Monogenic Fields with Odd Class Number

by

Artane Siad

A thesis submitted in conformity with the requirements
for the degree of Doctor of Philosophy

Graduate Department of Mathematics
University of Toronto

© Copyright 2021 by Artane Siad

Monogenic Fields with Odd Class Number

Artane Siad
Doctor of Philosophy

Graduate Department of Mathematics
University of Toronto
2021

Abstract

We prove an upper bound on the average number of 2-torsion elements in the class group monogenised fields of any degree $n \geq 3$, and, conditional on a widely expected tail estimate, compute this average exactly. As an application, we show that there are infinitely many number fields with odd class number in any even degree and signature. This completes a line of results on class number parity going back to Gauss.

Acknowledgments

First and foremost, I want to express my deepest gratitude to my advisor Arul Shankar. I could not have asked for a better advisor. His enthusiasm, generosity, openness, and constant encouragement have shaped my growth as a mathematician and as a person in more ways than I can name. His work, vision, and energy have been and continue to be a source of inspiration.

During my time at the University of Toronto, I have benefited enormously from my interactions with several mathematicians. Special thanks to Marco Gualtieri, Stephen Kudla, Jim Arthur, Jacob Tsimerman, Ila Varma, Sarah Mayes-Tang, Faisal Al-Faisal, Stanley Xiao, and Michael Groechenig for helping me at key moments.

I am grateful to Manjul Bhargava, Jonathan Hanke, Ashvin Swaminathan, and Ila Varma for useful discussions and helpful comments on the two articles that form this thesis.

My experience in graduate school would not have been so filled with joy without my friends in Cambridge and Toronto. Thanks for the good times, past, present and future!

I want to thank the administrative staff in the math department and, in particular, Jemima Merisca.

I warmly thank the Fields Institute for making non-trivial contributions to my caffeine and caloric intake in the pre-pandemic years and, more seriously, for providing an excellent environment to work and interact with researchers from around the world.

Lastly, to my brother Abshir, my parents Souad and Wilwal, and my grandmother Jacqueline, thank you for being a constant source of love and support. Writing this thesis would not have been possible without you.

Contents

Chapter 1

Odd degree

1.1 Introduction

The Cohen–Lenstra–Martinet–Malle heuristics which were developed in a series of groundbreaking works [19, 21, 22, 20, 35], constitute our best conjectural description of the distribution of the p^∞-part of the class group, $\mathrm{Cl}(K)[p^\infty]$, over families of number fields K of fixed degree and signature ordered by discriminant for "good" primes p. We say that a prime p is "good" if it is coprime to the degree of the field and "bad" otherwise.

So far, only two cases of these heuristics have been settled. In 1971, Davenport and Heilbronn [25] calculated the average number of 3-torsion elements in the class group of quadratic fields. In 2005, Bhargava calculated the average number of 2-torsion in the class group of cubic fields.

Theorem 1.1.1 (Davenport–Heilbronn, [25]). *Let (r_1, r_2) denote the signature. The average number of 3-torsion elements in the class group of isomorphism classes of quadratic fields ordered by discriminant is:*

(r_1, r_2)	$\mathrm{Avg}\Big(\#\mathrm{Cl}_3(K)\Big)$
$(2, 0)$	$3/4$
$(0, 1)$	2

Theorem 1.1.2 (Bhargava, [6]). *Let (r_1, r_2) denote the signature. The average number of 2-torsion elements in the class group of isomorphism classes of cubic fields ordered by discriminant is:*

(r_1, r_2)	$\mathrm{Avg}\Big(\#\mathrm{Cl}_2(K)\Big)$
$(3, 0)$	$5/4$
$(1, 1)$	$3/2$

The heuristics are expected to hold under any natural ordering on the family of fields and not just when ordering by discriminant. In [29], Ho–Shankar–Varma found evidence to support this expectation by showing that the average number of 2-torsion elements in the class group of fields associated to binary n-ic forms, ordered either by naive height or by

Julia invariant, coincided with the value predicted from the Cohen–Lenstra–Martinet–Malle heuristics.

Theorem 1.1.3 (Ho–Shankar–Varma [29])**.** *Let $n \geq 3$ be an odd integers. Let $\mathfrak{R}$ be the family of fields associated to binary n-ic forms ordered by naive height or by Julia invariant. The average number of 2-torsion elements in the class group of fields in $\mathfrak{R}$ satisfies the bound:*

$$\operatorname{Avg}(\mathrm{Cl}_2, \mathfrak{R}) \leq 1 + \frac{1}{2^{r_1+r_2-1}}$$

with equality conditional on a tail estimate.

Interestingly, the work of Bhargava–Varma [14, 15] and Ho–Shankar–Varma [29] showed that these averages remain the same when one imposes finitely many local conditions or even an *acceptable family* of local conditions. A set of local conditions is called *acceptable* if for large enough primes p it includes all fields with discriminant indivisible by p^2.

It then becomes natural to ask about the effect of global conditions on averages of this kind. In [10], Bhargava–Hanke–Shankar showed that *monogenicity* had the effect of doubling the average number of non-trivial 2-torsion elements in the class group!

Theorem 1.1.4 (Bhargava–Hanke–Shankar, [10])**.** *Let (r_1, r_2) denote the signature. The average number of 2-torsion elements in the class group of isomorphism classes of monogenised cubic fields ordered by "naive" height is:*

(r_1, r_2)	$\operatorname{Avg}\Big(\#\mathrm{Cl}_2(K)\colon K \textit{ is monogenic}\Big)$
$(3, 0)$	$3/2$
$(1, 1)$	2

In this paper, we show that this behaviour is not unique to cubic fields but indeed holds for any odd degree. More precisely, we prove that the average number of non-trivial 2-torsion elements in the class group of monogenised fields of odd degree ordered by naive height is twice that predicted by the Cohen–Lenstra–Martinet–Malle heuristic for the full family of fields.

1.1.1 Monogenised fields and rings

A number field K of degree n is said to be *monogenic* if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. The element α is called a *monogeniser* of the field K. A *monogenised* field is the data (K, α) of a monogenic field together with a choice of monogeniser.

It is expected that 100% of monogenic fields possess a unique monogeniser up to transformations of the form $\alpha \mapsto \pm\alpha + m$ for some $m \in \mathbb{Z}$, see [13]. This motivates the following definition.

Definition 1.1.5. Two monogenised fields (K, α) and (K', α') are said to be isomorphic if there exists a field isomorphism from K to K' taking α to $\pm\alpha' + m$ for some $m \in \mathbb{Z}$.

Thus, the expectation is that working with isomorphism classes of monogenised fields is statistically equivalent to working with isomorphism classes of monogenic fields. Nevertheless, if a statement holds for a "positive proportion" of *monogenised* fields, the same statement holds for "infinitely many" *monogenic* fields by using the arguments of [29] combined with the construction of strongly quasi-reduced elements from [13].

The height we choose for monogenised fields/rings has a convenient interpretation. Each isomorphism class of monogenised field contains a unique element (K, α_0) with the property that $0 \leq \mathrm{tr}(\alpha_0) < n$. If $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ is the minimal polynomial of α_0, we define the *naive* height of the isomorphism class to be:

$$H\Big([(K, \alpha_0)] \Big) = \max_i \Big\{ |a_i|^{1/i} \Big\}.$$

Similarly, we can define *monogenised* rings and the *naive* height of their isomorphism classes. In Section 2.2, we will see that the set of monogenised rings is in natural bijection with the set of monic degree n polynomials. This equips monogenised rings with natural local measures, and we can speak of families of fields in $\mathfrak{R}^{r_1,r_2}$ associated with sets of local specifications $(\Sigma_p)_p$ on monic polynomials.

We denote by $\mathfrak{R}^{r_1,r_2}$ the collection of isomorphism classes of monogenised orders of signature (r_1, r_2) ordered by naive height and by $\mathfrak{R}^{r_1,r_2}_{\max}$ the subcollection consisting of maximal orders. For an monogenic ring $\mathcal{O} \in \mathfrak{R}^{r_1,r_2}$, denote by $\mathrm{Cl}_2(\mathcal{O})$ the 2-torsion subgroup of the ideal class group $\mathrm{Cl}(\mathcal{O})$ of $\mathcal{O}$ and by $\mathcal{I}_2(\mathcal{O})$ the group of 2-torsion ideals of $\mathcal{O}$.

1.1.2 Outline of the results

In our main theorem for fields, we find the average number of 2-torsion elements in the class group and narrow class group of monogenised fields ordered by naive height, conditional on a tail estimate.

Theorem 1.1.6 (Main theorem for monogenic fields)**.** *Let $\mathfrak{R} \subset \mathfrak{R}^{r_1,r_2}_{\max}$ be a family of monogenised fields corresponding to an acceptable collection of local specifications $\Sigma = (\Sigma_p)_p$.*

The average number of 2-torsion elements in the class group of fields in $\mathfrak{R}$ satisfies the bound:

$$\mathrm{Avg}(\mathrm{Cl}_2, \mathfrak{R}) \leq 1 + \frac{2}{2^{r_1+r_2-1}}$$

with equality conditional on a tail estimate.

The average number of 2-torsion elements in the narrow class group of fields in $\mathfrak{R}$ satisfies the bound:

$$\mathrm{Avg}(\mathrm{Cl}_2^+, \mathfrak{R}) \leq 1 + \frac{1}{2^{\frac{n-1}{2}}} + \frac{1}{2^{r_2}}$$

with equality conditional on a tail estimate.

These averages have several interesting consequences. Indeed, we obtain all of the corollaries of Ho–Shankar–Varma [29] with the added adjective "monogenic".

Corollary 1.1.7. *Let $n \geq 3$ be an odd integer, (r_1, r_2) a choice of signature, and $\mathfrak{R} \subset \mathfrak{R}^{r_1,r_2}_{\max}$ a family of monogenised fields corresponding to an acceptable family of local specifications $\Sigma = (\Sigma_p)_p$.*

1) The proportion of fields in $\mathfrak{R}$ which have odd class number is at least

$$1 - \frac{2}{2^{r_1+r_2-1}}.$$

2) The proportion of fields in $\mathfrak{R}$ which have odd narrow class number is at least

$$1 - \frac{1}{2^{\frac{n-1}{2}}} - \frac{1}{2^{r_2}}.$$

In particular, there are infinitely many degree n monogenic S_n-fields with signature (r_1, r_2) which have odd class number and infinitely many which have units of every signature.

We also deduce asymptotic lower bounds for the number of monogenised fields having odd class numbers when these fields are ordered by discriminant just as in [29].

Corollary 1.1.8. *Let $n \geq 3$ be an odd integer, (r_1, r_2) a choice of signature, and $\mathfrak{R} \subset \mathfrak{R}^{r_1,r_2}_{\max}$ be an acceptable family of monogenised fields. Then the following asymptotic estimates hold.*

1) $\#\{R \in \mathfrak{R} \colon\ |\mathrm{Disc}\,(R)| < X \text{ and } 2 \nmid |\mathrm{Cl}\,(R)|\} \gg X^{\frac{1}{2}+\frac{1}{n}}$.

2) If $r_2 \neq 0$, then we have $\#\left\{R \in \mathfrak{R} \colon\ |\mathrm{Disc}\,(R)| < X \text{ and } 2 \nmid \left|\mathrm{Cl}^+\,(R)\right|\right\} \gg X^{\frac{1}{2}+\frac{1}{n}}$.

We also obtain an unconditional statement for *very large* families of monogenised *rings*. We call a family of monogenised orders *very large* if for large enough p, there are no local conditions at p.

Theorem 1.1.9 (Main theorem for monogenic rings)**.** *Let $n \geq 3$ be an odd integer and (r_1, r_2) a choice of signature. Let $\mathfrak{R} \subset \mathfrak{R}^{r_1,r_2}$ be a very large family of monogenised orders with the property that local conditions at 2 are given modulo 2.*

1) The average over $\mathcal{O} \in \mathfrak{R}$ of the quantity

$$|\mathrm{Cl}_2(\mathcal{O})| - \frac{1}{2^{r_1+r_2-1}}\,|\mathcal{I}_2(\mathcal{O})|$$

is equal to $1 + \frac{1}{2^{r_1+r_2-1}}$.

2) The average over $\mathcal{O} \in \mathfrak{R}$ of the quantity

$$\left|\mathrm{Cl}_2^+(\mathcal{O})\right| - \frac{1}{2^{r_2}}\,|\mathcal{I}_2(\mathcal{O})|$$

is equal to $1 + \frac{1}{2^{\frac{n-1}{2}}}$.

Remark 1.1.10. We remark that our arguments give the "dual" proof of the monogenic result of Bhargava–Hanke–Shankar [10] in the cubic case. Indeed, they work with pairs of half-integral symmetric matrices while we work with the dual lattice which consists of pairs of integral symmetric matrices. The advantage is that our "dual" proof generalises to all higher dimension since Wood's parametrisation [45] continues to hold, while the parametrisation in terms pairs of half-integral symmetric matrices does not.

1.1.3 Organisation of the chapter

In Section 2.2, we parametrise isomorphism classes of monogenised rings of degree n in terms of certain monic polynomials of degree n with integer coefficients (SPACE A). In Section 2.2, we use Wood's parametrisation [45] to express the 2-torsion ideal classes of rings in $\mathfrak{R}^{r_1,r_2}$ in terms of certain $\mathrm{SL}_n(\mathbb{Z})$ orbits of pairs of $n \times n$ integral symmetric matrices (A, B) subject to the constraint $\det(A) = (-1)^{\frac{n-1}{2}}$ (SPACE B). The main results are then proven by finding asymptotic formulae for the number of elements of (SPACE A) and of (SPACE B) of height at most X, and then evaluating the limit of the ratio as X tends to infinity. The asymptotic formula for (SPACE B) was computed by Bhargava–Shankar–Wang in [13] and we recall it at the end of Section 2.2.

The constraint $\det(A) = (-1)^{\frac{n-1}{2}}$ complicates the direct application of techniques from the geometry of numbers because one needs to count orbits for the action of the group $\mathrm{SL}_n(\mathbb{Z})$ on the *hypersurface* defined by $\det(A) = (-1)^{\frac{n-1}{2}}$. To circumvent this complication, we borrow an idea of [10] and "linearise" the problem by noting that the collection $\mathscr{L}_{\mathbb{Z}}$ of $\mathrm{SL}_n(\mathbb{Z})$ equivalence classes of symmetric integral matrices of determinant $(-1)^{\frac{n-1}{2}}$ is finite. Counting $\mathrm{SL}_n(\mathbb{Z})$ orbits on the space of pairs (A, B) with the constraint $\det(A) = (-1)^{\frac{n-1}{2}}$ is thus reduced to counting $\mathrm{SO}_{A_0}(\mathbb{Z})$ orbits on the space of pairs (A_0, B) over all $A_0 \in \mathscr{L}_{\mathbb{Z}}$.

In Sections 1.3-1.6, the geometry of number techniques developed in [12, 11] are applied to count the relevant orbits in these slices. However, the arguments are complicated by the fact that we consider an infinite set of representations simultaneously and the fact that the A_0 have maximal $\mathbb{Q}$-anisotropic subspaces of varying dimensions. The latter is a novel feature not present in [8] or [39] which both dealt with split orthogonal groups. In Section 2.5, we adapt the sieves of [29] to restrict the count to orbits associated to invertible ideal classes of orders and to maximal orders. For maximal orders, the lower bound obtained is conditional on a tail estimate just as in [29].

In Section 2.10, the counts on the individual slices are aggregated into the full count by summing over all the elements of $\mathscr{L}_{\mathbb{Z}}$. Calculating this sum is delicate because it relies on evaluating non-trivial masses for each of the A_0 slices at the 2-adic place and the Archimedean place. We find these masses in Section 2.8 and Section 1.8 by establishing equidistribution results.

1.1.4 Generalisations

The methods of this paper can be used to study averages of monogenised fields in even degree, as well as averages for rings and fields of odd degree associated to binary forms with leading coefficient N via Wood's parametrisation [44].

For rings and fields of odd degree associated to polynomials with leading coefficient N, our methods can be applied directly to give asymptotic formulas. But now the equi-distribution results present much more difficulty and involve classification theorems for pairs of forms over $\mathbb{Z}/p\mathbb{Z}$ as given by Dickson. In forthcoming work [42], Swaminathan shows that these averages in both the even and the odd cases can be reduced to the monogenic averages together with an additional term correcting for cuspidal over-count!

1.2 The parametrisations

1.2.1 The parametrisation of monogenised n-ic rings

In order to count the number of monogenised n-ic rings having bounded height, we will use the following parametrisation in terms of binary n-ic forms:

Definition 1.2.1. Let $U = \mathrm{Sym}_n(2)$ denote the space of binary n-ic forms. We denote by $U_1 \subset U$ the space of all monic binary n-ic forms $f(x, y) = x^n + a_{n-1}x^{n-1}y + \ldots + a_0y^n$. The group GL_2 acts on U via the twisted action $\gamma \cdot f(x, y) := \det(\gamma)^{-1}f((x, y) \cdot \gamma)$ for $\gamma \in \mathrm{GL}_2$ and $f \in U$. Let $F \subset \mathrm{GL}_2$ denote the group of lower triangular unipotent matrices. Then the action of F on U preserves U_1 and yields an action of F on U_1.

We say that a pair (R, α) is a monogenised n-ic ring if R is an n-ic ring and α is an element of R such that $R = \mathbb{Z}[\alpha]$. Two monogenised n-ic rings (R, α) and (R, α') are said to be isomorphic if R and R' are isomorphic via a ring isomorphism sending α to $\alpha' + m$ for some $m \in \mathbb{Z}$. We then have the following explicit parametrisation of monogenised n-ic rings in terms of the orbit data introduced above:

Theorem 1.2.2. *There is a natural bijection between isomorphism classes of monogenised n-ic rings and $F(\mathbb{Z})$-orbits on $U_1(\mathbb{Z})$.*

Proof. Consider the map sending a monic binary n-ic form $f(x, y) \in U_1(\mathbb{Z})$ to the monogenised n-ic ring $R_f := \left(\frac{\mathbb{Z}[\theta]}{(f(\theta,1))}, \theta\right)$. This map descends to a map from $F(\mathbb{Z})\backslash U_1(\mathbb{Z})$ to isomorphism classes of monogenised n-ic rings which we denote by Φ. Indeed, if $g = \gamma \cdot f$ for $\gamma = \left[\begin{smallmatrix} 1 & 0 \\ m & 1 \end{smallmatrix}\right] \in F(\mathbb{Z})$, then $g(\theta, 1) = f(\theta + m, 1)$ and the monogenised ring $\left(\frac{\mathbb{Z}[\theta]}{(f(\theta,1))}, \theta\right)$ is isomorphic to the monogenised ring $\left(\frac{\mathbb{Z}[\theta]}{(f(\theta+m,1))}, \theta\right)$ through $\theta \mapsto \theta + m$. To verify that Φ is surjective, note that it was already surjective as a map from monic binary n-ic forms to monogenised n-ic rings. To verify that Φ is injective, suppose that $\Phi(f) = \left(\frac{\mathbb{Z}[\theta]}{(f(\theta,1))}, \theta\right)$ is isomorphic to $\Phi(g) = \left(\frac{\mathbb{Z}[\omega]}{(g(\omega,1))}, \omega\right)$. Then $\theta \mapsto \omega + m$ for some $m \in \mathbb{Z}$ under this isomorphism. Consequently, $f(\theta, 1) = 0$ in $\Phi(f)$ means that $f(\omega + m, 1) = 0$ in $\Phi(g)$. In other words, the polynomial $g(\omega, 1)$ divides $f(\omega + m, 1)$. But since both are monic, we must have $g(\omega, 1) = f(\omega + m, 1)$. Thus, $g = \left[\begin{smallmatrix} 1 & 0 \\ m & 1 \end{smallmatrix}\right] \cdot f$ and $g = f$ in $F(\mathbb{Z})\backslash U_1(\mathbb{Z})$. □

Remark 1.2.3. The results above hold for all n (even or odd).

Remark 1.2.4. The expectation is that 100% of monogenic fields have a unique monogenised representative, i.e. 100% of all monogenic fields can be expressed as $\mathbb{Z}[\pm\theta]$ in a unique way up to translation of $\pm\theta$ by an integer. So, in what follows, we are counting the monogenic fields if we believe this expectation. Furthermore, Hilbert's irreducibility theorem tells us that a proportion of 100% of monogenic/monogenised fields have Galois group S_n.

1.2.2 The parametrisation of ideal classes of order 2 in monogenised rings

We now present the parametrisation of order 2 ideal classes in monogenic rings by pairs of symmetric matrices. This parametrisation is due to Wood, in [44] and [45], and in the case $n = 3$ due to the work of Bhargava, [5]. The statements that we use are essentially the same as those of Ho–Shankar–Varma, in [29]. We first describe the parametrisation for principal ideal domains. We then specialise to $\mathbb{R}$, $\mathbb{Z}_p$, and $\mathbb{Z}$.

We define the space of pairs of symmetric matrices.

Definition 1.2.5. Let T be a base ring. Let

$$V(T) = T^2 \otimes \mathrm{Sym}^2(T^n)$$

be the space of pairs of symmetric $n \times n$ matrices with coefficients in T. The group $\mathrm{SL}_n(T)$ acts on $V(T)$ by change of basis. In other words, if $\gamma \in \mathrm{SL}_n(T)$ and $(A, B) \in V(T)$, we define

$$\gamma(A, B) = (\gamma^t A \gamma, \gamma^t B \gamma),$$

where γ^t denotes the transpose of γ.

There is a natural map from this space of pairs of matrices, $V(T)$, to the space of polynomials, $U(T)$, called the resolvent map.

Definition 1.2.6 (The resolvent map π)**.** Let T be a base ring. We define the resolvent map $\pi \colon V(T) \to U(T)$ by

$$(A, B) \mapsto (-1)^{\frac{n-1}{2}} \det(Ax - B).$$

The resolvent map π is $\mathrm{SL}_n(T)$ invariant. We write $f_{(A,B)} := \pi(A, B)$ for the resolvent form of the $\mathrm{SL}_n(T)$-equivalence class of the pair (A, B). We say that a pair $(A, B) \in V(T)$ is non-degenerate if the associated binary form $f_{(A,B)}$ is non-degenerate (i.e. has non-zero discriminant).

Now, let T be an principal ideal domain and $f \in U_1(T)$. The following result of Wood parametrises ideal classes of the ring $R_f = \frac{T[x]}{(f(x))}$ in terms of $\mathrm{SL}_n(T)$-orbits on $V(T)$.

Theorem 1.2.7 (Wood [44] [45]). *Take a non-degenerate monic binary n-ic form $f \in U_1(T)$ and let $R_f = \frac{T[x]}{(f(x))}$. We have a bijection between $\mathrm{SL}_n^{\pm}(T)$-orbits of pairs $(A, B) \in V(T)$ with $f_{(A,B)} = f$ and equivalence classes of pairs (I, δ) where $I \subset R_f$ is an ideal of R_f and $\delta \in R_f^{\times}$ such that $I^2 \subset (\delta)$ as ideals and $N(I)^2 = N(\delta)$. The classes (I, δ) and (I', δ') are equivalent if there exists a $\kappa \in K_f^{\times}$ with the property that $I = \kappa I'$ and $\delta = \kappa^2 \delta$.*

They also describe the stabilisers.

Lemma 1.2.8 (Ho–Shankar–Varma, [29]). *The stabiliser of $(A, B) \in \pi^{-1}(f)$ in the group $\mathrm{SL}_n(T)$ corresponds to the norm 1 elements of the 2-torsion in the units of R_f,*

$$R_f^{\times}[2]_{N\equiv 1}.$$

1.2.3 The parametrisation over fields and $\mathbb{Z}_p$

Over a field or $\mathbb{Z}_p$, the parametrisation reduces to the following.

Lemma 1.2.9 (Ho–Shankar–Varma, [29]). *Let f be a monic separable non-degenerate binary n-ic form with coefficients in T, for T a field or $\mathbb{Z}_p$. The projective $\mathrm{SL}_n(T)$-orbits of $V(T)$ with invariant binary n-ic form f are in bijection with*

$$\left(R_f^{\times}/(R_f^{\times})^2\right)_{N\equiv 1}.$$

1.2.4 The parametrisation over $\mathbb{Z}$

In this section, we relate the integral orbits to 2-torsion in the class group following Ho–Shankar–Varma.

Let $\mathcal{O}$ be an order in a degree n number field whose Galois group is S_n. We let $H(\mathcal{O})$ denote the set of pairs (I, δ) consisting of a fractional ideal $I \subset \mathcal{O}$ and an element $\delta \in K^{\times}$ such that $I^2 \subset (\delta)$, $N(I)^2 = N(\delta)$ and such that the ideal I is projective (i.e. invertible as a fractional ideal). The set $H(\mathcal{O})$ is equipped with a natural composition law defined by component wise multiplication.

There is a map from $H(\mathcal{O})$ to the 2-torsion of the class group of the order $\mathcal{O}$ given by forgetting about the δ component. This map is surjective, and the fibres depend only on the rank of the unit group of $\mathcal{O}$. It is also possible to relate $H(\mathcal{O})$ to 2-torsion in the narrow class group of $\mathcal{O}$. The following is done in Ho–Shankar–Varma.

Lemma 1.2.10 (Ho–Shankar–Varma, [29]). *Let $\mathcal{O}$ be an order in an S_n-number field of degree n and signature (r_1, r_2). Then*

$$|H(\mathcal{O})| = 2^{r_1+r_2-1}|\mathrm{Cl}_2(\mathcal{O})|.$$

Furthermore, if $H^+(\mathcal{O})$ denotes the subgroup of $H(\mathcal{O})$ consisting of pairs (I, δ) such that δ is positive under every real embedding of the fraction field of $\mathcal{O}$, then

$$|H^+(\mathcal{O})| = 2^{r_2}|\mathrm{Cl}_2^+(\mathcal{O})|.$$

Finally, we record two theorems from Ho–Shankar–Varma. They characterise those elements of $V(\mathbb{Z})$ which correspond to the 2-torsion subgroup of the ideal group of $\mathcal{O}$, $\mathcal{I}_2(\mathcal{O})$. That is the group of fractional ideals of $\mathcal{O}$ with the property that $I^2 = \mathcal{O}$. If $\mathcal{O}$ is a maximal order, the only element in $\mathcal{I}_2(\mathcal{O})$ is the trivial element of the class group of $\mathcal{O}$.

Definition 1.2.11. A pair $(A, B) \in V(\mathbb{Q})$ is said to be reducible if the quadrics corresponding to A and B in $\mathbb{P}^{n-1}(\mathbb{Q})$ have a dimension $(n-1)/2$ common rational isotropic subspace.

Lemma 1.2.12 (Ho–Shankar–Varma, [29]). *Let (A, B) be a projective element $V(\mathbb{Z})$ with primitive, irreducible, and non-degenerate resultant form. Let (I, δ) be the corresponding pair. Then δ is a square in $(R_f \otimes_{\mathbb{Z}} \mathbb{Q})^\times$ if and only if (A, B) is reducible.*

The following result characterises the elements of V which correspond to elements of $I_2(\mathcal{O})$ and is due to Ho–Shankar–Varma.

Lemma 1.2.13 (Ho–Shankar–Varma, [29]). *Let $\mathcal{O}_f$ be an order corresponding to the integral primitive irreducible and non-degenerate binary n-ic form f. Then $I_2(\mathcal{O}_f)$ is in natural bijection with the set of projective reducible $\mathrm{SL}_n(\mathbb{Z})$-orbits on $V(\mathbb{Z}) \cap \pi^{-1}(f)$.*

Later, we will show that these elements make up most of the cusp and only a negligible fraction of the elements in the main body.

1.2.5 The counting problem

We count the average number of 2-torsion elements in the class group of monogenised rings and fields of odd degree. To make sense of this, we order the monogenic fields using the naive height on the minimal polynomial of a generator of the ring of integers whose trace is in $[0, n)$. Take a monic integral polynomial $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \in \mathbb{Z}[x]$. We define the naive height of f by:

$$H(f) := \max\{|a_i|^{1/i}\} = \max\{|a_1|, |a_2|^{1/2}, \ldots, |a_n|^{1/n}\}.$$

Note that H has the property that

$$H(\lambda B) = \lambda H(f)$$

so that H is homogeneous of degree 1. This will be needed when we apply arguments from the geometry of numbers. The goal of the paper is to determine the following averages:

$$\lim_{X \to \infty} \frac{\sum\limits_{\substack{\mathcal{O} \in \mathfrak{R} \\ H(\mathcal{O}) < X}} |\mathrm{Cl}_2(\mathcal{O})| - |I_2(\mathcal{O})|}{\sum\limits_{\substack{\mathcal{O} \in \mathfrak{R} \\ H(\mathcal{O}) < X}} 1}$$

and

$$\lim_{X\to\infty} \frac{\sum\limits_{\substack{\mathcal{O}\in\mathfrak{R}\\ H(\mathcal{O})<X}} \left|\mathrm{Cl}_2^+(\mathcal{O})\right| - |I_2(\mathcal{O})|}{\sum\limits_{\substack{\mathcal{O}\in\mathfrak{R}\\ H(\mathcal{O})<X}} 1},$$

where $\mathfrak{R} \subset \mathfrak{R}^{r_1,r_2}$ is any acceptable family of monogenic rings (an acceptable family is one which includes all rings with squarefree discriminant).

The asymptotic formula for the denominator comes from the work of Bhargava–Shankar–Wang, [13].

Theorem 1.2.14 (Bhargava–Shankar–Wang, [13])**.** *Let $S = (S_p)$ be an acceptable collection of local specifications. If $0 \leq b < n$ is fixed and $U_{1,b}$ denotes the set of monic polynomial whose x^{n-1} coefficient is b, then we have*

$$\left|U_{1,b}^{r_2}(S)^{\mathrm{irr}}_{<X}\right| = \mathrm{Vol}(U_{1,b}^{r_2}(\mathbb{R})_{<X}) \prod_p \mathrm{Vol}(S_p) + o(X^{\frac{n(n+1)}{2}-1}).$$

As $\mathrm{Vol}(S_{\infty,H<X})$ grows like $X^{\frac{n(n+1)}{2}-1}$, the main term dominates the error term. There is a power saving error term in their work, but we will not need it in what follows.

1.3 Reduction theory

Fix an element $A \in \mathscr{L}_{\mathbb{Z}}$ and $\delta \in \mathcal{T}(r_2)$. We build a finite cover of the fundamental domain for the action of $\mathrm{SO}_A(\mathbb{Z})$ on $V_A^{r_2,\delta}(\mathbb{R})$.

Definition 1.3.1. The height of an element in $B \in V_A^{r_2,\delta}$ is defined to be the height of the associated resolvent polynomial. That is, $H(B) := H\left((-1)^{\frac{n-1}{2}}\det(Ax - B)\right)$.

The construction of [7] can be adapted to give a fundamental set $R_A^{r_2,\delta}$ for the action of $\mathrm{SO}_A(\mathbb{R})$ on $V_A^{r_2,\delta}(\mathbb{R})$ (which could be empty) with the following properties:

1. The set $R_A^{r_2,\delta}$ is a semi-algebraic.
2. If $R_A^{r_2,\delta}(X)$ denotes the set of elements of height at most X, then the coefficients of elements $B \in R_A^{r_2,\delta}(X)$ are bounded by $O(X)$. The implied constant is independent of B.

We define an indicator function that records whether $V_A^{r_2,\delta}(\mathbb{R})$ is empty.

Definition 1.3.2. We define the indicator function

$$\chi_A(\delta) := \begin{cases} 1 & \text{if } V_A^{r_2,\delta}(\mathbb{R}) \neq \emptyset \\ 0 & \text{otherwise} \end{cases}.$$

We can build now build a cover of a fundamental domain for the action of $\mathrm{SO}_A(\mathbb{Z})$ on $V_A^{r_2,\delta}(\mathbb{R})$. To do so, we pick a fundamental domain $\mathcal{F}_A$ for the action of $\mathrm{SO}_A(\mathbb{Z})$ on $\mathrm{SO}_A(\mathbb{R})$ and act on $R_A^{r_2,\delta}$. This gives a $\sigma(r_2)$ cover of a fundamental domain for the action of $\mathrm{SO}_A(\mathbb{Z})$ where $\sigma(r_2) = 2^{r_1+r_2-1}$ is the size of the stabiliser in $\mathrm{SO}_A(\mathbb{R})$ of an element $v \in V_A^{r_2,\delta}(\mathbb{R})$.

Proposition 1.3.3. *Let $\mathcal{F}_A$ be a fundamental domain for the action of $\mathrm{SO}_A(\mathbb{Z})$ on $\mathrm{SO}_A(\mathbb{R})$. Then*

1. *If $\chi_A(\delta) = 1$, $\mathcal{F}_A \cdot R_A^{r_2,\delta}$ is an $\sigma(r_2)$–fold cover of a fundamental domain for the action of $\mathrm{SO}_A(\mathbb{Z})$ on $V_A^{r_2,\delta}(\mathbb{R})$, where we regard $\mathcal{F}_A \cdot R_A^{r_2,\delta}$ as a multiset.*
2. *If $\chi_A(\delta) = 0$, then $\emptyset$ is a fundamental domain.*

Proof. The stabiliser in $\mathrm{SO}_A(\mathbb{R})$ of an element $B \in V_A^{r_2,\delta}(\mathbb{R})$ coincides with the stabiliser in $\mathrm{SL}_n(\mathbb{R})$ of (A, B) which has size $\sigma(r_2)$. □

Remark 1.3.4. The characteristic functions will be used to define the Archimedean mass and will make the steps of the computation in Section 2.10 more transparent.

1.4 Averaging and cutting off the cusp

There are two distinct cases, the case where A is anisotropic over $\mathbb{Q}$ and the case where A is isotropic over $\mathbb{Q}$. In each case, we need to establish that: 1) the number of absolutely irreducible integral points in the cuspidal region is negligible, and 2) the number of reducible integral points in the main body is negligible.

We define absolutely irreducible points and reducible points and set the notation for the remainder of this section.

Definition 1.4.1. An element $v \in V(\mathbb{Z})$ is said to be absolutely irreducible if v does not correspond to the identity element in the class group and the resolvent of v corresponds to an order in an S_n-field. An element which is not absolutely irreducible is said to be reducible.

We have the following theorem which gives conditions on reducibility. It is a restatement of the criterion which appears in Ho–Shankar–Varma [29].

Theorem 1.4.2 (Reducibility criterion, [29])**.** *Let $(A, B) \in V(\mathbb{Z})$ be such that all the variables in one of the following sets vanish. Then (A, B) is reducible.*

1. ***The squares:*** $\left\{a_{ij}, b_{ij} | 1 \leq i, j \leq \frac{n-1}{2}\right\}$.
   These pairs correspond to the identity element in the class group.
2. ***The rectangles:*** $\{a_{ij}, b_{ij} | 1 \leq i \leq k, 1 \leq j \leq n-k\}$ *for some* $1 \leq k \leq n-1$.
   These pairs correspond to the resolvent having repeated roots.

Definition 1.4.3. Let A be a fixed quadratic form in $\mathscr{L}_{\mathbb{Z}}$ and fix $0 \leq b < n$. We let $V_A \subset V$ denote the space of pairs (A, B), where B is arbitrary. Note that the resolvent map takes V_A to U. Now, we let $V_{A,b}$ denote the inverse image under the resolvent map of the set U_b. It is easy to see that $V_{A,b}$ is an affine subspace of V_A of dimension $\frac{n(n+1)}{2} - 1$.

Definition 1.4.4. Let $S \subset V_{A,b}^{r_2;\delta}(\mathbb{Z}) := V_{A,b}^{r_2;\delta}(\mathbb{R}) \cap V_{A,b}(\mathbb{Z})$ be an $\mathrm{SO}_A(\mathbb{Z})$ invariant set. Denote by $N(S;X)$ the number of absolutely irreducible $\mathrm{SO}_A(\mathbb{Z})$-orbits on S that have height bounded by X. For any $L \subset V_A(\mathbb{Z})$, let L^{irr} denote the set of absolutely irreducible elements. Note that any absolutely irreducible element has a resolvent form corresponding to an order $\mathcal{O}$ in an S_n-number field and so $\mathcal{O}^\times[2]_{N\equiv 1}$ is trivial. As a result, the stabiliser in $\mathrm{SO}_A(\mathbb{Z})$ of absolutely irreducible elements is trivial.

Therefore, we have

$$N(S;X) = \frac{1}{\sigma(r_2)} \#\{\mathcal{F}_A \cdot R_A^{r_2,\delta}(X) \cap S^{\mathrm{irr}}\}.$$

The goal of this section is to obtain an asymptotic formula for $N_H(S;X)$.

1.4.1 The case of A anisotropic over $\mathbb{Q}$

When A is anisotropic, we can pick a compact fundamental domain $\mathcal{F}_A$ for the action of $\mathrm{SO}_A(\mathbb{Z})$ on $\mathrm{SO}_A(\mathbb{R})$. It then follows that $\mathcal{F}_A \cdot R_{A,b}^{r_2,\delta}$ is bounded. To estimate the number of absolutely irreducible integral points in the fundamental domain for the action of $SO_A(\mathbb{Z})$ on $V_{A,b}^{r_2,\delta}$, we can apply results from the geometry of numbers directly. The goal here is to use Davenport's refinement of the Lipschitz method on $\mathcal{F}_A \cdot R_{A,b}^{r_2,\delta}(X)$ to obtain the desired asymptotic formula.

We will need the following version of Davenport's lemma.

Lemma 1.4.5 (Davenport's Lemma)**.** *Let $E \subset \mathbb{R}^n$ be a bounded semi-algebraic multiset with maximum multiplicity at most m which is defined by k algebraic inequalities of each having degree at most l. Let E' be the image of E under any upper/lower triangular unipotent transformation. Then the number of integral points in E' counted with multiplicity is*

$$\mathrm{Vol}(E) + O_{m,k,l}\left(\max\{\mathrm{Vol}(\overline{E}), 1\}\right)$$

where $\mathrm{Vol}(\overline{E})$ denotes the greatest d-dimensional volume of a projection of E onto a d-dimensional coordinate hyperplane for $1 \le d \le n-1$.

Remark 1.4.6. We note that although Davenport's lemma holds in the more general setting of o-minimal structures, the most common use is in the semi-algebraic setting.

Lemma 1.4.7. *The number of integral points in $\mathcal{F}_A \cdot R_{A,b}^{r_2;\delta}$ which are not absolutely irreducible is bounded by $o\left(X^{\frac{n(n+1)}{2}-1}\right)$.*

Proof. We may write

$$V(\mathbb{Z}) = \left(\cup V(\mathbb{Z})^{\neq k}\right) \bigcup V(\mathbb{Z})^{\mathrm{red}},$$

where $V(\mathbb{Z})^{\mathrm{red}}$ denotes elements which are reducible in the sense of Theorem 1.4.2.

Fix a prime p. Let $V(\mathbb{F}_p)^{=k}$ denote the set of elements whose resolvent factors into a product of an irreducible factor of degree k and $n-k$ distinct linear factors. Let $V(\mathbb{F}_p)^{\mathrm{irr}}$

denote the set of elements of $V(\mathbb{F}_p)^{\mathrm{irr}}$ with the property that every lift to $V(\mathbb{Z})$ does not belong to $V(\mathbb{Z})^{\mathrm{red}}$. We obtain the same estimates as in Ho–Shankar–Varma, and this finishes the proposition. □

Theorem 1.4.8. *Let $A \in \mathscr{L}_{\mathbb{Z}}$ be anisotropic over $\mathbb{Q}$. We have*

$$N(V^{r_2,\delta}_{A,b}(\mathbb{Z});X) = \frac{1}{\sigma(r_2)}\mathrm{Vol}\left(\mathcal{F}_A \cdot R^{r_2,\delta}_{A,b}(X)\right) + o(X^{\frac{n(n+1)}{2}-1}).$$

1.4.2 The case of A isotropic over $\mathbb{Q}$

Suppose now that A is isotropic over $\mathbb{Q}$. Then there exists for some unique pair p, q such that $n = p + q$ and $\frac{n-1}{2} \equiv q \mod 2$, there exists an element $g_A \in \mathrm{SL}_n(\mathbb{Q})$ such that $g_A^t A g_A = A_{pq}$ where

$$A_{pq} := \begin{pmatrix} & & & & & 1 \\ & & & & \iddots & \\ & & & 1 & & \\ & & \pm I_{|p-q|} & & & \\ & 1 & & & & \\ \iddots & & & & & \\ 1 & & & & & \end{pmatrix}.$$

The ± on the identity block is determined by the sign of $p - q$. We define m to be the minimum of p and q, $m = \min\{p, q\}$.

Remark 1.4.9. In general, (n-monogenic or even), we can take A to a matrix of the form above over $\mathbb{Q}$ with the identity block replaced by an anisotropic quadratic form over $\mathbb{Q}$ having the same determinant as A and in diagonal form.

Now for $K = \mathbb{R}$ or $\mathbb{Q}$, we consider the maps

$$\begin{aligned} \sigma_V &\colon V^{r_2,\delta}_{A,b} \to V^{r_2,\delta}_{A_{pq},b} \\ \sigma_A &\colon \mathrm{SO}_A(K) \to \mathrm{SO}_{A_{pq}}(K) \end{aligned}$$

defined by $\sigma_V(A, B) = (A_{pq}, g_A^t B g_A)$ and $\sigma_A(h) = g_A^t h (g_A^t)^{-1}$. We note that

$$H(A, B) = H(\sigma_V(A, B))$$

since $\pi \circ \sigma_V = \pi$. Furthermore, $\sigma_V(h \cdot v) = \sigma_A(h) \cdot \sigma_V(v)$.

Now, we denote by $\mathcal{L} \subset V^{r_2,\delta}_{A_{pq},b}(\mathbb{R})$ the lattice $\sigma_V\left(V^{r_2,\delta}_{A_{pq},b}(\mathbb{Z})\right)$. We denote by $\Gamma \subset \mathrm{SO}_{A_{pq}}(\mathbb{R})$ the subgroup $\sigma_A(\mathrm{SO}_A(\mathbb{Z}))$. This subgroup is commensurable with $\mathrm{SO}_{A_{pq}}(\mathbb{Z})$. Therefore, there exists a fundamental domain $\mathcal{F}$ for the action of Γ on $\mathrm{SO}_{A_{pq}}(\mathbb{R})$ which is contained in a finite union of $\mathrm{SO}_{A_{pq}}(\mathbb{Q})$ translates of a Siegel domain, $\bigcup_i g_i\mathcal{S}$ for $g_i \in \mathrm{SO}_{A_{pq}}(\mathbb{Q})$. This is known from [17].

The choice of the standard A_{pq} as above is convenient at this point. Indeed, we may now choose as our Siegel domain $\mathcal{S}$, the product NTK where we choose K to be compact, N to be a subgroup of the group of lower triangular matrices with 1 on the diagonal and T to be

$$T := \left\{ \begin{pmatrix} t_1^{-1} & & & & & & \\ & \ddots & & & & & \\ & & t_m^{-1} & & & & \\ & & & I_{|p-q|} & & & \\ & & & & t_m & & \\ & & & & & \ddots & \\ & & & & & & t_1 \end{pmatrix} : t_1/t_2 > c, \dots, t_{m-1}/t_m > c, t_m > c \right\}$$

for some constant $c > 0$. This can be found in many sources, see for instance [16], [38], or [37].

Note that $s_i = t_i/t_{i+1}$, $0 \leq i \leq m-1$ and $s_m = t_m$ forms a set of simple roots. Moreover, if we denote by e^ρ the exponential of the half sum of the positive roots counted with multiplicities, we have

$$\begin{aligned} e^{\rho(H)} &= \prod_{i=1}^m t_i^{\frac{p+q}{2}-i} \\ &= \prod_{i=1}^m \left(\prod_{j=i}^m s_j \right)^{\frac{p+q}{2}-i} \\ &= \prod_{i=1}^m s_i^{\left(\sum_{j=1}^i \frac{p+q}{2}-j\right)} \\ &= \prod_{i=1}^m s_i^{i\left(\frac{p+q-i-1}{2}\right)}. \end{aligned}$$

We now fix some notation for our choice of Haar measure on $G = \mathrm{SO}_{A_{pq}}$. We let dg denote the Haar measure on G, dn denote the Haar measure on the unipotent group N, and dk denote the Haar measure on the compact group K. For every $1 \leq i \leq m$ we write $d^\times t_i = \frac{dt_i}{t_i}$ and $d^\times s_i = \frac{ds_i}{s_i}$. Furthermore, we write $dt = \prod_{i=1}^m dt_i$, $d^\times t = \prod_{i=1}^m d^\times t_i$ and $ds = \prod_{i=1}^m ds_i$, $d^\times s = \prod_{i=1}^m d^\times s_i$.

Changing variables between the t-coordinates and the s-coordinates gives us

$$dt = \left(\prod_{i=1}^m s_i^{i-1} \right) ds.$$

We thus find

$$d^\times t = \frac{1}{t_1 \cdots t_m} dt$$

$$\begin{aligned}
&= \frac{1}{\prod_{i=1}^{m} s_i^i}\left(\prod_{i=1}^{m} s_i^{i-1}\right) ds \\
&= \frac{1}{s_1 \cdots s_m} ds \\
&= d^\times s.
\end{aligned}$$

Therefore, the Haar measure is given in NAK-coordinates by

$$\begin{aligned}
dg &= e^{-2\rho(H)} du\, d^\times t\, dk \\
&= \prod_{i=1}^{m} t_i^{2i-p-q} du\, d^\times t\, dk \\
&= \prod_{i=1}^{m} s_i^{i(i+1-p-q)} du\, d^\times s\, dk.
\end{aligned}$$

We define the main body and the cuspidal region of the multiset $\mathcal{F}_A \cdot R_{A,b}^{r_2,\delta}$.

Definition 1.4.10 (Main body and cuspidal region)**.** The *main body* consists of all the elements of $\mathcal{F}_A \cdot R_{A,b}^{r_2,\delta}$ for which $|b_{11}| \geq 1$. The *cuspidal region* consists of all the elements for which $|b_{11}| < 1$.

We are now ready to cut off the cuspidal region.

Construction 1.4.11 (Partial order on the coordinates of V_A)**.** We construct a partial order on the $n(n+1)/2$ coefficients $\{b_{ij}\}$ for $i \leq j$. These define a set of coordinates on B which we denote by U.

The partial order records the scaling of the different elements of B under the action of the torus.

Definition 1.4.12. The weight $w(b_{ij})$ of an element $b_{ij} \in U$ is the factor by which b_{ij} scales under the action of $(t_1^{-1}, \ldots, t_m^{-1}, 1, \ldots, 1, t_m, \ldots, t_1) \in T$.

We compute the weights in both the t-coordinates and the s-coordinates on T, recalling that $i \leq j$:

1) $w(b_{11}) = t_1^{-2} = s_1^{-2} \cdots s_m^{-2}$;

2) $w(b_{ij}) = t_i^{-1} t_j^{-1} = s_i^{-1} \cdots s_{j-1}^{-1} s_j^{-2} \cdots s_n^{-2}$ if $i \leq m$ and $j \leq m$;

3) $w(b_{ij}) = t_i^{-1} = s_i^{-1} \cdots s_n^{-1}$ if $i \leq m$ and $m+1 \leq j \leq m+|p-q|$;

4) $w(b_{ij}) = t_i^{-1} t_{n-j+1} = s_i^{-1} \cdots s_{n-j}^{-1}$ if $i \leq m$ and $m+|p-q|+1 \leq j \leq n$;

5) $w(b_{ij}) = 1$ if $m+1 \leq i \leq m+|p-q|$ and $m+1 \leq j \leq m+|p-q|$;

6) $w(b_{ij}) = t_{n-j+1} = s_{n-j+1} \cdots s_n$ if $m+1 \leq i \leq m+|p-q|$ and $m+|p-q|+1 \leq j \leq n$;

7) $w(b_{ij}) = t_{n-i+1}t_{n-j+1} = s_{n-i+1}\cdots s_{n-j}s_{n-j+1}^2\cdots s_n^2$ if $m+|p-q|+1 \leq i \leq n$ and $m+|p-q|+1 \leq j \leq n$.

We are now ready to define a partial order on U.

Definition 1.4.13 (A partial order on subsets of U)**.** Let b and b' be two elements of the set of coordinates U. We say that $b \prec b'$ if in the expression for $w(b)$ in the s-coordinates, the exponents of the variables $s_1, \cdots, s_m$ are smaller than or equal to the corresponding exponents appearing in the expression for $w(b')$ in the s-coordinates. The relation $\prec$ defines a partial order on U.

Example 1.4.14. We have $b_{11} \prec b_{m+1\,m+1}$ because $w(b_{11}) = s_1^{-2}\cdots s_m^{-2}$ while $w(b_{m+1\,m+1}) = 1 = s_1^0\cdots s_m^0$. On the other hand, $b_{1\,n-2}$ and $b_{2\,n-3}$ cannot be compared in $\prec$ because $w(b_{1\,n-2}) = s_1^{-1}s_2^{-1}$ while $w(b_{2\,n-3}) = s_2^{-1}s_3^{-1}$. The important thing to note about the partial order $(U, \prec)$ is that if $i \leq i'$ and $j \leq j'$ then

$$b_{ij} \prec b_{i'j'}.$$

We now take a closer look at the process of cutting off the cusp in a specific case before moving on to the general case.

Example 1.4.15 (Base case of cusp cutting induction for $|p-q| > 1$)**.** As the first non-trivial interesting example, let us consider the case $n = 5$, $m = 1$. Then $A_{1\,4}$ is given by

$$A_{1\,4} = \begin{pmatrix} & & & & 1 \\ & -1 & & & \\ & & -1 & & \\ & & & -1 & \\ 1 & & & & \end{pmatrix}.$$

The torus is

$$T = \left\{ \begin{pmatrix} t^{-1} & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & t \end{pmatrix} : t > c \right\}.$$

The s-coordinates are the same as the t-coordinates and the Haar measure takes the form

$$dg = du\,\frac{1}{t^3}d^\times t\,dk.$$

We now record how elements of the torus act on elements of $K \cdot R^{r_2,\delta}_{A_{1\,4},b}(X)$. Remember that the action of $G = \mathrm{SO}_{A_{1\,4}}$ is given by conjugation $g \cdot v = gvg^t$. Letting T act on $K \cdot R^{r_2,\delta}_{A_{1\,4},b}(X)$

we find

$$t\cdot v=\begin{pmatrix} t^{-2} & t^{-1} & t^{-1} & t^{-1} & 1\\ t^{-1} & 1 & 1 & 1 & t\\ t^{-1} & 1 & 1 & 1 & t\\ t^{-1} & 1 & 1 & 1 & t\\ 1 & t & t & t & t^2 \end{pmatrix} O(X).$$

From this, it is easy to read off the weights.

Finally, the elements of the group N have the form:

$$\begin{pmatrix} A_1 & & \\ B_2 & I_{|p-q|} & \\ C & B_3 & A_3 \end{pmatrix}$$

where A_1 and A_2 are lower triangular with 1s on the diagonal and there are relations among A_1, A_3, B_2, B_3 and C.

For any subset of U containing b_{11}, we now want to estimate

$$\widetilde{I}(U_1,X)=X^{14-\#U_1}\int_{t\in T_X}\prod_{b_{ij}\notin U_1} w(b_{ij})\frac{d^\times t}{t^3}.$$

For this example, we can do this very concretely. Remember that in T_X we have the bound $t<CX$. We calculate some values to get a better feel for the situation. We have:

$$\widetilde{I}(\emptyset,X)=X^{14}\int_{t=c}^{CX}\frac{d^\times t}{t^3}=X^{14}\int_{t=c}^{CX}\frac{dt}{t^4}=O(X^{14}),$$

as expected.

If U_1 is any subset of the middle block, we also obtain

$$\widetilde{I}(U_1,X)=X^{14-\#U_1}\int_{t=c}^{CX}\frac{d^\times t}{t^3}=X^{14}\int_{t=c}^{CX}\frac{dt}{t^4}=O(X^{11-\#U_1}).$$

Now, let us examine strict subsets of the first ending at the off-anti-diagonal. By the monotonicity structure of $\prec$, we only need to find three different integrals.

$$\begin{aligned}
\widetilde{I}(\{b_{11},b_{12},b_{13}\},X) &= X^{11}\int_{t=c}^{CX} t^4\frac{d^\times t}{t^3}=X^{11}\int_{t=c}^{CX} dt=O(X^{12})\\
\widetilde{I}(\{b_{11},b_{12}\},X) &= X^{12}\int_{t=c}^{CX} t^3\frac{d^\times t}{t^3}=X^{12}\int_{t=c}^{CX}\frac{dt}{t}=O(X^{12}\ln X)=O_\epsilon(X^{12+\epsilon})\\
\widetilde{I}(\{b_{11}\},X) &= X^{13}\int_{t=c}^{CX} t^2\frac{d^\times t}{t^3}=X^{13}\int_{t=c}^{CX}\frac{dt}{t^2}=O(X^{13})
\end{aligned}$$

Therefore,

$$N(V_A(\mathbb{Z})(U_1);X)=O_\epsilon\left(X^{13+\epsilon}\right)$$

for all $U_1 \subset U$ such that $b_{11} \in U_1$. The number of absolutely irreducible elements in the cusp which have height at most X is thus $O_\epsilon(X^{14-1+\epsilon})$ and we have cut off the cusp!

Example 1.4.16 (Base case of cusp cutting induction for $|p-q|=1$)**.** We now do the case $n=5$, $m=2$ before moving on to cutting off the cusp in the general case. We see that torus elements act as follows:

$$t \cdot v = \begin{pmatrix} t_1^{-2} & t_1^{-1}t_2^{-1} & t_1^{-1} & t_1^{-1}t_2 & 1 \\ t_2^{-1}t_1^{-1} & t_2^{-2} & t_2^{-1} & 1 & t_2^{-1}t_1 \\ t_1^{-1} & t_2^{-1} & 1 & t_2 & t_1 \\ t_2t_1^{-1} & 1 & t_2 & t_2^2 & t_2t_1 \\ 1 & t_1t_2^{-1} & t_1 & t_1t_2 & t_1^2 \end{pmatrix} O(X).$$

From this, it is easy to read off the weights. The Haar measure takes the form

$$dg = du\, \frac{1}{t_1^3 t_2} d^\times t\, dk = du\, \frac{1}{s_1^3 s_2^4} d^\times s\, dk.$$

For any subset of U containing b_{11}, we now want to estimate

$$\widetilde{I}(U_1, X) = X^{14-\#U_1} \int_{t \in T_X} \prod_{b_{ij} \notin U_1} w(b_{ij}) \frac{d^\times s}{s_1^3 s_2^4}.$$

We only need to look at proper subsets of $U_0 = \{b_{11}, b_{12}, b_{13}, b_{22}\}$ which are left-closed and up-closed. In this case we can exclude the subset $\{b_{11}, b_{12}, b_{22}\}$ by the ***Squares*** part of the criterion for irreducibility. and recall that we have the bound $s_1, s_2 < CX$. Let's compute:

$$\begin{aligned} \widetilde{I}(\{b_{11}\}, X) &= X^{13} \int_{s_1,s_2=c}^{CX} s_1^2 s_2^2 \frac{d^\times s}{s_1^3 s_2^4} = X^{13} \int_{s_1,s_2=c}^{CX} \frac{d^\times s}{s_1 s_2^2} = O(X^{13}) \\ \widetilde{I}(\{b_{11}, b_{12}\}, X) &= X^{12} \int_{s_1,s_2=c}^{CX} s_1^3 s_2^4 \frac{d^\times s}{s_1^3 s_2^4} = X^{12} \int_{s_1,s_2=c}^{CX} d^\times s = O_\epsilon(X^{12+\epsilon}) \\ \widetilde{I}(\{b_{11}, b_{12}, b_{13}\}, X) &= X^{11} \int_{s_1,s_2=c}^{CX} s_1^4 s_2^5 \frac{d^\times s}{s_1^3 s_2^4} = X^{11} \int_{s_1,s_2=c}^{CX} s_1 s_2 d^\times s = O_\epsilon(X^{13+\epsilon}) \\ \widetilde{I}(\{b_{11}, b_{12}, b_{22}\}, X) &= X^{11} \int_{s_1,s_2=c}^{CX} s_1^3 s_2^6 \frac{d^\times s}{s_1^3 s_2^4} = X^{11} \int_{s_1,s_2=c}^{CX} s_2^2 d^\times s = O_\epsilon(X^{13+\epsilon}). \end{aligned}$$

The number of absolutely irreducible elements in the cusp which have height at most X is thus $O_\epsilon(X^{14-1+\epsilon})$ and we have cut off the cusp!

We recall that we had

$$N_H(S; X) = \frac{1}{\sigma(r_2)} \#\{\mathcal{F}_A \cdot R_A^{r_2,\delta}(X) \cap S^{\mathrm{irr}}\}.$$

Now, let G_0 be a bounded open K-invariant ball in $\mathrm{SO}_{A_{pq}}(\mathbb{R})$. We can average the above expression by the usual trick to obtain

$$N_H(S;X) = \frac{1}{\sigma(r_2)\mathrm{Vol}(G_0)} \int_{h\in\mathcal{F}_A} \#\left\{hG_0R_A^{r_2,\delta}(X)\cap S^{\mathrm{irr}}\right\} dh.$$

Now, again we may use classical arguments to see that the number of absolutely irreducible integral points in the cusp which have height at most X is

$$O\left(\int_{t\in T} \#\left\{tG_0R_A^{r_2,\delta}(X)\cap S^{\mathrm{irr}}\right\} \prod_{i=1}^{m} s_i^{i(i+1-p-q)} d^\times s\right).$$

Definition 1.4.17. Let $U_1 \subset U$ be a subset of the set of coordinates. We define

$$V_A(\mathbb{R})(U_1) = \{B \in V_A(\mathbb{R})\colon\ |b_{ij}(B)| < 1 \text{ if and only if } b_{ij} \in U_1\}$$

and

$$V_A(\mathbb{Z})(U_1) = V_A(\mathbb{Z}) \cap V_A(\mathbb{R})(U_1).$$

It thus suffices to show that

$$N(V_A(\mathbb{Z})(U_1);X) = O_\epsilon\left(X^{\left(\frac{n(n+1)}{2}-1\right)-1+\epsilon}\right)$$

for all $U_1 \subset U$ such that $b_{11} \in U_1$.

We now explain how the description of reducible elements gives us a priori bounds on the coordinates s_i. Let C be an absolute constant such that CX bounds the absolute value of all the coordinates of elements $B \in G_0R_A^{r_2,\delta}(X)$.

If $(s_1^{-1},\ldots,s_m^{-1},1,\ldots,1,s_m,\ldots,s_1) \in T$ and $CXw(b_{i_0\, n-i_0}) < 1$ for some $i_0 \in \{1,\ldots,m\}$, then $CXw(b_{ij}) < 1$ for all $i \le i_0$ and $j \le n-i_0$. This comes from the ***Rectangles*** part of the criterion for reducibility. Therefore, we may assume that

$$s_i < CX$$

for all $i \in \{1,\ldots,m\}$.

Let us write T_X to denote the set of $t = (s_1^{-1},\ldots,s_m^{-1},1,\ldots,1,s_m,\ldots,s_1) \in T$ which satisfy this condition.

Now Davenport's lemma gives us

$$\begin{aligned} N(V(\mathbb{Z})(U_1);X) &= O\left(\int_{t\in T_X} \mathrm{Vol}(tG_0R_A^{r_2,\delta}(X)\cap V(\mathbb{R})(U_1)) \prod_{i=1}^{m} s_i^{i(i+1-p-q)} d^\times s\right) \\ &= O\left(X^{\left(\frac{n(n+1)}{2}-1\right)-\#U_1} \int_{t\in T_X} \prod_{b_{ij}\notin U_1} w(b_{ij}) \prod_{i=1}^{m} s_i^{i(i+1-n)} d^\times s\right). \end{aligned}$$

So, we have reduced our problem to one of estimating the following integrals.

Definition 1.4.18. The active integral of $U_1 \subset U$ is defined by

$$\widetilde{I}(U_1, X) := X^{\left(\frac{n(n+1)}{2}-1\right)-\#U_1} \int_{t \in T_X} \prod_{b_{ij} \notin U_1} w(b_{ij}) \prod_{i=1}^{m} s_i^{i(i+1-n)} d^\times s.$$

Recall, that $b_{ij} \prec b_{i_0 j_0}$ when $i \leq i_0$ and $j \leq j_0$. Therefore, if $U_1 \subset U$ contains $b_{i_0 j_0}$ but not b_{ij}, then

$$\widetilde{I}\left(U_1 \setminus \{b_{i_0 j_0}\} \cup \{b_{ij}\}, X\right) \geq \widetilde{I}(U_1, X).$$

As a result, in order to obtain an upper bound for $\widetilde{I}(U_1, X)$ we may assume that if $b_{i_0 j_0} \in U_1$, then $b_{ij} \in U_1$ for all $i \leq i_0$ and $j \leq j_0$.

Furthermore, suppose U_1 contains any element on, or on the right of, the off anti-diagonal within the first m-rows. In that case, we are in the case of ***Rectangles*** in the criterion for reducibility and so $N(V(\mathbb{Z})(U_1); X) = 0$.

Definition 1.4.19. We define the subset $U_0 \subset U$ as the set of coordinates b_{ij} such that $i \leq j$, $i \leq m$, and $i + j \leq n - 1$.

Now, if $|p - q| = 1$, every element in $V(\mathbb{Z})(U_0)$ is reducible and it suffices to consider $\widetilde{I}(U_1, X)$ for all $U_1 \subsetneq U_0$. On the other hand if $|p - q| > 1$ we need to consider all $U_1 \subset U$.

Since the product of the weight over all the coordinates is 1, we make the following definition.

Definition 1.4.20. We define for a subset $U_1 \subset U$

$$I(U_1, X) = X^{\frac{n(n+1)}{2}-1} \widetilde{I}(U_1, X) = X^{-\#U_1} \int_{t \in T_X} \prod_{b_{ij} \in U_1} w(b_{ij})^{-1} \prod_{i=1}^{m} s_i^{i(i+1-n)} d^\times s.$$

We are now ready to states and prove the main cusp cutting lemma.

Lemma 1.4.21 (Main cusp cutting estimate)**.** *Let U_1 be a non-empty proper subset of U_0. Then we have the estimate*

$$I(U_1, X) = O_\epsilon\left(X^{-1+\epsilon}\right).$$

We also have $I(\emptyset) = O(1)$ and $I(U_0) = O\left(X^{m(2m+1-n)+\epsilon}\right)$.

Proof. We prove this lemma via a combinatorial argument using induction on m. Recall that $n = 2m + |p - q|$. The cases $|p - q| = 1$ and $|p - q| > 1$ turn out to be slightly different. We handle them separately.

To start, let us assume that $|p - q| > 1$. First, we compute $I(U_0, X)$

$$\begin{aligned} I(U_0, X) &= X^{-\#U_0} \int_{t \in T_X} \prod_{b_{ij} \in U_0} w(b_{ij})^{-1} \prod_{i=1}^{m} s_i^{i(i+1-n)} d^\times s. \\ &= X^{-m(n-(m+1))} \int_{t \in T_X} \left(t_1^{n-2+1} t_2^{n-4+2} t_3^{n-6+2} \cdots t_m^{n-2m+2}\right) \prod_{i=1}^{m} t_i^{2i-n} d^\times t \end{aligned}$$

$$
\begin{aligned}
&= X^{-m(n-(m+1))} \int_{t\in T_X} t_1 t_2^2 \cdots t_m^2 d^\times t \\
&= X^{-m(n-(m+1))} \int_{s_1,\ldots,s_m=c}^{CX} s_1 s_2^3 s_3^5 \cdots s_m^{2m-1} d^\times s \\
&= O\left(X^{-m(n-(m+1))+m^2}\right) \\
&= O\left(X^{m(2m+1-n)}\right) \\
&= O\left(X^{-m(|p-q|-1)}\right).
\end{aligned}
$$

We also compute $I(\emptyset, X)$ directly

$$
I(\emptyset, X) = \int_{s_1,\ldots,s_n=c}^{CX} \prod_{i=1}^{m} s_i^{i(i+1-n)} d^\times s = O(1).
$$

Now, let U_1' denote $U_0 \setminus U_1$. Define $I_m'(U_1', X) := I(U_1, X)$. Then we have:

$$
\begin{aligned}
I_m'(U_1', X) &= X^{\#U_1' - m(n-(m+1))} \int_{t\in T_X} \left(\prod_{b_{ij}\in U_1'} w(b_{ij}) \right) t_1 t_2^2 \cdots t_m^2 d^\times t. \\
&= X^{\#U_1' - m(n-(m+1))} \int_{s_1,\ldots,s_m=c}^{XC} \left(\prod_{b_{ij}\in U_1'} w(b_{ij}) \right) s_1 s_2^3 \cdots s_m^{2m-1} d^\times s.
\end{aligned}
$$

We now work out the base case of the induction. When $m = 1$, we have

$$
\begin{aligned}
I_1(\emptyset, X) &= O\left(1\right) \\
I_1(\{b_{11}\}, X) &= X^{-1} \int_{s_1=c}^{XC} s_1^2 s_1^{2-n} d^\times s = O_\epsilon\left(X^{-1+\epsilon}\right) \\
I_1(\{b_{11},\ldots,b_{1k}\}, X) &= X^{-k} \int_{s_1=c}^{XC} s_1^2 s_1^{k-1} s_1^{2-n} d^\times s = O_\epsilon\left(X^{-1+\epsilon}\right) \\
I_1(\{b_{11},\ldots,b_{1\,n-2}\}, X) &= X^{-n+2} \int_{s_1=c}^{XC} s_1 d^\times s = O_\epsilon\left(X^{1-|p-q|+\epsilon}\right) \\
I_1(U_0, X) &= O_\epsilon\left(X^{1-|p-q|+\epsilon}\right).
\end{aligned}
$$

In particular, we see that when $|p-q| > 1$, all these quantities are $O_\epsilon(X^{-1+\epsilon})$. We will use this estimate in the induction step.

Now, suppose that $m \geq 2$.

Now, for any decomposition $k = k_1 + k_2$ we have:

$$
\int_c^{CX} s^k d^\times s \ll_{c,C} \int_c^{CX} s^{k_1} d^\times s \int_c^{CX} s^{k_2} d^\times s.
$$

Consequently, we see that $I'_n(U'_1, X)$ is bounded by the product

$$I'_n(U'_1, X) \leq J_m(U'_2, X)\, K_m(U'_3, X),$$

where U'_2 consist of all the elements of U'_1 in the first row, U'_3 consists of the rest of the elements of U'_1, and

$$\begin{aligned} J_m(U'_2, X) \ &= \left(X^{\#U'_2-(n-2)} \int_{s_1,\ldots,s_n=c}^{CX} \left(\prod_{b_{1j}\in U'_2} w(b_{1j}) \right) s_1 s_2^2 \cdots s_m^2 d^\times s \right) \\ K_m(U'_3, X) &= \left(X^{\#U'_3-\#U_0+(n-2)} \int_{s_2,\ldots,s_n=c}^{CX} \left(\prod_{b_{ij}\in U'_3} w(b_{ij}) \right) s_2 s_3^3 \cdots s_m^{2m-3} d^\times s \right). \end{aligned}$$

Note that $K_m(U'_3, X) = I_{m-1}(U'_3, X)$ and we can estimate it by induction. Now, U_1 is left-closed and non-empty and hence the subset U'_2 is either empty or of the form $\{b_{1\,k}, \ldots, b_{1\,n-2}\}$ for $k \geq 2$.

Now, if $U'_2 = \emptyset$:

$$J_m(U'_2, X) = X^{2-n} \int_{s_1,\ldots,s_n=c}^{CX} s_1 s_2^2 \cdots s_m^2 d^\times s = O_\epsilon\left(X^{2m-1-n+2}\right) = O_\epsilon\left(X^{1-|p-q|+\epsilon}\right) = O_\epsilon\left(X^{-1+\epsilon}\right).$$

Now, if $k = 2$, then:

$$\begin{aligned} J_m(U'_2, X) &= X^{-1} \int_{s_1,\ldots,s_n=c}^{CX} t_1^{3-n} t_2^{-1} s_1 s_2^2 \cdots s_m^2 d^\times s \\ &= X^{-1} \int_{s_1,\ldots,s_n=c}^{CX} s_1^{3-n} s_2^{3-n} \cdots s_m^{3-n} s_2^{-1} \cdots s_m^{-1} s_1 s_2^2 \cdots s_m^2 d^\times s \\ &= X^{-1} \int_{s_1,\ldots,s_n=c}^{CX} s_1^{3-n} s_2^{3-n} \cdots s_m^{3-n} s_1 s_2 \cdots s_m d^\times s \\ &= X^{-1} \int_{s_1,\ldots,s_n=c}^{CX} s_1^{4-n} s_2^{4-n} \cdots s_m^{4-n} d^\times s \\ &= O_\epsilon(X^{-1+\epsilon}) \end{aligned}$$

Now, if $k = 3$, then:

$$\begin{aligned} J_m(U'_2, X) &= X^{-2} \int_{s_1,\ldots,s_n=c}^{CX} t_1^{4-n} s_1 s_2^2 \cdots s_m^2 d^\times s \\ &= X^{-2} \int_{s_1,\ldots,s_n=c}^{CX} s_1^{4-n} s_2^{4-n} \cdots s_m^{4-n} s_1 s_2^2 \cdots s_m^2 d^\times s \\ &= X^{-2} \int_{s_1,\ldots,s_n=c}^{CX} s_1^{5-n} s_2^{6-n} \cdots s_m^{6-n} d^\times s \\ &= O_\epsilon\left(X^{-2+\epsilon}\right). \end{aligned}$$

If $4 \leq k \leq m$, then:

$$\begin{aligned}
J_m(U_2', X) &= X^{1-k} \int_{s_1,\ldots,s_n=c}^{CX} t_1^{-((n-2)-k+1)} t_k^{-1} \cdots t_m^{-1} t_m \cdots t_3 s_1 s_2^2 \cdots s_m^2 d^\times s \\
&= X^{1-k} \int_{s_1,\ldots,s_n=c}^{CX} t_1^{-((n-2)-k+1)} t_3 \cdots t_{k-1} s_1 s_2^2 \cdots s_m^2 d^\times s \\
&= X^{1-k} \int_{s_1,\ldots,s_n=c}^{CX} t_1^{-((n-2)-k+1)} s_3 s_4^2 \cdots s_{k-1}^{k-3} s_1 s_2^2 \cdots s_m^2 d^\times s \\
&= X^{1-k} \int_{s_1,\ldots,s_n=c}^{CX} t_1^{-((n-2)-k+1)} s_1 s_2^2 s_3^3 s_4^4 s_{k-1}^{k-1} s_k^2 \cdots s_m^2 d^\times s \\
&= O_\epsilon(X^{1-k+\epsilon}).
\end{aligned}$$

If $m+1 \leq k < m + |p-q|$, then:

$$\begin{aligned}
J_m(U_2', X) &= X^{1-k} \int_{s_1,\ldots,s_n=c}^{CX} t_1^{-((n-2)-k+1)} t_m \cdots t_3 s_1 s_2^2 \cdots s_m^2 d^\times s \\
&= X^{1-k} \int_{s_1,\ldots,s_n=c}^{CX} t_1^{-((n-2)-k+1)} t_3 \cdots t_m s_1 s_2^2 \cdots s_m^2 d^\times s \\
&= X^{1-k} \int_{s_1,\ldots,s_n=c}^{CX} t_1^{-((n-2)-k+1)} s_3 s_4^2 \cdots s_m^{m-2} s_1 s_2^2 \cdots s_m^2 d^\times s \\
&= X^{1-k} \int_{s_1,\ldots,s_n=c}^{CX} t_1^{-((n-2)-k+1)} s_1 s_2^2 s_3^3 s_4^4 \cdots s_m^m d^\times s \\
&= O_\epsilon(X^{1-k+\epsilon}).
\end{aligned}$$

If $m + |p-q| \leq k \leq n-2$, then:

$$\begin{aligned}
J_m(U_2', X) &= X^{1-k} \int_{s_1,\ldots,s_n=c}^{CX} t_1^{-((n-2)-k+1)} t_{n-2-k+3} \cdots t_3 s_1 s_2^2 \cdots s_m^2 d^\times s \\
&= X^{1-k} \int_{s_1,\ldots,s_n=c}^{CX} t_1^{-((n-2)-k+1)} t_3 \cdots t_{n-k+1} s_1 s_2^2 \cdots s_m^2 d^\times s \\
&= X^{1-k} \int_{s_1,\ldots,s_n=c}^{CX} t_1^{-((n-2)-k+1)} s_3 s_4^2 \cdots s_{n-k+1}^{n-k-1} s_{n-k+2}^{n-k-1} \cdots s_m^{n-k-1} s_1 s_2^2 \cdots s_m^2 d^\times s \\
&= X^{1-k} \int_{s_1,\ldots,s_n=c}^{CX} t_1^{-((n-2)-k+1)} s_1 s_2^2 s_3^3 s_4^4 \cdots s_{n-k+1}^{n-k+1} s_{n-k+2}^{n-k+1} \cdots s_m^{n-k+1} d^\times s \\
&= X^{1-k} \int_{s_1,\ldots,s_n=c}^{CX} s_1^{-(n-k)+1} s_2^{-(n-k)+1} \cdots s_m^{-(n-k)+1} s_1 s_2^2 s_3^3 s_4^4 \cdots s_{n-k+1}^{n-k+1} s_{n-k+2}^{n-k+1} \cdots s_m^{n-k+1} d^\times s \\
&= X^{1-k} \int_{s_1,\ldots,s_n=c}^{CX} s_1^{-(n-k)+2} s_2^{-(n-k)+3} \cdots s_{n-k-1}^0 s_{n-k}^1 s_{n-k+1}^2 \cdots s_m^2 d^\times s \\
&= O_\epsilon(X^{k-(n-2)-|p-q|+\epsilon}).
\end{aligned}$$

Therefore, in all cases we find

$$J_m(U_2', X) = O_\epsilon(X^{-1+\epsilon}).$$

The lemma now follows by induction on m used to bound $I'_{m-1}(U_3', X)$ by $O_\epsilon(X^{-1+\epsilon})$.

We now explain how to deal with the case $|p-q| = 1$. In this case, we will have to make use of the ***Squares*** part of the reducibility criterion. This will guarantee that $U_1 \neq U_0$. Here, in the base case $m = 1$ of the induction, we have that all the cases are $O(1)$. This is not a problem. By the ***Squares*** part of the reducibility criterion there are no irreducible elements in the cusp here. Thus, we can start the induction at $m = 2$. Example 3.16 shows that the estimates of $I(\emptyset, X) = O(1)$ and $O_\epsilon(X^{-1+\epsilon})$ for the rest does hold for this base case. Now, for $m \geq 3$ the rest of the estimates obtained above remain valid. That is

$$J_m(U_2', X) = O_\epsilon(X^{-1+\epsilon})$$

if $U_2' \neq \emptyset$, while $J_m(\emptyset, X) = O(1)$.

So we have to rewrite the induction step slightly. We do so as follows. If U_2' is non-empty, then the lemma follows by induction on m used to bound $I'_{m-1}(U_3', X)$ by $O_\epsilon(X^{\epsilon})$. If on the other hand U_2' is empty, then U_3' must be non-empty since U_1' is non-empty. This holds because the ***Squares*** part of the reducibility criterion implies that $U_1 \neq U_0$. If $U_3' \neq U_0 \setminus \{b_{1\,1}, \ldots, b_{1\,n-2}\}$, then by induction $I'_{m-1}(U_3', X) = O_\epsilon(X^{-1+\epsilon})$. So the last outstanding case is when $U_1 = \{b_{1\,1}, \ldots, b_{1\,n-2}\}$. In this case, a direct computation or an application of [8] gives the result. This completes the proof of the main cusp cutting lemma. □

Remark 1.4.22. The proof of the previous theorem was inspired by the induction argument of [39].

Remark 1.4.23. The proof shows that we get much better error terms for $I(U_1, X)$ than in the statement of the theorem.

Proposition 1.4.24. *The number of absolutely irreducible elements in the cusp which have height at most X is $O_\epsilon\left(X^{\left(\frac{n(n+1)}{2}-1\right)-1+\epsilon}\right)$.*

As in the anisotropic cases, we find that the number of reducible elements in the main body is negligible.

Lemma 1.4.25. *The number of integral points in the main body of $\mathcal{F}_A \cdot R_{A,b}^{r_2,\delta}$ which are not absolutely irreducible is bounded by $o\left(X^{\frac{n(n+1)}{2}-1}\right)$.*

Proof. The proof is identical to the anisotropic case. □

Theorem 1.4.26. *Let $A \in \mathscr{L}_{\mathbb{Z}}$ be isotropic over $\mathbb{Q}$. We have*

$$N(V_{A,b}^{r_2,\delta}(\mathbb{Z}); X) = \frac{1}{\sigma(r_2)}\mathrm{Vol}\left(\mathcal{F}_A \cdot R_{A,b}^{r_2,\delta}(X)\right) + o\left(X^{\frac{n(n+1)}{2}-1}\right).$$

Remark 1.4.27. By Witt's decomposition theorem, the results of this section hold in the odd N-monogenic case verbatim.

1.5 Sieving to very large and acceptable collections

In this section, we determine the asymptotic formulas for certain families of rings and fields. The results of this section are adaptations of those found in [29]. We begin with the definition of a family of local specifications. Fix $A \in \mathscr{L}_{\mathbb{Z}}$ and an integer $0 \leq b \leq n-1$.

Definition 1.5.1 (Collection of local specifications and the associated set)**.** We say that a family $\Lambda_{A,b} = (\Lambda_{A,b,\nu})_{\nu}$ of subsets $\Lambda_{A,b,\nu} \subset V_{A,b}(\mathcal{O}_{\nu})$ indexed by the places ν of $\mathbb{Q}$ is a **collection of local specifications** if: 1) for each finite prime p the set $\Lambda_{A,b,p} \subset V_{A,b}(\mathbb{Z}_p) \setminus \{\Delta = 0\}$ is an open subset which is non-empty and whose boundary has measure 0; and 2) at $\nu = \infty$, we have $\Lambda_{A,b,\infty} = V_{A,b}^{r_2,\delta}(\mathbb{R})$ for some integer r_2 with $0 \leq r_2 \leq \frac{n-1}{2}$ and $\delta \in \mathcal{T}(r_2)$. We associate the set $\mathcal{V}(\Lambda_{A,b}) := \{v \in V_{A,b}(\mathbb{Z})\colon \forall \nu \, (v \in \Lambda_{A,b,\nu})\}$ to the collection of local specifications $\Lambda_{A,b} = (\Lambda_{A,b,\nu})_{\nu}$.

1.5.1 Sieving to projective elements

Definition 1.5.2. For a prime p, we denote by $V_{A,b}(\mathbb{Z}_p)^{\mathrm{proj}}$ the set of elements $v \in V_{A,b}(\mathbb{Z}_p)$ which correspond to a projective pair (I, δ) (i.e. with the property that $I^2 = (\delta)$) under the parametrisation.

We have

$$V_{A,b}^{r_2,\mathrm{proj}}(\mathbb{Z}) = V_{A,b}^{r_2}(\mathbb{Z}) \bigcap \left(\bigcap_p V_{A,b}^{\mathrm{proj}}(\mathbb{Z}) \right).$$

Definition 1.5.3. We denote by $W_{A,b,p}$ the set of elements in $V_{A,b}(\mathbb{Z})$ that do not belong to $V_{A,b}^{\mathrm{proj}}(\mathbb{Z}_p)$.

We need estimates for the number of elements in $W_{A,b,p}$ for large p. We have the following theorem whose proof is an almost verbatim adaptation of the one presented in [29] to the case at hand.

Theorem 1.5.4. *We have*

$$N\left(\cup_{p\geq M} W_{A,b,p}, X\right) = O\left(\frac{X^{\frac{n(n+1)}{2}-1}}{M^{1-\epsilon}}\right) + o\left(X^{\frac{n(n+1)}{2}}\right)$$

where the implied constant is independent of X and M.

Proof. One shows just as in [29] that $W_{A,b,p} \subset V(\mathbb{Z}_p)$ is the pre-image of some subset of $V_{A,b}(\mathbb{F}_p)$ under the reduction modulo p map by using Nakayama's lemma. Making the necessary adjustments, the proof proceeds just as in [29], noting that the reduction modulo p of $W_{A,b,p}$ has codimension greater than 2 in $V_{A,b}(\mathbb{F}_p)$ (being non-projective modulo p and having discriminant divisible by p give at least 2 conditions). □

We now define the concept of *very large collections of local specifications* and state the asymptotic formula. Roughly, a collection of local specifications is very large if for large enough primes p, it includes all elements of V which are projective at p.

Definition 1.5.5 (Very large collection of local specifications)**.** Let $\Lambda_{A,b} = (\Lambda_{A,b,\nu})_\nu$ be a collection of local specifications. We say that $\Lambda_{A,b}$ is **very large** if for all but finitely many primes, the sets $\Lambda_{A,b,p}$ contains all projective elements of $V_{A,b}(\mathbb{Z}_p)$. If $\Lambda_{A,b}$ is very large, we also say that the associated set $\mathcal{V}(\Lambda_{A,b})$ is very large.

Theorem 1.5.6. *Let r_2 be an integer such that $0 \leq r_2 \leq \frac{n-1}{2}$ and let $\delta \in \mathcal{T}(r_2)$. Then for a very large collection of local specifications $\Lambda_{A,b}$ such that $\Lambda_{A,b,\infty} = V_{A,b}^{r_2,\delta}(\mathbb{R})$, we have*

$$N(\mathcal{V}(\Lambda_{A,b}^{\delta}), X) = \frac{1}{\sigma(r_2)} \mathrm{Vol}(\mathcal{F}_A \cdot R_{A,b}^{r_2,\delta}(X)) \prod_p \mathrm{Vol}(\Lambda_{A,b,p}) + o\left(X^{\frac{n(n-1)}{2}-1}\right),$$

where the volume of subsets of $V_{A,b}(\mathbb{R})$ are computed with respect to the Euclidean measure normalized so that $V_{A,b}(\mathbb{Z})$ has covolume 1 and the volumes of subsets of $V_{A,b}(\mathbb{Z}_p)$ are computed with respect to the Euclidean measure normalized so that $V_{A,b}(\mathbb{Z}_p)$ has measure 1.

1.5.2 Sieving to acceptable sets conditional on a tail estimate

We now define the concept of *acceptable collections of local specifications* and state the asymptotic formula. Roughly, a collection of local specifications is acceptable if for large enough primes p, it includes all fields with discriminant indivisible by p^2.

Definition 1.5.7 (Acceptable collection of local specifications)**.** Let $\Lambda_{A,b} = (\Lambda_{A,b,\nu})_\nu$ be a collection of local specifications. We say that $\Lambda_{A,b}$ is **acceptable** if for all but finitely many primes, the set $\Lambda_{A,b,p}$ contains all elements of $V_{A,b}(\mathbb{Z}_p)$ whose discriminant is not divisible by p^2. If $\Lambda_{A,b}$ is acceptable, we also say that the associated set $\mathcal{V}(\Lambda_{A,b})$ is acceptable.

We have the following unconditional asymptotic inequality.

Theorem 1.5.8. *Let $\Lambda_{A,b} = (\Lambda_{A,b,\nu})_\nu$ be an acceptable collection of local specifications.*

$$N(\mathcal{V}(\Lambda_{A,b}), X) \leq \frac{1}{\sigma(r_2)} \mathrm{Vol}(\mathcal{F}_A \cdot R_{A,b}^{r_2,\delta}(X)) \prod_p \mathrm{Vol}(\Lambda_{A,b,p}) + o\left(X^{\frac{n(n+1)}{2}-1}\right),$$

where the volume of subsets of $V_{A,b}(\mathbb{R})$ are computed with respect to the Euclidean measure normalized so that $V_{A,b}(\mathbb{Z})$ has covolume 1 *and the volumes of subsets of $V_{A,b}(\mathbb{Z}_p)$ are computed with respect to the Euclidean measure normalized so that $V_{A,b}(\mathbb{Z}_p)$ has measure* 1.

The following tail estimates are known for $n = 3$ and likely to be true for $n \geq 5$. Indeed they follow from a suitable version of the *abc* conjecture by work of Granville.

Definition 1.5.9. Let p be a prime. We denote by $\mathcal{W}_{A,b,p}$ the set of elements $v \in V_{A,b}(\mathbb{Z})$ such that $p^2 \mid \Delta(v)$.

Conjecture 1.5.10 (Conjectural tail estimates)**.** *We have*

$$N(\cup_{p\geq M}\mathcal{W}_{A,b,p},X)=O\left(\frac{X^{\frac{n(n+1)}{2}-1}}{M^{1-\epsilon}}\right)+o\left(X^{\frac{n(n+1)}{2}-1}\right)$$

where the implied constant is independent of X and M.

We have the following asymptotic formula conditional on the preceding tail estimates.

Theorem 1.5.11. *Suppose that the preceding tail estimates hold. Let r_2 be an integer such that $0 \leq r_2 \leq \frac{n-1}{2}$ and let $\delta \in \mathcal{T}(r_2)$. Then for an acceptable collection of local specifications $\Lambda_{A,b}$ such that $\Lambda_{A,b}(\infty) = V_{A,b}^{r_2,\delta}(\mathbb{R})$ we have*

$$N(\mathcal{V}(\Lambda_{A,b}^{\delta}),X)=\frac{1}{\sigma(r_2)}\mathrm{Vol}(\mathcal{F}_A\cdot R_A^{r_2,\delta}(X))\prod_p\mathrm{Vol}(\Lambda_{A,b,p})+o\left(X^{\frac{n(n-1)}{2}-1}\right),$$

where the volume of subsets of $V_{A,b}(\mathbb{R})$ are computed with respect to the Euclidean measure normalized so that $V_{A,b}(\mathbb{Z})$ has covolume 1 and the volumes of subsets of $V_{A,b}(\mathbb{Z}_p)$ are computed with respect to the Euclidean measure normalized so that $V_{A,b}(\mathbb{Z}_p)$ has measure 1.

1.6 The product of local volumes and the local mass

1.6.1 The change of measure fomula

To compute the volumes of sets and multi-sets in $V_{A,b}(\mathbb{R})$ and $V_{A,b}(\mathbb{Z}_p)$, we have the following version of the change of variable formula. Let dv and df denote the Euclidean measure on $V_{A,b}$ and $U_{A,b}$ respectively normalized so that $V_{A,b}(\mathbb{Z})$ and $U_{A,b}(\mathbb{Z})$ have co-volume 1. Furthermore, let ω be an algebraic differential form generating the rank 1 module of top degree left-invariant differential forms on SO_A over $\mathbb{Z}$.

Proposition 1.6.1 (Change of measure formula)**.** *Let $K = \mathbb{Z}_p, \mathbb{R}$ or $\mathbb{C}$,. Let $|\cdot|$ denote the usual absolute value on K and let $s\colon U_{1,b}(K) \to V_{A,b}(K)$ be a continuous map such that $\pi(f) =$ for each $f \in U_{1,b}$. Then there exists a rational non-zero constant $\mathcal{J}_A$, independent of K and s, such that for any measurable function ϕ on $V_{A,b}(K)$, we have:*

$$\int\limits_{\mathrm{SO}_A(K)\cdot s(U_{1,b}(K))}\phi(v)\,dv=|\mathcal{J}_A|\int_{f\in U_{1,b}(K)}\int_{g\in\mathrm{SO}_A(K)}\phi(g\cdot s(f))\,\omega(g)\,df$$

$$\int\limits_{V_{A,b}(K)}\phi(v)dv=|\mathcal{J}_A|\int\limits_{\substack{f\in U_{1,b}(K)\\ \Delta(f)\neq0}}\left(\sum_{v\in\frac{V_{A,b}(K)\cap\pi^{-1}(f)}{\mathrm{SO}_A(K)}}\frac{1}{\#\mathrm{Stab}_{\mathrm{SO}_A(\mathbb{Z}_p)}(v)}\int\limits_{g\in\mathrm{SO}_A(K)}\phi(g\cdot v)\,\omega(g)\right)df$$

where $\frac{V_{A,b}(K)\cap\pi^{-1}(f)}{\mathrm{SO}_A(K)}$ denotes a set of representatives for the action of $\mathrm{SO}_A(\mathbb{Z}_p)$ on $V_{A,b}(\mathbb{Z}_p)\cap\pi^{-1}(f)$.

We can simplify the second integral above by introducing a local mass.

Definition 1.6.2 (Local mass formula)**.** Let p be a prime, $f \in U_{1,b}(\mathbb{Z}_p)$ and $A \in \mathscr{L}_{\mathbb{Z}}$. We define the local mass of f at p in A, $m_p(f, A)$ to be

$$m_p(f,A) := \sum_{v \in \frac{V_{A,b}(\mathbb{Z}_p)\cap\pi^{-1}(f)}{\mathrm{SO}_A(\mathbb{Z}_p)}} \frac{1}{\#\mathrm{Stab}_{\mathrm{SO}_A(\mathbb{Z}_p)}(v)}.$$

We now have the following formula for the local volumes appearing in the asymptotic formula.

Proposition 1.6.3. *We have*

$$\mathrm{Vol}\left(\mathcal{F}_A \cdot R_{A,b}^{r_2;\delta}(X)\right) = \chi_A(\delta)\,|\mathcal{J}_A|\,\mathrm{Vol}(\mathcal{F}_A^{\delta})\mathrm{Vol}(U(\mathbb{R})^{r_2}_{H<X}).$$

Let $S_p \subset U_{1,b}(\mathbb{Z}_p)$ be a non-empty open set whose boundary has measure 0. Consider the set $\Lambda_{A,b,p} = V_{A,b}(\mathbb{Z}_p) \cap \pi^{-1}(S_p)$. Then we have

$$\mathrm{Vol}(\Lambda_{A,b,p}) = |\mathcal{J}_A|_p\,\mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\int_{f\in S_p} m_p(f,A)\,df.$$

1.6.2 Computing the local masses

We now define the infinite mass and compute $m_p(f, A)$ for all $p \neq 2, \infty$.

Definition 1.6.4 (The infinite mass)**.** Let $A \in \mathscr{L}_{\mathbb{Z}}$ and r_2 be an integer such that $0 \le r_2 \le \frac{n-1}{2}$. The infinite mass of A with respect to r_2 is defined to be

$$m_\infty(r_2, A) = \sum_{\delta\in\mathcal{T}(r_2)} \chi_A(\delta).$$

The following lemma isolates the main properties of the local masses for all p, including the Archimedean place.

Lemma 1.6.5 (Main properties of the local masses)**.** *The local masses $m_p(f, A)$ and $m_\infty(A)$ have the following properties.*

1. *If $\gamma \in \mathrm{SL}_n(\mathbb{Z}_p)$, we have*
$$m_p(f, \gamma^t A\gamma) = m_p(f, A).$$

2. *If $\gamma \in \mathrm{SL}_n(\mathbb{R})$, we have*
$$m_\infty(r_2, \gamma^t A\gamma) = m_\infty(r_2, A).$$

3. *In particular, if A_1 and A_2 are unimodular integral matrices lying in the same genus, we have*
$$m_p(f, A_1) = m_p(f, A_2)$$

for all primes p and

$$m_\infty(r_2, A_1) = m_\infty(r_2, A_2).$$

4. *The sum of $m_2(f, A)$ over a set of representatives for the unimodular orbits of the action of $\mathrm{SL}_n(\mathbb{Z}_2)$ on $\mathrm{Sym}_n(\mathbb{Z}_2)$ is*

$$\sum_{\substack{A \in \frac{\mathrm{Sym}_n(\mathbb{Z}_2)}{\mathrm{SL}_n(\mathbb{Z}_2)} \\ \det(A) = 1 \in \frac{\mathbb{Z}_2}{\mathbb{Z}_2^2}}} m_2(f, A) = 2^{n-1}.$$

5. *The sum of $m_p(f, A)$ over a set of representatives for the unimodular orbits of the action of $\mathrm{SL}_n(\mathbb{Z}_p)$ on $\mathrm{Sym}_n(\mathbb{Z}_p)$ is*

$$\sum_{\substack{A \in \frac{\mathrm{Sym}_n(\mathbb{Z}_p)}{\mathrm{SL}_n(\mathbb{Z}_p)} \\ \det(A) = 1 \in \frac{\mathbb{Z}_p}{\mathbb{Z}_p^2}}} m_p(f, A) = 1.$$

6. *The sum of $m_\infty(r_2, A)$ over a set of representatives for unimodular the orbits of the action of $\mathrm{SL}_n(\mathbb{R})$ on $\mathrm{Sym}_n(\mathbb{R})$ is*

$$\sum_{\substack{A \in \frac{\mathrm{Sym}_n(\mathbb{R})}{\mathrm{SL}_n(\mathbb{R})} \\ \det(A) = 1 \in \frac{\mathbb{R}}{\mathbb{R}^2}}} m_\infty(r_2, A) = 2^{r_1 - 1}.$$

We can now compute the local masses for all $p \neq 2, \infty$.

Corollary 1.6.6 (Local masses for $p \neq 2, \infty$)**.** *For $A \in \mathscr{L}_\mathbb{Z}$ and $p \neq 2, \infty$ we have*

$$m_p(f, A) = 1.$$

The computation of the local masses at $p = 2, \infty$ is more delicate and is the object of the following sections.

1.7 Point count and the 2-adic mass

Remark 1.7.1. In the proofs, we assume that the local conditions are modulo 2. Nevertheless, in the case of rings which are maximal at the prime 2, we can remove this assumption. Indeed, we can use the even, non-degenerate, $\mathbb{F}_2$ quadratic form on the $\mathbb{F}_2$ vector space $(R_f^\times/(R_f^\times)^2)_{N\equiv 1}$ introduced [8], whose kernel is the set of split forms, to calculate the local masses exactly. Doing so gives the same values as those obtained here at each maximal form f, and so we can remove the assumption that the local conditions are modulo 2 in our theorems concerning fields.

In this section, we calculate the integral of the 2-mass, $\int_{f\in S_2} m_2(f,A)\,df$, by comparing the 2-adic volumes of different indefinite special orthogonal groups.

By the classification of quadratic forms over $\mathbb{Z}_2$, there are only two determinant $(-1)^{\frac{n-1}{2}}$ classically integral quadratic forms over $\mathbb{Z}_2$ of odd dimension n up to $\mathrm{SL}_n(\mathbb{Z}_2)$ equivalence. See for instance [30] or [24]. They are

For $n \equiv 1 \mod 4$ we can take:

$$\mathfrak{M}_1 = \begin{pmatrix} 1 &&&&& \\ & \ddots &&&& \\ && 1 &&& \\ &&& 1 && \\ &&&& 1 & \\ &&&&& 1 \end{pmatrix}, \quad \mathfrak{M}_{-1} = \begin{pmatrix} 1 &&&&& \\ & \ddots &&&& \\ && 1 &&& \\ &&& 1 && \\ &&&& -1 & \\ &&&&& -1 \end{pmatrix}.$$

For $n \equiv 3 \mod 4$ we can take:

$$\mathfrak{M}_1 = \begin{pmatrix} 1 &&&&& \\ & \ddots &&&& \\ && 1 &&& \\ &&& 1 && \\ &&&& 1 & \\ &&&&& -1 \end{pmatrix}, \quad \mathfrak{M}_{-1} = \begin{pmatrix} 1 &&&&& \\ & \ddots &&&& \\ && 1 &&& \\ &&& -1 && \\ &&&& -1 & \\ &&&&& -1 \end{pmatrix}.$$

Remark 1.7.2. We have chosen the subscripts to match the Hasse–Witt symbol of the bilinear form.

First, we state the basic constraint obtained in the last section.

Lemma 1.7.3. *For any $f \in U_{1,b}(\mathbb{Z}_2)$, we have*

$$m_2(f,\mathfrak{M}_1) + m_2(f,\mathfrak{M}_{-1}) = 2^{n-1}.$$

We give names to the integral of the 2-adic masses over S_2.

Definition 1.7.4. We define

$$c_2(n,\mathfrak{M}_1) = \int_{f\in S_2} m_2(f,\mathfrak{M}_1)\,df$$
$$c_2(n,\mathfrak{M}_{-1}) = \int_{f\in S_2} m_2(f,\mathfrak{M}_{-1})\,df.$$

In this notation, the lemma above states

$$c_2(\mathfrak{M}_1) + c_2(\mathfrak{M}_{-1}) = 2^{n-1}\mathrm{Vol}(S_2).$$

Therefore, in order to determine the value of $c_2(\mathfrak{M}_1)$ and $c_2(\mathfrak{M}_{-1})$, it is sufficient to find their ratio. We recall the following expressions which were a corollary of the change of measure formula:

$$\begin{aligned}\mathrm{Vol}(\Lambda_{\mathfrak{M}_1}(2)) &= |\mathcal{J}_{\mathfrak{M}_1}|_2 \,\mathrm{Vol}(\mathrm{SO}_{\mathfrak{M}_1}(\mathbb{Z}_2)) \int_{f\in S_p} m_2(f,\mathfrak{M}_1)\,df \\ &= c_2(n,\mathfrak{M}_1)\Bigg(\,|\mathcal{J}_{\mathfrak{M}_1}|_2 \,\mathrm{Vol}(\mathrm{SO}_{\mathfrak{M}_1}(\mathbb{Z}_2))\Bigg)\end{aligned}$$

and

$$\begin{aligned}\mathrm{Vol}(\Lambda_{\mathfrak{M}_{-1}}(2)) &= \left|\mathcal{J}_{\mathfrak{M}_{-1}}\right|_2 \mathrm{Vol}(\mathrm{SO}_{\mathfrak{M}_{-1}}(\mathbb{Z}_2)) \int_{f\in S_2} m_p(f,\mathfrak{M}_{-1})\,df \\ &= c_2(n,\mathfrak{M}_{-1})\Bigg(\,\left|\mathcal{J}_{\mathfrak{M}_{-1}}\right|_2 \mathrm{Vol}(\mathrm{SO}_{\mathfrak{M}_{-1}}(\mathbb{Z}_2))\Bigg).\end{aligned}$$

We now come to the heart of the argument. It is composed of two parts. First, we show that $\mathrm{Vol}(\Lambda_{\mathfrak{M}_1}(2)) = \mathrm{Vol}(\Lambda_{\mathfrak{M}_{-1}}(2))$ and $\mathcal{J}_{\mathfrak{M}_1} = \mathcal{J}_{\mathfrak{M}_{-1}}$. Second, we calculate ratio of the volumes $\mathrm{Vol}(\mathrm{SO}_{\mathfrak{M}_1}(\mathbb{Z}_2))$ and $\mathrm{Vol}(\mathrm{SO}_{\mathfrak{M}_{-1}}(\mathbb{Z}_2))$. Together, this will yield the value of the ratio of $c_2(\mathfrak{M}_1)$ and $c_2(\mathfrak{M}_{-1})$, and hence their individual values.

We deduce the equality of volumes $\mathrm{Vol}(\Lambda_{\mathfrak{M}_1}(2)) = \mathrm{Vol}(\Lambda_{\mathfrak{M}_{-1}}(2))$ using an argument which uses the that $\mathfrak{M}_1$ and $\mathfrak{M}_{-1}$ have the same reduction modulo 2.

Lemma 1.7.5 (Point count). *Let $S_2 \subset U_{1,b}(\mathbb{Z}_2)$ be a local condition on the space of monic polynomials at the prime 2 defined modulo 2. Denote by $\Lambda_{\mathfrak{M}_1}(2)$ and $\Lambda_{\mathfrak{M}_1}(2)$ the pre-images in $V_{\mathfrak{M}_1,b}(\mathbb{Z}_2)$ and $V_{\mathfrak{M}_{-1},b}(\mathbb{Z}_2)$ respectively of S_2 under the resolvent map π. Then the volumes of these two sets are equal*

$$\mathrm{Vol}(\Lambda_{\mathfrak{M}_1}(2)) = \mathrm{Vol}(\Lambda_{\mathfrak{M}_{-1}}(2)).$$

Proof. The canonical representatives $\mathfrak{M}_1$ and $\mathfrak{M}_{-1}$ are equal modulo 2. Since $\Lambda_{\mathfrak{M}_1}(2)$ and $\Lambda_{\mathfrak{M}_{-1}}(2)$ are defined by imposing congruence conditions modulo 2 on $V_{\mathfrak{M}_1,b}(\mathbb{Z}_2)$ and $V_{\mathfrak{M}_{-1},b}(\mathbb{Z}_2)$, the result follows. □

Lemma 1.7.6. *The rational numbers giving the Jacobian change of variables for $\mathfrak{M}_1$ and $\mathfrak{M}_{-1}$ are equal when the volume forms on the associated special orthogonal groups are those associated to point counting modulo increasing powers of p:*

$$\mathcal{J}_{\mathfrak{M}_1} = \mathcal{J}_{\mathfrak{M}_{-1}}.$$

In particular, their 2-adic valuations are the same

$$|\mathcal{J}_{\mathfrak{M}_1}|_2 = \left|\mathcal{J}_{\mathfrak{M}_{-1}}\right|_2.$$

Proof. We sketch the proof of the change of variables formula from Bhargava–Shankar in [11] and explain how to deduce the lemma from their argument. The proof of the change of variables formula over the rings we are interested in proceeds by proving that over $\mathbb{C}$ the identity

$$\int_{\mathrm{SO}_A(\mathbb{C})\cdot s(U_{1,b}(\mathbb{C}))} \phi(v)\,dv = |\mathcal{J}_A| \int_{f\in U_{1,b}(\mathbb{C})} \int_{\gamma\in \mathrm{SO}_A(\mathbb{C})} \phi(\gamma\cdot s(f))\,\omega(\gamma)\,df$$

holds for some non-zero rational number $\mathcal{J}_A \in \mathbb{Q}^\times$. The principle of permanence of identities then gives the result for $K = \mathbb{Z}_p, \mathbb{R}$, or $\mathbb{C}$ with the same $\mathcal{J}_A$.

Now, $\mathcal{J}_A$ can be realized as the Jacobian change of variables of the map

$$\psi_s^A \colon \mathrm{SO}_A(\mathbb{C}) \times U_{1,b}(\mathbb{C}) \to V_b(\mathbb{C})$$

given by $\psi_s^A(\gamma, f) = \gamma\cdot s(f)$ for any analytic section $s\colon U_{1,b}(\mathbb{C}) \to V_{A,b}(\mathbb{C})$.

Thus, the lemma will follow from comparing the Jacobian change of variables of the maps $\psi_s^{\mathfrak{M}_1}$ and $\psi_s^{\mathfrak{M}_{-1}}$.

Now, fix a matrix $g \in \mathrm{SL}_n(\mathbb{C})$ such that $\mathfrak{M}_1 = g\mathfrak{M}_{-1}g^t$.

Consider the map

$$\sigma_G \colon \mathrm{SO}_{\mathfrak{M}_1}(\mathbb{C}) \to \mathrm{SO}_{\mathfrak{M}_{-1}}(\mathbb{C})$$

defined by $\sigma_G(h) = ghg^{-1}$.

Now, fix an analytic section $s_1\colon U_{1,b}(\mathbb{C}) \to V_{\mathfrak{M}_1,b}(\mathbb{C})$ and define the analytic section $s_{-1}\colon U_{1,b}(\mathbb{C}) \to V_{\mathfrak{M}_{-1},b}(\mathbb{C})$ to be $s_{-1} := g\cdot s_1$. The following diagram commutes

$$\begin{tikzcd}
\mathrm{SO}_{\mathfrak{M}_1}(\mathbb{C}) \times U_{1,b}(\mathbb{C}) \arrow[r, "\psi_s^{\mathfrak{M}_1}"] \arrow[d, "\sigma_G\times\mathrm{id}"'] & V_b(\mathbb{C}) \arrow[d, "g\cdot"] \\
\mathrm{SO}_{\mathfrak{M}_{-1}}(\mathbb{C}) \times U_{1,b}(\mathbb{C}) \arrow[r, "\psi_{s_{-1}}^{\mathfrak{M}_{-1}}"'] & V_b(\mathbb{C})
\end{tikzcd}.$$

The fact that $\det(g) = 1$, that the Jacobian change of variable of $\psi_s^{\mathfrak{M}_1}$ and $\psi_{s'}^{\mathfrak{M}_{-1}}$ are constants, and the diagram above taken together imply that $\mathcal{J}_{\mathfrak{M}_1} = \mathcal{J}_{\mathfrak{M}_{-1}}$ as desired. In particular, the 2-adic valuations of those rational numbers are equal and we find $|\mathcal{J}_{\mathfrak{M}_1}|_2 = \left|\mathcal{J}_{\mathfrak{M}_{-1}}\right|_2$. □

We can now use calculations related to the Smith–Minkowski–Siegel mass formula to find the ratio between the volumes of the 2-adic points of the special orthogonal groups $\mathrm{SO}_{\mathfrak{M}_1}$ and $\mathrm{SO}_{\mathfrak{M}_{-1}}$.

Proposition 1.7.7. *We have the following ratio*

$$\frac{c_2\left(n, \mathfrak{M}_1\right)}{c_2\left(n, \mathfrak{M}_{-1}\right)} = \frac{\mathrm{Vol}(\Lambda_{\mathfrak{M}_1}(2))\left(\left|\mathcal{J}_{\mathfrak{M}_{-1}}\right|_2 \mathrm{Vol}(\mathrm{SO}_{\mathfrak{M}_{-1}}(\mathbb{Z}_2))\right)}{\mathrm{Vol}(\Lambda_{\mathfrak{M}_{-1}}(2))\left(|\mathcal{J}_{\mathfrak{M}_1}|_2 \mathrm{Vol}(\mathrm{SO}_{\mathfrak{M}_1}(\mathbb{Z}_2))\right)} = \frac{\mathrm{Vol}(\mathrm{SO}_{\mathfrak{M}_{-1}}(\mathbb{Z}_2))}{\mathrm{Vol}(\mathrm{SO}_{\mathfrak{M}_1}(\mathbb{Z}_2))}$$

$$= \frac{2^{n-1} \pm_8 2^{\frac{n-1}{2}}}{2^{n-1} \mp_8 2^{\frac{n-1}{2}}},$$

where $\pm_8$ *is* $+$ *if* n *is congruent to* 1 *or* $3 \mod 8$ *and* $-$ *otherwise.*

Proof. The first two equalities above follow directly from the preceding lemmata. The value of the ratio of the volumes of $\mathrm{SO}_{\mathfrak{M}_1}(\mathbb{Z}_2)$ and $\mathrm{SO}_{\mathfrak{M}_{-1}}(\mathbb{Z}_2)$ is inversely proportional to the ratio of the 2-adic densities of the lattices defined by $\mathfrak{M}_1$ and $\mathfrak{M}_{-1}$.

To find the ratio of the 2-adic densities of the lattices defined by $\mathfrak{M}_1$ and $\mathfrak{M}_{-1}$, it is sufficient to find the ratio of the *diagonal factors* $M_2(\mathfrak{M}_1)$ and $M_2(\mathfrak{M}_{-1})$ in the language of Sloane–Conway, [23].

There are general formulae for computing the value of the diagonal factors at every prime. These turn out to be rather subtle in the case of $p = 2$, depending not only on the form of each Jordan factor but on the full Jordan decomposition, in contrast to the case of odd primes.

Nevertheless, in our case we have that $\mathfrak{M}_1$ and $\mathfrak{M}_{-1}$ are already in 2-adic Jordan form. Moreover, $\mathfrak{M}_1$ is *free*, *odd*, and has *octane value* 1 (mod 8) if $n \equiv 1, 3 \pmod 8$ and 5 (mod 8) if $n \equiv 5, 7 \pmod 8$. On the other hand, $\mathfrak{M}_{-1}$ is *free*, *odd*, and has *octane value* 5 (mod 8) if $n \equiv 1, 3 \pmod 8$ and 1 (mod 8) if $n \equiv 5, 7 \pmod 8$.

We may now apply the formulae for the diagonal factor of Conway–Sloane, [23], to find that the diagonal factors have the form

$$M_2(\mathfrak{M}_1) = \frac{1}{2\prod_{i=1}^{\frac{n-1}{2}-1}(1-2^{-2i})} \frac{1}{1 \mp_8 2^{-\frac{n-1}{2}}}$$
$$M_2(\mathfrak{M}_{-1}) = \frac{1}{2\prod_{i=1}^{\frac{n-1}{2}-1}(1-2^{-2i})} \frac{1}{1 \pm_8 2^{-\frac{n-1}{2}}}.$$

This completes the proof of the last equality of the lemma. □

We have obtained the values for the 2-adic mass.

Corollary 1.7.8. *The* 2*-adic masses satisfy the following identities:*

$$c_2(n, \mathfrak{M}_1) + c_2(n, \mathfrak{M}_{-1}) = 2^{n-1}\mathrm{Vol}(S_2)$$
$$c_2(n, \mathfrak{M}_0) - c_2(n, \mathfrak{M}_{-1}) = \pm_8 2^{\frac{n-1}{2}}\mathrm{Vol}(S_2),$$

where $\pm_8$ *is* $+$ *if* n *is congruent to* 1 *or* $3 \mod 8$ *and* $-$ *otherwise. In particular, we find:*

$$c_2(n, \mathfrak{M}_1) = \frac{1}{2}\left(2^{n-1} \pm_8 2^{\frac{n-1}{2}}\right)\mathrm{Vol}(S_2)$$
$$c_2(n, \mathfrak{M}_{-1}) = \frac{1}{2}\left(2^{n-1} \mp_8 2^{\frac{n-1}{2}}\right)\mathrm{Vol}(S_2).$$

1.8 A spectral theorem for the indefinite special orthogonal groups

We now describe the distribution of the δ among the V_A by using a version of the spectral theorem for SO_A combined with a modified parametrisation of the $\mathrm{SO}_A(\mathbb{R})$ orbits on $V_A(\mathbb{R}) \bigcap \pi^{-1}(f)$.

We begin by presenting an alternative parametrisation of the SO_A orbits on $V_A \bigcap \pi^{-1}(f)$

Theorem 1.8.1. *Let $A \in \mathscr{L}_{\mathbb{Z}}$. Consider the bilinear form $W_A = \langle \cdot, \cdot \rangle_A$ whose matrix is A. Then, given $f \in U_1$, there is a natural correspondence between SO_{W_A}-conjugacy classes of self-adjoint operators with characteristic polynomial f and SO_A-orbits on $V_A \bigcap \pi^{-1}(f)$.*

Proof. We note that for each $A \in \mathscr{L}_{\mathbb{Z}}$ we can represent the orbit data

$$\Big(\mathrm{SO}_A, V_A \cap \pi^{-1}(f)\Big)$$

where SO_A acts via $g \cdot (A, B) = (A, g^t B g)$, in terms of the orbit data

$$\left(\mathrm{SO}_{W_A}, \left\{ M \in \mathrm{Mat}_n \Big|_{f=(-1)^{\frac{n-1}{2}}\det(Ix-M)}^{AM=M^tA} \right\}\right)$$

where SO_{W_A} acts on the set of M via $\gamma \cdot M = \gamma M \gamma^{-1}$. Note that this last space is the space of self-adjoint operators with characteristic polynomial $\pm f$. Indeed, consider the maps

$$(A, B) \mapsto A^{-1}B$$

and

$$M \mapsto (A, AM).$$

These maps are immediately seen to descend to isomorphisms on the quotients. □

Remark 1.8.2. The parametrisation above does not depend on the base.

We can now modify an argument of Bhargava–Gross [8] to describe the real SO_A orbits on $V_A \bigcap \pi^{-1}(f)$. As a corollary, we find the distribution of the elements δ of $\mathcal{T}(r_2)$ among the slices V_A over $\mathbb{R}$.

We first explore the example of f, having no complex roots before presenting the general case.

Example 1.8.3. We first deal with the case of $f \in \mathbb{R}[x]$ having no complex roots. First, it is clear that the number of $\mathrm{SO}_A(\mathbb{R})$ orbits on $V_A(\mathbb{R}) \bigcap \pi^{-1}(f)$ is equal to the number of δ which lie in V_A. By the above theorem, the number of δ which lie in $V_A(\mathbb{R}) \bigcap \pi^{-1}(f)$ is thus the number of SO_{W_A} orbits on the W_A self-adjoint operators with characteristic polynomial f. Indeed, such an operator is diagonalisable and has n eigenspaces of dimension 1. The quadratic space defined by W_A decomposes as an orthogonal direct sum of these spaces. For the signatures to match, we must have a subset of q_A of these eigenspaces being negative definite for W_A. The subset of these eigenspaces which are negative definite determines the real orbit of T. We need some notation for the signature of the quadratic space W_A. Let's suppose that A, and thus the quadratic space defined by W_A, has signature (p_A, q_A). Therefore, the number of δ which land in $V_A(\mathbb{R}) \bigcap \pi^{-1}(f)$ is $\binom{n}{q_A}$.

We now proceed to the general case. We want to find the distribution of the δ which land in $V_A(\mathbb{R}) \bigcap \pi^{-1}(f)$ when f has complex roots. Towards this goal, let's suppose that f has r_1 real roots and $2r_2$ complex roots. Now consider a W_A self-adjoint operator T with characteristic polynomial f. This operator has r_1 eigenspaces of dimension 1 and r_2 eigenspaces of dimension 2. The quadratic space defined by W_A decomposes as an orthogonal direct sum of these eigenspaces. To proceed with the argument, we need some notation for the signature of the quadratic space W_A. Let's suppose that A, and thus the quadratic space defined by W_A, has signature (p_A, q_A). Now, since each of the 2-dimensional eigenspaces has signature $(1, 1)$ we deduce that:

a) $p_A \geq r_2$;

b) $q_A \geq r_2$; and

c) the number of 1-dimensional eigenspaces which are negative definite for W_A is

$$q_A - r_2.$$

The subset of the 1-dimensional eigenspaces which are negative definite determines the real orbit of T. Therefore, the number of δ which land in $V_A(\mathbb{R}) \bigcap \pi^{-1}(f)$ is indeed

$$\binom{r_1}{q_A - r_2}.$$

Remark 1.8.4. The argument presented above is an extension of an idea of Bhargava–Gross which dealt with A totally split over $\mathbb{R}$.

We have computed the value of the infinite mass, $m_\infty(f, A)$, and we record the distribution obtained above as an equidistribution result.

Theorem 1.8.5 (Equidistribution of $\mathcal{T}(r_2)$ in $\mathrm{SO}_n(\mathbb{R})\backslash\mathrm{Sym}_n(\mathbb{R})$)**.** *Let $A \in \mathscr{L}_\mathbb{Z}$ and $0 \leq r_2 \leq \frac{n-1}{2}$. If A has q negative eigenvalues, the infinite mass $m_\infty(r_2, A)$, which is the number of δ in $\mathcal{T}(r_2)$ such that the matrix A_δ associated to δ has q negative eigenvalues, is given by*

$$m_\infty(r_2, A) = \binom{r_1}{q - r_2}.$$

In particular, if $q < r_2$, there are no δ which land in any V_A for which A has signature $(n - q, q)$.

For the final calculation, we are interested in the sum of the total masses over all genera which have a fixed Hasse–Witt symbol. We write $c_{\infty,0}$ for the sum of the infinite masses across all genera which have Hasse–Witt symbol equal to 1 and $c_{\infty,2}$ for the sum of the infinite masses across all genera which have Hasse–Witt symbol equal to -1.

Lemma 1.8.6. *Let l be an odd number. Then*

$$\sum_{k=0}^{\frac{l-1}{2}} \binom{l}{2k} = 2^{l-1}$$

and

$$\sum_{k=0}^{\frac{l-1}{2}} (-1)^k \binom{l}{2k} = \pm_8' 2^{\frac{l-1}{2}}$$

where $\pm_8'$ is $+$ if l is congruent to -1 or $1 \mod 8$ and $-$ otherwise. Furthermore, we have

$$\sum_{k=0}^{\frac{l-1}{2}} \binom{l}{2k+1} = 2^{l-1}$$

and

$$\sum_{k=0}^{\frac{l-1}{2}} (-1)^k \binom{l}{2k+1} = \pm_8'' 2^{\frac{l-1}{2}}$$

where $\pm_8''$ is $+$ if l is congruent to 1 or $3 \mod 8$ and $-$ otherwise.

Proof. These identities follow from the binomial formula. Indeed, for the first one, note that $2^l = (1+1)^l = \sum_{k=0}^{\frac{l-1}{2}} \binom{l}{2k} + \sum_{k=0}^{\frac{l-1}{2}} \binom{l}{2k+1}$ while $0 = (1-1)^l = \sum_{k=0}^{\frac{l-1}{2}} \binom{l}{2k} - \sum_{k=0}^{\frac{l-1}{2}} \binom{l}{2k+1}$. Thus $\sum_{k=0}^{\frac{l-1}{2}} \binom{l}{2k} = 2^{l-1}$. For the second one, examine $(1+i)^l$ in the complex plane. For notational clarity, let us write $\alpha = (1+i)^l$. On the one hand, $\alpha = \sum_{k=0}^{l} \binom{l}{k} i^k = \left(\sum_{k=0}^{\frac{l-1}{2}} (-1)^k \binom{l}{2k}\right) + i\left(\sum_{k=0}^{\frac{l-1}{2}} (-1)^k \binom{l}{2k+1}\right)$. On the other hand, $\alpha = 2^{\frac{l}{2}} e^{i\frac{l\pi}{4}}$ since $1+i = \sqrt{2}e^{i\frac{\pi}{4}}$. So we find $\mathfrak{Re}(\alpha) = \pm\mathfrak{Im}(\alpha)$, $2^l = \mathfrak{Re}(\alpha)^2 + \mathfrak{Im}(\alpha)^2$ and $\mathfrak{Re}(\alpha) > 0$ if and only if l is congruent to $-1, 0, 1 \mod 8$. Thus $\sum_{k=0}^{\frac{l-1}{2}} (-1)^k \binom{l}{2k} = \pm_8' 2^{\frac{l-1}{2}}$. The proof of the second set of identites follows from examining $\mathfrak{Im}(\alpha)$. □

We have obtained the values for the total infinite mass.

Corollary 1.8.7. *The total infinite masses satisfy the following identities:*

$$c_{\infty,0} + c_{\infty,2} = 2^{r_1 - 1}$$
$$c_{\infty,0} - c_{\infty,2} = \pm_8 2^{\frac{r_1 - 1}{2}},$$

where $\pm_8$ is $+$ if n is congruent to 1 or $3 \mod 8$ and $-$ otherwise.

In particular, we find:

$$\begin{aligned} c_{\infty,0} &= \frac{1}{2}\left(2^{r_1-1} \pm_8 2^{\frac{r_1-1}{2}}\right) \\ c_{\infty,2} &= \frac{1}{2}\left(2^{r_1-1} \mp_8 2^{\frac{r_1-1}{2}}\right). \end{aligned}$$

1.9 Statistical consequences

We now calculate the average 2–torsion by assembling all the elements we have developed.

Let $\mathscr{L}_{\mathbb{Z}}$ denote a set of representatives of unimodular integral matrices under the action of $\mathrm{SL}_n(\mathbb{Z})$. Denote by $\mathcal{G}_{\mathbb{Z}}$ the set of genera of quadratic n-ary forms containing a unimodular integral element. Notice that $\mathcal{G}_{\mathbb{Z}}$ partitions $\mathscr{L}_{\mathbb{Z}}$. We have to estimate the following sum:

$$\frac{\sum\limits_{\substack{\mathcal{O}\in\mathfrak{R},\\ H(\mathcal{O})<X}} 2^{r_1+r_2-1}\left|\mathrm{Cl}_2(\mathcal{O})\right| - \left|\mathcal{I}_2(\mathcal{O})\right|}{\left(\sum\limits_{0\leq b<n} \mathrm{Vol}(U_{1,b}^{r_2}(\mathbb{R}))_{<X}\right)\prod\limits_p \mathrm{Vol}(S_p)} + o(1).$$

Now, by the preceding sections, we know that this sum is equal to:

$$= \frac{\sum\limits_{0\leq b<n}\sum\limits_{\delta\in\mathcal{T}(r_2)}\sum\limits_{A\in\mathscr{L}_{\mathbb{Z}}} N_H(\mathcal{V}(\Lambda_{A,b}^{\delta}), X)}{\left(\sum\limits_{0\leq b<n} \mathrm{Vol}(U_{1,b}^{r_2}(\mathbb{R}))_{<X}\right)\prod\limits_p \mathrm{Vol}(S_p)}.$$

Expanding, we find:

$$= \sum_{\delta\in\mathcal{T}(r_2)}\sum_{A\in\mathscr{L}_{\mathbb{Z}}} \frac{1}{\sigma(r_2)}\mathrm{Vol}(\mathcal{F}_A^{\delta})\prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\prod_{p\neq 2} m_p(A)\frac{\int_{f\in S_2} m_2(f,A)df}{\mathrm{Vol}(S_2)}.$$

The indicator functions come into play at this point.

$$= \sum_{\delta\in\mathcal{T}(r_2)}\sum_{A\in\mathscr{L}_{\mathbb{Z}}} \frac{1}{\sigma(r_2)}\chi_A(\delta)\mathrm{Vol}(\mathcal{F}_A)\prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\frac{\int_{f\in S_2} m_2(f,A)df}{\mathrm{Vol}(S_2)}$$

We now break up the collection $\mathscr{L}_\mathbb{Z}$ into genera and sum over the forms in each genus separately before summing over the distinct genera. Since, both the characteristic function and the p-adic masses are constant over the forms in a single genus, they factor out of the inner sum.

$$\begin{aligned}
&= \sum_{\delta\in\mathcal{T}(r_2)} \sum_{\mathcal{G}\in\mathcal{G}_\mathbb{Z}} \sum_{A\in\mathcal{G}\cap\mathscr{L}_\mathbb{Z}} \frac{1}{\sigma(r_2)}\chi_A(\delta)\mathrm{Vol}(\mathcal{F}_A)\prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\frac{\int_{f\in S_2} m_2(f,A)df}{\mathrm{Vol}(S_2)} \\
&= \sum_{\delta\in\mathcal{T}(r_2)} \sum_{\mathcal{G}\in\mathcal{G}_\mathbb{Z}} \frac{1}{\sigma(r_2)}\chi_\mathcal{G}(\delta)\frac{\int_{f\in S_2} m_2(f,\mathcal{G})df}{\mathrm{Vol}(S_2)} \left(\sum_{A\in\mathcal{G}\cap\mathscr{L}_\mathbb{Z}} \mathrm{Vol}(\mathcal{F}_A)\prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p)) \right)
\end{aligned}$$

Now, the inner sum gives the Tamagawa number of the special orthogonal group of an integral form in a genus. It is known to always be equal 2, see for instance [32] and [26]. We denote it by $\tau(\mathrm{SO})$.

$$= \tau(\mathrm{SO}) \sum_{\delta\in\mathcal{T}(r_2)} \sum_{\mathcal{G}\in\mathcal{G}_\mathbb{Z}} \frac{1}{\sigma(r_2)}\chi_\mathcal{G}(\delta)\frac{\int_{f\in S_2} m_2(f,\mathcal{G})df}{\mathrm{Vol}(S_2)}$$

At this point, we simplify the sum using the fact that $\sigma(r_2) = \frac{1}{2^{r_1+r_2-1}}$, the value of the 2-adic mass, the value of the infinite mass, and the classification of genera of unimodular integral quadratic forms as it appears in [18] or [24].

$$\begin{aligned}
&= \frac{\tau(\mathrm{SO})}{2^{r_1+r_2-1}} \sum_{\delta\in\mathcal{T}(r_2)} \sum_{\mathcal{G}\in\mathcal{G}_\mathbb{Z}} \chi_\mathcal{G}(\delta)\frac{\int_{f\in S_2} m_2(f,\mathcal{G})df}{\mathrm{Vol}(S_2)} \\
&= \frac{\tau(\mathrm{SO})}{2^{r_1+r_2-1}} \sum_{\mathcal{G}\in\mathcal{G}_\mathbb{Z}} \sum_{\delta\in\mathcal{T}(r_2)} \chi_\mathcal{G}(\delta)\frac{\int_{f\in S_2} m_2(f,\mathcal{G})df}{\mathrm{Vol}(S_2)} \\
&= \frac{\tau(\mathrm{SO})}{2^{r_1+r_2-1}} \sum_{\mathcal{G}\in\mathcal{G}_\mathbb{Z}} \left(\frac{\int_{f\in S_2} m_2(f,\mathcal{G})df}{\mathrm{Vol}(S_2)} \sum_{\delta\in\mathcal{T}(r_2)} \chi_\mathcal{G}(\delta) \right) \\
&= \frac{\tau(\mathrm{SO})}{2^{r_1+r_2-1}} \Big(c_2(\mathfrak{M}_1)c_{\infty,0} + c_2(\mathfrak{M}_{-1})c_{\infty,2} \Big)
\end{aligned}$$

Now, these values being known from previous sections, we substitute them and simplify.

$$\begin{aligned}
&= \frac{1}{2^{r_1+r_2-1}} \cdot 2 \cdot \frac{1}{4} \left(\left(2^{n-1} \pm_8 2^{\frac{n-1}{2}}\right)\left(2^{r_1} \pm_8 2^{\frac{r_1-1}{2}}\right) + \left(2^{n-1} \mp_8 2^{\frac{n-1}{2}}\right)\left(2^{r_1-1} \mp_8 2^{\frac{r_1-1}{2}}\right) \right) \\
&= \frac{1}{2^{r_1+r_2-1}} \cdot 2 \cdot \frac{1}{4} \left(\left(2^{n-1} - 2^{\frac{n-1}{2}}\right)\left(2^{r_1} - 2^{\frac{r_1-1}{2}}\right) + \left(2^{n-1} + 2^{\frac{n-1}{2}}\right)\left(2^{r_1-1} + 2^{\frac{r_1-1}{2}}\right) \right) \\
&= \frac{1}{2^{r_1+r_2-1}} \cdot 2 \cdot \frac{1}{4} \left(2 \cdot \left(2^{n+r_1-2} + 2^{\frac{n+r_1-2}{2}} \right) \right) \\
&= 2^{r_1+r_2-1} + 1.
\end{aligned}$$

We now present the corresponding computation for the narrow class group. The setup is the same as above, with the exception that we now sum over $\delta_{\gg 0} = (11\cdots 1) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$

instead of the entire collection $\mathcal{T}(r_2)$. Apart from this, the computation proceeds in the same way as above and we leave it in its raw form.

$$
\begin{aligned}
&\frac{\sum\limits_{\substack{\mathcal{O}\in\mathfrak{R},\\ H(\mathcal{O})<X}} 2^{r_2}\left|\mathrm{Cl}_2^+(\mathcal{O})\right| - |\mathcal{I}_2(\mathcal{O})|}{\left(\sum\limits_{0\leq b<n}\mathrm{Vol}(U^{r_2}_{1,b}(\mathbb{R}))_{<X}\right)\prod\limits_p \mathrm{Vol}(S_p)} + o(1)\\
&= \frac{\sum\limits_{0\leq b<n}\sum\limits_{A\in\mathscr{L}_{\mathbb{Z}}} N_H(\mathcal{V}(\Lambda^{\delta\gg0}_{A,b}),X)}{\left(\sum\limits_{0\leq b<n}\mathrm{Vol}(U^{r_2}_{1,b}(\mathbb{R}))_{<X}\right)\prod\limits_p \mathrm{Vol}(S_p)}\\
&= \sum_{A\in\mathscr{L}_{\mathbb{Z}}}\frac{1}{\sigma(r_2)}\mathrm{Vol}(\mathcal{F}_A^{\delta\gg0})\prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\prod_{p\neq2} m_p(A)\frac{\int_{f\in S_2} m_2(f,A)df}{\mathrm{Vol}(S_2)}\\
&= \sum_{A\in\mathscr{L}_{\mathbb{Z}}}\frac{1}{\sigma(r_2)}\chi_A(\delta_{\gg0})\mathrm{Vol}(\mathcal{F}_A)\prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\frac{\int_{f\in S_2} m_2(f,A)df}{\mathrm{Vol}(S_2)}\\
&= \sum_{\mathcal{G}\in\mathcal{G}_{\mathbb{Z}}}\sum_{A\in\mathcal{G}\cap\mathscr{L}_{\mathbb{Z}}}\frac{1}{\sigma(r_2)}\chi_A(\delta_{\gg0})\mathrm{Vol}(\mathcal{F}_A)\prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\frac{\int_{f\in S_2} m_2(f,A)df}{\mathrm{Vol}(S_2)}\\
&= \sum_{\mathcal{G}\in\mathcal{G}_{\mathbb{Z}}}\frac{1}{\sigma(r_2)}\chi_{\mathcal{G}}(\delta_{\gg0})\frac{\int_{f\in S_2} m_2(f,\mathcal{G})df}{\mathrm{Vol}(S_2)}\left(\sum_{A\in\mathcal{G}\cap\mathscr{L}_{\mathbb{Z}}}\mathrm{Vol}(\mathcal{F}_A)\prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\right)\\
&= \tau(\mathrm{SO})\sum_{\mathcal{G}\in\mathcal{G}_{\mathbb{Z}}}\frac{1}{\sigma(r_2)}\chi_{\mathcal{G}}(\delta_{\gg0})\frac{\int_{f\in S_2} m_2(f,\mathcal{G})df}{\mathrm{Vol}(S_2)}\\
&= \frac{\tau(\mathrm{SO})}{2^{r_1+r_2-1}}\sum_{\mathcal{G}\in\mathcal{G}_{\mathbb{Z}}}\chi_{\mathcal{G}}(\delta_{\gg0})\frac{\int_{f\in S_2} m_2(f,\mathcal{G})df}{\mathrm{Vol}(S_2)}\\
&= \frac{1}{2^{r_1+r_2-1}}\cdot 2\cdot\frac{1}{2}\left(2^{n-1}+2^{\frac{n-1}{2}}\right)\\
&= 2^{r_2}+\frac{2^{r_2}}{2^{\frac{n-1}{2}}}.
\end{aligned}
$$

Thus we obtain the following averages for the class group and the narrow class group of monogenic fields.

$$
\mathrm{Avg}_{\text{monogenic}}\Big(\mathrm{Cl}_2\Big) = \lim_{X\to\infty}\frac{\sum\limits_{\substack{\mathcal{O}\in\mathfrak{R},\\ H(\mathcal{O})<X}} |\mathrm{Cl}_2(\mathcal{O})|}{\sum\limits_{\substack{\mathcal{O}\in\mathfrak{R},\\ H(\mathcal{O})<X}} 1}
$$

$$
\begin{aligned}
&= \lim_{X\to\infty} \frac{1}{2^{r_1+r_2-1}} \left(\frac{\displaystyle\sum_{0\le b<n} \sum_{\delta\in\mathcal{T}(r_2)} \sum_{A\in\mathscr{L}_{\mathbb{Z}}} N_H(\mathcal{V}(\Lambda^{\delta}_{A,b}), X)}{\displaystyle\sum_{\substack{\mathcal{O}\in\mathfrak{R},\\ H(\mathcal{O})<X}} 1} + 1 \right) \\
&= \frac{1}{2^{r_1+r_2-1}} \Big(\big(2^{r_1+r_2-1}+1\big) + 1 \Big) \\
&= 1 + \frac{2}{2^{r_1+r_2-1}} \\
&= 1 + \frac{1}{2^{r_1+r_2-2}}.
\end{aligned}
$$

$$
\begin{aligned}
\operatorname{Avg}_{\text{monogenic}}\left(\mathrm{Cl}_2^+\right) &= \lim_{X\to\infty} \frac{\displaystyle\sum_{\substack{\mathcal{O}\in\mathfrak{R},\\ H(\mathcal{O})<X}} \left|\mathrm{Cl}_2^+(\mathcal{O})\right|}{\displaystyle\sum_{\substack{\mathcal{O}\in\mathfrak{R},\\ H(\mathcal{O})<X}} 1} \\
&= \lim_{X\to\infty} \frac{1}{2^{r_2}} \left(\frac{\displaystyle\sum_{0\le b<n} \sum_{A\in\mathscr{L}_{\mathbb{Z}}} N_H(\mathcal{V}(\Lambda^{\delta\gg 0}_{A,b}), X)}{\displaystyle\sum_{\substack{\mathcal{O}\in\mathfrak{R},\\ H(\mathcal{O})<X}} 1} + 1 \right) \\
&= \frac{1}{2^{r_2}} \left(\left(2^{r_2} + \frac{2^{r_2}}{2^{\frac{n-1}{2}}} \right) + 1 \right) \\
&= 1 + \frac{1}{2^{\frac{n-1}{2}}} + \frac{1}{2^{r_2}}
\end{aligned}
$$

Remark 1.9.1. The calculations in this section go through in the even case.

Example 1.9.2. In the case $(n, r_1, 2r_2) = (3, 3, 0)$ we find

$$
\begin{aligned}
\operatorname{Avg}_{\text{monogenic}}\left(\mathrm{Cl}_2\right) &= 1 + \frac{2}{2^2} = \frac{3}{2} \\
\operatorname{Avg}_{\text{monogenic}}\left(\mathrm{Cl}_2^+\right) &= 1 + \frac{1}{2} + 1 = \frac{5}{2}.
\end{aligned}
$$

In the case $(n, r_1, 2r_2) = (3, 1, 2)$ we find

$$
\begin{aligned}
\operatorname{Avg}_{\text{monogenic}}\left(\mathrm{Cl}_2\right) &= 1 + \frac{2}{2^1} = 2 \\
\operatorname{Avg}_{\text{monogenic}}\left(\mathrm{Cl}_2^+\right) &= 1 + \frac{1}{2} + \frac{1}{2} = 2.
\end{aligned}
$$

Therefore, we recover the result of Bhargava–Hanke–Shankar in the monogenic cubic case [10].

We can deduce lower density estimates.

Corollary 1.9.3. *Let $n \geq 3$ be an odd integer, (r_1, r_2) a choice of signature, and $\mathfrak{R} \subset \mathfrak{R}^{r_1,r_2}_{\max}$ a family of monogenised rings corresponding to an acceptable family of binary forms. Then the following positive proportion estimates hold.*

1. *The proportion of maximal orders in $\mathfrak{R}$ which have odd class number is at least*

$$1 - \frac{1}{2^{r_1+r_2-2}}.$$

2. *The proportion of maximal orders in $\mathfrak{R}$ which have odd narrow class number is at least*

$$1 - \frac{1}{2^{n-1}} - \frac{1}{2^{r_2}}.$$

Consequently, a proportion of at least

$$1 - \frac{1}{2^{n-1}} - \frac{1}{2^{r_2}}$$

maximal orders in $\mathfrak{R}$ have a narrow class number equal to their class number. In particular, there are infinitely many monogenic number fields with units of every signature.

We can also deduce asymptotic lower bounds for the number of monogenic fields having odd class numbers when these fields are ordered by discriminant.

Corollary 1.9.4. *Let $n \geq 3$ be an odd integer, (r_1, r_2) a choice of signature, and $\mathfrak{R} \subset \mathfrak{R}^{r_1,r_2}_{\max}$ a family of monogenised rings corresponding to an acceptable family of binary forms. Then the following asymptotic estimates hold.*

1. $\#\{R \in \mathfrak{R} \colon\ |\mathrm{Disc}\,(R)| < X \text{ and } 2 \nmid |\mathrm{Cl}\,(R)|\} \gg X^{\frac{n(n+1)/2-1}{n(n-1)}}$.

2. *If $r_2 \neq 0$, then*

$$\#\left\{R \in \mathfrak{R} \colon\ |\mathrm{Disc}\,(R)| < X \text{ and } 2 \nmid \left|\mathrm{Cl}^+\,(R)\right|\right\} \gg X^{\frac{n(n+1)/2-1}{n(n-1)}}.$$

Finally, we can state the unconditional result for the concerning average 2-torsion in the class group and narrow class group of monogenic rings.

Theorem 1.9.5. *Let $n \geq 3$ be an odd integer and (r_1, r_2) a choice of signature.*

1. *The average over $\mathcal{O} \in \mathfrak{R}^{r_1,r_2}$ of*

$$|\mathrm{Cl}_2(\mathcal{O})| - \frac{1}{2^{r_1+r_2-1}}\,|\mathcal{I}_2(\mathcal{O})|$$

is equal to $1 + \frac{1}{2^{r_1+r_2-1}}$.

2. *The average over $\mathcal{O} \in \mathfrak{R}^{r_1,r_2}$ of*

$$\left|\mathrm{Cl}_2^+(\mathcal{O})\right| - \frac{1}{2^{r_2}}\,|\mathcal{I}_2(\mathcal{O})|$$

is equal to $1 + \frac{1}{2^{\frac{n-1}{2}}}$.

Furthermore, these numbers do not change when we average over any very large family in $\mathfrak{R}^{r_1,r_2}$.

Chapter 2

Even degree

2.1 Introduction

In 1801, Gauss introduced class groups in his *Disquisitiones Arithmeticae* [27], and posed what is recorded as the first question concerning their behaviour over families: are there infinitely many quadratic fields with class number 1? This question, in the real quadratic case, is still open. Nevertheless, Gauss proved that there were infinitely many quadratic fields with odd class number.

That result has been generalised, first to cubic fields by Bhargava [6], and then to all odd degrees by Ho–Shankar–Varma [29].

Theorem 2.1.1 (Bhargava [6], Ho–Shankar–Varma [29])**.** *For any odd degree n and signature (r_1, r_2), there are infinitely many fields of degree n and signature (r_1, r_2) that have odd class number.*

As a corollary of our main theorem, we generalise Gauss's result to all fields of even degree.

Theorem 2.1.2. *Let $n \geq 4$ be an even integer. For each choice of signature (r_1, r_2), there are infinitely fields of degree n and signature (r_1, r_2) that have odd class number.*

To obtain his result, Gauss calculated the size of the 2-part of the narrow class group of quadratic fields. Knowing the 2-part of the narrow class group gives information about unit signatures. As a corollary to our main theorem, we generalise to even degree the result of [14] and [29] that in each odd degree, there are infinitely many fields which have units of every possible signature.

Theorem 2.1.3. *Let $n \geq 4$ be an even integer. For each choice of signature (r_1, r_2) with $r_2 = 2$ if $n = 4$ and $r_2 > 0$ otherwise, there are infinitely many fields of degree n and signature (r_1, r_2) that have units of units of every signature.*

These results come from bounding the average size of the 2-torsion part of the class group and narrow class group of monogenised fields of even degree. This means that we can add the adjectives monogenic and S_n to Theorems 2.1.2 and 2.1.3.

2.1.1 Class group heuristics

The Cohen–Lenstra–Martinet–Malle heuristics which were developed in a series of groundbreaking works [19, 21, 22, 20, 35], constitute our best conjectural description of the distribution of the p^∞-part of the class group, $\mathrm{Cl}(K)[p^\infty]$, over families of number fields K of fixed degree and signature ordered by discriminant for "good" primes p. We say that a prime p is "good" if it is coprime to the degree of the field and "bad" otherwise.

Predictions arising from these heuristics have only been verified in two cases. Davenport and Heilbronn [25] calculated the average number of 3-torsion elements in the class group of quadratic fields, and Bhargava [6] calculated the average number of 2-torsion in the class group of cubic fields. The heuristics are expected to hold under any natural ordering on the family of fields, and not just when ordering by discriminant. In [29], Ho–Shankar–Varma found evidence to support this expectation by showing that the average number of 2-torsion elements in the class group of fields associated to binary n-ic forms, ordered either by naive height or by Julia invariant, coincided with the values predicted from the heuristics.

Remarkably, in all of the cases above (see also [14]), the averages remain the same when one imposes finitely many local conditions or even an *acceptable family* of local conditions. We call a set of local conditions *acceptable* if for large enough primes p, it includes all fields with discriminant indivisible by p^2. It then becomes natural to ask about the effect of global conditions on the averages. Bhargava–Hanke–Shankar found in [10] that monogenicity had the effect of doubling the average number of non-trivial elements in the 2-torsion part of the class group of cubic fields! In the first chapter of this thesis, we generalised this result to all odd degrees.

Theorem 2.1.4 ([40]). *Let $n \geq 3$ be an odd integers. Let $\mathfrak{R}$ be an acceptable family of monogenised fields ordered by naive height. The average number of 2-torsion elements in the class group of fields in $\mathfrak{R}$ satisfies the bound:*

$$\mathrm{Avg}(\mathrm{Cl}_2, \mathfrak{R}) \leq 1 + \frac{2}{2^{r_1+r_2-1}}$$

with equality conditional on a tail estimate.

Despite remarkable progress on refining, understanding and streamlining these heuristics (see [47, 43, 46, 3, 4, 34, 33]), nothing has been proposed so far to describe the distribution of p-torsion in the class group for "bad" primes p. In particular, there is no prediction for the average number of the 2-torsion elements in the class group, narrow class group or oriented class group of number fields of even degree.

The most serious reason for this gap seems to be the presence of *genus theory.* Indeed, it is unclear how the $1/\mathrm{Aut}(\cdot)$ count of Cohen–Lenstra mixes with the "deterministic" input from genus theory. Even in the quadratic case, Gerth conjectured [28] and Smith proved [41], that one needs to throw out the 2-part to recover a $1/\mathrm{Aut}(\cdot)$ count. A less severe obstacle concerns the presence of 2-nd roots of unity in the base field. Malle showed that roots of unity in the base field affected Cohen–Lenstra averages and it is unknown to what extent this phenomenon intervenes when genus theory is involved.

We now clarify what we mean by *genus theory*. In *Disquisitiones Arithmeticae* [27], Gauss determined the structure of the 2-torsion part of the narrow class group of quadratic fields by relating it to binary quadratic forms with a composition law.

Theorem 2.1.5 (Gauss's genus theory [27])**.** *Let K be a quadratic field, $\Delta_{K/\mathbb{Q}}$ its discriminant and $\mathrm{Cl}_2^+[K]$ the 2-torsion in its narrow class group. Let $\omega(\Delta_{K/\mathbb{Q}})$ denote the number of distinct prime factors of $\Delta_{K/\mathbb{Q}}$. Then the 2-torsion in the narrow class group of K is given by*

$$\mathrm{Cl}_2^+[K] \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\omega(\Delta_{K/\mathbb{Q}})-1}.$$

The basic idea behind this theorem is that a ramified prime q contributes a 2-torsion element to the narrow class group since it must split as $(q) = \mathfrak{a}^2$ for some prime ideal $\mathfrak{a}$. It is this feature that we call *genus theory* in the context of Cohen–Lenstra averages. More precisely, if p is a "bad" prime, then primes q which ramify as $(q) = \mathfrak{a}^p$ for some ideal $\mathfrak{a}$ are a source of p-torsion elements in the class group.

In this paper, we bound the average number of 2-torsion elements in the *class group*, *narrow class group* and *oriented class group* of monogenised fields of even degree at least 4 (unramified at 2) (and compute it precisely conditional on a tail estimate). These averages are the first of their kind (in degree at least 3) to be calculated in a setting where genus theory, roots of unity, and global conditions all play a part.

2.1.2 Preliminary definitions

A number field K of degree n is said to be *monogenic* if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. The element α is called a *monogeniser* of the field K. A *monogenised* field is the data (K, α) of a monogenic field together with a choice of monogeniser. It is known that a monogenic field has finitely many monogenisers up to transformations of the form $\alpha \mapsto \pm\alpha + m$ for some $m \in \mathbb{Z}$. Futhermore, it is expected that 100% of monogenic fields possess a unique monogeniser up to transformations of the form $\alpha \mapsto \pm\alpha + m$ for some $m \in \mathbb{Z}$, see [13]. This motivates the following definition.

Definition 2.1.6. Two monogenised fields (K, α) and (K', α') are said to be isomorphic if there exists a field isomorphism from K to K' taking α to $\pm\alpha' + m$ for some $m \in \mathbb{Z}$.

Thus, we expect monogenised fields to be statistically equivalent to monogenic fields when computing averages. Nevertheless, suppose a statement holds for a "positive proportion" of *monogenised* fields. In that case, the same statement is true for "infinitely many" *monogenic* fields by using the arguments of [29] combined with the construction of strongly quasi-reduced elements of [13].

The height we choose for monogenised fields has a convenient interpretation. Each isomorphism class of monogenised field contains a unique element (K, α_0) with the property that $0 \leq \operatorname{tr}(\alpha_0) < n$. If $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ is the minimal polynomial of α_0, we define the *naive height* of the isomorphism class to be:

$$H\Big([(K, \alpha_0)] \Big) = \max_i \Big\{ |a_i|^{1/i} \Big\}.$$

We denote by $\mathfrak{R}^{r_1, r_2}$ the collection of isomorphism classes of monogenised S_n-fields of signature (r_1, r_2) ordered by naive height. In Section 2.2, we will see that the set of monogenised fields is in natural bijection with the set of monic degree n polynomials. This bijection equips the set of monogenised fields with a natural local measure, and we can speak of families of fields in $\mathfrak{R}^{r_1, r_2}$ associated with sets of local specifications $(\Sigma_p)_p$ on monic polynomials.

We will also need the notion of oriented class groups to state our results. An *oriented ideal* is a pair (I, ε) consisting of a fractional ideal I together with an orientation $\varepsilon = \pm 1$. We say that an oriented ideal is a *principal oriented ideal* if it is of the form $((\alpha), \operatorname{sgn}(N(\alpha)))$.

Definition 2.1.7. The *oriented class group*, $\mathrm{Cl}^*(K)$, of a number field K consists of the set of oriented fractional ideals of K modulo the principal oriented fractional ideals. The operation is component-wise multiplication.

Recall that $\mathrm{Cl}^*(K)$ is isomorphic to the usual class group of K if K has a unit of negative norm and is a $\mathbb{Z}/2\mathbb{Z}$ extension of the usual class group if K does not have a unit of negative norm, [9]. Notice that when K does not have a unit of negative norm, 2-torsion in the oriented class group is not always twice as big as 2-torsion in the usual class group. The reason is that some 4-torsion elements in the oriented class group could map to 2-torsion elements in the ordinary class group under the forgetful map.

2.1.3 Outline of the results

To quantify the contribution of genus theory in each of our averages, we introduce a local quantity that tracks the proportion of fields in the family which are *evenly ramified* at p, i.e. where $(p) = \mathfrak{a}^2$ for some ideal $\mathfrak{a}$.

Definition 2.1.8. Let $\mathfrak{R} \subset \mathfrak{R}^{r_1, r_2}$ be a family of fields corresponding to an acceptable family of local specifications $\Sigma = (\Sigma_p)_p$. We define $r_p(\mathfrak{R})$, the *even ramification density* of $\mathfrak{R}$ at p, as the density in Σ_p of elements of Σ_p which are evenly ramified at p.

Theorem 2.1.9 (Main theorem). *Let $\mathfrak{R} \subset \mathfrak{R}^{r_1, r_2}$ be a family of fields (unramified at 2 and with local conditions at 2 given modulo 2) corresponding to an acceptable family of local specifications $\Sigma = (\Sigma_p)_p$ and let $r_p(\mathfrak{R})$ denotes its even ramification density at p.*

If $r_1 = 0$, the average number of 2-torsion elements in the class group, narrow class group, and oriented class group of fields in $\mathfrak{R}$ satisfies the bound:

$$\operatorname{Avg}(\mathrm{Cl}_2, \mathfrak{R}) = \operatorname{Avg}(\mathrm{Cl}_2^+, \mathfrak{R}) = \frac{1}{2}\operatorname{Avg}(\mathrm{Cl}_2^*, \mathfrak{R}) \leq \prod_{p \neq 2} (1 + r_p(\mathfrak{R})) \left(1 + \frac{2}{2^{r_2}}\right) + \frac{1}{2^{r_2}} \qquad (2.1)$$

with equality conditional on tail estimate.

If $r_1 > 0$, the average number of 2-torsion elements in the oriented class group of fields in $\mathfrak{R}$ satisfies the bound:

$$\operatorname{Avg}(\mathrm{Cl}_2^*, \mathfrak{R}) \leq \prod_{p \neq 2}(1 + r_p(\mathfrak{R})) \left(1 + \frac{2}{2^{r_1+r_2-1}}\right) + \frac{1}{2^{r_1+r_2-1}} \tag{2.2}$$

with equality conditional on tail estimate.

If $r_1 > 0$, the average number of 2-torsion elements in the narrow class group of fields in $\mathfrak{R}$ satisfies the bound:

$$\operatorname{Avg}(\mathrm{Cl}_2^+, \mathfrak{R}) \leq \prod_{p \neq 2}(1 + r_p(\mathfrak{R})) \left(1 + \frac{2}{2^{\frac{n}{2}}}\right) + \frac{1}{2^{r_2}} \tag{2.3}$$

with equality conditional on tail estimate.

If $r_1 > 0$, the average number of 2-torsion elements in the class group of fields in $\mathfrak{R}$ satisfies the bound:

$$\begin{aligned}\operatorname{Avg}(\mathrm{Cl}_2, \mathfrak{R}) \leq \frac{1}{2} \prod_{p\equiv 1 \ mod \ 4}(1 + r_p(\mathfrak{R})) &\left(\prod_{p\equiv 3 \ mod \ 4}(1 - r_p(\mathfrak{R})) + \prod_{p\equiv 3 \ mod \ 4}(1 + r_p(\mathfrak{R})) \right) \\ + \frac{1 + 2\prod_{p\neq 2}(1 + r_p(\mathfrak{R}))}{2^{r_1+r_2}}&\end{aligned} \tag{2.4}$$

with equality conditional on tail estimate.

Remark 2.1.10. The various infinite products of the form $\prod_p(1 \pm r_p(\mathfrak{R}))$ appearing in the averages above converge. This is because $r_p(\mathfrak{R})$ is $O(p^{-2})$ as $p \to \infty$ for any acceptable family, as can be seen by combining estimates from [1] and [36].

These averages have several interesting consequences, two of which were mentioned earlier. First, they generalise a theorem of Gauss stating that there are infinitely many quadratic fields with odd class number. For odd degree, Ho–Shankar–Varma proved in [29] that there are infinitely many fields of fixed odd degree and signature (r_1, r_2) with odd class number. For even degree, the corresponding problem has remained open for degrees strictly larger than 4. In degree 4, the result is known for biquadratic fields (see Koymans–Pagano in [31]) but not for S_4-fields to the author's knowledge.

Corollary 2.1.11. *Let $n \geq 4$ be an even integer. For each choice of signature (r_1, r_2), there are infinitely many degree n monogenic S_n-fields with signature (r_1, r_2) that have odd class number.*

Second, the averages show that there are infinitely many even degree fields with units of every signature.

Corollary 2.1.12. *Let $n \geq 4$ be an even integer. For each choice of signature (r_1, r_2) with*

$r_2 = 2$ if $n = 4$ and $r_2 > 0$ otherwise, there are infinitely many fields of degree n and signature (r_1, r_2) that have units of units of every signature.

Third, we also deduce asymptotic lower bounds for the number of monogenised fields having odd class numbers when these fields are ordered by discriminant just as in [29].

Corollary 2.1.13. *Let $n \geq 4$ be an even integer, (r_1, r_2) a choice of signature, and $\mathfrak{R} \subset \mathfrak{R}^{r_1,r_2}$ an acceptable family of non-evenly ramified monogenised fields. Then the following asymptotic estimates hold.*

1) $\#\left\{R \in \mathfrak{R} \colon\ |\mathrm{Disc}\,(R)| < X \,\mathrm{and}\, 2 \nmid |\mathrm{Cl}\,(R)|\right\} \gg X^{\frac{1}{2}+\frac{1}{n}}$.

2) For $r_2 = 2$ when $n = 4$, and $r_2 \neq 0$ otherwise, we have

$$\#\left\{R \in \mathfrak{R} \colon\ |\mathrm{Disc}\,(R)| < X \,\mathrm{and}\, 2 \nmid \left|\mathrm{Cl}^{+}\,(R)\right|\right\} \gg X^{\frac{1}{2}+\frac{1}{n}}.$$

3) If $r_1 \neq 0$ and $r_1 + r_2 \geq 3$, we have

$$\#\left\{R \in \mathfrak{R} \colon\ |\mathrm{Disc}\,(R)| < X \,\mathrm{and}\, 2 \nmid |\mathrm{Cl}^{*}\,(R)|\right\} \gg X^{\frac{1}{2}+\frac{1}{n}}.$$

Fourth, conditional on a tail estimate, they show that genus theory is the only added complexity to consider for "bad" primes. Indeed, the formula for $\mathrm{Avg}(\mathrm{Cl}_2, \mathfrak{R})$ when all $r_p(\mathfrak{R}) = 0$ is only slightly different from the one for the average 2-torsion in the class group of monogenised fields of odd degree [40].

Corollary 2.1.14. *Let $n \geq 4$ be an even integers. Let $\mathfrak{R} \subset \mathfrak{R}^{r_1,r_2}$ be a family of fields (unramified at 2 and with local conditions at 2 given modulo 2) corresponding to an acceptable family of local specifications $\Sigma = (\Sigma_p)_p$ and such that the even ramification density at all primes is zero, $r_p(\mathfrak{R}) = 0$.*

The average number of 2-torsion elements in the class group of fields in $\mathfrak{R}$ satisfies the bound:

$$\mathrm{Avg}(\mathrm{Cl}_2, \mathfrak{R}) \leq 1 + \frac{3}{2^{r_1+r_2}},$$

with equality conditional on a tail estimate.

Lastly, they offer hints as to the "right answer" for Cohen–Lenstra averages for "bad" primes.

Remark 2.1.15. The assumption that the families considered are unramified at 2 and have local conditions at 2 given modulo 2 is an artefact of the particulars of the mass computation at 2 and does not change the validity of the "positive proportion" versions of the corollaries above. We expect to be able to remove it in the future and to be able to upgrade the theorems to compute the average value of $|\mathrm{Cl}_2(\mathcal{O})| - \frac{1}{2^{r_1+r_2}}\,|\mathcal{I}_2(\mathcal{O})|$ for orders which are not necessarily maximal.

2.1.4 Strategy

The strategy used to prove the main theorem is roughly the same as that used in [40]. We apply Wood's parametrisation [44, 45] of 2-torsion ideal classes in rings associated to monic binary forms in terms of integral orbits for certain representations to reduce the question to an asymptotic counting problem in the geometry of numbers. The calculation reduces to counting integral orbits for a group acting on a variety. However, unlike in the odd degree case [40], a slight change in the choice of group and variety leads to a significant difference in the arithmetic information that is encoded. This feature is unique to the even degree case and arises because there are fields of even degree which don't possess units of negative norm (in odd degree, the unit -1 has norm -1).

We begin by describing the case of the *oriented class group.* When computing averages for 2-torsion in the oriented class group, the relevant space is the set of $\mathrm{SL}_n(\mathbb{Z})$-orbits of pairs of integral symmetric matrices (A, B) with the constraint $\det(A) = (-1)^{\frac{n}{2}}$. To apply the geometry of numbers, we borrow the idea of [10] and "linearise" the problem by noting that up to $\mathrm{SL}_n(\mathbb{Z})$, there are only finitely many equivalence classes of symmetric integral matrices of determinant $(-1)^{\frac{n}{2}}$. We denote this finite collection by $\mathscr{L}_{\mathbb{Z}}$. Counting $\mathrm{SL}_n(\mathbb{Z})$ orbits on the space of pairs (A, B) with the constraint $\det(A) = (-1)^{\frac{n}{2}}$ is thus reduced to counting $\mathrm{SO}_{A_0}(\mathbb{Z})$ orbits on the space of pairs (A_0, B). We handle this count in the usual way, and we get the inequality of the main theorem conditional on a tail estimate. A new feature unique to the even degree case appears when computing the local masses. There is extra local mass at primes which are evenly ramified!

Now, to compute the average 2-torsion in the *class group*, one cannot directly use the results for the oriented class group. Indeed, when K does not have a unit of negative norm, some 4-torsion elements in the oriented class group map to 2-torsion elements in the usual class group under the forgetful map. These elements are captured by pairs (A, B) where $\det(A) = -1 \cdot (-1)^{\frac{n}{2}}$. This means that we need to run the strategy above on $\mathrm{SL}_n^{\pm}$-orbits on the space of pairs (A, B) of bilinear forms with $\det(A) = \pm 1$. A new feature appears in the final calculation because the local masses for $\det(A) = (-1)^{\frac{n}{2}}$ and $\det(A) = -1 \cdot (-1)^{\frac{n}{2}}$ behave differently at primes congruent to 3 mod 4. This is why the averages for the class group look more complicated than those for the oriented and narrow class groups.

2.1.5 Organisation of the chapter

In Section 2.2 we recall the parametrisation of 2-torsion ideal classes in the oriented class group in terms of SL_n-orbits on pairs integral symmetric matrices. This parametrisation already appears in [9], albeit with a small mistake which we correct. In Sections 2.3-2.6, we run the geometry of numbers arguments to obtain an asymptotic formula for the number of 2-torsion elements in the oriented class group of monogenised fields of height at most X in terms of a product of local volumes dependent on X. Because we use a square-free sieve dependent on a conjectural tail estimate to bound the 2-torsion from below in terms of the product of local volumes, this equality is conditional. In Section 2.7 we compute the total local mass. It is there that we find genus theory at play in the guise of extra orbits at evenly ramified primes. In Sections 2.8 and Section 2.9 we see how the total local masses distribute among the (A_0, B) slices by applying the equidistribution techniques of [40]. Lastly, we complete the proof of the main theorem for the oriented class group in Section 2.10 by summing the A_0 counts over all $A_0 \in \mathscr{L}_{\mathbb{Z}}$. In Section 2.11, we repeat the steps above to prove the main theorem for class groups and narrow class groups. We can recycle most of the counting arguments, but the parametrisation and the final count are much more subtle.

2.2 The parametrisations

2.2.1 The parametrisation of monogenised n-ic rings

In order to count the number of monogenised n-ic rings having bounded height, we will use the following parametrisation in terms of binary n-ic forms:

Definition 2.2.1. Let $U = \mathrm{Sym}_n(2)$ denote the space of binary n-ic forms. We denote by $U_1 \subset U$ the space of all monic binary n-ic forms $f(x, y) = x^n + a_{n-1}x^{n-1}y + \ldots + a_0y^n$. The group GL_2 acts on U via the twisted action $\gamma \cdot f(x, y) := \det(\gamma)^{-1}f((x, y) \cdot \gamma)$ for $\gamma \in \mathrm{GL}_2$ and $f \in U$. Let $F \subset \mathrm{GL}_2$ denote the group of lower triangular unipotent matrices. Then the action of F on U preserves U_1 and yields an action of F on U_1.

We say that a pair (R, α) is a monogenised n-ic ring if R is an n-ic ring and α is an element of R such that $R = \mathbb{Z}[\alpha]$. Two monogenised n-ic rings (R, α) and (R, α') are said to be isomorphic if R and R' are isomorphic via a ring isomorphism sending α to $\alpha' + m$ for some $m \in \mathbb{Z}$. We then have the following explicit parametrisation of monogenised n-ic rings in terms of the orbit data introduced above:

Theorem 2.2.2. *There is a natural bijection between isomorphism classes of monogenised n-ic rings and $F(\mathbb{Z})$-orbits on $U_1(\mathbb{Z})$.*

Proof. Consider the map sending a monic binary n-ic form $f(x, y) \in U_1(\mathbb{Z})$ to the monogenised n-ic ring $R_f := \left(\frac{\mathbb{Z}[\theta]}{(f(\theta,1))}, \theta\right)$. This map descends to a map from $F(\mathbb{Z})\backslash U_1(\mathbb{Z})$ to isomorphism classes of monogenised n-ic rings which we denote by Φ. Indeed, if $g = \gamma \cdot f$ for $\gamma = \left[\begin{smallmatrix} 1 & 0 \\ m & 1 \end{smallmatrix}\right] \in F(\mathbb{Z})$, then $g(\theta, 1) = f(\theta + m, 1)$ and the monogenised ring $\left(\frac{\mathbb{Z}[\theta]}{(f(\theta,1))}, \theta\right)$ is isomorphic to the monogenised ring $\left(\frac{\mathbb{Z}[\theta]}{(f(\theta+m,1))}, \theta\right)$ through $\theta \mapsto \theta + m$. To verify that Φ is surjective, note that it was already surjective as a map from monic binary n-ic forms to monogenised n-ic rings. To verify that Φ is injective, suppose that $\Phi(f) = \left(\frac{\mathbb{Z}[\theta]}{(f(\theta,1))}, \theta\right)$ is isomorphic to $\Phi(g) = \left(\frac{\mathbb{Z}[\omega]}{(g(\omega,1))}, \omega\right)$. Then $\theta \mapsto \omega + m$ for some $m \in \mathbb{Z}$ under this isomorphism. Consequently, $f(\theta, 1) = 0$ in $\Phi(f)$ means that $f(\omega + m, 1) = 0$ in $\Phi(g)$. In other words, the polynomial $g(\omega, 1)$ divides $f(\omega + m, 1)$. But since both are monic, we must have $g(\omega, 1) = f(\omega + m, 1)$. Thus, $g = \left[\begin{smallmatrix} 1 & 0 \\ m & 1 \end{smallmatrix}\right] \cdot f$ and $g = f$ in $F(\mathbb{Z})\backslash U_1(\mathbb{Z})$. □

2.2.2 Orbits of pairs of symmetric bilinear forms

We define the space of pairs of symmetric matrices as well as the resolvent map.

Definition 2.2.3. Let T be a base ring. Let

$$V(T) = T^2 \otimes \mathrm{Sym}^2(T^n)$$

be the space of pairs of symmetric $n \times n$ matrices with coefficients in T. The group $\mathrm{GL}_n(T)$ acts on $V(T)$ by change of basis. In other words, if $\gamma \in \mathrm{GL}_n(T)$ and $(A, B) \in V(T)$, we define

$$\gamma(A, B) = (\gamma^t A\gamma, \gamma^t B\gamma),$$

where γ^t denotes the transpose of γ.

There is a natural map from this space of pairs of matrices, $V(T)$, to the space of polynomials, $U(T)$, called the resolvent map.

Definition 2.2.4 (The resolvent map π)**.** Let T be a base ring. We define the resolvent map $\pi\colon V(T) \to U(T)$ by

$$(A, B) \mapsto \mathrm{disc}(Ax - By) = (-1)^{\frac{n}{2}} \det(Ax - B).$$

We say that a pair $(A, B) \in V(T)$ is non-degenerate if the associated binary form $f_{(A,B)}$ is non-degenerate (has non-zero discriminant).

Example 2.2.5. In contrast to the odd case, when the degree n is even, there might not exist for every $f \in \mathbb{Z}[x, y]$ a pair $(A, B) \in V(\mathbb{Z})$ whose resolvent polynomial is f. For instance, the binary form $-x^2 - y^2$ is not resolvent polynomial of any element of $V(\mathbb{R})$. For monic f, however, the torsor is always non-empty! For example, x^2+y^2 is the resolvent of $\left(\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]\right)$ and $x^2 - y^2$ is the resolvent of $\left(\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]\right)$.

We now describe the rigid parametrisation of pairs of symmetric bilinear forms.

2.2.3 Rigid parametrisation of pairs of symmetric bilinear forms

Let T be a principal ideal domain. Recall the rigid parametrisation of the pairs of bilinear forms $(A, B) \in V(T)$ with resolvent polynomial equal to f in terms of the based fractional ideal data for R_f.

Theorem 2.2.6 ([45])**.** *Take a non-degenerate binary n-ic form $f \in U_1(T)$ and let $R_f = \frac{T[x]}{(f(x))}$. We have a bijection between $\mathrm{SL}_n^{\pm}(T)$-orbits of pairs $(A, B) \in V(T)$ with $f_{(A,B)} = f$ and equivalence classes of pairs (I, δ) where $I \subset R_f$ is an ideal of R_f and $\delta \in R_f^{\times}$ such that $I^2 \subset \delta R_f^{n-3}$ as ideals and $N(I)^2 = N(\delta)N(R_f^{n-3})$. The classes (I, δ) and (I', δ') are equivalent if there exists a $\kappa \in K_f^{\times}$ with the property that $I = \kappa I'$ and $\delta = \kappa^2\delta$.*

2.2.4 $\mathrm{SL}_n(\mathbb{Z})$-orbits and the oriented class group

We now let $\mathrm{SL}_n(T)$ act on V by change of basis. This action corresponds, at the level of equivalence classes of triples $(I, \mathcal{B}, \delta)$, to the action of $\mathrm{SL}_n(T)$ on the basis $\mathcal{B}$ of the fractional ideal I. This action only changes the basis and does not change I, δ, nor the orientation of $\mathcal{B}$. In particular, it does not change the defining conditions:

1) $I^2 \subset \delta R_f^{n-3}$

2) $N(I)^2 = N(\delta)N(R_f^{n-3})$

The rigid parametrisation can be used to describe $\mathrm{SL}_n(\mathbb{Z})$-orbits.

Theorem 2.2.7 ([9]). *Let f be a non-degenerate monic binary n-ic form $f \in U_1(\mathbb{Z})$, let $R_f = \frac{\mathbb{Z}[x]}{(f(x))}$ and $K_f = R_f \otimes_{\mathbb{Z}} \mathbb{Q}$. The $\mathrm{SL}_n(\mathbb{Z})$ orbits on pairs symmetric bilinear forms $(A, B) \in V(\mathbb{Z})$ with $f_{(A,B)} = f$ are in bijection with equivalence classes of triples*

$$(I, \varepsilon, \delta)$$

where $I \subset K_f$ is a fractional ideal of R_f, $\varepsilon = \pm 1$ indicates the orientation of I, and $\delta \in K_f^\times$ is such that $I^2 \subset \delta R_f$ as ideals and the norm equation $N(I)^2 = N(\delta)$ holds (as oriented ideals). Two triples (I, ε, δ) and $(I', \varepsilon', \delta')$ are equivalent if there exists a $\kappa \in K_f^\times$ with the property that $I = \kappa I'$, $\varepsilon = \mathrm{sgn}(N(\kappa))\varepsilon'$ and $\delta = \kappa^2 \delta'$.

We recall the definition of the *oriented class group* of an order in a number field.

Definition 2.2.8. The *oriented class group*, $\mathrm{Cl}^*(\mathcal{O})$, of an order $\mathcal{O}$ consists of the set of oriented fractional ideals of $\mathcal{O}$ modulo the principal oriented fractional ideals of $\mathcal{O}$. We recall that $\mathrm{Cl}^*(\mathcal{O})$ is isomorphic to the usual class group of $\mathcal{O}$ when $\mathcal{O}$ has a unit of negative norm and is $\mathbb{Z}/2\mathbb{Z}$ extension of the usual class group of $\mathcal{O}$ otherwise.

We now describe the relation between $\mathrm{SL}_n(\mathbb{Z})$-orbits and the 2-torsion part of the oriented class group of R_f.

Definition 2.2.9. Let $\mathcal{O}$ be an order in an S_n-field K. A triple (I, ε, δ) consisting of a fractional ideal I of $\mathcal{O}$, $\varepsilon = \pm 1$ indicating an orientation of I, and $\delta \in K^\times$ such that $I^2 \subset \delta\mathcal{O}$ and $N(I)^2 = N(\delta)$ is said to be projective if the ideal I is invertible. Equivalently, a triple (I, ε, δ) is projective if $I^2 = \delta\mathcal{O}$. For an S_n-order $\mathcal{O}$, we write $H^*(\mathcal{O})$ for the set of equivalence classes (in the sense of the theorem above) of projective triples of $\mathcal{O}$. Component wise multiplication turns $H^*(\mathcal{O})$ into a group.

As the oriented class group is comprised of invertible oriented ideals, let us consider the restriction of the parametrisation above to the set $H^*(\mathcal{O})$. Consider the forgetful map:

$$H^*(\mathcal{O}) \longrightarrow \mathrm{Cl}_2^*(\mathcal{O})$$

given by sending a triple forgetting about the δ component. This is a surjective group homomorphism. Let's analyse its kernel.

Elements $(I_0, \varepsilon_0, \delta_0)$ in the kernel of this forgetful map have the property that $I_0 = (\alpha)$ for some α in K as oriented ideals. Thus, $(I_0, \varepsilon_0, \delta_0) \sim ((\alpha), \mathrm{sgn}(\mathrm{N}(\alpha)), \delta_0) \sim (\mathcal{O}, 1, \alpha^{-2}\delta_0)$. Now, $\mathcal{O} = \alpha^{-2}\delta_0\mathcal{O}$ and $1 = N(\alpha^{-2}\delta_0)$. This implies that $(I_0, \varepsilon_0, \delta_0)$ is equivalent to $(\mathcal{O}, 1, u)$ where u is norm 1 unit of $\mathcal{O}^\times$. We are allowed to further mod out u by squares of units of $K^\times$ which fix the oriented ideal $(\mathcal{O}, 1)$. These are precisely the norm 1 units of $\mathcal{O}$. The sequence above can thus be completed to a short exact sequence:

$$1 \longrightarrow \frac{\mathcal{O}^\times_{N\equiv 1}}{(\mathcal{O}^\times_{N\equiv 1})^2} \longrightarrow H^*(\mathcal{O}) \longrightarrow \mathrm{Cl}_2^*(\mathcal{O}) \longrightarrow 1.$$

Applying Dirichlet's unit theorem allows us to compute that:

$$\left|\frac{\mathcal{O}^\times_{N\equiv 1}}{(\mathcal{O}^\times_{N\equiv 1})^2}\right| = \begin{cases} 2^{r_1+r_2} & \text{if } \mathcal{O} \text{ has a unit of norm } -1 \\ 2^{r_1+r_2} & \text{otherwise} \end{cases}.$$

We thus obtain the following formula for the number of elements in $H^*(\mathcal{O})$.

Lemma 2.2.10. *Let $\mathcal{O}$ be an order in an S_n-number field of degree n and signature (r_1, r_2). Then:*

$$|H^*(\mathcal{O})| = 2^{r_1+r_2}\left|\mathrm{Cl}_2^*(\mathcal{O})\right|.$$

We now proceed to the description of the points in the cuspidal regions.

Here is the version of the reducibility criterion in Ho–Shankar–Varma which is valid in even degree. Roughly, for (A, B) to be reducible, all we need is to have the two components of some $\mathrm{SL}_n(\mathbb{Q})$ translate of (A, B) contain a common subsquare which is zero except at possibly one entry on the diagonal.

Lemma 2.2.11 (Even degree distinguished orbits lemma)**.** *$(A, B) \in V(\mathbb{Q})$ is distinguished if and only if there is an $\mathrm{SL}_n(\mathbb{Q})$ translate of (A, B) with the property that*

$$a_{i,j} = b_{i,j} = 0$$

for all $1 \le i, j \le \frac{n}{2}$ except for $i = j = \frac{n}{2}$ for which $a_{\frac{n}{2}\frac{n}{2}} = 0 \neq b_{\frac{n}{2}\frac{n}{2}}$.

Proof. By [39], we know that a self adjoint operator in $V_f(\mathbb{Q})$ is distinguished if and only if there exists a $\mathbb{Q}$ rational $\frac{n-2}{2}$ plane X such that $\mathrm{Span}\{X, TX\}$ is an isotropic $\frac{n-2}{2}+1$ plane. It thus suffices to translate this condition into the second condition in the statement of the lemma.

First, let's suppose that (A, B) are such that $a_{i,j} = b_{i,j} = 0$ for all $1 \le i, j \le \frac{n}{2} - 1$ except for $i = j = \frac{n}{2}$ for which $a_{\frac{n}{2}\frac{n}{2}} = 0 \neq b_{\frac{n}{2}\frac{n}{2}}$. Let $\{e_1, \ldots, e_{\frac{n}{2}}, f_1, \ldots, f_{\frac{n}{2}}\}$ be the standard basis and let $T = A^{-1}B$. Then, let us set $X = \{e_1, \ldots, e_{\frac{n}{2}-1}\}$. We claim that $\mathrm{Span}\{X, TX\}$ is an isotropic $\frac{n}{2}$ plane. Indeed, $B(e_i) \in \mathrm{Span}\{f_1, \ldots, f_{\frac{n}{2}}\}$ for $1 \le i \le \frac{n}{2} - 1$ and thus $A^{-1}B(e_i) \in \mathrm{Span}\{e_1, \ldots, e_{\frac{n}{2}}\}$. Therefore, (A, B) is distinguished in that case.

The other direction is easy. For instance, it follows directly from the arguments of [39] or a direct calculation from Melanie Wood's parametrisation. □

Definition 2.2.12. Let $\mathcal{O}$ be an order. We denote by $\mathcal{I}_2^*(\mathcal{O})$ the 2-torsion subgroup of the oriented ideal group of $\mathcal{O}$.

Proposition 2.2.13. *Let $\mathcal{O}_f$ be an order corresponding to the integral primitive irreducible non-degenerate monic binary form f. Then, $\mathcal{I}_2^*(\mathcal{O}_f)$ is in natural bijection with the set of projective reducible $\mathrm{SL}_n(\mathbb{Z})$-orbits on $V(\mathbb{Z}) \cap \pi^{-1}(f)$.*

In particular, for maximal rings, there are always exactly 2 projective reducible orbits. This will come into play when we calculate the final averages in Section 2.10.

SL_n-orbits over fields and local rings

In this section, we compute the number orbits, and the size of the stabilisers for the action of SL_n on the arithmetic rings $\mathbb{Z}_p$, $\mathbb{Q}$, and $\mathbb{R}$. Let T be a principal ideal domain. We first restate the rigid parametrisation in this case.

Theorem 2.2.14 ([9])**.** *Let f be a non-degenerate monic binary n-ic form $f \in U_1(T)$, let $R_f = \frac{T[x]}{(f(x))}$ and $K_f = R_f \otimes_{\mathbb{Z}} \mathbb{Q}$. The $\mathrm{SL}_n(T)$ orbits on pairs symmetric bilinear forms $(A, B) \in V(T)$ with $f_{(A,B)} = f$ are in bijection with equivalence classes of triples*

$$(I, s, \delta)$$

where $I \subset K_f$ is a fractional ideal of R_f, s is in the fraction field of T and is such that $N(I) = sT$, and $\delta \in K_f^\times$ such that $I^2 \subset \delta R_f$ as ideals and the norm equation $s^2 = N(\delta)$ holds. Two triples (I, s, δ) and (I', s', δ') are equivalent if there exists a $\kappa \in K_f^\times$ with the property that $I = \kappa I'$, $s = N(\kappa)s'$, and $\delta = \kappa^2\delta'$.

Then, we have the following theorem whose proof is straightforward.

Lemma 2.2.15. *The stabiliser in $\mathrm{SL}_n(T)$ corresponds to the 2-torsion of $R_f^\times$ which have norm 1:*

$$R_f^\times[2]_{N\equiv 1}.$$

Remark 2.2.16. It follows that the $\mathrm{SL}_n(\mathbb{Q})$ stabiliser of any element v whose resolvent is irreducible is equal to 2.

Just as in [29], we can compute the number of orbits with the caveat that we need to distinguish the case where f has an odd degree factor, from the case where all of f's factors are even.

Lemma 2.2.17. *Let T be a field or $\mathbb{Z}_p$. Let f be a monic separable, non-degenerate binary form in $U_1(T)$. Then the projective $\mathrm{SL}_n(T)$ orbits of $V(T)$ with resolvent f are in bijection with elements of*

$$(R_f^\times/(R_f^\times)^2)_{N\equiv 1}.$$

if $R_f[2]$ has an element of norm -1 and have a 2-to-1 map to

$$(R_f^\times/(R_f^\times)^2)_{N\equiv 1}$$

if $R_f[2]$ does not have an element of norm -1.

Remark 2.2.18. We can describe the real orbits. Suppose that f is a non-degenerate monic polynomial of degree n with r_1 real roots and $2r_2$ complex roots. If $r_1 = 0$, then there are 2 $\mathrm{SL}_n(\mathbb{R})$ orbits in $V(\mathbb{R})$ with resolvent polynomial f. If $r_1 > 1$, there are 2^{r_1-1} $\mathrm{SL}_n(\mathbb{R})$ orbits in $V(\mathbb{R})$ with resolvent polynomial f. Furthermore, for $r_1 = 0$, the stabiliser has size 2^{r_2} while for $r_1 > 0$ it has size $2^{r_1+r_2-1}$. The size of the stabilizer depends only on r_2 and we denote it by $\sigma(r_2)$.

2.2.5 The counting problem

We first count the average number of 2-torsion elements in the oriented class group of monogenised rings and fields of even degree. To make sense of this, we order monogenised fields using the naive height on the minimal polynomial of a generator of the ring of integers whose trace is contained in $[0, n)$. Take a monic integral polynomial $f(x) = x^n + a_1x^{n-1} + \ldots + a_n \in \mathbb{Z}[x]$. We define the naive height of f by:

$$H(f) := \max\{|a_i|^{1/i}\} = \max\{|a_1|, |a_2|^{1/2}, \ldots, |a_n|^{1/n}\}.$$

Note that H has the property that

$$H(\lambda B) = \lambda H(f)$$

so that H is homogeneous of degree 1. This will be needed when we apply arguments from the geometry of numbers. The goal of the paper is to determine the following averages:

$$\lim_{X\to\infty} \frac{\sum\limits_{\substack{\mathcal{O}\in\mathfrak{R}\\ H(\mathcal{O})<X}} |\mathrm{Cl}_2^*(\mathcal{O})| - |\mathcal{I}_2^*(\mathcal{O})|}{\sum\limits_{\substack{\mathcal{O}\in\mathfrak{R}\\ H(\mathcal{O})<X}} 1},$$

$$\lim_{X\to\infty} \frac{\sum\limits_{\substack{\mathcal{O}\in\mathfrak{R}\\ H(\mathcal{O})<X}} |\mathrm{Cl}_2(\mathcal{O})| - |\mathcal{I}_2(\mathcal{O})|}{\sum\limits_{\substack{\mathcal{O}\in\mathfrak{R}\\ H(\mathcal{O})<X}} 1},$$

and

$$\lim_{X\to\infty} \frac{\sum\limits_{\substack{\mathcal{O}\in\mathfrak{R}\\ H(\mathcal{O})<X}} \left|\mathrm{Cl}_2^+(\mathcal{O})\right| - |\mathcal{I}_2(\mathcal{O})|}{\sum\limits_{\substack{\mathcal{O}\in\mathfrak{R}\\ H(\mathcal{O})<X}} 1},$$

where $\mathfrak{R} \subset \mathfrak{R}^{r_1,r_2}$ is any acceptable family of monogenic rings (an acceptable family is one which includes all rings with squarefree discriminant). The asymptotic formula for the denominator is found in the work of Bhargava–Shankar–Wang, [13].

Theorem 2.2.19 (Bhargava–Shankar–Wang, [13])**.** *Let $S = (S_p)$ be an acceptable collection of local specifications. If $0 \leq b < n$ is fixed and $U_{1,b}$ denotes the set of monic polynomial whose x^{n-1} coefficient is b, then we have*

$$\left|U_{1,b}^{r_2}(S)_{<X}^{\mathrm{irr}}\right| = \mathrm{Vol}(U_{1,b}^{r_2}(\mathbb{R})_{<X}) \prod_p \mathrm{Vol}(S_p) + o(X^{\frac{n(n+1)}{2}-1}).$$

Now $\mathrm{Vol}(S_{\infty,H<X})$ grows like $X^{\frac{n(n+1)}{2}-1}$. Thus, the main term dominates the error term.

2.3 Reduction theory

Fix an element $A \in \mathscr{L}_{\mathbb{Z}}$ and $\delta \in \mathcal{T}(r_2)$. We build a finite cover of the fundamental domain for the action of $\mathrm{SO}_A(\mathbb{Z})$ on $V_A^{r_2,\delta}(\mathbb{R})$.

Definition 2.3.1. The height of an element in $B \in V_A^{r_2,\delta}$ is defined to be the height of the associated resolvent polynomial. That is,

$$H(B) := H(\mathrm{disc}(Ax - By)) = H\left((-1)^{\frac{n}{2}} \det(Ax - B)\right).$$

The construction of [7] can be adapted to give a fundamental set $R_A^{r_2,\delta}$ for the action of $\mathrm{SO}_A(\mathbb{R})$ on $V_A^{r_2,\delta}(\mathbb{R})$ (which could be empty) with the following properties:

1. The set $R_A^{r_2,\delta}$ is a semi-algebraic.
2. If $R_A^{r_2,\delta}(X)$ denotes the set of elements of height at most X, then the coefficients of elements $B \in R_A^{r_2,\delta}(X)$ are bounded by $O(X)$. The implied constant is independent of B.

We define an indicator function that records whether $V_A^{r_2,\delta}(\mathbb{R})$ is empty.

Definition 2.3.2. We define the indicator function

$$\chi_A(\delta) := \begin{cases} 1 & \text{if } V_A^{r_2,\delta}(\mathbb{R}) \neq \emptyset \\ 0 & \text{otherwise} \end{cases}.$$

We can build now build a cover of a fundamental domain for the action of $\mathrm{SO}_A(\mathbb{Z})$ on $V_A^{r_2,\delta}(\mathbb{R})$. To do so, we pick a fundamental domain $\mathcal{F}_A$ for the action of $\mathrm{SO}_A(\mathbb{Z})$ on $\mathrm{SO}_A(\mathbb{R})$ and act on $R_A^{r_2,\delta}$. This gives a $\frac{\sigma(r_2)}{2}$ cover of a fundamental domain for the action of $\mathrm{SO}_A(\mathbb{Z})$ where $\sigma(r_2)$ is the size of the stabiliser in $\mathrm{SO}_A(\mathbb{R})$ of an element $v \in V_A^{r_2,\delta}(\mathbb{R})$.

Proposition 2.3.3. *Let $\mathcal{F}_A$ be a fundamental domain for the action of $\mathrm{SO}_A(\mathbb{Z})$ on $\mathrm{SO}_A(\mathbb{R})$. Then*

1. *If $\chi_A(\delta) = 1$, $\mathcal{F}_A \cdot R_A^{r_2,\delta}$ is an $\frac{\sigma(r_2)}{2}$–fold cover of a fundamental domain for the action of* $\mathrm{SO}_A(\mathbb{Z})$ *on $V_A^{r_2,\delta}(\mathbb{R})$, where we regard $\mathcal{F}_A \cdot R_A^{r_2,\delta}$ as a multiset.*

2. *If $\chi_A(\delta) = 0$, then $\emptyset$ is a fundamental domain.*

Proof. The stabiliser in $\mathrm{SO}_A(\mathbb{R})$ of an element $B \in V_A^{r_2,\delta}(\mathbb{R})$ coincides with the stabiliser in $\mathrm{SL}_n(\mathbb{R})$ of (A, B) which has size $\sigma(r_2)$. The factor of $\frac{1}{2}$ comes from the fact that -1 also always stabilises (A, B). □

Remark 2.3.4. The characteristic functions will be used to define the archimedean mass and will make the final computation more transparent.

2.4 Averaging and cutting off the cusp

For the purpose of cutting off the cusp and averaging, it suffices to work with SO_A instead of SO_A since $\mathrm{SO}_A(\mathbb{Z})\backslash\mathrm{SO}_A(\mathbb{R})$ is in bijection with $\mathrm{SO}_A(\mathbb{Z})\backslash\mathrm{SO}_A(\mathbb{R})$.

There are now two different cases to consider: 1) the case where A is anisotropic over $\mathbb{Q}$ and 2) the case where A is isotropic over $\mathbb{Q}$. For each, we need to show that:

1. the number of absolutely irreducible integral points in the cuspidal region is negligible; and

2. the number of reducible integral points in the main body is negligible.

We define absolutely irreducible points and reducible points and set the notation for the remainder of this section.

Definition 2.4.1. An element $v \in V(\mathbb{Z})$ is said to be absolutely irreducible if v does not correspond to the identity element in the class group and the resolvent of v corresponds to an order in an S_n-field. An element which is not absolutely irreducible is said to be reducible.

We have the following theorem which gives conditions on reducibility.

Theorem 2.4.2 (Reducibility criterion)**.** *Let $(A, B) \in V(\mathbb{Z})$ be such that all the variables in one of the following sets vanish. Then (A, B) is reducible.*

1. ***The modified squares:***

$$\{a_{i,j}, b_{i,j}\}$$

for all $1 \leq i, j \leq \frac{n}{2}$ except for $i = j = \frac{n}{2}$ where $a_{\frac{n}{2}\frac{n}{2}} = 0$.
These pairs correspond to the identity element in the class group.

2. ***The rectangles:***

$$\{a_{ij}, b_{ij} | 1 \leq i \leq k, 1 \leq j \leq n-k\}$$

for some $1 \leq k \leq n-1$.

These pairs correspond to the resolvent having repeated roots.

We define the affine spaces $V_{A,b}$ just as we did in the odd degree case [40].

Definition 2.4.3. Let A be a fixed quadratic form in $\mathscr{L}_{\mathbb{Z}}$ and fix $0 \leq b < n$. We let $V_A \subset V$ denote the space of pairs (A, B), where B is arbitrary. Note that the resolvent map takes V_A to U. Now, we let $V_{A,b}$ denote the inverse image under the resolvent map of the set U_b. It is easy to see that $V_{A,b}$ is an affine subspace of V_A of dimension $\frac{n(n+1)}{2} - 1$.

Definition 2.4.4. Let $S \subset V_{A,b}^{r_2;\delta}(\mathbb{Z}) := V_{A,b}^{r_2;\delta}(\mathbb{R}) \cap V_{A,b}(\mathbb{Z})$ be an $\mathrm{SO}_A(\mathbb{Z})$ invariant set. Denote by $N_H(S;X)$ the number of absolutely irreducible $\mathrm{SO}_A(\mathbb{Z})$-orbits on S that have height bounded by X. For any $L \subset V_A(\mathbb{Z})$, let L^{irr} denote the set of absolutely irreducible elements. Note that any absolutely irreducible element has a resolvent form corresponding to an order $\mathcal{O}$ in an S_n-number field and so $\mathcal{O}^{\times}[2]$ has size 2. As a result, the stabiliser in $\mathrm{SO}_A(\mathbb{Z})$ of absolutely irreducible elements has size 2.

Therefore, we have

$$N_H(S;X) = \frac{2}{\sigma(r_2)} \#\{\mathcal{F}_A \cdot R_A^{r_2,\delta}(X) \cap S^{\mathrm{irr}}\}.$$

The goal of this section is to obtain an asymptotic formula for $N_H(S;X)$.

2.4.1 The case of A anisotropic over $\mathbb{Q}$

When A is anisotropic, we can pick a compact fundamental domain $\mathcal{F}_A$ for the action of $\mathrm{SO}_A(\mathbb{Z})$ on $\mathrm{SO}_A(\mathbb{R})$. It then follows that $\mathcal{F}_A \cdot R_{A,b}^{r_2,\delta}$ is bounded. To estimate the number of absolutely irreducible integral points in the fundamental domain for the action of $\mathrm{SO}_A(\mathbb{Z})$ on $V_{A,b}^{r_2,\delta}$, we apply results from the geometry of numbers directly. We use Davenport's refinement of the Lipschitz method on $\mathcal{F}_A \cdot R_{A,b}^{r_2,\delta}(X)$ to obtain the desired asymptotic formula.

We will need the following version of Davenport's lemma.

Lemma 2.4.5 (Davenport's Lemma)**.** *Let $E \subset \mathbb{R}^n$ be a bounded semi-algebraic multiset with maximum multiplicity at most m which is defined by k algebraic inequalities of each having degree at most l. Let E' be the image of E under any upper/lower triangular unipotent transformation. Then the number of integral points in E' counted with multiplicity is*

$$\mathrm{Vol}(E) + O_{m,k,l}\left(\max\{\mathrm{Vol}(\overline{E}), 1\}\right)$$

where $\mathrm{Vol}(\overline{E})$ *denotes the greatest d-dimensional volume of a projection of E onto a d-dimensional coordinate hyperplane for* $1 \leq d \leq n-1$.

Lemma 2.4.6. *The number of integral points in $\mathcal{F}_A \cdot R_{A,b}^{r_2,\delta}$ which are not absolutely irreducible is bounded by* $o\left(X^{\frac{n(n+1)}{2}-1}\right)$.

Proof. The proof is the same as in [40], and follows directly from adapting the results of Ho–Shankar–Varma [29]. □

We thus obtain the following asymptotic formula for $N_H(S;X)$.

Theorem 2.4.7. *Let $A \in \mathscr{L}_{\mathbb{Z}}$ be anisotropic over $\mathbb{Q}$. We have*

$$N(V_{A,b}^{r_2,\delta}(\mathbb{Z});X) = \frac{1}{\sigma(r_2)}\mathrm{Vol}\left(\mathcal{F}_A \cdot R_{A,b}^{r_2,\delta}(X)\right) + o(X^{\frac{n(n+1)}{2}-1}).$$

2.4.2 The case of A isotropic over $\mathbb{Q}$

The arguments are almost the same as in the odd degree case [40] except for the totally split case where the Iwasawa coordinates change slightly.

Suppose now that A is isotropic over $\mathbb{Q}$. Then there exists an element $g_A \in \mathrm{SL}_n(\mathbb{Q})$ such that $g_A^t A g_A = A_{F_0}$ where

$$A_{F_0} := \begin{pmatrix} & & & & & 1 \\ & & & & \iddots & \\ & & & 1 & & \\ & & F_0 & & & \\ & 1 & & & & \\ \iddots & & & & & \\ 1 & & & & & \end{pmatrix}.$$

where F_0 is a $\mathbb{Q}$ anisotropic form. We define $m = \frac{n-\dim(F_0)}{2}$. We note that $0 < m \leq \frac{n}{2}$.

Now for $K = \mathbb{Q}$ or $\mathbb{R}$, we consider the maps

$$\sigma_V \colon V_{A,b}^{r_2,\delta} \to V_{A_{F_0},b}^{r_2,\delta}$$
$$\sigma_A \colon \mathrm{SO}_A(K) \to \mathrm{SO}_{A_{F_0}}(K)$$

defined by $\sigma_V(A,B) = (A_{F_0}, g_A^t B g_A)$ and $\sigma_A(h) = g_A^t h (g_A^t)^{-1}$. We note that

$$H(A,B) = H(\sigma_V(A,B))$$

since $\pi \circ \sigma_V = \pi$. Furthermore, $\sigma_V(h \cdot v) = \sigma_A(h) \cdot \sigma_V(v)$.

Now, we denote by $\mathcal{L} \subset V_{A_{F_0},b}^{r_2,\delta}(\mathbb{R})$ the lattice $\sigma_V\left(V_{A_{F_0},b}^{r_2,\delta}(\mathbb{Z})\right)$. We denote by $\Gamma \subset \mathrm{SO}_{A_{F_0}}(\mathbb{R})$ the subgroup $\sigma_A(\mathrm{SO}_A(\mathbb{Z}))$. This subgroup is commensurable with $\mathrm{SO}_{A_{F_0}}(\mathbb{Z})$. Therefore, there exists a fundamental domain $\mathcal{F}$ for the action of Γ on $\mathrm{SO}_{A_{F_0}}(\mathbb{R})$ which is contained in a finite union of $\mathrm{SO}_{A_{F_0}}(\mathbb{Q})$ translates of a Siegel domain, $\bigcup_i g_i\mathcal{S}$ for $g_i \in \mathrm{SO}_{A_{F_0}}(\mathbb{Q})$. This is known from [17].

The choice of the standard A_{F_0} as above is convenient at this point. Indeed, we may now choose as our Siegel domain $\mathcal{S}$ the product NTK where we choose K to be compact, N to be a subgroup of the group of lower triangular matrices with 1 on the diagonal and T to be

$$T := \left\{ \begin{pmatrix} t_1^{-1} & & & & & & \\ & \ddots & & & & & \\ & & t_m^{-1} & & & & \\ & & & I_{\dim(F_0)} & & & \\ & & & & t_m & & \\ & & & & & \ddots & \\ & & & & & & t_1 \end{pmatrix} : t_1/t_2 > c, \dots, t_{m-1}/t_m > c, t_m > c \right\}$$

for some constant $c > 0$ if $\dim(F_0) > 0$ and

$$T_0 := \left\{ \begin{pmatrix} t_1^{-1} & & & & & \\ & \ddots & & & & \\ & & t_m^{-1} & & & \\ & & & t_m & & \\ & & & & \ddots & \\ & & & & & t_1 \end{pmatrix} : t_1/t_2 > c, \dots, t_{m-1}/t_m > c, t_{m-1}t_m > c \right\}$$

for some constant $c > 0$ if $\dim(F_0) = 0$. This can be found in many sources, see for instance [16], [38], or [37].

When $m < \frac{n}{2}$, note that $s_i = t_i/t_{i+1}$, $0 \leq i \leq m-1$ and $s_m = t_m$ forms a set of simple roots.

When $m = \frac{n}{2}$, note that $s_i = t_i/t_{i+1}$, $0 \leq i \leq m-1$ and $s_m = t_{m-1}t_m$ forms a set of simple roots.

Moreover, if we denote by e^ρ the exponential of the half sum of the positive roots counted with multiplicities, we have

$$e^\rho = \prod_{i=1}^{m} t_i^{\frac{n}{2}-i}.$$

When $m < \frac{n}{2}$, we find:

$$\begin{aligned} e^\rho &= \prod_{i=1}^{m} t_i^{\frac{n}{2}-i} \\ &= \prod_{i=1}^{m} \left(\prod_{j=i}^{m} s_j \right)^{\frac{n}{2}-i} \\ &= \prod_{i=1}^{m} s_i^{\left(\sum_{j=1}^{i} \frac{n}{2}-j\right)} \\ &= \prod_{i=1}^{m} s_i^{i\left(\frac{n-i-1}{2}\right)}. \end{aligned}$$

When $m = \frac{n}{2}$, we find:

$$\begin{aligned}
e^{\rho} &= \prod_{i=1}^{m} t_i^{\frac{n}{2}-i} \\
&= \prod_{i=1}^{m-2} \left((s_{m-1}s_m)^{-\frac{1}{2}} \prod_{j=i}^{m} s_j \right)^{\frac{n}{2}-i} (s_{m-1}s_m)^{\frac{1}{2}} \\
&= \prod_{i=1}^{m-2} s_i^{i\left(\frac{n-i-1}{2}\right)} (s_{m-1}s_m)^{\frac{1}{2}} (s_{m-1}s_m)^{\frac{1}{2}(m-2)(\frac{n}{2}-\frac{m-1}{2})} \\
&= \prod_{i=1}^{m-2} s_i^{i\left(\frac{n-i-1}{2}\right)} (s_{m-1}s_m)^{\frac{n(n-2)}{16}}.
\end{aligned}$$

We now fix some notation for our choice of Haar measure on $G = \mathrm{SO}_{A_{F_0}}$. We let dg denote the Haar measure on G, dn denote the Haar measure on the unipotent group N, and dk denote the Haar measure on the compact group K. For every $1 \leq i \leq m$ we write $d^{\times}t_i = \frac{dt_i}{t_i}$ and $d^{\times}s_i = \frac{ds_i}{s_i}$. Furthermore, we write $dt = \prod_{i=1}^{m} dt_i$, $d^{\times}t = \prod_{i=1}^{m} d^{\times}t_i$ and $ds = \prod_{i=1}^{m} ds_i$, $d^{\times}s = \prod_{i=1}^{m} d^{\times}s_i$.

Changing variables between the t-coordinates and the s-coordinates gives us

$$d^{\times}t = d^{\times}s.$$

Therefore, if $m < \frac{n}{2}$, the Haar measure is given in NTK-coordinates by

$$\begin{aligned}
dg &= e^{-2\rho} du\, d^{\times}t\, dk \\
&= \prod_{i=1}^{m} t_i^{2i-n} du\, d^{\times}t\, dk \\
&= \prod_{i=1}^{m} s_i^{i(i+1-n)} du\, d^{\times}s\, dk.
\end{aligned}$$

Therefore, if $m = \frac{n}{2}$, the Haar measure is given in NTK-coordinates by

$$\begin{aligned}
dg &= e^{-2\rho} du\, d^{\times}t\, dk \\
&= \prod_{i=1}^{m} t_i^{2i-n} du\, d^{\times}t\, dk \\
&= \prod_{i=1}^{m-2} s_i^{i(i+1-n)} (s_{m-1}s_m)^{-\frac{n(n-2)}{8}} du\, d^{\times}s\, dk.
\end{aligned}$$

We define the main body and the cuspidal region of the multiset $\mathcal{F}_A \cdot R_{A,b}^{r_2,\delta}$.

Definition 2.4.8 (Main body and cuspidal region)**.** The *main body* consists of all the elements of $\mathcal{F}_A \cdot R_{A,b}^{r_2,\delta}$ for which $|b_{11}| \geq 1$. The *cuspidal region* consists of all the elements for which $|b_{11}| < 1$.

We are now ready to cut off the cuspidal region.

Construction 2.4.9 (Partial order on the coordinates of V_A)**.** We construct a partial order on the $n(n+1)/2$ coefficients $\{b_{ij}\}$ for $i \leq j$. These define a set of coordinates on B which we denote by U.

Definition 2.4.10. The weight $w(b_{ij})$ of an element $b_{ij} \in U$ is the factor by which b_{ij} scales under the action of $(t_1^{-1}, \ldots, t_m^{-1}, 1, \ldots, 1, t_m, \ldots, t_1) \in T$.

We are now ready to define a partial order on U.

Definition 2.4.11 (A partial order on subsets of U)**.** Let b and b' be two elements of the set of coordinates U. We say that $b \prec b'$ if in the expression for $w(b)$ in the s-coordinates, the exponents of the variables $s_1, \cdots, s_m$ are smaller than or equal to the corresponding exponents appearing in the expression for $w(b')$ in the s-coordinates. The relation $\prec$ defines a partial order on U.

Example 2.4.12. We have $b_{11} \prec b_{m+1\,m+1}$ because $w(b_{11}) = s_1^{-2} \cdots s_m^{-2}$ while $w(b_{m+1\,m+1}) = 1 = s_1^0 \cdots s_m^0$. On the other hand, $b_{1\,n-2}$ and $b_{2\,n-3}$ cannot be compared in $\prec$ because $w(b_{1\,n-2}) = s_1^{-1}s_2^{-1}$ while $w(b_{2\,n-3}) = s_2^{-1}s_3^{-1}$. The important thing to note about the partial order $(U, \prec)$ is that if $i \leq i'$ and $j \leq j'$ then

$$b_{ij} \prec b_{i'j'}.$$

We now cut off the cusp in two specific cases which will serve as bases cases in the proof by induction of the general case.

Example 2.4.13 (Base case of cusp cutting induction for $\dim(F_0) = 0$)**.** We now do the case $n = 4$, $m = 2$ before moving on to cutting off the cusp in the general case. We see that torus elements act as follows:

$$t \cdot v = \begin{pmatrix} t_1^{-2} & t_1^{-1}t_2^{-1} & t_1^{-1}t_2 & 1 \\ t_1^{-1}t_2^{-1} & t_2^{-2} & 1 & t_1t_2^{-1} \\ t_1^{-1}t_2 & 1 & t_2^2 & t_1t_2 \\ 1 & t_1t_2^{-1} & t_1t_2 & t_1^2 \end{pmatrix} O(X).$$

We can now easily read off the weights. The Haar measure takes the form

$$dg = du\,\frac{1}{t_1^2}d^\times t\,dk = du\,\frac{1}{s_1s_2}d^\times s\,dk.$$

For any subset of U containing b_{11}, we now want to estimate

$$\widetilde{I}(U_1, X) = X^{9-\#U_1}\int_{t\in T_X}\prod_{b_{ij}\notin U_1} w(b_{ij})\frac{d^\times s}{s_1s_2}.$$

We only need to look at proper subsets of $U_0 = \{b_{11}\}$ which are left-closed and up-closed. Recall that we have the bound $s_1 < CX$ and $s_2 < C^2X^2$. Let's compute:

$$\widetilde{I}(\{b_{11}\}, X) = X^8 \int_{s_1=c}^{CX} \int_{s_2=c}^{C^2X^2} s_1 s_2 \frac{d^\times s}{s_1 s_2} = X^8 \int_{s_1=c}^{CX} \int_{s_2=c}^{C^2X^2} d^\times s = O_\epsilon(X^{8+\epsilon})$$

The number of absolutely irreducible elements in the cusp which have height at most X is thus $O_\epsilon(X^{9-1+\epsilon})$ and we just barely cut off the cusp! The induction argument given below shows that in all other cases, we have much more room.

We recall that we had

$$N_H(S;X) = \frac{1}{\sigma(r_2)} \#\{\mathcal{F}_A \cdot R_A^{r_2,\delta}(X) \cap S^{\text{irr}}\}.$$

Now, let G_0 be a bounded open K-invariant ball in $\mathrm{SO}_{A_{F_0}}(\mathbb{R})$. We can average the above expression by the usual trick to obtain

$$N_H(S;X) = \frac{1}{\sigma(r_2)\mathrm{Vol}(G_0)} \int_{h\in\mathcal{F}_A} \#\left\{hG_0 R_A^{r_2,\delta}(X) \cap S^{\text{irr}}\right\} dh.$$

Now, again we may use classical arguments to see that the number of absolutely irreducible integral points in the cusp which have height at most X is

$$O\left(\int_{t\in T} \#\left\{tG_0 R_A^{r_2,\delta}(X) \cap S^{\text{irr}}\right\} \prod_{i=1}^{m} s_i^{i(i+1-n)} d^\times s\right)$$

when $m < \frac{n}{2}$ and

$$O\left(\int_{t\in T} \#\left\{tG_0 R_A^{r_2,\delta}(X) \cap S^{\text{irr}}\right\} \prod_{i=1}^{m} s_i^{i(i+1-n)} (s_{m-1}s_m)^{-\frac{n(n-2)}{8}} d^\times s\right)$$

when $m = \frac{n}{2}$.

Definition 2.4.14. Let $U_1 \subset U$ be a subset of the set of coordinates. We define

$$V_A(\mathbb{R})(U_1) = \{B \in V_A(\mathbb{R})\colon\ |b_{ij}(B)| < 1 \text{ if and only if } b_{ij} \in U_1\}$$

and

$$V_A(\mathbb{Z})(U_1) = V_A(\mathbb{Z}) \cap V_A(\mathbb{R})(U_1).$$

It thus suffices to show that

$$N(V_A(\mathbb{Z})(U_1); X) = O_\epsilon\left(X^{\left(\frac{n(n+1)}{2}-1\right)-1+\epsilon}\right)$$

for all $U_1 \subset U$ such that $b_{11} \in U_1$.

We get a priori bounds on the coordinates s_i from the reducibility criterion. Let C be an absolute constant such that CX bounds the absolute value of all the coordinates of elements $B \in G_0 R_A^{r_2,\delta}(X)$.

If $(s_1^{-1}, \ldots, s_m^{-1}, 1, \ldots, 1, s_m, \ldots, s_1) \in T$ and $CXw(b_{i_0\, n-i_0}) < 1$ for some $i_0 \in \{1, \ldots, m\}$, then $CXw(b_{ij}) < 1$ for all $i \leq i_0$ and $j \leq n - i_0$. This comes from the ***Rectangles*** part of the criterion for reducibility. Therefore, we may assume that

$$s_i < CX$$

for all $i \in \{1, \ldots, m\}$ if $m < \frac{n}{2}$ and that

$$s_i < CX$$

for all $i \in \{1, \ldots, m-1\}$ and $s_m < C^2X^2$ if $m = \frac{n}{2}$.

Let us write T_X to denote the set of $t = (s_1, \ldots, s_m) \in T$ which satisfy this condition.

Now Davenport's lemma gives us

$$\begin{aligned} N(V(\mathbb{Z})(U_1); X) &= O\left(\int_{t \in T_X} \mathrm{Vol}(tG_0 R_A^{r_2,\delta}(X) \cap V(\mathbb{R})(U_1)) \prod_{i=1}^{m} s_i^{i(i+1-n)} d^\times s\right) \\ &= O\left(X^{\left(\frac{n(n+1)}{2}-1\right)-\#U_1} \int_{t \in T_X} \prod_{b_{ij} \notin U_1} w(b_{ij}) \prod_{i=1}^{m} s_i^{i(i+1-n)} d^\times s\right). \end{aligned}$$

for $m < \frac{n}{2}$ and

$$\begin{aligned} N(V(\mathbb{Z})(U_1); X) &= O\left(\int_{t \in T_X} \mathrm{Vol}(tG_0 R_A^{r_2,\delta}(X) \cap V(\mathbb{R})(U_1)) \prod_{i=1}^{m} s_i^{i(i+1-n)} d^\times s\right) \\ &= O\left(X^{\left(\frac{n(n+1)}{2}-1\right)-\#U_1} \int_{t \in T_X} \prod_{b_{ij} \notin U_1} w(b_{ij}) \prod_{i=1}^{m} s_i^{i(i+1-n)} (s_{m-1}s_m)^{-\frac{n(n-2)}{8}} d^\times s\right). \end{aligned}$$

for $m = \frac{n}{2}$.

So, we have reduced our problem to one of estimating the following integrals.

Definition 2.4.15. The active integral of $U_1 \subset U$ is defined by

$$\widetilde{I}(U_1, X) := X^{\left(\frac{n(n+1)}{2}-1\right)-\#U_1} \int_{t \in T_X} \prod_{b_{ij} \notin U_1} w(b_{ij}) \prod_{i=1}^{m} s_i^{i(i+1-n)} d^\times s$$

if $m < \frac{n}{2}$ and

$$\widetilde{I}(U_1, X) := X^{\left(\frac{n(n+1)}{2}-1\right)-\#U_1} \int_{t \in T_X} \prod_{b_{ij} \notin U_1} w(b_{ij}) \prod_{i=1}^{m} s_i^{i(i+1-n)} (s_{m-1}s_m)^{-\frac{n(n-2)}{8}} d^\times s$$

if $m = \frac{n}{2}$.

Recall, that $b_{ij} \prec b_{i_0j_0}$ when $i \leq i_0$ and $j \leq j_0$. Therefore, if $U_1 \subset U$ contains $b_{i_0j_0}$ but not b_{ij}, then

$$\widetilde{I}\,(U_1 \setminus \{b_{i_0j_0}\} \cup \{b_{ij}\}, X) \geq \widetilde{I}(U_1, X).$$

As a result, in order to obtain an upper bound for $\widetilde{I}(U_1, X)$ we may assume that if $b_{i_0j_0} \in U_1$, then $b_{ij} \in U_1$ for all $i \leq i_0$ and $j \leq j_0$. In other words, we may assume that U_1 is both left closed and up closed.

Furthermore, such a set U_1 cannot contain any element on, or on the right of, the off anti-diagonal within the first m-rows, since otherwise, we would be in the case of ***Rectangles*** in the reducibility criterion and so $N(V(\mathbb{Z})(U_1); X) = 0$.

Definition 2.4.16. We define the subset $U_0 \subset U$ as the set of coordinates b_{ij} such that $i \leq j$, $i \leq m$, and $i + j \leq n - 1$.

Now, if $m = \frac{n}{2}$, every element in $V(\mathbb{Z})(U_0)$ is reducible and it suffices to consider $\widetilde{I}(U_1, X)$ for all $U_1 \subsetneq U_0$. On the other hand if $m < \frac{n}{2}$ we need to consider all $U_1 \subset U$.

Since the product of the weight over all the coordinates is 1, we make the following definition.

Definition 2.4.17. We define for a subset $U_1 \subset U$

$$I(U_1, X) = X^{\frac{n(n+1)}{2}-1}\widetilde{I}(U_1, X) = X^{-\#U_1} \int_{t \in T_X} \prod_{b_{ij} \in U_1} w(b_{ij})^{-1} \prod_{i=1}^{m} s_i^{i(i+1-n)} d^\times s$$

if $m < \frac{n}{2}$ and

$$I(U_1, X) = X^{\frac{n(n+1)}{2}-1}\widetilde{I}(U_1, X) = X^{-\#U_1} \int_{t \in T_X} \prod_{b_{ij} \in U_1} w(b_{ij})^{-1} \prod_{i=1}^{m} s_i^{i(i+1-n)} (s_{m-1}s_m)^{-\frac{n(n-2)}{8}} d^\times s$$

if $m = \frac{n}{2}$.

We are now ready to state and prove the main cusp cutting lemma.

Lemma 2.4.18 (Main cusp cutting estimate)**.** *Let U_1 be a non-empty proper subset of U_0. Then we have the estimate*

$$I(U_1, X) = O_\epsilon\left(X^{-1+\epsilon}\right).$$

We also have $I(\emptyset) = O_\epsilon(1)$ and $I(U_0) = O_\epsilon(1)$.

Proof. We prove this lemma via a combinatorial argument using induction on m. Recall that $n = 2m + \dim(F_0)$. The cases $\dim(F_0) \geq 2$ and $\dim(F_0) = 0$ are slightly different and we handle them separately.

The case $\dim(F_0) = 0$ is actually the same as is [39] with a different normalization of the height. It thus suffices to deal with the case $\dim(F_0) \geq 2$. In this case, the estimates obtained in odd degree apply just as well here, thereby completing the proof. □

Proposition 2.4.19. *The number of absolutely irreducible elements in the cusp which have height at most X is $O_\epsilon\left(X^{\left(\frac{n(n+1)}{2}-1\right)-1+\epsilon}\right)$.*

We also find that the number of reducible elements in the main body is negligible.

Lemma 2.4.20. *The number of integral points in the main body of $\mathcal{F}_A \cdot R_{A,b}^{r_2,\delta}$ which are not absolutely irreducible is bounded by $o\left(X^{\frac{n(n+1)}{2}-1}\right)$.*

Proof. The proof is identical to the anisotropic case. □

Therefore, we find the following asymptotic formula.

Theorem 2.4.21. *Let $A \in \mathscr{L}_{\mathbb{Z}}$ be isotropic over $\mathbb{Q}$. We have*

$$N(V_{A,b}^{r_2,\delta}(\mathbb{Z}); X) = \frac{1}{\sigma(r_2)}\mathrm{Vol}\left(\mathcal{F}_A \cdot R_{A,b}^{r_2,\delta}(X)\right) + o\left(X^{\frac{n(n+1)}{2}-1}\right).$$

Remark 2.4.22. We can upgrade the results of this section to deal with A not having the property that the $\mathbb{Q}$ degree of SO_A is equal to its $\mathbb{R}$ degree. To do so, it suffices to push through the arguments with generalised Siegel sets instead of the usual Siegel sets. We can deal with the compact parts of M^0 which appear by using the o-minimal version of Davenport's lemma (see [2]).

2.5 Sieving to very large and acceptable collections

In this section, we determine the desired asymptotic formulas. The results and proof contained in this section are adaptations of those of [29] to the case at hand and are repeated from Part I [40] for the reader's convenience. We begin with the definition of a family of local specifications.

Definition 2.5.1 (Collection of local specifications and the associated set)**.** We say that a family $\Lambda_{A,b} = (\Lambda_{A,b,\nu})_\nu$ of subsets $\Lambda_{A,b,\nu} \subset V_{A,b}(\mathcal{O}_\nu)$ indexed by the places ν of $\mathbb{Q}$ is a **collection of local specifications** if: 1) for each finite prime p the set $\Lambda_{A,b,p} \subset V_{A,b}(\mathbb{Z}_p) \setminus \{\Delta = 0\}$ is an open subset which is non-empty and whose boundary has measure 0; and 2) at $\nu = \infty$, we have $\Lambda_{A,b,\infty} = V_{A,b}^{r_2,\delta}(\mathbb{R})$ for some integer r_2 with $0 \leq r_2 \leq \frac{n-1}{2}$ and $\delta \in \mathcal{T}(r_2)$. We associate the set $\mathcal{V}(\Lambda_{A,b}) := \{v \in V_{A,b}(\mathbb{Z}) \colon \forall \nu\, (v \in \Lambda_{A,b,\nu})\}$ to the collection of local specifications $\Lambda_{A,b} = (\Lambda_{A,b,\nu})_\nu$.

2.5.1 Sieving to projective elements

Definition 2.5.2. For a prime p, we denote by $V_{A,b}(\mathbb{Z}_p)^{\mathrm{proj}}$ the set of elements $v \in V_{A,b}(\mathbb{Z}_p)$ which correspond to a projective pair (I, δ) (i.e. with the property that $I^2 = (\delta)$) under the parametrisation.

We have

$$V_{A,b}^{r_2,\mathrm{proj}}(\mathbb{Z}) = V_{A,b}^{r_2}(\mathbb{Z}) \bigcap \left(\bigcap_p V_{A,b}^{\mathrm{proj}}(\mathbb{Z})\right).$$

Definition 2.5.3. We denote by $W_{A,b,p}$ the set of elements in $V_{A,b}(\mathbb{Z})$ that do not belong to $V_{A,b}^{\mathrm{proj}}(\mathbb{Z}_p)$.

As in Part I [40], we have the following estimate on the number of element of $W_{A,b,p}$ for large p.

Theorem 2.5.4. *We have*

$$N\left(\cup_{p\geq M}W_{A,b,p},X\right)=O\left(\frac{X^{\frac{n(n+1)}{2}-1}}{M^{1-\epsilon}}\right)+o\left(X^{\frac{n(n+1)}{2}}\right)$$

where the implied constant is independent of X and M.

We now define the concept of *very large collections of local specifications* and state the asymptotic formula. Roughly, a collection of local specifications is very large if for large enough primes p, it includes all elements of V which are projective at p.

Definition 2.5.5 (Very large collection of local specifications)**.** Let $\Lambda_{A,b}=\left(\Lambda_{A,b,\nu}\right)_\nu$ be a collection of local specifications. We say that $\Lambda_{A,b}$ is **very large** if for all but finitely many primes, the sets $\Lambda_{A,b,p}$ contains all projective elements of $V_{A,b}(\mathbb{Z}_p)$. If $\Lambda_{A,b}$ is very large, we also say that the associated set $\mathcal{V}(\Lambda_{A,b})$ is very large.

Theorem 2.5.6. *Let r_2 be an integer such that $0\leq r_2\leq\frac{n-1}{2}$ and let $\delta\in\mathcal{T}(r_2)$. Then for a very large collection of local specifications $\Lambda_{A,b}$ such that $\Lambda_{A,b,\infty}=V_{A,b}^{r_2,\delta}(\mathbb{R})$, we have*

$$N(\mathcal{V}(\Lambda_{A,b}^{\delta}),X)=\frac{1}{\sigma(r_2)}\mathrm{Vol}(\mathcal{F}_A\cdot R_{A,b}^{r_2,\delta}(X))\prod_p\mathrm{Vol}(\Lambda_{A,b,p})+o\left(X^{\frac{n(n-1)}{2}-1}\right),$$

where the volume of subsets of $V_{A,b}(\mathbb{R})$ are computed with respect to the Euclidean measure normalized so that $V_{A,b}(\mathbb{Z})$ has covolume 1 and the volumes of subsets of $V_{A,b}(\mathbb{Z}_p)$ are computed with respect to the Euclidean measure normalized so that $V_{A,b}(\mathbb{Z}_p)$ has measure 1.

2.5.2 Sieving to acceptable sets conditional on a tail estimate

We now define the concept of *acceptable collections of local specifications* and state the asymptotic formula. Roughly, a collection of local specifications is acceptable if for large enough primes p, it includes all fields with discriminant indivisible by p^2.

Definition 2.5.7 (Acceptable collection of local specifications)**.** Let $\Lambda_{A,b}=\left(\Lambda_{A,b,\nu}\right)_\nu$ be a collection of local specifications. We say that $\Lambda_{A,b}$ is **acceptable** if for all but finitely many primes, the set $\Lambda_{A,b,p}$ contains all elements of $V_{A,b}(\mathbb{Z}_p)$ whose discriminant is not divisible by p^2. If $\Lambda_{A,b}$ is acceptable, we also say that the associated set $\mathcal{V}(\Lambda_{A,b})$ is acceptable.

We have the following unconditional asymptotic inequality.

Theorem 2.5.8. *Let $\Lambda_{A,b} = (\Lambda_{A,b,\nu})_\nu$ be an acceptable collection of local specifications.*

$$N(\mathcal{V}(\Lambda_{A,b}), X) \leq \frac{1}{\sigma(r_2)} \mathrm{Vol}(\mathcal{F}_A \cdot R^{r_2,\delta}_{A,b}(X)) \prod_p \mathrm{Vol}(\Lambda_{A,b,p}) + o\left(X^{\frac{n(n+1)}{2}-1}\right),$$

where the volume of subsets of $V_{A,b}(\mathbb{R})$ are computed with respect to the Euclidean measure normalized so that $V_{A,b}(\mathbb{Z})$ has covolume 1 and the volumes of subsets of $V_{A,b}(\mathbb{Z}_p)$ are computed with respect to the Euclidean measure normalized so that $V_{A,b}(\mathbb{Z}_p)$ has measure 1.

The following tail estimates are known for $n = 4$ as will be shown in a forthcoming work with Arul Shankar and likely to be true for $n \geq 6$. Indeed they follow from a suitable version of the *abc* conjecture by work of Granville.

Definition 2.5.9. Let p be a prime. We denote by $\mathcal{W}_{A,b,p}$ the set of elements $v \in V_{A,b}(\mathbb{Z})$ such that $p^2 \mid \Delta(v)$.

Conjecture 2.5.10 (Conjectural tail estimates)**.** *We have*

$$N(\cup_{p\geq M}\mathcal{W}_{A,b,p}, X) = O\left(\frac{X^{\frac{n(n+1)}{2}-1}}{M^{1-\epsilon}}\right) + o\left(X^{\frac{n(n+1)}{2}-1}\right)$$

where the implied constant is independent of X and M.

We have the following asymptotic formula conditional on the preceding tail estimates.

Theorem 2.5.11. *Suppose that the preceding tail estimates hold. Let r_2 be an integer such that $0 \leq r_2 \leq \frac{n-1}{2}$ and let $\delta \in \mathcal{T}(r_2)$. Then for an acceptable collection of local specifications $\Lambda_{A,b}$ such that $\Lambda_{A,b}(\infty) = V^{r_2,\delta}_{A,b}(\mathbb{R})$ we have*

$$N(\mathcal{V}(\Lambda^\delta_{A,b}), X) = \frac{1}{\sigma(r_2)} \mathrm{Vol}(\mathcal{F}_A \cdot R^{r_2,\delta}_{A}(X)) \prod_p \mathrm{Vol}(\Lambda_{A,b,p}) + o\left(X^{\frac{n(n-1)}{2}-1}\right),$$

where the volume of subsets of $V_{A,b}(\mathbb{R})$ are computed with respect to the Euclidean measure normalized so that $V_{A,b}(\mathbb{Z})$ has covolume 1 and the volumes of subsets of $V_{A,b}(\mathbb{Z}_p)$ are computed with respect to the Euclidean measure normalized so that $V_{A,b}(\mathbb{Z}_p)$ has measure 1.

2.6 Change of measure formula

To compute the volumes of sets and multi-sets in $V_{A,b}(\mathbb{R})$ and $V_{A,b}(\mathbb{Z}_p)$, we have the following version of the change of variable formula. Let dv and df denote the Euclidean measure on $V_{A,b}$ and $U_{A,b}$ respectively normalized so that $V_{A,b}(\mathbb{Z})$ and $U_{A,b}(\mathbb{Z})$ have co-volume 1. Furthermore, let ω be an algebraic differential form generating the rank 1 module of top degree left-invariant differential forms on SO_A over $\mathbb{Z}$.

Proposition 2.6.1 (Change of measure formula)**.** *Let $K = \mathbb{Z}_p, \mathbb{R}$ or $\mathbb{C}$,. Let $|\cdot|$ denote the usual absolute value on K and let $s\colon U_{1,b}(K) \to V_{A,b}(K)$ be a continuous map such that*

$\pi(f) =$ for each $f \in U_{1,b}$. Then there exists a rational non-zero constant $\mathcal{J}_A$, independent of K and s, such that for any measurable function ϕ on $V_{A,b}(K)$, we have:

$$\int\limits_{\mathrm{SO}_A(K)\cdot s(U_{1,b}(K))} \phi(v)\,dv = |\mathcal{J}_A| \int_{f\in U_{1,b}(K)} \int_{g\in \mathrm{SO}_A(K)} \phi(g\cdot s(f))\,\omega(g)\,df$$

$$\int\limits_{V_{A,b}(K)} \phi(v)dv = |\mathcal{J}_A| \int\limits_{\substack{f\in U_{1,b}(K)\\ \Delta(f)\neq 0}} \left(\sum_{v\in \frac{V_{A,b}(K)\cap\pi^{-1}(f)}{\mathrm{SO}_A(K)}} \frac{1}{\#\mathrm{Stab}_{\mathrm{SO}_A(\mathbb{Z}_p)}(v)} \int\limits_{g\in\mathrm{SO}_A(K)} \phi(g\cdot v)\,\omega(g) \right) df$$

where $\frac{V_{A,b}(K)\cap\pi^{-1}(f)}{\mathrm{SO}_A(K)}$ denotes a set of representatives for the action of $\mathrm{SO}_A(\mathbb{Z}_p)$ *on $V_{A,b}(\mathbb{Z}_p)\cap \pi^{-1}(f)$.*

We can simplify the second integral above by introducing a local mass.

Definition 2.6.2 (Local mass formula)**.** Let p be a prime, $f \in U_{1,b}(\mathbb{Z}_p)$ and $A \in \mathscr{L}_{\mathbb{Z}}$. We define the local mass of f at p in A, $m_p(f, A)$ to be

$$m_p(f,A) := \sum_{v\in \frac{V_{A,b}(\mathbb{Z}_p)\cap\pi^{-1}(f)}{\mathrm{SO}_A(\mathbb{Z}_p)}} \frac{1}{\#\mathrm{Stab}_{\mathrm{SO}_A(\mathbb{Z}_p)}(v)}.$$

We now have the following formula for the local volumes appearing in the asymptotic formula.

Proposition 2.6.3. *We have*

$$\mathrm{Vol}\left(\mathcal{F}_A\cdot R^{r_2,\delta}_{A,b}(X)\right) = \chi_A(\delta)\,|\mathcal{J}_A|\,\mathrm{Vol}(\mathcal{F}^{\delta}_A)\mathrm{Vol}(U(\mathbb{R})^{r_2}_{H<X}).$$

Let $S_p \subset U_{1,b}(\mathbb{Z}_p)$ be a non-empty open set whose boundary has measure 0*. Consider the set $\Lambda_{A,b,p} = V_{A,b}(\mathbb{Z}_p)\cap\pi^{-1}(S_p)$. Then we have*

$$\mathrm{Vol}(\Lambda_{A,b,p}) = |\mathcal{J}_A|_p\,\mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p)) \int_{f\in S_p} m_p(f,A)\,df.$$

2.7 The product of local volumes and the local mass

The calculation of the total mass is slightly more delicate here, and we divide it into a couple of lemmas. Recall from Lemma 2.2.17 that the number of orbits divided by the stabiliser over $\mathbb{Z}_p$ (which is equal to $(R_f^{\times})[2]_{N\equiv 1}$ in this case) is always equal to $2\frac{1}{R_f^{\times}[2]}(R_f^{\times}/(R_f^{\times})^2)_{N\equiv 1}$. We thus focus our attention on $\frac{1}{R_f^{\times}[2]}(R_f^{\times}/(R_f^{\times})^2)_{N\equiv 1}$.

Lemma 2.7.1 (Total quantity)**.** *Let R be a non-degenerate ring of degree n over $\mathbb{Z}_p$. The quantity*

$$\frac{|R^{\times}/(R^{\times})^2|}{|R^{\times}[2]|}$$

is equal to 1 *if* $p \neq 2$ *and to* 2^n *if* $p = 2$.

Proof. The following sequence is exact:

$$0 \longrightarrow R^\times[2] \longrightarrow R^\times \xrightarrow{(\cdot)^2} R^\times \longrightarrow R^\times/(R^\times)^2 \longrightarrow 0.$$

Let us note that $R^\times$ is the direct product of a finite abelian subgroup F and $\mathbb{Z}_p^n$ (written additively). The exact sequence above is thus the direct sum of the corresponding exact sequence on F and on $\mathbb{Z}_p^n$. Computing the Euler characteristic on F we find:

$$\frac{|F/F^2|}{|F[2]|} = 1.$$

The exact sequence on the free part takes the form:

$$0 \longrightarrow \mathbb{Z}_p^n \xrightarrow{\times 2} \mathbb{Z}_p^n \longrightarrow \mathbb{Z}_p^n/(2\mathbb{Z}_p)^n \longrightarrow 0.$$

In order to extract information from this part, we need to treat the cases $p \neq 2$ and $p = 2$ separately. For $p \neq 2$, the map $\times 2$ is surjective so the free part contributes a factor of 1. For $p = 2$, the module $(2\mathbb{Z}_2)^n$ has index 2^n in $\mathbb{Z}_2^n$ and so the free part contributes a factor of 2^n. This completes the proof the lemma. □

Lemma 2.7.2 (Norm isolation)**.** *Let* R *be a non-degenerate ring of degree* n *over* $\mathbb{Z}_p$. *Let* N *denote the norm map from* $N\colon R^\times/(R^\times)^2 \to \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$. *The quantity*

$$\frac{|(R^\times/(R^\times)^2)_{N\equiv 1}|}{|R^\times[2]|}$$

is equal to $\frac{1}{|N(R^\times)|}$ *if* $p \neq 2$ *and to* $\frac{2^n}{|N(R^\times)|}$ *if* $p = 2$.

Proof. The first isomorphism theorem gives us $N(R^\times) \cong \frac{(R^\times/(R^\times)^2)}{(R^\times/(R^\times)^2)_{N\equiv 1}}$. Since everything is finite we get:

$$\left|R^\times/(R^\times)^2)_{N\equiv 1}\right| = \frac{|R^\times/(R^\times)^2)|}{|N(R^\times)|}$$

and the result follows from the previous lemma. □

In particular, we get the following statement concerning the total local masses for maximal rings which are not evenly ramified at 2. It follows from the previous lemma and the fact that if $\mathcal{O}^\times$ is the ring of integers of a finite extension of $\mathbb{Q}_p$, the norm map $N\colon \mathcal{O}^\times/(\mathcal{O}^\times)^2 \to \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$ is surjective when the extension has odd ramification degree and not surjective when $p \neq 2$ and the extension has even ramification degree.

Lemma 2.7.3. *The total local mass for* $f \in \mathbb{Z}_p[x]$ *maximal and not evenly ramified at* p *is* *given by:*

$$m_p(f) = \begin{cases} 2^{n-1} & \text{if } p = 2 \\ 1 & \text{if } p \neq 2 \end{cases}.$$

The total local mass for $f \in \mathbb{Z}_p[x]$, $p \neq 2$, maximal and evenly ramified is given by:

$$m_p(f) = 2.$$

Remark 2.7.4. Thus, even ramification has a doubling effect on the total local mass. Heuristically, this is because if f has even ramification at the prime p, then the ideal (p) splits into a product of prime ideals $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ each appearing to an even power e_i, and thus we can write $(p) = I^2$. So we have constructed a 2-torsion ideal in the oriented ideal class group. The fact that the total mass is twice as large means that on average, these ideals contribute one extra generator to the 2-torsion in the oriented ideal class group.

2.7.1 Computing the local masses

We now define the infinite mass and compute $m_p(f, A)$ for all $p \neq 2, \infty$.

Definition 2.7.5 (The infinite mass)**.** Let $A \in \mathscr{L}_{\mathbb{Z}}$ and r_2 be an integer such that $0 \leq r_2 \leq \frac{n-1}{2}$. The infinite mass of A with respect to r_2 is defined to be

$$m_\infty(r_2, A) = \sum_{\delta \in \mathcal{T}(r_2)} \chi_A(\delta).$$

The following lemma isolates the main properties of the local masses for all p, including the Archimedean place.

Lemma 2.7.6 (Main properties of the local masses)**.** *The local masses $m_p(f, A)$ and $m_\infty(A)$ have the following properties.*

1. *If $\gamma \in \mathrm{SL}_n(\mathbb{Z}_p)$, we have*
$$m_p(f, \gamma^t A \gamma) = m_p(f, A).$$

2. *If $\gamma \in \mathrm{SL}_n(\mathbb{R})$, we have*
$$m_\infty(r_2, \gamma^t A \gamma) = m_\infty(r_2, A).$$

3. *In particular, if A_1 and A_2 are unimodular integral matrices lying in the same genus, we have*
$$m_p(f, A_1) = m_p(f, A_2)$$
for all primes p and
$$m_\infty(r_2, A_1) = m_\infty(r_2, A_2).$$

4. *The sum of $m_2(f, A)$ over a set of representatives for the unimodular orbits of the action*

of $\mathrm{SL}_n(\mathbb{Z}_2)$ *on* $\mathrm{Sym}_n(\mathbb{Z}_2)$ *is*

$$\sum_{\substack{A \in \frac{\mathrm{Sym}_n(\mathbb{Z}_2)}{\mathrm{SL}_n(\mathbb{Z}_2)} \\ \det(A)=1 \in \frac{\mathbb{Z}_2}{\mathbb{Z}_2^2}}} m_2(f,A) = m_2(f).$$

5. *The sum of* $m_p(f,A)$ *over a set of representatives for the unimodular orbits of the action of* $\mathrm{SL}_n(\mathbb{Z}_p)$ *on* $\mathrm{Sym}_n(\mathbb{Z}_p)$ *is*

$$\sum_{\substack{A \in \frac{\mathrm{Sym}_n(\mathbb{Z}_p)}{\mathrm{SL}_n(\mathbb{Z}_p)} \\ \det(A)=1 \in \frac{\mathbb{Z}_p}{\mathbb{Z}_p^2}}} m_p(f,A) = m_p(f).$$

6. *The sum of* $m_\infty(r_2, A)$ *over a set of representatives for unimodular the orbits of the action of* $\mathrm{SL}_n(\mathbb{R})$ *on* $\mathrm{Sym}_n(\mathbb{R})$ *is*

$$\sum_{\substack{A \in \frac{\mathrm{Sym}_n(\mathbb{R})}{\mathrm{SL}_n(\mathbb{R})} \\ \det(A)=1 \in \frac{\mathbb{R}}{\mathbb{R}^2}}} m_\infty(r_2, A) = 2^{r_1 - 1}$$

if $r_1 > 0$ *and*

$$\sum_{\substack{A \in \frac{\mathrm{Sym}_n(\mathbb{R})}{\mathrm{SL}_n(\mathbb{R})} \\ \det(A)=1 \in \frac{\mathbb{R}}{\mathbb{R}^2}}} m_\infty(r_2, A) = 2$$

if $r_1 = 0$.

We can now compute the local masses for all $p \neq 2, \infty$ by noting that there is a unique $\mathrm{SL}_n(\mathbb{Z}_p)$ equivalence class of bilinear forms with determinant 1.

Corollary 2.7.7 (Local masses for $p \neq 2, \infty$)**.** *For* $A \in \mathscr{L}_\mathbb{Z}$ *and* $p \neq 2, \infty$ *we have*

$$m_p(f,A) = \begin{cases} 2 & \text{if } f \text{ is evenly ramified at } p \\ 1 & \text{otherwise} \end{cases}.$$

The computation of the local masses at $p = 2, \infty$ is more delicate and is the object of the following sections.

2.8 Point count and the 2-adic mass

We compute the 2-adic mass for polynomials which are not evenly ramified at the prime 2. We begin by showing that this restriction allows us to exclude type II genera from our considerations.

Theorem 2.8.1 (Type II genera and over-ramification at 2)**.** *Let A be the hyperbolic unimodular symmetric bilinear form over $\mathbb{F}_2$. Then the image under the resolvent map of $V_A(\mathbb{F}_2)$ lies in*

$$\mathbb{F}_2[x^2] = \Big(\mathbb{F}_2[x]\Big)^2.$$

Therefore, pairs whose first component is hyperbolic modulo 2 correspond to ideal classes of monogenic orders which are "over-ramified" at 2 in the sense that (2) splits as a product of even powers of primes ideals. In particular, the discriminant of the resolvent polynomials of such pairs is not squarefree at 2. Furthermore, the statement of the theorem holds if $\mathbb{F}_2$ is replaced by any ring of characteristic 2.

Proof. Without loss of generality we can let A be the matrix with 1 s on the anti-diagonal and B be any symmetric matrix. We proceed by examining the resolvent polynomial from the perspective of universal algebra. Let us introduce the multivariate polynomial

$$\Phi(X_1, \ldots, X_{\frac{n}{2}}, Y_{\frac{n}{2}}, \ldots, Y_1) \in \mathbb{F}_2[X_1, \ldots, X_{\frac{n}{2}}, Y_{\frac{n}{2}}, \ldots, Y_1]$$

which we define as the determinant:

$$\begin{vmatrix} b_{1\,1} & b_{1\,2} & \vdots & b_{1\,n-1} & Y_1 + b_{1\,n} \\ b_{2\,1} & b_{2\,2} & \vdots & Y_2 + b_{2\,n-1} & b_{2\,n} \\ \cdots & \cdots & \iddots & \cdots & \cdots \\ b_{n-1\,1} & X_2 + b_{n-1\,2} & \vdots & b_{n-1\,n-1} & b_{n-1\,n} \\ X_1 + b_{n\,1} & b_{n\,2} & \vdots & b_{n\,n-1} & b_{n\,n} \end{vmatrix}.$$

For this polynomial, we claim that there is a natural bijection between the set of monomials which are divisible by Y_i but not X_i and the set of monomials which are divisible by X_i but not Y_i. Indeed, the map which exchanges X_i and Y_i is easily seen to give a bijection since the matrix (b_{ij}) is symmetric and $-1 = 1$ in a ring of characteristic 2.

We can use this observation to deduce that $\Phi(X, \ldots, X, X, \ldots, X) = \pi(A, B)$ contains only monomials of even degree. For this purpose, it is suffices to show that the only monomials appearing in $\Phi(X_1, \ldots, X_{\frac{n}{2}}, X_{\frac{n}{2}}, \ldots, X_1)$ are those of even degree (the degree of the monomial $X_1^{e_1} X_2^{e_2} \cdots X_{\frac{n}{2}}^{e_n}$ is defined to be $e_1 + \ldots + e_n$). But this follows immediately from the observation made in the previous paragraph. Indeed, a monomial of odd degree in the polynomial $\Phi(X_1, \ldots, X_{\frac{n}{2}}, X_{\frac{n}{2}}, \ldots, X_1)$ comes from a sum of monomials in $\Phi(X_1, \ldots, X_{\frac{n}{2}}, Y_{\frac{n}{2}}, \ldots, Y_1)$, the elements of this sum coming in pairs one of which is divisible by X_i but not by Y_i for some $1 \leq i \leq \frac{n}{2}$, the other of which is divisible by Y_i but not by X_i, and which are such that exchanging the variable X_i and Y_i maps each of the monomials to the other. □

We can now apply the methods of [40] to obtain the 2-adic masses for polynomials which are not over-ramified at the prime 2.

By the classification of quadratic forms over $\mathbb{Z}_2$, there are only two odd, determinant $(-1)^{\frac{n}{2}}$ classically integral quadratic forms over $\mathbb{Z}_2$ of even dimension n up to $\mathrm{SL}_n(\mathbb{Z}_2)$ equivalence. See for instance [30] or [24].

For $n \equiv 0 \mod 4$ we can take:

$$\mathfrak{M}_1 = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix}, \quad \mathfrak{M}_{-1} = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & -1 & \\ & & & & & -1 \end{pmatrix}.$$

For $n \equiv 2 \mod 4$ we can take:

$$\mathfrak{M}_1 = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & -1 \end{pmatrix}, \quad \mathfrak{M}_{-1} = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & -1 & & \\ & & & & -1 & \\ & & & & & -1 \end{pmatrix}.$$

Remark 2.8.2. We have chosen the subscripts above to match the Hasse–Witt symbol of the respective bilinear forms.

We now state the constraint imposed on the total mass by the local mass.

Lemma 2.8.3. *For any $f \in U_{1,b}(\mathbb{Z}_2)$, we have*

$$m_2(f, \mathfrak{M}_1) + m_2(f, \mathfrak{M}_{-1}) = 2^{n-1}.$$

We give names to the integral of the 2-adic masses over S_2.

Definition 2.8.4. Define

$$c_2(n, \mathfrak{M}_1) = \int_{f \in S_2} m_2(f, \mathfrak{M}_1)\, df$$
$$c_2(n, \mathfrak{M}_{-1}) = \int_{f \in S_2} m_2(f, \mathfrak{M}_{-1})\, df.$$

Lemma 2.8.5 (Point count)**.** *Let $S_2 \subset U_{1,b}(\mathbb{Z}_2)$ be a local condition on the space of non-over-ramified monic polynomials at the prime 2 defined modulo 2. Denote by $\Lambda_{\mathfrak{M}_1}(2)$ and $\Lambda_{\mathfrak{M}_{-1}}(2)$ the pre-images in $V_{\mathfrak{M}_1,b}(\mathbb{Z}_2)$ and $V_{\mathfrak{M}_{-1},b}(\mathbb{Z}_2)$ respectively of S_2 under the resolvent map π. Then the volumes of these two sets are equal*

$$\mathrm{Vol}(\Lambda_{\mathfrak{M}_1}(2)) = \mathrm{Vol}(\Lambda_{\mathfrak{M}_{-1}}(2)).$$

Proof. The canonical representatives $\mathfrak{M}_1$ and $\mathfrak{M}_{-1}$ are equal modulo 2. Since $\Lambda_{\mathfrak{M}_1}(2)$ and $\Lambda_{\mathfrak{M}_{-1}}(2)$ are defined by imposing congruence conditions modulo 2 on $V_{\mathfrak{M}_1,b}(\mathbb{Z}_2)$ and $V_{\mathfrak{M}_{-1},b}(\mathbb{Z}_2)$, the result follows. □

As in [40] we find.

Lemma 2.8.6. *The rational numbers giving the Jacobian change of variables for $\mathfrak{M}_1$ and $\mathfrak{M}_{-1}$ are equal when the volume forms on the associated special orthogonal groups are those associated to point counting modulo increasing powers of p:*

$$\mathcal{J}_{\mathfrak{M}_1} = \mathcal{J}_{\mathfrak{M}_{-1}}.$$

In particular, their 2-adic valuations are the same

$$\left|\mathcal{J}_{\mathfrak{M}_1}\right|_2 = \left|\mathcal{J}_{\mathfrak{M}_{-1}}\right|_2.$$

Finally, we compute the ratio of the 2-adic masses by finding the ratio between the volumes of the 2-adic points of the special orthogonal groups $\mathrm{SO}_{\mathfrak{M}_1}$ and $\mathrm{SO}_{\mathfrak{M}_{-1}}$.

Proposition 2.8.7 (Volume ratio for Type I genera)**.** *We have*

$$\frac{c_2\left(n,\mathfrak{M}_1\right)}{c_2\left(n,\mathfrak{M}_{-1}\right)} = \frac{\mathrm{Vol}(\Lambda_{\mathfrak{M}_1}(2))\left(\left|\mathcal{J}_{\mathfrak{M}_{-1}}\right|_2 \mathrm{Vol}(\mathrm{SO}_{\mathfrak{M}_{-1}}(\mathbb{Z}_2))\right)}{\mathrm{Vol}(\Lambda_{\mathfrak{M}_{-1}}(2))\left(\left|\mathcal{J}_{\mathfrak{M}_1}\right|_2 \mathrm{Vol}(\mathrm{SO}_{\mathfrak{M}_1}(\mathbb{Z}_2))\right)} = \frac{\mathrm{Vol}(\mathrm{SO}_{\mathfrak{M}_{-1}}(\mathbb{Z}_2))}{\mathrm{Vol}(\mathrm{SO}_{\mathfrak{M}_1}(\mathbb{Z}_2))}$$
$$= \frac{2^{n-2} \pm_8 2^{\frac{n-2}{2}}}{2^{n-2} \mp_8 2^{\frac{n-2}{2}}},$$

where $\pm_8$ *is* $+$ *if* n *is congruent to* 0 *or* $2 \mod 8$ *and* $-$ *otherwise.*

Proof. This calculation is the same as in [40]. Care is needed to keep track of the of the *octane values* of $\mathfrak{M}_1$ and $\mathfrak{M}_{-1}$ for different congruence classes of n modulo 8 resulting in the cases for $\pm_8$. We find that $\mathfrak{M}_1$ has octane value 0 (mod 8) if $n \equiv 0 \pmod 8$, 4 (mod 8) if $n \equiv 4 \pmod 8$, 0 (mod 8) if $n \equiv 2 \pmod 8$, and 4 (mod 8) if $n \equiv 6 \pmod 8$. On the other hand, we find that $\mathfrak{M}_{-1}$ has octane value 4 (mod 8) if $n \equiv 0 \pmod 8$, 0 (mod 8) if $n \equiv 4 \pmod 8$, 4 (mod 8) if $n \equiv 2 \pmod 8$, and 0 (mod 8) if $n \equiv 6 \pmod 8$. □

We thus obtain the values for the 2-adic mass.

Corollary 2.8.8. *The 2-adic masses satisfy the following identities:*

$$c_2(n,\mathfrak{M}_1) + c_2(n,\mathfrak{M}_{-1}) = 2^{n-1}\mathrm{Vol}(S_2)$$
$$c_2(n,\mathfrak{M}_1) - c_2(n,\mathfrak{M}_{-1}) = \pm_8 2^{\frac{n-2}{2}+1}\mathrm{Vol}(S_2).$$

In particular:

$$\begin{aligned} c_2(n, \mathfrak{M}_1) &= \left(2^{n-2} \pm_8 2^{\frac{n-2}{2}}\right) \operatorname{Vol}(S_2) \\ c_2(n, \mathfrak{M}_{-1}) &= \left(2^{n-2} \mp_8 2^{\frac{n-2}{2}}\right) \operatorname{Vol}(S_2) \end{aligned}$$

where $\pm_8$ *is* $+$ *if* n *is congruent to* 0 *or* $2 \mod 8$ *and* $-$ *otherwise.*

2.9 The infinite mass

In this section, we calculate the infinite masses. We begin by describing the distribution of δ among the different A slices as in [40].

Definition 2.9.1. Let $\delta \in \mathcal{T}(r_2)$. Define $\Omega_-(\delta)$ to be the number of negative eigenvalues of the first component of the orbit associated to δ.

Theorem 2.9.2 (Signature distribution of first components of $\mathcal{T}(r_2)$)**.** *If* $r_1 > 0$*, the number of* δ *in* $\mathcal{T}(r_2)$ *such that* $\Omega_-(\delta) = q$ *is*

$$\binom{r_1}{q - r_2}.$$

In particular, if $q < r_2$*, there are no* $\delta \in \mathcal{T}(r_2)$ *which land in any* V_A *for which* A *has signature* $(n-q, q)$*. If* $r_1 = 0$*, there are* 2 *orbits which both land on the split slice.*

Proof. The proof is the same as in [40]. □

To make the final calculation more transparent, we state the relation between the value of $\Omega_-(\cdot)$ and the Hasse–Witt symbol. We also obtain a couple of useful combinatorial identities.

If $n \equiv 0 \pmod 4$, we are considering real bilinear forms with determinant 1. Among those, the ones which satisfy $\Omega(\delta) \equiv 0 \pmod 4$ have Hasse–Witt symbol 1, while those which satisy $\Omega(\delta) \equiv 2 \pmod 4$ have Hasse–Witt symbol -1.

If $n \equiv 2 \pmod 4$, we are considering real bilinear forms with determinant -1. Among those, the ones which satisfy $\Omega(\delta) \equiv 1 \pmod 4$ have Hasse–Witt symbol 1, while those which satisy $\Omega(\delta) \equiv 3 \pmod 4$ have Hasse–Witt symbol -1.

We now define the infinite mass of an integral quadratic form $A \in \mathscr{L}_{\mathbb{Z}}$ to be the number of $\delta \in \mathcal{T}(r_2)$ whose associated orbit in V intersects V_A non-trivially.

Definition 2.9.3 (The infinite mass)**.** Let $A \in \mathscr{L}_{\mathbb{Z}}$ and r_2 be an integer such that $0 \le r_2 \le \frac{n-1}{2}$. The infinite mass of A with respect to r_2 is defined to be

$$m_\infty(r_2, A) = \sum_{\delta \in \mathcal{T}(r_2)} \chi_A(\delta).$$

Above, we found that these infinite masses were equal to specific binomial coefficients. We now compute closed forms for certain *total infinite masses* arising when summing infinite masses over genera having the same 2-adic reduction.

Definition 2.9.4 (The total infinite mass)**.** Let $\mathcal{G}_2$ be set of equivalence classes of unimodular bilinear forms over $\mathbb{Z}_2$ of dimension n. Then $\mathcal{G}_2 = \{\mathfrak{M}_{-1}, \mathfrak{M}_1, \mathfrak{M}_{\text{Type II}}\}$ where $\mathfrak{M}_{-1}$ and $\mathfrak{M}_1$ are the odd unimodular forms with Hasse–Witt symbol -1 and 1 respectively (canonical representative were described in the last section) and $\mathfrak{M}_{\text{Type II}}$ is simply the bilinear form with 1 on the anti-diagonal. Note that $\mathfrak{M}_{\text{Type II}}$ has Hasse–Witt symbol 1 if $n \equiv 0, 2 \pmod 8$ and -1 if $n \equiv 4, 6 \pmod 8$. The *total infinite mass*, $c_\infty(r_1, \mathfrak{M}_\blacksquare)$, associated to an element $\mathfrak{M}_\blacksquare \in \mathcal{G}_2$ is defined to be the sum of the infinite masses over all genera whose $\mathbb{Z}_2$ reduction coincides with $\mathfrak{M}_\blacksquare$.

Calculating the total infinite mass now becomes a question of evaluating sums of binomial coefficients in arithmetic progression.

Corollary 2.9.5. *The infinite masses are as follows:*

$$c_\infty(r_1, \mathfrak{M}_1) = 2^{r_1-2} \pm_8 2^{\frac{r_1-2}{2}}$$
$$c_\infty(r_1, \mathfrak{M}_{-1}) = 2^{r_1-2} \mp_8 2^{\frac{r_1-2}{2}}.$$

where $\pm_8$ *is* $+$ *if* n *is congruent to* 0 *or* 2 (mod 8) *and* $-$ *otherwise. Furthermore,* $c_\infty(r_1, \mathfrak{M}_{\textit{Type II}}) = c_\infty(r_1, \mathfrak{M}_1)$ *if* $n \equiv 0, 2 \pmod 8$ *and* $c_\infty(r_1, \mathfrak{M}_{\textit{Type II}}) = c_\infty(r_1, \mathfrak{M}_{-1})$ *if* $n \equiv 4, 6 \pmod 8$.

2.10 Statistical consequences

We now pool together the elements assembled in the previous sections to compute the averages. We treat the cases $r_1 = 0$ and $r_1 > 0$ separately starting with totally imaginary orders. For simplicity, we present the computation for fields which are non-evenly ramified at all primes p. We state the general theorem in the last subsection.

2.10.1 Oriented class group averages for non-evenly ramified totally imaginary fields

$$\frac{\sum\limits_{\substack{\mathcal{O}\in\mathfrak{R},\\ H(\mathcal{O})<X}} 2^{r_2}\,|\mathrm{Cl}_2^*(\mathcal{O})| - |\mathcal{I}_2^*(\mathcal{O})|}{\left(\sum\limits_{0\le b<n} \mathrm{Vol}(U_{1,b}^{r_2}(\mathbb{R}))_{<X}\right)\prod\limits_p \mathrm{Vol}(S_p)} + o(1).$$

Now, by the preceding sections, we know that this sum is equal to:

$$= \frac{\sum\limits_{0\leq b<n}\sum\limits_{\delta\in\mathcal{T}(r_2)}\sum\limits_{A\in\mathscr{L}_{\mathbb{Z}}} N_H(\mathcal{V}(\Lambda^{\delta}_{A,b}),X)}{\left(\sum\limits_{0\leq b<n}\mathrm{Vol}(U^{r_2}_{1,b}(\mathbb{R}))_{<X}\right)\prod\limits_p \mathrm{Vol}(S_p)}.$$

Expanding, we find:

$$= \sum_{\delta\in\mathcal{T}(r_2)}\sum_{A\in\mathscr{L}_{\mathbb{Z}}}\frac{2}{\sigma(r_2)}\mathrm{Vol}(\mathcal{F}^{\delta}_A)\prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\prod_{p\neq 2} m_p(A)\frac{\int_{f\in S_2} m_2(f,A)df}{\mathrm{Vol}(S_2)}.$$

The indicator functions come into play at this point.

$$= \sum_{\delta\in\mathcal{T}(r_2)}\sum_{A\in\mathscr{L}_{\mathbb{Z}}}\frac{2}{\sigma(r_2)}\chi_A(\delta)\mathrm{Vol}(\mathcal{F}_A)\prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\frac{\int_{f\in S_2} m_2(f,A)df}{\mathrm{Vol}(S_2)}$$

We now break up the collection $\mathscr{L}_{\mathbb{Z}}$ into genera and sum over the forms in each genus separately before summing over the distinct genera. Since, both the characteristic function and the p-adic masses are constant over the forms in a single genus, they factor out of the inner sum.

$$= \sum_{\delta\in\mathcal{T}(r_2)}\sum_{\mathcal{G}\in\mathcal{G}_{\mathbb{Z}}}\sum_{A\in\mathcal{G}\cap\mathscr{L}_{\mathbb{Z}}}\frac{2}{\sigma(r_2)}\chi_A(\delta)\mathrm{Vol}(\mathcal{F}_A)\prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\frac{\int_{f\in S_2} m_2(f,A)df}{\mathrm{Vol}(S_2)}$$

$$= \sum_{\delta\in\mathcal{T}(r_2)}\sum_{\mathcal{G}\in\mathcal{G}_{\mathbb{Z}}}\frac{2}{\sigma(r_2)}\chi_{\mathcal{G}}(\delta)\frac{\int_{f\in S_2} m_2(f,\mathcal{G})df}{\mathrm{Vol}(S_2)}\left(\sum_{A\in\mathcal{G}\cap\mathscr{L}_{\mathbb{Z}}}\mathrm{Vol}(\mathcal{F}_A)\prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\right)$$

Now, the inner sum gives the Tamagawa number of the special orthogonal group of an integral form in a genus. It is known to always be equal 2, see for instance [32] and [26]. We denote it by $\tau(\mathrm{SO})$.

$$= \tau(\mathrm{SO})\sum_{\delta\in\mathcal{T}(r_2)}\sum_{\mathcal{G}\in\mathcal{G}_{\mathbb{Z}}}\frac{2}{\sigma(r_2)}\chi_{\mathcal{G}}(\delta)\frac{\int_{f\in S_2} m_2(f,\mathcal{G})df}{\mathrm{Vol}(S_2)}$$

At this point, we simplify the sum using the fact that $\sigma(r_2) = \frac{1}{2^{r_2}}$, the value of the 2-adic mass, the value of the infinite mass, and the classification of genera of unimodular integral quadratic forms as it appears in [18] or [24].

$$= \frac{\tau(\mathrm{SO})}{2^{r_2-1}}\sum_{\delta\in\mathcal{T}(r_2)}\sum_{\mathcal{G}\in\mathcal{G}_{\mathbb{Z}}}\chi_{\mathcal{G}}(\delta)\frac{\int_{f\in S_2} m_2(f,\mathcal{G})df}{\mathrm{Vol}(S_2)}$$

$$= \frac{\tau(\mathrm{SO})}{2^{r_2-1}}\sum_{\mathcal{G}\in\mathcal{G}_{\mathbb{Z}}}\sum_{\delta\in\mathcal{T}(r_2)}\chi_{\mathcal{G}}(\delta)\frac{\int_{f\in S_2} m_2(f,\mathcal{G})df}{\mathrm{Vol}(S_2)}$$

$$= \frac{\tau(\mathrm{SO})}{2^{r_2-1}} \sum_{\mathcal{G}\in\mathcal{G}_{\mathbb{Z}}} \left(\frac{\int_{f\in S_2} m_2(f,\mathcal{G})df}{\mathrm{Vol}(S_2)} \sum_{\delta\in\mathcal{T}(r_2)} \chi_{\mathcal{G}}(\delta) \right)$$
$$= \frac{\tau(\mathrm{SO})}{2^{r_2-1}} \Big(c_2(\mathfrak{M}_1)c_{\infty,0} + c_2(\mathfrak{M}_{-1})c_{\infty,2} \Big)$$

Now, these values being known from previous sections, we substitute them and simplify.

$$= \frac{1}{2^{r_2-1}} \cdot 4 \left(2^{n-2} + 2^{\frac{n-2}{2}} \right)$$
$$= \frac{1}{2^{r_2-1}} \cdot 4 \left(2^{2r_2-2} + 2^{r_2-1} \right)$$
$$= 2(2^{r_2} + 2)$$

Therefore, since there are no units of negative norm for totally imaginary fields, the 2 torsion in the oriented class group is twice as large as the 2 torsion in the class group, we find that the average number of 2 torsion elements in the class group of totally imaginary fields of even degree at least 4 is:

$$\boxed{\mathrm{Avg}(\mathrm{Cl}_2, \text{totally imaginary}) = 1 + \frac{3}{2^{r_2}}} \quad .$$

2.10.2 Oriented class group averages for non-evenly ramified not totally imaginary fields

The computation for $r_1 > 0$ proceeds in a similar way.

$$\frac{\sum_{\substack{\mathcal{O}\in\mathfrak{R},\\ H(\mathcal{O})<X}} |\mathcal{H}^*(\mathcal{O})| - |\mathcal{I}_2^*(\mathcal{O})|}{\left(\sum_{0\le b<n} \mathrm{Vol}(U_{1,b}^{r_2}(\mathbb{R}))_{<X} \right) \prod_p \mathrm{Vol}(S_p)} + o(1).$$

Now, by the preceding sections, we know that this sum is equal to:

$$= \frac{\sum_{0\le b<n} \sum_{\delta\in\mathcal{T}(r_2)} \sum_{A\in\mathscr{L}_{\mathbb{Z}}} N_H(\mathcal{V}(\Lambda_{A,b}^{\delta}), X)}{\left(\sum_{0\le b<n} \mathrm{Vol}(U_{1,b}^{r_2}(\mathbb{R}))_{<X} \right) \prod_p \mathrm{Vol}(S_p)}.$$

Expanding, we find:

$$= \sum_{\delta\in\mathcal{T}(r_2)} \sum_{A\in\mathscr{L}_{\mathbb{Z}}} \frac{2}{\sigma(r_2)} \mathrm{Vol}(\mathcal{F}_A^{\delta}) \prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p)) \prod_{p\neq 2} m_p(A) \frac{\int_{f\in S_2} m_2(f,A)df}{\mathrm{Vol}(S_2)}.$$

The indicator functions come into play at this point.

$$= \sum_{\delta \in \mathcal{T}(r_2)} \sum_{A \in \mathscr{L}_{\mathbb{Z}}} \frac{2}{\sigma(r_2)} \chi_A(\delta) \mathrm{Vol}(\mathcal{F}_A) \prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p)) \frac{\int_{f \in S_2} m_2(f, A) df}{\mathrm{Vol}(S_2)}$$

We now break up the collection $\mathscr{L}_{\mathbb{Z}}$ into genera and sum over the forms in each genus separately before summing over the distinct genera. Since, both the characteristic function and the p-adic masses are constant over the forms in a single genus, they factor out of the inner sum.

$$\begin{aligned}
&= \sum_{\delta \in \mathcal{T}(r_2)} \sum_{\mathcal{G} \in \mathcal{G}_{\mathbb{Z}}} \sum_{A \in \mathcal{G} \cap \mathscr{L}_{\mathbb{Z}}} \frac{2}{\sigma(r_2)} \chi_A(\delta) \mathrm{Vol}(\mathcal{F}_A) \prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p)) \frac{\int_{f \in S_2} m_2(f, A) df}{\mathrm{Vol}(S_2)} \\
&= \sum_{\delta \in \mathcal{T}(r_2)} \sum_{\mathcal{G} \in \mathcal{G}_{\mathbb{Z}}} \frac{2}{\sigma(r_2)} \chi_{\mathcal{G}}(\delta) \frac{\int_{f \in S_2} m_2(f, \mathcal{G}) df}{\mathrm{Vol}(S_2)} \left(\sum_{A \in \mathcal{G} \cap \mathscr{L}_{\mathbb{Z}}} \mathrm{Vol}(\mathcal{F}_A) \prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p)) \right)
\end{aligned}$$

Now, the inner sum gives the Tamagawa number of the special orthogonal group of an integral form in a genus. It is known to always be equal 2, see for instance [32] and [26]. We denote it by $\tau(\mathrm{SO})$.

$$= \tau(\mathrm{SO}) \sum_{\delta \in \mathcal{T}(r_2)} \sum_{\mathcal{G} \in \mathcal{G}_{\mathbb{Z}}} \frac{2}{\sigma(r_2)} \chi_{\mathcal{G}}(\delta) \frac{\int_{f \in S_2} m_2(f, \mathcal{G}) df}{\mathrm{Vol}(S_2)}$$

At this point, we simplify the sum using the fact that $\sigma(r_2) = \frac{1}{2^{r_1+r_2-1}}$, the value of the 2-adic mass, the value of the infinite mass, and the classification of genera of unimodular integral quadratic forms as it appears in [18] or [24].

$$\begin{aligned}
&= \frac{2\tau(\mathrm{SO})}{2^{r_1+r_2-1}} \sum_{\delta \in \mathcal{T}(r_2)} \sum_{\mathcal{G} \in \mathcal{G}_{\mathbb{Z}}} \chi_{\mathcal{G}}(\delta) \frac{\int_{f \in S_2} m_2(f, \mathcal{G}) df}{\mathrm{Vol}(S_2)} \\
&= \frac{\tau(\mathrm{SO})}{2^{r_1+r_2-2}} \sum_{\mathcal{G} \in \mathcal{G}_{\mathbb{Z}}} \sum_{\delta \in \mathcal{T}(r_2)} \chi_{\mathcal{G}}(\delta) \frac{\int_{f \in S_2} m_2(f, \mathcal{G}) df}{\mathrm{Vol}(S_2)} \\
&= \frac{\tau(\mathrm{SO})}{2^{r_1+r_2-2}} \sum_{\mathcal{G} \in \mathcal{G}_{\mathbb{Z}}} \left(\frac{\int_{f \in S_2} m_2(f, \mathcal{G}) df}{\mathrm{Vol}(S_2)} \sum_{\delta \in \mathcal{T}(r_2)} \chi_{\mathcal{G}}(\delta) \right) \\
&= \frac{\tau(\mathrm{SO})}{2^{r_1+r_2-2}} \left(c_2(\mathfrak{M}_1) c_{\infty,0} + c_2(\mathfrak{M}_{-1}) c_{\infty,2} \right)
\end{aligned}$$

Now, these values being known from previous sections, we substitute them and simplify.

$$\begin{aligned}
&= \frac{1}{2^{r_1+r_2-2}} \cdot 2 \left((2^{n-2} \pm_8 2^{\frac{n-2}{2}})(2^{r_1-2} \pm_8 2^{\frac{r_1-2}{2}}) + (2^{n-2} \mp_8 2^{\frac{n-2}{2}})(2^{r_1-2} \mp_8 2^{\frac{r_1-2}{2}}) \right) \\
&= \frac{1}{2^{r_1+r_2-2}} \cdot 2 \cdot 2 \left(2^{n+r_1-4} + 2^{\frac{n+r_1-4}{2}} \right) \\
&= 8 \left(2^{r_1+r_2-3} + 2^{-1} \right)
\end{aligned}$$

$$= 2^{r_1+r_2} + 4$$

Therefore, this leads to the following formula for average 2-torsion in the oriented class group of non-evenly ramified fields with at least one real embedding:

$$\boxed{\mathrm{Avg}(\mathrm{Cl}_2^*) = 1 + \frac{3}{2^{r_1+r_2-1}}} \quad .$$

2.10.3 General oriented class group averages

For simplicity, we carried out the calculations of the previous subsections under the assumption that there was no even ramification. In general, even ramification increases the mass at $p \neq 2$ from 1 to 2. If we take this into account, the computations of the previous section carry through with an additional term which captures this increase in total mass.

Definition 2.10.1. Let $\mathfrak{R} \subset \mathfrak{R}^{r_1,r_2}$ be a family of rings (unramified at 2) corresponding to an acceptable family of local specifications $\Sigma = (\Sigma_p)_p$. We define the *even ramification density* at p, $r_p(\mathfrak{R})$, as the density in Σ_p of elements of Σ_p which are evenly ramified at p.

We obtain the following averages by calculating as above.

Theorem 2.10.2 (General Averages for the oriented class group). *Let $\mathfrak{R} \subset \mathfrak{R}^{r_1,r_2}$ be a family of rings (unramified at 2) corresponding to an acceptable family of local specifications $\Sigma = (\Sigma_p)_p$ and let $r_p(\mathfrak{R})$ denotes its even ramification density at p.*

If $r_1 = 0$, the average number of 2-torsion elements in the oriented class group over $\mathfrak{R}$ is given by:

$$\boxed{\mathrm{Avg}(\mathrm{Cl}_2^*, \mathfrak{R}) = 2\prod_{p\neq 2}(1 + r_p(\mathfrak{R}))\left(1 + \frac{2}{2^{r_2}}\right) + \frac{2}{2^{r_2}}} \quad .$$

If $r_1 > 0$, the average number of 2-torsion elements in the oriented class group over $\mathfrak{R}$ is given by:

$$\boxed{\mathrm{Avg}(\mathrm{Cl}_2^*, \mathfrak{R}) = \prod_{p\neq 2}(1 + r_p(\mathfrak{R}))\left(1 + \frac{2}{2^{r_1+r_2-1}}\right) + \frac{1}{2^{r_1+r_2-1}}} \quad .$$

Remark 2.10.3. A priori, we have to be careful about summing over the b because the even ramification densities at different values of b might be different. However, this occurs only at primes p which divide n. For those finitely many primes, the quantity $\sum_{0\leq b\leq n-1}\prod_{p|n}(1 + r_{p,b}(\mathfrak{R}))$ when expanded is a finite sum of densities, which can then be factored again to give $\prod_{p|n}(1 + r_p(\mathfrak{R}))$. The same considerations apply to the final calculations in the next section. (Thanks to Ashvin Swaminathan and Arul Shankar for pointing out this issue and telling me how to fix it).

2.11 Averages for the class group and narrow class group

We can handle the question of computing the average number of 2-torsion elements in the usual class group by looking at $\mathrm{SL}_n^{\pm}$-orbits. The catch is that to get a torsor of the full class group, we must capture ideals with the property that $I^2 = (\alpha)$ with $\alpha \in K^\times$ and $N(\alpha) < 0$ in the rigid parametrisation. But those occur when we consider $-f$ instead of our monic f. Of course, this now introduces potential double-counting for rings that have a unit of negative norm. But this is offset by the fact that the fibre space $((R_f^\times)_{N\equiv 1})/((R_f^\times)^2)$ is half as large when R_f has a unit of negative norm as opposed to when it does not. We therefore recover the result of [45] that the set of pairs (A, B) with resolvent polynomial equal to $\pm f$ is an extension by $R_f^\times/(R_f^\times)^2$ of a torsor of the 2-torsion in the class group of R_f.

We explain the parametrisation in more detail.

2.11.1 Rigid parametrisation by pairs of symmetric bilinear forms

Let T be a principal ideal domain. Recall once again the rigid parametrisation of the pairs of bilinear forms $(A, B) \in V(T)$ with resolvent polynomial equal to f in terms of the based fractional ideal data for R_f.

Theorem 2.11.1 ([45])**.** *Take a non-degenerate binary n-ic form $f \in U(T)$ and let $R_f = \frac{T[x]}{(f(x))}$. Then the pairs symmetric bilinear forms $(A, B) \in V(T)$ with $f_{(A,B)} = f$ are in bijection with equivalence classes of triples*

$$(I, \mathcal{B}, \delta)$$

where $I \subset K_f$ is a based fractional ideal of R_f with basis $\mathcal{B}$ given by a T module isomorphism $\mathcal{B}\colon I \to T^n$, $\delta \in K_f^\times$ such that $I^2 \subset \delta R_f^{n-3}$ as ideals and the norm equation holds $N(I)^2 = N(\delta)N(R_f^{n-3})$ (as based ideals). Two triples $(I, \mathcal{B}, \delta)$ and $(I', \mathcal{B}', \delta')$ are equivalent if there exists a $\kappa \in K_f^\times$ with the property that $I = \kappa I'$, $\mathcal{B} \circ (\times\kappa) = \mathcal{B}'$ and $\delta = \kappa^2\delta$.

2.11.2 $\mathrm{SL}_n^{\pm}(\mathbb{Z})$-orbits and the class group

We now let $\mathrm{SL}_n^{\pm}(T)$ act on V by change of basis. This action corresponds, at the level of equivalence classes of triples $(I, \mathcal{B}, \delta)$, to the action of $\mathrm{SL}_n^{\pm}(T)$ on the basis $\mathcal{B}$ of the fractional ideal I. This action only changes the basis and does not change I nor δ. In particular, it does not change the defining conditions:

1) $I^2 \subset \delta R_f^{n-3}$

2) $N(I)^2 = N(\delta)N(R_f^{n-3})$

Indeed, acting by an element of $\mathrm{SL}_n^{\pm}(T)$ with negative determinant reverses the orientation of the ideal I, but since the second condition only depends on $N(I)^2$, this is immaterial.

The rigid parametrisation can be reformulated to describe $\mathrm{SL}_n^{\pm}(\mathbb{Z})$ orbits.

Theorem 2.11.2. *Let f be a non-degenerate monic binary n-ic form $f \in U_1(\mathbb{Z})$, let $R_f = \frac{\mathbb{Z}[x]}{(f(x))}$ and $K_f = R_f \otimes_{\mathbb{Z}} \mathbb{Q}$. The $\mathrm{SL}_n^{\pm}(\mathbb{Z})$ orbits on pairs symmetric bilinear forms $(A, B) \in V(\mathbb{Z})$ with $f_{(A,B)} = f$ are in bijection with equivalence classes of pairs*

$$(I, \delta)$$

where $I \subset K_f$ is a fractional ideal of R_f, and $\delta \in K_f^{\times}$ is such that $I^2 \subset \delta R_f$ as ideals and the norm equation $N(I)^2 = N(\delta)$ holds. Two pairs (I, δ) and (I', δ') are equivalent if there exists a $\kappa \in K_f^{\times}$ with the property that $I = \kappa I'$ and $\delta = \kappa^2 \delta'$. The same theorem holds for $-f$, except that now the norm condition is $N(I)^2 = -N(\delta)$.

We now describe the relation between $\mathrm{SL}_n^{\pm}(\mathbb{Z})$ orbits on $\pi^{-1}(\pm f) \subset V(\mathbb{Z})$ and the 2-torsion part of the class group of R_f.

Definition 2.11.3. Let $\mathcal{O}$ be an order in an S_n-field K. A pair (I, δ) consisting of a fractional ideal I of $\mathcal{O}$ and $\delta \in K^{\times}$ such that $I^2 \subset \delta\mathcal{O}$ and $N(I)^2 = \pm N(\delta)$ is said to be projective if the ideal I is invertible. Equivalently, a pair (I, δ) is projective if $I^2 = (\delta)$. For an S_n-order $\mathcal{O}$, we write $H(\mathcal{O})$ for the set of equivalence classes (in the sense of the theorem above) of projective pairs on $\mathcal{O}$. Component wise multiplication turns $H(\mathcal{O})$ into a group.

As the class group is comprised invertible ideals, let us consider the restriction of the parametrisation above to the set $H(\mathcal{O})$. Consider the forgetful map:

$$H(\mathcal{O}) \longrightarrow \mathrm{Cl}_2(\mathcal{O})$$

which forgets about the parameter δ. This map is plainly a surjective group homomorphism. Let's analyse its kernel.

Elements (I_0, δ_0) in the kernel of this forgetful map are such that $I_0^2 = (\delta)$ and $N(\delta_0) = \pm N(I_0)^2$ and have the property that $I_0 = (\alpha)$ for some α in K as ideals. Thus, $(I_0, \delta_0) \sim ((\alpha), \delta_0) \sim (\mathcal{O}, \alpha^{-2}\delta_0)$. Now, $\mathcal{O} = \alpha^{-2}\delta_0\mathcal{O}$ and $\pm 1 = N(\alpha^{-2}\delta_0)$. This implies that (I_0, δ_0) is equivalent to $(\mathcal{O}, u)$ where u is norm ± 1 unit of $\mathcal{O}^{\times}$. We are allowed to further mod out u by squares of elements of $K^{\times}$ which fix the ideal $\mathcal{O}$. But those are precisely the units of $\mathcal{O}$. The sequence above can thus be completed to the following short exact sequence:

$$1 \longrightarrow \frac{\mathcal{O}^{\times}}{(\mathcal{O}^{\times})^2} \longrightarrow H(\mathcal{O}) \longrightarrow \mathrm{Cl}_2(\mathcal{O}) \longrightarrow 1.$$

Applying Dirichlet's unit theorem allows us to compute that:

$$\left| \frac{\mathcal{O}^{\times}}{(\mathcal{O}^{\times})^2} \right| = 2^{r_1 + r_2}.$$

We thus obtain the following formula for the number of elements in $H(\mathcal{O})$.

Lemma 2.11.4. *Let $\mathcal{O}$ be an order in an S_n-number field of degree n and signature (r_1, r_2).*

Then:

$$|H(\mathcal{O})| = 2^{r_1+r_2} \left|\mathrm{Cl}_2(\mathcal{O})\right|.$$

We can also say something about the narrow class group in this context. The proof that the fibres have the right size is exactly the same as in [29].

Lemma 2.11.5. *if $H^+(\mathcal{O})$ denotes the subgroup of $H(\mathcal{O})$ consisting of pairs (I,δ) such that δ is positive under every real embedding of the fraction field of $\mathcal{O}$, then*

$$|H^+(\mathcal{O})| = 2^{r_2}|\mathrm{Cl}_2^+(\mathcal{O})|.$$

We now proceed to the description of the points in the cuspidal regions.

Lemma 2.11.6 (Even degree distinguished orbits lemma)**.** *$(A,B) \in V(\mathbb{Q})$ is distinguished if and only if there is an $\mathrm{SL}_n^{\pm}(\mathbb{Q})$ translate of (A,B) with the property that*

$$a_{i,j} = b_{i,j} = 0$$

for all $1 \leq i,j \leq \frac{n}{2}$ except for $i = j = \frac{n}{2}$ for which $a_{\frac{n}{2}\frac{n}{2}} = 0 \neq b_{\frac{n}{2}\frac{n}{2}}$.

Definition 2.11.7. Let $\mathcal{O}$ be an order. We denote by $\mathcal{I}_2(\mathcal{O})$ the 2-torsion subgroup of the ideal group of $\mathcal{O}$.

Proposition 2.11.8. *Let $\mathcal{O}_f$ be an order corresponding to the integral primitive irreducible non-degenerate monic binary form f. Then, $\mathcal{I}_2(\mathcal{O}_f)$ is in natural bijection with the set of projective reducible $\mathrm{SL}_n^{\pm}(\mathbb{Z})$-orbits on $V(\mathbb{Z}) \cap \pi^{-1}(f)$.*

SL_n-orbits over fields and local rings

In this section, we compute the number orbits, and the size of the stabilisers for the action of SL_n on the arithmetic rings $\mathbb{Z}_p$, $\mathbb{Q}$, and $\mathbb{R}$. Let T be a principal ideal domain. We first restate the rigid parametrisation in this case.

Theorem 2.11.9 ([9])**.** *Let f be a non-degenerate monic binary n-ic form $f \in U_1(T)$, let $R_f = \frac{T[x]}{(f(x))}$ and $K_f = R_f \otimes_{\mathbb{Z}} \mathbb{Q}$. The $\mathrm{SL}_n^{\pm}(T)$ orbits on pairs symmetric bilinear forms $(A,B) \in V(T)$ with $f_{(A,B)} = f$ are in bijection with equivalence classes of pairs*

$$(I,\delta)$$

where $I \subset K_f$ is a fractional ideal of R_f and $\delta \in K_f^{\times}$ such that $I^2 \subset \delta R_f$ as ideals and the norm equation $N(I)^2 = N(\delta)$ holds. Two pairs (I,δ) and (I',δ') are equivalent if there exists a $\kappa \in K_f^{\times}$ with the property that $I = \kappa I'$ and $\delta = \kappa^2\delta'$.

Then, we have the following theorem whose proof is straightforward.

Lemma 2.11.10. *The stabiliser in $\mathrm{SL}_n^{\pm}(T)$ corresponds to the 2-torsion of $R_f^{\times}$:*

$$R_f^{\times}[2].$$

Remark 2.11.11. It follows that the $\mathrm{SL}_n^{\pm}(\mathbb{Q})$ stabiliser of any element v whose resolvent is irreducible is equal to 2.

Just as in [29], we can compute the number of orbits with the caveat that we need to distinguish the case where f has an odd degree factor from the case where all the factors of f are even.

Lemma 2.11.12. *Let T be a field or $\mathbb{Z}_p$. Let f be a monic separable, non-degenerate binary form in $U_1(T)$. Then the projective $\mathrm{SL}_n(T)$ orbits of $V(T)$ with resolvent $\pm f$ are in bijection with elements of*

$$(R_f^{\times}/(R_f^{\times})^2)_{N\equiv\pm 1}.$$

Remark 2.11.13. We now describe the real orbits in the case where the leading coefficient of f is 1 and in the case where the leading coefficient is -1. Suppose that f is a non-degenerate polynomial of degree n with r_1 real roots and $2r_2$ complex roots. First, suppose that the leading coefficient of f is -1. If $r_1 = 0$ there are no real orbits while if $r_1 > 0$, there are 2^{r_1-1} orbits and the stabiliser has size $2^{r_1+r_2}$. Now, suppose that the leading coefficient of f is 1. If $r_1 = 0$, there is 1 real orbit while if $r_1 > 0$, there are 2^{r_1-1} real orbits. In both cases, the stabiliser has size $2^{r_1+r_2}$.

Now, instead of considering SO_A orbits, we think O_A orbits. Then the reduction theory, the cusp cutoff, the sieve, as well as the change of variable formula carry through precisely as above. We, therefore, obtain the following proposition.

Proposition 2.11.14. *We have*

$$\mathrm{Vol}\left(\mathcal{F}_A \cdot R_A^{r_2,\delta}(X)\right) = \chi_A(\delta)\,|\mathcal{J}_A|\,\mathrm{Vol}(\mathcal{F}_A)\mathrm{Vol}(U(\mathbb{R})_{H<X}^{r_2}).$$

Let $S_p \subset U_{1,b}(\mathbb{Z}_p)$ be a closed subset whose boundary has measure 0. Consider the set $\Lambda(A)_p = V_{A,b}(\mathbb{Z}_p) \cap \pi^{-1}(S_p)$. Then we have

$$\mathrm{Vol}(\Lambda_A(p)) = |\mathcal{J}_A|_p\,\mathrm{Vol}(\mathrm{O}_A(\mathbb{Z}_p)) \int_{f\in S_p} m_p(f,A)\,df$$

where

$$m_p(f,A) := \sum_{v\in\frac{V_{A,b}(\mathbb{Z}_p)\cap\pi^{-1}(f)}{\mathrm{O}_A(\mathbb{Z}_p)}} \frac{1}{\#\mathrm{Stab}_{\mathrm{O}_A(\mathbb{Z}_p)}(v)}.$$

The computation of the total local mass could be slightly more delicate since we need to differentiate the case of f having leading coefficient ±1. We treat this in detail in the next subsection.

2.11.3 The product of local volumes and the local mass

The total mass for the case where f has leading coefficient 1 is the following.

Lemma 2.11.15 (+1 total mass)**.** *Let R be a non-degenerate ring of degree n over $\mathbb{Z}_p$. Let N denote the norm map from $N\colon R^\times/(R^\times)^2 \to \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$. The quantity*

$$\frac{|(R^\times/(R^\times)^2)_{N\equiv 1}|}{|R^\times[2]|}$$

is equal to $\frac{1}{|N(R^\times)|}$ if $p \neq 2$ and to $\frac{2^n}{|N(R^\times)|}$ if $p = 2$.

The total mass for the case where f has leading coefficient -1 is the following.

Lemma 2.11.16 (-1 total mass)**.** *Let R be a non-degenerate ring of degree n over $\mathbb{Z}_p$. Let N denote the norm map from $N\colon R^\times/(R^\times)^2 \to \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$. The quantity*

$$\frac{|(R^\times/(R^\times)^2)_{N\equiv -1}|}{|R^\times[2]|}$$

is equal to 0 if -1 is not in the image of N. Otherwise, it is equal to $\frac{1}{|N(R^\times)|}$ if $p \neq 2$ and to $\frac{2^n}{|N(R^\times)|}$ if $p = 2$.

Proof. The fibres of a group homorphism are either empty or are of the same size as the kernel. The size of the kernel was calculated in the previous lemma. □

In particular, we get the following statement concerning the total local masses for maximal rings which not evenly ramified at 2.

Lemma 2.11.17. *The total local mass for $f \in \mathbb{Z}_p[x]$ maximal and not evenly ramified is given by:*

$$m_p^\pm(f) = \begin{cases} 2^{n-2} & \text{if } p = 2 \\ \frac{1}{2} & \text{if } p \neq 2 \end{cases}.$$

The total local mass for $f \in \mathbb{Z}_p[x]$, $p \neq 2$, maximal and evenly ramified is given by:

$$m_p^+(f) = 1$$

$$m_p^-(f) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ 0 & \text{if } p \equiv 3 \mod 4 \end{cases}.$$

Proof. -1 is not in the image of the norm map when f is maximal and evenly ramified at $p \equiv 3 \mod 4$. □

2.11.4 Distribution of total local masses among genera

The distribution techniques work well here. As soon as the total mass is known, knowing the local mass for each genus is straightforward easy. We note the results here.

Let $p \neq 2$. Then, up to $\mathrm{SL}_n^\pm(\mathbb{Z}_p)$ equivalence, there is a unique bilinear form of determinant 1 and a unique bilinear form of determinant -1. Both have Hasse-Witt symbol equal to 1. Therefore, the local masses are the same as before.

The computation of the local masses at $p = 2, \infty$ is more delicate and is treated in the next to subsections.

2.11.5 Point count and the 2-adic masses

For $p = 2$, up to $\mathrm{SL}_n^{\pm}(\mathbb{Z}_2)$ equivalence, there are 3 quadratic forms of determinant 1 and 2 quadratic forms of determinant -1. By restricting to rings which are not evenly ramified at 2, we eliminate one of the forms of determinant 1.

For $n \equiv 0 \mod 4$ we can take:

$$\mathfrak{M}_1^+ = \begin{pmatrix} 1 &&&&& \\ & \ddots &&&& \\ && 1 &&& \\ &&& 1 && \\ &&&& 1 & \\ &&&&& 1 \end{pmatrix}, \quad \mathfrak{M}_{-1}^+ = \begin{pmatrix} 1 &&&&& \\ & \ddots &&&& \\ && 1 &&& \\ &&& 1 && \\ &&&& -1 & \\ &&&&& -1 \end{pmatrix}.$$

$$\mathfrak{M}_1^- = \begin{pmatrix} 1 &&&&& \\ & \ddots &&&& \\ && 1 &&& \\ &&& 1 && \\ &&&& 1 & \\ &&&&& -1 \end{pmatrix}, \quad \mathfrak{M}_{-1}^- = \begin{pmatrix} 1 &&&&& \\ & \ddots &&&& \\ && 1 &&& \\ &&& -1 && \\ &&&& -1 & \\ &&&&& -1 \end{pmatrix}.$$

For $n \equiv 2 \mod 4$ we can take:

$$\mathfrak{M}_1^+ = \begin{pmatrix} 1 &&&&& \\ & \ddots &&&& \\ && 1 &&& \\ &&& 1 && \\ &&&& 1 & \\ &&&&& -1 \end{pmatrix}, \quad \mathfrak{M}_{-1}^+ = \begin{pmatrix} 1 &&&&& \\ & \ddots &&&& \\ && 1 &&& \\ &&& -1 && \\ &&&& -1 & \\ &&&&& -1 \end{pmatrix}.$$

$$\mathfrak{M}_1^- = \begin{pmatrix} 1 &&&&& \\ & \ddots &&&& \\ && 1 &&& \\ &&& 1 && \\ &&&& 1 & \\ &&&&& 1 \end{pmatrix}, \quad \mathfrak{M}_{-1}^- = \begin{pmatrix} 1 &&&&& \\ & \ddots &&&& \\ && 1 &&& \\ &&& 1 && \\ &&&& -1 & \\ &&&&& -1 \end{pmatrix}.$$

The superscripts indicate the sign of $(-1)^{\frac{n}{2}} \det(\cdot)$ and the subscripts indicate the Hasse-Witt symbol.

Now, the argument proceeds just as before except that now the *octane values* of $\mathfrak{M}_1^-$ and $\mathfrak{M}_{-1}^-$ are now $\pm 2 \mod 8$. This means that the volumes of the respective orthogonal groups are equal and thus that the masses at 2 are equal! We summarise the numbers in the following lemma.

Corollary 2.11.18. *The* 2*-adic masses are:*

$$\begin{aligned} c_2(n, \mathfrak{M}_1^+) \ &= \frac{1}{2}\left(2^{n-2} \pm_8 2^{\frac{n-2}{2}}\right) \mathrm{Vol}(S_2) \\ c_2(n, \mathfrak{M}_{-1}^+) &= \frac{1}{2}\left(2^{n-2} \mp_8 2^{\frac{n-2}{2}}\right) \mathrm{Vol}(S_2) \\ c_2(n, \mathfrak{M}_1^-) \ &= \frac{1}{2}\left(2^{n-2}\right) \mathrm{Vol}(S_2) \\ c_2(n, \mathfrak{M}_{-1}^-) &= \frac{1}{2}\left(2^{n-2}\right) \mathrm{Vol}(S_2) \end{aligned}$$

where $\pm_8$ *is* $+$ *if* n *is congruent to* 0 *or* $2 \mod 8$ *and* $-$ *otherwise.*

2.11.6 The infinite masses

We assume that $r_1 > 0$ since the totally imaginary case was already covered. Since the 2-adic masses for leading coefficient -1 are equal across genera, we will only need to know the total infinite mass, which is 2^{r_1-1}.

2.11.7 Statistical consequences

We now pool together the elements assembled in the previous subsections to compute the averages.

The computation basically carries through as above. In order to deal with the Tamagawa number and the half-integral local masses (which at first might seem to multiply to 0), one needs to use the following facts. If $\mathcal{G}$ denotes a genus, then we have the following identity of local volumes:

$$\mathrm{Vol}(\mathrm{O}_A(\mathbb{Z}_p)) = 2\mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p)),$$

$$\sum_{A \in \mathcal{G}} \mathrm{Vol}(\mathrm{O}_A(\mathbb{Z}) \backslash \mathrm{O}_A(\mathbb{R})) \prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p)) = 2,$$

where the sum is over all $\mathrm{SL}^{\pm}(\mathbb{Z})$ equivalence classes of integral representatives in $\mathcal{G}$.

We now proceed with the computation.

Definition 2.11.19. Let $\mathfrak{R} \subset \mathfrak{R}^{r_1,r_2}$ be a family of rings (unramified at 2) corresponding to an acceptable family of local specifications $\Sigma = (\Sigma_p)_p$. We define the *even ramification density* at p, $r_p(\mathfrak{R})$, as the density in Σ_p of elements of Σ_p which are evenly ramified at p.

Let $\mathscr{L}_{\mathbb{Z}}^+$ denote a set of representatives of integral bilinear forms of determinant 1 under the action of $\mathrm{SL}_n^{\pm}(\mathbb{Z})$ and let $\mathscr{L}_{\mathbb{Z}}^-$ denote a set of representatives of integral bilinear forms of determinant -1 under the action of $\mathrm{SL}_n^{\pm}(\mathbb{Z})$. Denote by $\mathcal{G}_{\mathbb{Z}}^+$ the set of genera of quadratic

n-ary forms containing an integral element of determinant 1 and denote by $\mathcal{G}_{\mathbb{Z}}^{-}$ the set of genera of quadratic n-ary forms containing an integral element of determinant -1. Notice that $\mathcal{G}_{\mathbb{Z}}^{+}$ partitions $\mathscr{L}_{\mathbb{Z}}^{+}$ and that $\mathcal{G}_{\mathbb{Z}}^{-}$ partitions $\mathscr{L}_{\mathbb{Z}}^{-}$.

$$\frac{\sum\limits_{\substack{\mathcal{O}\in\mathfrak{R},\\ H(\mathcal{O})<X}} |\mathcal{H}(\mathcal{O})| - |\mathcal{I}_2(\mathcal{O})|}{\left(\sum\limits_{0\leq b<n} \mathrm{Vol}(U_{1,b}^{r_2}(\mathbb{R}))_{<X}\right)\prod\limits_{p}\mathrm{Vol}(S_p)} + o(1).$$

Now, by the preceding sections, we know that this sum is equal to:

$$= \frac{\sum\limits_{0\leq b<n}\sum\limits_{\delta\in\mathcal{T}(r_2)}\sum\limits_{A\in\mathscr{L}_{\mathbb{Z}}^{-}} N_H(\mathcal{V}(\Lambda_{A,b}^{\delta}),X) + \sum\limits_{0\leq b<n}\sum\limits_{\delta\in\mathcal{T}(r_2)}\sum\limits_{A\in\mathscr{L}_{\mathbb{Z}}^{+}} N_H(\mathcal{V}(\Lambda_{A,b}^{\delta}),X)}{\left(\sum\limits_{0\leq b<n} \mathrm{Vol}(U_{1,b}^{r_2}(\mathbb{R}))_{<X}\right)\prod\limits_{p}\mathrm{Vol}(S_p)}.$$

Expanding, we find that the first sum is equal to:

$$\sum_{\delta\in\mathcal{T}(r_2)}\sum_{A\in\mathscr{L}_{\mathbb{Z}}^{-}}\frac{2}{\sigma(r_2)}\mathrm{Vol}(\mathcal{F}_A^{\delta})\prod_p\mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\prod_{p\equiv 1 \bmod 4}(1+r_p(\mathfrak{R}))\prod_{p\equiv 3 \bmod 4}(1-r_p(\mathfrak{R}))\frac{\int_{f\in S_2}2m_2(f,A)df}{\mathrm{Vol}(S_2)}.$$

Expanding, we find that the second sum is equal to:

$$\sum_{\delta\in\mathcal{T}(r_2)}\sum_{A\in\mathscr{L}_{\mathbb{Z}}^{+}}\frac{2}{\sigma(r_2)}\mathrm{Vol}(\mathcal{F}_A^{\delta})\prod_p\mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\prod_{p\neq 2}(1+r_p(\mathfrak{R}))\frac{\int_{f\in S_2}2m_2(f,A)df}{\mathrm{Vol}(S_2)}.$$

We can now process both of these sums separately just as we did before by breaking up $\mathscr{L}_{\mathbb{Z}}^{-}$ and $\mathscr{L}_{\mathbb{Z}}^{+}$ into genera and then first summing within each genus and then across the different genera.

After this is done, the $\mathscr{L}_{\mathbb{Z}}^{-}$ sum becomes:

$$\frac{2\tau(\mathrm{SO})}{2^{r_1+r_2}}\left(2c_2(n,\mathfrak{M}_1^{-})c_{\infty,0}+2c_2(n,\mathfrak{M}_{-1}^{-})c_{\infty,2}\right)\left(\prod_{p\equiv 1 \bmod 4}(1+r_p(\mathfrak{R}))\prod_{p\equiv 3 \bmod 4}(1-r_p(\mathfrak{R}))\right)$$

$$= \frac{1}{2^{r_1+r_2-1}}\cdot 2\cdot 2^{n-2}\cdot 2^{r_1-1}\cdot\left(\prod_{p\equiv 1 \bmod 4}(1+r_p(\mathfrak{R}))\prod_{p\equiv 3 \bmod 4}(1-r_p(\mathfrak{R}))\right)$$

$$= 2^{r_1+r_2-1}\left(\prod_{p\equiv 1 \bmod 4}(1+r_p(\mathfrak{R}))\prod_{p\equiv 3 \bmod 4}(1-r_p(\mathfrak{R}))\right)$$

And the $\mathscr{L}_{\mathbb{Z}}^{+}$ sum becomes:

$$\begin{aligned}
&\frac{2\tau(\mathrm{SO})}{2^{r_1+r_2}}\left(2c_2(n,\mathfrak{M}_1^+)c_{\infty,0}+2c_2(n,\mathfrak{M}_{-1}^+)c_{\infty,2}\right)\left(\prod_{p\neq 2}(1+r_p(\mathfrak{R}))\right)\\
&=\frac{1}{2^{r_1+r_2-1}}\cdot 2\cdot 2\left(2^{n+r_1-4}+2^{\frac{n+r_1-4}{2}}\right)\cdot\left(\prod_{p\neq 2}(1+r_p(\mathfrak{R}))\right)\\
&=\left(2^{r_1+r_2-1}+2\right)\left(\prod_{p\neq 2}(1+r_p(\mathfrak{R}))\right)
\end{aligned}$$

Therefore, we find the following formula for average 2-torsion in the class group of fields square-free at 2 with at least one real embedding:

$$\boxed{\begin{aligned}\mathrm{Avg}(\mathrm{Cl}_2,\mathfrak{R}) = \frac{1}{2}\prod_{p\equiv 1 \bmod 4}(1+r_p(\mathfrak{R}))\left(\prod_{p\equiv 3 \bmod 4}(1-r_p(\mathfrak{R}))+\prod_{p\equiv 3 \bmod 4}(1+r_p(\mathfrak{R}))\right)\\
+\frac{1+2\prod_{p\neq 2}(1+r_p(\mathfrak{R}))}{2^{r_1+r_2}}\end{aligned}}\ .$$

As a sanity check, note that $\left(\prod_{p\equiv 3 \bmod 4}(1-r_p(\mathfrak{R}))+\prod_{p\equiv 3 \bmod 4}(1+r_p(\mathfrak{R}))\right)\geq 2$, so the quantity above is always greater than 1.

The computation for the narrow class group is similar and gives us:

$$\begin{aligned}
&\frac{\displaystyle\sum_{\substack{\mathcal{O}\in\mathfrak{R},\\ H(\mathcal{O})<X}} 2^{r_2}\left|\mathrm{Cl}_2^+(\mathcal{O})\right|-|\mathcal{I}_2(\mathcal{O})|}{\left(\displaystyle\sum_{0\leq b<n}\mathrm{Vol}(U_{1,b}^{r_2}(\mathbb{R}))_{<X}\right)\displaystyle\prod_p\mathrm{Vol}(S_p)}+o(1)\\
&=\frac{\displaystyle\sum_{0\leq b<n}\sum_{A\in\mathscr{L}_{\mathbb{Z}}^{\pm}}N_H(\mathcal{V}(\Lambda_{A,b}^{\delta\gg 0}),X)}{\left(\displaystyle\sum_{0\leq b<n}\mathrm{Vol}(U_{1,b}^{r_2}(\mathbb{R}))_{<X}\right)\displaystyle\prod_p\mathrm{Vol}(S_p)}\\
&=\sum_{A\in\mathscr{L}_{\mathbb{Z}}^{\pm}}\frac{2}{\sigma(r_2)}\mathrm{Vol}(\mathcal{F}_A^{\delta\gg 0})\prod_p\mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\left(\prod_{p\neq 2}(1+r_p(\mathfrak{R}))\right)\frac{\int_{f\in S_2}2m_2(f,A)df}{\mathrm{Vol}(S_2)}\\
&=\sum_{A\in\mathscr{L}_{\mathbb{Z}}^{\pm}}\frac{2}{\sigma(r_2)}\chi_A(\delta_{\gg 0})\mathrm{Vol}(\mathcal{F}_A)\prod_p\mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\frac{\int_{f\in S_2}2m_2(f,A)df}{\mathrm{Vol}(S_2)}\left(\prod_{p\neq 2}(1+r_p(\mathfrak{R}))\right)\\
&=\sum_{\mathcal{G}\in\mathcal{G}_{\mathbb{Z}}}\sum_{A\in\mathcal{G}\cap\mathscr{L}_{\mathbb{Z}}}\frac{2}{\sigma(r_2)}\chi_A(\delta_{\gg 0})\mathrm{Vol}(\mathcal{F}_A)\prod_p\mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\frac{\int_{f\in S_2}2m_2(f,A)df}{\mathrm{Vol}(S_2)}\left(\prod_{p\neq 2}(1+r_p(\mathfrak{R}))\right)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\mathcal{G}\in\mathcal{G}_{\mathbb{Z}}} \frac{2}{\sigma(r_2)}\chi_{\mathcal{G}}(\delta_{\gg 0})\frac{\int_{f\in S_2} 2m_2(f,\mathcal{G})df}{\mathrm{Vol}(S_2)}\left(\sum_{A\in\mathcal{G}\cap\mathscr{L}_{\mathbb{Z}}}\mathrm{Vol}(\mathcal{F}_A)\prod_p \mathrm{Vol}(\mathrm{SO}_A(\mathbb{Z}_p))\right)\left(\prod_{p\neq 2}(1+r_p(\mathfrak{R}))\right)\\
&= \tau(\mathrm{SO})\sum_{\mathcal{G}\in\mathcal{G}_{\mathbb{Z}}} \frac{2}{\sigma(r_2)}\chi_{\mathcal{G}}(\delta_{\gg 0})\frac{\int_{f\in S_2} 2m_2(f,\mathcal{G})df}{\mathrm{Vol}(S_2)}\left(\prod_{p\neq 2}(1+r_p(\mathfrak{R}))\right)\\
&= \frac{2\tau(\mathrm{SO})}{2^{r_1+r_2}}\sum_{\mathcal{G}\in\mathcal{G}_{\mathbb{Z}}} \chi_{\mathcal{G}}(\delta_{\gg 0})\frac{\int_{f\in S_2} 2m_2(f,\mathcal{G})df}{\mathrm{Vol}(S_2)}\left(\prod_{p\neq 2}(1+r_p(\mathfrak{R}))\right)\\
&= \frac{1}{2^{r_1+r_2-1}}\cdot 2\left(2^{n-2}+2^{\frac{n-2}{2}}\right)\left(\prod_{p\neq 2}(1+r_p(\mathfrak{R}))\right)\\
&= \left(2^{r_2}+\frac{2^{r_2}}{2^{\frac{n-2}{2}}}\right)\left(\prod_{p\neq 2}(1+r_p(\mathfrak{R}))\right).
\end{aligned}
$$

Therefore, we find the following formula for average 2-torsion in the narrow class group of fields unramified at 2:

$$
\boxed{\mathrm{Avg}(\mathrm{Cl}_2^+,\mathfrak{R}) = \prod_{p\neq 2}(1+r_p(\mathfrak{R}))\left(1+\frac{2}{2^{\frac{n}{2}}}\right)+\frac{1}{2^{r_2}}}\ .
$$

Note that for totally imaginary fields, the narrow class group is the same as the class group and that the formulas do agree in that case!

Bibliography

[1] Avner Ash, Jos Brakenhoff, and Theodore Zarrabi. Equality of polynomial and field discriminants. *Experiment. Math.*, 16(3):367–374, 2007.

[2] Fabrizio Barroero and Martin Widmer. Counting lattice points and O-minimal structures. *Int. Math. Res. Not. IMRN*, (18):4932–4957, 2014.

[3] Alex Bartel, Henri Johnston, and Hendrik W. Lenstra Jr. Galois module structure of oriented arakelov class groups, 2020.

[4] Alex Bartel and Hendrik W. Lenstra, Jr. On class groups of random number fields. *Proc. Lond. Math. Soc. (3)*, 121(4):927–953, 2020.

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

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

[7] Manjul Bhargava. Most hyperelliptic curves over $\mathbb{Q}$ have no rational points, 2013.

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

[9] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang. Arithmetic invariant theory II: Pure inner forms and obstructions to the existence of orbits. In *Representations of reductive groups*, volume 312 of *Progr. Math.*, pages 139–171. Birkhäuser/Springer, Cham, 2015.

[10] Manjul Bhargava, Jonathan Hanke, and Arul Shankar. The mean number of 2-torsion elements in the class groups of n-monogenized cubic fields, 2020.

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

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

[13] Manjul Bhargava, Arul Shankar, and Xiaoheng Wang. Squarefree values of polynomial discriminants i, 2016.

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

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

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

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

[18] J. W. S. Cassels. *Rational quadratic forms*, volume 13 of *London Mathematical Society Monographs*. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978.

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

[20] H. Cohen and J. Martinet. Class groups of number fields: numerical heuristics. *Math. Comp.*, 48(177):123–137, 1987.

[21] Henri Cohen and Jacques Martinet. Étude heuristique des groupes de classes des corps de nombres. *J. Reine Angew. Math.*, 404:39–76, 1990.

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

[23] J. H. Conway and N. J. A. Sloane. Low-dimensional lattices. IV. The mass formula. *Proc. Roy. Soc. London Ser. A*, 419(1857):259–286, 1988.

[24] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, second edition, 1993. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.

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

[26] Alex Eskin, Zeév Rudnick, and Peter Sarnak. A proof of Siegel's weight formula. *Internat. Math. Res. Notices*, (5):65–69, 1991.

[27] Carl Friedrich Gauss. *Disquisitiones arithmeticae.* Translated into English by Arthur A. Clarke, S. J. Yale University Press, New Haven, Conn.-London, 1966.

[28] Frank Gerth, III. The 4-class ranks of quadratic fields. *Invent. Math.*, 77(3):489–515, 1984.

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

[30] Burton W. Jones. A canonical quadratic form for the ring of 2-adic integers. *Duke Math. J.*, 11:715–727, 1944.

[31] Peter Koymans and Carlo Pagano. Higher genus theory. *International Mathematics Research Notices*, August 2020.

[32] R. P. Langlands. The volume of the fundamental domain for some arithmetical subgroups of Chevalley groups. In *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, pages 143–148. Amer. Math. Soc., Providence, R.I., 1966.

[33] Michael Lipnowski, Will Sawin, and Jacob Tsimerman. Cohen-lenstra heuristics and bilinear pairings in the presence of roots of unity, 2020.

[34] Michael Lipnowski and Jacob Tsimerman. Cohen-Lenstra heuristics for étale group schemes and symplectic pairings. *Compos. Math.*, 155(4):758–775, 2019.

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

[36] Bjorn Poonen. Squarefree values of multivariable polynomials. *Duke Math. J.*, 118(2):353–373, 2003.

[37] P. Sawyer. Spherical functions on $\mathrm{SO}_0(p,q)/\mathrm{SO}(p) \times \mathrm{SO}(q)$. *Canad. Math. Bull.*, 42(4):486–498, 1999.

[38] P. Sawyer. Computing the Iwasawa decomposition of the classical Lie groups of noncompact type using the QR decomposition. *Linear Algebra Appl.*, 493:573–579, 2016.

[39] Arul Shankar and Xiaoheng Wang. Average size of the 2-selmer group of jacobians of monic even hyperelliptic curves. 2013.

[40] Artane Siad. Monogenic fields with odd class number part i: odd degree, 2020. `https://arxiv.org/abs/2011.08834`.

[41] Alexander Smith. Governing fields and statistics for 4-selmer groups and 8-class groups, 2016.

[42] Ashvin Swaminathan. Average 2-torsion in class groups of rings associated to binary n-ic forms, 2020. in preparation.

[43] Weitong Wang and Melanie Matchett Wood. Moments and interpretations of the cohen-lenstra-martinet heuristics, 2019.

[44] Melanie Matchett Wood. Rings and ideals parameterized by binary n-ic forms. *J. Lond. Math. Soc. (2)*, 83(1):208–231, 2011.

[45] Melanie Matchett Wood. Parametrization of ideal classes in rings associated to binary forms. *J. Reine Angew. Math.*, 689:169–199, 2014.

[46] Melanie Matchett Wood. Cohen-Lenstra heuristics and local conditions. *Res. Number Theory*, 4(4):Paper No. 41, 22, 2018.

[47] Melanie Matchett Wood. Random integral matrices and the Cohen-Lenstra heuristics. *Amer. J. Math.*, 141(2):383–398, 2019.