\mathbb{R})_0$ for the sake of convenience, we can rewrite the expression (21) as follows:

$$\begin{aligned}
&\sharp\left(\frac{(W_{n,f_1}^{(r_1)}(\mathbb{Z})_{\mathrm{red}})_X}{\mathcal{G}_n(\mathbb{Z})}\right) = \\
&\qquad \frac{1}{C_H}\int_{s\in\mathcal{A}^\star}\int_{u\in\mathcal{N}^\star(s)}\int_{\theta\in(K\cap\{\pm\mathrm{id}\})\backslash K} \#\big(us\theta H\cdot L_{f_1}^{(r_1)} \cap W_n(\mathbb{Z})_0)_X\big)d\theta du(\delta(s)ds) + o(X^{\frac{n^2+n-2}{2}}) = \\
&\qquad \frac{1}{C_H}\int_{s\in\mathcal{A}^\star}\int_{u\in\mathcal{N}^\star(s)} \#(\mathcal{B}(u,s)_X \cap W_n(\mathbb{Z}))du(\delta(s)ds) + o(X^{\frac{n^2+n-2}{2}}),
\end{aligned} \tag{22}$$

where the last step follows because $\theta H = H$ for each $\theta \in K$ and because $\int_{\theta\in(K\cap\{\pm\mathrm{id}\})\backslash K} d\theta = 1$.

4.2. **Slicing.** To evaluate (22), we now cut the region $\mathcal{B}(u,s)$ into slices, one for each possible value of the n-tuple $(b_{1(n-1)},\dots,b_{\lfloor\frac{n}{2}\rfloor\lceil\frac{n}{2}\rceil})$. For any $b = (b_1,\dots,b_{\lfloor\frac{n}{2}\rfloor}) \in (\mathbb{R}\smallsetminus\{0\})^{\lfloor\frac{n}{2}\rfloor}$, let $\mathcal{B}_b(u,s) \subset \mathcal{B}(u,s)$ be the subset of elements $B = [b_{ij}]$ such that $b_{i(n-i)} = b_i$ for each $i \in \{1,\dots,\lfloor\frac{n}{2}\rfloor\}$. Then we can express the integrand of (22) as follows:

$$\#(\mathcal{B}(u,s)_X \cap W_n(\mathbb{Z})) = \sum_{\substack{b\in\mathbb{Z}^{\lfloor\frac{n}{2}\rfloor}\\ b_i\neq 0\,\forall i}} \#(\mathcal{B}_b(u,s)_X \cap W_n(\mathbb{Z})), \tag{23}$$

By examining the action of s on an element $B = [b_{ij}] \in W_n(\mathbb{R})$, one readily verifies that if w_{ij} denotes the quantity by which s scales the matrix entry b_{ij} for each pair $(i,j) \in \{1,\dots,n\}^2$, then the following equalities hold:

$$w_{i(n-i)} = \begin{cases} s_i^{-1}, & \text{if } i \in \{1,\dots,\lfloor\frac{n}{2}\rfloor\}\smallsetminus\{\frac{n}{2}\},\\ s_{\frac{n-2}{2}}s_{\frac{n}{2}}{}^{-1}, & \text{if } i = \frac{n}{2}, \end{cases} \tag{24}$$

[8] Technically, [7, Proposition 10.7] and [37, Proposition 23] are stated in the case where $f_1 = 0$ and for a differently normalized height, but one readily verifies that their proofs go through for any fixed $f_1 \in \mathbb{Z}$ and for the height H.

[9] We note that this bound can be improved to $O_\epsilon(X^{\frac{n^2+n-2}{2}-\frac{1}{5}+\epsilon})$ by an application of the Selberg sieve (see [13, Proofs of Propositions 3.5 and 4.4]).

$$\prod_{i=1}^{n}\prod_{j=\max\{j,n+1-j\}}^{n} w_{ij} = \begin{cases} \prod_{i=1}^{\lfloor \frac{n}{2}\rfloor} s_i^{-i^2+2i(\lfloor \frac{n}{2}\rfloor+1)}, & \text{if } n \text{ is odd,} \\ s_{\frac{n-2}{2}}^{\frac{n^2+2n-16}{8}} s_{\frac{n}{2}}^{\frac{n^2+2n}{8}} \prod_{i=1}^{\frac{n-4}{2}} s_i^{-i^2+i(n+1)}, & \text{if } n \text{ is even.} \end{cases} \tag{25}$$

In order to count lattice points in the set $\mathcal{B}_b(u,s)_X$, we use the following result due to Davenport.

Proposition 19 ([20, Theorem])**.** *Let $\mathcal{R}$ be a bounded, semi-algebraic multiset in $\mathbb{R}^n$ having maximum multiplicity m that is defined by at most k polynomial inequalities, each having degree at most ℓ. Let $\mathcal{R}'$ denote the image of $\mathcal{R}$ under any (upper or lower) triangular, unipotent transformation of $\mathbb{R}^n$. Then the number of integer lattice points (counted with multiplicity) contained in the region $\mathcal{R}'$ is given by*

$$\mathrm{Vol}(\mathcal{R}) + O(\max\{\mathrm{Vol}(\overline{\mathcal{R}}), 1\}),$$

where $\mathrm{Vol}(\overline{\mathcal{R}})$ denotes the greatest d-dimensional volume of any projection of $\mathcal{R}$ onto a coordinate subspace obtained by equating $n-d$ coordinates to zero, where d ranges over all values in $\{1,\dots,n-1\}$. The implied constant in the second summand depends only on n, m, k, and ℓ.

Using Proposition 19 in conjunction with (25), it follows that the summand on the right-hand side of (23) can be expressed as

$$\#(\mathcal{B}_b(u,s)_X \cap W_n(\mathbb{Z})) = \mathrm{Vol}(\mathcal{B}_b(u,s)_X) + [\text{error}], \text{ where} \tag{26}$$

$$[\text{error}] = \begin{cases} O\left(X^{\lfloor \frac{n}{2}\rfloor^2+2\lfloor \frac{n}{2}\rfloor-1} \cdot \prod_{i=1}^{\lfloor \frac{n}{2}\rfloor} s_i^{-i^2+2i(\lfloor \frac{n}{2}\rfloor+1)}\right), & \text{if } n \text{ is odd,} \\ O\left(X^{\frac{n^2+2n-8}{4}} \cdot s_{\frac{n-2}{2}}^{\frac{n^2+2n-16}{8}} s_{\frac{n}{2}}^{\frac{n^2+2n}{8}} \prod_{i=1}^{\frac{n-4}{2}} s_i^{-i^2+i(n+1)}\right), & \text{if } n \text{ is even,} \end{cases}$$

where the implied constant is independent of b. Combining (22), (23), and (26) yields the following:

$$\sharp\left(\frac{(W_{n,f_1}^{(r_1)}(\mathbb{Z})_{\mathrm{red}})_X}{\mathcal{G}_n(\mathbb{Z})}\right) = \frac{1}{C_H} \sum_{\substack{b\in\mathbb{Z}^{\lfloor \frac{n}{2}\rfloor} \\ b_i\neq 0\,\forall i}} \left(\int_{s\in\mathcal{A}^\star} \int_{u\in\mathcal{N}^\star(s)} \mathrm{Vol}(\mathcal{B}_b(u,s)_X) du(\delta(s)ds) + \int_{s\in\mathcal{A}^\star} \int_{u\in\mathcal{N}^\star(s)} [\text{error}] du(\delta(s)ds) \right) + o(X^{\frac{n^2+n-2}{2}}). \tag{27}$$

The following lemma shows that the second term on the right-hand side of (27) is negligible:

Lemma 20. *The second term on the right-hand side of* (27) *is $o(X^{\frac{n^2+n-2}{2}})$.*

Proof. Combining (17) and (26) yields the following bound:

$$[\text{error}]\delta(s) \ll \begin{cases} X^{\lfloor \frac{n}{2}\rfloor^2+2\lfloor \frac{n}{2}\rfloor-1} \cdot \prod_{i=1}^{\lfloor \frac{n}{2}\rfloor} s_i^{2i-1}, & \text{if } n \text{ is odd,} \\ X^{\frac{n^2+2n-8}{4}} \cdot s_{\frac{n-2}{2}}^{\frac{n-6}{2}} s_{\frac{n}{2}}^{\frac{n-2}{2}} \prod_{i=1}^{\frac{n-4}{2}} s_i^{2i-1}, & \text{if } n \text{ is even.} \end{cases} \tag{28}$$

We next bound the ranges of $s_1,\dots,s_{\lfloor \frac{n}{2}\rfloor}$. By our construction of the section σ, we have that $b_{i(n-i)} \ll X$ for each i as $B=[b_{ij}]$ ranges through elements of $\mathcal{B}(0,1)_X$. Thus, for any fixed value of $b=(b_1,\dots,b_{\lfloor \frac{n}{2}\rfloor})$, the largest possible value of s_i such that $\mathcal{B}_b(u,s)_X \neq \varnothing$ is $O(X|b_i|^{-1})$ for each $i\in\{1,\dots,\lfloor \frac{n}{2}\rfloor\}$ when n is odd and for each $i\in\{1,\dots,\frac{n-2}{2}\}$ when n is even. If n is even and $i=\frac{n}{2}$, then one checks that the largest possible value of $s_{\frac{n}{2}}$ such that $\mathcal{B}_b(u,s)_X \neq \varnothing$ is $O(Xs_{\frac{n-2}{2}}|b_{\frac{n}{2}}|^{-1})$. Using these bounds together with the estimate (28) and bounding the integral over u by an absolute constant, we find that the second term on the right-hand side of (27) is

$$\ll X^{\lfloor \frac{n}{2}\rfloor^2+2\lfloor \frac{n}{2}\rfloor-1} \cdot \sum_{b\in(\mathbb{Z}_{>0})^{\lfloor \frac{n}{2}\rfloor}} \int_{\substack{s_i\in[c_2,O(Xb_i^{-1})] \\ i\in\{1,\dots,\lfloor \frac{n}{2}\rfloor\}}} \prod_{i=1}^{\lfloor \frac{n}{2}\rfloor} s_i^{2i-1} ds \tag{29}$$

$$\ll X^{2\lfloor \frac{n}{2}\rfloor^2+3\lfloor \frac{n}{2}\rfloor-1}\cdot \sum_{b\in(\mathbb{Z}_{>0})^{\lfloor \frac{n}{2}\rfloor}}\prod_{i=1}^{\lfloor \frac{n}{2}\rfloor} b_i^{-2i} \ll X^{\frac{n^2+n-4}{2}} = o(X^{\frac{n^2+n-2}{2}})$$

when n is odd, and

$$\begin{aligned}(30)\qquad &\ll X^{\frac{n^2+2n-8}{4}}\cdot \sum_{b\in(\mathbb{Z}_{>0})^{\frac{n}{2}}}\int_{\substack{s_i\in[c_2,O(Xb_i^{-1})]\\ i\in\{1,\dots,\frac{n-2}{2}\}}}\int_{s_{\frac{n}{2}}=c_2}^{O(Xs_{\frac{n-2}{2}}b_{\frac{n}{2}}^{-1})} s_{\frac{n-2}{2}}{}^{\frac{n-6}{2}} s_{\frac{n}{2}}{}^{\frac{n-2}{2}}\prod_{i=1}^{\frac{n-4}{2}} s_i^{2i-1}ds\\ &\ll X^{\frac{n^2+n-4}{2}}\cdot \sum_{b\in(\mathbb{Z}_{>0})^{\frac{n}{2}}} b_{\frac{n}{2}}{}^{-\frac{n}{2}}\cdot\prod_{i=1}^{\frac{n-2}{2}} b_i^{-2i} \ll X^{\frac{n^2+n-4}{2}} = o(X^{\frac{n^2+n-2}{2}})\end{aligned}$$

when n is even. □

Applying Lemma 20 to (27) yields that

$$(31)\quad \sharp\left(\frac{(W_{n,f_1}^{(r_1)}(\mathbb{Z})_{\mathrm{red}})_X}{\mathcal{G}_n(\mathbb{Z})}\right) = \frac{1}{C_H}\sum_{\substack{b\in\mathbb{Z}^{\lfloor \frac{n}{2}\rfloor}\\ b_i\neq 0\,\forall i}}\int_{s\in\mathcal{A}^\star}\int_{u\in\mathcal{N}^\star(s)}\mathrm{Vol}(\mathcal{B}_b(u,s)_X)du(\delta(s)ds) + o(X^{\frac{n^2+n-2}{2}}).$$

We now manipulate the integrand in (31) to extract its dependence on the slicing indices $b_1,\dots,b_{\lfloor \frac{n}{2}\rfloor}$. Because unipotent transformations leave volumes unchanged, we have that

$$(32)\qquad \mathrm{Vol}(\mathcal{B}_b(u,s)_X) = \mathrm{Vol}(\mathcal{B}_b(0,s)_X).$$

Thus, the integrand is independent of $u\in\mathcal{N}^\star(s)$, and so the integral over u gives a factor of $\mathrm{Vol}(\mathcal{N}^\star(s))$. By our construction of the box-shaped fundamental domain $\mathcal{F}$ in §3, we have the following equality for all $s\in\mathcal{A}^\star$ such that s_i is sufficiently large for each i:

$$(33)\qquad \mathrm{Vol}(\mathcal{N}^\star(s)) = \begin{cases}1, & \text{if } n \text{ is odd,}\\ 2^{-\frac{n-2}{2}}, & \text{if } n \text{ is even.}\end{cases}$$

Using (24) to determine how s scales the slicing indices and (25) to determine how s scales the other coordinates of $W_{n,f_1}(\mathbb{R})_0$, we deduce that

$$(34)\quad \mathrm{Vol}(\mathcal{B}_b(0,s)_X)\delta(s) = \begin{cases}\prod_{i=1}^{\lfloor \frac{n}{2}\rfloor} s_i^{2i-1}\cdot \mathrm{Vol}(\mathcal{B}_{(b_1s_1,\dots,b_{\lfloor \frac{n}{2}\rfloor}s_{\lfloor \frac{n}{2}\rfloor})}(0,1)_X), & \text{if } n \text{ is odd,}\\ s_{\frac{n-2}{2}}{}^{\frac{n-6}{2}} s_{\frac{n}{2}}{}^{\frac{n-2}{2}}\cdot\prod_{i=2}^{\frac{n-4}{2}} s_i^{2i-1}\cdot \mathrm{Vol}(\mathcal{B}_{(b_1s_1,\dots,b_{\frac{n-2}{2}}s_{\frac{n-2}{2}},b_{\frac{n}{2}}s_{\frac{n-2}{2}}^{-1}s_{\frac{n}{2}})}(0,1)_X), & \text{if } n \text{ is even.}\end{cases}$$

Let $\mathcal{B}_\beta := \mathcal{B}_\beta(0,1)$ for any $\beta=(\beta_1,\dots,\beta_{\lfloor \frac{n}{2}\rfloor})\in(\mathbb{R}\smallsetminus\{0\})^{\lfloor \frac{n}{2}\rfloor}$. We want to reduce to the case where $\beta_i>0$ for each $i\in\{1,\dots,\lfloor \frac{n}{2}\rfloor\}$. To do this, let G be as in §3.2, and observe that for every $\beta\in(\mathbb{R}\smallsetminus\{0\})^{\lfloor \frac{n}{2}\rfloor}$, there exists $g\in G$ such that $\mathcal{B}_\beta = g\cdot\mathcal{B}_{(|\beta_1|,\dots,|\beta_{\lfloor \frac{n}{2}\rfloor}|)}$. Thus, we have that

$$(35)\qquad \mathrm{Vol}\left((\mathcal{B}_\beta)_X\right) = \mathrm{Vol}\left((\mathcal{B}_{(|\beta_1|,\dots,|\beta_{\lfloor \frac{n}{2}\rfloor}|)})_X\right)$$

for any $\beta\in(\mathbb{R}_{>0})^{\lfloor \frac{n}{2}\rfloor}$ and $X>0$. Setting $\beta_i=|b_is_i|$ for each $i\in\{1,\dots,\lfloor \frac{n}{2}\rfloor\}$ when n is odd and for each $i\in\{1,\dots,\frac{n-2}{2}\}$ when n is even, setting $\beta_{\frac{n}{2}}=|b_{\frac{n}{2}}s_{\frac{n-2}{2}}^{-1}s_{\frac{n}{2}}|$, and substituting this along

with (32), (33), (34), and (35) into (31) yields that

(36)

$$\sharp\left(\frac{(W_{n,f_1}^{(r_1)}(\mathbb{Z})_{\mathrm{red}})_X}{\mathcal{G}_n(\mathbb{Z})}\right) = \frac{1}{C_H}\cdot \sum_{b\in(\mathbb{Z}>0)^{\lfloor \frac{n}{2}\rfloor}} \left(\prod_{i=1}^{\lfloor \frac{n}{2}\rfloor -1} b_i^{-2i}\right)\cdot$$

$$\left\{\begin{array}{ll} 2^{\lfloor \frac{n}{2}\rfloor} b_{\lfloor \frac{n}{2}\rfloor}^{\ 1-n} \displaystyle\int_{\substack{\beta_i\geq c_2 b_i \\ i\in\{1,\ldots,\lfloor \frac{n}{2}\rfloor\}}} \left(\prod_{i=1}^{\lfloor \frac{n}{2}\rfloor} \beta_i^{2i-1}\right)\cdot \mathrm{Vol}((\mathcal{B}_\beta)_X)\cdot \mathrm{Vol}(\mathcal{N}^\star(s_{\beta,b}))d\beta, & \text{if } n \text{ is odd,} \\ 2^{\frac{n}{2}} b_{\frac{n}{2}}^{\ -\frac{n}{2}} \displaystyle\int_{\substack{\beta_i\geq c_2 b_i \\ i\in\{1,\ldots,\frac{n-2}{2}\}}} \int_{\beta_{\frac{n}{2}}\geq c_2 \frac{b_{\frac{n}{2}}}{b_{\frac{n-2}{2}}}} \left(\beta_{\frac{n}{2}}^{\ \frac{n-2}{2}} \prod_{i=1}^{\frac{n-2}{2}} \beta_i^{2i-1}\right)\cdot \mathrm{Vol}((\mathcal{B}_\beta)_X)\cdot \mathrm{Vol}(\mathcal{N}^\star(s_{\beta,b}))d\beta, & \text{if } n \text{ is even,} \end{array}\right\} +$$

$$o(X^{\frac{n^2+n-2}{2}})$$

where $\beta := (\beta_1,\ldots,\beta_{\lfloor \frac{n}{2}\rfloor})$, $d\beta := \prod_{i=1}^{\lfloor \frac{n}{2}\rfloor} d\beta_i$, and

$$s_{\beta,b} = \begin{cases} \big(|\beta_1 b_1^{-1}|,\ldots,|\beta_{\lfloor \frac{n}{2}\rfloor} b_{\lfloor \frac{n}{2}\rfloor}^{-1}|\big), & \text{if } n \text{ is odd,} \\ \big(|\beta_1 b_1^{-1}|,\ldots,|\beta_{\frac{n-2}{2}} b_{\frac{n-2}{2}}^{-1}|,|\beta_{\frac{n-2}{2}}\beta_{\frac{n}{2}}(b_{\frac{n-2}{2}}b_{\frac{n}{2}})^{-1}|\big), & \text{if } n \text{ is even.} \end{cases}$$

The following lemma not only allows us to extend the region of integration to $\beta_i > 0$ for each $i \in \{1,\ldots,\lfloor \frac{n}{2}\rfloor\}$, but also permits us to eliminate the factors of $\mathrm{Vol}(\mathcal{N}^\star(s_{\beta,b}))$ in (36):

Lemma 21. *The expression on the right-hand side of* (36) *is, up to a negligible error, unchanged if we replace the regions of integration with the regions $\beta_i > 0$ for each $i \in \{1,\ldots,\lfloor \frac{n}{2}\rfloor\}$ and if we replace the factors of $\mathrm{Vol}(\mathcal{N}^\star(s_{\beta,b}))$ with the values on the right-hand side of* (33).

Proof. Fix a real number $\Gamma \geq c_2$. Observe that to prove the lemma, it suffices to choose a subset $I \subset \{1,\ldots,\lfloor \frac{n}{2}\rfloor\}$, replace the region of integration for β_i with $\beta_i \in [0,\Gamma b_i]$ for each $i \in I \smallsetminus \{\frac{n}{2}\}$ and with $\beta_{\frac{n}{2}} \in [0,\Gamma b_{\frac{n}{2}} b_{\frac{n-2}{2}}^{-1}]$ if $\frac{n}{2} \in I$, and demonstrate that the resulting quantity is negligible. For the sake of brevity, we do this when $I = \{1\}$ and $n \geq 5$; the analysis for the other choices of the set I is entirely analogous, and the analysis for $n \in \{3,4\}$ is relatively easy.

Take $\beta_1 \in [0,\Gamma b_1]$. By our construction of the section σ, we have that $\mathrm{Vol}(\mathcal{B}_\beta(X)) \ll X^{\lfloor \frac{n}{2}\rfloor^2+2\lfloor \frac{n}{2}\rfloor}$ if n is odd and $\mathrm{Vol}(\mathcal{B}_\beta(X)) \ll X^{\frac{n^2+2n-4}{4}}$ if n is even, where the implied constant is independent of $\beta \in (\mathbb{R}_{>0})^{\lfloor \frac{n}{2}\rfloor}$. Further notice that for each $i \in \{1,\ldots,\lfloor \frac{n}{2}\rfloor\}$, the largest possible value of β_i such that $\mathcal{B}_\beta(X) \neq \varnothing$ is $O(X)$; this also implies that we may truncate the summation over b on the right-hand side of (36) to the set where $b_i \ll X$ for each $i \in \{1,\ldots,\lfloor \frac{n}{2}\rfloor\}$. Upon substituting these estimates into (36) and replacing the region of integration for β_1 with $\beta_1 \in [0,\ b_1]$, we obtain

$$\sum_{\substack{b\in(\mathbb{Z}>0)^{\lfloor \frac{n}{2}\rfloor} \\ b_i\ll X\ \forall i}} \left(\prod_{i=1}^{\lfloor \frac{n}{2}\rfloor} b_i^{-2i}\right) \int_{\beta_1=0}^{\Gamma b_1} \int_{\substack{\beta_i\in[\Gamma b_i, O(X)] \\ i\in\{2,\ldots,\lfloor \frac{n}{2}\rfloor\}}} \left(\prod_{i=1}^{\lfloor \frac{n}{2}\rfloor} \beta_i^{2i-1}\right)\cdot X^{\lfloor \frac{n}{2}\rfloor^2+2\lfloor \frac{n}{2}\rfloor} d\beta$$

$$\ll X^{\frac{n^2+n-4}{2}} = o(X^{\frac{n^2+n-2}{2}})$$

when n is odd, and

$$\sum_{\substack{b\in(\mathbb{Z}>0)^{\lfloor \frac{n}{2}\rfloor} \\ b_i\ll X\ \forall i}} \left(\prod_{i=1}^{\lfloor \frac{n}{2}\rfloor -1} b_i^{-2i}\right)\cdot b_{\frac{n}{2}}^{\ -\frac{n}{2}} \int_{\beta_1=0}^{\Gamma b_1} \int_{\substack{\beta_i\in[\Gamma b_i, O(X)] \\ i\in\{2,\ldots,\frac{n-2}{2}\}}} \int_{\beta_{\frac{n}{2}}=\Gamma\frac{b_{\frac{n}{2}}}{b_{\frac{n-2}{2}}}}^{O(X)} \beta_{\frac{n}{2}}^{\ \frac{n-2}{2}} \left(\prod_{i=1}^{\frac{n-2}{2}} \beta_i^{2i-1}\right)\cdot X^{\frac{n^2+2n-4}{4}} d\beta$$

$$\ll X^{\frac{n^2+n-4}{2}} = o(X^{\frac{n^2+n-2}{2}})$$

when n is even. This proves the lemma when $I = \{1\}$ and $n \geq 5$. □

Combining Lemma 21 with (36), we obtain the following bound, in which each β_i is integrated from 0 up to ∞:

$$\sharp\left(\frac{(W_{n,f_1}^{(r_1)}(\mathbb{Z})_{\mathrm{red}})_X}{\mathcal{G}_n(\mathbb{Z})}\right) = \frac{1}{C_H}\cdot \sum_{b\in(\mathbb{Z}_{>0})^{\lfloor\frac{n}{2}\rfloor}} \left(\prod_{i=1}^{\lfloor\frac{n}{2}\rfloor-1} b_i^{-2i}\right)\cdot \tag{37}$$
$$\left\{\begin{array}{l} 2^{\lfloor\frac{n}{2}\rfloor} b_{\lfloor\frac{n}{2}\rfloor}{}^{1-n} \displaystyle\int_{\substack{\beta_i\geq 0\\ i\in\{1,\dots,\lfloor\frac{n}{2}\rfloor\}}} \left(\prod_{i=1}^{\lfloor\frac{n}{2}\rfloor}\beta_i^{2i-1}\right)\cdot \mathrm{Vol}((\mathcal{B}_\beta)_X)d\beta, \text{ if } n \text{ is odd,} \\ 2b_{\frac{n}{2}}{}^{-\frac{n}{2}} \displaystyle\int_{\substack{\beta_i\geq 0\\ i\in\{1,\dots,\frac{n}{2}\}}} \left(\beta_{\frac{n}{2}}{}^{\frac{n-2}{2}}\prod_{i=1}^{\frac{n-2}{2}}\beta_i^{2i-1}\right)\cdot \mathrm{Vol}((\mathcal{B}_\beta)_X)d\beta, \text{ if } n \text{ is even,} \end{array}\right\} + o(X^{\frac{n^2+n-2}{2}}).$$

Theorem 18 now follows from (37) by performing a change-of-variables and evaluating the sum over the slicing indices b_i.

5. A Jacobian change-of-variables formula

The objective of this section is to prove the following result, which gives an asymptotic formula for the quantity $\sharp((N\times\mathcal{G}_n)(\mathbb{Z})\backslash(W_n^{(r_1)}(\mathbb{Z})_{\mathrm{red}})_X)$:

Theorem 22 (Variant of Theorem 4)**.** *We have that*

$$\sharp\left(\frac{(W_n^{(r_1)}(\mathbb{Z})_{\mathrm{red}})_X}{(N\times\mathcal{G}_n)(\mathbb{Z})}\right) = \left\{\begin{array}{ll} \left(\displaystyle\prod_{i=1}^{\lfloor\frac{n}{2}\rfloor}\zeta(2i)\right)\cdot N_n^{(r_1)}(X) + o\big(X^{\frac{n^2+n-2}{2}}\big), & \text{if } n \text{ is odd,} \\ \left(2^{-\frac{n}{2}}\zeta(\tfrac{n}{2})\displaystyle\prod_{i=1}^{\frac{n-2}{2}}\zeta(2i)\right)\cdot N_n^{(r_1)}(X) + o\big(X^{\frac{n^2+n-2}{2}}\big), & \text{if } n \text{ is even.} \end{array}\right.$$

Let $N_{n,f_1}^{(r_1)}(X) := \mathrm{Vol}\left(U_{n,f_1}^{(r_1)}(\mathbb{R})_X\right)$, and observe that $N_{n,f_1}^{(r_1)}(X)$ is independent of f_1. Upon fibering over f_1, we see that proving Theorem 22 amounts to proving the following for each fixed f_1:

$$\sharp\left(\frac{(W_{n,f_1}^{(r_1)}(\mathbb{Z})_{\mathrm{red}})_X}{\mathcal{G}_n(\mathbb{Z})}\right) = \left\{\begin{array}{ll} \left(\displaystyle\prod_{i=1}^{\lfloor\frac{n}{2}\rfloor}\zeta(2i)\right)\cdot N_{n,f_1}^{(r_1)}(X) + o\big(X^{\frac{n^2+n-2}{2}}\big), & \text{if } n \text{ is odd,} \\ \left(2^{1-\frac{n}{2}}\zeta(\tfrac{n}{2})\displaystyle\prod_{i=1}^{\frac{n-2}{2}}\zeta(2i)\right)\cdot N_{n,f_1}^{(r_1)}(X) + o\big(X^{\frac{n^2+n-2}{2}}\big), & \text{if } n \text{ is even.} \end{array}\right. \tag{38}$$

By Theorem 18, proving the asymptotic (38) amounts to computing C_X. The remainder of this section is devoted to the computation of C_X, which we achieve by means of a Jacobian change-of-variables argument.

5.1. **Setting up the change-of-variables.** Let $\mathcal{K}\subset\mathcal{G}_n(\mathbb{R})$ denote a maximal compact subgroup containing K. Notice that C_X must be independent of the choice of the region H and of the fundamental set $L_{f_1}^{(r_1)}$ for the action of $\mathcal{G}_n(\mathbb{R})$ on $W_{n,f_1}^{(r_1)}(\mathbb{R})$, so long as H is a left-K-invariant subset of $\mathcal{G}_n(\mathbb{R})$ that is the closure of a nonempty open set. Thus, we may assume for the sake of convenience that H is also inversion-invariant, and thus right-$\mathcal{K}$-invariant too (note that this can be arranged while still ensuring that H is the closure of a nonempty open set). By this assumption

and by the uniqueness of the Iwasawa decomposition, there exists a compact subset $H' \subset \mathcal{A} \cdot \mathcal{N}$ such that $H = H' \cdot \mathcal{K} \subset (\mathcal{A} \cdot \mathcal{N}) \cdot \mathcal{K} = \mathcal{G}_n(\mathbb{R})$.

Since the action of $\mathcal{A} \cdot \mathcal{N}$ preserves $\{B \in W_{n,f_1}(\mathbb{R})_0 : b_{i(n-i)}(B) > 0 \text{ for each } i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}\}$, the region of integration in the numerator of C_X can be expressed as

$$\begin{aligned} \mathcal{B}_X &= \left\{B \in \left(((H' \cdot \mathcal{K}) \cdot L_{f_1}^{(r_1)})_0\right)_X : b_{i(n-i)}(B) > 0 \text{ for each } i \in \{1, \dots, \lfloor \tfrac{n}{2} \rfloor\}\right\} \\ &= H' \cdot \left\{B \in \left((\mathcal{K} \cdot L_{f_1}^{(r_1)})_0\right)_X : b_{i(n-i)}(B) > 0 \text{ for each } i \in \{1, \dots, \lfloor \tfrac{n}{2} \rfloor\}\right\}. \end{aligned} \tag{39}$$

We then have the following lemma, which allows us to conveniently reexpress the set $(\mathcal{K} \cdot L_{f_1}^{(r_1)})_0$:

Lemma 23. *There exist continuous functions $\theta_j \colon L_{f_1}^{(r_1)} \to \mathcal{K}$ for each $j \in \{1, \dots, n_{r_1}\}$ such that θ_1 is the constant function with value $\mathrm{id} \in \mathcal{K}$ and such that for each $B \in L_{f_1}^{(r_1)}$, we have the following equality of sets:*

$$\{\theta_j : j \in \{1, \dots, n_{r_1}\}\} = \left\{\theta \in \mathcal{K} : \theta \cdot B \in W_{n,f_1}(\mathbb{R})_0 \text{ and } b_{i(n-i)}(\theta \cdot B) > 0 \text{ for each } i \in \{1, \dots, \lfloor \tfrac{n}{2} \rfloor\}\right\}. \tag{40}$$

Moreover, for each $B \in L_{f_1}^{(r_1)}$, the elements $\theta_j(B)$ for $j \in \{1, \dots, n_{r_1}\}$ are distinct.

Proof. Let $g_j \colon L_{f_1}^{(r_1)} \to \mathcal{G}_n(\mathbb{R})$ be functions such that g_1 is the constant function with value $\mathrm{id} \in \mathcal{G}_n(\mathbb{R})$ and such that for each $B \in L_{f_1}^{(r_1)}$, we have the following equality of sets:

$$\{g_j : j \in \{1, \dots, n_{r_1}\}\} = \mathrm{Stab}_{\mathcal{G}_n(\mathbb{R})}(B).$$

Since the subgroup $\mathrm{Stab}_{\mathcal{G}_n(\mathbb{R})}(B) \subset \mathrm{GL}_n(\mathbb{R})$ is cut out by polynomial equations whose coefficients are polynomials in the entries of the matrix B, we may assume that the functions g_j are continuous.

Let $\pi \colon \mathcal{G}_n(\mathbb{R}) \to \mathcal{K}$ be obtained by postcomposing the diffeomorphism $\mathcal{G}_n(\mathbb{R}) \to \mathcal{A} \times \mathcal{N} \times \mathcal{K}$ given by the Iwasawa decomposition with the projection map $\mathcal{A} \times \mathcal{N} \times \mathcal{K} \to \mathcal{K}$, and for each $j \in \{1, \dots, n_{r_1}\}$, let $\theta_j \colon L_{f_1}^{(r_1)} \to \mathcal{K}$ be defined by $\theta_j = \pi \circ g_j$. Then, observe that θ_1 is the constant function with value $\mathrm{id} \in \mathcal{K}$ and that $\theta_j \cdot B \in W_{n,f_1}(\mathbb{R})_0$ for each $j \in \{1, \dots, n_{r_1}\}$ and $B \in L_{f_1}^{(r_1)}$. We have thus proven that the left-hand side of (40) is contained in the right-hand side.

Suppose that $\theta \in \mathcal{K}$ and $B \in L_{f_1}^{(r_1)}$ is such that $\theta \cdot B \in W_{n,f_1}(\mathbb{R})_0$ and $b_{i(n-i)}(\theta \cdot b) > 0$ for each $i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}$. It is a consequence of the proof of Lemma 26 (to follow) that $\mathcal{A} \cdot \mathcal{N}$ acts simply transitively on the set of elements $B' \in W_{n,f_1}(\mathbb{R})_0$ such that $b_{i(n-i)}(B') > 0$ for each $i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}$ and such that $\mathrm{inv}(x \cdot A_0 + z \cdot B') = \mathrm{inv}(x \cdot A_0 + z \cdot B)$. Thus, there exists $h \in \mathcal{A} \cdot \mathcal{N}$ such that $h \cdot B = \theta \cdot B$, so $h^{-1}\theta \in \mathrm{Stab}_{\mathcal{G}_n(\mathbb{R})}(B)$, implying that $h^{-1}\theta = g_j(B)$ for some $j \in \{1, \dots, n_{r_1}\}$. But then $\theta = \pi(h^{-1}\theta) = \pi(g_j(B)) = \theta_j(B)$. We have thus proven that the right-hand side of (40) is contained in the left-hand side.

Finally, if the elements $\theta_j(B)$ for $j \in \{1, \dots, n_{r_1}\}$ were not distinct for some $B \in L_{f_1}^{(r_1)}$, then it would follow that $\mathrm{Stab}_{\mathcal{A} \cdot \mathcal{N}}(B)$ contains a nontrivial element, which is impossible. □

It follows from combining (39) and Lemma 23 that

$$\mathcal{B} = \bigsqcup_{j=1}^{n_{r_1}} H' \cdot \mathcal{B}_j, \quad \text{where} \quad \mathcal{B}_j := \left\{\theta_j(B) \cdot B : B \in L_{f_1}^{(r_1)}\right\}, \tag{41}$$

so the numerator of C_X is given by

$$\begin{cases} \displaystyle\sum_{j=1}^{n_{r_1}} \int_{B \in H' \cdot (\mathcal{B}_j)_X} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} |b_{i(n-i)}(B)|^{2i-1} dB, & \text{if } n \text{ is odd,} \\ \displaystyle\sum_{j=1}^{n_{r_1}} \int_{B \in H' \cdot (\mathcal{B}_j)_X} |b_{\frac{n}{2}\frac{n}{2}}(B)|^{\frac{n-2}{2}} \prod_{i=1}^{\frac{n-2}{2}} |b_{i(n-i)}(B)|^{2i-1} dB, & \text{if } n \text{ is even,} \end{cases} \tag{42}$$

5.2. **Calculating the Jacobian.** To compute (42), we first show that all of the terms in the sum (42) are in fact equal to each other. This follows immediately from the Jacobian change-of-variables formula established in the next proposition, by taking $\widetilde{\sigma}$ to be defined by $\widetilde{\sigma}(B) = \theta_j(\sigma(B)) \cdot \sigma(B)$ for each $j \in \{1, \dots, n_{r_1}\}$, where σ is as defined in §3.3.

Proposition 24. *Let $\widetilde{\sigma}\colon \mathbb{R}^{n-1} \to W_{n,f_1}^{(r_1)}(\mathbb{R})_0$ be a continuous function such that for each $(n-1)$-tuple $f = (f_2, \dots, f_n) \in \mathbb{R}^{n-1}$, we have $\mathrm{inv}(x \cdot A_0 + z \cdot \widetilde{\sigma}(f)) = x^n + \sum_{i=1}^n f_i x^{n-i} z^i$. Let $\mathcal{R} \subset \mathbb{R}^{n-1}$ be any bounded open set contained in the complement of the locus of forms of discriminant 0. Then there is a nonzero rational constant $\mathcal{J} \in \mathbb{Q}^\times$, depending only on the degree n, such that*

$$\int_{B \in H' \cdot \widetilde{\sigma}(\mathcal{R})} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} |b_{i(n-i)}(B)|^{2i-1} dB = |\mathcal{J}| \int_{f \in \mathcal{R}} \int_{h \in H'} dh df$$

when n is odd, and

$$\int_{B \in H' \cdot \widetilde{\sigma}(\mathcal{R})} |b_{\frac{n}{2}\frac{n}{2}}(B)|^{\frac{n-2}{2}} \prod_{i=1}^{\frac{n-2}{2}} |b_{i(n-i)}(B)|^{2i-1} dB = |\mathcal{J}| \int_{f \in \mathcal{R}} \int_{h \in H'} dh df$$

when n is even, where dh denotes the Haar measure on $\mathcal{A} \cdot \mathcal{N}$ and is given explicitly by

$$dh = \begin{cases} \left(\prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} s_i^{-i^2 + 2i\lfloor \frac{n}{2} \rfloor - 1} \right) ds du, & \text{if } n \text{ is odd,} \\ \left(\left(s_{\frac{n-2}{2}} s_{\frac{n}{2}}\right)^{\frac{n^2-2n-8}{8}} \prod_{i=1}^{\frac{n-4}{2}} s_i^{-i^2 + i(n-1) - 1} \right) ds du, & \text{if } n \text{ is even.} \end{cases}$$

Proof. By the Stone-Weierstrass Theorem, any continuous real-valued function on $\mathcal{R}$ is the uniform limit of differentiable functions. Thus, to prove the lemma, we may assume that $\widetilde{\sigma}$ is differentiable on R. Under this assumption, the following change-of-measure formula holds for any measurable function $\phi\colon H' \cdot \widetilde{\sigma}(\mathcal{R}) \to \mathbb{R}$:

$$\int_{B \in H' \cdot \widetilde{\sigma}(\mathcal{R})} \phi(B) dB = \int_{f \in \mathcal{R}} \int_{h = su \in H'} \phi(h \cdot \widetilde{\sigma}(f)) \cdot |\mathcal{J}_{\widetilde{\sigma}}(h, f)| ds du df, \tag{43}$$

where $\mathcal{J}_{\widetilde{\sigma}}(h, f)$ denotes the determinant of the Jacobian matrix arising from the change-of-variables taking the coordinate $B \in H' \cdot \widetilde{\sigma}(\mathcal{R})$ to the coordinates $(h, f) = (s, u, f) \in H' \times \mathcal{R}$. It is likely infeasible to directly compute $\mathcal{J}_{\widetilde{\sigma}}$ for arbitrary n and $\widetilde{\sigma}$.[10] Instead, we compute $\mathcal{J}_{\widetilde{\sigma}}$ indirectly by first extracting its dependence on h and then relating $\mathcal{J}_{\widetilde{\sigma}}$ to $\mathcal{J}_{\sigma_0}$, which is easier to compute. (Recall that σ_0 is the section with polynomial entries defined in §3.3.)

In the following lemma, we derive the dependence of $\mathcal{J}_{\widetilde{\sigma}}$ on h:

Lemma 25. *Let $f \in \mathcal{R}$. The quantity*

$$\mathcal{J}_{\widetilde{\sigma}}(h, f) \cdot \begin{cases} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} s_i^{i^2 - 2i(\lfloor \frac{n}{2} \rfloor + 1) + 2}, & \text{if } n \text{ is odd,} \\ s_{\frac{n-2}{2}}^{\frac{-n^2-2n+24}{8}} s_{\frac{n}{2}}^{\frac{-n^2-2n+16}{8}} \prod_{i=1}^{\frac{n-4}{2}} s_i^{i^2 - i(n+1) + 2}, & \text{if } n \text{ is even} \end{cases} \tag{44}$$

is independent of $h = (s, u) = (s_1, \dots, s_{\lfloor \frac{n}{2} \rfloor}, u) \in \mathcal{A} \cdot \mathcal{N}$.

Proof of Lemma 25. We first show that the quantity (44) is independent of s. To do this, fix $\overline{s} = (\overline{s}_1, \dots, \overline{s}_{\lfloor \frac{n}{2} \rfloor}) \in \mathcal{A}$, and consider the transformation on $W_{n,f_1}(\mathbb{R})_0$ that sends $B = [b_{ij}] \mapsto [\overline{w}_{ij} \cdot b_{ij}]$, where $\overline{w}_{ij}$ is defined in terms of $\overline{s}$ just like w_{ij} is defined in terms of s in the paragraph immediately

[10] For small values of n and a particular $\widetilde{\sigma}$, it is possible to compute $\mathcal{J}_{\widetilde{\sigma}}$ using a computer algebra system.

preceding (24). Then using (24) and (25), we find that under this transformation, the measure dB on $W_{n,f_1}(\mathbb{R})_0$ scales as follows:

$$dB \mapsto \begin{cases} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \overline{s}_i^{-i^2+2i(\lfloor \frac{n}{2} \rfloor+1)-1}, & \text{if } n \text{ is odd,} \\ \overline{s}_{\frac{n-2}{2}}^{\frac{n^2+2n-16}{8}} \overline{s}_{\frac{n}{2}}^{\frac{n^2+2n-8}{8}} \prod_{i=1}^{\frac{n-4}{2}} \overline{s}_i^{-i^2+i(n+1)-1}, & \text{if } n \text{ is even} \end{cases} \cdot dB. \tag{45}$$

But by construction, this transformation acts on $(\mathcal{A} \cdot \mathcal{N}) \times \mathcal{R}$ by sending $(s, u, f) \mapsto (\overline{s} \cdot s, u, f)$. Under this transformation, the measure $dsdudf$ on $(\mathcal{A} \cdot \mathcal{N}) \times \mathcal{R}$ scales as follows:

$$dsdudf \mapsto \left(\prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \overline{s}_i \right) \cdot dsdudf. \tag{46}$$

By (45) and (46), we can express $\mathcal{J}_{\widetilde{\sigma}}(\overline{s} \cdot s, u, f)$ in terms of $\mathcal{J}_{\widetilde{\sigma}}(s, u, f)$ as follows:

$$\mathcal{J}_{\widetilde{\sigma}}(\overline{s} \cdot s, u, f) = \mathcal{J}_{\widetilde{\sigma}}(s, u, f) \cdot \begin{cases} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \overline{s}_i^{-i^2+2i(\lfloor \frac{n}{2} \rfloor+1)-2}, & \text{if } n \text{ is odd,} \\ \overline{s}_{\frac{n-2}{2}}^{\frac{n^2+2n-24}{8}} \overline{s}_{\frac{n}{2}}^{\frac{n^2+2n-16}{8}} \prod_{i=1}^{\frac{n-4}{2}} \overline{s}_i^{-i^2+i(n+1)-2}, & \text{if } n \text{ is even.} \end{cases} \tag{47}$$

That the quantity (44) is independent of s then follows by applying the following steps to (47): set $s = 1$, replace every instance of the symbol $\overline{s}$ with the symbol s, and rearrange the result.

We now use an analogous argument to show that the quantity (44) is independent of u. Fix $\overline{u} \in \mathcal{N}$, and consider the transformation on $W_{n,f_1}(\mathbb{R})_0$ given by multiplication by $\overline{u}$. Under this transformation, the measure dB on $W_{n,f_1}(\mathbb{R})_0$ is invariant because $\overline{u}$ is unipotent. This transformation acts on $(\mathcal{A} \cdot \mathcal{N}) \times \mathcal{R}$ by sending $(s, u, f) \mapsto (s, \overline{u}_s + u, f)$, where for any $s \in \mathcal{A}$ and $u \in \mathcal{N}$, we write $u_s \in \mathcal{N}$ to denote the unique element satisfying the relation $us = su_s$. Under this transformation, the measure $dsdudf$ on $(\mathcal{A} \cdot \mathcal{N}) \times \mathcal{R}$ changes as follows: $dsdudf \mapsto dsd(\overline{u}_s + u)df = dsdudf$. It follows that

$$\mathcal{J}_{\widetilde{\sigma}}(s, \overline{u}_s + u, f) = \mathcal{J}_{\widetilde{\sigma}}(s, u, f). \tag{48}$$

Since the quantity (44) is independent of s, it is equal to $\mathcal{J}_{\widetilde{\sigma}}(1, u, f)$. That $\mathcal{J}_{\widetilde{\sigma}}(1, u, f)$ is independent of u then follows by applying the following steps to (48): set $(s, u) = (1, 0)$, observe that $\overline{u}_1 = \overline{u}$, and replace the symbol $\overline{u}$ with the symbol u.

This completes the proof of Lemma 25. □

Note that the result of Lemma 25 holds for any differentiable function $\widetilde{\sigma}$ as in the statement of the proposition; in particular, the lemma holds for $\widetilde{\sigma} = \sigma_0$. Since the quantity (44) is independent of h, we may unambiguously denote it by $\mathcal{J}_{\widetilde{\sigma}}(f)$.

The next lemma characterizes the relationship between $\widetilde{\sigma}$ and σ_0 in a way that will allow us to express $\mathcal{J}_{\widetilde{\sigma}}$ in terms of $\mathcal{J}_{\sigma_0}$:

Lemma 26. *There exist differentiable functions $\widetilde{u}\colon \mathcal{R} \to \mathcal{N}$ and $\widetilde{s}\colon \mathcal{R} \to \mathcal{A}$ such that for every $f \in \mathcal{R}$, we have $\widetilde{\sigma}(f) = \big(\widetilde{u}(f)\widetilde{s}(f)\big) \cdot \sigma_0(f)$.*

Proof of Lemma 26. We first construct $\widetilde{u}$. Using (10) and (11), we observe that for any $B \in W_n(\mathbb{R})_0$ such that $b_{i(n-i)}(B) \neq 0$ for each $i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}$, we have the following:

- Let $\widetilde{u}_{21} \in \mathbb{R}$ be such that $b_{1n}(B) + b_{1(n-1)}(B) \cdot \widetilde{u}_{21} = \frac{f_1}{n}$. By abuse of notation, let $\widetilde{u}_{21} \in \mathcal{N}$ denote the matrix whose row-2, column-1 entry is $\widetilde{u}_{21}$ but all of whose remaining unipotent coordinates are 0. We redefine B to be $\widetilde{u}_{21} \cdot B$.
- Let $\widetilde{u}_{32} \in \mathbb{R}$ be such that $b_{2(n-1)}(B) + b_{2(n-2)}(B) \cdot \widetilde{u}_{32} = \frac{f_1}{n}$; abusing notation once again, we redefine B to be $\widetilde{u}_{32} \cdot B$. Next, let $\widetilde{u}_{31} \in \mathbb{R}$ be such that $b_{2n}(B) + b_{2(n-2)}(B) \cdot \widetilde{u}_{31} = 0$; we redefine B to be $\widetilde{u}_{31} \cdot B$.

- Let $k \in \{3, \dots, n-1\}$, and suppose that we have already defined $\widetilde{u}_{ij}$ for each pair (i,j) such that $i \in \{2, \dots, k-1\}$ and $j \in \{1, \dots, \min\{i-1, n-i\}\}$, successively replacing B with $\widetilde{u}_{ij} \cdot B$ each time. We now explain how to define $\widetilde{u}_{ij}$ for $i = k$. Let $\widetilde{u}_{k\min\{k-1,n-k\}} \in \mathbb{R}$ be such that

$$b_{(k-1)\max\{k+1,n-k+2\}}(B) + b_{(k-1)(n-k+1)}(B) \cdot \widetilde{u}_{k\min\{k-1,n-k\}} = \frac{f_1}{n};$$

we redefine B to be $\widetilde{u}_{k\min\{k-1,n-k\}} \cdot B$. Next, let $\widetilde{u}_{k\min\{k-2,n-k-1\}} \in \mathbb{R}$ be such that

$$b_{(k-1)\max\{k+2,n-k+3\}}(B) + b_{(k-1)(n-k+1)}(B) \cdot \widetilde{u}_{k\min\{k-2,n-k-1\}} = 0;$$

we redefine B to be $\widetilde{u}_{k\min\{k-2,n-k-1\}} \cdot B$.

Continuing in this manner, let $k' \in \{1, \dots, \min\{k-2, n-k-1\}\}$, and suppose that we have defined $\widetilde{u}_{kj}$ for all $j \in \{\min\{k-k', n-k-k'+1\}, \dots, \min\{k-1, n-k\}\}$. Let $\widetilde{u}_{k\min\{k-k'-1,n-k-k'\}} \in \mathbb{R}$ be such that

$$b_{(k-1)\max\{k+k'+1,n-k+k'+2\}}(B) + b_{(k-1)(n-k+1)}(B) \cdot \widetilde{u}_{k\min\{k-k'-1,n-k-k'\}} = 0;$$

we redefine B to be $\widetilde{u}_{k\min\{k-k'-1,n-k-k'\}} \cdot B$.

Let $\widetilde{u}(f)$ be the composition of the $\widetilde{u}_{ij}$ in the order prescribed above. Then since each $\widetilde{u}_{ij}$ is a polynomial function of the previously constructed $\widetilde{u}_{i'j'}$ and of the entries of B together with the inverses of the entries $b_{i'(n-i')}(B)$, it follows that $\widetilde{u}$ is a differentiable function of f.

Define a function $\widetilde{s}_i$ as follows: let $\widetilde{s}_i(f) := b_{i(n-i)}(\widetilde{\sigma}(f))$ for each $i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\} \smallsetminus \{\frac{n}{2}\}$, let $\widetilde{s}_{\frac{n}{2}}(f) := b_{\frac{n}{2}\frac{n}{2}}(\widetilde{\sigma}(f)) b_{(\frac{n}{2}-1)(\frac{n}{2}+1)}(\widetilde{\sigma}(f))^{-1}$, and let $\widetilde{s} = (\widetilde{s}_1, \dots, \widetilde{s}_{\lfloor \frac{n}{2} \rfloor})$. Since $\widetilde{\sigma}$ is differentiable, it follows that $\widetilde{s}$ is differentiable too; note further that because we have assumed $\mathcal{R}$ to be contained in the complement of the locus of forms of discriminant 0, it follows from [7, Lemma 10.3] when n is odd and from [40, Part (2) of Theorem 4.2] when n is even that $\widetilde{s}_i(f) \neq 0$ for every $i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}$ and $f \in \mathcal{R}$, and so $\widetilde{s}(f)$ is invertible for every $f \in \mathcal{R}$.

We have defined $\widetilde{u}$ and $\widetilde{s}$ in such a way that $\big(\widetilde{u}(f)\widetilde{s}(f)\big)^{-1} \cdot \widetilde{\sigma}(f)$ lies in the image of σ_0; i.e., we have that $\big(\widetilde{u}(f)\widetilde{s}(f)\big)^{-1} \cdot \widetilde{\sigma}(f) = \sigma_0(f')$ for some $f' \in \mathbb{R}^{n-1}$. But it then follows that

$$\begin{aligned} x^n + \sum_{i=1}^{n} f_i' x^{n-i} z^i &= \mathrm{inv}(x \cdot A_0 + z \cdot \sigma_0(f')) = \mathrm{inv}\left(x \cdot A_0 + z \cdot (\widetilde{u}(f)\widetilde{s}(f))^{-1} \cdot \widetilde{\sigma}(f)\right) \\ &= \mathrm{inv}\left(x \cdot A_0 + z \cdot \widetilde{\sigma}(f)\right) = x^n + \sum_{i=1}^{n} f_i x^{n-i} z^i, \end{aligned}$$

so we conclude that $f = f'$. This completes the proof of Lemma 26. □

Let $\widetilde{u}$ and $\widetilde{s}$ be as in the statement of Lemma 26. Consider the transformation on $(\mathcal{A} \cdot \mathcal{N}) \times \mathcal{R}$ that sends $(h, f) \mapsto \big(h \cdot \widetilde{u}(f) \cdot \widetilde{s}(f), f\big)$. One verifies by inspection that under this transformation, the measures ds_i, du, and df change as follows for each $i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}$:

$$\begin{aligned} &ds_i \mapsto \widetilde{s}_i(f) ds_i + *, \\ &du \mapsto \left\{ \begin{array}{ll} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \widetilde{s}_i(f)^{i^2 - 2i\lfloor \frac{n}{2} \rfloor}, & \text{if } n \text{ is odd,} \\ \big(\widetilde{s}_{\frac{n-2}{2}}(f)\widetilde{s}_{\frac{n}{2}}(f)\big)^{\frac{-n^2+2n}{8}} \prod_{i=1}^{\frac{n-4}{2}} \widetilde{s}_i(f)^{i^2 - i(n-1)}, & \text{if } n \text{ is even} \end{array} \right\} \cdot du + *, \text{ and} \\ &df \mapsto df, \end{aligned} \tag{49}$$

where the symbol "$*$" is shorthand for "some multiple of df." It follows from (49) that the measure $dsdudf = ds \wedge du \wedge df$ scales as follows:

$$dsdudf \mapsto \left\{ \begin{array}{ll} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \widetilde{s}_i(f)^{i^2 - 2i\lfloor \frac{n}{2} \rfloor + 1}, & \text{if } n \text{ is odd,} \\ \big(\widetilde{s}_{\frac{n-2}{2}}(f)\widetilde{s}_{\frac{n}{2}}(f)\big)^{\frac{-n^2+2n+8}{8}} \prod_{i=1}^{\frac{n-4}{2}} \widetilde{s}_i(f)^{i^2 - i(n-1) + 1}, & \text{if } n \text{ is even} \end{array} \right\} \cdot dsdudf. \tag{50}$$

Upon combining Lemma 25 and (50), we obtain the following expression of $\mathcal{J}_{\widetilde{\sigma}}$ in terms of $\mathcal{J}_{\sigma_0}$:

$$\mathcal{J}_{\widetilde{\sigma}}(f) = \mathcal{J}_{\sigma_0}(f) \cdot \begin{cases} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \widetilde{s}_i(f)^{2i-1}, & \text{if } n \text{ is odd,} \\ \widetilde{s}_{\frac{n-2}{2}}(f)^{\frac{n-4}{2}} \widetilde{s}_{\frac{n}{2}}(f)^{\frac{n-2}{2}} \prod_{i=1}^{\frac{n-4}{2}} \widetilde{s}_i(f)^{2i-1}, & \text{if } n \text{ is even.} \end{cases} \tag{51}$$

Then, upon combining (43), Lemma 25, and (51), we obtain the following equality:

$$\begin{aligned} \int_{B \in H' \cdot \widetilde{\sigma}(\mathcal{R})} \phi(B) dB = \int_{f \in \mathcal{R}} \int_{h = su \in H'} \phi(h \cdot \widetilde{s}(f)) \cdot |\mathcal{J}_{\sigma_0}(f)| \cdot \\ \begin{cases} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \left(\widetilde{s}_i(f) s_i\right)^{2i-1}, & \text{if } n \text{ is odd,} \\ \left(\widetilde{s}_{\frac{n-2}{2}}(f) s_{\frac{n-2}{2}}\right)^{\frac{n-4}{2}} \left(\widetilde{s}_{\frac{n}{2}}(f) s_{\frac{n}{2}}\right)^{\frac{n-2}{2}} \prod_{i=1}^{\frac{n-4}{2}} \left(\widetilde{s}_i(f) s_i\right)^{2i-1}, & \text{if } n \text{ is even} \end{cases} \cdot dh df. \end{aligned} \tag{52}$$

Taking the function ϕ to be defined by

$$\phi(B) = \begin{cases} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} |b_{i(n-i)}(B)|^{2i-1}, & \text{if } n \text{ is odd,} \\ |b_{\frac{n}{2}\frac{n}{2}}(B)|^{\frac{n-2}{2}} \prod_{i=2}^{\frac{n}{2}} |b_{i(n-i)}(B)|^{2i-1}, & \text{if } n \text{ is even} \end{cases}$$

and observing that

$$\begin{aligned} b_{i(n-i)}\big(h \cdot \widetilde{\sigma}(f)\big) = b_{i(n-i)}\big(h \cdot \widetilde{u}(f) \cdot \widetilde{s}(f) \cdot \sigma_0(f)\big) = \\ \begin{cases} \left(\widetilde{s}_i(f) s_i\right)^{-1}, & \text{if } i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\} \smallsetminus \{\frac{n}{2}\}, \\ \left(\widetilde{s}_{\frac{n-2}{2}}(f) s_{\frac{n-2}{2}}\right)\left(\widetilde{s}_{\frac{n}{2}}(f) s_{\frac{n}{2}}\right)^{-1}, & \text{if } i = \frac{n}{2} \end{cases} \cdot b_{i(n-i)}\big(\sigma_0(f)\big), \end{aligned}$$

we deduce from (52) that the proposition holds with the constant $\mathcal{J}$ replaced by the function $\mathcal{J}_{\sigma_0}(f)$ (within the integrand).

We have reduced the proof of Proposition 24 to showing that $\mathcal{J}_{\sigma_0}(f) = \mathcal{J}$ is a constant function with nonzero rational value. We achieve this in the following lemma:

Lemma 27. *There is a nonzero rational constant $\mathcal{J} \in \mathbb{Q}^\times$, depending only on the degree n, such that $\mathcal{J}_{\sigma_0}(f) = \mathcal{J}$ for every $f \in \mathbb{R}^{n-1}$.*

Proof of Lemma 27. We claim that it suffices to consider the case where $f_1 = 0$. First observe that if we put $\sigma_0' := \sigma_0 - \frac{f_1}{n} \cdot A_0$, then $\mathcal{J}_{\sigma_0'}(h, f) = \mathcal{J}_{\sigma_0}(h, f)$, because $g \cdot \left(-\frac{f_1}{n} \cdot A_0\right) \cdot g^T = A_0$ for any $g \in \mathcal{G}_n(\mathbb{R})$. Next, let $\widetilde{f} \in \mathbb{R}^{n-1}$ be the coefficients of the form $\widetilde{F}$ arising from the form $F(x, z) = x^n + \sum_{i=1}^n f_i x^{n-i} z^i$ as in (16). Observe that $\mathcal{J}_{\sigma_0'}(h, \widetilde{f}) = \mathcal{J}_{\sigma_0'}(h, f)$, because the Jacobian for the change of variables from f to $\widetilde{f}$ is 1. Combining these two observations, we deduce that $\mathcal{J}_{\sigma_0'}(h, \widetilde{f}) = \mathcal{J}_{\sigma_0}(h, f)$. Now, notice that when $\mathcal{J}_{\sigma_0'}(h, \widetilde{f})$ is expressed as a function of the $\widetilde{f}_i$, it is formally the same as $\mathcal{J}_{\sigma_0}(h, f)$ expressed as a function of the f_i when $f_1 = 0$. Thus, the claim holds, and we assume that $f_1 = 0$ in the remainder of the proof of Lemma 27.

We now show that $\mathcal{J}_{\sigma_0}(f)$ is a nonzero rational constant, independent of f. To do this, let $c > 0$, and consider the transformation on $W_n(\mathbb{R})_0$ that sends $B \mapsto c \cdot B$. Under this transformation, the measure dB on $W_n(\mathbb{R})_0$ evidently scales as follows:

$$dB \mapsto \begin{cases} c^{\lfloor \frac{n}{2} \rfloor^2 + 3\lfloor \frac{n}{2} \rfloor}, & \text{if } n \text{ is odd,} \\ c^{\frac{n^2+4n-4}{4}}, & \text{if } n \text{ is even} \end{cases} \cdot dB \tag{53}$$

On the other hand, one verifies by inspection that this transformation acts on $(\mathcal{A} \cdot \mathcal{N}) \times \mathbb{R}^{n-1}$ in such a way that:

- $s_i \mapsto c^{-1} \cdot s_i$ for each $i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\} \smallsetminus \{\frac{n}{2}\}$ and $s_{\frac{n}{2}} \mapsto c^{-2} \cdot s_{\frac{n}{2}}$, so the measure ds_i scales as $ds_i \mapsto c^{-1} \cdot ds_i$ for each $i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\} \smallsetminus \{\frac{n}{2}\}$ and $ds_{\frac{n}{2}} \mapsto c^{-2} \cdot ds_{\frac{n}{2}}$; and

- the measures du and df change as follows:

$$du \mapsto \left\{ \begin{array}{ll} c^{\frac{4\lfloor \frac{n}{2} \rfloor^3+3\lfloor \frac{n}{2} \rfloor^2-\lfloor \frac{n}{2} \rfloor}{6}}, & \text{if } n \text{ is odd,} \\ c^{\frac{2n^3-3n^2-2n}{24}}, & \text{if } n \text{ is even} \end{array} \right\} \cdot du \quad \text{and} \quad df \mapsto c^{\frac{n^2+n-2}{2}} \cdot df.$$

It follows that the measure $dsdudf$ on $(\mathcal{A} \cdot \mathcal{N}) \times \mathbb{R}^{n-1}$ scales as

$$dsdudf \mapsto \left\{ \begin{array}{ll} c^{\frac{4\lfloor \frac{n}{2} \rfloor^3+15\lfloor \frac{n}{2} \rfloor^2+11\lfloor \frac{n}{2} \rfloor}{6}}, & \text{if } n \text{ is odd,} \\ c^{\frac{2n^3+9n^2-2n-48}{24}}, & \text{if } n \text{ is even} \end{array} \right\} \cdot dsdudf. \tag{54}$$

Combining Lemma 25 with (53) and (54) yields the identity $\mathcal{J}_{\sigma_0}(f_c) = \mathcal{J}_{\sigma_0}(f)$ for any element $f = (f_2, \dots, f_n) \in \mathbb{R}^{n-1}$, where we write f_c to denote the element $f_c := (c^2 \cdot f_2, \dots, c^n \cdot f_n)$.

Since the entries of $\sigma_0(f)$ are polynomials in the components of f with rational coefficients, it follows that $\mathcal{J}_{\sigma_0}(f)$ is a polynomial in the f_i with rational coefficients. Thus, taking the limit as $c \to 0$ in the identity $\mathcal{J}_{\sigma_0}(f_c) = \mathcal{J}_{\sigma_0}(f)$, we deduce that $\mathcal{J}_{\sigma_0}(f) = \mathcal{J}_{\sigma_0}(0)$ is a rational constant, independent of f. That $\mathcal{J}_{\sigma_0}(0) \neq 0$ follows upon observing that $(\mathcal{A} \cdot \mathcal{N}) \cdot \sigma_0(\mathbb{R}^{n-1})$ is a set of full measure in $W_n(\mathbb{R})_0$. This completes the proof of Lemma 27. □

This completes the proof of Proposition 24. □

We now take $\mathcal{R} = U_{n,f_1}^{(r_1)}(\mathbb{R})_X$ (where we identify $U_{n,f_1}^{(r_1)}(\mathbb{R})$ with a subset of $\mathbb{R}^{n-1}$). Combining (42) and Proposition 24 yields that the numerator of C_X is given by

$$n_{r_1} \cdot N_{n,f_1}^{(r_1)}(X) \cdot |\mathcal{J}| \int_{h \in H'} dh = n_{r_1} \cdot N_{n,f_1}^{(r_1)}(X) \cdot \frac{\mathrm{Vol}(\mathcal{K}H')}{\mathrm{Vol}(\mathcal{K})}, \tag{55}$$

where $\mathrm{Vol}(\mathcal{K}H')$ is computed with respect to the Haar measure on $\mathcal{G}_n(\mathbb{R}) = \mathcal{K} \cdot \mathcal{A} \cdot \mathcal{N}$ obtained by inverting the Haar measure (17) on $\mathcal{G}_n(\mathbb{R}) = \mathcal{N} \cdot \mathcal{A} \cdot \mathcal{K}$. On the other hand, note that the denominator of C_X is given by

$$\int_{h \in H} dh = \mathrm{Vol}(H) = \mathrm{Vol}(H'\mathcal{K}), \tag{56}$$

where $\mathrm{Vol}(H'\mathcal{K})$ is computed with respect to the Haar measure (17). Then, the following lemma allows us to simplify C_X:

Lemma 28. *We have that $\mathcal{K}H' = H'\mathcal{K}$, and in particular that* $\mathrm{Vol}(\mathcal{K}H') = \mathrm{Vol}(H'\mathcal{K})$.

Proof. Since $H = H'\mathcal{K}$ is left-$\mathcal{K}$-invariant and inversion-invariant, it follows that

$$\mathcal{K}H' \subset \mathcal{K}H'\mathcal{K} = H'\mathcal{K} = H = H^{-1} = \mathcal{K}(H')^{-1}. \tag{57}$$

Since the Iwasawa decomposition is unique, (57) implies that $H' \subset (H')^{-1}$, and hence also that $H' = (H')^{-1}$. Thus, we conclude that $H'\mathcal{K} = \mathcal{K}(H')^{-1} = \mathcal{K}H'$, as desired. □

Finally, combining Lemma 28 together with (55) and (56) yields that

$$C_X = \begin{cases} n_{r_1} \cdot N_{n,f_1}^{(r_1)}(X) \cdot |\mathcal{J}|, & \text{if } n \text{ is odd,} \\ \frac{1}{4} n_{r_1} \cdot N_{n,f_1}^{(r_1)}(X) \cdot |\mathcal{J}|, & \text{if } n \text{ is even.} \end{cases} \tag{58}$$

where the extra factor of $\frac{1}{4}$ when n is even arises because we normalized the measure $d\theta$ so that $\int_{\theta \in (K \cap \{\pm \mathrm{id}\}) \backslash K} d\theta = 1$. Upon substituting (58) into Theorem 18, we obtain (38) with "=" replaced by "$\leq$," up to the calculation of $\mathcal{J}$ (which we do in Proposition 30, to follow). Simply repeating the argument in §4.1–4.2 with $\mathcal{S}_2$ replaced by the smaller Siegel set $\mathcal{S}_1$ yields the reverse inequality.

Remark. In this section, we counted reducible elements in the lattice translate $W_{n,f_1}^{(r_1)}(\mathbb{Z}) \subset W_n^{(r_1)}(\mathbb{Z})$ for fixed f_1 to account for the action of the group $N(\mathbb{Z})$ on monic binary forms. The methods of this section can be easily adapted to count reducible elements in $W_n^{(r_1)}(\mathbb{Z})$, where f_1 is allowed to vary. The only significant difference is that the analogue of Lemma 27 produces a Jacobian constant $\mathcal{J}'$ that is *sometimes* different from $\mathcal{J}$. Indeed, a simple calculation reveals that $|\mathcal{J}'| = |\mathcal{J}|$ when n is odd but that $|\mathcal{J}'| = \frac{1}{2} \cdot |\mathcal{J}|$ when n is even.

5.3. **Computing the value of $\mathcal{J}$.** In this section, we first use a "principle of permanence of identities" argument (cf. [2, §14.3]) to deduce an analogue of Proposition 24 over $\mathbb{Z}_p$ for primes p. We then compute certain local integrals over $\mathbb{Z}_p$ via a point-counting argument over $\mathbb{F}_p$ (and, when $p = 2$, $\mathbb{Z}/2^m\mathbb{Z}$ for sufficiently large m). Comparing the values of the local integrals obtained by using these two methods yields the value of $|\mathcal{J}|_p$. Since this method applies to all primes p, we obtain the value of $|\mathcal{J}|$.

Proposition 29. *For any $\mathcal{P}(\mathbb{Z}_p)$-invariant measurable function $\phi_p \colon W_n(\mathbb{Z}_p)_0 \to \mathbb{R}$, we have that*

$$\int_{B \in W_n(\mathbb{Z}_p)_0} \phi_p(B) \cdot \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} |b_{i(n-i)}(B)|_p^{2i-1} dB = |\mathcal{J}'|_p \cdot \mathrm{Vol}(\mathcal{P}(\mathbb{Z}_p)) \int_{\substack{f \in \mathbb{Z}_p^n \\ \mathrm{Disc}(f) \neq 0}} \Bigg(\sum_{\substack{B \in \mathcal{P}(\mathbb{Z}_p) \backslash W_n(\mathbb{Z}_p)_0 \\ \mathrm{inv}(x \cdot A_0 + z \cdot B) = F_f(x,z)}} \phi_p(B) \Bigg) df \tag{59}$$

when n is odd, and

$$\int_{B \in W_n(\mathbb{Z}_p)_0} \phi_p(B) \cdot |b_{\frac{n}{2}\frac{n}{2}}(B)|_p^{\frac{n-2}{2}} \prod_{i=1}^{\frac{n-2}{2}} |b_{i(n-i)}(B)|_p^{2i-1} dB = \frac{1}{2} \cdot |\mathcal{J}'|_p \cdot \mathrm{Vol}(\mathcal{P}(\mathbb{Z}_p)) \int_{\substack{f \in \mathbb{Z}_p^n \\ \mathrm{Disc}(f) \neq 0}} \Bigg(\sum_{\substack{B \in \mathcal{P}(\mathbb{Z}_p) \backslash W_n(\mathbb{Z}_p)_0 \\ \mathrm{inv}(x \cdot A_0 + z \cdot B) = F_f(x,z)}} \phi_p(B) \Bigg) df \tag{60}$$

when n is even, where for $f \in \mathbb{Z}_p^n$, we write F_f to denote $F_f(x,z) = x^n + \sum_{i=1}^n f_i x^{n-i} z^i$.

Proof. We prove the proposition in the case where $n = 3$; the proof for $n > 3$ is essentially identical. Let $\mathcal{R} \subset \mathbb{Z}_p^3 \smallsetminus \{f : \mathrm{Disc}(F_f) = 0\}$ be an open subset, let $\widetilde{\sigma} \colon \mathcal{R} \to W_3(\mathbb{Z}_p)_0$ be a continuous function such that for each triple $f \in \mathbb{Z}_p^3$ we have $\mathrm{inv}(x \cdot A_0 + z \cdot \widetilde{\sigma}(f)) = F_f(x,z)$, and let $\phi_p \colon W_3(\mathbb{Z}_p)_0 \to \mathbb{R}$ be a measurable function. Upon applying the principle of permanence of identities to the proof of Proposition 24, we obtain the following result:

$$\int_{B \in \mathcal{P}(\mathbb{Z}_p) \cdot \widetilde{\sigma}(\mathcal{R})} \phi_p(B) \cdot |b_{12}(B)|_p dB = |\mathcal{J}'|_p \int_{f \in \mathcal{R}} \int_{h \in \mathcal{P}(\mathbb{Z}_p)} \phi_p(h \cdot \widetilde{\sigma}(f)) dh df, \tag{61}$$

where dh denotes the measure $ds_1 du$ on $\mathcal{P}(\mathbb{Z}_p) = \mathcal{A}(\mathbb{Z}_p) \cdot \mathcal{N}(\mathbb{Z}_p)$. Just as [11, Proposition 3.12] is deduced from [11, Proposition 3.11], it follows from (61) that

$$\int_{B \in W_3(\mathbb{Z}_p)_0} \phi_p(B) \cdot |b_{12}(B)|_p dB = |\mathcal{J}'|_p \int_{\substack{f \in \mathbb{Z}_p^3 \\ \mathrm{Disc}(f) \neq 0}} \Bigg(\sum_{\substack{B \in \mathcal{P}(\mathbb{Z}_p) \backslash W_3(\mathbb{Z}_p)_0 \\ \mathrm{inv}(x \cdot A_0 + z \cdot B) = F_f(x,z)}} \int_{h \in \mathcal{P}(\mathbb{Z}_p)} \frac{\phi_p(h \cdot B)}{\# \mathrm{Stab}_{\mathcal{P}(\mathbb{Z}_p)}(f)} dh \Bigg) df \tag{62}$$

When ϕ_p is $\mathcal{P}(\mathbb{Z}_p)$-invariant, we have $\phi_p(h \cdot B) = \phi_p(B)$ for any $h \in \mathcal{P}(\mathbb{Z}_p)$ and $B \in W_3(\mathbb{Z}_p)_0$. The proposition then follows from (62) upon observing that $\mathrm{Stab}_{\mathcal{P}(\mathbb{Z}_p)}(B) = \{1\}$ for any $B \in W_3(\mathbb{Z}_p)_0$ with $\mathrm{disc}(\mathrm{inv}(x \cdot A_0 + z \cdot B)) \neq 0$ and that $\mathrm{Vol}(\mathcal{P}(\mathbb{Z}_p)) = \mathrm{Vol}(\mathcal{N}(\mathbb{Z}_p)) \cdot \mathrm{Vol}(\mathcal{A}(\mathbb{Z}_p)) = 1 \cdot (1 - p^{-1})$.

Note that we must use $\mathcal{J}'$ instead of $\mathcal{J}$, because the integrals on the left-hand sides of (59) and (60) are over all elements of $W_n(\mathbb{Z}_p)_0$, not just those with fixed f_1. The extra factor of $\frac{1}{2}$ when n is even arises because in this case, $\mathrm{Stab}_{\mathcal{P}(\mathbb{Z}_p)}(B) = \{\pm \mathrm{id}\}$ for any $B \in W_n(\mathbb{Z}_p)_0$ such that

$\mathrm{Disc}(\mathrm{inv}(x \cdot A_0 + z \cdot B)) \neq 0$, whereas such B have trivial stabilizer when n is odd. For future reference, we note that

$$\mathrm{Vol}(\mathcal{P}(\mathbb{Z}_p)) = \begin{cases} (1-p^{-1})^{\lfloor \frac{n}{2} \rfloor}, & \text{if } p > 2, \\ 2^{-2\lfloor \frac{n}{2} \rfloor}, & \text{if } p = 2 \text{ and } n \text{ is odd}, \\ 2^{-\frac{n}{2}}, & \text{if } p = 2 \text{ and } n \text{ is even}. \end{cases} \tag{63}$$

□

We are now in position to compute the Jacobian constants $|\mathcal{J}|$ and $|\mathcal{J}'|$:

Proposition 30. *We have $|\mathcal{J}| = |\mathcal{J}'| = 2^{-\lfloor \frac{n}{2} \rfloor}$ if n is odd and $\frac{1}{2} \cdot |\mathcal{J}| = |\mathcal{J}'| = 2^{-\frac{n}{2}}$ if n is even.*

Proof. To compute $|\mathcal{J}|$, it suffices to compute $|\mathcal{J}|_p$ for every prime p since $\mathcal{J} \in \mathbb{Q}^\times$ by Lemma 27. It further suffices to compute $|\mathcal{J}'|_p$, since the rational constants $\mathcal{J}$ and $\mathcal{J}'$ differ by at most a factor of 2. We now split into cases depending on the parity of p:

Case 1: $p > 2$: Fix a form $F \in U_n(\mathbb{F}_p)$ of nonzero discriminant, and let $\phi_p \colon W_n(\mathbb{Z}_p)_0 \to \mathbb{R}$ be the indicator function of the set

$$\Sigma_F := \{B \in W_n(\mathbb{Z}_p)_0 : |b_{i(n-i)}(B)|_p = 1 \text{ for } i \in \{1, \dots, \lfloor \tfrac{n}{2} \rfloor\},\ \mathrm{inv}(x \cdot A_0 + z \cdot B) \equiv F(x,z) \pmod p\}.$$

It follows from the proof of Lemma 26 that the group $\mathcal{P}(\mathbb{Z}_p)$ acts transitively on the set

$$\{B \in W_n(\mathbb{Z}_p)_0 : |b_{i(n-i)}(B)|_p = 1 \text{ for } i \in \{1, \dots, \lfloor \tfrac{n}{2} \rfloor\},\ \mathrm{inv}(x \cdot A_0 + z \cdot B) = F'(x,z)\} \tag{64}$$

for any $F' \in U_n(\mathbb{Z}_p)$, with trivial stabilizer when n is odd and with stabilizer $\{\pm \mathrm{id}\}$ when n is even. Hence, the right-hand sides of (59) and (60) are given by

$$|\mathcal{J}'|_p \cdot \mathrm{Vol}(\mathcal{P}(\mathbb{Z}_p)) \int_{\substack{f \in \mathbb{Z}_p^n \\ F_f(x,z) \equiv F(x,z) \pmod p}} \begin{cases} 1, & \text{if } n \text{ is odd}, \\ 2^{-1}, & \text{if } n \text{ is even} \end{cases} df = \tag{65}$$

$$|\mathcal{J}'|_p \cdot \mathrm{Vol}(\mathcal{P}(\mathbb{Z}_p)) \cdot p^{-n} \cdot \begin{cases} 1, & \text{if } n \text{ is odd}, \\ 2^{-1}, & \text{if } n \text{ is even}. \end{cases}$$

On the other hand, the proof of Lemma 26 also implies that the group $\mathcal{P}(\mathbb{F}_p)$ acts transitively on the mod-p reduction $\overline{\Sigma}_F$ of Σ_F, with trivial stabilizer when n is odd and with stabilizer $\{\pm \mathrm{id}\}$ when n is even. Thus, we have that

$$\#\overline{\Sigma}_F = \#\mathcal{P}(\mathbb{F}_p) \cdot \begin{cases} 1, & \text{if } n \text{ is odd}, \\ 2^{-1}, & \text{if } n \text{ is even} \end{cases} = \mathrm{Vol}(\mathcal{P}(\mathbb{Z}_p)) \cdot \begin{cases} p^{\frac{n^2-1}{4}}, & \text{if } n \text{ is odd}, \\ 2^{-1} \cdot p^{\frac{n^2}{4}}, & \text{if } n \text{ is even}. \end{cases} \tag{66}$$

Using (82) and (66), we find that the left-hand sides of (59) and (60) are given by

$$\int_{B \in \Sigma_F} dB = \frac{\#\overline{\Sigma}_F}{\#W_n(\mathbb{F}_p)_0} = \mathrm{Vol}(\mathcal{P}(\mathbb{Z}_p)) \cdot p^{-n} \cdot \begin{cases} 1, & \text{if } n \text{ is odd}, \\ 2^{-1}, & \text{if } n \text{ is even}. \end{cases} \tag{67}$$

Now, Proposition 29 tells us (65) and (67) must be equal, so we conclude that $|\mathcal{J}'|_p = 1$.

Case 2: $p = 2$: The argument in this case is analogous to that of Case 1, so we highlight the differences. Let $m \in \mathbb{Z}_{>0}$ be sufficiently large, and fix $F(x,z) = x^n + \sum_{i=1}^n f_i x^{n-i} z^i \in U_n(\mathbb{Z}/2^m\mathbb{Z})$ of nonzero discriminant such that $f_i = 0$ for each odd $i \in \{1, \dots, n-1\}$, and let $\phi_2 \colon W_n(\mathbb{Z}_2)_0 \to \mathbb{R}$ be the indicator function of the set

$$\Sigma_F := \{B \in W_n(\mathbb{Z}_2)_0 : |b_{i(n-i)}(B)|_2 = 1 \text{ for } i \in \{1, \dots, \lfloor \tfrac{n}{2} \rfloor\},\ \mathrm{inv}(x \cdot A_0 + z \cdot B) \equiv F(x,z) \pmod{2^m}\}.$$

It follows from the proof of Lemma 26 that the group $\mathcal{P}(\mathbb{Z}_2)$ acts transitively on the set in (64) for any $F' \in U_n(\mathbb{Z}_2)$ whose $x^i z^{n-i}$-coefficient is even for each odd $i \in \{1, \dots, n-1\}$, with trivial

stabilizer when n is odd and with stabilizer $\{\pm \mathrm{id}\}$ when n is even. Thus, by analogy with (65), we find that the right-hand sides of (59) and (60) are given by

$$|\mathcal{J}'|_2 \cdot \mathrm{Vol}(\mathcal{P}(\mathbb{Z}_2)) \cdot 2^{-mn} \cdot \begin{cases} 1, & \text{if } n \text{ is odd,} \\ 2^{-1}, & \text{if } n \text{ is even.} \end{cases} \tag{68}$$

On the other hand, the proof of Lemma 26 also implies that the action of the group $\mathcal{P}(\mathbb{Z}/2^m\mathbb{Z})$ on the mod-2^m reduction $\overline{\Sigma}_F$ of Σ_F has $2^{\lfloor \frac{n}{2} \rfloor}$ distinct orbits, each of which has trivial stabilizer when n is odd and has stabilizer $\{\pm \mathrm{id}\}$ when n is even. By analogy with (67), we find that the left-hand sides of (59) and (60) are given by

$$2^{\lfloor \frac{n}{2} \rfloor} \cdot \mathrm{Vol}(\mathcal{P}(\mathbb{Z}_2)) \cdot 2^{-mn} \cdot \begin{cases} 1, & \text{if } n \text{ is odd,} \\ 2^{-1}, & \text{if } n \text{ is even.} \end{cases} \tag{69}$$

Now, Proposition 29 tells us (68) and (69) must be equal, so we conclude that $|\mathcal{J}'|_2 = 2^{\lfloor \frac{n}{2} \rfloor}$. □

Combining Proposition 30 with (58) and Theorem 18 yields (38), thus proving Theorem 22.

6. Congruence conditions

In this section, we show how the method used in §4–5 to prove Theorem 4 can be adapted to count reducible orbits of $\mathcal{G}_n(\mathbb{Z})$ on $W_n(\mathbb{Z})$ satisfying congruence conditions, and hence to prove Theorem 5. We then take $n = 3$ and apply Theorem 5 to compute the average 2-torsion in the ideal group in monogenized cubic orders, thus proving Theorem 2.

6.1. **Sieving to big families.** We say that a subset $S \subset W_n(\mathbb{Z})$ is a *big family* if we have $S = W_n^{(r_1)}(\mathbb{Z}) \cap \bigcap_p S_p$, where the sets $S_p \subset W_n(\mathbb{Z}_p)$ satisfy the following properties:

(1) S_p is $(N \times \mathcal{G}_n)(\mathbb{Z}_p)$-invariant and is the preimage under reduction modulo p^j of a nonempty subset of $W_n(\mathbb{Z}/p^j\mathbb{Z})$ for some $j > 0$ for each prime p; and
(2) S_p contains all ($\mathcal{G}_n(\mathbb{Z}_p)$-orbits of) elements $B \in W_n(\mathbb{Z}_p)_0$ such that, for all sufficiently large p, we have that $b_{i(n-i)}(B)$ is a p-adic unit for some i.

Note that a big family S is necessarily $(N \times \mathcal{G}_n)(\mathbb{Z})$-invariant. Given such a family S, we have the following asymptotic for $\sharp\big((N \times \mathcal{G}_n)(\mathbb{Z}) \backslash S_{\mathrm{red}}\big)$:

Theorem 31. *Suppose that $S \subset W_n(\mathbb{Z})$ is a big family. Then we have that*

$$\sharp\left(\frac{S_{\mathrm{red}}}{(N \times \mathcal{G}_n)(\mathbb{Z})}\right) = N_n^{(r_1)}(X) \cdot |\mathcal{J}| \cdot \left\{ \begin{array}{ll} \left(\prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \zeta(2i)\right) \cdot 2^{\lfloor \frac{n}{2} \rfloor} \cdot \prod_p \xi_{n,p} \int_{B \in (S_p)_0} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} |b_{i(n-i)}(B)|_p^{2i-1} dB, & \text{if } n \text{ is odd,} \\ \left(\zeta(\frac{n}{2}) \prod_{i=1}^{\frac{n-2}{2}} \zeta(2i)\right) \cdot \frac{1}{2} \cdot \prod_p \xi_{n,p} \int_{B \in (S_p)_0} |b_{\frac{n}{2}\frac{n}{2}}(B)|_p^{\frac{n-2}{2}} \prod_{i=1}^{\frac{n-2}{2}} |b_{i(n-i)}(B)|_p^{2i-1} dB, & \text{if } n \text{ is even} \end{array} \right\} + o(X^{\frac{n^2+n-2}{2}}). \tag{70}$$

where $\xi_{n,p} = \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \frac{1-p^{-2i}}{1-p^{-1}}$ if n is odd and $\xi_{n,p} = \frac{1-p^{-\frac{n}{2}}}{1-p^{-1}} \prod_{i=1}^{\frac{n-2}{2}} \frac{1-p^{-2i}}{1-p^{-1}}$ if n is even.

Proof. Let n be odd (the argument for even n is identical), and suppose that the theorem holds with W_n replaced by W_{n,f_1} and $(S_p)_0$ replaced by $(S_p)_0 \cap W_{n,f_1}(\mathbb{Z}_p)$. Summing the count for fixed f_1 over the possible values of f_1 yields (70) with the product of p-adic densities on the right-hand side replaced by the following expression:

$$\frac{1}{n} \cdot \sum_{f_1=0}^{n-1} \prod_p \xi_{n,p} \int_{B \in (S_p)_0 \cap W_{n,f_1}(\mathbb{Z}_p)} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} |b_{i(n-i)}(B)|_p^{2i-1} dB. \tag{71}$$

Let $n = \prod_p p^{f_p}$ denote the prime factorization of n. Through an application of the Chinese Remainder Theorem, we can reexpress (71) as

$$\prod_p \xi_{n,p} \cdot \frac{1}{p^{f_p}} \cdot \sum_{f_1 \in \mathbb{Z}/p^{f_p}\mathbb{Z}} \int_{B \in (S_p)_0 \cap W_{n,f_1}(\mathbb{Z}_p)} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} |b_{i(n-i)}(B)|_p^{2i-1} dB. \tag{72}$$

Now, for any measurable $N(\mathbb{Z}_p)$-invariant function $\phi_p \colon W_n(\mathbb{Z}_p)_0 \to \mathbb{R}$, it follows from a Jacobian change-of-variables that

$$\frac{1}{p^{f_p}} \cdot \sum_{f_1 \in \mathbb{Z}/p^{f_p}\mathbb{Z}} \int_{B \in W_{n,f_1}(\mathbb{Z}_p)} \phi_p(B) dB = \int_{B \in W_n(\mathbb{Z}_p)_0} \phi_p(B) dB. \tag{73}$$

Thus, taking ϕ_p to be product of the indicator function of S_p with the function $\prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} |b_{i(n-i)}(B)|_p^{2i-1}$ and combining (72) with (73) yields (70) when n is odd.

We have thus shown that it suffices to prove the theorem with f_1 fixed, which we do as follows. To begin with we shall assume that the big family $S \subset W_{n,f_1}(\mathbb{Z})$ is defined by *finitely many* congruence conditions, meaning that $S_p = W_{n,f_1}(\mathbb{Z}_p)$ for all but finitely many p. To simplify the exposition, we will additionally restrict our consideration to the case where $n = 3$ and $f_1 = 0$, as the proof is identical for larger values of n and f_1.

Observe that there exist integers $m, k > 0$ such that the set S may be regarded as the disjoint union of k translates $\mathcal{L}_1, \dots, \mathcal{L}_k$ of the lattice $m \cdot W_{3,0}(\mathbb{Z})$. Given $r \in (\mathbb{Z}/m\mathbb{Z})^\times$ and $B \in W(\mathbb{Z}/m\mathbb{Z})$, denote by $r \cdot B \in W_{3,0}(\mathbb{Z}/m\mathbb{Z})$ the element that arises by acting on B with the element of $\mathcal{A}(\mathbb{Z}/m\mathbb{Z})$ corresponding to r. Then any element $B' \in W_{3,0}^{(r_1)}(\mathbb{Z})$ such that $B' \equiv r \cdot B \pmod m$ for some $r \in (\mathbb{Z}/m\mathbb{Z})^\times$ and $B \in S$ is also an element of S, because S is the preimage in $W_{3,0}^{(r_1)}(\mathbb{Z})$ of an $\mathcal{G}_3(\mathbb{Z}/m\mathbb{Z})$-invariant subset of $W_{3,0}(\mathbb{Z}/m\mathbb{Z})$. Thus, the group $(\mathbb{Z}/m\mathbb{Z})^\times$ acts on the set of lattice translates $\{\mathcal{L}_1, \dots, \mathcal{L}_k\}$, and it suffices to prove the theorem with the set S replaced by a single $(\mathbb{Z}/m\mathbb{Z})^\times$-orbit on the set of lattice translates $\{\mathcal{L}_1, \dots, \mathcal{L}_k\}$. Without loss of generality, we may assume that this orbit comprises the lattice translates $\mathcal{L}_1, \dots, \mathcal{L}_\ell$ for some $\ell \in \{1, \dots, k\}$.

For $j \in \{1, \dots, \ell\}$, write $\mathcal{L}_j = B_j + m \cdot W_{3,0}(\mathbb{Z})$, where $B_j \in W_{3,0}(\mathbb{Z})$. The computation of $\#(\mathcal{G}_3(\mathbb{Z})\backslash((\mathcal{L}_j \cap W_{3,0}^{(r_1)}(\mathbb{R}))_{\mathrm{red}})_X)$ is analogous to that of $\#(\mathcal{G}_3(\mathbb{Z})\backslash(W_{3,0}^{(r_1)}(\mathbb{Z})_{\mathrm{red}})_X)$ in §4.1–§4.2, so we summarize the key points. By analogy with (22), we have that

$$\#\left(\frac{((\mathcal{L}_j \cap W_{3,0}^{(r_1)}(\mathbb{R}))_{\mathrm{red}})_X}{\mathcal{G}_3(\mathbb{Z})}\right) = \frac{1}{C_H} \int_{s \in \mathcal{A}^\star} \int_{u \in \mathcal{N}^\star(s_1)} \#(\mathcal{B}(u, s_1)_X \cap (\mathcal{L}_j)_0) du \frac{ds_1}{s_1^2} + o(X). \tag{74}$$

First suppose $a_j \not\equiv 0 \pmod m$. Then $(\mathcal{L}_j)_0 = \varnothing$, and so $\#(\mathcal{G}_3(\mathbb{Z})\backslash((\mathcal{L}_j \cap W_{3,0}^{(r_1)}(\mathbb{R}))_{\mathrm{red}})_X) = o(X)$; on the other hand, we must also have that $((\mathcal{L}_j)_p)_0 = \varnothing$ for some prime $p \mid m$, so the theorem holds in this case. We may thus assume that $b_{11}(B_j) \equiv 0 \pmod m$ and in fact that $b_{11}(B_j) = 0$. Then, slicing yields a sum over $b \equiv b_{12}(B_j) \pmod m$, and the application of Proposition 19 gives an additional factor of m^{-3} because we are counting lattice points in the 3-dimensional region $\mathcal{B}_b(u, s_1)_X$ on a lattice translate of $m \cdot V(\mathbb{Z})$. Thus, by analogy with (27), we have that

$$\#\left(\frac{((\mathcal{L}_j \cap V^{(i)}(\mathbb{R}))_{\mathrm{red}})_X}{\mathcal{G}_3(\mathbb{Z})}\right) = \frac{1}{C_H} \sum_{\substack{b \in \mathbb{Z} \\ b \neq 0 \\ b \equiv b_j \pmod m}} \int_{s_1 \geq \Gamma} \int_{u \in \mathcal{N}^\star(s_1)} m^{-3} \cdot \mathrm{Vol}(\mathcal{B}_b(u, s_1)_X) du \frac{ds_1}{s_1^2} + o(X) \tag{75}$$

Let $m' := \gcd(b_j, m)$; observe that m' is independent of $j \in \{1, \dots, \ell\}$ because the set $\{\mathcal{L}_1, \dots, \mathcal{L}_\ell\}$ is a $(\mathbb{Z}/m\mathbb{Z})^\times$-orbit. Further notice that every mod-m residue class b such that $\gcd(b, m) = m'$ is represented exactly once among the b_j. Consequently, after summing (75) over $j \in \{1, \dots, \ell\}$, we

obtain by analogy with (37) that

$$\#\left(\frac{(S_{\mathrm{red}})_X}{\mathcal{G}_3(\mathbb{Z})}\right) = \sum_{\substack{b\in\mathbb{Z}_{>0}\\ \gcd(b,m)=m'}} b^{-2}\cdot\frac{1}{C_H}\int_{\beta\geq 0} m^{-3}\cdot\beta\cdot\mathrm{Vol}(\mathcal{B}_\beta(X))d\beta + o(X) \tag{76}$$
$$= m^{-3}m'^{-2}\cdot\Bigg(\prod_{p\mid mm'^{-1}}(1-p^{-2})\Bigg)\cdot\zeta(2)\cdot N_3^{(r_1)}(X)+o(X).$$

On the other hand, if we write $e_p := \nu_p(m)$ and $e'_p := \nu_p(m')$ for each prime p, we have that

$$\int_{B\in((\mathcal{L}_j)_p)_0}|b_{12}(B)|_p dB = \begin{cases}\displaystyle\int_{\substack{B\in W_{3,0}(\mathbb{Z}_p)_0\\ B\equiv B_j \,(\mathrm{mod}\, p^{e_p})}}|b_{12}(B)|_p dF = p^{-5e_p}\cdot(1+p^{-1})^{-1}, & \text{if } p\nmid mm'^{-1},\\ \displaystyle\int_{\substack{B\in W_{3,0}(\mathbb{Z}_p)_0\\ B\equiv B_j \,(\mathrm{mod}\, p^{e_p})}}|b_{12}(B)|_p dB = p^{-4e_p-e'_p}, & \text{if } p\mid mm'^{-1},\end{cases} \tag{77}$$

where the last step above follows from splitting the regions $\{B\in W_{3,0}(\mathbb{Z}_p)_0 : B\equiv B_j \pmod{p^{e_p}}\}$ and $W_{3,0}(\mathbb{Z}_p)_0$ into level sets for the function $|b_{12}(B)|_p$, integrating on each level set, and summing up. Then, since $\ell = \#\big(\mathbb{Z}/(mm'^{-1})\mathbb{Z}\big)^\times = \prod_{p\mid mm'^{-1}} p^{e_p-e'_p}(1-p^{-1})$, summing (77) over $j\in\{1,\dots,\ell\}$ and multiplying over all primes p yields that

$$\prod_p(1+p^{-1})\int_{B\in(S_p)_0}|b_{12}(B)|_p dB = \#\big(\mathbb{Z}/(mm'^{-1})\mathbb{Z}\big)^\times\cdot\prod_p\int_{B\in((\mathcal{L}_1)_p)_0}|b_{12}(B)|_p dB = \tag{78}$$
$$\prod_{p\nmid mm'^{-1}}p^{-5e_p}\cdot\prod_{p\mid mm'^{-1}}p^{-3e_p-2e'_p}\cdot(1-p^{-2}) = m^{-3}m'^{-2}\cdot\prod_{p\mid mm'^{-1}}(1-p^{-2}).$$

Comparing (76) and (78) yields the theorem when S is replaced by $\bigsqcup_{j=1}^{\ell}\mathcal{L}_j$, as desired.

It remains to prove the theorem in the case where S is defined by infinitely many congruence conditions. First note that the proof of (38) (or [13, Theorem 1.5]) implies the following uniformity estimate: the number of $\mathcal{G}_n(\mathbb{Z})$-orbits of $B\in(W_{n,f_1}^{(r_1)}(\mathbb{Z})_{\mathrm{red}})_X$ with $b_{i(n-i)}(B)$ divisible by some prime larger than $Y>1$, for some i, is $O\big(X^{\frac{n^2+n-2}{2}}Y^{-1}\big)+O_\epsilon\big(X^{\frac{n^2+n-2}{2}-\frac{1}{5}+\epsilon}\big)$, where the implied constant is independent of X and Y. Given this uniformity estimate, Theorem 31 follows from the "finitely many congruence conditions" case by applying an inclusion-exclusion sieve. □

Remark. In the proof of Theorem 31, the assumption that S is the preimage of an $\mathcal{G}_n(\mathbb{Z}/m\mathbb{Z})$-invariant subset of $W_n(\mathbb{Z}/m\mathbb{Z})$ caused the slicing parameters of the elements of S to be invariant under multiplication by units modulo m. It is important to note that Theorem 31 does *not* always hold without this invariance.

Theorem 31 gives a formula for the number of lattice points of bounded height satisfying big sets of congruence conditions in cusps of fundamental sets for the action of $(N\times\mathcal{G}_n)(\mathbb{Z})$ on $W_n(\mathbb{R})$ that is easy to compute in some cases. For example, as part of the proof of Theorem 2 in §6.2, we directly compute the p-adic local factor on the right-hand side of (70) in the case where $n=3$ and $S_p\subset W_3(\mathbb{Z}_p)$ is the subset of projective elements. The formula in Theorem 31 also turns out to be convenient for estimating the contribution of elements having big stabilizer (see the remark after Theorem 22 for the definition) to $\sharp\big((N\times\mathcal{G}_n)(\mathbb{Z})\backslash W_n^{(r_1)}(\mathbb{Z})_{\mathrm{red}}\big)$. To this end, let

$$W_n^{(r_1)}(\mathbb{Z})_{\mathrm{bigstab}} := \big\{B\in W_n^{(r_1)}(\mathbb{Z}) : \mathrm{Stab}_{\mathcal{G}_n(\mathbb{Z})}(B) \text{ is big}\big\}.$$

Then we have the following bound:

Proposition 32. *We have that* $\sharp\big((N\times\mathcal{G}_n)(\mathbb{Z})\backslash\big(W_n^{(r_1)}(\mathbb{Z})_{\mathrm{bigstab}}\big)_{\mathrm{red}}\big) = o\big(X^{\frac{n^2+n-2}{2}}\big)$.

Proof. From of Theorem 6, it follows that $\mathrm{Stab}_{\mathcal{G}_n(\mathbb{Z})}(B)$ is big only if the form $\mathrm{inv}(x\cdot A_0+z\cdot B)$ is reducible over $\mathbb{Z}$. Thus, letting

$$W_n(\mathbb{Z}_p)_{\mathrm{split}} := \{B\in W_n(\mathbb{Z}_p) : \mathrm{inv}(x\cdot A_0+z\cdot B) \text{ is reducible modulo } p\}$$

for each prime p, we have that $W_n^{(r_1)}(\mathbb{Z})_{\mathrm{bigstab}} \subset W_n^{(r_1)}(\mathbb{Z})\cap\bigcap_p W_n(\mathbb{Z}_p)_{\mathrm{split}}$. Then, upon combining Theorem 31 with the trivial bound $|x|_p\le 1$ for any $x\in\mathbb{Z}_p$, we deduce that

$$\lim_{X\to\infty}\frac{\sharp\big((N\times\mathcal{G}_n)(\mathbb{Z})\backslash\big(W_n^{(r_1)}(\mathbb{Z})_{\mathrm{bigstab}}\big)_{\mathrm{red}}\big)}{X^{\frac{n^2+n-2}{2}}} \ll \prod_{p<Y}(1+p^{-1})^2\int_{B\in(W_n(\mathbb{Z}_p)_{\mathrm{split}})_0} dB \tag{79}$$

for any number $Y>0$, where the implied constant is independent of Y. To prove the proposition, it now suffices to estimate the factor at p on the right-hand side of (79) for each prime $p\gg 1$.

For a ring R, consider the subgroup $\mathcal{A}(R),\mathcal{N}(R)\subset \mathrm{SO}_{A_0}(R)$ defined as follows:

- $\mathcal{A}(R)$ is the subgroup whose elements are those of the form (12) when n is odd and of the form (13) when n is even, where $s_i\in R^\times$ for each $i\in\{1,\dots,\lfloor\frac{n}{2}\rfloor\}$.
- $\mathcal{N}(R)$ is the subgroup of all lower-triangular unipotent matrices with entries in R.

Let $\mathcal{P}(R) := \mathcal{A}(R)\cdot\mathcal{N}(R)\subset \mathrm{SO}_{A_0}(R)$, and observe that the action of $\mathcal{P}(R)$ on $W_n(R)$ preserves the subspace $W_n(R)_0$. We now take $R=\mathbb{F}_p$. When $p>2$, it follows from the proof of Lemma 26 that $\mathcal{P}(\mathbb{F}_p)$ acts simply transitively on the set $\mathcal{O}_F := \{B\in W_n(\mathbb{F}_p)_0 : \mathrm{inv}(x\cdot A_0+z\cdot B)=F(x,z)\}$ for any separable form $F\in U_n(\mathbb{F}_p)$. Thus, we have for such a form F that

$$\#\mathcal{O}_F = \#\mathcal{P}(\mathbb{F}_p) = (1-p^{-1})^{\lfloor\frac{n}{2}\rfloor}\cdot\begin{cases} p^{\frac{n^2-1}{4}}, & \text{if } n \text{ is odd},\\ p^{\frac{n^2}{4}}, & \text{if } n \text{ is even}.\end{cases} \tag{80}$$

It is a well-known result (e.g., see [7, §10.7]) that the number of irreducible separable forms $F\in U_n(\mathbb{F}_p)$ is given by the following asymptotic formula:

$$n^{-1}\cdot p^n + O(p^{n-1}), \tag{81}$$

where the implied constant is independent of the prime p. Combining (80) with (81) together with the fact that

$$\dim_{\mathbb{F}_p} W_n(\mathbb{F}_p)_0 = \begin{cases}\frac{n^2-1}{4}+n, & \text{if } n \text{ is odd},\\ \frac{n^2}{4}+n, & \text{if } n \text{ is even}\end{cases} \tag{82}$$

yields the following bound:

$$\begin{aligned}\int_{B\in(W_n(\mathbb{Z}_p)_{\mathrm{split}})_0} dB &\le 1-\left\{\begin{array}{ll}\frac{\left((1-p^{-1})^{\lfloor\frac{n}{2}\rfloor}\cdot p^{\frac{n^2-1}{4}}\right)\cdot(n^{-1}\cdot p^n+O(p^{n-1}))}{p^{\frac{n^2-1}{4}+n}}, & \text{if } n \text{ is odd},\\ \frac{\left((1-p^{-1})^{\lfloor\frac{n}{2}\rfloor}\cdot p^{\frac{n^2}{4}}\right)\cdot(n^{-1}\cdot p^n+O(p^{n-1}))}{p^{\frac{n^2}{4}+n}}, & \text{if } n \text{ is even}\end{array}\right\}\\ &\le 1-n^{-1}-O(p^{-1}).\end{aligned} \tag{83}$$

Substituting the bound (83) into the right-hand side of (79) and taking the limit as $Y\to\infty$ on both sides yields the proposition. □

While Theorem 31 has its uses, it is not easy to apply when S is defined by congruence conditions involving the coefficients of the binary forms $F\in U^{(r_1)}(\mathbb{Z})$. We now express the p-adic local factors on the right-hand side of (70) in a form that is more convenient in the case where S is defined by such congruence conditions. In order to extract the dependence of the local factors on the coefficients of the binary forms, we perform what is in essence the same change-of-variables that we used in the proof of Proposition 24. We thus obtain the following formula:

Combining Theorem 22 with Proposition 32 yields Theorem 4. Finally, combining Theorem 31 with Propositions 32 and 30 yields Theorem 31.

Taking ϕ_p to be the indicator function of $(S_p)_0$ for each prime p in Proposition 29, combining the result with Theorem 31, and observing that

$$\prod_p |\mathcal{J}'|_p \cdot \xi_{n,p} \cdot \mathrm{Vol}(\mathcal{P}(\mathbb{Z}_p)) = \begin{cases} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \zeta(2i)^{-1}, & \text{if } n \text{ is odd,} \\ 2^{\frac{n}{2}} \cdot \zeta(\frac{n}{2})^{-1} \prod_{i=1}^{\frac{n-2}{2}} \zeta(2i)^{-1}, & \text{if } n \text{ is even} \end{cases}$$

yields the following:

Theorem 33. *Suppose that $S \subset W_n(\mathbb{Z})$ is a big family. Then we have that*

$$\#\left(\frac{S_{\mathrm{red}}}{(N \times \mathcal{G}_n)(\mathbb{Z})}\right) = N_n^{(r_1)}(X) \cdot \prod_p \int_{\substack{f \in \mathbb{Z}_p^n \\ \mathrm{Disc}(f) \neq 0}} \#\left(\frac{\mathrm{inv}^{-1}(f) \cap (S_p)_0}{\mathcal{P}(\mathbb{Z}_p)}\right) df + o\big(X^{\frac{n^2+n-2}{2}}\big). \tag{84}$$

We say that a subset $\Sigma \subset U_n(\mathbb{Z})$ is *defined by finitely many congruence conditions* if we have $\Sigma = U_n^{(r_1)}(\mathbb{Z}) \cap \bigcap_p \Sigma_p$, where the sets $\Sigma_p \subset U_n(\mathbb{Z}_p)$ satisfy the following properties: (1) Σ_p is the preimage under reduction modulo p^j of a nonempty subset of $U_n(\mathbb{Z}/p^j\mathbb{Z})$ for some $j > 0$ for each prime p; and (2) Σ_p contains all of $U_n(\mathbb{Z}_p)$ for all sufficiently large p. Observe that if $\Sigma \subset \mathbb{Z}$ is defined by finitely many congruence conditions, then so is $\mathrm{inv}^{-1}(\Sigma) \subset W_n(\mathbb{Z})$; thus, Theorem 5 is a special case of Theorem 33.

6.2. **Computing the volume of projective elements.** Let $W_n(\mathbb{Z}_p)^{\mathrm{proj}}$ denote the subset of projective elements of $W_n(\mathbb{Z}_p)$. In this section, we prove Theorem 2 by applying Theorem 31 in the case where $n = 3$ and $S_p = W_3(\mathbb{Z}_p)^{\mathrm{proj}}$ for every prime p.

Let $B = [b_{ij}] \in W_3(\mathbb{Z}_p)_0$. Then Proposition 8 implies that B fails to be projective if and only if

$$b_{12} \equiv b_{23}^2 + (b_{13} - b_{22})b_{33} \equiv 0 \pmod{p}. \tag{85}$$

Let $t := b_{13} - b_{22}$. The equation $b_{23}^2 + tb_{33}$ defines a smooth conic curve in the projective plane $\mathbb{P}^2_{\mathbb{F}_p}$ with coordinates $[b_{23} : t : b_{33}]$. This curve has exactly $p+1$ points over $\mathbb{F}_p$, and so the (affine) equation $b_{23}^2 + tb_{33} \equiv 0 \pmod{p}$ has p^2 solutions in the three variables b_{23}, t, b_{33}, and it further follows that the equation $b_{23}^2 + (b_{13} - b_{22})b_{33} \equiv 0 \pmod{p}$ has p^3 solutions in the four variables $b_{13}, b_{22}, b_{23}, b_{33}$.

From the previous paragraph, we deduce that for every integer $k \geq 0$, the p-adic density of the level set $\mathscr{W}_k := \{B \in W_3(\mathbb{Z}_p)_0^{\mathrm{proj}} : \nu_p(b_{12}(B)) = k\}$ in $W_3(\mathbb{Z}_p)_0$ is given by $1 - p^{-1}$ if $k = 0$ and by $p^{-k}(1 - p^{-1})^2$ if $k > 0$. Summing over the level sets $\mathscr{W}_k$ yields that

$$\begin{aligned} \int_{B \in W_3(\mathbb{Z}_p)_0^{\mathrm{proj}}} |b_{12}(B)|_p dB &= \sum_{k \geq 0} \int_{B \in \mathscr{W}_k} p^{-k} dB = (1 - p^{-1}) + \sum_{k \geq 1} p^{-2k}(1 - p^{-1})^2 \\ &= 1 - p^{-1} + p^{-2}(1 + p^{-1})^{-1}(1 - p^{-1}). \end{aligned} \tag{86}$$

Now, let $W_3^{(r_1)}(\mathbb{Z})^{\mathrm{proj}}$ denote the subset of projective elements of $W_3^{(r_1)}(\mathbb{Z})$. Substituting (86) into Theorem 31 and dividing by $N_3^{(r_1)}(X)$ yields Theorem 2.

Acknowledgments

The first-named author was supported by an NSERC discovery grant and a Sloan fellowship, the second-named author was supported by Queen Elizabeth II/Steve Halperin Scholarship in Science and Technology at the University of Toronto, and the third-named author was supported by the NSF Graduate Research Fellowship. We thank Manjul Bhargava for engaging with us in several enlightening conversations and for offering many comments and suggestions. We are also grateful to Noam D. Elkies, Aaron Landesman, Aurel Page, and Peter Sarnak for helpful discussions, and to Will Sawin for suggesting the proof of Lemma 14.

References

[1] S. A. Altuğ, A. Shankar, I. Varma, and K. H. Wilson. The number of D_4-fields ordered by conductor. *J. Eur. Math. Soc. (JEMS)*, 23(8):2733–2785, 2021.

[2] M. Artin. *Algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

[3] M. Bhargava. Higher composition laws. II. On cubic analogues of Gauss composition. *Ann. of Math. (2)*, 159(2):865–886, 2004.

[4] M. Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math. (2)*, 162(2):1031–1063, 2005.

[5] M. Bhargava. Higher composition laws. IV. The parametrization of quintic rings. *Ann. of Math. (2)*, 167(1):53–94, 2008.

[6] M. Bhargava. The density of discriminants of quintic rings and fields. *Ann. of Math. (2)*, 172(3):1559–1591, 2010.

[7] M. Bhargava and B. H. Gross. The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point. In *Automorphic representations and L-functions*, volume 22 of *Tata Inst. Fundam. Res. Stud. Math.*, pages 23–91. Tata Inst. Fund. Res., Mumbai, 2013.

[8] M. Bhargava, J. Hanke, and A. Shankar. The mean number of 2-torsion elements in class groups of n-monogenized cubic fields. *arXiv preprint 2010.15744*, 2020.

[9] M. Bhargava and A. Shankar. The average number of elements in the 4-selmer groups of elliptic curves is 7, 2013.

[10] M. Bhargava and A. Shankar. The average size of the 5-selmer group of elliptic curves is 6, and the average rank is less than 1, 2013.

[11] M. Bhargava and A. Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Ann. of Math. (2)*, 181(1):191–242, 2015.

[12] M. Bhargava and A. Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Ann. of Math. (2)*, 181(2):587–621, 2015.

[13] M. Bhargava, A. Shankar, and X. Wang. Squarefree values of polynomial discriminants I. *arXiv preprint 1611.09806*, 2016.

[14] M. Bhargava and I. Varma. On the mean number of 2-torsion elements in the class groups, narrow class groups, and ideal groups of cubic orders and fields. *Duke Math. J.*, 164(10):1911–1933, 2015.

[15] M. Bhargava and I. Varma. The mean number of 3-torsion elements in the class groups and ideal groups of quadratic orders. *Proc. Lond. Math. Soc. (3)*, 112(2):235–266, 2016.

[16] A. Borel. Ensembles fondamentaux pour les groupes arithmétiques. In *Colloq. Théorie des Groupes Algébriques (Bruxelles, 1962)*, pages 23–40. Librairie Universitaire, Louvain; GauthierVillars, Paris, 1962.

[17] A. Borel and Harish-Chandra. Arithmetic subgroups of algebraic groups. *Ann. of Math. (2)*, 75:485–535, 1962.

[18] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[19] H. Cohen and J. Martinet. Heuristics on class groups: some good primes are not too good. *Math. Comp.*, 63(207):329–334, 1994.

[20] H. Davenport. On a principle of Lipschitz. *J. London Math. Soc.*, 26:179–183, 1951.

[21] H. Davenport. On the class-number of binary cubic forms. I. *J. London Math. Soc.*, 26:183–192, 1951.

[22] H. Davenport. On the class-number of binary cubic forms. II. *J. London Math. Soc.*, 26:192–198, 1951.

[23] H. Davenport. Corrigendum: On the Class-Number of Binary Cubic Forms (I). *J. London Math. Soc.*, 27(4):512, 1952.

[24] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551):405–420, 1971.

[25] D. Gordon, D. Grenier, and A. Terras. Hecke operators and the fundamental domain for $\mathrm{SL}(3, \mathbf{Z})$. *Math. Comp.*, 48(177):159–178, 1987.

[26] D. Grenier. Fundamental domains for the general linear group. *Pacific J. Math.*, 132(2):293–317, 1988.

[27] D. Grenier. On the shape of fundamental domains in $\mathrm{GL}(n, \mathbb{R})/\mathrm{O}(n)$. *Pacific J. Math.*, 160(1):53–66, 1993.

[28] F. Gundlach. *Parametrizing Extensions with Fixed Galois Group*. ProQuest LLC, Ann Arbor, MI, 2019. Thesis (Ph.D.)–Princeton University.

[29] W. Ho, A. Shankar, and I. Varma. Odd degree number fields with odd class number. *Duke Math. J.*, 167(5):995–1047, 2018.

[30] G. Malle. On the distribution of class groups of number fields. *Experiment. Math.*, 19(4):465–474, 2010.

[31] F. Mertens. Ueber einige asymptotische Gesetze der Zahlentheorie. *J. Reine Angew. Math.*, 77:289–338, 1874.

[32] D. W. Morris. *Introduction to arithmetic groups*. Deductive Press, 2015.

[33] V. Platonov and A. Rapinchuk. *Algebraic groups and number theory*, volume 139 of *Pure and Applied Mathematics*. Academic Press, Inc., Boston, MA, 1994. Translated from the 1991 Russian original by R. Rowen.

[34] G. C. Sanjaya and X. Wang. On the squarefree values of $a^4 + b^3$. *arXiv preprint 2107.10380*, 2021.

[35] P. Sarnak and A. Strömbergsson. Minima of Epstein's zeta function and heights of flat tori. *Invent. Math.*, 165(1):115–151, 2006.
[36] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.
[37] A. Shankar and X. Wang. Rational points on hyperelliptic curves having a marked non-Weierstrass point. *Compos. Math.*, 154(1):188–222, 2018.
[38] T. Shintani. On Dirichlet series whose coefficients are class numbers of integral binary cubic forms. *J. Math. Soc. Japan*, 24:132–188, 1972.
[39] A. Siad. Monogenic fields with odd class number part I: odd degree. *arXiv preprint 2011.08834*, 2020.
[40] A. Siad. Monogenic fields with odd class number part II: even degree. *arXiv preprint 2011.08842*, 2020.
[41] C. L. Siegel. The average measure of quadratic forms with given determinant and signature. *Ann. of Math. (2)*, 45:667–685, 1944.
[42] A. Swaminathan. Average 2-torsion in class groups of rings associated to binary n-ic forms. *arXiv preprint 2011.13578*, 2020.
[43] L. Y. Vulakh. Units in some families of algebraic number fields. *Trans. Amer. Math. Soc.*, 356(6):2325–2348, 2004.
[44] M. M. Wood. *Moduli spaces for rings and ideals*. ProQuest LLC, Ann Arbor, MI, 2009. Thesis (Ph.D.)–Princeton University.
[45] M. M. Wood. Parametrization of ideal classes in rings associated to binary forms. *J. Reine Angew. Math.*, 689:169–199, 2014.

Department of Mathematics, University of Toronto, Toronto, OT M5S 1A1
E-mail address, Arul Shankar: arul.shnkr@gmail.com

Department of Mathematics, Princeton University, Princeton, NJ 08540
School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540
E-mail address, Artane Siad: as4426@princeton.edu

Department of Mathematics, Princeton University, Princeton, NJ 08544
E-mail address, Ashvin A. Swaminathan: ashvins@math.princeton.edu

Department of Mathematics, University of Toronto, Toronto, OT M5S 1A1
E-mail address, Ila Varma: ila@math.toronto.edu