

# *Algebra & Number Theory*

Volume 19  
2025  
No. 6

**Geometry-of-numbers methods in the cusp**

Arul Shankar, Artane Siad, Ashvin A. Swaminathan and Ila Varma



# Geometry-of-numbers methods in the cusp

Arul Shankar, Artane Siad, Ashvin A. Swaminathan and Ila Varma

We develop new methods for counting integral orbits having bounded invariants that lie inside the cusps of fundamental domains for coregular representations. We illustrate these methods for a representation of cardinal interest in number theory, namely that of the split orthogonal group acting on the space of quadratic forms.

1. Introduction	1099
2. Counting reducible integral orbits on binary quartic forms	1108
3. Reduction theory for the action of $G(\mathbb{Z})$ on $W(\mathbb{R})$	1118
4. The action of the subgroup $\mathcal{P}$ on the reducible hyperplane $W_0$	1127
5. Counting reducible $G(\mathbb{Z})$ -orbits on $W(\mathbb{Z})$	1131
6. A local-to-global principle for the action of $\mathcal{P}(\mathbb{Z})$ on $W_0(\mathbb{Z})$	1138
Acknowledgments	1142
References	1143

## 1. Introduction

A *coregular representation*  $(G, W)$  consists of a reductive algebraic group  $G$ , defined over  $\mathbb{Z}$ , and a finite-dimensional representation  $W$  of  $G$ , also defined over  $\mathbb{Z}$ , such that the ring of polynomial invariants for the action of the semisimplification of  $G$  on  $W$  is freely generated (say by the elements  $p_1, \dots, p_k$ ). We then say that  $U = \text{Aff}^k$  is the *space of relative invariants*, and note that for any ring  $R$  we have the natural map  $W(R) \rightarrow U(R)$  given by  $w \mapsto (p_1(w), \dots, p_k(w))$ <sup>1</sup> is freely and finitely generated over  $\mathbb{Z}$ . Many objects of interest in number theory and arithmetic geometry admit natural parametrizations in terms of integral orbits of coregular representations. Typically, these parametrizations impose the following three pieces of structure on the pair  $(G, W)$  and the associated invariant space  $U$ :

- (1) an algebraic notion of *nondegeneracy* for the orbits of  $G$  on  $W$ ;
- (2) a natural notion of *height* on  $U(\mathbb{R})$ , which then lifts to a  $G(\mathbb{R})$ -invariant notion of height on  $W(\mathbb{R})$ ;
- (3) an arithmetic notion of *irreducibility* for the orbits of  $G(\mathbb{Z})$  on  $W(\mathbb{Z})$ .

We note that *prehomogeneous* representations, i.e., representations whose rings of invariants are generated by a single element, are all coregular. In that case, the single generating invariant (usually termed the discriminant) is the height that is used.

*MSC2020:* primary 11R29, 11R45; secondary 11H55, 11E76.

*Keywords:* geometry-of-numbers, coregular representations, fundamental domain, cusps, irreducibility.

<sup>1</sup>More algebrogeometrically, the ring of relative invariants is  $\mathbb{Z}[W]^G$ , while the space of relative invariants is  $U := W // G = \text{Spec}(\mathbb{Z}[W]^G)$ .

A landmark result of Borel and Harish-Chandra [19] implies that the number of nondegenerate  $G(\mathbb{Z})$ -orbits on  $W(\mathbb{Z})$  having bounded height is finite. In light of this result, it is natural to ask the following fundamental question: *what are the asymptotics for the number of nondegenerate  $G(\mathbb{Z})$ -orbits on  $W(\mathbb{Z})$  having bounded height?* Answering this question for just those integral orbits that are *irreducible* has proven to be a problem with significant applications in arithmetic statistics, the study of distributions of arithmetic objects. Indeed, counting integral irreducible orbits of coregular representations played a key role in the proofs of many breakthrough results, from determining asymptotics for  $S_n$ -number fields of small fixed degree ordered by discriminant (see [2; 4; 24; 29]), to computing average sizes of  $p$ -class groups in certain families of number fields for small primes  $p$  (see [2; 14; 15; 24; 31; 46; 47; 49]), to calculating average  $n$ -Selmer ranks of elliptic curves and hyperelliptic Jacobians for small  $n$  (see [6; 7; 8; 9; 10; 15; 32; 33; 40; 43]), and many more.

More recently, counting *reducible* integral orbits of coregular representations has emerged as a problem of significant interest in its own right, yielding applications toward determining the sizes of the 3-torsion in the class groups of quadratic orders [11; 45], counting octic  $D_4$ -number fields ordered by Artin conductor [1] and by discriminant [42], studying families of elliptic curves ordered by conductor [44], and carrying out squarefree sieves on families of polynomials [16] and binary  $n$ -ic forms [17]. However, in all of these applications, the counts of reducible orbits were obtained using ad hoc methods. Furthermore, the latter three results cited above do not actually prove asymptotics, and merely obtain upper bounds on the number of reducible orbits of bounded height. This is in stark contrast with the case of irreducible orbits, for which systematic methods have been developed to obtain precise asymptotics with power-saving error terms.

The purpose of this article is to devise new systematic techniques for counting reducible orbits. We illustrate our techniques for a representation that features prominently in the literature on arithmetic statistics, namely the action of the orthogonal group of the split  $n$ -ary quadratic form on the space of quadratic forms in  $n$  variables, where  $n \geq 3$  is an arbitrary fixed integer. In particular, we provide a complete answer to the fundamental question stated above for each representation in this infinite family indexed by  $n$ ; see Section 1.3 for precise statements of our main theorems. Before proving these general theorems, we provide the reader with a gentle introduction to our new method by illustrating how it applies in the context of a low-dimensional example, namely the action of  $\mathrm{PGL}_2$  on the space  $\mathrm{Sym}_4(2)$  of binary quartic forms; see Section 2.

**1.1. Background on orbit-counting, and relation to earlier work.** In this section, we summarize the orbit-counting methods that feature in the literature on arithmetic statistics leading up to the present article, and we describe the context for our new methods of counting reducible orbits.

*The critical dichotomy.* Let  $(G, W)$  be a coregular representation with space of relative invariants  $U$ , and suppose that a family of arithmetic objects can be parametrized in terms of certain  $G(\mathbb{Z})$ -orbits on  $W(\mathbb{Z})$ . We note that a natural source of examples of such coregular representations are *prehomogeneous* representations, i.e., the ring of relative invariants is generated by a single element, usually called the *discriminant*.

Further suppose that the space  $U(\mathbb{R})$  admits a natural notion of height, and define the height of (the  $G(\mathbb{R})$ -orbit of) an element  $w \in W(\mathbb{R})$  to be the height of the image of  $w$  under the natural map  $W(\mathbb{R}) \rightarrow U(\mathbb{R})$ . In the prehomogeneous case, this height is usually taken to be the absolute value of the discriminant. 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  $G(\mathbb{Z})$  on  $W(\mathbb{R})$ . This latter problem is complicated by the fact that the fundamental domain  $\mathcal{D}$  is usually not compact, even for the subset  $\mathcal{D}_X$  of points in  $\mathcal{D}$  with height less than  $X$ . Indeed, the height-bounded fundamental domain  $\mathcal{D}_X$  typically consists of a bounded region known as the *main body*, along with one or more *cusps*, which are long tentacle-like regions going off to infinity.

Surprisingly, in most of the coregular representations considered in the literature thus far, the following dichotomy holds:

- (1) A proportion of 100% of irreducible orbits lie in the main body; and a proportion of 100% of points in the main body are irreducible.
- (2) A proportion of 100% of reducible orbits lie in the cusp; and a proportion of 100% of points in the cusp are reducible.

If properties (1) and (2) above hold, then the count of points in the main body of  $\mathcal{D}_X$  gives an asymptotic for the number of irreducible  $G(\mathbb{Z})$ -orbits on  $W(\mathbb{Z})$  having height less than  $X$ . This main body count can be determined in a systematic way: using geometry-of-numbers methods, the count can be expressed in terms of the volume of the main body, and this volume can then be computed by performing a suitable change-of-variables. The difficulty in counting the reducible orbits, which predominate in the cusp(s) of  $\mathcal{D}_X$ , is that geometry-of-numbers methods do not directly apply in such regions. In fact, the asymptotic count of reducible orbits is *not* given in terms of the volume of the corresponding cuspidal regions. In the examples treated in this paper, we find that the volume of the cuspidal region is an underestimate, and that the actual answer is given in terms of a certain weighted volume.

*Historical context.* The development and use of the orbit-counting strategy summarized above goes back centuries. Mertens [34] and Siegel [48] studied the action of  $GL_2$  on the space  $\text{Sym}_2(2)$  of binary quadratic forms, which has a unique polynomial invariant, namely the discriminant. They developed geometry-of-numbers methods to count the number of  $GL_2(\mathbb{Z})$ -orbits on  $\text{Sym}_2 \mathbb{Z}^2$  with bounded discriminant, resolving conjectures of Gauss on the average sizes of class numbers of quadratic orders. In the series of papers [22; 23], Davenport considered the action of  $GL_2$  on the space  $(\text{Sym}^3(2))^*$  of binary cubic forms, which also has the discriminant as its unique polynomial invariant. Using the strategy described above, he obtained asymptotics for the number of irreducible  $GL_2(\mathbb{Z})$ -orbits on  $(\text{Sym}^3 \mathbb{Z}^2)^*$  having bounded discriminant, and in collaboration with Heilbronn, he combined these asymptotics with results from class field theory and sieve methods to determine the density of discriminants of cubic fields [24].

The main obstruction to generalizing the work of Mertens, Siegel, and Davenport–Heilbronn to other representations was proving that the number of irreducible points in the cusps is negligible. A pioneering advance was made by Bhargava (see [4]), who introduced an “averaging” method that has the effect

of thickening the cusps, making them a bit more amenable to doing geometry-of-numbers. Bhargava's averaging method, which applies to general coregular representations, 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. However, the averaging method has, until the present paper, only been used to obtain upper bounds in the cusp and new methods are needed to obtain precise asymptotics.

**1.2. Notation and setup.** We first study a concrete representation in Section 2, before proceeding to our main results on families of representations. The concrete representation we consider is that of  $\mathrm{PGL}_2$  acting on binary quartic forms. The notation in this case is quite manageable, and largely follows that of [9]. In this section, we introduce the other (family of) representations studied in this paper, and we set up the notation necessary to state our main results. Let  $\mathcal{A}$  be the antidiagonal  $n \times n$  matrix with all antidiagonal entries equal to 1; if viewed as a quadratic form, we note that  $\mathcal{A}$  is split (i.e., it has a maximal isotropic space defined over  $\mathbb{Q}$ ) and unimodular.

*The representation.* We first define the group  $G$ , which is slightly different for  $n$  odd and  $n$  even:

- When  $n$  is odd, we take  $G := \mathrm{SO}_{\mathcal{A}}$  to be the split special orthogonal group scheme over  $\mathbb{Z}$  corresponding to  $\mathcal{A}$ . That is, we have  $G(R) = \{g \in \mathrm{SL}_n(R) : g^t \mathcal{A} g = \mathcal{A}\}$  for any  $\mathbb{Z}$ -algebra  $R$ .
- When  $n$  is even, we take  $G := \mathrm{O}_{\mathcal{A}} / \mu_2$  to be the split projective orthogonal group scheme over  $\mathbb{Z}$  corresponding to  $\mathcal{A}$ . That is, we take  $G$  to be the cokernel of the inclusion  $\mu_2 \hookrightarrow \mathrm{O}_{\mathcal{A}}$  of group schemes over  $\mathbb{Z}$ , where  $\mathrm{O}_{\mathcal{A}} := \{g \in \mathrm{GL}_n(R) : g^t \mathcal{A} g = \mathcal{A}\}$  for any  $\mathbb{Z}$ -algebra  $R$ .

We now define the representation  $W$  of  $G$ . Let  $W$  denote the affine  $\mathbb{Z}$ -scheme whose  $R$ -points consist of the set of  $n \times n$  symmetric matrices with entries in  $R$  (i.e., classically integral quadratic forms over  $R$ ). Then  $W$  has a natural structure as a  $G$ -representation, where the (left) action is given by  $g \cdot B = (g^{-1})^t B g^{-1}$  for  $g \in G$  and  $B \in W$ . We note that  $W$  can also be interpreted as the space of self-adjoint operators for  $\mathcal{A}$  over  $R$  by identifying a self-adjoint operator  $T$  with  $B = -\mathcal{A}T \in W$ .

The orbits of the representation of  $G$  on  $W$  have been studied extensively in the literature. For example, Bhargava and Gross [6] (resp. Shankar and Wang [43]) obtained asymptotics for the number of *irreducible* orbits of  $G(\mathbb{Z})$  on  $W(\mathbb{Z})$  having bounded height when  $n$  is odd (resp., when  $n$  is even). These asymptotics have yielded a striking array of applications: they were utilized by the aforementioned authors to bound the average sizes of the 2-Selmer groups of monic hyperelliptic Jacobians of any given dimension, by Swaminathan to prove that most odd-degree binary forms fail to primitively represent a square [50], and by Siad [46; 47] to bound the average size of the 2-torsion subgroup of the class groups of monogenic fields of any given degree. Furthermore, by proving an upper bound on the *reducible* orbits of this representation, Bhargava, Shankar, and Wang [16] determined the probability that a monic integral polynomial has squarefree discriminant.

*The invariants.* Let  $U$  denote the affine  $\mathbb{Z}$ -scheme whose  $R$ -points consist of monic degree- $n$  polynomials with coefficients in  $R$ . For any element  $B \in W(R)$ , the monic degree- $n$  polynomial

$$\mathrm{inv}(B) := (-1)^{\lfloor \frac{n}{2} \rfloor} \det(x\mathcal{A} + B) \in U(R) \quad (1)$$

is invariant under the action of  $G(R)$ ; in fact, by [20, Section 8.3, part (VI) of Section 13.2], its coefficients freely generate the ring of polynomial invariants for the action of  $G$  on  $W$ . Given  $f \in U(R)$ , we write

$$\text{inv}^{-1}(f) := \{B \in W(R) : \text{inv}(B) = f\}.$$

*The notion of nondegeneracy.* Let  $R$  be an integral domain. Then we say that a monic polynomial with coefficients in  $R$  is *nondegenerate* if it has nonzero discriminant. We say that an element  $B \in W(R)$  is *nondegenerate* if the monic polynomial  $\text{inv}(B)$  has nonzero discriminant.

When  $R = \mathbb{Z}$  or  $\mathbb{R}$ , it is convenient to partition the set of nondegenerate elements in  $U(R)$  according to the number of real roots, and to lift this partition to  $W(R)$ . To this end, let  $0 < r \leq n$  be odd if  $n$  is odd, and let  $0 \leq r \leq n$  be even if  $n$  is even. For  $R = \mathbb{Z}$  or  $\mathbb{R}$ , we define

$$\begin{aligned} U(R)^{(r)} &:= \{f \in U(R) : f \text{ is nondegenerate and exactly } r \text{ real roots}\}, \\ W(R)^{(r)} &:= \{B \in W(R) : \text{inv}(B) \in U(R)^{(r)}\}. \end{aligned}$$

*The height.* We order elements of  $U(\mathbb{R})$  and  $W(\mathbb{R})$  by *height*. Given a polynomial

$$f(x) = x^n + \sum_{i=1}^n f_i x^{n-i} \in U(\mathbb{R}),$$

we define its *height*  $H(f)$  by

$$H(f) := \max_{1 \leq i \leq n} \{|f_i|^{1/i}\},$$

and given  $B \in W(\mathbb{R})$ , we define its height by  $H(B) := H(\text{inv}(B))$ . For any  $X > 0$ , we write

$$N^{(r)}(X) := \#\{f \in U(\mathbb{Z})^{(r)} : H(f) < X\}.$$

Notice that we have

$$N^{(r)}(X) \sim \mathcal{V}^{(r)}(X) := \text{Vol}(\{f \in U(\mathbb{R})^{(r)} : H(f) < X\}) \asymp X^{\dim W} = X^{\frac{n^2+n}{2}},$$

where the volume is computed with respect to the Euclidean measure on  $U(\mathbb{R})$ , normalized so that  $U(\mathbb{Z})$  has covolume 1.

*The notion of reducibility.* When  $R$  is a principal ideal domain with field of fractions  $K$ , we can partition the nondegenerate elements in  $W(R)$  into two natural  $G(R)$ -invariant subsets. We call (the  $G(R)$ -orbit of) a nondegenerate element  $B \in W(R)$  *reducible* if:

- $\mathcal{A}$  and  $B$ , viewed as quadratic forms, share a maximal isotropic subspace over  $K$  if  $n$  is odd, or
- $B$  has an isotropic subspace of dimension  $\frac{n-2}{2}$  over  $K$  contained within a maximal isotropic subspace for  $\mathcal{A}$  over  $K$  if  $n$  is even.

We say that  $B \in W(R)$  is *irreducible* if it is nondegenerate and not reducible. There are a few good arithmetic reasons to think of such elements as reducible. For example, pairs  $(\mathcal{A}, B)$  correspond to triples  $(R', I, \delta)$ , where  $R'$  is a rank  $n$  ring over  $R$ ,  $I$  is an ideal in  $R'$ , and  $\delta \in L^\times / L^{\times 2}$ , where  $L = R' \otimes K$ , such that  $I^2 \subset (\delta)$  and  $N(I)^2 = N(\delta)$ . Then it was proven in [46; 47] that  $(\mathcal{A}, B)$  is reducible if and only if  $\delta \equiv 1$ .

As another example, pairs  $(\mathcal{A}, B)$  also correspond to classes  $\sigma \in H^1(K, J[2])$ , where  $J$  is the Jacobian of the monic hyperelliptic curve  $y^2 = \pm \det(\mathcal{A} + B)$ , and  $(\mathcal{A}, B)$  is reducible if and only if  $\sigma$  is trivial.

Write the coordinates of  $W$  as  $[b_{ij}]_{1 \leq i \leq j \leq n}$ . Let  $W_0$  be the subscheme of  $W$  obtained by setting  $b_{ij} = 0$  for all  $(i, j)$  with  $i + j < n$ . Observe that, if  $R$  is a principal ideal domain, then every element of  $W_0(R)$  is reducible; for this reason, we call  $W_0$  the *reducible hyperplane*. The reducible hyperplane is sent to itself under the action of the lower-triangular subgroup  $\mathcal{P} \subset G$ , and so we obtain a well-defined representation of  $\mathcal{P}$  on  $W_0$ . In what follows, for a  $\mathbb{Z}$ -algebra  $R$  and any subset  $S \subset W(R)$ , we sometimes write  $S_0 \subset S$  to denote the subset  $S \cap W_0(R)$ .

**1.3. Statements of main theorems.** Having set up the notation, we are now in position to state our first main result. Define the constants  $C_n^{\text{fin}}$  and  $C_{n,r}^{\text{inf}}$  as

$$C_n^{\text{fin}} := \begin{cases} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \zeta(2i) & \text{if } 2 \nmid n, \\ \zeta\left(\frac{n}{2}\right) \prod_{i=1}^{\frac{n-2}{2}} \zeta(2i) & \text{if } 2 \mid n, \end{cases} \quad C_{n,r}^{\text{inf}} := \begin{cases} \mathcal{V}^{(r)}(1) & \text{if } 2 \nmid n, \\ 2^{-\frac{n}{2}} \mathcal{V}^{(r)}(1) & \text{if } 2 \mid n. \end{cases}$$

Then we have the following result, which gives the total count of reducible  $G(\mathbb{Z})$ -orbits on  $W(\mathbb{Z})^{(r)}$ :

**Theorem 1.** *The number of reducible  $G(\mathbb{Z})$ -orbits on  $W(\mathbb{Z})^{(r)}$  having height up to  $X$  is given by*

$$C_n^{\text{fin}} \cdot (C_{n,r}^{\text{inf}} \cdot X^{\frac{n^2+n}{2}}) + o(X^{\frac{n^2+n}{2}}).$$

**Remark.** The factor  $C_{n,r}^{\text{inf}} \cdot X^{(n^2+n)/2}$  occurring in [Theorem 1](#) is an asymptotic for the number of invariant polynomials that arise from orbits of height up to  $X$ . Notice that  $C_{n,r}^{\text{inf}} \cdot X^{(n^2+n)/2} \sim N^{(r)}(X)$  when  $n$  is odd and that  $C_{n,r}^{\text{inf}} \cdot X^{(n^2+n)/2} \sim 2^{-n/2} N^{(r)}(X)$  when  $n$  is even. The extra factor of  $2^{-n/2}$  occurs when  $n$  is even because, for any  $B \in W(\mathbb{Z})$ , the  $x^i$ -coefficient of  $\text{inv}(B)$  is divisible by 2 for every odd number  $i \in \{1, 3, \dots, n - 1\}$  (see [\[47, Theorem 80\]](#)).

As mentioned above, the corresponding asymptotics for the irreducible  $G(\mathbb{Z})$ -orbits on  $W(\mathbb{Z})^{(r)}$  have been obtained previously in [\[6, Theorem 10.1 and equation \(10.27\)\]](#) when  $n$  is odd and in [\[43, Theorem 20 and equation \(38\)\]](#) when  $n$  is even. The main term exponents for the irreducible and reducible cases are the same, and remarkably, the asymptotics for both cases have the same leading constant  $C_n^{\text{fin}}$ , up to a rational factor! Even more surprisingly, the manner in which  $C_n^{\text{fin}}$  arises is completely different for the irreducible and reducible counts. In the irreducible case, this constant arises from the fundamental volume of the group  $G$ —i.e., the volume with respect to a suitably normalized Haar measure of  $G(\mathbb{Z}) \backslash G(\mathbb{R})$ . However, in the reducible case considered in this paper, it arises from a summation of volumes of lower-dimensional slices of the cuspidal regions of a fundamental domain for  $G(\mathbb{Z})$  on  $W(\mathbb{R})$ . These slices have negligible volume unless they are very high up in the cusp. Thus, they do not detect most of the main body volume, and this appears to be a genuinely different way of obtaining the constant  $C_n^{\text{fin}}$ .

In light of the above discussion, we are led to pose the following natural question, which we have answered in the affirmative for the action of  $G$  on  $W$ :

**Question 2.** Let  $(G, W)$  be a coregular representation with natural notions of nondegeneracy, height, and reducibility. Let  $N^{\text{irr}}(X)$  (resp.,  $N^{\text{red}}(X)$ ) denote the number of irreducible (resp., reducible)  $G(\mathbb{Z})$ -orbits on  $W(\mathbb{Z})$  having height less than  $X$ .

- (a) Is it true that as  $X$  tends to infinity we have  $N^{\text{irr}}(X) \asymp N^{\text{red}}(X)$ ?
- (b) If so, then is it true that  $\lim_{X \rightarrow \infty} (N^{\text{irr}}(X)/N^{\text{red}}(X))$  is a rational constant?

We note that the answers to both parts of [Question 2](#) are also “yes” for the action of  $\text{GL}_2$  on  $\text{Sym}_3(2)$  by work of Shintani [[45](#), Chapter 2, Section 7, Remark 2] and Bhargava and Varma [[11](#), Section 4.1.2]. It follows by combining our results in [Section 2](#) with the irreducible count obtained by Bhargava and Shankar in their paper on binary quartic forms [[9](#)] that the answers are also “yes” for the action of  $\text{GL}_2$  on  $\text{Sym}_4(2)$ . On the other hand, the answer to the first part of [Question 2](#) is “no” for the action of  $\text{SL}_n$  on  $2 \otimes \text{Sym}^2(n)$ , where  $n \geq 4$  is an arbitrary even integer; indeed, it was shown in work of Bhargava [[5](#)] that  $N^{\text{red}}(X) = o(N^{\text{irr}}(X))$  for this representation. The situation is more complicated for the action of  $\text{GL}_2 \times \text{SL}_3$  on  $2 \otimes \text{Sym}_2(3)$ . Bhargava proved in [[2](#), Theorem 7] that  $N^{\text{irr}}(X) \asymp X$ , and it is well known that  $N^{\text{red}}(X) \asymp X \log X$ . However, the reducible orbits of this representation can be partitioned into several natural subsets, and as was shown by Swaminathan [[51](#)] using the methods developed in the present paper, the answers to both parts of [Question 2](#) are “yes” if we restrict to one of these subsets.

Our next main results concern families defined by certain infinite sets of congruence conditions. We call a subset  $S \subset W(\mathbb{Z})$  a *big family* if  $S = W(\mathbb{Z})^{(r)} \cap \bigcap_p S_p$ , where the sets  $S_p \subset W(\mathbb{Z}_p)$  satisfy the following properties:

- (1)  $S_p$  is  $G(\mathbb{Z}_p)$ -invariant and is the preimage under reduction modulo  $p^j$  of a nonempty subset of  $W(\mathbb{Z}/p^j\mathbb{Z})$  for some  $j > 0$  for each  $p$ ; and
- (2)  $S_p$  contains all  $(G(\mathbb{Z}_p)$ -orbits of) elements  $B \in W_0(\mathbb{Z}_p)$  such that, for all  $p \gg 1$ , we have that  $b_{i(n-i)}(B)$  is a  $p$ -adic unit for some  $i$ .

Note that a big family  $S$  is necessarily  $G(\mathbb{Z})$ -invariant.

Our first result on reducible orbits in big families is stated in terms of a polynomial function  $\lambda$  on the reducible hyperplane  $W_0$ , defined explicitly by

$$\lambda(B) := \begin{cases} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} b_{i(n-i)}(B)^{2i-1} & \text{if } 2 \nmid n, \\ b_{\frac{n}{2}}(B)^{\frac{n-2}{2}} \prod_{i=1}^{\frac{n-2}{2}} b_{i(n-i)}(B)^{2i-1} & \text{if } 2 \mid n. \end{cases} \tag{2}$$

Given this definition of  $\lambda$ , we have the following asymptotic formula:

**Theorem 3.** Let  $S$  be a big family. Then the number of reducible  $G(\mathbb{Z})$ -orbits on  $S$  of height up to  $X$  is given by

$$C_{n,r}^{\text{inf}} \cdot \left( \prod_p \left( 1 - \frac{1}{p} \right)^{-\lfloor \frac{n}{2} \rfloor} \int_{B \in (S_p)_0} |\lambda(B)|_p dB \right) \cdot X^{\frac{n^2+n}{2}} + o(X^{\frac{n^2+n}{2}}),$$

where  $dB$  denotes the Euclidean measure on  $W_0(\mathbb{Z}_p)$ , normalized so that  $W_0(\mathbb{Z}_p)$  has volume 1, and where  $|\cdot|_p$  denotes the usual  $p$ -adic absolute value.

Our second result on reducible orbits in big families, which is equivalent to [Theorem 3](#), is stated in terms of a product of local orbit counts for the action of  $\mathcal{P}$  on  $W_0$ :

**Theorem 4.** *Let  $S$  be a big family. Then the number of reducible  $G(\mathbb{Z})$ -orbits on  $S$  of height up to  $X$  is given by*

$$\left( \prod_p \int_{f \in U(\mathbb{Z}_p)} \# \left( \frac{\text{inv}^{-1}(f) \cap (S_p)_0}{\mathcal{P}(\mathbb{Z}_p)} \right) df \right) \cdot N^{(r)}(X) + o(X^{\frac{n^2+n}{2}}), \quad (3)$$

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

The local product in (3) looks similar to many other mass formulas in related works with one major difference: the group in question,  $\mathcal{P}$ , is not reductive. To prove [Theorem 4](#), it is therefore necessary for us to get some control over orbits of this nonreductive group, which we do in, e.g., [Section 6.3](#).

**1.4. Methods of proof.** To prove our main results, we introduce two new methods of determining asymptotics for reducible orbits, and we describe them both as follows.

*Method I.* Our first method proceeds by directly counting points in the cusp(s) of an “averaged” fundamental domain  $\mathcal{D}$  for the action of  $G(\mathbb{Z})$  on  $W(\mathbb{R})$ . This suffices to get the count of reducible orbits because, by the results in [\[6; 43\]](#), properties (1) and (2) in [Section 1.1](#) are satisfied for the action of  $G$  on  $W$ . This method requires us to construct fundamental domains  $\mathcal{D}$  for the action of  $G(\mathbb{Z})$  on  $W(\mathbb{R})$ , which in turn requires us to construct a fundamental domain  $\mathcal{F}$  for the action of  $G(\mathbb{Z})$  on  $G(\mathbb{R})$ . Unlike in most previous situations, it is simply not enough for us to invoke the work of Borel and Harish-Chandra [\[18; 19\]](#), who constructed fundamental domains for general semisimple groups. Indeed, our argument relies on  $\mathcal{F}$  being *box-shaped at infinity*, meaning that  $\mathcal{F}$  looks like a Siegel domain in a neighborhood of the cusp. We prove the existence of such fundamental domains for our groups  $G$ .

The region  $\mathcal{D}$  is too skewed for a direct geometry-of-numbers argument to give anything better than an upper bound for the number of points it contains. To resolve this issue, we cut up the region  $\mathcal{D}$  into a countable collection of nicer-looking slices. Within each slice, we prove that the count of the integral points is asymptotic to the volume of the slice. Summing up over all slices yields the desired total asymptotic. Our slicing method constitutes the first higher-dimensional generalization of an argument developed in [\[13\]](#), which treated the simpler case of the cusps arising from the group  $\text{GL}_2$ .

Summing up the volumes of the slices gives us the desired asymptotic in terms of weighted volumes of certain sets in the reducible hyperplane  $W_0(\mathbb{R}) \subset W(\mathbb{R})$ , where the volumes are computed with respect to the weight  $\lambda$  defined in (2). We evaluate these weighted volumes by proving a Jacobian change-of-variables formula that transforms the measure  $\lambda$  on  $W_0$  into the product of the Euclidean measure on  $U(\mathbb{R})$  with the Haar measure on the lower-triangular subgroup  $\mathcal{P}(\mathbb{R}) \subset G(\mathbb{R})$ . Such change-of-variable results have previously been proven when the group under consideration is unimodular (see, e.g., [\[9, Section 3.4\]](#)), but the fact that the group  $\mathcal{P}$  fails to be unimodular presents significant new challenges.

Method I, as applied to the representation of  $G$  on  $W$ , requires very complicated indexing and notation. To make Method I more readily comprehensible for the reader, we begin in [Section 2](#) by illustrating the

method in the case of  $\mathrm{PGL}_2$  acting on  $\mathrm{Sym}_4(2)$ , before proceeding with the parallel, but much more complicated, case of  $G$  acting on  $W$  starting in Section 3. We note that Section 2 can be read more or less independently of the rest of the paper.

*Method II.* Our second method proceeds by means of the following four steps. First, we claim that the asymptotics for the number of reducible  $G(\mathbb{Z})$ -orbits on  $W(\mathbb{Z})$  are the same as the asymptotics for the number of  $\mathcal{P}(\mathbb{Z})$ -orbits on  $W_0(\mathbb{Z})$ . This claim is an immediate corollary of the following two facts:

- (a) If  $B_1, B_2 \in W_0(\mathbb{Z})$  are equivalent under  $G(\mathbb{Z})$  but not under  $\mathcal{P}(\mathbb{Z})$ , then  $B_1$  and  $B_2$  have nontrivial stabilizer in  $G(\mathbb{Q})$ , but as we establish in Proposition 32, all but negligibly many  $G(\mathbb{Z})$ -equivalence classes on  $W_0(\mathbb{Z})$  have trivial stabilizer in  $G(\mathbb{Q})$ .
- (b) As shown in [6, Proposition 10.7] and [43, Proposition 23], all but negligibly many reducible  $G(\mathbb{Z})$ -orbits on  $W(\mathbb{Z})$  have a representative lying on the reducible hyperplane  $W_0(\mathbb{Z})$ .

The second step is to develop the reduction theory for the action of  $\mathcal{P}$  on  $W_0$ . Specifically, we prove that, for any field  $K$ , the group  $\mathcal{P}(K)$  acts *simply transitively* on the set of elements in  $W_0(K)$  having any fixed nondegenerate invariant polynomial. Using the fact that the group  $\mathcal{P}$  has class number 1 over  $\mathbb{Q}$ , we then deduce that the orbits of  $\mathcal{P}(\mathbb{Z})$  on  $W_0(\mathbb{Z})$  satisfy the following strong local-to-global principle:

**Theorem 5.** *Let  $f \in U(\mathbb{Z})$  be a nondegenerate monic degree- $n$  polynomial, and when  $n$  is even, suppose that the  $x^i$ -coefficient of  $f$  is divisible by 2 for each odd  $i$ . For each prime  $p$ , choose  $B_p \in W_0(\mathbb{Z}_p)$  such that  $\mathrm{inv}(B) = f$ . Then there exists  $B \in W_0(\mathbb{Z})$ , unique up to the action of  $\mathcal{P}(\mathbb{Z})$ , such that  $B$  is  $\mathcal{P}(\mathbb{Z}_p)$ -equivalent to  $B_p$  for each prime  $p$ .*

In fact, we prove a more general version of Theorem 5, namely Theorem 34, applying to representations of groups having class number 1 over  $\mathbb{Q}$ .

By Theorem 5, the number of  $\mathcal{P}(\mathbb{Z})$ -orbits on  $W_0(\mathbb{Z})$  with nondegenerate invariant polynomial  $f$  is simply the product over all primes  $p$  of the number of  $\mathcal{P}(\mathbb{Z}_p)$ -orbits on  $W_0(\mathbb{Z}_p)$  lying above  $f$ . The third step is to sum this local product formula over all invariant polynomials of bounded height. A key ingredient for evaluating the sum is to verify that there are not too many orbits with large value of  $\lambda$ . This was verified in [16], where an upper bound of roughly the correct order of magnitude was obtained for the number of  $\mathcal{P}(\mathbb{Z})$ -orbits on  $W_0(\mathbb{Z})$  with large value of  $\lambda$ .<sup>2</sup> We thus arrive at the surprising conclusion that, at least for the representation of  $G$  on  $W$ , an upper bound on the number of reducible orbits can be indirectly used to deduce a precise asymptotic!

The resulting asymptotic for the total count of reducible orbits is now expressed in terms of a product of local orbit counts, as in Theorem 4. The fourth and final step is to evaluate this product. We do this by using the previously mentioned Jacobian change-of-variables formula in reverse! This expresses the local orbit count at a prime  $p$  as a certain  $p$ -adic integral, thus yielding Theorem 3; evaluating each of these integrals and multiplying them all together yields the total asymptotic in Theorem 1.

---

<sup>2</sup>An even stronger upper bound for the number of orbits with large value of  $\lambda$  can be obtained using Method I, by simply summing over those slices with large value of  $\lambda$ ; see Theorem 33 (to follow).

**Remark.** For the coregular representations considered in this paper, both of the above methods are sufficient to obtain asymptotics for the number of reducible elements. Method I gives a direct proof of [Theorem 3](#), while Method II gives a direct proof of [Theorem 4](#). Moreover, the main terms in these two theorems can be related to each other using a Jacobian change-of-variables. However, for certain representations such as those considered in [\[51; 36\]](#), Method II can be directly applied while applying Method I seems more complicated. Moreover, for certain representations such as those considered in [\[1\]](#), Method II is inapplicable, while Method I can be used.

**1.5. Other applications of our methods.** We expect that both of the methods that we introduce in this paper can be used to count reducible orbits for other representations.

Our methods have already been used to derive arithmetic applications beyond the results of this paper. Swaminathan [\[51\]](#) counted reducible orbits for the action of  $\mathrm{SL}_n$  on  $2 \otimes \mathrm{Sym}^2(n)$ , where  $n$  is odd, and used this to prove asymptotics for counts of 2-torsion in the ideal class groups of cubic orders in the case  $n = 3$ . (A similar application could be pursued for counting quintic rings, which also correspond to integral orbits of a coregular representation via a parametrization of Bhargava [\[3\]](#).) Also, Oller [\[36\]](#) counted reducible orbits in all the Vinberg representations in Thorne’s thesis [\[52\]](#), and also carried out squarefree sieves in all these cases.

One possible line of inquiry is to study the action of  $\mathrm{GL}_2$  on the space of binary  $n$ -ic forms for  $n \geq 5$ . We carry out the case  $n = 4$  in [Section 2](#); the  $n = 3$  case is similar and would give a simpler proof of the results of Shintani and Bhargava–Varma mentioned previously. The spaces are not coregular for  $n \geq 5$ , but when integral orbits are ordered by Julia invariant, Bhargava and Yang [\[12\]](#) determined asymptotics for the number of irreducible orbits. We expect the methods introduced in this paper to have applications towards counting the reducible orbits, ordered by Julia invariant, for these spaces. Other arithmetically interesting families of coregular representations for which the question of counting reducible orbits remains open may be found in the thesis of Ho [\[30\]](#).

## 2. Counting reducible integral orbits on binary quartic forms

In this section, we determine asymptotics for the number of reducible orbits of bounded height for the action of  $\mathrm{PGL}_2$  on the space of integral binary quartic forms. Our purpose is to illustrate Method I (see [Section 1.4](#)) in the context of a low-dimensional example, with the view of making the higher-dimensional application treated in [Sections 3–6](#) more readily comprehensible.

This section can be read more or less independently of the rest of the paper. We remark that some of the notation used within this section is recycled in subsequent sections to denote different but analogous objects. As none of the objects introduced in this section are used in subsequent sections, we do not expect this to cause ambiguity.

*Setup.* Let  $V$  denote the affine  $\mathbb{Z}$ -scheme whose  $R$ -points consist of binary quartic forms with coefficients in  $R$ ; i.e., we have

$$V(R) := \{f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 : a, b, c, d, e \in R\}.$$

The group  $\mathrm{PGL}_2$  acts on  $V$  via  $(g \cdot f)(x, y) := (\det g)^{-2} \times f((x, y) \cdot g)$ . The ring of invariants for the action of  $\mathrm{PGL}_2$  on  $V$  is freely generated by two invariants, denoted by  $I$  and  $J$ . For the form  $f(x, y)$  written as above, these invariants are given explicitly by

$$I(f) = 12ae - 3bd + c^2, \quad J(f) = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3.$$

For convenience, we define  $\mathrm{inv} : V \rightarrow \mathbb{A}^2$  to be the map that sends  $f$  to  $(I(f), J(f))$ . The image of this map over  $\mathbb{Z}$  is not all of  $\mathbb{A}^2(\mathbb{Z})$ , but is defined by congruence conditions modulo 27; see [9, Theorem 1.7].

We define a  $\mathrm{PGL}_2(\mathbb{R})$ -invariant *height*  $H$  on  $V(\mathbb{R})$  via  $H(f) := \max\{|I(f)|^3, J(f)^2/4\}$ . We say that a binary quartic form  $f$  is *nondegenerate* if its *discriminant*  $\Delta(f) := (4I(f)^3 - J(f)^2)/27$  is nonzero. More generally, we say that a pair  $(I, J)$  is nondegenerate if the quantity  $\Delta(I, J) := (4I^3 - J^2)/27$  is nonzero (so a binary quartic form is nondegenerate if and only if its invariants are nondegenerate). For  $i \in \{0, 1, 2\}$  and  $R = \mathbb{Z}$  or  $\mathbb{R}$ , we let  $V(R)^{(i)}$  denote the set of nondegenerate elements in  $V(R)$  having  $i$  pairs of complex conjugate roots and  $4 - 2i$  real roots in  $\mathbb{P}^1(\mathbb{C})$ .

A nondegenerate binary quartic form  $f \in V(R)$  is said to be *reducible* if it factors over  $R$ . It follows from [9, Lemma 2.3] that the number of reducible orbits on  $V(\mathbb{Z})$  having height bounded by  $X$  and factoring into the product of two irreducible quadratic forms is  $O(X^{2/3+\epsilon})$ , and thus negligible. That is, 100% of reducible orbits have at least one rational (and thus at least one real) linear factor. Therefore, for the purposes of this section, it suffices to restrict our attention to counting orbits of binary quartic forms that possess a rational linear factor, which amounts to counting reducible integral orbits in the sets  $V(\mathbb{R})^{(0)}$  and  $V(\mathbb{R})^{(1)}$ .

Let  $V_0(R) \subset V(R)$  be the “reducible hyperplane” consisting of those forms  $f$  with  $a = 0$  (i.e., those forms  $f$  that are divisible by  $y$ ). The reducible hyperplane is sent to itself under the action of the lower-triangular subgroup  $P \subset \mathrm{PGL}_2$ ,<sup>3</sup> and so we obtain a well-defined representation of  $P$  on  $V_0$ . In what follows, for a  $\mathbb{Z}$ -algebra  $R$  and any subset  $S \subset V(R)$ , we sometimes write  $S_0 \subset S$  to denote the subset  $S \cap V_0(R)$ .

*Main results.* Given the above setup, the main result of this section is as follows, by analogy with [Theorem 1](#):

**Theorem 6.** *The number of reducible  $\mathrm{PGL}_2(\mathbb{Z})$ -orbits on  $V(\mathbb{Z})^{(i)}$  having height less than  $X$  is*

$$\zeta(2) \cdot \left(\frac{8+24i}{135} \cdot X^{\frac{5}{6}}\right) + O_\epsilon(X^{\frac{3}{4}+\epsilon}).$$

**Remark.** The factor  $\frac{8+24i}{135} \cdot X^{5/6}$  occurring in [Theorem 6](#) is an asymptotic for the number of pairs  $(I, J)$  that arise as invariants of orbits of height up to  $X$  (see [9, Proposition 2.10]). The factor of  $\frac{8+24i}{135}$  comprises two parts: the first is a factor of  $\frac{8+24i}{5}$ , which is the volume of the space of invariants of height at most 1 in  $V(\mathbb{R})^{(i)}$ , and the second is a factor of  $\frac{1}{27}$ , which occurs because not every pair  $(I, J) \in \mathbb{R}^2$  arises as the set of invariants of a binary quartic form in  $V(R)$ .

<sup>3</sup>More precisely, for a ring  $R$ , we define  $P(R)$  to be the image of the subgroup of lower triangular matrices in  $\mathrm{GL}_2(R)$  under the map  $\mathrm{GL}_2(R) \rightarrow \mathrm{PGL}_2(R)$ .

Next, we consider subsets of  $V(\mathbb{Z})$  cut out by certain (possibly) infinite sets of congruence conditions. We call  $S \subset V(\mathbb{Z})$  a *big family* if  $S = V(\mathbb{Z})^{(i)} \cap \bigcap_p S_p$ , for  $i \in \{0, 1\}$ , where the sets  $S_p \subset V(\mathbb{Z}_p)$  satisfy the following properties:

- (1)  $S_p$  is  $\mathrm{PGL}_2(\mathbb{Z}_p)$ -invariant and is the preimage under reduction modulo  $p^j$  of a nonempty subset of  $V(\mathbb{Z}/p^j\mathbb{Z})$  for some  $j > 0$  for each  $p$ .
- (2) For all  $p \gg 1$ , the set  $S_p$  contains (all  $\mathrm{PGL}_2(\mathbb{Z}_p)$ -orbits of) all elements  $f(x, y) \in V(\mathbb{Z}_p)$  such that  $a(f) = 0$  and  $b(f)$  is a  $p$ -adic unit, where  $a(f)$  and  $b(f)$  denote the  $x^4$ - and  $x^3y$ -coefficients of  $f(x, y)$ , respectively.

We then have the following result, by analogy with [Theorem 3](#):

**Theorem 7.** *Let  $S \subset V(\mathbb{Z})^{(i)}$  be a big family. Then the number of reducible  $\mathrm{PGL}_2(\mathbb{Z})$ -orbits on  $S$  of height less than  $X$  is*

$$\left(\frac{8+24i}{135} \cdot X^{\frac{5}{6}}\right) \cdot \prod_p (1 - p^{-1})^{-1} \int_{f \in (S_p)_0} |b(f)|_p df + O_\epsilon(X^{\frac{3}{4}+\epsilon}).$$

Finally, by analogy with [Theorem 4](#), we have the following result, which is equivalent to [Theorem 7](#):

**Theorem 8.** *Let  $S \subset V(\mathbb{Z})^{(i)}$  be a big family. Then the number of reducible  $\mathrm{PGL}_2(\mathbb{Z})$ -orbits on  $S$  of height less than  $X$  is*

$$\left(\prod_p \int_{(I,J) \in \mathbb{Z}_p^2} \# \left( \frac{\mathrm{inv}^{-1}(I, J) \cap (S_p)_0}{P(\mathbb{Z}_p)} \right) dI dJ \right) \cdot \left(\frac{8+24i}{5} \cdot X^{\frac{5}{6}}\right) + O_\epsilon(X^{\frac{3}{4}+\epsilon}).$$

**2.1. Reduction theory for the action of  $\mathrm{PGL}_2(\mathbb{Z})$  on  $V(\mathbb{R})$ .** To count orbits of  $\mathrm{PGL}_2(\mathbb{Z})$  on  $V(\mathbb{Z})$ , we realize these orbits as lattice points in fundamental sets for the action of  $\mathrm{PGL}_2(\mathbb{Z})$  on  $V(\mathbb{R})$ . In this section, we construct such fundamental sets by means of a two-step process: first, in [Section 2.1.1](#), we describe a fundamental domain  $\mathcal{F}$  for the action of  $\mathrm{PGL}_2(\mathbb{Z})$  on  $\mathrm{PGL}_2(\mathbb{R})$ ; subsequently, in [Section 2.1.2](#), we combine  $\mathcal{F}$  with fundamental sets for the action of  $\mathrm{PGL}_2(\mathbb{R})$  on  $V(\mathbb{R})$ .

**2.1.1. A box-shaped fundamental domain for  $\mathrm{PGL}_2(\mathbb{Z}) \curvearrowright \mathrm{PGL}_2(\mathbb{R})$ .** We start by recalling Gauss’ fundamental domain for the action of  $\mathrm{PGL}_2(\mathbb{Z})$  on  $\mathrm{PGL}_2(\mathbb{R})$ , rephrased in terms of the Iwasawa decomposition of  $\mathrm{PGL}_2(\mathbb{R})$ , which we now recall. Let  $N$  be the (algebraic) subgroup of  $\mathrm{PGL}_2$  consisting of lower triangular unipotent matrices  $\begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}$ , let  $T$  be the maximal torus defined by  $T = \left\{ \begin{bmatrix} t^{-1} & 0 \\ 0 & t \end{bmatrix} : t \in \mathbb{R}_{>0} \right\}$ , and let  $K = \mathrm{SO}_2(\mathbb{R})/\{\pm \mathrm{id}\}$ . We often abuse notation by writing  $u$  and  $t$  for the corresponding elements of  $N(\mathbb{R})$  and  $A$ . If we let  $T' = \{t \in T : t \geq \sqrt[4]{3}/\sqrt{2}\}$ , then for each  $t \in T'$ , there exists a compact subset  $N'(t) \subset \left[-\frac{1}{2}, \frac{1}{2}\right]$  such that the set

$$\{ut : u \in N'(t), t \in T'\} \cdot K \tag{4}$$

is a fundamental domain  $\mathcal{F}$  for the action of  $\mathrm{PGL}_2(\mathbb{Z})$  on  $\mathrm{PGL}_2(\mathbb{R})$ . It is well known that  $N'(t) = \left[-\frac{1}{2}, \frac{1}{2}\right]$  for all  $t \geq 1$ ; consequently, we say that this fundamental domain is *box-shaped at infinity*. This property of the fundamental domain is essential for our proof.

We denote elements of  $K$  by  $\theta$ . With respect to the coordinates  $u$  on  $N(\mathbb{R})$ ,  $t$  on  $T$ , and  $\theta$  on  $K$ , the Haar measure  $dg$  on  $\mathrm{PGL}_2(\mathbb{R})$  is given by

$$dg = d\theta \, du(t^{-2} d^\times t), \tag{5}$$

where  $d^\times t = dt/t$ . Above,  $d\theta$  is normalized so that  $\int_{\theta \in K} d\theta = 1$ , and  $du$  is normalized so that  $N(\mathbb{Z})$  has covolume 1 in  $N(\mathbb{R})$ .

**2.1.2. Fundamental sets for  $\mathrm{PGL}_2(\mathbb{R}) \curvearrowright V(\mathbb{R})$  and  $\mathrm{PGL}_2(\mathbb{Z}) \curvearrowright V(\mathbb{R})$ .** The action of  $\mathrm{PGL}_2(\mathbb{R})$  on  $V(\mathbb{R})^{(0)} \sqcup V(\mathbb{R})^{(1)}$  has one orbit per set of *nondegenerate invariants* — i.e., a pair of invariants  $(I, J) \in \mathbb{R}^2$  such that  $\Delta(I, J) := 4I^3 - J^2 \neq 0$ . This orbit belongs to  $V(\mathbb{R})^{(0)}$  when  $\Delta(I, J) > 0$  and to  $V(\mathbb{R})^{(1)}$  when  $\Delta(I, J) < 0$ . Consider the function  $\sigma_0$  given by

$$\sigma_0 : \mathbb{R}^2 \setminus \{\Delta = 0\} \rightarrow V(\mathbb{R}), \quad (I, J) \mapsto x^3y - \frac{1}{3}Ixy^3 - \frac{1}{27}Jy^4. \tag{6}$$

It is easy to check that  $\sigma_0$  is a section of the map  $\mathrm{inv}$ , meaning that the invariants of  $\sigma_0(I, J)$  are  $I$  and  $J$ . For  $i \in \{0, 1\}$ , we take our fundamental sets for the action of  $\mathrm{PGL}_2(\mathbb{R})$  on  $V(\mathbb{R})$  to be

$$\mathcal{R}^{(i)} := \mathbb{R}_{>0} \cdot \{\sigma_0(I, J) : (-1)^i \Delta(I, J) > 0, H(I, J) = 1\}.$$

Finally, we note that the stabilizer  $\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{R})}(f)$  is independent of the choice of  $f \in V(\mathbb{R})^{(i)}$ ; letting  $n_i := \#\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{R})}(f)$  for any  $f \in V(\mathbb{R})^{(i)}$ , one readily verifies that  $n_0 = 4$  and  $n_1 = 2$ .

We conclude that the multiset  $\mathcal{F} \cdot \mathcal{R}^{(i)}$  is a cover for a fundamental domain for the action of  $\mathrm{PGL}_2(\mathbb{Z})$  on  $V(\mathbb{R})^{(i)}$ . More precisely, every  $\mathrm{PGL}_2(\mathbb{Z})$ -orbit of  $f \in V(\mathbb{R})^{(i)}$  is represented exactly  $n_i / \#\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{Z})}(f)$  times in  $\mathcal{F} \cdot \mathcal{R}^{(i)}$ .

**2.2. The action of the subgroup  $P$  on the reducible hyperplane  $V_0$ .** In this section, we examine the action of the lower-triangular (parabolic) subgroup  $P$  on the reducible hyperplane  $V_0$ . Specifically, in [Section 2.2.1](#), we show that over many interesting base rings  $R$ , the action of  $P(R)$  on the set of forms in  $V_0(R)$  lying over a given nondegenerate pair of invariants is simply transitive. Then, in [Section 2.2.2](#), we prove a Jacobian change-of-variables formula relating the Euclidean measure on  $V_0(R)$  to the product of the Haar measure on  $P(R)$  with the Euclidean measure on  $R^2$ . This formula will be applied in [Sections 2.3.3–2.3.4](#).

**2.2.1. Reduction theory for the action of  $P$  on  $V_0$ .** Let  $R$  be a field or  $\mathbb{Z}_p$  for some prime  $p$ . Then we have the following result, which classifies the orbits and stabilizers of  $P(R)$  on  $V_0(R)$ :

**Proposition 9.** *Let  $R$  be as above, and let  $(I, J) \in R^2$  be such that  $\Delta(I, J)$  is a unit. Then the set of binary quartic forms in  $V_0(R)$  with invariants  $I$  and  $J$  is either empty or consists of a single  $P(R)$ -orbit, and the stabilizer of any element in this orbit is trivial.*

*Proof.* Given a form  $f(x, y) = bx^3y + cx^2y^2 + dxy^3 + ey^4 \in V_0(R)$  having invariants  $I$  and  $J$ , we first note that  $b^2 \mid \Delta(f) = \Delta(I, J)$ . Thus, if  $\Delta(I, J)$  is a unit, then so is  $b$ . As a consequence, by replacing  $f(x, y)$  with a  $P(R)$ -translate, we can arrange that  $b = 1$ . When  $R \neq \mathbb{Z}_3$ , we have that  $3 \in R^\times$ , and

hence by replacing  $f$  with the  $P(R)$ -translate  $f(x - c/3y, y)$ , we may assume that  $c = 0$ . When  $R = \mathbb{Z}_3$ , we may similarly replace  $f$  with a  $P(R)$ -translate to arrange that  $c \in \{0, 1, 2\}$  (depending on the residue classes of  $I$  modulo 9 and  $J$  modulo 27). Once this has been done, the values of  $d$  and  $e$  are respectively determined by  $I$  and  $J$  (since  $a = 0$  implies linear relations between  $(I, J)$  and  $(d, e)$ ). This proves that the set of elements in  $V_0(R)$  with invariants  $I$  and  $J$  (if nonempty) form a single  $P(R)$ -orbit.

Next, we prove the claim regarding the stabilizer in  $P(R)$  of  $f \in V_0(R)$ . Suppose that an element  $g \in P(R)$ , represented by a matrix with coefficients 1 and  $u$  on the diagonal and  $n$  in the lower left coordinate, fixes  $f$ . First note that since  $b$  is a unit, the  $x^2y^2$ -coefficient of  $g \cdot f(x, y)$  will change unless  $n = 0$ . Assume thus that  $n = 0$ . Next note that the  $x^3y$ -coefficient of  $g \cdot f(x, y)$  is  $u^{-1}b$ , implying that  $u = 1$ , as needed. □

The above result has the following immediate consequence by specializing to the case  $R = \mathbb{R}$ .

**Lemma 10.** *Let  $(I, J) \in \mathbb{R}^2$  be nondegenerate. Then the set  $\{f \in \text{inv}^{-1}(f)_0 : b(f) > 0\}$  consists of a single  $N(\mathbb{R})T$ -orbit.*

**2.2.2. A Jacobian change-of-variables formula.** Proposition 9 implies that when  $R = \mathbb{R}$  or  $\mathbb{Z}_p$  for a prime  $p$ , the space  $V_0(R)$  is a fibration over  $R^2$ , where the generic fiber can be identified with  $P(R)$ , so long as it is nonempty. Thus, the Euclidean measure on  $V_0(R)$  should be related to the product of the Haar measure on  $P(R)$  with the Euclidean measure on  $R^2$ . The following proposition gives a Jacobian change-of-variables formula relating these measures:

**Proposition 11.** *Let  $R = \mathbb{R}$  or  $\mathbb{Z}_p$  for some prime  $p$ , and let  $\phi : V_0(R) \rightarrow \mathbb{R}$  be a measurable function. Then we have*

$$\int_{f \in V_0(R)} \phi(f) |b(f)| df = \frac{2}{27} \int_{\substack{(I, J) \in \mathbb{R}^2 \\ \Delta(I, J) \neq 0}} \left( \sum_{f \in \frac{\text{inv}^{-1}(I, J)_0}{P(R)}} \int_{h \in P(R)} \phi(h \cdot f) dh \right) dI dJ,$$

where  $df$ ,  $dI$ , and  $dJ$  are Euclidean measures, where  $dh$  is the right Haar measure on  $P$  given by  $dh = t du dt$ , and where  $|\cdot|$  denotes the usual absolute value on  $R$ .

*Proof.* First note that the result for  $R = \mathbb{R}$  implies the result for  $R = \mathbb{Z}_p$  by the principle of permanence of identities, so it suffices to treat the case  $R = \mathbb{R}$ . Recall the construction of the section  $\sigma_0$  in (6). Proposition 9 implies that we have

$$V_0(\mathbb{R}) = P(\mathbb{R}) \cdot \sigma_0(\{(I, J) \in \mathbb{R}^2 : \Delta(I, J) \neq 0\}).$$

Thus, the theorem follows from the equality

$$\int_{f \in P(\mathbb{R}) \cdot \sigma_0(\mathbb{R}^2 \setminus \{\Delta=0\})} \phi(f) |b(f)| df = \frac{2}{27} \int_{(I, J) \in \mathbb{R}^2} \int_{h \in P(\mathbb{R})} \phi(h \cdot \sigma_0(I, J)) dh dI dJ, \tag{7}$$

which in turn is a consequence of the following Jacobian change-of-variables computation. First note that a typical element of the region of integration on the left-hand side of (7) is given by

$$(tu) \cdot \sigma_0(I, J) = \frac{1}{t^2} x^3 y + 3u x^2 y^2 + \left( 3u^2 t^2 - \frac{I t^2}{3} \right) x y^3 + \left( u^3 t^4 - \frac{I u t^4}{3} - \frac{J t^4}{27} \right) y^4.$$

By taking partial derivatives with respect to  $t, u, I,$  and  $J$  of the coefficients of the binary quartic form on the right-hand side above and arranging these partials into matrix form, we find that the Jacobian determinant relating the measures  $df$  and  $dt du dI dJ$  is given by

$$\begin{vmatrix} -2t^{-3} & 0 & 6u^2t - \frac{2}{3}It & 4u^3t^3 - \frac{4}{3}Iut^3 - \frac{4}{27}Jt^3 \\ & 3 & 6ut^2 & 3u^2t^4 - \frac{1}{3}It^4 \\ & & -\frac{1}{3}t^2 & -\frac{1}{3}ut^4 \\ & & & -\frac{1}{27}t^4 \end{vmatrix} = -\frac{2}{27}t^3.$$

Therefore, we have

$$df = \frac{2}{27}t^3 dt du dI dJ.$$

Equation (7) then follows, since  $b((tu) \cdot \sigma_0(I, J)) = t^{-2}$ . □

**2.3. Counting reducible  $\text{PGL}_2(\mathbb{Z})$ -orbits on  $V(\mathbb{Z})$ .** Let  $i \in \{0, 1\}$ . In this section, we obtain asymptotics for the number of reducible orbits of  $\text{PGL}_2(\mathbb{Z})$  on  $V_0(\mathbb{Z})^{(i)}$  of bounded height, thus proving Theorems 6–8. To simplify the exposition in the rest of this section, we introduce the following notation:

- For any set  $S \subset V(\mathbb{Z})$ , let  $S_{\text{red}} \subset S$  be the subset of forms in  $S$  having a rational linear factor; for  $X > 0$ , let

$$S_X := \{B \in S : H(B) < X\},$$

and as before, let  $S_0 := S \cap V_0(\mathbb{Z})$  be the set of elements of  $S$  that lie on the reducible hyperplane.

- Let  $G_0 \subset \text{PGL}_2(\mathbb{R})$  be a fixed nonempty open bounded set such that  $G_0^{-1} = G_0$  and  $G_0$  is left- and right-invariant under the group  $K'$  generated by  $K$  together with the diagonal matrix having diagonal entries 1 and  $-1$ . Such a set can be constructed by starting with a nonempty open bounded set  $G'_0$  and taking  $G_0 = K'(G'_0 \cup G_0'^{-1})K'$ .

- Define the multiset  $\mathcal{B}_\infty$  by

$$\mathcal{B}_\infty := G_0 \cdot \mathcal{R}^{(i)} \cap V_0(\mathbb{R}).$$

Set  $\mathcal{B} := (\mathcal{B}_\infty)_1$ , and note that by the construction of  $\mathcal{R}$ , we have  $(\mathcal{B}_\infty)_X = X^{1/6}\mathcal{B}$ .

- We define the quantity  $C(\mathcal{B})$  by

$$C(\mathcal{B}) := \frac{1}{\tilde{n}_i \text{Vol}(G_0)} \cdot \int_{f \in \mathcal{B}} |b(f)| df, \tag{8}$$

where the volume of  $G_0$  is computed using the Haar measure  $dg$ , and where  $\tilde{n}_i = 2n_i$ , with  $n_i$  as defined in Section 2.1.2.

- For a finite set  $\Sigma$  of  $\text{PGL}_2(\mathbb{Z})$ -orbits on  $V(\mathbb{Z})$ , let  $\#\Sigma$  be the number of elements of  $\Sigma$ , where each  $f \in \Sigma$  is counted with weight  $1/\#\text{Stab}_{\text{PGL}_2(\mathbb{Z})}(f)$ .

**2.3.1. Averaging over fundamental domains.** We begin by applying Bhargava’s averaging technique, developed in [2; 4]. By an argument identical to [9, Theorem 2.5], which involves averaging over translates

of the fundamental domain  $\mathcal{F}$  by elements of  $G_0$  and performing a suitable change-of-variables, we have

$$\begin{aligned} \#'\left(\frac{(V^{(i)}(\mathbb{Z})_{\text{red}})_X}{\text{PGL}_2(\mathbb{Z})}\right) &= \frac{1}{n_i} \cdot \#(\mathcal{F}h \cdot \mathcal{R}^{(i)} \cap (V(\mathbb{Z})_{\text{red}})_X) \\ &= \frac{1}{n_i \text{Vol}(G_0)} \int_{g \in \mathcal{F}} \#(gG_0 \cdot \mathcal{R}_X^{(i)} \cap V(\mathbb{Z})_{\text{red}}) dg, \end{aligned} \tag{9}$$

Then we have the following result:

**Proposition 12.** *We have*

$$\#\left(\frac{(V^{(i)}(\mathbb{Z})_{\text{red}})_X}{\text{PGL}_2(\mathbb{Z})}\right) = \frac{1}{n_i \text{Vol}(G_0)} \int_{t=1}^{\infty} \int_{u=-\frac{1}{2}}^{\frac{1}{2}} \#(utX^{\frac{1}{6}}\mathcal{B} \cap V_0(\mathbb{Z}))t^{-2} du d^{\times}t + O_{\epsilon}(X^{\frac{3}{4}+\epsilon}), \tag{10}$$

where  $\mathcal{B}$  is the multiset

$$\mathcal{B} := (\mathcal{B}_{\infty})_1 := G_0 \cdot \mathcal{R}_1^{(i)} \cap V_0(\mathbb{R}).$$

*Proof.* The number of reducible (and irreducible)  $\text{PGL}_2(\mathbb{Z})$ -orbits on  $V(\mathbb{Z})$  that have nontrivial integral stabilizer was proven in [9, Lemma 2.4] to be bounded  $O(X^{3/4+\epsilon})$ . Thus, we may replace the  $\#'$  in (9) with  $\#$  at the cost of an error of  $O(X^{3/4+\epsilon})$ . We split the fundamental domain  $\mathcal{F}$  as

$$\mathcal{F} = \mathcal{F}' \sqcup \{utk : u \in [-\frac{1}{2}, \frac{1}{2}], t \geq 1, k \in K\},$$

where  $\mathcal{F}'$  is absolutely bounded. When the integral over  $\mathcal{F}$  is restricted to the compact region  $\mathcal{F}'$ , it is clear that the number of forms with vanishing  $x^4$ -coefficient is bounded by  $O(X^{2/3})$ . By [9, Lemma 2.3], the number of reducible forms with nonzero  $x^4$ -coefficient is bounded by  $O_{\epsilon}(X^{2/3+\epsilon})$ . These error terms are sufficiently small. The proposition then follows upon noting that, by the left  $K$ -invariance of  $G_0$ , the set  $gG_0\mathcal{R}^{(i)}$  is independent of  $\theta$  when  $g$  is written as  $g = ut\theta$  in Iwasawa coordinates.  $\square$

**2.3.2. Slicing.** Throughout this subsection we set  $Y := X^{1/6}$ . The integrand of the right-hand side of (10) is the number of integral points in the region  $utY\mathcal{B} \cap V_0(\mathbb{R})$ . This region is typically quite skewed: indeed, whenever  $t$  is high up in the cusp, the  $x^3y$ -coefficient is small, so the volumes of the projections of the set  $utY\mathcal{B}$  away from this coefficient have the same order of magnitude as the volume of  $utY\mathcal{B}$  itself. Furthermore, the region where  $t$  is high up in the cusp contributes most of the lattice points that we are interested in counting! We resolve this issue in this section by fibering the region  $utY\mathcal{B} \cap V_0(\mathbb{R})$  by the  $x^3y$ -coefficient and using a result of Davenport to estimate the number of lattice points on each fiber.

We now partition the region  $utY\mathcal{B}$  into slices, one for each possible value of the  $x^3y$ -coefficient. For any  $b \in \mathbb{R} \setminus \{0\}$ , and any  $S \subset V(\mathbb{R})$ , let  $S|_b$  denote the *slice of  $S$  at  $b$* , i.e., the subset of forms in  $S$  with  $x^4$ -coefficient equal to 0 and  $x^3y$ -coefficient equal to  $b$ . Then we can express the integrand of the right-hand side of (10) as

$$\#(utY\mathcal{B} \cap V_0(\mathbb{Z})) = \sum_{b \in \mathbb{Z}, b \neq 0} \#((utY\mathcal{B})|_b \cap V(\mathbb{Z})) = \sum_{b \in \mathbb{Z}, b \neq 0} \text{Vol}((utY\mathcal{B})|_b)(1 + O(Y^{-1})), \tag{11}$$

where the final estimate is a consequence of the following proposition, due to Davenport:

**Proposition 13** [21]. *Let  $\mathcal{R}$  be a bounded, semialgebraic multiset in  $\mathbb{R}^n$  having maximum multiplicity  $m$  that is defined by at most  $k$  polynomial inequalities, each having degree at most  $\ell$ . 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*

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

where  $\text{Vol}(\overline{\mathcal{R}})$  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  $\ell$ .

Now, since unipotent transformations preserve both the value of  $b$  and the volume, we have

$$\text{Vol}((utY\mathcal{B})|_b) = \text{Vol}((tY\mathcal{B})|_b).$$

Combining (11) with Proposition 12 yields

$$\begin{aligned} \# \left( \frac{(V^{(i)}(\mathbb{Z})_{\text{red}})_X}{\text{PGL}_2(\mathbb{Z})} \right) &= \frac{1}{n_i \text{Vol}(G_0)} \sum_{b \in \mathbb{Z} \setminus \{0\}} \int_{1 \leq t \ll Y^{1/2}/|b|^{1/2}} \text{Vol}((tY\mathcal{B})|_b) (1 + O(Y^{-1})) t^{-2} du d^\times t + O_\epsilon(X^{\frac{3}{4}+\epsilon}). \end{aligned} \quad (12)$$

The bound in the region of integration above is obtained by noting that the value of  $|b|$  is bounded above by  $O(Y)$ , and, for each fixed  $b \neq 0$ , the range of  $t$  goes up to  $Y^{1/2}/\sqrt{|b|}$ , since the  $x^3y$ -coefficients of elements in  $utY\mathcal{B}$  are  $\ll t^{-2}Y$ . We bound the error term in the right-hand side of (12) by

$$\ll Y^{-1} \text{Vol}((tY\mathcal{B})|_b) \ll \sum_{b=1}^{O(Y)} \int_{t=1}^{O(Y^{1/2}/\sqrt{b})} Y^2 t^6 \frac{d^\times t}{t^2} \ll Y^4 \sum_{b=1}^{O(Y)} b^{-2} \ll X^{\frac{3}{2}}. \quad (13)$$

Substituting the estimate (13) into (12) yields

$$\# \left( \frac{(V^{(i)}(\mathbb{Z})_{\text{red}})_X}{\text{PGL}_2(\mathbb{Z})} \right) = \frac{1}{n_i \text{Vol}(G_0)} \sum_{b \in \mathbb{Z} \setminus \{0\}} \int_{1 \leq t \ll Y^{1/2}/|b|^{1/2}} \text{Vol}((tY\mathcal{B})|_b) \frac{d^\times t}{t^2} + O_\epsilon(X^{\frac{3}{4}+\epsilon}). \quad (14)$$

We now manipulate the integrand in (14) to extract its dependence on the slicing index  $b$ . Because unipotent transformations leave volumes unchanged, and the action of  $t$  on  $V(\mathbb{R})$  scales the  $x^i y^j$ -coefficient by  $t^{i-j}$ , we have

$$\text{Vol}((tY\mathcal{B})|_b) = Y^3 \text{Vol}((t\mathcal{B})|_{b/Y}) = t^6 X^{1/2} \text{Vol}(\mathcal{B}|_{t^2 b/Y}). \quad (15)$$

Since  $G_0$  is left- $K'$ -invariant and since the diagonal matrix with entries 1 and  $-1$  belongs to  $K'$ , it follows that  $\text{Vol}(\mathcal{B}|_\beta) = \text{Vol}(\mathcal{B}|_{-\beta})$  for any  $\beta \in \mathbb{R} \setminus \{0\}$ . Hence, setting  $\beta = t^2 b/Y$  (which gives  $d^\times \beta = 2d^\times t$ ),

we obtain

$$\begin{aligned} \#\left(\frac{(V^{(i)}(\mathbb{Z})_{\text{red}})_X}{\text{PGL}_2(\mathbb{Z})}\right) &= \frac{X^{1/2}}{2n_i \text{Vol}(G_0)} \sum_{b \in \mathbb{Z} \setminus \{0\}} b^{-2} \int_{|b|/Y \leq \beta \ll 1} Y^2 \beta^2 \text{Vol}(\mathcal{B}|\beta) d^\times \beta + O_\epsilon(X^{\frac{3}{4}+\epsilon}) \\ &= \frac{X^{5/6}}{n_i \text{Vol}(G_0)} \sum_{b=1}^\infty b^{-2} \int_{\beta \geq 0} \beta \text{Vol}(\mathcal{B}|\beta) d\beta + O_\epsilon(X^{\frac{3}{4}+\epsilon}), \end{aligned} \tag{16}$$

where the second line above follows since  $\mathcal{B}|\beta$  is a bounded set and  $\text{Vol}(\mathcal{B}|\beta) \ll 1$ . It therefore follows that

$$\#\left(\frac{(V^{(i)}(\mathbb{Z})_{\text{red}})_X}{\text{PGL}_2(\mathbb{Z})}\right) = \zeta(2) \cdot C(\mathcal{B}) \cdot X^{\frac{5}{6}} + O_\epsilon(X^{\frac{3}{4}+\epsilon}), \tag{17}$$

where  $C(\mathcal{B})$  was defined in (8). Note that while going from (14) to (17), we pick up a factor of  $\frac{1}{2}$  from  $d^\times \beta = 2d^\times t$ , a factor of 2 from restricting the sum over  $b \in \mathbb{Z}$  to the sum over  $b > 0$ , and another factor of  $\frac{1}{2}$  by replacing the integral over  $\beta \geq 0$  to the integral over all  $\beta$  in the definition of  $C(\mathcal{B})$  (which is equivalent to the integral over all  $f \in \mathcal{B}$ ).

**2.3.3. Computing the constant.** In this section, we compute the value of  $C(\mathcal{B})$ . Recall that we defined  $\mathcal{B}$  to be the multiset  $\mathcal{B} := G_0 \cdot \mathcal{R}_1^{(i)} \cap V_0(\mathbb{R})$ . Since  $G_0$  is right  $K'$ -invariant, we may write  $G_0 = SK'$  for some  $S \subset N(\mathbb{R})T$ . Hence, we have

$$\mathcal{B} = SK' \cdot \mathcal{R}_1^{(i)} \cap V_0(\mathbb{R}) = S \cdot (K'\mathcal{R}_1^{(i)})_0.$$

We then have the following lemma concerning the multiplicity of the fiber of  $(K'\mathcal{R}^{(i)})_0$  over  $\text{inv}(V(\mathbb{R})^{(i)}) \subset \mathbb{R}^2$ :

**Lemma 14.** *The map  $\text{inv} : (K'\mathcal{R}^{(i)})_0 \rightarrow \{\text{inv}(V(\mathbb{R})^{(i)})\}$  is  $\tilde{n}_i$  to 1.*

*Proof.* We begin by noting the map is certainly surjective since the invariants  $I$  and  $J$  of  $x^3y + dxy^2 + ey^3$  are linear in  $d$  and  $e$ , respectively. It thus suffices to prove that the map

$$\text{inv} : \{f \in (K'\mathcal{R}^{(i)})_0 : b(f) > 0\} \rightarrow \text{inv}(V(\mathbb{R})^{(i)})$$

is  $n_i$  to 1. This is a consequence of the following two facts: first, the stabilizer in  $\text{PGL}_2(\mathbb{R})$  of any element in the image has size  $n_i$ , and second, the group  $N(\mathbb{R})T$  acts simply transitively on  $\text{inv}^{-1}(I, J) \cap V_0(\mathbb{R})$  for any  $(I, J) \in \text{inv}(V(\mathbb{R})^{(i)})$  by Lemma 10. Indeed, given  $f \in \mathcal{R}^{(i)}$  having invariants  $(I, J)$ , and  $p\theta \in \text{Stab}_{\text{PGL}_2(\mathbb{R})}(f)$  with  $p \in N(\mathbb{R})T$  and  $\theta \in K'$ , the element  $\theta f = p^{-1}f$  belongs to  $(K'\mathcal{R}^{(i)})_0$  and has invariants  $(I, J)$ . This association yields the result.  $\square$

We are now in position to compute the constant  $C(\mathcal{B})$ :

**Proposition 15.** *We have*

$$C(\mathcal{B}) = \frac{1}{27} \text{Vol}\{(I, J) \in \mathbb{R}^2 : (-1)^i \Delta(I, J) > 0, H(I, J) < 1\}.$$

*Proof.* We have

$$\begin{aligned}
 C(\mathcal{B}) &= \frac{1}{\tilde{n}_i \operatorname{Vol}(G_0)} \int_{f \in \mathcal{B}} |b(f)| \, df = \frac{1}{\tilde{n}_i \operatorname{Vol}(G_0)} \int_{f \in \mathcal{S} \cdot (K' \mathcal{R}_1^{(i)})_0} |b(f)| \, df \\
 &= \frac{2}{27 \operatorname{Vol}(G_0)} \int_{\substack{(I,J) \in \mathbb{R}^2 \\ (-1)^i \Delta(I,J) > 0 \\ H(I,J) < 1}} \int_{h \in \mathcal{S}} dh \, dI \, dJ \\
 &= \frac{2 \operatorname{Vol}_{\text{right}}(\mathcal{S}) \operatorname{Vol}\{(I, J) \in \mathbb{R}^2 : (-1)^i \Delta(I, J) > 0, H(I, J) < 1\}}{27 \operatorname{Vol}(SK')}, \tag{18}
 \end{aligned}$$

where the second line follows by applying the Jacobian change-of-variables established in [Proposition 11](#) along with [Lemma 14](#). In the third line,  $\operatorname{Vol}_{\text{right}}(\mathcal{S})$  denotes the volume of  $\mathcal{S}$  with respect to the right Haar measure on  $P(\mathbb{R})$ . But since  $\operatorname{Vol}(K)$  is normalized to be equal to 1, we have that  $\operatorname{Vol}_{\text{right}}(\mathcal{S}) = \frac{1}{2} \operatorname{Vol}(K'S)$ , where the volume is computed with respect to the Haar measure on  $G(\mathbb{R})$ . The next lemma demonstrates that  $\operatorname{Vol}(K'S) = \operatorname{Vol}(SK')$ :

**Lemma 16.** *We have  $K'S = SK'$ , and in particular  $\operatorname{Vol}(K'S) = \operatorname{Vol}(SK')$ .*

*Proof of Lemma 16.* Since  $G_0 = SK'$  is left- $K'$ -invariant and inversion-invariant, it follows that

$$K'S \subset K'SK' = SK' = G_0 = G_0^{-1} = K'S^{-1}. \tag{19}$$

Since the Iwasawa decomposition of  $\operatorname{PGL}_2(\mathbb{R})$  is unique, (19) implies that  $\mathcal{S} \subset \mathcal{S}^{-1}$ , and hence also that  $\mathcal{S} = \mathcal{S}^{-1}$ . Thus,  $SK' = K'S^{-1} = K'S$ , as desired. □

Combining (18) with the result of [Lemma 16](#) completes the proof of [Proposition 15](#). □

**2.3.4. Congruence conditions.** We now prove [Theorem 7](#). Let  $\mathcal{S} \subset V(\mathbb{Z})^{(i)}$  be a big family, and suppose for now that  $\mathcal{S}$  is defined by congruence conditions at finitely many places (i.e., suppose that  $\mathcal{S}_p = V(\mathbb{Z}_p)$  for all primes  $p \gg 1$ ). For each  $b \in \mathbb{Z}_p \setminus \{0\}$ , let

$$(S_p)_0|_b := \{f \in (S_p)_0 : b(f) = b\},$$

and for each  $b \in \mathbb{Z} \setminus \{0\}$ , let  $\nu(S_0|_b) := \prod_p \operatorname{Vol}((S_p)_0|_b)$  denote the density of the slice  $S_0|_b$  in  $V_0(\mathbb{Z})|_b$ ; here, each  $p$ -adic volume  $\operatorname{Vol}((S_p)_0|_b)$  is computed with respect to the Euclidean measure on  $V_0(\mathbb{Z}_p)|_b$ , normalized so that  $V_0(\mathbb{Z}_p)|_b$  has volume 1. Then an argument identical to the one used to obtain (14) yields the asymptotic formula

$$\#\left(\frac{(S_{\text{red}})_X}{\operatorname{PGL}_2(\mathbb{Z})}\right) = \frac{1}{n_i \operatorname{Vol}(G_0)} \sum_{b \in \mathbb{Z} \setminus \{0\}} \nu(S_0|_b) \int_{t \geq 1} \operatorname{Vol}((tYB)|_b) t^{-2} d^\times t + O_\epsilon(X^{\frac{3}{4}+\epsilon}). \tag{20}$$

Note that the upper bound on  $t$  in (14) can be omitted, since if  $t > cY^{1/2}/b^{1/2}$  for some sufficiently large constant  $c$ , then  $(tYB)|_b$  is empty. The  $\operatorname{PGL}_2(\mathbb{Z})$ -invariance of  $\mathcal{S}$  implies that  $\nu(S_0|_b) = \nu(S_0|_{|b|})$  for all  $b$ . Hence, the argument used to deduce (16) and (17) yields the estimate

$$\#\left(\frac{(S_{\text{red}})_X}{\operatorname{PGL}_2(\mathbb{Z})}\right) = C(\mathcal{B}) \cdot \left(\sum_{b=1}^{\infty} \frac{\nu(S_0|_b)}{b^2}\right) \cdot X^{\frac{5}{6}} + O_\epsilon(X^{\frac{3}{4}+\epsilon}). \tag{21}$$

To evaluate the sum over  $b$  on the right-hand side of (21), we use the following property, which is a consequence of the fact that  $S$  is a big family: if  $p$  is a prime and  $b, b' \in \mathbb{Z}_p \setminus \{0\}$  are elements such that  $|b_i|_p = |b'_i|_p$  for each  $i$ , then  $\text{Vol}((S_p)_0|_b) = \text{Vol}((S_p)_0|_{b'})$ . By repeatedly using this property, we obtain the chain of equalities

$$\begin{aligned} \sum_{b=1}^{\infty} \frac{v(S_0|_b)}{b^2} &= \prod_p \sum_{i=0}^{\infty} \frac{\text{Vol}((S_p)_0|_{p^i})}{p^{2i}} \\ &= \prod_p \left(1 - \frac{1}{p}\right)^{-1} \int_{\substack{b \in \mathbb{Z}_p \\ b \neq 0}} |b|_p \text{Vol}((S_p)_0|_b) db \\ &= \prod_p \left(1 - \frac{1}{p}\right)^{-1} \int_{f \in (S_p)_0} |b(f)|_p df, \end{aligned}$$

where the second line above follows by partitioning the region of integration  $\mathbb{Z}_p \setminus \{0\}$  into level sets for the integrand and summing over all such level sets, and where the last line above follows just as in (17).

It remains to handle the case where  $S$  is a big family defined by congruence conditions at infinitely many places. This case follows by using an inclusion-exclusion sieve<sup>4</sup> in conjunction with the following bound on the number of  $\text{PGL}_2(\mathbb{Z})$ -equivalence classes of forms  $f$  with large  $b(f)$ -value:

**Theorem 17.** *Fix a real number  $M > 0$ . Then the number of  $\text{PGL}_2(\mathbb{Z})$ -equivalence classes of (or equivalently,  $P(\mathbb{Z})$ -orbits of) elements of the set  $\{f \in V_0(\mathbb{Z}) : H(f) < X, |b(f)| \geq M\}$  is bounded by  $O(X^{5/6}/M) + O_\epsilon(X^{3/4+\epsilon})$ , where the implied constant is independent of  $M$ .*

*Proof.* The required bound follows immediately from the proof of Theorem 6 by simply summing (16) over only those  $b$  such that  $|b| \geq M$ . □

This concludes the proof of Theorem 7. We finish by noting that Theorem 8 follows from Theorem 7 by applying the Jacobian change-of-variables result in Proposition 11 to each  $p$ -adic integral.

### 3. Reduction theory for the action of $G(\mathbb{Z})$ on $W(\mathbb{R})$

Fix an integer  $n \geq 3$ . In this section, we construct finite covers of a fundamental set for the action of  $G(\mathbb{Z})$  on  $W(\mathbb{R})$ . As in Section 2.1, we achieve this in two steps: first, in Sections 3.1–3.2, we choose a certain fundamental domain  $\mathcal{F}$  for the action of  $G(\mathbb{Z})$  on  $G(\mathbb{R})$ , and then in Section 3.3, we combine  $\mathcal{F}$  with fundamental sets for the action of  $G(\mathbb{R})$  on  $W(\mathbb{R})$  to construct our required covers.

Note that it suffices to construct a fundamental domain for  $O_A(\mathbb{Z})$  on  $O_A(\mathbb{R})$ , as such a domain would also be a fundamental domain for  $G(\mathbb{Z})$  on  $G(\mathbb{R})$ . Indeed, when  $n$  is odd, this follows because  $O_A(\mathbb{Z})$  contains an element of determinant  $-1$ , namely, the negative of the identity matrix. When  $n$  is even, this follows because the 2-torsion elements of  $O_A(\mathbb{R})$  are contained in  $O_A(\mathbb{Z})$ . Thus, in Sections 3.1–3.2, we work with the group  $O_A$ . Furthermore, for our counting purposes, we cannot simply use any fundamental

---

<sup>4</sup>We do not flesh out the sieving argument here to avoid being repetitive, because in Section 6.3 (to follow), we use the same sort of argument to prove Theorem 4.



which it occurs). We often abbreviate the tuple

$$(u_{ij} : i \in \{2, \dots, n-1\}, j \in \{1, \dots, \min\{i-1, n-i\}\})$$

by  $u$  and abuse notation by writing  $u$  for the corresponding element of  $N(\mathbb{R})$ .

Elements of  $T$  have the form  $s = \text{diag}(t_1, \dots, t_n)$ , with  $t_i t_{n-i+1} = 1$  for  $i \in \{1, \dots, \lceil \frac{n}{2} \rceil\}$ . (Note in particular that when  $n$  is odd, we have  $t_{(n+1)/2} = 1$ .) In the sequel, it will be convenient to use the following alternative coordinates for  $T$ . Define the coordinates  $(s_1, \dots, s_{\lfloor n/2 \rfloor})$  to be such that  $(t_1, \dots, t_{\lfloor n/2 \rfloor})$  is equal to

$$\left( \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} s_i^{-1}, \prod_{i=2}^{\lfloor \frac{n}{2} \rfloor} s_i^{-1}, \dots, s_{\lfloor \frac{n}{2} \rfloor}^{-1} \right) \quad \text{if } 2 \nmid n, \tag{24}$$

$$\left( \mathfrak{s}_n^{-1} \cdot \prod_{i=1}^{\frac{n-4}{2}} s_i^{-1}, \mathfrak{s}_n^{-1} \cdot \prod_{i=2}^{\frac{n-4}{2}} s_i^{-1}, \dots, \mathfrak{s}_n^{-1} \cdot s_{\frac{n-4}{2}}^{-1}, \mathfrak{s}_n^{-1}, \mathfrak{s}_n^{-1} \cdot s_{\frac{n-2}{2}} \right) \quad \text{if } 2 \mid n, \tag{25}$$

where  $s_i > 0$  for each  $i$  and where  $\mathfrak{s}_n := \sqrt{s_{(n-2)/2} s_{(n)/2}}$  when  $n$  is even.

We denote the elements of  $K$  by  $\theta$ . With respect to the coordinates  $u$  on  $N(\mathbb{R})$ ,  $s$  on  $T$ , and  $\theta$  on  $K$ , the Haar measure  $dg$  on  $O_{\mathcal{A}}(\mathbb{R})$  is given by

$$dg = d\theta \, du(\delta(s) \, d^\times s), \tag{26}$$

where

$$du := \prod_{i=1}^{\lceil \frac{n}{2} \rceil} \prod_{j=1}^{i-1} du_{ij}, \quad d^\times s := \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \frac{ds_i}{s_i}, \quad \delta(s) := \begin{cases} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} s_i^{i^2-2i} & \text{if } 2 \nmid n, \\ (s_{\frac{n-2}{2}} s_{\frac{n}{2}})^{-\frac{n^2-2n}{8}} \prod_{i=1}^{\frac{n-4}{2}} s_i^{i^2-i(n-1)} & \text{if } 2 \mid n. \end{cases}$$

Above,  $d\theta$  is normalized so that  $\int_{\theta \in \{\pm \text{id}\} \backslash K} d\theta = 1$ , and  $du$  is normalized so that  $N(\mathbb{Z})$  has covolume 1 in  $N(\mathbb{R})$ .

**3.2. A box-shaped fundamental domain for  $O_{\mathcal{A}}(\mathbb{Z}) \curvearrowright O_{\mathcal{A}}(\mathbb{R})$ .** A fundamental domain  $\mathcal{F}$  is said to be *box-shaped at infinity* if it can be sandwiched as  $S_1 \subset \mathcal{F} \subset S_2$ , where  $S_1 \subset S_2$  are nested generalized Siegel sets<sup>5</sup> satisfying the following conditions:

- (a) There exists an open subset  $\mathcal{U}_1 \subset \mathfrak{S}_1$  of full measure such that every  $O_{\mathcal{A}}(\mathbb{Z})$ -orbit on  $O_{\mathcal{A}}(\mathbb{R})$  meets  $\mathcal{U}_1$  at most once.
- (b) Every  $O_{\mathcal{A}}(\mathbb{Z})$ -orbit on  $O_{\mathcal{A}}(\mathbb{R})$  meets  $S_2$  at least once.
- (c) The set  $S_2 \setminus S_1$  is empty “sufficiently high in the cusp,” in the sense that, for some  $c > 0$ , the set  $T_c := \{s = (s_1, \dots, s_{\lfloor n/2 \rfloor}) \in T : s_i > c \text{ for all } i\}$  has the property that  $S_1 \cap NT_c K = S_2 \cap NT_c K$ .

<sup>5</sup>Here, a fundamental domain  $\mathcal{F} \subset O_{\mathcal{A}}(\mathbb{R})$  is defined to be a measurable subset such that there exists a subset  $\mathcal{M} \subset O_{\mathcal{A}}(\mathbb{R})$  of full measure with the property that every  $g \in \mathcal{M}$  is  $O_{\mathcal{A}}(\mathbb{Z})$ -equivalent to a unique element of  $\mathcal{F}$ . By a generalized Siegel set, we mean a finite union of Siegel sets.

Because they are defined by simple equations in the cusp, box-shaped fundamental domains are particularly amenable to explicit computations. For instance, we use the box-shaped property to evaluate a certain integral that arises in the proof of [Theorem 1](#) (see [\(35\)](#)). As another example of the utility of box-shaped fundamental domains, see [\[27; 28\]](#), where Grenier proved the analogue of [Theorem 18](#) for the group  $SL_n$  and remarked that his result could be used to compute certain integrals of Eisenstein series that arise when generalizing Selberg’s trace formula to the group  $SL_n(\mathbb{Z})$ . Grenier’s work has had a number of applications in the literature (see, e.g., [\[26; 38; 53\]](#)), and as explained in [Section 3.2](#) (to follow), it plays a central role in our proof of [Theorem 18](#).

In this subsection, we construct a box-shaped fundamental domain for the action of  $O_{\mathcal{A}}(\mathbb{Z})$  on  $O_{\mathcal{A}}(\mathbb{R})$ . Specifically, we prove the following result:

**Theorem 18.** *There exists a fundamental domain for the action of  $O_{\mathcal{A}}(\mathbb{Z})$  on  $O_{\mathcal{A}}(\mathbb{R})$  that is box-shaped at infinity.*

Our proof of [Theorem 18](#) occurs over the next five subsections and is structured as follows:

- First, in [Section 3.2.1](#), we show that it suffices to construct the nested generalized Siegel sets  $S_1 \subset S_2$  satisfying the properties (a)–(c) enumerated above.
- Next, in [Section 3.2.2](#), we construct  $S_2$  in terms of a certain compact subset  $\mathcal{N} \subset N(\mathbb{R})$ , and in [Section 3.2.3](#), we make a convenient explicit choice for the set  $\mathcal{N}$ .
- It then remains to construct  $S_1$ , which we do using the aforementioned work of Grenier. Specifically, in [Section 3.2.4](#), we recall the construction of Grenier’s domain, and in [Section 3.2.5](#), we use his result to construct  $S_1$ .

**3.2.1. Reduction to constructing  $S_1$  and  $S_2$ .** The following lemma reduces the problem of constructing the desired fundamental domain  $\mathcal{F}$  into the simpler problem of constructing  $S_1$  and  $S_2$ :

**Lemma 19.** *Let  $\Lambda$  be a discrete subgroup of a Lie group  $\mathcal{G}$  and denote by  $\mathcal{B}(\mathcal{G})$  the Borel  $\sigma$ -algebra of  $\mathcal{G}$ . Suppose that  $S$  and  $S'$  are sets in  $\mathcal{B}(\mathcal{G})$  with the property that the maps  $S \rightarrow \mathcal{G}/\Lambda$  and  $S' \rightarrow \mathcal{G}/\Lambda$  induced by  $s \mapsto s\Lambda$  are, respectively, injective and surjective. Then there is a fundamental domain  $\mathcal{F}$  in  $\mathcal{B}(\mathcal{G})$  for the action of  $\Lambda$  on  $\mathcal{G}$  such that  $S \subset \mathcal{F} \subset S'$ .*

*Proof.* The argument is analogous to the proof of [\[35, Lemma 4.1.1\]](#). Since  $\Lambda$  is discrete, we can find a nonempty open subset  $U \subset \mathcal{G}$  such that  $U^{-1}U \cap \Lambda = \{\text{id}\}$ . Since  $\mathcal{G}$  is second countable, we can find a sequence of elements  $\{g_n\} \subset \mathcal{G}$  such that  $\mathcal{G} = \bigcup_{n=1}^{\infty} g_n U$ . Let  $S'' = S' \setminus S\Lambda$  and set

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

Lastly, define  $\mathcal{F} = S \cup \mathcal{F}'$  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  $\sigma$ -algebra. It is simple to check that the induced map  $\mathcal{F} \rightarrow \mathcal{G}/\Lambda$  sending  $x$  to  $x\Lambda$  is bijective. We conclude that  $\mathcal{F}$  is a fundamental domain. □

**3.2.2. Constructing  $S_2$ .** We now construct  $S_2$  in terms of a certain compact subset  $\mathcal{N} \subset N(\mathbb{R})$ , to be chosen explicitly in the next subsection. This construction is in essence due to Borel and Harish-Chandra (see [6, Section 9.2] and [43, Section 4.1], which specialize the results of [18; 19] for semisimple groups to the case of the group  $SO_A$ ). By [18, Théorème 2.4 and Exemple 2.5], there exist a constant  $c_2 > 0$  and a compact set  $\mathcal{N} \subset N(\mathbb{R})$  such that if we take

$$T_2 := \{s = (s_1, \dots, s_{\lfloor n/2 \rfloor}) \in T : s_i > c_2 \text{ for all } i\},$$

then the set

$$S_2 := \mathcal{N} T_2 (\{\pm \text{id}\} \backslash K) \tag{27}$$

meets every orbit of  $O_A(\mathbb{Z})$  on  $O_A(\mathbb{R})$  at least once (hence satisfying property (b) above), where  $\{\pm \text{id}\} \backslash K$  denotes some strict fundamental domain for the action of the group  $\{\pm \text{id}\}$  by left-multiplication on  $K$  (where “strict” means that every coset of  $\{\pm \text{id}\}$  has a unique representative).<sup>6</sup>

**3.2.3. Choosing  $\mathcal{N}$ .** Having constructed  $S_2$  in terms of  $\mathcal{N}$ , we now make an explicit choice of  $\mathcal{N}$  that will be convenient in what follows. Let  $\bar{\mathcal{N}} \subset N(\mathbb{R})$  be the subset defined as

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

The following lemma implies that by chopping  $\mathcal{N}$  into pieces and translating them via elements of  $N(\mathbb{R}) \cap O_A(\mathbb{Z})$ , we can replace  $\mathcal{N}$  with a subset of  $\bar{\mathcal{N}}$ :

**Lemma 20.** *Let  $u \in N(\mathbb{R})$ . Then there exists  $\bar{u} \in N(\mathbb{R}) \cap O_A(\mathbb{Z})$  such that  $\bar{u}u \in \bar{\mathcal{N}}$ . Moreover, there exists an open subset  $\mathcal{U}_3 \subset N(\mathbb{R})$  of full measure such that for any  $u \in \mathcal{U}_3$  there is precisely one element  $\bar{u} \in N(\mathbb{R}) \cap O_A(\mathbb{Z})$  such that  $\bar{u}u \in \bar{\mathcal{N}}$ .*

*Proof.* We construct  $\bar{u}$  inductively. Upon inspecting the coordinate system on  $N$  provided in Section 3.1, we arrive at the following observation: if  $k \in \{0, \dots, n-3\}$  is an integer and  $u' \in N(\mathbb{R})$  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  $u_1 \in N(\mathbb{R}) \cap O_A(\mathbb{Z})$  such that  $|(u_1)_{i(i-1)} + u_{i(i-1)}| \leq \frac{1}{2}$  for each  $i \in \{2, \dots, \lfloor \frac{n}{2} \rfloor\}$  and such that, for  $n$  odd, we have  $|(u_1)_{\lceil n/2 \rceil \lfloor n/2 \rfloor} + u_{\lceil n/2 \rceil \lfloor n/2 \rfloor}| \leq 1$ . Suppose for some  $k \in \{0, \dots, n-4\}$  we have chosen  $u_\ell \in N(\mathbb{R}) \cap O_A(\mathbb{Z})$  for each  $\ell \in \{1, \dots, k+1\}$ ; then, by the observation, we may choose  $u_{k+2} \in N(\mathbb{R}) \cap O_A(\mathbb{Z})$  such that  $|(u_1)_{i(i-k-2)} + u_{i(i-k-2)}| \leq \frac{1}{2}$  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  $|(u_1)_{\lceil n/2 \rceil (\lceil n/2 \rceil - k - 2)} + u_{\lceil n/2 \rceil (\lceil n/2 \rceil - k - 2)}| \leq 1$ . Having constructed  $u_\ell$  for each  $\ell \in \{1, \dots, n-2\}$ , we then take  $\bar{u} = \prod_{\ell=1}^{n-2} u_{n-2-\ell}$ .

As for uniqueness on an open subset of full measure, it suffices to show that  $\bar{u}$  is unique when  $u$  lies in the interior of  $\bar{\mathcal{N}}$ , for then we can take  $\mathcal{U}_3$  to be the union of all  $(N(\mathbb{R}) \cap O_A(\mathbb{Z}))$ -translates of the interior

<sup>6</sup>A priori, [18, Théorème 2.4] states that a finite number  $\sigma$  of translates of Siegel sets can be found such that their union meets every orbit of  $O_A(\mathbb{Z})$  on  $O_A(\mathbb{R})/K$  at least once; here,  $\sigma = \#(O_A(\mathbb{Z}) \backslash O_A(\mathbb{Q})/\mathcal{P}(\mathbb{Q}))$ . But since the algebraic group  $O_A$  has class number 1, it follows from [37, Propositions 5.4 and 5.10] that  $\sigma = 1$ .

of  $\bar{\mathcal{N}}$ . So take  $u \in \bar{\mathcal{N}}$ . If  $\bar{u}u \in \bar{\mathcal{N}}$  for some  $\bar{u} \in N(\mathbb{R}) \cap O_{\mathcal{A}}(\mathbb{Z})$ , then the aforementioned observation, together with the fact that  $u$  lies in the interior of  $\bar{\mathcal{N}}$ , implies that  $\bar{u}_{i(i-1)} = 0$  for each  $i$ . Proceeding inductively as we did to prove existence, we find that  $\bar{u} = \text{id}$ .  $\square$

By Lemma 20, we may assume that  $\mathcal{N} \subset \bar{\mathcal{N}}$ . We next show that  $\mathcal{N}$  can be chosen to lie within an even smaller subset of  $\bar{\mathcal{N}}$ . Let  $\Gamma \subset O_{\mathcal{A}}(\mathbb{Z})$  denote the subgroup of diagonal matrices with integer entries. One readily verifies that  $\Gamma$  satisfies the following properties:

- $\Gamma$  is a subgroup of  $K$  of order  $2^{\lceil n/2 \rceil}$  centralizing  $T$ ;
- Conjugation by elements of  $\Gamma$  defines a group action on  $\bar{\mathcal{N}}$  with the property that for any  $\rho \in \Gamma$  and  $u \in \bar{\mathcal{N}}$ , we have  $|(\rho \cdot u)_{ij}| = |u_{ij}|$  for all  $i, j$ .
- The orbit of every element of  $\bar{\mathcal{N}}$  under the action of  $\Gamma$  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  $u_{\lceil n/2 \rceil \lfloor n/2 \rfloor} \in [-1, -\frac{1}{2}] \cup [0, \frac{1}{2}]$ . 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

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

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

**3.2.4. Grenier’s domain.** In the following subsection, we shall deduce the construction of the set  $\mathcal{S}_1$  from a slight reformulation of Grenier’s explicit box-shaped fundamental domain  $\mathcal{F}$  for the action of  $\text{SL}_n^{\pm}(\mathbb{Z})$  on  $\text{SL}_n^{\pm}(\mathbb{R})$  (see [28]). To state this reformulation, we must introduce some notation. Let  $\mathcal{N} \subset \text{SL}_n^{\pm}(\mathbb{R})$  denote the subgroup of lower-triangular unipotent matrices; for an element  $u \in \mathcal{N}$ , we denote by  $u_{ij}$  the row- $i$ , column- $j$  entry of  $u$ . Let  $\bar{\mathcal{N}}$  be the set defined by

$$\bar{\mathcal{N}} := \left\{ u \in \mathcal{N} : |u_{ij}| \leq \frac{1}{2} \text{ for all } i, j \right\}.$$

Let  $\mathcal{T} \subset \text{SL}_n^{\pm}(\mathbb{R})$  denote the subgroup of diagonal matrices with positive entries; for an element  $s \in \mathcal{T}$ , 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  $\mathcal{K} \subset \text{SL}_n^{\pm}(\mathbb{R})$  denote a maximal compact subgroup containing  $K$ .

Consider the subset  $\mathcal{N}' \subset \bar{\mathcal{N}}$  defined as

$$\begin{aligned} \mathcal{N}' := \left\{ u \in \bar{\mathcal{N}} : u_{i(i-1)} \in [0, \frac{1}{2}] \text{ for each } i \in \{2, \dots, \lfloor \frac{n}{2} \rfloor\}, \right. \\ \left. u_{i(i-1)} \in [-\frac{1}{2}, 0] \text{ for each } i \in \left\{ \lfloor \frac{n}{2} \rfloor + 2, \dots, n \right\}, \right. \\ \left. u_{(\lceil \frac{n}{2} \rceil + 1) \lfloor \frac{n}{2} \rfloor} \in [-\frac{1}{2}, 0] \text{ if } 2 \nmid n, u_{(\frac{n+2}{2}) \frac{n}{2}} \in [-\frac{1}{2}, \frac{1}{2}] \text{ if } 2 \mid n \right\}. \end{aligned}$$

Let  $\mathcal{T}' := \{s \in \mathcal{T} : s_i > c_1 \text{ for all } i\}$  for a sufficiently large constant  $c_1 > c_2$ . Let  $\varepsilon_n \in \mathcal{K}$  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  $\{\pm \text{id}, \pm \varepsilon_n\} \setminus \mathcal{K}$  denote some strict fundamental domain for the action of the group  $\{\pm \text{id}, \pm \varepsilon_n\}$  by left-multiplication on  $K$ .

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

**Lemma 21.** *For every sufficiently large  $c_1 > 0$ , the following property holds: If*

$$us\theta, u's'\theta' \in \mathcal{N}' \mathcal{T}' (\{\pm \text{id}, \pm \varepsilon_n\} \setminus \mathcal{K})$$

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

*Proof.* In [27], Grenier constructed a fundamental domain  $\overline{\mathcal{F}} \subset \mathcal{N} \mathcal{T}$  for the action of  $\text{SL}_n^\pm(\mathbb{Z})$  on  $\text{SL}_n^\pm(\mathbb{R})/\mathcal{K}$ . The domain  $\overline{\mathcal{F}}$  has the property that no two points in its interior are  $\text{SL}_n^\pm(\mathbb{Z})$ -equivalent. In [28, Theorem 1], Grenier established that, for every sufficiently large  $c_1 > 0$ , we have  $\mathcal{N}'' \mathcal{T}' \subset \overline{\mathcal{F}}$ , where  $\mathcal{N}'' = \{u \in \mathcal{N}' : u_{((n+2)/2)(n/2)} \in [0, \frac{1}{2}]\}$ . Consequently, the set  $\overline{\mathcal{F}}(\{\pm \text{id}\} \setminus \mathcal{K})$  is a fundamental domain for the action of  $\text{SL}_n^\pm(\mathbb{Z})$  on  $\text{SL}_n^\pm(\mathbb{R})$  containing  $\mathcal{N}'' \mathcal{T}'(\{\pm \text{id}\} \setminus \mathcal{K})$ . Since  $\varepsilon_n \mathcal{N}'' \varepsilon_n = \mathcal{N}'$ , it follows that there is a fundamental domain for the action of  $\text{SL}_n^\pm(\mathbb{Z})$  on  $\text{SL}_n^\pm(\mathbb{R})$  containing  $\mathcal{N}' \mathcal{T}'(\{\pm \text{id}, \pm \varepsilon_n\} \setminus \mathcal{K})$ . If we have two distinct  $\text{SL}_n^\pm(\mathbb{Z})$ -equivalent elements  $us\theta, u's'\theta' \in \mathcal{N}' \mathcal{T}'(\{\pm \text{id}, \pm \varepsilon_n\} \setminus \mathcal{K})$  such that  $u, u'$  lie in the interior of  $\mathcal{N}'$ , then one can find two distinct elements of the interior of  $\overline{\mathcal{F}}$  that are  $\text{SL}_n^\pm(\mathbb{Z})$ -equivalent, which is a contradiction.  $\square$

**3.2.5. Constructing  $\mathcal{S}_1$ .** Let  $T_1 := \{s \in T : s_i > c_1 \text{ for all } i\}$ , where the constant  $c_1 > 0$  is to be chosen shortly. We then take

$$\mathcal{S}_1 := \mathcal{N} T_1 (\{\pm \text{id}\} \setminus K).$$

It is evident that  $\mathcal{S}_1$  and  $\mathcal{S}_2$  satisfy property (c) above. The following lemma states that we can choose  $c_1$  so that  $\mathcal{S}_1$  lies within  $\mathcal{S}_2$  and satisfies property (a) above:

**Lemma 22.** *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  $\text{O}_A(\mathbb{Z})$  on  $\text{O}_A(\mathbb{R})$  meets  $\mathcal{U}_1$  at most once.*

*Proof.* 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 stabilizer under left-multiplication by  $\text{O}_A(\mathbb{Z})$  of  $us\theta \in \text{O}_A(\mathbb{R})/K$  is given by  $\{\pm \text{id}\}$ .
- There exists a unique element  $u_0 \in \mathcal{N} \cap \text{SL}_n^\pm(\mathbb{Z})$  such that  $u_0u$  lies in the interior of  $\mathcal{N}'$ .

To see why we can arrange for the first property above to hold on an open subset of full measure, we use the following lemma:

**Lemma 23.** *There exists an open subset  $\mathcal{U} \subset \text{O}_A(\mathbb{R})/K$  of full measure such that the stabilizer in  $\text{O}_A(\mathbb{Z})$  of any  $g \in \mathcal{U}$  is given by  $K \cap \{\pm \text{id}\}$ .*

*Proof of Lemma 23.* Let  $\overline{\mathcal{F}}$  be any fundamental domain for  $\text{O}_A(\mathbb{Z})$  on  $\text{O}_A(\mathbb{R})/K$ , and let  $g$  be an element of the interior of  $\overline{\mathcal{F}}$ . If  $\gamma \in \text{O}_A(\mathbb{Z})$  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  $\gamma$  stabilizes every element of  $U$ . Since left-multiplication by  $\gamma$  defines a real-analytic function on  $\text{O}_A(\mathbb{R})/K$ , and since

$O_{\mathcal{A}}(\mathbb{R})/K$  is connected (as  $K$  meets both of the two connected components of  $O_{\mathcal{A}}(\mathbb{R})$ ), it follows that  $\gamma$  stabilizes all of  $O_{\mathcal{A}}(\mathbb{R})/K$ .

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

Finally, let  $\mathcal{U}$  be the union of all  $O_{\mathcal{A}}(\mathbb{Z})$ -translates of the interior of  $\bar{\mathcal{F}}$ . Then  $\mathcal{U}$  is an open subset of full measure, and we have shown above that the stabilizer in  $O_{\mathcal{A}}(\mathbb{Z})$  of any  $g \in \mathcal{U}$  is contained in  $\{\pm \text{id}\}$ , as desired. This completes the proof of [Lemma 23](#). □

As for the second property, observe that by the definitions of  $\mathcal{N}$  and  $\mathcal{N}'$ , 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 20](#) for the group  $SL_n^{\pm}$ , one finds that there exists at least one  $u_0 \in \mathcal{N} \cap SL_n^{\pm}(\mathbb{Z})$  such that  $u_0u \in \mathcal{N}'$ . By our explicit characterization of the elements of  $\mathcal{N}$  (see [\(22\)](#) and [\(23\)](#)), the row- $i$ , column- $j$  entry of  $u$  is a nonconstant polynomial in the unipotent coordinates for every pair  $(i, j)$  with  $i > j + 1$ . Thus, there exists an open subset  $\mathcal{U}_2 \subset \mathcal{N}$  of full measure such that for any  $u \in \mathcal{U}_2$  and  $u_0 \in \mathcal{N} \cap SL_n^{\pm}(\mathbb{Z})$ , the row- $i$ , column- $j$  entry of  $u_0u$  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  $u \in \mathcal{U}_2$  and  $u_0 \in \mathcal{N} \cap SL_n^{\pm}(\mathbb{Z})$  we have  $u_0u \in \mathcal{N}'$ , then  $u_0u$  must in fact lie in the interior of  $\mathcal{N}'$ , and imitating the proof of uniqueness in [Lemma 20](#) 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  $g \in O_{\mathcal{A}}(\mathbb{Z})$ . Let  $\varepsilon, \varepsilon' \in \{\pm \text{id}, \pm \varepsilon_n\}$  be such that  $\varepsilon\theta, \varepsilon'\theta' \in \{\pm \text{id}, \pm \varepsilon_n\} \setminus \mathcal{K}$ . Let  $u_0, u'_0 \in \mathcal{N} \cap SL_n^{\pm}(\mathbb{Z})$  be the unique elements such that  $u_0(\varepsilon u \varepsilon), u'_0(\varepsilon' u' \varepsilon')$  lie in the interior of  $\mathcal{N}'$ . Since  $s_i, s'_i > c_1$  for all  $i$ , it follows from [Lemma 21](#) 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

$$u_0(\varepsilon u \varepsilon) = u'_0(\varepsilon' u' \varepsilon'), \quad s = s', \quad \varepsilon\theta = \varepsilon'\theta'. \tag{28}$$

The third equality in [\(28\)](#) implies that  $\varepsilon\varepsilon' \in K$ , so since  $\varepsilon_n \notin K$  when  $n$  is even, it follows that  $\varepsilon\varepsilon' = \pm \text{id}$ . But  $(\{\pm \text{id}\} \setminus K)$  contains either  $\theta$  or  $-\theta$  and not both, meaning that  $\varepsilon\varepsilon' = \text{id}$ . Combining this with the first equality in [\(28\)](#) yields that  $u$  is a translate of  $u'$  by an element of  $\mathcal{N} \cap SL_n^{\pm}(\mathbb{Z})$ , and hence by an element of  $\mathcal{N} \cap O_{\mathcal{A}}(\mathbb{Z})$ . The uniqueness statement in [Lemma 20](#) then implies that  $u = u'$ . We conclude that  $us\theta = u's'\theta'$ .

This completes the proof of [Lemma 22](#), and hence also that of [Theorem 18](#). □

**3.3. Fundamental sets for  $G(\mathbb{R}) \curvearrowright W(\mathbb{R})$  and  $G(\mathbb{Z}) \curvearrowright W(\mathbb{R})$ .** Let  $r$  and  $s$  be nonnegative integers with  $r + 2s = n$ . We define  $U(\mathbb{R})^{(r)}$  to be the set of monic polynomial  $f(x)$  of degree  $n$  with  $r$  distinct real roots and  $s$  distinct pairs of complex conjugate roots. We let  $W(\mathbb{R})^{(r)}$  denote  $\text{inv}^{-1}(U(\mathbb{R})^{(r)})$ , and let  $W(\mathbb{R})^{(r),\text{red}}$  be the set of elements in  $W(\mathbb{R})^{(r)}$  that are reducible over  $\mathbb{R}$ . Let  $f$  be an element in  $U(\mathbb{R})^{(r)}$ . From [\[6, Section 9\]](#) and [\[43, Section 4\]](#), we know that the set  $\{B \in W(\mathbb{R})^{(r),\text{red}} : \text{inv}(B) = f\}$  consists of

a single  $G(\mathbb{R})$ -orbit, and also that the quantity

$$\theta_r := \# \text{Stab}_{G(\mathbb{R})}(B) \tag{29}$$

is independent of the choice of  $B \in W(\mathbb{R})^{(r)}$ .

We next exhibit an explicit representative of the reducible  $G(\mathbb{R})$ -orbit of  $\text{inv}^{-1}(f)$  for polynomials  $f \in U(\mathbb{R})$ . Denote the coefficients of  $f$  by  $f(x) = x^n + f_1x^{n-1} + \dots + f_n$ , and define  $\sigma_0 : U(\mathbb{R}) \rightarrow W_0(\mathbb{R})$  by

$$\sigma_0(f) := \begin{bmatrix} & & & & & & & & & & 1 & 0 \\ & & & & & & & & & \ddots & 0 & \\ & & & & & & & & & & & \\ & & & & & & & & & & 1 & 0 \\ & & & & & & & & & & 1 & f_1 & -\frac{f_2}{2} \\ & & & & & & & & & & 1 & 0 & -\frac{f_2}{2} & -f_3 & \ddots \\ & & & & & & & & & \ddots & & & & & \ddots & -\frac{f_{n-3}}{2} \\ & & & & & & & & & & & & & & & & -\frac{f_{n-3}}{2} & -f_{n-2} & -\frac{f_{n-1}}{2} \\ & & & & & & & & & & & & & & & & & & & -\frac{f_{n-1}}{2} & -f_n \\ 1 & 0 & \\ 0 & \end{bmatrix}$$

if  $n$  is odd, and by

$$\sigma_0(f) := \begin{bmatrix} & & & & & & & & & & 1 & 0 \\ & & & & & & & & & & \ddots & 0 \\ & & & & & & & & & & & \\ & & & & & & & & & & 1 & 0 \\ & & & & & & & & & & 1 & -\frac{f_1}{2} \\ & & & & & & & & & & 1 & -\frac{f_1}{2} & \frac{f_1^2}{4} & -f_2 & -\frac{f_3}{2} \\ & & & & & & & & & & 1 & 0 & -\frac{f_3}{2} & -f_4 & \ddots \\ & & & & & & & & & \ddots & & & & & \ddots & \ddots & -\frac{f_{n-3}}{2} \\ & -\frac{f_{n-3}}{2} & -f_{n-2} & -\frac{f_{n-1}}{2} \\ 1 & 0 & -\frac{f_{n-1}}{2} & -f_n \\ 0 & -\frac{f_{n-1}}{2} & -f_n \end{bmatrix}$$

if  $n$  is even. These sections are constructed and used in [16, equations (11) and (27)]. It is easy to check that we have  $\text{inv}(\sigma_0(f)) = f$ , and so  $\sigma_0$  is indeed a section. This explicit section  $\sigma_0$  is useful in the proof of Proposition 27 (to follow), for its image consists of matrices whose entries are polynomials in the  $f_i$ . However, in Section 5.2 (also to follow), we shall require a section  $\sigma$  with image consisting of elements  $B$  whose entries are  $O(H(B))$ . To this end, we rescale  $\sigma_0$ : given  $f \in U(\mathbb{R})$  having height  $Y$  and nonzero discriminant, set  $f_1(x) := f(x/Y)$ . Then  $H(f_1) = 1$ , and we define the section  $\sigma$  by  $\sigma(f) := H(f)\sigma(f_1)$ . It is easy to check that  $\sigma$  is also a section, and that the coefficients of  $B$  in the image of  $\sigma$  are bounded by  $O(H(B))$ . We now define  $\mathcal{R}^{(r)}$  to be  $\sigma(U(\mathbb{R})^{(r)}) \subset W(\mathbb{R})^{(r),\text{red}}$ .

Finally, we have the following result, which follows immediately from an argument parallel to [9, Section 2.1]:

**Proposition 24.** *The multiset  $\mathcal{F} \cdot \mathcal{R}^{(r)}$  is a cover of a fundamental domain for the action of  $G(\mathbb{Z})$  on  $W(\mathbb{R})^{(r),\text{red}}$ . More precisely, every  $G(\mathbb{Z})$ -orbit of  $B \in W(\mathbb{R})^{(r),\text{red}}$  is represented exactly  $\theta_r / \#\text{Stab}_{G(\mathbb{R})}(B)$  times in  $\mathcal{F} \cdot \mathcal{R}^{(r)}$ .*

#### 4. The action of the subgroup $\mathcal{P}$ on the reducible hyperplane $W_0$

In this section, we examine the action of the lower-triangular (parabolic) subgroup  $\mathcal{P}$  on the reducible hyperplane  $W_0$ . Specifically, in Section 4.1, we show that over many interesting base rings  $R$ , the action of  $\mathcal{P}(R)$  on the set of elements in  $W_0(R)$  lying over a given nondegenerate invariant polynomial is simply transitive. Then, in Section 4.2, we prove a Jacobian change-of-variables formula relating the Euclidean measure on  $W_0(R)$  to the product of the Haar measure on  $\mathcal{P}(R)$  with the Euclidean measure on  $U(R)$ . This formula will be applied in Sections 5.3–5.4 and 6.3.

**4.1. Reduction theory for the action of  $\mathcal{P}$  on  $W_0$ .** Let  $R$  be either a field or  $\mathbb{Z}_p$  for some prime  $p$ . Then, by analogy with Proposition 9, we have the following result, which classifies the orbits and stabilizers of  $\mathcal{P}(R)$  on  $W_0(R)$ :

**Proposition 25.** *Let  $R$  be as above, and let  $f \in U(R)$  be an element with unit discriminant. Then  $\text{inv}^{-1}(f) \cap W_0(R)$  consists of a single  $\mathcal{P}(R)$ -orbit, and the stabilizer of any element of this unique orbit is trivial.*

*Proof.* We first prove the transitivity claim for any integral domain  $R$  in which 2 is invertible (this includes every field of characteristic not 2, as well as  $\mathbb{Z}_p$  for odd primes  $p$ ). Let  $B = [b_{ij}]$  be any element in  $\text{inv}^{-1}(f) \cap W_0(R)$ . The idea of the proof is to show that  $B$  can be transformed under the group  $\mathcal{P}(R)$  into an element of the image of the section  $\sigma_0$ , which is defined over  $R$  because we assumed that  $2 \in R^\times$ . Since distinct elements in the image of  $\sigma_0$  have distinct invariants, it will follow that  $B$  is  $\mathcal{P}(R)$ -equivalent to  $\sigma_0(f)$ , as necessary.

We now translate  $B$  into the image of  $\sigma_0$ . First, notice that each  $b_{i(n-i)}$  is a unit in  $R$ : indeed, the discriminant of  $f$  is a unit in  $R$ , and each  $b_{i(n-i)}$  divides the discriminant of  $f$ . Thus, we may use the action of the diagonal matrices in  $\mathcal{P}(R)$  to transform each  $b_{i(n-i)}$  into 1, and we may assume in what follows that  $b_{i(n-i)} = 1$  for each  $i$ .

Next, using the coefficients of  $N$  given in (22) and (23), we abuse notation by denoting, for any  $v_{ij} \in R$ , an element in  $N(R)$  called  $\tilde{u}_{ij}$ , whose  $u_{ij}$ -coefficient is  $v_{ij}$ , and whose other coefficients are 0. We successively replace  $B$  by  $N(R)$ -translates of itself by means of the following steps:

- (1) Let  $v_{21} \in R$  be such that  $b_{1n} + \tilde{u}_{21} = 0$ . In other words,  $v_{21} = -b_{1n}$ . We redefine  $B$  to be  $\tilde{u}_{21} \cdot B$ . We now have  $b_{1n} = 0$ .
- (2) Set  $v_{32} := -b_{2(n-1)}$ , and redefine  $B$  to be  $\tilde{u}_{32} \cdot B$ . Next, set  $v_{31} := -b_{2n}$  and redefine  $B$  to be  $\tilde{u}_{31} \cdot B$ . We now have  $b_{2(n-1)} = b_{2n} = 0$ .
- ( $k$ ) Let  $k \in \{3, \dots, n-2\}$ , and suppose that we have transformed the first  $k-1$  rows (and hence the first  $k-1$  columns) of  $B$  into the required form. We now explain how to transform the  $k$ -th row (and column)

of  $B$  into what is needed; i.e., we explain how to clear out the entries  $b_{k(n-j)}$  for  $j$  in the appropriate range. First set

$$v_{(k+1)\min\{k,n-k-1\}} := -b_{k\max\{k+2,n-k+1\}}$$

and redefine  $B$  to be  $\tilde{u}_{(k+1)\min\{k,n-k-1\}} \cdot B$ . Next set

$$v_{(k+1)\min\{k-1,n-k-2\}} := -b_{k\max\{k+3,n-k+2\}}$$

and redefine  $B$  to be  $\tilde{u}_{(k+1)\min\{k-1,n-k-2\}} \cdot B$ . These two steps clear out  $b_{k\max\{k+2,n-k+1\}}$  and  $b_{k\max\{k+3,n-k+2\}}$ . Continuing in this manner, let  $k' \in \{3, \dots, \min\{k-1, n-k-2\}\}$ , and suppose that we have cleared out  $b_{kj}$  for  $j \in \max\{k+2, n-k+1\}, \dots, \max\{k+k'+1, n-k+k'\}$ . Then set

$$v_{(k+1)\min\{k-k',n-k-k'-1\}} := b_{k\max\{k+k'+2,n-k+k'+1\}},$$

and redefine  $B$  to be  $\tilde{u}_{(k+1)\min\{k-k',n-k-k'-1\}} \cdot B$ . This process has now cleared out the all of the required entries in the  $k$ -th row of  $B$ .

Having transformed the first  $n-2$  rows (and therefore columns) of  $B$  into the required form, note that the last two rows are already as required. We have thus replaced  $B$  by an  $\mathcal{P}(R)$ -translate to ensure that  $B$  lies in the image of  $\sigma_0$ , as desired.

We now handle the case where  $R = \mathbb{Z}_2$ . In this case, when  $n$  is even, the argument given above works without change. But it does not quite work when  $n$  is odd, because every element  $u \in N(\mathbb{Z}_2)$  has the property that  $u_{\lfloor n/2 \rfloor j}$  is divisible by 2 for each  $j \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}$  (see (22)). Thus, in step  $(\lfloor \frac{n}{2} \rfloor)$  of the process outlined above, the action of  $N(\mathbb{Z}_2)$  can only be used to make the entries  $b_{\lfloor n/2 \rfloor j}$  equal to either 0 or 1. Consequently, once all the steps have been completed, the resulting matrix  $B$  may fail to lie in the image of  $\sigma_0(f)$ , but only because some of the entries  $b_{\lfloor n/2 \rfloor j}$  might be equal to 1. Now, it is easy to verify that such a matrix  $B$  has  $b_{\lfloor n/2 \rfloor j} = 1$  if and only if the  $x^{2n-2j+1}$ -coefficient of  $f$  is odd. Thus, the arrangement of 0's and 1's in the  $\lfloor \frac{n}{2} \rfloor$ -th row of  $B$  is uniquely determined by the invariants, and the claim follows.

We finally handle the case where  $R$  is a field of characteristic 2. In this case, when  $n$  is even, every element of  $W_0(R)$  has discriminant zero, and so the claim is moot. When  $n$  is odd, the argument used in the case  $R = \mathbb{Z}_2$  works without change.

The claim regarding the stabilizers of elements in  $W_0(R)$  follows by inspection. Indeed, any element of  $\mathcal{P}(R)$  stabilizing  $B$  must fix each  $b_{i(n-i)}$  and hence must lie in the subgroup  $N(R) \subset \mathcal{P}(R)$ ; moreover, any element of  $u \in N(R)$  can be factored as  $u = \prod \tilde{u}_{ij}$ , and it follows from the points enumerated above that  $u$  stabilizes  $B$  if and only if each  $\tilde{u}_{ij}$  stabilizes  $B$ , which happens if and only if each  $\tilde{u}_{ij}$  is the identity matrix. (Note: this stabilizer computation works over any integral domain  $R$ .)  $\square$

By analogy with Lemma 10, the above result has the following immediate consequence by specializing to the case  $R = \mathbb{R}$ :

**Lemma 26.** *Let  $f \in U(\mathbb{R})$  be nondegenerate. Then the set  $\{B \in \text{inv}^{-1}(f)_0 : b_{k(n-k)}(B) > 0 \text{ for each } k\}$  consists of a single  $N(\mathbb{R})T$ -orbit.*

**4.2. A Jacobian change-of-variables formula.** Proposition 25 implies that when  $R = \mathbb{R}$  or  $\mathbb{Z}_p$  for a prime  $p$ , the space  $W_0(R)$  is a fibration over  $U(R)$ , where the generic fiber can be identified with  $\mathcal{P}(R)$ , so long as it is nonempty. Thus, the Euclidean measure on  $W_0(R)$  should be related to the product of the Haar measure on  $\mathcal{P}(R)$  with the Euclidean measure on  $U(R)$ . By analogy with Proposition 11, the following result shows that the relationship between these measures is governed by the polynomial function  $\lambda$  on  $W_0$  defined as in (2):

**Proposition 27.** *Let  $R = \mathbb{R}$  or  $\mathbb{Z}_p$  for some prime  $p$ . Let  $\phi : W_0(R) \rightarrow \mathbb{R}$  be a measurable function. Then there exists a nonzero rational number  $\mathcal{J} \in \mathbb{Q}^\times$  such that*

$$\int_{B \in W_0(R)} \phi(B) |\lambda(B)| dB = |\mathcal{J}| \int_{\substack{f \in U(R) \\ \text{disc}(f) \neq 0}} \left( \sum_{B \in \frac{\text{inv}^{-1}(f)_0}{\mathcal{P}(R)}} \int_{h \in \mathcal{P}(R)} \phi(h \cdot B) dh \right) df,$$

where  $dB$  and  $df$  are Euclidean measures, where  $dh$  is the right Haar measure on  $\mathcal{P}$  given by  $dh = \delta(s)^{-1} du d^\times s$ , and where  $|-|$  denotes the usual absolute value on  $R$ .

**Remark.** Unlike in Proposition 11, which concerns a representation of small dimension, we cannot prove Proposition 27 by means of a direct computation. Instead, we follow the general four-step strategy used to prove [9, Propositions 3.7, 3.10], which establish an analogous change-of-variables formula in a simpler setting, where the group  $\mathcal{P}$  is replaced by a semisimple group, and the factor of  $|\lambda(B)|$  is not present. The first step is to note that a similar equation holds, where the Jacobian constant  $\mathcal{J}$  is replaced by a Jacobian function that a priori depends on the section  $\sigma$ , the group element  $h$ , and the invariant  $f$ . Second, the Jacobian function is shown to be independent of the group element  $h$  using left-invariance of the Haar measure (which does not hold in our case). Third, the Jacobian function is shown to be independent of the section  $\sigma$  using right-invariance of Haar measure (which does hold in our case, and the independence on the section follows in exactly the same way). Finally, once independence of  $\sigma$  has been established, the section can be chosen to be a polynomial map, from which independence on the invariant can be easily deduced by comparing degrees and dimensions of the invariants and spaces involved. This final step also goes through without change for us.

Thus, the main difference in our case is that the Haar measure  $dh$  is not left-invariant. As we demonstrate below, the extra factor of  $|\lambda(B)|$  captures how the volumes of sets in  $W_0(R)$  transform under left-translation by group elements and therefore compensates for the failure of the measure  $dh$  to be left-invariant.

*Proof of Proposition 27.* Let  $\mathcal{U} \subset U(\mathbb{R})$  be an open set, and let  $\sigma : \mathcal{U} \rightarrow W_0(\mathbb{R})$  be a continuous section (such as the section  $\sigma_0$  constructed in Section 3.3) with respect to  $\text{inv}$ . We first claim that we have

$$\int_{B \in \mathcal{P}(\mathbb{R}) \cdot \sigma(\mathcal{U})} \phi(B) |\lambda(B)| dB = |\mathcal{J}| \int_{f \in \mathcal{U}} \int_{h \in \mathcal{P}(\mathbb{R})} \phi(h \cdot \sigma(f)) dh df \tag{30}$$

for some nonzero rational constant  $\mathcal{J} \in \mathbb{Q}^\times$ . We prove (30) in a series of steps. First, by the Stone–Weierstrass theorem, we may assume that  $\sigma$  is piecewise analytic, in which case we have

$$\int_{B \in \mathcal{P}(\mathbb{R}) \cdot \sigma(\mathcal{U})} \phi(B) |\lambda(B)| dB = \int_{f \in \mathcal{U}} \int_{h \in \mathcal{P}(\mathbb{R})} |\mathcal{J}_\triangleright(h, f)| \phi(h \cdot \sigma(f)) dh df,$$

where  $\mathcal{J}_\sigma(h, f)$  denotes the determinant of the Jacobian matrix arising from the change-of-variables taking the measure  $\lambda(B) dB$  on to the product measure  $dh df$ . Note in particular that the function  $\mathcal{J}_\sigma$  is piecewise continuous in both arguments  $h$  and  $f$ .

Second, we show that  $\mathcal{J}_\sigma(h, f)$  is independent of  $h$ . To do this, fix  $\gamma \in \mathcal{P}(\mathbb{R})$ , and consider the transformation on  $W_0(\mathbb{R})$  sending  $B$  to  $\gamma \cdot B$ . Then there is a character  $\chi_\lambda : \mathcal{P}(\mathbb{R}) \rightarrow \mathbb{R}_{>0}$  such that  $\lambda(\gamma \cdot B)d(\gamma \cdot B) = \chi_\lambda(\gamma)\lambda(B)dB$ ; note that  $\chi_\lambda$  exists because  $\lambda(B)$  is a product of coefficients that are unchanged by the action of  $N(\mathbb{R})$ . In fact, writing  $\gamma = tu = su$ , the elementary computation

$$\begin{aligned} \lambda(\gamma \cdot B) d(\gamma \cdot B) &= \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} (t_i/t_{i+1})^{1-2i} \lambda(B) t_1^{n-1} \prod_{i=2}^{\lfloor \frac{n}{2} \rfloor} t_i^{n-2i+2} dB \\ &= t_1^{n-2} \prod_{i=2}^{\lfloor \frac{n}{2} \rfloor} t_i^{n-2i} \lambda(B) dB = \delta(s)^{-1} \lambda(B) dB \end{aligned}$$

for odd  $n$  (and a similar one for even  $n$ ) reveals that  $\chi_\lambda(\gamma) = \delta(s)^{-1}$  for  $\gamma = su$ . On the other hand, the transformation  $B \mapsto \gamma \cdot B$  acts on  $\mathcal{P}(\mathbb{R}) \times \mathcal{U}$  by sending  $(h, f)$  to  $(\gamma h, f)$ . Letting  $\rho : \mathcal{P}(\mathbb{R}) \rightarrow \mathbb{R}_{>0}$  denote the modulus for the left action of  $\mathcal{P}$  on the right Haar measure  $dh$ , we see that

$$\mathcal{J}_\sigma(\gamma h, f) d(\gamma h) df = \rho(\gamma) \mathcal{J}_\sigma(h, f) dh df. \tag{31}$$

By definition,  $\rho(\gamma) = \delta(s)^{-1}$  for  $\gamma = su$ , and so we have  $\rho(\gamma) = \chi_\lambda(\gamma)$ . Therefore, we have

$$\mathcal{J}_\sigma(\gamma h, f) d(\gamma h) df = \lambda(\gamma B) dB = \chi_\lambda(\gamma)\lambda(B) dB = \chi_\lambda(\gamma)\mathcal{J}_\sigma(h, f) dh df. \tag{32}$$

Comparing (31) and (32), we see that  $\mathcal{J}_\sigma(h, f) = \mathcal{J}(f)$  is independent of  $h$ .

Third, that  $\mathcal{J}_\sigma(h, f)$  is independent of  $\sigma$  follows from an argument identical to Step 2 in the proof of [9, Proposition 3.10]; this step relies crucially on the fact that the measure  $dh$  is right-invariant. Thus, we can take  $\sigma$  to be the polynomial section  $\sigma_0$  defined in Section 3.3. Having made this choice of section, that  $\mathcal{J}_{\sigma_0}(h, f)$  is independent of  $f$  and given by a nonzero rational constant follows from an argument identical to Steps 3 and 4 in the proof of [9, Proposition 3.10].

We have therefore proven (30). Proposition 27 now follows from (30) and the principle of permanence of identities in a manner identical to how [9, Proposition 3.7] is deduced from [9, Proposition 3.10].  $\square$

We conclude this section by computing the value of the Jacobian constant  $|\mathcal{J}| \in \mathbb{Q}^\times$  that arises in Proposition 27:

**Proposition 28.** *The value of  $|\mathcal{J}|$  is 1 when  $n$  is odd and  $2^{-n/2}$  when  $n$  is even.*

*Proof.* To compute  $|\mathcal{J}|$ , it suffices to compute  $|\mathcal{J}|_p$  for each  $p$  since  $\mathcal{J} \in \mathbb{Q}^\times$ . To do this, we construct convenient sets in  $W_0(\mathbb{Z}_p)$  whose volumes are computed in two different ways: first, using Proposition 27, and second, via an  $\mathbb{F}_p$ -point count. Equating the two answers yields the value of  $|\mathcal{J}|_p$ .

*Case 1:*  $p > 2$ . Fix a nondegenerate polynomial  $f \in U(\mathbb{F}_p)$ , and let  $\phi_p : W_0(\mathbb{Z}_p) \rightarrow \mathbb{R}$  be the indicator function of the set

$$\Sigma := \{B \in W_0(\mathbb{Z}_p) : \text{inv}(B) \equiv f \pmod{p}\}.$$

By [Proposition 25](#), the group  $\mathcal{P}(\mathbb{Z}_p)$  acts simply transitively on the set of elements in  $\Sigma$  having any fixed invariant polynomial. Hence, from [Proposition 27](#), we obtain

$$\text{Vol}(\Sigma) = |\mathcal{J}|_p \cdot \text{Vol}(\mathcal{P}(\mathbb{Z}_p)) \int_{\substack{g \in U(\mathbb{Z}_p) \\ g \equiv f \pmod{p}}} dg = |\mathcal{J}|_p \cdot \text{Vol}(\mathcal{P}(\mathbb{Z}_p)) \cdot p^{-\dim U}. \tag{33}$$

On the other hand, [Proposition 25](#) also implies that the group  $\mathcal{P}(\mathbb{F}_p)$  acts simply transitively on the mod- $p$  reduction  $\bar{\Sigma}$  of  $\Sigma$ . Thus, we have

$$\#\bar{\Sigma} = \#\mathcal{P}(\mathbb{F}_p). \tag{34}$$

Since  $\text{Vol}(\Sigma) = p^{-\dim W_0} \cdot \#\bar{\Sigma}$ ,  $\text{Vol}(\mathcal{P}(\mathbb{Z}_p)) = p^{-\dim \mathcal{P}} \cdot \#\mathcal{P}(\mathbb{F}_p)$ , and  $\dim \mathcal{P} + \dim U = \dim W_0$ , we obtain from (33) and (34) that  $|\mathcal{J}|_p = 1$  for all odd primes  $p$ .

*Case 2:  $p = 2$ .* The proof here is similar to Case 1, so we highlight the differences. Pick an integer  $m \gg 1$ , and set  $q = 2^m$ . This time, we pick the polynomial  $f(x) = x^n \in U(\mathbb{Z}/q\mathbb{Z})$ , and we define the set

$$\Sigma := \{B \in W_0(\mathbb{Z}_2) : |b_{i(n-i)}(B)|_2 = 1 \text{ for all } i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}, \text{inv}(B) \equiv f \pmod{q}\}.$$

As before, we obtain

$$\text{Vol}(\Sigma) = |\mathcal{J}|_2 \cdot \text{Vol}(\mathcal{P}(\mathbb{Z}_2)) \cdot q^{-\dim U}.$$

However, the situation over  $\mathbb{Z}/q\mathbb{Z}$  is more complicated. Here, the mod- $q$  reduction  $\bar{\Sigma}$  of  $\Sigma$  breaks up into  $2^{\lfloor n/2 \rfloor}$  different  $\mathcal{P}(\mathbb{Z}/q\mathbb{Z})$ -orbits. Indeed, the  $\lfloor \frac{n}{2} \rfloor$  different coefficients labeled  $-\frac{f_i}{2}$  in the image of  $\sigma_0(f)$  in [Section 3.3](#) can be taken to be either 0 or  $\frac{q}{2}$ , and this gives exactly  $2^{\lfloor n/2 \rfloor}$  different elements that are inequivalent under the action of  $\mathcal{P}(\mathbb{Z}/q\mathbb{Z})$ . Therefore, this time we have

$$\#\bar{\Sigma} = 2^{\lfloor \frac{n}{2} \rfloor} \cdot \#\mathcal{P}(\mathbb{Z}/q\mathbb{Z}).$$

As before, we have  $\text{Vol}(\Sigma) = q^{-\dim W_0} \cdot \#\bar{\Sigma}$ , and it is easy to check that we have  $\text{Vol}(\mathcal{P}(\mathbb{Z}_2)) = 2^{\lfloor n/2 \rfloor} q^{-\dim \mathcal{P}} \cdot \#\mathcal{P}(\mathbb{Z}/q\mathbb{Z})$  when  $n$  is odd and  $\text{Vol}(\mathcal{P}(\mathbb{Z}_2)) = q^{-\dim \mathcal{P}} \cdot \#\mathcal{P}(\mathbb{Z}/q\mathbb{Z})$  when  $n$  is even. It follows that  $|\mathcal{J}|_2 = 1$  when  $n$  is odd and  $|\mathcal{J}|_2 = 2^{n/2}$  when  $n$  is even.  $\square$

### 5. Counting reducible $G(\mathbb{Z})$ -orbits on $W(\mathbb{Z})$

Let  $n \geq 3$ ,  $r$ , and  $s$  be nonnegative integers with  $r + 2s = n$ .<sup>7</sup> In this section, we obtain asymptotics for the number of reducible orbits of  $G(\mathbb{Z})$  on  $W(\mathbb{Z})^{(r)}$  of bounded height, thereby proving [Theorems 1, 3, and 4](#) using Method I. The proofs using Method II are given in the next section.

To simplify the exposition in the rest of this section, we introduce the following notation:

- For any set  $S \subset W(\mathbb{Z})$ , let  $S_{\text{red}} \subset S$  be the subset of reducible elements of  $S$ ; for  $X > 0$ , let  $S_X := \{B \in S : H(B) < X\}$ ; and as before, let  $S_0 := S \cap W_0(\mathbb{Z})$  be the set of elements of  $S$  that lie on the reducible hyperplane.

<sup>7</sup>Note that definitions of quantities introduced in what follows may implicitly depend on  $r$ .

- Let  $G_0 \subset G(\mathbb{R})$  be a fixed nonempty open bounded set such that  $G_0^{-1} = G_0$  and  $G_0$  is left- and right- $K$ -invariant. As explained in Section 2.3, such a set can be constructed by starting with a nonempty open bounded set  $G'_0$  and taking  $G_0 = K(G'_0 \cup G'^{-1}_0)K$ .

- Define the multiset  $\mathcal{B}_\infty$  by

$$\mathcal{B}_\infty := G_0 \cdot \mathcal{R}^{(r)} \cap W_0(\mathbb{R}).$$

Set  $\mathcal{B} := (\mathcal{B}_\infty)_1$ , and note that by the construction of  $\mathcal{R}$ , we have  $(\mathcal{B}_\infty)_X = X\mathcal{B}$ .

- We define the quantity  $C(\mathcal{B})$  by

$$C(\mathcal{B}) := \frac{1}{\tilde{\theta}_r \text{Vol}(G_0)} \cdot \int_{B \in \mathcal{B}} |\lambda(B)| \, dB,$$

where the volume of  $G_0$  is computed using the Haar measure  $dg$ , and where  $\tilde{\theta}_r := 2^{\lceil n/2 \rceil} \theta_r$ , with  $\theta_r$  as defined in (29).

- For a finite set  $\Sigma$  of  $G(\mathbb{Z})$ -orbits on  $W(\mathbb{Z})$ , let  $\#\Sigma$  be the number of elements of  $\Sigma$ , where each  $B \in \Sigma$  is counted with weight  $1/\#\text{Stab}_{G(\mathbb{Z})}(B)$ .

This section is organized as follows. After setting up Bhargava’s averaging method in Section 5.1, we reduce the problem of counting reducible  $G(\mathbb{Z})$ -orbits on  $W(\mathbb{Z})$  to a question of counting integer points in various regions of  $W_0(\mathbb{Z})$ . This is accomplished in Proposition 29 by combining previously obtained “main ball” counting estimates. The advantage of this result over simply applying the averaging method over the nonreductive group  $\mathcal{P}$  is that the integral in the right-hand side of (36) goes over  $T_1$  instead of  $T$ . This comes at a cost of a fairly large (but sufficient for our purposes) error term. The regions in  $W_0(\mathbb{R})$  that we need to count in are very skewed. In Section 5.2, we use a slicing method to express the point count in terms of certain constants that are expressed as products of local integrals. In Section 5.3, we use our Jacobian change-of-variables from the previous section to evaluate the contribution to these constants from the infinite place. Finally, in Section 5.4, we evaluate the contribution from finite places, and also carry out a squarefree sieve proving Theorems 1, 3, and 4.

**5.1. Averaging over fundamental domains.** As in Section 2.3.1, we begin by applying Bhargava’s averaging technique, developed in [2; 4]. Let  $\mathcal{F}$  be a fundamental domain for the action of  $G(\mathbb{Z})$  on  $G(\mathbb{R})$  that is box-shaped at infinity (recall that such an  $\mathcal{F}$  exists by Theorem 18). Then, by analogy with (9), we obtain

$$\#\left(\frac{(W(\mathbb{Z})_{\text{red}})^{(r)}_X}{G(\mathbb{Z})}\right) = \frac{1}{\theta_r \text{Vol}(G_0)} \int_{g \in \mathcal{F}} \#(gG_0 \cdot \mathcal{R}_X^{(r)} \cap W(\mathbb{Z})_{\text{red}}) \, dg. \tag{35}$$

Since  $\mathcal{F}$  is a box-shaped fundamental domain, it follows that we can write, up to a measure-0 set,  $\mathcal{F}$  as the disjoint union  $\mathcal{F}' \cup \mathcal{N}T_1(\{\pm \text{id}\} \setminus K)$ , where  $\mathcal{N}$  is the compact subset of  $N(\mathbb{R})$  determined in Section 3.2.3,

$$T_1 := \{s = (s_1, \dots, s_{\lfloor n/2 \rfloor}) \in T : s_i > c_1 \text{ for all } i\}$$

is a subset of  $T$ , and  $\mathcal{F}'$  is a subset of

$$\mathcal{N}\{s = (s_1, \dots, s_{\lfloor n/2 \rfloor}) \in T : s_i \leq c_1 \text{ for some } i\}(\{\pm \text{id}\} \setminus K).$$

By combining counting results from [6; 16; 43], we prove the following result, in partial analogy with Proposition 12:

**Proposition 29.** *We have*

$$\#'\left(\frac{(W(\mathbb{Z})_{\text{red}}^{(r)})_X}{G(\mathbb{Z})}\right) = \frac{1}{\tilde{\theta}_r \text{Vol}(G_0)} \int_{us \in \bar{\mathcal{N}}T_1} \#(usXB \cap W_0(\mathbb{Z}))\delta(s) du d^\times s + O_\epsilon(X^{\frac{n^2+n-0.4}{2}+\epsilon}), \quad (36)$$

where  $B$  is the multiset  $B := (B_\infty)_1 := G_0 \cdot \mathcal{R}_1^{(r)} \cap W_0(\mathbb{R})$ , and  $\bar{\mathcal{N}}$  is defined in Section 3.2.3.

*Proof.* Recall that  $B = [b_{ij}] \in W_0(\mathbb{R})$  if and only if  $b_{ij} = 0$  for all  $i + j < n$ . Borrowing terminology from [17], we break up the integral on the right-hand side of (35) into three regions, the main body, the shallow cusp, and the deep cusp, and we estimate the contributions from each region separately.

The main body is the region of the integral over  $\mathcal{F}$  consisting of  $g \in \mathcal{F}$  such that  $gG_0 \cdot \mathcal{R}_X^{(r)}$  contains integer points  $B \in W(\mathbb{Z})$  with  $b_{11} \neq 0$ . The number of *reducible* elements in the main ball has been shown to be negligible in [6, Proposition 10.7] (for odd  $n$ ) and [43, Proposition 23] (for even  $n$ ). These estimates have been improved to a power-saving bound of  $O_\epsilon(X^{(n^2+n-0.4)/2+\epsilon})$  in Propositions 2.6 and 3.5 of [16], respectively.

Next, the shallow cusp is the region of the integral over  $\mathcal{F}$  consisting of  $g \in \mathcal{F}$  such that every  $B \in gG_0 \cdot \mathcal{R}_X^{(r)}$  satisfies  $|b_{11}| < 1$ , and such that  $gG_0 \cdot \mathcal{R}_X^{(r)}$  contains integer points  $B \in W(\mathbb{Z})$  with  $b_{\lfloor(n-1)/2\rfloor, \lfloor(n-1)/2\rfloor} \neq 0$ . The proofs of [6, Proposition 10.5] (for odd  $n$ ) and [43, Proposition 21] (for even  $n$ ) prove that the number of elements in the shallow cusp is bounded by  $O(X^{(n^2+n-2)/2})$ . Together, these bounds imply

$$\#'\left(\frac{(W(\mathbb{Z})_{\text{red}}^{(r)})_X}{G(\mathbb{Z})}\right) = \frac{1}{\theta_r \text{Vol}(G_0)} \int_{g \in \mathcal{F}} \#(gG_0 \cdot \mathcal{R}_X^{(r)} \cap W_0(\mathbb{Z})) dg + O_\epsilon(X^{\frac{n^2+n-0.4}{2}+\epsilon}).$$

We now claim that the above estimate also holds when the region of integration  $\mathcal{F}$  is replaced by the region  $\mathcal{N}T_1$ . To prove this claim, we show that the above integral is negligible when  $\mathcal{F}$  is replaced by  $\mathcal{F}'$ . However, this also follows from the previous bounds since  $\mathcal{F}'$  lies within the main body and the shallow cusp. Indeed, note that for an element  $ntk \in \mathcal{F}$  to lie within the deep cusp (i.e., in the cusp but not the shallow cusp), we must have  $\log t_{\lfloor(n-1)/2\rfloor} \gg \log X$ . Moreover, since  $ntk \in \mathcal{F}$ , the condition  $\log t_{\lfloor(n-1)/2\rfloor} \gg \log X$  automatically implies that  $\log s_i \gg \log X$  for every  $i$ , and thus  $ntk \notin \mathcal{F}'$ . Finally, we replace  $\mathcal{N}$  with  $\bar{\mathcal{N}}$  (see Section 3.2.3 for the definition), and to compensate, we divide by the order of the subgroup  $\Gamma \subset K$ , which is  $2^{\lfloor n/2 \rfloor}$ . The result now follows from the definitions of  $\theta_r$  and  $\tilde{\theta}_r$ .  $\square$

**5.2. Slicing.** Just like in Section 2.3.2, Proposition 13 is not by itself sufficient to estimate the number of integral points in the region  $usXB$ , which is typically quite skewed. Instead, we fiber the region  $usXB$  by the coefficients  $b_{1(n-1)}, \dots, b_{\lfloor n/2 \rfloor, \lfloor n/2 \rfloor}$ . For any  $b = (b_1, \dots, b_{\lfloor n/2 \rfloor}) \in (\mathbb{R} \setminus \{0\})^{\lfloor n/2 \rfloor}$ , and any  $S \subset W(\mathbb{R})$ , let  $S|_b$  denote the *slice of  $S$  at  $b$* , i.e.,

$$S|_b := \{B \in S \cap W_0(\mathbb{R}) : b_{k(n-k)}(B) = b_k \text{ for all } k \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}\}.$$

We can express the integrand of the right-hand side of (36) as

$$\#(usXB \cap W(\mathbb{Z})) = \sum_{\substack{b \in \mathbb{Z}^{\lfloor n/2 \rfloor} \\ b_i \neq 0 \forall i}} \#((usXB)|_b \cap W(\mathbb{Z})). \tag{37}$$

By examining the action of  $s$  on an element  $B = [b_{ij}] \in W(\mathbb{R})$ , we define the *weight*  $w_{ij} = w(b_{ij})$  to be the quantity by which  $s$  scales the matrix entry  $b_{ij}$  for each pair  $(i, j) \in \{1, \dots, n\}^2$ . For any subset  $S$  of coefficients  $b_{ij}$  of  $W(\mathbb{R})$ , we let  $w(S)$  denote the product of the weights of all the elements in  $S$ . From Proposition 13, it follows that

$$\#((usXB)|_b \cap W(\mathbb{Z})) = \text{Vol}((usXB)|_b)(1 + O(X^{-1})), \tag{38}$$

where the error term is seen to be  $X^{-1}$  times the main term as follows. The weight of every coefficient in  $W_0(\mathbb{R})$  not being sliced over is  $\gg 1$ : indeed, note that  $w(b_{k(n+1-k)}) = 1$  for each  $k$ , and that the remaining weights are all at least as big. As a consequence, the range of each coefficient varying in  $(usXB)_b$  is  $\gg X$ , and the volume of  $(usXB)|_b$  is asymptotic to the product of the ranges of these varying coefficients. Proposition 13 then yields a saving of size  $X$ , as necessary.

Now, since unipotent transformations preserve both the value of  $b$  and the volume, we have

$$\text{Vol}((usXB)|_b) = \text{Vol}((sXB)|_b).$$

Recall that we have normalized measures to ensure  $\text{Vol}(\bar{N}) = 1$ . Therefore, (36), (37), and (38) yield

$$\#'\left(\frac{(W(\mathbb{Z})_{\text{red}}^{(r)})_X}{G(\mathbb{Z})}\right) = \frac{1}{\bar{\theta}_r \text{Vol}(G_0)} \sum_{\substack{b \in \mathbb{Z}^{\lfloor n/2 \rfloor} \\ b_i \neq 0 \forall i}} \int_{s \in T_1} \text{Vol}((sXB)|_b) \delta(s) d^\times s + O_\epsilon(X^{\frac{n^2+n-0.4}{2} + \epsilon}). \tag{39}$$

Define an action of  $T$  on  $(\mathbb{R} \setminus \{0\})^{\lfloor n/2 \rfloor}$  by setting  $s((b_i)_i) := (w(b_{i(n-i)})b_i)_i$ . For fixed  $X$  and  $b = (b_i)_i \in (\mathbb{R} \setminus \{0\})^{\lfloor n/2 \rfloor}$ , we write  $X^{-1}s^{-1}(b) =: \beta =: (\beta_i)_i$ . Let  $S$  denote the set of coefficients of  $W_0$ , and write  $S = S_0 \sqcup S^b$ , where  $S_0$  is the set of all  $b_{i(n-i)}$ , and  $S^b := S \setminus S_0$ . Since  $(sXB)|_b = sX(B|_\beta)$ , it follows that

$$\text{Vol}((sXB)|_b) = \text{Vol}(sX(B|_\beta)) = X^{\dim(S^b)} w(S^b) \text{Vol}(B|_\beta). \tag{40}$$

Consider the change of variables  $s_i \mapsto \beta_i$ , and note that  $d^\times s = d^\times \beta := \prod_i (d\beta_i / \beta_i)$ . Write  $n = 2g + 1$  when  $n$  is odd, and  $n = 2g + 2$  when  $n$  is even. We have  $s_k = X\beta_k b_k^{-1}$  for all  $1 \leq k \leq g$ . When  $n$  is even, we further have  $s_{g+1} = X^2 \beta_g \beta_{g+1} b_g^{-1} b_{g+1}^{-1}$ . A direct computation now yields that

$$X^{\dim S^b} w(S^b) \delta(s) = \begin{cases} X^{\dim S^b} \prod_{k=1}^g s_k^{2k} & \text{for } n \text{ odd,} \\ X^{\dim S^b} (s_g^{g-1} s_{g+1}^{g+1}) \prod_{k=1}^{g-1} s_k^{2k} & \text{for } n \text{ even.} \end{cases}$$

Therefore, defining  $\mathcal{Z}(a_1, \dots, a_g) := \prod_{k=1}^g a_k^{2k}$  when  $n = 2g + 1$  is odd and  $\mathcal{Z}(a_1, \dots, a_{g+1}) := a_{g+1}^{g+1} \prod_{k=1}^g a_k^{2k}$  when  $n = 2g + 2$  is even, we have

$$X^{\dim S^b} w(S^b) \delta(s) = X^{\frac{n^2+n}{2}} \frac{\mathcal{Z}(\beta)}{\mathcal{Z}(b)}. \tag{41}$$

We now examine each individual summand on the right-hand side of (39). For  $b = (b_i)_i \in (\mathbb{R} \setminus \{0\})^{\lfloor n/2 \rfloor}$ , let  $|b|$  denote  $(|b_i|)_i$ . Recall that  $G_0$  is  $K$ -invariant, and recall from Section 3.2.3 that  $K$  contains every diagonal matrix in  $G(\mathbb{Z})$  with each entry  $\pm 1$ . It follows that we have  $\text{Vol}(\mathcal{B}|_b) = \text{Vol}(\mathcal{B}|_{|b|})$ . Therefore, from (40) and (41), we deduce that

$$\int_{s \in T_1} \text{Vol}((sX\mathcal{B})|_b)\delta(s) d^\times s = \frac{X^{\frac{n^2+n}{2}}}{\mathcal{Z}(|b|)} \int_{\beta \in \mathbb{R}_{\geq 0}^{\lfloor n/2 \rfloor} \setminus T'_1} \mathcal{Z}(\beta) \text{Vol}(\mathcal{B}|_\beta) d^\times \beta$$

for each  $b = (b_i)_i \in (\mathbb{Z} \setminus \{0\})^{\lfloor n/2 \rfloor}$ , where  $T'_1$  is a region contained in the set of those  $\beta$  for which  $\beta_i \ll X^{-1}$  for at least one  $i$ . Since  $\mathcal{B}$  is a bounded set and the integral of  $\mathcal{Z}(\beta)d^\times \beta$  over  $T'_1$  is clearly bounded by  $O(X^{-1})$ , we find that

$$\begin{aligned} \int_{s \in T_1} \text{Vol}((sX\mathcal{B})|_b)\delta(s) d^\times s &= \frac{X^{\frac{n^2+n}{2}}}{\mathcal{Z}(|b|)} \int_{\beta \in \mathbb{R}_{> 0}^{\lfloor n/2 \rfloor}} \mathcal{Z}(\beta) \text{Vol}(\mathcal{B}|_\beta) d^\times \beta + O(X^{\frac{n^2+n-2}{2}}) \\ &= \frac{X^{\frac{n^2+n}{2}}}{\mathcal{Z}(|b|)} \int_{B \in \mathcal{B}^+} \lambda(B) dB + O(X^{\frac{n^2+n-2}{2}}), \end{aligned} \tag{42}$$

where  $\mathcal{B}^+ := \{B \in \mathcal{B} : b_{i(n-i)}(B) > 0 \text{ for all } i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}\}$ . Substituting (42) into (39) and summing over  $b$ , we immediately obtain

$$\#'\left(\frac{(W(\mathbb{Z})_{\text{red}}^{(r)})_X}{G(\mathbb{Z})}\right) = C(\mathcal{B}) \cdot C_n^{\text{fin}} \cdot X^{\frac{n^2+n}{2}} + O_\epsilon(X^{\frac{n^2+n-0.4}{2} + \epsilon}). \tag{43}$$

To recover Theorem 1 from (43), it remains to prove two facts: first, that the constant  $C(\mathcal{B})$  is equal to  $C_{n,r}^{\text{inf}}$ , and second, that the  $\#'$ -count and the  $\#$ -count differ by only a negligible amount. We verify these facts in the next two subsections.

**5.3. Computing the constant.** In this subsection, we compute the value of  $C(\mathcal{B})$ . Recall that we defined  $\mathcal{B}$  to be the multiset  $\mathcal{B} := G_0 \cdot \mathcal{R}_1^{(r)} \cap W_0(\mathbb{R})$ . Since  $G_0$  is right- $K$ -invariant, we may write  $G_0 = SK$  for some  $S \subset N(\mathbb{R})T$ . Hence, we have that  $\mathcal{B} = SK \cdot \mathcal{R}_1^{(r)} \cap W_0(\mathbb{R}) = S \cdot (K\mathcal{R}_1^{(r)})_0$ . Then, by analogy with Lemma 14, we have the following lemma concerning the multiplicity of the fiber of  $(K\mathcal{R}^{(r)})_0$  over  $U(\mathbb{R})^{(r)}$ :

**Lemma 30.** *The map  $\text{inv} : (K\mathcal{R}^{(r)})_0 \rightarrow U(\mathbb{R})^{(r)}$  is  $\tilde{\theta}_r$ -to-1.*

*Proof.* It suffices to prove the map  $\text{inv} : \{B \in (K\mathcal{R}^{(r)})_0 : b_{i(n-i)}(B) > 0 \text{ for all } i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}\} \rightarrow U(\mathbb{R})^{(r)}$  is  $\theta_r$ -to-1. This is a consequence of the following two facts: first, the stabilizer in  $G(\mathbb{R})$  of any element of  $W(\mathbb{R})^{(r)}$  has size  $\theta_r$ , and second, the group  $N(\mathbb{R})T$  acts simply transitively on  $\text{inv}^{-1}(f) \cap W_0(\mathbb{R})$  for any  $f \in U(\mathbb{R})^{(r)}$  by Lemma 26. Indeed, given  $B \in \mathcal{R}^{(r)}$  having invariant polynomial  $f$ , and  $pk \in \text{Stab}_{G(\mathbb{R})}(B)$  with  $p \in N(\mathbb{R})T$  and  $\theta \in K$ , the element  $\theta B = p^{-1}B$  belongs to  $(K\mathcal{R}^{(r)})_0$  and has invariant polynomial  $f$ . This association yields the result.  $\square$

Now, by analogy with Proposition 15, we are in position to compute the constant  $C(\mathcal{B})$ :

**Proposition 31.** *We have that  $C(\mathcal{B}) = C_{n,r}^{\text{inf}}$ .*

*Proof.* We have

$$C(\mathcal{B}) = \frac{1}{\theta_r \text{Vol}(G_0)} \int_{\mathcal{B} \in \mathcal{S} \cdot (K\mathcal{R}_1^{(r)})_0} |\lambda(\mathcal{B})| d\mathcal{B} = \frac{|\mathcal{J}| \text{Vol}_{\text{right}}(\mathcal{S}) \text{Vol}(\{f \in U(\mathbb{R})^{(r)} : H(f) < 1\})}{\text{Vol}(\mathcal{SK})}, \tag{44}$$

where the second equality follows from applying the Jacobian change-of-variables established in [Proposition 27](#) along with [Lemma 30](#), and where  $\text{Vol}_{\text{right}}(\mathcal{S})$  denotes the volume of  $\mathcal{S}$  with respect to the right Haar measure on  $\mathcal{P}(\mathbb{R})$ . But since  $\text{Vol}(K)$  is normalized to be equal to 1, we have  $\text{Vol}_{\text{right}}(\mathcal{S}) = \text{Vol}(K\mathcal{S})$ . In complete analogy with [Lemma 16](#), we have  $\text{Vol}(K\mathcal{S}) = \text{Vol}(\mathcal{SK})$ . Combining this with (44) and the computation of  $|\mathcal{J}|$  performed in [Proposition 28](#) completes the proof of [Proposition 31](#).  $\square$

For the last missing ingredient in the proof of [Theorem 1](#), we prove that there is no asymptotic difference between the  $\#'$ -count and the  $\#$ -count. To this end, let  $W(\mathbb{Z})_{\text{bs}} := \{B \in W(\mathbb{Z})_{\text{red}}^{(r)} : \text{Stab}_{G(\mathbb{Z})}(B) \neq 1\}$ . Then we have the following result:

**Proposition 32.** *We have*

$$\#\left(\frac{(W(\mathbb{Z})_{\text{bs}})X}{G(\mathbb{Z})}\right) = O_\epsilon(X^{\frac{n^2+n-0.4}{2}+\epsilon}).$$

*Proof.* Following (36) and (39), we have

$$\begin{aligned} \#\left(\frac{(W(\mathbb{Z})_{\text{bs}})X}{G(\mathbb{Z})}\right) &\ll \int_{us \in \mathcal{N}T_1} \#(usXB \cap W(\mathbb{Z})_{\text{bs}})\delta(s) du d^\times s \\ &\ll \sum_{\substack{b \in \mathbb{Z}^{\lfloor n/2 \rfloor} \\ b_i \neq 0 \forall i}} \int_{s \in T_1} \#(sXB|_b \cap (W(\mathbb{Z})_{\text{bs}}))\delta(s) du d^\times s, \end{aligned}$$

up to an error of  $X^{(n^2+n-0.4)/2+\epsilon}$ .

Next, note that if  $B \in W(\mathbb{Z})_{\text{bs}}$ , then the reduction of  $B \pmod p$  has a nontrivial stabilizer for every prime  $p$ . Fix  $b = (b_i)_i \in (\mathbb{Z} \setminus \{0\})^{\lfloor n/2 \rfloor}$ , and let  $p$  be a prime such that  $p \nmid \prod b_i$ . We claim that a positive proportion of elements in  $W_0(\mathbb{F}_p)|_b := \{B \in W_0(\mathbb{F}_p) : b_{k(n-k)}(B) = b_k \text{ for all } k \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}\}$  have trivial stabilizer in  $G(\mathbb{F}_p)$ . Indeed, this is true for every  $B \in W(\mathbb{F}_p)$  whose invariant polynomial is irreducible over  $\mathbb{F}_p$  when  $n$  is odd (see [6, Section 10.7]), and for every  $B \in W(\mathbb{F}_p)$  whose invariant polynomial is a linear polynomial times an irreducible polynomial over  $\mathbb{F}_p$  when  $n$  is even (see [43, proof of Proposition 23]). A positive proportion of invariant polynomials satisfy these splitting criteria, and the fiber in  $W_0(\mathbb{F}_p)|_b$  over each polynomial has the same size (in fact, this size is  $\#N(\mathbb{F}_p)$ ). A power-saving estimate for each summand in the above equation now follows by using the Selberg sieve analogously to the argument in [41]. (Indeed, a power-saving bound from the Selberg sieve only requires the ability to count these integer points with a power-saving error term, and requires a positive proportion of mod  $p$  residue classes to be avoided. We omit the details of the computation of the precise power-saving exponent since the argument closely follows that in [41].) The proposition now follows since the sum over  $b$  converges absolutely.  $\square$

[Theorem 1](#) now follows from (43) and [Propositions 31](#) and [32](#).

**5.4. Congruence conditions.** We now prove [Theorem 3](#). Let  $S \subset W(\mathbb{Z})^{(r)}$  be a big family, and suppose for now that  $S$  is defined by congruence conditions at finitely many places (i.e., suppose that  $S_p = W(\mathbb{Z}_p)$  for all primes  $p \gg 1$ ). For each  $b \in (\mathbb{Z}_p \setminus \{0\})^{\lfloor n/2 \rfloor}$ , let

$$(S_p)_0|_b := \{B \in (S_p)_0 : b_{i(n-i)}(B) = b_i \text{ for all } i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}\},$$

and for each  $b \in (\mathbb{Z} \setminus \{0\})^{\lfloor n/2 \rfloor}$ , let  $\nu(S_0|_b) := \prod_p \text{Vol}((S_p)_0|_b)$  denote the density of the slice  $S_0|_b$  in  $W_0(\mathbb{Z})|_b$ ; here, each  $p$ -adic volume  $\text{Vol}((S_p)_0|_b)$  is computed with respect to the Euclidean measure on  $W_0(\mathbb{Z}_p)|_b$ , normalized so that  $W_0(\mathbb{Z}_p)|_b$  has volume 1. Then an argument identical to the one used to obtain [\(39\)](#) yields the asymptotic formula

$$\#\left(\frac{(S_{\text{red}})_X}{G(\mathbb{Z})}\right) = \frac{1}{\theta_r \text{Vol}(G_0)} \sum_{\substack{b \in \mathbb{Z}^{\lfloor n/2 \rfloor} \\ b_i \neq 0 \forall i}} \nu(S_0|_b) \int_{s \in T_1} \text{Vol}((sX B)|_b) \delta(s) d^\times s + O_\epsilon(X^{\frac{n^2+n-0.4}{2}+\epsilon}). \quad (45)$$

The  $G(\mathbb{Z})$ -invariance of  $S$  implies that  $\nu(S_0|_b) = \nu(S_0|_{|b|})$  for all  $b$ . Hence, [\(42\)](#) and [\(45\)](#) yield the estimate

$$\#\left(\frac{(S_{\text{red}})_X}{G(\mathbb{Z})}\right) = C(\mathcal{B}) \cdot \left( \sum_{\substack{b \in \mathbb{Z}^{\lfloor n/2 \rfloor} \\ b_i > 0 \forall i}} \frac{\nu(S_0|_b)}{\mathcal{Z}(b)} \right) \cdot X^{\frac{n^2+n}{2}} + O_\epsilon(X^{\frac{n^2+n-0.4}{2}+\epsilon}). \quad (46)$$

To evaluate the sum over  $b$  on the right-hand side of [\(46\)](#), we use the following property, which is a consequence of the fact that  $S$  is a big family: if  $p$  is a prime and  $b, b' \in (\mathbb{Z}_p \setminus \{0\})^{\lfloor n/2 \rfloor}$  are elements such that  $|b_i|_p = |b'_i|_p$  for each  $i$ , then  $\text{Vol}((S_p)_0|_b) = \text{Vol}((S_p)_0|_{b'})$ . By repeatedly using this property, we obtain the chain of equalities

$$\begin{aligned} \sum_{\substack{b \in \mathbb{Z}^{\lfloor n/2 \rfloor} \\ b_i > 0 \forall i}} \frac{\nu(S_0|_b)}{\mathcal{Z}(b)} &= \prod_p \sum_{\substack{(i) \in \mathbb{Z}^{\lfloor n/2 \rfloor} \\ i_j \geq 0 \forall j}} \frac{\text{Vol}((S_p)_0|_{(p^{i_1}, \dots, p^{i_{\lfloor n/2 \rfloor}})})}{\mathcal{Z}(p^{i_1}, \dots, p^{i_{\lfloor n/2 \rfloor}})} \\ &= \prod_p \left(1 - \frac{1}{p}\right)^{-\lfloor \frac{n}{2} \rfloor} \int_{\substack{b \in \mathbb{Z}_p^{\lfloor n/2 \rfloor} \\ b_i \neq 0 \forall i}} \frac{\text{Vol}((S_p)_0|_{(|b_1|_p^{-1}, \dots, |b_{\lfloor \frac{n}{2} \rfloor}|_p^{-1})})}{\mathcal{Z}(|b_1|_p^{-1}, \dots, |b_{\lfloor \frac{n}{2} \rfloor}|_p^{-1}) \prod_i |b_i|_p} db \\ &= \prod_p \left(1 - \frac{1}{p}\right)^{-\lfloor \frac{n}{2} \rfloor} \int_{\substack{b \in \mathbb{Z}_p^{\lfloor n/2 \rfloor} \\ b_i \neq 0 \forall i}} \left| \frac{\mathcal{Z}(b)}{\prod_i b_i} \right|_p \text{Vol}((S_p)_0|_b) db \\ &= \prod_p \left(1 - \frac{1}{p}\right)^{-\lfloor \frac{n}{2} \rfloor} \int_{B \in (S_p)_0} |\lambda(B)|_p dB, \end{aligned}$$

where the second line above follows by partitioning the region of integration  $(\mathbb{Z}_p \setminus \{0\})^{\lfloor n/2 \rfloor}$  into level sets for the integrand and summing over all such level sets, and where the last line above follows just as in [\(42\)](#).

It remains to handle the case where  $S$  is a big family defined by congruence conditions at infinitely many places. By abuse of notation, let  $\mathcal{Z}$  be the polynomial on  $W_0$  defined by  $\mathcal{Z}(B) := \mathcal{Z}(b_{1(n-1)}(B), \dots, b_{\lfloor n/2 \rfloor \lceil n/2 \rceil}(B))$ . Then the case of infinitely many places follows from the case

of finitely many places by using the following bound on the number of  $G(\mathbb{Z})$ -equivalence classes of elements with large  $\mathcal{Z}$ -value, in conjunction with an inclusion-exclusion sieve:<sup>8</sup>

**Theorem 33.** *Fix a real number  $M > 0$ . Then the number of  $G(\mathbb{Z})$ -equivalence classes of (or equivalently,  $\mathcal{P}(\mathbb{Z})$ -orbits of) elements of the set  $\{B \in W_0(\mathbb{Z}) : H(B) < X, |\mathcal{Z}(B)| \geq M^2\}$  is bounded by  $O(X^{(n^2+n)/2}/M) + O_\epsilon(X^{(n^2+n-0.4)/2+\epsilon})$ , where the implied constant is independent of  $M$ .*

*Proof.* The required bound follows immediately from the proof of [Theorem 1](#) by simply summing [\(42\)](#) over only those  $b$  such that  $|\mathcal{Z}(b)| \geq M^2$ .  $\square$

**Remark.** [Theorem 33](#) constitutes a slight strengthening of a result previously proven in [[16](#), Sections 2.3–2.4 and 3.3–3.4], where Bhargava, Shankar, and Wang used the averaging method to obtain an upper bound of  $O_\epsilon(X^{(n^2+n)/2+\epsilon}/M) + O_\epsilon(X^{(n^2+n-0.4)/2+\epsilon})$ .

This concludes the proof of [Theorem 3](#). We finish by noting that [Theorem 4](#) follows from [Theorem 3](#) by applying the Jacobian change-of-variables result in [Proposition 27](#) to each  $p$ -adic integral, with  $\phi$  taken to be the characteristic function of  $(S_p)_0$ . Indeed, [Propositions 27](#) and [28](#) together imply the equality of each factor at the odd primes; at  $p = 2$ , there is an extra factor of  $2^{n/2}$  when  $n$  is even, which perfectly accounts for the corresponding factor at infinity.

## 6. A local-to-global principle for the action of $\mathcal{P}(\mathbb{Z})$ on $W_0(\mathbb{Z})$

In this section, we develop an alternative method for counting reducible  $G(\mathbb{Z})$ -orbits on  $W(\mathbb{Z})$ . This method, which we called “Method II” in [Section 1.4](#), consists of the following steps:

- First, in [Section 6.1](#), we consider a general representation with trivial generic stabilizer, and we prove that the integral orbits of such a representation satisfy a strong local-to-global principle, which is stated precisely in [Theorem 34](#).
- As shown in [Proposition 25](#), the action of the group  $\mathcal{P}$  on the reducible hyperplane  $W_0$  is a representation with trivial generic stabilizer. In [Section 6.2](#), we deduce [Theorem 5](#) by applying [Theorem 34](#) to the action of  $\mathcal{P}$  on  $W_0$ .
- Finally, in [Section 6.3](#), we explain how to use [Theorem 5](#) to deduce asymptotics for the number of  $\mathcal{P}(\mathbb{Z})$ -orbits on  $W_0(\mathbb{Z})$ —and hence also for the number of reducible  $G(\mathbb{Z})$ -orbits on  $W(\mathbb{Z})$ . The main analytic ingredient is an upper bound obtained by Bhargava, Shankar, and Wang on the number of  $\mathcal{P}(\mathbb{Z})$ -orbits of elements  $B \in W_0(\mathbb{Z})$  with the property that  $\lambda(B)$  is large.

**6.1. Group actions with trivial stabilizers.** In this section, we work with the following data: an algebraic group  $H$ , finite-dimensional  $H$ -representations  $V$  and  $I$ , and an  $H$ -equivariant morphism  $\phi : V \rightarrow I$ , all defined over  $\mathbb{Z}$ . Note that we do not require  $\phi$  to be a linear map. Any polynomial map will suffice. Suppose that the group  $H$  has class number 1 over  $\mathbb{Q}$ , meaning that  $H(\mathbb{A}_{\mathbb{Q}})$  is the product of its subgroups

<sup>8</sup>Just as in [Section 2.3.4](#), we do not flesh out the sieving argument here to avoid being repetitive, because in [Section 6.3](#) (to follow), we use the same sort of argument to prove [Theorem 4](#).

$H(\mathbb{A}_{\mathbb{Z}})$  and  $H(\mathbb{Q})$  (i.e., for every  $h \in H(\mathbb{A}_{\mathbb{Q}})$ , there exist  $h' \in H(\mathbb{A}_{\mathbb{Z}})$  and  $h'' \in H(\mathbb{Q})$  such that  $h = h'h''$ ). Here  $\mathbb{A}_{\mathbb{Q}}$  denotes the ring of adèles, and  $\mathbb{A}_{\mathbb{Z}}$  is the ring of everywhere integral adèles. Suppose further that, for some nonempty open subscheme  $\mathcal{I} \subset I$ , defined over  $\mathbb{Z}$ , the following two assumptions hold:

- (1) For every  $i \in \mathcal{I}(\mathbb{C})$ , the set  $\{v \in V(\mathbb{C}) : \phi(v) = i\}$  forms a single nonempty  $H(\mathbb{C})$ -orbit.
- (2) For every  $i \in \mathcal{I}(\mathbb{C})$  and every (or equivalently, any)  $v \in V(\mathbb{C})$  with  $\phi(v) = i$ , we have  $\text{Stab}_{H(\mathbb{C})}(v) = 1$ .

In this setting, we prove the following strong local-to-global principle for the action of  $H$  on  $V$ :

**Theorem 34.** *Suppose that  $i \in \mathcal{I}(\mathbb{Z})$  is an element contained in the image  $\phi(V(\mathbb{Z}))$ . For each prime  $p$ , let  $v_p \in V(\mathbb{Z}_p)$  be such that  $\phi(v_p) = i$ . Then there exists  $v \in V(\mathbb{Z})$ , unique up to the action of  $H(\mathbb{Z})$ , such that  $v$  is  $H(\mathbb{Z}_p)$ -equivalent to  $v_p$  for each prime  $p$ .*

Before we give the proof of [Theorem 34](#), we first use assumptions (1) and (2) enumerated above to deduce that an analogue of assumption (1) holds for any subfield  $K \subset \mathbb{C}$ :

**Lemma 35.** *Let  $K \subset \mathbb{C}$  be a subfield. For every  $i \in \mathcal{I}(K)$ , the set  $\{v \in V(K) : \phi(v) = i\}$  consists of single  $H(K)$ -orbit.*

*Proof.* Let  $i \in \mathcal{I}(K)$ , and let  $v, v' \in V(K)$  with  $\phi(v) = \phi(v') = i$ . By assumption (1), there exists  $h \in H(\mathbb{C})$  such that  $v' = h \cdot v$ . Then for any  $\sigma \in \text{Gal}(\mathbb{C}/K)$ , we have  $v' = \sigma h \cdot v$ , so  $h^{-1}\sigma h \in \text{Stab}_{H(\mathbb{C})}(v) = 1$  by assumption (2). It follows that  $h$  is fixed by  $\text{Gal}(\mathbb{C}/K)$ , and so  $h \in H(K)$ , as necessary.  $\square$

We now use [Lemma 35](#), assumption (2), and the fact that  $H$  has class number 1 over  $\mathbb{Q}$  to complete the proof of the theorem:

*Proof of Theorem 34.* Let us temporarily drop assumption (2). For a principal ideal domain  $R$  with fraction field  $K$  and an element  $v \in V(R)$ , define  $H(K)_v := \{h \in H(K) : h \cdot v \in H(R)\}$ . Then it is clear that the set of  $H(R)$ -orbits contained in the  $H(K)$ -orbit of an element  $v \in V(R)$  is in natural bijection with the double coset space  $H(R) \backslash H(K)_v / \text{Stab}_{H(K)}(v)$ . With assumption (2) reinstated, this double coset space is simply given by  $H(R) \backslash H(K)_v$  as long as the  $H$ -invariant of  $v$  lies in the subset  $\mathcal{I}(R) \subset I(R)$ .

Now, using the fact that  $H$  has class number 1 over  $\mathbb{Q}$ , it is proven in [\[9, proof of Proposition 3.6\]](#)<sup>9</sup> that the diagonal embedding  $H(\mathbb{Q}) \hookrightarrow \prod_p H(\mathbb{Q}_p)$  induces a bijection

$$H(\mathbb{Z}) \backslash H(\mathbb{Q})_{v_0} \longrightarrow \prod_p H(\mathbb{Z}_p) \backslash H(\mathbb{Q}_p)_{v_0}. \tag{47}$$

Let  $v_0 \in V(\mathbb{Z})$  be an element such that  $\phi(v_0) = i$ . By the result of the previous paragraph, the bijection in [\(47\)](#) may be regarded as identifying the set of  $H(\mathbb{Z})$ -orbits contained in the  $H(\mathbb{Q})$ -orbit of  $v_0$  with the product over all primes  $p$  of the set of  $H(\mathbb{Z}_p)$ -orbits contained in the  $H(\mathbb{Q}_p)$ -orbit of  $v_0$ .

By [Lemma 35](#), which implies that the  $H(\mathbb{Q}_p)$ -orbit of  $v_0$  is equal to that of  $v_p$  for each prime  $p$ , we may view the tuple  $(v_p)_p$  as an element of the right-hand side of [\(47\)](#). Then, under the bijection, the tuple  $(v_p)_p$  corresponds to the  $H(\mathbb{Z})$ -orbit of the desired element  $v \in V(\mathbb{Z})$ .  $\square$

<sup>9</sup>To be clear, [\[9, Proposition 3.6\]](#) concerns the case  $H = \text{PGL}_2$ , but it is evident that the same argument goes through for any group  $H$  of class number 1 over  $\mathbb{Q}$ .

**6.2. Proof of Theorem 5.** We now deduce Theorem 5 from Theorem 34. To do so, we take  $H = \mathcal{P}$ ,  $V = W_0$ ,  $I = U$ ,  $\phi = \text{inv}$ , and  $\mathcal{I} \subset U$  to be the open subscheme consisting of nondegenerate polynomials. Note that the group  $\mathcal{P}$  clearly has class number 1 over  $\mathbb{Q}$ , and note that assumptions (1) and (2) follow immediately from Proposition 25. Applying Theorem 34 then yields the following: for any  $f \in \mathcal{I}(\mathbb{Z})$ , if there exists  $B_0 \in W_0(\mathbb{Z})$  such that  $\text{inv}(B_0) = f$  and if there exists  $B_p \in W_0(\mathbb{Z}_p)$  such that  $\text{inv}(B_p) = f$  for each prime  $p$ , then there exists  $B \in W_0(\mathbb{Z})$ , unique up to the action of  $\mathcal{P}(\mathbb{Z})$ , such that  $B$  is  $\mathcal{P}(\mathbb{Z}_p)$ -equivalent to  $B_p$  for each prime  $p$ . To prove Theorem 5, it now remains to verify the existence of the elements  $B_0$  and  $B_p$  for each prime  $p$ .

When  $n$  is even, the existence of the elements  $B_0$  and  $B_p$  is implied by the existence of the integral section  $\sigma_0$  given in Section 3.3—indeed, when  $n$  is even, we have restricted our consideration to those monic polynomials whose  $x^i$ -coefficients are divisible by 2 for each odd  $i$ , so the section  $\sigma_0$  is defined over  $\mathbb{Z}$  in this case. On the other hand, when  $n$  is odd, the section  $\sigma_0$  is not defined over  $\mathbb{Z}$ . Instead, it is shown in [31, Section 4.1] that for any principal ideal domain  $R$  and for each  $f \in U(R)$  there exists a pair  $(A, B)$  of  $n \times n$  symmetric matrices with entries in  $R$  such that:  $A$  is split over  $K = \text{Frac}(R)$ ;  $A$  and  $B$  share a maximal isotropic space over  $K$ ; and  $\det(xA + yB) = (-1)^{\lfloor n/2 \rfloor} f(x, y)$ . By the classification of unimodular symmetric bilinear forms (see [39, Chapter VI]),  $A$  is  $\text{GL}_n(R)$ -equivalent to  $A$ . By translating  $B$  with the same element of  $\text{GL}_n(R)$ , we obtain  $B' \in W_0(R)$  satisfying  $\text{inv}(B') = f$ .

**6.3. Proof of Theorem 4.** We now use Theorem 5 to give a second proof of Theorem 4. We call a subset  $\mathfrak{S} \subset W_0(\mathbb{Z})$  a *big family* if  $\mathfrak{S} = W(\mathbb{Z})_0^{(r)} \cap \bigcap_p \mathfrak{S}_p$ , where the sets  $\mathfrak{S}_p \subset W_0(\mathbb{Z}_p)$  satisfy the following properties:

- (1)  $\mathfrak{S}_p$  is  $\mathcal{P}(\mathbb{Z}_p)$ -invariant and is the preimage under reduction modulo  $p^j$  of a nonempty subset of  $W_0(\mathbb{Z}/p^j\mathbb{Z})$  for some  $j > 0$  for each  $p$ .
- (2)  $\mathfrak{S}_p$  contains all elements  $B \in W_0(\mathbb{Z}_p)$  such that, for all  $p \gg 1$ , we have that  $b_{i(n-i)}(B)$  is a  $p$ -adic unit for some  $i$ .

We then have the following variant of Theorem 4, from which Theorem 4 readily follows by taking  $\mathfrak{S}_p = (S_p)_0$  for each  $p$ . Indeed, given this choice of  $\mathfrak{S}$ , the asymptotics for reducible  $G(\mathbb{Z})$ -orbits on  $S$  are the same as those for  $\mathcal{P}(\mathbb{Z})$ -orbits on  $\mathfrak{S}$ , as explained in Section 1.4.

**Theorem 36.** *Let  $\mathfrak{S} \subset W_0(\mathbb{Z})$  be a big family. Then the number of  $\mathcal{P}(\mathbb{Z})$ -orbits on  $\mathfrak{S}$  of height up to  $X$  is given by*

$$\left( \prod_p \int_{f \in U(\mathbb{Z}_p)} \# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}_p}{\mathcal{P}(\mathbb{Z}_p)} \right) df \right) \cdot N^{(r)}(X) + o(X^{\frac{n^2+n}{2}}), \tag{48}$$

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

*Proof.* To start, fix an integer  $\mathfrak{b} \geq 1$ , and suppose its prime factorization is given by  $\mathfrak{b} = \prod_p p^{e_p}$ . We first prove an analogue of Theorem 4 for the subfamily  $\mathfrak{S}(\mathfrak{b}) := \{B \in \mathfrak{S} : |\mathcal{Z}(B)| = \mathfrak{b}\}$ . Note that the subfamily  $\mathfrak{S}(\mathfrak{b})$  is itself a big family, where  $\mathfrak{S}(\mathfrak{b})_p = \{B \in \mathfrak{S}_p : |\mathcal{Z}(B)|_p = |\mathfrak{b}|_p\}$ .

If  $\mathfrak{S}(\mathfrak{b}) = \emptyset$ , then the result is tautologically true, so we may assume that  $\mathfrak{S}(\mathfrak{b}) \neq \emptyset$ . For each prime  $p \mid \mathfrak{b}$ , we partition  $U(\mathbb{Z}_p)$  as  $U(\mathbb{Z}_p) = \bigsqcup_{j=1}^{m_p} U_{p,j}$ , where each  $U_{p,j}$  is a level set for the function that sends  $f \in U(\mathbb{Z}_p)$  to  $\#(\mathcal{P}(\mathbb{Z}_p) \setminus (\text{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})_p))$ . Write “ $E(m)$ ” to mean “a power of  $m$  that depends only on  $n$  and  $\mathfrak{S}$ .” Then set  $U_{p,j}$  is defined by congruence conditions modulo  $E(p^{e_p})$ . The quantity  $\#(\mathcal{P}(\mathbb{Z}_p) \setminus (\text{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})_p))$  is independent of the choice of  $f \in U_{p,j}$  (by the definition of a level set) and is evidently bounded by  $E(p^{e_p})$ .

Now for each prime  $p \nmid \mathfrak{b}$ , the proof of Proposition 25 implies that  $\#(\mathcal{P}(\mathbb{Z}_p) \setminus (\text{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})_p)) = 1$  for each  $f \in \text{inv}(\mathfrak{S}(\mathfrak{b})_p)$ . It then follows from Theorem 5 that the quantity

$$\# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})}{\mathcal{P}(\mathbb{Z})} \right) = \prod_p \# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})_p}{\mathcal{P}(\mathbb{Z}_p)} \right) = \prod_{p \mid \mathfrak{b}} \# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})_p}{\mathcal{P}(\mathbb{Z}_p)} \right) \tag{49}$$

is independent of the choice of  $f \in \text{inv}(\mathfrak{S}(\mathfrak{b})) \cap \bigcap_p U_{p,j_p}$ . Therefore, for each tuple  $(j_p)_{p \mid \mathfrak{b}} \in \prod_{p \mid \mathfrak{b}} \{1, \dots, m_p\}$ , we have

$$\sum_{\substack{f \in U(\mathbb{Z}) \cap \bigcap_p U_{p,j_p} \\ H(f) < X}} \# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})}{\mathcal{P}(\mathbb{Z})} \right) = \# \left( \frac{\text{inv}^{-1}(f^*) \cap \mathfrak{S}(\mathfrak{b})}{\mathcal{P}(\mathbb{Z})} \right) \cdot \sum_{\substack{f \in \text{inv}(\mathfrak{S}(\mathfrak{b})) \cap \bigcap_p U_{p,j_p} \\ H(f) < X}} 1, \tag{50}$$

where  $f^* \in \text{inv}(\mathfrak{S}(\mathfrak{b})) \cap \bigcap_p U_{p,j_p}$  is any fixed element. Since  $\mathfrak{S}$  is a big family, it follows that  $\text{inv}(\mathfrak{S}(\mathfrak{b})_p) = U(\mathbb{Z}_p)$  for every  $p \gg 1$  that does not divide  $\mathfrak{b}$ . As the set  $\text{inv}(\mathfrak{S}(\mathfrak{b})) \cap \bigcap_p U_{p,j_p}$  is defined by congruence conditions modulo  $E(\mathfrak{b})$ , since  $\text{inv}(\mathfrak{S}(\mathfrak{b})_p) \cap U_{p,j_p}$  is defined by congruence conditions modulo  $E(p^{e_p})$  for each  $p$ , we obtain the asymptotic

$$\sum_{\substack{f \in \text{inv}(\mathfrak{S}(\mathfrak{b})) \cap \bigcap_p U_{p,j_p} \\ H(f) < X}} 1 = N^{(r)}(X) \cdot \prod_{p \mid \mathfrak{b}} \int_{f \in \text{inv}(\mathfrak{S}(\mathfrak{b})_p) \cap U_{p,j_p}} df \cdot \prod_{p \nmid \mathfrak{b}} \int_{f \in \text{inv}(\mathfrak{S}(\mathfrak{b})_p)} df + O_\epsilon(E(\mathfrak{b})X^{\frac{n^2+n-0.4}{2}+\epsilon}). \tag{51}$$

Substituting the asymptotic (51) into the right-hand side of (50), applying (49) to the resulting expression, and summing that over tuples  $(j_p)_{p \mid \mathfrak{b}} \in \prod_{p \mid \mathfrak{b}} \{1, \dots, m_p\}$  yields

$$\sum_{\substack{f \in U(\mathbb{Z}) \\ H(f) < X}} \# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})}{\mathcal{P}(\mathbb{Z})} \right) = N^{(r)}(X) \cdot \prod_p \int_{f \in U(\mathbb{Z}_p)} \# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})_p}{\mathcal{P}(\mathbb{Z}_p)} \right) df + O_\epsilon(E(\mathfrak{b})X^{\frac{n^2+n-0.4}{2}+\epsilon}). \tag{52}$$

Next, we prove that the theorem holds with “=” replaced by “ $\geq$ ”. For any real number  $M > 1$ , let  $\mathfrak{S}(M) := \{B \in \mathfrak{S} : |\mathcal{Z}(B)| < M^2\}$ . Summing (52) over  $\mathfrak{b} < M$  yields

$$\sum_{\substack{f \in U(\mathbb{Z}) \\ H(f) < X}} \# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}(M)}{\mathcal{P}(\mathbb{Z})} \right) = N^{(r)}(X) \cdot \sum_{\mathfrak{b} < M} \prod_p \int_{f \in U(\mathbb{Z}_p)} \# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})_p}{\mathcal{P}(\mathbb{Z}_p)} \right) df + O_\epsilon(E(M)X^{\frac{n^2+n-0.4}{2}+\epsilon}). \tag{53}$$

Dividing (53) through by  $N^{(r)}(X)$  and letting  $X \rightarrow \infty$ , we find that

$$\liminf_{X \rightarrow \infty} \frac{\sum_{\substack{f \in U(\mathbb{Z}) \\ H(f) < X}} \# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}}{\mathcal{P}(\mathbb{Z})} \right)}{N^{(r)}(X)} \geq \sum_{\mathfrak{b} < M} \prod_p \int_{f \in U(\mathbb{Z}_p)} \# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})_p}{\mathcal{P}(\mathbb{Z}_p)} \right) df. \quad (54)$$

Now, letting  $M \rightarrow \infty$  on the right-hand side of (54) and factoring the sum into an Euler product, we obtain

$$\begin{aligned} \sum_{\mathfrak{b}=1}^{\infty} \prod_p \int_{f \in U(\mathbb{Z}_p)} \# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})_p}{\mathcal{P}(\mathbb{Z}_p)} \right) df &= \prod_p \sum_{e=0}^{\infty} \int_{f \in U(\mathbb{Z}_p)} \# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}(p^e)_p}{\mathcal{P}(\mathbb{Z}_p)} \right) df \\ &= \prod_p \int_{f \in U(\mathbb{Z}_p)} \# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}_p}{\mathcal{P}(\mathbb{Z}_p)} \right) df. \end{aligned} \quad (55)$$

Combining (54) with (55), we find that Theorem 4 holds with “=” replaced by “ $\geq$ ”. Note that it is not a priori clear whether the infinite sum on the left-hand side of (55) converges, but even if it were to diverge, it would still be equal to the product on the right-hand side! To show that the sum does indeed converge, one can apply the Jacobian change-of-variables result in Proposition 27 to each  $p$ -adic integral; it is then clear that the summand at  $\mathfrak{b}$  is  $O(\mathfrak{b}^{-1} \prod_{p|\mathfrak{b}} p^{-1})$ , which is sufficient, as the sum of the reciprocals of the powerful numbers converges (see [25]).

It thus remains to prove the theorem with “=” replaced by “ $\leq$ ”. Let  $\mathfrak{S}(M)' := \mathfrak{S} \setminus \mathfrak{S}(M)$ . Then for each  $B \in \mathfrak{S}(M)'$ , we have that  $|\mathcal{Z}(B)| \geq M^2$ . From Theorem 33, it follows that

$$\sum_{\substack{f \in U(\mathbb{Z}) \\ H(f) < X}} \# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}(M)'}{\mathcal{P}(\mathbb{Z})} \right) = O(X^{\frac{n^2+n}{2}}/M) + O_{\epsilon}(X^{\frac{n^2+n-0.4}{2}+\epsilon}). \quad (56)$$

On the other hand, it follows from (53) that

$$\begin{aligned} \sum_{\substack{f \in U(\mathbb{Z}) \\ H(f) < X}} \# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}(M)}{\mathcal{P}(\mathbb{Z})} \right) \\ \leq N^{(r)}(X) \cdot \prod_p \int_{f \in U(\mathbb{Z}_p)} \# \left( \frac{\text{inv}^{-1}(f) \cap \mathfrak{S}_p}{\mathcal{P}(\mathbb{Z}_p)} \right) df + O_{\epsilon}(E(M)X^{\frac{n^2+n-0.4}{2}+\epsilon}). \end{aligned} \quad (57)$$

Taking  $M$  to grow as a sufficiently small power of  $X$  and combining (56) with (57) yields Theorem 36, and hence also Theorem 4.  $\square$

We finish by noting that Theorems 1 and 3 follow from Theorem 4 by applying the Jacobian change-of-variables result in Proposition 27 to each  $p$ -adic integral.

### Acknowledgments

We thank Manjul Bhargava for several enlightening conversations, for providing numerous helpful comments and suggestions, and for offering feedback on earlier drafts of this paper. We thank the

anonymous referee for giving us detailed feedback that helped us improve the exposition and readability of the paper. We are also grateful to Alex Bartel, Noam D. Elkies, Andrew Granville, Jef Laga, Aaron Landesman, Aurel Page, Peter Sarnak, and Melanie Matchett Wood for helpful discussions, and to Will Sawin for suggesting the proof of [Lemma 23](#).

Shankar was supported by a National Sciences and Engineering Research Council of Canada discovery grant and a Sloan fellowship. Siad was supported by a Queen Elizabeth II/Steve Halperin Scholarship in Science and Technology at the University of Toronto during the initial phase of this project and is grateful to Princeton University and the Institute for Advanced Study for providing excellent working conditions during its final stage. Swaminathan was supported by the National Science Foundation, under the Graduate Research Fellowship, as well as award no. 2202839.

## 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.* **23**:8 (2021), 2733–2785. [MR](#) [Zbl](#)
- [2] M. Bhargava, “The density of discriminants of quartic rings and fields”, *Ann. of Math. (2)* **162**:2 (2005), 1031–1063. [MR](#) [Zbl](#)
- [3] M. Bhargava, “Higher composition laws, IV: The parametrization of quintic rings”, *Ann. of Math. (2)* **167**:1 (2008), 53–94. [MR](#) [Zbl](#)
- [4] M. Bhargava, “The density of discriminants of quintic rings and fields”, *Ann. of Math. (2)* **172**:3 (2010), 1559–1591. [MR](#) [Zbl](#)
- [5] M. Bhargava, “Most hyperelliptic curves over  $\mathbb{Q}$  have no rational points”, preprint, 2013. [arXiv 1308.0395](#)
- [6] M. Bhargava and B. H. Gross, “The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point”, pp. 23–91 in *Automorphic representations and L-functions* (Mumbai, 2012), edited by D. Prasad et al., Tata Inst. Fundam. Res. Stud. Math. **22**, Tata Inst. Fund. Res., Mumbai, 2013. [MR](#) [Zbl](#)
- [7] M. Bhargava and A. Shankar, “The average number of elements in the 4-Selmer groups of elliptic curves is 7”, preprint, 2013. [arXiv 1312.7333](#)
- [8] 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”, preprint, 2013. [arXiv 1312.7859](#)
- [9] 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 (2015), 191–242. [MR](#) [Zbl](#)
- [10] 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 (2015), 587–621. [MR](#) [Zbl](#)
- [11] 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 (2016), 235–266. [MR](#) [Zbl](#)
- [12] M. Bhargava and A. Yang, “On the number of integral binary  $n$ -ic forms having bounded Julia invariant”, *Bull. Lond. Math. Soc.* **54**:4 (2022), 1232–1248. [MR](#) [Zbl](#)
- [13] M. Bhargava, A. Shankar, and J. Tsimerman, “On the Davenport–Heilbronn theorems and second order terms”, *Invent. Math.* **193**:2 (2013), 439–499. [MR](#) [Zbl](#)
- [14] M. Bhargava, J. Hanke, and A. Shankar, “The mean number of 2-torsion elements in the class groups of  $n$ -monogenized cubic fields”, preprint, 2020. [arXiv 2010.15744](#)
- [15] M. Bhargava, A. Shankar, and A. Swaminathan, “The second moment of the size of the 2-Selmer group of elliptic curves”, preprint, 2021. [arXiv 2110.09063](#)
- [16] M. Bhargava, A. Shankar, and X. Wang, “Squarefree values of polynomial discriminants, I”, *Invent. Math.* **228**:3 (2022), 1037–1073. [MR](#) [Zbl](#)

- [17] M. Bhargava, A. Shankar, and X. Wang, “Squarefree values of polynomial discriminants, II”, preprint, 2022. [arXiv 2207.05592](#)
- [18] A. Borel, “Ensembles fondamentaux pour les groupes arithmétiques”, pp. 23–40 in *Colloque sur la théorie des groupes algébriques* (Brussels, 1962), Librairie Univ., Louvain, Belgium, 1962. [MR Zbl](#)
- [19] A. Borel and Harish-Chandra, “Arithmetic subgroups of algebraic groups”, *Ann. of Math. (2)* **75** (1962), 485–535. [MR Zbl](#)
- [20] N. Bourbaki, *Groupes et algèbres de Lie, Chapitres VII–VIII*, Actualités Scientifiques et Industrielles **1364**, Hermann, Paris, 1975. Translated as *Lie groups and Lie algebras*, Springer, 2005. [MR Zbl](#)
- [21] H. Davenport, “On a principle of Lipschitz”, *J. Lond. Math. Soc.* **26** (1951), 179–183. [MR Zbl](#)
- [22] H. Davenport, “On the class-number of binary cubic forms, I”, *J. Lond. Math. Soc.* **26** (1951), 183–192. Correction in **27:4** (1952), 52. [MR Zbl](#)
- [23] H. Davenport, “On the class-number of binary cubic forms, II”, *J. Lond. Math. Soc.* **26** (1951), 192–198. [MR Zbl](#)
- [24] H. Davenport and H. Heilbronn, “On the density of discriminants of cubic fields, II”, *Proc. Roy. Soc. Lond. Ser. A* **322**:1551 (1971), 405–420. [MR Zbl](#)
- [25] S. W. Golomb, “Powerful numbers”, *Amer. Math. Monthly* **77** (1970), 848–855. [MR Zbl](#)
- [26] D. Gordon, D. Grenier, and A. Terras, “Hecke operators and the fundamental domain for  $SL(3, \mathbb{Z})$ ”, *Math. Comp.* **48**:177 (1987), 159–178. [MR Zbl](#)
- [27] D. Grenier, “Fundamental domains for the general linear group”, *Pacific J. Math.* **132**:2 (1988), 293–317. [MR Zbl](#)
- [28] D. Grenier, “On the shape of fundamental domains in  $GL(n, \mathbb{R})/O(n)$ ”, *Pacific J. Math.* **160**:1 (1993), 53–66. [MR Zbl](#)
- [29] F. Gundlach, *Parametrizing extensions with fixed Galois group*, Ph.D. thesis, Princeton University, 2019, available at <https://www.proquest.com/docview/2302691956>.
- [30] W. Ho, *Orbit parametrizations of curves*, Ph.D. thesis, Princeton University, 2009, available at <https://www.proquest.com/docview/304989584>.
- [31] W. Ho, A. Shankar, and I. Varma, “Odd degree number fields with odd class number”, *Duke Math. J.* **167**:5 (2018), 995–1047. [MR Zbl](#)
- [32] J. Laga, “The average size of the 2-Selmer group of a family of non-hyperelliptic curves of genus 3”, *Algebra Number Theory* **16**:5 (2022), 1161–1212. [MR Zbl](#)
- [33] J. Laga, “Graded Lie algebras, compactified Jacobians and arithmetic statistics”, *J. Eur. Math. Soc.* (online publication October 2024).
- [34] F. Mertens, “Ueber einige asymptotische Gesetze der Zahlentheorie”, *J. Reine Angew. Math.* **77** (1874), 289–338. [MR Zbl](#)
- [35] D. W. Morris, *Introduction to arithmetic groups*, Deductive Press, Lethbridge, AB, 2015. [MR Zbl](#)
- [36] M. Oller, “The density of ADE families of curves having squarefree discriminant”, preprint, 2023. [arXiv 2306.05961](#)
- [37] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Pure Appl. Math. **139**, Academic Press, Boston, MA, 1994. [MR Zbl](#)
- [38] P. Sarnak and A. Strömbergsson, “Minima of Epstein’s zeta function and heights of flat tori”, *Invent. Math.* **165**:1 (2006), 115–151. [MR Zbl](#)
- [39] J.-P. Serre, *A course in arithmetic*, Grad. Texts in Math. **7**, Springer, 1973. [MR Zbl](#)
- [40] A. N. Shankar, “2-Selmer groups of hyperelliptic curves with marked points”, *Trans. Amer. Math. Soc.* **372**:1 (2019), 267–304. [MR Zbl](#)
- [41] A. Shankar and J. Tsimerman, “Counting  $S_5$ -fields with a power saving error term”, *Forum Math. Sigma* **2** (2014), art. id. e13. [MR Zbl](#)
- [42] A. Shankar and I. Varma, “Malle’s conjecture for octic  $d_4$ -fields”, in preparation.
- [43] A. Shankar and X. Wang, “Rational points on hyperelliptic curves having a marked non-Weierstrass point”, *Compos. Math.* **154**:1 (2018), 188–222. [MR Zbl](#)
- [44] A. N. Shankar, A. Shankar, and X. Wang, “Large families of elliptic curves ordered by conductor”, *Compos. Math.* **157**:7 (2021), 1538–1583. [MR Zbl](#)

- [45] T. Shintani, “On Dirichlet series whose coefficients are class numbers of integral binary cubic forms”, *J. Math. Soc. Japan* **24** (1972), 132–188. [MR](#) [Zbl](#)
- [46] A. Siad, “Effect of monogenicity on 2-torsion in the class group of number fields of odd degree”, preprint, 2020. [arXiv 2011.08834](#)
- [47] A. Siad, “Monogenic fields with odd class number, II: Even degree”, preprint, 2020. [arXiv 2011.08842](#)
- [48] C. L. Siegel, “The average measure of quadratic forms with given determinant and signature”, *Ann. of Math. (2)* **45** (1944), 667–685. [MR](#) [Zbl](#)
- [49] A. A. Swaminathan, “A new parametrization for ideal classes in rings defined by binary forms, and applications”, *J. Reine Angew. Math.* **798** (2023), 143–191. [MR](#) [Zbl](#)
- [50] A. A. Swaminathan, “Most odd-degree binary forms fail to primitively represent a square”, *Compos. Math.* **160**:3 (2024), 481–517. [MR](#) [Zbl](#)
- [51] A. A. Swaminathan, “The mean number of 2-torsion elements in the class groups of cubic orders”, *Comment. Math. Helv.* **100**:2 (2025), 225–267. [MR](#) [Zbl](#)
- [52] J. A. Thorne, *The arithmetic of simple singularities*, 2012.
- [53] L. Y. Vulakh, “Units in some families of algebraic number fields”, *Trans. Amer. Math. Soc.* **356**:6 (2004), 2325–2348. [MR](#) [Zbl](#)

Communicated by Andrew Granville

Received 2022-08-24

Revised 2024-07-30

Accepted 2024-09-03

[arul.shnkr@gmail.com](mailto:arul.shnkr@gmail.com)

*Department of Mathematics, University of Toronto, Toronto, ON, Canada*

[as4426@princeton.edu](mailto:as4426@princeton.edu)

*Department of Mathematics, Princeton University, Princeton, NJ, United States  
School of Mathematics, Institute for Advanced Study, Princeton, NJ,  
United States*

[swaminathan@math.harvard.edu](mailto:swaminathan@math.harvard.edu)

*Department of Mathematics, Harvard University, Cambridge, MA, United States*

[ila@math.toronto.edu](mailto:ila@math.toronto.edu)

*Department of Mathematics, University of Toronto, Toronto, ON, Canada*

# Algebra & Number Theory

[msp.org/ant](http://msp.org/ant)

## EDITORS

### MANAGING EDITOR

Antoine Chambert-Loir  
Université Paris-Diderot  
France

### EDITORIAL BOARD CHAIR

David Eisenbud  
University of California  
Berkeley, USA

## BOARD OF EDITORS

Jason P. Bell	University of Waterloo, Canada	Philippe Michel	École Polytechnique Fédérale de Lausanne
Bhargav Bhatt	University of Michigan, USA	Martin Olsson	University of California, Berkeley, USA
Frank Calegari	University of Chicago, USA	Irena Peeva	Cornell University, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Saclay, France	Jonathan Pila	University of Oxford, UK
Brian D. Conrad	Stanford University, USA	Anand Pillay	University of Notre Dame, USA
Samit Dasgupta	Duke University, USA	Bjorn Poonen	Massachusetts Institute of Technology, USA
Hélène Esnault	Freie Universität Berlin, Germany	Victor Reiner	University of Minnesota, USA
Gavril Farkas	Humboldt Universität zu Berlin, Germany	Peter Sarnak	Princeton University, USA
Sergey Fomin	University of Michigan, USA	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Vasudevan Srinivas	SUNY Buffalo, USA
Wee Teck Gan	National University of Singapore	Shunsuke Takagi	University of Tokyo, Japan
Andrew Granville	Université de Montréal, Canada	Pham Huu Tiep	Rutgers University, USA
Ben J. Green	University of Oxford, UK	Ravi Vakil	Stanford University, USA
Christopher Hacon	University of Utah, USA	Akshay Venkatesh	Institute for Advanced Study, USA
Roger Heath-Brown	Oxford University, UK	Melanie Matchett Wood	Harvard University, USA
János Kollár	Princeton University, USA	Shou-Wu Zhang	Princeton University, USA
Michael J. Larsen	Indiana University Bloomington, USA		

## PRODUCTION

[production@msp.org](mailto:production@msp.org)

Silvio Levy, Scientific Editor

---

See inside back cover or [msp.org/ant](http://msp.org/ant) for submission instructions.

---

The subscription price for 2025 is US \$565/year for the electronic version, and \$820/year (+\$70, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.


---

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

---

ANT peer review and production are managed by EditFLOW<sup>®</sup> from MSP.

PUBLISHED BY

 **mathematical sciences publishers**  
nonprofit scientific publishing

<http://msp.org/>

© 2025 Mathematical Sciences Publishers

# Algebra & Number Theory

Volume 19    No. 6    2025

---

<a href="#">Semistable representations as limits of crystalline representations</a>	1049
ANAND CHITRAO, EKNATH GHATE and SEIDAI YASUDA	
<a href="#">Geometry-of-numbers methods in the cusp</a>	1099
ARUL SHANKAR, ARTANE SIAD, ASHVIN A. SWAMINATHAN and ILA VARMA	
<a href="#">Explicit isogenies of prime degree over number fields</a>	1147
BARINDER S. BANWAIT and MAARTEN DERICKX	
<a href="#">Ideals in enveloping algebras of affine Kac–Moody algebras</a>	1199
REKHA BISWAL and SUSAN J. SIERRA	
<a href="#">The integral Chow ring of weighted blow-ups</a>	1231
VERONICA ARENA and STEPHEN OBINNA	