**From the holdings of the Department of Special Collections , Princeton University Library, Princeton, NJ**

These documents are either in the public domain, or can only be used for educational and research purposes (Fair use) as per U.S. Copyright law (text below). By accessing this file, all users agree that their use falls in the public domain or within fair use as defined by the copyrightlaw. We do not charge any permission or usage fees for the publication of images of material inour collections, including those provided by Princeton University Library, via our website, catalog, or directly from staff.For more information regarding copyright, credit, and citation please review the information onthe Copyright, Credit and Citation Guidelines page of our website.
https://library.princeton.edu/special-collections/policies/copyright-credit-and-citation-guidelines. If you have any questions, including how to order higher-quality images from the collection, contact Special Collections Public Services via our Ask Us! Form. https://library.princeton.edu/special-collections/ask-us

---

Doctoral Dissertations, 2011-2026 Mathematics

2022

# 2-Selmer groups, 2-class groups, and the arithmetic of binary forms

Swaminathan, Ashvin Anand

Princeton, NJ : Princeton University

---

http://arks.princeton.edu/ark:/88435/dsp012v23vx55w

*U.S. Copyright law: The copyright law of the United States (Title 17, §108, United States Code) governs the making of photocopies or other reproductions of copyrighted material. Under certain conditions specified in the law, libraries and archives are authorized to furnish a photocopy or other reproduction. One of these specified conditions is that the photocopy or reproduction is not to be used for any purpose other than private study, scholarship, or research. If a user makes a request for, or later uses, a photocopy or reproduction for purposes in excess of fair use that user may be liable for copyright infringement. This institution reserves the right to refuse to accept a copying order if, in its judgment, fulfillment of the order would involve a violation of copyright law. https://www.copyright.gov/title17/title17.pdf*

# 2-Selmer groups, 2-class groups, and the arithmetic of binary forms

Ashvin A. Swaminathan

A Dissertation
Presented to the Faculty
of Princeton University
in Candidacy for the Degree
of Doctor of Philosophy

Recommended for Acceptance
by the Department of
Mathematics
Adviser: Manjul Bhargava

May 2022

© Copyright by Ashvin A. Swaminathan, 2022.

All Rights Reserved

# Abstract

This thesis concerns the arithmetic of binary forms, with a particular emphasis on studying 2-class groups of the rings and fields defined by such forms, as well as 2-Selmer groups of hyperelliptic curves and related Diophantine objects. The keystone result of this thesis is an orbit parametrization of square roots of the ideal class of the inverse different of rings defined by binary forms (see §1). This parametrization, which can be construed as a new integral model of a "higher composition law" discovered by Bhargava and generalized by Wood, was the missing ingredient needed to solve a range of open problems concerning distributions of class groups, Selmer groups, and more. For instance, in this thesis, we apply the parametrization to bound the average size of the 2-class group in families of number fields defined by binary $n$-ic forms, where $n \geq 3$ is an arbitrary integer, odd or even (see §2). We also apply it to prove that most "superelliptic equations" of the form $z^2 = f(x, y)$, where $f$ is an integral binary form of odd degree, have a Brauer–Manin obstruction to having a primitive integer solution (see §3). Moreover, in joint work with Bhargava and Shankar, we use the parametrization to prove that when locally soluble genus-1 curves over $\mathbb{Q}$ are ordered by height, the average size of the 2-Selmer group is at most 6, and further that when elliptic curves over $\mathbb{Q}$ are ordered by height, the second moment of the size of the 2-Selmer group is at most 15, confirming well-known conjectures of Poonen and Rains (see §4). Finally, in joint work with Shankar, Siad, and Varma, we use the parametrization to determine the average size of the 2-class group in families of monogenic degree-$n$ orders, enumerated by height; for this application, we develop a new method for counting integral orbits having bounded invariants and satisfying local conditions that lie in the cusps of fundamental domains for coregular representations (see §5).

# Acknowledgements

To begin with, I would like to express my deepest gratitude to my advisor, Manjul Bhargava, for suggesting the questions that led to this thesis, for collaborating with me on a number of them, for providing me with invaluable mathematical and professional advice, and for taking the time to read and offer detailed feedback on my work. Manjul's infectious optimism and boundless creativity inspired me to persevere at times when it was difficult to see where my research was headed. I would often go into meetings with Manjul thinking the worst, that there was little hope of solving the problem at hand, only to come out feeling as though I had completely misjudged the situation, that there were many exciting avenues to pursue and that a solution ought to be within reach. He was usually right!

I would like to thank Arul Shankar for being such an insightful teacher and collaborator. As an undergraduate at Harvard, I had the unusual privilege of taking the entire number theory sequence with Arul, and my experiences in his class played an important role in my decision to pursue a PhD in arithmetic statistics. And it was a pleasure to do research with Arul: he has the remarkable ability to listen to ideas that I had dismissed as futile, to realize their viability, and to elevate them beyond the scope of my imagination.

I would like to thank Peter Sarnak for taking the time to meet with me and discuss my work, for suggesting a number of interesting new directions to pursue, and for sharing his uniquely global perspective on mathematics with me. I am grateful to him, as well as to Chris Skinner, for serving on my thesis defense committee, and I thank Shou-Wu Zhang for being my first-year advisor and thesis reader.

I thank Jordan S. Ellenberg for posing the question on square roots of the ideal class of the inverse different that led to this thesis, and I am grateful to Melanie Matchett Wood, whose foundational work on parametrizations of ideal classes in rings associated to binary forms served as a primary inspiration for this thesis. I also thank Melanie for taking the time to answer my questions about her work.

I would like to thank many other mathematicians who contributed to this thesis. I thank

my other collaborators Jan-Hendrik Evertse, Kálmán Győry, László Remete, Artane Siad, and Ila Varma. I am grateful to Levent Alpöge, Nils Bruin, Sungmun Cho, Benedict Gross, Aaron Landesman, Bjorn Poonen, Michael Stoll, David Zureick-Brown, and Jerry Wang for engaging with me in enlightening conversations, for answering my questions, and for sharing their insights. I am also grateful to Alex Bartel, Noam D. Elkies, Andrew Granville, Brendan Hassett, Wei Ho, Daniel Loughran, Evan O'Dorney, David McKinnon, Kumar Murty, Aurel Page, Anand Patel, Beth Romano, Will Sawin, Ari Shnidman, Efthymios Sofos, James Tao, John Voight, and Don Zagier for helpful discussions.

I am grateful to Jill LeClair for helping me navigate graduate school, for promptly and tirelessly answering the dozens of questions I sent her by email, and for assisting me at times when I did not know whom else to turn to.

I thank Simon Rubinstein-Salzedo and Daniel M. Kane for introducing me to the world of mathematical research. I am grateful to Joe Gallian and Ken Ono for providing me with the opportunity to hone my research skills at their respective REU programs, and I thank Jesse Thorner and David Zureick-Brown for working closely with me during my two summers at the Emory REU. And I thank Joe Harris and Anand Patel, my undergraduate senior thesis advisors, for guiding me through my first experience of writing a dissertation and for continuing to advise me as I made the transition to graduate school.

This thesis was supported by the NSF Graduate Research Fellowship under grant number DGE-1656466 and by the Paul and Daisy Soros Fellowship. I am grateful to Paul and Daisy Soros for their vision and generosity, and for their commitment to supporting the dreams of immigrant families like mine. I thank Craig Harwood, Nikka Landau, and Yulian Ramos for supporting me throughout my tenure as a PD Soros fellow and beyond.

Finally, I thank my Amma, Appa, Pattis, and Thathas for their unflinching faith in my abilities and for their undying love and support.

To Amma and Appa.

# Contents


Abstract . . . . . 3

Acknowledgements . . . . . 4

**1 New parametrization for ideal classes in rings defined by binary forms 12**

1.1 Introduction . . . . . 12

1.1.1 Relation to earlier work . . . . . 14

1.1.2 Organization . . . . . 15

1.2 Rings and ideals associated to binary forms . . . . . 15

1.3 Representations on pairs of symmetric matrices . . . . . 18

1.3.1 Representation of $G_n$ . . . . . 19

1.3.2 Action on pairs $(A, B)$ with $\det A = \pm 1$: a linearization trick . . . . . 20

1.3.3 Representation of $(\mathrm{SL}_n / \mu_2)(R)$ on $W_n(R)$ for a PID $R$ . . . . . 22

1.4 Orbit parametrization . . . . . 24

1.4.1 Construction of an integral orbit . . . . . 24

1.4.2 Ranks of orbits arising from the parametrization . . . . . 33

1.4.3 Orbits over fields . . . . . 35

**2 Average 2-torsion in class groups of number fields defined by binary forms 39**

2.1 Introduction . . . . . 39

2.1.1 Main results on class group distributions . . . . . 40

2.1.2 Comparison with class group heuristics . . . . . 44

2.1.3 Method of proof and organization . . . . . 48

2.2 Preliminaries on counting 2-torsion classes . . . . . 48
2.2.1 Case 1: $R = \mathbb{Z}$ and $n$ is odd . . . . . 49
2.2.2 Case 2: $R = \mathbb{Z}$ and $n$ is even . . . . . 51
2.3 Orbits over $\mathbb{Z}_p$ . . . . . 53
2.3.1 Preliminaries on binary forms over $\mathbb{Z}_p$ . . . . . 53
2.3.2 Pre-projective orbits . . . . . 54
2.3.3 Density calculations . . . . . 58
2.4 Distinguishedness and reducibility . . . . . 62
2.4.1 Uniqueness of integral representatives . . . . . 63
2.4.2 Existence of integral representatives, part $(i)$ . . . . . 64
2.4.3 Existence, part $(ii)$: $n$, $\nu_p(f_0)$ are odd . . . . . 66
2.4.4 Existence, part $(iii)$: $n$ is odd, $\nu_p(f_0)$ is even . . . . . 68
2.4.5 On a question of Emerton . . . . . 69
2.5 Proofs of the main results on class group statistics . . . . . 72
2.5.1 Counting $N(\mathbb{Z})$-orbits of binary forms with fixed leading coefficient . 73
2.5.2 Counting $(N \times \mathcal{G}_{A_0})(\mathbb{Z})$-orbits of on $W_{A_0}(\mathbb{Z})$ . . . . . 75
2.5.3 Sieving to square roots of the class of the inverse different . . . . . 79
2.5.4 The final step . . . . . 84
2.A Appendix: 2-adic orbit counting via 2-descent . . . . . 91

**3 Most odd-degree binary forms fail to primitively represent a square 95**
3.1 Introduction . . . . . 95
3.1.1 Superelliptic stacky curves . . . . . 96
3.1.2 Main results . . . . . 97
3.1.3 Method of proof and organization . . . . . 100
3.2 Construction of an integral orbit from a primitive integer solution . . . . . 101
3.2.1 The construction . . . . . 101
3.2.2 Distinguished points . . . . . 107

3.3 Counting orbits arising from local points . . . 109
3.3.1 Orbits over $\mathbb{R}$ . . . 109
3.3.2 Bounding $\mathrm{Vol}(\mathscr{P}_p)$ for $2 \neq p \nmid f_0$ . . . 111
3.3.3 Bounding $\mathrm{Vol}(\mathscr{P}_2)$ for $2 = p \nmid f_0$ . . . 113
3.3.4 Orbits over $\mathbb{Z}_p$ . . . 117
3.3.5 Orbits over $\mathbb{Q}_p$ for $p \mid f_0$ . . . 118
3.4 Proof of Theorem 61 . . . 120
3.4.1 Counting irreducible integral orbits of bounded height . . . 120
3.4.2 Sieving to orbits arising from local points when $2 \nmid f_0$ . . . 124
3.4.3 The final step . . . 128
3.5 Obstruction to the Hasse principle and the proof of Theorem 62 . . . 133
3.5.1 The Jacobian of a superelliptic stacky curve . . . 133
3.5.2 Defining the Brauer–Manin obstruction for $\mathscr{S}_F$ . . . 135
3.5.3 2-Coverings . . . 137
3.5.4 Proof of Theorem 62 . . . 141

**4 The second moment of the size of the 2-Selmer group of elliptic curves 144**
4.1 Introduction . . . 144
4.1.1 Statements of main results . . . 145
4.1.2 Background on hyperelliptic curves and their Selmer groups . . . 147
4.1.3 Method of proof and organization . . . 148
4.2 Parametrization of 2-Selmer groups of hyperelliptic Jacobians . . . 155
4.2.1 Construction of rational orbits via Galois cohomology . . . 155
4.2.2 Construction of integral representatives . . . 159
4.3 2-Selmer groups of elliptic curves, and orbits of small rank . . . 170
4.3.1 Representation of $\mathrm{PGL}_2$ on binary quartic forms . . . 171
4.3.2 Construction of special integral representatives . . . 172
4.3.3 Ranks of special elements . . . 177

4.4 Preliminary results about functions on coregular spaces . . . . . 179
4.4.1 Application to the representation of $\mathrm{PGL}_2$ on $V$ . . . . . 182
4.4.2 Application to the representations of $\mathrm{SL}_4$ on $W$ and $\mathrm{PSO}_{\mathscr{A}_4}$ on $W_{\mathscr{A}_4}$ . 185
4.5 Counting special integral orbits via equidistribution . . . . . 190
4.5.1 Counting special $\mathrm{SL}_4(\mathbb{Z})$-orbits on $W_4(\mathbb{Z})$ . . . . . 192
4.5.2 Fourier analysis on the space of $n \times n$ symmetric matrices . . . . . 201
4.5.3 Counting special $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})$-orbits on $W_{\mathscr{A}_4}(\mathbb{Z})$ . . . . . 203
4.6 The second moment of $|\mathrm{Sel}_2(E)|$ . . . . . 210
4.6.1 Slicing over the leading coefficient . . . . . 212
4.6.2 Introducing local masses on $W_{\mathscr{A}_4}(\mathbb{Z})$ . . . . . 213
4.6.3 Truncating the local masses and applying the counting results . . . . 217
4.6.4 Computing the local volumes and summing over leading coefficients . 220
4.A Appendix: Integral orbits from odd-degree divisors on hyperelliptic curves . 226
4.A.1 Summary of the problem . . . . . 226
4.A.2 Proof of Theorem 152 . . . . . 228
4.B Appendix: The second moment of the size of the 2-class group of monogenic cubic fields . . . . . 239
4.B.1 Notation . . . . . 239
4.B.2 Main result . . . . . 240
4.B.3 Comparison with class group heuristics . . . . . 241
4.B.4 Algebraic preliminaries . . . . . 242
4.B.5 Proof of Theorem 97 . . . . . 245

**5 Geometry-of-numbers methods in the cusp, and applications 250**
5.1 Introduction . . . . . 250
5.1.1 Background on geometry-of-numbers methods . . . . . 251
5.1.2 Main results on counting in cusps . . . . . 253
5.1.3 Main results on class group distributions . . . . . 256

5.2 Reduction theory . . . . . 258
5.2.1 A box-shaped fundamental domain for $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}) \curvearrowright \mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ . . . . . 259
5.2.2 A pair of nested generalized Siegel sets for $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}) \curvearrowright \mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ . . . . . 261
5.2.3 Fundamental sets for $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R}) \curvearrowright W_{\mathscr{A}_n,f_1}(\mathbb{R})$ and $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}) \curvearrowright W_{\mathscr{A}_n,f_1}(\mathbb{R})$ . 269
5.2.4 Action of lower-triangular subgroup on reducible hyperplane . . . . . 271
5.3 Counting reducible $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$-orbits on $W_{\mathscr{A}_n}(\mathbb{Z})$ . . . . . 274
5.3.1 Averaging over fundamental domains . . . . . 275
5.3.2 Slicing . . . . . 276
5.4 A Jacobian change-of-variables formula . . . . . 282
5.4.1 Setting up the change-of-variables . . . . . 283
5.4.2 Calculating the Jacobian . . . . . 285
5.4.3 Computing the value of $\mathcal{J}$ . . . . . 289
5.5 Congruence conditions . . . . . 293
5.5.1 Sieving to big families . . . . . 293
5.6 Application to counting 2-torsion ideals . . . . . 300
5.6.1 Preliminaries on 2-torsion ideals . . . . . 300
5.6.2 Computing the volume of pre-projective elements . . . . . 302

**Bibliography** **306**

# Chapter 1

# New parametrization for ideal classes in rings defined by binary forms

This chapter is largely based on my paper [116, §§1.1–1.3, §2], with some results also drawn from my joint work [28, §2.5] with Manjul Bhargava and Arul Shankar.

## 1.1 Introduction

A famous theorem of Hecke [70, Theorem 176] states that the ideal class of the different of the ring of integers of a number field is a perfect square. Motivated by Hecke's result, Ellenberg posed the following question:

**Question** (Ellenberg, [61])**.** *Could there be a "parametrization" in anything like Bhargava's sense for cubic rings together with a square root of [the ideal class of the] inverse different?*

The main contribution of this chapter is to give a positive answer to Ellenberg's question, not just for cubic rings, but for rings of *any* degree $n \geq 3$ defined by integral binary $n$-ic forms. Specifically, let $f$ be a separable primitive integral binary form of degree $n \geq 3$ with leading coefficient $f(1,0) = f_0 \neq 0$, and let $R_f$ denote the ring of global sections of the subscheme of $\mathbb{P}^1_{\mathbb{Z}}$ cut out by $f$. Letting $G_n := \mathrm{SL}_n$ if $n$ is odd and $G_n := \mathrm{SL}_n^{\pm} = \{g \in \mathrm{GL}_n : \det g = \pm 1\}$

if $n$ is even, we prove the following roughly stated orbit parametrization result, to be made precise in §1.4.1:

**Theorem 1.** *Square roots of the class of the inverse different of $R_f$ naturally give rise to $G_n(\mathbb{Z})$-orbits of pairs $(A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2\mathbb{Z}^n$ of symmetric $n \times n$ integer matrices such that*

$$\det(xA + yB) = \pm f_0^{-1} f(x, f_0 y) \in \mathbb{Z}[x, y],$$

*where $g \in G_n(\mathbb{Z})$ acts on $(A, B)$ via $g \cdot (A, B) = (gAg^T, gBg^T)$. The locus of pairs $(A, B)$ that arise in this way is cut out of the hypersurface $\det A = \pm 1$ by congruence conditions modulo $f_0^{n-1}$.*

This new orbit parametrization has made it possible to pursue a range of statistical applications concerning class groups of number fields and rational/integral points on varieties/stacks. As examples:

- In §2, we apply Theorem 1 to bound (and precisely determine, conditional on a uniformity estimate) the average size of the 2-class group in families of number fields defined by binary $n$-ic forms, where $n \geq 3$ is arbitrary (see Theorems 23 to 27). Similar bounds and conditional equalities have previously been proven in many cases, such as when $n$ is odd (see, e.g., the work of Ho–Shankar–Varma [71]) or when the binary forms under consideration are monic (see, e.g., the work of Siad [108, 109]). The new parametrization in Theorem 1 allows us to handle all cases simultaneously, including the non-monic even-degree case, which was not amenable to existing methods.

- In §3, we use Theorem 1 to prove that most integral odd-degree binary forms fail to primitively represent a square because of a Brauer–Manin obstruction.

- In §4, joint with Bhargava and Shankar, we apply Theorem 1 to bound the second moment of the size of the 2-Selmer group of elliptic curves.

### 1.1.1 Relation to earlier work

Theorem 1 gives a new integral model of a "higher composition law" discovered by Bhargava and generalized by Wood. In his thesis [6, Theorem 4], Bhargava demonstrated that when $\deg f = 3$, the elements of $\mathrm{Cl}(R_f)[2]$—i.e., square roots of the trivial class—are parametrized by pairs $(A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^3$ such that $\det(xA + yB) = \pm f(x, y)$. More generally, let $I_f^k$ be the space of global sections of the pullback to $\operatorname{Spec} R_f$ of the line bundle of degree $k$ on $\mathbb{P}^1_{\mathbb{Z}}$. In her thesis [126, Theorem 1.3], Wood proved that when $\deg f = n \geq 3$, square roots of the class of $I_f^{n-3}$ are parametrized by pairs $(A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ such that $\det(xA + yB) = \pm f(x, y)$.

These results of Bhargava and Wood precipitated two decades of progress in arithmetic statistics. Indeed, their parametrizations were used to (1) prove that most hyperelliptic curves have no rational points [11], (2) bound the average 2-torsion in the class groups of rings defined by odd-degree binary forms [18, 30, 71] or by monic binary forms [108, 109], and (3) determine the density of integer polynomials with squarefree discriminant [29, 99]. Related parametrizations on the space of pairs of symmetric integer matrices were used to bound the average size of the 2-Selmer groups in families of hyperelliptic curves with marked points [15, 26, 106].

Despite their remarkable versatility, the parametrizations of Bhargava and Wood have what is, in view of certain applications, a fundamental limitation: when $n$ is even and $|f_0| > 1$, the class of $I_f^{n-3}$ *sometimes* fails to have a square root. Furthermore, the forms $f$ for which this failure occurs are expected to contribute non-negligibly to the average size of $\mathrm{Cl}(R_f)[2]$. This limitation is the reason why the papers [18, 30, 71, 108, 109] on average 2-torsion in class groups considered only those rings defined by odd-degree or monic binary forms; more broadly, the inability to parametrize 2-torsion in class groups of rings defined by general even-degree binary forms has been one of many key impediments to formulating and verifying analogues of the Cohen–Lenstra heuristics for 2-class groups of number fields of even degree $n > 2$, for which 2 is a so-called "bad prime" (see §2.1.2).

The new parametrization in Theorem 1 overcomes the limitation described above. Indeed, a result of Simon [124, Theorem 2.4] states that $I_f^{n-2}$ represents the class of the inverse different of $R_f$, so Theorem 1 gives a parametrization of square roots of the class of $I_f^{n-2}$, rather than $I_f^{n-3}$. Such square roots *always* exist when $n$ is even; moreover, when $n$ is odd, Hecke's theorem implies that such square roots exist as long as $R_f$ is the maximal order in its fraction field. Consequently, as we show in §2, Theorem 1 can be used to study the distribution of 2-class groups of number fields defined by binary forms of *any* degree $n \geq 3$.

As it happens, the failure of $I_f^{n-3}$ to have a square root plays a crucial role in [17], where Bhargava, Gross, and Wang used it to prove that a positive proportion of hyperelliptic curves of any given genus have no odd-degree closed points. Essentially, they show that if $C_f$ denotes the curve $z^2 = f(x, y)$, locally soluble 2-covers of the variety $\mathrm{Pic}^1(C_f)$ give rise to square roots of the class of $I_f^{n-3}$; thus, if no such square root exists, $\mathrm{Pic}^1(C_f)$ has no rational points. On the other hand, this construction is insufficient to study locally soluble 2-covers of $\mathrm{Pic}^0(C_f)$, unless $C_f$ has an odd-degree closed point, in which case $\mathrm{Pic}^0(C_f) \simeq \mathrm{Pic}^1(C_f)$. It is for this reason that the papers [15, 26, 106] on average sizes of 2-Selmer groups restricted their consideration to *special* families of curves with marked points. In contrast, as we show in §4, Theorem 1 can be used to study the distribution of the 2-Selmer group for the *universal* family of locally soluble hyperelliptic curves of any given genus

### 1.1.2 Organization

First, in §1.4, we introduce the new parametrization alluded to in Theorem 1 and prove several useful properties about it.

## 1.2 Rings and ideals associated to binary forms

Let $n \geq 3$ and $f_0 \neq 0$ be integers. Let $V_n$ denote the affine scheme over $\mathbb{Z}$ whose $R$-points are given by $\mathrm{Sym}_n R^2$ for any $\mathbb{Z}$-algebra $R$ (i.e., binary $n$-ic forms over $R$), and Let $V_{n,f_0} \subset V_n$

be the subscheme corresponding to forms $f \in V_n(R)$ with leading coefficient $f(x,1) = f_0$.

Now let $R$ be a principal ideal domain (PID) with field of fractions $K$.[1] Let $f_0 \in R \smallsetminus \{0\}$, and fix a binary $n$-ic form $f = f(x,y) = \sum_{i=0}^{n} f_i x^{n-i} y^i \in V_{n,f_0}(R)$ that is separable over $K$. Consider the étale $K$-algebra $K_f := K[x]/(f(x,1))$, and let $\theta$ denote the image of $x$ in $K_f$. For each $i \in \{1, \dots, n-1\}$, let $p_i$ be the polynomial defined by $p_i(t) := \sum_{j=0}^{i-1} f_j t^{i-j}$, and let $\zeta_i := p_i(\theta)$. To the binary form $f$, there is a naturally associated free $R$-submodule $R_f \subset K_f$ having rank $n$ and $R$-basis given by

$$R_f := R\langle 1, \zeta_1, \zeta_2, \dots, \zeta_{n-1} \rangle. \tag{1.1}$$

The module $R_f$ has been studied extensively in the literature. In [32, proof of Lemma 3], Birch and Merriman proved that the discriminant of $f$ is equal to the discriminant of $R_f$, and in [87, Proposition 1.1], Nakagawa proved that $R_f$ is actually a ring with the following multiplication table: taking $1 \le i \le j \le n-1$ and setting $\zeta_0 := 1$ and $\zeta_n := -f_n$ for convenience, we have

$$\zeta_i \zeta_j = \sum_{k=j+1}^{\min\{i+j,n\}} f_{i+j-k} \zeta_k - \sum_{k=\max\{i+j-n,1\}}^{i} f_{i+j-k} \zeta_k.^2 \tag{1.2}$$

Also contained in $K_f$ is a natural family of free $R$-submodules $I_f^k$ of rank $n$ for each integer $k \in \{0, \dots, n-1\}$, having $R$-basis given by

$$I_f^k := R\langle 1, \theta, \dots, \theta^k, \zeta_{k+1}, \dots, \zeta_{n-1} \rangle. \tag{1.3}$$

For concreteness, we note that $I_f^0 = R_f$ is the unit ideal and that $I_f^{n-1} = R[\theta]$. By [124, Proposition A.1], each $I_f^k$ is an $R_f$-module and hence a fractional ideal of $R_f$; moreover, the notation $I_f^k$ makes sense, since $I_f^k$ is the $k^{\text{th}}$ power of $I_f^1$. By [124, Corollary 2.5 and Propo-

[1] We typically take $R$ to be $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_p$, $\mathbb{Z}/p\mathbb{Z}$, or $\mathbb{Q}_p$, where $p \in \mathbb{Z}$ is a prime.

[2] Nakagawa's results are stated for irreducible forms $f$, but as noted in [124, §2.1], their proofs continue to hold even otherwise.

sition A.4], if $n > 2$, the fractional ideals $I_f^k$ are invertible precisely when $R_f$ is Gorenstein, which happens precisely when $f$ is primitive (i.e., $\gcd(f_0, \ldots, f_n) = 1$).

*Remark* 2. The ring $R_f$ and ideals $I_f^k$ admit a simple geometric interpretation: indeed, by [124, §1], we have

$$\operatorname{Spec} R_f = \operatorname{Proj}\big(\mathbb{Z}[x,y]/(f(x,y))\big) \hookrightarrow \operatorname{Proj} \mathbb{Z}[x,y] = \mathbb{P}^1_{\mathbb{Z}}, \tag{1.4}$$

so $R_f$ can be thought of as the coordinate ring of the closed subscheme of $\mathbb{P}^1_{\mathbb{Z}}$ naturally associated to the binary form $f$. Letting $\mathcal{O}_{R_f}(k)$ denote the pullback to $\operatorname{Spec} R_f$ along the closed embedding (1.4) of the line bundle of degree $k$ on $\mathbb{P}^1_{\mathbb{Z}}$, we have that $I_f^k \simeq H^0(\mathcal{O}_{R_f}(k))$ as $R_f$-modules.

Given a fractional ideal $I$ of $R_f$ with specified basis (i.e., a *based* fractional ideal), the *norm* of $I$, denoted by $\mathrm{N}(I)$, is the determinant of the $K$-linear transformation taking the basis of $I$ to the basis of $R_f$ in (1.1). It is easy to check that $\mathrm{N}(I_f^k) = f_0^{-k}$ for each $k$ with respect to the basis in (1.3). The norm of $\kappa \in K_f^\times$ is the determinant of the $K$-linear transformation taking the basis $\langle 1, \zeta_1, \ldots, \zeta_{n-1}\rangle$ to the basis $\langle \kappa, \kappa\zeta_1, \ldots, \kappa\zeta_{n-1}\rangle$. Note that we have the multiplicativity relation

$$\mathrm{N}(\kappa I) = \mathrm{N}(\kappa)\,\mathrm{N}(I) \tag{1.5}$$

for any $\kappa \in K_f^\times$ and based fractional ideal $I$ of $R_f$, where we regard $\kappa \cdot I$ as having the basis given by multiplying each basis element of $I$ by $\kappa$.

The ideal $I_f^{n-2}$ plays a key role in the parametrization that we introduce in §1.4.1. Indeed, by [124, Theorem 2.4] (cf. [111, Proposition 14]), $[I_f^{n-2}]$ is the class of the inverse different of $R_f$; i.e., we have that

$$[I_f^{n-2}] = \big[\operatorname{Hom}_{\mathbb{Z}}(R_f, \mathbb{Z})\big] \in \mathrm{Cl}(R_f). \tag{1.6}$$

Thus, to parametrize square roots of the ideal class of the inverse different of $R_f$, we can work with the ideal $I_f^{n-2}$, which has the virtue of possessing the explicit $\mathbb{Z}$-basis given by (1.3).

*Remark* 3. There is a geometric way to verify (1.6). Indeed, the class of the inverse different of $R_f$ corresponds to the class of the relative dualizing sheaf $\omega_{R_f/\mathbb{Z}}$ of $\operatorname{Spec} R_f$ over $\operatorname{Spec} \mathbb{Z}$. Thus, it suffices to show that $I_f^{n-2} \simeq H^0(\omega_{R_f/\mathbb{Z}})$ as $R_f$-modules. Note that $\omega_{R_f/\mathbb{Z}}$ is isomorphic to the dualizing sheaf $\omega_{R_f}$ of $\operatorname{Spec} R_f$ as $\mathrm{Cl}(\mathbb{Z}) = \{1\}$, so applying the adjunction formula to (1.4) yields that $\omega_{R_f/\mathbb{Z}} \simeq \omega_{R_f} \simeq \mathcal{O}_{R_f}(n-2)$. It follows that $I_f^{n-2} \simeq H^0(\mathcal{O}_{R_f}(n-2)) \simeq H^0(\omega_{R_f/\mathbb{Z}})$ as $R_f$-modules.

We now discuss how $K_f$, $R_f$, and $I_f^k$ transform under the action of $\gamma \in \mathrm{GL}_2(R)$ on binary $n$-ic forms defined by $\gamma \cdot f = f((x,y)\cdot\gamma)$. If $f' = \gamma \cdot f$, then $K_{f'} \simeq K_f$, and the rings $R_{f'}$ and $R_f$ are identified under this isomorphism (see [87, Proposition 1.2] or [124, §2.3]). On the other hand, the ideals $I_{f'}^k$ and $I_f^k$ are isomorphic as $R_f$-modules but *need not* be identified under the isomorphism $K_{f'} \simeq K_f$. Indeed, as explained in [11, (7)], these ideals are related as follows: if $\gamma = \left[\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right]$ is such that $-t\theta + s \neq 0$ (equivalently, $f'$ has nonzero leading coefficient), then for each $k \in \{0, 1, \ldots, n-1\}$, the composition

$$I_f^k \xhookrightarrow{\phi_{k,\gamma}} K_f \xrightarrow{\sim} K_{f'} \tag{1.7}$$

is an injective map of $R_f$-modules having image equal to $I_{f'}^k$, where $\phi_{k,\gamma}$ sends each $\delta \in I_f^k$ to $(-t\theta + s)^{-k}\delta \in K_f$. When $k = 0$, we recover the identification $R_f = I_f^0$ with $R_{f'} = I_{f'}^0$ from (1.7). Let $N \subset \mathrm{GL}_2$ denote the lower-triangular unipotent subgroup. When $\gamma \in N(R)$, we have $-t\theta + s = 1$, so $\phi_{k,\gamma}$ is the identity map in this case.

## 1.3 Representations on pairs of symmetric matrices

Let $n \geq 3$ be an integer. In this section, we recall various representations involving the space of pairs of symmetric $n \times n$ matrices. These representations play a key role in stating our new parametrization and are crucial to the applications considered in §2–5. We start

in §1.3.1 by introducing the representation of $G_n$ on the space of pairs of symmetric $n \times n$ matrices. Since our parametrization produces pairs $(A, B)$ lying on the hypersurface where $\det A = \pm 1$, it is important to understand how the action of $G_n$ restricts to this (non-linear) hypersurface; in §1.3.2, we explain a "linearization trick" that recasts this restricted action in terms of a finite union of (linear) representations of orthogonal groups. We finish in §1.3.3 by discussing a related representation that occurs only when $n$ is even, namely the action of the group $(\mathrm{SL}_n / \mu_2)(R)$ on the space of pairs of symmetric $n \times n$ matrices over a PID $R$.

### 1.3.1 Representation of $G_n$

We first define the representation of $G_n$ on $W_n$. Let $\mathrm{Mat}_n$ denote the affine scheme over $\mathbb{Z}$ whose $R$-points are given by the set of $n \times n$ matrices with entries in $R$ for any $\mathbb{Z}$-algebra $R$. Let $V_{n,1} \subset \mathrm{Mat}_n$ denote the subscheme over $\mathbb{Z}$ whose $R$-points are given by $\mathrm{Sym}_2 R^n$ for any $\mathbb{Z}$-algebra $R$ (i.e., symmetric $n \times n$ matrices with entries in $R$, or equivalently, classically integral $n$-ary quadratic forms over $R$), and let $W_n = U_n \times U_n$ be the space of pairs of $n$-ary quadratic forms. Then $W_n$ has a natural structure of $G_n$-representation given as follows: for any element $g \in G_n(R)$ and any pair $(A, B) \in W_n(R)$, let

$$g \cdot (A, B) = \left(gAg^T, gBg^T\right) \in W_n(R),$$

where for a matrix $M$, we write $M^T$ for its transpose. When $n$ is odd, the action of $-\mathrm{id} \in \mathrm{SL}_n^{\pm}(R)$ centralizes elements of $W_n(R)$, which is why we work with $G_n = \mathrm{SL}_n$ instead of $\mathrm{SL}_n^{\pm}$.

We now describe the invariants of the action of $G_n$ on $W_n$. Given a pair $(A, B) \in W_n(R)$, we define the *resolvent* of $(A, B)$ to be the binary $n$-ic form $(-1)^{\lfloor \frac{n}{2} \rfloor} \det(xA + yB) \in V_n(R)$. Let $\iota \colon W_n \to V_n$ be the function that takes a pair of symmetric $n \times n$ matrices to its resolvent, and consider the $n+1$ homogeneous degree-$n$ polynomial functions $f_0 \circ \iota, \ldots, f_n \circ \iota \colon W_n \to \mathbb{A}^1_{\mathbb{Z}}$, where $f_i \colon V_n \to \mathbb{A}^1_{\mathbb{Z}}$ denotes the function that sends a form $f = f(x, y) \in V_n(R)$ to its $x^{n-i}y^i$-coefficient for each $i \in \{0, \ldots, n\}$. One checks that these functions are $G_n$-invariant; in fact,

they freely generate the ring of polynomial invariants for the action of $G_n$ on $W_n$.

### 1.3.2 Action on pairs $(A, B)$ with $\det A = \pm 1$: a linearization trick

We now describe how the action of $G_n$ on $W_n$ restricts to the hypersurface consisting of pairs where $\det A = \pm 1$. For this, we use the following linearization trick introduced in [18, §1.3]. Let $R$ be any $\mathbb{Z}$-algebra. The trick relies on the following pair of observations:

- If a pair $(A, B) \in W_n(R)$ is such that $\det A = \pm(-1)^{\lfloor \frac{n}{2} \rfloor}$, then the matrix $T = -A^{-1}B \in \mathrm{Mat}_n(R)$ is self-adjoint with respect to $A$ (i.e., $T^T A = AT$), and the characteristic polynomial $\mathrm{ch}_T$ of $T$ is $\mathrm{ch}_T(x) = \pm(\iota(A, B))(x, 1)$ (where the $\pm$ sign matches the sign of $\det A$, so that $\mathrm{ch}_T$ is monic).

- If $T \in \mathrm{Mat}_n(R)$ is self-adjoint with respect to a matrix $A \in U_n(R)$ such that $\det A = \pm(-1)^{\lfloor \frac{n}{2} \rfloor}$, then $-AT$ is symmetric, and $\mathrm{ch}_T(x) = \pm(\iota(A, -AT))(x, 1)$.

Now, let $A_0 \in U_n(R)$ with $\det \mathscr{A}_n = \pm(-1)^{\lfloor \frac{n}{2} \rfloor}$, and let $\mathcal{G}_{A_0}$ be the orthogonal group scheme over $\mathbb{Z}$ whose $S$-points are given by

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

Let $W_{A_0}$ be the affine scheme over $\mathbb{Z}$ whose $R$-points are given by

$$W_{A_0}(R) := \{T \in \mathrm{Mat}_n(R) : T^T A_0 = A_0 T\}.$$

Observe that $W_{A_0}$ has a natural structure of $\mathcal{G}_{A_0}$-representation, where for any $g \in \mathcal{G}_{A_0}(R)$ and $T \in W_{A_0}(R)$, we have $g \cdot T = gTg^{-1}$. Then the two observations itemized above imply

that we have the following stabilizer-preserving bijection for any form $f \in V_{n,1}(R)$:

$$\left\{ \begin{array}{c} (A,B) \in G_n(R)\backslash W_n(R) \\ \text{with } \iota(A,B) = \pm f \end{array} \right\} \leftrightsquigarrow \bigsqcup_{A_0} \left\{ \begin{array}{c} T \in \mathcal{G}_{A_0}(R)\backslash W_{A_0}(R) \\ \text{with } \mathrm{ch}_T(x) = f(x,1) \end{array} \right\} \tag{1.8}$$

where on the right-hand side of (1.8), the union runs over representatives $A_0$ of the set of $G_n(R)$-classes of symmetric matrices $A_0 \in \mathrm{Mat}_n(R)$ such that $\det A_0 = \pm(-1)^{\lfloor \frac{n}{2} \rfloor}$.

*Remark* 4. We sometimes find it more convenient to work not with $T \in W_A(R)$ but with $B = -AT$, which is an symmetric $n \times n$ matrix with entries in $R$. Thus, in what follows we sometimes abuse notation by writing $B \in W_A(R)$ to mean "the symmetric $n \times n$ matrix arising from the self-adjoint operator $T = -A^{-1}B \in W_A(R)$." In this language, the action of an element $g \in \mathcal{G}_A(R)$ on $T \in W_A(R)$ is written as $B \mapsto (g^{-1})^T B g^{-1}$. We further abuse notation by writing $\iota\colon W_A \to V$ for the function that sends $B \mapsto \iota(A,B)$.

Now, let $R$ be an integral domain with field of fractions $K$ having characteristic not equal to 2, and let $\mathscr{A}_n \in U_{n,1}(R)$ be the antidiagonal matrix with all antidiagonal entries equal to 1. For the applications in §3 and §5, which concern the case where $n$ is odd, we will only need to consider those pairs $(A,B) \in W_n(R)$ such that $A$ is split over $K$, meaning that the symmetric bilinear form associated to $A$ has a maximal isotropic space defined over $K$. It follows from [101, Chapter V, §2.2] that, when $n$ is odd, any such $A$ belongs to the $G_n(R)$-orbit of $\mathscr{A}_n$. Thus, in this case, we can just take $A_0 = \mathscr{A}_n$ in (1.8), and we obtain the following stabilizer-preserving bijection for any separable $f \in V_{n,1}(R)$:

$$\left\{ \begin{array}{c} (A,B) \in G_n(R)\backslash W_n(R) \text{ with } \iota(A,B) = \pm f \\ \text{such that } A \text{ is split over } K \end{array} \right\} \leftrightsquigarrow \left\{ \begin{array}{c} B \in \mathcal{G}_{\mathscr{A}_n}(R)\backslash W_{\mathscr{A}_n}(R) \\ \text{with } \iota(B) = \pm f \end{array} \right\} \tag{1.9}$$

### 1.3.3 Representation of $(\mathrm{SL}_n/\mu_2)(R)$ on $W_n(R)$ for a PID $R$

In this section, we take $n$ to be even, and we fix a PID $R$ with field of fractions $K$. Within $\mathrm{SL}_n$, we have the subgroup scheme $\mu_2$, with the inclusion $\mu_2 \hookrightarrow \mathrm{SL}_n$ defined on $R$-points by sending $r \in \mu_2(R)$ to $r \times \mathrm{id} \in \mathrm{SL}_n(R)$. We now use the action of $\mathrm{SL}_n$ on $W$ to obtain an action of $(\mathrm{SL}_n/\mu_2)(R)$ on $W_n(R)$ in the case where $R$ is a PID. To do this, we must first explicitly characterize the elements of $(\mathrm{SL}_n/\mu_2)(R)$. Upon inspecting the first few terms of the long exact sequence in flat cohomology arising from the short exact sequence $1 \to \mu_2 \to \mathrm{SL}_n \to \mathrm{SL}_n/\mu_2 \to 1$, we obtain the following short exact sequence:

$$1 \longrightarrow \mathrm{SL}_n(R)/\mu_2(R) \longrightarrow (\mathrm{SL}_n/\mu_2)(R) \longrightarrow H^1(R,\mu_2) \longrightarrow H^1(R,\mathrm{SL}_n). \quad (1.10)$$

We may identify $H^1(R,\mu_2)$ with the group $R^\times/R^{\times 2}$ via Kummer theory and $H^1(R,\mathrm{SL}_n)$ with the trivial group via Hilbert's Theorem 90. Let $K_{\mathrm{sep}}$ denote the separable closure of $K$, and for each $r \in R^\times/R^{\times 2}$, let $\varepsilon_r \in \mathrm{SL}_n(K_{\mathrm{sep}})$ be the diagonal matrix with diagonal entries given by $\frac{n}{2}$ copies of $\sqrt{r}$ followed by $\frac{n}{2}$ copies of $\frac{1}{\sqrt{r}}$. We then have the following characterization of the group $(\mathrm{SL}_n/\mu_2)(R)$ in terms of the matrices $\varepsilon_r$:

**Lemma 5.** *The group $(\mathrm{SL}_n/\mu_2)(R)$ is the subgroup of $\mathrm{SL}_n(K_{\mathrm{sep}})/\{\pm \mathrm{id}\}$ consisting of (classes of) matrices of the form $g\varepsilon_r$, where $g \in \mathrm{SL}_n(R)$ and $r \in R^\times/R^{\times 2}$.*

*Proof.* When $R = K$ is a field, the exact sequence (1.10) may be viewed as a sequence in Galois cohomology, in which case the lemma is proven in [16, §4.4]. For a general PID $R$, applying (1.10) to both $R$ and its field of fractions $K$ yields the following commutative diagram with exact rows, in which all vertical maps are injective:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{SL}_n(R)/\mu_2(R) & \longrightarrow & (\mathrm{SL}_n/\mu_2)(R) & \longrightarrow & R^\times/R^{\times 2} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{SL}_n(K)/\mu_2(K) & \longrightarrow & (\mathrm{SL}_n/\mu_2)(K) & \longrightarrow & K^\times/K^{\times 2} & \longrightarrow & 1. \end{array} \quad (1.11)$$

Because the lemma holds for $K$, it follows from (1.11) that $(\mathrm{SL}_n/\mu_2)(R)$ is contained in

the subgroup of $\mathrm{SL}_n(K_{\mathrm{sep}})/\{\pm \mathrm{id}\}$ consisting of (classes of) matrices of the form $g\varepsilon_r$, where $g \in \mathrm{SL}_n(K)$ and $r \in R^\times/R^{\times 2}$. Now, choose an element $g\varepsilon_r \in (\mathrm{SL}_n/\mu_2)(R)$ of this form. Since $\mathrm{SL}_n(R)/\mu_2(R)$ is a normal subgroup of $(\mathrm{SL}_n/\mu_2)(R)$, the element $g\varepsilon_r$ normalizes $\mathrm{SL}_n(R)$. But one easily checks that $\varepsilon_r$ normalizes $\mathrm{SL}_n(R)$, so $g$ must normalize $\mathrm{SL}_n(R)$ too. Because $\mathrm{SL}_n(R)$ is its own normalizer in $\mathrm{SL}_n(K)$, we conclude that $g \in \mathrm{SL}_n(R)$, as desired. □

We are now ready to define the action of $(\mathrm{SL}_n/\mu_2)(R)$ on $W_n(R)$. Given (the class of) an element $g\varepsilon_r \in (\mathrm{SL}_n/\mu_2)(R)$, where $g \in \mathrm{SL}_n(R)$ and $r \in R^\times/R^{\times 2}$, we let

$$(g\varepsilon_r)\cdot(A,B) = \big((g\varepsilon_r)A(g\varepsilon_r)^T, (g\varepsilon_r)B(g\varepsilon_r)^T\big) \in W_n(R)$$

for any pair $(A,B) \in W_n(R)$. This action is well-defined because the subgroup $\mu_2(R) \subset \mathrm{SL}_n(R)$ acts trivially on $W_n(R)$, and it also preserves the resolvent $\iota(A,B)$.

We now explain the analogue of the linearization trick described in §1.3.2 for the action of $(\mathrm{SL}_n/\mu_2)(R)$ on $W_n(R)$. For the application in §4, we will only need to consider those pairs $(A,B) \in W_n(R)$ such that $A$ is split over $K$ and such that the symmetric bilinear form associated to $A$ is even (i.e., $xAx^T$ is divisible by 2 for every $x \in R^n$). It follows from [101, Chapter V, §2.2] that any such $A$ belongs to the $G_n(R)$-orbit of $\mathscr{A}_n$. Thus, in this case, we can just take $A_0 = \mathscr{A}_n$. Let $\mathrm{PSO}_{\mathscr{A}_n} = \mathrm{SO}_{\mathscr{A}_n}/\mu_2$ be the projective orthogonal group associated to $\mathscr{A}_n$. Then the space $W_{\mathscr{A}_n}(R)$ has a natural structure of $\mathrm{PSO}_{\mathscr{A}_n}(R)$-representation, given as follows: for any element $g \in \mathrm{PSO}_{\mathscr{A}_n}(R)$, regard $g$ as an element of $(\mathrm{SL}_n/\mu_2)(R)$ via the inclusion $\mathrm{PSO}_{\mathscr{A}_n}(R) \hookrightarrow (\mathrm{SL}_n/\mu_2)(R)$ induced by the inclusion $\mathrm{SO}_{\mathscr{A}_n} \hookrightarrow \mathrm{SL}_n$, and let $g \cdot B = gBg^T \in W_{\mathscr{A}_n}(R)$ for any $B \in W_{\mathscr{A}_n}(R)$. By analogy with (1.9), we obtain the following stabilizer-preserving bijection:

$$\left\{ \begin{array}{c} (A,B) \in (\mathrm{SL}_n/\mu_2)(R)\backslash W_n(R) \text{ with } \iota(A,B) = \pm f \\ \text{such that } A \text{ is split over } K \text{ and even over } R \end{array} \right\} \leftrightsquigarrow \left\{ \begin{array}{c} B \in \mathrm{PSO}_{\mathscr{A}_n}(R)\backslash W_{\mathscr{A}_n}(R) \\ \text{with } \iota(B) = \pm f \end{array} \right\} \tag{1.12}$$

## 1.4 Orbit parametrization

Retain the setting of §1.2 (i.e., let $n$, $f_0$, $R$, and $f$ be as in §1.2). Consider the monic form $f_0^{-1} f(x, f_0 y) \in V_{n,1}(R)$; we call this form the *monicized form* of $f$ and denote it by $f^{\mathsf{mon}}$. The map $\mathsf{mon}\colon V_{f_0} \to V_1$ that sends a binary $n$-ic form to its monicization is injective; we call the left-inverse to this map *demonicization at* $f_0$, and we denote the demonicization of a form $g$ at $f_0$ by $g_{f_0}^{\mathsf{dem}}$.

Fix a unit $r \in R^\times$. Let $I$ be a based fractional ideal of $R_f$, and suppose that there exists $\alpha \in K_f^\times$ such that

$$I^2 \subset \alpha I_f^{n-2} \quad \text{and} \quad \mathrm{N}(I)^2 = r\,\mathrm{N}(\alpha)\,\mathrm{N}(I_f^{n-2}).^3 \tag{1.13}$$

In this section, we show that the pair $(I, \alpha)$ naturally gives rise to a $G_n(R)$-orbit of a pair $(A, B) \in W_n(R)$ such that $\iota(A, B) = r f^{\mathsf{mon}}$. Moreover, we provide a complete characterization of all pairs $(A, B) \in W_n(R)$ that arise in this manner. These results are summarized in Theorem 13 (to follow), which gives a precise formulation of Theorem 1.

### 1.4.1 Construction of an integral orbit

Consider the symmetric bilinear form

$$\langle -, - \rangle \colon I \times I \to K_f, \quad (\beta, \gamma) \mapsto \langle \beta, \gamma \rangle = \alpha^{-1} \beta \gamma. \tag{1.14}$$

By assumption, $\langle -, - \rangle$ has image contained in $I_f^{n-2}$. Next, let $\pi_{n-2}, \pi_{n-1} \in \mathrm{Hom}_R(I_f^{n-2}, R)$ be the maps defined on the $R$-basis (1.3) of $I_f^{n-2}$ by

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

[3] Note that if $I$ is invertible, then the norm condition in (1.13) forces $I^2 = \alpha I_f^{n-2}$.

Let $A$ and $B$ be the matrices in $U_n(R)$ representing the symmetric bilinear forms $\pi_{n-1} \circ \langle -, - \rangle$ and $\pi_{n-2} \circ \langle -, - \rangle \colon I \times I \to R$, respectively, with respect to the chosen basis of $I$.

**Theorem 6.** *Given the above setup, we have that* $\iota(A, B) = r f^{\mathsf{mon}}$.

*Proof.* Observe that $f^{\mathsf{mon}}(x, 1)$ is the characteristic polynomial of $f_0\theta \in K_f$. The idea of the proof is to show that the characteristic polynomial of the *matrix* $-A^{-1}B$ is equal to the characteristic polynomial of the *number* $f_0\theta$. We carry this strategy out through a pair of lemmas as follows.

**Lemma 7.** *We have that* $\det A = (-1)^{\lfloor \frac{n}{2} \rfloor} r$*, so in particular,* $A$ *is invertible over* $R$*, and the characteristic polynomial of* $-A^{-1}B$ *is* $\det(x\mathrm{id} - (-A^{-1}B)) = (-1)^{\lfloor \frac{n}{2} \rfloor} r^{-1} \det(xA + B)$.

*Proof of Lemma 7.* To begin, notice that $\det A$ is equal to the determinant of the bilinear map $\Sigma \colon I \times (\alpha^{-1} I) \to R$ defined by $(\beta, \gamma) \mapsto \pi_{n-1}(\beta\gamma)$. Next, consider the bilinear form $\Sigma' \colon I_f^{n-1} \times I_f^{n-1} \to K$ defined by $(\alpha, \beta) \mapsto \pi_{n-1}(\alpha\beta)$. We claim that it suffices to show that $\det \Sigma' = (-1)^{\lfloor \frac{n}{2} \rfloor} f_0^{-n}$. Indeed, note that $\Sigma$ is obtained from $\Sigma'$ via the following two steps:

- change the $K$-basis of the left-hand factor from the basis (1.3) of $I_f^{n-1}$ to that of $I$; and
- change the $K$-basis of the right-hand factor from the basis (1.3) of $I_f^{n-1}$ to the basis of $\alpha^{-1} I$ given by scaling each element of the chosen basis of $I$ by $\alpha^{-1}$.

Using the fact that $\Sigma$ and $\Sigma'$ are related by the above two changes-of-basis, we deduce that

$$\det \Sigma = \det \Sigma' \cdot \frac{\mathrm{N}(I)}{\mathrm{N}(I_f^{n-1})} \cdot \frac{\mathrm{N}(\alpha^{-1}) \, \mathrm{N}(I)}{\mathrm{N}(I_f^{n-1})} = \det \Sigma' \cdot r f_0^n,$$

where the last equality follows from the assumption that $\mathrm{N}(I)^2 = r \, \mathrm{N}(\alpha) \, \mathrm{N}(I_f^{n-2})$.

That $\det \Sigma' = (-1)^{\lfloor \frac{n}{2} \rfloor} f_0^{-n}$ is a consequence of the following claim: the matrix representing $\Sigma'$ with respect to the basis of $I_f^{n-1}$ given in (1.3) (namely, $I_f^{n-1} = R\langle 1, \theta, \ldots, \theta^{n-1} \rangle$) is lower antitriangular, with each antidiagonal entry equal to $-f_0^{-1}$. But this is easy: for $i, j \in \{0, \ldots, n-2\}$, we have $\Sigma'(\theta^i, \theta^j) = \pi_{n-1}(\theta^{i+j})$, which equals 0 when $i + j \leq n - 2$ and $-f_0^{-1}$ when $i + j = n - 1$. $\square$

To show that the characteristic polynomials of $f_0\theta$ and $-A^{-1}B$ are equal, it suffices to show that the actions of $f_0\theta$ and $-A^{-1}B$ by left-multiplication on $I$ are equal. It follows from Lemma 7 that the form $\pi_{n-1} \circ \langle -, - \rangle$ is nondegenerate, in the sense that the map $I \to \mathrm{Hom}_R(I, R)$ that sends $\beta \in I$ to the functional $\pi_{n-1}(\langle \beta, - \rangle)$ is an isomorphism. Thus, it suffices to prove the following:

**Lemma 8.** *We have that* $\pi_{n-1}(\langle \beta, f_0\theta \cdot \gamma \rangle) = \pi_{n-1}(\langle \beta, -A^{-1}B \cdot \gamma \rangle)$.

*Proof of Lemma 8.* It suffices to prove $\pi_{n-1}(\langle \beta, f_0\theta \cdot \gamma \rangle) = -\pi_{n-2}(\langle \beta, \gamma \rangle)$, as

$$-\pi_{n-2}(\langle \beta, \gamma \rangle) = \beta \cdot -B \cdot \gamma = \beta \cdot -AA^{-1}B \cdot \gamma = \pi_{n-1}(\langle \beta, -A^{-1}B \cdot \gamma \rangle).$$

To prove this, it suffices to prove the more general statement that if we extend $\pi_{n-1}$ and $\pi_{n-2}$ to maps $K_f \simeq I_f^{n-2} \otimes_R K \to K$, then $\pi_{n-1}(\rho f_0 \theta) = -\pi_{n-2}(\rho)$ for any $\rho \in K_f$. By [126, Corollary 2.2], we have $\pi_{n-1}(\rho f_0 \theta) = -a$, where $a$ is the coefficient of $\zeta_{n-2}$ when $\rho f_0$ is expressed in the basis $\langle 1, \theta, \ldots, \theta^{n-3}, \zeta_{n-2}, \zeta_{n-1} \rangle$. Then $a = f_0^{-1}\pi_{n-2}(\rho f_0) = \pi_{n-2}(\rho)$. □

This concludes the proof of Theorem 6. □

We say that two pairs $(I_1, \alpha_1)$ and $(I_2, \alpha_2)$, where $I_1, I_2$ are based fractional ideals of $R_f$ and $\alpha_1, \alpha_2 \in K_f^\times$ with $I_i^2 \subset \alpha_i I_f^{n-2}$ and $\mathrm{N}(I_i)^2 = r\,\mathrm{N}(\alpha_i)\,\mathrm{N}(I_f^{n-2})$ for each $i \in \{1, 2\}$, are *equivalent* if there exists $\kappa \in K_f^\times$ such that the based ideals $I_1$ and $\kappa I_2$ are equal up to a $G_n(R)$-change-of-basis and such that $\alpha_1 = \kappa^2 \alpha_2$. Evidently, if $(I_1, \alpha_1)$ and $(I_2, \alpha_2)$ are equivalent, then they give rise to the same $G_n(R)$-orbit on $W_n(R)$ via the above construction. Letting $H_{f,r}$ denote the set of equivalence classes of pairs $(I, \alpha)$ of the form (1.13), we have thus constructed a map of sets

$$\mathsf{orb}_{f,r} \colon H_{f,r} \longrightarrow G_n(R) \backslash \big\{ (A, B) \in W_n(R) : \iota(A, B) = r f^{\mathsf{mon}} \big\}.$$

**Proposition 9.** *The map* $\mathsf{orb}_{f,r}$ *is one-to-one.*

*Proof.* Let $(I_1, \alpha_1), (I_2, \alpha_2) \in H_{f,r}$ be such that $\mathsf{orb}_{f,r}(I_1, \alpha_1) = \mathsf{orb}_{f,r}(I_2, \alpha_2)$, and choose a representative $(A, B) \in W_n(R)$ of this common orbit. The proof of Theorem 6 implies that for each $i$, we can replace the chosen basis of $I_i$ with a $G_n(R)$-translate such that the map of left-multiplication by $f_0\theta$ on $I_i$ is given by the matrix $-A^{-1}B$ with respect to the translated basis. Having made these replacements, it follows that $I_1 \simeq I_2$ as based $R_f$-modules and hence as based fractional ideals of $R_f$, since multiplication by $f_0\theta$ determines the $R_f$-module structure. Thus, there exists $\kappa \in K_f^\times$ such that $I_1 = \kappa I_2$ and such that the chosen basis of $I_1$ is obtained by scaling each element in the chosen basis of $I_2$ by $\kappa$. By replacing $I_2$ with $\kappa I_2$ and $\alpha_2$ with $\kappa^2\alpha_2$, we may assume that $I_1 = I_2 = I$. Upon making these replacements, we obtain two elements $(I, \alpha_1), (I, \alpha_2) \in H_{f,r}$ such that, with respect to some chosen basis of $I$, both $\mathsf{orb}_{f,r}(I, \alpha_1)$ and $\mathsf{orb}_{f,r}(I, \alpha_2)$ are represented by the pair $(A, B) \in W_n(R)$.

It remains to show that $\alpha_1 = \alpha_2$. Let $\phi_1, \phi_2 \in \mathrm{Hom}_{R_f}(I \otimes_{R_f} I, I_f^{n-2})$ be defined by

$$\phi_i \colon I \otimes_{R_f} I \to I_f^{n-2}, \quad \phi_i(\beta \otimes \gamma) = \alpha_i^{-1}\beta\gamma \quad \text{for each } i \in \{1, 2\}$$

Then it suffices to show that $\phi_1 = \phi_2$. By [126, Proposition 2.5], post-composition with $\pi_{n-1}$ yields an isomorphism $\mathrm{Hom}_{R_f}(I \otimes_{R_f} I, I_f^{n-2}) \xrightarrow{\sim} \mathrm{Hom}_R(I \otimes_{R_f} I, R)$ of $R_f$-modules, so it suffices to show that the images of $\phi_1$ and $\phi_2$ under this isomorphism are equal. But these images are both represented by $A$ with respect to the chosen basis of $I$, so they must be equal. □

If $f_0 \notin R^\times$, then not every pair $(A, B) \in W_n(R)$ with $\iota(A, B) = rf^{\mathsf{mon}}$ necessarily lies in $\mathsf{orb}_{f,r}(H_{f,r})$. The next theorem characterizes the orbits that lie in the image of $\mathsf{orb}_{f,r}$:

**Theorem 10.** *Let $(A, B) \in W_n(R)$ be such that $\iota(A, B) = rf^{\mathsf{mon}}$. Then the $G_n(R)$-orbit of $(A, B)$ lies in the image of the map $\mathsf{orb}_{f,r}$ if and only if*

$$p_i(f_0^{-1} \times -A^{-1}B) \in \mathrm{Mat}_n(R) \quad \textit{for each} \quad i \in \{1, \ldots, n-1\}. \tag{1.15}$$

*Proof.* Let $(A, B)$ be as in the theorem statement. We first check that (1.15) is satisfied

when the $G_n(R)$-orbit of $(A, B)$ is equal to $\mathsf{orb}_{f,r}(I, \alpha)$ for some $(I, \alpha) \in H_{f,r}$. In this case, it follows from the proof of Theorem 6 that for each $i \in \{1, \ldots, n-1\}$, the action of $\zeta_i \in R_f$ by left-multiplication on $I$ is given by $p_i\big(\frac{1}{f_0} \cdot -A^{-1}B\big)$ with respect to some basis of $I$. Since $I$ is an $R_f$-module, this action is integral, and the matrix $p_i\big(\frac{1}{f_0} \cdot -A^{-1}B\big)$ must have entries in $R$.

Now suppose $(A, B)$ satisfies (1.15). Let $I$ be a free $R$-module of rank $n$, and choose an $R$-basis of $I$. We endow the $R$-module $I$ with the structure of $R_{f^{\mathsf{mon}}}$-module by defining the action of $f_0\theta$ on $I$ to be left-multiplication by the matrix $-A^{-1}B$ with respect to the chosen basis (note that $R_{f^{\mathsf{mon}}}$ is the subring of $R_f$ generated over $R$ by the element $f_0\theta$). For each $i \in \{0, \ldots, n-1\}$, let $\varphi_i \colon I \to I \otimes_{R_{f^{\mathsf{mon}}}} R_f$ be the map of $R_{f^{\mathsf{mon}}}$-modules that sends $\rho \mapsto \rho \otimes \zeta_i$. The conditions (1.15) imply that $\phi_i(I) \subset I$ for each $i$, where we regard $I$ as an $R_{f^{\mathsf{mon}}}$-submodule of $I \otimes_{R_{f^{\mathsf{mon}}}} R_F$ via the map $\beta \mapsto \beta \otimes 1$. Thus, the structure of $R_{f^{\mathsf{mon}}}$-module on $I$ extends to a structure of $R_f$-module, so $I$ is isomorphic to a fractional ideal of $R_f$. For convenience, we rescale $I$ so that $1 \in I$.

Having constructed $I$, we next construct a map $\Phi \colon I \otimes_{R_f} I \to I_f^{n-2}$ of $R_f$-modules. Consider the map $\Psi \colon I \otimes_R I \to R$ defined by $\beta \otimes \gamma \mapsto \beta \cdot A \cdot \gamma$, where $\beta$ and $\gamma$ are respectively viewed as row and column matrices with entries in $R$ with respect to the chosen basis of $I$. Then, under the identification $\mathrm{Hom}_R(I \otimes_R I, R) \simeq \mathrm{Hom}_R(I, \mathrm{Hom}_R(I, R))$, the map $\Psi$ corresponds to a map of $R$-modules $\Psi' \colon I \to \mathrm{Hom}_R(I, R)$. Observe that $\mathrm{Hom}_R(I, R)$ has a natural $R_f$-module structure, defined by $(\rho \cdot \varphi)(\beta) = \varphi(\rho\beta)$ for each $\rho \in R_f$, $\varphi \in \mathrm{Hom}_R(I, R)$, and $\beta \in I$. We now claim that $\Psi'$ is compatible with the actions of $R_f$ on $I$ and on $\mathrm{Hom}_R(I, R)$ and thus extends to a map of $R_f$-modules. Take $\beta, \gamma \in I$; to prove the claim, it suffices to show that

$$(\Psi'(f_0\theta\beta))(\gamma) = (f_0\theta \cdot (\Psi'(\beta)))(\gamma), \tag{1.16}$$

because the action of $f_0\theta$ determines the $R_f$-module structures of both $M$ and $\mathrm{Hom}_R(I, R)$. By definition, the left-hand side of (1.16) evaluates to

$$(\Psi'(f_0\theta\beta))(\gamma) = (f_0\theta\beta) \cdot A \cdot \gamma = (\beta \cdot (-A^{-1}B)^T) \cdot A \cdot \gamma = -\beta \cdot B \cdot \gamma, \tag{1.17}$$

and the right-hand side of (1.16) evaluates to

$$(f_0\theta \cdot (\Psi'(\beta)))(\gamma) = (\Psi'(\beta))(f_0\theta\gamma) = \beta \cdot A \cdot (-A^{-1}B \cdot \gamma) = -\beta \cdot B \cdot \gamma. \tag{1.18}$$

Comparing (1.17) and (1.18) yields the claim. By [126, Proposition 2.5], post-composition with $\pi_{n-1}$ gives an isomorphism $\mathrm{Hom}_R(I, R) \xrightarrow{\sim} \mathrm{Hom}_{R_f}(I, I_f^{n-2})$ of $R_f$-modules. Post-composing $\Psi'$ with this isomorphism yields a map of $R_f$-modules $\Psi''\colon I \to \mathrm{Hom}_{R_f}(I, I_f^{n-2})$. Let $\Phi\colon I \otimes_{R_f} I \to I_f^{n-2}$ be the image of $\Psi''$ under the identification

$$\mathrm{Hom}_{R_f}(I, \mathrm{Hom}_{R_f}(I, I_f^{n-2})) \simeq \mathrm{Hom}_{R_f}(I \otimes_{R_f} I, I_f^{n-2}).$$

By construction, the matrix representing the bilinear map $\pi_{n-1} \circ \Phi$ with respect to the chosen basis of $I$ is equal to $A$. As we showed in the proof of Lemma 8, we have $\pi_{n-1}(\rho f_0\theta) = -\pi_{n-2}(\rho)$ for any $\rho \in K_f$. Thus, for any $\beta \otimes \gamma \in I \otimes_{R_f} I$, we have that

$$\begin{aligned}
(\pi_{n-2} \circ \Phi)(\beta \otimes \gamma) &= \pi_{n-2}(\Phi(\beta \otimes \gamma)) = -\pi_{n-1}(\Phi(\beta \otimes \gamma) f_0\theta) \\
&= -\pi_{n-1}(\Phi(\beta \otimes (f_0\theta\gamma))) = -\pi_{n-1}(\Phi(\beta \otimes (-A^{-1}B \cdot \gamma))) \\
&= -(\pi_{n-1} \circ \Phi)(\beta \otimes (-A^{-1}B \cdot \gamma)) = -\beta \cdot A \cdot (-A^{-1}B \cdot \gamma) \\
&= \beta \cdot B \cdot \gamma,
\end{aligned}$$

so $B$ represents the bilinear map $\pi_{n-2} \circ \Phi$ with respect to the chosen basis of $I$.

It remains to show that there is $\alpha \in K_f^\times$ such that $\Phi$ coincides with the bilinear form that sends $\beta \otimes \gamma \mapsto \alpha^{-1}\beta\gamma$ (implying, in particular, that $I^2 \subset \alpha I_f^{n-2}$), and such that $\mathrm{N}(I)^2 = r\,\mathrm{N}(\alpha)\,\mathrm{N}(I_f^{n-2})$. To do this, fix elements $\beta_0, \gamma_0 \in I \cap K_f^\times$. For any $\beta, \gamma \in I$, let $\beta', \gamma' \in R_f \cap K_f^\times$ and $\beta'', \gamma'' \in R_f$ be such that $\beta\beta' = \beta_0\beta'' \in R_f$ and $\gamma\gamma' = \gamma_0\gamma'' \in R_f$. Then

$$\Phi(\beta \otimes \gamma) = \frac{\Phi((\beta\beta') \otimes (\gamma\gamma'))}{\beta'\gamma'} = \frac{\beta''\gamma''}{\beta'\gamma'} \cdot \Phi(\beta_0 \otimes \gamma_0) = (\beta\gamma) \cdot \frac{\Phi(\beta_0 \otimes \gamma_0)}{\beta_0\gamma_0}. \tag{1.19}$$

Let $\alpha' = \Phi(\beta_0 \otimes \gamma_0)/(\beta_0\gamma_0) \in K_f$. Then by (1.19), we have that $\Phi(\beta \otimes \gamma) = (\beta\gamma)\alpha'$, so since $A$ represents the map $\pi_{n-1} \circ \Phi$ with respect to the chosen basis of $I$, it follows that $\det A$ is equal to the determinant of the bilinear map $\Sigma\colon I \times (\alpha' I) \to R$ defined by $(\beta, \gamma) \mapsto \pi_{n-1}(\beta\gamma)$. Using the fact that $\det A = (-1)^{\lfloor \frac{n}{2} \rfloor} r$ (because $\mathrm{inv}(A) = r f^{\mathsf{mon}}(1,0)$ by assumption) together with the argument in the proof of Lemma 7, we find that

$$(-1)^{\lfloor \frac{n}{2} \rfloor} r = \det A = \det \Sigma = (-1)^{\lfloor \frac{n}{2} \rfloor} \frac{\mathrm{N}(\alpha')\,\mathrm{N}(I)^2}{\mathrm{N}(I_f^{n-2})}. \tag{1.20}$$

It follows from (1.20) that $\mathrm{N}(I)^2\,\mathrm{N}(\alpha') = r\,\mathrm{N}(I_f^{n-2})$, so since $\mathrm{N}(I)$, $\mathrm{N}(I_f^{n-2}) \in K^\times$ (as $I$ has rank $n$ over $R$ and $f_0 \neq 0$), we deduce that $\alpha' \in K_f^\times$, and the desired value $\alpha \in K_f^\times$ is simply given by $\alpha = \alpha'^{-1}$. □

Theorem 10 shows that the locus of pairs $(A, B) \in W_n(R)$ that arise via the above construction from binary forms in $V_{n,f_0}(R)$ is cut out by congruence conditions modulo $f_0^{n-1}$. It is a consequence of Theorem 18 (to follow) that these conditions amount to stipulating that $\wedge^i B \equiv 0 \pmod{f_0^{i-1}}$ for each $i \in \{2, \ldots, n\}$ when $f$ is primitive, and that when $R_f$ is the maximal order in $K_f$, they amount to stipulating that $B \pmod{f_0}$ is of rank $\leq 1$ (i.e., $B$ is a multiple of the square of a linear form modulo $f_0$). These simpler conditions play a crucial role in §4 (see, in particular, §4.3.2), where we use them to prove that the pairs $(A, B)$ arising from forms in $V_{n,f_0}(R)$ are, to an extent, equidistributed modulo $f_0$. This equidistribution result allows us to overcome the dependency of the parametrization on $f_0$.

We now determine the stabilizers of orbits arising from the above construction:

**Proposition 11.** *Let $(I, \alpha) \in H_{f,r}$, and let $\mathrm{End}_{R_f}(I)$ be the ring of $R_f$-module endomorphisms of $I$. The stabilizer in $G_n(R)$ of any representative of $\mathsf{orb}_{f,r}(I, \alpha)$ is isomorphic to the finite abelian group $\mathrm{End}_{R_f}(I)^\times[2]_{\mathrm{N}\equiv 1} := \{\rho \in \mathrm{End}_{R_f}(I)^\times[2] : \mathrm{N}(\rho) = 1\}$ if $n$ is odd and $\mathrm{End}_{R_f}(I)^\times[2]$ if $n$ is even.*

*Proof.* Let $(A, B) \in W_n(R)$ be a representative of $\mathsf{orb}_{f,r}(I, \alpha)$, and let $\mathrm{Stab}_{G_n(R)}(A, B)$ denote

the stabilizer of $(A, B)$ in $G_n(R)$. Then observe that

$$\mathrm{Stab}_{G_n(R)}(A, B) \subset Z := \{g \in \mathrm{GL}_n(K) : g \cdot -A^{-1}B \cdot g^{-1} = -A^{-1}B\}.$$

But as we computed in the proof of Theorem 6, $-A^{-1}B$ has separable characteristic polynomial $f^{\mathsf{mon}}(x, 1)$, so upon examining the rational canonical form of $-A^{-1}B$, we find that $Z = K[-A^{-1}B] \simeq K[f_0\theta] = K_f$. Thus, if $g = \mathrm{Stab}_{G_n(R)}(A, B)$, then $g$ is the matrix $g = m_\rho$ of multiplication by $\rho$ for some $\rho \in K_f^\times$. Since $g$ defines an invertible map of $R_f$-modules $g\colon I \to I$, we have $m_\rho \in \mathrm{End}_{R_f}(I)^\times$. Moreover, the bilinear maps $I \times I \to K_f$ defined by sending $(\beta, \gamma)$ to $\alpha^{-1}\beta\gamma$ and $\alpha^{-1}(\rho\beta)(\rho\gamma)$ must coincide, implying that $\rho^2 = 1$, and hence that $m_\rho \in \mathrm{End}_{R_f}(I)^\times[2]$.

Conversely, by imitating the argument in (1.19), we see that every $R_f$-module endomorphism of $I$ is given by multiplication by an element of $K_f$. In particular, we have $\mathrm{End}_{R_f}(I)^\times[2] \subset K_f^\times[2]$, and it is clear that the action of $K_f^\times[2]$ stabilizes $(A, B)$. Finally, the stabilizer of $(A, B)$ in $\mathrm{SL}_n(R)$ is the determinant-1 subgroup of $\mathrm{End}_{R_f}(I)^\times[2]$, which is simply $\mathrm{End}_{R_f}(I)^\times[2]_{\mathrm{N}\equiv 1}$. □

*Remark* 12. Note that $\mathrm{End}_{R_f}(I) \supset R_f$ and that this containment is an equality when the fractional ideal $I$ is invertible.

Combining the results obtained in this section thus far (namely, Theorem 6, Proposition 9, Theorem 10, and Proposition 11), we obtain the following precise formulation of Theorem 1:

**Theorem 13.** *The map* $\mathsf{orb}_{f,r}$ *defines a bijection from* $H_f$ *to the set of all* $G_n(R)$*-orbits of pairs* $(A, B) \in W_n(R)$ *such that:*

(a) $\iota(A, B) = rf^{\mathsf{mon}}$*; and*

(b) $p_i\big(f_0^{-1} \times -A^{-1}B\big) \in \mathrm{Mat}_n(R)$ *for each* $i \in \{1, \ldots, n-1\}$.

*Moreover, the above construction defines a natural bijection between* $G_n(R)$*-orbits on* $W_n(R)$ *satisfying the conditions* (a) *and* (b) *with equivalence classes of pairs* $(I, \alpha) \in H_{f,r}$*. The*

*stabilizer in $G_n(R)$ of the orbit corresponding to $(I, \alpha)$ is isomorphic to $\mathrm{End}_{R_f}(I)^\times[2]_{\mathrm{N}\equiv 1}$ if $n$ is odd and $\mathrm{End}_{R_f}(I)^\times[2]$ if $n$ is even.*

We often find it convenient to replace the binary $n$-ic form $f$ with an $\mathrm{SL}_2(R)$-translate thereof. We must therefore understand how the parametrization interacts with the action of $\mathrm{SL}_2$ on $V_n$. The following lemma establishes that the parametrization is covariant with respect to this action:

**Lemma 14.** *Let $\gamma = \left[\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right] \in \mathrm{SL}_2(R)$ be such that $-t\theta + s \neq 0$, and let $f' = \gamma \cdot f$. Then $\gamma$ induces a bijection between $H_{f,r}$ and $H_{f',r}$.*

*Proof.* Let $(A, B) \in W_n(R)$ with $\iota(A, B) = f^{\mathsf{mon}}$, and suppose that $(A, B)$ arises from a pair $(I, \alpha) \in H_{f,r}$. Then it follows from (1.7) that the pair $\big(\phi_{\frac{n}{2},\gamma}(I), \phi_{2,\gamma}(\alpha)\big)$ belongs to $H_{f',r}$. The desired bijection is given by $(I, \alpha) \mapsto \big(\phi_{\frac{n}{2},\gamma}(I), \phi_{2,\gamma}(\alpha)\big)$. □

**Example 15.** When $\gamma \in N(R) \subset \mathrm{SL}_2(R)$, the bijection in lemma 14 is given explicitly by $(A, B) \mapsto (A, f_0\gamma_{21}A + B)$, where $\gamma_{21}$ denotes the row-2, column-1 entry of $\gamma$.

We finish this section by taking $n$ to be even and translating Theorem 6 into statements about $(\mathrm{SL}_n/\mu_2)(R)$-orbits on $W_n(R)$; for the application in §4, we only need to do this in the case where $r = 1$. Let $\widetilde{H}_{f,r}$ denote the set of equivalence classes of pairs $(I, \alpha)$ of the form (1.13) with $r = 1$, with respect to the following modified equivalence relation: two pairs $(I_1, \alpha_1)$ and $(I_2, \alpha_2)$ are identified if there exists $\kappa \in K_f^\times$ and $\epsilon \in R^\times$ such that the based fractional ideals $I_2$ and $\kappa I_1$ are equal up to a $\mathrm{GL}_n(R)$-change-of-basis, $\mathrm{N}(I_2) = \mathrm{N}(\kappa)\epsilon^{\frac{n}{2}}\,\mathrm{N}(I_1)$, and $\alpha_2 = \kappa^2\epsilon\alpha_1$. Evidently, if $(I_1, \alpha_1)$ and $(I_2, \alpha_2)$ are equivalent under this modified relation, then the pairs in $W_n(R)$ that arise from $(I_1, \alpha_1)$ and $(I_2, \alpha_2)$ via the above construction belong to the same $(\mathrm{SL}_n/\mu_2)(R)$-orbit on $W_n(R)$. Thus, we have constructed a map of sets

$$\widetilde{\mathsf{orb}}_{f,1} \colon \widetilde{H}_{f,1} \to (\mathrm{SL}_n/\mu_2)(R)\backslash\big\{(A, B) \in W_n(R) : \iota(A, B) = f^{\mathsf{mon}}\big\}$$

In fact, by imitating the argument used to deduce [17, Theorem 17] from [17, Theorem 16], we obtain the following parametrization of $(\mathrm{SL}_n/\mu_2)(R)$-orbits on $W_n(R)$ from Theorem 6:

**Theorem 16.** *The map* $\widetilde{\mathsf{orb}}_{f,1}$ *defines a bijection from* $\widetilde{H}_{f,1}$ *to the set of all* $(\mathrm{SL}_n/\mu_2)(R)$*-orbits on* $W_n(R)$ *such that conditions* (a) *and* (b) *in Theorem 13 are satisfied with* $r = 1$*. The stabilizer in* $(\mathrm{SL}_n/\mu_2)(R)$ *of the orbit corresponding to the pair* $(I, \alpha) \in \widetilde{H}_{f,1}$ *is an elementary abelian* 2*-group that contains the group* $(\mathrm{End}_{R_f}(I)^\times[2])_{\mathrm{N}\equiv 1}/R^\times[2]$.

*Remark* 17. The parametrization developed in this section is inspired by [126], where Wood proves similar theorems in which the multiplication table of an ideal of $R_f$ gives rise to a pair $(A, B) \in W_n(R)$ with $\iota(A, B) = f$, rather than $f^{\mathsf{mon}}$.

### 1.4.2 Ranks of orbits arising from the parametrization

Now let $R = \mathbb{Z}_p$ for a prime $p$. In this section, we work with the action of the group $G_n$ and with the map $\mathsf{orb}_{f,r}$, although everything works just as well with $G_n$ replaced by $\mathrm{SL}_n/\mu_2$ and $\mathsf{orb}_{f,1}$ replaced by $\widetilde{\mathsf{orb}}_{f,1}$ when $n$ is even.

A pair $(A, B) \in W_n(\mathbb{Z}_p)$ with $\iota(A, B) = rf^{\mathsf{mon}}$ lies in the image of $\mathsf{orb}_{f,r}$ if certain congruence conditions modulo $f_0^{n-1}$, given by condition (b) in the statement of Theorem 6, are satisfied. Each of these conditions is of the following shape: for some $i \in \{1, \ldots, n\}$, a certain linear combination of the $i \times i$ minors of $-A^{-1}B$ must be divisible by $f_0^{i-1}$. For these conditions to hold, it is sufficient that $B$ be of *rank* $\leq 1$ *modulo* $f_0$, meaning that the $n$-ary quadratic form associated to $B$ is a multiple of the square of a linear form modulo $f_0$. More generally, it suffices for $B$ to be *special at* $f_0$, by which we mean that $\wedge^i B \equiv 0 \pmod{f_0^{i-1}}$ for each $i \in \{2, \ldots, n\}$. Note that if $B \in U_n(\mathbb{Z}_p)$ is special at $f_0$, then the following properties hold:

- $gB'g^T$ is also special at $f_0$ for any $g \in G_n(\mathbb{Z}_p)$ and $B' \in U_n(\mathbb{Z}_p)$ such that $B' \equiv B \pmod{f_0}$; and
- The pair $(A, B)$ lies in the image of $\mathsf{orb}_{\iota(A,B)^{\mathsf{dem}}_{f_0},r}$ for any $A \in U_n(\mathbb{Z}_p)$ with $\mathrm{inv}\, A = r$.

In this section, we prove the following result, which states that the pairs $(A, B) \in W_n(\mathbb{Z}_p)$ with $\iota(A, B) = rf^{\mathsf{mon}}$ that lie in the image of $\mathsf{orb}_{f,r}$ are often such that $B$ is of rank $\leq 1$ modulo $f_0$, and are very often such that $B$ is special at $f_0$.

**Theorem 18.** *Suppose $p \mid f_0$, and let $(A, B) \in W_n(\mathbb{Z}_p)$ be a pair lying in the image of $\mathsf{orb}_{f,r}$. If $p \nmid f_1$, then $B$ is of rank $\leq 1$ modulo $f_0$. If $f$ is primitive, then $B$ is special at $f_0$.*

*Proof.* We split into two cases, according as $p \nmid f_1$ or $f$ is primitive:

*Case 1*: We first show that $B$ is of rank 1 modulo $p$. Since $\operatorname{inv} A = r \in \mathbb{Z}_p^\times$, it suffices to prove that $-A^{-1}B$ is of rank 1 modulo $p$. First, observe that the characteristic polynomial of $-A^{-1}B$ over $\mathbb{F}_p$ is equal to $f^{\mathsf{mon}}(x, 1) \equiv x^n + f_1 x^{n-1} \pmod{p}$. Next, taking $i = 2$ in condition (b) in Theorem 6 yields that

$$p_2(\tfrac{1}{f_0} \times -A^{-1}B) = \tfrac{1}{f_0}\big((-A^{-1}B)^2 + f_1(-A^{-1}B))\big) \in \operatorname{Mat}_n(\mathbb{Z}_p), \tag{1.21}$$

and so the minimal polynomial of $-A^{-1}B$ over $\mathbb{F}_p$ is equal to $x^2 + f_1 x$. Comparing the characteristic and minimal polynomials of $-A^{-1}B$, we deduce that the rational canonical form of $-A^{-1}B$ over $\mathbb{F}_p$ must be diagonal with the first $n-1$ diagonal entries equal to 0 and last diagonal entry nonzero, as desired.

By the previous paragraph along with the $p$-adic Jordan decomposition, we may assume that $B$ is diagonal with the first $n-1$ diagonal entries divisible by $p$ and last diagonal entry a $p$-adic unit. Multiplying (1.21) through by $A$, we find that

$$BA^{-1}B - f_1 B \equiv 0 \pmod{f_0}. \tag{1.22}$$

Since $\nu_p(f_1) = 0$ and since $p$ divides each of the first $n-1$ diagonal entries of $B$, the $p$-adic valuation of each of the first $n-1$ diagonal entries of $BA^{-1}B$ is strictly larger than that of the corresponding diagonal entry of $-f_1 B$. Thus, in order for (1.22) to be satisfied, the $p$-adic valuation of each of the first $n-1$ diagonal entries of $B$ must be at least as big as $\nu_p(f_0)$, as necessary.

*Case 2*: Since $f$ is primitive, it factorizes over $\mathbb{Z}_p$ as $f = F_1 \times (f/F_1)$, where $F_1$ is a unit multiple of $y^{e_1} \bmod p$ for some $e_1 \in \{1, \ldots, n\}$ and $f/F_1$ is a monic binary form (cf. §2.3.1,

to follow). Then we have the product decomposition $R_f \simeq R_{F_1} \times R_{f/F_1}$. Thus, any fractional ideal $I$ of $R_f$ may be expressed as a product $J_{F_1} \times J_{f/F_1}$, where $J_{F_1}$ and $J_{f/F_1}$ are fractional ideals of $R_{F_1}$ and $R_{f/F_1}$, respectively.

Let $(I, \alpha) \in H_{f,r}$. Then expressing $I$ as a product $J_{F_1} \times J_{f/F_1}$, we see that $\mathsf{orb}_{f,r}(I, \alpha)$ must contain an element $(A, B) \in W_n(\mathbb{Z}_p)$ such that both $A$ and $B$ are block-diagonal with one $e_1 \times e_1$ block followed by one $(n - e_1) \times (n - e_1)$ block. Let $A_{F_1}, B_{F_1}$ denote the $e_1 \times e_1$ blocks of $A, B$, and let $A_{f/F_1}, B_{f/F_1}$ denote their $(n - e_1) \times (n - e_1)$ blocks.

The proof of Theorem 6 shows that $-A^{-1}B$ is the matrix of multiplication by $f_0\theta \in R_f$ on the basis of $I$ obtained by concatenating bases of $I_1$ and $I_2$. It follows that $-A_{F_1}^{-1}B_{F_1}$ (resp., $-A_{f/F_1}^{-1}B_{f/F_1}$) is the matrix of multiplication by $f_0\theta \in R_{F_1}$ (resp., $f_0\theta \in R_{f/F_1}$) on the basis of $J_{F_1}$ (resp., $J_{f/F_1}$). We immediately see that $B_{f/F_1} \equiv 0 \pmod{f_0}$, since $f/F_1$ has unit leading coefficient, which implies that $\theta \in R_{f/F_1}$ and hence that $f_0^{-1}B_{f/F_1}$ has integral entries. As for $B_{F_1}$, we have that $\det(xA_{F_1} + yB_{F_1})$ is a unit multiple of $F_1^{\mathsf{mon}}(x, y)$, since $F_1^{\mathsf{mon}}(x, 1)$ is the characteristic polynomial of multiplication by $f_0\theta$ on $K_{F_1}$. The $y^{e_1}$-coefficient of $F_1$ is a unit, so it follows that $\nu_p(\det B_{F_1}) = \nu_p(f_0)(n-1)$, and taking $i = n - 1$ in condition (b) of Theorem 6 yields that $\wedge^{n-1}B_{F_1} \equiv 0 \pmod{f_0^{n-2}}$ (cf. proof of Theorem 111, to follow). Consequently, in the $p$-adic Jordan decomposition (see [48, p. 104–107]) of $B_{F_1}$, the $p$-adic valuation of each diagonal entry is at most $\nu_p(f_0)$. Thus, if $B_{F_1}$ is not special at $f_0$, then $\nu_p(\det B_{F_1}) < \nu_p(f_0)(n-1)$, which is a contradiction. □

### 1.4.3 Orbits over fields

When $R = K$ is a field, the parametrization developed in §1.4.1 simplifies considerably. Let $f \in V_{n,f_0}(K)$ be separable, let $r \in K^\times$, and let $(I, \alpha) \in H_{f,r}$. Over $K$, the data of a based fractional ideal of $R_f = K_f$ is encoded in its basis, so the condition that $I^2 \subset \alpha I_f^{n-2}$ holds trivially in this setting. Since the parametrization is only concerned with based fractional ideals up to multiplication by elements of $K_f^\times$ and change-of-basis by an element of $G_n(K)$, we may replace every instance of the based fractional ideal $I$ with $|\,\mathrm{N}(I)|$. But the value

of $\alpha \in K_f^\times$ determines $|\,\mathrm{N}(I)|$ via the condition that $\mathrm{N}(I)^2 = r\,\mathrm{N}(\alpha)\,\mathrm{N}(I_f^{n-2})$, so we may unambiguously express the pair $(I, \alpha)$ as $(K_f, \alpha)$. Moreover, the conditions (1.15) hold trivially because $f_0$ is a unit in $K$. We thus obtain the following result:

**Proposition 19.** *The assignment $(K_f, \alpha) \mapsto f_0^n \alpha$ defines a bijection between the elements of the set $H_{f,r}$ (which parametrizes $G_n(K)$-orbits of pairs $(A, B) \in W_n(K)$ such that $\iota(A, B) = rf^{\mathsf{mon}}$) and those of the set $(K_f^\times / K_f^{\times 2})_{\mathrm{N} \equiv r}$. The stabilizer in $G_n(K)$ of such an orbit is isomorphic to $K_f^\times[2]_{\mathrm{N}\equiv 1}$ if $n$ is odd and $K_f^\times[2]$ if $n$ is even.*

We say that the $G_n(K)$-orbit of a pair $(A, B) \in W_n(K)$ satisfying $\iota(A, B) = rf^{\mathsf{mon}}$ is *distinguished* if it corresponds under the bijection given by Proposition 19 to $1 \in K_f^\times / K_f^{\times 2}$ when $n$ is odd and to $1 \in K_f^\times / K_f^{\times 2} K^\times$ when $n$ is even. One verifies as in [15, §4.1] (resp., [105, §2.2]) that when $n$ is odd (resp., even), a pair $(A, B) \in W_n(K)$ belongs to the distinguished $G_n(K)$-orbit if and only if (the symmetric bilinear forms associated to) $A$ and $B$ share a maximal isotropic subspace defined over $K$ (resp., $B$ has an isotropic subspace of dimension $\frac{n-2}{2}$ defined over $K$ contained within a maximal isotropic subspace for $A$ defined over $K$).

We also consider a notion closely related to distinguishedness called reducibility: the $G_n(K)$-orbit of a pair $(A, B) \in W_n(K)$ satisfying $\iota(A, B) = rf^{\mathsf{mon}}$ is *reducible* if it corresponds under the bijection given by Proposition 19 to $1 \in K_f^\times / K_f^{\times 2}$. Note that reducible orbits are distinguished and that the converse holds when $n$ is odd (but not when $n$ is even).

We say that the $\mathcal{G}_{\mathscr{A}_n}(K)$-orbit of $B \in W_{\mathscr{A}_n}(K)$ is distinguished/reducible if the corresponding $G_n(K)$-orbit of $(\mathscr{A}_n, B) \in W_n(K)$ is distinguished/reducible. We will have occasion to use the following explicit characterization of reducible $\mathcal{G}_{\mathscr{A}_n}(K)$-orbits on $W_{\mathscr{A}_n}(K)$:

**Proposition 20** ([15, Proposition 4.4] and [105, Proposition 7])**.** *An element $B \in W_{\mathscr{A}_n}(R)$ is reducible if and only if for some $\mathcal{G}_{\mathscr{A}_n}(K)$-translate $B' = [b'_{ij}] \in W_{\mathscr{A}_n}(K)$ of $B$ we have that $b'_{ij} = 0$ for all pairs $(i, j)$ such that $i + j \leq n - 1$.*

Next, by imitating the argument used to deduce [17, Corollary 20] from (the proof of) [17, Theorem 17], we obtain the following corollary of (the proof of) Theorem 16 parametrizing

the orbits of $(\mathrm{SL}_n/\mu_2)(K)$ on $W_n(K)$ when $n$ is even and $r = 1$:

**Proposition 21.** *The elements of the set $\widetilde{H}_{f,1}$ (which parametrizes $(\mathrm{SL}_n/\mu_2)(K)$-orbits of pairs $(A, B) \in W(K)$ such that $\iota(A, B) = f^{\mathsf{mon}}$) are in natural bijection with equivalence classes of pairs $(\varepsilon, \alpha)$ consisting of numbers $\varepsilon \in K^\times$ and $\alpha \in K_f^\times$ such that $\varepsilon^2 = \mathrm{N}(\alpha) f_0^{2-n}$, where we declare two such pairs $(\varepsilon, \alpha)$ and $(\varepsilon', \alpha')$ equivalent if there exist numbers $\kappa \in K_f^\times$ and $r \in K^\times$ such that $\varepsilon' = \mathrm{N}(\kappa) r^{\frac{n}{2}} \varepsilon$ and $\alpha' = \kappa^2 r \alpha$. The stabilizer subscheme in $\mathrm{SL}_n/\mu_2$, viewed as a $K$-scheme, of the orbit corresponding to $(\varepsilon, \alpha)$ is isomorphic to $(\mathrm{Res}_{K_f/K} \mu_2)_{\mathrm{N}\equiv 1}/\mu_2$.*

*Moreover, the map from $\widetilde{H}_{f,1}$ to $(K_f^\times/K_f^{\times 2}K^\times)_{\mathrm{N}\equiv 1}$ defined by sending $(\varepsilon, \alpha) \mapsto \alpha$ is an at most two-to-one surjection.*

We say that an $(\mathrm{SL}_n/\mu_2)(K)$-orbit on $W_n(K)$ is distinguished if it corresponds via Proposition 21 to $1 \in K_f^\times/K_f^{\times 2}K^\times$. Similarly, we say that the $\mathrm{PSO}_{\mathscr{A}_n}(K)$-orbit of $B \in W_{\mathscr{A}_n}(K)$ is distinguished if the corresponding $(\mathrm{SL}_n/\mu_2)(K)$-orbit of $(\mathscr{A}_n, B) \in W_n(K)$ is distinguished.

Now let $R$ be a PID. As an application of the parametrization of rational orbits, we finish by describing how a $G_n(R)$-orbit on $W_n(R)$ lying in the image of $\mathsf{orb}_{f,r}$ transforms when $f$ is replaced with a scalar multiple of itself by an element of $R \smallsetminus \{0\}$ (not necessarily a unit):

**Lemma 22.** *Suppose that the $G_n(R)$-orbit of $(A, B) \in W_n(R)$ lies in $\mathsf{orb}_{f,r}(H_{f,r})$, and let $\lambda \in R \smallsetminus \{0\}$. Then the $G_n(R)$-orbit of $(A, \lambda B) \in W_n(R)$ lies in $\mathsf{orb}_{\widetilde{f},r}(H_{\widetilde{f},r})$, where $\widetilde{f} = \lambda f$. Moreover, the $G_n(K)$-orbit of $(A, \lambda B)$ corresponds via the bijection in Proposition 19 to the class of $\lambda^{-1}\alpha \in (K_f^\times/K_f^{\times 2})_{\mathrm{N}\equiv 1}$.*

*Proof.* One verifies by inspection that the pair $(A, \lambda B) \in W_n(R)$ satisfies the conditions (a) and (b) in Theorem 13, with $f$ replaced by $\widetilde{f} := \lambda f$. To compute the $G_n(K)$-orbit of $(A, \lambda B)$, we work over $K$, where based fractional ideals are just bases. The operation of replacing the pair $(A, B)$ with $(A, \lambda B)$ transforms the resolvent $\iota(A, B) = f^{\mathsf{mon}}$ into the new

form $\iota(A, \lambda B) = \widetilde{f}^{\mathsf{mon}}$. For each of $I_f^{n-2}$ and $I_{\widetilde{f}}^{n-2}$, the basis (1.3) is given by

$$I_f^{n-2} = K\langle 1, \theta, \theta^2, \ldots, \theta^{n-2}, \zeta_{n-1}\rangle \quad \text{and} \quad I_{\widetilde{f}}^{n-2} = K\langle 1, \theta, \theta^2, \ldots, \theta^{n-2}, \lambda\zeta_{n-1}\rangle. \tag{1.23}$$

Suppose $(A, B)$ corresponds to a pair $(I, \alpha)$ via Theorem 6. We claim that the pair $(I, \lambda^{-1}\alpha) \in H_{\widetilde{f},r}$, and that it corresponds to $(A, \lambda B)$ via Theorem 6. Upon comparing the bases in (1.23), it is evident that the bilinear forms $\pi_{n-1} \circ \langle -, - \rangle$ and $\pi_{n-2} \circ \langle -, - \rangle$ arising from the pair $(I, \lambda^{-1}\alpha)$ are represented by the matrices $A$ and $\lambda B$ with respect to the chosen basis of $I$. It thus remains to verify that the pair $(I, \lambda^{-1}\alpha) \in H_{\widetilde{f},r}$. Let N denote the based fractional ideal norm with respect to the basis (1.1) of $R_f$, and let $\widetilde{\mathrm{N}}$ denote this norm with respect to the basis (1.1) of $R_{\widetilde{f}}$. Then a calculation reveals that $\widetilde{\mathrm{N}}(I) = \lambda^{1-n}\,\mathrm{N}(I)$ for any basis $I$. Note that this does *not* extend to norms of numbers: it follows from the definition of the norm of a number in §1.2 that $\widetilde{\mathrm{N}}(\alpha) = \mathrm{N}(\alpha)$. It now suffices to show that $\widetilde{\mathrm{N}}(I)^2 = r\widetilde{\mathrm{N}}\big(\lambda^{-1}\alpha\big)(\lambda f_0)^{2-n}$, which is equivalent to showing that $\big(\lambda^{1-n}\,\mathrm{N}(I)\big)^2 = r\big(\lambda^{-n}\,\mathrm{N}(\alpha)\big)(\lambda f_0)^{2-n}$, but this holds since $\mathrm{N}(I)^2 = r\,\mathrm{N}(\alpha) f_0^{2-n}$. □

# Chapter 2

# Average 2-torsion in class groups of number fields defined by binary forms

This chapter is largely based on my paper [116], with some results also drawn from my joint work [14] with Manjul Bhargava, Jan-Hendrik Evertse, Kálmán Győry, and László Remete.

## 2.1 Introduction

An order $\mathcal{O}$ in a number field $K$ of degree $n$ is said to be *monogenic* if it is singly generated as an algebra over $\mathbb{Z}$. More generally, for an integer $f_0 \neq 0$, we say that the order $\mathcal{O}$ is $f_0$-*monogenic* if there exists a binary form $f \in V_{n,f_0}(\mathbb{Z})$ such that $\mathcal{O} \simeq R_f$. Note that when $|f_0| = 1$, the notions of $f_0$-monogenicity and monogenicity coincide.

In recent work [18], Bhargava, Hanke, and Shankar made a surprising discovery: imposing the condition of $f_0$-monogenicity has the effect of increasing the average size of the 2-torsion in the class groups of *cubic* number fields (i.e., the case $n = 3$). In [108, 109], Siad showed that an analogous increase occurs for *monogenic* number fields of *any* given degree $n \geq 3$ (i.e., the case $|f_0| = 1$). The purpose of this chapter is to use the parametrization developed in §1 to study the effect of $f_0$-monogenicity on the average 2-torsion in class groups of degree-$n$ number fields for *any* $f_0 \neq 0$ and $n \geq 3$. Specifically, we determine upper bounds on the

average size of the 2-torsion in the class groups of $f_0$-monogenic number fields of given degree $n \geq 3$, and conditional on a uniformity estimate, we show that these bounds are optimal.

For this application, our parametrization has two key advantages. Firstly, it allows us to obtain the 2-class group average for every choice of the pair $(f_0, n)$ *simultaneously*, including the case where $|f_0| > 1$ and $n$ is even, which was not previously tractable. Secondly, as the parametrization is leading-coefficient-dependent, it is conducive to applications concerning binary forms with fixed leading coefficient. Thus, although the case where $|f_0| > 1$ and $n$ is odd can be handled using the parametrizations of Bhargava and Wood mentioned in §1.1.1, our new parametrization leads to a simpler proof. By generalizing an equidistribution argument that we develop in §4, one can average the main results of this chapter over all leading coefficients and thus deduce analogues for the full family of integral binary forms of given degree; we plan to carry this out in future work.

While $f_0$-monogenicity may seem at first glance to be an unnatural condition, the bounds we obtain (which are conditionally the exact values) depend in a surprisingly beautiful way on $f_0$. As explained in §2.1.2 (to follow), our results suggest that imposing the condition of $f_0$-monogenicity causes the average 2-torsion in the class group to increase, relative to the value predicted by the heuristics of Cohen–Lenstra [46], Cohen–Martinet [47], Malle [83], and Breen [36]. When $n$ is odd, the size of this increase decays rapidly to zero as the number of odd-multiplicity prime factors of $f_0$ grows, whereas when $n$ is even, the size of this increase is bounded away from zero, independent of $f_0$. The manner in which the averages depend on $f_0$ demonstrates that $f_0$-monogenicity is a natural and interesting condition to study in the context of class group distributions for number fields.

### 2.1.1 Main results on class group distributions

In this section, we state our results concerning the effect of $f_0$-monogenicity on the average size of the 2-torsion in class groups of number fields.

#### 2.1.1.1 Notation

We begin by introducing the necessary notation. If $R = \mathbb{Z}$ or $\mathbb{Z}_p$ for a prime $p$, we adorn $V_n(R)$ or $V_{n,f_0}(R)$ with a subscript $_{\max}$ to indicate the subset of forms $f$ such that: (a) $R_f$ is the maximal order in $K_f$, and (b) 2 does not ramify in $R_f$. If $R = \mathbb{Z}$ or $\mathbb{R}$, we use a superscript $^{r_1,r_2}$ to indicate the subset of forms $f$ such that $K_f$ has real signature $(r_1, r_2)$ (i.e., $r_1$ real roots and $r_2$ pairs of complex conjugate roots).

Observe that the group $N(\mathbb{Z})$ acts on $V_{n,f_0}(\mathbb{Z})$, and recall from §1.2 that $N(\mathbb{Z})$-equivalent forms define isomorphic rings. Thus, to minimize redundancies in the families of number fields under consideration, we count binary forms in $V_{n,f_0}(\mathbb{Z})$ up to the action of $N(\mathbb{Z})$. For $f \in V_{n,f_0}(\mathbb{R})$, we define its height $\mathrm{H}(f)$ as follows: letting

$$\widetilde{f}(x,y) = x^n + \sum_{i=2}^{n} \widetilde{f}_i x^{n-i} y^i \in V_{n,1}(\mathbb{R}) \tag{2.1}$$

denote the unique $N(\mathbb{R})$-translate of $f^{\mathsf{mon}}$ with $x^{n-1}y$-coefficient 0, then we put

$$\mathrm{H}(f) := \max\{|\widetilde{f}_i|^{1/i} : 2 \le i \le n\}. \tag{2.2}$$

Note that H descends to a well-defined height function on $N(\mathbb{Z})\backslash V_{n,f_0}(\mathbb{R})$. Given an $N(\mathbb{Z})$-invariant subset $\mathcal{F} \subset V_{n,f_0}(\mathbb{Z})$ and an $N(\mathbb{Z})$-invariant map $\phi\colon \mathcal{F} \to \mathbb{Z}_{\ge 0}$, the average value of $\phi$ on $\mathcal{F}$ is given by

$$\operatorname*{Avg}_{f\in\mathcal{F}} \phi(f) := \lim_{X\to\infty} \left(\sum_{\substack{f\in N(\mathbb{Z})\backslash\mathcal{F} \\ \mathrm{H}(f)<X}} \phi(f)\right) \Big/ \left(\sum_{\substack{f\in N(\mathbb{Z})\backslash\mathcal{F} \\ \mathrm{H}(f)<X}} 1\right) \tag{2.3}$$

We write $\mathrm{Avg}_{f\in\mathcal{F}}\,\phi(F) \le \star$ if the limsup as $X \to \infty$ of the fraction in (2.3) is at most $\star$.

#### 2.1.1.2 Statements of results, part $(i)$: odd degree

Factor $f_0$ as $f_0 = m^2 k$, where $k$ is squarefree. Our first main result bounds (and conditionally determines) the average 2-torsion in the class groups of the ($f_0$-monogenic) number fields

cut out by binary forms in $V_{n,f_0}(\mathbb{Z})^{r_1,r_2}_{\max}$, generalizing [18, Theorem 5] and [108, Theorem 6]:

**Theorem 23.** *Let $n \geq 3$ be odd. Then we have*

$$\operatorname*{Avg}_{f \in V_{n,f_0}(\mathbb{Z})^{r_1,r_2}_{\max}} \#\operatorname{Cl}(R_f)[2] \leq 1 + 2^{1-r_1-r_2}\left(1 + \frac{1}{k^{\frac{n-3}{2}}\sigma(k)}\right) \tag{2.4}$$

*where $\sigma(k) := \sum_{1 \leq d \mid k} d$. If the estimate* (2.45) *holds, then we have equality in* (2.4).

In fact, our methods allow us to prove a generalization of Theorem 23 to families of fields in $V_{n,f_0}(\mathbb{Z})^{r_1,r_2}_{\max}$ satisfying certain "acceptable" infinite sets of local conditions (see §2.5.1 for the precise definition). To state this generalization, we make the following definition: for a prime $p \mid k$, we say that a primitive form $f \in V_{n,f_0}(\mathbb{Z}_p)$ is *squareful* if $f/y$ is a unit multiple of a perfect square modulo $p$. Note that, by [88, Proposition 8.3], squarefulness amounts to a condition on the splitting type of $p$ in $R_f$. Then we have the following result, generalizing [18, Theorem 7]:

**Theorem 24.** *Let $n \geq 3$ be odd, and let $\Sigma$ be a family of local specifications defining an "acceptable" subfamily $V_{n,f_0}(\Sigma) \subset V_{n,f_0}(\mathbb{Z})^{r_1,r_2}_{\max}$. For each prime $p$, let $r_p(\Sigma)$ denote the $p$-adic density of forms $f \in V_{n,f_0}(\Sigma)$ that are squareful at $p$. Then we have*

$$\operatorname*{Avg}_{f \in V_{n,f_0}(\Sigma)} \#\operatorname{Cl}(R_f)[2] \leq 1 + 2^{1-r_1-r_2}\left(1 + \prod_{p \mid k} r_p(\Sigma)\right) \tag{2.5}$$

*If the estimate* (2.45) *holds, then we have equality in* (2.5).

The squareful densities $r_p(\Sigma)$ can be calculated in various cases of interest. For example, the $p$-adic density of squareful forms among forms defining maximal orders is given by Theorem 49 to be $p^{\frac{1-n}{2}}(1+p^{-1})^{-1}$, and substituting this density into Theorem 24 yields Theorem 23. Upon applying Theorem 24 to the subset of forms that *fail* to be squareful in at least one place, we obtain the following result, generalizing [18, Theorem 6]:

**Theorem 25.** *With notation as in Theorem 24, suppose $r_p(\Sigma) = 0$ for some prime $p \mid k$. Then we have*

$$\operatorname*{Avg}_{f \in V_{n,f_0}(\Sigma)} \#\operatorname{Cl}(R_f)[2] \leq 1 + 2^{1-r_1-r_2}. \tag{2.6}$$

*If the estimate* (2.45) *holds, then we have equality in* (2.6).

#### 2.1.1.3 Statements of results, part (*ii*): even degree

We say that a primitive form $f \in \mathcal{F}_n(f_0, \mathbb{Z}_p)$ is *evenly ramified* if $f$ is a unit multiple of a perfect square modulo $p$. Note that, by [88, Proposition 8.3], $f$ being evenly ramified amounts to $p$ having total ramification of degree 2 in $R_f$. Our next result bounds (and conditionally determines) the average 2-torsion in the ordinary class groups and narrow class groups of the ($f_0$-monogenic) number fields cut out by binary forms in $V_{n,f_0}(\mathbb{Z})^{r_1,r_2}_{\max}$, generalizing [109, Theorem 9]:

**Theorem 26.** *Let $n \geq 4$ be even, and let $\Sigma$ be a family of local specifications defining an "acceptable" subfamily $\mathcal{F}_n(f_0, \Sigma) \subset V_{n,f_0}(\mathbb{Z})^{r_1,r_2}_{\max}$. For each prime $p$, let $r_p(\Sigma)$ denote the $p$-adic density of forms $f \in \mathcal{F}_n(f_0, \Sigma)$ that are evenly ramified at $p$. If $r_1 = 0$, then $\#\operatorname{Cl}(R_f)[2] = \#\operatorname{Cl}^+(R_f)[2]$, and*

$$\operatorname*{Avg}_{f \in V_{n,f_0}(\Sigma)} \#\operatorname{Cl}(R_f)[2] \leq (1 + 2^{2-r_2}) \prod_{p>2} (1 + r_p(\Sigma)) \tag{2.7}$$

*If $r_1 > 0$, then we have the following pair of inequalities:*

$$\operatorname*{Avg}_{f \in V_{n,f_0}(\Sigma)} \#\operatorname{Cl}(R_f)[2] \leq \frac{1}{2}\left((1 + 2^{3-r_1-r_2}) \prod_{p>2} (1 + r_p(\Sigma)) + \prod_{p>2} \left(1 + (-1)^{\frac{p-1}{2}} r_p(\Sigma)\right)\right) \tag{2.8}$$

$$\operatorname*{Avg}_{f \in V_{n,f_0}(\Sigma)} \#\operatorname{Cl}^+(R_f)[2] \leq (1 + 2^{-r_2} + 2^{1-\frac{n}{2}}) \prod_{p>2} (1 + r_p(\Sigma)) \tag{2.9}$$

*If the estimate* (2.45) *holds, then we have equality in* (2.7), (2.8), *and* (2.9).

The even ramification densities $r_p(\Sigma)$ can be calculated in various cases of interest. For example, if $p \nmid f_0$, the $p$-adic density of evenly ramified forms among forms defining maximal orders is given by Theorem 42 to be $p^{-\frac{n}{2}}(1+p^{-1})^{-1}$. However, unlike in the odd-degree case, substituting this formula for $r_p(\Sigma)$ into any one of (2.7), (2.8), or (2.9) fails to produce a closed-form expression. Upon applying Theorem 26 to the subset of forms that are nowhere evenly ramified, we obtain the following result, generalizing [109, Corollary 12]:

**Theorem 27.** *With notation as in Theorem 26, suppose $r_p(\Sigma) = 0$ for every $p$. If $r_1 = 0$, then $\#\operatorname{Cl}(R_f)[2] = \#\operatorname{Cl}^+(R_f)[2]$, and*

$$\operatorname*{Avg}_{f \in V_{n,f_0}(\Sigma)} \#\operatorname{Cl}(R_f)[2] \leq 1 + 2^{2-r_2} \tag{2.10}$$

*If $r_1 > 0$, then we have the following pair of inequalities:*

$$\operatorname*{Avg}_{f \in V_{n,f_0}(\Sigma)} \#\operatorname{Cl}(R_f)[2] \leq 1 + 2^{2-r_1-r_2} \tag{2.11}$$

$$\operatorname*{Avg}_{f \in V_{n,f_0}(\Sigma)} \#\operatorname{Cl}^+(R_f)[2] \leq 1 + 2^{-r_2} + 2^{1-\frac{n}{2}} \tag{2.12}$$

*If the estimate* (2.45) *holds, then we have equality in* (2.10), (2.11), *and* (2.12).

An easy consequence of Theorem 27 is that number fields cut out by even-degree binary forms (with any fixed nonzero leading coefficient) often have odd class number; a similar result for odd-degree forms (with varying leading coefficient) was proven in Ho–Shankar–Varma [71, Corollary 6.7].

**Corollary 28.** *The density of $f \in V_{n,f_0}(\mathbb{Z})^{r_1,r_2}_{\max}$ with $2 \nmid \#\operatorname{Cl}(R_f)$ is $1 - O(2^{-\frac{n}{2}})$.*

### 2.1.2 Comparison with class group heuristics

In their foundational paper [46], Cohen and Lenstra formulated definitive heuristics for the distribution of the class groups of quadratic fields. Their heuristics were later generalized

by Cohen and Martinet to predict the distribution of class groups of number fields of any fixed degree over a fixed base field, with the caveat that their predictions about the $p$-part of the class group only apply when $p$ is a so-called *good* prime [47]. Subsequently, Malle adjusted the heuristics of Cohen–Martinet to account for discrepancies in the $p$-parts of the class groups of field extensions over a base field containing the $p^{\text{th}}$-roots of unity [83]. The heuristics of Cohen–Lenstra–Martinet–Malle yield the following prediction about the average size of the 2-torsion in class groups of odd-degree number fields:

**Conjecture 29** (Cohen–Lenstra–Martinet–Malle)**.** *Let $n \geq 3$ be odd. Consider the set of isomorphism classes of degree-$n$ number fields with real signature $(r_1, r_2)$ and Galois group $S_n$. When these fields are ordered by discriminant, the average size of the 2-torsion in the class group is $1 + 2^{1-r_1-r_2}$.*

To this day, only one case of Conjecture 29 has ever been proven: using a variant of the parametrization mentioned in §1.1.1, Bhargava determined the average 2-torsion in class groups of cubic number fields [8]. Prior to Bhargava, the only other case of the Cohen–Lenstra–Martinet–Malle heuristics that had been tackled was that of the average 3-torsion in class groups of quadratic fields, the determination of which is due to Davenport and Heilbronn in their seminal paper [58].

In the years since Bhargava's breakthrough, a considerable body of evidence has been generated to support the view that Conjecture 29 remains robust when one passes to subfamilies of fields defined by local or global conditions. For instance, Bhargava and Varma showed that, in the cubic case, the average stays the same for subfamilies of fields satisfying infinite sets of local conditions [30]. Subsequently, Ho, Shankar, and Varma considered families of fields cut out by odd-degree binary forms and applied Wood's generalization of Bhargava's parametrization to prove that the average 2-torsion in their class groups is as predicted by Conjecture 29—even though fields cut out by binary $n$-ic forms are expected to be sparse among all degree-$n$ fields as soon as $n > 3$.

In light of the apparent robustness of Conjecture 29, Theorems 23 and 24 are surprising:

somehow, imposing the condition of $f_0$-monogenicity causes the average 2-torsion in the class group to deviate from the conjectured value. The effect of $f_0$-monogenicity on the averages in (2.4) and (2.5) can be seen in the extra term $2^{1-r_1-r_2}\prod_{p|k} r_p(\Sigma)$, which is nonzero whenever a positive density of the forms under consideration are squareful at each prime $p \mid k$.

The problem of studying the distribution of the 2-parts, or more generally the 2-Sylow subgroups, of class groups of even-degree number fields is far more subtle—here, 2 is a bad prime in the sense of Cohen–Martinet. Significant progress has been made in the quadratic case: Fouvry and Klüners determined the distribution of the 4-torsion [64] in class groups of quadratic fields, and Smith recently handled the case of the $2^d$-torsion for every $d \geq 2$ [112]. Along with Siad's results in the monogenic case, Theorems 26 and 27 are the first of their kind to describe the distribution of the 2-torsion in class groups of number fields of even degree $n \geq 4$.

A complete set of heuristics for the distribution of the 2-torsion in class groups of even-degree number fields remains to be formulated. A key obstacle to formulating such heuristics has been understanding the effect of even ramification (also known as genus theory in the sense of Gauss), which can cause the 2-torsion in the class group to increase. At least for number fields cut out by binary forms, Theorem 26 shows that even ramification at a prime $p$ has a doubling effect on the average 2-torsion in the class group. This is not surprising: if an integral binary form $f$ defining a maximal order $R_f$ is evenly ramified over $\mathbb{Z}_p$, then the ideal $(p)$ has a square root, which could contribute to the 2-torsion in the class group of $R_f$.

Nonetheless, in the absence of even ramification, we have the following recent conjecture of Breen (see [36, Conjecture 6.0.2]), building on the work of Cohen–Lenstra–Martinet–Malle:

**Conjecture 30.** *Let $n \geq 4$ be even. Consider the set of isomorphism classes of nowhere-evenly-ramified degree-$n$ number fields with real signature $(r_1, r_2)$ and Galois group $S_n$. When these fields are ordered by discriminant, the average size of the 2-torsion in the class group is $1 + 2^{1-r_1-r_2}$.*

The average we obtained in Theorem 27 is notably larger than that predicted in Con-

jecture 30. This bears both similarities to and differences from the odd-degree case: while imposing the condition of $f_0$-monogenicity has an increasing effect on the mean number of 2-torsion elements in the class groups of number fields of *any* degree $n \geq 3$, this effect *vanishes* (resp., *remains constant*) upon averaging this mean over all leading coefficients when $n$ is odd (resp., even).

In light of the above discussion, it is natural to ask: *Why* does $f_0$-monogenicity have an increasing effect on the average 2-torsion? The results of this chapter bring us closer to answering this question. To see how, note that the extra 2-torsion is supported in the odd-degree case on fields cut out by binary forms that are squareful at every prime $p \mid k$, and in the even-degree case on all fields cut out by binary forms. The fields on which the extra 2-torsion is supported share a beautiful property: the set of square roots of the class of the inverse different—which constitutes a torsor of the 2-torsion in the class group—has a "distinguished" element, in a sense to be made precise in §2.4. Indeed, we have the following result:

**Theorem 31.** *Let $n \geq 3$, and take a primitive form $f \in V_{n,f_0}(\mathbb{Z})^{r_1,r_2}$. If $n$ is even or if $n$ is odd and $F$ belongs to $V_{n,f_0}(\mathbb{Z}_p)_{\max}$ for each prime $p \mid f_0$ and is squareful at each $p \mid k$, then the ideal class of the inverse different of $R_f$ has a "distinguished" square root.*

We expect that the presence of a distinguished square root of the class of the inverse different plays a role in causing the aforementioned increase in the average 2-torsion in the class group, and it remains open to determine the precise mechanism by which this increase occurs.

*Remark* 32. As it happens, Hecke's theorem does not extend to all non-maximal orders in number fields. Indeed in [111, §4], Simon shows that when $f(x,y) = 7x^3+10x^2y+5xy^2+6y^3$, the ring $R_f$ is not the maximal order in $K_f$ and the class of the inverse different of $R_f$ is not a square! Nonetheless, Theorem 31 implies that when forms $f \in V_{n,f_0}(\mathbb{Z})^{r_1,r_2}$ are ordered by height, a positive proportion are such that $R_f$ satisfies the conclusion of Hecke's theorem despite not being maximal.

### 2.1.3 Method of proof and organization

We now summarize the proofs of our main results. Because the parametrization developed in §1 produces $G_n(\mathbb{Z})$-orbits of pairs $(A, B) \in W_n(\mathbb{Z})$ such that $\iota(A, B) = \pm f^{\mathsf{mon}}$ as output, it has the effect of reducing the problem of counting 2-torsion classes in rings associated to forms with fixed leading coefficient into the simpler problem of counting $G_n(\mathbb{Z})$-orbits on $W_n(\mathbb{Z})$ over the space of forms with leading coefficient $\pm 1$, which is precisely the problem that Siad solved in [108, 109]. By reducing the non-monic case to the monic case (up to a sign), our new parametrization allows us to largely avoid doing the intricate mass calculations that form a key ingredient in the argument in [18].

We start in §2.2 by explaining the connection between our parametrization, which *a priori* concerns the class of the inverse different, and the problem of counting 2-torsion elements in class groups. Next, in §2.3, we characterize the orbits of $G_n(R)$ on $W_n(R)$ that arise from square roots of the class of the inverse different, where $R = \mathbb{Z}_p$ for a prime $p$. In §2.4, we describe the distinguished orbits arising from square roots of the class of the inverse different, and we prove Theorem 31. Finally, in §2.5, we complete the proofs of the main results by combining our parametrization, the characterization of $p$-adic orbits and distinguished orbits from §§2.3–2.4, and the asymptotics for the number of $G_n(\mathbb{Z})$-orbits on $W_n(\mathbb{Z})$ of bounded height that Siad obtained in [108, 109]. The trickiest part of this final step is sieving to orbits that satisfy 2-adic local specifications, which we achieve using *ad hoc* techniques.

## 2.2 Preliminaries on counting 2-torsion classes

Retain the setting of §1.4 (i.e., let $n$, $f_0$, $R$, $f$, and $r$ be as in §1.4). Let $r \in R^\times$, and let $(I, \alpha) \in H_{f,r}$. As noted at the start of §1.4, if $I$ is invertible (equivalently, projective as an $R_f$-module),[1] then the condition that $\mathrm{N}(I)^2 = r\,\mathrm{N}(\alpha)\,\mathrm{N}(I_f^{n-2})$ forces the containment $I^2 \subset \alpha I_f^{n-2}$ to be an equality. Let $H_{f,r}^* \subset H_{f,r}$ be the subset of equivalence classes of pairs

[1] Invertibility is in general a nontrivial condition, for a based fractional ideal $I \in H_{f,r}$ need *not* be invertible when $R_f$ is not the maximal order in $K_f$.

$(I, \alpha)$ such that $I$ is invertible. We say an orbit in $\mathsf{orb}_{f,r}(H_{f,r})$ is *pre-projective* if it belongs to the subset $\mathsf{orb}_{f,r}(H^*_{f,r})$. We list some properties of pre-projective orbits below:

- When $R = \mathbb{Z}$, a fractional ideal $I$ of $R_f$ is invertible if and only if $\mathbb{Z}_p \otimes_{\mathbb{Z}} I$ is invertible as a fractional ideal of $\mathbb{Z}_p \otimes_{\mathbb{Z}} R_f$ for every prime $p$.
- When $R = \mathbb{Z}_p$, [71, proof of Theorem 5.1] implies that the locus of pre-projective elements of $W_n(\mathbb{Z}_p)$ is defined by congruence conditions modulo a power $p^{m_p}$, where $m_p = 1$ if $p \nmid f_0$.
- If $f' = h \cdot f$ for some $h \in N(R)$, then the bijection $H_{f,r} \to H_{f',r}$ defined in Lemma 14 restricts to a bijection $H^*_{f,r} \to H^*_{f',r}$.

Let $R = \mathbb{Z}$, let $f$ be irreducible, and suppose that $R_f$ is the maximal order in the number field $K_f$. For a fractional ideal $I$ of $R_f$, we denote its ideal class by $[I] \in \mathrm{Cl}(R_f)$. The set of square roots of $[I_f^{n-2}]$ is a torsor for $\mathrm{Cl}(R_f)[2]$, and by Hecke's theorem, this torsor is nonempty. Thus, the problem of counting elements of $\mathrm{Cl}(R_f)[2]$ is equivalent to that of counting square roots of $[I_f^{n-2}]$. We now explain how to use the parametrization developed in §1 to count such square roots.

### 2.2.1 Case 1: $R = \mathbb{Z}$ and $n$ is odd

In this case, we obtain the following formula for $\#\,\mathrm{Cl}(R_f)[2]$:

**Lemma 33.** *Let $n$ be odd, and let $f \in V_{n,f_0}(\mathbb{Z})^{r_1,r_2}_{\max}$. Then we have that*

$$\#\,\mathrm{Cl}(R_f)[2] = \frac{\#\mathsf{orb}_{f,1}(H^*_{f,1})}{2^{r_1+r_2-1}}.$$

*Proof.* Since $I_f^{n-2}$ represents the class of the inverse different in $\mathrm{Cl}(R_f)$, every invertible based fractional ideal $I$ representing a square root of the class of the inverse different satisfies $I^2 = \alpha I_f^{n-2}$ for some element $\alpha \in K_f^\times$ (depending on $I$). In particular, by taking norms on both sides, we find that there exists $r \in \{\pm 1\}$ such that $\mathrm{N}(I)^2 = r\,\mathrm{N}(\alpha)\,\mathrm{N}(I_f^{n-2})$. By making

the replacement $\alpha \mapsto r\alpha$, we can ensure that $r = 1$. Thus, we obtain a surjective map of sets

$$H^*_{f,1} \twoheadrightarrow \left\{\text{square roots of } [I_f^{n-2}]\right\}, \quad (I, \alpha) \mapsto [I]. \tag{2.13}$$

Suppose $H^*_{f,1} \neq \varnothing$ (i.e., $[I_f^{n-2}]$ is a square in $\mathrm{Cl}(R_f)$). If $(I_1, \alpha_1), (I_2, \alpha_2) \in H^*_{f,1}$ map to the same class under the map (2.13), we can replace $(I_2, \alpha_2)$ with a representative of its equivalence class such that $I_1 = I_2$ as based fractional ideals. Letting $I = I_1 = I_2$, we find that

$$\alpha_1 I_f^{n-2} = I^2 = \alpha_2 I_f^{n-2} \quad \text{and} \quad \mathrm{N}(\alpha_1)\,\mathrm{N}(I_f^{n-2}) = \mathrm{N}(I)^2 = \mathrm{N}(\alpha_2)\,\mathrm{N}(I_f^{n-2}),$$

implying that $\alpha_1/\alpha_2 \in (R_f^\times)_{\mathrm{N}\equiv 1} := \{\rho \in R_f^\times : \mathrm{N}(\rho) = 1\}$. Moreover, if $(I, \alpha) \in H_{f,r}$ for any $r \in R^\times$, then $(I, \rho^2\alpha) \sim (\rho^{-1}I, \alpha) \sim (I, \alpha)$ for any $\rho \in (R_f^\times)_{\mathrm{N}\equiv 1}$. Thus, the preimage of any square root of $[I_f^{n-2}]$ under (2.13) is in bijection with $(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv 1} := \{\rho \in R_f^\times/R_f^{\times 2} : \mathrm{N}(\rho) = 1 \in \mathbb{Z}^\times/\mathbb{Z}^{\times 2}\}$, and so,

$$\#\left\{\text{square roots of } [I_f^{n-2}]\right\} = \frac{\#H^*_{f,1}}{\#(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv 1}} = \frac{\#\mathsf{orb}_{f,1}(H^*_{f,1})}{\#(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv 1}}. \tag{2.14}$$

It is not hard to compute the denominator of the right-hand side of (2.14): indeed, if $f$ has $r_1$ real roots and $r_2$ pairs of complex conjugate roots, Dirichlet's Unit Theorem tells us that we have $R_f^\times \simeq \Gamma \times \mathbb{Z}^{r_1+r_2-1}$ where $\Gamma$ is a finite abelian group, and since $-1 \in R_f^\times$, we can choose the generators of the free part of $R_f^\times$ to all have norm 1. Because $\#(\Gamma/\Gamma^2) = \#\Gamma[2] = \#\{\pm 1\} = 2$, we have that $\#(\Gamma/\Gamma^2)_{\mathrm{N}\equiv 1} = 1$, so we find that

$$\#(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv 1} = 2^{r_1+r_2-1}. \tag{2.15}$$

Combining (2.14) and (2.15) yields the lemma. □

### 2.2.2 Case 2: $R = \mathbb{Z}$ and $n$ is even

In this case, we obtain the following formula for $\#\operatorname{Cl}(R_f)[2]$:

**Lemma 34.** *Let $n$ be even, and let $f \in V_{n,f_0}(\mathbb{Z})^{r_1,r_2}_{\max}$. Then we have that*

$$\#\operatorname{Cl}(R_f)[2] = \frac{\#\mathsf{orb}_{f,1}(H^*_{f,1}) + \#\mathsf{orb}_{f,-1}(H^*_{f,-1})}{2^{r_1+r_2}}.$$

*Proof.* Just as in the proof of Lemma 33, if $I$ is an invertible based fractional ideal representing a square root of the class of the inverse different, then $I^2 = \alpha I_f^{n-2}$ for some $\alpha \in K_f^\times$, and there exists $r \in \{\pm 1\}$ such that $\mathrm{N}(I)^2 = r\,\mathrm{N}(\alpha)\,\mathrm{N}(I_f^{n-2})$. But when $n$ is even, we might *not necessarily* be able to replace $\alpha$ by a suitable multiple to reduce to the case where $r = 1$.

First suppose that there does *not* exist $\rho \in R_f^\times$ such that $\mathrm{N}(\rho) = -1$. Then the images of $H^*_{F,1}$ and of $H^*_{f,-1}$ under the map that sends a pair $(I, \alpha)$ to $[I] \in \left\{\text{square roots of } [I_f^{n-2}]\right\}$ must be disjoint: indeed, if there is a based fractional ideal $I$ of $R_f$ such that $(I, \alpha_1) \in H^*_{f,1}$ and $(I, \alpha_2) \in H^*_{f,-1}$, then $\alpha_1 I_f^{n-2} = I^2 = \alpha_2 I_f^{n-2}$, so $\alpha_1/\alpha_2 \in R_f^\times$ but $\mathrm{N}(\alpha_1/\alpha_2) = -1$, which is a contradiction. We thus obtain a surjective map of sets

$$H^*_{f,1} \sqcup H^*_{f,-1} \twoheadrightarrow \left\{\text{square roots of } [I_f^{n-2}]\right\}, \quad (I, \alpha) \mapsto [I] \tag{2.16}$$

such that each fiber of the map (2.16) is entirely contained in precisely one of $H^*_{f,1}$ or $H^*_{f,-1}$. By an argument similar to that given in the proof of Lemma 33, one checks that each of the fibers of the map (2.16) is in bijection with $(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv 1}$ and hence has size $\#(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv 1}$. Since we assumed that $R_f^\times$ has no elements of negative norm, $(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv 1} = R_f^\times/R_f^{\times 2}$, and Dirichlet's Unit Theorem implies that $\#(R_f^\times/R_f^{\times 2}) = 2^{r_1+r_2}$, where $f$ has $r_1$ real roots and $r_2$ pairs of complex conjugate roots. Thus,

$$\#\left\{\text{square roots of } [I_f^{n-2}]\right\} = \frac{\#\mathsf{orb}_{f,1}(H^*_{f,1}) + \#\mathsf{orb}_{f,-1}(H^*_{f,-1})}{2^{r_1+r_2}}. \tag{2.17}$$

Next, if there *does* exist $\rho \in R_f^\times$ such that $\mathrm{N}(\rho) = -1$, we can take $r = 1$ by replacing $\alpha$ with

$\rho\alpha$ when $\mathrm{N}(\alpha) < 0$ and keeping $\alpha$ the same when $\mathrm{N}(\alpha) > 0$. We thus obtain a surjective map of sets

$$H^*_{f,1} \twoheadrightarrow \left\{\text{square roots of } [I_f^{n-2}]\right\}, \quad (I,\alpha) \mapsto [I]. \tag{2.18}$$

One checks that each of the fibers of the map (2.18) is in bijection with $(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv 1}$ and hence has size $\#(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv 1}$. Since we assumed $R_f^\times$ has an element of negative norm, Dirichlet's Unit Theorem gives $\#(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv 1} = 2^{r_1+r_2-1}$. Thus,

$$\#\left\{\text{square roots of } [I_f^{n-2}]\right\} = \frac{\#\mathsf{orb}_{f,1}(H^*_{f,1})}{2^{r_1+r_2-1}}, \tag{2.19}$$

Now, in the above analysis, we could just as well have taken $r = -1$ by replacing $\alpha$ with $\rho\alpha$ when $\mathrm{N}(\alpha) > 0$ and keeping $\alpha$ the same when $\mathrm{N}(\alpha) < 0$. Thus,

$$\#\left\{\text{square roots of } [I_f^{n-2}]\right\} = \frac{\#\mathsf{orb}_{f,-1}(H^*_{f,-1})}{2^{r_1+r_2-1}}, \tag{2.20}$$

so by combining (2.19) and (2.20), we see that the formula (2.17) *always* holds. □

Finally, let $H^{*,+}_{f,1} \subset H^*_{f,1}$ be the subset of elements $(I,\alpha)$ such that $\alpha$ is a totally positive element of $K_f$. Then we obtain the following formula for $\#\,\mathrm{Cl}^+(R_f)[2]$:

**Lemma 35.** *Let $n$ be even, and let $F \in V_{n,f_0}(\mathbb{Z})^{r_1,r_2}_{\max}$. Then we have that*

$$\#\,\mathrm{Cl}^+(R_f)[2] = \frac{\#\mathsf{orb}_{f,1}(H^{*,+}_{f,1})}{2^{r_2}}.$$

*Proof.* Consider the surjective map of sets $H^{*,+}_{f,1} \twoheadrightarrow \mathrm{Cl}^+(R_f)[2]$ that sends a pair $(I,\alpha)$ to the narrow class of $I \cdot I_f^{\frac{2-n}{2}}$. It follows immediately from [71, proof of Lemma 2.4][2] that each of the fibers of this map has size $2^{r_2}$. □

[2]Note that, although [71, Lemma 2.4] is stated for number fields of odd degree with Galois group equal to the full symmetric group, the proof goes through for any number field.

## 2.3 Orbits over $\mathbb{Z}_p$

In this section, we take $R = \mathbb{Z}_p$ for a prime $p$, and we characterize the pre-projective orbits of $G_n(\mathbb{Z}_p)$ on $W_n(\mathbb{Z}_p)$ that arise from the parametrization. We also calculate the squareful and even ramification densities $r_p(\Sigma)$ for interesting families of local specifications $\Sigma$.

### 2.3.1 Preliminaries on binary forms over $\mathbb{Z}_p$

Let $f \in V_{n,f_0}(\mathbb{Z}_p)$ be separable and primitive, and factor $f$ over $\mathbb{Z}_p$ as $f(x,y) = \prod_{i=1}^m F_i(x,y)$ in such a way that the following three properties hold:

- The leading coefficient of $F_1$ is $f_0$, and the leading coefficient of $F_i$ is 1 for each $i \in \{2,\dots,m\}$;
- The reduction of $F_1$ modulo $p$ is given by $\kappa y^{e_1}$ for some $\kappa \in \mathbb{F}_p^\times$ and for some $e_1 \geq 0$; and
- For each $i \in \{2,\dots,m\}$, the reduction of $F_i$ modulo $p$ is $\overline{F}_i^{e_i}$ for some integers $e_i > 0$ and irreducible forms $\overline{F}_i$ over $\mathbb{F}_p$ such that $\overline{F}_1 := y, \overline{F}_2, \dots, \overline{F}_m$ are pairwise coprime.

We call any factorization of $f$ satisfying the above three properties a *canonical factorization* of $f$; Hensel's Lemma implies that there always exists a unique canonical factorization of $f$ up to permutation of $F_2,\dots,F_m$. The ring $R_f$ is evidently contained in the product ring $\prod_{i=1}^m R_{F_i}$, and comparing discriminants yields that this containment is in fact an equality.

We say that $f$ is *evenly ramified* if $e_i$ is even for each $i \in \{1,\dots,m\}$; note in particular that if $f$ is evenly ramified, then $n = \deg f$ is even. We also define a similar notion for odd-degree forms: if $n$ is odd, we say that $f$ is *squareful* if $e_i$ is even for each $i \in \{2,\dots,m\}$. Finally, let $\nu_p(f_0)$ denote the $p$-adic valuation of $f_0$; observe that $e_1 = 0$ if and only if $\nu_p(f_0) = 0$.

In what follows, we require a way to ascertain whether $R_f$ is maximal for a given binary form $f \in \mathbb{Z}_p[x,y]$. For this, we rely on the following result, known as *Dedekind's criterion*:

**Theorem 36** ([59, Theorem 2])**.** *Let $H \in \mathbb{Z}_p[x,y]$ be a primitive binary form with $H(1,0) \neq 0$. Factor $H$ over $\mathbb{F}_p$ as $\overline{H} = \prod_{i=1}^\ell \overline{H}_i^{h_i}$, where $\overline{H}_i \in \mathbb{F}_p[x,y]$ is irreducible for each $i$.*

*Let $H_1 \in \mathbb{Z}_p[x,y]$ be any (binary form) lift $\overline{H}_1 := \prod_{i=1}^{\ell} \overline{H}_i$, let $H_2 \in \mathbb{Z}_p[x,y]$ be any lift of $\overline{H}/\overline{H}_1$, and let $H_3 = p^{-1}(H_1H_2 - H) \in \mathbb{Z}_p[x,y]$. Then $R_H$ is maximal if and only if* $\gcd(\overline{H}_1, \overline{H}_2, \overline{H}_3) = 1$.

Theorem 36 implies that maximality over $\mathbb{Z}_p$ is determined by congruence conditions modulo $p^2$. The following restatement of Dedekind's criterion will prove convenient in §2.3.2:

**Lemma 37.** *Let $H \in \mathbb{Z}_p[x,y]$ be a binary form with unit leading coefficient. The ring $R_H$ is maximal if and only if there does not exist a monic form $H' \in \mathbb{Z}_p[x,y]$ such that its reduction $\overline{H}' \in \mathbb{F}_p[x,y]$ is irreducible and such that $H \in (p^2, pH', H'^2) \subset \mathbb{Z}_p[x,y]$.*

*Proof.* The lemma follows from Theorem 36 in the same way that [4, Corollary 3.2] follows from [4, Lemma 3.1], which is Dedekind's criterion for monic single-variable polynomials. □

When $\nu_p(f_0) > 0$, Dedekind's criterion yields the following result, which restricts the possible values of the pair $(\nu_p(f_0), e_1)$ in a canonical factorization of $f$ when $R_f$ is maximal:

**Lemma 38.** *If $\nu_p(f_0) > 0$, then $R_{F_1}$ is maximal if and only if* $\min\{\nu_p(f_0), e_1\} = 1$.

*Proof.* When $e_1 = 1$, $R_{F_1}$ is maximal, so suppose $e_1 > 1$. Let $H = F_1$, $H_1 = y$, and $H_2 = y^{e_1-1}$. Then the leading coefficient of $H_3 = p^{-1}(H_1H_2 - H)$ is divisible by $p^{\nu_p(f_0)-1}$, and so $\gcd(\overline{H}_1, \overline{H}_2, \overline{H}_3) = 1$ if and only if $\nu_p(f_0) = 1$; the lemma then follows from Theorem 36. □

### 2.3.2 Pre-projective orbits

We now describe the pre-projective orbits of $G_n(\mathbb{Z}_p)$ on $W_n(\mathbb{Z}_p)$ arising from the parametrization. In particular, we obtain formulas for $\#\mathsf{orb}_{f,r}(H^*_{f,r})$ that depend on the parity of $p$, whether $f$ is evenly ramified, and whether $r$ is a quadratic residue modulo $p$.

**Theorem 39.** *Let $f$ be as in §2.3.1, and let $r \in \mathbb{Z}_p^\times$. The elements of $\mathsf{orb}_{f,r}(H^*_{f,r})$ are in bijection with those of $(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv r} := \{\rho \in R_f^\times/R_f^{\times 2} : \mathrm{N}(\rho) = r \in \mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2}\}$, and we have*

*the following formulas:*

$$\#\mathsf{orb}_{f,r}(H^*_{f,r}) = \#(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv r} = \tag{2.21}$$
$$\begin{cases} \frac{1}{2}\#R_f^\times[2], & \text{if } p>2 \text{ and } f \text{ is not evenly ramified,} \\ \#R_f^\times[2], & \text{if } p>2,\ f \text{ is evenly ramified, and } r=1\in\mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2}, \\ 0, & \text{if } p>2,\ f \text{ is evenly ramified, and } r\neq 1\in\mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2}, \\ 2^{n-2}\#R_f^\times[2], & \text{if } p=2,\ R_f \text{ is maximal, and } f \text{ is not evenly ramified.} \end{cases}$$

*The stabilizer* $\mathrm{Stab}_{G_n(\mathbb{Z}_p)}(A,B)$ *in* $G_n(\mathbb{Z}_p)$ *of any representative* $(A,B)\in W_n(\mathbb{Z}_p)$ *of any element of* $\mathsf{orb}_{f,r}(H^*_{f,r})$ *is isomorphic to* $R_f^\times[2]_{\mathrm{N}\equiv 1}$ *if* $n$ *is odd and to* $R_f^\times[2]$ *if* $n$ *is even.*

*Remark* 40. If $f$ is evenly ramified, then taking $r=-1\in\mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2}$ in (2.21) yields that $\#\mathsf{orb}_{f,-1}(H^*_{f,-1}) = \#R_f^\times[2]$ if $p\equiv 1 \pmod 4$ and that $\#\mathsf{orb}_{f,-1}(H^*_{f,-1})=0$ if $p\equiv 3 \pmod 4$. Let $m$ be the number of irreducible factors of $f$ over $\mathbb{Z}_p$. When $R_f$ is maximal, the quantities on the right-hand side of (2.21) are $2^{m-1}$, $2^m$, 0, $2^{m+n-2}$, respectively, and the stabilizer size is $2^{m-1}$ for $n$ odd and $2^m$ for $n$ even.

*Proof of Theorem 39.* Since $R_f$ is a module-finite extension of the complete local ring $\mathbb{Z}_p$, it is a finite product of complete local rings (see [72]), implying that every invertible fractional ideal of $R_f$ is principal. Since we took $f$ to be primitive, the based fractional ideal $I_f$ is invertible, and so there exists $\gamma'\in K_f^\times$ such that $I_f=(\gamma')$ as ideals (*not necessarily* as based ideals). *A priori*, all we know is that $\mathrm{N}(\gamma') = r'\,\mathrm{N}(I_f)$ for some $r'\in\mathbb{Z}_p^\times$, since the norm of an ideal depends on the choice of basis. Letting $\gamma=r'\gamma'$, we find that $I_f=(\gamma)$ and that $\mathrm{N}(\gamma^{n-2}) = r'^{(n+1)(n-2)}\,\mathrm{N}(I_f^{n-2})$.

To prove the desired bijection, it suffices by Proposition 9 to show that the elements of $H^*_{f,r}$ are in bijection with those of $(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv r}$. We do this by constructing mutually inverse maps in both directions. For the forward direction, let $(I,\alpha)\in H^*_{f,r}$. By the observation above, $I=(\beta)$ as ideals and $\mathrm{N}(I) = r''\,\mathrm{N}(\beta)$ for some $\beta\in K_f$ and $r''\in\mathbb{Z}_p^\times$. Then

$(I,\alpha) \sim ((1),\beta^{-2}\alpha)$, where the unit ideal $(1)$ has the basis given by scaling each basis element of $I$ by $\beta^{-1}$. It follows that $(1)^2 = \beta^{-2}\alpha(\gamma)^{n-2}$, so $\rho := \beta^{-2}\alpha\gamma^{n-2} \in R_f^\times$. But we also have

$$r''^2 = \mathrm{N}((1))^2 = r\,\mathrm{N}(\beta^{-2}\alpha)\,\mathrm{N}(I_f^{n-2}) = rr'^{-(n+1)(n-2)}\,\mathrm{N}(\rho). \tag{2.22}$$

It follows from (2.22) that $\mathrm{N}(\rho) = r \in \mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2}$. Since $\beta$ is only unique up to scaling by elements of $R_f^\times$, the assignment $(I,\alpha) \mapsto \rho$ yields a map of sets $\Sigma_1 \colon H_{f,r}^* \to (R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv r}$.

For the reverse direction, let $\rho \in R_f^\times$ be a representative of an element of $(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv r}$. Then $\alpha := \rho\gamma^{2-n}$ satisfies $(1)^2 = \alpha I_f^{n-2}$ as ideals and $\mathrm{N}(\alpha) = \mathrm{N}(\rho)\,\mathrm{N}(\gamma^{2-n}) = r\widetilde{r}^2\,\mathrm{N}(I_f^{n-2})^{-1}$ for some $\widetilde{r} \in \mathbb{Z}_p^\times$. Upon endowing the unit ideal $(1)$ with any basis such that $\mathrm{N}((1)) = \widetilde{r}$, we find that $((1),\alpha) \in H_{f,r}^*$. If we had chosen a different representative $\rho' \in R_f^\times$ of the same element of $(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv r}$, then the resulting pair $((1),\alpha')$ would be equivalent to the scaling of the pair $((1),\alpha)$ by the factor $\rho'/\rho$. Thus, the assignment $\rho \mapsto ((1),\alpha)$ gives a well-defined map of sets $\Sigma_2 \colon (R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv r} \to H_{f,r}^*$. (In particular, note that $H_{f,r}^*$ is nonempty when $(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv r}$ is.) One checks that the maps $\Sigma_1$ and $\Sigma_2$ are mutually inverse.

We now compute $\#(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv r}$. Recall that the unit group $R_f^\times$ can be expressed as $R_f^\times \simeq \Gamma_p \times \mathbb{Z}_p^n$, where $\Gamma_p$ is a finite abelian group. Upon observing that $\#(\Gamma_p/\Gamma_p^2) = \#\Gamma_p[2]$ and that $\Gamma_p[2] = R_f^\times[2]$, we find that

$$\#(R_f^\times/R_f^{\times 2}) = \#(\Gamma_p/\Gamma_p^2)\cdot\big(\#(\mathbb{Z}_p/2\mathbb{Z}_p)\big)^n = \begin{cases} \#R_f^\times[2], & \text{if } p > 2, \\ 2^n\#R_f^\times[2], & \text{if } p = 2. \end{cases} \tag{2.23}$$

To determine $\#(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv r}$ from the value of $\#(R_f^\times/R_f^{\times 2})$ given in (2.23), consider the norm map

$$R_f^\times/R_f^{\times 2} \to \mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2}, \quad \rho \mapsto \mathrm{N}(\rho). \tag{2.24}$$

It follows from (2.23) and the fact that the map (2.24) is a group homomorphism that

$$\#(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv r} = \tag{2.25}$$
$$\begin{cases} \frac{1}{2}\#R_f^\times[2], & \text{if } p>2 \text{ and (2.24) is surjective,} \\ \#R_f^\times[2], & \text{if } p>2, \text{ (2.24) is not surjective, and } r=1\in\mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2}, \\ 0, & \text{if } p>2, \text{ (2.24) is not surjective, and } r\neq 1\in\mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2}, \\ 2^{n-2}\#R_f^\times[2], & \text{if } p=2 \text{ and (2.24) is surjective.} \end{cases}$$

The formulas (2.21) then follow immediately from (2.25) and the next lemma:

**Lemma 41.** *If $p>2$, then (2.24) is surjective if and only if $f$ is not evenly ramified. If $p=2$, then (2.24) is surjective if $R_f$ is maximal and $f$ is not evenly ramified.*

*Proof of Lemma 41.* Suppose $p>2$. We claim that if the lemma holds for $f$, then it also holds for any separable degree-$n$ form $f'\in\mathbb{Z}_p[x,y]$ such that $f'\equiv f \pmod p$. To see why, let $m_\kappa$ be the matrix of multiplication by $\kappa\in K_f^\times$ on the $K$-vector space $K_f$ with respect to the basis (1.1). If we express $\kappa$ in the basis (1.1) as $\kappa=\sum_{i=1}^n \kappa_i\zeta_i$, then using the multiplication table (1.2), one verifies that each matrix entry of $m_\kappa$—and hence also the norm $\mathrm{N}(\kappa)=\det m_\kappa$—is a polynomial function in the $\kappa_i$ and $f_i$ with integer coefficients. Now, (2.24) is surjective if and only if the norm, viewed as a polynomial function in the $\kappa_i$ and $f_i$, represents a quadratic nonresidue modulo $p$, and if this happens for $f$, then it must also happen for the mod-$p$ translate $f'$.

We next claim that we can choose $f'\equiv f \pmod p$ such that $R_{f'}$ is maximal. It suffices to prove this with $f$ replaced by $F_i$ for each $i$. If $e_i=1$ for any $i$, then $R_{F_i}$ must be maximal, so suppose $e_i>1$. Let $\widehat{F}_i\in\mathbb{Z}_p[x,y]$ be any lift of $\overline{F}_i$ with $\deg\widehat{F}_i=\deg\overline{F}_i$. Then $F_i':=\widehat{F}_i^{e_i}+py^{\deg F_i}\in\mathbb{Z}_p[x,y]$ does the job when $i>2$: indeed, taking $H=F_i'$, $H_1=\widehat{F}_i$, and $H_2=\widehat{F}_i^{e_i-1}$ in Dedekind's criterion, we see that $H_3=y^{\deg F_i}$, meaning that $\gcd(\overline{H}_1,\overline{H}_2,\overline{H}_3)=1$. Similarly, $F_1':=\widehat{F}_1^{e_1}+px^{e_1}$ does the job when $i=1$. We may thus

assume $R_f$ is maximal.

We now claim that $F_i$ is irreducible for each $i$. Indeed, suppose $F_i$ is not irreducible for some $i$, and let $\widehat{F}_i \in \mathbb{Z}_p[x,y]$ be any lift of $\overline{F}_i$. Then $F_i = (\widehat{F}_i^a + pJ_1)(\widehat{F}_i^b + pJ_2)$ for some forms $J_1, J_2 \in \mathbb{Z}_p[x,y]$ and integers $a, b > 0$ such that $a + b = e_i$. It follows that $F_i \in (p^2, p\widehat{F}_i, \widehat{F}_i^2) \subset \mathbb{Z}_p[x,y]$, so $F_i$ fails Dedekind's criterion as stated in Lemma 37, with $x$ and $y$ switched. Thus, $R_{F_i}$ is not maximal.

As the $F_i$ are irreducible, $K_{F_i}$ is a field extension of $\mathbb{Q}_p$ with ramification degree $e_i$ for each $i$, and the mod-$p$ reduction of the image of the norm map $\mathrm{N}_{R_{F_i}/\mathbb{Z}_p} \colon R_{F_i}^\times \to \mathbb{Z}_p^\times$ is equal to $(\mathbb{Z}/p\mathbb{Z})^{\times e_i}$ for each $i$. Thus, (2.24) is surjective if and only if $e_i$ is odd for some $i$, which occurs if and only if $f$ is not evenly ramified. When $p = 2$, we have $\mathbb{Z}_2^{\times e_i} \subset \mathrm{N}_{R_{F_i}/\mathbb{Z}_2}(R_{F_i}^\times)$, so (2.24) is surjective if $e_i$ is odd for some $i$. This completes the proof of Lemma 41. □

Finally, the characterization of the stabilizer follows from Proposition 11 upon observing that $\mathrm{End}_{R_f}(I)^\times[2] = R_f^\times[2]$ when $I$ is invertible. This completes the proof of Theorem 39. □

### 2.3.3 Density calculations

As is evident from (2.21), the size $\#\mathsf{orb}_{f,r}(H_{f,r}^*)$ depends on whether $f$ is evenly ramified, which can only occur when $n$ is even. The following theorem tells us how often forms in $V_{n,f_0}(\mathbb{Z}_p)_{\max}$ are evenly ramified:

**Theorem 42.** *Let $n$ be even. The $p$-adic density of forms $F \in V_{n,f_0}(\mathbb{Z}_p)_{\max}$ such that $f$ is evenly ramified is given by*

$$\begin{cases} p^{-\frac{n}{2}}(1+p^{-1})^{-1}, & \text{if } \nu_p(f_0) \in \{0,1\}, \\ 0, & \text{if } \nu_p(f_0) > 1. \end{cases} \tag{2.26}$$

*Proof.* Let $S := V_{n,f_0}(\mathbb{Z}_p)_{\max}$, and let $S' \subset V_{n,f_0}(\mathbb{Z}_p)$ be the subset of evenly ramified forms. For a set $\Sigma \subset V_{n,f_0}(\mathbb{Z}_p)$, let $\delta_\Sigma$ denote the $p$-adic density of $\Sigma$ in $V_{n,f_0}(\mathbb{Z}_p)$. Observe that to prove (2.26), it suffices to compute $\delta_{S'}/\delta_S$. We compute the densities $\delta_S$ and $\delta_{S'}$ as follows:

**Computation of $\delta_S$**

First suppose $\nu_p(f_0) = 0$. Then $\delta_S$ is equal to the $p$-adic density of monic polynomials $f \in \mathbb{Z}_p[x]$ of degree $n$ such that the ring $\mathbb{Z}_p[x]/(f)$ is maximal. This latter density can be computed for any degree $n$ (not just even $n$) using Dedekind's criterion (see [4, Proposition 3.5]) and is given by 1 when $n \leq 1$ and by $1 - p^{-2}$ when $n \geq 2$.

Next, if $\nu_p(f_0) > 0$, then $\min\{e_1, \nu_p(f_0)\} = 1$ by Lemma 38, so suppose $\nu_p(f_0) = 1$. In this case, the exponent $e_1$ can be any number from 1 up to $n$, and the coefficient $\kappa$ of $y^{e_1}$ in the reduction of $F_1$ modulo $p$ can be any element of $\mathbb{F}_p^\times$. Summing the $p$-adic density of forms $F \in V_{n-e_1,1}(\mathbb{Z}_p)_{\max}$ over the possible values of $e_1$, $\kappa$, we find that

$$\delta_S = \sum_{\kappa \in \mathbb{F}_p^\times} \left( p^{-n} + p^{1-n} + \sum_{\ell=1}^{n-2} p^{-\ell}(1 - p^{-2}) \right) = 1 - p^{-2}, \tag{2.27}$$

where in the sum over $\kappa$ on the right-hand side of (2.27), the first term corresponds to forms $f$ such that $e_1 = n$, the second term corresponds to forms $f$ such that $e_1 = n-1$, and the $\ell^{\text{th}}$ term in the inner sum corresponds to forms $f$ such that $e_1 = \ell$ for each $\ell \in \{1, \ldots, n-2\}$.

Finally, suppose that $\nu_p(f_0) > 1$. Then $e_1 = 1$, so $R_{F_1}$ is automatically maximal, and $R_f$ is maximal if and only if $R_{f/F_1}$ is maximal, which occurs with probability 1 when $n = 2$ and with probability $1 - p^{-2}$ when $n > 2$. Thus, upon summing over the possible values of $\kappa$, we find that

$$\delta_S = \begin{cases} \sum_{\kappa \in \mathbb{F}_p^\times} p^{-1} = 1 - p^{-1}, & \text{if } n = 2, \\ \sum_{\kappa \in \mathbb{F}_p^\times} p^{-1}(1 - p^{-2}) = (1 - p^{-1})(1 - p^{-2}), & \text{if } n > 2. \end{cases}$$

**Computation of $\delta_{S'}$**

For any integer $m \geq 1$, let $\delta_{2m}$ denote the $p$-adic density in $V_{2m,1}(\mathbb{Z}_p)_{\max}$ of forms $H$ such that $H$ is a perfect square modulo $p$.

If $\nu_p(f_0) = 0$, then $e_1 = 0$, so in this case

$$\delta_{S'} = \delta_n. \tag{2.28}$$

Next, suppose that $f \in S_1$ and $\nu_p(f_0) > 0$. Then we once again have by Lemma 38 that $\min\{e_1, \nu_p(f_0)\} = 1$, so suppose that $\nu_p(f_0) = 1$. In this case, the exponent $e_1$ can be any even number from 2 up to $n$, and the coefficient $\kappa$ of $y^{e_1}$ in the reduction of $F_1$ modulo $p$ can be any element of $\mathbb{F}_p^\times$. Summing the $p$-adic density $\delta_{2n+1-\ell}$ of forms $f \in V_{n-e_1,1}(\mathbb{Z}_p)_{\max}$ such that $f$ is a square modulo $p$ over the possible values of $e_1$, $\kappa$, we find that

$$\delta_{S'} = \sum_{\kappa \in \mathbb{F}_p^\times} \sum_{\substack{2 \le e_1 \le n \\ e_1 \equiv 0 \bmod 2}} p^{-e_1} \delta_{n-e_1}. \tag{2.29}$$

Finally, if $\nu_p(f_0) > 1$, then $e_1 = 1$, so $f$ cannot be evenly ramified. Thus, $\delta_{S'} = 0$ in this case.

It now remains to compute the $p$-adic densities $\delta_{2m}$, which we do in the following proposition. Our method of proof follows Lenstra's computation (see [4, §3]) of the $p$-adic density of monic polynomials $f \in \mathbb{Z}_p[x]$ such that $\mathbb{Z}_p[x]/(f)$ is the maximal order in $\mathbb{Q}_p[x]/(f)$.

**Proposition 43.** *We have that $\delta_0 = 1$ and $\delta_{2m} = p^{-m}(1 - p^{-1})$ for $m \ge 1$.*

*Proof of Proposition 43.* The case $m = 0$ is obvious, so fix $m \ge 1$. Because the criterion for maximality stated in Lemma 37 depends only on the residue class of $H$ in $\mathcal{P} := (\mathbb{Z}/p^2\mathbb{Z})[x, y]$, it suffices to work modulo $p^2$, where the ideal $(p^2, pH', H'^2) \subset \mathbb{Z}_p[x, y]$ reduces to the ideal $(pH', H'^2) \subset (\mathbb{Z}/p^2\mathbb{Z})[x, y]$. To apply Lemma 37, we need to introduce some notation. For each $i \in \{0, \dots, 2m\}$ and any $H' \in \mathcal{P}$:

- Let $\mathcal{P}_i \subset \mathcal{P}$ be the subset of binary forms on $\mathcal{P}$ having degree at most $i$, and let $\overline{\mathcal{P}}_i$ be the reduction of $\mathcal{P}_i$ modulo $p$;
- Let $\mathcal{P}_{i,\mathsf{mon}} \subset \mathcal{P}_i$ be the subset of monic binary forms having degree equal to $i$, and let $\overline{\mathcal{P}}_{i,\mathsf{mon}}$ be the reduction of $\mathcal{P}_{i,\mathsf{mon}}$ modulo $p$;

- Let $\mathcal{P}^{(2)}_{i,\mathsf{mon}} \subset \mathcal{P}_{i,\mathsf{mon}}$ be the subset of forms whose reductions modulo $p$ are perfect squares ($\mathcal{P}^{(2)}_{i,\mathsf{mon}} \neq \varnothing$ if and only if $i$ is even), and let $\overline{\mathcal{P}}^{(2)}_{i,\mathsf{mon}}$ be the reduction of $\mathcal{P}^{(2)}_{i,\mathsf{mon}}$ modulo $p$;
- Let $J_{H'} = (pH', H'^2) \cap \mathcal{P}^{(2)}_{2m,\mathsf{mon}} \subset \mathcal{P}$.

**Lemma 44.** *Let $H'_1, \dots, H'_\ell \in \mathcal{P}$ be such that their reductions modulo $p$ are irreducible and distinct, and let $H' = \prod_{i=1}^{\ell} H'_i$. Then we have that*

$$\frac{\#\left(\bigcap_{i=1}^{\ell} J_{H'_i}\right)}{\#\mathcal{P}_{2m,\mathsf{mon}}} = \begin{cases} 0, & \text{if } \deg H' > m, \\ p^{-m-2\deg H'}, & \text{otherwise.} \end{cases}$$

*Proof of Lemma 44.* It is clear that $\#\mathcal{P}_{2m,\mathsf{mon}} = p^{4m}$. One checks by following the proof of [4, Lemma 3.3] that $\bigcap_{i=1}^{\ell} J_{H'_i} = J_{H'}$, so it remains to compute $\#J_{H'}$. By definition, $J_{H'}$ contains no monic elements and is thus empty when $\deg H'^2 = 2\deg H' > 2m$, so $\#J_{H'} = 0$ when $\deg H' > m$.

Now suppose that $\deg H' \leq m$. Consider the map of sets

$$\overline{\mathcal{P}}^{(2)}_{2m-2\deg H',\mathsf{mon}} \times \overline{\mathcal{P}}_{2m-\deg H'-1} \to J_{H'} \tag{2.30}$$

defined in the following manner: for each pair $(\overline{H}'', \overline{H}''') \in \overline{\mathcal{P}}^{(2)}_{2m-2\deg H',\mathsf{mon}} \times \overline{\mathcal{P}}_{2m-\deg H'-1}$, choose a lift $(H'', H''') \in \mathcal{P}^{(2)}_{2m-2\deg H',\mathsf{mon}} \times \mathcal{P}_{2m-\deg H'-1}$, and let the image of $(\overline{H}'', \overline{H}''')$ be given by $H''H'^2 + pH'''H'$. By imitating [4, proof of Proposition 3.4], one checks that the map in (2.30) is a bijection, so we have that

$$\#J_{H'} = \left(\#\overline{\mathcal{P}}^{(2)}_{2m-2\deg H',\mathsf{mon}}\right)\left(\#\overline{\mathcal{P}}_{2m-\deg H'-1}\right) = p^{m-\deg H'} p^{2m-\deg H'}. \quad \square$$

By the Principle of Inclusion-Exclusion, we deduce from Lemma 44 that

$$\delta_{2m} = p^{-m} \sum_{\ell \geq 0} \sum_{\{\overline{H}'_1, \dots, \overline{H}'_\ell\}} (-1)^\ell p^{-2\sum_{i=1}^{\ell} \deg \overline{H}'_i}, \tag{2.31}$$

where the inner sum in (2.31) is taken over sets $\{\overline{H}'_1, \dots, \overline{H}'_\ell\} \subset (\mathbb{Z}/p\mathbb{Z})[x,y]$ of monic irreducible binary forms such that $2\sum_{i=1}^{\ell} \deg \overline{H}'_i \leq 2m$. A computation reveals that the double sum in (2.31) is none other than the coefficient of $t^{2m}$ in the power series expansion of the generating function

$$K(t) = (1-t)^{-1} \prod_{\overline{H}'} \left(1 - \frac{t^{2\deg H'}}{p^{-2\deg H'}}\right).$$

Let $\zeta_{\mathbb{A}^1_{\mathbb{F}_p}}(s)$ be the $\zeta$-function of the variety $\mathbb{A}^1_{\mathbb{F}_p} = \operatorname{Spec} \mathbb{F}_p[x]$, and recall that $\zeta_{\mathbb{A}^1_{\mathbb{F}_p}}(s) = (1-ps)^{-1}$. Expanding $\zeta_{\mathbb{A}^1_{\mathbb{F}_p}}(s)$ into its Euler product reveals that

$$K(t) = (1-t)^{-1}\zeta_{\mathbb{A}^1_{\mathbb{F}_p}}(p^{-2}t^2)^{-1} = (1-t)^{-1}(1-p^{-1}t^2). \tag{2.32}$$

Since the coefficient of $t^{2m}$ on the right-hand side of (2.32) is equal to $1-p^{-1}$, it follows from (2.31) that $\delta_{2m} = p^{-m}(1-p^{-1})$, as desired. □

Substituting the result of Proposition 43 into (2.28) and (2.29) yields that $\delta'_S = p^{-\frac{n}{2}}(1-p^{-1})$ when $\nu_p(f_0) \in \{0,1\}$. This completes the proof of Theorem 42. □

## 2.4 Distinguishedness and reducibility

Let $R = \mathbb{Z}$, and let $f \in V_{n,f_0}(\mathbb{Z})_{\max}$. In §2.2, we reduced the problem of counting 2-torsion classes of $R_f$ to that of computing $\#\mathsf{orb}_{f,\pm 1}(H^*_{f,\pm 1})$. This amounts to determining asymptotics for the number of lattice points of bounded height in a fundamental set for the action of $G_n(\mathbb{Z})$ on $W_n(\mathbb{R})$ lying on the hypersurface of pairs $(A,B)$ where $\det A = \pm 1$. In [108,109], Siad uses the linearization trick explained in §1.3.2 together with geometry-of-numbers methods to obtain such asymptotics, albeit for the number of non-distinguished orbits of bounded height. In this section, we use algebraic arguments to describe the frequency with which integral orbits arising via the maps $\mathsf{orb}_{f,\pm 1}$ are distinguished.

### 2.4.1 Uniqueness of integral representatives

Let $r \in \{\pm 1\}$. To study distinguished $G_n(\mathbb{Q})$-orbits arising from elements of $H^*_{f,r}$ via the construction in §1.4.1, it suffices to consider the case where $r = 1$. Indeed, when $n$ is odd, the map $(I, \alpha) \mapsto (I, -\alpha)$ defines a bijection between $H^*_{f,1}$ and $H^*_{f,-1}$, and when $n$ is even, any $(I, \alpha) \in H^*_{f,-1}$ satisfies the property that $\mathrm{N}(\alpha) = -1 \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, so by Proposition 19, the $G_n(\mathbb{Q})$-orbit containing $\mathsf{orb}_{f,-1}(I, \alpha)$ cannot possibly correspond to $1 \in K_f^\times/K_f^{\times 2}\mathbb{Q}^\times$.

The following proposition tells us how many elements of $H^*_{f,1}$ give rise to the distinguished $G_n(\mathbb{Q})$-orbit, if such elements exist at all:

**Proposition 45.** *We have the following two points:*

- *Let $n$ be odd. If there exists an element $(I, \alpha) \in H^*_{f,1}$ such that the $G_n(\mathbb{Q})$-orbit containing $\mathsf{orb}_{f,1}(I, \alpha)$ is distinguished, there is precisely one such element.*
- *Let $n$ be even, and let $\mathsf{ev}_f := \{\text{primes } p : f \text{ is evenly ramified modulo } p\}$. If there exists an element $(I, \alpha) \in H^*_{f,1}$ such that the $G_n(\mathbb{Q})$-orbit containing $\mathsf{orb}_{f,1}(I, \alpha)$ is distinguished, there are at most $2^{\#\mathsf{ev}_f+1}$ such elements, with equality if $K_f$ has no quadratic subfields.*

*Proof.* Let $n$ be odd, and suppose there exist two distinct fractional ideals $I$ and $I'$ of $R_f$ such that both $(I, 1)$ and $(I', 1)$ are elements of $H^*_{f,1}$. Then, since $R_f$ is maximal, we have $I^2 = I_f^{n-2} = I'^2$, implying that $I = I'$.

Next, let $n$ be even. Observe that we have the equality

$$\ker\left(K_f^\times/K_f^{\times 2} \to K_f^\times/K_f^{\times 2}\mathbb{Q}^\times\right) = \mathbb{Q}^\times/(\mathbb{Q}^\times \cap K_f^{\times 2}), \tag{2.33}$$

From (2.33), we see that if $(I, \alpha) \in H^*_{f,1}$ gives rise to the distinguished $G_n(\mathbb{Q})$-orbit, we can rescale $(I, \alpha)$ so that $|\alpha| \in \mathbb{Q}^\times$ is a product of distinct primes. But then $(\alpha) = \left(I I_f^{\frac{2-n}{2}}\right)^2$, so each prime dividing $\alpha$ must lie in the set $\mathsf{ev}_f$. The number of possibilities for $\alpha$ modulo $\mathbb{Q}^\times \cap K_f^{\times 2}$ is at most $2^{\#\mathsf{ev}_f+1}$, with equality if $K_f$ has no quadratic subfields. □

*Remark* 46. The condition that $K_f$ has no quadratic subfields in the second point of Proposition 45 is a mild one: indeed, this conditions holds for 100% of forms $f \in V_{n,f_0}(\mathbb{Z})_{\max}$, since such forms have Galois group isomorphic to the full symmetric group 100% of the time.

### 2.4.2 Existence of integral representatives, part $(i)$

Let $f \in V_{n,f_0}(\mathbb{Z})$ be primitive. It now remains to determine precise conditions under which distinguished integral orbits arise via the map $\mathsf{orb}_{f,1}$. When $n$ is even, there *always* exists a pair $(I,\alpha) \in H^*_{f,1}$ such that the $G_n(\mathbb{Q})$-orbit containing $\mathsf{orb}_{f,1}(I,\alpha)$ is distinguished: indeed, take $I = I_f^{\frac{n-2}{2}}$ and $\alpha = 1$. On the other hand, when $n$ is odd, it is *often not* the case that there exists a pair $(I,\alpha) \in H^*_{f,1}$ such that the $G_n(\mathbb{Q})$-orbit containing $\mathsf{orb}(I,\alpha)$ is distinguished. The rest of this section is devoted to proving this assertion for odd $n$.

The $G_n(\mathbb{Q})$-orbit containing $\mathsf{orb}_{f,1}(I,\alpha)$ is distinguished if and only if the $G_n(\mathbb{Q}_v)$-orbit containing $\mathsf{orb}_{f,1}(I,\alpha)$ is distinguished for every place $v$ of $\mathbb{Q}$. In particular, if there exists a pair $(I,\alpha) \in H^*_{f,1}$ such that $\mathsf{orb}_{f,1}(I,\alpha)$ is distinguished over $\mathbb{Q}$, then for every place $v$, there exists a pair $(I_v,\alpha_v) \in H^*_{f,1}$ over $\mathbb{Z}_v$ such that $\mathsf{orb}_{f,1}(I_v,\alpha_v)$ is distinguished over $\mathbb{Q}_v$ (here, $\mathbb{Z}_v = \mathbb{R}$ when $v = \infty$). The following proposition establishes the converse:

**Proposition 47.** *Suppose that for each place $v$ of $\mathbb{Q}$, there exists an invertible based fractional ideal $I_v$ of $R_f \otimes_{\mathbb{Z}} \mathbb{Z}_v$ such that $(I_v, f_0^{n-2}) \in H^*_{f,1}$ over $\mathbb{Z}_v$. Then there exists an invertible based fractional ideal $I$ of $R_f$ such that $(I, f_0^{n-2}) \in H^*_{F,1}$ over $\mathbb{Z}$.*

*Proof.* Let $\mathbb{A}_{\mathbb{Q}}$ be the ring of adèles, and let $\mathbb{A}_{\mathbb{Z}} \subset \mathbb{A}_{\mathbb{Q}}$ be the subring of integral adèles. Recall that $G_n$ has class number 1; i.e., for every $g \in G_n(\mathbb{A}_{\mathbb{Q}})$, there exists $g' \in G_n(\mathbb{A}_{\mathbb{Z}})$ and $g'' \in G_n(\mathbb{Q})$ such that $g = g'g''$, where we view $G_n(\mathbb{Q})$ as the subring of principal adèles of $G_n(\mathbb{A}_{\mathbb{Q}})$.

Let $(A,B) \in W_n(\mathbb{Q})$ be an arbitrary fixed representative of the distinguished orbit of $G_n$ over $\mathbb{Q}$. Notice that the base-change of $(A,B)$ from $\mathbb{Q}$ to $\mathbb{Q}_v$ lies in $W_n(\mathbb{Z}_v)$ for all but finitely many places $v$. The assumption that there exists an invertible based fractional ideal $I_v$ of $R_f \otimes_{\mathbb{Z}} \mathbb{Z}_v$ such that $(I_v, f_0^{n-2}) \in H^*_{f,1}$ over $\mathbb{Z}_v$ implies that the distinguished orbit has a

pre-projective representative over $\mathbb{Z}_p$ arising from the construction in §1.4.1 for every place $v$. Thus, there exists $g_v \in G_n(\mathbb{Q}_v)$ for each $v$ such that the following two conditions hold: (1) $g_v \in G(\mathbb{Z}_v)$ for all but finitely many $v$; and (2) $g_v \cdot (A, B) \in \mathsf{orb}_{f,1}(I_v, f_0^{n-2})$. It follows that the list $g = (g_v)_v$ is an element of $G_n(\mathbb{A}_\mathbb{Q})$. By the observation in the previous paragraph, there exist $g' \in G_n(\mathbb{A}_\mathbb{Z})$ and $g'' \in G_n(\mathbb{Q})$ such that $g = g'g''$. Combining our results, we find that

$$g \cdot (A, B) \in W_n(\mathbb{A}_\mathbb{Z}) \Longrightarrow g'' \cdot (A, B) \in W_n(\mathbb{A}_\mathbb{Z}).$$

As $g'' \in G_n(\mathbb{Q}) \subset G_n(\mathbb{A}_\mathbb{Q})$ and $(A, B) \in W_n(\mathbb{Z}) \subset W_n(\mathbb{A}_\mathbb{Q})$, we deduce that $g'' \cdot (A, B) \in W_n(\mathbb{Z})$. We must now show that there exists an invertible based fractional ideal $I$ of $R_f$ such that $g'' \cdot (A, B) \in \mathsf{orb}_{f,1}(I, f_0^{n-2})$. By Theorem 10, the $G_n(\mathbb{Z})$-orbit of $g'' \cdot (A, B)$ is an element of $\mathsf{orb}_{f,1}(H_{f,1}^*)$ if and only if $g'' \cdot (A, B)$ satisfies the congruence conditions in (1.15) as well as the congruence conditions that define pre-projectivity (see §2.2), but this follows because we have that $g_v \cdot (A, B) \in \mathsf{orb}_{f,1}(I_v, f_0^{n-2})$ and that $(I_v, f_0^{n-2}) \in H_{f,1}^*$ for every place $v$. □

Proposition 47 reduces the problem of ascertaining when the distinguished orbit arises globally to the problem of determining the conditions under which the distinguished orbit arises everywhere locally. In the rest of this section, we derive these local conditions.

When $R = K$ is a field and $f \in V_{n,f_0}(K)$ is separable, Proposition 19 implies that there exists $(A, B) \in W_n(K)$ with $\iota(A, B) = f^{\mathsf{mon}}$ and with distinguished $G_n(K)$-orbit; moreover, by Theorem 10, there exists $(I, \alpha) \in H_{f,1} = H_{f,1}^*$ such that $(A, B)$ represents the orbit $\mathsf{orb}_{f,1}(I, \alpha)$. In particular, when $v = \infty$, so that $R = K = \mathbb{R}$, the distinguished orbit always arises.

Next, let $v = p$ be prime, and let $R = \mathbb{Z}_p$. Let $n$ be odd, and let $f \in V_{n,f_0}(\mathbb{Z})$ be primitive. We split our analysis of $p$-adic distinguished orbits into cases based on the parity of $\nu_p(f_0)$:

### 2.4.3 Existence, part $(ii)$: $n$, $\nu_p(f_0)$ are odd

In this case, the next theorem tells us when the distinguished $G_n(\mathbb{Q}_p)$-orbit contains an element of $\mathsf{orb}_{f,1}(H^*_{f,1})$, assuming $R_f$ is maximal:

**Proposition 48.** *Let $\nu_p(f_0)$ be odd, and let $f \in V_{n,f_0}(\mathbb{Z}_p)_{\max}$. There exists $(I,\alpha) \in H^*_{f,1}$ such that the $G_n(\mathbb{Q}_p)$-orbit containing $\mathsf{orb}_{f,1}(I,\alpha)$ is distinguished if and only if $f$ is squareful.*

*Proof.* Let $f = \prod_{i=1}^m F_i$ be a canonical factorization of $f$. Suppose that $e_j$ is odd for some $j \in \{2,\dots,m\}$, and let $(I,\alpha) \in H^*_{f,1}$ be any element. For the forward direction, it suffices by Proposition 19 to show that $f_0^n I_f$ is not a square as a fractional ideal of $R_f$.

Under the identification $R_f \simeq \prod_{i=1}^m R_{F_i}$, the fractional ideal $I_f$ is identified with $\prod_{i=1}^m I_{F_i}$, where $I_{F_i}$ is a fractional ideal of $R_{F_i}$ for each $i \in \{1,\dots,m\}$. Now, $I_{F_j} = (1)$ is the unit ideal because $F_j$ is monic, so the $j^{\text{th}}$ factor of $f_0^n I_f$ is equal to the fractional ideal $f_0^n I_{F_j} = (p^{\nu_p(f_0)n})$, which is not a square. Indeed, if $(p^{\nu_p(f_0)n})$ were a square, then $(p)$ would be a square because $\nu_p(f_0)$ and $n$ are odd, but this is impossible: by the proof of Lemma 41, $F_j$ is irreducible, so $K_{F_j}$ is a ramified extension of $\mathbb{Q}_p$ with odd ramification degree $e_j$. As $f_0^n I_{F_j}$ is not a square, neither is $f_0^n I_f$.

For the reverse direction, suppose that $e_i$ is even for each $i \in \{2,\dots,m\}$. It then suffices to construct a based fractional ideal $I$ of $R_f$ such that $I^2 = f_0^n I_f^{n-2}$ and such that $\mathrm{N}(I)^2 = \mathrm{N}(f_0^n)\,\mathrm{N}(I_f^{n-2})$. To do this, it further suffices to construct for each $i \in \{1,\dots,m\}$ a based fractional ideal $I_i$ of $R_{F_i}$ such that $I_i^2 = f_0^n I_{F_i}^{n-2}$ and $\mathrm{N}(I_i)^2 = \mathrm{N}(f_0^n)\,\mathrm{N}(I_{F_i}^{n-2})$. We first handle $i \in \{2,\dots,m\}$. For such $i$, we have that $K_{F_i}$ is a ramified extension of $\mathbb{Q}_p$ with even ramification degree $e_i$, so $(p)$ is a square as an ideal of $R_{F_i}$. Thus, there exists an invertible fractional ideal $I_i$ of $R_{F_i}$ such that $I_i^2 = (p^{\nu_p(f_0)n}) = f_0^n I_{F_i}^{n-2}$. But $\mathrm{N}(f_0^n)\,\mathrm{N}(I_{F_i}^{n-2}) = f_0^{n \deg F_i}$, which is a perfect square since $2 \mid e_i$ and $e_i \mid \deg F_i$. So, there exists a basis of $I_i$ with respect to which $\mathrm{N}(I_i)^2 = \mathrm{N}(f_0^n)\,\mathrm{N}(I_{F_i}^{n-2})$.

We now take $i = 1$. Note that $e_1$ must be odd since $e_j$ is even for each $j \in \{2,\dots,m\}$ and $n$ is odd. If $e_1 > 1$, Lemma 38 tells us that the polynomial $F_1(1,x)$ is Eisenstein. Thus,

in this case, $K_{F_1}$ is a totally ramified extension of $\mathbb{Q}_p$ having degree $e_1$, and $\nu_p(f_0) = 1$. If $\mathfrak{p} \subset \mathcal{O}_{K_{F_1}}$ is the prime lying above $(p) \subset \mathbb{Z}_p$, then $(\mathrm{N}(\mathfrak{p})) = (p)$ as ideals of $\mathbb{Z}_p$, so since $(\mathrm{N}(I_{F_1})) = (p^{-\nu_p(f_0)}) = (p)^{-1}$, we conclude that there is a basis of $\mathfrak{p}^{-1}$ such that $I_{F_1} = \mathfrak{p}^{-1}$ as based fractional ideals of $R_{F_1}$. Therefore, when $e_1 > 1$, we have that $f_0^n I_{F_1}^{n-2} = \mathfrak{p}^{(e_1-1)n+2}$, which is a square, and when $e_1 = 1$, we have that $f_0^n I_{F_1}^{n-2} = (f_0^2)$, which is also a square. Letting $I_1$ be an invertible fractional ideal of $R_{F_1}$ such that $I_1^2 = f_0^n I_{F_1}^{n-2}$, the fact that $\mathrm{N}(f_0^n)\,\mathrm{N}(I_{F_1}^{n-2}) = f_0^{(e_1-1)n+2}$ is a perfect square implies that we can choose a basis of $I_1$ with respect to which $\mathrm{N}(I_1)^2 = \mathrm{N}(f_0^n)\,\mathrm{N}(I_{F_1}^{n-2})$.

This concludes the proof of Proposition 48. □

In the next theorem, we compute the $p$-adic density of forms $f \in V_{n,f_0}(\mathbb{Z}_p)_{\max}$ satisfying the criterion for distinguishedness obtained in Proposition 48:

**Theorem 49.** *Retain the setting of Proposition 48. The $p$-adic density of the subset of squareful elements in $V_{n,f_0}(\mathbb{Z}_p)_{\max}$ is given by $p^{\frac{1-n}{2}}(1+p^{-1})^{-1}$.*

*Proof.* Let $S := V_{n,f_0}(\mathbb{Z}_p)_{\max}$ and $S' := \{F \in V_{n,f_0}(\mathbb{Z}_p)_{\max} : f \text{ is squareful}\}$. Let $\delta_S$ denote the $p$-adic density of $S$ in $V_{n,f_0}(\mathbb{Z}_p)$, and let $\delta_{S'}$ denote the $p$-adic density of $S'$ in $V_{n,f_0}(\mathbb{Z}_p)$. Then the desired $p$-adic density of $S'$ in $S$ is $\delta_{S'}/\delta_S$.

By Lemma 38, we have $\min\{e_1, \nu_p(f_0)\} = 1$. By a computation entirely analogous to that of the density $\delta_S$ in the proof of Theorem 42, we then find that

$$\delta_S = \begin{cases} \sum\limits_{\kappa \in \mathbb{F}_p^\times} \left(p^{-n} + p^{1-n} + \sum_{\ell=1}^{n-2} p^{-\ell}(1-p^{-2})\right) = 1 - p^{-2}, & \text{if } \nu_p(f_0) = 1, \\ (1-p^{-1})(1-p^{-2}), & \text{if } \nu_p(f_0) > 1. \end{cases} \tag{2.34}$$

Let $\delta_{2m}$ denote the $p$-adic density in $V_{2m,1}(\mathbb{Z}_p)_{\max}$ of forms $H$ such that $H$ is a perfect square modulo $p$ as in the proof of Theorem 42. By imitating the computation of the density

$\delta_{S'}$ in the proof of Theorem 42, we find that

$$\delta_{S'} = \tag{2.35}$$
$$\begin{cases} \sum_{\kappa \in \mathbb{F}_p^\times} \sum_{\substack{1 \le e_1 \le n \\ e_1 \equiv 1 \bmod 2}} p^{-e_1} \delta_{n-e_1} = p^{\frac{1-n}{2}}(1-p^{-1}), & \text{if } \nu_p(f_0) = 1, \\ (1-p^{-1})\delta_{n-1} = p^{\frac{1-n}{2}}(1-p^{-1})^2, & \text{if } \nu_p(f_0) > 1. \end{cases}$$

where the second equality in each case of (2.35) follows from Proposition 43. □

### 2.4.4 Existence, part *(iii)*: $n$ is odd, $\nu_p(f_0)$ is even

In this case, there exists $(I, \alpha) \in H^*_{f,1}$ such that the $G_n(\mathbb{Q}_p)$-orbit containing $\mathsf{orb}_{f,1}(I, \alpha)$ is distinguished, assuming $R_f$ is maximal when $\nu_p(f_0) > 0$:

**Proposition 50.** *Let $\nu_p(f_0)$ be even, let $f \in V_{n,f_0}(\mathbb{Z}_p)$ if $\nu_p(f_0) = 0$, and let $f \in V_{n,f_0}(\mathbb{Z}_p)_{\max}$ if $\nu_p(f_0) > 0$. Then there exists a fractional ideal $I$ of $R_f$ such that $(I, f_0^n) \in H^*_{f,1}$.*

*Proof.* If $\nu_p(f_0) = 0$, then $f_0 \in \mathbb{Z}_p^\times$, and so $f_0^n I_f = (1)$ is the unit ideal. Taking $I = (1)$, we find that $I^2 = f_0^n I_f^{n-2}$; because $\mathrm{N}(f_0^n)\,\mathrm{N}(I_f^{n-2}) = f_0^{n^2-n+2}$ is a perfect square, there exists a basis of $I$ such that $\mathrm{N}(I)^2 = \mathrm{N}(f_0^n)\,\mathrm{N}(I_f^{n-2})$.

If $\nu_p(f_0) > 0$, then by Lemma 38, we have that $e_1 = 1$ because $\nu_p(f_0)$ is even. It suffices to show that there exist based fractional ideals $I_1$ of $R_{F_1}$ and $I'$ of $R_{f/F_1}$ such that the following four conditions are satisfied: $I_1^2 = f_0^n I_{F_1}^{n-2}$, $\mathrm{N}(I_1)^2 = \mathrm{N}(f_0^n)\,\mathrm{N}(I_{F_1}^{n-2})$, $I'^2 = f_0^n I_{f/F_1}^{n-2}$, and $\mathrm{N}(I')^2 = \mathrm{N}(f_0^n)\,\mathrm{N}(I_{f/F_1}^{n-2})$. Notice that $f_0^n I_{F_1} = (f_0^2)$, which is a square, and $\mathrm{N}(f_0^n)\,\mathrm{N}(I_{F_1}^{n-2}) = f_0^2$, which is a square, so we can take $I_1 = (f_0)$ and give it a basis with respect to which $\mathrm{N}(I_1)^2 = \mathrm{N}(f_0^n)\,\mathrm{N}(I_{F_1}^{n-2})$. We also have $f_0^n I_{f/F_1}^{n-2} = (p^{\nu_p(f_0)n})$, which is a square, and that $\mathrm{N}(f_0^n)\,\mathrm{N}(I_{f/F_1}^{n-2}) = f_0^{n\deg(f/F_1)}$, which is a square as $\deg(f/F_1) = n-1$ is even. Thus, there exists a based fractional ideal $I'$ such that $I'^2 = f_0^n I_{f/F_1}^{n-2}$ and $\mathrm{N}(I')^2 = \mathrm{N}(f_0^n)\,\mathrm{N}(I_{f/F_1}^{n-2})$. □

Together, Propositions 47, 48, and 50 give an explicit construction of a "distinguished" square root of the class of the inverse different of $R_F$ for any primitive $f \in V_{n,f_0}(\mathbb{Z})^{r_1,r_2} \cap$

$\bigcap_{p|f_0} V_{n,f_0}(\mathbb{Z}_p)_{\max}$ that is squareful over $\mathbb{Z}_p$ for each $p \mid k$, thus proving Theorem 31.

### 2.4.5 On a question of Emerton

Theorem 31 gives a partial answer to a question of Emerton, who was motivated by Hecke's theorem to ask whether the class of the different of a number field $K$ has a canonical square root [62]. While the answer is likely "no" in general, Theorem 31 tells us that we can sometimes pick out natural square roots when $\mathcal{O}_K$ has additional structure. Under certain conditions when $n$ is odd, we can pick out a square root of the class of $I_f^{n-2}$ that gives rise to the distinguished $G_n(\mathbb{Q})$-orbit, but this square root is highly dependent on $f$: it remains unchanged if we replace $f$ by any translate under the subgroup $N(\mathbb{Z}) \subset \mathrm{GL}_2(\mathbb{Z})$, but it is *not* invariant under the action of the full group $\mathrm{GL}_2(\mathbb{Z})$. On the other hand, when $n$ is even, $I_f^{\frac{2-n}{2}}$ represents a square root of the class of the different, and this class remains unchanged if we replace $f$ by any $\mathrm{GL}_2(\mathbb{Z})$-translate. But this class is not particularly canonical either: if $f, f'$ are forms such that $\mathcal{O}_K = R_f = R_{f'}$, they are *not necessarily* $\mathrm{GL}_2(\mathbb{Z})$-equivalent, and the ideals $I_f^{\frac{2-n}{2}}$, $I_{f'}^{\frac{2-n}{2}}$ may represent distinct square roots of the class of the different of $\mathcal{O}_K$. Indeed, the following theorem gives an example of this phenomenon in the case where $n = 4$:

**Theorem 51.** *Let*

$$f(x,y) = 4x^4 - x^3y - 62x^2y^2 + 13xy^3 + 255y^4 \quad \textit{and} \quad g(x,y) = 5x^4 - x^3y - 2x^2y^2 - 7xy^3 - 6y^4.$$

*Then $R_f$ and $R_g$ are isomorphic, but there is no isomorphism between $R_f$ and $R_g$ under which the ideal classes of $I_f$ and $I_g$ are identified. In fact, $I_f$ is principal, whereas $I_g$ is not.*

*Proof.* We first prove that $R_f$ and $R_g$ are isomorphic. Consider the map $\upsilon\colon V_4(\mathbb{Z}) \to \mathbb{Z}^2 \otimes_{\mathbb{Z}}$

$\mathrm{Sym}^2 \mathbb{Z}^3$ sending a binary quartic form $F(x,y) = \sum_{i=0}^{4} f_i x^{4-i} y^i$ to the pair

$$(A_{\frac{1g}{2}}, B_f) := \left[ \begin{bmatrix} 0 & 0 & \frac{1}{2} \\ 0 & -1 & 0 \\ \frac{1}{2} & 0 & 0 \end{bmatrix}, \begin{bmatrix} f_0 & \frac{f_1}{2} & 0 \\ \frac{f_1}{2} & f_2 & \frac{f_3}{2} \\ 0 & \frac{f_3}{2} & f_4 \end{bmatrix} \right]$$

Here, $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}^2 \mathbb{Z}^3$ denotes the space of integral ternary quadratic forms (as opposed to the space $W_3(\mathbb{Z})$ of integer-matrix ternary quadratic forms). The group $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ acts on the space $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}^2 \mathbb{Z}^3$ via

$$\left(\gamma, \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)\right) \cdot (A, B) = (r \times \gamma A \gamma^T + s \times \gamma B \gamma^T, t \times \gamma A \gamma^T + u \times \gamma B \gamma^T),$$

so we may think of $F$ as giving rise to an orbit of $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ on $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}^2 \mathbb{Z}^3$ via the map $\upsilon$. We then have the following result, which translates properties about rings associated to binary quartic forms into properties about the corresponding orbits of $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ on $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}^2 \mathbb{Z}^3$:

**Proposition 52.** *Let $f, g \in V_4(\mathbb{Z})$ be such that $\upsilon(f)$ and $\upsilon(g)$ are equivalent under the action of $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$. Then $R_f$ and $R_g$ are isomorphic. If $f$ and $g$ are $\mathrm{GL}_2(\mathbb{Z})$-equivalent, then $\upsilon(f)$ and $\upsilon(g)$ are equivalent under the action of $\mathrm{GL}_3(\mathbb{Z}) \subset \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$.*

*Proof of Proposition 52.* This is an immediate consequence of the parametrization of quartic rings given in [7, Theorem 2] together with [125, Lemma 2.2], which explains how the rings associated to binary quartic forms fit into this parametrization. □

To prove that $R_f$ and $R_g$ are isomorphic, it suffices by Proposition 52 to exhibit the pair

$(\gamma, \left[\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right]) \in \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ such that $(\gamma, \left[\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right]) \cdot (A_0, B_g) = (A_0, B_f)$. A calculation reveals

$$\gamma = \begin{bmatrix} 0 & 2 & -1 \\ -1 & 0 & 1 \\ -3 & -15 & 10 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} r & s \\ t & u \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 63 \end{bmatrix}$$

do the job. Upon observing that $f$ and $g$ have (the same) squarefree discriminant, which implies that $R_f \simeq R_g$ is maximal, verifying that $I_f$ is principal and that $I_g$ is not can be achieved in `sage` using the following code:

```
R.<x> = PolynomialRing(QQ)
K.<a> = NumberField(4*x^4-x^3-62*x^2+13*x+255)
K.ideal(1,a,4*a^2-a,4*a^3-a^2-62*a).is_principal(proof = True)
L.<b> = NumberField(5*x^4-x^3-2*x^2-7*x-6)
L.ideal(1,b,5*b^2-b,5*b^3-b^2-2*b).is_principal(proof = True)
```

In fact, one can use `sage` to verify that $\mathrm{Cl}(R_f = R_g)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, so $[I_g]$ is the nontrivial class, which squares to $[I_f]$. This completes the proof of Theorem 51. □

We now briefly explain how to search for examples such as the one presented in Theorem 51. For simplicity, we restrict our search to irreducible forms $f \in V_4(\mathbb{Z})$ of squarefree discriminant (so that, in particular, $R_f$ is maximal). We claim that we can impose the following condition without loss of generality:

*Property (i): $I_f$ is not principal, and $\mathrm{Cl}(R_f)[2]$ has a nontrivial element.*

For the first part of the claim, note that if the desired form $g$ exists, then at least one of $I_f$ or $I_g$ is not principal. As for the second part, recall that $I_f^2$ represents the class of the inverse different of $R_f$. In particular, if $R_f$ is isomorphic to $R_g$ for some $g \in V_4(\mathbb{Z})$, then $[I_f]$ and $[I_g]$ square to the same element of $\mathrm{Cl}(R_f)$. Thus, if $[I_f] \neq [I_g]$ do not lie in the same class, then

$\mathrm{Cl}(R_f)[2]$ has a nontrivial element, namely $[I_f I_g^{-1}]$. Note that it is not *a priori* obvious that a polynomial $f$ satisfying Property (i) exists, but a computer search reveals many examples.

Having narrowed our search to forms $f$ satisfying Property (i), we now explain how to construct $g \in V_4(\mathbb{Z})$ such that $R_f$ and $R_g$ are isomorphic but $f$ and $g$ are not $\mathrm{GL}_2(\mathbb{Z})$-equivalent (note that, by (1.7), $f$ and $g$ must be $\mathrm{GL}_2(\mathbb{Z})$-inequivalent for $I_f I_g^{-1}$ to be non-principal). To construct such a $g$, we claim that it suffices to impose the following condition:

*Property (ii): We have that* $\det B_f = 1$ *and that* $B_f$ *is isotropic over* $\mathbb{Q}$.

Suppose Property (ii) is satisfied. Then it follows from the classification of integral ternary quadratic forms that there exists a transformation $\gamma \in \mathrm{GL}_3(\mathbb{Z})$ such that $\gamma B_f \gamma^T = A_0$. Let $B = \gamma A_0 \gamma^T$, and let $b$ denote the row-1, column-3 entry of $B$. Acting on the pair $\gamma \cdot (A_0, B_f) = (B, A_0)$ via $\left[\begin{smallmatrix} 0 & 1 \\ 1 & -b \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{Z})$, we obtain a pair of the shape $(A_0, B_g)$, where $g \in V_4(\mathbb{Z})$. By Proposition 52, $R_f$ and $R_g$ are isomorphic.

Now, if $f$ and $g$ are $\mathrm{GL}_2(\mathbb{Z})$-equivalent, then the stabilizer of the pair $(A_0, B_f)$ in $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ would contain a nontrivial element. But this is impossible: the stabilizer of $(A_0, B_f)$ is simply the group of automorphisms of the ring $R_f$, but because $R_f$ has squarefree discriminant, it has no nontrivial automorphisms. Thus, we have the claim.

One can then generate forms $f \in V_4(\mathbb{Z})$ satisfying Properties (i) and (ii), apply the above procedure to obtain the form $g$, and check whether $I_f I_g^{-1}$ is principal.

## 2.5 Proofs of the main results on class group statistics

Let $f \in V_{n,f_0}(\mathbb{Z})_{\max}$. In §3.2, we proved Lemmas 33, 34, and 35, which reduce the problem of computing the number of 2-torsion elements in the (ordinary or narrow) class group of the ring $R_f$ to the problem of calculating the three quantities

$$\#\mathsf{orb}_{f,1}(H^*_{f,1}), \quad \#\mathsf{orb}_{f,-1}(H^*_{f,-1}), \quad \text{and} \quad \#\mathsf{orb}_{f,1}(H^{*,+}_{f,1}). \tag{2.36}$$

To prove the theorems stated in §2.1.1, we must bound (and conditionally determine) the average values of these quantities as $f$ ranges through subfamilies of $V_{n,f_0}(\mathbb{Z})_{\max}$. In this section, we compute these averages by combining geometry-of-numbers results from [108,109] with the local orbit-counting results and density calculations obtained in §2.3.

### 2.5.1 Counting $N(\mathbb{Z})$-orbits of binary forms with fixed leading coefficient

For each prime $p$, let $\Sigma_p \subset V_{n,f_0}(\mathbb{Z}_p)$ be a nonempty $N(\mathbb{Z}_p)$-invariant open set of primitive forms with boundary of measure 0, and let $\Sigma_\infty = V_{n,f_0}(\mathbb{R})^{r_1,r_2}$. We call the family $\Sigma = (\Sigma_v)_v$ over places $v$ of $\mathbb{Q}$ a *family of local specifications* and define

$$V_{n,f_0}(\Sigma) := \{f \in V_{n,f_0}(\mathbb{Z}) : f \in \Sigma_v \text{ for all places } v\}.$$

We call $\Sigma$ *acceptable* if $\Sigma_p$ contains all $f \in V_{n,f_0}(\mathbb{Z}_p)$ with discriminant indivisible by $p^2$ for all $p \gg 1$ and if $\Sigma_2$ is the preimage in $V_{n,f_0}(\mathbb{Z}_2)$ of a set of separable forms in $V_{n,f_0}(\mathbb{Z}/2\mathbb{Z})$.

Let $\Sigma$ be an acceptable family of local specifications with $\Sigma_\infty = V_{n,f_0}(\mathbb{R})^{r_1,r_2}$. As explained in §1.2, if $f, f' \in V_{n,f_0}(\mathbb{Z})$ are $N(\mathbb{Z})$-translates of each other, then $R_f \simeq R_{f'}$. To minimize the multiplicity with which a given ring arises from our family $V_{n,f_0}(\Sigma)$, we compute the averages of the quantities (2.36) over elements of the quotient family $N(\mathbb{Z})\backslash V_{n,f_0}(\Sigma)$.[3] Observe that for every $f \in V_{n,f_0}(\Sigma)$, there exists a unique integer $b \in \{0, \dots, nf_0 - 1\}$ such that $f$ is an $N(\mathbb{Z})$-translate of a form whose $x^{n-1}y$-coefficient is equal to $b$. Thus, the set $N(\mathbb{Z})\backslash V_{n,f_0}(\Sigma)$ can be expressed as

$$N(\mathbb{Z})\backslash V_{n,f_0}(\Sigma) = \bigsqcup_{b=0}^{f_0 n-1} \{f \in V_{n,f_0}(\Sigma) : b \text{ is the } x^{n-1}y\text{-coefficient of } f\}. \tag{2.37}$$

Using (2.37), we may think of $N(\mathbb{Z})\backslash V_{n,f_0}(\Sigma)$ as a subset of $V_{n,f_0}(\Sigma)$. Similarly, we can view

[3] We could also average the quantities (2.36) over $V_{n,f_0}(\Sigma)$, and the results in §2.1.1 would remain essentially unchanged.

$N(\mathbb{Z})\backslash V_{n,f_0}(\mathbb{R})$ as a subset of $V_{n,f_0}(\mathbb{R})$ by identifying each class in $N(\mathbb{Z})\backslash V_{n,f_0}(\mathbb{R})$ with the unique representative in $V_{n,f_0}(\mathbb{R})$ that has $x^{n-1}y$-coefficient lying in the interval $[0, f_0 n - 1)$.

For any subset $S \subset V_{n,f_0}(\mathbb{R})$ and real number $X > 0$, let $S_X := \{f \in S : \mathrm{H}(f) < X\}$, where the height function H is as defined in §2.1.1.1. In addition, for any subset $S \subset V_{n,f_0}(\mathbb{Z})$, let $S^{\mathrm{irr}} := \{f \in S : f \text{ is irreducible}\}$. We then have the following theorem, which gives us an asymptotic for how many elements of $N(\mathbb{Z})\backslash V_{n,f_0}(\Sigma)$ there are of height up to $X$:

**Theorem 53.** *Let $\Sigma$ be an acceptable family of local specifications. Then we have*

$$\#\big(N(\mathbb{Z})\backslash V_{n,f_0}(\Sigma)^{\mathrm{irr}}_X\big) = \mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X) \cdot \prod_p \mathrm{Vol}(\Sigma_p) + o\big(X^{\frac{n(n+1)}{2}-1}\big), \tag{2.38}$$

*where the real volume is computed with respect to the Euclidean measure on $V_{n,f_0}(\mathbb{R})$ normalized so that $\mathrm{Vol}(V_{n,f_0}(\mathbb{R})/V_{n,f_0}(\mathbb{Z})) = 1$, and where the $p$-adic volumes are computed with respect to the Euclidean measure on $V_{n,f_0}(\mathbb{Z}_p)$ normalized so that $\mathrm{Vol}(V_{n,f_0}(\mathbb{Z}_p)) = 1$.*

*Proof.* The theorem can be deduced using the uniformity estimate given in the next result, Theorem 54, in the same way that [26, Theorem 2.21] is proven using [26, Theorem 2.13]. Indeed, the first half of the proof of [26, Theorem 2.21] can be imitated to prove (2.38) with "=" replaced by "$\leq$"; then, by using Theorem 54 in place of [26, Theorem 2.13], the second half of the proof of [26, Theorem 2.21] can be imitated to prove (2.38) with "=" replaced by "$\geq$." □

The next theorem supplies the uniformity estimate needed to prove Theorem 53:

**Theorem 54.** *Let $\mathcal{V}_{n,f_0}(p) := \{f \in V_{n,f_0}(\mathbb{Z}) : p^2 \mid \text{discriminant of } f\}$. For any real number $M$ that is larger than each prime divisor of $f_0$, and for any $\varepsilon \in (0,1)$, we have*

$$\#\bigg(\bigcup_{p>M} N(\mathbb{Z})\backslash \mathcal{V}_{n,f_0}(p)_X\bigg) = O\bigg(\frac{X^{\frac{n(n+1)}{2}-1+\varepsilon}}{M}\bigg) + o\big(X^{\frac{n(n+1)}{2}-1}\big), \tag{2.39}$$

*where the implied constant in the big-O is independent of $X$, $M$.*

*Proof.* We first prove (2.39) in the case where $f_0 = 1$. In this case, [29, Theorem 1.5] implies that (2.39) holds if we make the following two replacements: (1) work with the family $V_{n,1}(\mathbb{Z})$ as opposed to the family $N(\mathbb{Z})\backslash V_{n,1}(\mathbb{Z})$; and (2) replace H with $\widetilde{\mathrm{H}}$, which is defined on $f \in V_{n,1}(\mathbb{R})$ by $\widetilde{\mathrm{H}}(f) = \max\{|f_i|^{1/i} : 2 \le i \le n\}$. These two replacements can be easily undone. Indeed, to deal with the first replacement, the proof of [29, Theorem 1.5] can be modified (as suggested in [29, discussion after Theorem 6.4]) to obtain the analogous result for the family $N(\mathbb{Z})\backslash V_{n,1}(\mathbb{Z})$. To deal with the second replacement, we note that the functions H and $\widetilde{\mathrm{H}}$ are "comparable," in the sense that $\widetilde{\mathrm{H}}(f) = O(\mathrm{H}(f))$ for all $f \in V_{n,1}(\mathbb{R})$. It follows that (2.39) holds when $f_0 = 1$.

We now deduce the case $f_0 \neq 1$ from the case $f_0 = 1$. Let $\mathsf{mon}\colon V_{n,f_0}(\mathbb{R}) \to V_{n,1}(\mathbb{R})$ denote the map that sends a binary form $f$ to its monicized form $f^{\mathsf{mon}}$. Notice that $\mathsf{mon}$ is one-to-one, that $\mathrm{H}(f^{\mathsf{mon}}) = \mathrm{H}(f)$, and that the ratio of the discriminants of $f^{\mathsf{mon}}$ and $f$ is a power of $f_0$. Thus, for any prime $p$ larger than every prime divisor of $f_0$, we have

$$\mathsf{mon}(\mathcal{V}_{n,f_0}(p)_X) \subset \mathcal{V}_{n,1}(p)_X. \tag{2.40}$$

Taking the union over primes $p > M$ on both sides of (2.40) and estimating the right-hand side by applying (2.39) for the case $f_0 = 1$ yields the theorem in all cases. □

### 2.5.2 Counting $(N \times \mathcal{G}_{A_0})(\mathbb{Z})$-orbits of on $W_{A_0}(\mathbb{Z})$

To average the quantities (2.36) over $f \in V_{n,f_0}(\Sigma)$, we need a way to count $G_n(\mathbb{Z})$-orbits of pairs $(A, B) \in W_n(\mathbb{Z})$ arising from elements of $H^*_{f,\pm 1}$. However, if $(A, B)$ represents such a $G_n(\mathbb{Z})$-orbit, then $\operatorname{inv} A = \pm 1$, so we would need to count integral points on the hypersurfaces in $W_n(\mathbb{R})$ defined by the equations $\operatorname{inv} A = \pm 1$. Because these hypersurfaces are non-linear, this count would be difficult to perform directly. To circumvent this issue, we use the linearization trick described in §1.3.2, which tells us that instead of counting $G_n(\mathbb{Z})$-orbits on pairs $(A, B) \in W_n(\mathbb{Z})$ satisfying $\operatorname{inv}(A) = \pm 1$, we can just count $\mathcal{G}_{A_0}(\mathbb{Z})$-orbits on

matrices $T \in W_{A_0}(\mathbb{Z})$, where $A_0$ ranges through a finite set of possibilities.

Fix a symmetric matrix $A_0 \in U_n(\mathbb{Z})$ satisfying $\operatorname{inv} A_0 = \pm 1$. Let $R$ be any $\mathbb{Z}$-algebra, and for $h \in N(R)$ and $T \in W_{A_0}(R)$, let $h \cdot T := -f_0 h_{21} \operatorname{id} + T$. This gives a well-defined action of $N(R)$ on $W_{A_0}(R)$.

We call $T \in W_{A_0}(\mathbb{Z}_p)$ *pre-projective* if $(A_0, -A_0 T) \in W_n(\mathbb{Z}_p)$ is pre-projective in the sense of §2.2. Let $\Sigma$ be an acceptable family of local specifications, and for each prime $p$, let

$$W_{A_0}(\Sigma_p) := \left\{ T \in W_{A_0}(\mathbb{Z}_p) : \begin{array}{c} T \text{ is pre-projective and} \\ \operatorname{ch}_T(x) = f^{\mathsf{mon}}(x,1) \text{ for some } f \in \Sigma_p \end{array} \right\}.$$

Next, let $(r_1, r_2)$ be a real signature of a degree-$n$ number field, and let $f \in V_{n,\pm 1}(\mathbb{R})^{r_1,r_2}$ be separable. It follows from Proposition 19 that the $G_n(\mathbb{R})$-orbits of pairs $(A, B) \in W_n(\mathbb{R})$ such that $\iota(A, B) = f$ are in bijection with the elements of $(K_f^\times / K_f^{\times 2})_{\mathrm{N} \equiv 1}$ if $n$ is odd (resp., $K_f^\times / K_f^{\times 2}$ if $n$ is even). It is easy to check that one may identify the group $K_f^\times / K_f^{\times 2}$ with the group $(\mathbb{R}^\times / \mathbb{R}^{\times 2})^{r_1}$, but we now choose such an identification in a way that is natural with respect to the binary form $f$. Let $\theta_1 < \theta_2 < \cdots < \theta_{r_1}$ denote the real roots of $f$. Then

$$K_f = \mathbb{R}[x]/(f(x,1)) \simeq \left( \prod_{i=1}^{r_1} \mathbb{R}[x]/(x - \theta_i) \right) \times \mathbb{C}^{r_2} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \tag{2.41}$$

and the identification in (2.41) descends to a natural identification $K_f^\times / K_f^{\times 2} \simeq (\mathbb{R}^\times / \mathbb{R}^{\times 2})^{r_1}$. Given this, we say that a $G_n(\mathbb{R})$-orbit of a pair $(A_0, B) \in W_n(\mathbb{R})$ is of type $\sigma \in (\mathbb{R}^\times / \mathbb{R}^{\times 2})^{r_1}$ if $f = \iota(A_0, B) \in V_{n,\pm 1}(\mathbb{R})^{r_1,r_2}$ is separable and if the corresponding element of $K_f^\times / K_f^{\times 2}$ is identified with $\sigma$.

Now, fix $\sigma \in (\mathbb{R}^\times / \mathbb{R}^{\times 2})^{r_1}_{\mathrm{N} \equiv 1}$ if $n$ is odd (resp., $\sigma \in (\mathbb{R}^\times / \mathbb{R}^{\times 2})^{r_1}$) if $n$ is even), and let

$$W_{A_0}(\Sigma_\infty)^\sigma = \{T \in W_{A_0}(\mathbb{R}) : G_n(\mathbb{R})\text{-orbit of } (A_0, -A_0 T) \text{ has type } \sigma\}.$$

The set $W_{A_0}(\Sigma_\infty)^\sigma$ is nonempty if and only if there exists $T \in W_{A_0}(\mathbb{R})$ such that the $G_n(\mathbb{R})$-

orbit of $(A_0, -A_0T)$ has type $\sigma$. To keep track of whether $W_{A_0}(\Sigma_\infty)^\sigma$ is empty, we let

$$\chi_{A_0}(\sigma) = \begin{cases} 1, & \text{if } W_{A_0}(\Sigma_\infty)^\sigma \neq \varnothing, \\ 0, & \text{otherwise.} \end{cases}$$

Given the sets $W_{A_0}(\Sigma_p)$ and $W_{A_0}(\Sigma_\infty)^\sigma$, we define

$$W_{A_0}(\Sigma)^\sigma := W_{A_0}(\mathbb{Z}) \cap W_{A_0}(\Sigma_\infty)^\sigma \cap \bigcap_p W_{A_0}(\Sigma_p).$$

As we are averaging the quantities (2.36) over $N(\mathbb{Z})$-orbits of forms in $V_{n,f_0}(\mathbb{Z})$, we are interested only in elements of $W_{A_0}(\Sigma)^\sigma$ up to the action of $(N \times \mathcal{G}_{A_0})(\mathbb{Z})$. One readily verifies that the set $W_{A_0}(\Sigma)^\sigma$ is $(N \times \mathcal{G}_{A_0})(\mathbb{Z})$-invariant.

To count elements of $(N \times \mathcal{G}_{A_0})(\mathbb{Z})\backslash W_{A_0}(\Sigma)^\sigma$, we need a way to order them. To this end, let $T \in W_{A_0}(\mathbb{R})$ be such that $\mathrm{ch}_T(x) = f(x, 1)$ for some form $f \in V_{n,1}(\mathbb{Z})$. We then define the height $\mathrm{H}(T)$ of $T \in W_{A_0}(\mathbb{R})$ in terms of the height H defined in (2.2) as follows:

$$\mathrm{H}(T) := \mathrm{H}(f), \tag{2.42}$$

The group $(N \times \mathcal{G}_{A_0})(\mathbb{R})$ acts on $T \in W_{A_0}(\mathbb{R})$ via $(g, h) \cdot T = -f_0 h_{21} \,\mathrm{id} + gTg^{-1}$. It follows from (2.2) and (2.42) that $\mathrm{H}(T) = \mathrm{H}((g, h) \cdot T)$ for any $(g, h) \in (N \times \mathcal{G}_{A_0})(\mathbb{R})$ and $T \in W_{A_0}(\mathbb{R})$. Thus, H descends to a well-defined height function on $(N \times \mathcal{G}_{A_0})(\mathbb{Z})\backslash W_{A_0}(\mathbb{R})$.

For any subset $S \subset W_{A_0}(\mathbb{R})$ and real number $X > 0$, let $S_X := \{T \in S : \mathrm{H}(T) < X\}$. For $T \in W_{A_0}(\mathbb{Z})$, we say that the $\mathcal{G}_{A_0}(\mathbb{Q})$-orbit of $T$ is *distinguished* if the $G_n(\mathbb{Q})$-orbit of the pair $(A_0, -A_0T) \in W_n(\mathbb{Z})$ is distinguished. For any subset $S \subset W_{A_0}(\mathbb{Z})$, let

$$S^{\mathrm{irr}} := \{T \in S : \mathrm{ch}_T \text{ is irreducible and the } \mathcal{G}_{A_0}(\mathbb{Q})\text{-orbit of } T \text{ is non-distinguished}\}.$$

We then have the following theorem, which gives an asymptotic for how many non-distinguished

elements of $(N \times \mathcal{G}_{A_0})(\mathbb{Z})\backslash W_{A_0}(\Sigma)^\sigma$ there are of height up to $X$:

**Theorem 55.** *With notation as above, we have that*

$$\#\big((N \times \mathcal{G}_{A_0})(\mathbb{Z})\backslash (W_{A_0}(\Sigma)^\sigma)^{\mathrm{irr}}_X\big) \leq 2^{1-r_1-r_2} \cdot \tau_{\mathcal{G}_{A_0}} \cdot \chi_{A_0}(\sigma) \cdot \mathrm{Vol}\left(\mathsf{mon}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X)\right) \cdot \prod_p \mathcal{J}(A_0, \Sigma_p) + o\big(X^{\frac{n(n+1)}{2}-1}\big), \tag{2.43}$$

*where for $A \in U_n(\mathbb{Z}_p)$ with $\det A \in \mathbb{Z}_p^\times$ and $\mathcal{S} \subset V_{n,f_0}(\mathbb{Z}_p)^{\max}$, we write*

$$\mathcal{J}(A, \mathcal{S}) := \int_{f \in \mathsf{mon}(\mathcal{S})} \sum_{\substack{T \in \mathcal{G}_A(\mathbb{Z}_p)\backslash W_A(\mathcal{S}) \\ \mathrm{ch}_T(x) = f(x,1)}} \frac{df}{\#\,\mathrm{Stab}_{\mathcal{G}_A}(T)} \cdot \begin{cases} 1, & \text{if } n \text{ is odd,} \\ 2, & \text{if } n \text{ is even,} \end{cases}$$

*where $dF$ is the Euclidean measure on $V_{n,1}(\mathbb{Z}_p)$ normalized as in Theorem 53, and where*

$$\tau_{\mathcal{G}_{A_0}} := \mathrm{Vol}\left(\mathcal{G}_{A_0}(\mathbb{Z})\backslash \mathcal{G}_{A_0}(\mathbb{R})\right) \cdot \begin{cases} \prod_p \mathrm{Vol}(\mathcal{G}_{A_0}(\mathbb{Z}_p)), & \text{if } n \text{ is odd,} \\ \prod_p \frac{1}{2}\,\mathrm{Vol}(\mathcal{G}_{A_0}(\mathbb{Z}_p)), & \text{if } n \text{ is even.} \end{cases} \tag{2.44}$$

*In (2.44), the volumes are computed with respect to the Haar measure on $\mathcal{G}_{A_0}$.*

*Let $\mathcal{W}_{A_0,p} := \{T \in W_{A_0}(\mathbb{Z}) : p^2 \mid \text{discriminant of } \mathrm{ch}_T\}$. Then equality holds in (2.43) if $\Sigma$ is very large, or if the following uniformity estimate holds: for any $M > 0$ and $\varepsilon \in (0,1)$, we have that*

$$\#\left(\bigcup_{p>M} (N \times \mathcal{G}_{A_0})(\mathbb{Z})\backslash(\mathcal{W}_{A_0,p})_X\right) = O\left(\frac{X^{\frac{n(n+1)}{2}-1}}{M^{1-\varepsilon}}\right) + o\big(X^{\frac{n(n+1)}{2}-1}\big), \tag{2.45}$$

*where the implied constant in the big-O is independent of $X, M$.*

*Proof.* The theorem follows by combining [108, Theorems 59, 61, 63, and 66 and Proposition 69] if $n$ is odd (resp., [109, Theorems 62, 64, 66, and 69 and Proposition 72] if $n$ is even) and applying these results to the set $W_{A_0}(\Sigma)^\sigma$. □

*Remark* 56. As stated in [108, §5.2] and [109, §5.2], the uniformity estimate in (2.45) holds for $n = 3$ and is expected to hold for $n \geq 4$ too.

### 2.5.3 Sieving to square roots of the class of the inverse different

Let $r = 1$ if $n$ is odd and $r = \pm 1$ if $n$ is even. As in §2.5.2, we fix an acceptable family $\Sigma$ of local specifications such that $V_{n,f_0}(\Sigma) \subset V_{n,f_0}(\mathbb{Z})_{\max}$ and a symmetric matrix $A_0 \in U_n(\mathbb{Z})$ such that $\operatorname{inv} A_0 = r$. In this section, we use the results of §2.3 to compute each of the local factors on the right-hand side of (2.43). We combine these computations to deduce the main theorems in §2.5.4.

The local factor at $\infty$ on the right-hand side of (2.43) is

$$\operatorname{Vol}(\mathsf{mon}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X)) = |f_0|^{\frac{n(n-1)}{2}} \cdot \operatorname{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X), \tag{2.46}$$

where the equality follows from computing the Jacobian determinant of the map $\mathsf{mon}$. To compute the factors $\mathcal{J}(A_0, \Sigma_p)$ at primes $p$, we split into cases depending on the parity of $p$ and value of $r$.

#### 2.5.3.1 Case $(i)$: $p$ is odd

By [48, p. 104-105], there is precisely one symmetric bilinear form over $\mathbb{Z}_p$ having rank $n$ and determinant $r(-1)^{\lfloor \frac{n}{2} \rfloor}$ up to $G_n(\mathbb{Z}_p)$-equivalence, so for every $F \in \Sigma_p$, we have by (1.8) in combination with Theorem 39 that

$$\#\{T \in \mathcal{G}_{A_0}(\mathbb{Z}_p)\backslash W_{A_0}(\Sigma_p) : \operatorname{ch}_T(x) = f^{\mathsf{mon}}(x,1)\} = \#\mathsf{orb}_{f,r}(H^*_{f,r}) = \tag{2.47}$$

$$\begin{cases} \frac{1}{2}\#R_f^\times[2], & \text{if } f \text{ is not evenly ramified,} \\ \#R_f^\times[2], & \text{if } f \text{ is evenly ramified, and } r = 1 \in \mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2}, \\ 0, & \text{if } f \text{ is evenly ramified, and } r \neq 1 \in \mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2}, \end{cases}$$

Furthermore, for every $T \in \mathcal{G}_{A_0}(\mathbb{Z}_p)\backslash W_{A_0}(\Sigma_p)$ such that $\mathrm{ch}_T(x) = f^{\mathsf{mon}}(x,1)$, we have

$$\#\operatorname{Stab}_{\mathcal{G}_{A_0}(\mathbb{Z}_p)}(T) = \begin{cases} \#R_f^\times[2]_{\mathrm{N}\equiv 1} = \frac{1}{2}\#R_f^\times[2], & \text{if } n \text{ is odd,} \\ \#R_f^\times[2], & \text{if } n \text{ is even.} \end{cases} \tag{2.48}$$

When $n$ is even, let $r_p(\Sigma)$ be as in Theorem 26. Using (2.47) and (2.48), we see that

$$\mathcal{J}(A_0,\Sigma_p) = |f_0|_p^{\frac{n(n-1)}{2}} \cdot \mathrm{Vol}(\Sigma_p) \cdot \begin{cases} 1, & \text{if } n \text{ is odd,} \\ 1 + r_p(\Sigma), & \text{if } n \text{ is even and } r = 1 \text{ or if } r = -1 \text{ and } p \equiv 1 \,(\mathrm{mod}\ 4), \\ 1 - r_p(\Sigma), & \text{if } n \text{ is even and } r = -1 \text{ and } p \equiv 3 \,(\mathrm{mod}\ 4), \end{cases} \tag{2.49}$$

where $|-|_p = p^{-\nu_p(-)}$ denotes the standard $p$-adic absolute value.

#### 2.5.3.2 Interlude on octane values

In order to treat the case where $p = 2$, we pause to introduce the necessary background on symmetric bilinear forms over $\mathbb{Z}_2$. Such a form is said to be of Type I if it has a unit diagonal entry and of Type II otherwise. As explained in [49, §5], $G_n(\mathbb{Z}_2)$-equivalence classes of symmetric bilinear forms over $\mathbb{Z}_2$ of given rank, given type, and given unit determinant are classified according to their so-called *octane value*, which is a number $\mathfrak{o} \in \mathbb{Z}/8\mathbb{Z}$.

Let $\rho \in \mathbb{Z}_2^\times$, and take a matrix $A \in U_n(\mathbb{Z}_2)$ of Type I with $\det A = \rho$. Then we can replace $A$ by a $G_n(\mathbb{Z}_2)$-translate that is diagonal. Upon doing so, the octane value of $A$ is simply the mod-8 reduction of the number of diagonal entries congruent to $1 \pmod 4$ minus the number of diagonal entries congruent to $3 \pmod 4$. It follows from [73, Lemma 3] that when $n \geq 3$, there are two options for the octane value of such a matrix $A$; we denote these options by $\mathfrak{o}_n(\rho)^+$ and $\mathfrak{o}_n(\rho)^-$. When $n = 2$, there are two options $\mathfrak{o}_2(\rho)^+$ and $\mathfrak{o}_2(\rho)^-$ if $\rho \equiv 1 \pmod 4$, but just one option $\mathfrak{o}_2(\rho)^+ = \mathfrak{o}_2(\rho)^-$ if $\rho \equiv 3 \pmod 4$. The values of $\mathfrak{o}_n(\rho)^\pm$

are given in Table 2.1.

| Determinant | Dimension $n \pmod 4$ | | | |
|---|---|---|---|---|
| $\rho \pmod 4$ | 0 | 1 | 2 | 3 |
| 1 | $(0,4)$ | $(1,5)$ | $(2,6)$ | $(7,3)$ |
| 3 | $(2,6)$ | $(7,3)$ | $(0,4)^\dagger$ | $(1,5)$ |

Table 2.1: The octane values $(\mathfrak{o}_n(\rho)^+, \mathfrak{o}_n(\rho)^-)$, as a function of $n \pmod 4$ and $\rho \pmod 4$. The superscript $^\dagger$ indicates that when $n = 2$ and $\rho \equiv 3 \pmod 4$, there is just one option for the octane value, namely $\mathfrak{o}_2(\rho)^+ = \mathfrak{o}_2(\rho)^- = 0$.

For each $G_n(\mathbb{Z}_2)$-equivalence class of Type I symmetric $n \times n$ matrices, determinant $\rho$, and octane value $\mathfrak{o}_n(\rho)^\pm$, we pick a representative and denote it by $A_n[\rho]^\pm$.

#### 2.5.3.3 Case $(ii)$: $p = 2$, $r = 1$

By [109, Theorem 80], if $(A, B) \in W_n(\mathbb{Z}_2)$ is such that $A$ is a unit-determinant symmetric bilinear form of Type II, then $\iota(A, B)$ is evenly ramified. Since forms $F \in \Sigma_2$ are necessarily separable modulo 2, their monicizations are not evenly ramified, so we may assume that $A_0$ is of Type I. (For a partial treatment of the case where $F$ is inseparable modulo 2, see Appendix 2.A.) By §2.5.3.2, we have *two* options, namely $A_n\left[(-1)^{\lfloor \frac{n}{2} \rfloor}\right]^\pm$, for the $G_n(\mathbb{Z}_2)$-equivalence class of $A_0$. We now split into sub-cases depending on the parity of $f_0$.

*Case $(ii)(a)$: $2 \nmid f_0$.* Let $\rho \in \mathbb{Z}_2^\times$, and let $\mathcal{S} \subset V_{n,f_0}(\mathbb{Z}_2)_{\max}$. The next result determines the quantity $\mathcal{J}(A_n[\rho]^\pm, \mathcal{S})$ for "acceptable" choices of the set $\mathcal{S}$:

**Proposition 57.** *Let $n \geq 2$. With notation as above, suppose that $\mathcal{S}$ is the preimage in*

$V_{n,f_0}(\mathbb{Z}_2)$ *of a set of separable forms in* $V_{n,f_0}(\mathbb{Z}/2\mathbb{Z})$. *Then we have*

$$\frac{\mathcal{J}(A_n[\rho]^{\pm},\mathcal{S})}{\mathrm{Vol}(\mathcal{S})} = \begin{cases} 2^{\frac{n-2}{2}}\left(2^{\frac{n-2}{2}}\pm 1\right), & \text{if } (\mathfrak{o}_n(\rho)^+,\mathfrak{o}_n(\rho)^-) = (0,4), \\ 2^{\frac{n-3}{2}}\left(2^{\frac{n-1}{2}}\pm 1\right), & \text{if } (\mathfrak{o}_n(\rho)^+,\mathfrak{o}_n(\rho)^-) = (1,5), \\ 2^{n-2}, & \text{if } (\mathfrak{o}_n(\rho)^+,\mathfrak{o}_n(\rho)^-) = (2,6), \\ 2^{\frac{n-3}{2}}\left(2^{\frac{n-1}{2}}\mp 1\right), & \text{if } (\mathfrak{o}_n(\rho)^+,\mathfrak{o}_n(\rho)^-) = (7,3), \\ 2, & \text{if } n=2 \text{ and } (\mathfrak{o}_2(\rho)^+,\mathfrak{o}_2(\rho)^-) = (0,0). \end{cases} \tag{2.50}$$

*Proof.* When $f_0 = 1$ and $n \geq 3$, this is proven in [108, Corollary 80] and [109, Corollary 113], and one checks the proof goes through when $f_0 \in \mathbb{Z}_2^\times$ is any unit, and even when $n = 2$. □

Note in particular that the values on the right-hand side of (2.50) are independent of the choice of $\mathcal{S}$. In what follows, if $A \in U_n(\mathbb{Z}_2)$ is $G_n(\mathbb{Z}_2)$-equivalent to $A_n[\rho]^{\pm}$, we write $\chi_2(A)$ for the corresponding value on the right-hand side of (2.50). Proposition 57 then implies that

$$\mathcal{J}(A_0,\Sigma_2) = \mathrm{Vol}(\Sigma_2)\cdot\chi_2(A_0). \tag{2.51}$$

*Case (ii)(b):* $2 \mid f_0$. In this case, the monicizations of forms in $\Sigma_2$ are necessarily *inseparable* modulo 2, and so the argument in Case (ii)(a) does not immediately apply. Instead, we will reduce to the setting of Case (ii)(a) as follows.

Take $f \in \Sigma_2$, let $f = \prod_{i=1}^k F_i$ be a canonical factorization of $f$, and let $(I,\alpha) \in H^*_{f,1}$. Recall the notation from the proof of Case 2 of Theorem 18. Then one easily checks that the map sending $(A,B)$ to $(A_{f/F_1}, f_0^{-1}B_{f/F_1})$ induces a bijection

$$\mathsf{orb}_{f,1}(H^*_{f,1}) \leftrightsquigarrow \bigsqcup_{\rho\in\{1,3,5,7\}} \mathsf{orb}_{f/F_1,(-1)^n\rho^{-1}}\left(H^*_{f/F_1,(-1)^n\rho^{-1}}\right) \tag{2.52}$$

Using the bijection in (2.52) to evaluate $\mathcal{J}\big(A_n\big[(-1)^{\lfloor\frac{n}{2}\rfloor}\big]^{\pm},\Sigma_2\big)$, we find that

$$\mathcal{J}\big(A_n\big[(-1)^{\lfloor\frac{n}{2}\rfloor}\big]^{\pm},\Sigma_2\big) = \tag{2.53}$$
$$\frac{1}{2}\,|f_0|^{\frac{n(n-1)}{2}} \sum_{\rho\in\{1,3,5,7\}} \begin{cases} \mathcal{J}\big(A_{n-1}\big[(-1)^{\lfloor\frac{n}{2}\rfloor}\rho^{-1}\big]^{\pm},\Sigma_2'\big), & \text{if } \rho\equiv 1\,(\mathrm{mod}\,4),\\ \mathcal{J}\big(A_{n-1}\big[(-1)^{\lfloor\frac{n}{2}\rfloor}\rho^{-1}\big]^{\mp},\Sigma_2'\big), & \text{if } \rho\equiv 3\,(\mathrm{mod}\,4), \end{cases}$$

where the factor of $\frac{1}{2}$ accounts for the fact that $G_n$ switches between $\mathrm{SL}_n$ and $\mathrm{SL}_n^{\pm}$ depending on the parity of $n$, and where $\Sigma_2'\subset V_{n-1,1}(\mathbb{Z}_2)_{\max}$ is the preimage of the set $\{\overline{f}/\overline{F}_1 : f\in\Sigma_2\}\subset V_{n-1,1}(\mathbb{Z}/2\mathbb{Z})$. Because $\Sigma_2$ is "acceptable," every element of $\Sigma_2'$ is separable modulo 2, so we can use Proposition 57 to compute the right-hand side of (2.53). Upon doing so, and upon observing that $\mathrm{Vol}(\Sigma_2')=\mathrm{Vol}(\Sigma_2)$, we deduce that

$$\mathcal{J}(A_0,\Sigma_2) = |f_0|_2^{\frac{n(n-1)}{2}}\cdot\mathrm{Vol}(\Sigma_2)\cdot\chi_2(A_0). \tag{2.54}$$

#### 2.5.3.4 Case (*iii*): $p=2$, $r=-1$

By §2.5.3.2, we have *two* options, namely $A_n\big[(-1)^{1+\lfloor\frac{n}{2}\rfloor}\big]^{\pm}$, for the $G_n(\mathbb{Z}_2)$-equivalence class of $A_0$. But $A_n\big[(-1)^{1+\lfloor\frac{n}{2}\rfloor}\big]^{+}$ is $G_n(\mathbb{Z}_2)$-equivalent to $-A_n\big[(-1)^{1+\lfloor\frac{n}{2}\rfloor}\big]^{-}$, so the map $(A,B)\mapsto(-A,-B)$ defines a bijection between the $G_n(\mathbb{Z}_2)$-orbits of $(A,B)\in\mathsf{orb}_{f,-1}(H^*_{f,-1})$ such that $A$ is $G_n(\mathbb{Z}_2)$-equivalent to $A_n\big[(-1)^{1+\lfloor\frac{n}{2}\rfloor}\big]^{+}$ and the $G_n(\mathbb{Z}_2)$-orbits of $(A,B)\in\mathsf{orb}_{f,-1}(H^*_{f,-1})$ such that $A$ is $G_n(\mathbb{Z}_2)$-equivalent to $A_n\big[(-1)^{1+\lfloor\frac{n}{2}\rfloor}\big]^{-}$. By Theorem 39, we have

$$\#\mathsf{orb}_{f,-1}(H^*_{f,-1}) = 2^{n-2}\#R_f^{\times}[2] = 2^{m+n-2}$$

and that $\#\,\mathrm{Stab}_{\mathcal{G}_{A_0}(\mathbb{Z}_2)}(T)=\#R_f^{\times}[2]=2^m$ for every $T\in\mathcal{G}_{A_0}\backslash W_{A_0}(\Sigma_2)$, so

$$\mathcal{J}(A_0,\Sigma_2) = |f_0|_2^{\frac{n(n-1)}{2}}\cdot\mathrm{Vol}(\Sigma_2)\cdot\chi_2(A_0). \tag{2.55}$$

Comparing (2.51), (2.54), and (2.55), we see that (2.55) holds regardless of whether or not $2 \mid f_0$ or $r = \pm 1$.

### 2.5.4 The final step

We now combine the calculations of the local factors in §2.5.3 with the asymptotic from Theorem 55 to prove the results in §2.1.1.

*Proof of Theorem 24.* Fix an odd integer $n \geq 3$ and a real signature $(r_1, r_2)$ of a degree-$n$ field. Let $\Sigma$ be an acceptable family of local specifications such that $V_{n,f_0}(\Sigma) \subset V_{n,f_0}(\mathbb{Z})^{r_1,r_2}_{\max}$. Given an irreducible form $f \in V_{n,f_0}(\Sigma)$, the set $\mathsf{orb}_{f,1}(H^*_{f,1})$ splits as

$$\mathsf{orb}_{f,1}(H^*_{f,1}) = \mathsf{orb}_{f,1}(H^*_{f,1})^{\mathrm{irr}} \sqcup \mathsf{orb}_{f,1}(H^*_{f,1})^{\mathrm{red}}, \tag{2.56}$$

where $\mathsf{orb}_{f,1}(H^*_{f,1})^{\mathrm{irr}}$ is the subset of $G_n(\mathbb{Z})$-orbits that are non-distinguished over $\mathbb{Q}$ and where $\mathsf{orb}_{f,1}(H^*_{f,1})^{\mathrm{red}}$ is its complement.

Let $f_0$ factor as $f_0 = m^2 k$ where $k$ is squarefree, and let $r_p(\Sigma)$ be defined as in Theorem 24. It follows from Propositions 45, 47, 48, and 50, and Theorem 53 that, on the one hand,

$$\sum_{f \in V_{n,f_0}(\Sigma)_X} \#\mathsf{orb}_{f,1}(H^*_{f,1})^{\mathrm{red}} = \tag{2.57}$$
$$\mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X) \cdot \prod_p \mathrm{Vol}(\Sigma_p) \cdot \prod_{p \mid k} r_p(\Sigma) + o\big(X^{\frac{n(n+1)}{2}-1}\big).$$

Let $\mathscr{L}^+_{\mathbb{Z}}$ denote the set of $G_n(\mathbb{Z})$-equivalence classes of symmetric $n \times n$ integer matrices of determinant $(-1)^{\lfloor \frac{n}{2} \rfloor}$. On the other hand, combining Theorem 55 with (2.46), (2.49), and (2.55), simplifying the result using the identity $|f_0| \prod_p |f_0|_p = 1$, and rearranging yields:

$$\sum_{f \in V_{n,f_0}(\Sigma)_X} \#\mathsf{orb}_{f,1}(H^*_{f,1})^{\mathrm{irr}} = \sum_{A_0 \in \mathscr{L}^+_{\mathbb{Z}}} \sum_{\sigma} \#\big((N \times \mathcal{G}_{A_0})(\mathbb{Z})\backslash(W_{A_0}(\Sigma)^\sigma)^{\mathrm{irr}}_X\big) \tag{2.58}$$

$$\leq 2^{1-r_1-r_2} \cdot \mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X) \cdot \prod_p \mathrm{Vol}(\Sigma_p) \cdot$$
$$\sum_{A_0 \in \mathscr{L}_{\mathbb{Z}}^+} \tau_{\mathcal{G}_{A_0}} \cdot \chi_2(A_0) \cdot \sum_\sigma \chi_{A_0}(\sigma) + o\big(X^{\frac{n(n+1)}{2}-1}\big).$$

The fact that the parametrization in §1.4.1 reduces the non-monic case to the monic case now pays dividends: the sum over $A_0 \in \mathscr{L}_{\mathbb{Z}}^+$ in the third line of (2.58) arises in the work of Siad, so we need not re-compute it. Indeed, it follows from [108, §9, p. 35] that

$$\sum_{A_0 \in \mathscr{L}_{\mathbb{Z}}^+} \tau_{\mathcal{G}_{A_0}} \cdot \chi_2(A_0) \cdot \sum_\sigma \chi_{A_0}(\sigma) = 2^{n+r_1-2} + 2^{\frac{n+r_1-2}{2}} = \big(2^{r_1+r_2-1}\big)^2 + 2^{r_1+r_2-1}. \tag{2.59}$$

Substituting (2.59) into (2.58), we find that

$$\sum_{f \in V_{n,f_0}(\Sigma)_X} \#\mathsf{orb}_{f,1}(H_{f,1}^*)^{\mathrm{irr}} \leq \tag{2.60}$$
$$\big(1 + 2^{r_1+r_2-1}\big) \cdot \mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X) \cdot \prod_p \mathrm{Vol}(\Sigma_p) + o\big(X^{\frac{n(n+1)}{2}-1}\big).$$

Using Theorem 53 together with (2.56), (2.57), and (2.60), we find that

$$\operatorname*{Avg}_{f \in V_{n,f_0}(\Sigma)} \#\mathsf{orb}_{f,1}(H_{f,1}^*) \leq$$
$$\lim_{X \to \infty} \frac{\Big(1 + 2^{r_1+r_2-1} + \prod_{p|k} r_p(\Sigma)\Big) \cdot \mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X) \cdot \prod_p \mathrm{Vol}(\Sigma_p)}{\mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X) \cdot \prod_p \mathrm{Vol}(\Sigma_p)} =$$
$$1 + 2^{r_1+r_2-1} + \prod_{p|k} r_p(\Sigma). \tag{2.61}$$

The inequalities above are equalities when the estimate (2.45) holds. Theorem 24 then follows from substituting the bound in (2.61) into the formula in Lemma 33. □

*Proof of Theorem 26.* Fix an even integer $n \geq 4$ and a real signature $(r_1, r_2)$ of a degree-$n$ field. Let $\Sigma$ be an acceptable family of local specifications such that $V_{n,f_0}(\Sigma) \subset V_{n,f_0}(\mathbb{Z})^{r_1,r_2}_{\max}$. Given an irreducible form $F \in V_{n,f_0}(\Sigma)$, (2.56) continues to hold in this setting. It follows

from Proposition 45 and Remark 46 that

$$\sum_{f\in V_{n,f_0}(\Sigma)_X} \#\mathsf{orb}_{f,1}(H_{f,1}^*)^{\mathrm{red}} = \sum_{f\in V_{n,f_0}(\Sigma)_X} 2^{\#\mathsf{ev}_f+1} + o\big(X^{\frac{n(n+1)}{2}}\big). \tag{2.62}$$

The following proposition gives a formula for the sum on the right-hand side of (2.62):

**Proposition 58.** *We have that*

$$\sum_{f\in V_{n,f_0}(\Sigma)_X} 2^{\#\mathsf{ev}_f+1} = 2\cdot \mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X)\cdot\prod_p \mathrm{Vol}(\Sigma_p)\cdot(1+r_p(\Sigma)) + o\big(X^{\frac{n(n+1)}{2}}\big). \tag{2.63}$$

*Proof of Proposition 58.* Let $M>0$ be a constant. First, it is clear that (2.63) holds if we make the following adjustments: (1) replace $\mathsf{ev}_f$ with $\{p\in\mathsf{ev}_f : p<M\}$, and (2) remove the factor $1+r_p(\Sigma)$ for each prime $p>M$. Taking the limit as $M\to\infty$, we see that (2.63) holds with "$\geq$" instead of "=." It thus remains to prove (2.63) with "$\leq$" instead of "=."

Let $\delta,\varepsilon>0$ be constants. Since even ramification is a codimension-$\frac{n}{2}$ condition on $V_{n,f_0}$, an application of the geometric sieve (see [12, proof of Theorem 3.3], as well as the paragraph concerning inhomogeneous heights in [29, p. 4]) yields

$$\#\left\{f\in V_{n,f_0}(\mathbb{Z})_X : \begin{array}{c}\exists \text{ squarefree } m\in\mathbb{Z} \text{ s. t. } m>X^\delta \\ \text{and } p\in\mathsf{ev}_f \text{ for every } p\mid m\end{array}\right\} \ll \frac{X^{\frac{n(n+1)}{2}-1}}{X^{\delta\frac{n-2}{2}}} + X^{\frac{n^2}{2}+\varepsilon}. \tag{2.64}$$

Now, if $\mathrm{H}(f)<X$, the number of prime factors of the discriminant of $f$ is $O(\log X/\log\log X)$, so on the left-hand side of (2.63), each $f$ is counted with multiplicity at most $2^{O(\log X/\log\log X)} = O(X^\varepsilon)$. Combining this bound with (2.64), we see that forms $f$ that are evenly ramified at a set of primes whose product exceeds $X^\delta$ contribute negligibly to the left-hand side of (2.63).

Let $r_p(\Sigma)$ be defined as in Theorem 26, let $M>0$ be a constant, and let $\Pi$ be the set of squarefree numbers up to $X^\delta$. We now bound the contribution from forms $f$ that are evenly

ramified at a set of primes whose product is at most $X^\delta$. We have

$$\sum_{\substack{f\in V_{n,f_0}(\Sigma)_X \\ \prod_{p\in \mathsf{ev}_f} p\le X^\delta}} 2^{\#\mathsf{ev}_f} \le$$

$$\mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X)\cdot\prod_{p<M}\mathrm{Vol}(\Sigma_p)\cdot\sum_{m\in\Pi}\Big[\prod_{p|m} r_p(\Sigma)+O\big(X^{\frac{n(n+1)}{2}-3}\big)\Big]\le$$

$$\mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X)\cdot\prod_{p<M}\mathrm{Vol}(\Sigma_p)\cdot\prod_{p}(1+r_p(\Sigma))+o\big(X^{\frac{n(n+1)}{2}-1}\big). \tag{2.65}$$

Taking the limit as $M\to\infty$ in (2.65) proves (2.63) with "=" replaced by "$\le$." □

Let $\mathscr{L}_{\mathbb{Z}}^+$ denote the set of $G_n(\mathbb{Z})$-equivalence classes of symmetric $n\times n$ integer matrices of determinant $(-1)^{\lfloor\frac{n}{2}\rfloor}$. On the other hand, combining Theorem 55 with (2.46), (2.49), and (2.55), simplifying the result using the identity $|f_0|\prod_p|f_0|_p=1$, and rearranging yields:

$$\sum_{f\in V_{n,f_0}(\Sigma)_X}\#\mathsf{orb}_{f,1}(H_{f,1}^*)^{\mathrm{irr}}=\sum_{A_0\in\mathscr{L}_{\mathbb{Z}}^+}\sum_{\sigma}\#\big((N\times\mathcal{G}_{A_0})(\mathbb{Z})\backslash(W_{A_0}(\Sigma)^\sigma)_X^{\mathrm{irr}}\big) \tag{2.66}$$

$$\le 2^{1-r_1-r_2}\cdot\mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X)\cdot\prod_p\mathrm{Vol}(\Sigma_p)\cdot(1+r_p(\Sigma))\cdot$$

$$\sum_{A_0\in\mathscr{L}_{\mathbb{Z}}^+}\tau_{\mathcal{G}_{A_0}}\cdot\chi_2(A_0)\cdot\sum_\sigma\chi_{A_0}(\sigma)+o\big(X^{\frac{n(n+1)}{2}-1}\big).$$

Again, the sum over $A_0\in\mathscr{L}_{\mathbb{Z}}^+$ in the third line of (2.66) arises in the work of Siad, so we need not re-compute it. Indeed, it follows from [109, §10.1, p. 35 and §11.7, p. 45] that

$$\sum_{A_0\in\mathscr{L}_{\mathbb{Z}}^+}\tau_{\mathcal{G}_{A_0}}\cdot\chi_2(A_0)\cdot\sum_\sigma\chi_{A_0}(\sigma)= \tag{2.67}$$

$$\begin{cases}2^{n-1}+2^{\frac{n}{2}}=2^{2r_2-1}+2^{r_2}, & \text{if } r_1=0,\\ 2^{n+r_1-2}+2^{\frac{n+r_1}{2}}=\big(2^{r_1+r_2-1}\big)^2+2^{r_1+r_2}, & \text{if } r_1>0.\end{cases}$$

Substituting (2.67) into (2.66), we find that

$$\sum_{f\in V_{n,f_0}(\Sigma)_X} \#\mathsf{orb}_{f,1}(H^*_{f,1})^{\mathrm{irr}} \leq \left\{\begin{array}{ll} 2+2^{r_2}, & \text{if } r_1=0,\\ 2+2^{r_1+r_2-1}, & \text{if } r_1>0 \end{array}\right\} \cdot \mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X)\cdot \prod_p \mathrm{Vol}(\Sigma_p)\cdot(1+r_p(\Sigma)) + o\big(X^{\frac{n(n+1)}{2}-1}\big). \tag{2.68}$$

Using Theorem 53 together with (2.56), (2.62), and (2.68), we find that

$$\begin{aligned} &\operatorname*{Avg}_{f\in V_{n,f_0}(\Sigma)} \#\mathsf{orb}_{f,1}(H^*_{f,1}) \leq \\ &\lim_{X\to\infty} \frac{\left\{\begin{array}{ll} 4+2^{r_2}, & \text{if } r_1=0,\\ 4+2^{r_1+r_2-1}, & \text{if } r_1>0 \end{array}\right\} \cdot \mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X)\cdot\prod_p \mathrm{Vol}(\Sigma_p)\cdot(1+r_p(\Sigma))}{\mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X)\cdot\prod_p \mathrm{Vol}(\Sigma_p)} = \\ &\left\{\begin{array}{ll} 4+2^{r_2}, & \text{if } r_1=0,\\ 4+2^{r_1+r_2-1}, & \text{if } r_1>0 \end{array}\right\} \cdot \prod_{p>2}(1+r_p(\Sigma)). \end{aligned} \tag{2.69}$$

Having dealt with the average of $\#\mathsf{orb}_{f,1}(H^*_{f,1})$, we now turn our attention to the average of $\#\mathsf{orb}_{f,-1}(H^*_{f,-1})$. Since $\#\mathsf{orb}_{f,-1}(H^*_{f,-1})=0$ if $r_1=0$, assume $r_1>0$, and let $f\in V_{n,f_0}(\Sigma)$ be irreducible. As explained in §2.4.1, every element of $\mathsf{orb}_{f,-1}(H^*_{f,-1})$ is non-distinguished. Thus, if we let $\mathscr{L}^-_{\mathbb{Z}}$ denote the set of $G_n(\mathbb{Z})$-equivalence classes of symmetric $n\times n$ integer matrices of determinant $(-1)^{1+\lfloor\frac{n}{2}\rfloor}$, then combining Theorem 55 with (2.46), (2.49), and (2.55), simplifying the result using the identity $|f_0|\prod_p |f_0|_p=1$, and rearranging yields:

$$\begin{aligned} &\sum_{f\in V_{n,f_0}(\Sigma)_X} \#\mathsf{orb}_{f,-1}(H^*_{f,-1}) = \sum_{A_0\in\mathscr{L}^-_{\mathbb{Z}}}\sum_{\sigma} \#\big((N\times\mathcal{G}_{A_0})(\mathbb{Z})\backslash(W_{A_0}(\Sigma)^\sigma)^{\mathrm{irr}}_X\big) \leq \\ &2^{1-r_1-r_2}\cdot\mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X)\cdot\prod_p \mathrm{Vol}(\Sigma_p)\cdot\big(1+(-1)^{\frac{p-1}{2}}\cdot r_p(\Sigma)\big)\cdot \\ &\qquad\qquad \sum_{A_0\in\mathscr{L}^-_{\mathbb{Z}}} \tau_{\mathcal{G}_{A_0}}\cdot\chi_2(A_0)\cdot\sum_\sigma \chi_{A_0}(\sigma) + o\big(X^{\frac{n(n+1)}{2}-1}\big). \end{aligned} \tag{2.70}$$

Again, the sum over $A_0 \in \mathscr{L}_{\mathbb{Z}}^-$ in the third line of (2.70) arises in the work of Siad on monic forms, so we need not re-compute it. Indeed, it follows from [109, §11.7, p. 45] that

$$\sum_{A_0 \in \mathscr{L}_{\mathbb{Z}}^-} \tau_{\mathcal{G}_{A_0}} \cdot \chi_2(A_0) \cdot \sum_{\sigma} \chi_{A_0}(\sigma) = 2^{n+r_1-2} = \left(2^{r_1+r_2-1}\right)^2. \tag{2.71}$$

Substituting (2.71) into (2.70), we find that

$$\sum_{f \in V_{n,f_0}(\Sigma)_X} \#\mathsf{orb}_{f,-1}(H_{f,-1}^*) \leq 2^{r_1+r_2-1} \cdot \mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X) \cdot \tag{2.72}$$
$$\prod_p \mathrm{Vol}(\Sigma_p) \cdot \left(1 + (-1)^{\frac{p-1}{2}} \cdot r_p(\Sigma)\right) + o\left(X^{\frac{n(n+1)}{2}-1}\right).$$

Using Theorem 53 together with (2.72), we find that

$$\begin{aligned} &\operatorname*{Avg}_{f \in V_{n,f_0}(\Sigma)} \#\mathsf{orb}_{f,-1}(H_{f,-1}^*) \leq \\ &\lim_{X \to \infty} \frac{2^{r_1+r_2-1} \cdot \mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X) \cdot \prod_p \mathrm{Vol}(\Sigma_p) \cdot \left(1 + (-1)^{\frac{p-1}{2}} \cdot r_p(\Sigma)\right)}{\mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X) \cdot \prod_p \mathrm{Vol}(\Sigma_p)} = \\ &2^{r_1+r_2-1} \cdot \prod_{p>2} \left(1 + (-1)^{\frac{p-1}{2}} \cdot r_p(\Sigma)\right). \end{aligned} \tag{2.73}$$

The inequalities above are equalities when the estimate (2.45) holds. The statements about the class group in (2.7) and (2.8) then follow from substituting the bound in (2.69), as well as the bound in (2.73) (or simply 0 when $r_1 = 0$), into the formula in Lemma 34. Since we have that $\#\,\mathrm{Cl}(R_f)[2] = \#\,\mathrm{Cl}^+(R_f)[2]$ when $r_1 = 0$, the statement about the narrow class group in (2.7) follows from the corresponding statement about the class group.

We now consider the average of $\#\mathsf{orb}_{f,1}(H_{f,1}^{*,+})$. Let $r_1 > 0$, and let $f \in V_{n,f_0}(\Sigma)$. The set $\mathsf{orb}_{f,1}(H_{f,1}^{*,+})$ splits as

$$\mathsf{orb}_{f,1}(H_{f,1}^{*,+}) = \mathsf{orb}_{f,1}(H_{f,1}^{*,+})^{\mathrm{irr}} \sqcup \mathsf{orb}_{f,1}(H_{f,1}^{*,+})^{\mathrm{red}}, \tag{2.74}$$

where $\mathsf{orb}_{f,1}(H_{f,1}^{*,+})^{\mathrm{irr}}$ is the subset of $G_n(\mathbb{Z})$-orbits that are non-distinguished over $\mathbb{Q}$ and

where $\mathsf{orb}_{f,1}(H_{f,1}^{*,+})^{\mathrm{red}}$ is its complement. Because the elements of $\mathsf{orb}_{f,1}(H_{f,1}^{*,+})^{\mathrm{red}}$ are distinguished over $\mathbb{Q}$, they are necessarily distinguished over $\mathbb{R}$, so under the identification (2.41), they all correspond to the same totally positive element $\sigma_0 = (1, \dots, 1) \in (\mathbb{R}^\times/\mathbb{R}^{\times 2})^{r_1}$. By the proof of Proposition 45 and the remark following it, the set $\mathsf{orb}_{f,1}(H_{f,1}^{*,+})^{\mathrm{red}}$ has size $2^{\#\mathsf{ev}_f}$ for 100% of forms $f$. It then follows from Theorem 53 and Proposition 58 that, on the one hand, we have

$$\begin{aligned}\sum_{f \in V_{n,f_0}(\Sigma)_X} \#\mathsf{orb}_{f,1}(H_{f,1}^{*,+})^{\mathrm{red}} &= \sum_{f \in V_{n,f_0}(\Sigma)_X} 2^{\#\mathsf{ev}_f} + o\big(X^{\frac{n(n+1)}{2}}\big) \\ &= \mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X) \cdot \prod_p \mathrm{Vol}(\Sigma_p) \cdot (1 + r_p(\Sigma)) + o\big(X^{\frac{n(n+1)}{2}}\big).\end{aligned} \tag{2.75}$$

On the other hand, combining Theorem 55 with (2.46), (2.49), and (2.55), simplifying the result using the identity $|f_0| \prod_p |f_0|_p = 1$, and rearranging yields:

$$\begin{aligned}\sum_{f \in V_{n,f_0}(\Sigma)_X} \#\mathsf{orb}_{f,1}(H_{f,1}^{*,+})^{\mathrm{irr}} &= \sum_{A_0 \in \mathscr{L}_{\mathbb{Z}}^+} \#\big((N \times \mathcal{G}_{A_0})(\mathbb{Z})\backslash(W_{A_0}(\Sigma)^{\sigma_0})_X^{\mathrm{irr}}\big) \\ &\le 2^{1-r_1-r_2} \cdot \mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X) \cdot \prod_p \mathrm{Vol}(\Sigma_p) \cdot (1 + r_p(\Sigma)) \cdot \\ &\qquad \sum_{A_0 \in \mathscr{L}_{\mathbb{Z}}^+} \tau_{\mathcal{G}_{A_0}} \cdot \chi_2(A_0) \cdot \chi_{A_0}(\sigma_0) + o\big(X^{\frac{n(n+1)}{2}-1}\big).\end{aligned} \tag{2.76}$$

Once again, the sum over $A_0 \in \mathscr{L}_{\mathbb{Z}}^+$ in the third line of (2.66) arises in the work of Siad on monic forms, so we need not re-compute it. Indeed, it follows from [109, §10.1, p. 35 and §11.7, p. 45] that

$$\sum_{A_0 \in \mathscr{L}_{\mathbb{Z}}^+} \tau_{\mathcal{G}_{A_0}} \cdot \chi_2(A_0) \cdot \chi_{A_0}(\sigma_0) = 2^{n-1} + 2^{\frac{n}{2}} = 2^{r_1+2r_2-1} + 2^{\frac{r_1+2r_2}{2}}. \tag{2.77}$$

Substituting (2.77) into (2.76), we find that

$$\sum_{f \in V_{n,f_0}(\Sigma)_X} \#\mathsf{orb}_{f,1}(H_{f,1}^{*,+})^{\mathrm{irr}} \le \big(2^{r_2} + 2^{\frac{2-r_1}{2}}\big) \cdot \mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X) \cdot \tag{2.78}$$

$$\prod_p \mathrm{Vol}(\Sigma_p)\cdot(1+r_p(\Sigma)) + o\big(X^{\frac{n(n+1)}{2}-1}\big).$$

Using Theorem 53 together with (2.74), (2.75), and (2.78), we find that

$$\begin{aligned}
&\operatorname*{Avg}_{f\in V_{n,f_0}(\Sigma)} \#\mathsf{orb}_{f,1}(H^{*,+}_{f,1}) \leq \\
&\lim_{X\to\infty} \frac{\big(1+2^{r_2}+2^{\frac{2-r_1}{2}}\big)\cdot \mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X)\cdot\prod_p \mathrm{Vol}(\Sigma_p)\cdot(1+r_p(\Sigma))}{\mathrm{Vol}(N(\mathbb{Z})\backslash(\Sigma_\infty)_X)\cdot\prod_p \mathrm{Vol}(\Sigma_p)} = \\
&\big(1+2^{r_2}+2^{\frac{2-r_1}{2}}\big)\cdot\prod_{p>2}(1+r_p(\Sigma)). \qquad (2.79)
\end{aligned}$$

The inequalities above are equalities when the estimate (2.45) holds. The statement about the narrow class group in (2.9) follows from substituting the bound in (2.79) into the formula in Lemma 35. □

## 2.A Appendix: 2-adic orbit counting via 2-descent

In this section, we take $n$ and $f_0$ to be odd, fix $f \in V_{n,f_0}(\mathbb{Z}_2)_{\max}$, and prove:

**Proposition 59.** *The number of $G_n(\mathbb{Z}_2)$-orbits of pairs $(A,B)\in \mathsf{orb}_{f,1}(H^*_{f,1})$ such that $A$ is $G_n(\mathbb{Z}_2)$-equivalent to $A_n\big[(-1)^{\lfloor\frac{n}{2}\rfloor}\big]^{\pm}$ is $2^{m+\frac{n-5}{2}}\big(2^{\frac{n-1}{2}}\pm 1\big)$.*

*Proof.* The proof proceeds by using the connection established in [15] between studying 2-torsion ideal classes of the ring $R_{f^{\mathsf{mon}}}$ and performing a 2-descent on the Jacobian $J_{f^{\mathsf{mon}}}$ of the monic odd-degree hyperelliptic curve $y^2 = f^{\mathsf{mon}}(x,1)$.

Let $\mathscr{G}_{\mathbb{Q}_2} := \mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$, and for simplicity, abbreviate $A_n\big[(-1)^{\lfloor\frac{n}{2}\rfloor}\big]^{\pm}$ by $A^{\pm}$. Fix $(A',B')\in W_n(\mathbb{Q}_2)$ with $\iota(A',B') = f^{\mathsf{mon}}$ and with distinguished $G_n(\mathbb{Q}_2)$-orbit. Then [15, §4.1] implies that $A'$ is split over $\mathbb{Q}_2$ and is thus $G_n(\mathbb{Q}_2)$-equivalent to $A^+$. As shown in [15, §4.2], the set $(K_f^\times/K_f^{\times 2})_{\mathrm{N}\equiv 1}$ parametrizing $G_n(\mathbb{Q}_2)$-orbits of pairs $(A,B)\in W_n(\mathbb{Q}_2)$ with $\iota(A,B) = f^{\mathsf{mon}}$ (cf. Proposition 19) is identified with the Galois cohomology group $H^1(\mathscr{G}_{\mathbb{Q}_2}, \mathrm{Stab}_{G_n(\mathbb{Q}_2)}(A',B'))$. Composing this identification with the map on $H^1(\mathscr{G}_{\mathbb{Q}_2},-)$ induced by the inclusion of groups

$\mathrm{Stab}_{G_n(\mathbb{Q}_2)}(A', B') \hookrightarrow \mathcal{G}_{A^+}$ yields

$$(K_f^\times / K_f^{\times 2})_{\mathrm{N}\equiv 1} \simeq H^1(\mathscr{G}_{\mathbb{Q}_2}, \mathrm{Stab}_{G_n(\mathbb{Q}_2)}(A', B')) \to H^1(\mathscr{G}_{\mathbb{Q}_2}, \mathcal{G}_{A^+}). \tag{2.80}$$

By realizing $\mathcal{G}_{A^+}$ as the $\mu_2$-quotient of its universal cover, we get an isomorphism

$$H^1(\mathscr{G}_{\mathbb{Q}_2}, \mathcal{G}_{A^+}) \simeq H^1(\mathscr{G}_{\mathbb{Q}_2}, \mu_2). \tag{2.81}$$

Observing that $H^1(\mathscr{G}_{\mathbb{Q}_2}, \mu_2) \simeq \mathbb{Z}/2\mathbb{Z}$ and combining (2.80) and (2.81), we get a map

$$Q\colon (K_f^\times / K_f^{\times 2})_{\mathrm{N}\equiv 1} \to \mathbb{Z}/2\mathbb{Z}.$$

As is demonstrated in [15, §4.2 and §6.2], the zero-set of the map $Q$ consists precisely of the $G_n(\mathbb{Q}_2)$-orbits of pairs of the form $(A^+, B) \in W_n(\mathbb{Q}_2)$ such that $\iota(A, B) = f^{\mathsf{mon}}$.

Because we have assumed that $R_f = R_{f^{\mathsf{mon}}}$ is maximal, the obvious map

$$(R_f^\times / R_f^{\times 2})_{\mathrm{N}\equiv 1} \to (K_f^\times / K_f^{\times 2})_{\mathrm{N}\equiv 1} \tag{2.82}$$

is an inclusion. Then [15, §6.2] implies that if we precompose $Q$ with the inclusion (2.82) and identify $\mathsf{orb}_{f,1}(H_{f,1}^*)$ with $(R_f^\times / R_f^{\times 2})_{\mathrm{N}\equiv 1}$ via Theorem 39, then the zero-set of the resulting map

$$Q'\colon \mathsf{orb}_{f,1}(H_{f,1}^*) \to \mathbb{Z}/2\mathbb{Z},$$

which we denote by $\ker Q'$ (even though $Q'$ is not a group homomorphism), consists precisely of those orbits in $\mathsf{orb}_{f,1}(H_{f,1}^*)$ represented by pairs of the form $(A^+, B) \in W_n(\mathbb{Z}_2)$. Thus, the number of elements $(A, B) \in \mathsf{orb}_{f,1}(H_{f,1}^*)$ such that $A \simeq A^+$ (resp., $A^-$) is given by $\#\ker Q'$ (resp., $\#(\mathsf{orb}_{f,1}(H_{f,1}^*) \smallsetminus \ker Q')$). By Theorem 39, we have that $\#\mathsf{orb}_{f,1}(H_{f,1}^*) = 2^{m+n-2}$, where $m$ is the number of irreducible factors of $f$ over $\mathbb{Z}_2$, so it remains to compute $\#\ker Q'$.

As it happens, the map $Q$ is a nondegenerate even quadratic form on the $(\mathbb{Z}/2\mathbb{Z})$-vector

space $(K_f^\times/K_f^{\times 2})_{\mathrm{N}\equiv 1}$ with values in $\mathbb{Z}/2\mathbb{Z}$. Indeed, as explained in [15, §5.1], we have an identification $\mathrm{Stab}_{G_n(\mathbb{Q}_2)}(A,B) \simeq J_{f^{\mathsf{mon}}}[2]$ of group schemes over $\mathbb{Q}_2$, and $Q$ coincides via this identification with the following map induced by the Weil pairing $J_{f^{\mathsf{mon}}}[2] \times J_{f^{\mathsf{mon}}}[2] \to \mu_2$:

$$H^1(\mathscr{G}_{\mathbb{Q}_2}, J_{f^{\mathsf{mon}}}[2]) \to H^1(\mathscr{G}_{\mathbb{Q}_2}, \mu_2) \tag{2.83}$$

By [92, Proposition 4.10], the $(\mathbb{Z}/2\mathbb{Z})$-vector subspace

$$J_{f^{\mathsf{mon}}}(\mathbb{Q}_2)/2J_{f^{\mathsf{mon}}}(\mathbb{Q}_2) \hookrightarrow H^1(\mathscr{G}_{\mathbb{Q}_2}, J_{f^{\mathsf{mon}}}[2]) \tag{2.84}$$

is a maximal isotropic space for the quadratic form (2.83), and hence also for $Q$. The size of this maximal isotropic space is given by [113, Lemma 4.4] (cf. [15, §6.2]) to be $\#(J_{f^{\mathsf{mon}}}(\mathbb{Q}_2)/2J_{f^{\mathsf{mon}}}(\mathbb{Q}_2)) = 2^{m+\frac{n-3}{2}}$. Moreover, by [15, §8.2], the inclusion (2.84) factors through the inclusion (2.82), so $J_{f^{\mathsf{mon}}}(\mathbb{Q}_2)/2J_{f^{\mathsf{mon}}}(\mathbb{Q}_2)$ may be thought of as a $(\mathbb{Z}/2\mathbb{Z})$-vector subspace of $\mathsf{orb}_{f,1}(H^*_{f,1})$. Because $Q$ is even and nondegenerate, the rank of $Q'$ is given by

$$\operatorname{rk} Q' = 2\left(\dim_{\mathbb{Z}/2\mathbb{Z}}\left(\mathsf{orb}_{f,1}(H^*_{f,1})\right) - \dim_{\mathbb{Z}/2\mathbb{Z}}\left(J_{f^{\mathsf{mon}}}(\mathbb{Q}_2)/2J_{f^{\mathsf{mon}}}(\mathbb{Q}_2)\right)\right) = n-1.$$

It then follows from [82, Theorem 6.32] that

$$\begin{aligned} \#\ker Q' &= 2^{\dim_{\mathbb{Z}/2\mathbb{Z}}(\mathsf{orb}_{f,1}(H^*_{f,1}))-\operatorname{rk} Q'}\left(2^{\operatorname{rk} Q'-1} + 2^{\frac{\operatorname{rk} Q'-2}{2}}\right) \\ &= 2^{m+\frac{n-5}{2}}\left(2^{\frac{n-1}{2}}+1\right), \end{aligned} \tag{2.85}$$

and the size of its complement in $\mathsf{orb}_{f,1}(H^*_{f,1})$ is given by

$$\begin{aligned} \#(\mathsf{orb}_{f,1}(H^*_{f,1}) \smallsetminus \ker Q') &= 2^{m+n-2} - 2^{m+\frac{n-5}{2}}\left(2^{\frac{n-1}{2}}+1\right) \\ &= 2^{m+\frac{n-5}{2}}\left(2^{\frac{n-1}{2}}-1\right). \end{aligned} \tag{2.86}$$

□

*Remark* 60. When $n$ is even and $r = 1$, the 2-descent strategy used in §2.5.3.1 becomes far

more complicated: for instance, when $n \equiv 2 \pmod 4$, the analogue of the quadratic form $Q$ may fail to be even (see [91, Theorem 3.9 and Example 3.12]).

# Chapter 3

# Most odd-degree binary forms fail to primitively represent a square

This chapter is based on my paper [117].

## 3.1 Introduction

Let $f \in V_n(\mathbb{Z})$ be a separable integral binary form of degree $n \geq 5$. When $n$ is even, the subscheme $C_f$ of the weighted projective plane $\mathbb{P}^2_{\mathbb{Q}}(1, 1, \frac{n}{2})$ cut out by the equation $z^2 = f(x, y)$ is known as a *hyperelliptic curve*, and by Faltings' Theorem (see [63, Satz 7]), the curve $C_f$ has only finitely many rational points. In [11, Theorem 1], Bhargava established the following "strong asymptotic form" of Faltings' Theorem for hyperelliptic curves: when integral binary $n$-ic forms are ordered by height, the density of forms $f$ such that the curve $C_f$ has a rational point is $o(2^{-\frac{n}{2}})$. In other words, most even-degree binary forms fail to represent a square.

When $n$ is odd, the equation $z^2 = f(x, y)$ is called *superelliptic*. In contrast with the case of hyperelliptic curves, the problem of studying rational solutions to superelliptic equations

is trivial: given any pair $(x_0, y_0) \in \mathbb{Q}^2$, the triple

$$(x, y, z) = \left(x_0 f(x_0, y_0), y_0 f(x_0, y_0), f(x_0, y_0)^{\frac{n+1}{2}}\right) \in \mathbb{Q}^3 \tag{3.1}$$

is a solution to the equation $z^2 = f(x, y)$, and in fact, the subscheme $S_f \subset \mathbb{P}^2_{\mathbb{Q}}(2, 2, 2n+1)$ cut out by this equation is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$.

On the other hand, the problem of studying *primitive integer solutions*—i.e., triples $(x_0, y_0, z_0) \in \mathbb{Z}^3$ such that $z_0^2 = f(x_0, y_0)$ and $\gcd(x_0, y_0) = 1$—is considerably more interesting. For instance, a result of Darmon and Granville states that $z^2 = f(x, y)$ has only finitely many primitive integer solutions (see [53, Theorem 1']). Given this analogue of Faltings' Theorem, it is natural to expect that an analogue of Bhargava's strong asymptotic form holds for primitive integer solutions to superelliptic equations. The purpose of this chapter is to prove this expectation, i.e., that most integral odd-degree binary forms fail to *primitively* represent a square. Specifically, we prove that primitive integer solutions to $z^2 = f(x, y)$ give rise to square roots of the class of the inverse different of the ring $R_f$, and we apply the parametrization of such square roots developed in §1 to prove that most superelliptic equations $z^2 = f(x, y)$, where $f$ ranges over separable integral binary forms of sufficiently large odd degree $n$ with fixed leading coefficient $f_0 \in \mathbb{Z} \smallsetminus \pm\mathbb{Z}^2$, have no primitive integer solutions. We further show that most such equations have a Brauer–Manin obstruction to being soluble.

### 3.1.1 Superelliptic stacky curves

In the rest of this chapter, it will be convenient to reinterpret primitive integer solutions to the superelliptic equation $z^2 = f(x, y)$ as integral points on a certain *stacky curve*, which we denote by $\mathscr{S}_f$ and define as follows. Consider the punctured affine surface

$$\widetilde{S}_f := V(z^2 = f(x, y)) \subset \mathbb{A}^3_{\mathbb{Z}} \smallsetminus \{(0, 0, 0)\}. \tag{3.2}$$

The group $\mathbb{G}_m$ acts by scaling on $\widetilde{S}_f$ via $\lambda \cdot (x_0, y_0, z_0) = (\lambda^2 x_0, \lambda^2 y_0, \lambda^n z_0)$. The map $\widetilde{S}_f \to \mathbb{P}^1_{\mathbb{Z}}$ defined by $(x, y, z) \to [x : y]$ is $\mathbb{G}_m$-equivariant, and the field of $\mathbb{G}_m$-invariant rational functions on $\widetilde{S}_f$ is generated by $x/y$, so the scheme quotient $\widetilde{S}_f/\mathbb{G}_m$ is isomorphic to $\mathbb{P}^1_{\mathbb{Z}}$. The associated stack quotient $\mathscr{S}_f := [\widetilde{S}_f/\mathbb{G}_m]$ is a stacky curve with coarse moduli space $\mathbb{P}^1_{\mathbb{Z}}$. The $\mathbb{G}_m$-action on $\widetilde{S}_f$ has a nontrivial stabilizer isomorphic to the group scheme $\mu_2$ if and only if $z = 0$, so $\mathscr{S}_f$ has a "$\frac{1}{2}$-point" at each of the $n$ distinct roots of $f$ over the algebraic closure.

Let $R$ be a principal ideal domain. We say that a triple $(x_0, y_0, z_0)$ is *$R$-primitive* if we have $Rx_0 + Ry_0 = R$. The set of $R$-primitive solutions to $z^2 = f(x, y)$ is readily seen to be in bijection with the set $\widetilde{S}_f(R)$ of morphisms $\operatorname{Spec} R \to \widetilde{S}_f$ (i.e., $R$-points of $\widetilde{S}_f$), which in turn corresponds bijectively with the set $\mathscr{S}_f(R)$: indeed, specifying a map $\operatorname{Spec} R \to \mathscr{S}_f$ is definitionally equivalent to specifying a map $L \to \widetilde{S}_f$, where $L$ is a torsor of $\operatorname{Spec} R$ by $\mathbb{G}_m$, but $\operatorname{Spec} R$ has no nontrivial $\mathbb{G}_m$-torsors. In what follows, we abuse notation by writing $\mathscr{S}_f(R)$ for the set of $R$-primitive solutions to $z^2 = f(x, y)$, regardless of whether $f$ is separable.

### 3.1.2 Main results

Our results concern families of superelliptic equations $z^2 = f(x, z)$ of degree $n \geq 3$ having fixed leading coefficient $f_0 := f(1, 0) \in \mathbb{Z} \smallsetminus \{0\}$. Suppose that $|f_0|$ is not a square, factor $f_0$ as $f_0 = m^2 k$, where $k$ is squarefree, and define the following quantities:

$$\mu_{f_0} := \prod_{p|k} \left( \frac{1}{p^2} + \frac{p-1}{p^{\frac{n+1}{2}}} \right) \quad \text{and} \quad \mu'_{f_0} := \prod_{p|k} \left( 1 - \frac{1}{p^{2p+1}} \right)$$

For simplicity, we sometimes write $V_{n,f_0}(\mathbb{Z})$ to mean the family of superelliptic equations or superelliptic stacky curves defined by the forms in $V_{n,f_0}(\mathbb{Z})$. The *height* $H(f)$ of a binary form $f(x, y) = \sum_{i=0}^{n} f_i x^{n-i} y^i \in V_{n,f_0}(\mathbb{Z})$ is defined as follows

$$H(f) := \max\{|f_0^{i-1} f_i|^{n(n-1)/i} : i = 1, \ldots, n\}.$$

With this setup, we prove the following analogue for superelliptic stacky curves of [11, Theorem 1]:

**Theorem 61.** *For every sufficiently large odd integer $n$, most superelliptic stacky curves in the family $V_{n,f_0}(\mathbb{Z})$ have no primitive integer solutions. More precisely:*

(a) *Suppose $2 \nmid f_0$. For every odd integer $n \geq 11$, a positive proportion of forms $f \in V_{n,f_0}(\mathbb{Z})$, when ordered by height, have the property that $\mathscr{S}_f(\mathbb{Z}) = \varnothing$. Moreover, the lower density of forms $f \in V_{n,f_0}(\mathbb{Z})$ such that $\mathscr{S}_f(\mathbb{Z}) = \varnothing$ is at least $1 - \mu_{f_0} + o(2^{\frac{-n}{2}})$.*

(b) *Suppose $2 \mid f_0$. The lower density of forms $f \in V_{n,f_0}(\mathbb{Z})$ such that $\mathscr{S}_f(\mathbb{Z}) = \varnothing$ is at least $1 - \mu_{f_0} + O(2^{-\varepsilon_1 n^{\varepsilon_2}})$ for some real numbers $\varepsilon_1, \varepsilon_2 > 0$.*

As shown in Table 3.1, the quantity $1 - \mu_{f_0}$—which by Theorem 61 constitutes a lower bound on the density of insoluble equations in $V_{n,f_0}(\mathbb{Z})$ in the large-$n$ limit—rapidly approaches 1 as the number of prime factors of $k$ grows. Furthermore, the method used to prove Theorem 61 can be easily adapted to obtain a similar result when the family $V_{n,f_0}(\mathbb{Z})$ is replaced by any subfamily defined by congruence conditions modulo finitely many prime powers.

Note that Theorem 61 is subject to the condition that $|f_0|$ is *not* a square. When $|f_0|$ is a square, every form $f \in V_{n,f_0}(\mathbb{Z})$ is such that $z^2 = f(x, y)$ has a trivial solution, namely $(x, y, z) = (\text{sign}(f_0), 0, \sqrt{|f_0|})$. We expect that for most $f \in V_{n,f_0}(\mathbb{Z})$, the equation $z^2 = f(x, y)$ has no solutions other than the trivial one. The presence of the trivial solution renders this expectation difficult to prove: e.g., to obtain the analogous result for rational points on monic odd-degree hyperelliptic curves, Poonen and Stoll [94] combined work of Bhargava and Gross [15] on equidistribution of the 2-Selmer elements of the Jacobians of these curves with a variant of Chabauty's method (cf. [105], in which Shankar and Wang treat the even-degree case, as well as the work of Thorne and Romano [98] and Laga [79], which prove similar theorems for certain families of non-hyperelliptic curves). To the author's knowledge, analogues of the notion of Selmer group and of Chabauty's method remain to be formulated for superelliptic stacky curves.

| $\{p \mid k\} \supset$ | $\{2\}$ | $\{3\}$ | $\{5\}$ | $\{2,3\}$ | $\{2,5\}$ | $\{3,7\}$ | $\{2,3,7\}$ |
|---|---|---|---|---|---|---|---|
| $\lim_{n\to\infty} 1-\mu_{f_0} \geq$ | 75.0% | 88.8% | 96.0% | 97.2% | 99.0% | 99.7% | 99.9% |
| $\lim_{n\to\infty} \mu'_{f_0}-\mu_{f_0} \geq$ | 71.8% | 88.8% | 95.9% | 94.0% | 95.8% | 99.7% | 96.7% |

Table 3.1: A table demonstrating the strength of the limiting lower bounds $\lim_{n\to\infty} 1-\mu_{f_0}$ (resp., $\lim_{n\to\infty} \mu'_{f_0}-\mu_{f_0}$) on the density of insoluble superelliptic equations given by Theorem 61 (resp., on the density of superelliptic equations having a Brauer–Manin obstruction to solubility given by Theorem 62).

In the course of proving Theorem 61, we actually prove the stronger statement that most superelliptic stacky curves have a 2-descent obstruction to having an integral point. Since these stacky curves typically have integral points everywhere locally, it follows that most of them fail the Hasse principle (i.e., do *not* have a $\mathbb{Z}$-point despite having a $\mathbb{Z}_v$-point for every place $v$ of $\mathbb{Q}$) due to a 2-descent obstruction. Upon showing that such a 2-descent obstruction yields a case of the Brauer–Manin obstruction, we obtain the following analogue for superelliptic stacky curves of [11, Corollary 4] (see also the work of Thorne [119] and Thorne and Romano [97], which prove similar theorems for certain families of non-hyperelliptic curves):

**Theorem 62.** *The lower density of forms $f \in V_{n,f_0}(\mathbb{Z})$, when ordered by height, such that the stacky curve $\mathscr{S}_f$ fails the Hasse principle due to the Brauer–Manin obstruction is at least $\mu'_{f_0}-\mu_{f_0}+o(2^{-\frac{n}{2}})$ if $2 \nmid f_0$ and is at least $\mu'_{f_0}-\mu_{f_0}+O(2^{-\varepsilon_1 n^{\varepsilon_2}})$ for some $\varepsilon_1,\varepsilon_2>0$ if $2 \mid f_0$.*

The proportion $\mu'_{f_0}-\mu_{f_0}$, which can be thought of as a lower bound on the density of superelliptic equations with leading coefficient $f_0$ having a Brauer–Manin obstruction to solubility in the large-$n$ limit, approaches $\approx 96.7\%$ as the number of prime factors of $k$ grows; see Table 3.1.

The *genus* of a stacky curve can be defined in terms of the Euler characteristic of an orbifold curve; see [52, section entitled "Orbifolds, and the topology of $M$-curves"]. In [21], Bhargava and Poonen prove that all (suitably defined) stacky curves $S$ of genus less than $\frac{1}{2}$ over $\mathbb{Z}$ satisfy the Hasse principle; i.e., if $S(\mathbb{R}) \neq \varnothing$ and $S(\mathbb{Z}_p) \neq \varnothing$ for every prime $p \in \mathbb{Z}$, then $S(\mathbb{Z}) \neq \varnothing$. On the other hand, there is no guarantee that a stacky curve of genus

at least $\frac{1}{2}$ satisfies the Hasse principle: indeed, for any separable integral binary form $f$ of degree $n \geq 3$, the genus of the associated stacky curve $\mathscr{S}_f$ is given by $\frac{n}{4} > \frac{1}{2}$, and Theorem 62 demonstrates that these stacky curves often fail the Hasse principle.

### 3.1.3 Method of proof and organization

Our strategy is to transform the problem of counting soluble superelliptic equations into one of counting integral orbits of a certain representation by devising a suitable orbit construction. In §3.2, we prove that elements of $\mathscr{S}_f(\mathbb{Z})$ naturally give rise to certain square roots of the class of $I_f^{n-2}$. Via the parametrization developed in §1 together with the linearization trick discussed in §1.3.2, these square roots correspond to certain orbits for the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on self-adjoint operators $T \in W_{\mathscr{A}_n}(\mathbb{Z})$, where $\mathrm{ch}_T(x) = f^{\mathsf{mon}}(x, 1)$.[1]

As the parametrization developed in §1 is leading-coefficient-dependent and is thus particularly well-suited for applications concerning binary forms with fixed leading coefficient (such as the application treated in the present chapter, as well as the one treated in §2). By generalizing an equidistribution argument that we develop in §4, one can average the bounds in Theorems 61 and 62 over all leading coefficients and thus deduce analogues of these theorems for the full family of superelliptic equations of given degree. In this chapter, we fix the leading coefficient for two reasons: doing so simplifies the orbit-counting and allows us to prove a stronger result, that within each *thin* subfamily of superelliptic equations with fixed leading coefficient, most members fail the Hasse principle.

In §3.3, we bound the $p$-adic density of the set of elements in $W_{\mathscr{A}_n}(\mathbb{Z}_p)$ that arise from $\mathbb{Z}_p$-primitive solutions via the orbit construction in §3.2 for each prime $p$. In §3.4, we prove Theorem 61 by combining these density bounds with orbit-counting results of Bhargava and Gross (see [15, §10]). Finally, in §3.5, we define the notions of 2-descent obstruction and Brauer–Manin obstruction for superelliptic stacky curves, and we prove Theorem 62.

[1]Incidentally, the orbits of $\mathcal{G}_{\mathscr{A}_n}$ on $W_{\mathscr{A}_n}$ also correspond to 2-Selmer elements of the Jacobians of hyperelliptic curves (see the works [15, 105], as well as §4).

## 3.2 Construction of an integral orbit from a primitive integer solution

Retain the setting of §1.4 (i.e., let $n$, $f_0$, $R$, $f$, and $r$ be as in §1.4) with $n \geq 3$ odd and $r = 1$, and assume that $K$ is of characteristic 0. In §3.2.1, we prove that points $(x_0, y_0, z_0) \in \mathscr{S}_f(R)$ give rise to certain orbits of $\mathcal{G}_{\mathscr{A}_n}(R)$ on $W_{\mathscr{A}_n}(R)$ with characteristic polynomial $f_{\mathsf{mon}}(x, 1)$. To produce the desired orbit, it suffices by Theorem 13 and (1.9) to construct a pair $(I, \alpha) \in H_{f,1}$ such that the matrix $A$ that arises defines a split symmetric bilinear form over $K$. Our construction extends a result of Simon, who constructs the desired pair $(I, \alpha)$ under the following special conditions: $f$ is primitive and irreducible and $z_0$ is coprime to the index of $R_f$ in its integral closure (see [111, Corollary 4]). We finish in §3.2.2 by describing when the orbits arising from the construction are distinguished.

### 3.2.1 The construction

Let $(x_0, y_0, z_0) \in \mathscr{S}_f(R)$. For convenience, we say that the point $(x_0, y_0, z_0)$ is a *Weierstrass point* if $z_0 = 0$ and a *non-Weierstrass point* otherwise. Note that if $z_0 = 0$, then $y_0 \neq 0$ because $f_0 \neq 0$, so the binary form $f$ factors uniquely as

$$f(x, y) = \big(x - \tfrac{x_0}{y_0} \cdot y\big)\widetilde{f}(x, y) \tag{3.3}$$

where $\widetilde{f} \in V_{n-1,f_0}(R)$.

We start by transforming the pair $(x_0, y_0)$ into a pair with simpler coordinates by constructing a suitable $\gamma \in \mathrm{SL}_2(R)$ such that $(x_0, y_0) \cdot \gamma = (0, 1)$. Let $b_0, d_0 \in R$ be any elements such that $b_0 x_0 + d_0 y_0 = 1$ (such $b_0, d_0$ exist since $Rx_0 + Ry_0 = R$). We claim that there exists $\upsilon \in R$ such that $(d_0 - \upsilon x_0) + \theta(b_0 + \upsilon y_0) \in K_f^\times$. Indeed, if we were to have $(d_0 - \upsilon x_0) + \theta(b_0 + \upsilon y_0) \in K_f \smallsetminus K_f^\times$, then the pair $(x, y) = (d_0 - \upsilon x_0, -b_0 - \upsilon y_0)$ is a root of the equation $f(x, y) = 0$, which has finitely many roots up to scaling, implying that we

can choose $\upsilon$ to avoid this outcome (since $K$ is of characteristic 0). Take any such $\upsilon \in R$, let $b = b_0 + \upsilon y_0$ and $d = d_0 - \upsilon x_0$, and let $\gamma = \left[\begin{smallmatrix} y_0 & b \\ -x_0 & d \end{smallmatrix}\right]$. Now, let $f'$ be defined by

$$f'(x,y) = f((x,y)\cdot\gamma^{-1}) = \sum_{i=0}^{n} f'_i x^{n-i} y^i \in V_n(R).$$

Note that $f'_{2n+1} = y_0^2$ and that $f'_0 \neq 0$ since $f'_0 = f_0 \cdot \mathrm{N}(d+\theta b)$. If $y_0 = 0$, the binary form $f'$ factors uniquely as

$$f'(x,y) = x\widetilde{f}'(x,y),$$

where $\widetilde{f}' \in V_{n-1,f'_0}(R)$; further observe that $f'_{2n} = \widetilde{f}(x_0,y_0) \neq 0$ because $f$ is separable. Let $\theta' = (-x_0+\theta y_0)/(d+\theta b)$ be the root of $f'(x,1)$ in $K_{f'} = K_f$, and consider the free rank-$n$ $R$-submodule $I' \subset K_{f'}$ defined by

$$I' := R\langle \xi, \theta', \ldots, \theta'^{\frac{n-1}{2}}, \zeta'_{\frac{n+1}{2}}, \ldots, \zeta'_{n-1}\rangle, \quad \text{where} \quad \xi := \begin{cases} y_0 & \text{if } z_0 \neq 0, \\ \zeta'_{n-1} + f'_{n-1} & \text{if } z_0 = 0. \end{cases} \tag{3.4}$$

Observe that the $R$-module $I'$ is a fractional ideal of $R_{f'}$ that resembles the fractional ideal $I^n_{f'}$, the only difference being that the basis element $1 \in I^n_{f'}$ is replaced by $\xi \in I'$.

**Lemma 63.** *We have that*

$$I'^2 \subset \alpha' \cdot I^{n-2}_{f'}, \quad \textit{where} \quad \alpha' := \begin{cases} -\theta' & \textit{if } z_0 \neq 0, \\ \widetilde{f}'(\theta',1) - \theta' & \textit{if } z_0 = 0 \end{cases}$$

*and that* $\mathrm{N}(I')^2 = \mathrm{N}(\alpha')\,\mathrm{N}(I^{n-2}_{f'})$.

*Proof.* Recall from (1.3) that the fractional ideal $I^{n-2}_{f'}$ has the $\mathbb{Z}$-basis

$$I^{n-2}_{f'} = R\langle 1, \theta', \ldots, \theta'^{n-2}, \zeta'_{n-1}\rangle.$$

To prove the claimed containment, it suffices to check that when each of the pairwise products

of the basis elements of $I'$ in (3.4) is divided by $\alpha'$, what results is an element of $I_{f'}^{2n-1}$. We have the following computations:

$$\begin{aligned}
\xi^2/\alpha' &= \zeta'_{n-1} + f'_{n-1} \\
(\xi \cdot \theta'^i)/\alpha' &= -y_0 \theta'^{i-1} && \text{for } i \in \{1, \dots, \tfrac{n-1}{2}\} \\
(\xi \cdot \zeta'_j)/\alpha' &= -y_0 \zeta'_{j-1} - y_0 f'_{j-1} && \text{for } j \in \{\tfrac{n+1}{2}, \dots, n-1\} \\
(\theta'^i \cdot \theta'^j)/\alpha' &= -\theta'^{i+j-1} && \text{for } i, j \in \{1, \dots, \tfrac{n-1}{2}\} \\
(\theta'^i \cdot \zeta'_j)/\alpha' &= -\theta'^{i-1} \zeta'_j && \text{for } i \in \{1, \dots, \tfrac{n-1}{2}\},\ j \in \{\tfrac{n+1}{2}, \dots, n-1\} \\
(\zeta'_i \cdot \zeta'_j)/\alpha' &= -\zeta'_i \zeta'_{j-1} - f'_{j-1} \zeta'_i && \text{for } i, j \in \{\tfrac{n+1}{2}, \dots, n-1\}
\end{aligned}$$

Using the fact that $\zeta'_i \in R_{f'}$ for each $i \in \{0, \dots, n\}$ together with the fact that $I_{f'}^{n-2}$ is closed under multiplication by elements in $R_{f'}$, one readily verifies that each of the expressions obtained on the right-hand side above is an element of $I_{f'}^{n-2}$. Crucially, these expressions do not depend in piecewise fashion on the value of $z_0$, even though $\xi$ and $\alpha'$ do (see Remark 66).

As for the second part of the lemma, using $\mathrm{N}\left(I_{f'}^{\frac{n-1}{2}}\right) = {f'_0}^{\frac{1-n}{2}}$, we find that $\mathrm{N}(I') = \widetilde{\xi} {f'_0}^{\frac{1-n}{2}}$, where $\widetilde{\xi} = \xi = z_0$ if $z_0 \neq 0$ and $\widetilde{\xi} = \xi - \zeta'_{n-1} = f'_{n-1}$ if $z_0 = 0$. Moreover, a calculation reveals that $\mathrm{N}(\alpha') = \widetilde{\xi}^2 \cdot {f'_0}^{-1}$. Combining these norm calculations, we deduce that

$$\mathrm{N}(I')^2 = \left(\widetilde{\xi} {f'_0}^{\frac{1-n}{2}}\right)^2 = (\widetilde{\xi}^2 {f'_0}^{-1})({f'_0}^{-(n-2)}) = \mathrm{N}(\alpha')\,\mathrm{N}(I_{f'}^{n-2}) \qquad \square$$

We now transform $I'$ and $\alpha'$ back from $R_{f'}$ to $R_f$. Recall from (1.7) that

$$I_f^{\frac{n-1}{2}} = \phi_{\frac{n-1}{2},\gamma}\left(I_{f'}^{\frac{n-1}{2}}\right) = (-b\theta' + y_0)^{\frac{1-n}{2}} I_{f'}^{\frac{n-1}{2}},$$

where we can invert $-b\theta' + y_0$ because its inverse is equal to $d + \theta b$. Since $I'$ resembles $I_{f'}^{\frac{n-1}{2}}$, it makes sense to consider the fractional ideal

$$I := \phi_{\frac{n-1}{2},\gamma}(I') = (-b\theta' + y_0)^{\frac{1-n}{2}} I' = (d + \theta b)^{\frac{n-1}{2}} I', \tag{3.5}$$

which has norm given by

$$\mathrm{N}(I) = \mathrm{N}\left((d+\theta b)^{\frac{n-1}{2}} \cdot I'\right) = \mathrm{N}(d+\theta b)^{\frac{n-1}{2}} \cdot \mathrm{N}(I') = \widetilde{\xi} f_0^{\frac{1-n}{2}} \tag{3.6}$$

where we used the multiplicativity relation (1.5). Similarly, let $\alpha \in K_f^\times$ be defined as follows:

$$\alpha := \phi_{1,\gamma}(\alpha') = \frac{\alpha'}{-b\theta' + y_0} = \begin{cases} x_0 - \theta y_0 & \text{if } z_0 \neq 0, \\ \widetilde{f}(y_0\theta, y_0) + (x_0 - \theta y_0) & \text{if } z_0 = 0. \end{cases} \tag{3.7}$$

It then follows from Lemma 63 that

$$I^2 \subset \frac{\alpha'}{-b\theta' + y_0} \cdot \frac{I_{f'}^{n-2}}{(-b\theta' + y_0)^{n-2}} = \delta \cdot I_f^{n-2}, \tag{3.8}$$

where in the last step above, we used the fact that

$$I_f^{n-2} = \phi_{n-2,\gamma}(I_{f'}^{n-2}) = (-b\theta' + y_0)^{-(n-2)} \cdot I_{f'}^{n-2}.$$

Notice that $\mathrm{N}(I)^2 = \mathrm{N}(\alpha)\,\mathrm{N}(I_f)^{n-2}$ (this can be verified directly from (3.6) and (3.7), but it also follows from the fact that $\mathrm{N}(I')^2 = \mathrm{N}(\alpha')\,\mathrm{N}(I_{f'})^{n-2}$ by Lemma 63).

**Lemma 64.** *The fractional ideal $I$ is well-defined, in the sense that it does not depend on the choice of $\gamma = \left[\begin{smallmatrix} y_0 & b \\ -x_0 & d \end{smallmatrix}\right] \in \mathrm{SL}_2(R)$ satisfying $(x_0, y_0) \cdot \gamma = (0,1)$ and $d + \theta b \in K_f^\times$.*

*Proof.* Let $\gamma = \left[\begin{smallmatrix} y_0 & b \\ -x_0 & d \end{smallmatrix}\right] \in \mathrm{SL}_2(R)$ satisfying $(x_0, y_0) \cdot \gamma = (0,1)$ and $d + \theta b \in K_f^\times$ as above. Any other $\check{\gamma} \in \mathrm{SL}_2(R)$ satisfying $(x_0, y_0) \cdot \check{\gamma}$ to $(0,1)$ is a right-translate of $\gamma$ by an element of the stabilizer of $(0,1)$, which is the group of unipotent matrices $M_\upsilon = \left[\begin{smallmatrix} 1 & \upsilon \\ 0 & 1 \end{smallmatrix}\right]$ for $\upsilon \in R$. So take $\upsilon \in R$, and let

$$\check{\gamma} = \gamma \cdot M_\upsilon = \begin{bmatrix} y_0 & b + \upsilon y_0 \\ -x_0 & d - \upsilon x_0 \end{bmatrix}$$

Let $\check{f}(x,y) = f((x,y)\cdot\check{\gamma}^{-1}) = \sum_{i=0}^n \check{f}_i x^{n-i} y^i$, and let $\check{\theta}$ be the root of $\check{f}(x,1)$ in $K_f$. Assume

that $\upsilon$ has been chosen so that $(d - \upsilon x_0) + \theta(b + \upsilon y_0) \in K_f^\times$, and notice that

$$\check{\theta} = \frac{-x_0 + \theta y_0}{(d - \upsilon x_0) + \theta(b + \upsilon y_0)} = \frac{\theta'}{1 + \theta' \upsilon}. \tag{3.9}$$

Just as we associated a pair $(I', \alpha')$ to $\gamma$, we can associate a pair $(\check{I}, \check{\alpha})$ to $\check{\gamma}$ satisfying the analogous properties $\check{I}^2 \subset \check{\alpha} I_{\check{f}}^{n-2}$ and $\mathrm{N}(\check{I})^2 = \mathrm{N}(\check{\alpha})\,\mathrm{N}(I_{\check{f}}^{n-2})$. To prove the lemma, it suffices to show that

$$\phi_{\frac{n-1}{2},\gamma}(I') = \phi_{\frac{n-1}{2},\check{\gamma}}(\check{I}) \quad \text{and} \quad \phi_{1,\gamma}(\delta') = \phi_{1,\check{\gamma}}(\check{\delta}), \tag{3.10}$$

The second equality in (3.10) is readily deduced by inspecting (3.7); as for the first equality, notice that it is equivalent to the following:

$$\left(\frac{-b\theta' + y_0}{-(b + \upsilon y_0)\check{\theta} + y_0}\right)^{\frac{n-1}{2}} \check{I} = I'. \tag{3.11}$$

Using (3.9), we find that the fraction in parentheses in (3.11) is equal to $1 + \upsilon\theta'$. Now, observe that we can express the ideals $I'$ and $\check{I}$ as

$$I' = R\langle \widetilde{\xi}, \theta' I_{f'}^{\frac{n-3}{2}} \rangle \quad \text{and} \quad \check{I} = R\langle \widetilde{\xi}, \check{\theta} I_{\check{f}}^{\frac{n-3}{2}} \rangle, \tag{3.12}$$

where $\widetilde{\xi} = z_0$ if $z_0 \neq 0$ and $\widetilde{\xi} = f'_{n-1} = \check{f}_{n-1}$ if $z_0 = 0$. Upon combining (3.11) and (3.12), we find that

$$\begin{aligned}(1 + \upsilon\theta')^{\frac{n-1}{2}} \widetilde{I} &= R\big\langle (1 + \upsilon\theta')^{\frac{n-1}{2}} \widetilde{\xi}, ((1 + \upsilon\theta')\widetilde{\theta})((1 + \upsilon\theta') I_{\widetilde{f}})^{\frac{n-3}{2}} \big\rangle \\ &= R\big\langle (1 + \upsilon\theta')^{\frac{n-1}{2}} \widetilde{\xi}, \theta' I_{f'}^{\frac{n-3}{2}} \big\rangle = I',\end{aligned}$$

where the last step above follows because $\theta'^i \in I'$ for each $i \in \{0, \ldots, \frac{n-1}{2}\}$. □

By applying the correspondence in Theorem 13 to the pair $(I, \alpha)$ constructed above, we see that the point $(x_0, y_0, z_0) \in \mathscr{S}_f(R)$ gives rise to a pair $(A, B) \in W_n(R)$ with $\iota(A, B) = f^{\mathsf{mon}}$. To complete the construction, it remains to verify that $A$ is split:

**Lemma 65.** *The matrix $A$ defines a split quadratic form over $K$.*

*Proof.* It suffices to exhibit an $n$-dimensional isotropic space $X$ over $K$ for the quadratic form defined by $A$. We claim that

$$X = K\langle x_0 - \theta y_0, \theta(x_0 - \theta y_0), \ldots, \theta^{\frac{n-3}{2}}(x_0 - \theta y_0)\rangle \subset K_f$$

does the job. Indeed, since $f$ is separable, the elements $\theta^i(x_0 - \theta y_0)$ for $i \in \{0, \ldots, \frac{n-3}{2}\}$ are linearly independent over $K$: if $z_0 \neq 0$, then this follows because the elements $\theta^i \in K_f$ for $i \in \{0, \ldots, \frac{n-3}{2}\}$ are linearly independent and $x_0 - \theta y_0$ is an invertible element of $K_f$; if $z_0 = 0$, then this follows because the elements $\theta^i \in K_{\widetilde{f}}$ for $i \in \{0, \ldots, \frac{n-3}{2}\}$ are linearly independent and $x_0 - \theta y_0$ is an invertible element of $K_{\widetilde{f}}$. Thus, we have that $\dim_K X = \frac{n-1}{2}$. Moreover, notice that

$$\pi_{n-1}(\langle \theta^i(x_0 - \theta y_0), \theta^j(x_0 - \theta y_0)\rangle) = \pi_{n-1}(x_0\theta^{i+j} - y_0\theta^{i+j+1}) = 0$$

for any $i, j \in \{0, \ldots, \frac{n-3}{2}\}$. □

*Remark* 66. We defined the pair $(I, \alpha)$ in piecewise fashion, according as $z_0 \neq 0$ or $z_0 = 0$. The resulting pair $(A, B)$ nevertheless admits a "functorial" definition: indeed, the entries of $A$ and $B$ are polynomial functions in $x_0, y_0, z_0, b, d$ and the coefficients of $f$. Thus, if our purpose was simply to construct orbits from integral points, we could have carried out the construction for $z_0 \neq 0$ and specialized the resulting pair of matrices to the case $z_0 = 0$. However, our proofs of Theorems 61 and 62 require knowledge of the element $\alpha \in K_f^\times$ corresponding to the orbit arising from an integral point, and it is difficult to reverse-engineer $\alpha$ from a representative $(A, B)$ of such an orbit.

In [11, §2], Bhargava establishes an analogous construction for rational points on hyperelliptic curves, one that takes a *non*-Weierstrass point on a hyperelliptic curve $z^2 = f(x, y)$ of even degree $n$ and produces a pair $(I, \alpha)$ of a fractional ideal $I$ and $\alpha \in K_f^\times$ such that

$I^2 \subset \alpha I_f^{n-3}$ and $\mathrm{N}(I)^2 = \mathrm{N}(\alpha)\,\mathrm{N}(I_f^{n-3})$. By Wood's parametrization (see [126, Theorem 5.7]), the pair $(I, \alpha)$ gives rise to a pair $(A, B) \in W_n(R)$ such that $\iota(A, B) = f$. To handle Weierstrass points, Bhargava uses the aforementioned specialization trick but does not determine the element $\alpha \in K_f^\times$ corresponding to the specialized orbit, even though this data seems necessary for the proofs of [11, Theorem 3 and Corollary 4] to go through. We note here that the piecewise construction of the pair $(I, \alpha)$ given in this section can be modified to work for hyperelliptic curves, thus yielding complete proofs of [11, Theorem 3 and Corollary 4].

*Remark* 67. That $\iota(A, B) = f^{\mathsf{mon}}$, that $A$ defines a split quadratic form, and that the stabilizer of $(A, B)$ contains a subgroup isomorphic to $R_f^\times[2]$ are properties that hold *formally*. Thus, if we replace $R$ with any base ring and $f$ is *any* form in $V_n(R)$, *any* $R$-primitive solution $(x, y, z) = (x_0, y_0, z_0) \in R^3$ to the superelliptic equation $z^2 = f(x, y)$ gives rise to a pair of matrices $(A, B) \in W_n(R)$ such that $\iota(A, B) = f^{\mathsf{mon}}$ and such that the stabilizer in $\mathrm{SL}_n(R)$ contains a subgroup isomorphic to $R_f^\times[2]_{\mathrm{N}\equiv 1}$. If the base ring $R$ is an integral domain, then $A$ defines a split quadratic form over the fraction field $K$ of $R$. Note that these properties hold even if we do not assume that $f_0 \neq 0$, that $f$ is separable, and that $K$ has characteristic 0, despite the fact that we used these assumptions to derive the construction.

### 3.2.2 Distinguished points

We say that a point $(x_0, y_0, z_0) \in \mathscr{S}_f(R)$ is *distinguished* if its associated $\mathcal{G}_{\mathscr{A}_n}(K)$-orbit is distinguished. Note that Proposition 19 implies that $(x_0, y_0, z_0)$ is distinguished if and only if $f_0(x_0 - \theta y_0)$ is a square in $K_f^\times$.

When $f_0$ is a multiple of a perfect square by a unit $u \in R^\times$, $\mathscr{S}_f$ has a trivial $R$-point, namely $(u, 0, \sqrt{u^{2n+1} f_0})$. Since $f_0(u - \theta \cdot 0) = u f_0 \in K_f^{\times 2}$, the orbits associated to these trivial solutions are always distinguished. Whether a primitive integer solution is distinguished is *not necessarily* invariant under replacing $f$ with an $\mathrm{SL}_2(R)$-translate. Indeed, suppose $(x_0, y_0, z_0) \in \mathscr{S}_f(R)$, take $\gamma \in \mathrm{SL}_2(R)$ such that $(x_0, y_0) \cdot \gamma = (1, 0)$, and let $f'(x, y) = f((x, y) \cdot \gamma^{-1})$. Then the point $(1, 0, z_0) \in \mathscr{S}_{f'}(R)$ is distinguished, regardless of whether the

point $(x_0, y_0, z_0) \in \mathscr{S}_f(R)$ is distinguished. Nevertheless, whether a solution is distinguished is *always* preserved under replacing $f$ with a translate by an element of $N(R)$.

Now take $R = \mathbb{Z}$. When $|f_0|$ is not a perfect square, we show in §2.4.3 that the non-square factors of $|f_0|$ tend to obstruct the distinguished $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q})$-orbit from arising via the map $\mathsf{orb}_{f,1}$. More precisely, we have the following result, which states that there are strong limitations on the forms $f \in V_{n,f_0}(\mathbb{Z})$ for which some point of $\mathscr{S}_f(\mathbb{Z})$ is distinguished:

**Proposition 68.** *Let $f \in V_{n,f_0}(\mathbb{Z})$ be separable, and suppose that there exists a point of $\mathscr{S}_f(\mathbb{Z})$ giving rise to the distinguished $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q})$-orbit via the construction in §3.2. Then one of the following two mutually exclusive possibilities holds for each prime $p \mid k$:*

(a) *$R_f \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is not maximal in $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_p$; or*

(b) *$R_f \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is maximal in $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and $f/y$ is a unit multiple of a square modulo $p$.*

*Moreover, the density of binary forms $f \in V_{n,f_0}(\mathbb{Z})$ such that one of the conditions* (a) *or* (b) *holds for every prime $p \mid k$ is equal to $\mu_{f_0} := \prod_{p|k} \left( \frac{1}{p^2} + \frac{p-1}{p^{\frac{n+1}{2}}} \right)$.*

*Proof.* Let $p \mid k$. By Proposition 48, if $f \in V_{n,f_0}(\mathbb{Z})$ is such that some element of $\mathsf{orb}_{f,1}(H_{f,1})$ has distinguished $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)$-orbit, then one of conditions (a) or (b) in the theorem statement holds. By [4, Proposition 3.5], the $p$-adic density of $f \in V_{n,f_0}(\mathbb{Z}_p)$ satisfying (a) is $p^{-2}$, and it follows from Theorem 49 that the $p$-adic density of $f \in V_{n,f_0}(\mathbb{Z}_p)$ satisfying (b) is $p^{-\frac{n+1}{2}}(p-1)$. The proposition follows by combining these density calculations. □

Proposition 68 implies that points of $\mathscr{S}_f(\mathbb{Z})$ often fail to be distinguished—a fact that is crucial for the proofs of Theorems 61 and 62, because the geometry-of-numbers results from [15, §9] that we apply in §3.4 to count orbits of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $W_{\mathscr{A}_n}(\mathbb{Z})$ only give us a count of the non-distinguished orbits.

## 3.3 Counting orbits arising from local points

Let $\mathscr{P}$ denote the ($\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$-invariant) subset of integral elements of $W_{\mathscr{A}_n}(\mathbb{Z})$ that arise via the construction in §3.2.1 from separable forms $f \in V_{n,f_0}(\mathbb{Z})$. It is hard to describe $\mathscr{P}$ explicitly, and hence to determine a precise count of the number of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$-orbits on $\mathscr{P}$ having bounded height. However, $\mathscr{P}$ is contained within a subset of $W_{\mathscr{A}_n}(\mathbb{Z})$ defined by local conditions: indeed, $\mathscr{P} \subset W_{\mathscr{A}_n}(\mathbb{Z}) \cap \bigcap_v \mathscr{P}_v$, where for each place $v$ of $\mathbb{Q}$, we write $\mathscr{P}_v$ for the subset of $W_{\mathscr{A}_n}(\mathbb{Z}_v)$ that arises via the construction from separable forms $f \in V_{n,f_0}(\mathbb{Z}_v)$. To prove Theorem 61, our strategy is to *bound* the number of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$-orbits on $\mathscr{P}$ of bounded height by counting the total number of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$-orbits on $W_{\mathscr{A}_n}(\mathbb{Z})$ of bounded height and sieving to those orbits that belong to $\mathscr{P}_v$ for many places $v$.

A key step in this strategy is, roughly speaking, to control the size of $\mathscr{P}_v$ for each $v$. The purpose of this section is to carry out this step. In §3.3.1, we determine the number of orbits arising via the construction from a given separable form $f \in V_{n,f_0}(\mathbb{R})$. In §3.3.2, we bound the $p$-adic density of $\mathscr{P}_p$ for odd primes $p \nmid f_0$ by working over $\mathbb{Z}/p\mathbb{Z}$, and in §3.3.3, we bound the 2-adic density of $\mathscr{P}_2$ when $2 \nmid f_0$ by working over $\mathbb{Z}/8\mathbb{Z}$. In §3.3.4, we take $p \mid f_0$ and work over $\mathbb{Z}_p$ to bound the number of orbits arising via the construction from forms $f \in V_{n,f_0}(\mathbb{Z}_p)$ that define the maximal order. We finish in §3.3.5 by working over $\mathbb{Q}_p$ to handle the remaining cases.

### 3.3.1 Orbits over $\mathbb{R}$

For each $m \in \{0, \dots, \frac{n-1}{2}\}$, let $\mathcal{I}(m) \subset V_{n,1}(\mathbb{R})$ be the set of separable monic degree-$n$ polynomials over $\mathbb{R}$ having exactly $2m+1$ real roots.

**Proposition 69.** *There are exactly $2m+1$ orbits of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ on $W_{\mathscr{A}_n}(\mathbb{R})$ that arise from points in $\mathscr{S}_f(\mathbb{R})$.*

*Proof.* Let $f \in V_{n,f_0}(\mathbb{R})$. Suppose that $f^{\mathsf{mon}} \in \mathcal{I}(m)$ with real roots given in increasing order by $\lambda_1 < \cdots < \lambda_{2m+1}$, where $m \in \{0, \dots, \frac{n-1}{2}\}$. We now compute the number of orbits of

$\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ on $W_{\mathscr{A}_n}(\mathbb{R})$ having characteristic polynomial $f^{\mathsf{mon}}$ that arise from points in $\mathscr{S}_f(\mathbb{R})$ via the construction in §3.2. The $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$-orbit associated to a point $(x_0, y_0, z_0) \in \mathscr{S}_f(\mathbb{R})$ is identified via the correspondence in Proposition 19 with some $f_0\alpha \in (K_f^\times/K_f^{\times 2})_{\mathrm{N}\equiv 1}$. This class is represented by a sequence of the form

$$\big(f_0(x_0 - \lambda_1 y_0), \ldots, f_0(x_0 - \lambda_{2m+1} y_0), b_1, \ldots, b_{\frac{n-1}{2}-m}\big) \in \mathbb{R}^{2m+1} \times \mathbb{C}^{\frac{n-1}{2}-m} \simeq K_f. \tag{3.13}$$

Otherwise, if $z_0 = 0$, then $\frac{x_0}{y_0} = \lambda_j$ for some $j$; letting $\widetilde{f}$ be as in (3.3), we see that the class $f_0\alpha \in (K_f^\times/K_f^{\times 2})_{\mathrm{N}\equiv 1}$ is represented by a sequence of the form

$$(f_0(x_0 - \lambda_1 y_0), \ldots, f_0\widetilde{f}(x_0, y_0), \ldots, f_0(x_0 - \lambda_{2m+1} y_0), b_1, \ldots, b_{\frac{n-1}{2}-m}) \in \mathbb{R}^{2m+1} \times \mathbb{C}^{\frac{n-1}{2}-m}, \tag{3.14}$$

where the term $f_0\widetilde{f}(x_0, y_0)$ in (3.14) replaces the term $f_0(x_0 - \lambda_j y_0)$ in (3.13). The class in $(K_f^\times/K_f^{\times 2})_{\mathrm{N}\equiv 1}$ of the sequence in (3.13) or in (3.14) is given by the sequence of signs of its first $2m+1$ terms. Because $\mathrm{N}(b_j) > 0$ for every $j$, the condition that $\mathrm{N}(f_0\alpha)$ is a square in $\mathbb{R}^\times$ is equivalent to the condition that $\prod_{i=1}^{2m+1} f_0(x_0 - \lambda_i y_0) > 0$ if $z_0 \neq 0$ and $(f_0\widetilde{f}(x_0, y_0)) \prod_{\substack{i=1 \\ i\neq j}}^{2m+1} f_0(x_0 - \lambda_i y_0) > 0$ if $z_0 = 0$. We now split into cases based on the signs of $f_0$ and $y_0$:

*Case 1a*: $f_0 > 0$, $y_0 > 0$. First suppose $z_0 \neq 0$. In this case, the sign of $f_0(x_0 - \lambda_i y_0)$ is equal to the sign of $(x_0/y_0) - \lambda_i$. The possible sequences of signs of the $f_0(x_0 - \lambda_i y_0)$ are therefore

$$+---\cdots-,\ +++-\cdots-,\ \ldots,\ ++++\cdots+, \tag{3.15}$$

giving a total of $m+1$ orbits. We label the sign sequences in (3.15) from left to right by an index $\tau$ that runs from 1 up to $m+1$. If $z_0 = 0$ and $\frac{x_0}{y_0} = \lambda_j$, then because $\lambda_i < \lambda_j$ when $i < j$ and $\lambda_i > \lambda_j$ when $i > j$, we obtain the same sign sequences as those listed in (3.15).

*Case 1b*: $f_0 > 0$, $y_0 < 0$. First suppose $z_0 \neq 0$. In this case, the sign of $f_0(x_0 - \lambda_i y_0)$ is equal

to the opposite of the sign of $(x_0/y_0)-\lambda_i$. The possible sequences of signs of the $f_0(x_0-\lambda_i y_0)$ are therefore

$$+++\cdots++,\ --+\cdots++,\ \ldots,\ --\cdots-+, \tag{3.16}$$

giving a total of $m+1$ orbits. We label the sign sequences in (3.16) from left to right by an index $\tau$ that runs from $m+1$ up to $2m+1$. (Note that the first sign sequence in (3.16) is the same as the last sign sequence in (3.15), which is why they share the same value of $\tau$.) If $z_0 = 0$, we again obtain the same sign sequences as those listed in (3.16).

*Case 2a*: $f_0 < 0$, $y_0 > 0$. The possible sign sequences are the same as those listed in (3.16), and we label them from left to right by an index $\tau$ that runs from $m+1$ up to $2m+1$.

*Case 2b*: $f_0 < 0$, $y_0 < 0$. The possible sign sequences are the same as those listed in (3.15), and we label them from left to right by an index $\tau$ that runs from 1 up to $m+1$. □

For each $m \in \{0, \ldots, \frac{n-1}{2}\}$ and $\tau \in \{1, \ldots, 2m+1\}$, we write $W_{\mathscr{A}_n}^{(m,\tau)} \subset W_{\mathscr{A}_n}(\mathbb{R})$ for the subset of operators $T$ such that $\mathrm{ch}_T \in \mathcal{I}(m)$ and such that the $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$-orbit of $T$ gives rise (via the correspondence in Proposition 19 and the above discussion) to the sign sequence with index $\tau$.

### 3.3.2 Bounding $\mathrm{Vol}(\mathscr{P}_p)$ for $2 \neq p \nmid f_0$

Let $\mathrm{Vol}(\mathscr{P}_p)$ denote the $p$-adic density of $\mathscr{P}_p$ in $W_{\mathscr{A}_n}(\mathbb{Z}_p)$ (i.e., the volume of $\mathscr{P}_p$ with respect to the Euclidean measure on $W_{\mathscr{A}_n}(\mathbb{Z}_p)$ normalized so that the volume of $W_{\mathscr{A}_n}(\mathbb{Z}_p)$ is 1). Let $\mathcal{I}_p(m)$ denote the set of monic degree-$n$ polynomials over $\mathbb{Z}/p\mathbb{Z}$ (*not necessarily* separable) with $m$ distinct irreducible factors. When $2 \neq p \nmid f_0$, we get the following bound on $\mathrm{Vol}(\mathscr{P}_p)$:

**Proposition 70.** *We have that*

$$\mathrm{Vol}(\mathscr{P}_p) \leq \min\left\{1, \sum_{m=1}^{n} \frac{p+1}{2^{m-1}} \cdot \frac{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})}{p^{\frac{n(n-1)}{2}}} \cdot \frac{\#\mathcal{I}_p(m)}{p^n}\right\}$$

*Proof.* Given a monic degree-$n$ polynomial $f$ over $\mathbb{Z}/p\mathbb{Z}$, let $\overline{\Sigma}_f^{\mathrm{sol}} \subset W_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})$ denote the

mod-$p$ reduction of the subset $\{T \in \mathscr{P}_p : \mathrm{ch}_T \equiv f \pmod p\}$. Because $\mathcal{G}_{\mathscr{A}_n}$ is smooth over $\mathbb{Z}_p$, the map $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p) \to \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})$ is surjective, implying that $\overline{\Sigma}_f^{\mathrm{sol}}$ is $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})$-invariant. Then we have

$$\mathrm{Vol}(\mathscr{P}_p) \leq \sum_{m=1}^{n} \sum_{f \in \mathcal{I}_p(m)} \frac{\#\overline{\Sigma}_f^{\mathrm{sol}}}{p^{\dim W_{\mathscr{A}_n}}} = \sum_{m=1}^{n} \sum_{f \in \mathcal{I}_p(m)} \sum_{T \in \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z}) \backslash \overline{\Sigma}_f^{\mathrm{sol}}} \frac{\#\mathcal{O}(T)}{p^{\frac{n(n+1)}{2}}}, \tag{3.17}$$

where for each $T \in W_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})$, we denote by $\mathcal{O}(T)$ the $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})$-orbit of $T$. Let $\mathrm{Stab}(T) \subset \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})$ be the stabilizer of $T$. Substituting $\#\mathcal{O}(T) = \#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})/\#\,\mathrm{Stab}(T)$ into (3.17) yields that

$$\mathrm{Vol}(\mathscr{P}_p) \leq \sum_{m=1}^{n} \sum_{f \in \mathcal{I}_p(m)} \sum_{T \in \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z}) \backslash \overline{\Sigma}_f^{\mathrm{sol}}} \frac{1}{\#\,\mathrm{Stab}(T)} \cdot \frac{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})}{p^{\frac{n(n+1)}{2}}}. \tag{3.18}$$

The following lemma gives a lower bound for $\#\,\mathrm{Stab}(T)$ that is independent of $f \in \mathscr{I}_p(m)$:

**Lemma 71.** *For $T \in \overline{\Sigma}_f^{\mathrm{sol}}$, we have that $\#\,\mathrm{Stab}(T) \geq 2^{m-1}$.*

*Proof of Lemma 71.* Let $K_f = (\mathbb{Z}/p\mathbb{Z})[x]/(f)$. By Proposition 19, (1.9), and Remark 67, we have that $\#\,\mathrm{Stab}(T) \geq \#K_f^{\times}[2]_{\mathrm{N}\equiv 1}$. Letting $f$ split over $\mathbb{Z}/p\mathbb{Z}$ as $f = \prod_{i=1}^{m} F_i^{n_i}$, where the $F_i$ are distinct and irreducible, we have that $K_f \simeq \prod_{i=1}^{m} (\mathbb{Z}/p\mathbb{Z})[x]/(F_i^{n_i})$. Consequently, $K_f^{\times}[2]$ contains the $2^m$ elements of the form $(\pm 1, \ldots, \pm 1)$. Exactly half of these elements have norm 1, so $\#K_f^{\times}[2]_{\mathrm{N}\equiv 1} \geq 2^{m-1}$. □

To bound the right-hand side of (3.18), it remains to control the number of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})$-orbits on $\overline{\Sigma}_f^{\mathrm{sol}}$. But there can only be as many orbits as there are points in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, which has size $p+1$. Combining this observation with (3.18) and Lemma 71 yields the result. □

*Remark* 72. It is well-known (see [15, §6.1]) that for each odd prime $p$, we have

$$\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z}) = p^{\left(\frac{n-1}{2}\right)^2} \prod_{i=1}^{\frac{n-1}{2}} (p^{2i} - 1) \leq p^{\frac{n(n-1)}{2}}. \tag{3.19}$$

### 3.3.3 Bounding $\mathrm{Vol}(\mathscr{P}_2)$ for $2 = p \nmid f_0$

Here, it turns out to be ineffective to work over $\mathbb{Z}/2\mathbb{Z}$ or even $\mathbb{Z}/4\mathbb{Z}$; instead, we work over $\mathbb{Z}/8\mathbb{Z}$. Let $\mathcal{I}_8(m)$ denote the set of monic degree-$n$ polynomials in $(\mathbb{Z}/8\mathbb{Z})[x]$ having $m$ distinct irreducible factors over $\mathbb{Z}/2\mathbb{Z}$. When $2 = p \nmid f_0$, we obtain the following bound on $\mathrm{Vol}(\mathscr{P}_2)$:

**Proposition 73.** *We have that*

$$\mathrm{Vol}(\mathscr{P}_2) \leq \min\left\{1, \sum_{m=1}^{n} \frac{12}{2^{n+m-2}} \cdot 2 \cdot \frac{\#\mathcal{I}_8(m)}{8^n}\right\}$$

*Proof.* Given a monic degree-$n$ polynomial $f$ over $\mathbb{Z}/8\mathbb{Z}$, let $\overline{\Sigma}_f^{\mathrm{sol}} \subset W_{\mathscr{A}_n}(\mathbb{Z}/8\mathbb{Z})$ denote the closure under the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/8\mathbb{Z})$ of the mod-8 reduction of the subset $\{T \in \mathscr{P}_2 : \mathrm{ch}_T \equiv f \pmod 8\}$ (note that this subset may not be *a priori* $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/8\mathbb{Z})$-invariant, because $\mathcal{G}_{\mathscr{A}_n}$ is not smooth over $\mathbb{Z}_2$ and the map $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_2) \to \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/8\mathbb{Z})$ is not surjective). Then we have

$$\mathrm{Vol}(\mathscr{P}_2) \leq \sum_{m=1}^{n} \sum_{f \in \mathcal{I}_8(m)} \frac{\#\overline{\Sigma}_f^{\mathrm{sol}}}{8^{\dim W_{\mathscr{A}_n}}} = \sum_{m=1}^{n} \sum_{f \in \mathcal{I}_8(m)} \sum_{T \in \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/8\mathbb{Z}) \backslash \overline{\Sigma}_f^{\mathrm{sol}}} \frac{\#\mathcal{O}(T)}{8^{\frac{n(n+1)}{2}}}, \tag{3.20}$$

where for each $T \in W_{\mathscr{A}_n}(\mathbb{Z}/8\mathbb{Z})$, we denote by $\mathcal{O}(T)$ the $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/8\mathbb{Z})$-orbit of $T$. Let $\mathrm{Stab}(T) \subset \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/8\mathbb{Z})$ denote the stabilizer of $T$. Substituting $\#\mathcal{O}(T) = \#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/8\mathbb{Z})/\#\,\mathrm{Stab}(T)$ into (3.20) yields that

$$\mathrm{Vol}(\mathscr{P}_2) \leq \sum_{m=1}^{n} \sum_{f \in \mathcal{I}_8(m)} \sum_{T \in \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/8\mathbb{Z}) \backslash \overline{\Sigma}_f^{\mathrm{sol}}} \frac{1}{\#\,\mathrm{Stab}(T)} \cdot \frac{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/8\mathbb{Z})}{8^{\frac{n(n+1)}{2}}}. \tag{3.21}$$

The following lemma gives a lower bound for $\#\,\mathrm{Stab}(T)$ that is independent of $f \in \mathscr{I}_8(m)$:

**Lemma 74.** *For $T \in \overline{\Sigma}_f^{\mathrm{sol}}$, we have that $\#\,\mathrm{Stab}(T) \geq 2^{n+m-2}$.*

*Proof of Lemma 74.* Let $R_f = (\mathbb{Z}/8\mathbb{Z})[x]/(f)$. By Theorem 13, (1.9), and Remark 67, we have that $\#\,\mathrm{Stab}(T) \geq \#R_f^{\times}[2]_{\mathrm{N}\equiv 1}$. Let $f$ split over $\mathbb{Z}/8\mathbb{Z}$ as $f = \prod_{i=1}^{m} F_i$, where the $F_i$

have the property that their mod-2 reductions are powers of distinct irreducible polynomials. Then it follows from [81, Theorem 7] together with the Chinese Remainder Theorem that $R_f \simeq \prod_{i=1}^{m} (\mathbb{Z}/8\mathbb{Z})[x]/(F_i)$, and $R_f^\times[2]$ contains the $2^{n+m}$ elements of the form

$$\left( \dots, \rho_0 + \sum_{j=1}^{d_i - 1} \rho_j \theta_i^j, \dots \right) \in \prod_{i=1}^{m} (\mathbb{Z}/8\mathbb{Z})[x]/(F_i),$$

where $\rho_0$ is any element of $(\mathbb{Z}/8\mathbb{Z})^\times$ and $\rho_j$ is any element of $\{0, 4\} \subset \mathbb{Z}/8\mathbb{Z}$ for each $j$, $\theta_i$ is the image of $x$ in $(\mathbb{Z}/8\mathbb{Z})[x]/(F_i)$, and $d_i = \deg F_i$ for each $i$. At least $\frac{1}{4}$ of these elements have norm 1, so $\#\operatorname{Stab}(T) \geq \#R_F^\times[2]_{\mathrm{N}\equiv 1} \geq 2^{n+m-2}$. □

Let $\widehat{\mathcal{G}_{\mathscr{A}_n}}$ be the split odd orthogonal group scheme, defined in the same way as $\mathcal{G}_{\mathscr{A}_n}$ but without the determinant-1 condition. Observe that the determinant map $\det\colon \widehat{\mathcal{G}_{\mathscr{A}_n}}(\mathbb{Z}/8\mathbb{Z}) \to (\mathbb{Z}/8\mathbb{Z})^\times$ is surjective: for each $\sigma \in (\mathbb{Z}/8\mathbb{Z})^\times$, the diagonal matrix with row-$\frac{n+1}{2}$, column-$\frac{n+1}{2}$ entry equal to $\sigma$ and all other diagonal entries equal to 1 is orthogonal with respect to $\mathscr{A}_n$ and has determinant $\sigma$. Combining this observation with the computation of $\#\widehat{\mathcal{G}_{\mathscr{A}_n}}(\mathbb{Z}/8\mathbb{Z})$ in Proposition 75 (to follow) yields

$$\frac{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/8\mathbb{Z})}{8^{\frac{n(n-1)}{2}}} = \frac{\#\widehat{\mathcal{G}_{\mathscr{A}_n}}(\mathbb{Z}/8\mathbb{Z})}{4 \cdot 8^{\frac{n(n-1)}{2}}} = 2 \cdot \frac{\left(2^{\frac{n-1}{2}} - 1\right) \cdot \prod_{i=1}^{\frac{n-3}{2}} (2^{2i} - 1)}{2^{\left(\frac{n-1}{2}\right)^2}} \leq 2 \cdot 1 = 2. \tag{3.22}$$

To bound the right-hand side of (3.21), it remains to control the number of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/8\mathbb{Z})$-orbits on $\overline{\Sigma}_f^{\mathrm{sol}}$. But there can only be as many orbits as there are points in $\mathbb{P}^1(\mathbb{Z}/8\mathbb{Z})$, which has size 12. Combining this observation with (3.21), Lemma 74, Proposition 75, and (3.22) yields the result. □

In the following proposition, we obtain the value of $\#\widehat{\mathcal{G}_{\mathscr{A}_n}}(\mathbb{Z}/8\mathbb{Z})$, which was used in (3.22):

**Proposition 75.** *We have that*

$$\#\widehat{\mathcal{G}_{\mathscr{A}_n}}(\mathbb{Z}/8\mathbb{Z}) = 2^{\frac{5n^2-4n+11}{4}} \left(2^{\frac{n-1}{2}} - 1\right) \prod_{i=1}^{\frac{n-3}{2}} (2^{2i} - 1)$$

*when* $n \geq 3$, *and* $\#\widehat{\mathcal{G}_{\mathscr{A}_n}}(\mathbb{Z}/8\mathbb{Z}) = 4$ *when* $n = 1$.

*Proof.* We apply the recursive formula for computing sizes of orthogonal groups modulo 8 given in [96, §4.1.3]. The first step is to diagonalize $\mathscr{A}_n$. One readily verifies that there exists $g_1 \in \mathrm{GL}_n(\mathbb{Z})$ such that $g_1 \mathscr{A}_n g_1^T$ is equal to the diagonal matrix with first $\frac{n+1}{2}$ diagonal entries equal to 1 and remaining $\frac{n-1}{2}$ diagonal entries equal to $-1$. By [73, proof of Lemma 3], there exists $g_2 \in \mathrm{GL}_n(\mathbb{Z}_2)$ such that $g_2 g_1 \mathscr{A}_n g_1^T g_2^T$ is equivalent modulo 8 to the following diagonal matrix:

$$\begin{bmatrix} 1 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 & 0 & 0 \\ 0 & \cdots & 0 & a_1 & 0 & 0 \\ 0 & \cdots & 0 & 0 & a_2 & 0 \\ 0 & \cdots & 0 & 0 & 0 & a_3 \end{bmatrix}, \text{ where } (a_1, a_2, a_3) = \begin{cases} (1,1,1), & \text{if } n \equiv 1 \pmod 8, \\ (1,1,7), & \text{if } n \equiv 3 \pmod 8, \\ (1,3,3), & \text{if } n \equiv 5 \pmod 8, \\ (3,3,7), & \text{if } n \equiv 7 \pmod 8 \end{cases} \tag{3.23}$$

Using (3.23) together with the recursive formula displayed in [96, §4.1.3] yields that

$$\#\widehat{\mathcal{G}_{\mathscr{A}_n}}(\mathbb{Z}/8\mathbb{Z}) = \prod_{j=1}^{n} \left(8^j + 4^{j+1} f(u_{n-j}) + 2(4\sqrt{2})^j \cos(\tfrac{\pi}{4} K_{n-j}) - 8 4^j h(u_{n-j})\right), \tag{3.24}$$

where the functions $f$ and $h$ are defined by

$$f(u_i) = \begin{cases} 1, & \text{if } u_i \equiv 0 \pmod 8, \\ -1, & \text{if } u_i \equiv 4 \pmod 8, \\ 0, & \text{otherwise} \end{cases} \quad \text{and} \quad h(u_i) = \begin{cases} 1, & \text{if } i < n-1 \text{ and } u_i \equiv 0 \pmod 8, \\ 0, & \text{otherwise} \end{cases}$$

and where the quantities $u_i$ and $h_i$ are given as follows:

*Case 1:* $(a_1, a_2, a_3) = (1, 1, 1)$. We have that

$$u_{n-j} = j - 1 \quad \text{and} \quad K_{n-j} = j - 2. \tag{3.25}$$

*Case 2:* $(a_1, a_2, a_3) = (1, 1, 7)$. We have that

$$u_{n-j} = \begin{cases} j+5, & \text{if } j \geq 2, \\ 0, & \text{if } j = 1 \end{cases} \quad \text{and} \quad K_{n-j} = \begin{cases} j-4, & \text{if } j \geq 2, \\ -15, & \text{if } j = 1 \end{cases} \tag{3.26}$$

*Case 3:* $(a_1, a_2, a_3) = (1, 3, 3)$. We have that

$$u_{n-j} = \begin{cases} j+3, & \text{if } j \geq 3, \\ 3, & \text{if } j = 2, \\ 0, & \text{if } j = 1 \end{cases} \quad \text{and} \quad K_{n-j} = \begin{cases} j-6, & \text{if } j \geq 3, \\ -8, & \text{if } j = 2, \\ -7, & \text{if } j = 1 \end{cases} \tag{3.27}$$

*Case 4:* $(a_1, a_2, a_3) = (3, 3, 7)$. We have that

$$u_{n-j} = \begin{cases} j+9, & \text{if } j \geq 4, \\ 10, & \text{if } j = 3, \\ 7, & \text{if } j = 2, \\ 0, & \text{if } j = 1 \end{cases} \quad \text{and} \quad K_{n-j} = \begin{cases} j-8, & \text{if } j \geq 4, \\ -9, & \text{if } j = 3, \\ -8, & \text{if } j = 2, \\ -15, & \text{if } j = 1 \end{cases} \tag{3.28}$$

Now, substituting (3.25), (3.26), (3.27), and (3.28) into (3.24) and simplifying yields the desired formula.

We can also compute $\#\widehat{\mathcal{G}_{\mathscr{A}_n}}(\mathbb{Z}/8\mathbb{Z})$ by comparing two different formulas for a quantity known as "the 2-adic density of the quadratic lattice" defined by the matrix $\mathscr{A}_n$, which is up

to normalization the same as the 2-adic volume of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_2)$ with respect to Haar measure. We denote this quantity by $\alpha_2$. One of the two formulas for $\alpha_2$ is given in [45], where Cho constructs a smooth model of the group scheme $\mathcal{G}_{\mathscr{A}_n}$ over $\mathbb{Z}_2$. Letting $\widetilde{\mathcal{G}_{\mathscr{A}_n}}$ denote the special fiber of this smooth model, one can show by applying [45, Lemma 4.2, Remark 4.3, and Theorem 5.2] that

$$\alpha_2 = 2 \cdot 2^{-\frac{n(n-1)}{2}} \cdot \#\widetilde{\mathcal{G}_{\mathscr{A}_n}}(\mathbb{Z}/2\mathbb{Z}) = 2^{\frac{-n^2+3n+4}{2}} \cdot \#\,\mathrm{SO}_{n-1}(\mathbb{Z}/2\mathbb{Z}), \tag{3.29}$$

where $\mathrm{SO}_{n-1}$ denotes the special orthogonal group on an $(n-1)$-dimensional split orthogonal space. To be precise, $\alpha_2$ is defined in [45] to be $\frac{1}{2}$ of the quantity in (3.29), to account for the number of connected components of $\mathcal{G}_{\mathscr{A}_n}$ in $\widehat{\mathcal{G}_{\mathscr{A}_n}}$. However, we have removed this factor of $\frac{1}{2}$ to make the definition of $\alpha_2$ consistent with the one given by Conway and Sloane in [49, §12], who define $\alpha_2$ by

$$\alpha_2 = \frac{\#\widehat{\mathcal{G}_{\mathscr{A}_n}}(\mathbb{Z}/2^r\mathbb{Z})}{(2^r)^{\frac{n(n-1)}{2}}} \tag{3.30}$$

for any sufficiently large positive integer $r$. It follows from [75, Proposition 5.6.1(ii) and proof of Lemma 5.6.5] that we can take $r = 3$ in (3.30). Comparing (3.29) and (3.30) together with the fact that $\#\,\mathrm{SO}_{n-1}(\mathbb{Z}/2\mathbb{Z}) = 2^{\frac{n^2-4n+3}{4}}\left(2^{\frac{n-1}{2}}-1\right)\prod_{i=1}^{\frac{n-3}{2}}(2^{2i}-1)$ for $n \geq 3$ (see [45, §6]) yields that

$$\#\widehat{\mathcal{G}_{\mathscr{A}_n}}(\mathbb{Z}/8\mathbb{Z}) = 2^{n^2+2} \cdot \#\,\mathrm{SO}_{n-1}(\mathbb{Z}/2\mathbb{Z}) = 2^{\frac{5n^2-4n+11}{4}}\left(2^{\frac{n-1}{2}}-1\right)\prod_{i=1}^{\frac{n-3}{2}}(2^{2i}-1). \qquad \square$$

*Remark* 76. The strategy for the second proof of Proposition 75 can likewise be used to obtain a formula for $\#\widehat{\mathcal{G}_{\mathscr{A}_n}}(\mathbb{Z}/2^r\mathbb{Z})$ for each $r \geq 3$.

### 3.3.4 Orbits over $\mathbb{Z}_p$

Let $p$ be an odd prime. When $f$ is such that $R_f$ is the maximal order in $K_f$, we have the following loose bound for the number of orbits arising from points in $\mathscr{S}_f(\mathbb{Z}_p)$:

**Proposition 77.** *Let $p$ be an odd prime, and suppose that $R_f$ is maximal. Then there are at most $2^{m-1}$ orbits of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)$ on $W_{\mathscr{A}_n}(\mathbb{Z}_p)$ arising from points of $\mathscr{S}_f(\mathbb{Z}_p)$ via the construction in §3.2. The size of the stabilizer in $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)$ of any such orbit is $2^{m-1}$.*

*Proof.* By Theorem 39, the number of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)$-orbits on $W_{\mathscr{A}_n}(\mathbb{Z}_p)$ arising from elements of $H_{f,1}$ via the correspondence in Theorem 13 is equal to $\#(R_f^\times/R_f^{\times 2})_{\mathrm{N}\equiv 1} = 2^{m-1}$. By Theorem 13 and (1.9), the stabilizer of any such orbit has size $\#R_f^\times[2]_{\mathrm{N}\equiv 1} = 2^{m-1}$. □

When $p \nmid f_0$, Propositions 70 and 75 give tighter control on the size of $\mathscr{P}_p$ than Proposition 77, which we will only use for odd primes $p \mid f_0$. When $p \mid f_0$, it does not suffice to obtain a bound of the form $\mathrm{Vol}(\mathscr{P}_p) \ll 1$ (like the bounds obtained in Proposition 70 and 75). Indeed, since proving Theorems 61 and 62 involves averaging over *monicizations* of forms in $V_{n,f_0}(\mathbb{Z})$ (see §3.4.2), we must show that $\mathrm{Vol}(\mathscr{P}_p)$ is $\ll |f_0|_p^{\frac{n(n-1)}{2}}$, which is the $p$-adic density of the set of monicizations of forms in $V_{n,f_0}(\mathbb{Z}_p)$. At least for those forms $f \in V_{n,f_0}(\mathbb{Z}_p)_{\max}$, Proposition 77 will be enough to obtain the desired bound on $\mathrm{Vol}(\mathscr{P}_p)$.

### 3.3.5 Orbits over $\mathbb{Q}_p$ for $p \mid f_0$

Proposition 77 only applies when $R_f$ is the maximal order in $K_f$; in this section, we handle the remaining forms $f$ by controlling the number of orbits of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)$ on $W_{\mathscr{A}_n}(\mathbb{Q}_p)$ that can arise from points of $\mathscr{S}_f(\mathbb{Z}_p)$. To this end, suppose that $f \in V_{n,f_0}(\mathbb{Z}_p)$ splits as a product $m$ distinct irreducible factors over $\mathbb{Z}_p$. Then we have the following result:

**Proposition 78.** *Let $p$ be an odd (resp., even) prime. Then there are at most $2^{m+1}$ (resp., $2^{\frac{n+3}{2}+m}$) orbits of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)$ on $W_{\mathscr{A}_n}(\mathbb{Q}_p)$ arising from points of $\mathscr{S}_f(\mathbb{Z}_p)$ via the construction in §3.2. The size of the stabilizer in $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)$ of any such orbit is $\#K_f^\times[2]_{\mathrm{N}\equiv 1} = 2^{m-1}$.*

*Proof.* By Proposition 19 and (1.9), it is sufficient to bound the number of elements of $(K_f^\times/K_f^{\times 2})_{\mathrm{N}\equiv 1}$ of the form $f_0\alpha$, where $\alpha$ is the second coordinate of a pair $(I,\alpha) \in H_{f,1}$ arising from a points of $\mathscr{S}_f(\mathbb{Z}_p)$ via the construction in §3.2.

Fix $y_0 \in \mathbb{Z}_p$, and consider the monic odd-degree hyperelliptic curve $C_{f,y_0}$ of genus $\frac{n-1}{2}$ over $\mathbb{Q}_p$ defined by the affine equation $C_{f,y_0}\colon z^2 = f^{\mathsf{mon}}(x, y_0)$. Notice that $C_{f,y_0}$ is a quadratic twist of $C_{f,1}$ and that for $y_0' \in \mathbb{Z}_p$, the curves $C_{f,y_0}$ and $C_{f,y_0'}$ are isomorphic over $\mathbb{Q}_p$ when $y_0$ and $y_0'$ represent the same class in $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$. Let $\{\eta_1, \dots, \eta_\ell\} \subset \mathbb{Z}_p$ denote a complete set of representatives of elements of $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, and note that we can take $\ell = 4$ when $p$ is odd and $\ell = 8$ when $p = 2$. Then each $C_{f,y_0}$ is isomorphic to one of $C_{f,\eta_1}, \dots, C_{f,\eta_\ell}$.

Let $(x_0, y_0, z_0) \in \mathscr{S}_f(\mathbb{Z}_p)$ giving rise to a pair $(I, \alpha)$. Then the point $(f_0 x_0, z_0)$ is a $\mathbb{Q}_p$-rational point on the curve $C_{f,y_0}$ and hence is identified with a $\mathbb{Q}_p$-rational point $(x_0', z_0')$ on one of the curves $C_{f,\eta_i}$. In [15, §5], Bhargava and Gross show that points in $C_{f,\eta_i}(\mathbb{Q}_p)$ naturally give rise to orbits of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)$ on $W_{\mathscr{A}_n}(\mathbb{Q}_p)$ having characteristic polynomial $f^{\mathsf{mon}}(x, \eta_i)$. Under the construction of Bhargava and Gross, points of $C_{f,\eta_i}(\mathbb{Q}_p)$ give rise to $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)$-orbits on $W_{\mathscr{A}_n}(\mathbb{Q}_p)$ via the following composition:

$$C_{f,\eta_i}(\mathbb{Q}_p) \to J_i(\mathbb{Q}_p)/2J_i(\mathbb{Q}_p) \to H^1(\mathscr{G}_{\mathbb{Q}_p}, J_i[2]) \simeq (K_f^\times/K_f^{\times 2})_{\mathrm{N}\equiv 1}, \tag{3.31}$$

where $J_i$ is the Jacobian of $C_{f,\eta_i}$ and where we identify the set of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)$-orbits on $W_{\mathscr{A}_n}(\mathbb{Q}_p)$ having characteristic polynomial $f^{\mathsf{mon}}(x, y_0)$ with $(K_f^\times/K_f^{\times 2})_{\mathrm{N}\equiv 1}$ via Proposition 19. The composite map in (3.31) is known as the *Cassels map* and was first studied by Cassels in [44].

Let $\theta' \in K_f$ be the image of $x$ under the identification $\mathbb{Q}_p[x]/f^{\mathsf{mon}}(x, 1) \simeq K_f$. If $z_0 = 0$, then $f^{\mathsf{mon}}(x, \eta_i y)$ factors uniquely as

$$f^{\mathsf{mon}}(x, \eta_i y) = \big(x - f_0 \tfrac{x_0}{y_0}\eta_i y\big)\widetilde{f}^{\mathsf{mon}}(x, \eta_i y)$$

where $\widetilde{f}^{\mathsf{mon}} \in V_{n-1,1}(\mathbb{Z}_p)$. (The notation $\widetilde{f}^{\mathsf{mon}}$ makes sense, because $\widetilde{f}^{\mathsf{mon}}$ is indeed the monicized form of $\widetilde{f}$ as defined in (3.3).) Using the explicit description of the Cassels map

stated in [39, §2], one finds that the point $(x_0', c') \in C_{f,\eta_i}(\mathbb{Q}_p)$ gives rise to the class

$$\left.\begin{array}{ll} x_0' - \theta'\eta_i, & \text{if } z_0 \neq 0, \\ \widetilde{f}^{\mathsf{mon}}(\theta'\eta_i, \eta_i) + (x_0' - \theta'\eta_i), & \text{if } z_0 = 0 \end{array}\right\} \equiv f_0\alpha \in (K_f^\times / K_f^{\times 2})_{\mathrm{N}\equiv 1}.$$

Meanwhile, by Proposition 19, the class in $(K_f^\times/K_f^{\times 2})_{\mathrm{N}\equiv 1}$ corresponding to $(x_0, y_0, z_0) \in \mathscr{S}_f(\mathbb{Z}_p)$ is also $f_0\alpha$. Thus, the number of elements of $(K_f^\times/K_f^{\times 2})_{\mathrm{N}\equiv 1}$ of the form $f_0\alpha$ arising form points of $\mathscr{S}_f(\mathbb{Z}_p)$ is bounded above by the total number of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)$-orbits on $W_{\mathscr{A}_n}(\mathbb{Q}_p)$ arising from $\mathbb{Q}_p$-rational points on any one of the finitely many curves $C_{f,\eta_1}, \ldots, C_{f,\eta_\ell}$. By [15, §6.2], the number of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)$-orbits on $W_{\mathscr{A}_n}(\mathbb{Q}_p)$ arising from each $C_{f,\eta_i}$ is at most $2^{m_i-1}$ when $p$ is odd (resp., $2^{\frac{n-3}{2}+m_i}$ when $p=2$), where $m_i$ is the number of distinct irreducible factors of $f^{\mathsf{mon}}(x, \eta_i)$. But clearly $m_i = m$ for each $i$, so we get the desired upper bound of $\ell \cdot 2^{m-1}$ when $p$ is odd (resp., $2^{\frac{n-3}{2}+m}$ when $p=2$).

As for the statement about stabilizers, by Proposition 19 and (1.9), the stabilizer of any orbit arising via $\mathsf{orb}_{f,1}$ is isomorphic to $K_f^\times[2]_{\mathrm{N}\equiv 1}$, which has size $\#K_f^\times[2]_{\mathrm{N}\equiv 1} = 2^{m-1}$. □

## 3.4 Proof of Theorem 61

For a monic polynomial $f(x) = x^{2n+1} + \sum_{i=1}^n c_i x^{n-i} \in \mathbb{Z}[x]$, let the *height* of $f$ be defined by $H(f) := H(c_1, \ldots, c_{2n+1}) := \max\{|c_i|^{n(n-1)/i} : i = 1, \ldots, n\}$. For an element $T \in W_{\mathscr{A}_n}(\mathbb{Z})$, let the *height* of (the $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$-orbit of) $T$ be defined by $H(T) = H(\mathrm{ch}_T)$. We say that (the $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$-orbit of) $T$ is *irreducible* if $\mathrm{ch}_T$ is separable and the $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q})$-orbit of $T$ is non-distinguished.

### 3.4.1 Counting irreducible integral orbits of bounded height

In this section, we give a count of the number of irreducible orbits of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $W_{\mathscr{A}_n}(\mathbb{Z})$ of bounded height. We use this count in §3.4.2, where we sieve to those integral orbits that arise from integral points.

Recalling the notation defined in §3.3.1, fix $m \in \{0, \ldots, \frac{n-1}{2}\}$ and $\tau \in \{1, \ldots, 2m+1\}$.

Let $W_{\mathscr{A}_n}(\mathbb{Z})^{(m,\tau)} := W_{\mathscr{A}_n}^{(m,\tau)} \cap W_{\mathscr{A}_n}(\mathbb{Z})$, and let $N(W_{\mathscr{A}_n}(\mathbb{Z})^{(m,\tau)}; X)$ denote the number of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$-orbits of irreducible elements $T \in W_{\mathscr{A}_n}(\mathbb{Z})^{(m,\tau)}$ satisfying $H(T) < X$. Then we have the following adaptation of [15, Theorem 10.1 and (10.27)]:

**Theorem 79.** *There exists a nonzero constant $\mathcal{J} \in \mathbb{Q}$ such that*

$$N(W_{\mathscr{A}_n}(\mathbb{Z})^{(m,\tau)}; X) = \frac{|\mathcal{J}|}{2^{m+\frac{n-1}{2}}} \cdot \mathrm{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})\backslash\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})) \cdot \int_{\substack{(c_1,\ldots,c_{2n+1})\in\mathcal{I}(m) \\ H(c_1,\ldots,c_n)<X}} dc_1 \cdots dc_n + o(X^{\frac{n+1}{2n-2}}),$$

*where the fundamental volume* $\mathrm{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})\backslash\mathcal{G}_{\mathscr{A}_n}(\mathbb{R}))$ *is computed with respect to a differential $\omega$ that generates the rank-*1 *module of top-degree differentials of $G$ over $\mathbb{Z}$.*

*Proof.* In [15], Bhargava and Gross work with the subrepresentation $W'_{\mathscr{A}_n} \subset W_{\mathscr{A}_n}$ consisting of the traceless operators in $W_{\mathscr{A}_n}$. Such traceless operators have characteristic polynomial with the coefficient $c_1$ of the term $x^{n-1}$ equal to 0. They prove that $N(W'_{\mathscr{A}_n}(\mathbb{Z})^{(m,\tau)}; X)$ is given by a formula (see [15, Theorem 10.1 and (10.27)]) that is almost identical to the formula in the statement of Theorem 79, except that the value of $\mathcal{J}$ may be different and the integral runs over $(0, c_2, \ldots, c_n) \in \mathcal{I}(m)$. By simply lifting the restriction that $c_1 = 0$, it is not hard to check that the proof of [15, Theorem 10.1 and (10.27)] carries over with minimal modifications to prove Theorem 79. □

In the following lemma, we derive an upper bound on the constant $|\mathcal{J}|$ in Theorem 79:

**Lemma 80.** *We have that*

$$|\mathcal{J}| \leq 2^{n-1} \cdot \mathrm{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_2)) \cdot \prod_{p>2} \frac{p^{\frac{n(n-1)}{2}} \cdot \mathrm{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p))}{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})}.$$

*Proof.* Let $R = \mathbb{C}$, $\mathbb{R}$, or $\mathbb{Z}_p$ where $p$ is a prime. Let $\mathcal{R} \subset R^n$ be any open subset, and let $s\colon \mathcal{R} \to W_{\mathscr{A}_n}(R)$ be a continuous function such that the characteristic polynomial of $s(c_1, \ldots, c_n)$ is given by $x^n + \sum_{i=1}^n c_i x^{n-i}$ for every $(c_1, \ldots, c_n) \in \mathcal{R}$. The constant $\mathcal{J}$ arises as a multiplicative factor in the following change-of-measure formula:

**Proposition 81.** *For any measurable function $\phi$ on $W_{\mathscr{A}_n}(R)$, we have*

$$\int_{T \in \mathcal{G}_{\mathscr{A}_n}(R) \cdot s(\mathcal{R})} \phi(T) dT = |\mathcal{J}| \cdot \int_{\mathcal{R}} \int_{\mathcal{G}_{\mathscr{A}_n}(R)} \phi(g \cdot s(c_1, \ldots, c_n)) \omega(g) dr,$$

*where we regard $\mathcal{G}_{\mathscr{A}_n}(R) \cdot s(\mathcal{R})$ as a multiset, $|-|$ denotes the standard absolute value on $R$, $dT$ is the Euclidean measure on $W_{\mathscr{A}_n}(R)$, and $dr$ is the restriction to $\mathcal{R}$ of the Euclidean measure on $R^n$.*

*Proof of Proposition 81.* The proof is identical to that of [26, Proposition 3.11]. □

In particular, the constant $\mathcal{J}$ is independent of the choices of $R = \mathbb{C}$, $\mathbb{R}$, or $\mathbb{Z}_p$ and of the region $\mathcal{R}$ and the functions $s$ and $\phi$. Thus, to compute $|\mathcal{J}|$, we can make the following convenient choices: take $R = \mathbb{Z}_p$, so that $|-| = |-|_p$; take

$$\mathcal{R} = \left\{ (c_1, \ldots, c_n) \in \mathbb{Z}_p^n : x^n + \sum_{i=1}^{n} c_i x^{n-i} \equiv f \pmod{p} \right\}$$

for a fixed monic irreducible degree-$n$ polynomial $f \in (\mathbb{Z}/p\mathbb{Z})[x]$; letting $\Sigma_f := \{T \in W_{\mathscr{A}_n}(\mathbb{Z}_p) : \mathrm{ch}_T \equiv f \pmod{p}\}$, take $s$ to be any continuous right-inverse to the function that sends $T \in \Sigma_f$ to the list of coefficients of $\mathrm{ch}_T$; and take $\phi$ to be the function that sends $T \in \Sigma_f$ to $\frac{1}{\#\,\mathrm{Stab}(T)}$, where $\mathrm{Stab}(T) \subset \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)$ is the stabilizer of $T$, and sends $T \in W_{\mathscr{A}_n}(\mathbb{Z}_p) \smallsetminus \Sigma_f$ to 0. The existence of the right-inverse $s$ is well-known; see, e.g., §5.2.3.

Because $\phi$ is $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)$-invariant, Proposition 81 yields that for the above convenient choices, we have on the one hand that

$$\begin{aligned} \mathrm{Vol}(\Sigma_f) &= \int_{T \in \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p) \cdot s(\mathcal{R})} \frac{1}{\#\,\mathrm{Stab}(T)} dT \\ &= |\mathcal{J}|_p \cdot \mathrm{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)) \cdot \int_{f' \equiv f \,(\mathrm{mod}\, p)} \sum_{\substack{T \in \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p) \backslash \Sigma_f \\ \mathrm{ch}_T = f'}} \frac{1}{\#\,\mathrm{Stab}(T)} dr. \end{aligned} \tag{3.32}$$

First suppose $p \neq 2$. We now compute the sum in the integrand in (3.32). Because we chose

$f$ to be irreducible over $\mathbb{Z}/p\mathbb{Z}$, the ring $R_{f'} := \mathbb{Z}_p[x]/(f')$ is the maximal order in its field of fractions $K_{f'}$, and it is in fact the unique local ring of rank $n$ over $\mathbb{Z}_p$ having residue field $\mathbb{F}_{p^n}$ (hence $R_{f'}$ does not depend on the choice of $f'$). Then by Theorem 39, there is precisely one $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)$-orbit with characteristic polynomial $f'$, and the size of the stabilizer of this orbit is equal to $\#R_{f'}^{\times}[2]_{\mathrm{N}\equiv 1} = 1$. Thus, we find that

$$\sum_{\substack{T \in \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)\backslash \Sigma_f \\ \mathrm{ch}_T = f'}} \frac{1}{\#\operatorname{Stab}(T)} = 1. \tag{3.33}$$

Combining (3.32) and (3.33) yields that

$$\operatorname{Vol}(\Sigma_f) = |\mathcal{J}|_p \cdot \operatorname{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)) \cdot \int_{f' \equiv f \,(\mathrm{mod}\, p)} dr = |\mathcal{J}|_p \cdot \frac{\operatorname{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p))}{p^n}. \tag{3.34}$$

Let $\overline{\Sigma}_f := \{T \in W_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z}) : \mathrm{ch}_T = f\}$. Then the mod-$p$ reduction map $\Sigma_f \to \overline{\Sigma}_f$ is surjective, and we have by [15, §6.1] that $\#\overline{\Sigma}_f = \#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})$. Thus, we have on the other hand that

$$\operatorname{Vol}(\Sigma_f) = \frac{\#\overline{\Sigma}_f}{p^{\dim W_{\mathscr{A}_n}}} = \frac{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})}{p^{\frac{n(n+1)}{2}}}. \tag{3.35}$$

Equating (3.34) and (3.35) yields that

$$|\mathcal{J}|_p = \frac{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})}{p^{\frac{n(n-1)}{2}} \cdot \operatorname{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p))} \tag{3.36}$$

when $p \neq 2$.

Next, suppose $p = 2$. We now derive an upper bound on the sum in the integrand in (3.32). By Theorem 39, the number of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_2)$-orbits with characteristic polynomial $f'$ is equal to $2^{\frac{n-3}{2}}\left(2^{\frac{n-1}{2}}+1\right)$. The size of the stabilizer of any such orbit is equal to $\#R_{f'}^{\times}[2]_{\mathrm{N}\equiv 1} = 1$, so we find that

$$\sum_{\substack{T \in \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)\backslash \Sigma_f \\ \mathrm{ch}_T = f'}} \frac{1}{\#\operatorname{Stab}(T)} = 2^{\frac{n-3}{2}}\left(2^{\frac{n-1}{2}}+1\right). \tag{3.37}$$

Combining (3.32) and (3.37) yields that

$$\mathrm{Vol}(\Sigma_f) = |\mathcal{J}|_2 \cdot \mathrm{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_2)) \cdot \frac{2^{\frac{n-3}{2}}\left(2^{\frac{n-1}{2}}+1\right)}{2^n}. \tag{3.38}$$

Let $\overline{\Sigma}_f = \{T \in W_{\mathscr{A}_n}(\mathbb{Z}/2\mathbb{Z}) : \mathrm{ch}_T = f\}$. Then the mod-2 reduction map $\Sigma_f \to \overline{\Sigma}_f$ is surjective, and by (1.9) and Proposition 19, the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/2\mathbb{Z})$ on $\overline{\Sigma}_f$ is simply transitive, so $\#\overline{\Sigma}_f = \#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/2\mathbb{Z})$. Thus, we have on the other hand that

$$\mathrm{Vol}(\Sigma_f) = \frac{\#\overline{\Sigma}_f}{2^{\dim W_{\mathscr{A}_n}}} = \frac{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/2\mathbb{Z})}{2^{\frac{n(n+1)}{2}}}. \tag{3.39}$$

Combining (3.38) and (3.39) yields that

$$|\mathcal{J}|_2^{-1} = 2^{n-1} \cdot \mathrm{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_2)) \cdot \frac{2^{\frac{n^2-2n-1}{2}}\left(2^{\frac{n-1}{2}}+1\right)}{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/2\mathbb{Z})} \tag{3.40}$$

Since $\mathcal{G}_{\mathscr{A}_n}$ is not smooth over $\mathbb{Z}_2$, computing $\mathrm{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_2))$ is far more complicated, but we do not need to know the value of $\mathrm{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_2))$ for our purpose. The value of $\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/2\mathbb{Z})$ is given in [45, §6] to be $\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/2\mathbb{Z}) = 2^{\left(\frac{n-1}{2}\right)^2}\prod_{i=1}^{\frac{n-1}{2}}(2^{2i}-1)$, so it follows that

$$\frac{2^{\frac{n^2-2n-1}{2}}\left(2^{\frac{n-1}{2}}+1\right)}{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/2\mathbb{Z})} = \left(2^{-1}+2^{-\frac{n+1}{2}}\right)\prod_{i=1}^{\frac{n-1}{2}}(1-2^{-2i})^{-1} \leq 1. \tag{3.41}$$

Applying the identity

$$|\mathcal{J}|\prod_p |\mathcal{J}|_p = 1 \tag{3.42}$$

to (3.36), (3.40), and (3.41) completes the proof of Lemma 80. □

### 3.4.2 Sieving to orbits arising from local points when $2 \nmid f_0$

Let $V_{n,f_0}(\mathbb{Z})^*$ be the subset of all $F \in V_{n,f_0}(\mathbb{Z})$ satisfying both conditions in Proposition 68 for every prime $p \mid k$. Let $\delta$ be the upper density of forms $F \in V_{n,f_0}(\mathbb{Z})$, enumerated by

height, such that $\mathscr{S}_f(\mathbb{Z}) \neq \varnothing$. Then $\delta$ is bounded as follows:

$$\delta \leq \lim_{X\to\infty} \frac{\#\{f \in V_{n,f_0}(\mathbb{Z})^* : H(f) < X\} + \#\big(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q})\backslash\{T \in W_{\mathscr{A}_n}(\mathbb{Z}) : T \text{ is good, } H(T) < X\}\big)}{\#\{f \in V_{n,f_0}(\mathbb{Z}) : H(f) < X\}}, \tag{3.43}$$

where we say that $T \in W_{\mathscr{A}_n}(\mathbb{Z})$ is *good* if it is irreducible and $T \in \mathscr{P}_v$ for every place $v$. The first term in the numerator and the denominator on the right-hand side of (3.43) are respectively given by

$$\#\{f \in V_{n,f_0}(\mathbb{Z})^* : H(f) < X\} = \mu_{f_0} \cdot f_0^{-\frac{n(n-1)}{2}} \cdot 2^n \cdot X^{\frac{n+1}{2n-2}} + o(X^{\frac{n+1}{2n-2}}), \quad \text{and} \tag{3.44}$$

$$\#\{f \in V_{n,f_0}(\mathbb{Z}) : H(f) < X\} = f_0^{-\frac{n(n-1)}{2}} \cdot 2^n \cdot X^{\frac{n+1}{2n-2}} + o(X^{\frac{n+1}{2n-2}}). \tag{3.45}$$

We now bound the second term in the numerator on the right-hand side of (3.43). To do this, we use the following result, which generalizes Theorem 79 by giving an upper bound on the number of integral orbits of height up to $X$ satisfying certain infinite sets of local conditions:

**Theorem 82** (cf. [15, Theorem 10.12])**.** *Let $\phi\colon W_{\mathscr{A}_n}(\mathbb{Z}) \to [0,1] \subset \mathbb{R}$ be a function such that there exists a function $\phi_p\colon W_{\mathscr{A}_n}(\mathbb{Z}_p) \to [0,1]$ for each prime $p$ satisfying the following:*

- *For all $T \in W_{\mathscr{A}_n}(\mathbb{Z})$, the product $\prod_p \phi_p(T)$ converges to $\phi(T)$; and*
- *For each $p$, the function $\phi_p$ is locally constant outside a closed set $S_p \subset W_{\mathscr{A}_n}(\mathbb{Z}_p)$ of measure 0.*

*Let $N_\phi(W_{\mathscr{A}_n}(\mathbb{Z})^{m,\tau}; X)$ be the number of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$-orbits of irreducible elements $T \in W_{\mathscr{A}_n}(\mathbb{Z})^{m,\tau}$ satisfying $H(T) < X$, where each orbit $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}) \cdot T$ is counted with weight $\phi(T) := \prod_p \phi_p(T)$. Then we have that*

$$N_\phi(W_{\mathscr{A}_n}(\mathbb{Z})^{(m,\tau)}; X) \leq N(W_{\mathscr{A}_n}(\mathbb{Z})^{(m,\tau)}; X) \prod_p \int_{T\in W_{\mathscr{A}_n}(\mathbb{Z}_p)} \phi_p(T)dT + o(X^{\frac{n+1}{2n-2}}).$$

*Proof.* The proof is identical to the first half of the proof of [26, Theorem 2.21] (note that

the "acceptable" hypothesis in [26, Theorem 2.21] is not needed for the upper bound in Theorem 82). □

To apply Theorem 82 to bound the second term in the numerator of (3.43), we need to choose the weight functions $\phi_p$. Given $T \in W_{\mathscr{A}_n}(\mathbb{Z})$, denote by $m(T)$ the quantity

$$m(T) := \sum_{T' \in \mathcal{O}(T)} \frac{\#\operatorname{Stab}_{\mathbb{Q}}(T')}{\#\operatorname{Stab}_{\mathbb{Z}}(T')} = \sum_{T' \in \mathcal{O}(T)} \frac{\#\operatorname{Stab}_{\mathbb{Q}}(T)}{\#\operatorname{Stab}_{\mathbb{Z}}(T')},$$

where $\mathcal{O}(T)$ denotes a set of representatives for the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on the $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q})$-orbit of $T$, and where $\operatorname{Stab}_{\mathbb{Q}}(T')$ and $\operatorname{Stab}_{\mathbb{Z}}(T')$ respectively denote the stabilizers of $T'$ in $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q})$ and $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$. By [15, Proposition 10.8], counting $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q})$-orbits on $W_{\mathscr{A}_n}(\mathbb{Z})$ is, up to a negligible error, no different from counting $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$-orbits on $W_{\mathscr{A}_n}(\mathbb{Z})$, where the $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$-orbit of $T \in W_{\mathscr{A}_n}(\mathbb{Z})$ is weighted by $1/m(T)$.

The weight $m(T)$ can be expressed as a product over primes $p$ of local weights $m_p(T)$. Indeed, as stated in [15, (11.3)], we have that

$$m(T) = \prod_p m_p(T), \quad \text{where} \quad m_p(T) := \sum_{T' \in \mathcal{O}_p(T)} \frac{\#\operatorname{Stab}_{\mathbb{Q}_p}(T)}{\#\operatorname{Stab}_{\mathbb{Z}_p}(T')}, \tag{3.46}$$

where $\mathcal{O}_p(T)$ denotes a set of representatives for the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)$ on the $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)$-orbit of $T$, and where $\operatorname{Stab}_{\mathbb{Q}_p}(T')$ and $\operatorname{Stab}_{\mathbb{Z}_p}(T')$ respectively denote the stabilizers of $T'$ in $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)$ and $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)$.

For each prime $p$, let $\psi_p \colon W_{\mathscr{A}_n}(\mathbb{Z}_p) \to \{0,1\} \subset \mathbb{R}$ be the indicator function of elements $T \in \mathscr{P}_p$ such that $\operatorname{ch}_T$ is separable. Then upon taking $\phi_p = \psi_p/m_p$ for each $p$, Proposition 69 and Theorem 82 together imply that the numerator of (3.43) is bounded above by

$$\sum_{m=0}^{\frac{n-1}{2}} \sum_{\tau=1}^{2m+1} N(W_{\mathscr{A}_n}(\mathbb{Z})^{m,\tau}; X) \cdot \prod_p \int_{T \in W_{\mathscr{A}_n}(\mathbb{Z}_p)} \frac{\psi_p(T)}{m_p(T)} dT + o(X^{\frac{n+1}{2n-2}}). \tag{3.47}$$

In the following proposition, we give a formula for the integrals over $W_{\mathscr{A}_n}(\mathbb{Z}_p)$ in (3.47):

**Proposition 83.** *Let $p$ be a prime and let $\psi$ be a continuous $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)$-invariant function on $W_{\mathscr{A}_n}(\mathbb{Z}_p)$ such that every element $T \in W_{\mathscr{A}_n}(\mathbb{Z}_p)$ in the support of $\psi$ is separable. Then we have*

$$\int_{T\in W_{\mathscr{A}_n}(\mathbb{Z}_p)} \frac{\psi(T)}{m_p(T)} dT = |\mathcal{J}|_p \cdot \mathrm{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)) \cdot \int_{(c_1,\dots,c_n)\in\mathbb{Z}_p^n} \sum_{\substack{T\in\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)\backslash W_{\mathscr{A}_n}(\mathbb{Z}_p) \\ \mathrm{ch}_T = x^n + c_1 x^{n-1} + \cdots + c_n}} \frac{\psi(T)}{\#\,\mathrm{Stab}_{\mathbb{Q}_p}(T)}\, dc_1 \cdots dc_n,$$

*where $\mathcal{J} \in \mathbb{Q}$ is the same constant that appears in Theorem 79.*

*Proof.* The proof is identical to that of [15, Corollary 11.3]. □

If $2 \neq p \mid f_0$, combining Proposition 78, Lemma 80, and Proposition 83 yields that

$$\begin{aligned}\int_{T\in W_{\mathscr{A}_n}(\mathbb{Z}_p)} \frac{\psi_p(T)}{m_p(T)} dT &\leq |\mathcal{J}|_p \cdot \mathrm{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)) \cdot \int_{\substack{\vec{c}=(c_1,\dots,c_n)\in\mathbb{Z}_p^n \\ f_0^{i-1} | c_i \text{ for every } i}} \frac{2^{m(\vec{c})+1}}{2^{m(\vec{c})-1}}\, dc_1 \cdots dc_n, \\ &= 4 \cdot \mathrm{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)) \cdot |f_0|_p^{\frac{n(n-1)}{2}}, \end{aligned} \tag{3.48}$$

where $m(\vec{c})$ is the number of irreducible factors of the polynomial $x^n + \sum_{i=1}^n c_i x^{n-i} \in \mathbb{Z}_p[x]$. Similarly, when $2 = p \mid f_0$, combining Proposition 78 and Proposition 83 yields that

$$\int_{T\in W_{\mathscr{A}_n}(\mathbb{Z}_2)} \frac{\psi_2(T)}{m_2(T)} dT \leq 8 \cdot 2^{\frac{n-1}{2}} \cdot |\mathcal{J}|_2 \cdot \mathrm{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_2)) \cdot |f_0|_2^{\frac{n(n-1)}{2}}. \tag{3.49}$$

Next, for odd primes $p \nmid f_0$, Proposition 70 gives an upper bound on $\mathrm{Vol}(\mathscr{P}_p) = \int_{T\in W_{\mathscr{A}_n}(\mathbb{Z}_p)} \psi_p(T) dT$. Upon observing that $m_p(T) \geq 1$, we deduce that the factor at $p$ in (3.47) is bounded by

$$\int_{T\in W_{\mathscr{A}_n}(\mathbb{Z}_p)} \frac{\psi_p(T)}{m_p(T)} dT \leq \mathrm{Vol}(\mathscr{P}_p) \leq \min\left\{1, \sum_{m=1}^n \frac{p+1}{2^{m-1}} \cdot \mathrm{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)) \cdot \frac{\#\mathcal{I}_p(m)}{p^n}\right\} \tag{3.50}$$

If $2 = p \nmid f_0$, then we can use Proposition 73 to similarly deduce that

$$\int_{T \in W_{\mathscr{A}_n}(\mathbb{Z}_2)} \frac{\psi_2(T)}{m_2(T)} dT \leq \mathrm{Vol}(\mathscr{P}_2) \leq \sum_{m=1}^{n} \frac{12}{2^{n+m-2}} \cdot 2 \cdot \frac{\#\mathcal{I}_8(m)}{8^n}. \tag{3.51}$$

### 3.4.3 The final step

By [80], the Tamagawa number of $\mathcal{G}_{\mathscr{A}_n}$ is equal to 2, so we have

$$\mathrm{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}) \backslash \mathcal{G}_{\mathscr{A}_n}(\mathbb{R})) \prod_p \mathrm{Vol}(\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)) = 2. \tag{3.52}$$

We can now apply Theorem 79, Lemma 80, and the bounds in (3.48), (3.49), (3.50), and (3.51) to bound (3.47); combining the result with (3.44) and (3.45) gives a bound on $\delta$ via (3.43). Then, simplifying this bound using (3.42) and (3.52), we draw the following conclusions:

*Case 1:* $2 \nmid f_0$. When $2 \nmid f_0$, we have

$$\delta - \mu_{f_0} \ll \left( \sum_{m=0}^{\frac{n-1}{2}} 2^{n-1} \cdot \frac{2m+1}{2^{\frac{n-1}{2}+m}} \cdot \mu(\mathcal{I}(m)) \right) \cdot \left( \sum_{m=1}^{n} \frac{1}{2^{n+m-1}} \cdot \frac{\#\mathcal{I}_8(m)}{8^n} \right) \cdot \tag{3.53}$$
$$\left( \prod_{p \nmid 2 f_0} \min \left\{ \frac{p^{\frac{n(n-1)}{2}}}{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})}, \sum_{m=1}^{n} \frac{p+1}{2^{m-1}} \cdot \frac{\#\mathcal{I}_p(m)}{p^n} \right\} \right)$$

where $\mu(\mathcal{I}(m)) := (2^n \cdot X^{\frac{n+1}{2n-2}})^{-1} \cdot \int_{\substack{(c_1,\ldots,c_n) \in \mathcal{I}(m) \\ H(c_1,\ldots,c_n) < X}} dc_1 \cdots dc_n$ denotes the probability that a monic degree-$n$ polynomial over $\mathbb{R}$ has $2m+1$ real roots, and where the implied constant is independent of $n$. In (3.53), the archimedean factor is $O(2^{\frac{n}{2}})$, the factor at primes dividing $f_0$ is $O(1)$, and the factor at 2 is $O(2^{-n})$.

We now bound the factor at odd primes not dividing $f_0$. The following lemma allows us to bound the factors at primes less than a small power of the degree $n$:

**Lemma 84.** *We have for each fixed $A \in (0, 1/3) \subset \mathbb{R}$ that*

$$\prod_{3 \leq p \leq n^A} \sum_{m=1}^{n} \frac{p+1}{2^{m-1}} \cdot \frac{\#\mathcal{I}_p(m)}{p^n} \ll 2^{-\varepsilon_1 n^{\varepsilon_2}},$$

*where $\varepsilon_1, \varepsilon_2 > 0$ are real numbers that may depend on $A$.*

*Proof.* We first estimate each factor in the product over primes. We split the sum at the prime $p$ into two ranges, one for $m \leq \frac{1}{2}\log n$ and one for $m > \frac{1}{2}\log n$. We bound the sum over $m > \frac{1}{2}\log n$ as follows:

$$\sum_{\frac{1}{2}\log n < m \leq n} \frac{p+1}{2^{m-1}} \cdot \frac{\#\mathcal{I}_p(m)}{p^n} \leq \sum_{\frac{1}{2}\log n < m \leq n} \frac{p+1}{2^{m-1}} \leq \frac{2(p+1)}{\sqrt{n}}. \tag{3.54}$$

For the sum over $m < \frac{1}{2}\log n$, we rely on the following result of Afshar and Porritt:[2]

**Theorem 85** ([1, Remark 2.11])**.** *Let $p$ be a prime, and let $1 \leq m \leq \log n$. Then we have the following uniform estimate:*

$$\frac{\#\mathcal{I}_p(m)}{p^n} = \frac{1}{n} \cdot \frac{(\log n)^{m-1}}{(m-1)!} \cdot \left( D_p\left(\frac{m-1}{\log n}\right) + O\left(\frac{m}{(\log n)^2}\right)\right)$$

*where the implied constant is absolute (i.e., does not depend on $p$), and where the function $D_p$ is defined as follows. Letting $\mathcal{I} \subset (\mathbb{Z}/p\mathbb{Z})[x]$ be the set of all monic irreducible polynomials, we have that*

$$D_p(z) = \frac{E(1/p, z)}{\Gamma(1+z)}, \quad \text{where} \quad E(x, z) = \prod_{f \in \mathcal{I}} \left(1 + \frac{z x^{\deg f}}{1 - x^{\deg f}}\right) \cdot (1 - x^{\deg f})^z.$$

We now turn the very careful estimate in Theorem 85 into a more easily usable form.

[2]Note that a result of this type was first proven by Car in [42]; the dependence of the error term on the prime $p$ was made explicit in [1].

First, notice that for any $x \in (0, 1/2) \subset \mathbb{R}$ and $z \in (0, 1)$ we have

$$\left(1 + \frac{zx}{1-x}\right) \cdot (1-x)^z \leq \left(1 + \frac{zx}{1-x}\right) \cdot (1 - zx) = 1 + \frac{(z - z^2)x^2}{1-x} \leq 1 + x^2. \tag{3.55}$$

By Carlitz's Theorem (see [43]), there are exactly $p^{d-1}$ monic separable polynomials of degree $d$ over $\mathbb{Z}/p\mathbb{Z}$, and hence at most $p^{d-1}$ monic irreducible polynomials of degree $d$ over $\mathbb{Z}/p\mathbb{Z}$. Using this together with (3.55), we deduce that

$$E(1/p, z) \leq \prod_{f \in \mathcal{I}} (1 + p^{-2 \deg f}) \leq \prod_{d=1}^{\infty} (1 + p^{-2d})^{p^{d-1}}. \tag{3.56}$$

To estimate the right-hand side of (3.56), we take its logarithm and apply the bound $\log(1 + x) \leq x$ (which holds for $x > -1$):

$$\log \left( \prod_{d=1}^{\infty} (1 + p^{-2d})^{p^{d-1}} \right) = \sum_{d=1}^{\infty} p^{d-1} \cdot \log(1 + p^{-2d}) \leq \sum_{d=1}^{\infty} p^{d-1} \cdot p^{-2d} = \frac{1}{p(p-1)}. \tag{3.57}$$

Taking $p = 2$ in (3.57) and using the fact that $\Gamma(1 + z) > 1/2$, we have for any prime $p$, any $1 \leq m \leq \log n$, and all sufficiently large $n$ that

$$D_p \left( \frac{m-1}{\log n} \right) + O\left( \frac{m}{(\log n)^2} \right) \leq 2\sqrt{e} + O\left( \frac{m}{(\log n)^2} \right) \leq 4, \tag{3.58}$$

where $e$ denotes the usual base of the natural logarithm. Upon combining (3.54), (3.58), and Theorem 85, we find for all sufficiently large $n$ that

$$\begin{aligned} \sum_{m=1}^{n} \frac{p+1}{2^{m-1}} \cdot \frac{\#\mathcal{I}_p(m)}{p^n} &\leq \frac{2(p+1)}{\sqrt{n}} + \sum_{1 \leq m \leq \frac{1}{2}\log n} \frac{4(p+1)}{n} \cdot \frac{(\frac{1}{2}\log n)^{m-1}}{(m-1)!} \\ &\leq \frac{2(p+1)}{\sqrt{n}} + \frac{4(p+1)}{n} \cdot e^{\frac{1}{2}\log n} = \frac{6p+6}{\sqrt{n}} \leq \frac{8p}{\sqrt{n}}, \end{aligned} \tag{3.59}$$

where we have used the fact that $\sum_{i=0}^{N} \frac{x^i}{i!} \leq e^x$ for any $x > 0$ and integer $N \geq 0$. By Erdős' proof of Bertrand's Postulate, we have $\prod_{p<N} < 4^N$ for any $N \geq 3$. By the Prime Number

Theorem, for any $\varepsilon > 0$, there exists an integer $N > 0$ such that for all $N' > N$, the number of primes less than or equal to $N'$ is at least $(1-\varepsilon) \cdot \frac{N'}{\log N'}$ and is at most $(1+\varepsilon) \cdot \frac{N'}{\log N'}$. Combining this fact with (3.59), we find for any fixed $A < 1/3$ and all sufficiently large $n$ (where "large" depends on $A$ and $\varepsilon$) that

$$\prod_{3 \le p \le n^A} \sum_{m=1}^{n} \frac{p+1}{2^{m-1}} \cdot \frac{\#\mathcal{I}_p(m)}{p^n} \le \frac{8^{(1+\varepsilon)\cdot \frac{n^A}{A \log n}} \cdot 4^{n^A}}{(\sqrt{n})^{(1-\varepsilon)\cdot \frac{n^A}{A \log n}}} \ll 2^{-\varepsilon_1 n^{\varepsilon_2}},$$

for some real numbers $\varepsilon_2, \varepsilon_2 > 0$. □

The following lemma allows us to bound the factors at the remaining primes:

**Lemma 86.** *We have that*

$$\prod_{p>2} \frac{p^{\frac{n(n-1)}{2}}}{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})} \ll 1,$$

*where the implied constant does not depend on $n$.*

*Proof.* From (3.19), it follows that

$$\log \frac{p^{\frac{n(n-1)}{2}}}{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})} = \sum_{i=1}^{\frac{n-1}{2}} -\log(1-p^{-2i}) \le 2 \cdot \sum_{i=1}^{\frac{n-1}{2}} p^{-2i} \le \frac{2}{p^2-1}, \tag{3.60}$$

where we have applied the bound $-\log(1-x) \le 2x$, which holds for $x \in (0, 1/2) \subset \mathbb{R}$. It is not hard to check (by comparing derivatives) that $\frac{2}{p^2-1} \le \log(1+p^{-\frac{3}{2}})$ for each $p \ge 5$. Thus,

$$\prod_{p>2} \frac{p^{\frac{n(n-1)}{2}}}{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})} \le \frac{e^{\frac{1}{4}}}{(1+2^{-\frac{3}{2}})(1+3^{-\frac{3}{2}})} \cdot \prod_{p} (1+p^{-\frac{3}{2}}) \ll 1.$$ □

It follows from Lemmas 84 and 86 that the factor at the odd primes not dividing $f_0$ is $O(2^{-\varepsilon_1 n^{\varepsilon_2}})$ for some real numbers $\varepsilon_1, \varepsilon_2 > 0$, so by (3.53), we have $\delta = \mu_{f_0} + o(2^{-\frac{n}{2}})$. This completes the proof of the second statement in part (a) of Theorem 61.

We now determine the smallest $n$ for which our method yields that a positive proportion of superelliptic stacky curves in $V_{n,f_0}(\mathbb{Z})$ are insoluble. To this end, let $V_{n,f_0}(\mathbb{Z})_{\max}$ be the set

of forms $f \in V_{n,f_0}(\mathbb{Z})$ such that $R_f \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is the maximal order in $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_p$ for every prime $p \mid f_0$ and such that condition (b) in Proposition 68 fails for some prime $p \mid k$. Let $\delta_{\max}$ be the upper density of forms $f \in V_{n,f_0}(\mathbb{Z})_{\max}$, enumerated by height, such that $\mathscr{S}_f(\mathbb{Z}) \neq \varnothing$. For each prime $p \mid f_0$, instead of applying Propositions 78 and 83 to obtain the bound (3.48), we can apply Proposition 77 together with the trivial bound $m_p(T) \geq 1$; doing so yields the following explicit bound on $\delta_{\max}$:

$$\delta_{\max} \leq 2 \cdot \left( \sum_{m=0}^{\frac{n-1}{2}} 2^{n-1} \cdot \frac{2m+1}{2^{\frac{n-1}{2}+m}} \cdot \mu(\mathscr{I}(m)) \right) \cdot \left( \sum_{m=1}^{n} \frac{12}{2^{n+m-2}} \cdot \frac{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/8\mathbb{Z})}{8^{\frac{n(n-1)}{2}}} \cdot \frac{\#\mathscr{I}_8(m)}{8^n} \right) \cdot \left( \prod_{p>2} \frac{p^{\frac{n(n-1)}{2}}}{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})} \right) \tag{3.61}$$

Upon applying the estimates

$$\sum_{m=0}^{\frac{n-1}{2}} \frac{2m+1}{2^{\frac{n-1}{2}+m}} \cdot \mu(\mathscr{I}(m)) \leq \frac{3}{2} \cdot \sum_{m=0}^{\frac{n-1}{2}} \mu(\mathscr{I}(m)) = \frac{3}{2} \quad \text{and} \quad \frac{\#\mathscr{I}_8(m)}{8^n} \leq 1, \tag{3.62}$$

we deduce that $\delta_{\max} < 2^{\frac{15-n}{2}} \leq 1$ whenever $n \geq 15$. By explicitly computing $\frac{\#\mathscr{I}_8(m)}{8^n}$ in `sage` for $n < 15$, one can check that we also have $\delta_{\max} < 1$ when $n \in \{11, 13\}$. Since the density of $V_{n,f_0}(\mathbb{Z})_{\max}$ in $V_{n,f_0}(\mathbb{Z})$ is positive, this completes the proof of the first statement in part (a) of Theorem 61.

*Case 2:* $2 \mid f_0$. When $2 \mid f_0$, we have

$$\delta - \mu_{f_0} \ll \left( \sum_{m=0}^{\frac{n-1}{2}} \frac{2m+1}{2^{\frac{n-1}{2}+m}} \cdot \mu(\mathcal{I}(m)) \right) \cdot 2^{\frac{n-1}{2}} \cdot \left( \prod_{p \nmid f_0} \min \left\{ \frac{p^{\frac{n(n-1)}{2}}}{\#\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/p\mathbb{Z})}, \sum_{m=1}^{n} \frac{p+1}{2^{m-1}} \cdot \frac{\#\mathcal{I}_p(m)}{p^n} \right\} \right) \tag{3.63}$$

where the implied constant is independent of $n$. In (3.63), the archimedean factor is $O(2^{-\frac{n}{2}})$, the factor at 2 is $O(2^{\frac{n}{2}})$, and the factor at primes dividing $f_0$ is $O(1)$. It follows from Lemmas 84 and 86 that the factor at the primes not dividing $f_0$ is $O(2^{-\varepsilon_1 n^{\varepsilon_2}})$ for some real

numbers $\varepsilon_1, \varepsilon_2 > 0$, so $\delta = \mu_{f_0} + O(2^{-\varepsilon_1 n^{\varepsilon_2}})$ in this case. This completes the proof of part (b) of Theorem 61.

*Remark* 87. In [60], it is shown that the density of real degree-$N$ polynomials (not necessarily monic) having fewer than $\log(N+1)/\log\log(N+1)$ real zeros is $O((N+1)^{-b+o(1)})$ for some absolute constant $b > 0$. We expect that one can imitate the proof of this density result to obtain an analogous theorem for monic polynomials. Given such an analogue, it may be possible to improve (albeit modestly) the bounds on $\delta$ that we obtained above by bounding the probability $\mu(\mathcal{I}(m))$.

## 3.5 Obstruction to the Hasse principle and the proof of Theorem 62

In this section, we study how often superelliptic stacky curves satisfy the Hasse principle using the method of descent. Specifically, upon defining the Jacobian of a superelliptic stacky curve, we describe 2-coverings of such stacky curves, and we modify the proof of Theorem 61 to show that such stacky curves often have no locally soluble 2-coverings and thus fail the Hasse principle. Upon showing that such a 2-covering obstruction to solubility is a special case of the Brauer–Manin obstruction, we obtain Theorem 62.

### 3.5.1 The Jacobian of a superelliptic stacky curve

Given any $(A, B) \in W_n(K)$ with $\iota(A, B) = f^{\mathsf{mon}}$, we may regard $A$ and $B$ as quadratic forms cutting out a pair of quadric hypersurfaces $Q_A$ and $Q_B$ in $\mathbb{P}^{n-1}_K$. Let $\mathscr{F}_{(A,B)}$ denote the Fano scheme parametrizing $\frac{n-3}{2}$-dimensional linear spaces contained in the base locus $Q_A \cap Q_B$ of the pencil of quadric hypersurfaces spanned by $Q_A$ and $Q_B$. The following proposition states that $\mathscr{F}_{(A,B)}$ is a torsor of the Jacobian of $\mathscr{S}_f$:

**Proposition 88.** *Let $(A, B) \in W_n(K)$ with $\iota(A, B) = f^{\mathsf{mon}}$. Then, if $\#K$ is sufficiently large, $\mathscr{F}_{(A,B)}$ is a torsor over $K$ of the Jacobian of the stacky curve $\mathscr{S}_f$.*

*Proof.* The Jacobian of a stacky curve $\mathscr{X}$ is defined to be the $0^{\text{th}}$-degree component $\mathrm{Pic}^0(\mathscr{X})$ of the group $\mathrm{Pic}(\mathscr{X})$ of divisors on $\mathscr{X}$ modulo principal divisors. Let $K_{\mathrm{sep}}$ be a separable closure of $K$, and let $\theta_1, \dots, \theta_n \in \mathbb{P}^1_K(K_{\mathrm{sep}})$ be the roots of $f$. Applying the correspondence between isomorphism classes of line bundles and divisor classes to [40, proof of Proposition 2.2] yields that $\mathrm{Pic}^0(\mathscr{S}_f)$ is the group generated by the classes of the divisors $(\frac{1}{2}\theta_i - \frac{1}{2}\theta_j)$ subject to the relations $2 \cdot (\frac{1}{2}\theta_i - \frac{1}{2}\theta_j) = 0$ for $1 \le i < j \le n$; i.e., we have

$$\mathrm{Pic}^0(\mathscr{S}_f) = (\mathbb{Z}/2\mathbb{Z})\langle(\tfrac{1}{2}\theta_i - \tfrac{1}{2}\theta_j) : 1 \le i < j \le n\rangle.$$

There is a natural right action of the absolute Galois group $\mathscr{G}_K := \mathrm{Gal}(K_{\mathrm{sep}}/K)$ on $\mathrm{Pic}^0(\mathscr{S}_f)$: for $\sigma \in \mathscr{G}_K$, we have $(\frac{1}{2}\theta_i - \frac{1}{2}\theta_i) \cdot \sigma = (\frac{1}{2}(\sigma^{-1} \cdot \theta_i) - \frac{1}{2}(\sigma^{-1} \cdot \theta_j))$.

A result of Wang (see [122, Corollary 2.5]) implies that, as long as $\#K$ is sufficiently large, the Fano scheme $\mathscr{F}_{(A,B)}$ is a torsor over $K$ of the 2-torsion subgroup $J[2]$ of the Jacobian $J$ of the monic odd-degree hyperelliptic curve $y^2 = f^{\mathsf{mon}}(x, 1)$. Thus, to prove that $\mathscr{F}_{(A,B)}$ is a torsor of $\mathrm{Pic}^0(\mathscr{S}_f)$, it suffices to show that there is a $\mathscr{G}_K$-equivariant isomorphism $\mathrm{Pic}^0(\mathscr{S}_f) \simeq J[2]$. But this is clear: the classes of $(\theta_i - \theta_j)$ for $1 \le i < j \le n$ generate $J[2](K_{\mathrm{sep}})$ over $\mathbb{Z}/2\mathbb{Z}$. □

Note in particular that the $G_n(K)$-orbit of $(A, B)$ is distinguished if and only if $\mathscr{F}_{(A,B)}$ is the trivial torsor of the Jacobian of $\mathscr{S}_f$ (which happens if and only if $\mathscr{F}_{(A,B)}(K) \neq \varnothing$).

*Remark* 89. As it happens, Proposition 88 admits an analogue for pencils of even-dimensional quadric hypersurfaces; see the work of Wang [122] (generalizing previous work of Reid [95, Theorem 4.8]), showing that when $n$ is even, the Fano scheme of maximal linear spaces in the base locus of a pencil of quadric hypersurfaces generated by a pair $(A, B) \in W_n(K)$ is a torsor of the Jacobian of the hyperelliptic curve cut out by the equation $z^2 = \mathrm{inv}(xA + yB)$.

We conclude this section by explaining how to visualize the simply transitive action of $\mathrm{Pic}^0(\mathscr{S}_f)$ on $\mathscr{F}_{(A,B)}(K_{\mathrm{sep}})$ from Proposition 88. For each $i \in \{1, \dots, n\}$, let $Q_i$ be the singular fiber lying over the point $\theta_i$ in the pencil of quadrics spanned by $Q_A$ and $Q_B$. Suppose that $T$ is generic, so that each of the quadrics $Q_i$ is a simple cone with cone point $q_i$. Let $\mathscr{F}_{(A,B)}(K_{\mathrm{sep}}) = \{p_1, \dots, p_{2^{n-1}}\}$, and for each $\ell \in \{1, \dots, 2^{n-1}\}$, let $\overline{p}_\ell$ denote the corresponding linear subspace of $\mathbb{P}^{n-1}_{K_{\mathrm{sep}}}$. We illustrate this in the case where $n = 3$ in Figure 1.

We define an action of $\mathrm{Pic}^0(\mathscr{S}_f)$ on $\mathscr{F}_{(A,B)}(K_{\mathrm{sep}})$ by first specifying how each $(\frac{1}{2}\theta_i)$ acts on $\mathscr{F}_{(A,B)}(K_{\mathrm{sep}})$. Let $L_{i\ell} \subset \mathbb{P}^{n-1}_{K_{\mathrm{sep}}}$ be the linear span of the $\frac{n-3}{2}$-plane $\overline{p}_\ell$ and the point $q_i$ for each pair $(i, \ell)$. By [95, Theorem 3.8], there exists precisely one element $p_{i(\ell)} \in \mathscr{F}_{(A,B)}(K_{\mathrm{sep}}) \smallsetminus \{p_\ell\}$ such that $\overline{p}_{i(\ell)} \subset L_{i\ell}$. For each $i$, let $(\frac{1}{2}\theta_i)$ act on $\mathscr{F}_{(A,B)}$ by swapping $p_\ell$ and $p_{i(\ell)}$ for each $\ell$. Then for each pair $(i, j)$, the divisor $(\frac{1}{2}\theta_i - \frac{1}{2}\theta_j)$ acts on $\mathscr{F}_{(A,B)}$ by swapping $p_\ell$ with $p_{i(j(\ell))} = p_{j(i(\ell))}$ for each $\ell$. When $n = 1$, for example, the divisor $(\frac{1}{2}\theta_1 - \frac{1}{2}\theta_2)$ acts on $\mathscr{F}_{(A,B)}$ by sending $(p_1, p_2, p_3, p_4)$ to $(p_3, p_4, p_1, p_2)$, as we demonstrate in Figure 1.

### 3.5.2 Defining the Brauer–Manin obstruction for $\mathscr{S}_F$

Let $f$ be a separable integral binary form of odd degree $n \geq 3$. While a suitable theory of Brauer–Manin obstruction for stacks remains to be developed, such a theory is not required in the context of superelliptic stacky curves. Indeed, we can exploit the fact that the stack $\mathscr{S}_f$ is defined as a quotient of the punctured affine surface $\widetilde{S}_f$ (see (3.2)), where the usual theory of the Brauer–Manin obstruction for varieties applies.

Let $\widetilde{S}_{f,\mathbb{Q}} = \widetilde{S}_f \otimes_{\mathbb{Z}} \mathbb{Q}$, and let $\widetilde{S}_{f,\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$ denote the usual Brauer–Manin set of the $\mathbb{Q}$-variety $\widetilde{S}_{f,\mathbb{Q}}$ (see [41, §1] for the definition). Let

$$\widetilde{S}_f(\mathbb{A}_{\mathbb{Q}})^{\mathrm{int}} := \prod_v \widetilde{S}_f(\mathbb{Z}_v) \tag{3.64}$$

be the set of adelic points of $\widetilde{S}_f$ that are integral in every place (i.e., the set of everywhere-primitive adelic solutions to the superelliptic equation $z^2 = f(x, y)$, or equivalently, the set

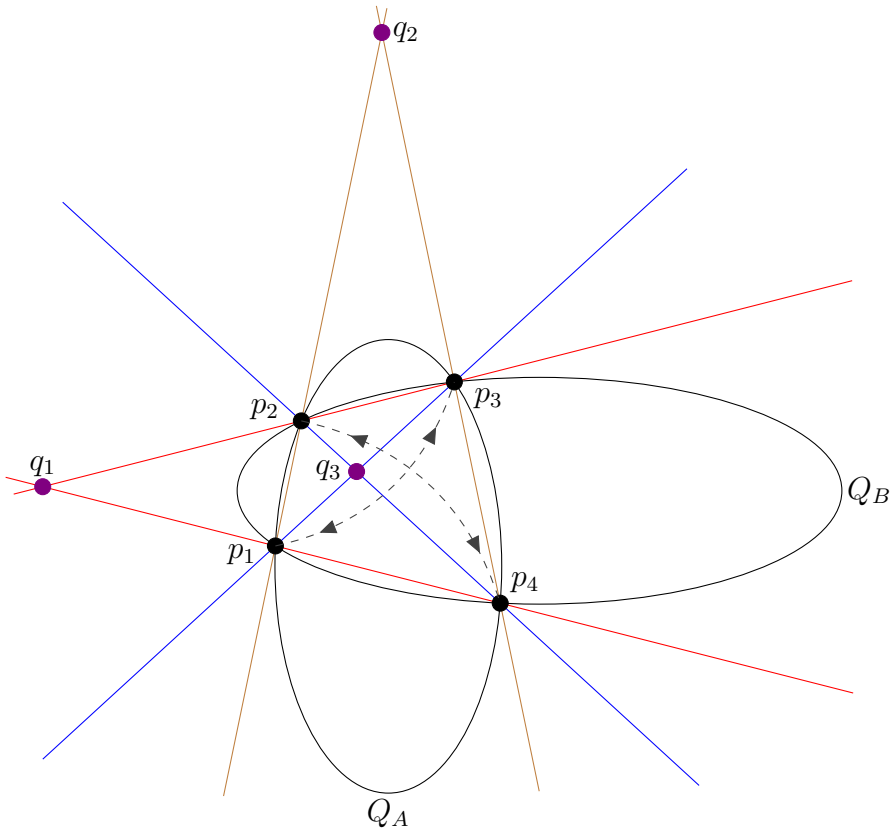



Figure 1: The pencil of conics spanned by $Q_A$ and $Q_B$ in $\mathbb{P}^2_{K_{\text{sep}}}$, with singular fibers $Q_1$, $Q_2$, and $Q_3$ having cone points $q_1$, $q_2$, and $q_3$, respectively. In this case, $\mathscr{F}_{(A,B)}(K_{\text{sep}}) = Q_A \cap Q_B = \{p_1, p_2, p_3, p_4\}$. The dashed arrows display the action of the degree-0 divisor $(\frac{1}{2}\theta_1 - \frac{1}{2}\theta_2)$ on $\mathscr{F}_{(A,B)}$.

of everywhere-integral adelic points on the stacky curve $\mathscr{S}_f$). With this notation in place, we define the *Brauer–Manin set* of $\mathscr{S}_f$ by

$$\mathscr{S}_f(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} := \widetilde{S}_f(\mathbb{A}_{\mathbb{Q}})^{\mathrm{int}} \cap \widetilde{S}_{f,\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}, \tag{3.65}$$

and we say that $\mathscr{S}_f$ *has a Brauer–Manin obstruction to having an integral point* if its Brauer–Manin set is empty (i.e., if $\mathscr{S}_f(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \varnothing$).

Because we have defined $\mathscr{S}_f(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$ as a subset of $\widetilde{S}_{f,\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$, we can use the method of descent as laid out for open varieties in [41] to obtain a set-theoretic "upper bound" on $\mathscr{S}_f(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$. Indeed, suppose that we have a torsor $\rho\colon Z \to \widetilde{S}_{f,\mathbb{Q}}$ by a group of multiplicative type or connected algebraic group $\Gamma$ (all defined over $\mathbb{Q}$). Let

$$\widetilde{S}_{f,\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}})^{\rho} := \bigcup_{\sigma \in H^1(\mathscr{G}_{\mathbb{Q}}, \Gamma(\overline{\mathbb{Q}}))} \rho^{\sigma}(Z^{\sigma}(\mathbb{A}_{\mathbb{Q}})) \tag{3.66}$$

be the descent set of $\rho$, where $\rho^{\sigma}\colon Z^{\sigma} \to \widetilde{S}_{f,\mathbb{Q}}$ is the twist of $\rho\colon Z \to \widetilde{S}_{f,\mathbb{Q}}$ by a 1-cocycle representing $\sigma \in H^1(\mathscr{G}_{\mathbb{Q}}, \Gamma(\overline{\mathbb{Q}}))$. Since $\widetilde{S}_{f,\mathbb{Q}}$ is smooth and geometrically integral, [41, Theorem 1.1] implies that

$$\widetilde{S}_{f,\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} \subset \widetilde{S}_{f,\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}})^{\rho}. \tag{3.67}$$

It follows from (3.65) and (3.67) that $\mathscr{S}_f$ has a Brauer–Manin obstruction to having an integral point if it has an obstruction to descent by $\Gamma$-torsors in the sense that we have $\widetilde{S}_f(\mathbb{A}_{\mathbb{Q}})^{\mathrm{int}} \cap \widetilde{S}_{f,\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}})^{\rho} = \varnothing$.

### 3.5.3 2-Coverings

Let $K$ be a field of characteristic not equal to 2, let $f_0 \in K^{\times}$, and let $f \in V_{n,f_0}(K)$ be separable. Let $\theta_1, \dots, \theta_n \in K_{\mathrm{sep}}$ be the distinct roots of the polynomial $f(x,1)$, and for each $\sigma \in \mathscr{G}_K$ and $i \in \{1, \dots, n\}$, let $\sigma(i) \in \{1, \dots, n\}$ be defined by $\theta_{\sigma(i)} = \sigma(\theta_i)$. Let $\widetilde{S}_f$ and $\mathscr{S}_f$ respectively denote the corresponding punctured affine surface and stacky curve (which are now de-

fined over $K$, as opposed to $\mathbb{Z}$). In this section, we specialize the discussion of descent in §3.5.2 to the case where $\Gamma$ is equal to the Jacobian $\mathrm{Pic}^0(\mathscr{S}_f)$ of $\mathscr{S}_f$ (see §3.3). Notice that $\mathrm{Pic}^0(\mathscr{S}_f)$ is a group of multiplicative type, because over $K_{\mathrm{sep}}$, it is isomorphic to a finite product of copies of $\mathbb{Z}/2\mathbb{Z}$ and is thus diagonalizable. Thus, we can apply (3.67) to $\mathrm{Pic}^0(\mathscr{S}_f)$-torsors.

A Galois étale covering defined over $K$ with Galois group isomorphic to $\mathrm{Pic}^0(\mathscr{S}_f)$ as $\mathscr{G}_K$-modules is called a 2-*covering*. Our strategy for describing the 2-coverings of $\widetilde{S}_f$ is to describe the 2-coverings of $\mathscr{S}_f$ and pull back along the quotient map $\widetilde{S}_f \to [\widetilde{S}_f/\mathbb{G}_m] = \mathscr{S}_f$. We now briefly recall the results of [37, §5], in which Bruin and Flynn explicitly construct all 2-coverings of $\mathscr{S}_f$ up to isomorphism over $K$ (see also [38, §3]). Consider the projective space $\mathbb{P}^{n-1}_K$ with homogeneous coordinates $[Z_1 : \cdots : Z_n]$ such that $\mathscr{G}_K$ acts on $Z_i$ by $\sigma \cdot Z_i = Z_{\sigma(i)}$. The *distinguished covering* is defined to be the closed subscheme $C^1 \subset \mathbb{P}^{n-1}_K$ cut out by the homogeneous ideal

$$I^1 := \big((\theta_i - \theta_j)(Z_\ell^2 - Z_m^2) - (\theta_\ell - \theta_m)(Z_i^2 - Z_j^2) : i, j, \ell, m \in \{1, \ldots, n\}\big).$$

Let $\pi^1 \colon C^1 \to \mathbb{P}^1_K$ be the map defined by

$$\pi^1([Z_1 : \cdots : Z_n]) = \frac{\theta_j Z_i^2 - \theta_i Z_j^2}{Z_i^2 - Z_j^2}$$

for any distinct $i, j \in \{1, \ldots, n\}$. For each class $\alpha \in H^1(\mathscr{G}_K, \mathrm{Pic}^0(\mathscr{S}_f))$, the twist of $\pi^1 \colon C^1 \to \mathbb{P}^1_K$ by $\alpha$ is given explicitly as follows. By [15, last paragraphs of §4.2 and §5.1], $H^1(\mathscr{G}_\mathbb{Q}, \mathrm{Pic}^0(\mathscr{S}_f))$ can be identified with $(K_f^\times / K_f^{\times 2})_{\mathrm{N}\equiv 1}$, so we may think of $\alpha$ as being an element of $(K_f^\times / K_f^{\times 2})_{\mathrm{N}\equiv 1}$. Let $(\alpha_1, \ldots, \alpha_n)$ be the image of $\alpha$ under the map $K_f^\times / K_f^{\times 2} \to \big((K_{\mathrm{sep}})^\times / (K_{\mathrm{sep}})^{\times 2}\big)^n$ given by taking the product of the distinct embeddings of each field component of $K_f$ into $K_{\mathrm{sep}}$. Then the twist of $C^1$ by $\alpha$ is the closed subscheme $C^\alpha \subset \mathbb{P}^{n-1}_K$ cut out by the homogeneous ideal

$$I^\alpha := \big((\theta_i - \theta_j)(\alpha_\ell Z_\ell^2 - \alpha_m Z_m^2) - (\theta_\ell - \theta_m)(\alpha_i Z_i^2 - \alpha_j Z_j^2) : i, j, \ell, m \in \{1, \ldots, n\}\big),$$

and the twist of $\pi^1 \colon C^1 \to \mathbb{P}^1_K$ is the map $\pi^\alpha \colon C^\alpha \to \mathbb{P}^1_K$ defined by

$$\pi^\alpha([Z_1 : \cdots : Z_n]) = \frac{\theta_j \alpha_i Z_i^2 - \theta_i \alpha_j Z_j^2}{\alpha_i Z_i^2 - \alpha_j Z_j^2}$$

for any distinct $i, j \in \{1, \ldots, n\}$. The following theorem enumerates the basic properties of the maps $\pi^\alpha \colon C^\alpha \to \mathbb{P}^1_K$:

**Theorem 90** ([37, Lemma 5.10] and [38, §3.1])**.** *With notation as above, we have:*

(a) *For each $\alpha \in (K_f^\times / K_f^{\times 2})_{\mathrm{N}\equiv 1}$, the scheme $C_\alpha$ is a smooth, geometrically irreducible, projective curve of genus $\frac{n-1}{2} \cdot 2^{n-2} - 3 \cdot 2^{n-3} + 1$;*

(b) *The action of $\mathscr{G}_K$ leaves both $I^\alpha$ and $\pi^\alpha$ invariant, so the map $\pi^\alpha \colon C^\alpha \to \mathbb{P}^1_K$ is defined over $K$;*

(c) *The map $\pi^\alpha$ is a covering map with Galois group generated by the automorphisms $\tau_i \colon C^\alpha \to C^\alpha$ defined by $Z_i \to -Z_i$ for each $i \in \{1, \ldots, n\}$; and*

(d) *We have that $\deg \pi^\alpha = 2^{n-1}$, that $\#(\pi^\alpha)^{-1}(\theta_i) = 2^{n-2}$, and that $\#(\pi^\alpha)^{-1}(\alpha) = 2^{n-1}$ for each $\alpha \in \mathbb{P}^1_K(K_{\mathrm{sep}}) \smallsetminus \{\theta_1, \ldots, \theta_n\}$.*

We now demonstrate that the map $\pi^\alpha$ can actually be thought of as a 2-covering $\pi^\alpha \colon C^\alpha \to \mathscr{S}_f$.

**Proposition 91.** *For any $\alpha \in (K_f^\times / K_f^{\times 2})_{\mathrm{N}\equiv 1}$, the map $\pi^\alpha$ factors through the coarse moduli map $\mathscr{S}_f \to \mathbb{P}^1_K$ to give a 2-covering $\pi^\alpha \colon C^\alpha \to \mathscr{S}_f$.*

*Proof.* Recall that a finite étale cover of $\mathscr{S}_f$ is the pullback via $\mathscr{S}_f \to \mathbb{P}^1_K$ of a finite cover of its coarse moduli space $\mathbb{P}^1_K$ that is ramified with ramification index 2 at every point in the preimage of $\theta_i \in \mathbb{P}^1_K(K_{\mathrm{sep}})$ for each $i$ (to account for the fact that $\mathscr{S}_f$ has a $\frac{1}{2}$-point at each $\theta_i$) and unramified everywhere else. It follows from part (d) of Theorem 90 that the branch locus of the map $\pi^\alpha$ consists precisely of the points $\theta_i$ and that each point in $(\pi^\alpha)^{-1}(\theta_i)$ has

ramification index 2. Thus, the map $\pi^\alpha$ factors through the stacky curve $\mathscr{S}_f$, giving an étale map $\pi^\alpha\colon C^\alpha \to \mathscr{S}_f$.

By parts (b) and (c) of Theorem 90, to prove that $\pi^\alpha$ is a 2-covering of $\mathscr{S}_f$ over $K$, it suffices to show that the group generated by the automorphisms $\tau_i$ is isomorphic to $\mathrm{Pic}^0(\mathscr{S}_f)$ as $\mathscr{G}_K$-modules. Let $J$ denote the Jacobian of the monic odd-degree hyperelliptic curve $y^2 = f^{\mathsf{mon}}(x,1)$. We claim that the map $\tau_i \mapsto (\theta_i - \infty) \in J[2](K_{\mathrm{sep}})$ defines a $\mathscr{G}_K$-equivariant isomorphism of groups. To see why this claim holds, note that the group generated by the automorphisms $\tau_i$ is isomorphic to

$$(\mathbb{Z}/2\mathbb{Z})\langle \tau_1, \ldots, \tau_n \rangle \Big/ \left( \prod_{i=1}^{n} \tau_i = 1 \right)$$

and the action of $\sigma \in \mathscr{G}_K$ on $\tau_i$ is given by $\sigma \cdot \tau_i = \tau_{\sigma^{-1}(i)}$, because the action of $\sigma$ on $Z_i$ is defined to be $\sigma(Z_i) = Z_{\sigma(i)}$. On the other hand, we have that

$$J[2](K_{\mathrm{sep}}) = (\mathbb{Z}/2\mathbb{Z})\langle (\theta_1 - \infty), \ldots, (\theta_n - \infty) \rangle \Big/ \left( \sum_{i=1}^{n} (\theta_i - \infty) \right)$$

and the action of $\sigma \in \mathscr{G}_K$ on $(\theta_i - \infty)$ is $(\theta_i - \infty)\cdot\sigma = (\sigma^{-1}\cdot\theta_i - \sigma^{-1}\cdot\infty) = (\theta_{\sigma^{-1}(i)} - \infty)$. Thus, we have the claim. The proposition now follows from the fact that $J[2] \simeq \mathrm{Pic}^0(\mathscr{S}_f)$ as $\mathscr{G}_K$-modules (see the proof of Proposition 88). □

*Remark* 92. Note that two coverings $\pi^{\alpha_1}\colon C^{\alpha_1} \to \mathscr{S}_f$ and $\pi^{\alpha_2}\colon C^{\alpha_2} \to \mathscr{S}_f$ are isomorphic (as coverings of $\mathscr{S}_f$ defined over $K$) if and only if $\alpha_1$ and $\alpha_2$ represent the same class in $(K_f^\times / K_f^{\times 2})_{\mathrm{N}\equiv 1}$.

Let $(x_0, y_0, z_0) \in \mathscr{S}_f(k)$, and let $\alpha \in K_f^\times$ be the element associated to the point $(x_0, y_0, z_0)$ via the construction in §3.2. By (3.7), we have that

$$\alpha = \begin{cases} x_0 - \theta y_0 & \text{if } z_0 \neq 0, \\ \widetilde{F}(y_0\theta, y_0) + (x_0 - \theta y_0) & \text{if } z_0 = 0 \end{cases}$$

where $\widetilde{f}$ is as in (3.3). With this notation, we have the following result, which tells us which 2-covering of $\mathscr{S}_f$ has the property that $(x_0, y_0, z_0)$ lies in the image of its $K$-rational points:

**Lemma 93.** *We have that* $(x_0, y_0, z_0) \in \pi^{f_0 \cdot \alpha}(C^{f_0 \cdot \alpha}(K)) \subset \mathscr{S}_f(K)$.

*Proof.* First suppose $z_0 \neq 0$. By construction, the point $[1 : 1 : \cdots : 1] \in C^{f_0 \cdot \alpha}(K)$ satisfies

$$\pi^{f_0 \cdot \alpha}([1 : 1 : \cdots : 1]) = \frac{\theta_j(f_0 \cdot \alpha_i) - \theta_i(f_0 \cdot \alpha_j)}{f_0 \cdot \alpha_i - f_0 \cdot \alpha_j} = \frac{\theta_j \cdot f_0(x_0 - \theta_i y_0) - \theta_i \cdot f_0(x_0 - \theta_j y_0)}{f_0(x_0 - \theta_i y_0) - f_0(x_0 - \theta_j y_0)} \tag{3.68}$$

$$= [x_0 : y_0] \in \mathbb{P}^1_K(K) = \mathscr{S}_f(K).$$

Now suppose $z_0 = 0$. Then one readily checks that the calculation in (3.68) goes through by replacing $[1 : 1 : \cdots : 1]$ with the point $[0 : 1 : 1 : \cdots : 1] \in C^{f_0 \cdot \alpha}(K)$. □

We have thus completed our description of the 2-coverings of $\mathscr{S}_f$. The 2-coverings of $\widetilde{S}_f$ are precisely the pullbacks of the coverings $\pi^\alpha \colon C^\alpha \to \mathscr{S}_f$ via the quotient map $\widetilde{S}_f \to \mathscr{S}_f$.

### 3.5.4 Proof of Theorem 62

Let $f \in V_{n,f_0}(\mathbb{Z})$ be irreducible, let $\alpha \in (K_f^\times / K_f^{\times 2})_{\mathrm{N}\equiv 1}$, and consider the associated 2-covering $\pi^\alpha \colon C^\alpha \to \mathscr{S}_f$ over $\mathbb{Q}$. We say that the 2-covering $\pi^\alpha$ is *locally soluble* if for every place $v$ of $\mathbb{Q}$, there exists a point $P_v \in \mathscr{S}_f(\mathbb{Z}_v)$ such that the number $\alpha_v$ associated to $P_v$ via (3.7) is such that $f_0 \cdot \alpha_v$ is equal to the image of $\alpha$ under the natural map $(K_f^\times / K_f^{\times 2})_{\mathrm{N}\equiv 1} \to ((K_f \otimes_{\mathbb{Q}} \mathbb{Q}_v)^\times / (K_f \otimes_{\mathbb{Q}} \mathbb{Q}_v)^{\times 2})_{\mathrm{N}\equiv 1}$. (Notice that in this situation, $P_v \in \pi^\alpha(C^\alpha(\mathbb{Q}_v))$ by Lemma 93.) Just as Bruin and Stoll did for hyperelliptic curves in [39, §2], we define the *fake* 2-*Selmer set* $\mathrm{Sel}^2_{\mathrm{fake}}(\mathscr{S}_f) \subset (K_f^\times / K_f^{\times 2})_{\mathrm{N}\equiv 1}$ to be the set of locally soluble 2-coverings of $\mathscr{S}_f$.

We claim that each element $\alpha \in \mathrm{Sel}^2_{\mathrm{fake}}(\mathscr{S}_f)$ gives rise to an orbit of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $W_{\mathscr{A}_n}(\mathbb{Z})$, the associated $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q})$-orbit of which is represented by the class $\alpha \in (K_f^\times / K_f^{\times 2})_{\mathrm{N}\equiv 1}$. For each place $v$, let $P_v \in \mathscr{S}_f(\mathbb{Z}_v) \cap \pi^\alpha(C^\alpha(\mathbb{Q}_v))$. Then via the construction in §3.2, $P_v$ naturally gives rise to an orbit of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_v)$ on $W_{\mathscr{A}_n}(\mathbb{Z}_v)$, the associated $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_v)$-orbit of which is represented

by the class $\alpha \in ((K_f \otimes_{\mathbb{Q}} \mathbb{Q}_v)^\times/(K_f \otimes_{\mathbb{Q}} \mathbb{Q}_v)^{\times 2})_{\mathrm{N}\equiv 1}$. Since the algebraic group $\mathcal{G}_{\mathscr{A}_n}$ has class number equal to 1, and since the orbit of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_v)$ on $W_{\mathscr{A}_n}(\mathbb{Q}_v)$ associated to $\alpha$ has a representative over $\mathbb{Z}_v$ for every place $v$, it follows that the orbit of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q})$ on $W_{\mathscr{A}_n}(\mathbb{Q})$ has representative over $\mathbb{Z}$. Thus, we have the claim.

In the next lemma, we relate the fake 2-Selmer set to the Brauer–Manin obstruction:

**Lemma 94.** *If* $\mathrm{Sel}^2_{\mathrm{fake}}(\mathscr{S}_f) = \varnothing$*, then* $\mathscr{S}_f$ *has a Brauer–Manin obstruction to having an integral point.*

*Proof.* Let $\pi\colon C \to \widetilde{S}_{f,\mathbb{Q}}$ be any 2-covering. We have by (3.64), (3.65), (3.66), and (3.67) that

$$\begin{aligned}\mathscr{S}_f(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} \subset \widetilde{S}_f(\mathbb{A}_{\mathbb{Q}})^{\mathrm{int}} \cap \widetilde{S}_{f,\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}})^{\pi} &= \left(\prod_v \mathscr{S}_f(\mathbb{Z}_v)\right) \cap \left(\bigcup_{\alpha \in H^1(\mathscr{G}_{\mathbb{Q}}, \mathrm{Pic}^0(\mathscr{S}_f)(\overline{\mathbb{Q}}))} \pi^\alpha(C^\alpha(\mathbb{A}_{\mathbb{Q}}))\right) \\ &\subset \bigcup_{\alpha \in \mathrm{Sel}^2_{\mathrm{fake}}(\mathscr{S}_f)} \pi^\alpha(C^\alpha(\mathbb{A}_{\mathbb{Q}})),\end{aligned}$$

and clearly the last union above is empty if $\mathrm{Sel}^2_{\mathrm{fake}}(\mathscr{S}_f) = \varnothing$. □

In proving Theorem 61, we imposed local conditions on $W_{\mathscr{A}_n}(\mathbb{Z})$ to sieve to the orbits that arise from local points at each place. By definition, the exact same local conditions define orbits that arise from elements of fake 2-Selmer sets. Moreover, if $f \in V_{n,f_0}(\mathbb{Z}) \smallsetminus V_{n,f_0}(\mathbb{Z})^*$, Proposition 68 implies that the distinguished covering is not everywhere locally soluble. Thus, by the argument in §3.4, we have the following result:

**Theorem 95.** *The upper density of forms* $f \in V_{n,f_0}(\mathbb{Z})$ *such that* $\mathrm{Sel}^2_{\mathrm{fake}}(\mathscr{S}_f) \neq \varnothing$ *is at most* $\mu_{f_0} + o(2^{-\frac{n}{2}})$ *when* $2 \nmid f_0$ *and at most* $\mu_{f_0} + O(2^{-\varepsilon_1 n^{\varepsilon_2}})$ *for some* $\varepsilon_1, \varepsilon_2 > 0$ *when* $2 \mid f_0$*.*

To prove Theorem 62, it remains to determine how often it is that the stacky curves $\mathscr{S}_f$ have integral points everywhere locally. We do so as follows:

**Lemma 96.** *The density of forms* $f \in V_{n,f_0}(\mathbb{Z})$ *such that* $\mathscr{S}_f(\mathbb{Z}_v) \neq \varnothing$ *for every place* $v$ *is at least* $\mu'_{f_0} + O(2^{-n})$*.*

*Proof.* By (3.1), we always have $\mathscr{S}_f(\mathbb{R}) \neq \varnothing$. If there is no prime $p \mid k$ such that $f(x_0, y_0) = 0$ for every $[x_0 : y_0] \in \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, then for any prime $p \mid k$, there exists a pair $(x_0, y_0) \in \mathbb{Z}^2$ such that $\gcd(x_0, y_0) = \gcd(f(x_0, y_0), p) = 1$, so $(x_0 f(x_0, y_0), y_0 f(x_0, y_0), f(x_0, y_0)^{\frac{n+1}{2}}) \in \mathscr{S}_f(\mathbb{Z}_p)$. On the other hand, if $p \mid k$ and the mod-$p$ reduction of $f$ has a simple zero at some point of $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, then $\mathscr{S}_f$ has a Weierstrass point over $\mathbb{Z}_p$ and is thus soluble. Moreover, for any prime $p$ such that $p \nmid k$ but $p \mid f_0$, we have $\left(k, 0, f_0^{\frac{1}{2}} k^{\frac{n}{2}}\right) \in \mathscr{S}_f(\mathbb{Z}_p)$, and for any prime $p \nmid f_0$, we have $\left(f_0, 0, f_0^{\frac{n+1}{2}}\right) \in \mathscr{S}_f(\mathbb{Z}_p)$.

If $p \mid k$, the $p$-adic density of forms $f \in V_{n,f_0}(\mathbb{Z})$ such that the mod-$p$ reduction of $f$ has a zero of multiplicity greater than 1 at each point of $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ is $p^{-2p-1}$ if $2p + 2 < n$ and $p^{-n}$ otherwise. Thus, the density of forms $f \in V_{n,f_0}(\mathbb{Z})$ such that $\mathscr{S}_f(\mathbb{Z}_v) \neq \varnothing$ for every place $v$ is at least $\prod_{p|k}(1 - p^{-2p-1} - p^{-n}) = \mu'_{f_0} + O(2^{-n})$. □

It follows from Theorem 95 and Lemma 96 that for all sufficiently large $n$, a positive proportion of $f \in V_{n,f_0}(\mathbb{Z})$ are such that $\mathrm{Sel}^2_{\mathrm{fake}}(\mathscr{S}_f) = \varnothing$ and $\mathscr{S}_f(\mathbb{Z}_v) \neq \varnothing$ for every place $v$. Indeed, we have that

$$(1 - \mu_{f_0}) + (\mu'_{f_0} + O(2^{-n})) = 1 - \prod_{p|k} \frac{1}{p^2} + \prod_{p|k} \left(1 - \frac{1}{p^{2p+1}}\right) + O(2^{-\frac{n}{2}}),$$

which is greater than 1 for every sufficiently large $n$. Theorem 62 now follows from Lemma 94.

# Chapter 4

# The second moment of the size of the 2-Selmer group of elliptic curves

This chapter is largely based on my joint work [28] with Manjul Bhargava and Arul Shankar.

## 4.1 Introduction

Let $f$ be a separable integral binary form of even degree $n \geq 4$. In this chapter, we prove that 2-Selmer elements of the Jacobian of the hyperelliptic curve $z^2 = f(x, y)$ give rise to square roots of the class of the inverse different of $R_f$, and we apply the parametrization of such square roots developed in §1 to prove new results about the distribution of the 2-Selmer groups of hyperelliptic Jacobians. Specifically, we resolve two new cases of the Poonen–Rains heuristics [92] by proving that the average size of the 2-Selmer group of locally soluble genus-1 curves is at most 6, and that the second moment of the size of the 2-Selmer group of elliptic curves is at most 15. Crucial to the proofs of these results are new equidistribution techniques involving Fourier analysis that allow us to overcome the dependence of the parametrization on the leading coefficient.

### 4.1.1 Statements of main results

Recall that every elliptic curve over $\mathbb{Q}$ is isomorphic to a unique curve of the form

$$E^{I,J}\colon y^2 = x^3 - \tfrac{I}{3}x - \tfrac{J}{27},$$

where $I, J$ are integers satisfying the following three conditions: $3 \mid I$, $27 \mid J$, and for every prime $p$, we have that $3p^4 \nmid I$ if $27p^6 \mid J$. The height of $E^{I,J}$ is defined to be $H(E^{I,J}) := H(I,J) := \frac{4}{27}\max\{|I|^3, J^2/4\}$.

In [22,24,26,27], Bhargava and Shankar determined, for each $n \in \{2,3,4,5\}$, the average size of the $n$-Selmer group in the universal family of elliptic curves over $\mathbb{Q}$ ordered by height. The purpose of this chapter is to prove an analogous result for the second moment of the size of the 2-Selmer group. Specifically, we prove the following theorem:

**Theorem 97.** *When elliptic curves over $\mathbb{Q}$ are ordered by height, the second moment of the size of the 2-Selmer group is at most 15.*

In fact, we prove that Theorem 97 holds for any subfamily of elliptic curves defined by any finite set or any acceptable infinite set of congruence conditions, and further that the upper bound of 15 is tight if one assumes a certain plausible uniformity estimate. Currently, the best lower bound that we know on the second moment is 10. Indeed, since $2^{2d} \geq 6 \times 2^d - 8$, where $d$ denotes the 2-Selmer rank, and since the average size of the 2-Selmer group is 3 (by [26, Theorem 1.1]), we obtain the lower bound $6 \times 3 - 8 = 10$ on the second moment.

A key ingredient in the proof of Theorem 97 is the determination of the average size of the 2-Selmer group of the Jacobian of locally soluble genus-1 curves:

**Theorem 98.** *Consider the family of locally soluble genus-1 curves of the form $z^2 = f(x,y)$, where $f$ is an irreducible integral binary quartic form up to $\mathrm{PGL}_2(\mathbb{Q})$-action. When these curves are ordered by the heights of their Jacobian elliptic curves, the average size of the 2-Selmer group of the Jacobian is at most 6.*

Theorems 97 and 98 confirm remarkable heuristics due to Poonen and Rains (see [92], cf. [20]), who modeled the $p$-Selmer group, where $p$ is a prime, as a random intersection of a discrete maximal isotropic subspace with a compact open maximal isotropic subspace in a locally compact quadratic space over the finite field $\mathbb{F}_p$. Using this model, they arrived at a conjecture for the distribution of the $p$-Selmer group of elliptic curves. As far as the moments of the distribution are concerned, Poonen and Rains made the following precise prediction:

**Conjecture 99** ([92, Conjecture 1.1(c)])**.** *Let $p$ be prime. The $m^{th}$ moment of the size of the $p$-Selmer group of elliptic curves over $\mathbb{Q}$ is $\prod_{i=1}^{m}(p^i+1)$.*

The only cases of Conjecture 99 that have been proven in the literature are the cases where $m = 1$ and $p \in \{2, 3, 5\}$ (see [24, 26, 27]). Theorem 97 constitutes the very first result toward Conjecture 99 in the case where $m > 1$. We note that the distribution of the $p$-Selmer group conjectured by Poonen and Rains is also expected to hold for various special families of elliptic curves, and for $p = 2$, significant progress has been made toward proving the conjecture for such families: In [69], Heath-Brown determined the distribution of the 2-Selmer group for the family of congruent number curves, and Swinnerton-Dyer (see [118]) and Kane (see [74]) showed that the same distribution holds for any family of quadratic twists of a single elliptic curve with full rational 2-torsion. Considerably more is known about 2-Selmer groups in quadratic twist families; see, for example, the works of Klagsbrun, Mazur, and Rubin computing the proportion of twists of a given elliptic curve $E$ with even 2-Selmer rank [76] and, when the 2-torsion of $E$ generates an $S_3$-cubic field, the proportion of twists with given 2-Selmer rank [77], as well as the very recent work of Smith [112] determining (under certain technical conditions) the distribution of the $2^k$-Selmer group in quadratic twist families of elliptic curves for every $k \geq 1$.

### 4.1.2 Background on hyperelliptic curves and their Selmer groups

Let $C/\mathbb{Q}$ be a hyperelliptic curve of positive genus $g$. Recall that $C$ is isomorphic to a curve of the form

$$C_f\colon z^2 = f(x,y) = f_0x^n + f_1x^{n-1}y + \cdots + f_ny^n,$$

where $n = 2g+2$ and the binary form $f = f(x,y)$ is separable with integer coefficients $f_i$, and where we regard $C_f$ as a curve embedded in the weighted projective plane $\mathbb{P}^2_{\mathbb{Q}}(1,1,g+1)$ with coordinates $[x:y:z]$.

Let $J = \mathrm{Jac}(C)$ be the Jacobian of $C$; if $C = C_f$, we write $J_f = \mathrm{Jac}(C_f)$. Recall that an *$n$-covering of $J$* is an unramified covering $\pi\colon Y \to J$ by a principal homogeneous space $Y$ for $J$, all defined over $\mathbb{Q}$, with the property that $\pi(y+a) = \pi(y) + na$ for any $y \in Y$ and $a \in J$. The degree of any $n$-covering is $n^{2g}$, and the fiber over the origin gives a principal homogeneous space for the $n$-torsion subgroup $J[n]$. The class of this homogeneous space in the Galois cohomology group $H^1(\mathbb{Q}, J[n])$ determines the $n$-covering $\pi$ up to isomorphism.

We say that a variety over $\mathbb{Q}$ is *soluble* if it has a point defined over $\mathbb{Q}$ and *locally soluble* if it has points defined over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every prime $p$. The elements of the *$n$-Selmer group* $\mathrm{Sel}_n(J) \subset H^1(\mathbb{Q}, J[n])$ are in bijection with the isomorphism classes of locally soluble $n$-coverings of $J$; under this correspondence, the elements of the subgroup $J(\mathbb{Q})/nJ(\mathbb{Q}) \subset \mathrm{Sel}_n(J)$ map to the isomorphism classes of soluble $n$-coverings of $J$.

An *$n$-covering of $C$* is an unramified covering $\pi\colon D \to C$ defined over $\mathbb{Q}$ that is Galois over $\overline{\mathbb{Q}}$ and whose Galois group is isomorphic to $J[n](\overline{\mathbb{Q}})$ as a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. If $C$ is soluble, then the Abel-Jacobi map realizes $C$ as a subvariety of $J$, and pullback under the inclusion $C \hookrightarrow J$ defines a bijection between the $n$-coverings of $J$ and those of $C$. When $g = 1$, this bijection preserves both solubility and local solubility.

### 4.1.3 Method of proof and organization

Computing the second moment of $|\operatorname{Sel}_2(E)|$ amounts to determining the average size of the set $\operatorname{Sel}_2(E)^2$ of pairs $(\pi_1, \pi_2)$ of isomorphism classes of locally soluble 2-coverings of $E$. We start by giving a simple heuristic for why the second moment of $|\operatorname{Sel}_2(E)|$ should be 15. To do this, fix a locally soluble 2-covering $\pi_1$ of an elliptic curve $E$, and consider the following cases:

*Case 1*: Suppose $\pi_1$ corresponds to the trivial element of $\operatorname{Sel}_2(E)$. Then $E$ can be arbitrary, and [26, Theorem 1.1] implies that there are 3 choices for $\pi_2$ on average.

*Case 2*: Suppose $\pi_1$ corresponds to a non-trivial element of $\operatorname{Sel}_2(E)$. Then [26, Theorem 1.1] implies that there are 2 choices for $\pi_1$ on average. Moreover, the elliptic curve $E$ cannot be arbitrary—it has a marked non-trivial 2-Selmer element, namely the one corresponding to $\pi_1$. We expect that this marked element gives an extra generator for the 2-Selmer group 100% of the time, and so, there should be $2 \times 3 = 6$ choices for $\pi_2$ on average, twice as many choices as in case 1.

Combining the results of cases 1 and 2, we conclude that there should be a total of $1 \times 3 + 2 \times 6 = 15$ choices for the pair $(\pi_1, \pi_2)$ on average, as desired.

Our proof of Theorem 97 essentially makes the above heuristic rigorous. To compute the average number of pairs of locally soluble 2-coverings of elliptic curves, we apply an enhanced version of the parametrize-and-count strategy used in [22,24,26,27] to determine the average value of $|\operatorname{Sel}_n(E)|$ for $n \in \{2, 3, 4, 5\}$. Our strategy consists of two pieces: an algebraic piece, in which one parametrizes the objects of interest in terms of the rational orbits of a certain coregular representation and constructs integral representatives for these orbits; and an analytic piece, in which one combines geometry-of-numbers and equidistribution techniques to count these integral representatives.

To parametrize pairs of locally soluble 2-coverings, we start by recalling the parametrization of individual locally soluble 2-coverings in terms of $\mathrm{PGL}_2(\mathbb{Q})$-orbits of binary quartic forms over $\mathbb{Q}$. For a binary quartic form $f \in \mathbb{Q}[x, y]$, we call $f$ (locally) soluble if $C_f$ is.

Letting $E = E^{I,J}$ for integers $I, J$, the parametrization states that the map $f \mapsto C_f$ defines a bijection between the set of $\mathrm{PGL}_2(\mathbb{Q})$-orbits of (locally) soluble binary quartic forms with $\mathrm{PGL}_2$-invariants $I, J$ and the set of isomorphism classes of (locally) soluble 2-coverings of $E$.

Our task is then to parametrize pairs $(f, f')$ of locally soluble binary quartic forms that have the same invariants $I, J$. We do this by fibering over the first element of the pair. Fix a locally soluble binary quartic form $f \in \mathbb{Q}[x, y]$ with invariants $I, J$. Let us first consider the case where $f$ is in fact soluble. Here, the set of locally soluble binary quartic forms $f' \in \mathbb{Q}[x, y]$ with invariants $I, J$ is in bijection with the locally soluble 2-coverings of $C_f$ (i.e., elements of $\mathrm{Sel}_2(J_f)$), or equivalently, locally soluble 4-coverings of $E$ (i.e., elements of $\mathrm{Sel}_4(E)$). As shown in [122], such coverings naturally correspond to certain orbits of the group $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$ acting via change-of-basis on pairs $(A, B) \in W_4(\mathbb{Q})$ such that $\iota(A, B) = f$. Thus, we may parametrize pairs $(f, f')$ of binary quartic forms, where $f$ is soluble and $f'$ is locally soluble, in terms of $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$-orbits of pairs $(A, B) \in W_4(\mathbb{Q})$ such that $\iota(A, B) = f$.

The case where $f$ is not soluble is far trickier, because locally soluble binary quartic forms $f' \in \mathbb{Q}[x, y]$ with the same invariants as $f$ are not always realizable as pairs $(A, B) \in W_4(\mathbb{Q})$ satisfying $\iota(A, B) = f$. Indeed, as shown in [17], such a pair $(A, B)$ might not even exist if $f$ is insoluble over $\mathbb{Q}$! To circumvent the possibility that $f$ might not be soluble, we simply manufacture a $\mathbb{Q}$-rational point by replacing $f$ with its *monicization* $f^{\mathsf{mon}}$, which is defined as follows: letting $f_0 \neq 0$ be the leading coefficient of $f$, we write $f^{\mathsf{mon}} := f_0^{-1} \times f(x, f_0 y)$. The soluble genus-1 curve $C_{f^{\mathsf{mon}}}$ is a quadratic twist of $C_f$ by $\mathbb{Q}(\sqrt{f_0})$, and its Jacobian is the elliptic curve $E^{f_0^2 I, f_0^3 J}$; we thus obtain identifications $E^{I,J}[2] \simeq E^{f_0^2 I, f_0^3 J}[2]$ and $J_f[2] \simeq J_{f^{\mathsf{mon}}}[2]$ of group schemes over $\mathbb{Q}$. These identifications induce isomorphisms

$$H^1(\mathbb{Q}, E^{I,J}[2]) \simeq H^1(\mathbb{Q}, E^{f_0^2 I, f_0^3 J}[2]), \quad \text{and} \tag{4.1}$$

$$H^1(\mathbb{Q}, J_f[2]) \simeq H^1(\mathbb{Q}, J_{f^{\mathsf{mon}}}[2]) \tag{4.2}$$

in Galois cohomology. The isomorphism (4.1) maps the classes of the locally soluble 2-coverings defined by $f$ and $f^{\mathsf{mon}}$ to each other. The isomorphism (4.2) allows us to identify locally soluble 2-coverings of $J_f$ with certain 2-coverings of $J_{f^{\mathsf{mon}}}$; crucially, we show that the 2-coverings of $J_{f^{\mathsf{mon}}}$ arising in this way correspond to $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$-orbits of pairs $(A,B) \in W_4(\mathbb{Q})$ such that $\iota(A,B) = f^{\mathsf{mon}}$, and further that these orbits have representatives defined over $\mathbb{Z}$ (up to a bounded factor). More precisely, we have the following result, which holds for binary forms of any even degree $n$ and which we prove in §4.2:

**Theorem 100.** *Let $f \in \mathbb{Z}[x,y]$ be a separable binary form of even degree $n$, and suppose that $C_f$ is locally soluble if $n \equiv 0 \pmod 4$. There is a natural injective map of sets*

$$\mathrm{Sel}_2(J_f) \hookrightarrow \left\{ \begin{array}{c} (\mathrm{SL}_n/\mu_2)(\mathbb{Q})\text{-orbits of } (A,B) \in W_n(\mathbb{Q}) \\ \text{such that } \iota(A,B) = f^{\mathsf{mon}} \end{array} \right\} \tag{4.3}$$

*Moreover, there exists an integer $\kappa \geq 1$ depending only on $n$ such that if we replace the binary $n$-ic form $f(x,y)$ with $g(x,y) = f(x,\kappa y)$, then the $(\mathrm{SL}_n/\mu_2)(\mathbb{Q})$-orbit arising from an element of $\mathrm{Sel}_2(J_g) \simeq \mathrm{Sel}_2(J_f)$ contains an integral representative of the form $(\mathscr{A}_n, B)$.*

Let $f$ be as in Theorem 100. To prove the theorem, we first show that the elements of $\mathrm{Sel}_2(J_f)$ correspond to square roots of the ideal class of the inverse different of $R_f$. We then apply the parametrization developed in §1, which relates square roots of the class of the inverse different of $R_f$ to pairs $(A,B) \in W_n(\mathbb{Z})$ such that $\iota(A,B) = f^{\mathsf{mon}}$.

Once the parametrization has been established, and pairs $(f, f')$ of 2-Selmer elements of elliptic curves have been mapped into $(\mathrm{SL}_4/\mu_2)(\mathbb{Z})$-orbits (equivalently, $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})$-orbits; see §1.3.3) of pairs $(\mathscr{A}_4, B)$ with $\iota(\mathscr{A}_4, B)(x,y) = f^{\mathsf{mon}}(x, \kappa y)$, we must then estimate the number of these orbits having bounded height. The analysis required to do this is considerably more complicated than that developed in previous works, such as [22] or [24], since the current parametrization is not in terms of orbits for a group acting on a single lattice, but rather for a group acting on a family of increasingly sparse subsets of a lattice. Indeed, fix an integer

$a \neq 0$. Then the set of forms $f^{\mathsf{mon}}$, as $f$ varies across binary quartic forms $ax^4 + \cdots$, has density $a^{-6}$ in the set of all monic binary quartic forms. Hence, we expect that the set of pairs $(\mathscr{A}_4, B)$ satisfying $\iota(\mathscr{A}_4, B) = f^{\mathsf{mon}}$ for some $f(x, y) = ax^4 + \cdots$ also has density around $a^{-6}$ in the set of all pairs $(\mathscr{A}_4, B)$.

The leading coefficient $a$ of $f$ grows with the height of the elliptic curve in question. In more concrete terms, let $E = E^{I,J}$ be an elliptic curve such that $H(E) = X^6$. (For the purpose of developing heuristics, this happens to be the most convenient height normalization to take; there are $\asymp X^5$ elliptic curves with height $\leq X^6$.) The set of non-trivial elements in the 2-Selmer group of $E$ (up to some slight subtleties at the prime 2 that we will ignore) admits a surjective map from the set of $\mathrm{PGL}_2(\mathbb{Z})$-orbits on the set of locally soluble binary quartic forms $f$ having invariants $I$ and $J$, such that $f$ has no rational linear factor. By definition, the height of each such form $f$ is also $X^6$. Reduction theory then implies that the $\mathrm{PGL}_2(\mathbb{Z})$-orbit of $f$ has a representative $g(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$, the coefficients of which satisfy the bounds

$$|a| \ll \frac{X}{t^4}, \quad |b| \ll \frac{X}{t^2}, \quad |c| \ll X, \quad |d| \ll t^2X, \quad |e| \ll t^4X,$$

where $t \geq \sqrt[4]{3}/\sqrt{2}$ is necessarily $\ll X^{1/4}$, for otherwise $a$ is forced to be 0. In the balance of this section, we will assume that $t = 1$ for the following reasons: this will simplify the notation considerably; the number of points when $t$ is large is negligible; and for small $t \neq 1$, the proof is identical to the proof when $t = 1$.

The monicization $f^{\mathsf{mon}}$ has coefficients 1, $b$, $ac$, $a^2d$, and $a^3d$, which satisfy the bounds

$$|b| \ll X, \quad |ac| \ll X^2, \quad |a^2d| \ll X^3, \quad |a^3e| \ll X^4.$$

Therefore, any lift $(\mathscr{A}_4, B)$ with $\iota(\mathscr{A}_4, B) = f^{\mathsf{mon}}$ has a representative $(\mathscr{A}_4, B')$ in its $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})$-orbit such that the coefficients $b'_{ij}$ of $B$ are all bounded by some constant times $X$, multiplied by some cuspidal factors that are easily bounded. Furthermore, the element $B'$, like $f$, sat-

isfies congruence conditions having density around $a^{-6}$. (This density is asymptotic to $a^{-6}$ when $a$ is squarefree, but the situation is more complicated when $a$ is divisible by a high power of a prime and is addressed in Lemma 146.) As we show in §4.3, one key feature of the parametrization is that these congruence conditions are actually defined modulo $a$, and not some higher power thereof. A matrix $B \in U_4(\mathbb{Z})$ satisfying these congruence conditions modulo $a$ is said to be *special at* $a$. The condition of being special at a squarefree integer $a$ is beautifully explicit: namely, $B$ must be of rank $\leq 1$ modulo $a$ (i.e., $B$ must be of rank $\leq 1$ modulo $p$ for every prime $p$ dividing $a$). On the contrary, the specialness condition at prime powers is significantly more involved.

Our task is now to determine, for each nonzero $a \asymp X$, an asymptotic for the number of $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})$-orbits on pairs $(\mathscr{A}_4, B)$, where the "height" of $B$ is bounded by $X$ and $B$ is special at $a$. We must then sum this asymptotic over $a$. Heuristically, the total sum is

$$\asymp \sum_{a \asymp X} a^{-6} X^{10} \asymp X^5.$$

This is exactly what we expect, and if made rigorous, could be used to show that the second moment of the size of the 2-Selmer groups of elliptic curves is finite.

However, there are several difficulties in carrying out this strategy. The first is that we need to keep precise control over the error dependence on both $X$ and $a$. When $a$ is around the size of $X$, this requires some additional methods going beyond the use of Davenport's lemma. After introducing the necessary setup in §4.4, we achieve this in §4.5 for squarefree $a$ by proving that special points are equidistributed modulo $a$; this is carried out via twisted Poisson summation together with a computation of the Fourier coefficients of the set of points special at $a$. This method proves the correct asymptotic along with a sufficiently small error term that is explicit in both $X$ and $a$.

Other difficulties arise in the cases not covered above. First, and less seriously, equidistribution methods are not as readily available when $a$ is a multiple of $p^2$ for some prime $p$,

since in this case we do not have sufficiently explicit descriptions of special elements. While this difficulty can be circumvented using the scale invariance of specialness, we choose to resolve it in a way that simultaneously handles the next difficulty.

The second difficulty, which is far more serious, is the following: the "height" function by which we need to count the elements $B$ is not a natural one (hence the scare quotes around the word "height"). Essentially, we must take the naive height on elliptic curves, which yields a $\mathrm{PGL}_2(\mathbb{Z})$-invariant height on the space $V_4(\mathbb{R})$ of binary quartic forms. We must then restrict this height, appropriately scaled, to the space $V_1(\mathbb{R})$ of monic binary quartic forms. Finally, we must lift the height from $V_1(\mathbb{R})$ to the space $W_{\mathscr{A}_4}(\mathbb{R})$ of pairs $(\mathscr{A}_4, B)$, where $B$ has real coefficients.

To see why this produces an unnatural height on $W_{\mathscr{A}_4}(\mathbb{R})$, consider the situation when $a = 1$. In this case, elements in a fundamental set for the action of $\mathrm{PGL}_2(\mathbb{R})$ on $V_4(\mathbb{R})$ with leading coefficient 1 and height less than $X$ consist of polynomials $f(x) = x^4 + bx^3 + cx^2 + dx + e$, the coefficients of which satisfy the bounds

$$b \ll X, \quad c \ll X, \quad d \ll X, \quad e \ll X.$$

When such a region is lifted to $W_{\mathscr{A}_4}(\mathbb{R})$, we obtain a set of elements $B$, the anti-traces of which can be as large as their determinants. Such a region is necessarily quite skewed, and neither Davenport's lemma nor our Fourier analytic methods suffice to count integer points within it while obtaining a sufficiently tight error term. It is not necessary to lower $a$ all the way down to 1: even when $a$ is around $X^{1-\kappa}$, with $\kappa > 1/12$, the associated region in $W_{\mathscr{A}_4}(\mathbb{R})$ is far too skewed, and we are unable to efficiently count integer points in it.

We resolve this problem in §4.5 as follows. Let $a$ be an integer that is small compared to $X$, say $a \asymp X^{1-\kappa}$ for some $\kappa > 0$. Then the set of elements in $V_1(\mathbb{R})$ with "height" less than $X$ consists of polynomials $f(x) = x^4 + bx^3 + cx^2 + dx + e$, where the coefficients of $f$ satisfy

the bounds

$$b \ll X, \quad c \ll X^{2-\kappa}, \quad d \ll X^{3-2\kappa}, \quad e \ll X^{4-3\kappa}.$$

These bounds, as explained before, lead to skewed regions upon lifting to $W_{\mathscr{A}_4}(\mathbb{R})$. Instead, we consider the region inside $V_4(\mathbb{R})$ consisting of elements $f(x,y) = a'x^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$, where the coefficients satisfy the bounds

$$a' \ll X^{\kappa}, \quad b \ll X, \quad c \ll X^{2-\kappa}, \quad d \ll X^{3-2\kappa}, \quad e \ll X^{4-3\kappa}. \tag{4.4}$$

Our goal is now to bound $\mathrm{SL}_4(\mathbb{Z})$-orbits on pairs $(A,B) \in W_4(\mathbb{Z})$ such that: the form $\iota(A,B)$ satisfies the coefficient bounds (4.4); $\det A = 1$; and $B$ is special at $a$. This is possible using traditional geometry-of-numbers methods, since the lift of the set of elements satisfying (4.4) to $W_4(\mathbb{R})$ is not skewed. Moreover, since we only require upper bounds in this case, it suffices to obtain a minimal saving from the condition $\det A = 1$.

We note that this unskewing process, wherein we expand the set of elements in $V_1(\mathbb{R})$ having bounded height, actually requires the action of $\mathrm{SL}_4$ on $W$; just having an action of $\mathrm{PSO}_{\mathscr{A}_4}$ on $W_{\mathscr{A}_4}$ would not suffice. When the powerful part of $a$ (the product of prime powers dividing $a$ with multiplicity greater than 1) is large, we similarly use the action of $\mathrm{SL}_4(\mathbb{Z})$ to obtain upper bounds on the number of $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})$-orbits on $W_{\mathscr{A}_4}(\mathbb{Z})$ with bounded height that are special at $a$. These upper bounds, both when $a$ is small and when the powerful part of $a$ is large, are not optimal. However, we show that because such integers $a$ appear as leading coefficients relatively rarely, their contribution to the second moment is negligible. Consequently, for the purpose of computing the second moment, it is enough to determine asymptotics for the number of $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})$-orbits on $W_{\mathscr{A}_4}(\mathbb{Z})$ of bounded height that are special at $a$ for those leading coefficients $a$ that are both close to $X$ and close to squarefree. As described above, we carry this out using equidistribution methods.

This results in an upper bound on the second moment of the size of the 2-Selmer group of elliptic curves in terms of a product of local integrals. We finish in §4.6 by evaluating

these integrals using a mass formula.

Up to some factors of 6 (see §4.2.2.3 for details), we show in §4.2 that when $n \equiv 2 \pmod 4$ or when $f$ is locally soluble, the 2-Selmer elements of $\mathrm{Jac}(C_f)$ naturally give rise to square roots of the ideal class of the fractional ideal $I_f^{n-2}$ (where $R = \mathbb{Z}$, $\mathbb{Q}$, or a completion thereof).

## 4.2 Parametrization of 2-Selmer groups of hyperelliptic Jacobians

The purpose of this section is to prove Theorem 100. We begin in §4.2.1 by constructing rational orbits from 2-Selmer elements. This construction of rational orbits can be regarded as a reformulation of a result of Stoll and van Luijk, namely [115, Theorem 1.1], in terms of the action of $\mathrm{SL}_n/\mu_2$ on $W$. Crucially, we show in §4.2.2 that the rational orbits arising from 2-Selmer elements have integral representatives, thus allowing us to use geometry-of-numbers methods to count 2-Selmer elements.

### 4.2.1 Construction of rational orbits via Galois cohomology

In this section, we first rephrase the parametrization of rational orbits in Proposition 21 in the language of Galois cohomology. We then apply this rephrasing to construct the desired rational orbits from 2-Selmer elements.

#### 4.2.1.1 Reinterpreting the parametrization using Galois cohomology

Take a pair $(A, B_0) \in W_n(K)$ with $\iota(A, B_0) = f^{\mathsf{mon}}$. Applying Proposition 21 to the separable closure $K_{\mathrm{sep}}$ of $K$, we see that there is a unique $(\mathrm{SL}_n/\mu_2)(K_{\mathrm{sep}})$-orbit on $W_n(K_{\mathrm{sep}})$ with resolvent $f^{\mathsf{mon}}$. Let $(A_f, B_f) \in W_n(K_{\mathrm{sep}})$ be a representative of this unique $(\mathrm{SL}_n/\mu_2)(K_{\mathrm{sep}})$-orbit. Then there exists $g \in (\mathrm{SL}_n/\mu_2)(K_{\mathrm{sep}})$ such that $(A, B_0) = g \cdot (A_f, B_f)$. For any $\sigma \in \mathrm{Gal}(K_{\mathrm{sep}}/K)$, we have that $(A, B_0) = {}^{\sigma}g \cdot (A_f, B_f)$, so $g^{-1\sigma}g \in \mathrm{Stab}_{(\mathrm{SL}_n/\mu_2)(K_{\mathrm{sep}})}(A_f, B_f)$,

and the map $\sigma \mapsto g^{-1\sigma}g$ defines a 1-cocycle on $\mathrm{Gal}(K_{\mathrm{sep}}/K)$ with values in

$$\mathrm{Stab}_{(\mathrm{SL}_n/\mu_2)(K_{\mathrm{sep}})}(A_f, B_f) \simeq \big((\mathrm{Res}_{K_f/K}\,\mu_2)_{\mathrm{N}\equiv 1}/\mu_2\big)(K_{\mathrm{sep}}),$$

the cohomology class of which depends only on the $(\mathrm{SL}_n/\mu_2)(K)$-orbit of $(A, B)$ and has trivial image under the map $\delta_K\colon H^1(K, (\mathrm{Res}_{K_f/K}\,\mu_2)_{\mathrm{N}\equiv 1}/\mu_2) \to H^1(K, \mathrm{SL}_n/\mu_2)$. This construction defines a bijection

$$\left\{ \begin{array}{l} (\mathrm{SL}_n/\mu_2)(K)\text{-orbits on } W_n(K) \\ \text{with resolvent } f^{\mathsf{mon}} \end{array} \right\} \longleftrightarrow \ker \delta_K. \tag{4.5}$$

From the long exact sequence in cohomology of the short exact sequence

$$1 \longrightarrow (\mathrm{Res}_{K_f/K}\,\mu_2)_{\mathrm{N}\equiv 1}/\mu_2 \longrightarrow \mathrm{Res}_{K_f/K}\,\mu_2/\mu_2 \xrightarrow{\mathrm{N}} \mu_2 \longrightarrow 1$$

we obtain the following surjective map:

$$\phi\colon H^1(K, (\mathrm{Res}_{K_f/K}\,\mu_2)_{\mathrm{N}\equiv 1}/\mu_2) \twoheadrightarrow \ker\big(\mathrm{N}\colon H^1(K, \mathrm{Res}_{K_f/K}\,\mu_2/\mu_2) \to H^1(K, \mu_2)\big) \tag{4.6}$$

As shown in [16, §4.4], the subset $\phi^{-1}((K_f^\times/K_f^{\times 2}K^\times)_{\mathrm{N}\equiv 1}) \subset H^1(K, (\mathrm{Res}_{K_f/K}\,\mu_2)_{\mathrm{N}\equiv 1}/\mu_2)$ lies in $\ker\delta_K$, so to prove that a class in $H^1(K, (\mathrm{Res}_{K_f/K}\,\mu_2)_{\mathrm{N}\equiv 1}/\mu_2)$ corresponds to an $(\mathrm{SL}_n/\mu_2)(K)$-orbit on $W_n(K)$ with resolvent $f^{\mathsf{mon}}$ under the bijection (4.5), it suffices to show that its image under $\phi$ lies in $(K_f^\times/K_f^{\times 2}K^\times)_{\mathrm{N}\equiv 1}$.

#### 4.2.1.2 The construction

To construct the map (4.3), we first work over a local field $K$ of characteristic not equal to 2. Let $f \in V_n(K)$ be a separable binary $n$-ic form with nonzero leading coefficient, and assume that $C_f$ is soluble over $K$ if $n \equiv 0 \pmod 4$. We shall now construct an injective map of sets

$$J_f(K)/2J_f(K) \hookrightarrow \left\{ \begin{array}{c} (\mathrm{SL}_n/\mu_2)(K)\text{-orbits of } (A,B) \in W_n(K) \\ \\ \text{such that } \iota(A,B) = f^{\mathsf{mon}} \end{array} \right\} \tag{4.7}$$

By [17, part (2) of Proposition 22], we have

$$J_f[2] \simeq (\mathrm{Res}_{K_f/K}\,\mu_2)_{\mathrm{N}\equiv 1}/\mu_2 \simeq (\mathrm{Res}_{K_{f^{\mathsf{mon}}}/K}\,\mu_2)_{\mathrm{N}\equiv 1}/\mu_2$$

as group schemes over $K$.

Upon combining the 2-descent map $J_f(K)/2J_f(K) \hookrightarrow H^1(K, J_f[2])$ with the cohomological description of the parametrization in Proposition 21 established in §4.2.1.1, we obtain the following commutative diagram:

$$\begin{array}{ccccc} J_f(K)/2J_f(K) & & \xrightarrow{\text{“}x-\theta\text{”}} & & (K_f^\times/K_f^{\times 2}K^\times)_{\mathrm{N}\equiv 1} \\ \downarrow & & & & \downarrow \\ H^1(K, J_f[2]) & \xrightarrow[\sim]{} & H^1(K, (\mathrm{Res}_{K_{f^{\mathsf{mon}}}/K}\,\mu_2)_{\mathrm{N}\equiv 1}/\mu_2) & \xrightarrow[\phi]{} & \ker \mathrm{N} \end{array} \tag{4.8}$$

where the homomorphism “$x-\theta$” in the top row of (4.8) is defined in [93, §5] and essentially evaluates the quantity $x-\theta$ on divisor classes. That the “$x-\theta$” map is defined on all of $J_f(K)/2J_f(K)$ follows from our assumption that $C_f$ is soluble when $n \equiv 0 \pmod 4$ (see [93, §10]). From (4.8), we see that the image of $J_f(K)/2J_f(K)$ in $\ker \mathrm{N}$ lies in the subset $(K_f^\times/K_f^{\times 2}K^\times)_{\mathrm{N}\equiv 1} \simeq (K_{f_{\mathsf{mon}}}^\times/K_{f_{\mathsf{mon}}}^{\times 2}K^\times)_{\mathrm{N}\equiv 1}$, so we conclude that the image of $J_f(K)/2J_f(K)$ in $H^1(K, (\mathrm{Res}_{K_{f^{\mathsf{mon}}}/K}\,\mu_2)_{\mathrm{N}\equiv 1}/\mu_2)$ lies in $\ker \delta_K$. Since classes in $\ker \delta_K$ correspond to orbits, we obtain the desired map (4.7).

Now let $K = \mathbb{Q}$. Since the group $\mathrm{SL}_n/\mu_2$ is an adjoint group, we have from [90, Theorem 6.22] that the map

$$H^1(\mathbb{Q}, \mathrm{SL}_n/\mu_2) \to \prod_v H^1(\mathbb{Q}_v, \mathrm{SL}_n/\mu_2)$$

is injective, where the product on the right-hand side is taken over all places $v$ of $\mathbb{Q}$. That the local map $J_f(\mathbb{Q}_v)/2J_f(\mathbb{Q}_v) \hookrightarrow H^1(\mathbb{Q}_v, J_f[2])$ has image contained in $\ker \delta_{\mathbb{Q}_v}$ for every place $v$ of $\mathbb{Q}$ then implies that the global map $\mathrm{Sel}_2(J_f) \hookrightarrow H^1(\mathbb{Q}, J_f[2])$ has image contained in $\ker \delta_{\mathbb{Q}}$, as desired.

We now claim that the $(\mathrm{SL}_n/\mu_2)(\mathbb{Q}_v)$-orbit (resp., $(\mathrm{SL}_n/\mu_2)(\mathbb{Q})$-orbit) arising from an element $\alpha_0 \in J_f(\mathbb{Q}_v)/2J_f(\mathbb{Q}_v)$ (resp., $\alpha_0 \in \mathrm{Sel}_2(J_f)$) admits a representative of the form $(\mathscr{A}_n, B)$ for some matrix $B \in W_{\mathscr{A}_n}(\mathbb{Q}_v)$ (resp., $B \in W_{\mathscr{A}_n}(\mathbb{Q})$). It suffices to prove the following:

**Proposition 101.** *Let $v$ be a place of $\mathbb{Q}$, and let $(A, B) \in W_n(\mathbb{Q}_v)$ be a representative of the orbit arising from an element of $J_f(\mathbb{Q}_v)/2J_f(\mathbb{Q}_v)$ via (4.7). Then $A$ is split over $\mathbb{Q}_v$.*

*Proof.* Choose an element $\alpha_0 \in J_f(\mathbb{Q}_v)/2J_f(\mathbb{Q}_v)$, and let $\alpha \in K_f^\times$ be a representative of $(x-\theta)(\alpha_0)$. It suffices to show that the symmetric bilinear form $\pi_{n-1} \circ \langle -, - \rangle \colon K_f \times K_f \to \mathbb{Q}_v$ has a maximal isotropic subspace defined over $\mathbb{Q}_v$. In [105, proof of Theorem 10], a maximal isotropic subspace over $\mathbb{Q}_v(\sqrt{f_0})$ is constructed, and an explicit basis $\big(\mathbb{Q}_v(\sqrt{f_0})\big)\langle v_1, \dots, v_{\frac{n}{2}} \rangle$ is given. This basis has the property that, for some integer $i \in \{1, \dots, \frac{n}{2}\}$, we have $v_j \in K_f$ for each $j \leq i$ and $v_j \in \sqrt{f_0} K_f$ for each $j > i$. Letting $v'_j := \sqrt{f_0^{-1}} v_j \in K_f$ for each $j > i$, we conclude that the basis $\mathbb{Q}_v\langle v_1, \dots, v_i, v'_{i+1}, \dots, v'_{\frac{n}{2}} \rangle$ defines a maximal isotropic subspace over $\mathbb{Q}_v$. □

By (1.12) and Proposition 101, we see that an element $\alpha_0 \in J_f(\mathbb{Q}_v)/2J_f(\mathbb{Q}_v)$ (resp., $\alpha_0 \in \mathrm{Sel}_2(J_f)$) gives rise to an orbit of $\mathrm{PSO}_{\mathscr{A}_n}(\mathbb{Q}_v)$ on $W_{\mathscr{A}_n}(\mathbb{Q}_v)$ (resp., $\mathrm{PSO}_{\mathscr{A}_n}(\mathbb{Q})$ on $W_{\mathscr{A}_n}(\mathbb{Q})$).

Let $K$ be any field. In what follows, when we consider binary forms with a fixed nonzero leading coefficient $f_0$, we say that an element $B \in W_{\mathscr{A}_n}(K)$ is *soluble* if it arises via the above construction from an element of $J_f(K)/2J_f(K)$ for some binary form $f \in V_{n,f_0}(K)$. When $K = \mathbb{Q}$, we say that an element $B \in W_{\mathscr{A}_n}(K)$ is *locally soluble* if it is soluble over $\mathbb{Q}_v$ for every place $v$ of $\mathbb{Q}$.

### 4.2.2 Construction of integral representatives

We now want to construct integral representatives for the rational orbits arising from 2-Selmer elements. To do this, it suffices to work over $K = \mathbb{Q}_p$. Let $f \in V_{n,f_0}(\mathbb{Z}_p)$ be a binary $n$-ic form with nonzero leading coefficient $f_0$ that is separable over $\mathbb{Q}_p$, and assume that $C_f$ is soluble over $\mathbb{Q}_p$ if $n \equiv 0 \pmod 4$. Fix an element $\alpha_0 \in J_f(\mathbb{Q}_p)/2J_f(\mathbb{Q}_p)$. We then have the following result, the proof of which occupies the balance of this section:

**Theorem 102.** *There exists an integer $\kappa \geq 1$ depending only on $n$ such that if we replace the binary $n$-ic form $f(x,y)$ with $g(x,y) = f(x,\kappa y)$, then the $(\mathrm{SL}_n/\mu_2)(\mathbb{Q}_p)$-orbit on $W_n(\mathbb{Q}_p)$ arising from $\alpha_0$, viewed as an element of $J_g(\mathbb{Q}_p)/2J_g(\mathbb{Q}_p)$, contains a representative of the form $(\mathscr{A}_n, B) \in W_n(\mathbb{Z}_p)$.*

We split the proof of Theorem 102 into three successively more complicated cases, depending on whether $f$ is primitive and on whether $p > n$. We start in §4.2.2.1 with the case where $f$ is primitive and $p > n$. In this case, it is not necessary to scale the variable $y$: we can construct an integral representative with resolvent $f$ itself. The construction is facilitated by the fact that we can replace a binary $n$-ic form with a suitable $\mathrm{SL}_2(\mathbb{Z}_p)$-translate whose leading coefficient is not divisible by $p$. Then, in §4.2.2.2, we modify the construction in §4.2.2.1 to handle imprimitive $f$ when $p > n$; here too, we obtain an integral representative with resolvent $f$. We conclude in §4.2.2.3 by building upon the construction in §4.2.2.2 to handle the case where $p < n$; here, we construct an integral representative with resolvent $f(x, p^{\mathcal{D}}y)$ for some integer $\mathcal{D} \geq 0$. We then take $\kappa = \prod_{p<n} p^{\mathcal{D}}$.

#### 4.2.2.1 Construction of integral representative for $f$ primitive and $p > n$

Suppose that $f$ is primitive and that $p > n$. Then there exists $\gamma = \left[\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z}_p)$ such that the binary $n$-ic form $f'(x,y) := f((x,y)\cdot\gamma) = \sum_{i=0}^{n} f'_i x^{n-i}y^i$ has leading coefficient $f'_0 \in \mathbb{Z}_p^\times$. Let $\theta' = \frac{-u+v\theta}{s-t\theta} \in K_{f'}$ be the root of $f'$, let $R_{f'} = \mathbb{Z}_p\langle\zeta'_1, \ldots, \zeta'_{n-1}\rangle$ be the basis elements (1.1) of $R_{f'}$ defined with respect to $\theta'$, and let $\mathrm{N}'$ denote the norm with respect to this basis. Let

$\alpha_0'$ be the image of $\alpha_0$ under the isomorphism $J_f(\mathbb{Q}_p)/2J_f(\mathbb{Q}_p) \simeq J_{f'}(\mathbb{Q}_p)/2J_{f'}(\mathbb{Q}_p)$ induced by $\gamma$. We first construct a pair $(I', \alpha')$, where $I'$ is a based fractional ideal of $R_{f'}$ and $\alpha' \in K_{f'}$ is a representative of $(x-\theta')(\alpha_0')$ such that ${I'}^2 \subset \alpha' I_{f'}^{n-2}$ and $\mathrm{N}'(I')^2 = \mathrm{N}'(\alpha'){f_0'}^{2-n}$. Then, the orbit corresponding to $(I', \alpha')$ has resolvent $f'$, so by Lemma 14, we can transform $(I', \alpha')$ into a pair $(I, \alpha)$ for $f$.

Since we assumed that either $n \equiv 0 \pmod 4$ and $C_{f'}(\mathbb{Q}_p) \neq \varnothing$ or $n \equiv 2 \pmod 4$, it follows from [17, Proposition 21] that there exists a rational divisor $\widetilde{D} \in \mathrm{Div}^0(C_{f'})(\mathbb{Q}_p)$ such that $\alpha_0' = [\widetilde{D}] \in J_{f'}(\mathbb{Q}_p)/2J_{f'}(\mathbb{Q}_p)$. The next lemma shows that we can replace the divisor $\widetilde{D}$ with a new divisor $D$ satisfying properties that turn out to be crucial in constructing the desired ideal $I'$. For monic forms $f'$, this lemma was proven in [121, §3]. Here, we extend that argument to handle classes $\widetilde{D} \in \mathrm{Div}^0(C_{f'})(\mathbb{Q}_p)$, where $f_0' \in \mathbb{Z}_p^\times$ is not necessarily equal to 1.

**Lemma 103.** *There exists an effective divisor $D = \sum_{i=1}^m (P_i') \in \mathrm{Div}(C_{f'})(\mathbb{Q}_p)$ such that the following three properties are satisfied:*

- $m \leq \frac{n}{2}$;
- $P_i' = (a_i', 1, c_i') \in C_{f'}(\overline{\mathbb{Q}}_p)$ *with* $a_i' \in \mathcal{O}_{\overline{\mathbb{Q}}_p}$ *and* $c_i' \neq 0$ *for each* $i \in \{1, \ldots, m\}$; *and*
- $(x-\theta')(D) = (x-\theta')(\widetilde{D}) \in (K_{f'}^\times / K_{f'}^{\times 2}\mathbb{Q}_p^\times)_{\mathrm{N}\equiv 1}$.

*Proof.* We construct the desired divisor $D$ in a sequence of three steps as follows:

Step 1: It is a standard fact (see [93, §5]) that there exists a principal divisor $D_1 \in \mathrm{Div}^0(C_{f'})(\mathbb{Q}_p)$ such that $\widetilde{D} + D_1$ is supported neither at the ramification points of $C_{f'}$ over $\mathbb{P}^1_{\mathbb{Q}_p}$, nor at the points $(1, 0, \pm\sqrt{f_0'}) \in C_{f'}(\overline{\mathbb{Q}}_p)$ lying above infinity in $\mathbb{P}^1_{\mathbb{Q}_p}$. We define $D$ to be $\widetilde{D} + D_1$; by translating $D$ with divisors of the form $2D'$, where $D'$ is the divisor corresponding to a closed point of $C_{f'}$ over $\mathbb{Q}_p$, we may assume that each point in the support of $D$ occur with multiplicity equal to 1. It is clear that $(x-\theta')(\widetilde{D}) = (x-\theta')(D)$.

Step 2: We now construct a divisor $D_2 \in \mathrm{Pic}^0(C_{f'})(\mathbb{Q}_p)$ such that $D - D_2$ has at most $\frac{n}{2}$ non-infinite points in its support. In the previous paragraph, we arranged for $D$ to take the

form $D = \sum_{i=1}^{k}(Q_i)$, where $Q_i = (\mathfrak{a}_i, 1, \mathfrak{c}_i) \in C_{f'}(\overline{\mathbb{Q}}_p)$ with $\mathfrak{c}_i \neq 0$ for each $i$. If $k > \frac{n}{2}$, let $\mathfrak{P} \in \mathbb{Q}_p[x]$ be the monic polynomial of degree $k$ defined by $\mathfrak{P}(x) = \prod_{i=1}^{k}(x - \mathfrak{a}_i)$, and let $\mathfrak{R} \in \mathbb{Q}_p[x]$ be the unique (not necessarily monic) polynomial of minimal degree at most $k-1$ such that $\mathfrak{R}(\mathfrak{a}_i) = \mathfrak{c}_i$ for each $i \in \{1, \ldots, k\}$. Then the polynomial $\mathfrak{R}(x)^2 - f'(x, 1) \in \mathbb{Q}_p[x]$ has a root $x = \mathfrak{a}_i$ for each $i \in \{1, \ldots, k\}$, so we have that $\mathfrak{R}(x)^2 - f'(x, 1) = \mathfrak{P}(x)\mathfrak{H}(x)$ for some polynomial $\mathfrak{H} \in \mathbb{Q}_p[x]$. Because $f'$ is separable over $\mathbb{Q}_p$, we have that $\mathfrak{H} \not\equiv 0$.

Consider the rational function $g := y - \mathfrak{R}(x)$ on $C_{f'}$. Note that $g$ is defined over $\mathbb{Q}_p$, that the zeros of $g$ are precisely the zeros of $\mathfrak{P}\mathfrak{H}$, and that the poles of $g$ lie over infinity. Thus, letting $\mathrm{div}(g)$ be the principal divisor associated to the function $g$, we have that $D - \mathrm{div}(g)$ is supported over the zeros of $\mathfrak{H}$ and over the infinite points. But since $k > \frac{n}{2}$, we have that

$$\deg \mathfrak{H} = \deg(\mathfrak{R}(x)^2 - f'(x, 1)) - \deg \mathfrak{P}(x) \leq k - 1,$$

so $D - \mathrm{div}(g)$ has strictly fewer than $k$ non-infinite points in its support. By iterating the above process, we obtain a sequence of functions $g = g_1, g_2, \ldots, g_\ell$ until $D - \sum_{i=1}^{\ell} \mathrm{div}(g_i)$ has at most $\frac{n}{2}$ non-infinite points in its support. We let $D_2 = \sum_{i=1}^{\ell} \mathrm{div}(g_i)$, and we redefine $D$ to be $D - D_2$. Just as in step 1, we modify $D$ so as to ensure that each point in the support of $D$ occurs with multiplicity 1. Once again, the above modifications leave $(x - \theta')(D)$ unchanged.

Step 3: We now claim that we can simply delete every point in the support of $D$ that is not of the form $(\mathfrak{a}, 1, \mathfrak{c})$, where $\mathfrak{a} \in \mathcal{O}_{\overline{\mathbb{Q}}_p}$. Observe that there are two ways for a point $(\mathfrak{a}, \mathfrak{b}, \mathfrak{c}) \in C_{f'}(\overline{\mathbb{Q}}_p)$ in the support of $D$ to fail to be in this form: either $\mathfrak{b} \neq 0$ and $\mathfrak{a}/\mathfrak{b} \notin \mathcal{O}_{\overline{\mathbb{Q}}_p}$, or $(\mathfrak{a}, \mathfrak{b}, \mathfrak{c}) = (1, 0, \pm\sqrt{f'_0})$ is one of the points at infinity. We handle each of these two cases as follows:

*Case 1*: First suppose that we have a point $Q_1 = (\mathfrak{a}_1, 1, \mathfrak{c}_1) \in C_{f'}(\overline{\mathbb{Q}}_p)$ in the support of $D$ such that $\mathfrak{a}_1 \notin \mathcal{O}_{\overline{\mathbb{Q}}_p}$. Let $\{Q_i = (\mathfrak{a}_i, 1, \mathfrak{c}_i) : 1 \leq i \leq k\}$ be the set of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-conjugates of $Q_1$; since $D$ is a rational divisor, each $Q_i$ occurs with the same multiplicity $\nu$. We claim that $\xi := \prod_{i=1}^{k}(\mathfrak{a}_i - \theta) \in K_{f'}^{\times 2}\mathbb{Q}_p^{\times}$. Indeed, since $\mathfrak{a}_i \notin \mathcal{O}_{\overline{\mathbb{Q}}_p}$, the denominator of $\xi$ is $p^j$ for

some integer $j > 0$, and for a suitable $u \in \mathbb{Z}_p^\times$, we have $up^j\xi \in K_f^{\times 2}$. We then redefine $D$ to be $D - \sum_{i=1}^k Q_i$.

*Case 2*: Now suppose that $(1, 0, \sqrt{f_0'}) \in C_f(\overline{\mathbb{Q}}_p)$ is in the support of $D$. If $f_0' \notin \mathbb{Q}_p^{\times 2}$, it follows that $(1, 0, -\sqrt{f_0'})$ is also in the support of $D$, and so the support of $D$ over the points at infinity is a multiple of the hyperelliptic class, and it follows from [93, Proposition 5.1] that this class lies in the kernel of the "$x - \theta'$" map. If $f_0' \in \mathbb{Q}_p^{\times 2}$, then [39, §2] implies that $(x - \theta')(1, 0, \pm\sqrt{f_0'}) = f_0' \equiv 1$. We may thus simply delete all of the infinite points in the support of $D$.

The modifications performed in both cases 1 and 2 above leave $(x - \theta')(D)$ unchanged. This completes the proof of the proposition. □

Let $D$ be as in Lemma 103. We proceed with the construction under the assumption that $m$ is even; at the end of this section, we explain how to deal with the case where $m$ is odd.

If $m = 0$, then we simply take $(I', \alpha') = \left(I_{f'}^{\frac{n-2}{2}}, 1\right)$. Now suppose that $m > 0$. We define polynomials $\mathcal{P}$, $\mathcal{R}$, and $\mathcal{H}$, much as in step 2 of the proof of Lemma 103, but this time, we strive to ensure that these polynomials have integral coefficients. Let $\mathcal{P} \in \mathbb{Q}_p[x]$ be the monic polynomial of degree $m$ defined by $\mathcal{P}(x) = \prod_{i=1}^m (x - a_i')$. By our construction of $D$ in Lemma 103, the class $\alpha' := \mathcal{P}(\theta') \in (K_f^\times / K_f^{\times 2}\mathbb{Q}_p^\times)_{\mathrm{N}\equiv 1}$ is equal to $(x - \theta')(\alpha_0')$. Next, let $\mathcal{R} \in \mathbb{Q}_p[x]$ be the unique (not necessarily monic) polynomial of minimal degree at most $m-1$ such that $\mathcal{R}(a_i') = c_i'$ for each $i \in \{1, \ldots, m\}$. Then the polynomial $\mathcal{R}(x)^2 - f'(x, 1) \in \mathbb{Q}_p[x]$ has a root at $x = a_i'$ for each $i$, so there exists $\mathcal{H} \in \mathbb{Q}_p[x]$ such that $\mathcal{R}(x)^2 - f'(x, 1) = \mathcal{P}(x)\mathcal{H}(x)$. Since we chose $D$ so that $a_i' \in \mathcal{O}_{\overline{\mathbb{Q}}_p}$ for each $i$, we have $\mathcal{P} \in \mathbb{Z}_p[x]$. We proceed under the assumption that we also have $\mathcal{R} \in \mathbb{Z}_p[x]$; at the end of this section, we explain how to handle the case where $\mathcal{R} \notin \mathbb{Z}_p[x]$. Then, since $\mathcal{P}, \mathcal{R}, f'(x, 1) \in \mathbb{Z}_p[x]$, it follows from the relation $\mathcal{R}(x)^2 - f'(x, 1) = \mathcal{P}(x)\mathcal{H}(x)$ that $\mathcal{H} \in \mathbb{Z}_p[x]$ as well.

Consider the following $R_{f'}$-submodule of $K_{f'}$:

$$I' = R_{f'}\langle \mathcal{R}(\theta'), \mathcal{P}(\theta') \rangle.$$

Note that $\theta' \in R_{f'}$ because $f_0' \in \mathbb{Z}_p^\times$, so since $\mathcal{P}, \mathcal{R} \in \mathbb{Z}_p[x]$, the fractional ideal $I'$ is in fact an integral ideal of $R_{f'}$. We now prove that the pair $(I', \alpha') \in H_{f',1}$:

**Lemma 104.** *We have $I'^2 \subset \alpha' I_{f'}^{n-2}$, and for some choice of a basis of $I'$, we have*

$$\mathrm{N}'(I')^2 = \mathrm{N}'(\alpha') {f_0'}^{2-n}.$$

*Proof.* Computing the square of $I'$ yields the following:

$$I'^2 = R_{f'}\langle \mathcal{R}(\theta')^2, \mathcal{R}(\theta')\mathcal{P}(\theta'), \mathcal{P}(\theta')^2 \rangle = \alpha' R_{f'} \langle \mathcal{H}(\theta'), \mathcal{R}(\theta'), \mathcal{P}(\theta') \rangle \subset \alpha' R_{f'},$$

where the last step above follows from the fact that $\theta' \in R_{f'}$ and $\mathcal{P}, \mathcal{R}, \mathcal{H} \in \mathbb{Z}_p[x]$. Since $p \nmid f_0'$, we have that $R_{f'} = I_{f'}^{n-2}$, and the first assertion follows.

That $\mathrm{N}'(I')^2$ and $\mathrm{N}'(\alpha'){f_0'}^{2-n}$ generate the same fractional ideal of $\mathbb{Z}_p$ follows immediately from [15, proof of Proposition 8.5]. Since both $\mathrm{N}'(I')^2$ and $\mathrm{N}'(\alpha'){f_0'}^{2-n}$ are elements of $\mathbb{Q}_p^{\times 2}$, we can choose a basis of $I'$ so as to ensure that $\mathrm{N}'(I')^2 = \mathrm{N}'(\alpha'){f_0'}^{2-n}$. □

Next suppose that $\mathcal{R} \notin \mathbb{Z}_p[x]$. Since $f_0' \in \mathbb{Z}_p^\times$, it follows from [105, proof of Proposition 12] (see also [15, proof of Proposition 8.5]) that we can modify $D$ so that it is supported on $m-2$ points while preserving the properties in Lemma 103. If the value of the new polynomial $\mathcal{R}$ arising from the modified divisor $D$ fails to be integral, we induct downward, repeating the process until $\mathcal{R}$ becomes integral or $D$ is supported on at most 1 point.

We now handle the case where $m$ is odd. After applying the steps in the proof of Lemma 103, the only way for this to fail is if we performed a deletion of an odd-degree closed point of $C_{f'}$ over $\mathbb{Q}_p$ in step 3. Regardless of whether this deletion occurred in case 1 or 2 of step 3, we must have $f_0' \in \mathbb{Q}_p^{\times 2}$, so the points $(1, 0, \pm\sqrt{f_0'})$ at infinity must be defined over $\mathbb{Q}_p$. In this case, if $m$ is odd, it follows from [17, proof of Proposition 34] that there exists a fractional ideal $I'$ of $R_{f'}$ such that $I'^2 \subset \alpha I_{f'}^{n-3}$ and $\mathrm{N}'(I')^2 = \mathrm{N}'(\alpha'){f_0'}^{3-n}$. But since $f_0' \in \mathbb{Z}_p^\times$, we have that $I_{f'}^{n-3} = I_{f'}^{n-2}$ as fractional ideals, and since $f_0' \in \mathbb{Q}_p^{\times 2}$, we can find a

basis of $I'$ with respect to which $\mathrm{N}'(I')^2 = \mathrm{N}'(\alpha')f_0'^{2-n}$.

#### 4.2.2.2 Construction of integral representative for $f$ imprimitive and $p > n$

Suppose that $\gcd(f_0, \ldots, f_n) = p^d$ for some $d > 0$ and that $p > n$. We first show that we can reduce the problem to the case where $d = 1$. Suppose that $d > 1$, and let $\widetilde{f} = p^{-2\lfloor d/2 \rfloor} f \in \mathbb{Z}_p[x, y]$; notice that the greatest common divisor of the coefficients of $\widetilde{f}$ is either 1 or $p$. Then $C_f \simeq C_{\widetilde{f}}$, and this isomorphism induces an identification $J_f(\mathbb{Q}_p)/2J_f(\mathbb{Q}_p) \simeq J_{\widetilde{f}}(\mathbb{Q}_p)/2J_{\widetilde{f}}(\mathbb{Q}_p)$; letting $\widetilde{\alpha}_0$ be the image of $\alpha_0$ under this identification, observe that $(x-\theta)(\alpha_0) = (x-\theta)(\widetilde{\alpha}_0)$.

Suppose that we have constructed a pair $(\widetilde{I}, \widetilde{\alpha}) \in H_{\widetilde{f},1}$, where $\widetilde{\alpha} \in K_{\widetilde{f}}^{\times} = K_f^{\times}$ is a representative of $(x-\theta)(\widetilde{\alpha}_0)$, and let $(A, B) \in W_n(\mathbb{Z}_p)$ be any representative of the corresponding $\mathrm{SL}_n^{\pm}(\mathbb{Z}_p)$-orbit. Then by Lemma 22, the pair $(A, p^{2\lfloor d/2 \rfloor}B) \in W_n(\mathbb{Z}_p)$ lies in the image of $\mathsf{orb}_{f,1}$, and its $G_n(\mathbb{Q}_p)$-orbit corresponds via Proposition 19 to $\widetilde{\alpha} = (x-\theta)(\alpha_0) \in K_f^{\times}/K_f^{\times 2}$, as desired. We have thus reduced the problem to the case where $d \in \{0, 1\}$; if $d = 0$, then the construction in §4.2.2.1 applies, so we assume that $d = 1$ in the remainder of this section.

Just like in §4.2.2.1, we now replace $f$ with its translate $f'(x, y) = f((x, y)\gamma)$ by an element $\gamma \in \mathrm{SL}_2(\mathbb{Z}_p)$; this time, however, we choose $\gamma$ so that $p$ divides the leading coefficient $f_0'$ of $f'$ exactly once (such a $\gamma$ exists because $p > n$). Recalling the notation from §4.2.2.1, it once again suffices by Lemma 14 to construct a pair $(I', \alpha')$, where $I'$ is a based fractional ideal of $R_{f'}$ and $\alpha' \in K_f'$ is a representative of $(x-\theta')(\alpha_0')$ such that $I'^2 \subset \alpha' I_{f'}^{n-2}$ and $\mathrm{N}'(I')^2 = \mathrm{N}'(\alpha')f_0'^{2-n}$.

Just like we argued in §4.2.2.1, [17, Proposition 21] implies that there exists a divisor $\widetilde{D} \in \mathrm{Div}^0(C_{f'})(\mathbb{Q}_p)$ such that $\alpha_0' = [\widetilde{D}] \in J_{f'}(\mathbb{Q}_p)/2J_{f'}(\mathbb{Q}_p)$. The following lemma gives the analogue of Lemma 103 in the present setting:

**Lemma 105.** *There exists an effective divisor $D = \sum_{i=1}^{m}(P_i') \in \mathrm{Div}(C_{f'})(\mathbb{Q}_p)$ such that the following three properties are satisfied:*

- *$m \leq \frac{n}{2}$ is even;*

- $P_i' = (a_i', 1, c_i') \in C_{f'}(\overline{\mathbb{Q}}_p)$ *with* $a_i' \in \mathcal{O}_{\overline{\mathbb{Q}}_p}$ *and* $c_i' \neq 0$ *for each* $i \in \{1, \ldots, m\}$*; and*
- $(x - \theta')(D) = (x - \theta')(\widetilde{D}) \in (K_{f'}^\times / K_{f'}^{\times 2} \mathbb{Q}_p^\times)_{\mathrm{N} \equiv 1}$.

*Proof.* Steps 1 and 2 in the proof of Lemma 103 go through without change. As for step 3, let $f''(x, y) = p^{-1} f'(x, y)$. Then the "$x - \theta'$" map for $f'$ is the same as that for $f''$; thus, the argument in case 1 of step 3 implies that we can delete all points of the form $(\mathfrak{a}, 1, \mathfrak{c})$ such that $\mathfrak{a} \notin \mathcal{O}_{\overline{\mathbb{Q}}_p}$. Since the points $(1, 0, \pm\sqrt{f_0'})$ are evidently not defined over $\mathbb{Q}_p$, the number $m$ must be even. □

Let $D$ be as in Lemma 105. If $m = 0$, then we simply take $(I', \alpha') = \left(I_{f'}^{\frac{n-2}{2}}, 1\right)$. Now suppose that $m > 0$. We define polynomials $\mathcal{P}$, $\mathcal{R}$, and $\mathcal{H}$, much as in §4.2.2.1, but this time, we strive to ensure not only that these polynomials have integral coefficients, but also that the coefficients of $\mathcal{R}$ are divisible by $p$. Let $\mathcal{P} \in \mathbb{Q}_p[x]$ be the monic polynomial of degree $m$ defined by $\mathcal{P}(x) = \prod_{i=1}^m (x - a_i')$. By our construction of $D$ in Lemma 105, the class $\alpha' := \mathcal{P}(\theta') \in (K_f^\times / K_f^{\times 2} \mathbb{Q}_p^\times)_{\mathrm{N} \equiv 1}$ is equal to $(x - \theta')(\alpha_0')$. Next, let $\mathcal{R} \in \mathbb{Q}_p[x]$ be the unique polynomial of minimal degree at most $m - 1$ such that $\mathcal{R}(a_i') = c_i'$ for each $i \in \{1, \ldots, m\}$. Then the polynomial $\mathcal{R}(x)^2 - f'(x, 1) \in \mathbb{Q}_p[x]$ has a root at $x = a_i'$ for each $i$, so there exists $\mathcal{H} \in \mathbb{Q}_p[x]$ such that $\mathcal{R}(x)^2 - f'(x, 1) = \mathcal{P}(x)\mathcal{H}(x)$. Since we chose $D$ so that $a_i' \in \mathcal{O}_{\overline{\mathbb{Q}}_p}$ for each $i$, we have that $\mathcal{P} \in \mathbb{Z}_p[x]$. We proceed under the assumption that we also have $\mathcal{R} \in p\mathbb{Z}_p[x]$; at the end of this section, we explain how to handle the case where $\mathcal{R} \notin p\mathbb{Z}_p[x]$. Then, since $\mathcal{P} \in \mathbb{Z}_p[x]$ is monic and $\mathcal{R}, f'(x, 1) \in p\mathbb{Z}_p[x]$, it follows from the relation $\mathcal{R}(x)^2 - f'(x, 1) = \mathcal{P}(x)\mathcal{H}(x)$ that $\mathcal{H} \in p\mathbb{Z}_p[x]$ as well.

Let $f''$ be as in the proof of Lemma 105, and consider the following $R_{f''}$-submodule of $K_{f''} = K_f$:

$$I'' := R_{f''} \langle p^{-1} \mathcal{R}(\theta'), \mathcal{P}(\theta') \rangle.$$

Note that $\theta' \in R_{f''}$ because $p^{-1} f_0' \in \mathbb{Z}_p^\times$, so since $\mathcal{P} \in \mathbb{Z}_p[x]$ and $\mathcal{R} \in p\mathbb{Z}_p[x]$, the fractional ideal $I''$ is in fact an integral ideal of $R_{f''}$. Letting $\mathrm{N}''$ denote the fractional ideal norm with respect to the basis (1.1) of $R_{f''}$, given explicitly by $\mathbb{Z}_p\langle 1, p^{-1}\zeta_1, \ldots, p^{-1}\zeta_{n-1} \rangle$, it follows

immediately from [15, proof of Proposition 8.5] that $p^m \,\mathrm{N}''(I'')^2$ and $\mathrm{N}''(\alpha')$ generate the same fractional ideal of $\mathbb{Z}_p$.

We now construct a list of elements that form part of a basis for $I''$ as a $\mathbb{Z}_p$-module:

**Lemma 106.** *Let $\ell := \frac{n-m-2}{2}$. Then the list $\mathcal{P}(\theta'), \theta'\mathcal{P}(\theta'), \ldots, \theta'^{\ell}\mathcal{P}(\theta') \in I''$ can be extended to a basis of $I''$ as a $\mathbb{Z}_p$-module.*

*Proof.* Because $I''$ is an integral ideal of $R_{f''}$, it suffices to prove that $s(\vec{x}) := \sum_{i=0}^{\ell} x_i \theta'^i \mathcal{P}(\theta')$ is primitive as an element of $R_{f''}$ (i.e., that we have $s(\vec{x}) = R_{f''} \smallsetminus pR_{f''}$) for every primitive tuple $\vec{x} = (x_0, \ldots, x_\ell) \in \mathbb{Z}_p^{\ell+1} \smallsetminus p\mathbb{Z}_p^{\ell+1}$. Given such a tuple $\vec{x}$, let $i \in \{0, \ldots, \ell\}$ be the largest index such that $x_i \in \mathbb{Z}_p^\times$. Then, when $s(\vec{x})$ is expressed in the power basis $\mathbb{Z}_p\langle 1, \theta', \ldots, \theta'^{n-1}\rangle$ of $R_{f''}$, the coefficient of $\theta'^{m+i}$ is a $p$-adic unit. Thus, $p^{-1}x \notin R_{f''}$. □

Consider the $R_{f''}$-submodule $pI'' \subset K_{f''}$. Then, by Lemma 106, we can find elements $\eta_1, \ldots, \eta_{n-\ell-1} \in pI''$ such that the following is a basis of $pI''$ as a $\mathbb{Z}_p$-module:

$$pI'' = \mathbb{Z}_p\big\langle \eta_1, \ldots, \eta_{n-\ell-1}, p\mathcal{P}(\theta'), \ldots, p\theta'^{\ell}\mathcal{P}(\theta')\big\rangle.$$

Let $I' \subset K_{f'}$ be the free rank-$n$ $\mathbb{Z}_p$-submodule with basis given by

$$I' = \mathbb{Z}_p\big\langle \eta_1, \ldots, \eta_{n-\ell-1}, \mathcal{P}(\theta'), \ldots, \theta'^{\ell}\mathcal{P}(\theta')\big\rangle.$$

**Lemma 107.** *The $\mathbb{Z}_p$-submodule $I' \subset K_{f'}$ is a fractional ideal of $R_{f'}$.*

*Proof.* It suffices to show that $I'$ is closed under multiplication by elements of $R_{f'}$. Since $pI''$ is closed under multiplication by elements of $R_{f''} \supset R_{f'}$, it suffices to verify that $\zeta_i' \theta'^j \mathcal{P}(\theta') \in I'$ for each $i \in \{1, \ldots, n-1\}$ and $j \in \{0, \ldots, \ell\}$, or equivalently that $(p\theta'^i)\mathcal{P}(\theta') \in I'$ for each $i \in \{1, \ldots, n+\ell-1\}$. But notice that $(p\theta'^i)\mathcal{P}(\theta') = \theta'^i(p\mathcal{P}(\theta')) \in pI'' \subset I'$, because $pI''$ is an $R_{f''}$-submodule of $K_{f''}$ and is hence closed under multiplication by powers of $\theta'$. □

We now prove that the pair $(I', \alpha') \in H_{f',1}$:

**Lemma 108.** *We have $I'^2 \subset \alpha' I_{f'}^{n-2}$, and for some choice of a basis of $I'$, we have*

$$\mathrm{N}'(I')^2 = \mathrm{N}'(\alpha') f_0'^{2-n}.$$

*Proof.* To prove the containment, it suffices to prove the following: that $\eta_i \eta_j \in \alpha' I_{f'}^{n-2}$ for each $i, j \in \{1, \ldots, n-\ell-1\}$, that $\eta_i \theta'^j \mathcal{P}(\theta') \in \alpha' I_{f'}^{n-2}$ for each $i \in \{1, \ldots, n-\ell-1\}$ and $j \in \{0, \ldots, \ell\}$, and that $\theta'^i \mathcal{P}(\theta')^2 \in \alpha' I_{f'}^{n-2}$ for each $i \in \{0, \ldots, 2\ell\}$. By construction, we have that $\eta_i \in pI''$ for each $i \in \{1, \ldots, n-\ell-1\}$. Thus, there exist $\beta_i, \gamma_i^{(0)}, \ldots, \gamma_i^{(\ell)} \in R_{f''}$ for each $i$ such that $\eta_i = \beta_i \mathcal{R}(\theta') + \sum_{k=0}^{\ell} \gamma_i^{(k)} (p\theta'^k \mathcal{P}(\theta'))$. Using the relation $\mathcal{R}(\theta')^2 = \mathcal{P}(\theta')\mathcal{H}(\theta')$, we find that

$$\alpha'^{-1}(\eta_i \eta_j) \equiv \beta_i \beta_j \mathcal{H}(\theta') \pmod{pR_{f''}}, \quad \text{and} \tag{4.9}$$

$$\alpha'^{-1}(\eta_i \theta'^j \mathcal{P}(\theta')) = \eta_i \theta'^j \equiv \beta_i \theta'^j \mathcal{R}(\theta') \pmod{pR_{f''}}. \tag{4.10}$$

Since $\mathcal{R}, \mathcal{H} \in p\mathbb{Z}_p[x]$, it follows from (4.9) and (4.10) that every term in the expression of $\alpha'^{-1}(\eta_i \eta_j)$ and of $\alpha'^{-1}(\eta_i \theta'^j \mathcal{P}(\theta'))$ in the power basis $\mathbb{Q}_p\langle 1, \theta', \ldots, \theta'^{n-1}\rangle$ has coefficient divisible by $p$. We deduce that $\eta_i \eta_j$ and $\eta_i \theta'^j \mathcal{P}(\theta')$ are contained in $\alpha' \mathcal{R}_{f'} \subset \alpha' I_{f'}^{n-2}$ for each possible $i, j$. Finally, notice that $\alpha'^{-1} \theta'^i \mathcal{P}(\theta')^2 = \theta'^i \mathcal{P}(\theta')$; since $\mathcal{P} \in \mathbb{Z}_p[x]$ has degree $m$, and since $\theta', \ldots, \theta'^{n-2} \in I_{f'}^{n-2}$, it follows that $\theta'^i \mathcal{P}(\theta')^2 \in \alpha' I_{f'}^{n-2}$ for each $i \in \{0, \ldots, 2\ell = n-m-2\}$.

Recall that $p^m \mathrm{N}''(I'')^2$ and $\mathrm{N}''(\alpha')$ generate the same fractional ideal of $\mathbb{Z}_p$. It follows that the same holds for $p^{m-2} \mathrm{N}'(pI'')^2$ and $\mathrm{N}'(\alpha')$, and hence also for $\mathrm{N}'(I')^2$ and $\mathrm{N}'(\alpha') f_0'^{2-n}$. Since both $\mathrm{N}'(I')^2$ and $\mathrm{N}'(\alpha') f_0'^{2-n}$ are elements of $\mathbb{Q}_p^{\times 2}$, we can choose a basis of $I'$ to ensure that $\mathrm{N}'(I')^2 = \mathrm{N}'(\alpha') f_0'^{2-n}$. □

Next, suppose that we have $\mathcal{R} \notin p\mathbb{Z}_p[x]$. Then we also have that $\mathcal{R}^2 \notin p\mathbb{Z}_p[x]$. Letting $j(x) = p^{-1}(\mathcal{R}(x)^2 - f'(x,1)) = p^{-1}\mathcal{P}(x)\mathcal{H}(x)$, it follows that the coefficient of $x^i$ in $j(x)$ is a $p$-adic unit if $i = n$ and a $p$-adic integer for every $i \in \{2m-1, \ldots, n-1\}$, and that the coefficient of $x^i$ in $j(x)$ has negative valuation for some $i \in \{0, \ldots, 2m-2\}$. Analyzing the Newton

polygon of $j$ then reveals that $j$ has at least $n-(2m-2)$ roots with negative valuation. Since $\mathcal{P}(x) \mid j(x)$ (as elements of $\mathbb{Q}_p[x]$), we also know that $j$ has $m$ roots with positive valuation at the $\mathscr{G}_{\mathbb{Q}_p}$-invariant list $a'_1, \ldots, a'_m \in \mathcal{O}_{\overline{\mathbb{Q}}_p}$. Thus, letting $D' \in \mathrm{Div}(C_{f'})(\overline{\mathbb{Q}}_p)$ be the divisor supported on the remaining roots of $j$ that have positive valuation, we find that $D' \in \mathrm{Div}(C_{f'})(\mathbb{Q}_p)$ and $\deg D' \leq m-2$.

Just like in Step 2 of the proof of Lemma 103, consider the function $g := y - \mathcal{R}(x)$ on $C_{f'}$. Note that $g$ is defined over $\mathbb{Q}_p$, that the zeros of $g$ are precisely the zeros of $j$, and that the poles of $g$ lie over infinity. Applying the argument in step 3 of the proof of Lemma 103 then implies that $D'$ satisfies the conditions of the lemma with $m$ replaced by $\deg D' \leq m-2$. The proof now concludes by downward induction on $m$; once $m = 1$, it is clear that $\mathcal{R} \in p\mathbb{Z}_p[x]$.

#### 4.2.2.3 Construction of integral representative for $p < n$

Now let $p < n$. As in §4.2.2.2, we reduce the problem to the case where $p^d = \gcd(f_0, \ldots, f_n) \in \{1, p\}$. However, we might *not necessarily* be able to replace $f$ with an $\mathrm{SL}_2(\mathbb{Z}_p)$-translate $f'$ such that $\nu_p(f'_0) = d$, where $\nu_p \colon \mathbb{Q}_p^\times \to \mathbb{Z}$ denotes the usual normalized $p$-adic valuation. Indeed, such a form $f'$ fails to exist precisely when $p < n$ and $f$ is divisible by $y\prod_{i=0}^{p-1}(x-iy)$ modulo $p$. Nonetheless, it follows from [5] that we can always find an $\mathrm{SL}_2(\mathbb{Z}_p)$-translate $f'$ of $f$ such that $\nu_p(f'_0) \leq d_1$ for some bounded integer $d_1 > 0$ depending only on the degree $n$.

Let $\widetilde{f}(x,y) = f'(x, p^{d_2}y)$, where $d_2 \geq d_1$ is an even integer, to be chosen shortly. Then $C_{f'} \simeq C_{\widetilde{f}}$, and this isomorphism induces an identification

$$J_{f'}(\mathbb{Q}_p)/2J_{f'}(\mathbb{Q}_p) \simeq J_{\widetilde{f}}(\mathbb{Q}_p)/2J_{\widetilde{f}}(\mathbb{Q}_p)$$

; letting $\widetilde{\alpha}_0$ be the image of $\alpha'_0$ under this identification, observe that

$$(x - \theta')(\alpha'_0) = (x - p^{d_2}\theta')(\widetilde{\alpha}_0).$$

Let $\widetilde{\alpha} \in K_{\widetilde{f}}^\times = K_{f'}^\times$ be a representative of $(x - p^{d_2}\theta')(\widetilde{\alpha}_0)$. Because $\widetilde{f}$ is a multiple of a

form with unit leading coefficient, the constructions described in §4.2.2.1–4.2.2.2 imply the existence of a pair $(\widetilde{I}, \widetilde{\alpha}) \in H_{\widetilde{f},1}$, with one caveat: when $p = 2$, the argument in case 1 of step 3 of the proof of Lemma 103 only goes through for $d_2 \gg 1$, where the implied constant depends only on $n$. Choosing $d_2$ so that this argument goes through, let $(\widetilde{A}, \widetilde{B}) \in W_n(\mathbb{Z}_p)$ be a representative of the $(\mathrm{SL}_n/\mu_2)(\mathbb{Z}_p)$-orbit corresponding to $(\widetilde{I}, \widetilde{\alpha})$ via Theorem 13.

Since the pair $(\widetilde{A}, \widetilde{B})$ has $\iota(\widetilde{A}, \widetilde{B}) = \widetilde{f}^{\mathsf{mon}}$, it follows that the pair $(\widetilde{A}, p^{-d_2}\widetilde{B}) \in W_n(\mathbb{Q}_p)$ has $\iota(\widetilde{A}, p^{-d_2}\widetilde{B}) = f'^{\mathsf{mon}}$. Imitating the proof of Lemma 22, we see that $(\widetilde{A}, p^{-d_2}\widetilde{B})$ corresponds via Theorem 13 to the pair $(\widetilde{I}, p^{(n-1)d_2}\widetilde{\alpha})$, where we view $\widetilde{I}$ as a basis for $K_{f'}$. By Lemma 14, the pair $(\widetilde{I}, p^{(n-1)d_2}\widetilde{\alpha})$ corresponds to a pair $(I, \alpha) \in H_{f,1}$. We then have the following lemma:

**Lemma 109.** *Let $(A, B) \in W_n(\mathbb{Q}_p)$ be the pair arising from $(I, \alpha)$ via Theorem 13. Then there exists an element $g \in \mathrm{SL}_n^{\pm}(\mathbb{Q}_p)$ satisfying the following two properties:* (1) *$gAg^T = \mathscr{A}_n$; and* (2) *When expressed in lowest terms, the denominators of the matrix entries of $g$ are bounded, depending only on $n$.*

*Proof.* We first claim that the matrix entries of $A$ have bounded denominators. Consider the map $\langle -, - \rangle^{\sim} \colon \widetilde{I} \times \widetilde{I} \to I_{\widetilde{f}}^2$ defined by $(\beta, \gamma) \mapsto (p^{(n-1)d_2}\widetilde{\alpha})^{-1}\beta\gamma$. It follows from the proof of Theorem 6 that, with respect to the chosen basis of $\widetilde{I}$ and the standard basis (1.3) of $I_{\widetilde{f}}^{n-2}$, the matrix entries of $\langle -, - \rangle^{\sim}$ are polynomial functions in the following quantities: the matrix entries of $A$ and $B$, the coefficients of $\widetilde{f}$, and ${f'_0}^{-1}$. Thus, the matrix entries of the map $\langle -, - \rangle^{\sim}$ have bounded denominators. From the proof of Lemma 14, we see that $I$ is a multiple of $\widetilde{I}$ and that $I_f^{n-2}$ is a multiple of $I_{\widetilde{f}}^{n-2}$; in this way, $I$ and $I_f^{n-2}$ inherit bases from $\widetilde{I}$ and $I_{\widetilde{f}}^{n-2}$. It is then clear that the matrix of the map $\langle -, - \rangle^{\sim}$ with respect to the chosen basis of $\widetilde{I}$ and the standard basis of $I_{\widetilde{f}}^{n-2}$ is equal to the matrix of the map $\langle -, - \rangle \colon I \times I \to I_f^{n-2}$ defined by $(\beta, \gamma) \mapsto \alpha^{-1}\beta\gamma$ with respect to the bases of $I$ and $I_f^{n-2}$ inherited from $\widetilde{I}$ and $I_{\widetilde{f}}^{n-2}$. Since the basis that $I_f^{n-2}$ inherits from $I_{\widetilde{f}}^{n-2}$ differs from the standard basis of $I_f^{n-2}$ by an element of $\mathrm{GL}_n(\mathbb{Z}_p)$, the matrix entries of the map $\langle -, - \rangle$ with respect to the basis of $I$ inherited from $\widetilde{I}$ and the standard basis of $I_f^{n-2}$, and hence the matrix entries of $A$ and $B$, have bounded denominators.

By Proposition 101, $A$ is split over $\mathbb{Q}_p$; by the $p$-adic Jordan decomposition, there exist finitely many $\mathrm{SL}_n^{\pm}(\mathbb{Z}_p)$-orbits of symmetric matrices in $\mathrm{Mat}_n(\mathbb{Q}_p)$ of determinant 1 whose matrix entries have bounded denominators. Combining these two observations with [85, Chapter I, Lemma 6.3], we see that there exists $g' \in \mathrm{SL}_n^{\pm}(\mathbb{Q}_p)$ such that its matrix entries have bounded denominators and such that $g'A{g'}^T = \left[\begin{array}{c|c} 0 & \mathrm{id} \\ \hline \mathrm{id} & 0 \end{array}\right] \in \mathrm{Mat}_n(\mathbb{Z}_p)$. Taking $g'' \in \mathrm{SL}_n^{\pm}(\mathbb{Q}_p)$ such that $g'' \left[\begin{array}{c|c} 0 & \mathrm{id} \\ \hline \mathrm{id} & 0 \end{array}\right] {g''}^T = \mathcal{A}$, we set $g = g''g'$. □

The matrix entries of $\widetilde{A}$ are integral, and the matrix entries of $p^{-d_2}\widetilde{B}$ have denominators bounded by $p^{d_2}$; thus, the matrix entries of $-\widetilde{A}^{-1}(p^{-d_2}\widetilde{B})$ have bounded denominators. For each $i \in \{0, \ldots, n-1\}$, let $m_i \colon K_f \to K_f$ denote the map of multiplication by $\zeta_i$. Then the proof of Theorem 6 implies that the matrix representing $m_i$ with respect to the basis of $\widetilde{I}$ has entries with bounded denominators for each $i$. Consequently, the matrix representing $m_i$ on $K_f$ with respect to the basis of $I$ inherited from $\widetilde{I}$ has entries with bounded denominators for each $i$. Letting $g \in \mathrm{SL}_n^{\pm}(\mathbb{Q}_p)$ be as in the statement of Lemma 109, it follows that the matrix representing $m_i$ with respect to the basis of $I$ obtained by applying $g$ to the basis inherited from $\widetilde{I}$ has entries with bounded denominators for each $i$. Since $B$ has bounded denominators, there exists a bounded even integer $\mathcal{D} \geq 0$ such that the pair $(gAg^T, g(p^{\mathcal{D}}B)g^T)$ is an element of $W_n(\mathbb{Z}_p)$ that lies in the image of $\mathsf{orb}_{f(x,p^{\mathcal{D}}y),1}$.

## 4.3 2-Selmer groups of elliptic curves, and orbits of small rank

In this section, we start by recalling the parametrization of 2-Selmer elements of elliptic curves by $\mathrm{PGL}_2(\mathbb{Q})$-orbits of integral binary quartic forms. Then, we strengthen the results of §1.4.2 on ranks of orbits arising from binary $n$-ic forms in the case where $n = 4$.

### 4.3.1 Representation of $\mathrm{PGL}_2$ on binary quartic forms

In this section, we define a certain representation of the group $\mathrm{PGL}_2$ on the space of binary quartic forms. As we explain in §4.3.1, this representation plays a key role in the parametrization of 2-Selmer elements of elliptic curves; see [26, § 1.2] for a thorough treatment.

Observe that $V_4$ has a natural structure of $\mathrm{PGL}_2$-representation, given as follows: for each element $\gamma \in \mathrm{PGL}_2(R)$, choose a lift $\widetilde{\gamma} \in \mathrm{GL}_2(R)$, and let

$$(\gamma \cdot f)(x, y) = (\det \widetilde{\gamma})^{-2} f((x, y)\widetilde{\gamma}) \in V_4(R) \tag{4.11}$$

for any binary quartic form $f \in V_4(R)$.

Let $a, b, c, d, e \colon V_4 \to \mathbb{A}^1_{\mathbb{Z}}$ be the functions defined by sending a binary quartic form to its $x^4$-, $x^3y$-, $x^2y^2$-, $xy^3$-, and $y^4$-coefficients, respectively. Consider the homogeneous polynomial functions $I, J \colon V_4 \to \mathbb{A}^1_{\mathbb{Z}}$ of respective degrees 2 and 3 defined in terms of the coefficient functions $a, b, c, d, e$ by the following formulas:

$$I = 12ae - 3bd + c^2 \quad \text{and} \quad J = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3.$$

Let Inv denote the affine plane $\mathbb{A}^2_{\mathbb{Z}}$, and let $\iota \colon V_4 \to \mathrm{Inv}$ be the function defined by $\iota = (I, J)$. One readily verifies that $\iota$ is $\mathrm{PGL}_2$-invariant; in fact, the functions $I$ and $J$ freely generate the ring of polynomial invariants for the action of $\mathrm{PGL}_2$ on $V_4$. In particular, the discriminant function $\Delta \colon V_4 \to \mathbb{A}^1_{\mathbb{Z}}$ is expressible as a polynomial in $I$ and $J$, and it is given explicitly by the formula

$$\Delta = (4I^3 - J^2)/27.$$

One key ingredient in the computation of the average size of the 2-Selmer groups of elliptic curves in [26] is the following parametrization of 2-Selmer elements of elliptic curves in terms of $\mathrm{PGL}_2(\mathbb{Q})$-orbits on $V_4(\mathbb{Z})$:

**Theorem 110** ([26, Theorem 3.5])**.** *Let $E = E^{I,J}$ be an elliptic curve over $\mathbb{Q}$. Then the*

*elements of* $\mathrm{Sel}_2(E^{I,J})$ *are in bijection with the set of* $\mathrm{PGL}_2(\mathbb{Q})$*-equivalence classes of locally soluble integral binary quartic forms with invariants* $2^4 I$ *and* $2^6 J$*.*

We note that the correspondence in Theorem 110 was originally introduced by Birch and Swinnerton-Dyer (see [33]) and was further developed by Cremona (see [50], as well as [19, 51, 114]).

### 4.3.2 Construction of special integral representatives

Let $R = \mathbb{Z}$ or $\mathbb{Z}_p$ for a prime $p$, and fix $a \in R \smallsetminus \{0\}$. The goal of this section is to show that the $(\mathrm{SL}_4/\mu_2)(K)$-orbit of any pair $(A, B) \in W_4(R)$ arising via the parametrization developed in §1 from a form in $V_{4,a}(R)$ admits an integral representative pair $(A', B') \in W_4(R)$ such that $B'$ is special at $a$. It suffices to prove this when $R = \mathbb{Z}_p$, which we do as follows:

**Theorem 111.** *Let* $f(x, y) = ax^4+bx^3y+cx^2y^2+dxy^3+ey^4 \in V_4(\mathbb{Z}_p)$*, and suppose that a pair* $(A, B) \in W_4(\mathbb{Z}_p)$ *lies in the image of* $\mathsf{orb}_{f,1}$*. Then there exists another pair* $(A', B') \in W_4(\mathbb{Z}_p)$ *belonging to the same* $(\mathrm{SL}_4/\mu_2)(\mathbb{Q}_p)$*-orbit as* $(A, B)$ *such that* $B'$ *is special at* $a$*.*[1]

*Proof.* We start by deciphering what it means for $(A, B)$ to lie in the image of $\mathsf{orb}_{f,1}$. Condition (a) in Theorem 13 tells us that $\iota(A, B) = f^{\mathsf{mon}}$, and so $a^3 \mid e(f^{\mathsf{mon}}) = \det B$. Condition (b) in Theorem 13 comprises the following three conditions, one for each value of $i \in \{1, 2, 3\}$:

(1): $i = 1$. We have $p_1(\frac{1}{a} \times -A^{-1}B) = -A^{-1}B \in \mathrm{Mat}_4(\mathbb{Z}_p)$; this is trivially true because $\det A = 1$.

(2): $i = 2$. We have $p_2(\frac{1}{a} \times -A^{-1}B) = \frac{1}{a}\big((A^{-1}B)^2 + b(-A^{-1}B)\big) \in \mathrm{Mat}_4(\mathbb{Z}_p)$. This is equivalent to stipulating that certain linear combinations of the $2 \times 2$ minors of $-A^{-1}B$ are divisible by $a$, and just as in (1.22), it can be rewritten in the following convenient form:

$$BA^{-1}B - bB \equiv 0 \pmod{a}. \tag{4.12}$$

[1]Note that if $f$ is primitive, then Theorem 111 follows immediately from Theorem 18.

(3): $i = 3$. We have $p_3(\frac{1}{a} \times -A^{-1}B) = \frac{1}{a^2}\big((A^{-1}B)^3 + b(A^{-1}B)^2 + ac(A^{-1}B)\big) \in \mathrm{Mat}_4(\mathbb{Z}_p)$. This is equivalent to stipulating that each non-principal $3 \times 3$ minor of $-A^{-1}B$ is divisible by $a^2$ and that the sum of each triple of principal $3 \times 3$ minors of $-A^{-1}B$ is divisible by $a^2$. But the $xy^3$-coefficient of $f^{\mathsf{mon}}$ is divisible by $a^2$ and is, up to sign, the sum of the principal $3 \times 3$ minors of $-A^{-1}B$. It follows that

$$\wedge^3 B \equiv 0 \pmod{a^2}. \tag{4.13}$$

Note that each of the above conditions is preserved under the action of $\mathrm{SL}_4^{\pm}(\mathbb{Z}_p)$, and so they continue to hold if we replace $(A, B)$ with any $\mathrm{SL}_4^{\pm}(\mathbb{Z}_p)$-translate thereof.

We now apply the $p$-adic Jordan decomposition to put $B$ into one of five possible shapes that are convenient to work with. By replacing the pair $(A, B)$ with a suitable $\mathrm{SL}_4^{\pm}(\mathbb{Z}_p)$-translate, we may assume that $B$ takes the following shape if $p$ is odd:

$$B = \begin{bmatrix} u_1 p^{\mathfrak{b}_1} & 0 & 0 & 0 \\ 0 & u_2 p^{\mathfrak{b}_2} & 0 & 0 \\ 0 & 0 & u_3 p^{\mathfrak{b}_3} & 0 \\ 0 & 0 & 0 & u_4 p^{\mathfrak{b}_4} \end{bmatrix} \tag{4.14}$$

where the $\mathfrak{b}_i \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ are such that $\mathfrak{b}_1 \geq \mathfrak{b}_2 \geq \mathfrak{b}_3 \geq \mathfrak{b}_4 \geq 0$ and $u_i \in \mathbb{Z}_p^{\times}$ for each $i \in \{1, \ldots, 4\}$. If $p = 2$, then $B$ can take any one of the following four shapes in addition to the shape (4.14):

$$B = \left[\begin{array}{c|cc} 2^{\mathfrak{b}_1}\overline{B}_1 & \multicolumn{2}{c}{0} \\ \hline & u_3 2^{\mathfrak{b}_3} & 0 \\ 0 & 0 & u_4 2^{\mathfrak{b}_4} \end{array}\right], \quad \left[\begin{array}{cc|c} u_1 2^{\mathfrak{b}_1} & 0 & \\ 0 & u_2 2^{\mathfrak{b}_2} & 0 \\ \hline \multicolumn{2}{c|}{0} & 2^{\mathfrak{b}_3}\overline{B}_3 \end{array}\right], \tag{4.15}$$

$$\left[\begin{array}{c|c} 2^{\mathfrak{b}_1}\overline{B}_1 & 0 \\ \hline 0 & 2^{\mathfrak{b}_3}\overline{B}_3 \end{array}\right], \quad \left[\begin{array}{c|c|c} u_1 2^{\mathfrak{b}_1} & 0 & 0 \\ \hline 0 & 2^{\mathfrak{b}_3}\overline{B}_3 & 0 \\ \hline 0 & 0 & u_4 2^{\mathfrak{b}_4} \end{array}\right]$$

where the $\mathfrak{b}_i \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ are valuations such that $\mathfrak{b}_1 \geq \mathfrak{b}_2 \geq \mathfrak{b}_3 \geq \mathfrak{b}_4 \geq 0$ and $u_i \in \mathbb{Z}_p^\times$ for each $i \in \{1, \ldots, 4\}$ and where $\overline{B}_i \in \mathrm{Mat}_2(\mathbb{Z}_2)$ is symmetric and has even diagonal entries and odd anti-diagonal entries for each $i \in \{1, 3\}$. We label the five cases in (4.14) and (4.15) in the above order as 1, 2, 3, 4, and 5.

We are now in position to prove the theorem. If $B$ is special at $a$, then we are done, so suppose that $B$ is *not* special at $a$. Then $\mathfrak{a} := \nu_p(a) > 0$, for the condition of being special at $a$ is trivial when $p \nmid a$. Moreover, condition (3) above implies that for some integer $\mathfrak{c} \in \{1, \ldots, \mathfrak{a}\}$, we have $\mathfrak{b}_3 + \mathfrak{b}_4 = \mathfrak{a} - \mathfrak{c}$ in cases 1 and 2; that $2\mathfrak{b}_3 = \mathfrak{a} - \mathfrak{c}$ in cases 3 and 4; and that $\mathfrak{b}_i \geq \mathfrak{a} + \mathfrak{c}$ for each $i \in \{1, 2\}$ in cases 1, 2, 3, and 4. In case 5, it is not possible for $B$ to fail to be special at $a$, because condition (3) implies that $2\mathfrak{b}_3 + \mathfrak{b}_4 \geq 2\mathfrak{a}$, from which it follows that $\mathfrak{b}_3 + \mathfrak{b}_4 \geq \mathfrak{a}$. We may thus disregard case 5 in the remainder of the proof.

Write $A = [a_{ij}]$, $A^{-1} = [\breve{a}_{ij}]$ and $B = [b_{ij}]$, where $i, j \in \{1, 2, 3, 4\}$. Then one readily verifies using (4.14) that we have the following identities:

$$BA^{-1}B - bB \equiv u_3 u_4 p^{\mathfrak{b}_3 + \mathfrak{b}_4} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -\breve{a}_{44} & \breve{a}_{34} \\ 0 & 0 & \breve{a}_{34} & -\breve{a}_{33} \end{bmatrix} \pmod{a} \tag{4.16}$$

in cases 1 and 2, and

$$BA^{-1}B - bB \equiv (\det \overline{B}_3)2^{2\mathfrak{b}_3} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -\breve{a}_{44} & \breve{a}_{34} \\ 0 & 0 & \breve{a}_{34} & -\breve{a}_{33} \end{bmatrix} \pmod{a} \tag{4.17}$$

in cases 3 and 4. Combining (4.16) and (4.17) with condition (2) above, reexpressed as in (4.12), yields that $p^{\mathfrak{c}} \mid \breve{a}_{ij}$ for each $i, j \in \{3, 4\}$. Using the fact that $\det A = 1$, a calculation reveals that

$$\breve{a}_{33}\breve{a}_{44} - \breve{a}_{34}^2 = a_{11}a_{22} - a_{12}^2.^2 \tag{4.18}$$

Combining (4.18) with the fact that $p^{\mathfrak{c}} \mid \breve{a}_{ij}$ for each $i, j \in \{3, 4\}$ yields that $p^{2\mathfrak{c}} \mid (a_{11}a_{22} - a_{12}^2)$.

We now claim that $p^{\mathfrak{c}} \mid a_{ij}$ for each $i, j \in \{1, 2\}$. First suppose that the symmetric bilinear form $\left[\begin{smallmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{smallmatrix}\right]$ is $p$-adically diagonalizable (i.e., its $p$-adic Jordan decomposition consists of two $1 \times 1$ blocks); note that this holds whenever $p$ is odd, but only sometimes when $p = 2$. Then, by replacing the pair $(A, B)$ with a suitable translate under the action of the subgroup $\mathrm{SL}_2(\mathbb{Z}_p) \subset \mathrm{SL}_4^{\pm}(\mathbb{Z}_p)$ that acts by change-of-basis on the first two rows and columns of $A$ and $B$, we may assume that $a_{11} = \upsilon_1 p^{\mathfrak{a}_1}$, $a_{12} = 0$, and $a_{22} = \upsilon_2 p^{\mathfrak{a}_2}$, where the $\mathfrak{a}_i$ are integers such that $\mathfrak{a}_1 \geq \mathfrak{a}_2 \geq 0$ and $\mathfrak{a}_1 + \mathfrak{a}_2 \geq 2\mathfrak{c}$, and where $\upsilon_i \in \mathbb{Z}_p^{\times}$ for each $i \in \{1, 2\}$. Note that this transformation alters the first two rows and columns of $B$, but it preserves the property that $p^{\mathfrak{a}+\mathfrak{c}} \mid b_{ij}$ for each $i \in \{1, 2\}$. A calculation then reveals that we have

$$\breve{a}_{33} = -(\upsilon_2 p^{\mathfrak{a}_2})a_{14}^2 - (\upsilon_1 p^{\mathfrak{a}_1})a_{24}^2 + (\upsilon_1\upsilon_2 p^{\mathfrak{a}_1+\mathfrak{a}_2})a_{44} \equiv -(\upsilon_2 p^{\mathfrak{a}_2})a_{14}^2 \pmod{p^{\mathfrak{c}}}, \tag{4.19}$$

$$\breve{a}_{44} = -(\upsilon_2 p^{\mathfrak{a}_2})a_{13}^2 - (\upsilon_1 p^{\mathfrak{a}_1})a_{23}^2 + (\upsilon_1\upsilon_2 p^{\mathfrak{a}_1+\mathfrak{a}_2})a_{33} \equiv -(\upsilon_2 p^{\mathfrak{a}_2})a_{13}^2 \pmod{p^{\mathfrak{c}}}, \tag{4.20}$$

where we have used the fact that $\mathfrak{a}_1 \geq \mathfrak{c}$ because $\mathfrak{a}_1 \geq \mathfrak{a}_2$ and $\mathfrak{a}_1 + \mathfrak{a}_2 \geq 2\mathfrak{c}$. Since $p^{\mathfrak{c}} \mid \breve{a}_{ii}$ for

[2] In fact, this identity holds for any symmetric $4 \times 4$ matrix of determinant 1 over any ring.

each $i \in \{3,4\}$, it follows from (4.19) and (4.20) that either $\mathfrak{a}_2 < \mathfrak{c}$ and $p \mid a_{1i}$ for each $i \in \{3,4\}$ or $\mathfrak{a}_2 \geq \mathfrak{a}$. But the first case is impossible, for it would imply that $\det A \equiv 0 \pmod{p}$, contradicting the fact that $\det A = 1$. Thus, $\mathfrak{a}_2 \geq \mathfrak{c}$, and the claim holds in this case. If $p = 2$ and the symmetric bilinear form $\left[\begin{smallmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{smallmatrix}\right]$ is not 2-adically diagonalizable, then it is a multiple of a symmetric matrix over $\mathbb{Z}_2$ having odd determinant, and the claim then follows from the fact that $2^{2\mathfrak{c}} \mid (a_{11}a_{22} - a_{12}^2)$.

We have now shown that, by replacing the pair $(A, B)$ with a suitable translate under the action of $\mathrm{SL}_4^{\pm}(\mathbb{Z}_p)$, we may assume that $A$ and $B$ take the following shape:

$$A = \left[\begin{array}{c|c} p^{\mathfrak{c}}\overline{A} & * \\ \hline * & * \end{array}\right] \text{ and } B = \left[\begin{array}{c|cc} p^{\mathfrak{a}+\mathfrak{c}}\overline{B} & 0 & \\ \hline & u_3 p^{\mathfrak{b}_3} & 0 \\ 0 & & \\ & 0 & u_4 p^{\mathfrak{b}_4} \end{array}\right] \text{ or } \left[\begin{array}{c|c} 2^{\mathfrak{a}+\mathfrak{c}}\overline{B} & 0 \\ \hline 0 & 2^{\mathfrak{b}_3}\overline{B}_3 \end{array}\right] \tag{4.21}$$

where $\overline{A}, \overline{B} \in U_2(\mathbb{Z}_p)$ and where "$*$" denotes an element of $\mathrm{Mat}_2(\mathbb{Z}_p)$ whose value is irrelevant.

Consider the diagonal matrix $\varepsilon_{p^{-\mathfrak{c}}} \in \mathrm{SL}_4(\overline{\mathbb{Q}}_p)$ with diagonal entries given by $\sqrt{p^{-\mathfrak{c}}}$, $\sqrt{p^{-\mathfrak{c}}}$, $1/\sqrt{p^{-\mathfrak{c}}}$, and $1/\sqrt{p^{-\mathfrak{c}}}$. By Lemma 5, the class of $\varepsilon_{p^{-\mathfrak{c}}}$ is an element of $(\mathrm{SL}_4/\mu_2)(\mathbb{Q}_p)$. We then define $(A', B') := \varepsilon_{p^{-\mathfrak{c}}} \cdot (A, B) \in W_4(\mathbb{Q}_p)$. Because $A$ and $B$ take the shapes given in (4.21), it follows that the pair $(A', B')$ is in fact an element of $W_4(\mathbb{Z}_p)$ and moreover that $B'$ is given by

$$B' = \left[\begin{array}{c|cc} p^{\mathfrak{a}}\overline{B} & 0 & \\ \hline & u_3 p^{\mathfrak{b}_3+\mathfrak{c}} & 0 \\ 0 & & \\ & 0 & u_4 p^{\mathfrak{b}_4+\mathfrak{c}} \end{array}\right] \quad \text{or} \quad \left[\begin{array}{c|c} 2^{\mathfrak{a}}\overline{B} & 0 \\ \hline 0 & 2^{\mathfrak{b}_3+\mathfrak{c}}\overline{B}_3 \end{array}\right] \tag{4.22}$$

Since $\mathfrak{b}_3 + \mathfrak{b}_4 = \mathfrak{a} - \mathfrak{c}$ in cases 1 and 2 and that $2\mathfrak{b}_3 = \mathfrak{a} - \mathfrak{c}$ in cases 3 and 4, it follows from (4.22) that the pair $(A', B')$ lies in the image of $\mathsf{orb}_{f,1}$, and that $B'$ is special at $a$. $\square$

### 4.3.3 Ranks of special elements

Let $m \geq 1$ be an integer, and write

$$\mathcal{L}_m := \{B \in U_4(R) : B \text{ is of rank} \leq 1 \text{ modulo } m\}.$$

Next, we say that $B \in U_4(R)$ is of *rank* $\leq 2$ *modulo* $m$ if for every prime $p \mid m$, when the $p$-adic Jordan decomposition of $B$ is expressed as in (4.14) and (4.15), we have $\mathfrak{b}_2 \geq \nu_p(m)$ in cases 1 and 3, $\mathfrak{b}_1 \geq \nu_p(m)$ in cases 2 and 4, and $\mathfrak{b}_3 \geq \nu_p(m)$ in case 5. Let $m' \geq 1$ be an integer. Then we write

$$\mathcal{L}_{m,m'} := \{B \in \mathcal{L}_m : B \text{ is of rank} \leq 2 \text{ modulo } mm'\}.$$

We have the following useful characterization of those matrices $B \in U_4(R)$ that are special at $a$ in terms of the sets $\mathcal{L}_m$ and $\mathcal{L}_{m,m'}$:

**Proposition 112.** *Let $B \in U_4(R)$, and suppose that $B$ is special at $a$. Then there exist integers $a_1, a_2, a_3 \geq 1$ such that the following properties hold:*

- *For each prime $p \mid a$, there exist integers $\mathfrak{e}_1 = \mathfrak{e}_1(p), \mathfrak{e}_2 = \mathfrak{e}_2(p) \geq 0$ such that*

$$\nu_p(a_1) = \mathfrak{e}_1, \quad \nu_p(a_2) = \nu_p(a) - 2\mathfrak{e}_1 + \mathfrak{e}_2, \quad \textit{and} \quad \nu_p(a_3) = \mathfrak{e}_1 - 2\mathfrak{e}_2; \quad \textit{and} \tag{4.23}$$

- *We have that $B \in a_1\mathcal{L}_{a_2,a_3}$.*

*Proof.* Fix a prime $p$. By the Chinese remainder theorem, it suffices to prove the proposition for $R = \mathbb{Z}_p$. We retain notation from the proof of Theorem 111, and we assume without loss of generality that $B$ is in one of the five cases listed in (4.14) and (4.15). In case 1, the exponents $\mathfrak{a}$, $\mathfrak{b}_2$, $\mathfrak{b}_3$, and $\mathfrak{b}_4$ satisfy the following properties:

$$\mathfrak{b}_2 \geq \mathfrak{b}_3 \geq \mathfrak{b}_4 \geq 0, \quad \mathfrak{b}_3 + \mathfrak{b}_4 \geq \mathfrak{a} \geq 0, \quad \text{and} \quad \mathfrak{b}_2 + \mathfrak{b}_3 + \mathfrak{b}_4 \geq 2\mathfrak{a}. \tag{4.24}$$

We first claim that there exists an integer $\mathfrak{e}_1$ such that

$$\max\{0, \mathfrak{a} - \mathfrak{b}_3, 2\mathfrak{a} - \mathfrak{b}_2 - \mathfrak{b}_3\} \leq \mathfrak{e}_1 \leq \min\{\mathfrak{b}_4, \tfrac{2\mathfrak{a}}{3}\}. \tag{4.25}$$

It suffices to check that each of the lower bounds on $\mathfrak{e}_1$ in (4.25) is less than or equal to each of the upper bounds. The three inequalities $0 \leq \mathfrak{b}_4$, $\mathfrak{a} - \mathfrak{b}_3 \leq \mathfrak{b}_4$, and $2\mathfrak{a} - \mathfrak{b}_2 - \mathfrak{b}_3 \leq \mathfrak{b}_4$ respectively follow from the three properties in (4.24). The inequality $0 \leq \frac{2\mathfrak{a}}{3}$ follows from the second property in (4.24). The inequality $\mathfrak{a} - \mathfrak{b}_3 \leq \frac{2\mathfrak{a}}{3}$ is equivalent to $\mathfrak{b}_3 \geq \frac{\mathfrak{a}}{3}$, but this holds since the first two properties in (4.24) imply that $\mathfrak{b}_3 \geq \frac{\mathfrak{a}}{2}$. The inequality $2\mathfrak{a} - \mathfrak{b}_2 - \mathfrak{b}_3 \leq \frac{2\mathfrak{a}}{3}$ is only relevant when $\mathfrak{b}_4 \geq \frac{2\mathfrak{a}}{3}$, and it is equivalent to $\mathfrak{b}_2 + \mathfrak{b}_3 \geq \frac{4\mathfrak{a}}{3}$, but this follows from the first property in (4.24).

We next claim that there exists an integer $\mathfrak{e}_2$ such that

$$\max\{0, \mathfrak{a} - \mathfrak{b}_2, 2\mathfrak{e}_1 - \mathfrak{a}\} \leq \mathfrak{e}_2 \leq \min\{\mathfrak{e}_1 - \mathfrak{a} + \mathfrak{b}_3, \tfrac{\mathfrak{e}_1}{2}\}. \tag{4.26}$$

Again, we check that each of the lower bounds on $\mathfrak{e}_2$ in (4.26) is less than or equal to each of the upper bounds. The inequalities $0 \leq \mathfrak{e}_1 - \mathfrak{a} + \mathfrak{b}_3$, $0 \leq \frac{\mathfrak{e}_1}{2}$, and $\mathfrak{a} - \mathfrak{b}_2 \leq \mathfrak{e}_1 - \mathfrak{a} + \mathfrak{b}_3$ follow from (4.25). The inequality $\mathfrak{a} - \mathfrak{b}_2 \leq \frac{\mathfrak{e}_1}{2}$ follows from the first property in (4.24) combined with (4.25). The inequality $2\mathfrak{e}_1 - \mathfrak{a} \leq \mathfrak{e}_1 - \mathfrak{a} + \mathfrak{b}_3$ is equivalent to $\mathfrak{e}_1 \leq \mathfrak{b}_3$, which follows from the first property in (4.24) combined with (4.25). The inequality $2\mathfrak{e}_1 - \mathfrak{a} \leq \frac{\mathfrak{e}_1}{2}$ is equivalent to $\mathfrak{e}_1 \leq \frac{2\mathfrak{a}}{3}$, which follows from (4.25).

Having chosen $\mathfrak{e}_1$ and $\mathfrak{e}_2$ to satisfy the conditions (4.25) and (4.26), respectively, we then take $a_1 = p^{\mathfrak{e}_1}$, $a_2 = p^{\mathfrak{a}-2\mathfrak{e}_1+\mathfrak{e}_2}$, and $a_3 = p^{\mathfrak{e}_1-2\mathfrak{e}_2}$. Since $\mathfrak{e}_1 \leq \mathfrak{b}_4$, the matrix $a_1^{-1}B$ lies in $U_4(\mathbb{Z}_p)$. Since $\mathfrak{a} - \mathfrak{e}_1 + \mathfrak{e}_2 \leq \mathfrak{b}_3$, the matrix $a_1^{-1}B$ is of rank $\leq 1$ modulo $a_2$. Finally, since $\mathfrak{a} - \mathfrak{e}_2 \leq \mathfrak{b}_2$, the matrix $a_1^{-1}B$ is of rank $\leq 2$ modulo $a_2a_3$.

A similar proof works for the other four cases. The argument in case 2 is the same as in case 1, with $\mathfrak{b}_2$ replaced by $\mathfrak{b}_1$. The argument in case 3 is the same as in case 1, with $\mathfrak{b}_3 = \mathfrak{b}_4$. The argument in case 4 is the same as in case 2, with $\mathfrak{b}_3 = \mathfrak{b}_4$. The argument in

case 5 is the same as in case 1, with $\mathfrak{b}_2 = \mathfrak{b}_3$. □

## 4.4 Preliminary results about functions on coregular spaces

Let $U$ be a vector space with an action by a semisimple group $G$. We make the following assumptions on $U$ and $G$:

- The ring of polynomial invariants for the action of $G(\mathbb{C})$ on $U(\mathbb{C})$ is freely generated by $n$ integer polynomials $I_1, \ldots, I_n$.
- There exists a $G$-invariant *discriminant* polynomial function $\Delta = \Delta_U$ on $U$ such that every orbit on which $\Delta$ does not vanish is semistable in the sense of GIT.
- Every semistable orbit is stable, i.e., has finite stabilizer.

Let $\mathbb{I}$ denote affine $n$-space. We then have the *invariant map* $\iota$ given by

$$\begin{aligned} \iota\colon U &\to \mathbb{I} \\ u &\mapsto \big(I_1(u), \ldots, I_n(u)\big), \end{aligned}$$

which satisfies $\iota(u) = \iota(g \cdot u)$ for all $u \in U$ and $g \in G$. Let $\mathcal{I} \subset \mathbb{I}(\mathbb{R})$ be an open set, not containing any elements where the discriminant vanishes. Let $\kappa\colon \mathcal{I} \to U(\mathbb{R})$ be a smooth *section*, i.e., we have $\iota(\kappa(I)) = I$ for every $I \in \mathcal{I}$. Assume that the size of the stabilizer in $G(\mathbb{R})$ of every element in the image of $\kappa$ is the same, say $\sigma$. Let $\phi\colon \mathbb{I}(\mathbb{R}) \to \mathbb{R}$ and $\Theta\colon G(\mathbb{R}) \to \mathbb{R}$ be smooth compactly supported functions. We define the function $\psi = \mathcal{S}(\phi, \Theta) = \mathcal{S}_\kappa(\phi, \Theta)\colon U(\mathbb{R}) \to \mathbb{R}$ as follows:

$$\mathcal{S}(\phi, \Theta)(u) := \sum_{\substack{(\gamma, I) \in G(\mathbb{R}) \times \mathcal{I} \\ \gamma \cdot \kappa(I) = u}} \Theta(\gamma)\phi(I). \tag{4.27}$$

Note that the above sum has length $\sigma$ for every $u$ in the image of $G(\mathbb{R}) \times \mathcal{I}$, and that $\mathcal{S}(\phi, \Theta)$ is also smooth and compactly supported.

The group $G(\mathbb{R})$ acts on the set of smooth functions on $U(\mathbb{R})$ via $(\gamma \cdot \psi)(u) := \psi(\gamma^{-1} \cdot u)$. We then have the following result, which constitutes a smoothed version of the averaging method (see [7, 26]):

**Theorem 113.** *Let notation be as above. Let $L \subset G(\mathbb{R}) \cdot \kappa(\mathcal{I})$ be any discrete $G(\mathbb{Z})$-invariant set, and let $T \colon L \to \mathbb{R}$ be a $G(\mathbb{Z})$-invariant function. Let $\mathcal{F}_G$ be a fundamental domain for the action of $G(\mathbb{Z})$ on $G(\mathbb{R})$, and let $d\gamma$ be a Haar-measure on $G(\mathbb{R})$. Let $\phi$ and $\Theta$ be smooth, compactly supported functions, and let $\psi = \mathcal{S}(\phi, \Theta)$. Then we have that*

$$\sum_{u \in \frac{L}{G(\mathbb{Z})}} \frac{T(u)}{|\mathrm{Stab}_{G(\mathbb{Z})}(u)|} \phi(\iota(u)) = \frac{1}{\sigma \mathrm{Vol}(\Theta)} \int_{\gamma \in \mathcal{F}_G} \Big( \sum_{u \in L} (\gamma \cdot \psi)(u) T(u) \Big) d\gamma,$$

*where* $\mathrm{Vol}(\Theta)$ *denotes* $\int_{\gamma \in G(\mathbb{R})} \Theta(\gamma) d\gamma$.

*Proof.* As usual, we regard $\mathcal{F}_G \cdot \kappa(\mathcal{I})$ as a multiset, in which an element $x \in U(\mathbb{R})$ is represented $\#\{(g, u) : g \in \mathcal{F}_G, u \in \kappa(\mathcal{I}), g \cdot u = x\}$ times. As in [26, (8)], the $G(\mathbb{Z})$-orbit of an element $x \in G(\mathbb{R}) \cdot \kappa(\mathcal{I})$ is represented

$$m(x) = \frac{\#\mathrm{Stab}_{G(\mathbb{R})}(x)}{\#\mathrm{Stab}_{G(\mathbb{Z})}(x)}$$

times in the multiset $\mathcal{F}_G \cdot \kappa(\mathcal{I})$. Therefore, we have

$$\sum_{x \in \frac{L}{G(\mathbb{Z})}} \frac{T(u)}{|\mathrm{Stab}_{G(\mathbb{Z})}(u)|} \phi(\iota(u)) = \frac{1}{\sigma} \sum_{\substack{x \in \mathcal{F}_G \cdot \kappa(\mathcal{I}) \\ x \in L}} T(x) \phi(\iota(x)). \tag{4.28}$$

Since for all $h \in G(\mathbb{R})$, the set $\mathcal{F}_G \cdot h$ is also a fundamental domain for the left action of

$G(\mathbb{Z})$ on $G(\mathbb{R})$, we have

$$\sum_{\substack{x\in\mathcal{F}_G\cdot\kappa(\mathcal{I})\\ x\in L}} T(x)\phi(\iota(x)) = \frac{1}{\mathrm{Vol}(\Theta)}\int_{g\in G(\mathbb{R})}\Big(\sum_{\substack{x\in g\mathcal{F}_G\cdot\kappa(\mathcal{I})\\ x\in L}} T(x)\phi(\iota(x))\Big)\Theta(g)dg. \tag{4.29}$$

For $x \in g\mathcal{F}_G \cdot \kappa(\mathcal{I})$, there exists a unique $x_I \in \kappa(\mathcal{I})$ such that $x$ and $x_I$ are in the same $G(\mathbb{R})$-orbit. Moreover, there exist a finite number of elements $g_1, \ldots, g_\sigma \in G(\mathbb{R})$ such that $g_j \cdot x_I = x$. For $x \in L$ with $\iota(x) = I$, we write the contribution from $x$ to the right hand side of (4.29) as

$$\begin{aligned}
\int_{g\in G(\mathbb{R})}\Big(\sum_{\substack{h\in\mathcal{F}_G\\ ghx_I=x}} T(x)\phi(I)\Big)\Theta(g)dg &= T(x)\phi(I)\sum_{j=1}^{\sigma}\int_{g\in G(\mathbb{R})}\#\{h\in\mathcal{F}_G : hg = g_j\}\Theta(g)dg\\
&= T(x)\phi(I)\sum_{j=1}^{\sigma}\int_{g\in(\mathcal{F}_G)^{-1}g_j}\Theta(g)dg\\
&= T(x)\int_{h\in\mathcal{F}_G}\Big(\sum_{j=1}^{\sigma}\Theta(h^{-1}g_j)\phi(I)\Big)dh\\
&= \int_{h\in\mathcal{F}_G}(h\cdot\psi)(x)T(x)dh.
\end{aligned}$$

Adding up over $x \in L$ in the right hand side of (4.29), we obtain

$$\sum_{\substack{x\in\mathcal{F}_G\cdot\kappa(\mathcal{I})\\ x\in L}} T(x)\phi(\iota(x)) = \frac{1}{\mathrm{Vol}(\Theta)}\int_{h\in\mathcal{F}_G}\Big(\sum_{x\in L}(h\cdot\psi)(x)T(x)\Big)dh.$$

Together with (4.28), we obtain the result. □

We now make the following further assumption on the pair $(G, U)$, namely, that we have

$$\sum_{j=1}^{n}\deg(I_n) = \dim(U).$$

In other words, the sum of the degrees of the invariants of $U$ equals its dimension. Let $dI$ and $du$ be top degree forms on $\mathbb{I}$ and $U$, respectively. We will assume that $dI$ and $du$ induce

Haar-measures on $\mathbb{I}(\mathbb{R})$ and $U(\mathbb{R})$, respectively, normalized so that the covolumes of $\mathbb{I}(\mathbb{Z})$ in $\mathbb{I}(\mathbb{R})$ and $U(\mathbb{Z})$ in $U(\mathbb{R})$ are 1. Let $\omega$ denote a top degree form on $G$ defined over $\mathbb{Z}$. Then, from [26, Remark 3.14], we have the following result.

**Theorem 114.** *Let $R$ be $\mathbb{R}$ or $\mathbb{Z}_p$, let $|\cdot|$ denote the usual normalized absolute value on $R$, and let $s\colon \mathbb{I}(R) \to U(R)$ be a continuous section of $\iota$. Then there exists a constant $\mathcal{J} \in \mathbb{Q}^\times$, independent of $R$ and $s$, such that for any measurable function $\phi$ on $U(R)$, we have:*

$$\int_{G(R)\cdot s(\mathbb{I}(R))} \phi(u)du = |\mathcal{J}| \int_{I\in\mathbb{I}(R)} \int_{g\in G(R)} \phi(g\cdot s(I))\omega(g)dI,$$

$$\int_{U(K)} \phi(u)du = |\mathcal{J}| \int_{\substack{I\in U(K)\\ \Delta(I)\neq 0}} \sum_{u\in \frac{\iota^{-1}(I)}{G(K)}} \frac{1}{\#\mathrm{Stab}_{G(K)}(u)} \int_{g\in G(K)} \phi(g\cdot u)\omega(g)df.$$

We have the following immediate consequence to Theorem 114.

**Corollary 115.** *Let $\phi\colon \mathbb{I}(\mathbb{R}) \to \mathbb{R}$ and $\Theta\colon G(\mathbb{R}) \to \mathbb{R}$ be smooth, compactly supported functions, and let $\psi = \mathcal{S}(\phi, \Theta)$. Then we have*

$$\mathrm{Vol}(\psi) = |\mathcal{J}|\mathrm{Vol}(\Theta)\mathrm{Vol}(\phi).$$

### 4.4.1 Application to the representation of $\mathrm{PGL}_2$ on $V$

For $i \in \{0,1,2\}$, let $V_4(\mathbb{R})^{(i)}$ denote the set of elements $f \in V_4(\mathbb{R})$ that have $4-2i$ distinct real roots and $i$ distinct pairs of complex conjugate roots in $\mathbb{P}^1_{\mathbb{C}}$. We write $V_4(\mathbb{R})^{(2)}$ as $V_4(\mathbb{R})^{(2+)} \cup V_4(\mathbb{R})^{(2-)}$, the union of positive definite and negative definite binary quartic forms. For any $L \subset V_4(\mathbb{R})$, we define $L^{(i)} := L \cap V_4(\mathbb{R})^{(i)}$ for each $i \in \{0,1,2,2+,2-\}$. Let $\mathrm{Inv}(\mathbb{R})^\pm$ denote the subsets of $\mathrm{Inv}(\mathbb{R})$ consisting of elements $(I,J)$ with $\pm\Delta(I,J) > 0$. The map $\iota$ sends $V_4(\mathbb{R})^{(1)}$ to $\mathrm{Inv}(\mathbb{R})^-$ and $V_4(\mathbb{R})^{(i)}$ to $\mathrm{Inv}(\mathbb{R})^+$ for $i \in \{0,2\}$. We write $V_4(\mathbb{R})^\pm := \iota^{-1}(\mathrm{Inv}(\mathbb{R})^\pm)$ and $V_4(\mathbb{Z})^\pm := V_4(\mathbb{R})^\pm \cap V_4(\mathbb{Z})$.

Let $\mathcal{H}\colon \mathrm{Inv}(\mathbb{R}) \to \mathbb{R}_{\geq 0}$ be a smooth, compactly supported function, which we will later take to be an approximation of the characteristic function of the set of elements in $\mathrm{Inv}(\mathbb{R})^\pm$

with height less than 1. For a real number $X > 0$, we set $\mathcal{H}_X(I,J) := \mathcal{H}(I/X^{1/3}, J/X^{1/2})$. We say that an element $f \in V_4(\mathbb{Z})$ is *generic* if $f$ is irreducible over $\mathbb{Q}$ and the stabilizer of $f$ in $\mathrm{PGL}_2(\mathbb{Q})$ is trivial. For any set $L \subset V_4(\mathbb{Z})$, we denote by $L^{\mathrm{gen}}$ the set of generic elements in $L$. For a $\mathrm{PGL}_2(\mathbb{Z})$-invariant function $T\colon V_4(\mathbb{Z}) \to \mathbb{R}$, an $i \in \{0, 1, 2+, 2-\}$, and a real number $X \geq 1$, we define

$$\begin{aligned} N_{\mathcal{H}}(V^{(i)}, T; X) &:= \sum_{f \in \frac{V_4(\mathbb{Z})^{(i)}}{\mathrm{PGL}_2(\mathbb{Z})}} \frac{T(f)}{|\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{Z})}(f)|} \mathcal{H}_X\big(\iota(f)\big); \\ N^{\mathrm{gen}}_{\mathcal{H}}(V^{(i)}, T; X) &:= \sum_{f \in \frac{V_4(\mathbb{Z})^{(i),\mathrm{gen}}}{\mathrm{PGL}_2(\mathbb{Z})}} T(f) \mathcal{H}_X\big(\iota(f)\big). \end{aligned}$$

#### 4.4.1.1 Construction of fundamental sets

The isomorphism class of the stabilizer in $\mathrm{PGL}_2(\mathbb{R})$ of an element $f \in V_4(\mathbb{R})$ with nonzero discriminant depends only on the sign of the discriminant of $f$. We denote the size of this stabilizer by $\sigma^{\pm}$, and have $\sigma_0 = \sigma_{2\pm} = \sigma^+ = 4$ and $\sigma_1 = \sigma^- = 2$. We construct sections

$$\begin{aligned} \kappa^{(i)}\colon \mathrm{Inv}(\mathbb{R})^+ &\to V_4(\mathbb{R})^{(i)}, \quad i \in \{0, 2+, 2-\}, \\ \kappa^{(1)}\colon \mathrm{Inv}(\mathbb{R})^- &\to V_4(\mathbb{R})^{(1)}, \end{aligned}$$

satisfying the following properties:

(a) We have $\iota(\kappa^{(i)}(I,J)) = (I,J)$ for each $i$ and every pair $(I,J) \in \mathrm{Inv}(\mathbb{R})^{\pm}$.

(b) The coefficients of $f(x,y) = \kappa^{(i)}(I,J)$ are bounded by $O(H(I,J)^{1/6})$.

The construction of these sections is standard. We denote the image of $\kappa^{(i)}$ in $V_4(\mathbb{R})^{(i)}$ by $\mathcal{R}_V^{(i)}$.

#### 4.4.1.2 Fundamental domain for the action of $\mathrm{PGL}_2(\mathbb{Z})$ on $\mathrm{PGL}_2(\mathbb{R})$

Let $\mathcal{F}_2$ denote Gauss's usual fundamental domain for $\mathrm{PGL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2(\mathbb{R})$ in $\mathrm{PGL}_2(\mathbb{R})$. It follows that $\mathcal{F}_2$ is contained in the Siegel set $\{ntk : n \in N_2, t \in T_2, k \in K_2\}$, where $K_2$ is

the real orthogonal group $\mathrm{SO}_2(\mathbb{R})$, $N_2$ consists of lower triangular unipotent elements with absolutely bounded coefficients, and

$$T_2 = \left\{ \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} : t \geq \sqrt[4]{3}/\sqrt{2} \right\}. \tag{4.30}$$

#### 4.4.1.3 Smoothed averaging over $\mathrm{PGL}_2(\mathbb{R})$

For a function $\psi\colon V_4(\mathbb{R}) \to \mathbb{C}$, and a positive real number $X > 0$, define $\psi_X\colon V_4(\mathbb{R}) \to \mathbb{C}$ to be $\psi_X(f) := \psi(f/X)$. Fix $i \in \{0, 1, 2+, 2-\}$. Given smooth, compactly supported functions $\mathcal{H}\colon \mathrm{Inv}(\mathbb{R}) \to \mathbb{R}_{\geq 0}$ and $\Theta\colon \mathrm{PGL}_2(\mathbb{R}) \to \mathbb{R}_{\geq 0}$, we obtain the smooth, compactly supported function $\mathcal{S}_{\kappa^{(i)}}(\mathcal{H}, \Theta) =: \psi^{(i)}\colon V_4(\mathbb{R})^{(i)} \to \mathbb{R}_{\geq 0}$. Let $X > 0$ be a real number. We clearly have

$$\mathcal{S}_A(\mathcal{H}_X, \Theta) = \mathcal{S}_A(\mathcal{H}, \Theta)_{X^{1/6}}.$$

For a $\mathrm{PGL}_2(\mathbb{Z})$-invariant function $T\colon V_4(\mathbb{Z})^{(i)} \to \mathbb{R}$, a function $\psi = \psi^{(i)}$ as above, and a real number $X > 0$, we define the integral $\mathcal{O}^{(i)}(T, \psi; X)$ to be

$$\mathcal{O}^{(i)}(T, \psi; X) := \int_{\gamma \in \mathcal{F}_2} \Big( \sum_{f \in V_4(\mathbb{Z})^{\mathrm{gen}}} (\gamma \cdot \psi_X)(f) T(f) \Big) d\gamma. \tag{4.31}$$

Then the following result is an immediate consequence of Theorem 113.

**Proposition 116.** *Let notation be as above. Fix $i \in \{0, 1, 2+, 2-\}$. Let $T\colon V_4(\mathbb{Z}) \to \mathbb{R}$ be a $\mathrm{PGL}_2(\mathbb{Z})$-invariant function, and let $\psi = \mathcal{S}_{V_4}(\mathcal{H}, \Theta)$. Then we have that*

$$N_{\mathcal{H}}^{\mathrm{gen}}(V^{(i)}, T; X) = \frac{1}{\sigma_i \mathrm{Vol}(\Theta)} \mathcal{O}^{(i)}(T, \psi; X^{1/6}).$$

### 4.4.2 Application to the representations of $\mathrm{SL}_4$ on $W$ and $\mathrm{PSO}_{\mathscr{A}_4}$ on $W_{\mathscr{A}_4}$

For $i \in \{0, 1, 2+, 2-\}$, the number of $\mathrm{SL}_4(\mathbb{R})$-orbits on $W_4(\mathbb{R})$ with resolvent $f$ for some fixed $f \in V_4(\mathbb{R})^{(i)}$ depends only on $i$. We denote this number by $\tau(i)$, and we write $W_4(\mathbb{R})^{(i)} = \iota^{-1}(V_4(\mathbb{R})^{(i)}$. Similarly, the number of $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{R})$-orbits (resp., soluble $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{R})$-orbits) on $W_{\mathscr{A}_4}(\mathbb{R})$ arising from some fixed $f \in V_4(\mathbb{R})^{(i)}$ depends only on $i$. We denote this number by $\tau_{\mathscr{A}_4}(i)$ (resp., $\tau^{\mathrm{sol}}_{\mathscr{A}_4}(i)$), and we write $W_{\mathscr{A}_4}(\mathbb{R})^{(i)} = \iota^{-1}(V_1(\mathbb{R})^{(i)})$. This yields a natural partition of the set of elements in $W_4(\mathbb{R})^{(i)}$ (resp., $W_{\mathscr{A}_4}(\mathbb{R})^{(i)}$) with nonzero discriminant into subsets $W_4(\mathbb{R})^{(i,j)}$ (resp., $W_{\mathscr{A}_4}(\mathbb{R})^{(i,j)}$) with $1 \le j \le \tau(i)$ (resp., $1 \le j \le \tau_{\mathscr{A}_4}(i)$).

Furthermore, the size of the stabilizer in $\mathrm{SL}_4(\mathbb{R})$ (resp., $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{R})$) of an element of $W_4(\mathbb{R})^{(i)}$ (resp., $W_{\mathscr{A}_4}(\mathbb{R})^{(i)}$) depends only on $i$. We denote this size by $\sigma(i)$ (resp., $\sigma_{\mathscr{A}_4}(i)$).

#### 4.4.2.1 Construction of fundamental sets

For each $i \in \{0, 1, 2+\}$, and for each $j$ with $1 \le j \le \tau(i)$ and $1 \le j \le \tau_{\mathscr{A}_4}(i)$, there exist smooth sections

$$\kappa^{(i,j)} \colon V_4(\mathbb{R})^{(i)} \;\to\; W_4(\mathbb{R})^{(i,j)},$$

$$\kappa^{(i,j)}_{\mathscr{A}_4} \colon V_1(\mathbb{R})^{(i)} \;\to\; W_{\mathscr{A}_4}(\mathbb{R})^{(i,j)},$$

respectively, satisfying $\iota(\kappa^{(i,j)}(f)) = f$ for every binary quartic form $f \in V_4(\mathbb{R})^{(i)}$ (resp., $\iota(\kappa^{(i,j)}_{\mathscr{A}_4}(f)) = f$ for every $f \in V_1(\mathbb{R})^{(i)}$) for each $i, j$. We denote the images of $\kappa^{(i,j)}$ and $\kappa^{(i,j)}_{\mathscr{A}_4}$ by $\mathcal{R}^{(i,j)}$ and $\mathcal{R}^{(i,j)}_{\mathscr{A}_4}$, respectively.

We can choose the section $\kappa^{(i,j)}$ so that the following is satisfied. For real numbers $Y, T > 1$, and for a binary quartic form $f(x, y) \in V_4(\mathbb{R})^{(i)}$ with coefficients $(a, b, c, d, e)$, such that $a = O(Y)$, $b = O(TY)$, $c = O(T^2Y)$, $d = O(T^3Y)$, and $e = O(T^4Y)$, the coefficients $a_{ij}$ and $b_{ij}$ of $(A, B) = \kappa^{(i,j)}(f)$ are bounded by $O(Y^{1/4})$ and $O(TY^{1/4})$, respectively. Similarly, we can choose $\kappa^{(i,j)}_{\mathscr{A}_4}$ such that the following is satisfied. For a real number $Y > 1$, and for a binary quartic form $f(x, y) \in V_4(\mathbb{R})^{(i)}$ with coefficients $a = \det(\mathscr{A}_4) = 1$, $b = O(Y)$, $c = O(Y^2)$,

$d = O(Y^3)$, and $e = O(Y^4)$, the coefficients $b_{ij}$ of $(\mathscr{A}_4, B) = \kappa_{\mathscr{A}_4}^{(i,j)}(f)$ are bounded by $O(Y)$.

#### 4.4.2.2 Fundamental domains for the action of $G(\mathbb{Z})$ on $G(\mathbb{R})$

We now describe Siegel sets containing fundamental domains $\mathcal{F}_4$ and $\mathcal{F}_{\mathscr{A}_4}$ for the actions of $\mathrm{SL}_4(\mathbb{Z})$ on $\mathrm{SL}_4(\mathbb{R})$ and $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})$ on $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{R})$, respectively.

We may choose a fundamental domain $\mathcal{F}_4$ for the action of $\mathrm{SL}_4(\mathbb{Z})$ on $\mathrm{SL}_4(\mathbb{R})$ contained in a Siegel domain $N_4T_4K_4$ in $\mathrm{SL}_4(\mathbb{R})$. Here, $K_4 = \mathrm{SO}_4(\mathbb{R})$ is a maximal compact subgroup of $\mathrm{SL}_4(\mathbb{R})$, $N_4$ consists of lower triangular unipotent elements with absolutely bounded coefficients, and $T_4$ is given by

$$T_4 = \left\{ \begin{bmatrix} s_1^{-3}s_2^{-1}s_3^{-1} & & & \\ & s_1s_2^{-1}s_3^{-1} & & \\ & & s_1s_2s_3^{-1} & \\ & & & s_1s_2s_3^3 \end{bmatrix} : s_1, s_2, s_3 > c \right\},$$

for some $c > 0$. The *weights* $w_{ij}$ of $a_{ij}$ and $b_{ij}$ are the eigenvalues for the torus action on the space dual to $W_4(\mathbb{R})$, and are given below: here $a_{ij}$ and $b_{ij}$ are the coefficients of $A$ and $B$, respectively, for $(A, B) \in W_4(\mathbb{R})$.

$$\begin{array}{llll} w_{11} = s_1^{-6}s_2^{-2}s_3^{-2} & w_{12} = s_1^{-2}s_2^{-2}s_3^{-2} & w_{13} = s_1^{-2}s_2^{0}s_3^{-2} & w_{14} = s_1^{-2}s_2^{0}s_3^{2} \\ & w_{22} = s_1^{2}s_2^{-2}s_3^{-2} & w_{23} = s_1^{2}s_2^{0}s_3^{-2} & w_{24} = s_1^{2}s_2^{0}s_3^{2} \\ & & w_{33} = s_1^{2}s_2^{2}s_3^{-2} & w_{34} = s_1^{2}s_2^{2}s_3^{2} \\ & & & w_{44} = s_1^{2}s_2^{2}s_3^{6} \end{array}$$

A Haar-measure on $\mathrm{SL}_4(\mathbb{R})$ in Iwasawa coordinates is $s_1^{-12}s_2^{-8}s_3^{-12}dnd^\times sdk$, where $dn$ is Euclidean measure on $N_4$, $d^\times s$ denotes $\prod_i d^\times s_i$, and $dk$ is probability Haar-measure on $\mathrm{SO}_4(\mathbb{R})$.

It follows from Lemma 5 that $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})\backslash\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{R}) \simeq \mathrm{SO}_{\mathscr{A}_4}(\mathbb{Z})\backslash\mathrm{SO}_{\mathscr{A}_4}(\mathbb{R})$, and so it suffices to construct a fundamental domain for the action of $\mathrm{SO}_{\mathscr{A}_4}(\mathbb{Z})$ on $\mathrm{SO}_{\mathscr{A}_4}(\mathbb{R})$. We may choose a fundamental domain $\mathcal{F}_{\mathscr{A}_4}$ for the action of $\mathrm{SO}_{\mathscr{A}_4}(\mathbb{Z})$ on $\mathrm{SO}_{\mathscr{A}_4}(\mathbb{R})$ contained in a Siegel domain $N_{\mathscr{A}_4}T_{\mathscr{A}_4}K_{\mathscr{A}_4}$ in $\mathrm{SO}_{\mathscr{A}_4}(\mathbb{R})$. Here, $K_{\mathscr{A}_4}$ is a maximal compact subgroup of $\mathrm{SO}_{\mathscr{A}_4}(\mathbb{R})$, $N_{\mathscr{A}_4}$ consists of lower triangular unipotent elements with absolutely bounded coefficients, and $T_{\mathscr{A}_4}$ is given by

$$T_{\mathscr{A}_4} = \left\{ \begin{bmatrix} s_1^{-1}s_2^{-1} & & & \\ & s_1^{-1}s_2 & & \\ & & s_1s_2^{-1} & \\ & & & s_1s_2 \end{bmatrix} : s_1, s_2 > c \right\},$$

for some $c > 0$. The group $\mathrm{SO}_{\mathscr{A}_4}(\mathbb{R})$ acts on $W_{\mathscr{A}_4}(\mathbb{R})$, and the weights $w(b_{ij})$ of the coefficients of $B$ for $(\mathscr{A}_4, B) \in W_{\mathscr{A}_4}(\mathbb{R})$ are as follows:

$$\begin{array}{llll} w(b_{11}) = s_1^{-2}s_2^{-2} & w(b_{12}) = s_1^{-2} & w(b_{13}) = s_2^{-2} & w(b_{14}) = 1 \\ & w(b_{22}) = s_1^{-2}s_2^{2} & w(b_{23}) = 1 & w(b_{24}) = s_2^2 \\ & & w(b_{33}) = s_1^2s_2^{-2} & w(b_{34}) = s_1^2 \\ & & & w(b_{44}) = s_1^2s_2^2 \end{array}$$

#### 4.4.2.3 Smoothed averaging over $\mathrm{SL}_4(\mathbb{R})$ and $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{R})$

Recall that for a function $\psi\colon V_4(\mathbb{R}) \to \mathbb{C}$ and a real number $X > 0$, we define $\psi_X\colon V_4(\mathbb{R}) \to \mathbb{C}$ via $\psi_X(f) = \psi(f/X)$. For a real number $Y > 0$, we define $\psi[Y]\colon V_4(\mathbb{R}) \to \mathbb{C}$ via

$$\psi[Y](f) := \left( \begin{bmatrix} Y^{-1/2} & & \\ & & Y^{1/2} \end{bmatrix} \cdot \psi \right)(f) = \psi\big(aY^2x^4 + bYx^3y + cx^2y^2 + dY^{-1}xy^3 + eY^{-2}y^4\big),$$

for $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + dy^4$. We say that an element $w$ in $W_4(\mathbb{Z})$ (resp., $W_A(\mathbb{Z})$) is *generic* if: (a) the element $w$ is not distinguished; (b) the stabilizer in $\mathrm{SL}_4(\mathbb{Q})$ (resp., $\mathrm{PSO}_A(\mathbb{Q})$) of $w$ is trivial; and (c) the resolvent of $w$ is generic. For any subset $L$ of $W_4(\mathbb{Z})$ or $W_A(\mathbb{Z})$, we denote the set of generic elements in $L$ by $L^{\mathrm{gen}}$. We now define the following counting functions on $W_4(\mathbb{Z})$:

$$\begin{aligned} N_\psi(W^{(i,j)}, T; X, Y) &:= \sum_{w \in \frac{W_4(\mathbb{Z})^{(i,j)}}{\mathrm{SL}_4(\mathbb{Z})}} \frac{T(w)}{|\mathrm{Stab}_{\mathrm{SL}_4(\mathbb{Z})}(w)|} \cdot (\psi_X[Y])(\iota(w)); \\ N_\psi^{\mathrm{gen}}(W^{(i,j)}, T; X, Y) &:= \sum_{w \in \frac{W_4(\mathbb{Z})^{(i,j),\mathrm{gen}}}{\mathrm{SL}_4(\mathbb{Z})}} T(w) \cdot (\psi_X[Y])(\iota(w)). \end{aligned} \tag{4.32}$$

Let $\Phi\colon W_4(\mathbb{R}) \to \mathbb{C}$ be a function. For real numbers $X > 0$ and $Y > 0$, we define $\Phi[X,Y]\colon W_4(\mathbb{R}) \to \mathbb{C}$ to be

$$(\Phi[X,Y])(A,B) := \Phi\Big(\frac{A}{X}, \frac{B}{Y}\Big). \tag{4.33}$$

We now have the following result.

**Proposition 117.** *Let $\psi\colon V_4(\mathbb{R}) \to \mathbb{R}$ be a smooth, compactly supported function. Let $T\colon W_4(\mathbb{Z}) \to \mathbb{R}$ be a $\mathrm{SL}_4(\mathbb{Z})$-invariant function. Let $\Theta\colon \mathrm{SL}_4(\mathbb{R}) \to \mathbb{R}$ be a smooth and compactly supported function. Let $\Phi$ denote $\mathcal{S}(\psi, \Theta)$. For positive real numbers $X$ and $Y$, we have that*

$$N_\psi^{\mathrm{gen}}(W^{(i,j)}, T; X, Y) = \frac{1}{\sigma(i)\mathrm{Vol}(\Theta)} \int_{\gamma \in \mathcal{F}_4} \Big( \sum_{w \in W_4(\mathbb{Z})^{(i,j),\mathrm{gen}}} T(w) \cdot (\gamma \cdot \Phi[Y^{-1/2}X^{1/4}, Y^{1/2}X^{1/4}])(w) \Big) d\gamma.$$

*Proof.* The only thing necessary to verify is that for positive real numbers $X$ and $Y$, we have

$$\mathcal{S}(\psi_X[Y], \Theta) = \mathcal{S}(\psi, \Theta)[Y^{-1/2}X^{1/4}, Y^{1/2}X^{1/4}].$$

This equality is apparent, and the result follows from Theorem 113. □

Let $A$ be a fixed symmetric $4\times 4$ matrix with $\det A = n$. Given a function $\psi\colon V_n(\mathbb{R}) \to \mathbb{C}$, define $\psi\{Y\}\colon V_n(\mathbb{R}) \to \mathbb{C}$ to be

$$\psi\{Y\}(f(x,y)) := \psi(f(x,y/Y)).$$

For a function $\Phi\colon W_A(\mathbb{R}) \to \mathbb{C}$, define $\Phi_Y\colon W_A(\mathbb{R}) \to \mathbb{C}$ via

$$\Phi_Y(B) := \Phi\Big(\frac{B}{Y}\Big).$$

Finally, for a $\mathrm{PSO}_A(\mathbb{Z})$-invariant function $T\colon W_A(\mathbb{Z}) \to \mathbb{R}$, we define

$$\begin{aligned} N_\psi(W_A^{(i,j)}, T; X) &:= \sum_{B \in \frac{W_A(\mathbb{Z})^{(i,j)}}{\mathrm{PSO}_A(\mathbb{Z})}} \frac{T(B)}{|\mathrm{Stab}_{\mathrm{PSO}_A(\mathbb{Z})}(B)|} \cdot \psi\{X\}(\iota(B)). \\ N_\psi^{\mathrm{gen}}(W_A^{(i,j)}, T; X) &:= \sum_{B \in \frac{W_A(\mathbb{Z})^{(i,j),\mathrm{gen}}}{\mathrm{PSO}_A(\mathbb{Z})}} T(B) \cdot \psi\{X\}(\iota(B)). \end{aligned}$$

Then we have the following consequence of Theorem 113.

**Proposition 118.** *Let $\psi\colon V_n(\mathbb{R}) \to \mathbb{R}$ be a smooth, compactly supported function. Let $T\colon W_A(\mathbb{Z}) \to \mathbb{R}$ be an $\mathrm{PSO}_A(\mathbb{Z})$-invariant function. Let $\Theta\colon \mathrm{PSO}_A(\mathbb{R}) \to \mathbb{R}$ be a smooth, compactly supported function. Let $\Phi$ denote $\mathcal{S}(\psi, \Theta)$. For a positive real number $X$, we have*

$$N_\psi^{\mathrm{gen}}(W_A^{(i,j)}, T; X) = \frac{1}{\sigma_A(i)\mathrm{Vol}(\Theta)} \int_{\gamma \in \mathcal{F}_A} \Big( \sum_{B \in W_A(\mathbb{Z})^{(i,j),\mathrm{gen}}} T(B)(\gamma \cdot \Phi_X)(B) \Big) d\gamma.$$

We will have occasion to use Proposition 118 in the situation detailed below. Let $\psi\colon V_4(\mathbb{R}) \to \mathbb{R}$ and $\Theta\colon \mathrm{PSO}_{\mathscr{A}_4}(\mathbb{R}) \to \mathbb{R}$ be fixed smooth compactly supported functions. Let $X$ and $Y$ be positive real numbers with $Y \ll X^{1/2}$. Consider the function $\psi_X[Y]\colon V_4(\mathbb{R}) \to \mathbb{R}$. We restrict $\psi_X[Y]$ to $V_1(\mathbb{R})$, obtaining a smooth, compactly supported function $\psi_{X,Y} := \psi_X[Y]|_1\colon V_1(\mathbb{R}) \to \mathbb{R}$. We then denote $\mathcal{S}(\psi_{X,Y}, \Theta)$ by $\Phi_{X,Y}$. The twisted functions $\psi_{X,Y}\{Y/X\}$ and $\Phi_{X,Y}[Y/X]$ are smooth and compactly supported on elements whose coefficients are $\ll 1$.

We denote them by $\psi^{(X,Y)}$ and $\Phi^{(X,Y)}$, respectively. Finally, parallel to (4.32), define

$$N_\psi^{\mathrm{gen}}(W_{\mathscr{A}_4}^{(i,j)}, T; X, Y) := \sum_{B \in \frac{W_{\mathscr{A}_4}(\mathbb{Z})^{(i,j),\mathrm{gen}}}{\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})}} T(B) \cdot (\psi_X[Y])(\iota(B))$$
$$= \sum_{B \in \frac{W_{\mathscr{A}_4}(\mathbb{Z})^{(i,j),\mathrm{gen}}}{\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})}} T(B) \cdot (\psi^{(X,Y)}\{X/Y\})(\iota(B)).$$

We then have the following immediate corollary to Proposition 118.

**Corollary 119.** *With notation as above, we have*

$$N_\psi^{\mathrm{gen}}(W_{\mathscr{A}_4}^{(i,j)}, T; X, Y) = \frac{1}{\sigma_{\mathscr{A}_4}(i)\mathrm{Vol}(\Theta)} \int_{\gamma \in \mathcal{F}_{\mathscr{A}_4}} \Big( \sum_{B \in W_{\mathscr{A}_4}(\mathbb{Z})^{(i,j),\mathrm{gen}}} T(B) \cdot (\gamma \cdot \Phi^{(X,Y)}[X/Y])(B) \Big) d\gamma.$$

## 4.5 Counting special integral orbits via equidistribution

For a function $T\colon \mathbb{Z}^n \to \mathbb{R}$ defined by congruence conditions, let $T_p\colon \mathbb{Z}_p^n \to \mathbb{R}$ be the closure of $T$ to $\mathbb{Z}_p^n$, and let

$$\nu_p(T) := \int_{\mathbb{Z}_p^n} T_p(v) dv, \quad \nu(T) := \int_{\widehat{\mathbb{Z}}^n} T(v) dv = \prod_p \nu_p(T),$$

where $dv$ is Euclidean measure on affine $n$-space, normalized so that $\mathbb{Z}^n$ has covolume 1 in $\mathbb{R}^n$. Let $0 < X$ and $0 < Y \ll \sqrt{X}$ be real numbers. The purpose of this section is to bound and estimate $N_\psi^{\mathrm{gen}}(W_{\mathscr{A}_4}^{(i,j)}, T; X, Y)$ for various functions $T\colon W_{\mathscr{A}_4}(\mathbb{Z}) \to \mathbb{R}$. We will prove two such results. The first result is an upper bound, to state which we need the following notation. For a prime $p$, define the quantities

$$\nu(p) := p^{-6}, \quad \nu(p^2) := p^{-12}, \quad \nu(p^3) := p^{-17}, \quad \nu(p^k) := p^{-11k/2},$$

for integers $k \geq 4$. For integers $n > 0$, we define $\nu(n)$ multiplicatively: $\nu(n) := \prod_{p^k \| n} \nu(p^k)$. Then we have the following:

**Theorem 120.** *Let $X$ and $Y$ be as above, and let $a$ be an integer such that $a \ll X^{1/4}Y^{1/2}$. Let $T_a \colon W_{\mathscr{A}_4} \to \mathbb{R}$ be the characteristic function of the set of non-distinguished elements $(\mathscr{A}_4, B) \in W_{\mathscr{A}_4}(\mathbb{Z})$ that are special at $a$. Let $\psi \colon V_4(\mathbb{R}) \to \mathbb{R}$ be a smooth and compactly supported function. Then we have that*

$$N_\psi(W_{\mathscr{A}_4}, T_a; X, Y) \ll_\epsilon \nu(a) X^{5-1/4+\epsilon} Y^{1/2}.$$

The above result has the following immediate consequence when $Y \ll X^{1/2-\delta}$.

**Corollary 121.** *Let notation be as in Theorem 120 with the added assumption that $Y \ll X^{1/2-\delta}$ for some $\delta > 0$. Then we have that*

$$N_\psi(W_{\mathscr{A}_4}, T_a; X, Y) \ll_\epsilon \nu(a) X^{5-\delta/2+\epsilon}.$$

A function $T \colon \mathbb{Z}^n \to \mathbb{R}$ is said to be *defined by finitely many congruence conditions* if there exists an integer $q > 0$ and a function $T_q \colon (\mathbb{Z}/q\mathbb{Z})^n \to \mathbb{R}$ such that $T$ is the lift of $T_q$ to $\mathbb{Z}^n$. Let $M_1$ and $M_2$ be positive real numbers. A function $T \colon W_{\mathscr{A}_4}(\mathbb{Z}) \to \mathbb{R}$ is said to be $(M_1, M_2)$-*acceptable* if $T$ is bounded and defined by congruence conditions modulo two relatively prime positive integers $b$ and $q$, where $b \ll M_1$, $q \ll M_2$, $q$ is squarefree, and the congruence conditions modulo every prime $p$ dividing $q$ is exactly that $T_p \colon W_{\mathscr{A}_4}(\mathbb{F}_p) \to \mathbb{R}$ is the characteristic function of the set of matrices that are of rank $\leq 1$ modulo $p$. We next use equidistribution methods to prove an estimate on $N_\psi^{\mathrm{gen}}(W_{\mathscr{A}_4}^{(i,j)}, T; X, Y)$ when $Y$ is close to $X^{1/2}$.

**Theorem 122.** *Let $\theta$ and $\delta$ be positive real numbers, which will eventually be picked to be sufficiently small. Let $X$ and $Y \gg X^{1/2-\delta}$ be positive real numbers. Let $T \colon W_{\mathscr{A}_4}(\mathbb{Z}) \to \mathbb{R}$ be an $(X^\theta, X^{1/2})$-acceptable function, with conditions defined modulo $b \leq X^\theta$ and $q \leq X^{1/2}$.*

*Then we have that*

$$N_{\psi}^{\mathrm{gen}}(W_{\mathscr{A}_4}^{(i,j)}, T; X, Y) = \frac{|\mathcal{J}_{\mathscr{A}_4}|}{\sigma_{\mathscr{A}_4}(i)} \mathrm{Vol}(\mathcal{F}_A)\nu(T)\mathrm{Vol}\big(\psi|_{\frac{Y^2}{X}}\big)X^4Y^2 + O\Big(\frac{X^{5+10\theta+60\delta-\lambda+\epsilon}}{q^6}\Big)$$

*where $\lambda > 0$ is an absolute constant independent of $\theta$ and $\delta$. Here, $\mathcal{J}_{\mathscr{A}_4}$ is the rational constant arising from Corollary 115 applied to the action of $\mathrm{PSO}_{\mathscr{A}_4}$ on $W_{\mathscr{A}_4}$.*

### 4.5.1 Counting special $\mathrm{SL}_4(\mathbb{Z})$-orbits on $W_4(\mathbb{Z})$

Let $\mathcal{D}$ be a bounded ball inside $U_4(\mathbb{R})$. Let $\gamma = (n, s, k) \in \mathrm{SL}_4(\mathbb{R})$ be an element where $s = (s_1, s_2, s_3)$, and let $Z > 1$ be a real number. For any $L \subset U_4(\mathbb{Z})$, consider the set

$$\mathcal{D}(L; \gamma, Z) = \big\{\gamma \cdot Z\mathcal{D} \cap L\big\}.$$

We will bound the number of elements in $\mathcal{D}(L; \gamma, Z)$ for various sets $L$. We begin with the following lemma:

**Lemma 123.** *Let $q = p^k$ be a prime power, and let $L_q^* \subset U_4(\mathbb{Z}/q\mathbb{Z})$ denote the set of matrices that, when viewed as quadratic forms, are squares of linear forms modulo $q$. Let $(a_{11}, a_{12}, a_{13}, a_{14}) \in (\mathbb{Z}/q\mathbb{Z})^4$ be a fixed tuple.*

(a) *Suppose that $a_{11} \not\equiv 0 \pmod q$ and that $p^\beta \parallel a_{11}$. Then there are no elements $B \in L_q^*$ with $b_{1i} = a_{1i}$ unless $\beta = 2\ell$ is even and $p^\ell \mid a_{1i}$ for $i \in \{2, 3, 4\}$, in which case $a_{11}$, $a_{12}$, $a_{13}$, and $a_{14}$ determine $B$ up to $O(p^{5\ell})$ choices.*

(b) *Suppose that $a_{11} \equiv 0 \pmod q$, and set $p^\ell = \gcd(a_{12}, a_{13}, a_{14})$. Then there are no elements $B \in L_q^*$ with $b_{1i} = a_{1i}$ unless $2\ell \geq k$, in which case $a_{11}$, $a_{12}$, $a_{13}$, and $a_{14}$ determine $B$ up to $O(p^{k+2\ell})$ choices.*

*Proof.* Any element $B \in L_q^*$ can be expressed as $B = (\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4)^2$ for $\alpha_i \in \mathbb{Z}/p^k\mathbb{Z}$. The coefficient $b_{11}$ of $B$ then satisfies $b_{11} \equiv \alpha_1^2 \pmod{p^k}$. Assume that $a_{11} \not\equiv 0$

(mod $p^k$). Clearly, the power of $p$ dividing $a_{11}$ must be even, say $2\ell$, for $a_{11}$ to occur as the leading coefficient of $B \in L_q$. Then the congruence $\alpha_1^2 \equiv a_{11} \pmod{p^k}$ determines $\alpha_1 \in \mathbb{Z}/p^k\mathbb{Z}$ up to $O(p^{2\ell})$ choices, and moreover $p^\ell \parallel \alpha_1$. Next, for $j \neq 1$, we consider the congruences $2\alpha_1\alpha_j \equiv a_{1j} \pmod{p^k}$. This implies that $p^\ell \mid a_{1j}$ for $j \in \{2,3,4\}$. Moreover, since $p^\ell \parallel \alpha_1$, the value of $a_{1j}$ determines $\alpha_j$ up to $O(p^\ell)$ possibilities. Thus, the values of $a_{11}$, $a_{12}$, $a_{13}$, and $a_{14}$, determine $\alpha_1$, $\alpha_2$, $\alpha_3$, and $\alpha_4$, and hence determine $B$, up to $O(p^{5\ell})$ possibilities.

We move on to part (b) of the lemma. Since $a_{11} \equiv 0 \pmod{p^k}$, we must have $p^\ell \parallel \alpha_1$, with $2\ell \geq k$, and since $2\alpha_1\alpha_j \equiv a_{1j} \pmod{p^k}$, it follows that $p^\ell \mid a_{1j}$ for $j \in \{2,3,4\}$. Therefore, $\alpha_1$ is determined up to $O(p^{k-\ell})$ choices, and as before, $\alpha_2$, $\alpha_3$, and $\alpha_4$ are determined up to $O(p^\ell)$ choices each. This gives a total of $O(p^{k+2\ell})$ choices for the $\alpha_i$, yielding the result. □

The lemma has the following application to the important case when $q$ is squarefree:

**Corollary 124.** *Let $q$ be a squarefree positive integer, and let $L_q \subset U_4(\mathbb{Z}/q\mathbb{Z})$ denote the set of matrices that are of rank $\leq 1$ modulo $q$. Let $q' \mid q$, and let $(a_{11}, a_{12}, a_{13}, a_{14}) \in (\mathbb{Z}/q\mathbb{Z})^4$ be a fixed tuple such that $a_{11} \equiv 0 \pmod{q'}$. Then there are no elements $B \in L_q$ with coefficients $b_{1i} = a_{1i}$ unless $q' \mid a_{1j}$ for $j \in \{2,3,4\}$, in which case $a_{11}$, $a_{12}$, $a_{13}$, and $a_{14}$ determine $B$ up to $O_\epsilon(q'^3 q^\epsilon)$ choices.*

*Proof.* The number of $B \in L_q$ with $b_{1j} = a_{1j}$ for $j \in \{1,2,3,4\}$ is at most the number of $B \in L_q^*$ such that for some $\gamma \in (\mathbb{Z}/q\mathbb{Z})^\times/(\mathbb{Z}/q\mathbb{Z})^{\times 2}$ we have $b_{1j} = \gamma a_{1j}$ for $j \in \{1,2,3,4\}$. Since $|(\mathbb{Z}/q\mathbb{Z})^\times/(\mathbb{Z}/q\mathbb{Z})^{\times 2}| \ll_\epsilon q^\epsilon$, it suffices to prove the lemma with $L_q$ replaced by $L_q^*$. The result then follows by applying Lemma 123 along with the Chinese remainder theorem. □

Next we have the following lemma describing conditions on the coefficients of $B$ imposed by $B$ being rank $\leq 2$ modulo a prime power.

**Lemma 125.** *Let $q = p^k$ be a prime power, and let $(a_{11}, a_{12}, a_{13}, a_{14}) \in (\mathbb{Z}/q\mathbb{Z})^4$ be fixed and nonzero. Then the condition that $B \in U_4(\mathbb{Z}/q\mathbb{Z})$ satisfies $b_{ij} = a_{1j}$ for $j \in \{1,2,3,4\}$ and to*

*be rank* $\leq 2$ *modulo* $q$ *forces* $B$ *to satisfy two independent conditions, one of density* $O(p^{-k})$*, and another of density* $O(p^{-1})$*.*

*Proof.* The first condition is simply that the $3 \times 3$ matrix $[b_{ij}]_{2 \leq i,j \leq 4}$ has determinant 0. When the tuple $(b_{11}, b_{12}, b_{13}, b_{14})$ is nonzero, the first condition is insufficient to ensure that $B$ is of rank $\leq 2$. Hence, there must be a second, necessarily independent, condition. The largest possible density for this condition is $O(1/p)$. □

Let $a, b > 0$ be integers. Let $\mathcal{L}_a$ be the set of elements in $U_4(\mathbb{Z})$ of rank $\leq 1$ modulo $a$, and let $\mathcal{L}_{a,b} \subset \mathcal{L}_a$ be the subset of element of rank $\leq 2$ modulo $ab$. Define the quantity $\mu(a, b)$ tby

$$\mu(a, b) := a^{-6} b^{-1} b_1^{-1}, \tag{4.34}$$

where $b_1$ is the product of primes of $b$ not dividing $a$. For any subset $S \subset U_4(\mathbb{Z})$ and two subsets $\mathrm{var}_1$, $\mathrm{var}_2$ of coefficients of $U$, let $S(\mathrm{var}_1; \mathrm{var}_2) \subset S$ be the subset of elements in which all coefficients in $\mathrm{var}_1$ vanish and no coefficients in $\mathrm{var}_2$ vanish. Let $U_1 \subset U$ be the determinant-1 subvariety. Then we have the following result:

**Lemma 126.** *Let* $\gamma \in \mathcal{F}_4$ *be such that* $\gamma = n(s_1, s_2, s_3)k$*. We define the quantity*

$$M(s) := M(s_1, s_2, s_3) := \max(1, s_1^2 s_2^2 s_3^{-2}, s_1^4 s_2^2 s_3^{-4}, s_1^6 s_3^{-6}).$$

*Let* $a$ *and* $b$ *be positive integers, and let* $Z$ *be a real number satisfying* $ab \ll Z$*. Then estimates on* $\#\mathcal{D}(L; \gamma, Z)$ *for the following choices of* $L$ *are as in the second column of the following table. Moreover, in order for* $\mathcal{D}(L; \gamma, Z)$ *to be nonempty, the condition listed in the third column must be true.*

*Proof.* First, note that the claims in the fourth column of the table follow immediately from the nonvanishing conditions stipulated in the second column. Hence it remains to prove the claims in the third column.

| # | $L$ | $\#\mathcal{D}(L;\gamma,Z) \ll$ | $\mathcal{D}(L;\gamma,Z) \neq \emptyset$ implies |
|---|---|---|---|
| **1** | $U_1(\mathbb{Z})(\emptyset;\{a_{11}\})$ | $s_1^{-2}s_3^{-2}Z^9$ | $s_1^6s_2^2s_3^2 \ll Z$ |
| **2** | $U_1(\mathbb{Z})(\{a_{11}\};\{a_{12}\})$ | $s_1^4s_2^2Z^8$ | $s_1^2s_2^2s_3^2 \ll Z$ |
| **3** | $U_1(\mathbb{Z})(\{a_{11},a_{12}\};\{a_{13},a_{22}\})$ | $s_1^6s_2^4s_3^2Z^7$ | $s_1^2s_3^2 \ll Z, \quad s_2^2s_3^2 \ll s_1^2Z$ |
| **4** | $U_1(\mathbb{Z})(\{a_{11},a_{12},a_{22}\};\{a_{13}\})$ | $s_1^4s_2^6s_3^4Z^6$ | $s_1^2s_3^2 \ll Z$ |
| **5** | $U_1(\mathbb{Z})(\{a_{11},a_{12},a_{13}\};\{a_{22}\})$ | $s_1^{10}s_2^2s_3^6Z^5$ | $s_1^2 \ll s_3^2Z, \quad s_2^2s_3^2 \ll s_1^2Z$ |
| **6** | $U_1(\mathbb{Z})(\{a_{11},a_{12},a_{13},a_{22}\};\emptyset)$ | $s_1^8s_2^6s_3^8Z^4$ | $s_1^2 \ll s_3^2Z, \quad s_3^2 \ll s_1^2Z$ |
| **a** | $\mathcal{L}_{a,b}(\emptyset;\{b_{11}\})$ | $\mu(a,b)s_1^{-6}s_3^6M(s)Z^{10+\epsilon}$ | $s_1^6s_2^2s_3^2 \ll Z$ |
| **b** | $\mathcal{L}_{a,b}(\{b_{11}\};\{b_{12}\})$ | $\sqrt{a}\mu(a,b)s_2^2s_3^8M(s)Z^{9+\epsilon}$ | $s_1^2s_2^2s_3^2 \ll Z$ |
| **c** | $\mathcal{L}_{a,b}(\{b_{11},b_{12}\};\emptyset)$ | $a\mu(a,b)s_1^4s_2^4s_3^{12}M(s)Z^{8+\epsilon}$ | |

We begin by proving the claims in the first six rows of the table. It will be convenient to divide into two cases: first assume that not all of $a_{11}$, $a_{12}$, and $a_{13}$ are 0. In this case, either $a_{24}$, $a_{34}$, or $a_{44}$ must arise in the determinant polynomial expansion of $\det(A)$ with nonzero coefficient. We then fiber over all but this one coefficient, and note that the condition $\det(A) = 1$ determines this coefficient uniquely (if it is integral at all). With this observation, Cases **1** through **4** follow immediately. To illustrate how, we briefly discuss Case **3**. Here $a_{11}$ and $a_{12}$ are set to 0. Since $a_{13}$ and $a_{22}$ are assumed to be nonzero, for there to exist integral points at all, it must be the case that the ranges $Zw(a_{13})$ and $Zw(a_{22})$ of $a_{13}$ and $a_{22}$, respectively, are $\gg 1$. This implies that the range $Zw(a_{ij}) \gg 1$ for all $(i,j)$ not equal to $(1,1)$ or $(1,2)$. Hence, the number of possibilities for all the coefficients $a_{ij}$ other than $a_{24}$ is $\ll$

$$\prod_{(i,j)\notin\{(1,1),(1,2),(2,4)\}} Zw(a_{ij}) = s_1^6s_2^4s_3^2Z^7,$$

as necessary. (When $a_{34}$ or $a_{44}$ is the excluded coefficient instead of $a_{24}$, the computation is similar and produces a better bound since we have $s_i \gg 1$.) This yields Case **3**, and Cases **1**, **2**, and **4** are similar.

Next, assume that $a_{11} = a_{12} = a_{13} = 0$. Then for $\det A$ to be nonzero, we must have $a_{14} = \pm 1$, and so

$$1 = \det A = \det \begin{bmatrix} a_{22} & a_{23} \\ a_{23} & a_{33} \end{bmatrix} \tag{4.35}$$

The coefficients $a_{24}$, $a_{34}$, and $a_{44}$ run freely and do not affect $\det A$. When $a_{22}$ is nonzero, as in Case **5**, we fiber over $a_{22}$ and $a_{23}$, and note that $a_{33}$ is then determined by the determinant condition to yield the result. When $a_{22} = 0$, as in Case **6**, we must have $a_{23} = \pm 1$. Then we fiber over $a_{33}$ to obtain the result.

We now turn out attention to the bottom part of the table. In each case, we will fiber over the coefficients $b_{11}$, $b_{12}$, $b_{13}$, and $b_{14}$, and use Lemma 123 to determine the number of possibilities of $B$ modulo $a$ given these coefficients. Then, for each fixed $b_{11}$, $b_{12}$, $b_{13}$, $b_{14}$, and $\bar{B} \pmod a$, we count the number of possibilities for $B$ as follows: Let $d = \gcd(b_{11}, b_{12}, b_{13}, b_{14}, b_1)$, where $b_1$ is the product of primes dividing $b$ which do not divide $a$. From Lemma 125 it follows that the density of possible $b_{22}, b_{23}, b_{24}, b_{33}, b_{34}, b_{44}$ is $\ll b^{-1}b_1^{-1}d$. It follows that the number of choices for the possible values $B$ is $\ll$

$$\prod_{(i,j):i\geq 2} \max\Big(\frac{Zw(b_{ij})}{f_{ij}}, 1\Big),$$

where $f_{ij}$ are factors one of which is $ab$, one of which is $ab_1/d$, and the rest are $a$. Since $ab \ll Z$, it follows that

$$\begin{aligned} \prod_{(i,j):i\geq 2} \max\Big(\frac{Zw(b_{ij})}{f_{ij}}, 1\Big) &\ll_\epsilon Z^{6+\epsilon} a^{-6} b^{-1} b_1^{-1} d s_1^6 s_2^4 s_3^{10} M(s) \\ &= d\mu(a,b) Z^{6+\epsilon} s_1^6 s_2^4 s_3^{10} M(s). \end{aligned} \tag{4.36}$$

Note that the $d/b_1$-density condition must necessarily be independent of the mod $a$ densities arising from the fact that $B \pmod a$ is fixed since $\gcd(a, b_1) = 1$.

Let $\Sigma_a$ be the set of primes dividing $a$. For a subset $S \subset \Sigma_a$, let $\overline{S} := \Sigma_a \smallsetminus S$, let $\Pi(S)$

be the set of positive integers divisible only by primes in $S$, and let $a_S$ be the part of $a$ coprime to every element of $S$. Turning now to Case **a**, Lemma 123 implies that the number of choices for $b_{11}$, $b_{12}$, $b_{13}$, and $b_{14}$, weighted by the number of arising possibilities for $B \pmod a$, such that $\gcd(b_{11}, b_{12}, b_{13}, b_{14}, b_1) = d$ is $\ll_\epsilon$

$$\sum_{S \subset \Sigma_a} \sum_{\substack{q \in \Pi(\overline{S}) \\ q^2 | a}} \sum_{\substack{q' \in \Pi(S) \\ q' | a_{\overline{S}} | q'^2}} \sum_{\substack{b_{1j} \ll Zw(b_{1j}) \\ dq^2 a_{\overline{S}} | b_{11}, dqq' | b_{1j}}} q^5 a_{\overline{S}} q'^2 \ll_\epsilon \frac{Z^{4+\epsilon}}{d^4} w(b_{11}) w(b_{12}) w(b_{13}) w(b_{14}) = \frac{Z^{4+\epsilon}}{d^4} s_1^{-12} s_2^{-4} s_3^{-4}.$$

Multiplying by the right-hand side of (4.36) and summing over $d \mid b_1$ yields the result for Case **a**.

Similarly, the numbers of choices for $b_{11}$, $b_{12}$, $b_{13}$, and $b_{14}$ with $\gcd(b_{11}, b_{12}, b_{13}, b_{14}, b_1) = d$, weighted by the number of possibilities for $A \pmod a$, in Cases **b**, **c** are respectively $\ll_\epsilon$

$$\sum_{S \subset \Sigma_a} \sum_{\substack{q' \in \Pi(S) \\ q' | a_S | q'^2}} \sum_{\substack{db_{12}, db_{13}, db_{14} \\ q' | b_{1j}}} a_S q'^2 \ll_\epsilon \frac{Z^{3+\epsilon}}{d^3} \frac{w(b_{12}) w(b_{13}) w(b_{14})}{q'^3} a q'^2 \ll_\epsilon \frac{Z^{3+\epsilon}}{d^3} a^{1/2} s_1^{-6} s_2^{-2} s_3^{-2},$$

$$\sum_{S \subset \Sigma_a} \sum_{\substack{q' \in \Pi(S) \\ q' | a_S | q'^2}} \sum_{\substack{db_{13}, db_{14} \\ q' | b_{1j}}} a_S q'^2 \ll_\epsilon \frac{Z^{1+\epsilon}}{d} \max\left\{ \frac{Z w(b_{13})}{q'}, 1 \right\} \frac{w(b_{14})}{q'} a q'^2 \ll_\epsilon \frac{Z^{2+\epsilon}}{d} a s_1^{-2} s_3^2.$$

Once again, multiplying by the right-hand side of (4.36) and summing over $d \mid b_1$ yields the result for Cases **b** and **c**. This concludes the proof of the lemma. □

For positive real numbers $X$ and $Y$, and $\gamma \in \mathrm{SL}_4(\mathbb{R})$, we define the quantity

$$N(\gamma; X, Y) := \#\big\{(A, B) \in \mathcal{D}(U_1(\mathbb{Z}); \gamma, X) \times \mathcal{D}(\mathcal{L}_{a,b}; \gamma, Y) : (A, B) \text{ is non-distinguished}\big\}.$$

We now have the following result.

**Proposition 127.** *Let $Y \gg X \geq 1$ be real numbers, and fix $\gamma = n(s_1, s_2, s_3)k \in \mathcal{F}_4$. Let $a$ and $b$ be positive integers such that $ab \ll Y$. Then we have that*

$$N(\gamma; X, Y) \ll_\epsilon \mu(a, b) X^9 Y^{10+\epsilon} s_1^{12} s_2^8 s_3^{12}.$$

*Proof.* We partition $U_1(\mathbb{Z})$ into the first six sets listed in the second column of Table 126, and partition $\mathcal{L}_{a,b}$ into the last three sets listed in the second column of Table 126. This gives us 18 cases to consider, and we label these cases **1a** through **6c**. A pair $(A, B) \in W_4(\mathbb{Z})$ with $\det A = 1$ and $a_{11} = a_{12} = a_{22} = b_{11} = b_{12} = 0$ is automatically distinguished, and so Cases **4c** and **6c** can be discarded.

Continuing with the **c**'s, note that the bound for Case **1c** follows directly from the relevant third column bounds of Lemma 126 and the inequality $a \ll Y$. The bound for Case **2c** follows directly from the relevant third column bounds, along with the relevant fourth column inequality and the inequality $a \ll Y$. The bound for Case **3c** follows directly from the relevant third column bounds, fourth column inequalities, and the inequalities $X \ll Y$ and $a \ll Y$. For Case **5c**, we observe that any pair $(A, B) \in W_4(\mathbb{Z})$ with $\det A = 1$ and $a_{11} = a_{12} = a_{13} = b_{11} = b_{12} = b_{13} = 0$ is automatically distinguished. This observation has two consequences: first, we may assume that $s_1^2 s_3^2 \ll Y$, and second, the bound for the number of eligible forms $B$ given in Lemma 126 can be improved to $a\mu(a,b)s_1^2 s_2^4 s_3^{10} M(s) Y^{8+\epsilon}$. Using these consequences along with the relevant fourth column inequalities and the inequalities $a \ll Y$ and $s_1^2 s_3^2 \ll Y$ yields Case **5c**.

We now move along to the **a**'s and **b**'s. It is easy to check that Cases **1a**, **2a**, **3a**, **4a**, **5a**, **1b**, **2b**, and **3b** follow directly from the bounds in the second column of Table 126. Case **6a** follows from the bound in the second column together with the inequality $s_3^2 \ll s_1^2 X$. Similarly, Case **5b** follows from the bound in the second column together with the inequalities $s_1^2 \ll s_3^2 X$ and $s_2^2 s_3^2 \ll s_1^2 X$, which should be used to make the powers of $s_1$ and $s_3$ equal in the product $\sqrt{a}\mu(a,b)X^5 Y^9 s_1^{10} s_2^4 s_3^{14} M(s)$.

This only leaves Case **6b**, which is the most intricate case stemming from the difficulty in controlling the exponent of $s_2$. We proceed as follows: Since $a_{11} = a_{12} = a_{22} = 0$, it follows that the quadratic form $Q(x,y) = b_{11}x^2 + b_{12}xy + b_{22}y^2$ must have nonzero discriminant for the pair $(A, B)$ to be irreducible. However, since $B \in \mathcal{L}_a$, it follows that $a \mid \Delta(Q)$, and in particular $|\Delta(Q)| \geq a$. Therefore, it follows that $Y^2 w(b_{12})^2 = Y^2 s_1^{-4} s_2^{-4} s_3^{-4} \gg a$, or

$s_1^2 s_2^2 s_3^2 \ll Y a^{-1/2}$. Denote the set

$$\mathcal{D}(U_1(\mathbb{Z})(\{a_{11}, a_{12}, a_{13}, a_{22}\}; \emptyset); \gamma, X) \times \mathcal{D}(\mathcal{L}_{a,b}(\{a_{11}\}, \{a_{12}\}); \gamma, Y)$$

by $T$. Now, from the bounds in the third column of Table 126, it follows that we have

$$\begin{aligned} \#\big\{(A,B) \in T : (A,B) \text{ is non-dist.}\big\} &\ll \sqrt{a}\mu(a,b) X^4 Y^9 s_1^8 s_2^8 s_3^{16} M(s) \\ &\ll \mu(a,b) X^4 Y^{10} s_1^6 s_2^6 s_3^{14} M(s), \end{aligned}$$

where the final inequality follows by multiplying the right-hand side of the first line by $Y a^{-1/2} s_1^{-2} s_2^{-2} s_3^{-2} \gg 1$. Using the inequalities $s_1^2 \ll X s_3^2$ and $s_3^2 \ll X s_1^2$ to ensure that the exponents of $s_1$ and $s_3$ in $s_1^6 s_3^{14} M(s)$ are equal, we obtain the required bound in Case **6b** as well. This concludes the proof of the proposition. □

We are now ready to prove Theorem 120:

**Proof of Theorem 120:** Let $T$ denote the characteristic function of the set of non-distinguished elements $(A, B) \in W_4(\mathbb{Z})$ that are special at $a$ and satisfy $\det A = 1$. Then we clearly have that

$$N_\psi(W_{\mathscr{A}_4}^{(i,j)}, T_a; X, Y) \leq N_\psi(W^{(i,j)}, T; X, Y).$$

From Proposition 117, it follows that we have

$$N_\psi(W^{(i,j)}, T; X, Y) \ll \int_{\gamma \in \mathcal{F}_4} \Big( \sum_{w \in W_4(\mathbb{Z})} T(w) \big(\gamma \cdot \Phi[Y^{-1/2} X^{1/4}, Y^{1/2} X^{1/4}]\big)(w) \Big) d\gamma \ll$$

$$\int_{\gamma \in \mathcal{F}_4} \#\big\{(A,B) \in \mathcal{D}\big(U_1(\mathbb{Z}); \gamma, \tfrac{X^{1/4}}{\sqrt{Y}}\big) \times \mathcal{D}(\mathcal{S}_a; \gamma, \sqrt{Y} X^{1/4}) \cap W_4(\mathbb{Z}) : (A,B) \text{ is non-dist.}\big\} d\gamma,$$

as long as $\mathcal{D} \subset U_4(\mathbb{R})$ is large enough that $\mathcal{D} \times \mathcal{D}$ contains the support of the compactly supported function $\Phi$, and where $\mathcal{S}_a$ denotes the set of elements $B \in U_4(\mathbb{Z})$ that are special at $a$.

By Proposition 112, we may write

$$\mathcal{S}_a = \bigcup_{b,c,d} b\mathcal{L}_{c,d},$$

where $b$, $c$, and $d$, are integers dividing $a$ that satisfy the following property: for each prime $p$ dividing $a$ with $p^k \| a$, there exist nonnegative integers $\alpha$ and $\beta$ such that $p^\alpha \| b$, $p^{k-2\alpha+\beta} \| c$, $p^{\alpha-2\beta} \| d$, $k - 2\alpha + \beta \geq 0$, and $\alpha \geq 2\beta$. Applying Proposition 127, on each triple $(b, c, d)$ (to apply the proposition for the set $b\mathcal{L}_{c,d}$ rather than $\mathcal{L}_{c,d}$, we simply divide each $B$ by $b$), we therefore obtain

$$\begin{aligned} N_\psi(W_{\mathscr{A}_4}^{(i,j)}, T_a; X, Y) &\ll_\epsilon \sum_{b,c,d} \int_{\substack{s_1,s_2,s_3 \gg 1 \\ s_i \ll X}} b^{-10}\mu(c,d)(Y^{-1/2}X^{1/4})^9 (Y^{1/2}X^{1/4})^{10+\epsilon} d^\times s \\ &\ll_\epsilon \sum_{b,c,d} b^{-10}\mu(c,d) X^{5-1/4+\epsilon} Y^{1/2}, \end{aligned} \tag{4.37}$$

since the term $s_1^{12}s_2^8s_3^{12}$ in Proposition 127 exactly cancels out with the Haar-measure factor. If $p^k \| a$, then the contribution from $p$ to $b^{-10}\mu(c,d)$ is easily checked to be

$$\begin{cases} p^{-6k+\alpha-4\beta+1}, & \text{if } k - 2\alpha + \beta = 0,\ \alpha - 2\beta > 0; \\ p^{-6k+\alpha-4\beta}, & \text{otherwise.} \end{cases}$$

We claim that the contribution from $p$ to $b^{-10}\mu(c,d)$ is $\leq$ the contribution of $p$ to $\nu(a)$ for each $k \geq 1$. Since $\alpha \leq k/2 + \beta/2$, this follows when $k \geq 4$. When $k = 1$, we must have $\alpha = \beta = 0$, and the claim follows. When $k = 2$ or $k = 3$, we either have $\alpha = \beta = 0$, or $\alpha = 1$ and $\beta = 0$. The claim is easily checked in all these cases. Therefore, we have $b^{-10}\mu(c,d) \leq \nu(a)$. Finally, since the number of triples $(b, c, d)$ being summed over is $O_\epsilon(a^\epsilon) = O_\epsilon(X^\epsilon)$, the result follows from (4.37). $\square$

### 4.5.2 Fourier analysis on the space of $n \times n$ symmetric matrices

In this section, we collect some Fourier analytic results on the space of quadratic forms. Since our results apply generally, we will work with the space $U_n$, for integers $n \geq 2$, specializing only occasionally to the space of quaternary quadratic forms.

#### 4.5.2.1 Preliminary definitions and results

Let $n \geq 2$ be an integer. For an integer $N$, let $\widehat{U_n(\mathbb{Z}/N\mathbb{Z})}$ be the Pontryagin dual of $U_n(\mathbb{Z}/N\mathbb{Z})$. Then $\widehat{U_n(\mathbb{Z}/N\mathbb{Z})}$ can be identified with $U_n(\mathbb{Z}/N\mathbb{Z}) = (\mathbb{Z}/N\mathbb{Z})^n$, where $D := \frac{n(n+1)}{2}$. We write elements $\chi \in \widehat{U_n(\mathbb{Z}/N\mathbb{Z})}$ as $D$-tuples $\chi = (\check{a}_{ij})_{1 \leq i \leq j \leq n}$ via the identification

$$\chi(B) := e\Big(\frac{\sum_{i,j} \check{a}_{ij} b_{ij}}{N}\Big) = \prod_{i,j} e\Big(\frac{\check{a}_{ij} b_{ij}}{N}\Big),$$

where $B = (b_{ij})_{i,j} \in U_n(\mathbb{Z}/N\mathbb{Z})$ and $e(x) := e^{2\pi i x}$. We also consider elements $\check{A} = [\check{a}_{ij}] \in \widehat{U_n(\mathbb{Z}/N\mathbb{Z})}$ as $n \times n$ symmetric matrices by regarding the $\check{a}_{ij}$ as the matrix entries.

For a function $\phi \colon U_n(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{C}$, we recall the definition of $\widehat{\phi} \colon \widehat{U_n(\mathbb{Z}/N\mathbb{Z})} \to \mathbb{C}$, the Fourier dual of $\phi$:

$$\widehat{\phi}(\chi) = \sum_{B \in U_n(\mathbb{Z}/N\mathbb{Z})} \phi(B)\chi(B).$$

Fourier duality then implies the equality

$$\frac{1}{N^D} \sum_{\chi} \widehat{\phi}(\chi)\overline{\chi(f)} = \phi(f).$$

Let $\widehat{U_n(\mathbb{Z})}$ denote the lattice in $U_n(\mathbb{R})$ dual to $U_n(\mathbb{Z})$. For every positive integer $N$, we have a natural identification of $\widehat{U_n(\mathbb{Z})}/N\widehat{U_n(\mathbb{Z})}$ with $\widehat{U_n(\mathbb{Z}/N\mathbb{Z})}$. The following result is a consequence of Poisson summation.

**Proposition 128.** *Let $\psi \colon U_n(\mathbb{R}) \to \mathbb{R}$ denote a smooth function with super polynomial decay. Let $N$ be a positive integer, and let $\phi \colon U_n(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{R}$ be any function. Then, for*

*positive real numbers $Y_{ij}$, we have*

$$\sum_{B=(b_{ij})\in U_n(\mathbb{Z}/N\mathbb{Z})} \psi\Big(\frac{b_{ij}}{Y_{ij}}\Big)\phi(B) = \frac{\prod_{i,j} Y_{ij}}{N^D} \sum_{\chi=(\check{a}_{ij})\in\widehat{U_n(\mathbb{Z})}} \widehat{\psi}\Big(\frac{Y_{ij}\check{a}_{ij}}{N}\Big)\widehat{\phi}(\chi).$$

#### 4.5.2.2 The Fourier transform of the set of rank-1 quadratic forms modulo a prime $p$

Let $p$ be an odd prime number. In the following result, we estimate the Fourier transform of the characteristic function $S\colon U_n(\mathbb{Z}/p\mathbb{Z}) \to \{0,1\}$ of the set of elements in $U_n(\mathbb{Z}/p\mathbb{Z})$ that are of rank $\leq 1$ modulo $p$.

**Proposition 129.** *With notation as above, we have the following bounds on $\widehat{S}$:*

$$|\widehat{S}(\chi)| \ll p^{n-\frac{\mathrm{rank}(\chi)}{2}}.$$

*Proof.* Let $\chi = (\check{a})_{ij}$ correspond to the quaternary quadratic form $\check{A}$. Since $S$ is $\mathrm{GL}_n(\mathbb{F}_p)$-invariant, it follows that for any $\gamma \in \mathrm{GL}_n(\mathbb{F}_p)$, we have $\widehat{S}(\chi) = \widehat{S}(\gamma\chi)$. Thus, we may assume that $\check{A}$ is diagonal, with coefficients $\alpha_1, \ldots, \alpha_n$. The support of $S$ is precisely the set

$$\{B = \gamma(\beta_1 x_1 + \cdots + \beta_n x_n)^2 : \gamma \in \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}, \beta_1, \ldots, \beta_n \in \mathbb{F}_p\}.$$

With $\chi$ and $B$ as above, we have $\chi(B) = e\Big(\frac{\sum \alpha_i\gamma\beta_i^2}{p}\Big)$. Therefore, we have that

$$\widehat{S}(\chi) \ll \sum_{\beta_i\in\mathbb{F}_p} e\Big(\frac{\sum \alpha_i\beta_i^2}{p}\Big) = \prod_{i=1}^n \sum_{\beta_i\in\mathbb{F}_p} e\Big(\frac{\alpha_i\beta_i^2}{p}\Big) = \prod_{i=1}^n g(\alpha_i, p),$$

where $g(\alpha_i, p)$ denotes the quadratic Gauss sum modulo $p$. Since we know that $|g(\alpha_i, p)|$ is $\sqrt{p}$ when $\alpha_i \neq 0$ and $p$ when $\alpha = 0$, the result follows. □

**Bounding the Fourier transform of certain smooth functions**

Let $\psi\colon V_4(\mathbb{R}) \to \mathbb{R}$ and $\Phi\colon \mathrm{PSO}_A(\mathbb{R}) \to \mathbb{R}$ be fixed smooth, compactly supported functions. Let $X, Y$ be real numbers with $0 < Y \ll X^{1/2}$. Recall that we restrict $\psi_X[Y]$ to $V_1(\mathbb{R})$, obtaining a smooth, compactly supported function $\psi_{X,Y}\colon V_1(\mathbb{R}) \to \mathbb{R}$. We then wrote $\mathcal{S}(\psi_{X,Y}, \Phi)$ for $\Phi_{X,Y}$. Finally, we wrote $\psi_{X,Y}[Y/X]$ and $\Phi_{X,Y}[Y/X]$, respectively, for $\psi^{(X,Y)}$ and $\Phi^{(X,Y)}$. Next, we estimate the Fourier transform of $\Phi^{(X,Y)}$:

**Lemma 130.** *The $m$th partial derivatives of $\Phi^{(X,Y)}$ are bounded by $O(X^{3m}/Y^{6m})$.*

*Proof.* It is immediately seen that $\Phi^{(X,Y)} = \mathcal{S}(\psi_{X,Y}\{Y/X\}, \Phi)$. Thus, the lemma follows from bounds on the derivatives of $\psi_{X,Y}\{Y/X\}$, which can be computed using the chain rule. □

As a standard consequence of the above lemma, we obtain the following result.

**Proposition 131.** *Let $Z$ denote $X^3/Y^6$. The Fourier transform of $\Phi^{(X,Y)}$ satisfies*

$$|\widehat{\Phi^{(X,Y)}}(\check{A})| \ll_M \frac{Z^M}{|\check{A}|^M},$$

*where $|\check{A}|$ denotes the $L^1$-norm of $A$.*

### 4.5.3 Counting special $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})$-orbits on $W_{\mathscr{A}_4}(\mathbb{Z})$

Let $\Phi\colon W_{\mathscr{A}_4}(\mathbb{R}) \to \mathbb{R}$ be a smooth function. Given a function $T\colon W_{\mathscr{A}_4}(\mathbb{Z}) \to \mathbb{R}$ that is $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})$-invariant, we define

$$N_\Phi(T; X) := \int_{\gamma \in \mathcal{F}_A} \Big( \sum_{B \in W_{\mathscr{A}_4}(\mathbb{Z})^{\mathrm{gen}}} T(B) \cdot (\gamma \cdot \Phi)(B/X) \Big) d\gamma. \tag{4.38}$$

Above, we take $d\gamma = s_1^{-2} s_2^{-2} dn d^\times s_1 d^\times s_2 dk$ for $\gamma = n(s_1, s_2)k$ in Iwasawa coordinates. Write $n(s_1, s_2)k = (s_1, s_2)n(s)k$ for $k \in K_{\mathscr{A}_4}$, $n \in N'$ and $(s_1, s_2) \in T'$. It is easily checked that $n(s)$ has absolutely bounded coefficients. Then for $\gamma = n(s_1, s_2)k$, we have $\gamma \cdot \Phi = (s_1, s_2) \cdot \Phi_{n(s)k}$, where $\Phi_{n(s)k}$ is smooth and has compact support independent of $(n, s) \in \mathcal{F}_{\mathscr{A}_4}$.

We assume that $T$ is bounded and $(X^\theta, X)$-acceptable, i.e., $T$ is defined via congruence conditions modulo two relatively prime positive integers $b \ll X^\theta$ and $q \ll X$, where $q$ is squarefree and the congruence condition modulo $q$ is simply the one which cuts out the elements having rank $\leq 1$ modulo $q$. For such functions $T$, we estimate $N_\Phi(T; X)$ in the following three steps: first, we bound the number of non-distinguished points in the cuspidal region of the integral. Second, we bound the number of non generic elements in the main ball of the integral. Third, we estimate the number of integer points in the main ball of the integral.

#### 4.5.3.1 Bounding the number of integer points in the cusp

Let $0 < q \ll X$ be squarefree, let $\mathcal{L}_q := \{B \in W_{\mathscr{A}_4}(\mathbb{Z}) : B \text{ is of rank} \leq 1 \text{ modulo } q\}$, and let $\mathcal{L}_q^{\mathrm{nd}}$ be the set of non-distinguished elements in $\mathcal{L}_q$. We prove the following result:

**Proposition 132.** *Fix $0 < \delta_1 < 1/4$. Then we have*

$$\int_{\substack{nsk\in\gamma\in\mathcal{F}_A \\ \max(s_1,s_2)\gg X^{\delta_1}}} \Big( \sum_{B\in\mathcal{L}_q^{\mathrm{nd}}} (\gamma\cdot\Phi)(B/X)\Big) d\gamma \ll_\epsilon \frac{X^{10-2\delta_1+\epsilon}}{q^6}.$$

We start by proving the following lemmas:

**Lemma 133.** *Every $B \in \mathcal{L}_q$ with $|b_{12}^2 - b_{11}b_{22}| < q$ is distinguished.*

*Proof.* The binary quadratic form $b_{11}x^2 + b_{12}xy + b_{22}y^2$ is a square modulo $q$ since $B$ belongs to $\mathcal{L}_q$. Hence, the discriminant $\Delta = b_{12}^2 - b_{11}b_{22}$ is divisible by $q$. The condition of the lemma now implies that $\Delta = 0$, and hence that $b_{11}x^2 + b_{12}xy + b_{22}y^2$ is a multiple of the square of a linear form. Thus, $B$ is distinguished. □

**Lemma 134.** *Let $1 \ll Y_1 \ll Y_2 \ll Y_3$ be positive real numbers such that $Y_2^2 \asymp Y_1Y_3$. Then the number of integer triples $(a_1, a_2, a_3) \in \mathbb{Z}^3$ such that $q \mid a_2^2 - a_1a_3$ and $|a_i| \ll Y_i$ is bounded by $O_\epsilon(Y_2(Y_1Y_3)^\epsilon(1 + Y_1Y_3/q))$.*

*Proof.* There are $O(Y_2)$ choices for $a_2$. Once we fix $a_2$, we have $a_1a_3 = a_2^2 + kq$ for some integer $k$. There are $O(1 + Y_1Y_3/q)$ choices for $k$. For each choice of $k$, the pair $(a_1, a_3)$ is fixed up to $(Y_1Y_3)^\epsilon$ choices. □

Let $\mathcal{L}^{\mathrm{nd}}_{q,b_{11}=0}$ and $\mathcal{L}^{\mathrm{nd}}_{q,b_{11}\neq 0}$ denote the subsets of $\mathcal{L}^{\mathrm{nd}}_q$ consisting of elements $(\mathscr{A}_4, B)$ with $b_{11} = 0$ and $b_{11} \neq 0$, respectively. For each divisor $q' \mid q$, let $\mathcal{L}^{\mathrm{nd}}_{q,b_{11}\neq 0}(q') = \{B \in \mathcal{L}^{\mathrm{nd}}_{q,b_{11}\neq 0} : q' \mid b_{11}(B)\}$. We have the following consequence of Lemma 134:

**Corollary 135.** *Write $\phi = \Phi_{n(s)k}$ for $n \in N'$, $s = (s_1, s_2) \in T'$. Then for $s_1 > s_2$ with $w(b_{11})X \gg q'$, we have*

$$\sum_{B \in \mathcal{L}^{\mathrm{nd}}_{q,b_{11}\neq 0}(q')} ((s_1, s_2) \cdot \phi_X)(B) \ll_\epsilon \frac{X^{10+\epsilon}}{q^6} + \frac{X^{8+\epsilon}s_1^4}{q^5}.$$

*Proof.* We fiber over $b_{11}$, $b_{12}$, $b_{22}$, $b_{13}$, and $b_{14}$. Since the binary quadratic form $b_{11}x^2 + b_{12}xy + b_{22}y^2$ is a square modulo $q$, Lemma 134 implies that the number of options for the triple $(b_{11}, b_{12}, b_{22})$ is bounded by $O_\epsilon(X^{1+\epsilon}(1/(q's_1^2) + X^2/(q'qs_1^6)))$. The number of options for the pair $(b_{13}, b_{14})$ is bounded by $O(X^2/(q'^2s_2^2))$.

Once these coefficients have been fixed, Corollary 124 implies that $B$ is determined modulo $q$ up to $O_\epsilon(q'^3q^\epsilon)$ choices. Since $Xw(b_{ij}) \gg X \gg q$ for the remaining coefficients, it is clear that we have

$$\sum_{B \in \mathcal{L}^{\mathrm{nd}}_{q,b_{11}\neq 0}(q')} ((s_1, s_2) \cdot \phi_X)(B) \ll_\epsilon X^{1+\epsilon}\Big(\frac{1}{q's_1^2} + \frac{X^2}{q'qs_1^6}\Big) \cdot \frac{X^2}{q'^2s_2^2} \cdot \frac{X^5q'^3q^\epsilon s_1^6 s_2^2}{q^5},$$

as necessary. □

We are now in position to prove Proposition 132.

**Proof of Proposition 132:** By symmetry, we may assume that $s_1 > s_2$ for $\gamma = n(s_1, s_2)k \in \mathcal{F}_{\mathscr{A}_4}$. Moreover, by Lemma 133, we may assume that $s_1 \ll X^{1/2}/q^{1/4}$. Thus, stratifying the set $\mathcal{L}^{\mathrm{nd}}_{q,b_{11}\neq 0}$ with the subsets $\mathcal{L}^{\mathrm{nd}}_{q,b_{11}\neq 0}(q')$ for $q' \mid q$ and applying Corollary 135 to each stratum,

we obtain

$$\int_{\substack{nsk\in\gamma\in\mathcal{F}_A\\ \max(s_1,s_2)\gg X^{\delta_1}}} \Big(\sum_{B\in\mathcal{L}^{\mathrm{nd}}_{q,b_{11}\neq 0}} (\gamma\cdot\Phi)(B/X)\Big)d\gamma \ll_\epsilon$$
$$q^\epsilon \int_{s_1\gg X^{\delta_1}}^{X^{1/2}/q^{1/4}}\int_{s_2=1}^{s_1}\Big(\frac{X^{10+\epsilon}}{q^6}+\frac{X^{8+\epsilon}s_1^4}{q^5}\Big)s_1^{-2}s_2^{-2}d^\times s_1 d^\times s_2,$$

which is sufficient.

Next suppose that $B\in\mathcal{L}^{\mathrm{nd}}_q$ with $b_{11}=0$. Then $b_{1j}\neq 0$ for $j\in\{2,3\}$ and $q$ divides $b_{1j}$ for $j\in\{2,3,4\}$. It follows that $Xw(b_{1j})\gg q$ for $j\in\{2,3,4\}$, which in turn implies that $Xw(b_{ij})\gg q$ for all $(i,j)\neq(1,1)$. Under these conditions, there are $\ll X^3w(b_{12})w(b_{13})w(b_{14})/q^3$ options for the tuple $(0=b_{11},b_{12},b_{13},b_{14})$. Once such a tuple has been fixed, it determines $B$ modulo $q$ up to $O_\epsilon(q^{3+\epsilon})$ choices by Corollary 124. Thus, we have

$$\begin{aligned}\int_{\substack{nsk\in\gamma\in\mathcal{F}_A\\ \max(s_1,s_2)\gg X^{\delta_1}}} \Big(\sum_{B\in\mathcal{L}^{\mathrm{nd}}_{q,b_{11}=0}} (\gamma\cdot\Phi)(B/X)\Big)d\gamma &\ll_\epsilon \int_{s_1\gg X^{\delta_1}}^{X^{1/2}/q^{1/2}}\int_{s_2=1}^{s_1}\frac{X^{9+\epsilon}}{q^6}w(b_{11})^{-1}s_1^{-2}s_2^{-2}d^\times s_1 d^\times s_2\\ &\ll_\epsilon \frac{X^{9+\epsilon}}{q^6},\end{aligned}$$

which is also sufficient. This concludes the proof of the proposition. □

#### 4.5.3.2 Bounding the number of non-distinguished elements in the main ball

Let $0<q\ll X$ be an integer (not necessarily squarefree), let $\mathcal{S}_q:=\{B\in W_{\mathscr{A}_4}(\mathbb{Z}): B \text{ is special at } q\}$, and for a set $S\subset W_{\mathscr{A}_4}(\mathbb{Z})$, let $S^{\mathrm{ngen}}$ denote the set of *non-generic* elements in $S$ (i.e., the set of elements in $S$ that are distinguished or have a non-trivial stabilizer in $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Q})$). The following result bounds the number of non-generic elements in the main ball.

**Proposition 136.** *Let $\delta_1>0$ be sufficiently small. Then, for a constant $\kappa>0$ independent of $\delta_1$, we have that*

$$\int_{\substack{nsk\in\gamma\in\mathcal{F}_A\\ \max(s_1,s_2)\ll X^{\delta_1}}} \Big(\sum_{B\in\mathcal{S}_q^{\mathrm{ngen}}} (\gamma\cdot\Phi_X)(B)\Big)d\gamma = O\Big(\frac{X^{10-\kappa}}{q^6}\Big).$$

*Proof.* It is a consequence of [78, Corollary 1.2] that the density of $\mathcal{S}_q$ in $W_{\mathscr{A}_4}(\mathbb{Z})$ is $O(q^{-6})$. The result then follows from using the Selberg sieve applied as in [104]. The only additional ingredient needed to apply the sieve is to show that for every prime $p > 2$, there exists a set $T_p$ (resp., $T_p'$) contained in $W_{\mathscr{A}_4}(\mathbb{F}_p)$ satisfying the following two properties: (1) every $B \in W_{\mathscr{A}_4}(\mathbb{Z})$ whose reduction modulo $p$ lies in $T_p$ (resp., $T_p'$) is non-distinguished (resp., has trivial stabilizer in $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Q})$); and (2) the size $\#T_p$ (resp., $\#T_p'$) is $\gg p^{10}$.

We now construct the sets $T_p$ and $T_p'$. For any separable monic binary quartic form $f \in V_1(\mathbb{F}_p)$, it follows from [105, Proposition 14] that the set of $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{F}_p)$-orbits on $W_{\mathscr{A}_4}(\mathbb{F}_p)$ with resolvent $f$ is in bijection with $J_f(\mathbb{F}_p)/2J_f(\mathbb{F}_p)$. It further follows from [105, Equation (8)] that the stabilizer of any element of such an orbit is isomorphic to $J_f(\mathbb{F}_p)[2]$. Thus, we can take $T_p$ to be the set of all $B \in W_{\mathscr{A}_4}(\mathbb{F}_p)$ with separable resolvent $\iota(B) = f$ corresponding to a non-trivial element of $J_f(\mathbb{F}_p)/2J_f(\mathbb{F}_p)$. Similarly, we can take $T_p'$ to be the set of all forms $B \in W_{\mathscr{A}_4}(\mathbb{F}_p)$ with separable resolvent $\iota(B) = f$ such that $J_f(\mathbb{F}_p)[2]$ is trivial.

It remains to show that the sizes of $T_p$ and $T_p'$ satisfy the required lower bounds. Recall that for any separable form $f \in V_1(\mathbb{F}_p)$, the 2-torsion subgroup $J_f[2]$ depends only on the splitting type of $f$ over $\mathbb{F}_p$. Since each unramified splitting type occurs with positive proportion (where by "positive," we mean "positive in the large-$p$ limit"), it follows from the orbit-stabilizer theorem that the set $T_p$ (resp., $T_p'$) comprises a positive proportion of $W_{\mathscr{A}_4}(\mathbb{F}_p)$—i.e., we have $\#T_p \gg p^{10}$ (resp., $\#T_p' \gg p^{10}$), as necessary. □

#### 4.5.3.3 Estimating the number of integer points in the main ball

Assume the Fourier transform of a smooth, compactly supported function $\Phi\colon W_{\mathscr{A}_4}(\mathbb{R})^{(i,j)} \to \mathbb{R}$ satisfies the bound $\widehat{\Phi}(\check{A}) \ll_M Z^M/|\check{A}|^M$, for some real number $Z > 0$. Then, for $\gamma = n(s_1, s_2)k \in \mathcal{F}_{\mathscr{A}_4}$, Proposition 128 gives

$$\sum_{B \in W_{\mathscr{A}_4}(\mathbb{Z})^{(i,j)}} T(B) \cdot ((s_1, s_2)\Phi_{n(s)k})(B/X) = X^{10}\widehat{\Phi}(0)\nu(T) + E. \tag{4.39}$$

The error term $E$ above is bounded by

$$\begin{aligned} E &\ll_\epsilon \frac{X^{10}}{(bq)^{10}} \sum_{\substack{0\neq \check{A}\in \widehat{W(\mathbb{Z})} \\ |\check{a}_{ij}|\ll (Zbq)^{1+\epsilon}/(Xw(b_{ij}))}} |\widehat{T}(\check{A})| \\ &\ll_\epsilon \frac{X^{10}}{(bq)^{10}} \cdot \frac{(Zbq)^{10+\epsilon}}{X^{10}} \max(s_1,s_2)^6 \min(s_1,s_2)^2 \cdot q^{7/2+\epsilon} b^{10} \qquad (4.40) \\ &\ll_\epsilon \max(s_1,s_2)^6 \min(s_1,s_2)^2 \cdot (Zb)^{10+\epsilon} q^{7/2+\epsilon}, \end{aligned}$$

where we use Proposition 129 to bound the value of $|\widehat{T}(\check{A})|$ by $q^{7/2+\epsilon}$ when $\check{A}$ is not 0 modulo $p$ for any $p$ dividing $q$. If the gcd of $q$ and all of the coefficients of $\check{A}$ is $q_1$, then we have a bound of $q^{7/2+\epsilon} q_1^{1/2}$ on $|\widehat{T}(\check{A})|$. However, we recover the required bound from the fact that every coefficient of such $\check{A}$ is a multiple of $q_1$, thereby shortening the sum over $\check{A}$.

We are ready to estimate $N_\Phi(T;X)$:

**Proposition 137.** *Let notation be as above. Then we have for some real numbers $\kappa > 0$ and any $0 < \delta_1 < 1/4$ that*

$$N_\Phi(T;X) = \mathrm{Vol}(\mathcal{F}_{\mathscr{A}_4}) X^{10} \widehat{\Phi}(0) \nu(T) + O\Big(\frac{X^{10-\kappa}}{q^6}\Big) + O_\epsilon\Big(\frac{X^{10-2\delta_1+\epsilon}}{q^6}\Big) + O_\epsilon\Big((Zb)^{10+\epsilon} q^{7/2+\epsilon} X^{4\delta_1}\Big).$$

*Proof.* From Propositions 132 and 136, we have

$$\begin{aligned} N_\Phi(T;X) &= \int_{\gamma\in\mathcal{F}_{\mathscr{A}_4}} \Big( \sum_{B\in W_{\mathscr{A}_4}(\mathbb{Z})^{(i,j),\mathrm{irr}}} (\gamma\cdot\Phi_X)(B) T(B)\Big) d\gamma \\ &= \int_{\substack{nsk=\gamma\in\mathcal{F}_{\mathscr{A}_4} \\ \max(s_1,s_2)\ll X^{\delta_1}}} \Big( \sum_{B\in W_{\mathscr{A}_4}(\mathbb{Z})^{(i,j)}} (\gamma\cdot\Phi_X)(B) T(B)\Big) d\gamma + O\Big(\frac{X^{10-\kappa}}{q^6}\Big) + O_\epsilon\Big(\frac{X^{10-2\delta_1+\epsilon}}{q^6}\Big). \end{aligned}$$

The main term in the second line of the above equation can be estimated using (4.39) and (4.40):

$$\int_{\substack{nsk\in\gamma\in\mathcal{F}_{\mathscr{A}_4} \\ \max(s_1,s_2)\ll X^{\delta_1}}} \Big( \sum_{B\in W_{\mathscr{A}_4}(\mathbb{Z})^{(i,j)}} (\gamma\cdot\Phi_X)(B) T(B)\Big) d\gamma =$$

$$\mathrm{Vol}(\mathcal{F}_{\mathscr{A}_4})X^{10}\widehat{\Phi}(0)\nu(T) + O_\epsilon\Big((Zb)^{10+\epsilon}q^{7/2+\epsilon}X^{4\delta_1+\epsilon}\Big),$$

as necessary. □

We are now ready to prove Theorem 122.

**Proof of Theorem 122:** Applying Corollary 119 yields

$$\begin{aligned} N_\psi^{\mathrm{gen}}(W_{\mathscr{A}_4}^{(i,j)}, T; X, Y) &= \frac{1}{\sigma_{\mathscr{A}_4}(i)\mathrm{Vol}(\Theta)}\int_{\gamma\in\mathcal{F}_{\mathscr{A}_4}}\Big(\sum_{B\in W_{\mathscr{A}_4}(\mathbb{Z})^{(i,j)}} T(B)(\gamma\cdot\Phi^{(X,Y)}[X/Y])(B)\Big)d\gamma \\ &= \frac{1}{\sigma_{\mathscr{A}_4}(i)\mathrm{Vol}(\Theta)}N_{\Phi^{(X,Y)}}(T; X/Y). \end{aligned}$$

We apply Proposition 137 to estimate $N_{\Phi^{(X,Y)}}(T; X/Y)$. First note that since $T$ is $(X^\theta, X^{1/2})$-acceptable, we have $b \ll X^\theta$ and $q \ll X^{1/2}$. Thus, the error term from the proposition is $\ll_\epsilon$

$$\frac{(X/Y)^{10-\kappa}}{q^6} + \frac{(X/Y)^{10-2\delta_1+\epsilon}}{q^6} + (Z)^{10+\epsilon}(X/Y)^{7/2+10\theta+4\delta_1+\epsilon},$$

for some $0 < \kappa$ and any $0 < \delta_1 < 1/4$. By assumption, we have $Y \gg X^{1/2-\delta}$, so by Proposition 131, we may take $Z = X^{6\delta}$. Therefore, the error term arising from Proposition 137 is $\ll_\epsilon$

$$\frac{(X^{1/2+\delta})^{10-\kappa}}{q^6} + \frac{(X^{1/2+\delta})^{10-2\delta_1+\epsilon}}{q^6} + (X^{1/2+\delta})^{7/2+10\theta+60\delta+4\delta_1+\epsilon} \ll_\epsilon \frac{X^{5-\lambda+10\theta+60\delta+\epsilon}}{q^6}$$

for some sufficiently small $\lambda > 0$. We now compute the main term to be

$$\begin{aligned}\frac{1}{\sigma_{\mathscr{A}_4}(i)}\mathrm{Vol}(\mathcal{F}_{\mathscr{A}_4})\frac{X^{10}}{Y^{10}}\frac{\widehat{\Phi^{(X,Y)}}(0)}{\mathrm{Vol}(\Theta)}\nu(T) &= \frac{|\mathcal{J}_{\mathscr{A}_4}|}{\sigma_{\mathscr{A}_4}(i)}\mathrm{Vol}(\mathcal{F}_{\mathscr{A}_4})\frac{X^{10}}{Y^{10}}\mathrm{Vol}(\psi^{(X,Y)})\nu(T)\\ &= \frac{|\mathcal{J}_{\mathscr{A}_4}|}{\sigma_{\mathscr{A}_4}(i)}\mathrm{Vol}(\mathcal{F}_{\mathscr{A}_4})\mathrm{Vol}(\psi_{X,Y})\nu(T)\\ &= \frac{|\mathcal{J}_{\mathscr{A}_4}|}{\sigma_{\mathscr{A}_4}(i)}\mathrm{Vol}(\mathcal{F}_{\mathscr{A}_4})\mathrm{Vol}\big(\psi|_{\frac{Y^2}{X}}\big)X^4Y^2\nu(T),\end{aligned}$$

where the first equality follows from Corollary 115, and the rest follow directly from the definitions of the various smooth functions involved. This concludes the proof of Theorem 122. □

## 4.6 The second moment of $|\mathrm{Sel}_2(E)|$

For $(I, J) \in \mathbb{Z}^2$ with $\Delta(I, J) \neq 0$, let $E^{I,J}$ denote the elliptic curve with invariants $I$ and $J$. We know from [26, Theorem 3.5] that $\mathrm{Sel}_2(E^{I,J})$ is in bijection with the set of $\mathrm{PGL}_2(\mathbb{Q})$-equivalence classes of locally soluble integral binary quartic forms with invariants $2^4I$ and $2^6J$. Let $\mathcal{F}$ be an acceptable collection of elliptic curves over $\mathbb{Q}$, and let $\mathcal{F}_{\mathrm{inv}}$ be the set

$$\mathcal{F}_{\mathrm{inv}} := \{(2^4I, 2^6J) \in \mathrm{Inv}(\mathbb{Z}) : E^{I,J} \in \mathcal{F}\}.$$

We denote the natural bijection $\mathcal{F} \to \mathcal{F}_{\mathrm{inv}}$ by $\iota$, and we write $\mathcal{F}^{\pm} := \iota^{-1}(\mathrm{Inv}(\mathbb{R})^{\pm})$. Let $\mathcal{H}\colon \mathrm{Inv}(\mathbb{R})^{\pm} \to \mathbb{R}$ be a smooth bounded function. Then, as in [26, §3.2], we have the equality

$$\sum_{E\in\mathcal{F}^{\pm}}(|\mathrm{Sel}_2(E)| - 1)\mathcal{H}_X(\iota(E)) = \sum_{f\in\frac{V_4(\mathbb{Z})^{\pm}}{\mathrm{PGL}_2(\mathbb{Z})}}\mathcal{N}(\mathcal{F}, f)\mathcal{H}_X(\iota(f)),$$

where $\mathcal{N}(\mathcal{F}, f)$ is defined below:

$$\mathcal{N}(\mathcal{F}, f) := \begin{cases} 1/n(f), & \text{if } f \text{ is locally soluble, has no rational linear factor, and } \iota(f) \in \mathcal{F}_{\text{inv}}; \\ 0, & \text{otherwise.} \end{cases}$$

Above, $n(f)$ is the number of $\mathrm{PGL}_2(\mathbb{Z})$-orbits in the $\mathrm{PGL}_2(\mathbb{Q})$-equivalence class of $f$ in $V_4(\mathbb{Z})$.

For an integral binary quartic form $f$, write $S(f) := \mathrm{Sel}_2(\mathrm{Jac}(C_f))$ and $|S|(f) := |\mathrm{Sel}_2(\mathrm{Jac}(C_f))|$. Then we have the following tautological identity:

$$\sum_{E \in \mathcal{F}^{\pm}} |\mathrm{Sel}_2(E)|(|\mathrm{Sel}_2(E)| - 1)\mathcal{H}_X(\iota(E)) \;\; = \sum_{f \in \frac{V_4(\mathbb{Z})^{\pm}}{\mathrm{PGL}_2(\mathbb{Z})}} \mathcal{N}(\mathcal{F}, f)|S|(f)\mathcal{H}_X(\iota(f)). \tag{4.41}$$

We will replace $\mathcal{N}(\mathcal{F}, f)$ with $\mathcal{M}(\mathcal{F}, f)$, where $\mathcal{M}(\mathcal{F}, f)$ defined below. The function $\mathcal{N}(\mathcal{F}, f)$ vanishes on $V_4(\mathbb{Z})^{(2-)}$, and we will define $\mathcal{M}(\mathcal{F}, f)$ to be 0 there too. For $i \in \{0, 1, 2+\}$, and $f \in V_4(\mathbb{Z})^{(i)}$ with nonzero discriminant, we define $\mathcal{M}(\mathcal{F}, f) = \prod_p \mathcal{M}_p(\mathcal{F}, f)$, where $\mathcal{M}_p(\mathcal{F}, f) \colon V_4(\mathbb{Z}_p) \to \mathbb{R}$ is as follows: letting $\mathcal{F}_{\text{inv},p}$ denote the $p$-adic closure of $\mathcal{F}_{\text{inv}}$ in $\mathrm{Inv}(\mathbb{Z}_p)$, we put

$$\mathcal{M}_p(\mathcal{F}, f) := \begin{cases} 1/m_p(f), & \text{if } f \text{ is soluble over } \mathbb{Q}_p \text{ and } \iota(f) \in \mathcal{F}_{\text{inv},p}; \\ 0, & \text{otherwise.} \end{cases}$$

Again, as in [26, §3.2], $m_p(f)$ denotes the number of $\mathrm{PGL}_2(\mathbb{Z}_p)$-orbits in the $\mathrm{PGL}_2(\mathbb{Q}_p)$-equivalence class of $f$ in $V_4(\mathbb{Z}_p)$. Over the next few subsections, we estimate the term

$$N_{\mathcal{H}}^{\text{gen}}(V^{(i)}, \mathcal{M}(\mathcal{F}, \cdot)|S|; X) = \sum_{f \in \frac{V_4(\mathbb{Z})^{(i)}}{\mathrm{PGL}_2(\mathbb{Z})}} \mathcal{M}(\mathcal{F}, f)|S|(f)\mathcal{H}_X(\iota(f)), \tag{4.42}$$

for smooth, compactly supported functions $\mathcal{H} \colon \mathrm{Inv}(\mathbb{R})^{\pm} \to \mathbb{R}$.

### 4.6.1 Slicing over the leading coefficient

Let $T\colon V_4(\mathbb{Z}) \to \mathbb{R}$ be a $\mathrm{PGL}_2(\mathbb{Z})$-invariant function, and fix $i \in \{0, 1, 2+\}$. By Proposition 116, we have that

$$N_{\mathcal{H}}^{\mathrm{gen}}(V^{(i)}, T; X) = \frac{1}{\sigma_i \mathrm{Vol}(\Theta)} \mathcal{O}(T, \psi; X^{1/6}),$$

where $\psi = \psi^{(i)} = \mathcal{S}_{V_4}(\mathcal{H}, \Theta)$. We may assume without loss of generality that $\psi$ is $\mathrm{SO}_2(\mathbb{R})$-invariant (this is guaranteed as long as $\Theta$ is $\mathrm{SO}_2(\mathbb{R})$-invariant). To evaluate the integral $\mathcal{O}(T, \psi; X)$, we fiber the sum over $f \in V_4(\mathbb{Z})^{\mathrm{gen}}$ by the value of $a(f)$, obtaining

$$\mathcal{O}(T, \psi; X) \;=\; \int_{(t,n)\in\mathcal{F}_2} \Big( \sum_{|a|\neq 0} \sum_{f\in V_{4,a}(\mathbb{Z})^{\mathrm{gen}}} T(f) \cdot ((t, t^{-2}n) \cdot \psi_X)(f) \Big) dn \frac{d^\times t}{t^2},$$

where $(t, t^{-2}n)$ denotes the matrix $\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \cdot \begin{bmatrix} 1 & \\ t^{-2}n & 1 \end{bmatrix}$. We will transform the innermost sum in the above equation into one over monic binary quartic forms as follows.

For $f \in V_{4,a}(\mathbb{Z})$, let $f^{\mathsf{mon}*} := (\kappa f)^{\mathsf{mon}}$, and for $g \in \mathsf{mon}(\kappa V_{4,a}(\mathbb{Z}))$, let $g_a^{\mathsf{dem}*} := \kappa^{-1} g_a^{\mathsf{dem}}$. For a function $\psi\colon V_4(\mathbb{R}) \to \mathbb{R}$ and a real number $n$, let $\psi^{(n)}$ denote $\begin{bmatrix} 1 & \\ n & 1 \end{bmatrix} \cdot \psi$. Then we have

$$\sum_{f\in V_{4,a}(\mathbb{Z})^{\mathrm{gen}}} T(f) \cdot ((t, t^{-2}n) \cdot \psi_X)(f) = \sum_{f\in V_{4,a}(\mathbb{Z})^{\mathrm{gen}}} T_a(f^{\mathsf{mon}*}) \cdot \big(\psi_{\kappa^2 a X}^{(t^{-2}n)}[\kappa a t^2]\big)(f^{\mathsf{mon}*}),$$

where for $g \in \mathsf{mon}(\kappa V_{4,a}(\mathbb{Z}))$, we write $T_a(g) := T(g_a^{\mathsf{dem}*})$. Then we immediately obtain the following result:

**Theorem 138.** *We have that*

$$N_{\mathcal{H}}^{\mathrm{gen}}(V^{(i)}, T; X) = \frac{1}{\sigma_i \mathrm{Vol}(\Theta)} \int_{(t,n)\in\mathcal{F}_2} \Big( \sum_{|a|\neq 0} \sum_{f\in V_{4,a}(\mathbb{Z})^{\mathrm{gen}}} T_a(f^{\mathsf{mon}*}) \cdot \big(\psi_{\kappa^2 a X^{1/6}}^{(t^{-2}n)}[\kappa a t^2]\big)(f^{\mathsf{mon}*}) \Big) dn \frac{d^\times t}{t^2}.$$

### 4.6.2 Introducing local masses on $W_{\mathscr{A}_4}(\mathbb{Z})$

Let $f \in V_4(\mathbb{Z})$ with $a(f) \neq 0$. From §4.2, we know that $S(f)$ is in bijection with the set of $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Q})$-equivalence classes on certain matrices $B \in W_{\mathscr{A}_4}(\mathbb{Z})$ with $\iota(B) = f^{\mathsf{mon}*}$ defined by local conditions. Moreover, by Theorem 111, every such $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Q})$-equivalence class has an element that is special at $a(f)$.

This motivates the definition of the following mass functions on $W_{\mathscr{A}_4}(\mathbb{Z})$. For each prime $p$, let $\mathcal{S}_p \subset W_{\mathscr{A}_4}(\mathbb{Z}_p)$ be a $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z}_p)$-invariant set. Denote the collection $(\mathcal{S}_p)_p$ by $\mathcal{S}$. Let $W_{\mathscr{A}_4}(\mathcal{S})$ be the set $W_{\mathscr{A}_4}(\mathbb{Z}) \cap \left(\cap_p \mathcal{S}_p\right)$, which is immediately seen to be $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})$-invariant. For an element $B \in \mathcal{S}_p$ (resp. $B \in W_{\mathscr{A}_4}(\mathcal{S})$), let $\mathcal{B}_p(B)$ (resp., $\mathcal{B}(B)$) be a set of representatives for the action of $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z}_p)$ (resp., $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})$) on the $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Q}_p)$-equivalence class (resp. $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Q})$-equivalence class) of $B$ in $\mathcal{S}_p$ (resp. $W_{\mathscr{A}_4}(\mathcal{S})$). Then, for $B \in W_{\mathscr{A}_4}(\mathcal{S})$, we define:

$$n(\mathcal{S}, B) := \sum_{B' \in \mathcal{B}(B)} 1; \qquad m(\mathcal{S}, B) := \sum_{B' \in \mathcal{B}(B)} \frac{|\mathrm{Stab}_{\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Q})}(B)|}{|\mathrm{Stab}_{\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})}(B')|}.$$

Analogously, for $B \in \mathcal{S}_p$, we define

$$m_p(\mathcal{S}_p, B) := \sum_{B' \in \mathcal{B}_p(B)} \frac{|\mathrm{Stab}_{\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Q}_p)}(B)|}{|\mathrm{Stab}_{\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z}_p)}(B')|}.$$

Then we have the following result whose proof is identical to that of [26, Proposition 3.6].

**Proposition 139.** *For $B \in W_{\mathscr{A}_4}(\mathcal{S})$, we have that $m(\mathcal{S}, B) = \prod_p m_p(\mathcal{S}_p, B)$.*

Now let $f$ be a binary quartic form and denote $a(f)$ by $a$. Let $\mathcal{S}(a) = (\mathcal{S}(a)_p)_p$ be defined as follows: for $p \parallel a$, we set $\mathcal{S}(a)_p$ to be the set of all elements in $W_{\mathscr{A}_4}(\mathbb{Z}_p)$ with rank $\leq 1$ modulo $p$; for all other primes $p$ we simply set $\mathcal{S}(a)_p = W_{\mathscr{A}_4}(\mathbb{Z}_p)$. We know that we have

$$|S|(f) = \sum_{\substack{B \in \frac{W_{\mathscr{A}_4}(\mathcal{S}(a)) \cap \iota^{-1}(f^{\mathsf{mon}*})}{\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})} \\ B \text{ loc. sol.}}} \frac{1}{n(\mathcal{S}(a), B)}. \tag{4.43}$$

Once again, since $m(\mathcal{S}(a),\cdot)$ has an Euler product while $n(\mathcal{S}(a),\cdot)$ does not, we replace $n(\mathcal{S}(a),\cdot)$ with $m(\mathcal{S}(a),\cdot)$ and define $\mathcal{M}_p(\mathcal{F};a)\colon W_{\mathscr{A}_4}(\mathcal{S}(a))\to\mathbb{R}$ as follows:

$$\mathcal{M}_p(\mathcal{F};a;B):=\begin{cases}\dfrac{\mathcal{M}_p(\mathcal{F},\iota(B)_a^{\mathsf{dem}*})}{m_p(\mathcal{S}(a)_p,B)} & \text{if } B \text{ is soluble at } p;\\[2ex] 0 & \text{otherwise,}\end{cases}$$

We define the global mass $\mathcal{M}(\mathcal{F};a;\cdot)$ as follows:

$$\begin{aligned}\mathcal{M}(\mathcal{F};a;\cdot)\colon W_{\mathscr{A}_4}(\mathbb{Z}) &\to \mathbb{R}\\ B &\mapsto \textstyle\prod_p \mathcal{M}_p(\mathcal{F};a;B)=\dfrac{\mathcal{M}(\mathcal{F},\iota(B)_a^{\mathsf{dem}*})}{m(\mathcal{S}(a),B)}.\end{aligned}$$

The masses $\mathcal{N}(\mathcal{F};a;B)$ and $\mathcal{M}(\mathcal{F};a;B)$ only differ on non-generic elements $B$. This motivates the following bound on the number of non-generic and non-distinguished orbits $B$:

**Lemma 140.** *Let $S$ denote the characteristic function of the set of elements in $W_{\mathscr{A}_4}(\mathbb{Z})$ that are non-generic and non-distinguished. Then we have for some $\lambda>0$ that*

$$\int_{t\gg 1}^{\ll X^{1/24}}\Big(\sum_{0\neq|a|\ll X^{1/6}/t^4} N_\psi(W_{\mathscr{A}_4}^{(i)},S;aX^{1/6},at^2)\Big)\frac{d^\times t}{t^2}\ll X^{5/6-\lambda}.$$

*Proof.* We split the sum over $a$ into the big range with $|a|>(X^{1/6}/t^4)^{1-\delta}$ and the small range with $|a|\le(X^{1/6}/t^4)^{1-\delta}$, for some $\delta>0$ to be chosen later. Using Proposition 136 for $a$ in the big range, we obtain

$$N_\psi(W_{\mathscr{A}_4}^{(i)},S;aX^{1/6},at^2)\ll\frac{X^{10/6-\kappa}}{t^{20}a^6}\ll t^4X^{4/6+\delta-\kappa},$$

for some $\kappa>0$ independent of $\delta$. For $a$ in the small range, we use Corollary 121 to obtain

the bound

$$N_\psi(W_{\mathscr{A}_4}^{(i)}, S; aX^{1/6}, at^2) \ll \frac{X^{5/6-\delta/2}}{a} \prod_{\substack{p^k \| a \\ k \geq 3}} p^{k/2}. \tag{4.44}$$

Summing the bound (4.44) over $a$ and integrating over $t$ gives a contribution that is $\ll_\epsilon$

$$X^{5/6-\delta/2+\epsilon} \sum_{\substack{1 \leq |c| \leq (X^{1/6}/t^4)^{1-\delta} \\ c \text{ cubeful}}} \frac{1}{\sqrt{c}} \ll_\epsilon X^{5/6-\delta/2+\epsilon},$$

as desired, where we say that $m$ is cubeful if, for each prime $p \mid m$, we have $p^3 \mid m$. □

Finally, for $i \in \{0, 1, 2+, 2-\}$, we define

$$\mathcal{I}^{(i)} = \frac{1}{\sigma_i \mathrm{Vol}(\Theta)} \int_{(t,n) \in \mathcal{F}_2} \Big( \sum_{|a| \neq 0} N_{\psi^{(t^{-2}n)}}^{\mathrm{gen}} \big( W_{\mathscr{A}_4}^{(i)}, \mathcal{M}(\mathcal{F}; a, \cdot); \kappa^2 a X^{1/6}, \kappa a t^2 \big) \Big) dn \frac{d^\times t}{t^2},$$

and set $\mathcal{I}^+ = \mathcal{I}^{(0)} + \mathcal{I}^{(2+)}$ and $\mathcal{I}^- = \mathcal{I}^{(1)}$. We now have the following result.

**Theorem 141.** *We have for some $\lambda > 0$ that*

$$\sum_{E \in \mathcal{F}^\pm} \sum_{\substack{\sigma \in \mathrm{Sel}_2(E) \\ \sigma \neq 1}} \big( |S_2(\sigma)| - 2 \big) \mathcal{H}_X(\iota(E)) = \mathcal{I}^\pm + O(X^{5/6-\lambda}). \tag{4.45}$$

*Proof.* We prove the result for negative-discriminant elliptic curves; the positive-discriminant case follows identically. As long as $f$ is generic, there are precisely two distinguished orbits arising from $f$. Thus, (4.41) and Theorem 138 imply that the left-hand side of (4.45) is

$$\frac{1}{\sigma_1 \mathrm{Vol}(\Theta)} \int_{(t,n) \in \mathcal{F}_2} \Big( \sum_{|a| \neq 0} \sum_{f \in V_{4,a}(\mathbb{Z})} \big( \psi_{\kappa^2 a X^{1/6}}^{(t^{-2}n)} [\kappa a t^2] \big) (f^{\mathsf{mon}*}) \mathcal{N}(\mathcal{F}, f) (|S|_a(f^{\mathsf{mon}*}) - 2) \Big) dn \frac{d^\times t}{t^2},$$

where as before, $|S|(g)$ denotes $|\mathrm{Sel}_2(J_g)|$, and $|S|_a(f) := |S|(f_a^{\mathsf{dem}*})$. The value of $|S|_a(f^{\mathsf{mon}*})$ is given in (4.43) in terms of a weighted sum of $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z})$-orbits on $W_{\mathscr{A}_4}(\mathbb{Z})$. We define

$\mathcal{N}\colon W_{\mathscr{A}_4}(\mathbb{Z}) \to \mathbb{R}$ via

$$\mathcal{N}(\mathcal{F}; a; B) := \begin{cases} \dfrac{\mathcal{N}(\mathcal{F}, \iota(B)_a^{\mathsf{dem}*})}{n(\mathcal{S}(a), B)}, & \text{if } B \text{ is locally soluble,} \\ \\ 0, & \text{otherwise,} \end{cases}$$

Therefore, we have that

$$\sum_{|a|\neq 0} \sum_{f \in V_{4,a}(\mathbb{Z})} \Big(\psi^{(t^{-2}n)}_{\kappa^2 a X^{1/6}}[\kappa a t^2]\big)(f^{\mathsf{mon}*})\mathcal{N}(\mathcal{F}, f)(|S|_a(f^{\mathsf{mon}*}) - 2)\Big) = \sum_{|a|\neq 0} N^{\mathrm{gen}}_{\psi^{(t^{-2}n)}}\big(W^{(1)}_{\mathscr{A}_4}, \mathcal{N}(\mathcal{F}; a; B); \kappa^2 a X^{1/6}, \kappa a t^2\big),$$

up to an error of $O(X^{5/6-\lambda})$ for some $\lambda > 0$, where the error term follows from bounding non-distinguished and non-generic elements using Lemma 140.

Since $\mathcal{N}(\mathcal{F}; a; B)$ differs from $\mathcal{M}(\mathcal{F}; a; B)$ only on elements $B$ that are not generic, it follows from Lemma 140 that we have

$$\sum_{|a|\neq 0} \sum_{f \in V_{4,a}(\mathbb{Z})} \Big(\psi^{(t^{-2}n)}_{\kappa^2 a X^{1/6}}[\kappa a t^2]\big)(f^{\mathsf{mon}*})\mathcal{N}(\mathcal{F}, f)(|S|_a(f^{\mathsf{mon}*}) - 2)\Big) = \sum_{|a|\neq 0} N^{\mathrm{gen}}_{\psi^{(t^{-2}n)}}\big(W^{(1)}_{\mathscr{A}_4}, \mathcal{M}(\mathcal{F}; a; B); \kappa^2 a X^{1/6}, \kappa a t^2\big),$$

up to an error of $O(X^{5/6-\lambda})$. The result now follows from integrating over $(t, n) \in \mathcal{F}_2$. $\square$

### 4.6.3 Truncating the local masses and applying the counting results

Recall that we choose (unique up to sign) top degree forms $\omega$ on $\mathrm{PSO}_{\mathscr{A}_4}$ and $\mathrm{PGL}_2$ for the application of Theorem 114. For primes $p$, we define

$$\tau_{\mathscr{A}_4}(p) := \int_{g \in \mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z}_p)} \omega(g); \qquad \tau(p) := \int_{g \in \mathrm{PGL}_2(\mathbb{Z}_p)} \omega(g).$$

Since the Tamagawa numbers of $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Q})$ and $\mathrm{PGL}_2(\mathbb{Q})$ are 4 and 2, respectively, we have for $Z > 0$ that

$$\begin{aligned} 4\tau_{\mathscr{A}_4}^{(Z)} &:= 4 \prod_{p>Z} \tau_{\mathscr{A}_4}(p)^{-1} &&= \mathrm{Vol}(\mathcal{F}_{\mathscr{A}_4}) \prod_{p \le Z} \tau_{\mathscr{A}_4}(p); \\ 2\tau^{(Z)} &:= 2 \prod_{p>Z} \tau(p)^{-1} &&= \mathrm{Vol}(\mathcal{F}_2) \prod_{p \le Z} \tau(p). \end{aligned} \tag{4.46}$$

For an integer $\ell > 0$, let $\mathcal{M}_{p,\ell}(\mathcal{F}; a; \cdot) \colon W_{\mathscr{A}_4}(\mathbb{Z}_p) \to \mathbb{R}$ be the best upper approximation of $\mathcal{M}_p(\mathcal{F}; a; \cdot)$ defined modulo $p^\ell$. For positive real numbers $r < s$, define the truncated mass

$$\mathcal{M}^{(r,s)}(\mathcal{F}; a; B) := \prod_{\substack{p<r,\, p^2 \nmid a \\ p^\ell < s \le p^{\ell+1}}} \mathcal{M}_{p,\ell}(\mathcal{F}; a; B) \times \prod_{\substack{p<r,\, p^2 \mid a \\ p^\ell < s \le p^{\ell+1}}} \mathcal{M}_{p,360\nu_p(a)+\ell}(\mathcal{F}; a; B) \times \prod_{r \le p,\, p \mid a} \mathcal{S}_p(a; B) \tag{4.47}$$

where, if $p^k \parallel a$, then $\mathcal{S}_p(a, \cdot)$ is the characteristic function of the set of elements that are special at $p^k$.

Let $\theta > 0$ be a real number that will eventually be picked to be sufficiently small. For a positive real number $X$, we define $X_\theta$ to be the largest integer satisfying $\prod_{i \le X_\theta} i < X^\theta$. We will consider the truncated function $\mathcal{M}^{(\log X_\theta, X_\theta)}(\mathcal{F}; a, \cdot)$ which satisfies $\mathcal{M}^{(\log X_\theta, X_\theta)}(\mathcal{F}; a; B) \ge \mathcal{M}(\mathcal{F}; a; B)$ for every $B \in W_{\mathscr{A}_4}(\mathbb{Z})$. For each place $v$ of $\mathbb{Q}$, define the ratio

$$\alpha_v := \frac{|E(\mathbb{Q}_v)/2E(\mathbb{Q}_v)|}{|E[2](\mathbb{Q}_v)|},$$

where $E$ is any elliptic curve over $\mathbb{Q}_v$. The ratio is independent of $E$, and depends only on $v$. The following lemma follows from [26, Lemma 3.20].

**Lemma 142.** *For large enough primes $p$, we have $\alpha_p = 1$. Moreover, $\prod_v \alpha_v = 1$.*

*Proof.* Indeed, we have $\alpha_\infty = \frac{1}{2}$, $\alpha_2 = 2$, and $\alpha_p = 1$ for odd primes $p$. □

Let $\mathcal{N}(M)$ denote the set of natural numbers whose squareful part is greater than $M$, and let $\kappa \ll 1$ be a sufficiently small positive real number. We say that a nonzero integer $a$ is *good* if $a \notin \mathcal{N}(X^\theta)$ and $a \geq (X^{1/6}/t^4)^{1-\kappa}$, and *bad* otherwise. For ease of notation, define

$$T_a := \begin{cases} \mathcal{M}^{(\log X_\theta, X_\theta)}(\mathcal{F}; a, \cdot), & \text{if } a \text{ is good,} \\ \tau_{\mathscr{A}_4}^{(\log X_\theta)} \mathcal{M}(\mathcal{F}; a, \cdot), & \text{if } a \text{ is bad.} \end{cases} \tag{4.48}$$

We then have the following result for good integers $a$:

**Proposition 143.** *Let $a$ be a good integer, and let $\psi \colon V_4(\mathbb{R}) \to \mathbb{R}$ be a smooth, compactly supported function. Then for some $\lambda > 0$ independent of the choice of the sufficiently small constants $\theta$ and $\kappa$, we have that*

$$N_\psi\big(W_{\mathscr{A}_4}^{(i)}, T_a; \kappa^2 a X^{1/6}, \kappa a t^2\big) \;=\; \alpha_\infty |\mathcal{J}_{\mathscr{A}_4}| \mathrm{Vol}(\mathcal{F}_{\mathscr{A}_4}) \nu(T_a) \mathrm{Vol}\big(\psi|_{\frac{at^4}{X^{1/6}}}\big) \kappa^{10} a^6 X^{4/6} t^4 + O\Big(\frac{X^{5/6-\lambda}}{a}\Big).$$

*Proof.* Recall that $\tau_{\mathscr{A}_4}^{\mathrm{sol}}(i)$ denotes the number of soluble $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{R})$-orbits on $\iota^{-1}(f)$ for any form $f \in V_4(\mathbb{R})^{(i)}$. We therefore have that

$$\sum_{j=1}^{\tau_{\mathscr{A}_4}^{\mathrm{sol}}(i)} \frac{1}{\sigma(i)} = \frac{\tau_{\mathscr{A}_4}^{\mathrm{sol}}(i)}{\sigma(i)} = \alpha_\infty. \tag{4.49}$$

We claim that the function $T_a$ is $((aX^{1/6})^{2166\theta}, (aX^{1/6})^{1/2})$-acceptable. To see why, note that the $p$-adic factor on the right-hand side of (4.47) is defined by congruence conditions modulo:

- $p^{\ell_p}$, where $\ell_p$ is the unique integer satisfying $p^{\ell_p} < X_\theta \leq p^{\ell_p+1}$, if $p < \log X_\theta$ and $p^2 \nmid a$;

- $p^{360\nu_p(a)+\ell_p}$, if $p < \log X_\theta$ and $p^2 \mid a$; and
- $p^{\nu_p(a)}$, if $p \geq \log X_\theta$, since $\mathcal{S}_p(a; B)$ is defined modulo $p^{\nu_p(a)}$ (see §4.3.2).

Thus, $T_a$ is defined by congruence conditions modulo $m_1 m_2$, where

$$m_1 = \prod_{\substack{p<\log X_\theta \\ p^2 \nmid a}} p^{\ell_p} \times \prod_{\substack{p<\log X_\theta \\ p^2 \mid a}} p^{360\nu_p(a)+\ell_p} \times \prod_{\substack{p\geq\log X_\theta \\ p^2 \mid a}} p^{\nu_p(a)} \quad \text{and} \quad m_2 = \prod_{\substack{p\geq\log X_\theta \\ p \| a}} p$$

Since $a \notin \mathcal{N}(X^\theta)$, we have that $m_1 \leq \prod_{i\leq X_\theta} i \times \prod_{p^2\mid a} p^{360\nu_p(a)} < X^{361\theta} \leq (aX^{1/6})^{2166\theta}$. Moreover, $m_2$ is squarefree with $m_2 \leq a \ll (aX^{1/6})^{1/2}$, $\gcd(m_1, m_2) = 1$, and the $p$-adic factor in the definition of $T_a$ at every prime $p \mid m_2$ is precisely the characteristic function of the set of matrices in $U_4(\mathbb{Z}_p)$ that are of rank $\leq 1$ modulo $p$. Thus, we have the claim. The proposition now follows by applying Theorem 122,using the relation (4.49), and observing that $a \leq m_1 m_2$. □

Finally, we have the following consequence of Proposition 143:

**Theorem 144.** *Let $i \in \{0, 1, 2+\}$. For some $\lambda > 0$, we have that*

$$\mathcal{I}^{(i)} \leq \frac{\alpha_\infty |\mathcal{J}_{\mathscr{A}_4}| \mathrm{Vol}(\mathcal{F}_{\mathscr{A}_4})}{\sigma_i \mathrm{Vol}(\Theta)} X^{4/6} \int_{\substack{(t,n)\in\mathcal{F}_2 \\ t\ll X^{1/24}}} \Big( \sum_{0<|a|\ll \frac{X^{1/6}}{t^4}} \kappa^{10} a^6 \nu(T_a) \mathrm{Vol}\big(\psi|_{\frac{at^4}{X^{1/6}}}\big) \Big) t^4 dn \frac{d^\times t}{t^2} + O(X^{5/6-\lambda}). \tag{4.50}$$

*Proof.* It suffices to prove that the contribution to the right-hand side of (4.50) from bad integers $a$ is $O(X^{5/6-\lambda})$. For such $a$, we have $T_a \ll \mathcal{M}(\mathcal{F}; a, \cdot)$, which is a bounded function supported on the set of elements $B$ that are special at $a$. By the proof of Theorem 120,

$$\nu(T_a) \ll \nu(|a|) = \prod_{p\|a} p^{-6} \times \prod_{p^2\|a} p^{-12} \times \prod_{p^3\|a} p^{-17} \times \prod_{\substack{p^k\|a \\ k\geq 4}} p^{-11k/2}. \tag{4.51}$$

Moreover, since $\psi$ is smooth and compactly supported, the factor of $\mathrm{Vol}\left(\psi|_{\frac{at^4}{X^{1/6}}}\right)$ in the right-hand side of (4.50) is absolutely bounded. This, along with (4.51), yields that the

contribution from bad integers $a$ is

$$\ll X^{4/6} \int_{t \ll X^{1/24}} \Big( \sum_{\substack{0<|a| \ll \frac{X^{1/6}}{t^4} \\ a \text{ bad}}} \prod_{\substack{p^k \| a \\ k \geq 3}} p^{k/2} \Big) t dt. \tag{4.52}$$

Using the bound $X^{1/6}/(at^4) \gg 1$, we find that the contribution to (4.52) from bad integers $a \in \mathcal{N}(X^\theta)$ is

$$X^{5/6} \Big( \sum_{\substack{0<|a| \ll \frac{X^{1/6}}{t^4} \\ a \in \mathcal{N}(X^\theta)}} \frac{1}{a} \prod_{\substack{p^k \| a \\ k \geq 3}} p^{k/2} \Big) \ll_\epsilon X^{5/6+\epsilon} \sum_{\substack{|b| \geq 1 \\ b \text{ squareful}}} \sum_{\substack{|c| \geq X^\theta / b \\ c \text{ cubeful}}} \frac{1}{b\sqrt{c}} \ll_\epsilon X^{5/6-\theta/6+\epsilon}. \tag{4.53}$$

Similarly, the contribution to (4.52) from bad integers $a \leq (X^{1/6}/t^4)^{1-\kappa}$ is

$$\ll_\epsilon X^{5/6-\kappa/6+\epsilon} \sum_{\substack{1 \leq |c| \leq (X^{1/6}/t^4)^{1-\kappa} \\ c \text{ cubeful}}} \frac{1}{\sqrt{c}} \ll_\epsilon X^{5/6-\kappa/6+\epsilon}. \tag{4.54}$$

Combining the bounds (4.53) and (4.54) yields the theorem. □

### 4.6.4 Computing the local volumes and summing over leading coefficients

Recall from (4.48) that we abbreviated the symbol $\mathcal{M}^{(\log X_\theta, X_\theta)}(\mathcal{F}; a, \cdot)$ by $T_a$. We begin with the following lemma.

**Lemma 145.** *Let $p$ be a prime, and let $\ell$ be a positive integer. Then we have that*

$$\nu_p(\mathcal{M}_{p,\ell}(\mathcal{F}; a; \cdot)) = \int_{W_{\mathscr{A}_4}(\mathbb{Z}_p)} \mathcal{M}_p(\mathcal{F}; a; B) dB + O(p^{-\ell/60}).$$

*Proof.* Recall that $\mathcal{M}_{p,\ell}(\mathcal{F}; a; \cdot)$ is the best upper approximation to $\mathcal{M}_p(\mathcal{F}; a; \cdot)$ defined modulo $p^\ell$. If two elements in $W_{\mathscr{A}_4}(\mathbb{Z}_p)$ that are congruent modulo $p^\ell$, say $B$ and $B + p^\ell B'$, have different values under $\mathcal{M}_p(\mathcal{F}; a; \cdot)$, then we may assume that there exists an element

$\gamma \in \mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Q}_p) \smallsetminus \mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z}_p)$ such that $\gamma \cdot B \in W_{\mathscr{A}_4}(\mathbb{Z}_p)$ but $\gamma \cdot (B + p^\ell B') \notin W_{\mathscr{A}_4}(\mathbb{Z}_p)$. We write $\gamma = \sigma_1 \gamma' \sigma_2$, where $\sigma_1$ and $\sigma_2$ belong to $\mathrm{PSO}_{\mathscr{A}_4}(\mathbb{Z}_p)$, and $\gamma'$ is a diagonal matrix. It therefore follows that $\gamma'\sigma_2 \cdot p^\ell B' \notin W_{\mathscr{A}_4}(\mathbb{Z}_p)$. In particular, it follows that $\gamma'$ has a nonzero coefficient whose valuation at $p$ is at most $-\ell/2$. However, since $\gamma'\sigma_2 \cdot B$ is integral, it is easy to deduce that the discriminant of $\sigma_2 \cdot B$, and hence the discriminant of $B$, is divisible by $p^{\ell/5}$. Therefore, we have

$$\nu_p(T_a) - \int_{W_{\mathscr{A}_4}(\mathbb{Z}_p)} \mathcal{M}_p(\mathcal{F}; a; B) dB \leq \mathrm{Vol}\big(\{B \in W_{\mathscr{A}_4}(\mathbb{Z}_p) : p^{\ell/5} \mid \Delta(B)\}\big).$$

A result of Serre (see [102, §3.2, Equation (57)]) implies the bound

$$\#\{B \in W_{\mathscr{A}_4}(\mathbb{Z}/p^n\mathbb{Z}) : p^n \mid \Delta(B)\} = O(p^{119n/12}),$$

which in turn implies that the volume above is bounded by $O(p^{-\ell/60})$, as necessary. □

We have the following immediate consequence of [78, Corollary 1.2]:

**Lemma 146.** *Let $b \geq a \geq 1$ be positive integers, and let $p$ be a prime. The $p$-adic density of matrices $Q \in U_4(\mathbb{Z}_p)$ such that $Q$ is of rank $\leq 1$ modulo $p^a$ and is of rank $\leq 2$ modulo $p^b$ is given by*

$$p^{-3a-3b} \times \begin{cases} 1, & \text{if } b = a, \\ 1 + p^{-2-4a}(1-p^{-7})^{-1}(1-p^{-3})(1-p^{7a-7b}), & \text{if } b > a. \end{cases}$$

We now have the following result.

**Proposition 147.** *For large enough $X$, we have the following bounds when $a$ is good:*

$$\nu_p(T_a) \leq \begin{cases} \alpha_p|\mathcal{J}_{\mathscr{A}_4}|_p|\kappa|_p^{10}|a|_p^6\tau_{\mathscr{A}_4}(p)\displaystyle\int_{V_{4,a}(\mathbb{Z}_p)}\mathcal{M}_p(\mathcal{F},f)df + O_\epsilon(p^{-\ell_p/60}X_\theta^\epsilon), & \text{if } \ p<\log X_\theta,\ p^2\nmid a; \\ \alpha_p|\mathcal{J}_{\mathscr{A}_4}|_p|\kappa|_p^{10}|a|_p^6\tau_{\mathscr{A}_4}(p)\displaystyle\int_{V_{4,a}(\mathbb{Z}_p)}\mathcal{M}_p(\mathcal{F},f)df + O(p^{-\ell_p/60}|a|_p^6), & \text{if } \ p<\log X_\theta,\ p^2\mid a; \\ |a|_p^6, & \text{if } \ p\geq \log X_\theta \text{ and } p^2\nmid a; \\ |a|_p^6 + O(p^{-1}|a|_p^6), & \text{if } \ p\geq \log X_\theta \text{ and } p^2\mid a. \end{cases}$$

*When $a$ is a bad integer, we have that*

$$\nu_p(T_a) = \begin{cases} \alpha_p|\mathcal{J}_{\mathscr{A}_4}|_p|\kappa|_p^{10}|a|_p^6\tau_{\mathscr{A}_4}(p)\displaystyle\int_{V_{4,a}(\mathbb{Z}_p)}\mathcal{M}_p(\mathcal{F},f)df, & \text{if } \ p<\log X_\theta; \\ \alpha_p|\mathcal{J}_{\mathscr{A}_4}|_p|a|_p^6\displaystyle\int_{V_{4,a}(\mathbb{Z}_p)}\mathcal{M}_p(\mathcal{F},f)df, & \text{if } \ p\geq \log X_\theta. \end{cases}$$

*Proof.* When $a$ is good and $p<\log X_\theta$ or when $a$ is bad, we first apply Lemma 145. The claim then follows from Theorem 114 in a manner similar to [26, Proposition 3.9].

Now assume that $a$ is good and that $p\geq \log X_\theta$. The real number $X$ may be chosen large enough to ensure that $|\kappa|_p=\alpha_p=|\mathcal{J}_{\mathscr{A}_4}|_p=1$. When $p\nmid a$, the result only claims an upper bound of 1, which follows from the fact that $\mathcal{M}_{p,\ell}(\mathcal{F};a;\cdot)$ is bounded above by 1. When $p\parallel a$, the result follows since $\mathcal{M}_p^{(\log X_\theta, X_\theta)}(\mathcal{F};a,\cdot)=\mathcal{S}_p(a;B)$, where $\mathcal{S}_p(a;B)$ is the characteristic function of the set of elements $B$ with $\mathbb{F}_p$-rank $\leq 1$. The $p$-adic density of these elements is precisely $1/p^6$.

Finally, when $p^k\parallel a$, for $k\geq 2$, we note that once again, $\mathcal{M}_p^{(\log X_\theta, X_\theta)}(\mathcal{F};a,\cdot)=\mathcal{S}_p(a;\cdot)$, the characteristic function of the set of elements that are special at $p$. Denote this set by $S$. By Proposition 112, $S$ is contained in the finite union of sets of the form $p^\alpha\mathcal{L}_{k-2\alpha+\beta,k-\alpha-\beta}$, where $\alpha$ and $\beta$ range over nonnegative integers satisfying $2\alpha\leq k+\beta$ and $2\beta\leq\alpha$. It follows immediately from Lemma 146 that the $p$-adic density of $p^\alpha\mathcal{L}_{k-2\alpha+\beta,k-\alpha-\beta}$ is $p^{-6k-\alpha}(1+O(p^{-6}))$. Summing up over the possible values of $\alpha$ and $\beta$ gives a total $p$-adic density of

$p^{-6k}(1+O(p^{-1}))$, as necessary. □

We have the following immediate consequence of the above proposition:

**Corollary 148.** *For large enough $X$, we have that*

$$\alpha_\infty|\mathcal{J}_{\mathscr{A}_4}|\mathrm{Vol}(\mathcal{F}_{\mathscr{A}_4})a^6\nu\big(\mathcal{M}^{(\log X_\theta, X_\theta)}(\mathcal{F};a,\cdot)\big) \leq 4\tau_{\mathscr{A}_4}^{\log X_\theta}\prod_{p\leq \log X_\theta}\int_{V_{4,a}(\mathbb{Z}_p)}\mathcal{M}_p(\mathcal{F},f)df + O_\epsilon\big(X_\theta^{-1/120+\epsilon}\big) + E(a),$$

*where* $E(a) := O\Big(\sum_{\substack{p^2|a\\ p\geq \log X_\theta}}\frac{1}{p}\Big)$.

*Proof.* For good integers $a$, this is a consequence of Proposition 147. For bad integers $a$, Proposition 147 implies the same bound with the truncated product over $p \leq \log X_\theta$ replaced by the product over all primes $p$ (and without the error terms!). But because $\mathcal{M}_p(\mathcal{F},\cdot) \leq 1$ for all sufficiently large $p$, the product over all $p$ is at most the truncated product over $p \leq \log X_\theta$ for large enough $X$. □

Next, we have the following lemma, which is a consequence of Riemann summation together with the fact that $\psi$ is compactly supported:

**Lemma 149.** *Let $Q < T_\theta$ for some $\theta < 1$, and for each $p \leq Q$, let $\phi_p\colon V_{4,a}(\mathbb{Z}_p) \to \mathbb{R}$ be an acceptable function. Then we have that*

$$\sum_{a\ll_\psi T}\left(\mathrm{Vol}\big(\psi|_{\frac{a}{T}}\big)\prod_{p\leq Q}\int_{V_{4,a}(\mathbb{Z}_p)}\phi_p(f)df\right) = T\mathrm{Vol}(\psi)\prod_{p\leq Q}\int_{V_4(\mathbb{Z}_p)}\phi_p(f)df + o(T),$$

*where "$a \ll_\psi T$" means that $a$ is at most a positive constant times $T$, where the constant depends on $\psi$.*

Recall the definition of $T_a$ in (4.48). Using Corollary 148 and Lemma 149, we find that

$$\sum_{0<|a|\ll_\psi \frac{X^{1/6}}{t^4}} \alpha_\infty |\mathcal{J}_{\mathscr{A}_4}| \mathrm{Vol}(\mathcal{F}_{\mathscr{A}_4}) a^6 \nu(T_a) \mathrm{Vol}\big(\psi|_{\frac{at^4}{X^{1/6}}}\big) \leq$$
$$\sum_{0<|a|\ll_\psi \frac{X^{1/6}}{t^4}} 4\mathrm{Vol}\big(\psi|_{\frac{at^4}{X^{1/6}}}\big) \Big(\tau_{\mathscr{A}_4}^{(\log X_\theta)} \prod_{p\leq \log X_\theta} \int_{V_{4,a}(\mathbb{Z}_p)} \mathcal{M}_p(\mathcal{F}, f) df + O(X_\theta^{-1/120+\epsilon} + E(a))\Big) \leq$$
$$4\tau_{\mathscr{A}_4}^{(\log X_\theta)} \frac{X^{1/6}}{t^4} \mathrm{Vol}(\psi) \prod_{p\leq \log X_\theta} \int_{V(\mathbb{Z}_p)} \mathcal{M}_p(\mathcal{F}, f) df + o\Big(\frac{X^{1/6}}{t^4}\Big) + O(E), \tag{4.55}$$

where we estimate the error term using the following lemma:

**Lemma 150.** *We have that*

$$\sum_{0<|a|\ll_\psi \frac{X^{1/6}}{t^4}} \mathrm{Vol}\big(\psi|_{\frac{at^4}{X^{1/6}}}\big)(X_\theta^{-1/120+\epsilon} + E(a)) \ll (\log X_\theta)^{-2} \frac{X^{1/6}}{t^4}.$$

*Proof.* The first term is easily bounded: we have

$$\sum_{0<|a|\ll_\psi \frac{X^{1/6}}{t^4}} X_\theta^{-1/120+\epsilon} \ll \frac{X^{1/6}}{t^4 X_\theta^{1/120-\epsilon}},$$

which is sufficient. For the second term, we interchange summation:

$$\sum_{0<|a|\ll_\psi \frac{X^{1/6}}{t^4}} E(a) \ll \sum_{p\geq \log X_\theta} \frac{1}{p} \times \frac{X^{1/6}}{p^2 t^4} \ll (\log X_\theta)^{-2} \frac{X^{1/6}}{t^4}.$$

This concludes the proof of the lemma. □

In conjunction with Theorem 144, the estimate (4.55) yields the following.

$$\mathcal{I}^{(i)} \leq \frac{4\tau_{\mathscr{A}_4}^{(\log X_\theta)} \mathrm{Vol}(\psi)}{\sigma_i \mathrm{Vol}(\Theta)} \mathrm{Vol}(\mathcal{F}_{\mathrm{PGL}}) \prod_{p\leq \log X_\theta} \mathrm{Vol}(\mathcal{M}_p(\mathcal{F}, \cdot)) X^{5/6} + o(X^{5/6}).$$

We know that $\mathrm{Vol}(\psi)/\mathrm{Vol}(\Theta) = |\mathcal{J}_{\mathrm{PGL}}| \mathrm{Vol}(\mathcal{H}^{\pm})$ and that $\mathrm{Vol}(\mathcal{M}_p(\mathcal{F}, \cdot)) = |\mathcal{J}_{\mathrm{PGL}}|_p \nu_p(\mathcal{F}) \alpha_p$.

Together with the equalities $1/\sigma_0 + 1/\sigma_{2+} = 1/\sigma_1 = \alpha_\infty$, we obtain

$$\mathcal{I}^{\pm} \leq 8\tau_{\mathscr{A}_4}^{(\log X_\theta)}\tau_{\mathrm{PGL}}^{(\log X_\theta)}\nu(\mathcal{F})\widehat{\mathcal{H}^{\pm}}(0)X^{5/6} + o(X^{5/6}).$$

Therefore, we have proven the following result.

**Theorem 151.** *We have that*

$$\lim_{X\to\infty} \frac{1}{\nu(\mathcal{F})\widehat{\mathcal{H}^{\pm}}(0)X^{5/6}} \sum_{E\in\mathcal{F}^{\pm}} \sum_{\substack{\sigma\in \mathrm{Sel}_2(E)\\ \sigma\neq 1}} \big(|S_2(\sigma)| - 2\big)\mathcal{H}_X(\iota(E)) \leq 8.$$

*Proof.* This follows since $\tau_{\mathscr{A}_4}^{(\log X_\theta)}$ and $\tau_{\mathrm{PGL}}^{(\log X_\theta)}$ tend to 1 as $X$ tends to infinity. □

Let $\chi^{\pm}\colon \mathrm{Inv}(\mathbb{R})^{\pm} \to \mathbb{R}$ be the characteristic function of the set of elements in $\mathrm{Inv}(\mathbb{R})^{\pm}$ with height $\leq 1$. For a sequence of real numbers $\epsilon \to 0$, consider smooth, compactly supported functions $\mathcal{H}_\epsilon^{\pm}$ such that

(a) For every $x \in \mathrm{Inv}(\mathbb{R})^{\pm}$, we have that $\mathcal{H}_\epsilon^{\pm}(x) > \chi^{\pm}(x)$.

(b) For every $\epsilon$, we have that

$$\int_{\mathrm{Inv}(\mathbb{R})} \big(\mathcal{H}_\epsilon^{\pm}(x) - \chi(x)\big) < \epsilon.$$

Then it follows that

$$\frac{1}{\nu(\mathcal{F})\widehat{\chi^{\pm}}(0)X^{5/6}} \sum_{\substack{E\in\mathcal{F}^{\pm}\\ H(E)<X}} |\mathrm{Sel}_2(E)|^2 =$$

$$3 + \frac{1}{\nu(\mathcal{F})\widehat{\chi^{\pm}}(0)X^{5/6}} \sum_{\substack{E\in\mathcal{F}^{\pm}\\ H(E)<X}} (|\mathrm{Sel}_2(E)| - 1)|\mathrm{Sel}_2(E)| + o(1) =$$

$$3 + \frac{1}{\nu(\mathcal{F})\widehat{\chi^{\pm}}(0)X^{5/6}} \sum_{\substack{E\in\mathcal{F}^{\pm}\\ H(E)<X}} \sum_{\substack{\sigma\in \mathrm{Sel}_2(E)\\ \sigma\neq 1}} \big((|S_2(\sigma)| - 2) + 2\big) + o(1) \leq$$

$$7 + \frac{1}{\nu(\mathcal{F})\widehat{\chi^{\pm}}(0)X^{5/6}} \sum_{E \in \mathcal{F}^{\pm}} \sum_{\substack{\sigma \in \mathrm{Sel}_2(E) \\ \sigma \neq 1}} \big(|S_2(\sigma)| - 2\big)\mathcal{H}^{\pm}_{\epsilon,X}(\iota(E)) + o(1) \leq$$

$$7 + \frac{8\nu(\mathcal{F})\widehat{\mathcal{H}^{\pm}_{\epsilon}}(0)X^{5/6}}{\nu(\mathcal{F})\widehat{\chi^{\pm}}(0)X^{5/6}} + o_{\epsilon}(1) \leq$$

$$15 + O(\epsilon) + o_{\epsilon}(1).$$

Letting $X$ tend to infinity first, and then letting $\epsilon$ tend to 0, we obtain Theorem 97.

# 4.A Appendix: Integral orbits from odd-degree divisors on hyperelliptic curves

Note: This section is written in the notation and conventions of the paper [17]. Specifically:

- Let $p$ be a prime number, and let $n \geq 4$ be even. For a binary form $f \in \mathbb{Q}_p[x, y]$ of even degree $n = 2g + 2 \geq 4$ having nonzero discriminant, we denote by $C_f \colon z^2 = f(x, y)$ the corresponding genus-$g$ hyperelliptic curve, by $J_f = \mathrm{Pic}^0_{C_f/\mathbb{Q}_p}$ the Jacobian of $C_f$, and by $J^1_f = \mathrm{Pic}^1_{C_f/\mathbb{Q}_p}$ the principal homogeneous space for $J_f$ whose points correspond to the divisor classes of degree one on $C_f$.

- Let $\theta \in K_f^{\times}$ be the root of $f$. We denote by "$x - \theta$" the Cassels map $\mathrm{Div}_{C_f/\mathbb{Q}_p} \to (K_f/K_f^{\times 2}\mathbb{Q}_p^{\times})_{N \equiv f_0}$ (see [39, §2] for the definition).

- We write $I_f(k)$ for the fractional ideal $I_f^k$ and $N$ for the norm N defined in §1.2.

- We say that a pair $(I, \alpha)$ of a based fractional ideal $I$ and a number $\alpha \in K_f^{\times}$ is *good* if $I^2 \subset \alpha I_f(n-3)$ and $N(I)^2 = N(\alpha)f_0^{3-n}$.

## 4.A.1 Summary of the problem

In [17], Bhargava, Gross, and Wang proved the remarkable result that a positive proportion of hyperelliptic curves over $\mathbb{Q}$ have no rational points over any odd-degree extension of $\mathbb{Q}$. The

main results of their work (namely, Theorems 1, 2, 5–7, and 10–12, as well as Corollaries 3, 8, and 9 in [17]) rely on the following integral orbit construction, which is stated in the paper as Theorem 15:

**Theorem 152.** *There exists a positive integer $\kappa$ depending only on $n$ such that, for any integral binary form $f(x,y)$ of even degree $n = 2g+2$ with $C : z^2 = f(x,y)$ locally soluble over $\mathbb{Q}$, every $(\mathrm{SL}_n/\mu_2)(\mathbb{Q})$-orbit of locally soluble pairs $(A,B) \in \mathbb{Q}^2 \otimes \mathrm{Sym}_2 \mathbb{Q}^n$ such that $\det(Ax - By) = \kappa^2 f(x,y)$ contains an element in $\mathbb{Z}^2 \otimes \mathrm{Sym}_2 \mathbb{Z}^n$. In other words, the $(\mathrm{SL}_n/\mu_2)(\mathbb{Q})$-equivalence classes of locally soluble pairs $(A,B) \in \mathbb{Z}^2 \otimes \mathrm{Sym}_2 \mathbb{Z}^n$ such that $\det(Ax - By) = \kappa^2 f(x,y)$ are in bijection with the elements of $\mathrm{Sel}_2(J^1)$.*

The proof of Theorem 152 is given in [17, §9]. The first step is to observe that it suffices to prove the theorem with $\mathbb{Z}$ and $\mathbb{Q}$ replaced by $\mathbb{Z}_p$ and $\mathbb{Q}_p$ for each prime $p$, so long as the constant $\kappa = \kappa_p$ is equal to 1 for all but finitely many primes $p$. The proof of this local version of the theorem, which may be found on pp. 478–480 in the paper, is only correct when $f$ has leading coefficient $f_0 \in \mathbb{Z}_p^\times$. Specifically, there are two gaps in the proof:

- The displayed equations in the middle of p. 479 verifying that $I_D^2 \subset f_0^{2m} \alpha_0 I_f(n-3)$ are not always correct, because the numbers $a_1, \ldots, a_m$ may fail to be integral when $f_0 \notin \mathbb{Z}_p^\times$.
- The specialization argument on p. 479 used to compute the norm $N(I_D)$ is not always correct when $f_0 \notin \mathbb{Z}_p^\times$, as can be verified by directly calculating $N(I_D)$ in small cases (e.g., by taking $n = 4$ and $m = 1$).

The purpose of this section is to give a correct proof of (the local version of) Theorem 152. To deal with the possibility that the leading coefficient may fail to be a unit, we apply the tripartite strategy introduced in §4.2.2, splitting the proof into three successively more complicated cases. First, in §4.A.2.1, we construct the desired integral representative for primitive forms over $\mathbb{Z}_p$ where $p > n$; here the construction is facilitated by the fact that we can replace a form with a suitable $\mathrm{SL}_2(\mathbb{Z}_p)$-translate whose leading coefficient is not divisible by $p$. Then, in §4.A.2.2, we modify the construction given in §4.A.2.1 to handle imprimitive

forms over $\mathbb{Z}_p$ where $p > n$. We conclude in §4.A.2.3 by building upon the construction in §4.A.2.2 to resolve the case of forms over $\mathbb{Z}_p$ where $p < n$; here, we construct an integral representative with resolvent $p^{d_2}f$, where $d_2 \geq 1$ is an integer depending only on $n$.

## 4.A.2 Proof of Theorem 152

Fix a binary form $f \in \mathbb{Z}_p[x, y]$ of nonzero discriminant satisfying $\mathrm{Div}^1(C_f)(\mathbb{Q}_p) \neq \varnothing$ along with an element $\alpha_0 \in J_f^1(\mathbb{Q}_p)/2J_f(\mathbb{Q}_p)$.

### 4.A.2.1 Construction of integral representative for $f$ primitive and $p > n$

Suppose that $f$ is primitive. Then, since $p > n$, there exists $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z}_p)$ such that the binary form

$$f'(x, y) := f((x, y) \cdot \gamma) = \sum_{i=0}^{n} f_i' x^{n-i} y^i$$

has leading coefficient $f_0' \in \mathbb{Z}_p^\times$. Let $\theta' = \frac{-c+d\theta}{a-b\theta} \in K_{f'}$ be the root of $f'$, let $R_{f'} = \mathbb{Z}_p\langle \zeta_1', \ldots, \zeta_{n-1}' \rangle$ denote the basis elements of $R_{f'}$ defined with respect to $\theta'$, and let $N'$ denote the norm with respect to this basis. Let $\alpha_0'$ be the image of $\alpha_0$ under the isomorphism $J_f^1(\mathbb{Q}_p)/2J_f(\mathbb{Q}_p) \simeq J_{f'}^1(\mathbb{Q}_p)/2J_{f'}(\mathbb{Q}_p)$ induced by $\gamma$. We first construct a pair $(I', \alpha')$, where $I'$ is a based fractional ideal of $R_{f'}$ and $\alpha' \in K_{f'}$ is a representative of $(x - \theta')(\alpha_0')$ such that $I'^2 \subset \alpha' I_{f'}(n-3)$ and $N'(I')^2 = N'(\alpha') f_0'^{3-n}$. Then, the orbit arising from $(I', \alpha')$ has resolvent $f'$, so upon applying $\gamma^{-1}$, we obtain the desired integral representative with resolvent $f$.

Because we have assumed that $\mathrm{Div}^1(C_f)(\mathbb{Q}_p) \neq \varnothing$, [17, Proposition 21] implies that there exists a rational divisor $\widetilde{D} \in \mathrm{Div}^1(C_{f'})(\mathbb{Q}_p)$ such that $\alpha_0' = [\widetilde{D}] \in J_{f'}^1(\mathbb{Q}_p)/2J_{f'}(\mathbb{Q}_p)$. The next lemma shows that we can replace the divisor $\widetilde{D}$ with a new divisor $D$ satisfying certain properties that turn out to be crucial in constructing the desired ideal $I'$. For monic forms $f'$, this lemma was proven in [121, §3]. Here, we extend that argument to handle classes $\widetilde{D} \in \mathrm{Pic}^1(C_{f'})(\mathbb{Q}_p)$, where $f_0' \in \mathbb{Z}_p^\times$ is not necessarily equal to 1.

**Lemma 153.** *There exists an effective divisor $D = \sum_{i=1}^{m}(P_i') \in \mathrm{Div}(C_{f'})(\mathbb{Q}_p)$ such that the following three properties are satisfied:*

- *$m \leq \frac{n}{2}$ is odd;*
- *$P_i' = (a_i', 1, c_i') \in C_{f'}(\overline{\mathbb{Q}}_p)$ with $a_i' \in \mathcal{O}_{\overline{\mathbb{Q}}_p}$ and $c_i' \neq 0$ for each $i \in \{1, \ldots, m\}$; and*
- *$(x - \theta')(D) = (x - \theta')(\widetilde{D}) \in (K_{f'}^{\times}/K_{f'}^{\times 2}\mathbb{Q}_p^{\times})_{N \equiv f_0'}$.*

*Proof.* We construct the desired divisor $D$ in a sequence of four steps as follows:

Step 1: It is a standard fact (see [93, §5]) that there exists a principal divisor $D_1 \in \mathrm{Div}^0(C_{f'})(\mathbb{Q}_p)$ such that $D + D_1$ is supported neither at the ramification points of $C_{f'}$ over $\mathbb{P}^1_{\mathbb{Q}_p}$, nor at the points $(1, 0, \pm\sqrt{f_0'}) \in C_{f'}(\overline{\mathbb{Q}}_p)$ lying above infinity in $\mathbb{P}^1_{\mathbb{Q}_p}$. We define $D$ to be $\widetilde{D} + D_1$; by translating $D$ with divisors of the form $2 \cdot D'$, where $D'$ is the divisor corresponding to a closed point of $C_{f'}$ over $\mathbb{Q}_p$, we may assume that each point in the support of $D$ occur with multiplicity equal to 1. It is clear that $(x - \theta')(\widetilde{D}) = (x - \theta')(D)$.

Step 2: We now construct a divisor $D_2 \in \mathrm{Pic}^0(C_{f'})(\mathbb{Q}_p)$ such that $D - D_2$ has at most $\frac{n}{2}$ non-infinite points in its support. In the previous paragraph, we arranged for $D$ to take the form $D = \sum_{i=1}^{k}(Q_i)$, where $Q_i = (\mathfrak{a}_i, 1, \mathfrak{c}_i) \in C_{f'}(\overline{\mathbb{Q}}_p)$ with $\mathfrak{c}_i \neq 0$ for each $i$. If $k > \frac{n}{2}$, let $\mathfrak{P} \in \mathbb{Q}_p[x]$ be the monic polynomial of degree $k$ defined by $\mathfrak{P}(x) = \prod_{i=1}^{k}(x - \mathfrak{a}_i)$, and let $\mathfrak{R} \in \mathbb{Q}_p[x]$ be the unique (not necessarily monic) polynomial of minimal degree at most $k-1$ such that $\mathfrak{R}(\mathfrak{a}_i) = \mathfrak{c}_i$ for each $i \in \{1, \ldots, k\}$. Then the polynomial $\mathfrak{R}(x)^2 - f'(x, 1) \in \mathbb{Q}_p[x]$ has a root $x = \mathfrak{a}_i$ for each $i \in \{1, \ldots, k\}$, so we have that $\mathfrak{R}(x)^2 - f'(x, 1) = \mathfrak{P}(x)\mathfrak{H}(x)$ for some polynomial $\mathfrak{H} \in \mathbb{Q}_p[x]$. Because $f'$ is separable over $\mathbb{Q}_p$, we have that $\mathfrak{H} \not\equiv 0$.

Consider the rational function $g := y - \mathfrak{R}(x)$ on $C_{f'}$. Note that $g$ is defined over $\mathbb{Q}_p$, that the zeros of $g$ are precisely the zeros of $\mathfrak{P} \cdot \mathfrak{H}$, and that the poles of $g$ lie over infinity. Thus, letting $\mathrm{div}(g)$ be the principal divisor associated to the function $g$, we have that $D - \mathrm{div}(g)$ is supported over the zeros of $\mathfrak{H}$ and over the infinite points. But since $k > \frac{n}{2}$, we have that

$$\deg \mathfrak{H} = \deg(\mathfrak{R}(x)^2 - f'(x, 1)) - \deg \mathfrak{P}(x) \leq k - 1,$$

so $D - \mathrm{div}(g)$ has strictly fewer than $k$ non-infinite points in its support. By iterating the above process, we obtain a sequence of functions $g = g_1, g_2, \ldots, g_\ell$ until $D - \sum_{i=1}^{\ell} \mathrm{div}(g_i)$ has at most $\frac{n}{2}$ non-infinite points in its support. We let $D_2 = \sum_{i=1}^{\ell} \mathrm{div}(g_i)$, and we redefine $D$ to be $D - D_2$. Just as in Step 1, we modify $D$ so as to ensure that each point in the support of $D$ occurs with multiplicity 1. Once again, the above modifications leave $(x - \theta')(D)$ unchanged.

Step 3: We now claim that we can simply delete every point in the support of $D$ that is not of the form $(\mathfrak{a}, 1, \mathfrak{c})$, where $\mathfrak{a} \in \mathcal{O}_{\overline{\mathbb{Q}}_p}$. Observe that there are two ways for a point $(\mathfrak{a}, \mathfrak{b}, \mathfrak{c}) \in C_{f'}(\overline{\mathbb{Q}}_p)$ in the support of $D$ to fail to be in this form: either $\mathfrak{b} \neq 0$ and $\mathfrak{a}/\mathfrak{b} \notin \mathcal{O}_{\overline{\mathbb{Q}}_p}$, or $(\mathfrak{a}, \mathfrak{b}, \mathfrak{c}) = (1, 0, \pm\sqrt{f'_0})$ is one of the points at infinity. We handle each of these two cases as follows:

*Case 1*: First suppose that we have a point $Q_1 = (\mathfrak{a}_1, 1, \mathfrak{c}_1) \in C_{f'}(\overline{\mathbb{Q}}_p)$ in the support of $D$ such that $\mathfrak{a}_1 \notin \mathcal{O}_{\overline{\mathbb{Q}}_p}$. Let $\{Q_i = (\mathfrak{a}_i, 1, \mathfrak{c}_i) : 1 \leq i \leq k\}$ be the set of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-conjugates of $Q_1$; since $D$ is a rational divisor, each $Q_i$ occurs with the same multiplicity $\nu$. We claim that $\chi := \prod_{i=1}^{k} (\mathfrak{a}_i - \theta') \in K_{f'}^{\times 2} \mathbb{Q}_p^{\times}$. Indeed, since $\mathfrak{a}_i \notin \mathcal{O}_{\overline{\mathbb{Q}}_p}$, the denominator of $\chi$ is equal to $p^j$ for some positive integer $j$, and for a suitable choice of $u \in \mathbb{Z}_p^{\times}$, we have $up^j\chi \in K_f^{\times 2}$. We then redefine $D$ to be $D - \sum_{i=1}^{k} Q_i$.

*Case 2*: Now suppose that $(1, 0, \sqrt{f'_0}) \in C_f(\overline{\mathbb{Q}}_p)$ is in the support of $D$. If $f'_0 \notin \mathbb{Q}_p^{\times 2}$, it follows that $(1, 0, -\sqrt{f'_0})$ is also in the support of $D$, and so the support of $D$ over the points at infinity is a multiple of the hyperelliptic class, and it follows from [93, Proposition 5.1] that this class lies in the kernel of the "$x - \theta'$" map. If $f'_0 \in \mathbb{Q}_p^{\times 2}$, then [39, §2] implies that $(x - \theta')(1, 0, \pm\sqrt{f'_0}) = f'_0 \equiv 1$. We may thus simply delete all of the infinite points in the support of $D$.

The modifications performed in both cases 1 and 2 above leave $(x - \theta')(D)$ unchanged.

Step 4: It now remains to adjust $D$ so that $m$ is odd. This may be arranged by means of the argument in [17, last paragraph of p. 478 to first paragraph of p. 479].

This completes the proof of the lemma. □

Let $D$ be as in Lemma 153. We define polynomials $\mathcal{P}$, $\mathcal{R}$, and $\mathcal{H}$, much as in Step 2 of the proof of Lemma 153; this time, however, we strive to ensure that these polynomials have integral coefficients. Let $\mathcal{P} \in \mathbb{Q}_p[x]$ be the monic polynomial of degree $m$ defined by

$$\mathcal{P}(x) = \prod_{i=1}^{m} (x - a_i').$$

By our construction of $D$ in Lemma 153, the class $\alpha' := \mathcal{P}(\theta') \in (K_f^\times / K_f^{\times 2} \mathbb{Q}_p^\times)_{N \equiv f_0'}$ is equal to $(x - \theta')(\alpha_0')$. Next, let $\mathcal{R} \in \mathbb{Q}_p[x]$ be the unique (not necessarily monic) polynomial of minimal degree at most $m - 1$ such that

$$\mathcal{R}(a_i') = c_i' \quad \text{for each } i \in \{1, \ldots, m\}.$$

Then the polynomial $\mathcal{R}(x)^2 - f'(x, 1) \in \mathbb{Q}_p[x]$ has a root at $x = a_i'$ for each $i \in \{1, \ldots, m\}$, so there exists a polynomial $\mathcal{H} \in \mathbb{Q}_p[x]$ such that $\mathcal{R}(x)^2 - f'(x, 1) = \mathcal{P}(x)\mathcal{H}(x)$. Because we chose $D$ so that $a_i' \in \mathcal{O}_{\overline{\mathbb{Q}}_p}$ for each $i$, we have that $\mathcal{P} \in \mathbb{Z}_p[x]$. We proceed under the assumption that we also have $\mathcal{R} \in \mathbb{Z}_p[x]$; at the end of this section, we explain how to deal with the case where $\mathcal{R} \notin \mathbb{Z}_p[x]$. Then, because $\mathcal{P}, \mathcal{R}, f'(x, 1) \in \mathbb{Z}_p[x]$, it follows from the relation $\mathcal{R}(x)^2 - f'(x, 1) = \mathcal{P}(x)\mathcal{H}(x)$ that $\mathcal{H} \in \mathbb{Z}_p[x]$ as well.

Consider the following $R_{f'}$-submodule of $K_{f'}$:

$$I' = R_{f'} \langle \mathcal{R}(\theta'), \mathcal{P}(\theta') \rangle.$$

Note that $\theta' \in R_{f'}$ because $f_0' \in \mathbb{Z}_p^\times$, so since $\mathcal{P}, \mathcal{R} \in \mathbb{Z}_p[x]$, the fractional ideal $I'$ is in fact an integral ideal of $R_{f'}$. We now prove that the pair $(I', \alpha')$ is good:

**Lemma 154.** *We have that $I'^2 \subset \alpha' I_{f'}(n-3)$, and for some choice of a basis of $I'$, we have that $N'(I')^2 = N'(\alpha') f_0'^{3-n}$.*

*Proof.* Computing the square of $I'$ yields the following:

$$I'^2 = R_{f'}\langle \mathcal{R}(\theta')^2, \mathcal{R}(\theta')\mathcal{P}(\theta'), \mathcal{P}(\theta')^2\rangle = \alpha' R_{f'}\langle \mathcal{H}(\theta'), \mathcal{R}(\theta'), \mathcal{P}(\theta')\rangle \subset \alpha' R_{f'},$$

where the last step above follows from the fact that $\theta' \in R_{f'}$ and $\mathcal{P}, \mathcal{R}, \mathcal{H} \in \mathbb{Z}_p[x]$. Since $p \nmid f'_0$, we have that $R_{f'} = I_{f'}(n-3)$, and the first assertion follows.

That $N'(I')^2$ and $N'(\alpha')f_0'^{3-n}$ generate the same fractional ideal of $\mathbb{Z}_p$ follows immediately from [15, proof of Proposition 8.5]. Since both $N'(I')^2$ and $N'(\alpha')f_0'^{3-n}$ are elements of $\mathbb{Q}_p^{\times 2}$, we can choose a basis of $I'$ so as to ensure that $N'(I')^2 = N'(\alpha')f_0'^{3-n}$. □

Next suppose that $\mathcal{R} \notin \mathbb{Z}_p[x]$. Then since $f'_0 \in \mathbb{Z}_p^\times$, it follows from [105, proof of Proposition 12] (see also [15, proof of Proposition 8.5]) that we can modify $D$ so that it is supported on at most $m-2$ points while still preserving the properties in Lemma 153. If the value of new polynomial $\mathcal{R}$ arising from the modified $D$ fails to be integral, we repeat the process until $\mathcal{R}$ becomes integral or $D$ is supported on at most 1 point. In the latter setting, if $D$ is supported on no points, then we apply Step 4 in the proof of Lemma 153; if $D$ is supported on 1 point, the polynomial $\mathcal{R}$ is readily seen to be integral.

#### 4.A.2.2 Construction of integral representative for $f$ imprimitive and $p > n$

Suppose that we have $\gcd(f_0, \ldots, f_n) = p^d$ for some $d > 0$. We first show that we can reduce the problem to the case where $d = 1$. To do this, suppose that $d > 1$, and let $\widetilde{f} = p^{-2\lfloor d/2 \rfloor} f \in \mathbb{Z}_p[x, y]$; notice that the greatest common divisor of the coefficients of $\widetilde{f}$ is either 1 or $p$. Then $C_f \simeq C_{\widetilde{f}}$, and this isomorphism induces an identification $J_f^1(\mathbb{Q}_p)/2J_f(\mathbb{Q}_p) \simeq J_{\widetilde{f}}^1(\mathbb{Q}_p)/2J_{\widetilde{f}}(\mathbb{Q}_p)$; letting $\widetilde{\alpha}_0$ be the image of $\alpha_0$ under this identification, observe that $(x-\theta)(\alpha_0) = (x-\theta)(\widetilde{\alpha}_0)$.

Now, suppose that we have constructed a pair $(\widetilde{I}, \widetilde{\alpha})$ that is good for $\widetilde{f}$, where $\widetilde{\alpha} \in K_{\widetilde{f}}^\times = K_f^\times$ is a representative of $(x-\theta)(\widetilde{\alpha}_0)$, and let $(A, B) \in \mathbb{Z}_p^2 \otimes_{\mathbb{Z}_p} \mathrm{Sym}_2 \mathbb{Z}_p^n$ be any representative of the corresponding $(\mathrm{SL}_n/\mu_2)(\mathbb{Z}_p)$-orbit. Let $\xi_d \in \mathrm{GL}_n(\mathbb{Q}_p)$ denote the diagonal matrix with

diagonal entries $p^{\lfloor d/2 \rfloor}$, 1, ..., 1. Consider the pair

$$\xi_d \cdot (A, B) := \left(\xi_d A \xi_d^T, \xi_d B \xi_d^T\right) \in \mathbb{Z}_p^2 \otimes_{\mathbb{Z}_p} \mathrm{Sym}_2 \mathbb{Z}_p^n,$$

and observe that it has resolvent $f$. In the following lemma, we determine the rational orbit of this new pair $\xi_d \cdot (A, B)$ explicitly:

**Lemma 155.** *The* $(\mathrm{SL}_n / \mu_2)(\mathbb{Q}_p)$*-orbit of* $\xi_d \cdot (A, B)$ *corresponds via the parametrization in [17, Theorem 16] to the class* $p^{-2\lfloor d/2 \rfloor} \widetilde{\alpha} \equiv \widetilde{\alpha} \in K_f^\times / K_f^{\times 2} \mathbb{Q}_p^\times$.

*Proof.* We work over $\mathbb{Q}_p$, where based fractional ideals are just bases. For each of $I_{\widetilde{f}}(n-3)$ and $I_f(n-3)$, the standard basis (see [17, §2]) is given by

$$I_{\widetilde{f}}(n-3) = \mathbb{Q}_p\langle 1, \theta, \ldots, \theta^{n-3}, p^{-2\lfloor d/2 \rfloor}\zeta_{n-2}, p^{-2\lfloor d/2 \rfloor}\zeta_{n-1}\rangle, \quad \text{and}$$
$$I_f(n-3) = \mathbb{Q}_p\langle 1, \theta, \ldots, \theta^{n-3}, \zeta_{n-2}, \zeta_{n-1}\rangle.$$

We claim that $\xi_d \cdot (A, B)$ corresponds to the pair $(\widetilde{I}', p^{-2\lfloor d/2 \rfloor}\widetilde{\alpha})$, where $\widetilde{I}'$ is obtained from $\widetilde{I}$ by scaling the first basis element by $p^{\lfloor d/2 \rfloor}$ (up to the orientation of $\widetilde{I}'$, which can be chosen as needed). Let $N$ (resp., $\widetilde{N}$) denote the based fractional ideal norm with respect to the standard basis of $R_f$ (resp., $R_{\widetilde{f}}$). Then a calculation reveals that $N(I) = p^{-2\lfloor d/2 \rfloor (n-1)} \widetilde{N}(I)$ for any basis $I$. Note that this does *not* extend to norms of numbers: it follows from the definition of the norm of a number that $\widetilde{N}(\widetilde{\alpha}) = N(\widetilde{\alpha})$. To prove the claim, it suffices to show that $N(\widetilde{I}')^2 = N(p^{-2\lfloor d/2 \rfloor}\widetilde{\alpha}) f_0^{3-n}$, which is equivalent to showing that

$$\left(p^{-2\lfloor d/2 \rfloor (n-1)} p^{\lfloor d/2 \rfloor} \widetilde{N}(\widetilde{I})\right)^2 = \left(p^{-2\lfloor d/2 \rfloor n} \widetilde{N}(\widetilde{\alpha})\right) f_0^{3-n},$$

but this follows from the fact that $\widetilde{N}(\widetilde{I})^2 = \widetilde{N}(\widetilde{\alpha})(p^{-2\lfloor d/2 \rfloor} f_0)^{3-n}$. □

We have thus reduced the problem to the case where $d \in \{0, 1\}$; if $d = 0$, then the construction in §4.A.2.1 applies, so we assume that $d = 1$ in the remainder of this section.

Just like in §4.A.2.1, we now replace $f$ with its translate $f'(x,y) = f((x,y)\cdot\gamma)$ by an element $\gamma \in \mathrm{SL}_2(\mathbb{Z}_p)$; this time, however, we choose $\gamma$ so that $p$ divides the leading coefficient $f'_0$ of $f'$ exactly once (such a $\gamma$ exists because $p > n$). Recalling the notation from §4.A.2.1, it once again suffices to construct a pair $(I', \alpha')$, where $I'$ is a based fractional ideal of $R_{f'}$ and $\alpha' \in K_{f'}$ is a representative of $(x-\theta')(\alpha'_0)$ such that $I'^2 \subset \alpha' I_{f'}(n-3)$ and $N'(I')^2 = N'(\alpha') f_0'^{3-n}$.

Just like we argued in §4.A.2.1, [17, Proposition 21] implies that there exists a rational divisor $\widetilde{D} \in \mathrm{Div}^1(C_{f'})(\mathbb{Q}_p)$ such that $\alpha'_0 = [\widetilde{D}] \in J^1_{f'}(\mathbb{Q}_p)/2J_{f'}(\mathbb{Q}_p)$. The following lemma gives the analogue of Lemma 153 in the present setting:

**Lemma 156.** *There exists an effective divisor $D = \sum_{i=1}^m (P'_i) \in \mathrm{Div}(C_{f'})(\mathbb{Q}_p)$ such that the following three properties are satisfied:*

- *$m \leq \frac{n}{2}$ is odd;*
- *$P'_i = (a'_i, 1, c'_i) \in C_{f'}(\overline{\mathbb{Q}}_p)$ with $a'_i \in \mathcal{O}_{\overline{\mathbb{Q}}_p}$ and $c'_i \neq 0$ for each $i \in \{1, \ldots, m\}$; and*
- *$(x-\theta')(D) = (x-\theta')(\widetilde{D}) \in K_{f'}^\times / K_{f'}^{\times 2}\mathbb{Q}_p^\times$.*

*Proof.* Steps 1 and 2 in the proof of Lemma 153 go through without change. As for Step 3, let $f''(x,y) = p^{-1}f'(x,y)$. Then the "$x-\theta'$" map for $f'$ is the same as that for $f''$; thus, the argument in case 1 of Step 3 implies that we can delete all points of the form $(\mathfrak{a}, 1, \mathfrak{c})$ such that $\mathfrak{a} \notin \mathcal{O}_{\overline{\mathbb{Q}}_p}$. Since the points $(1, 0, \pm\sqrt{f'_0})$ are evidently not defined over $\mathbb{Q}_p$, the number $m$ must be odd, and there is no need for Step 4. □

Let $D$ be as in Lemma 156. We define polynomials $\mathcal{P}$, $\mathcal{R}$, and $\mathcal{H}$, much as in §4.A.2.1; this time, however, we strive to ensure not only that these polynomials have integral coefficients, but also that the coefficients of $\mathcal{R}$ are divisible by $p$. Let $\mathcal{P} \in \mathbb{Q}_p[x]$ be the monic polynomial of degree $m$ defined by

$$\mathcal{P}(x) = \prod_{i=1}^m (x - a'_i).$$

By our construction of $D$ in Lemma 156, the class $\alpha' := \mathcal{P}(\theta') \in (K_f^\times / K_f^{\times 2}\mathbb{Q}_p^\times)_{N \equiv f_0'}$ is equal to $(x - \theta')(\alpha_0')$. Next, let $\mathcal{R} \in \mathbb{Q}_p[x]$ be the unique (not necessarily monic) polynomial of minimal degree at most $m-1$ such that

$$\mathcal{R}(a_i') = c_i' \quad \text{for each } i \in \{1, \dots, m\}.$$

Then the polynomial $\mathcal{R}(x)^2 - f'(x,1) \in \mathbb{Q}_p[x]$ has a root at $x = a_i'$ for each $i \in \{1, \dots, m\}$, so there exists a polynomial $\mathcal{H} \in \mathbb{Q}_p[x]$ such that $\mathcal{R}(x)^2 - f'(x,1) = \mathcal{P}(x)\mathcal{H}(x)$. Because we chose $D$ so that $a_i' \in \mathcal{O}_{\overline{\mathbb{Q}}_p}$ for each $i$, we have that $\mathcal{P} \in \mathbb{Z}_p[x]$. We proceed under the assumption that we also have $\mathcal{R} \in p\mathbb{Z}_p[x]$; at the end of this section, we explain how to deal with the case where $\mathcal{R} \notin p\mathbb{Z}_p[x]$. Then, because $\mathcal{P} \in \mathbb{Z}_p[x]$ is monic and $\mathcal{R}, f'(x,1) \in p\mathbb{Z}_p[x]$, it follows from the relation $\mathcal{R}(x)^2 - f'(x,1) = \mathcal{P}(x)\mathcal{H}(x)$ that $\mathcal{H} \in p\mathbb{Z}_p[x]$ as well.

Let $f''$ be as in the proof of Lemma 156, and consider the following $R_{f''}$-submodule of $K_{f''} = K_f$:

$$I'' := R_{f''}\langle p^{-1}\mathcal{R}(\theta'), \mathcal{P}(\theta')\rangle.$$

Note that $\theta' \in R_{f''}$ because $p^{-1}f_0' \in \mathbb{Z}_p^\times$, so since $\mathcal{P} \in \mathbb{Z}_p[x]$ and $\mathcal{R} \in p\mathbb{Z}_p[x]$, the fractional ideal $I''$ is in fact an integral ideal of $R_{f''}$. Letting $N''$ denote the fractional ideal norm with respect to the standard basis $\mathbb{Z}_p\langle 1, p^{-1}\zeta_1', \dots, p^{-1}\zeta_{n-1}'\rangle$ of $R_{f''}$, it follows immediately from [15, proof of Proposition 8.5] that $p^m N''(I'')^2$ and $N''(\alpha')$ generate the same fractional ideal of $\mathbb{Z}_p$.

We now construct a list of elements that form part of a basis for $I''$ as a $\mathbb{Z}_p$-module:

**Lemma 157.** *Let $\ell := \frac{n-m-3}{2}$. Then the list $\mathcal{P}(\theta'), \theta'\mathcal{P}(\theta'), \dots, \theta'^{\ell}\mathcal{P}(\theta') \in I''$ can be extended to a basis of $I''$ as a $\mathbb{Z}_p$-module.*

*Proof.* Because $I''$ is an integral ideal of $R_{f''}$, it suffices to prove that $s(\vec{x}) := \sum_{i=0}^{\ell} x_i \theta'^i \mathcal{P}(\theta')$ is primitive as an element of $R_{f''}$ (i.e., that we have $s(\vec{x}) = R_{f''} \smallsetminus pR_{f''}$) for every primitive tuple $\vec{x} = (x_0, \dots, x_\ell) \in \mathbb{Z}_p^{\ell+1} \smallsetminus p\mathbb{Z}_p^{\ell+1}$. Given such a tuple $\vec{x}$, let $i \in \{0, \dots, \ell\}$ be the largest index such that $x_i \in \mathbb{Z}_p^\times$. Then, when $s(\vec{x})$ is expressed in the power basis $\mathbb{Z}_p\langle 1, \theta', \dots, \theta'^{n-1}\rangle$ of $R_{f''}$, the coefficient of $\theta'^{m+i}$ is a $p$-adic unit. Thus, $p^{-1}x \notin R_{f''}$, as desired. □

Consider the $R_{f''}$-submodule $pI'' \subset K_{f''}$. Then, by Lemma 157, we can find $\eta_1, \ldots, \eta_{n-\ell-1} \in pI''$ such that the following is a basis of $pI''$ as a $\mathbb{Z}_p$-module:

$$pI'' = \mathbb{Z}_p\big\langle \eta_1, \ldots, \eta_{n-\ell-1}, p\mathcal{P}(\theta'), \ldots, p\theta'^{\ell}\mathcal{P}(\theta')\big\rangle.$$

Let $I' \subset K_{f'}$ be the free rank-$n$ $\mathbb{Z}_p$-submodule with basis given by

$$I' = \mathbb{Z}_p\big\langle \eta_1, \ldots, \eta_{n-\ell-1}, \mathcal{P}(\theta'), \ldots, \theta'^{\ell}\mathcal{P}(\theta')\big\rangle.$$

It turns out that the $\mathbb{Z}_p$-submodule $I' \subset K_{f'}$ has the structure of $R_{f'}$-module:

**Lemma 158.** *The $\mathbb{Z}_p$-submodule $I' \subset K_{f'}$ is a fractional ideal of $R_{f'}$.*

*Proof.* It suffices to show that $I'$ is closed under multiplication by elements of $R_{f'}$. Since $pI''$ is closed under multiplication by elements of $R_{f''} \supset R_{f'}$, it suffices to verify that $\zeta_i'\theta'^j\mathcal{P}(\theta') \in I'$ for each $i \in \{1, \ldots, n-1\}$ and $j \in \{0, \ldots, \ell\}$, or equivalently that $(p\theta'^i)\mathcal{P}(\theta') \in I'$ for each $i \in \{1, \ldots, n+\ell-1\}$. But notice that $(p\theta'^i)\mathcal{P}(\theta') = \theta'^i(p\mathcal{P}(\theta')) \in pI'' \subset I'$, because $pI''$ is an $R_{f''}$-submodule of $K_{f''}$ and is hence closed under multiplication by powers of $\theta'$. □

We now prove that the pair $(I', \alpha')$ is good:

**Lemma 159.** *We have that $I'^2 \subset \alpha' I_{f'}(n-3)$, and for some choice of a basis of $I'$, we have that $N'(I')^2 = N'(\alpha')f_0'^{3-n}$.*

*Proof.* To prove the containment, it suffices to prove the following: that $\eta_i\eta_j \in \alpha' I_{f'}^2$ for each $i, j \in \{1, \ldots, n-\ell-1\}$, that $\eta_i\theta'^j\mathcal{P}(\theta') \in \alpha' I_{f'}^2$ for each $i \in \{1, \ldots, n-\ell-1\}$ and $j \in \{0, \ldots, \ell\}$, and that $\theta'^i\mathcal{P}(\theta')^2 \in \alpha' I_{f'}^2$ for each $i \in \{0, \ldots, 2\ell\}$. By construction, we have that $\eta_i \in pI''$ for each $i \in \{1, \ldots, n-\ell-1\}$. Thus, there exist $\beta_i, \gamma_i^{(0)}, \ldots, \gamma_i^{(\ell)} \in R_{f''}$ for each $i$ such that $\eta_i = \beta_i\mathcal{R}(\theta') + \sum_{k=0}^{\ell}\gamma_i^{(k)}(p\theta'^k\mathcal{P}(\theta'))$. Using the relation $\mathcal{R}(\theta')^2 = \mathcal{P}(\theta')\mathcal{H}(\theta')$, we

find that

$$\alpha'^{-1}(\eta_i\eta_j) \equiv \beta_i\beta_j\mathcal{H}(\theta') \pmod{p \cdot R_{f''}}, \quad \text{and} \tag{4.56}$$

$$\alpha'^{-1}(\eta_i\theta'^j\mathcal{P}(\theta')) = \eta_i\theta'^j \equiv \beta_i\theta'^j\mathcal{R}(\theta') \pmod{p \cdot R_{f''}}. \tag{4.57}$$

Since $\mathcal{R}, \mathcal{H} \in p\mathbb{Z}_p[x]$, it follows from (4.56) and (4.57) that every term in the expression of $\alpha'^{-1}(\eta_i\eta_j)$ and of $\alpha'^{-1}(\eta_i\theta'^j\mathcal{P}(\theta'))$ in the power basis $\mathbb{Q}_p\langle 1, \theta', \ldots, \theta'^{n-1}\rangle$ has coefficient divisible by $p$. We deduce that $\eta_i\eta_j$ and $\eta_i\theta'^j\mathcal{P}(\theta')$ are contained in $\alpha'\mathcal{R}_{f'} \subset \alpha' I_{f'}(n-3)$ for each possible $i, j$. Finally, notice that $\alpha'^{-1}\theta'^i\mathcal{P}(\theta')^2 = \theta'^i\mathcal{P}(\theta')$; since $\mathcal{P} \in \mathbb{Z}_p[x]$ has degree $m$, and since $\theta', \ldots, \theta'^{n-3} \in I_{f'}(n-3)$, it follows that $\theta'^i\mathcal{P}(\theta')^2 \in \alpha' I_{f'}(n-3)$ for each $i \in \{0, \ldots, 2\ell = n-m-3\}$.

Recall that $p^m N''(I'')^2$ and $N''(\alpha')$ generate the same fractional ideal of $\mathbb{Z}_p$. It follows that same holds for $p^{m-2}N'(pI'')^2$ and $N'(\alpha')$, and hence also for $N'(I')^2$ and $N'(\alpha')f_0'^{3-n}$. Because both $N'(I')^2$ and $N'(\alpha')f_0'^{3-n}$ are elements of $\mathbb{Q}_p^{\times 2}$, we can choose a basis of $I'$ so as to ensure that $N'(I')^2 = N'(\alpha')f_0'^{3-n}$, as desired. □

Next, suppose that $\mathcal{R} \notin p\mathbb{Z}_p[x]$. Then we also have that $\mathcal{R}^2 \notin p\mathbb{Z}_p[x]$. Letting $j(x) = p^{-1}(\mathcal{R}(x)^2 - f'(x,1)) = p^{-1}\mathcal{P}(x)\mathcal{H}(x)$, it follows that the coefficient of $x^i$ in $j(x)$ is a $p$-adic unit if $i = n$ and a $p$-adic integer for every $i \in \{2m-1, \ldots, n-1\}$, and that the coefficient of $x^i$ in $j(x)$ has negative valuation for some $i \in \{0, \ldots, 2m-2\}$. An analysis of the Newton polygon of $j$ then reveals that $j$ has at least $n-(2m-2)$ roots with negative valuation. Since $\mathcal{P}(x) \mid j(x)$ (as elements of $\mathbb{Q}_p[x]$), we also know that $j$ has $m$ roots with positive valuation at the $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-invariant list of values $a_1', \ldots, a_m' \in \mathcal{O}_{\overline{\mathbb{Q}}_p}$. Thus, letting $D' \in \mathrm{Div}(C_{f'})(\overline{\mathbb{Q}}_p)$ denote the divisor supported on the remaining roots of $j$ that have positive valuation, we have that $D' \in \mathrm{Div}(C_{f'})(\mathbb{Q}_p)$ and that $\deg D' \leq m-2$.

Just like in Step 2 of the proof of Lemma 153, consider the function $g := y - \mathcal{R}(x)$ on $C_{f'}$. Note that $g$ is defined over $\mathbb{Q}_p$, that the zeros of $g$ are precisely the zeros of $j$, and that the poles of $g$ lie over infinity. Applying the argument in Step 3 of the proof of Lemma 153 then

implies that $D'$ satisfies the conditions of the lemma with $m$ replaced by $\deg D' \leq m-2$. The proof now concludes by downward induction on $m$; once $m = 1$, it is clear that $\mathcal{R} \in p\mathbb{Z}_p[x]$.

#### 4.A.2.3 Construction of integral representative for $p < n$

Now let $p < n$. Just as in §4.A.2.2, we reduce the problem to the case where $p^d = \gcd(f_0, \ldots, f_n) \in \{1, p\}$. However, we might *not necessarily* be able to replace $f$ with an $\mathrm{SL}_2(\mathbb{Z}_p)$-translate $f'$ such that $\nu_p(f'_0) = d$, where $\nu_p \colon \mathbb{Q}_p^\times \to \mathbb{Z}$ denotes the usual $p$-adic valuation. Indeed, such a form $f'$ fails to exist precisely when $p < n$ and $f$ is divisible by $y\prod_{i=0}^{p-1}(x - iy)$ modulo $p$. Nonetheless, it follows from [5] that we can always find an $\mathrm{SL}_2(\mathbb{Z}_p)$-translate $f'$ of $f$ such that $\nu_p(f'_0) \leq d_1$ for some bounded integer $d_1 > 0$ depending only on the degree $n$.

Let $\alpha'_0 \in J^1_{f'}(\mathbb{Q}_p)/2J_{f'}(\mathbb{Q}_p)$ be as in §4.A.2.1. Let $\widetilde{f}(x, y) = f'(x, p^{d_2}y)$, where $d_2 \geq d_1 - d$ is an even integer, to be chosen shortly. Then $C_{f'} \simeq C_{\widetilde{f}}$, and this isomorphism induces an identification $J^1_{f'}(\mathbb{Q}_p)/2J_{f'}(\mathbb{Q}_p) \simeq J^1_{\widetilde{f}}(\mathbb{Q}_p)/2J_{\widetilde{f}}(\mathbb{Q}_p)$; letting $\widetilde{\alpha}_0$ be the image of $\alpha'_0$ under this identification, observe that $(x - \theta')(\alpha'_0) = (x - p^{d_2}\theta')(\widetilde{\alpha}_0)$. Let $\widetilde{\alpha} \in K^\times_{\widetilde{f}} = K^\times_{f'}$ be a representative of $(x - p^{d_2}\theta')(\widetilde{\alpha}_0)$. Because $\widetilde{f}$ is a multiple of a form with unit leading coefficient, the constructions described in §4.A.2.1–4.A.2.2 imply the existence of a pair $(\widetilde{I}, \widetilde{\alpha})$ that is good for $\widetilde{f}$, with one caveat: when $p = 2$, the argument in case 1 of Step 3 of the proof of Lemma 153 only goes through for $d_2 \gg 1$, where the implied constant depends only on $n$. Choosing $d_2$ so that this argument goes through, let $(\widetilde{A}, \widetilde{B}) \in \mathbb{Z}_p^2 \otimes_{\mathbb{Z}_p} \mathrm{Sym}_2 \mathbb{Z}_p^n$ be a representative of the $(\mathrm{SL}_n/\mu_2)(\mathbb{Z}_p)$-orbit corresponding to $(\widetilde{I}, \widetilde{\alpha})$ via [17, Theorem 16].

Since the pair $(\widetilde{A}, \widetilde{B})$ has resolvent $\widetilde{f}$, it follows that the pair $(p^{d_2}\widetilde{A}, \widetilde{B}) \in \mathbb{Z}_p^2 \otimes_{\mathbb{Z}_p} \mathrm{Sym}_2 \mathbb{Z}_p^n$ has resolvent $p^{nd_2}f'$. By an argument analogous to that used to prove Lemma 155, one verifies that the pair $(p^{d_2}\widetilde{A}, \widetilde{B})$ corresponds via [17, Theorem 16] to the pair $(\widetilde{I}, p^{2d_2}\widetilde{\alpha})$, where we view $\widetilde{I}$ as a based fractional ideal for $K_{p^{nd_2}f'}$. Using the action of $\mathrm{SL}_2(\mathbb{Z}_p)$, we can then transform the pair $(\widetilde{I}, p^{2d_2}\widetilde{\alpha})$ into a pair $(I, \alpha)$ that is good for $p^{nd_2}f$, as desired.

## 4.B Appendix: The second moment of the size of the 2-class group of monogenic cubic fields

The purpose of this section is to apply the argument developed in this chapter to study the second moment of the size of the 2-class group in families of monogenic cubic number fields. Specifically, we prove that the second moment is bounded, and conditional on a uniformity estimate, we prove that the bound we obtain is optimal. This result is the first of its kind toward determining the second moment of a class group distribution for number fields of degree greater than two, and it provides further evidence of the observation established in work of Bhargava–Hanke–Shankar [18] and Siad [108, 109] that monogenicity has an increasing effect on the 2-class groups of cubic number fields (cf. the discussion in §2.1).

### 4.B.1 Notation

In this section, we order forms $f \in V_{3,1}(\mathbb{Z})$ by the following height function, which is a slight renormalization of the height used in §2:

$$H(f) := \max\{|I(f)|^3, J(f)^2/4\}, \quad \text{where}$$
$$I(f) := a^2 - 3b \quad \text{and} \quad J(f) := -2a^3 + 9ab - 27c.$$

Note that $H$ descends to a well-defined height function on $N(\mathbb{Z})\backslash V_{n,1}(\mathbb{R})$ (in fact, the pair $(I(f), J(f))$ uniquely determines the $N(\mathbb{Z})$-equivalence class of $f \in V_{3,1}(\mathbb{Z})$).

Consider the family $\mathcal{F}$ of elliptic curves $E^{I,J}$ over $\mathbb{Q}$ where $I, J$ are integers satisfying the following three conditions: $3 \mid I$, $27 \mid J$, and for every prime $p$, we have that $3p^4 \nmid I$ if $27p^6 \mid J$. Given a form $f \in V_{3,1}(\mathbb{Z})$ with $x^2y$-coefficient equal to $a$, we define the *elliptic*

*curve associated to* $f$ by

$$E_f := \begin{cases} E^{I(f),J(f)}, & \text{if } a \equiv 0 \pmod 3, \\ E^{81I(f),729J(f)}, & \text{otherwise.} \end{cases}$$

Note that the curve $E_f$ is independent of the equivalence class of $f$ and that $E_f \in \mathcal{F}$ for each $f$. We use the height function $H$ on monic binary cubic forms so as to be compatible with the height on elliptic curves used in this chapter.

## 4.B.2 Main result

In [18], Bhargava, Hanke, and Shankar proved the following theorem, which determines the *average* size of the 2-class group of monogenic cubic fields:

**Theorem 160** ([18, Theorem 7])**.** *When forms* $f \in N(\mathbb{Z})\backslash V_{3,1}(\mathbb{Z})^{r_1,r_2}_{\max}$ *with Galois group* $S_3$ *are ordered by the height* $H$*:*

(a) *The average size of* $\mathrm{Cl}(R_f)[2]$ *is* $3/2$ *if* $(r_1, r_2) = (3, 0)$*;*

(b) *The average size of* $\mathrm{Cl}(R_f)[2] = \mathrm{Cl}^+(R_f)[2]$ *is* $2$ *if* $(r_1, r_2) = (1, 1)$*;*

(c) *The average size of* $\mathrm{Cl}^+(R_f)[2]$ *is* $5/2$ *if* $(r_1, r_2) = (3, 0)$*.*

In this appendix, we prove the following result, which is an analogue of Theorem 160 for the *second moment* of the size of the 2-class group of monogenic cubic fields:

**Theorem 161.** *When forms* $f \in N(\mathbb{Z})\backslash V_{3,1}(\mathbb{Z})^{r_1,r_2}_{\max}$ *with Galois group* $S_3$ *are ordered by the height* $H$*:*

(a) *The second moment of the size of* $\mathrm{Cl}(R_f)[2]$ *is at most* $3$ *if* $(r_1, r_2) = (3, 0)$*;*

(b) *The second moment of the size of* $\mathrm{Cl}(R_f)[2] = \mathrm{Cl}^+(R_f)[2]$ *is at most* $6$ *if* $(r_1, r_2) = (1, 1)$*;*

(c) *The second moment of the size of* $\mathrm{Cl}^+(R_f)[2]$ *is at most* $10$ *if* $(r_1, r_2) = (3, 0)$*.*

*Moreover, the upper bounds of* 3, 6, *and* 10 *are optimal, conditional on a uniformity estimate.*

In fact, we prove that Theorem 97 holds if we instead average over forms satisfying acceptable families of local specifications; a similar generalization of Theorem 160 is stated in [18, Theorem 7].

The rest of this appendix is organized as follows. In §4.B.3, we compare the values obtained in Theorems 160 and 161 with the values predicted the Cohen–Lenstra–Martinet–Malle heuristics. In §4.B.4, we explain how the dual of the 2-class group of a monogenic cubic field can be parametrized in terms of $\mathrm{PGL}_2(\mathbb{Q})$-orbits of certain binary quartic forms, and hence in terms of 2-Selmer groups of certain elliptic curves. Thus, up to some modifications, proving Theorem 161 amounts to bounding the second moment of the size of the 2-Selmer groups of elliptic curves, which we achieved in Theorem 97. In §4.B.5, we explain in detail how the proof of Theorem 97 can be modified to give a proof of Theorem 161.

### 4.B.3 Comparison with class group heuristics

Theorem 160 was the first result of its kind to demonstrate that imposing a global condition on a family of number fields can have an altering effect on the distribution of its class groups. In context of previous work, this came as quite a surprise: indeed, as explained in [18, §1] and §2.1.2, there is a considerable body of evidence, both computational and theoretical, to suggest that class group distributions remain robust under the imposition of all manner of local and global conditions. In the case of cubic number fields $K$, the class group heuristics developed by Cohen and Lenstra [46], as generalized by Cohen and Martinet [47] and adjusted by Malle [83], make the following definitive prediction for the distribution of the 2-torsion subgroups $\mathrm{Cl}(K)[2]$ (resp., $\mathrm{Cl}^+(K)[2]$) of the class group (resp., narrow class group) of $K$:

**Conjecture 162** (Cohen–Lenstra–Martinet–Malle)**.** *Consider the set of isomorphism classes of cubic number fields with real signature* $(r_1, r_2)$ *and Galois group* $S_3$*. When these fields are ordered by discriminant:*

(a) *The average size of* $\mathrm{Cl}(K)[2]$ *is* $5/4$ *and the second moment is* $15/8$ *if* $(r_1, r_2) = (3, 0)$*;*

(b) *The average size of* $\mathrm{Cl}(K)[2] = \mathrm{Cl}^+(K)[2]$ *is* $3/2$ *and the second moment is* $3$ *if* $(r_1, r_2) = (1, 1)$*; and*

(c) *The average size of* $\mathrm{Cl}^+(K)[2]$ *is* $2$ *and the second moment is* $6$ *if* $(r_1, r_2) = (3, 0)$.

The claims in Conjecture 162(a),(b) about the average size of $\mathrm{Cl}(K)[2]$ were proven by Bhargava in [8, Theorem 5], and the claim in Conjecture 162(c) about the average size of $\mathrm{Cl}^+(K)[2]$ was proven by Bhargava and Varma in [30, Theorem 1]. Theorem 160 shows that imposing the condition of monogenicity causes the nontrivial part of the 2-class group to double on average. Theorem 161 suggests that this increasing effect is not confined to the first moment of the 2-class group distribution.

## 4.B.4 Algebraic preliminaries

In this section, we start by recalling the notion of the monogenic cubic resolvent form of a binary quartic form (§4.B.4.1). We then explain how dual 2-torsion ideal classes of $R_f$, where $f \in V_{3,1}(\mathbb{Z})_{\max}$, may be parametrized in terms of integral binary quartic forms with resolvent $f$ (§§4.B.4.2). We finish by combining these results with those of §4.3.1 to relate the 2-class groups of monogenic cubic fields to certain modified 2-Selmer sets associated to elliptic curves (§4.B.4.3).

### 4.B.4.1 Cubic resolvents of binary quartic forms

Let $g(x, y) = ax^4+bx^3y+cx^2y^2+dxy^3+ey^4 \in V_4(\mathbb{Z})$ be a binary quartic form with $\Delta(g) \neq 0$. We define the *cubic resolvent* form of $g$ to be the monic binary cubic form

$$\mathrm{Res}(g)(x, y) := x^3 + cx^2y + (bd - 4ae)xy^2 + (ad^2 + b^2e - 4ace)y^3 \in V_{3,1}(\mathbb{Z}).$$

The $N(\mathbb{Z})$-equivalence class of $\mathrm{Res}(g)$ is an invariant of the $\mathrm{PGL}_2(\mathbb{Z})$-orbit of $g$—indeed, we have that $I(g) = I(\mathrm{Res}(g))$ and that $J(g) = J(\mathrm{Res}(g))$ for any $g \in V_4(\mathbb{Z})$ (cf. [125, Theorem 1.1]). In particular, we have that $\Delta(g) = \Delta(\mathrm{Res}(g))$.

As explained in [8, §3.1], the resolvent $\mathrm{Res}(g)$ is maximal if and only if $g$ is nowhere evenly ramified. The conditions of being maximal and nowhere evenly ramified are invariant under $\mathrm{PGL}_2(\mathbb{Q})$-equivalence.

#### 4.B.4.2 Parametrization of dual 2-torsion classes of monogenic cubic fields

We now recall the parametrization of the dual of the 2-class group of a monogenic cubic field in terms of $\mathrm{PGL}_2(\mathbb{Z})$-orbits on $V_4(\mathbb{Z})$:

**Theorem 163.** *Let $f \in V_{3,1}(\mathbb{Z})_{\max}$ be an irreducible form with Galois group $S_3$. Then:*

(a) *If $\Delta(f) > 0$, then there is a canonical bijection between the elements of the dual group $\mathrm{Cl}^+(R_f)[2]^*$ and $\mathrm{PGL}_2(\mathbb{Q})$-equivalence classes of binary quartic forms $g \in V_4(\mathbb{Z})$ with $\mathrm{Res}(g)$ being $N(\mathbb{Z})$-equivalent to $f$.*

*Under this bijection, the elements of the dual group $\mathrm{Cl}(R_f)[2]^* \subset \mathrm{Cl}^+(R_f)[2]^*$ correspond to binary quartic forms $g$ that have four distinct real roots.*

(b) *If $\Delta(f) < 0$, there is a canonical bijection between the elements of the dual group $\mathrm{Cl}^+(K_f)[2]^* = \mathrm{Cl}(K_f)[2]^*$ and $\mathrm{PGL}_2(\mathbb{Q})$-equivalence classes of binary quartic forms $g \in V_4(\mathbb{Z})$ with $\mathrm{Res}(g)$ being $N(\mathbb{Z})$-equivalent to $f$.*

*Proof.* In [18, Theorem 2.15], the theorem is proven with "$\mathrm{PGL}_2(\mathbb{Q})$" replaced by "$\mathrm{PGL}_2(\mathbb{Z})$." It therefore remains to show that if $g \in V_4(\mathbb{Z})$ has maximal resolvent $\mathrm{Res}(g)$, then the $\mathrm{PGL}_2(\mathbb{Q})$-orbit of $g$ contains exactly one $\mathrm{PGL}_2(\mathbb{Z})$-orbit, but this was shown in [26, proof of Proposition 3.18]. □

### 4.B.4.3 Relating 2-class groups to modified 2-Selmer sets

Let $f \in V_{3,1}(\mathbb{Z})_{\max}$ be an irreducible form with Galois group $S_3$. Letting $a$ denote the $x^2y$-coefficient of $f$, define the constant $\kappa_a$ by

$$\kappa_a := \begin{cases} 4, & \text{if } a \equiv 0 \pmod 3, \\ 36, & \text{otherwise.} \end{cases}$$

Let $f^* \in V_{3,1}(\mathbb{Z})_{\max}$ be the form defined by $f^*(x,y) = f(x,-y)$. We then define the following sets, which we call the *modified 2-Selmer sets* associated to $f$:

$$\mathrm{Sel}_2^{(\mathrm{a})}(E_f) := \mathrm{Sel}_2(E_f) \cap \frac{V_4(\mathbb{R})^{(0)} \cap \kappa_a V_4(\mathbb{Z})}{\mathrm{PGL}_2(\mathbb{Q})},$$
$$\mathrm{Sel}_2^{(\mathrm{b})}(E_f) := \mathrm{Sel}_2(E_f) \cap \frac{V_4(\mathbb{R})^{(1)} \cap \kappa_a V_4(\mathbb{Z})}{\mathrm{PGL}_2(\mathbb{Q})}, \quad \text{and}$$
$$\mathrm{Sel}_2^{(\mathrm{c})}(E_f) := \left(\mathrm{Sel}_2(E_f) \cap \frac{\left(V_4(\mathbb{R})^{(0)} \sqcup V_4^{(2+)}(\mathbb{R})\right) \cap \kappa_a V_4(\mathbb{Z})}{\mathrm{PGL}_2(\mathbb{Q})}\right) \sqcup \left(\mathrm{Sel}_2(E_{f^*}) \cap \frac{V_4(\mathbb{R})^{(2+)} \cap \kappa_a V_4(\mathbb{Z})}{\mathrm{PGL}_2(\mathbb{Q})}\right)$$

Then we have the following result relating the size of $\mathrm{Cl}(R_f)[2]$ to the sizes of the modified 2-Selmer sets $\mathrm{Sel}_2^{\bullet}(E_f)$ defined above, where $\bullet \in \{(\mathrm{a}), (\mathrm{b}), (\mathrm{c})\}$:

**Theorem 164.** *Let $f$ be as above. Then:*

(a) *If $\Delta(f) > 0$, then $\#\,\mathrm{Cl}(R_f)[2] = \#\,\mathrm{Sel}_2^{(\mathrm{a})}(E_f)$;*

(b) *If $\Delta(f) < 0$, then $\#\,\mathrm{Cl}(R_f)[2] = \#\,\mathrm{Cl}^+(R_f)[2] = \#\,\mathrm{Sel}_2^{(\mathrm{b})}(E_f)$; and*

(c) *If $\Delta(f) > 0$, then $\#\,\mathrm{Cl}^+(R_f)[2] = \#\,\mathrm{Sel}_2^{(\mathrm{c})}(E_f)$.*

*Proof.* Take $\alpha^* \in \mathrm{Cl}(R_f)[2]^*$, let $g' \in V_4(\mathbb{Z})$ be the binary quartic form corresponding to $\alpha^*$ via Theorem 163. Since $\mathrm{Res}(g')$ is $N(\mathbb{Z})$-equivalent to $f$, which is maximal, we have that $g'$ is nowhere evenly ramified. An application of the Hasse–Weil bound then shows that $g'$ is everywhere locally soluble (see [13, Propositions 10-11]). Let $g \in V_4(\mathbb{Z})$ be the binary quartic form defined by $g = \kappa_a g'$. Note that $g$ is also locally soluble; thus, via Theorem 110,

we may view $g$ as an element of $\mathrm{Sel}_2(E_f)$. The map sending $\alpha^* \mapsto g$ realizes $\mathrm{Cl}(R_f)[2]^*$ as a subset of $\mathrm{Sel}_2(E_f) \cap V_4(\mathbb{R})^{(0)}$ or $\mathrm{Sel}_2(E_f) \cap V_4(\mathbb{R})^{(1)}$, according as $\Delta(f) > 0$ or $\Delta(f) < 0$. The image consists precisely of those classes of binary quartic forms divisible by $\kappa_a$.

Now suppose $\Delta(f) > 0$, and take $\alpha^* \in \mathrm{Cl}^+(R_f)[2]^*$. Then we proceed just as before, unless $g' \in V_4(\mathbb{R})^{(2-)}$, in which case we replace $g'$ with $-g'$ and repeat the above argument to get an element $g \in \mathrm{Sel}_2(E_{f^*})$. The map sending $\alpha^* \mapsto g$ realizes $\mathrm{Cl}^+(R_f)[2]^*$ as a subset of

$$\big(\mathrm{Sel}_2(E_f) \cap (V_4(\mathbb{R})^{(0)} \sqcup V_4(\mathbb{R})^{(2+)})\big) \sqcup \big(\mathrm{Sel}_2(E_{f^*}) \cap V_4(\mathbb{R})^{(2+)}\big),$$

and the image consists precisely of those classes of binary quartic forms divisible by $\kappa_a$. $\square$

## 4.B.5 Proof of Theorem 97

In this section, we start by sketching the idea of the proof (§4.B.5.1). As we shall see, to obtain a proof of Theorem 97, one simply needs to take the proof of Theorem 97 and make adjustments to certain local mass formulas that arise. After adjusting these masses (§§4.B.5.2–4.B.5.3), we finish by showing how the masses combine to yield Theorem 97 (§4.B.5.4).

### 4.B.5.1 The idea of the proof

In this subsection, we explain the ideal underlying the proofs of Theorem 97(a),(b); the remaining part is proven analogously.

Computing the second moment of $\#\,\mathrm{Cl}(R_f)[2]$ amounts to determining the average size of the set $\mathrm{Cl}(R_f)[2]^2$ of pairs $(\alpha_1, \alpha_2)$ of 2-torsion ideal classes of $R_f$, where $f$ ranges over $N(\mathbb{Z})\backslash V_{3,1}(\mathbb{Z})^{r_1,r_2}_{\mathrm{max}}$. To see why the second moment of $\#\,\mathrm{Cl}(R_f)[2]$ should be 3 if $(r_1, r_2) = (3, 0)$ and 6 if $(r_1, r_2) = (1, 1)$, fix a 2-torsion class $\alpha_1$ of such a ring $R_f$, and consider the following heuristic argument:

*Case 1*: Suppose $\alpha_1$ corresponds to the trivial element of $\mathrm{Cl}(R_f)[2]$. Then $f$ can be arbitrary, and [18, part (a) of Theorem 4] implies that the average number of choices for $\alpha_2$ on average

is $\frac{3}{2}$ if $(r_1, r_2) = (3, 0)$ and 2 if $(r_1, r_2) = (1, 1)$.

*Case 2*: Suppose $\alpha_1$ corresponds to a non-trivial element of $\mathrm{Cl}(R_f)[2]$. Then [18, part (b) of Theorem 4] implies that the average number of choices for $\alpha_1$ is $\frac{1}{2}$ if $(r_1, r_2) = (3, 0)$ and 1 if $(r_1, r_2) = (1, 1)$. Moreover, $f$ cannot be arbitrary — indeed, $\mathrm{Cl}(R_f)$ has a marked non-trivial 2-torsion element, namely the one corresponding to $\alpha_1$. We expect that this marked element gives an extra generator for $\mathrm{Cl}(R_f)[2]$ 100% of the time, and so, the average number of choices for $\alpha_2$ should be $2 \times \frac{3}{2} = 3$ if $(r_1, r_2) = (3, 0)$ and $2 \times 2 = 4$ if $(r_1, r_2) = (1, 1)$, twice as many choices as in case 1.

Combining the results of cases 1 and 2, we conclude that the average number of choices for the pair $(\alpha_1, \alpha_2)$ should be $1 \times \frac{3}{2} + \frac{1}{2} \times 3 = 3$ if $(r_1, r_2) = (3, 0)$ and $1 \times 2 + 1 \times 4 = 6$ if $(r_1, r_2) = (1, 1)$, as desired.

In this chapter, we proved that the second moment of the size of the 2-Selmer group of elliptic curves is at most 15 by making rigorous a heuristic similar to the one detailed above (cf. §4.1.3). The bound of 15 arises from evaluating a certain formula involving a product of local masses over all places $v$ of $\mathbb{Q}$; the local mass at $p$ is equal to 1 for every prime $p \geq 5$. Theorem 164 tells us that the masses at primes $p \geq 5$ stay the same when one replaces the symbol "Sel" with "$\mathrm{Sel}^\bullet$" for each $\bullet \in \{(a), (b), (c)\}$, and as we explain in the next two subsections, it also tells us how the masses at $\infty$, 2, and 3 change under this replacement.

### 4.B.5.2 The archimedean mass

Fix $a \in \{0, 1, 2\}$, and let $I' := \kappa_a^2 I$ and $J' := \kappa_a^3 J$. Let $f \in V_{3,1}(\mathbb{R})$ be a separable form with $x^2y$-coefficient $a$.

For each $i \in \{0, 2+, 2-\}$ if $\Delta(f) > 0$ and for $i = 1$ if $\Delta(f) < 0$, the action of $\mathrm{PGL}_2(\mathbb{R})$ on the set $\mathrm{Inv}^{-1}(I'(f), J'(f)) \cap V_4(\mathbb{R})^{(i)}$ consists of a single orbit; let $g_i(f)$ be a representative of this orbit. Letting $\bullet \in \{\mathrm{sol}, (a), (c)\}$ if $\Delta(f) > 0$ and $\bullet \in \{\mathrm{sol}, (b)\}$ if $\Delta(f) < 0$, define

the quantity $\alpha_\infty^\bullet(f)$ by

$$\alpha_\infty^\bullet(f) := \tag{4.58}$$
$$\begin{cases} \big(\#\operatorname{Stab}_{\mathrm{PGL}_2(\mathbb{R})}(g_0(f))\big)^{-1} + \big(\#\operatorname{Stab}_{\mathrm{PGL}_2(\mathbb{R})}(g_{2+}(f))\big)^{-1}, & \text{if } \bullet = \text{sol and } \Delta(f) > 0, \\ \big(\#\operatorname{Stab}_{\mathrm{PGL}_2(\mathbb{R})}(g_1(f))\big)^{-1}, & \text{if } \bullet = \text{sol and } \Delta(f) < 0, \\ \big(\#\operatorname{Stab}_{\mathrm{PGL}_2(\mathbb{R})}(g_0(f))\big)^{-1}, & \text{if } \bullet = \text{(a)}, \\ \big(\#\operatorname{Stab}_{\mathrm{PGL}_2(\mathbb{R})}(g_1(f))\big)^{-1}, & \text{if } \bullet = \text{(b)}, \\ \big(\#\operatorname{Stab}_{\mathrm{PGL}_2(\mathbb{R})}(g_0(f))\big)^{-1} + 2\big(\#\operatorname{Stab}_{\mathrm{PGL}_2(\mathbb{R})}(g_{2+}(f))\big)^{-1}, & \text{if } \bullet = \text{(c)}. \end{cases}$$

The following proposition determines the value of the quantity $\alpha_\infty^\bullet(f)$:

**Proposition 165.** *Let $f$ and $\bullet$ be as above. Then $\alpha_\infty^\bullet(f) = \alpha_\infty^\bullet$ is a constant with value $\frac{1}{2}$ when $\bullet = \mathrm{sol}$, $\frac{1}{4}$ when $\bullet = \text{(a)}$, $\frac{1}{2}$ when $\bullet = \text{(b)}$, and $\frac{3}{4}$ when $\bullet = \text{(c)}$.*

*Proof.* This follows immediately from [26, Lemma 2.2], where the values of the stabilizers occurring on the right-hand side of (4.58) are determined. □

### 4.B.5.3 The 2-adic and 3-adic local masses

Let $p \in \{2, 3\}$, and let $f \in V_{3,1}(\mathbb{Z}_p)_{\max}$ be a form with $x^2y$-coefficient $a$.

Let $V_4(\mathbb{Z}_p)^{\mathrm{sol}} \subset V_4(\mathbb{Z}_p)$ denote the subset of soluble binary quartic forms, and let $V_4(\mathbb{Z}_p)^+ \subset V_4(\mathbb{Z}_p)^{\mathrm{sol}}$ denote the subset of binary quartic forms divisible by $\kappa_a$. Letting $\bullet \in \{\mathrm{sol}, +\}$, define the quantity $\alpha_p^\bullet(f)$ by

$$\alpha_p^\bullet(f) := \sum_{g \in \frac{\mathrm{Inv}^{-1}(I'(f), J'(f)) \cap V_4(\mathbb{Z}_p)^\bullet}{\mathrm{PGL}_2(\mathbb{Q}_p)}} \big(\#\operatorname{Stab}_{\mathrm{PGL}_2(\mathbb{Q}_p)}(g)\big)^{-1}.$$

In [26, proof of Theorem 3.19], it is shown that $\alpha_p^{\mathrm{sol}}(f) = \alpha_p^{\mathrm{sol}}$ is a constant with value 2 when $p = 2$ and 1 when $p = 3$. The following proposition proves a similar result for $\alpha_p^+(f)$:

**Proposition 166.** *Let $p$ and $f$ be as above. Then $\alpha_p^+(f) = \alpha_p^+$ is a constant with value 1.*

*Proof.* By simply undoing the scaling by $\kappa_a$, we see that

$$\alpha_p^+ = \sum_{g \in \frac{\mathrm{Inv}^{-1}(I(f),J(f)) \cap V_4(\mathbb{Z}_p)}{\mathrm{PGL}_2(\mathbb{Q}_p)}} \big(\#\,\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{Q}_p)}(g)\big)^{-1}. \tag{4.59}$$

The mass on the right-hand side of (4.59) was determined in [18, Corollary 3.40] to be 1. □

#### 4.B.5.4 The final step

By making minor modifications to the proof of Theorem 97, we obtain the following result for the second moment of the size of $\mathrm{Sel}_2(E_f)$, where $f$ ranges over an acceptable family of monic maximal binary cubic forms:

**Theorem 167.** *Let $\Sigma$ be an acceptable family of local specifications defining an "acceptable" subfamily $V_{3,1}(\Sigma) \subset V_{3,1}(\mathbb{Z})_{\max}$. When forms $f \in N(\mathbb{Z}) \backslash V_{3,1}(\Sigma)$ with Galois group $S_3$ are ordered by height, the second moment of the size of $\mathrm{Sel}_2(E_f)$ is at most*

$$1 + 2\alpha_\infty^{\mathrm{sol}}\alpha_2^{\mathrm{sol}}\alpha_3^{\mathrm{sol}}\big(3 + 4\alpha_\infty^{\mathrm{sol}}\alpha_2^{\mathrm{sol}}\alpha_3^{\mathrm{sol}}\big) = 15,$$

*with equality conditional on a uniformity estimate.*

One verifies that the proof of Theorem 167 goes through with $\alpha_\infty^{\mathrm{sol}}$ replaced by $\alpha_\infty^{\bullet}$ for any $\bullet \in \{\text{(a), (b), (c)}\}$ and $\alpha_p^{\mathrm{sol}}$ replaced by $\alpha_p^+$ for each $p \in \{2, 3\}$. Thus, by analogy with Theorem 167, we obtain the following result, which by Theorem 164 is equivalent to Theorem 161:

**Theorem 168.** *Fix $\bullet \in \{\text{(a), (b), (c)}\}$. Let $\Sigma$ be an acceptable family of local specifications defining an "acceptable" subfamily $V_{3,1}(\Sigma) \subset V_{3,1}(\mathbb{Z})_{\max}$, where $V_{3,1}(\Sigma_\infty) = V_{3,1}(\mathbb{R})^{3,0}$ if $\bullet \in \{\text{(a), (c)}\}$ and $V_{3,1}(\Sigma_\infty) = V_{3,1}(\mathbb{R})^{1,1}$ if $\bullet = \text{(b)}$. When forms $f \in N(\mathbb{Z}) \backslash V_{3,1}(\Sigma)$ with*

*Galois group $S_3$ are ordered by height, the second moment of the size of* $\mathrm{Sel}_2^\bullet(E_f)$ *is at most*

$$1 + 2\alpha_\infty^\bullet \alpha_2^+ \alpha_3^+ \left(3 + 4\alpha_\infty^\bullet \alpha_2^+ \alpha_3^+\right) = \begin{cases} 3, & \text{if } \bullet = (\mathrm{a}), \\ 6, & \text{if } \bullet = (\mathrm{b}), \\ 10, & \text{if } \bullet = (\mathrm{c}), \end{cases}$$

*with equality conditional on a uniformity estimate.*

# Chapter 5

# Geometry-of-numbers methods in the cusp, and applications

This chapter is based on my joint work [103] with Arul Shankar, Artane Siad, and Ila Varma.

## 5.1 Introduction

Over the past two decades, many breakthroughs have been achieved in the field of arithmetic statistics by means of a general approach that involves invariant theory, geometry-of-numbers techniques, averaging methods, and sieve theory. Most notably, this approach has been applied to determine asymptotics for number fields of small fixed degree (see [8, 10, 58, 68]), compute average sizes of $p$-class groups in certain families of number fields for small primes $p$ (see [8, 18, 58, 71, 108, 109]), calculate average $n$-Selmer ranks of elliptic curves and hyperelliptic Jacobians for small $n$ (see [15, 23, 25, 26, 27, 105]), and more. The statements that have been tractable through this approach typically concern distributions of arithmetic objects that can be parametrized by *irreducible integral orbits of coregular representations*.

In special cases (see [2, 31]), this approach has been generalized using situation-specific techniques to study objects parametrized by *reducible* orbits. The purpose of this chapter is to develop a systematic method for counting *reducible integral orbits of coregular represen-*

*tations*. As an application of this method, we obtain formulas for the average 2-torsion in the class groups and ideal groups of monogenic orders of any fixed odd degree $n \geq 3$.

### 5.1.1 Background on geometry-of-numbers methods

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

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

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

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

arithmetic objects of bounded height in the family.

The development and use of this strategy goes back centuries. Mertens [84] and Siegel [110] developed geometry-of-numbers methods to count the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits on integral binary quadratic forms with bounded discriminant, resolving conjectures of Gauss on the average sizes of class numbers of quadratic orders. In the series of papers [55, 56, 57], Davenport obtained asymptotics for the number of irreducible $\mathrm{GL}_2(\mathbb{Z})$-orbits on integral binary cubic forms having bounded discriminant. Combining these asymptotics with results from class field theory and sieve methods, Davenport and Heilbronn determined the density of discriminants of cubic fields [58].

The main obstruction to generalizing the work of Mertens, Siegel, and Davenport–Heilbronn to other representations is proving that the number of irreducible points in the cusps is negligible. In the aforementioned works, *ad hoc* geometry-of-numbers techniques were used to *bound* the number of irreducible $\mathrm{GL}_2(\mathbb{Z})$-orbits that lie in cusps of the fundamental domains of binary quadratic and cubic forms. A pioneering advance was made by Bhargava (see [10]), who introduced an averaging technique that has the effect of "thickening" the cusps and that applies to general coregular representations. Bhargava's averaging technique gives a systematic way to bound the number of points in cuspidal regions and thus opened the door to study the distributions of a wide variety of arithmetic objects. However, these techniques only yield upper bounds and do not suffice to obtain precise asymptotics.

In this chapter, we develop a general method for determining asymptotics for the number of lattice points in the cuspidal regions of $\mathcal{D}_X$. These regions overwhelmingly contain *reducible* integral orbits of $\mathcal{G}$ on $W$. We illustrate this method for a representation of particular interest in number theory, namely the action of $\mathcal{G}_{\mathscr{A}_n}$ on $W_{\mathscr{A}_n}$. The irreducible orbits of this representation have been studied extensively in the literature. For example, see [15, Theorem 10.1] (resp., [105, Theorem 20]), where Bhargava and Gross (resp., Shankar and Wang) obtained asymptotics for the number of *irreducible* orbits of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $W_{\mathscr{A}_n}(\mathbb{Z})$ having bounded height when $n$ is odd (resp., when $n$ is even) and applied these asymptotics

to determine the average sizes of the 2-Selmer groups of monic hyperelliptic Jacobians of any given dimension. The asymptotics for the number of irreducible integral orbits of this representation also played a key role in the applications treated in §3–4.

Prior to the work presented in this chapter, asymptotics for reducible orbits have been determined in only a few special cases. Firstly, Shintani handled the case of $\mathrm{SL}_2(\mathbb{Z})$ acting on integer-matrix binary cubic forms using $\zeta$-function techniques (see [107, Chapter 2, §7, Remark 2]). This result was later recovered using a geometry-of-numbers argument by Bhargava and Varma (see [31, §4.1.2]), who applied it to determine the average size of the 3-torsion in class groups of quadratic orders. Secondly, in [2], Altug, Shankar, Varma, and Wilson used both $L$-function techniques and geometry-of-numbers methods to prove an asymptotic for certain reducible orbits of $\mathrm{GL}_2 \times \mathrm{SL}_3$ acting on pairs of ternary quadratic forms. However, all of these works rely crucially on situation-specific techniques and on the fact that the representations under consideration are of small dimension.

In general, since reducible orbits often contain rich arithmetic information (in addition to the works referenced above, see [29, 99]), we expect that our methods will have applications far beyond the results of this paper. For instance, we note that $D_5$-quintic rings correspond to reducible orbits via the relevant parametrizations (see [9, 123]).

### 5.1.2 Main results on counting in cusps

In this section, after setting the necessary notation, we describe our method for counting points in cusps of fundamental domains, and we explain how this method can be used to count reducible orbits of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $W_{\mathscr{A}_n}(\mathbb{Z})$.

#### 5.1.2.1 Notation and setup

Let $R$ be a $\mathbb{Z}$-algebra. For any subset $S \subset W_{\mathscr{A}_n}(R)$, let $S_0 \subset S$ be the subset consisting of elements $B = [b_{ij}]$ such that $b_{ij} = 0$ for all pairs $(i, j)$ such that $i + j \leq n - 1$. Letting $\mathcal{P}_n \subset \mathcal{G}_{\mathscr{A}_n}$ denote the lower-triangular subgroup, notice that the action of $\mathcal{G}_{\mathscr{A}_n}(R)$ on $W_{\mathscr{A}_n}(R)$

restricts to a well-defined action of $\mathcal{P}_n(R)$ on $W_{\mathscr{A}_n}(R)_0$. When $R$ is a PID, let $S_{\mathrm{red}} \subset S$ be the subset of reducible elements of $S$; in this case, we have $S_0 \subset S_{\mathrm{red}}$ by Proposition 20.

Next, retain the setting of §5.1.3 (i.e., let $n$ and $(r_1, r_2)$ be as in §5.1.3), and let $R = \mathbb{Z}$ or $\mathbb{R}$. We define the set

$$W_{\mathscr{A}_n}(R)^{r_1,r_2} := \{B \in W_{\mathscr{A}_n}(R) : \iota(\mathscr{A}_n, B) \in V_{n,1}(R)^{r_1,r_2}\}.$$

For any $X > 0$, let $N_n^{r_1,r_2}(X) := \#\{f \in N(\mathbb{Z})\backslash V_{n,1}(\mathbb{Z})^{r_1,r_2} : \mathrm{H}(f) < X\}$, and for any $S \subset W_{\mathscr{A}_n}(R)^{r_1,r_2}$, let $S_X := \{B \in S : \mathrm{H}(B) < X\}$.

#### 5.1.2.2 Statements of results

We prove the following asymptotic formula for the count of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$-orbits on $W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2}$:

**Theorem 169.** *If $n$ is odd, we have*

$$\#\left(\frac{(W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2}_{\mathrm{red}})_X}{(N \times \mathcal{G}_{\mathscr{A}_n})(\mathbb{Z})}\right) = \left(\prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \zeta(2i)\right) \cdot N_n^{r_1,r_2}(X) + o\big(X^{\frac{n^2+n-2}{2}}\big),$$

*and if $n$ is even, we have*

$$\#\left(\frac{(W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2}_{\mathrm{red}})_X}{(N \times \mathcal{G}_{\mathscr{A}_n})(\mathbb{Z})}\right) = \left(\zeta(\tfrac{n}{2}) \prod_{i=1}^{\frac{n-2}{2}} \zeta(2i)\right) \cdot \frac{N_n^{r_1,r_2}(X)}{2^{\frac{n}{2}}} + o\big(X^{\frac{n^2+n-2}{2}}\big).$$

*Remark* 170. We make two observations regarding the asymptotics obtained in Theorem 169. Firstly, the product of $\zeta$-values is the fundamental volume of $\mathcal{G}_{\mathscr{A}_n}$. Secondly, the factor of $2^{-\frac{n}{2}}$ that occurs in the asymptotic for even $n$ in Theorem 169 accounts for the fact that for any $B \in W_{\mathscr{A}_n}(\mathbb{Z})$, the $x^{n-i}y^i$-coefficient of $\iota(\mathscr{A}_n, B)$ is divisible by 2 for every odd number $i \in \{1, 3, \ldots, n-1\}$ (see [109, Theorem 80]).

We now outline the proof of Theorem 169, which occupies §5.2–§5.4, and also part of §5.5. We begin in §5.2 by constructing fundamental sets for the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $W_{\mathscr{A}_n}(\mathbb{R})$.

As we show in §5.2.3, this amounts to constructing a fundamental domain $\mathcal{F}$ for the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$. For the purpose of proving Theorem 169, it is *not* enough to simply invoke the work of Borel and Harish-Chandra (see [34, 35]), who constructed fundamental domains for general semisimple groups. Indeed, our argument in §5.3.2 relies on $\mathcal{F}$ being *box-shaped at infinity*, meaning that $\mathcal{F}$ looks like a Siegel domain in a neighborhood of the cusp. In §5.2.1–5.2.2, we define what it means for a fundamental domain to be box-shaped at infinity and prove that such fundamental domains exist for the group $\mathcal{G}_{\mathscr{A}_n}$ (see Theorem 176).

In §5.3, we prove an intermediate result (see Theorem 185) expressing the count of reducible orbits of height up to $X$ in terms of an integral $C_X$, which gives the volume of a certain subset of $W_{\mathscr{A}_n}(\mathbb{R})_0$ with respect to a certain measure $\lambda$. To prove this, we start in §5.3.1 by applying Bhargava's technique of averaging over translates of the domain $\mathcal{F}$ constructed in §5.2 to thicken the region in which we are counting lattice points. In this thickened region, all but a negligible number of reducible integral elements lie on the hyperplane $W_{\mathscr{A}_n}(\mathbb{R})_0 \subset W_{\mathscr{A}_n}(\mathbb{R})$. This reduces the problem of counting reducible $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$-orbits on $W_{\mathscr{A}_n}(\mathbb{Z})$ to that of counting lattice points lying in the cusp of our fundamental domain for $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $W_{\mathscr{A}_n}(\mathbb{R})$. Indeed, the cusp consists of elements $B = [b_{ij}]$ for which $b_{ij}$ is tiny for all $(i, j)$ such that $i+j \leq n-1$, so lattice points in the cusp necessarily lie in $W_{\mathscr{A}_n}(\mathbb{R})_0$.

As it happens, the thickened cusp is still too narrow for us to be able to use standard geometry-of-numbers methods to count lattice points in it. In §5.3.2, we overcome this difficulty by slicing the thickened cusp into ball-like regions, within each of which it is easier to count lattice points. Summing the count of lattice points over all slices yields Theorem 185. Then, up to a technicality concerning orbits with big integral stabilizer that we resolve in §5.5.1 (see Proposition 199), all that remains to deduce Theorem 169 from Theorem 185 is to compute the integral $C_X$. We achieve this in §5.4 by proving a Jacobian change-of-variables formula that transforms the measure $\lambda$ on $W_{\mathscr{A}_n}(\mathbb{R})_0$ into the product of the Euclidean measure on $V_{n,1}(\mathbb{R})$ with the Haar measure on the lower-triangular subgroup $\mathcal{P}_n \subset \mathcal{G}_{\mathscr{A}_n}$ (see Proposition 191). Such change-of-variable results have previously been proven

when the group under consideration is unimodular (see, e.g., [26, §3.4]), but the fact that the group $\mathcal{P}_n$ *fails* to be unimodular presents significant new challenges.

In §5.5.1, we show how the proof of Theorem 169 in §5.3–5.4 can be retrofitted to count reducible orbits in subsets $S \subset W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2}$ defined by congruence conditions (see Theorem 197). For those subsets $S$ that consist of elements $B \in W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2}$ such that the coefficients of $\iota(\mathscr{A}_n, B)$ satisfy finite sets of congruence conditions, Theorem 197 specializes to the following result:

**Theorem 171.** *Let $\Sigma = V_{n,1}(\mathbb{Z})^{r_1,r_2} \cap \bigcap_p \Sigma_p$ be a family of monic binary forms defined by finitely many congruence conditions. Then we have*

$$\#\left(\frac{(\iota^{-1}(\Sigma)_{\mathrm{red}})_X}{(N \times \mathcal{G}_{\mathscr{A}_n})(\mathbb{Z})}\right) = N_n^{r_1,r_2}(X) \cdot \prod_p \int_{f \in \Sigma_p} \epsilon_n \cdot \#\left(\frac{\iota^{-1}(f)_0}{\mathcal{P}_n(\mathbb{Z}_p)}\right) df + o\big(X^{\frac{n^2+n-2}{2}}\big), \qquad (5.1)$$

*where $df$ denotes the Euclidean measure on $V_{n,1}(\mathbb{Z}_p)$, normalized so that $V_{n,1}(\mathbb{Z}_p)$ has volume 1, and where $\epsilon_n = 1$ if $n$ is odd and $\epsilon_n = \frac{1}{2}$ if $n$ is even.*

*Remark* 172. The occurrence of the lower-triangular subgroup $\mathcal{P}_n$ in the proof of Theorem 169 and in the statement of Theorem 171 is no accident: indeed, Theorems 169 and 171 may be reinterpreted as providing asymptotics for the number of orbits of $(N \times \mathcal{P}_n)(\mathbb{Z})$ on $W_{\mathscr{A}_n}(\mathbb{Z})_0^{r_1,r_2}$ having bounded height. This is significant because there are obstacles to using the methods outlined in §5.1.1 to count orbits for representations of groups, like $\mathcal{P}_n$, that are not unimodular.

### 5.1.3 Main results on class group distributions

Retain the setting of §2.1.1.1 (i.e., let $n$, $f_0$, and $(r_1, r_2)$ be as in §2.1.1.1) with $f_0 = 1$.

As it happens, our results on counting in cusps can be applied to determine formulas for the average 2-torsion in the class groups and ideal groups of rings defined by monic binary forms (i.e., monogenic rings). For instance, in §5.6.1, we prove the following theorem, which

gives the average 2-torsion in the class groups of the (monogenic cubic) orders cut out by binary forms in $V_{3,1}(\mathbb{Z})^{r_1,r_2}$:

**Theorem 173.** *We have*

$$\operatorname*{Avg}_{f\in V_{3,1}(\mathbb{Z})^{r_1,r_2}} \#\operatorname{Cl}(R_f)[2] = 1 + 2^{1-r_1-r_2}\left(1+\frac{\zeta(2)}{\zeta(3)}\right)$$

In previous work of Bhargava, Hanke, and Shankar (see [18, Theorem 4]), the analogue of Theorem 173 was proven for the subfamily of monogenic *maximal* cubic orders (i.e., monogenic orders that are rings of integers of cubic fields). The key obstacle to generalizing [18, Theorem 4] to the full family of monogenic cubic orders is that a non-maximal order $\mathcal{O}$ can have nontrivial torsion in its ideal group $\mathcal{I}(\mathcal{O})$, and 2-torsion ideals can contribute to the 2-torsion subgroup of its class group $\operatorname{Cl}(\mathcal{O})$. The dichotomy between 2-torsion ideal classes that come from 2-torsion ideals of cubic orders and those that do not is beautifully captured in an orbit parametrization discovered by Bhargava (see [6]). Indeed, as shown by Bhargava and Varma in [30], if $\mathcal{O}$ is a cubic order and $I \in \mathcal{I}(\mathcal{O})[2]$ (resp., $I \notin \mathcal{I}(\mathcal{O})[2]$) is an ideal of $\mathcal{O}$ whose class in $\operatorname{Cl}(\mathcal{O})$ is 2-torsion, then $I$ corresponds via Bhargava's parametrization to a *reducible* (resp., *irreducible*) integral orbit of $G_3$ on $W_3$.[1]

In [108, Theorem 9], Siad applied Wood's generalization of Bhargava's parametrization[2] in conjunction with the aforementioned general approach for counting *irreducible* integral orbits to prove that

$$\operatorname*{Avg}_{f\in V_{n,1}(\mathbb{Z})^{r_1,r_2}} \#\operatorname{Cl}(R_f)[2] - 2^{1-r_1-r_2}\cdot \#\mathcal{I}(R_f)[2] = 1 + 2^{1-r_1-r_2}, \tag{5.2}$$

Determining the average 2-torsion in the class groups of monogenic degree-$n$ orders thus amounts to determining the average 2-torsion in their ideal groups; via the parametrization, this is equivalent to counting *reducible* pre-projective integral orbits of the relevant coregular

[1] See also the work [31], where Bhargava and Varma prove that an analogous dichotomy holds for 3-torsion classes of quadratic orders.

[2] Note that, for monic binary forms $f$, Wood's parametrization is equivalent to the parametrization given in §1. Indeed, when $f_0 = 1$, we have $I_f^{n-3} = R_f = I_f^{n-2}$.

representation, namely that of $\mathcal{G}_{\mathscr{A}_n}$ on $W_{\mathscr{A}_n}$. In §5.6.2, we apply a variant of Theorem 171 (namely, Theorem 200) to count these orbits, thus obtaining the following result:

**Theorem 174.** *For a finite abelian group $\Gamma$, write $\mathrm{rk}_2\,\Gamma := \dim_{\mathbb{F}_2}(\mathbb{F}_2 \otimes_{\mathbb{Z}} \Gamma)$, and for an order $\mathcal{O}$ in an étale algebra $K$, write $\overline{\mathcal{O}}$ for the integral closure of $\mathcal{O}$ in $K$. Then we have*

$$\operatorname*{Avg}_{f \in V_{n,1}(\mathbb{Z})^{r_1,r_2}} \#\mathcal{I}(R_f)[2] = \prod_p \operatorname*{Avg}_{[\mathcal{O}:\mathbb{Z}_p]=n} 2^{\mathrm{rk}_2(\overline{\mathcal{O}}^\times/\mathcal{O}^\times)} \le \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \zeta(2i) \le 1.82102, \quad \textit{and}$$

$$\operatorname*{Avg}_{f \in V_{n,1}(\mathbb{Z})^{r_1,r_2}} \#\operatorname{Cl}(R_f)[2] = 1 + 2^{1-r_1-r_2}\left(1 + \prod_p \operatorname*{Avg}_{[\mathcal{O}:\mathbb{Z}_p]=n} 2^{\mathrm{rk}_2(\overline{\mathcal{O}}^\times/\mathcal{O}^\times)}\right)$$

*where "$\mathrm{Avg}_{[\mathcal{O}:\mathbb{Z}_p]=n}$" denotes the average over monogenic degree-$n$ extensions of $\mathbb{Z}_p$.*

For elements of $W_{\mathscr{A}_3}(\mathbb{Z})$, the notion of pre-projectivity is sufficiently concrete that we can compute the local factors in Theorem 174 explicitly. We thus obtain the following result:

**Theorem 175.** *We have*

$$\operatorname*{Avg}_{f \in V_{3,1}(\mathbb{Z})^{r_1,r_2}} \#\mathcal{I}(R_f)[2] = \frac{\zeta(2)}{\zeta(3)}.$$

Strikingly, the average size in Theorem 175 is the same as the value determined in [31, Theorem 6] for the average 3-torsion in the ideal groups of (monogenic) quadratic orders!

## 5.2 Reduction theory

As in §2, we work with monic integral binary forms up to the action of $N(\mathbb{Z})$. We are thus interested in counting $(N \times \mathcal{G}_{\mathscr{A}_n})(\mathbb{Z})$-orbits on $W_{\mathscr{A}_n}(\mathbb{Z})_{\mathrm{red}}$. The first step toward counting these orbits is to realize them as lattice points in fundamental sets for the action of $(N \times \mathcal{G}_{\mathscr{A}_n})(\mathbb{Z})$ on $W_{\mathscr{A}_n}(\mathbb{R})$. In this section, we construct these fundamental sets.

Let $f_1 \in \{0, 1, \ldots, n-1\}$ when $n$ is odd and $f_1 \in \{0, 2, \ldots, n-2\}$ when $n$ is even, and

consider the subschemes $W_{\mathscr{A}_n,f_1} \subset W_{\mathscr{A}_n}$, $V_{n,1,f_1} \subset V_{n,1}$ defined by

$$W_{\mathscr{A}_n,f_1}(R) := \left\{ B \in W_{\mathscr{A}_n}(R) : \lim_{y\to 0}(y^{-1}(\iota(\mathscr{A}_n, B)(x,y) - x^n)) = f_1 \right\},$$
$$V_{n,1,f_1}(R) := \{ f \in V_{n,1}(R) : \lim_{y\to 0}(y^{-1}(f(x,y) - x^n)) = f_1 \}$$

for any $\mathbb{Z}$-algebra $R$. Since the $x^{n-1}y$-coefficient of a form in $V_{n,1}(\mathbb{Z})$ has only finitely many possibilities up to the action of $N(\mathbb{Z})$, it suffices to construct fundamental sets for the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $W_{\mathscr{A}_n,f_1}(\mathbb{R})$ for each choice of $f_1$.

We achieve this by means of a two-step process: we first construct a fundamental domain for $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ in §5.2.1–5.2.2, and we then combine this fundamental domain with fundamental sets for the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ on $W_{\mathscr{A}_n,f_1}(\mathbb{R})$ in §5.2.3. We conclude in §5.2.4 by using the results of the preceding subsections to study the action of the subgroup $\mathcal{P}_n(K) \subset \mathcal{G}_{\mathscr{A}_n}(K)$ on the subspace $W_{\mathscr{A}_n,f_1}(K)_0$, where $K$ is a field.

### 5.2.1 A box-shaped fundamental domain for $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}) \curvearrowright \mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$

A fundamental domain $\mathcal{F}$ is said to be *box-shaped at infinity* if it can be sandwiched as $\mathcal{S}_1 \subset \mathcal{F} \subset \mathcal{S}_2$, where $\mathcal{S}_1 \subset \mathcal{S}_2$ are nested generalized Siegel sets[3] for the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ satisfying the following three conditions:

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

In this subsection and the next, we construct a box-shaped fundamental domain for the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$. In particular, we prove the following theorem:

[3]See [90, §4.7, p. 224] for the definition of generalized Siegel set.

**Theorem 176.** *There exists a fundamental domain for the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ that is box-shaped at infinity.*

Because they are defined by simple equations in the cusp, box-shaped fundamental domains are particularly amenable to explicit computations. For instance, we use the box-shaped property to evaluate a certain integral that arises in the proof of Theorem 169; see (5.23). As another example of the utility of box-shaped fundamental domains, see [66,67], where Grenier proves the analogue of Theorem 176 for the group $\mathrm{SL}_n$ and remarks that his result could be used to compute certain integrals of Eisenstein series that arise when generalizing Selberg's trace formula to the group $\mathrm{SL}_n(\mathbb{Z})$. Grenier's work has had a number of applications in the literature (see, e.g., [65, 100, 120]), and as explained in §5.2.2 (to follow), it plays a central role in our proof of Theorem 176.

The construction of nested generalized Siegel sets $\mathcal{S}_1 \subset \mathcal{S}_2$ satisfying the three conditions itemized above is deferred to §5.2.2. Once $\mathcal{S}_1$ and $\mathcal{S}_2$ have been constructed, Theorem 176 then follows from the next lemma, which shows that there exists a fundamental domain sandwiched between them:

**Lemma 177.** *Let $\Lambda$ be a discrete subgroup of a Lie group $\mathcal{G}$ and denote by $\mathcal{B}(\mathcal{G})$ the Borel $\sigma$-algebra of $\mathcal{G}$. Suppose that $\mathcal{S}_1$ and $\mathcal{S}_2$ are sets in $\mathcal{B}(\mathcal{G})$ with the property that the maps $\mathcal{S}_1 \to \mathcal{G}/\Lambda$ and $\mathcal{S}_2 \to \mathcal{G}/\Lambda$ induced by $s \mapsto s\Lambda$ are, respectively, injective and surjective. Then there is a fundamental domain $\mathcal{F}$ in $\mathcal{B}(\mathcal{G})$ for the action of $\Lambda$ on $\mathcal{G}$ such that $\mathcal{S}_1 \subset \mathcal{F} \subset \mathcal{S}_2$.*

*Proof.* The argument is analogous to the proof of [86, Lemma 4.1.1]. Since $\Lambda$ is discrete, we can find a non-empty open subset $U \subset \mathcal{G}$ such that $U^{-1}U \cap \Lambda = \{\mathrm{id}\}$. Since $\mathcal{G}$ is second countable, we can find a sequence of elements $\{g_n\} \subset \mathcal{G}$ such that $\mathcal{G} = \bigcup_{n=1}^{\infty} g_n U$. Let $\mathcal{S}'' = \mathcal{S}_2 \smallsetminus \mathcal{S}_1\Lambda$ and set:

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

Lastly, define $\mathcal{F} = \mathcal{S} \cup \mathcal{F}'$ and note that this union is disjoint. Then $\mathcal{F} \in \mathcal{B}(\mathcal{G})$ since all the

operations used in its construction keep us in the $\sigma$-algebra. It is straightforward to check that the induced map $\mathcal{F} \to \mathcal{G}/\Lambda$ sending $x \mapsto x\Lambda$ is bijective. We conclude that $\mathcal{F}$ is a fundamental domain. $\square$

### 5.2.2 A pair of nested generalized Siegel sets for $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}) \curvearrowright \mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$

In this section, we complete the proof of Theorem 176 by constructing the nested generalized Siegel sets $\mathcal{S}_1 \subset \mathcal{S}_2$ referred to in §5.2.1. To begin with, observe that it suffices to construct the Siegel sets $\mathcal{S}_i$ for the action of $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{Z})$ on $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{R})$, because when $n$ is even, there exist elements in $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ having determinant $-1$. We therefore work with the group $\mathrm{SO}_{\mathscr{A}_n}$ throughout the rest of this subsubsection.

The construction of $\mathcal{S}_2$ is, in essence, due to Borel and Harish-Chandra (see [15, §9.2] and [105, §4.1], which specialize the results of [34] and [35] for semisimple groups to the case of the group $\mathrm{SO}_{\mathscr{A}_n}$). Let $\mathcal{N} \subset \mathrm{SO}_{\mathscr{A}_n}(\mathbb{R})$ denote the subgroup of lower-triangular unipotent matrices. A calculation shows that the elements of $\mathcal{N}$ are parametrized as in Figure 2, where the $u_{ij} \in \mathbb{R}$ for $i \in \{2, \ldots, n-1\}$ and $j \in \{1, \ldots, \min\{i-1, n-i\}\}$ are free parameters, and where the symbol "$*$" is shorthand and should be read as follows: if the "$*$" occurs in the row-$i$, column-$j$ entry, then it denotes "some polynomial of positive degree in the variables $\{u_{i'j'} : i' - j' \leq i - j\}$ with integer coefficients and no constant term" (the polynomial being abbreviated depends on the matrix entry in which it occurs). We often abbreviate the tuple $\big(u_{ij} : i \in \{2, \ldots, n-1\},\, j \in \{1, \ldots, \min\{i-1, n-i\}\}\big)$ by $u$ and abuse notation by writing $u$ for the corresponding element of $\mathcal{N}$.

Let $\mathcal{A}$ denote the subgroup of diagonal matrices in $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{R})$, all of whose entries are positive. The elements of $\mathcal{A}$, which is a maximal torus of $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{R})$ normalizing the unipotent subgroup $\mathcal{N}$, admit the following explicit parametrization: the $i^{\text{th}}$ diagonal entry is the

$$\begin{bmatrix}
1 & & & & & & & & & & \\
u_{21} & 1 & & & & & & & & & \\
u_{31} & u_{32} & 1 & & & & & & & & \\
\vdots & \vdots & \vdots & \ddots & & & & & & & \\
u_{(\lceil \frac{n}{2} \rceil -1)1} & u_{(\lceil \frac{n}{2} \rceil -1)2} & u_{(\lceil \frac{n}{2} \rceil -1)3} & \cdots & 1 & & & & & & \\
u_{\lceil \frac{n}{2} \rceil 1} & u_{\lceil \frac{n}{2} \rceil 2} & u_{\lceil \frac{n}{2} \rceil 3} & \cdots & u_{\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor} & 1 & & & & & \\
u_{(\lceil \frac{n}{2} \rceil +1)1} & u_{(\lceil \frac{n}{2} \rceil +1)2} & u_{(\lceil \frac{n}{2} \rceil +1)3} & \cdots & -\frac{1}{2}u^2_{\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor} + * & -u_{\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor} & 1 & & & & \\
\vdots & \vdots & \vdots & \iddots & \vdots & \vdots & \vdots & \ddots & & & \\
u_{(n-2)1} & u_{(n-2)2} & -\frac{1}{2}u^2_{\lceil \frac{n}{2} \rceil 3} + * & \cdots & * & * & * & \cdots & 1 & & \\
u_{(n-1)1} & -\frac{1}{2}u^2_{\lceil \frac{n}{2} \rceil 2} + * & * & \cdots & * & * & * & \cdots & -u_{32} & 1 & \\
-\frac{1}{2}u^2_{\lceil \frac{n}{2} \rceil 1} + * & * & * & \cdots & * & * & * & \cdots & * & -u_{21} & 1
\end{bmatrix} \tag{5.3}$$

$$\begin{bmatrix}
1 & & & & & & & & & & \\
u_{21} & 1 & & & & & & & & & \\
u_{31} & u_{32} & 1 & & & & & & & & \\
\vdots & \vdots & \vdots & \ddots & & & & & & & \\
u_{(\frac{n-2}{2})1} & u_{(\frac{n-2}{2})2} & u_{(\frac{n-2}{2})3} & \cdots & 1 & & & & & & \\
u_{\frac{n}{2}1} & u_{\frac{n}{2}2} & u_{\frac{n}{2}3} & \cdots & u_{\frac{n}{2}(\frac{n-2}{2})} & 1 & & & & & \\
u_{(\frac{n+2}{2})1} & u_{(\frac{n+2}{2})2} & u_{(\frac{n+2}{2})3} & \cdots & u_{(\frac{n+2}{2})(\frac{n-2}{2})} & 0 & 1 & & & & \\
u_{(\frac{n+4}{2})1} & u_{(\frac{n+4}{2})2} & u_{(\frac{n+4}{2})3} & \cdots & * & * & -u_{\frac{n}{2}(\frac{n-2}{2})} & 1 & & & \\
\vdots & \vdots & \vdots & \iddots & \vdots & \vdots & \vdots & \vdots & \ddots & & \\
u_{(n-2)1} & u_{(n-2)2} & * & \cdots & * & * & * & * & \cdots & 1 & \\
u_{(n-1)1} & * & * & \cdots & * & * & * & * & \cdots & -u_{32} & 1 \\
* & * & * & \cdots & * & * & * & * & \cdots & * & -u_{21} \quad 1
\end{bmatrix} \tag{5.4}$$

Figure 2: Parametrization of elements of $\mathcal{N}$.

reciprocal of the $(n-i)^{\text{th}}$, and the first $\lceil \frac{n}{2} \rceil$ diagonal entries can be expressed in the form

$$\prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} s_i^{-1}, \prod_{i=2}^{\lfloor \frac{n}{2} \rfloor} s_i^{-1}, \ldots, s_{\lfloor \frac{n}{2} \rfloor}^{-1}, 1, \qquad \text{if } 2 \nmid n, \tag{5.5}$$

$$\mathfrak{s}_n \cdot \prod_{i=1}^{\frac{n-4}{2}} s_i^{-1}, \mathfrak{s}_n \cdot \prod_{i=2}^{\frac{n-4}{2}} s_i^{-1}, \ldots, \mathfrak{s}_n, \mathfrak{s}_n \cdot s_{\frac{n-2}{2}}, \qquad \text{if } 2 \mid n, \tag{5.6}$$

where $s_i > 0$ for each $i$ and where $\mathfrak{s}_n := \sqrt{s_{\frac{n-2}{2}}^{-1} s_{\frac{n}{2}}^{-1}}$ when $n$ is even. For a given choice of $s_1, \ldots, s_{\lfloor \frac{n}{2} \rfloor} > 0$, we often abbreviate the tuple $(s_1, \ldots, s_{\lfloor \frac{n}{2} \rfloor})$ by $s$, and we often abuse notation by writing $s$ for the corresponding element of $\mathcal{A}$.

Let $K$ denote a maximal compact subgroup of $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{R})$; we denote elements of $K$ by $\theta$. Then, by [34, Théorème 2.4 and Exemple 2.5], there exists a constant $c_2 > 0$ and a compact set $\mathcal{N}' \subset \mathcal{N}$ such that if we take $\mathcal{A}' := \{s = (s_1, \ldots, s_{\lfloor \frac{n}{2} \rfloor}) \in \mathcal{A} : s_i > c_2 \text{ for all } i\}$, then the set

$$\mathcal{S}_2 := \mathcal{N}' \cdot \mathcal{A}' \cdot \big((K \cap \{\pm \mathrm{id}\}) \backslash K\big) \tag{5.7}$$

meets every orbit of $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{Z})$ on $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{R})$ (and hence every orbit of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$) at least once, where $(K \cap \{\pm \mathrm{id}\}) \backslash K$ denotes some fundamental domain for the action of $K \cap \{\pm \mathrm{id}\}$ by left-multiplication on $K$.[4] We take the quotient of $K$ by $K \cap \{\pm \mathrm{id}\}$ since $\pm \mathrm{id}$ stabilizes every element of $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{R})/K$. The next lemma computes the stabilizer of a generic element of $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{R})/K$:

**Lemma 178.** *There exists an open subset $\mathcal{U}_2 \subset \mathrm{SO}_{\mathscr{A}_n}(\mathbb{R})/K$ of full measure such that the stabilizer in $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{Z})$ of any $g \in \mathcal{U}_2$ is given by $K \cap \{\pm \mathrm{id}\}$.*

*Proof.* Let $\overline{\mathcal{F}}$ be any fundamental domain for $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{Z})$ on $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{R})/K$, and let $g$ be an element of the interior of $\overline{\mathcal{F}}$. If $\gamma \in \mathrm{SO}_{\mathscr{A}_n}(\mathbb{Z})$ stabilizes $g$, then there is an open neighborhood $U \ni g$ contained in the interior of $\overline{\mathcal{F}}$ such that $\gamma \cdot U$ is contained in the interior of $\overline{\mathcal{F}}$, implying

[4] *A priori*, [34, Théorème 2.4] states that a finite number $\sigma$ of translates of Siegel sets can be found such that their union meets every orbit of $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{Z})$ on $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{R})/K$ at least once; here, $\sigma = \#\big(\mathrm{SO}_{\mathscr{A}_n}(\mathbb{Z}) \backslash \mathrm{SO}_{\mathscr{A}_n}(\mathbb{Q}) / \mathcal{P}(\mathbb{Q})\big)$, where $\mathcal{P}(\mathbb{Q}) = (\mathcal{N} \cdot \mathcal{A}) \cap \mathrm{SO}_{\mathscr{A}_n}(\mathbb{Q})$. But since the algebraic group $\mathrm{SO}_{\mathscr{A}_n}$ has class number 1, it follows from [90, Propositions 5.4 and 5.10] that $\sigma = 1$.

in fact that $\gamma$ stabilizes every element of $U$. Since left-multiplication by $\gamma$ defines a real-analytic function on $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{R})/K$, and since $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{R})/K$ is connected (as $K$ meets both of the two connected components of $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{R})$), it follows that $\gamma$ stabilizes all of $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{R})/K$.

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

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

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

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

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

**Lemma 179.** *Let $u \in \mathcal{N}$. Then there exists $\overline{u} \in \mathcal{N} \cap \mathrm{SO}_{\mathscr{A}_n}(\mathbb{Z})$ such that $\overline{u}u \in \overline{\mathcal{N}}$. Moreover, there exists an open subset $\mathcal{U}_3 \subset \mathcal{N}$ of full measure such that for any $u \in \mathcal{U}_3$, there is precisely one element $\overline{u} \in \mathcal{N} \cap \mathrm{SO}_{\mathscr{A}_n}(\mathbb{Z})$ such that $\overline{u}u \in \overline{\mathcal{N}}$.*

*Proof.* We construct $\overline{u}$ inductively. Upon inspecting the characterization of elements of $\mathcal{N}$ provided earlier in this section, we arrive at the following observation: if $k \in \{0, \ldots, n-3\}$

is an integer and $u' \in \mathcal{N}$ is an element such that $u'_{ij} = 0$ for all $i, j$ such that $i - j \leq k$, then $(u'u)_{ij} = u'_{ij} + u_{ij}$ for all $i, j$ such that $i - j = k + 1$. By the observation, we may choose $u_1 \in \mathcal{N} \cap \mathrm{SO}_{\mathscr{A}_n}(\mathbb{Z})$ such that $\left|(u_1)_{i(i-1)} + u_{i(i-1)}\right| \leq \frac{1}{2}$ for each $i \in \{2, \ldots, \lfloor \frac{n}{2} \rfloor\}$ and such that, for $n$ odd, we have $\left|(u_1)_{\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor} + u_{\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor}\right| \leq 1$. Suppose for some $k \in \{0, \ldots, n-4\}$ we have chosen $u_\ell \in \mathcal{N} \cap \mathrm{SO}_{\mathscr{A}_n}(\mathbb{Z})$ for each $\ell \in \{1, \ldots, k+1\}$; then, by the observation, we may choose $u_{k+2} \in \mathcal{N} \cap \mathrm{SO}_{\mathscr{A}_n}(\mathbb{Z})$ such that $\left|(u_1)_{i(i-k-2)} + u_{i(i-k-2)}\right| \leq \frac{1}{2}$ for each $i \in \{k+3, \ldots, \lfloor \frac{n+k+2}{2} \rfloor\}$, unless $n$ is odd and $i = \lceil \frac{n}{2} \rceil$, in which case we can only arrange for $\left|(u_1)_{\lceil \frac{n}{2} \rceil (\lceil \frac{n}{2} \rceil - k - 2)} + u_{\lceil \frac{n}{2} \rceil (\lceil \frac{n}{2} \rceil - k - 2)}\right| \leq 1$. Having constructed $u_\ell$ for each $\ell \in \{1, \ldots, n-2\}$, we then take $\overline{u} = \prod_{\ell=1}^{n-2} u_{n-2-\ell}$.

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

By Lemma 179, we may assume that $\mathcal{N}' \subset \overline{\mathcal{N}}$. We next show that $\mathcal{N}'$ can be chosen to lie within an even smaller subset of $\overline{\mathcal{N}}$. Let $G \subset \mathrm{SO}_{\mathscr{A}_n}(\mathbb{Z})$ denote the subgroup of diagonal matrices with integer entries. One readily verifies that $G$ satisfies the following properties:

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

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

$$\widetilde{\mathcal{N}} := \left\{ u \in \overline{\mathcal{N}} : \begin{array}{c} u_{i(i-1)} \in [0, \frac{1}{2}] \text{ for each } i \in \{2, \dots, \lfloor \frac{n}{2} \rfloor\}; \\ u_{\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor} \in [-1, -\frac{1}{2}] \cup [0, \frac{1}{2}] \text{ if } 2 \nmid n \end{array} \right\}$$

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

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

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

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

**Proposition 180.** *There exists a constant $c_1 > 0$ for which (1) $\mathcal{S}_1 \subset \mathcal{S}_2$ and (2) there exists an open subset $\mathcal{U}_1 \subset \mathcal{S}_1$ of full measure such that every orbit of $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{Z})$ on $\mathrm{SO}_{\mathscr{A}_n}(\mathbb{R})$ meets $\mathcal{U}_1$ at most once.*

*Proof.* In [67], Grenier constructs an explicit fundamental domain $\mathcal{F}$ for the action of $\mathrm{SL}_n^{\pm}(\mathbb{Z})$ on $\mathrm{SL}_n^{\pm}(\mathbb{R})$ that is box-shaped at infinity. We shall deduce Proposition 180 from a slight reformulation of Grenier's result. To state this reformulation, we must introduce some notation. Let $\mathscr{N} \subset \mathrm{SL}_n^{\pm}(\mathbb{R})$ denote the subgroup of lower-triangular unipotent matrices; for an element $u \in \mathscr{N}$, we denote by $u_{ij}$ the row-$i$, column-$j$ entry of $u$. Let $\overline{\mathscr{N}}$ be the set defined by

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

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

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

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

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

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

**Lemma 181.** *For every sufficiently large $c_1 > 0$, the following holds: If $us\theta, u's'\theta' \in \mathscr{N}' \cdot \mathscr{A}' \cdot (\{\pm \mathrm{id}, \pm\varepsilon_n\}\backslash\mathscr{K})$ are $\mathrm{SL}_n^{\pm}(\mathbb{Z})$-equivalent elements such that $s_i, s_i' > c_1$ for all $i$ and such that $u, u'$ lie in the interior of $\mathscr{N}'$, then $us\theta = u's'\theta'$.*

*Proof of Lemma 181.* In [66], Grenier constructs a fundamental domain $\overline{\mathcal{F}} \subset \mathscr{N} \cdot \mathscr{A}$ for the action of $\mathrm{SL}_n^{\pm}(\mathbb{Z})$ on $\mathrm{SL}_n^{\pm}(\mathbb{R})/\mathscr{K}$. The domain $\overline{\mathcal{F}}$ has the property that no two points in its interior are $\mathrm{SL}_n^{\pm}(\mathbb{Z})$-equivalent. In [67, Theorem 1], Grenier establishes that, for every sufficiently large $c_1 > 0$, we have $\mathscr{N}'' \cdot \mathscr{A}' \subset \overline{\mathcal{F}}$, where $\mathscr{N}'' = \{u \in \mathscr{N}' : u_{(\frac{n+2}{2})\frac{n}{2}} \in [0, \frac{1}{2}]\}$. Consequently, the set $\overline{\mathcal{F}} \cdot (\{\pm \mathrm{id}\}\backslash\mathscr{K})$ is a fundamental domain for the action of $\mathrm{SL}_n^{\pm}(\mathbb{Z})$ on $\mathrm{SL}_n^{\pm}(\mathbb{R})$ containing $\mathscr{N}'' \cdot \mathscr{A}' \cdot (\{\pm \mathrm{id}\}\backslash\mathscr{K})$. Since $\varepsilon_n \cdot \mathscr{N}'' \cdot \varepsilon_n = \mathscr{N}'$, it follows that there is a fundamental domain for the action of $\mathrm{SL}_n^{\pm}(\mathbb{Z})$ on $\mathrm{SL}_n^{\pm}(\mathbb{R})$ containing $\mathscr{N}' \cdot \mathscr{A}' \cdot (\{\pm \mathrm{id}, \pm\varepsilon_n\}\backslash\mathscr{K})$. If we have two distinct $\mathrm{SL}_n^{\pm}(\mathbb{Z})$-equivalent elements $us\theta, u's'\theta' \in \mathscr{N}' \cdot \mathscr{A}' \cdot (\{\pm \mathrm{id}, \pm\varepsilon_n\}\backslash\mathscr{K})$ such that $u, u'$ lie in the interior of $\mathscr{N}'$, then one can find two distinct elements of the interior of $\overline{\mathcal{F}}$ that are $\mathrm{SL}_n^{\pm}(\mathbb{Z})$-equivalent, which is a contradiction. □

We now deduce Proposition 180 from Lemma 181. Let $\mathcal{U}_1$ be an open subset of full measure contained in the interior of $\mathcal{S}_1$ consisting of elements $us\theta$ satisfying the following

two properties:

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

To see why we can arrange for the second property above to hold on a open subset of full measure, observe that by the definitions of $\mathcal{N}'$ and $\mathscr{N}'$, the desired element $u_0$ must be such that $(u_0)_{i(i-1)} = 0$ for each $i$. Then, by proving the analogue of Lemma 179 for the group $\mathrm{SL}_n^{\pm}$, one finds that there exists at least one $u_0 \in \mathscr{N} \cap \mathrm{SL}_n^{\pm}(\mathbb{Z})$ such that $u_0 u \in \mathscr{N}'$. By our explicit characterization of the elements of $\mathcal{N}$ (see (5.3) and (5.4)), the row-$i$, column-$j$ entry of $u$ is a non-constant polynomial in the unipotent coordinates for every pair $(i, j)$ with $i > j+1$. Thus, there exists an open subset $\mathcal{U}_3 \subset \mathcal{N}$ of full measure such that for any $u \in \mathcal{U}_3$ and $u_0 \in \mathscr{N} \cap \mathrm{SL}_n^{\pm}(\mathbb{Z})$, the row-$i$, column-$j$ entry of $u_0 u$ is not an integer multiple of $\frac{1}{2}$ for every pair $(i, j)$ with $i > j$, unless $i + 1 = j = \frac{n}{2}$, in which case $u_{ij} = 0$. In particular, if for $u \in \mathcal{U}_3$ and $u_0 \in \mathscr{N} \cap \mathrm{SL}_n^{\pm}(\mathbb{Z})$ we have $u_0 u \in \mathscr{N}'$, then $u_0 u$ must in fact lie in the interior of $\mathscr{N}'$, and imitating the proof of uniqueness in Lemma 179 yields that $u_0$ must be unique.

With $\mathcal{U}_1$ defined, take $us\theta, u's'\theta' \in \mathcal{U}_1$ such that $g \cdot us\theta = u's'\theta'$ for some $g \in \mathrm{SO}_{\mathscr{A}_n}(\mathbb{Z})$. Let $\varepsilon, \varepsilon' \in \{\pm \mathrm{id}, \pm\varepsilon_n\}$ be such that $\varepsilon\theta, \varepsilon'\theta' \in \{\pm \mathrm{id}, \pm\varepsilon_n\} \backslash \mathscr{K}$. Let $u_0, u_0' \in \mathscr{N} \cap \mathrm{SL}_n^{\pm}(\mathbb{Z})$ be the unique elements such that $u_0(\varepsilon u \varepsilon), u_0'(\varepsilon' u' \varepsilon')$ lie in the interior of $\mathscr{N}'$. Since $s_i, s_i' > c_1$ for all $i$, Lemma 181 implies $u_0(\varepsilon u \varepsilon) s(\varepsilon\theta) = u_0'(\varepsilon' u' \varepsilon') s'(\varepsilon'\theta')$. The uniqueness of the Iwasawa decomposition implies

$$u_0(\varepsilon u \varepsilon) = u_0'(\varepsilon' u' \varepsilon'), \quad s = s', \quad \varepsilon\theta = \varepsilon'\theta'. \tag{5.8}$$

The third equality in (5.8) implies that $\varepsilon\varepsilon' \in K$, so since $\varepsilon_n \notin K$ when $n$ is even, it follows that $\varepsilon\varepsilon' = \pm \mathrm{id}$. But $(K \cap \{\pm \mathrm{id}\}) \backslash K$ contains either $\theta$ of $-\theta$ and not both, meaning that $\varepsilon\varepsilon' = \mathrm{id}$. Combining this with the first equality in (5.8) yields that $u$ is a translate of $u'$ by an element of $\mathscr{N} \cap \mathrm{SL}_n^{\pm}(\mathbb{Z})$, and hence by an element of $\mathcal{N} \cap \mathrm{SO}_{\mathscr{A}_n}(\mathbb{Z})$. The uniqueness

statement in Lemma 179 then implies that $u = u'$. We conclude that $us\theta = us'\theta'$. This completes the proof of Proposition 180. □

*Remark* 182. We proved Proposition 180 by simply deducing it from Grenier's explicit construction of a box-shaped fundamental domain for $\mathrm{SL}_n^{\pm}(\mathbb{Z})$ on $\mathrm{SL}_n^{\pm}(\mathbb{R})$. We expect that it is possible to construct an explicit box-shaped fundamental domain for $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ by mimicking Grenier's construction. Alternatively, when $n \in \{3, 4\}$, such a fundamental domain can be built using exceptional isomorphisms. For instance, take $n = 3$, and let $A_{\frac{1}{2}}$ be as in the proof of Theorem 51. Then one checks that $\mathcal{G}_{A_{\frac{1}{2}}}(\mathbb{Q}) = g\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q})g^{-1}$, where $g \in \mathrm{GL}_3(\mathbb{Q})$ is the diagonal matrix with diagonal entries $\frac{1}{2}$, 1, 1. Now, recall that we have an exceptional isomorphism $\mathrm{PGL}_2 \simeq \mathcal{G}_{A_{\frac{1}{2}}}$ of algebraic groups over $\mathbb{Z}$, induced by the adjoint representation of $\mathrm{PGL}_2$. Thus, $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ may be viewed as a lattice $\Gamma \subset \mathrm{PGL}_2(\mathbb{Q})$; a calculation shows that $\Gamma$ is the subgroup of $\mathrm{PGL}_2(\mathbb{Q})$ generated by the (classes of the) elements of the congruence subgroup $\Gamma^0(2) \subset \mathrm{SL}_2(\mathbb{Z})$ together with the matrices $\left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & 2 \\ -1 & 0 \end{smallmatrix}\right]$. It is then an elementary calculation to verify that the action of $\Gamma$ on $\mathrm{PGL}_2(\mathbb{R})/\mathrm{O}_2(\mathbb{R})$ has a fundamental domain in the upper half-plane $\mathbb{H}$ that is contained in the strip $\{z \in \mathbb{H} : \Re(z) \in [0, 1]\}$ and that contains the set $\{z \in \mathbb{H} : \Re(z) \in [0, 1], \Im(z) = y\}$ for every sufficiently large $y > 0$. A similar argument can be made when $n = 4$, using the exceptional isomorphism between the identity component of $\mathcal{G}_{\mathscr{A}_n}$ and the group $\mathrm{SL}_2 \times \mathrm{SL}_2$.

### 5.2.3 Fundamental sets for $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R}) \curvearrowright W_{\mathscr{A}_n,f_1}(\mathbb{R})$ and $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}) \curvearrowright W_{\mathscr{A}_n,f_1}(\mathbb{R})$

There is exactly one reducible $B \in W_{\mathscr{A}_n,f_1}(\mathbb{R})$ up to the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ with $\iota(\mathscr{A}_n, B) = f$ for each separable $f \in V_{n,1}(\mathbb{R})$; an explicit representative of this orbit is given as follows. Take any $(f_2, \dots, f_n) \in \mathbb{R}^{n-1}$, let $f(x, y) = x^n + \sum_{i=1}^n f_i x^{n-i} y^i \in V_{1,n}(\mathbb{R})$, and let $\widetilde{f} \in V_{1,n,0}(\mathbb{R})$ be as in (2.1). If we define a function $\sigma_0 \colon \mathbb{R}^{n-1} \to W_{\mathscr{A}_n,f_1}(\mathbb{R})$ by

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

if $n$ is odd, and by

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

if $n$ is even, then $\iota(\mathscr{A}_n, \sigma_0(f)) = f$. The explicit section $\sigma_0$ is useful in the proof of Proposition 191 (to follow), for its image consists of matrices whose entries are polynomials in the $f_i$. However, in Lemma 187 (also to follow), we shall require a section $\sigma$ with image consisting of matrices whose entries are $O(X)$ if $\mathrm{H}(f) \ll X$. To this end, let $(f_2, \ldots, f_n) \in \mathbb{R}^{n-1}$ be as above, and let $j \in \{2, \ldots, n\}$ be any index such that $\max\{|\widetilde{f}_i|^{\frac{1}{i}} : i \in \{2, \ldots, n\}\} = |\widetilde{f}_j|^{\frac{1}{j}}$. If we define

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

then $\iota(\mathscr{A}_n, \sigma(f_2, \ldots, f_n)) = f$.

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

$$W_{\mathscr{A}_n, f_1}(R)^{r_1, r_2} := W_{\mathscr{A}_n, f_1}(R) \cap W_{\mathscr{A}_n}(R)^{r_1, r_2},$$

where $R = \mathbb{Z}$ or $\mathbb{R}$. Let $L_{f_1}^{r_1, r_2}$ be the fundamental set for the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ on $W_{\mathscr{A}_n, f_1}(\mathbb{R})^{r_1, r_2}$ defined by

$$L_{f_1}^{r_1, r_2} := \left\{ \sigma(f_2, \ldots, f_n) : \begin{array}{c} (f_2, \ldots, f_n) \in \mathbb{R}^{n-1}, \\ x^n + \sum_{i=1}^n f_i x^{n-i} y^i \in V_{n, f_1}(\mathbb{R})^{r_1, r_2} \text{ has nonzero disc.} \end{array} \right\}$$

From the stabilizer statement in Theorem 13, it follows that $\#\operatorname{Stab}_{\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})}(B)$ is independent of $B \in W_{\mathscr{A}_n, f_1}(\mathbb{R})^{r_1, r_2}$; letting $n_{r_1, r_2} := \#\operatorname{Stab}_{\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})}(B)$ for any $B \in W_{\mathscr{A}_n, f_1}(\mathbb{R})^{r_1, r_2}$, one readily verifies that $n_{r_1, r_2} = 2^{r_1 + r_2 - 1}$ if $n$ is odd and $n_{r_1, r_2} = 2^{r_1 + r_2}$ if $n$ is even.

We are finally in position to construct a fundamental set for the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $W_{\mathscr{A}_n, f_1}(\mathbb{R})$. For each possible value of $r_1$ and $f_1$, we simply take our fundamental set to be the multiset $\mathcal{F} \cdot L_{f_1}^{r_1, r_2}$. Note that if $B \in (\mathcal{F} \cdot L_{f_1}^{r_1, r_2}) \cap W_{\mathscr{A}_n, f_1}(\mathbb{Z})$, then $B$ occurs with multiplicity $n_{r_1, r_2} / \#\operatorname{Stab}_{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})}(B)$.

### 5.2.4 Action of lower-triangular subgroup on reducible hyperplane

We first prove a result implying that, for any $f \in V_{n,1,f_1}(\mathbb{R})$ with $\Delta(f) \neq 0$, where $\Delta$ denotes the discriminant, the group $\mathcal{N} \cdot \mathcal{A}$ acts transitively on the set of $B \in W_{\mathscr{A}_n, f_1}(\mathbb{R})_0$ such that $b_{i(n-i)}(B) > 0$ for each $i \in \{1, \ldots, \lfloor \frac{n}{2} \rfloor\}$ and such that $\iota(A_n, B) = f$.

**Lemma 183.** *Let $\widetilde{\sigma} \colon V_{n,1,f_1}(\mathbb{R}) \to W_{\mathscr{A}_n, f_1}(\mathbb{R})_0$ be a differentiable function such that for each $f(x, y) = x^n + \sum_{i=1}^n f_i x^{n-i} y^i \in V_{n,1,f_1}(\mathbb{R})$, we have:*

- *$b_{i(n-i)}(\widetilde{\sigma}(f)) > 0$ for each $i \in \{1, \ldots, \lfloor \frac{n}{2} \rfloor\}$; and*
- *$\iota(\mathscr{A}_n, \widetilde{\sigma}(f)) = f$.*

*Let $\mathcal{R} \subset V_{n,1,f_1}(\mathbb{R})$ be an open subset consisting entirely of forms with nonzero discriminant. Then there exist differentiable functions $\widetilde{u}\colon \mathcal{R} \to \mathcal{N}$ and $\widetilde{s}\colon \mathcal{R} \to \mathcal{A}$ such that for each $f \in \mathcal{R}$, we have $\widetilde{\sigma}(f) = \big(\widetilde{u}(f)\widetilde{s}(f)\big) \cdot \sigma_0(f)$.*

*Proof.* We first construct $\widetilde{u}$. Using (5.3) and (5.4), we see that for any $B \in W_{\mathscr{A}_n,f_1}(\mathbb{R})_0$ such that $b_{i(n-i)}(B) \neq 0$ for each $i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}$, we have the following:

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

- Let $\widetilde{u}_{32} \in \mathbb{R}$ be such that $b_{2(n-1)}(B) + b_{2(n-2)}(B)\widetilde{u}_{32} = \frac{f_1}{n}$; abusing notation once again, we redefine $B$ to be $\widetilde{u}_{32} \cdot B$. Next, let $\widetilde{u}_{31} \in \mathbb{R}$ be such that $b_{2n}(B) + b_{2(n-2)}(B)\widetilde{u}_{31} = 0$; we redefine $B$ to be $\widetilde{u}_{31} \cdot B$.

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

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

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

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

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

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

$\widetilde{u}_{k\min\{k-k'-1,n-k-k'\}} \in \mathbb{R}$ be such that

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

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

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

Define functions $\widetilde{s}_i$ by $\widetilde{s}_i(f) := b_{i(n-i)}(\widetilde{\sigma}(f))$ for $i \in \{1, \ldots, \lfloor \frac{n}{2} \rfloor\} \smallsetminus \{\frac{n}{2}\}$ and $\widetilde{s}_{\frac{n}{2}}(f) := b_{\frac{n}{2}\frac{n}{2}}(\widetilde{\sigma}(f))b_{(\frac{n}{2}-1)(\frac{n}{2}+1)}(\widetilde{\sigma}(f))^{-1}$. Let $\widetilde{s} = (\widetilde{s}_1, \ldots, \widetilde{s}_{\lfloor \frac{n}{2} \rfloor})$. Since $\widetilde{\sigma}$ is differentiable, it follows that $\widetilde{s}$ is differentiable too; note further that because we have assumed $\mathcal{R}$ to be contained in the complement of the locus of forms of discriminant 0, it follows from [15, Lemma 10.3] when $n$ is odd and from [109, Part (2) of Theorem 4.2] when $n$ is even that $\widetilde{s}_i(f) > 0$ for every $i \in \{1, \ldots, \lfloor \frac{n}{2} \rfloor\}$ and $f \in \mathcal{R}$, and so $\widetilde{s}(f)$ is invertible for every $f \in \mathcal{R}$.

We have defined $\widetilde{u}$ and $\widetilde{s}$ in such a way that $\big(\widetilde{u}(f)\widetilde{s}(f)\big)^{-1} \cdot \widetilde{\sigma}(f)$ lies in the image of $\sigma_0$; i.e., we have $\big(\widetilde{u}(f)\widetilde{s}(f)\big)^{-1} \cdot \widetilde{\sigma}(f) = \sigma_0(f')$ for some $f' \in V_{n,1,f_1}(\mathbb{R})$. It then follows that

$$f' = \iota(\mathscr{A}_n, \sigma_0(f')) = \iota\big(\mathscr{A}_n, (\widetilde{u}(f)\widetilde{s}(f))^{-1} \cdot \widetilde{\sigma}(f)\big) = \iota\big(\mathscr{A}_n, \widetilde{\sigma}(f)\big) = f,$$

so we conclude that $f = f'$. □

The following lemma, the proof of which is immediate, describes the stabilizer of the action of $\mathcal{P}_n(K)$ on an element of $W_{\mathscr{A}_n}(K)_0$, where $K$ is any field:

**Lemma 184.** *Let $K$ be a field, and let $B \in W_{\mathscr{A}_n}(K)_0$ be such that $\Delta(\iota(\mathscr{A}_n, B)) \neq 0$. Then $\mathrm{Stab}_{\mathcal{P}_n(K)}(B) = \{\mathrm{id}\}$ if $n$ is odd and $\mathrm{Stab}_{\mathcal{P}_n(K)}(B) = \{\pm \mathrm{id}\}$ if $n$ is even.*

## 5.3 Counting reducible $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$-orbits on $W_{\mathscr{A}_n}(\mathbb{Z})$

Retain the setting of §5.2 (i.e., let $n$, $(r_1, r_2)$, and $f_1$ be as in §5.2).[5] In this section, we obtain asymptotics for the number of reducible orbits of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $W_{\mathscr{A}_n,f_1}(\mathbb{Z})^{r_1,r_2}$ of bounded height. We express these asymptotics in terms of a weighted volume of sets in $W_{\mathscr{A}_n}(\mathbb{R})$. To state the main result of this section, and to simplify the exposition in the rest of the paper, we introduce the following notation:

- Let $dB$ denote Euclidean measure on $W_{\mathscr{A}_n}(\mathbb{R})_0$, and we define $\lambda(B)$ by

$$\lambda(B) := \begin{cases} \displaystyle\prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} |b_{i(n-i)}(B)|^{2i-1}, & \text{if } 2 \nmid n, \\ \displaystyle |b_{\frac{n}{2}\frac{n}{2}}(B)|^{\frac{n-2}{2}} \prod_{i=1}^{\frac{n-2}{2}} |b_{i(n-i)}(B)|^{2i-1}, & \text{if } 2 \mid n. \end{cases} \tag{5.9}$$

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

$$\mathcal{B} := \left\{ B \in H \cdot L_{f_1}^{r_1,r_2} \cap W_{\mathscr{A}_n}(\mathbb{R})_0 : b_{i(n-i)} > 0 \text{ for each } i \in \{1, \dots, \lfloor \tfrac{n}{2} \rfloor\} \right\}.$$

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

$$dg = d\theta du(\delta(s)ds), \text{ where } du := \prod_{i=1}^{\lceil \frac{n}{2} \rceil} \prod_{j=1}^{i-1} du_{ij}, \; ds := \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} ds_i, \text{ and} \tag{5.10}$$

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

  where $d\theta$ is normalized so that $\int_{\theta \in (K \cap \{\pm \mathrm{id}\}) \backslash K} d\theta = 1$.

- Let $dh$ denote the restriction of $dg$ to $H$. We define the quantity $C_X$ by

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

[5] Note that definitions of quantities introduced in what follows may implicitly depend on $r_1$.

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

Then, over the next two subsections, we prove the following result, where we write "$a(X) \sim b(X)$" to mean that $a(X) = b(X) \cdot (1 + o(1))$ in the limit as $X \to \infty$:

**Theorem 185.** *We have that*

$$\sharp\left(\frac{(W_{\mathscr{A}_n,f_1}(\mathbb{Z})^{r_1,r_2}_{\mathrm{red}})_X}{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})}\right) \sim \frac{1}{n_{r_1,r_2}} \cdot \left\{\begin{array}{ll} 2^{\lfloor \frac{n}{2} \rfloor} \displaystyle\prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \zeta(2i), & \text{if } 2 \nmid n, \\ 4\zeta(\frac{n}{2}) \displaystyle\prod_{i=1}^{\frac{n-2}{2}} \zeta(2i), & \text{if } 2 \mid n \end{array}\right\} \cdot C_X. \tag{5.11}$$

### 5.3.1 Averaging over fundamental domains

In this section, we apply Bhargava's technique for averaging over fundamental domains to put the left-hand side of (5.11) into a more convenient form.

Let $\mathcal{F}$ be a fundamental domain for the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ that is box-shaped at infinity (recall that such an $\mathcal{F}$ exists by Theorem 176). For any given $h \in H$, we have

$$\sharp\left(\frac{(W_{\mathscr{A}_n,f_1}(\mathbb{Z})^{r_1,r_2}_{\mathrm{red}})_X}{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})}\right) = \left\{\begin{array}{ll} \frac{1}{n_{r_1,r_2}} \cdot \#\big(\mathcal{F}h \cdot L^{r_1,r_2}_{f_1} \cap (W_{\mathscr{A}_n}(\mathbb{Z})_{\mathrm{red}})_X\big), & \text{if } 2 \nmid n, \\ \frac{2}{n_{r_1,r_2}} \cdot \#\big(\mathcal{F}h \cdot L^{r_1,r_2}_{f_1} \cap (W_{\mathscr{A}_n}(\mathbb{Z})_{\mathrm{red}})_X\big), & \text{if } 2 \mid n. \end{array}\right. \tag{5.12}$$

Letting $C_H = n_{r_1,r_2} \int_{h \in H} dh$ if $n$ is odd and $C_H = \frac{n_{r_1,r_2}}{2} \int_{h \in H} dh$ if $n$ is even, and averaging (5.12) over $h \in H$, we find that

$$\sharp\left(\frac{(W_{\mathscr{A}_n,f_1}(\mathbb{Z})^{r_1,r_2}_{\mathrm{red}})_X}{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})}\right) = \frac{1}{C_H} \int_{h \in H} \#\big(\mathcal{F}h \cdot L^{r_1,r_2}_{f_1} \cap (W_{\mathscr{A}_n}(\mathbb{Z})_{\mathrm{red}})_X\big) dh. \tag{5.13}$$

By [15, Propositions 10.5, 10.7] when $2 \nmid n$ and [105, Propositions 21, 23] when $2 \mid n$,[6] the

[6]Technically, [15, Proposition 10.7] and [105, Proposition 23] are stated in the case where $f_1 = 0$ and for a differently normalized height, but one readily verifies that their proofs go through for any fixed $f_1 \in \mathbb{Z}$ and for the height H.

expected value of $\#\big(\mathcal{F}h \cdot L_{f_1}^{r_1,r_2} \cap (W_{\mathscr{A}_n}(\mathbb{Z})_{\mathrm{red}} \smallsetminus W_{\mathscr{A}_n}(\mathbb{Z})_0)_X\big)$ as $h \in H$ is drawn uniformly at random with respect to the measure $dh$ is $o(X^{\frac{n^2+n-2}{2}})$.[7] Consequently, up to a negligible error, we may replace $W_{\mathscr{A}_n}(\mathbb{Z})_{\mathrm{red}}$ in (5.13) with $W_{\mathscr{A}_n}(\mathbb{Z})_0$. Then, using a now-standard change-of-variables argument due to Bhargava (see, e.g., [15, §10.1]), it follows that

$$\sharp\left(\frac{(W_{\mathscr{A}_n,f_1}(\mathbb{Z})_{\mathrm{red}}^{r_1,r_2})_X}{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})}\right) \sim \frac{1}{C_H}\int_{g\in\mathcal{F}} \#\big(gH \cdot L_{f_1}^{r_1,r_2} \cap (W_{\mathscr{A}_n}(\mathbb{Z})_0)_X\big)dg. \tag{5.14}$$

For $\bullet \in \{\mathcal{N}, \mathcal{A}\}$, consider the map $\pi_\bullet\colon \mathcal{G}_{\mathscr{A}_n}(\mathbb{R}) \to \mathcal{A}$ obtained by post-composing the diffeomorphism $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R}) \to \mathcal{N}\times\mathcal{A}\times\mathcal{K}$ given by the Iwasawa decomposition with the projection map $\mathcal{N}\times\mathcal{A}\times\mathcal{K} \to \bullet$. Let $\mathcal{A}^\star := \pi_{\mathcal{A}}(\mathcal{F})$, and for each $s \in \mathcal{A}^\star$, let $\mathcal{N}^\star(s) := \pi_{\mathcal{N}}(\pi_{\mathcal{A}}^{-1}(s)\cap\mathcal{F})$; observe that $\mathcal{N}^\star(s)$ is bounded by construction. Then, setting $\mathcal{B}(u,s) := usH \cdot L_{f_1}^{r_1,r_2} \cap W_{\mathscr{A}_n}(\mathbb{R})_0$ for the sake of convenience, we can rewrite the expression (5.14) as follows:

$$\begin{aligned}
&\sharp\left(\frac{(W_{\mathscr{A}_n,f_1}(\mathbb{Z})_{\mathrm{red}}^{r_1,r_2})_X}{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})}\right) \sim \\
&\frac{1}{C_H}\int_{s\in\mathcal{A}^\star}\int_{u\in\mathcal{N}^\star(s)}\int_{\theta\in(K\cap\{\pm\mathrm{id}\})\backslash K} \#\big(us\theta H \cdot L_{f_1}^{r_1,r_2} \cap W_{\mathscr{A}_n}(\mathbb{Z})_0)_X\big)d\theta du(\delta(s)ds) \sim \\
&\frac{1}{C_H}\int_{s\in\mathcal{A}^\star}\int_{u\in\mathcal{N}^\star(s)} \#(\mathcal{B}(u,s)_X \cap W_{\mathscr{A}_n}(\mathbb{Z}))du(\delta(s)ds),
\end{aligned} \tag{5.15}$$

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

### 5.3.2 Slicing

To evaluate (5.15), we cut $\mathcal{B}(u,s)$ into slices, one for each value of $(b_{1(n-1)},\dots,b_{\lfloor\frac{n}{2}\rfloor\lceil\frac{n}{2}\rceil})$. For any $b = (b_1,\dots,b_{\lfloor\frac{n}{2}\rfloor}) \in (\mathbb{R}\smallsetminus\{0\})^{\lfloor\frac{n}{2}\rfloor}$, let $\mathcal{B}_b(u,s) \subset \mathcal{B}(u,s)$ be the subset of elements $B = [b_{ij}]$ such that $b_{i(n-i)} = b_i$ for each $i \in \{1,\dots,\lfloor\frac{n}{2}\rfloor\}$. Then we can express the integrand

[7] We note that this bound can be improved to $O_\epsilon(X^{\frac{n^2+n-2}{2}-\frac{1}{5}+\epsilon})$ by an application of the Selberg sieve (see [29, Proofs of Propositions 3.5 and 4.4]).

of (5.15) as

$$\#(\mathcal{B}(u,s)_X \cap W_{\mathscr{A}_n}(\mathbb{Z})) = \sum_{\substack{b \in \mathbb{Z}^{\lfloor \frac{n}{2} \rfloor} \\ b_i \neq 0 \, \forall i}} \#(\mathcal{B}_b(u,s)_X \cap W_{\mathscr{A}_n}(\mathbb{Z})), \tag{5.16}$$

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

$$w_{i(n-i)} = \begin{cases} s_i^{-1}, & \text{if } i \in \{1,\dots,\lfloor \frac{n}{2} \rfloor\} \smallsetminus \{\frac{n}{2}\}, \\ s_{\frac{n-2}{2}} {s_{\frac{n}{2}}}^{-1}, & \text{if } i = \frac{n}{2}, \end{cases} \tag{5.17}$$

$$\prod_{i=1}^{n} \prod_{j=\max\{i,n+1-i\}}^{n} w_{ij} = \begin{cases} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} s_i^{-i^2+2i(\lfloor \frac{n}{2} \rfloor+1)}, & \text{if } 2 \nmid n, \\ s_{\frac{n-2}{2}}^{\frac{n^2+2n-16}{8}} s_{\frac{n}{2}}^{\frac{n^2+2n}{8}} \prod_{i=1}^{\frac{n-4}{2}} s_i^{-i^2+i(n+1)}, & \text{if } 2 \mid n. \end{cases} \tag{5.18}$$

To count lattice points in $\mathcal{B}_b(u,s)_X$, we use the following result of Davenport:

**Proposition 186** ([54, Theorem])**.** *Let $\mathcal{R}$ be a bounded, semi-algebraic multiset in $\mathbb{R}^n$ having maximum multiplicity $m$ that is defined by at most $k$ polynomial inequalities, each having degree at most $\ell$. Let $\mathcal{R}'$ denote the image of $\mathcal{R}$ under any (upper or lower) triangular, unipotent transformation of $\mathbb{R}^n$. Then the number of lattice points (counted with multiplicity) contained in the region $\mathcal{R}'$ is given by*

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

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

Using Proposition 186 in conjunction with (5.18), it follows that the summand on the

right-hand side of (5.16) can be expressed as

$$\#(\mathcal{B}_b(u,s)_X \cap W_{\mathscr{A}_n}(\mathbb{Z})) = \mathrm{Vol}(\mathcal{B}_b(u,s)_X) + [\text{error}], \tag{5.19}$$

where the error term is bounded independent of $b$ as follows:

$$[\text{error}] \ll \begin{cases} X^{\lfloor \frac{n}{2}\rfloor^2+2\lfloor \frac{n}{2}\rfloor-1} \prod_{i=1}^{\lfloor \frac{n}{2}\rfloor} s_i^{-i^2+2i(\lfloor \frac{n}{2}\rfloor+1)}, & \text{if } 2\nmid n, \\ X^{\frac{n^2+2n-8}{4}} s_{\frac{n-2}{2}}^{\frac{n^2+2n-16}{8}} s_{\frac{n}{2}}^{\frac{n^2+2n}{8}} \prod_{i=1}^{\frac{n-4}{2}} s_i^{-i^2+i(n+1)}, & \text{if } 2\mid n. \end{cases}$$

Combining (5.15), (5.16), and (5.19) yields the following:

$$\sharp\left(\frac{(W_{\mathscr{A}_n,f_1}(\mathbb{Z})^{r_1,r_2}_{\mathrm{red}})_X}{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})}\right) \sim \tag{5.20}$$
$$\frac{1}{C_H} \sum_{\substack{b\in\mathbb{Z}^{\lfloor \frac{n}{2}\rfloor} \\ b_i\neq 0\,\forall i}} \left( \int_{s\in\mathcal{A}^\star} \int_{u\in\mathcal{N}^\star(s)} \big(\mathrm{Vol}(\mathcal{B}_b(u,s)_X) + [\text{error}]\big) du(\delta(s)ds) \right)$$

We now show that the integral of the error term in (5.20) is negligible:

**Lemma 187.** *The integral of the error term in* (5.20) *is* $o(X^{\frac{n^2+n-2}{2}})$.

*Proof.* Combining (5.10) and (5.19) yields the following bound:

$$[\text{error}]\delta(s) \ll \begin{cases} X^{\lfloor \frac{n}{2}\rfloor^2+2\lfloor \frac{n}{2}\rfloor-1} \prod_{i=1}^{\lfloor \frac{n}{2}\rfloor} s_i^{2i-1}, & \text{if } 2\nmid n, \\ X^{\frac{n^2+2n-8}{4}} s_{\frac{n-2}{2}}^{\frac{n-6}{2}} s_{\frac{n}{2}}^{\frac{n-2}{2}} \prod_{i=1}^{\frac{n-4}{2}} s_i^{2i-1}, & \text{if } 2\mid n. \end{cases} \tag{5.21}$$

We next bound the ranges of $s_1,\dots,s_{\lfloor \frac{n}{2}\rfloor}$. By our construction of the section $\sigma$, we have that $b_{i(n-i)} \ll X$ for each $i$ as $B=[b_{ij}]$ ranges through elements of $\mathcal{B}(0,1)_X$. Thus, for any fixed value of $b=(b_1,\dots,b_{\lfloor \frac{n}{2}\rfloor})$, the largest value of $s_i$ such that $\mathcal{B}_b(u,s)_X \neq \varnothing$ is $O(X|b_i|^{-1})$ for each $i\in\{1,\dots,\lfloor \frac{n}{2}\rfloor\}$ when $n$ is odd and for each $i\in\{1,\dots,\frac{n-2}{2}\}$ when $n$ is even. If $n$ is even and $i=\frac{n}{2}$, then one checks that the largest value of $s_{\frac{n}{2}}$ such that $\mathcal{B}_b(u,s)_X \neq \varnothing$ is $O(X s_{\frac{n-2}{2}} |b_{\frac{n}{2}}|^{-1})$. Using these bounds along with (5.21) and bounding the integral over $u$ by

an absolute constant, we see that the second term on the right-hand side of (5.20) is, when $n$ is odd,

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

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

and is, when $n$ is even,

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

$$\ll X^{\frac{n^2+n-4}{2}} \cdot \sum_{b \in (\mathbb{Z}_{>0})^{\frac{n}{2}}} b_{\frac{n}{2}}^{-\frac{n}{2}} \prod_{i=1}^{\frac{n-2}{2}} b_i^{-2i} \ll X^{\frac{n^2+n-4}{2}} = o\big(X^{\frac{n^2+n-2}{2}}\big). \qquad \square$$

Applying Lemma 187 to (5.20) yields that

$$\sharp\left(\frac{(W_{\mathscr{A}_n, f_1}(\mathbb{Z})^{r_1, r_2}_{\mathrm{red}})_X}{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})}\right) \sim \frac{1}{C_H} \sum_{\substack{b \in \mathbb{Z}^{\lfloor \frac{n}{2} \rfloor} \\ b_i \neq 0 \, \forall i}} \int_{s \in \mathcal{A}^\star} \int_{u \in \mathcal{N}^\star(s)} \mathrm{Vol}(\mathcal{B}_b(u,s)_X) du (\delta(s) ds). \tag{5.22}$$

We now manipulate the integrand in (5.22) to extract its dependence on the slicing indices $b_1, \dots, b_{\lfloor \frac{n}{2} \rfloor}$. Since unipotent transformations preserve volume, we have

$$\mathrm{Vol}(\mathcal{B}_b(u,s)_X) = \mathrm{Vol}(\mathcal{B}_b(0,s)_X). \tag{5.23}$$

Thus, the integrand is independent of $u \in \mathcal{N}^\star(s)$, so the integral over $u$ gives a factor of $\mathrm{Vol}(\mathcal{N}^\star(s))$. By our construction of the box-shaped fundamental domain $\mathcal{F}$ in §5.2, the

following holds for all $s \in \mathcal{A}^\star$ such that $s_i$ is sufficiently large for each $i$:

$$\mathrm{Vol}(\mathcal{N}^\star(s)) = \begin{cases} 1, & \text{if } 2 \nmid n, \\ 2^{-\frac{n-2}{2}}, & \text{if } 2 \mid n. \end{cases} \tag{5.24}$$

Using (5.17) to determine how $s$ scales the slicing indices and (5.18) to determine how $s$ scales the other coordinates of $W_{\mathscr{A}_n,f_1}(\mathbb{R})_0$, we deduce that

$$\mathrm{Vol}(\mathcal{B}_b(0,s)_X)\delta(s) = \tag{5.25}$$
$$\begin{cases} \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} s_i^{2i-1} \,\mathrm{Vol}(\mathcal{B}_{(b_1 s_1,\ldots,b_{\lfloor \frac{n}{2} \rfloor} s_{\lfloor \frac{n}{2} \rfloor})}(0,1)_X), & \text{if } 2 \nmid n, \\ s_{\frac{n-2}{2}}^{\frac{n-6}{2}} s_{\frac{n}{2}}^{\frac{n-2}{2}} \prod_{i=2}^{\frac{n-4}{2}} s_i^{2i-1} \,\mathrm{Vol}(\mathcal{B}_{(b_1 s_1,\ldots,b_{\frac{n-2}{2}} s_{\frac{n-2}{2}}, b_{\frac{n}{2}} s_{\frac{n-2}{2}}^{-1} s_{\frac{n}{2}})}(0,1)_X), & \text{if } 2 \mid n. \end{cases}$$

Let $\mathcal{B}_\beta := \mathcal{B}_\beta(0,1)$ for any $\beta = (\beta_1,\ldots,\beta_{\lfloor \frac{n}{2} \rfloor}) \in (\mathbb{R} \smallsetminus \{0\})^{\lfloor \frac{n}{2} \rfloor}$. We want to reduce to the case where $\beta_i > 0$ for each $i \in \{1,\ldots,\lfloor \frac{n}{2} \rfloor\}$. To do this, let $G$ be as in §5.2.2, and observe that for every $\beta \in (\mathbb{R} \smallsetminus \{0\})^{\lfloor \frac{n}{2} \rfloor}$, there exists $g \in G$ such that $\mathcal{B}_\beta = g \cdot \mathcal{B}_{(|\beta_1|,\ldots,|\beta_{\lfloor \frac{n}{2} \rfloor}|)}$. Thus, we have that

$$\mathrm{Vol}\left((\mathcal{B}_\beta)_X\right) = \mathrm{Vol}\left((\mathcal{B}_{(|\beta_1|,\ldots,|\beta_{\lfloor \frac{n}{2} \rfloor}|)})_X\right) \tag{5.26}$$

for any $\beta \in (\mathbb{R}_{>0})^{\lfloor \frac{n}{2} \rfloor}$ and $X > 0$. Setting $\beta_i = |b_i s_i|$ for each $i \in \{1,\ldots,\lfloor \frac{n}{2} \rfloor\}$ when $2 \nmid n$ and for each $i \in \{1,\ldots,\frac{n-2}{2}\}$ when $2 \mid n$, setting $\beta_{\frac{n}{2}} = |b_{\frac{n}{2}} s_{\frac{n-2}{2}}^{-1} s_{\frac{n}{2}}|$, and substituting this along with (5.23), (5.24), (5.25), and (5.26) into (5.22) yields

$$\sharp\left(\frac{(W_{\mathscr{A}_n,f_1}(\mathbb{Z})_{\mathrm{red}}^{r_1,r_2})_X}{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})}\right) \sim \frac{1}{C_H} \cdot 2^{\lfloor \frac{n}{2} \rfloor} \cdot \sum_{b \in (\mathbb{Z}_{>0})^{\lfloor \frac{n}{2} \rfloor}} \left( \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor - 1} b_i^{-2i} \right) \cdot \tag{5.27}$$
$$\begin{cases} b_{\lfloor \frac{n}{2} \rfloor}{}^{1-n} \displaystyle\int_{\substack{\beta_i \geq c_2 b_i \\ i \in \{1,\ldots,\lfloor \frac{n}{2} \rfloor\}}} \left( \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \beta_i^{2i-1} \right) \cdot \mathrm{Vol}((\mathcal{B}_\beta)_X) \cdot \mathrm{Vol}(\mathcal{N}^\star(s_{\beta,b}))d\beta, & \text{if } 2 \nmid n, \\ b_{\frac{n}{2}}{}^{-\frac{n}{2}} \displaystyle\int_{\substack{\beta_i \geq c_2 b_i \\ i \in \{1,\ldots,\frac{n-2}{2}\}}} \\ \qquad \displaystyle\int_{\beta_{\frac{n}{2}} \geq c_2 \frac{b_{\frac{n}{2}}}{b_{\frac{n-2}{2}}}} \left( \beta_{\frac{n}{2}}^{\frac{n-2}{2}} \prod_{i=1}^{\frac{n-2}{2}} \beta_i^{2i-1} \right) \cdot \mathrm{Vol}((\mathcal{B}_\beta)_X) \cdot \mathrm{Vol}(\mathcal{N}^\star(s_{\beta,b}))d\beta, & \text{if } 2 \mid n, \end{cases}$$

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

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

The following lemma not only allows us to extend the region of integration to $\beta_i > 0$ for each $i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}$, but also permits us to eliminate the factors of $\mathrm{Vol}(\mathcal{N}^\star(s_{\beta,b}))$ in (5.27):

**Lemma 188.** *The expression on the right-hand side of* (5.27) *is, up to a negligible error, unchanged if we replace the regions of integration with the regions $\beta_i > 0$ for each $i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}$ and if we replace the factors of* $\mathrm{Vol}(\mathcal{N}^\star(s_{\beta,b}))$ *with the values on the right-hand side of* (5.24)*.*

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

Take $\beta_1 \in [0, \Gamma b_1]$. By construction, we have $\mathrm{Vol}(\mathcal{B}_\beta(X)) \ll X^{\lfloor \frac{n}{2} \rfloor^2 + 2\lfloor \frac{n}{2} \rfloor}$ if $n$ is odd and $\mathrm{Vol}(\mathcal{B}_\beta(X)) \ll X^{\frac{n^2+2n-4}{4}}$ if $n$ is even, where the implied constant is independent of $\beta \in (\mathbb{R}_{>0})^{\lfloor \frac{n}{2} \rfloor}$. Further notice that for each $i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}$, the largest possible value of $\beta_i$ such that $\mathcal{B}_\beta(X) \neq \varnothing$ is $O(X)$; this also implies that we may truncate the summation over $b$ on the right-hand side of (5.27) to the set where $b_i \ll X$ for each $i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}$. Substituting these estimates into (5.27) and replacing the region of integration for $\beta_1$ with $\beta_1 \in [0,\ b_1]$ yields

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

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

when $n$ is odd, and

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

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

Combining Lemma 188 with (5.27), we obtain the following bound, in which each $\beta_i$ is integrated from 0 up to $\infty$:

$$\sharp\left(\frac{(W_{\mathscr{A}_n,f_1}(\mathbb{Z})^{r_1,r_2}_{\mathrm{red}})_X}{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})}\right)\sim\frac{1}{C_H}\cdot\sum_{b\in(\mathbb{Z}>0)^{\lfloor\frac{n}{2}\rfloor}}\Big(\prod_{i=1}^{\lfloor\frac{n}{2}\rfloor-1}b_i^{-2i}\Big)\cdot \tag{5.28}$$
$$\left\{\begin{array}{ll} 2^{\lfloor\frac{n}{2}\rfloor}b_{\lfloor\frac{n}{2}\rfloor}{}^{1-n}\displaystyle\int_{\substack{\beta_i\geq 0\\ i\in\{1,\dots,\lfloor\frac{n}{2}\rfloor\}}}\Big(\prod_{i=1}^{\lfloor\frac{n}{2}\rfloor}\beta_i^{2i-1}\Big)\cdot\mathrm{Vol}((\mathcal{B}_\beta)_X)d\beta, & \text{if } 2\nmid n,\\ 2b_{\frac{n}{2}}{}^{-\frac{n}{2}}\displaystyle\int_{\substack{\beta_i\geq 0\\ i\in\{1,\dots,\frac{n}{2}\}}}\Big(\beta_{\frac{n}{2}}{}^{\frac{n-2}{2}}\prod_{i=1}^{\frac{n-2}{2}}\beta_i^{2i-1}\Big)\cdot\mathrm{Vol}((\mathcal{B}_\beta)_X)d\beta, & \text{if } 2\mid n.\end{array}\right\}$$

Theorem 185 now follows from (5.28) by performing a change-of-variables and evaluating the sum over the slicing indices $b_i$.

## 5.4 A Jacobian change-of-variables formula

The objective of this section is to prove the following result, which gives an asymptotic formula for the quantity $\sharp((N\times\mathcal{G}_{\mathscr{A}_n})(\mathbb{Z})\backslash(W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2}_{\mathrm{red}})_X)$:

**Theorem 189** (Variant of Theorem 169)**.** *We have that*

$$\sharp\left(\frac{(W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2}_{\mathrm{red}})_X}{(N\times\mathcal{G}_{\mathscr{A}_n})(\mathbb{Z})}\right)\sim\begin{cases}\left(\prod_{i=1}^{\lfloor\frac{n}{2}\rfloor}\zeta(2i)\right)\cdot N_n^{r_1,r_2}(X), & \text{if } 2\nmid n,\\ \left(2^{-\frac{n}{2}}\zeta(\frac{n}{2})\prod_{i=1}^{\frac{n-2}{2}}\zeta(2i)\right)\cdot N_n^{r_1,r_2}(X), & \text{if } 2\mid n.\end{cases}$$

Let $N^{r_1,r_2}_{n,f_1}(X) := \mathrm{Vol}\left(V_{n,1,f_1}(\mathbb{R})^{r_1,r_2}_X\right)$, and observe that $N^{r_1,r_2}_{n,f_1}(X)$ is independent of $f_1$. Upon fibering over $f_1$, we see that proving Theorem 189 amounts to proving the following for each fixed $f_1$:

$$\sharp\left(\frac{(W_{\mathscr{A}_n,f_1}(\mathbb{Z})^{r_1,r_2}_{\mathrm{red}})_X}{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})}\right)\sim\begin{cases}\left(\prod_{i=1}^{\lfloor\frac{n}{2}\rfloor}\zeta(2i)\right)\cdot N^{r_1,r_2}_{n,f_1}(X), & \text{if } 2\nmid n,\\ \left(2^{1-\frac{n}{2}}\zeta(\frac{n}{2})\prod_{i=1}^{\frac{n-2}{2}}\zeta(2i)\right)\cdot N^{r_1,r_2}_{n,f_1}(X), & \text{if } 2\mid n.\end{cases}\tag{5.29}$$

By Theorem 185, proving the asymptotic (5.29) amounts to computing $C_X$. The remainder of this section is devoted to the computation of $C_X$, which we achieve by means of a Jacobian change-of-variables argument.

### 5.4.1 Setting up the change-of-variables

Let $\mathcal{K}\subset\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ denote a maximal compact subgroup containing $K$. Notice that $C_X$ must be independent of the choice of the region $H$ and of the fundamental set $L^{r_1,r_2}_{f_1}$ for the action of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ on $W_{\mathscr{A}_n,f_1}(\mathbb{R})^{r_1,r_2}$, so long as $H$ is a left-$K$-invariant subset of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ that is the closure of a nonempty open set. Thus, we may assume for the sake of convenience that $H$ is also inversion-invariant, and thus right-$\mathcal{K}$-invariant too (note that this can be arranged while still ensuring that $H$ is the closure of a nonempty open set). By this assumption and by the uniqueness of the Iwasawa decomposition, there exists a compact subset $H'\subset\mathcal{A}\cdot\mathcal{N}$ such that $H = H'\cdot\mathcal{K}\subset(\mathcal{A}\cdot\mathcal{N})\cdot\mathcal{K} = \mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$.

Because the action of $\mathcal{A}\cdot\mathcal{N}$ preserves $\{B\in W_{\mathscr{A}_n,f_1}(\mathbb{R})_0 : b_{i(n-i)}(B) > 0 \text{ for each } i\in$

$\{1, \dots, \lfloor \frac{n}{2} \rfloor\}\}$, the region of integration in the numerator of $C_X$ can be expressed as follows:

$$\begin{aligned} \mathcal{B}_X &= \left\{ B \in \left( ((H' \cdot \mathcal{K}) \cdot L_{f_1}^{r_1,r_2})_0 \right)_X : b_{i(n-i)}(B) > 0 \ \forall i \in \{1, \dots, \lfloor \tfrac{n}{2} \rfloor\} \right\} \\ &= H' \cdot \left\{ B \in \left( (\mathcal{K} \cdot L_{f_1}^{r_1,r_2})_0 \right)_X : b_{i(n-i)}(B) > 0 \ \forall i \in \{1, \dots, \lfloor \tfrac{n}{2} \rfloor\} \right\}. \end{aligned} \tag{5.30}$$

We then have the following lemma, which reexpresses the set $(\mathcal{K} \cdot L_{f_1}^{r_1,r_2})_0$:

**Lemma 190.** *For each index $j \in \{1, \dots, n_{r_1,r_2}\}$, there exist continuous functions $\theta_j \colon L_{f_1}^{r_1,r_2} \to \mathcal{K}$ such that $\theta_1$ is the constant function with value $\mathrm{id} \in \mathcal{K}$ and such that for each $B \in L_{f_1}^{r_1,r_2}$, we have the following equality of sets:*

$$\{\theta_j : j \in \{1, \dots, n_{r_1,r_2}\}\} = \left\{ \theta \in \mathcal{K} : \begin{array}{c} \theta \cdot B \in W_{\mathscr{A}_n, f_1}(\mathbb{R})_0, \\ b_{i(n-i)}(\theta \cdot B) > 0 \ \forall i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\} \end{array} \right\} \tag{5.31}$$

*and for each $B \in L_{f_1}^{r_1,r_2}$, the elements $\theta_j(B)$ for $j \in \{1, \dots, n_{r_1,r_2}\}$ are distinct.*

*Proof.* Let $g_j \colon L_{f_1}^{r_1,r_2} \to \mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ be functions such that $g_1$ is the constant function with value $\mathrm{id} \in \mathcal{G}_{\mathscr{A}_n}(\mathbb{R})$ and such that for each $B \in L_{f_1}^{r_1,r_2}$, we have the following equality of sets:

$$\{g_j : j \in \{1, \dots, n_{r_1,r_2}\}\} = \mathrm{Stab}_{\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})}(B).$$

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

Let $\pi \colon \mathcal{G}_{\mathscr{A}_n}(\mathbb{R}) \to \mathcal{K}$ be the map obtained by postcomposing the diffeomorphism $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R}) \to \mathcal{A} \times \mathcal{N} \times \mathcal{K}$ given by the Iwasawa decomposition with the projection map $\mathcal{A} \times \mathcal{N} \times \mathcal{K} \to \mathcal{K}$, and for each $j \in \{1, \dots, n_{r_1,r_2}\}$, let $\theta_j \colon L_{f_1}^{r_1,r_2} \to \mathcal{K}$ be defined by $\theta_j = \pi \circ g_j$. Then, observe that $\theta_1$ is the constant function with value $\mathrm{id} \in \mathcal{K}$ and that $\theta_j \cdot B \in W_{\mathscr{A}_n, f_1}(\mathbb{R})_0$ for each $j \in \{1, \dots, n_{r_1,r_2}\}$ and $B \in L_{f_1}^{r_1,r_2}$. We have thus proven that the left-hand side of (5.31) is contained in the right-hand side.

Suppose that $\theta \in \mathcal{K}$ and $B \in L_{f_1}^{r_1,r_2}$ is such that $\theta \cdot B \in W_{\mathscr{A}_n,f_1}(\mathbb{R})_0$ and $b_{i(n-i)}(\theta \cdot b) > 0$ for each $i \in \{1, \ldots, \lfloor \frac{n}{2} \rfloor\}$. By the proof of Lemma 183, the group $\mathcal{A} \cdot \mathcal{N}$ acts simply transitively on the set of elements $B' \in W_{\mathscr{A}_n,f_1}(\mathbb{R})_0$ such that $b_{i(n-i)}(B') > 0$ for each $i \in \{1, \ldots, \lfloor \frac{n}{2} \rfloor\}$ and such that $\iota(\mathscr{A}_n, B') = \iota(\mathscr{A}_n, B)$. Thus, there exists $h \in \mathcal{A} \cdot \mathcal{N}$ such that $h \cdot B = \theta \cdot B$, so $h^{-1}\theta \in \mathrm{Stab}_{\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})}(B)$, implying that $h^{-1}\theta = g_j(B)$ for some $j \in \{1, \ldots, n_{r_1,r_2}\}$. But then $\theta = \pi(h^{-1}\theta) = \pi(g_j(B)) = \theta_j(B)$. We have thus proven that the right-hand side of (5.31) is contained in the left-hand side.

Finally, if the elements $\theta_j(B)$ for $j \in \{1, \ldots, n_{r_1,r_2}\}$ were not distinct for some $B \in L_{f_1}^{r_1,r_2}$, then it would follow that $\mathrm{Stab}_{\mathcal{A}\cdot\mathcal{N}}(B)$ contains a nontrivial element, which is impossible. $\square$

It follows from combining (5.30) and Lemma 190 that

$$\mathcal{B} = \bigsqcup_{j=1}^{n_{r_1,r_2}} H' \cdot \mathcal{B}_j, \quad \text{where} \quad \mathcal{B}_j := \left\{\theta_j(B) \cdot B : B \in L_{f_1}^{r_1,r_2}\right\}, \tag{5.32}$$

so the numerator of $C_X$ is given by

$$\sum_{j=1}^{n_{r_1,r_2}} \int_{B \in H' \cdot (\mathcal{B}_j)_X} \lambda(B) dB. \tag{5.33}$$

### 5.4.2 Calculating the Jacobian

To compute (5.33), we first show that all of the terms in the sum (5.33) are in fact equal to each other. This follows immediately from the Jacobian change-of-variables formula established in the next proposition, by taking $\widetilde{\sigma}$ to be defined by $\widetilde{\sigma}(B) = \theta_j(\sigma(B)) \cdot \sigma(B)$ for each $j \in \{1, \ldots, n_{r_1,r_2}\}$, where $\sigma$ is as defined in §5.2.3.

**Proposition 191.** *Let $\widetilde{\sigma} \colon \mathbb{R}^{n-1} \to W_{\mathscr{A}_n,f_1}(\mathbb{R})_0^{r_1,r_2}$ be a continuous function such that for each $(n-1)$-tuple $f = (f_2, \ldots, f_n) \in \mathbb{R}^{n-1}$, we have $\iota(\mathscr{A}_n, \widetilde{\sigma}(f))(x, y) = x^n + \sum_{i=1}^n f_i x^{n-i} y^i$. Let $\mathcal{R} \subset \mathbb{R}^{n-1}$ be any bounded open set contained in the complement of the locus of forms of discriminant 0. Then there is a nonzero rational constant $\mathcal{J} \in \mathbb{Q}^\times$, depending only on the*

*degree $n$, such that*

$$\int_{B\in H'\cdot\widetilde{\sigma}(\mathcal{R})}\lambda(B)dB = |\mathcal{J}|\int_{f\in\mathcal{R}}\int_{h\in H'}dhdf,$$

*where $dh$ denotes a right Haar measure on $\mathcal{A}\cdot\mathcal{N}$ and is given by*

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

*Remark* 192. The point of Proposition 191 is that the Jacobian relating the measure $\lambda(B)dB$ on $W_{\mathscr{A}_n,f_1}$ to the product of the Euclidean measure $df$ on $V_{n,1,f_1}$ with the Haar measure $dh$ on $\mathcal{A}\cdot\mathcal{N}$ is a nonzero rational constant. A similar result is proved in [26, Proposition 3.10], albeit for the action of a semisimple group $G$ on a coregular space $V$. Crucial to the proof of [26, Proposition 3.10] is the fact that the Haar measure in question is unimodular—i.e., both left- and right-invariant. In our situation, the group $\mathcal{A}\cdot\mathcal{N}$ is *not* semisimple, and the measure $dh$ is *not* unimodular. Nonetheless, as we explain in the proof of the proposition, the factor of $\lambda(B)$ compensates exactly for the failure of the measure $dh$ to be left-invariant.

*Proof of Proposition 191.* We begin by assuming that $\widetilde{\sigma}$ is piecewise analytic, in which case we have that

$$\int_{B\in H'\cdot\widetilde{\sigma}(\mathcal{R})}\lambda(B)dB = \int_{f\in\mathcal{R}}\int_{h\in H'}\mathcal{J}_{\widetilde{\sigma}}(h,f)dhdf,$$

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

We begin by proving that $\mathcal{J}_{\widetilde{\sigma}}(h,f)$ is independent of $h$. To do this, fix $\gamma\in\mathcal{A}\cdot\mathcal{N}$, and consider the transformation on $W_{\mathscr{A}_n,f_1}(\mathbb{R})_0$ sending $B\mapsto\gamma\cdot B$. Then there is a character $\chi_\lambda\colon\mathcal{A}\cdot\mathcal{N}\to\mathbb{R}_{>0}$ such that $\lambda(\gamma\cdot B)d(\gamma\cdot B)=\chi_\lambda(\gamma)\lambda(B)dB$; note that $\chi_\lambda$ exists because $\lambda(B)$ is a product of coefficients that are unchanged by the action of $\mathcal{N}$. The corresponding

measure on $(\mathcal{A}\cdot\mathcal{N})\times\mathcal{R}$ is given by

$$\chi_\lambda(\gamma)\mathcal{J}_{\widetilde{\sigma}}(h,f)dhdf. \tag{5.34}$$

On the other hand, the transformation $B\mapsto\gamma\cdot B$ acts on $(\mathcal{A}\cdot\mathcal{N})\times\mathcal{R}$ by sending $(h,f)\mapsto(\gamma h,f)$. Letting $\rho\colon\mathcal{N}\cdot\mathcal{A}\to\mathbb{R}_{>0}$ denote the character transforming the right Haar measure to the left, we see that

$$\mathcal{J}_{\widetilde{\sigma}}(\gamma\cdot h,f)d(\gamma\cdot h)df=\rho(\gamma)\mathcal{J}_{\widetilde{\sigma}}(\gamma\cdot h,f)dhdf \tag{5.35}$$

Now, a computation reveals that if $\gamma=\overline{s}\cdot\overline{u}$ for $\overline{s}=(\overline{s}_1,\dots,\overline{s}_{\lfloor\frac{n}{2}\rfloor})\in\mathcal{A}$ and $\overline{u}\in\mathcal{N}$, we have

$$\chi_\lambda(\gamma)=\rho(\gamma)=\begin{cases}\prod_{i=1}^{\lfloor\frac{n}{2}\rfloor}\overline{s}_i^{-i^2+2i\lfloor\frac{n}{2}\rfloor}, & \text{if } 2\nmid n,\\ \left(\overline{s}_{\frac{n-2}{2}}\overline{s}_{\frac{n}{2}}\right)^{\frac{n^2-2n}{8}}\prod_{i=1}^{\frac{n-4}{2}}\overline{s}_i^{-i^2+i(n-1)}, & \text{if } 2\mid n.\end{cases}$$

Consequently, by comparing (5.34) and (5.35), we deduce that $\mathcal{J}_{\widetilde{\sigma}}(\gamma\cdot h,f)=\mathcal{J}_{\widetilde{\sigma}}(h,f)$, and setting $h=1$ yields the claimed independence.

That $\mathcal{J}_{\widetilde{\sigma}}(h,f)$ is independent of $\widetilde{\sigma}$ follows from an argument identical to Step 2 in the proof of [26, Proposition 3.10] (this step relies crucially on the fact that the measure $dh$ is right-invariant). Finally, that $\mathcal{J}_{\widetilde{\sigma}}(h,f)$ is independent of $f$ and given by a nonzero rational constant follow from an argument identical to Steps 3 and 4 in the proof of [26, Proposition 3.10]. $\square$

We now take $\mathcal{R}=V_{n,1,f_1}(\mathbb{R})_X^{r_1,r_2}$ (where we identify $V_{n,1,f_1}(\mathbb{R})^{r_1,r_2}$ with a subset of $\mathbb{R}^{n-1}$). Combining (5.33) and Proposition 191 yields that the numerator of $C_X$ is

$$n_{r_1,r_2}\cdot N_{n,f_1}^{r_1,r_2}(X)\cdot|\mathcal{J}|\int_{h\in H'}dh=n_{r_1,r_2}\cdot N_{n,f_1}^{r_1,r_2}(X)\cdot\frac{\mathrm{Vol}(\mathcal{K}H')}{\mathrm{Vol}(\mathcal{K})}, \tag{5.36}$$

where $\mathrm{Vol}(\mathcal{K}H')$ is computed with respect to the Haar measure on $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})=\mathcal{K}\cdot\mathcal{A}\cdot\mathcal{N}$ obtained by inverting the Haar measure (5.10) on $\mathcal{G}_{\mathscr{A}_n}(\mathbb{R})=\mathcal{N}\cdot\mathcal{A}\cdot\mathcal{K}$. On the other hand,

note that the denominator of $C_X$ is given by

$$\int_{h\in H} dh = \mathrm{Vol}(H) = \mathrm{Vol}(H'\mathcal{K}), \tag{5.37}$$

where $\mathrm{Vol}(H'\mathcal{K})$ is computed with respect to the Haar measure (5.10). Then, the following lemma allows us to simplify $C_X$:

**Lemma 193.** *We have $\mathcal{K}H' = H'\mathcal{K}$, and in particular* $\mathrm{Vol}(\mathcal{K}H') = \mathrm{Vol}(H'\mathcal{K})$.

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

$$\mathcal{K}H' \subset \mathcal{K}H'\mathcal{K} = H'\mathcal{K} = H = H^{-1} = \mathcal{K}(H')^{-1}. \tag{5.38}$$

Since the Iwasawa decomposition is unique, (5.38) implies that $H' \subset (H')^{-1}$, and hence also that $H' = (H')^{-1}$. Thus, $H'\mathcal{K} = \mathcal{K}(H')^{-1} = \mathcal{K}H'$, as desired. □

Finally, combining Lemma 193 together with (5.36) and (5.37) yields that

$$C_X = \begin{cases} n_{r_1,r_2} \cdot N_{n,f_1}^{r_1,r_2}(X) \cdot |\mathcal{J}|, & \text{if } 2 \nmid n, \\ \frac{1}{4} n_{r_1,r_2} \cdot N_{n,f_1}^{r_1,r_2}(X) \cdot |\mathcal{J}|, & \text{if } 2 \mid n. \end{cases} \tag{5.39}$$

where the extra factor of $\frac{1}{4}$ when $n$ is even arises since we normalized the measure $d\theta$ so that $\int_{\theta\in(K\cap\{\pm \mathrm{id}\})\backslash K} d\theta = 1$. Upon substituting (5.39) into Theorem 185, we obtain (5.29), up to the calculation of $\mathcal{J}$ (which we do in Proposition 196, to follow).

*Remark* 194. We counted reducible elements in $W_{\mathscr{A}_n,f_1}(\mathbb{Z})^{r_1,r_2} \subset W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2}$ for fixed $f_1$ to account for the action of the group $N(\mathbb{Z})$ on monic binary forms. The methods of this section can be easily adapted to count reducible elements in $W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2}$, where $f_1$ is allowed to vary. The only significant difference is that the analogue of Proposition 191 produces a Jacobian constant $\mathcal{J}'$ that is *sometimes* different from $\mathcal{J}$. Indeed, a simple calculation reveals that $|\mathcal{J}'| = |\mathcal{J}|$ when $n$ is odd but that $|\mathcal{J}'| = \frac{1}{2}|\mathcal{J}|$ when $n$ is even.

### 5.4.3 Computing the value of $\mathcal{J}$

In this section, we first use a "principle of permanence of identities" argument (cf. [3, §14.3]) to deduce an analogue of Proposition 191 over $\mathbb{Z}_p$ for primes $p$. We then compute certain local integrals over $\mathbb{Z}_p$ via a point-counting argument over $\mathbb{F}_p$ (and, when $p = 2$, $\mathbb{Z}/2^m\mathbb{Z}$ for sufficiently large $m$). Comparing the values of the local integrals obtained by using these two methods yields the value of $|\mathcal{J}|_p$. Since this method applies to all primes $p$, we obtain the value of $|\mathcal{J}|$.

**Proposition 195.** *Let $\lambda$ be as defined in* (5.9)*, with the archimedean absolute value replaced by the p-adic absolute value. Let $\phi_p \colon W_{\mathscr{A}_n}(\mathbb{Z}_p)_0 \to \mathbb{R}$ be a $\mathcal{P}(\mathbb{Z}_p)$-invariant measurable function. Then we have that*

$$\int_{B \in W_{\mathscr{A}_n}(\mathbb{Z}_p)_0} \phi_p(B)\lambda(B)dB = \tag{5.40}$$
$$\epsilon_n \cdot |\mathcal{J}'|_p \cdot \mathrm{Vol}(\mathcal{P}(\mathbb{Z}_p)) \int_{\substack{f \in \mathbb{Z}_p^n \\ \Delta(F_f) \neq 0}} \Bigg( \sum_{\substack{B \in \mathcal{P}(\mathbb{Z}_p) \setminus W_{\mathscr{A}_n}(\mathbb{Z}_p)_0 \\ \iota(\mathscr{A}_n, B) = F_f}} \phi_p(B) \Bigg) df,$$

*where $\epsilon_n = 1$ if $n$ is odd and $\epsilon_n = \frac{1}{2}$ if $n$ is even, and where for $f \in \mathbb{Z}_p^n$, we write $F_f$ to denote $F_f(x, y) = x^n + \sum_{i=1}^n f_i x^{n-i} y^i$.*

*Proof.* We prove the proposition in the case where $n = 3$; the proof for $n > 3$ is essentially identical. Let $\mathcal{R} \subset \mathbb{Z}_p^3 \smallsetminus \{f : \Delta(F_f) = 0\}$ be an open subset, let $\widetilde{\sigma} \colon \mathcal{R} \to W_3(\mathbb{Z}_p)_0$ be a continuous function such that for each triple $f \in \mathbb{Z}_p^3$ we have $\iota(\mathscr{A}_n, \widetilde{\sigma}(f)) = F_f$, and let $\phi_p \colon W_3(\mathbb{Z}_p)_0 \to \mathbb{R}$ be a measurable function. Upon applying the principle of permanence of identities to the proof of Proposition 191, we obtain the following result:

$$\int_{B \in \mathcal{P}(\mathbb{Z}_p) \cdot \widetilde{\sigma}(\mathcal{R})} \phi_p(B)|b_{12}(B)|_p dB = |\mathcal{J}'|_p \int_{f \in \mathcal{R}} \int_{h \in \mathcal{P}(\mathbb{Z}_p)} \phi_p(h \cdot \widetilde{\sigma}(f)) dh df, \tag{5.41}$$

where $dh$ denotes the measure $ds_1 du$ on $\mathcal{P}(\mathbb{Z}_p) = \mathcal{A}(\mathbb{Z}_p) \cdot \mathcal{N}(\mathbb{Z}_p)$. Just as [26, Proposition 3.12]

is deduced from [26, Proposition 3.11], it follows from (5.41) that

$$\int_{B\in W_3(\mathbb{Z}_p)_0} \phi_p(B)|b_{12}(B)|_p dB = \tag{5.42}$$
$$|\mathcal{J}'|_p \int_{\substack{f\in\mathbb{Z}_p^3\\ \Delta(F_f)\neq 0}} \Bigg( \sum_{\substack{B\in\mathcal{P}(\mathbb{Z}_p)\backslash W_3(\mathbb{Z}_p)_0\\ \iota(\mathscr{A}_n,B)=F_f}} \int_{h\in\mathcal{P}(\mathbb{Z}_p)} \frac{\phi_p(h\cdot B)}{\#\operatorname{Stab}_{\mathcal{P}(\mathbb{Z}_p)}(f)} dh \Bigg) df$$

When $\phi_p$ is $\mathcal{P}(\mathbb{Z}_p)$-invariant, we have $\phi_p(h\cdot B) = \phi_p(B)$ for any $h \in \mathcal{P}(\mathbb{Z}_p)$ and $B \in W_3(\mathbb{Z}_p)_0$. The proposition then follows from (5.42) upon observing that $\operatorname{Stab}_{\mathcal{P}(\mathbb{Z}_p)}(B) = \{1\}$ for any $B \in W_3(\mathbb{Z}_p)_0$ with $\Delta(\iota(\mathscr{A}_n, B)) \neq 0$ and that

$$\operatorname{Vol}(\mathcal{P}(\mathbb{Z}_p)) = \operatorname{Vol}(\mathcal{N}(\mathbb{Z}_p)) \cdot \operatorname{Vol}(\mathcal{A}(\mathbb{Z}_p)) = 1 \cdot (1 - p^{-1}).$$

Note that we must use $\mathcal{J}'$ instead of $\mathcal{J}$, because the integral on the left-hand side of (5.40) is over all elements of $W_{\mathscr{A}_n}(\mathbb{Z}_p)_0$, not just those with fixed $f_1$. The extra factor of $\frac{1}{2}$ when $n$ is even arises because in this case, $\operatorname{Stab}_{\mathcal{P}(\mathbb{Z}_p)}(B) = \{\pm \operatorname{id}\}$ for any $B \in W_{\mathscr{A}_n}(\mathbb{Z}_p)_0$ such that $\Delta(\iota(\mathscr{A}_n, B)) \neq 0$, whereas such $B$ have trivial stabilizer when $n$ is odd. For future reference, we record that

$$\operatorname{Vol}(\mathcal{P}(\mathbb{Z}_p)) = \begin{cases} (1-p^{-1})^{\lfloor \frac{n}{2} \rfloor}, & \text{if } p > 2, \\ 2^{-2\lfloor \frac{n}{2} \rfloor}, & \text{if } p = 2 \text{ and } 2 \nmid n, \\ 2^{-\frac{n}{2}}, & \text{if } p = 2 \text{ and } 2 \mid n. \end{cases} \tag{5.43}$$

□

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

**Proposition 196.** *We have that $|\mathcal{J}| = |\mathcal{J}'| = 2^{-\lfloor \frac{n}{2} \rfloor}$ if $n$ is odd and that $\frac{1}{2}|\mathcal{J}| = |\mathcal{J}'| = 2^{-\frac{n}{2}}$ if $n$ is even.*

*Proof.* To compute $|\mathcal{J}|$, it suffices to compute $|\mathcal{J}|_p$ for each $p$ since $\mathcal{J} \in \mathbb{Q}^\times$ by Proposition 191. It further suffices to compute $|\mathcal{J}'|_p$, since $\mathcal{J}, \mathcal{J}'$ differ by at most a factor of 2. We now split into cases depending on the parity of $p$:

*Case 1: $p > 2$*: Fix a separable form $f^* \in V_{n,1}(\mathbb{F}_p)$, and let $\phi_p \colon W_{\mathscr{A}_n}(\mathbb{Z}_p)_0 \to \mathbb{R}$ be the

indicator function of the set

$$\Sigma_{f^*} := \left\{ B \in W_{\mathscr{A}_n}(\mathbb{Z}_p)_0 : \begin{array}{c} |b_{i(n-i)}(B)|_p = 1 \ \forall i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}, \\ \iota(\mathscr{A}_n, B) \equiv f^* \pmod{p} \end{array} \right\}$$

From the proof of Lemma 183, we see that $\mathcal{P}(\mathbb{Z}_p)$ acts transitively on the set

$$\left\{ B \in W_{\mathscr{A}_n}(\mathbb{Z}_p)_0 : \begin{array}{c} |b_{i(n-i)}(B)|_p = 1 \ \forall i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}, \\ \iota(\mathscr{A}_n, B) = f' \end{array} \right\} \tag{5.44}$$

for any $f' \in V_{n,1}(\mathbb{Z}_p)$; by Lemma 184, this action has trivial stabilizer when $n$ is odd and stabilizer $\{\pm \mathrm{id}\}$ when $n$ is even. Hence, the right-hand side of (5.40) is given by

$$|\mathcal{J}'|_p \cdot \mathrm{Vol}(\mathcal{P}_n(\mathbb{Z}_p)) \int_{\substack{f \in \mathbb{Z}_p^n \\ F_f \equiv f^* \pmod{p}}} \left\{ \begin{array}{ll} 1, & \text{if } 2 \nmid n, \\ 2^{-1}, & \text{if } 2 \mid n \end{array} \right\} df = \tag{5.45}$$

$$|\mathcal{J}'|_p \cdot \mathrm{Vol}(\mathcal{P}_n(\mathbb{Z}_p)) \cdot p^{-n} \cdot \left\{ \begin{array}{ll} 1, & \text{if } 2 \nmid n, \\ 2^{-1}, & \text{if } 2 \mid n. \end{array} \right.$$

On the other hand, the proof of Lemma 183 also implies that the group $\mathcal{P}_n(\mathbb{F}_p)$ acts transitively on the mod-$p$ reduction $\overline{\Sigma}_{f^*}$ of $\Sigma_{f^*}$; by Lemma 184, this action has trivial stabilizer when $n$ is odd and stabilizer $\{\pm \mathrm{id}\}$ when $n$ is even. Thus, we have that

$$\#\overline{\Sigma}_{f^*} = \#\mathcal{P}_n(\mathbb{F}_p) \cdot \left\{ \begin{array}{ll} 1, & \text{if } 2 \nmid n, \\ 2^{-1}, & \text{if } 2 \mid n \end{array} \right\} = \mathrm{Vol}(\mathcal{P}_n(\mathbb{Z}_p)) \cdot \left\{ \begin{array}{ll} p^{\frac{n^2-1}{4}}, & \text{if } 2 \nmid n, \\ 2^{-1} \cdot p^{\frac{n^2}{4}}, & \text{if } 2 \mid n. \end{array} \right. \tag{5.46}$$

Using (5.62) and (5.46), we find that the left-hand side of (5.40) is given by

$$\int_{B\in\Sigma_{f^*}} dB = \frac{\#\overline{\Sigma}_{f^*}}{\#W_{\mathscr{A}_n}(\mathbb{F}_p)_0} = \mathrm{Vol}(\mathcal{P}_n(\mathbb{Z}_p))\cdot p^{-n}\cdot \begin{cases} 1, & \text{if } 2\nmid n, \\ 2^{-1}, & \text{if } 2\mid n. \end{cases} \tag{5.47}$$

Now, Proposition 195 tells us (5.45) and (5.47) must be equal, so $|\mathcal{J}'|_p = 1$.

*Case 2:* $p = 2$: The proof here is similar to Case 1, so we highlight the differences. Let $m \gg 1$ be an integer, fix $f^*(x,y) = x^n + \sum_{i=1}^n f_i x^{n-i}y^i \in V_{n,1}(\mathbb{Z}/2^m\mathbb{Z})$ of nonzero discriminant such that $f_i = 0$ for each odd $i \in \{1,\dots,n-1\}$, and let $\phi_2 \colon W_{\mathscr{A}_n}(\mathbb{Z}_2)_0 \to \mathbb{R}$ be the indicator function of the set

$$\Sigma_{f^*} := \left\{ B \in W_{\mathscr{A}_n}(\mathbb{Z}_2)_0 : \begin{array}{c} |b_{i(n-i)}(B)|_2 = 1 \ \forall i \in \{1,\dots,\lfloor \frac{n}{2}\rfloor\}, \\ \iota(\mathscr{A}_n, B) \equiv f^* \pmod{2^m} \end{array} \right\}$$

From the proof of Lemma 183, we see that $\mathcal{P}(\mathbb{Z}_2)$ acts transitively on the set in (5.44) for any $f' \in V_{n,1}(\mathbb{Z}_2)$ whose $x^i y^{n-i}$-coefficient is even for each odd $i \in \{1,\dots,n-1\}$; by Lemma 184, this action has trivial stabilizer when $n$ is odd and stabilizer $\{\pm \mathrm{id}\}$ when $n$ is even. Thus, by analogy with (5.45), the right-hand side of (5.40) is given by

$$|\mathcal{J}'|_2 \cdot \mathrm{Vol}(\mathcal{P}_n(\mathbb{Z}_2))\cdot 2^{-mn}\cdot \begin{cases} 1, & \text{if } 2\nmid n, \\ 2^{-1}, & \text{if } 2\mid n. \end{cases} \tag{5.48}$$

On the other hand, the proof of Lemma 183 also implies that the action of the group $\mathcal{P}_n(\mathbb{Z}/2^m\mathbb{Z})$ on the mod-$2^m$ reduction $\overline{\Sigma}_{f^*}$ of $\Sigma_{f^*}$ has $2^{\lfloor \frac{n}{2}\rfloor}$ distinct orbits; by Lemma 184, these orbits have trivial stabilizer when $n$ is odd and stabilizer $\{\pm \mathrm{id}\}$ when $n$ is even. By

analogy with (5.47), we find that the left-hand side of (5.40) is given by

$$2^{\lfloor \frac{n}{2} \rfloor} \cdot \mathrm{Vol}(\mathcal{P}_n(\mathbb{Z}_2)) \cdot 2^{-mn} \cdot \begin{cases} 1, & \text{if } 2 \nmid n, \\ 2^{-1}, & \text{if } 2 \mid n. \end{cases} \tag{5.49}$$

Now, Proposition 195 tells us (5.48) and (5.49) must be equal, so $|\mathcal{J}'|_2 = 2^{\lfloor \frac{n}{2} \rfloor}$. □

Combining Proposition 196 with (5.39) and Theorem 185 yields (5.29), thus completing the proof of Theorem 189.

## 5.5 Congruence conditions

In this section, we show how the method used in §5.3–5.4 to prove Theorem 169 can be adapted to count reducible orbits of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ on $W_{\mathscr{A}_n}(\mathbb{Z})$ satisfying congruence conditions, and hence to prove Theorem 171. We then take $n = 3$ and apply Theorem 171 to compute the average 2-torsion in the ideal group in monogenic cubic orders, thus proving Theorem 175.

### 5.5.1 Sieving to big families

We call a subset $S \subset W_{\mathscr{A}_n}(\mathbb{Z})$ a *big family* if $S = W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2} \cap \bigcap_p S_p$, where the sets $S_p \subset W_{\mathscr{A}_n}(\mathbb{Z}_p)$ satisfy the following properties:

(a) $S_p$ is $(N \times \mathcal{G}_{\mathscr{A}_n})(\mathbb{Z}_p)$-invariant and is the preimage under reduction modulo $p^j$ of a nonempty subset of $W_{\mathscr{A}_n}(\mathbb{Z}/p^j\mathbb{Z})$ for some $j > 0$ for each $p$; and

(b) $S_p$ contains all ($\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)$-orbits of) elements $B \in W_{\mathscr{A}_n}(\mathbb{Z}_p)_0$ such that, for all $p \gg 1$, we have that $b_{i(n-i)}(B)$ is a $p$-adic unit for some $i$.

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

**Theorem 197.** *Suppose that $S \subset W_{\mathscr{A}_n}(\mathbb{Z})$ is a big family. Then we have that*

$$\sharp\left(\frac{(S_{\mathrm{red}})_X}{(N \times \mathcal{G}_{\mathscr{A}_n})(\mathbb{Z})}\right) \sim N_n^{r_1,r_2}(X) \cdot |\mathcal{J}| \cdot \left\{ \begin{array}{ll} \left(\prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} \zeta(2i)\right) \cdot 2^{\lfloor \frac{n}{2} \rfloor} \cdot \prod_p \xi_{n,p} \int_{B \in (S_p)_0} \lambda(B) dB, & \text{if } 2 \nmid n, \\ \left(\zeta(\frac{n}{2}) \prod_{i=1}^{\frac{n-2}{2}} \zeta(2i)\right) \cdot \frac{1}{2} \cdot \prod_p \xi_{n,p} \int_{B \in (S_p)_0} \lambda(B) dB, & \text{if } 2 \mid n \end{array} \right\} \tag{5.50}$$

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

*Proof.* Let $n$ be odd (the proof for even $n$ is analogous), and suppose that the theorem holds with $W_{\mathscr{A}_n}$ replaced by $W_{\mathscr{A}_n,f_1}$ and $(S_p)_0$ replaced by $(S_p)_0 \cap W_{\mathscr{A}_n,f_1}(\mathbb{Z}_p)$. Summing the count for fixed $f_1$ over the possible values of $f_1$ yields (5.50) with the product of $p$-adic densities on the right-hand side replaced by the following:

$$\frac{1}{n} \cdot \sum_{f_1=0}^{n-1} \prod_p \xi_{n,p} \int_{B \in (S_p)_0 \cap W_{\mathscr{A}_n,f_1}(\mathbb{Z}_p)} \lambda(B) dB. \tag{5.51}$$

Let $n = \prod_p p^{f_p}$ denote the prime factorization of $n$. Through an application of the Chinese Remainder Theorem, we can reexpress (5.51) as

$$\prod_p \xi_{n,p} \cdot \frac{1}{p^{f_p}} \cdot \sum_{f_1 \in \mathbb{Z}/p^{f_p}\mathbb{Z}} \int_{B \in (S_p)_0 \cap W_{\mathscr{A}_n,f_1}(\mathbb{Z}_p)} \lambda(B) dB. \tag{5.52}$$

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

$$\frac{1}{p^{f_p}} \cdot \sum_{f_1 \in \mathbb{Z}/p^{f_p}\mathbb{Z}} \int_{B \in W_{\mathscr{A}_n,f_1}(\mathbb{Z}_p)} \phi_p(B) dB = \int_{B \in W_{\mathscr{A}_n}(\mathbb{Z}_p)_0} \phi_p(B) dB. \tag{5.53}$$

Thus, taking $\phi_p$ to be product of the indicator function of $S_p$ with the function $\lambda$ and combining (5.52) with (5.53) yields (5.50) when $n$ is odd.

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

Observe that there exist integers $m, k > 0$ such that the set $S$ may be regarded as the disjoint union of $k$ translates $\mathcal{L}_1, \dots, \mathcal{L}_k$ of the lattice $mW_{\mathscr{A}_3,0}(\mathbb{Z})$. Given $r \in (\mathbb{Z}/m\mathbb{Z})^\times$ and $B \in W_{\mathscr{A}_3,0}(\mathbb{Z}/m\mathbb{Z})$, denote by $r \cdot B \in W_{\mathscr{A}_3,0}(\mathbb{Z}/m\mathbb{Z})$ the element that arises by acting on $B$ with the element of $\mathcal{A}(\mathbb{Z}/m\mathbb{Z})$ corresponding to $r$. Then any element $B' \in W_{\mathscr{A}_3,0}(\mathbb{Z})^{r_1,r_2}$ such that $B' \equiv r \cdot B \pmod{m}$ for some $r \in (\mathbb{Z}/m\mathbb{Z})^\times$ and $B \in S$ is also an element of $S$, because $S$ is the preimage in $W_{\mathscr{A}_3,0}(\mathbb{Z})^{r_1,r_2}$ of an $\mathcal{G}_{\mathscr{A}_3}(\mathbb{Z}/m\mathbb{Z})$-invariant subset of $W_{\mathscr{A}_3,0}(\mathbb{Z}/m\mathbb{Z})$. Thus, the group $(\mathbb{Z}/m\mathbb{Z})^\times$ acts on the set of lattice translates $\{\mathcal{L}_1, \dots, \mathcal{L}_k\}$, and it suffices to prove the theorem with the set $S$ replaced by a single $(\mathbb{Z}/m\mathbb{Z})^\times$-orbit on the set of lattice translates $\{\mathcal{L}_1, \dots, \mathcal{L}_k\}$. Without loss of generality, we may assume that this orbit comprises the lattice translates $\mathcal{L}_1, \dots, \mathcal{L}_\ell$ for some $\ell \in \{1, \dots, k\}$.

For $j \in \{1, \dots, \ell\}$, write $\mathcal{L}_j = B_j + mW_{\mathscr{A}_3,0}(\mathbb{Z})$, where $B_j \in W_{\mathscr{A}_3,0}(\mathbb{Z})$. The computation of $\#(\mathcal{G}_{\mathscr{A}_3}(\mathbb{Z})\backslash((\mathcal{L}_j \cap W_{\mathscr{A}_3,0}(\mathbb{R})^{r_1,r_2})_{\mathrm{red}})_X)$ is analogous to that of $\#(\mathcal{G}_{\mathscr{A}_3}(\mathbb{Z})\backslash(W_{\mathscr{A}_3,0}(\mathbb{Z})^{r_1,r_2}_{\mathrm{red}})_X)$ in §5.3.1–§5.3.2, so we summarize the key points. By analogy with (5.15), we have

$$\#\left(\frac{((\mathcal{L}_j \cap W_{\mathscr{A}_3,0}(\mathbb{R})^{r_1,r_2})_{\mathrm{red}})_X}{\mathcal{G}_{\mathscr{A}_3}(\mathbb{Z})}\right) \sim \frac{1}{C_H}\int_{s\in\mathcal{A}^\star}\int_{u\in\mathcal{N}^\star(s_1)} \#(\mathcal{B}(u,s_1)_X \cap (\mathcal{L}_j)_0)du\frac{ds_1}{s_1^2}. \tag{5.54}$$

First suppose $a_j \not\equiv 0 \pmod{m}$. Then $(\mathcal{L}_j)_0 = \varnothing$, and it follows that we have

$$\#\left(\frac{((\mathcal{L}_j \cap W_{\mathscr{A}_3,0}(\mathbb{R})^{r_1,r_2})_{\mathrm{red}})_X}{\mathcal{G}_{\mathscr{A}_3}(\mathbb{Z})}\right) = o(X);$$

on the other hand, we must also have $((\mathcal{L}_j)_p)_0 = \varnothing$ for some prime $p \mid m$, so the theorem holds in this case. We may thus assume that $b_{11}(B_j) \equiv 0 \pmod{m}$ and in fact that $b_{11}(B_j) = 0$. Then, slicing yields a sum over $b \equiv b_{12}(B_j) \pmod{m}$, and the application of Proposition 186

gives a factor of $m^{-3}$ because we are counting lattice points in the 3-dimensional region $\mathcal{B}_b(u,s_1)_X$ on a lattice translate of $mW_{\mathscr{A}_3,0}(\mathbb{Z})$. Thus, by analogy with (5.20),

$$\#\left(\frac{((\mathcal{L}_j\cap W_{\mathscr{A}_3,0}(\mathbb{R})^{r_1,r_2})_{\mathrm{red}})_X}{\mathcal{G}_{\mathscr{A}_3}(\mathbb{Z})}\right)\sim\frac{1}{C_H}\sum_{\substack{b\in\mathbb{Z}\\ b\neq 0\\ b\equiv b_j\ (\mathrm{mod}\,m)}}\int_{s_1\geq\Gamma}\int_{u\in\mathcal{N}^\star(s_1)}m^{-3}\cdot\mathrm{Vol}(\mathcal{B}_b(u,s_1)_X)du\frac{ds_1}{s_1^2}. \tag{5.55}$$

Let $m':=\gcd(b_j,m)$; observe that $m'$ is independent of $j\in\{1,\dots,\ell\}$, as the set $\{\mathcal{L}_1,\dots,\mathcal{L}_\ell\}$ is a $(\mathbb{Z}/m\mathbb{Z})^\times$-orbit. Further notice that every mod-$m$ residue class $b$ such that $\gcd(b,m)=m'$ is represented exactly once among the $b_j$. Consequently, after summing (5.55) over $j\in\{1,\dots,\ell\}$, we obtain by analogy with (5.28) that

$$\begin{aligned}\#\left(\frac{(S_{\mathrm{red}})_X}{\mathcal{G}_{\mathscr{A}_3}(\mathbb{Z})}\right)&\sim\sum_{\substack{b\in\mathbb{Z}_{>0}\\ \gcd(b,m)=m'}}b^{-2}\cdot\frac{1}{C_H}\int_{\beta\geq 0}m^{-3}\cdot\beta\cdot\mathrm{Vol}(\mathcal{B}_\beta(X))d\beta\\ &\sim m^{-3}m'^{-2}\cdot\left(\prod_{p\mid mm'^{-1}}(1-p^{-2})\right)\cdot\zeta(2)\cdot N_3^{r_1,r_2}(X).\end{aligned} \tag{5.56}$$

On the other hand, writing $e_p:=\nu_p(m)$ and $e_p':=\nu_p(m')$ for each $p$, we have

$$\begin{aligned}&\int_{B\in((\mathcal{L}_j)_p)_0}|b_{12}(B)|_p dB=\\ &\begin{cases}\displaystyle\int_{\substack{B\in W_{\mathscr{A}_3,0}(\mathbb{Z}_p)_0\\ B\equiv B_j\ (\mathrm{mod}\,p^{e_p})}}|b_{12}(B)|_p dF=p^{-5e_p}(1+p^{-1})^{-1},&\text{if } p\nmid mm'^{-1},\\ \displaystyle\int_{\substack{B\in W_{\mathscr{A}_3,0}(\mathbb{Z}_p)_0\\ B\equiv B_j\ (\mathrm{mod}\,p^{e_p})}}|b_{12}(B)|_p dB=p^{-4e_p-e_p'},&\text{if } p\mid mm'^{-1},\end{cases}\end{aligned} \tag{5.57}$$

where the last step follows by splitting $\{B\in W_{\mathscr{A}_3,0}(\mathbb{Z}_p)_0 : B\equiv B_j\ (\mathrm{mod}\ p^{e_p})\}$ and $W_{\mathscr{A}_3,0}(\mathbb{Z}_p)_0$ into level sets for the function $|b_{12}(B)|_p$, integrating on each level set, and summing up. As $\ell=\#\big(\mathbb{Z}/(mm'^{-1})\mathbb{Z}\big)^\times=\prod_{p\mid mm'^{-1}}p^{e_p-e_p'}(1-p^{-1})$, summing (5.57) over $j\in\{1,\dots,\ell\}$ and multiplying over all $p$ yields that

$$\prod_p(1+p^{-1})\int_{B\in(S_p)_0}|b_{12}(B)|_p dB=\#\big(\mathbb{Z}/(mm'^{-1})\mathbb{Z}\big)^\times\cdot\prod_p\int_{B\in((\mathcal{L}_1)_p)_0}|b_{12}(B)|_p dB= \tag{5.58}$$

$$\prod_{p\nmid mm'^{-1}} p^{-5e_p} \cdot \prod_{p|mm'^{-1}} p^{-3e_p-2e'_p} \cdot (1-p^{-2}) = m^{-3}m'^{-2} \cdot \prod_{p|mm'^{-1}} (1-p^{-2}).$$

Comparing (5.56) and (5.58) yields the theorem when $S$ is replaced by $\bigsqcup_{j=1}^{\ell} \mathcal{L}_j$.

It remains to prove the theorem in the case where $S$ is defined by infinitely many congruence conditions. First note that the proof of (5.29) (or [29, Theorem 1.5]) implies the following uniformity estimate: the number of $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$-orbits of $B \in (W_{\mathscr{A}_n,f_1}(\mathbb{Z})^{r_1,r_2}_{\mathrm{red}})_X$ with $b_{i(n-i)}(B)$ divisible by some prime larger than $Y > 1$, for some $i$, is $O\big(X^{\frac{n^2+n-2}{2}}Y^{-1}\big) + O_\epsilon\big(X^{\frac{n^2+n-2}{2}-\frac{1}{5}+\epsilon}\big)$, where the implied constant is independent of $X, Y$. Given this estimate, Theorem 197 follows from the "finitely many congruence conditions" case by applying an inclusion-exclusion sieve. □

*Remark* 198. In the proof of Theorem 197, the assumption that $S$ is the preimage of an $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}/m\mathbb{Z})$-invariant subset of $W_{\mathscr{A}_n}(\mathbb{Z}/m\mathbb{Z})$ caused the slicing parameters of the elements of $S$ to be invariant under multiplication by units modulo $m$. It is important to note that Theorem 197 does *not* always hold without this invariance.

Theorem 197 gives a formula for the number of lattice points of bounded height satisfying big sets of congruence conditions in cusps of fundamental sets for the action of $(N \times \mathcal{G}_{\mathscr{A}_n})(\mathbb{Z})$ on $W_{\mathscr{A}_n}(\mathbb{R})$ that is easy to compute in some cases. For example, as part of the proof of Theorem 175 in §5.6.2, we directly compute the $p$-adic local factor on the right-hand side of (5.50) when $n = 3$ and $S_p \subset W_{\mathscr{A}_3}(\mathbb{Z}_p)$ is the subset of pre-projective elements. The formula in Theorem 197 is also convenient for estimating the contribution of elements having big stabilizer (see the remark after Theorem 189 for the definition) to $\sharp\big((N \times \mathcal{G}_{\mathscr{A}_n})(\mathbb{Z})\backslash W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2}_{\mathrm{red}}\big)$. To this end, let

$$W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2}_{\mathrm{bigstab}} := \big\{B \in W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2} : \mathrm{Stab}_{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})}(B) \text{ is big}\big\}.$$

Then we have the following bound:

**Proposition 199.** *We have* $\sharp\big((N \times \mathcal{G}_{\mathscr{A}_n})(\mathbb{Z})\backslash\big(W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2}_{\mathrm{bigstab}}\big)_{\mathrm{red}}\big) = o\big(X^{\frac{n^2+n-2}{2}}\big)$.

*Proof.* From of Theorem 13, it follows that $\mathrm{Stab}_{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})}(B)$ is big only if the form $\iota(\mathscr{A}_n, B)$ is reducible over $\mathbb{Z}$. Thus, letting

$$W_{\mathscr{A}_n}(\mathbb{Z}_p)_{\mathrm{split}} := \{B \in W_{\mathscr{A}_n}(\mathbb{Z}_p) : \iota(\mathscr{A}_n, B) \text{ is reducible modulo } p\}$$

for each $p$, we have $W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2}_{\mathrm{bigstab}} \subset W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2} \cap \bigcap_p W_{\mathscr{A}_n}(\mathbb{Z}_p)_{\mathrm{split}}$. Then, upon combining Theorem 197 with the trivial bound $|x|_p \leq 1$ for any $x \in \mathbb{Z}_p$, we have

$$\lim_{X\to\infty} \frac{\sharp\big((N \times \mathcal{G}_{\mathscr{A}_n})(\mathbb{Z})\backslash\big(W_{\mathscr{A}_n}(\mathbb{Z})^{r_1,r_2}_{\mathrm{bigstab}}\big)_{\mathrm{red}}\big)}{X^{\frac{n^2+n-2}{2}}} \ll \prod_{p<Y}(1+p^{-1})^2 \int_{B\in(W_{\mathscr{A}_n}(\mathbb{Z}_p)_{\mathrm{split}})_0} dB \tag{5.59}$$

for any number $Y > 0$, where the implied constant is independent of $Y$. To prove the proposition, it now suffices to estimate the factor at $p$ on the right-hand side of (5.59) for each prime $p \gg 1$.

For a $\mathbb{Z}$-algebra $R$, define subgroups $\mathcal{A}(R), \mathcal{N}(R) \subset \mathrm{SO}_{\mathscr{A}_n}(R)$ as follows:

- $\mathcal{A}(R)$ is the subgroup whose elements are those of the form (5.5) when $n$ is odd and of the form (5.6) when $n$ is even, where $s_i \in R^\times$ for each $i \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}$.
- $\mathcal{N}(R)$ is the subgroup of all lower-triangular unipotent matrices over $R$.

Let $\mathcal{P}(R) := \mathcal{A}(R) \cdot \mathcal{N}(R) \subset \mathrm{SO}_{\mathscr{A}_n}(R)$, and observe that the action of $\mathcal{P}(R)$ on $W_{\mathscr{A}_n}(R)$ preserves the subspace $W_{\mathscr{A}_n}(R)_0$. We now take $R = \mathbb{F}_p$. When $p > 2$, it follows from the proof of Lemma 183 that $\mathcal{P}(\mathbb{F}_p)$ acts simply transitively on the set $\mathcal{O}_f := \{B \in W_{\mathscr{A}_n}(\mathbb{F}_p)_0 : \iota(\mathscr{A}_n, B) = f\}$ for any separable form $f \in V_{n,1}(\mathbb{F}_p)$. Thus, we have for such a form $f$ that

$$\#\mathcal{O}_f = \#\mathcal{P}(\mathbb{F}_p) = (1-p^{-1})^{\lfloor \frac{n}{2} \rfloor} \cdot \begin{cases} p^{\frac{n^2-1}{4}}, & \text{if } 2 \nmid n, \\ p^{\frac{n^2}{4}}, & \text{if } 2 \mid n. \end{cases} \tag{5.60}$$

It is a well-known result (e.g., see [15, §10.7]) that the number of irreducible separable forms

$F \in V_{n,1}(\mathbb{F}_p)$ is given by the following asymptotic formula:

$$n^{-1}p^n + O(p^{n-1}), \tag{5.61}$$

where the implied constant is independent of the prime $p$. Combining (5.60) with (5.61) together with the fact that

$$\dim_{\mathbb{F}_p} W_{\mathscr{A}_n}(\mathbb{F}_p)_0 = \begin{cases} \frac{n^2-1}{4} + n, & \text{if } 2 \nmid n, \\ \frac{n^2}{4} + n, & \text{if } 2 \mid n \end{cases} \tag{5.62}$$

yields the following bound:

$$\begin{aligned} \int_{B \in (W_{\mathscr{A}_n}(\mathbb{Z}_p)_{\mathrm{split}})_0} dB &\leq 1 - \left\{ \begin{array}{ll} \frac{\left((1-p^{-1})^{\lfloor \frac{n}{2} \rfloor} p^{\frac{n^2-1}{4}}\right)(n^{-1}p^n + O(p^{n-1}))}{p^{\frac{n^2-1}{4}+n}}, & \text{if } 2 \nmid n, \\ \frac{\left((1-p^{-1})^{\lfloor \frac{n}{2} \rfloor} p^{\frac{n^2}{4}}\right)(n^{-1}p^n + O(p^{n-1}))}{p^{\frac{n^2}{4}+n}}, & \text{if } 2 \mid n \end{array} \right\} \\ &\leq 1 - n^{-1} - O(p^{-1}). \end{aligned} \tag{5.63}$$

Substituting the bound (5.63) into the right-hand side of (5.59) and taking the limit as $Y \to \infty$ on both sides yields the proposition. □

Combining Theorem 189 with Proposition 199 yields Theorem 169.

While Theorem 197 has its uses, it is not easy to apply when $S$ is defined by congruence conditions involving the coefficients of the binary forms $f \in V_{n,1}(\mathbb{Z})^{r_1,r_2}$. Using the $p$-adic change-of-variables result in Proposition 195, we can express the $p$-adic local factors on the right-hand side of (5.50) in a form that is more convenient in the case where $S$ is defined by such congruence conditions. Taking $\phi_p$ to be the indicator function of $(S_p)_0$ for each prime $p$ in Proposition 195, combining the result with Theorem 197 and Propositions 196 and 199,

and observing that

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

yields the following:

**Theorem 200.** *Suppose that $S \subset W_{\mathscr{A}_n}(\mathbb{Z})$ is a big family. Then we have that*

$$\#\left(\frac{(S_{\mathrm{red}})_X}{(N \times \mathcal{G}_{\mathscr{A}_n})(\mathbb{Z})}\right) \sim N_n^{r_1,r_2}(X) \cdot \prod_p \int_{\substack{f \in \mathbb{Z}_p^n \\ \Delta(F_f) \neq 0}} \epsilon_n \cdot \#\left(\frac{\mathrm{inv}^{-1}(f) \cap (S_p)_0}{\mathcal{P}(\mathbb{Z}_p)}\right) df, \tag{5.64}$$

*where $\epsilon_2 = 1$ if $n$ is odd and $\epsilon_2 = \frac{1}{2}$ if $n$ is even.*

We say that a subset $\Sigma \subset V_{n,1}(\mathbb{Z})$ is *defined by finitely many congruence conditions* if we have $\Sigma = V_{n,1}(\mathbb{Z})^{r_1,r_2} \cap \bigcap_p \Sigma_p$, where the sets $\Sigma_p \subset V_{n,1}(\mathbb{Z}_p)$ satisfy the following properties: (1) $\Sigma_p$ is the preimage under reduction modulo $p^j$ of a nonempty subset of $V_{n,1}(\mathbb{Z}/p^j\mathbb{Z})$ for some $j > 0$ for each prime $p$; and (2) $\Sigma_p$ contains all of $V_{n,1}(\mathbb{Z}_p)$ for all sufficiently large $p$. Observe that if $\Sigma \subset \mathbb{Z}$ is defined by finitely many congruence conditions, then so is $\mathrm{inv}^{-1}(\Sigma) \subset W_{\mathscr{A}_n}(\mathbb{Z})$; thus, Theorem 171 is a special case of Theorem 200.

## 5.6 Application to counting 2-torsion ideals

In this section, we apply the results on counting in cusps obtained in the preceding sections to study the distribution of 2-torsion ideals and ideal classes of monogenic orders.

### 5.6.1 Preliminaries on 2-torsion ideals

Retain the setting of §1.4 (i.e., let $n$, $f_0$, $R$, $f$, and $r$ be as in §1.4) with $n$ odd and $f_0 = 1$. Recall from §2.4.1 that, since $n$ is odd and since we are only interested in reducible orbits, it suffices to take $r = 1$.

First let $R = \mathbb{Z}$. We now explain how 2-torsion ideals of $R_f$ can be parametrized in terms of reducible orbits. Consider the map

$$\mathcal{I}(R_f)[2] \to G_n(\mathbb{Z})\backslash W_n(\mathbb{Z}) \tag{5.65}$$

of sets defined by sending an ideal $I \in \mathcal{I}(R_f)[2]$ to the pair $\mathsf{orb}_{f,1}(I, 1)$, where we give $I$ a basis so that $\mathrm{N}(I) = 1$. Since 2-torsion ideals are necessarily invertible, the map (5.65) factors through the map $\mathsf{orb}_{f,1}\colon H^*_{f,1} \to G_n(\mathbb{Z})\backslash W_n(\mathbb{Z})$; furthermore, by the definition of reducibility, the image of the map (5.65) consists entirely of reducible orbits. In fact, we have the following proposition, the proof of which is immediate:

**Proposition 201** ([71, Proposition 2.12])**.** *The map* (5.65) *defines a bijection between* $\mathcal{I}(R_f)[2]$ *and the set of* $G_n(\mathbb{Z})$*-orbits of pre-projective reducible pairs* $(A, B) \in W_n(\mathbb{Z})$ *with* $\iota(A, B) = f$*.*

*Remark* 202. When $R_f$ is maximal, any 2-torsion ideal of $R_f$ must be the unit ideal, so by Proposition 201, there is a unique reducible pair $(A, B) \in W_n(\mathbb{Z})$ up to the action of $G_n(\mathbb{Z})$ with $\iota(A, B) = f$ in this case (cf. Proposition 45).

We say that $B \in W_{\mathscr{A}_n}(\mathbb{Z})$ is pre-projective if the pair $(\mathscr{A}_n, B)$ is pre-projective. Combining Proposition 201 with (1.9), we obtain the following result parametrizing the elements of $\mathcal{I}(R_f)[2]$ in terms of reducible $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$ orbits on $W_{\mathscr{A}_n}(\mathbb{Z})$:

**Corollary 203.** *The elements of* $\mathcal{I}(R_f)[2]$ *are in bijection with the* $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z})$*-orbits of pre-projective reducible elements* $B \in W_{\mathscr{A}_n}(\mathbb{Z})$ *such that* $\iota(\mathscr{A}_n, B) = f$*.*

Now let $R$ be a PID. The next proposition identifies which elements of $W_n(R)$ are pre-projective (note that this proposition only applies to *monic* binary forms $f$; the condition of pre-projectivity is more complicated when $f_0$ has prime factors):

**Proposition 204.** *Let* $(A, B) \in W_n(R)$ *with* $\iota(A, B) = f$*. For each* $k \in \{0, \dots, n-1\}$*, let*

*$C^{(k)}$ be the $n \times n$ matrix over $R$ defined as follows:*

$$C^{(k)} = \begin{cases} A, & \text{if } k = n-1, \\ B, & \text{if } k = n-2, \\ \left(\sum_{i=0}^{n-k-3} f_i (BA^{-1})^{n-k-2-i}\right) B, & \text{if } k \in \{1, \dots, n-3\}, \\ \left(\sum_{i=0}^{n-1} f_i (BA^{-1})^{n-1-i}\right) A, & \text{if } k = 0. \end{cases} \tag{5.66}$$

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

*Proof.* Let $(I, \alpha) \in H_{f,1}$ such that $\mathsf{orb}_{f,1}(I, \alpha)$ contains the pair $(A, B)$. By [71, §2.2], the matrices $C^{(k)}$ are symmetric, and the matrix $M$ represents the map of $R$-modules $I \times I \to R_f$ in (1.14) with respect to the basis of $I \times I$ obtained by taking pairwise products of the basis elements of $I$. The fractional ideal $I$ is invertible if and only if $I^2 = (\alpha)$ (as opposed to just having a containment $I^2 \subset (\alpha)$), and this occurs if and only if the map $I \times I \to R_f$ is surjective, which in turn happens if and only if the $n \times n$ minors of $M$ have no common divisor. □

By Proposition 204, a pair $(A, B) \in W_n(\mathbb{Z})$ is pre-projective if and only if it is pre-projective over $\mathbb{Z}_p$ for every prime $p$; in particular, the locus of pre-projective pairs in $W_n(\mathbb{Z})$ is cut out by congruence conditions modulo each prime.

### 5.6.2 Computing the volume of pre-projective elements

By Corollary 203 and Proposition 204 along with (5.2), proving Theorems 173–175 amounts to determining the number of reducible $(N \times \mathcal{G}_{\mathscr{A}_n})(\mathbb{Z})$-orbits on $W_{\mathscr{A}_n}(\mathbb{Z})$ that are pre-projective over $\mathbb{Z}_p$ for every prime $p$. To this end, let $W_{\mathscr{A}_n}(\mathbb{Z}_p)^{\text{proj}}$ be the subset of pre-projective elements of $W_{\mathscr{A}_n}(\mathbb{Z}_p)$. In this section, we first prove Theorems 173 and 175 by

applying Theorem 197 in the case where $n = 3$ and $S_p = W_{\mathscr{A}_3}(\mathbb{Z}_p)^{\mathrm{proj}}$ for every prime $p$. We then prove Theorem 174 by applying Theorem 200 in the case where $n \geq 3$ and $S_p = W_{\mathscr{A}_n}(\mathbb{Z}_p)^{\mathrm{proj}}$ for every $p$.

*Proofs of Theorems 173 and 175.* Let $B = [b_{ij}] \in W_{\mathscr{A}_3}(\mathbb{Z}_p)_0$. Then Proposition 204 implies that $B$ fails to be pre-projective if and only if

$$b_{12} \equiv b_{23}^2 + (b_{13} - b_{22})b_{33} \equiv 0 \pmod{p}. \tag{5.67}$$

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

From the previous paragraph, we deduce that for every integer $k \geq 0$, the $p$-adic density of the level set $\mathscr{W}_k := \{B \in W_{\mathscr{A}_3}(\mathbb{Z}_p)_0^{\mathrm{proj}} : \nu_p(b_{12}(B)) = k\}$ in $W_{\mathscr{A}_3}(\mathbb{Z}_p)_0$ is given by $1 - p^{-1}$ if $k = 0$ and by $p^{-k}(1-p^{-1})^2$ if $k > 0$. Summing over the level sets $\mathscr{W}_k$ yields that

$$\begin{aligned}\int_{B \in W_3(\mathbb{Z}_p)_0^{\mathrm{proj}}} |b_{12}(B)|_p dB &= \sum_{k \geq 0} \int_{B \in \mathscr{W}_k} p^{-k} dB = (1 - p^{-1}) + \sum_{k \geq 1} p^{-2k}(1-p^{-1})^2 \\ &= 1 - p^{-1} + p^{-2}(1+p^{-1})^{-1}(1-p^{-1}).\end{aligned} \tag{5.68}$$

Let $(W_{\mathscr{A}_3}(\mathbb{Z})^{r_1,r_2})^{\mathrm{proj}}$ be the subset of pre-projective elements of $W_{\mathscr{A}_3}(\mathbb{Z})^{r_1,r_2}$. Substituting (5.68) into Theorem 197 and dividing by $N_3^{r_1,r_2}(X)$ yields Theorem 175. Theorem 173 then follows by combining the result of Theorem 175 with Siad's determination in [108, Theorem 9] of the average size of the quantity (5.2). □

*Proof of Theorem 174.* We have the following formula for the integrand of the $p$-adic local factor on the right-hand side of (5.64) when $S_p = W_{\mathscr{A}_n}(\mathbb{Z}_p)^{\mathrm{proj}}$:

**Proposition 205.** *Let $n \geq 3$ be odd, let $f \in V_{n,1}(\mathbb{Z}_p)$ be separable. Then*

$$\# \left( \frac{\mathrm{inv}^{-1}(f) \cap W_{\mathscr{A}_n}(\mathbb{Z}_p)_0^{\mathrm{proj}}}{\mathcal{P}(\mathbb{Z}_p)} \right) = 2^{\mathrm{rk}_2(\overline{R}_f^\times / R_f^\times)}.$$

*Proof of Proposition 205.* By the definition of reducibility and Theorem 39, the set of pre-projective reducible $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)$-orbits of elements $B \in W_{\mathscr{A}_n}(\mathbb{Z}_p)$ with $\iota(\mathscr{A}_n, B) = f$ is in bijection with

$$\ker\left((R_f^\times / R_f^{\times 2})_{\mathrm{N}\equiv 1} \to (K_f^\times / K_f^{\times 2})_{\mathrm{N}\equiv 1}\right) = \ker(R_f^\times / R_f^{\times 2} \to \overline{R}_f^\times / \overline{R}_f^{\times 2}). \tag{5.69}$$

Next, let us fix a $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)$-orbit $\mathcal{O}$ of reducible elements $B \in W_{\mathscr{A}_n}(\mathbb{Z}_p)$ satisfying $\iota(\mathscr{A}_n, B) = f$. The following lemma establishes that $\mathcal{O}$ necessarily meets the subset $W_{\mathscr{A}_n}(\mathbb{Z}_p)_0 \subset W_{\mathscr{A}_n}(\mathbb{Z}_p)$:

**Lemma 206.** *We have that $\mathcal{O}_0 \neq \varnothing$.*

*Proof of Lemma 206.* Let $B \in \mathcal{O}$. Since $B$ is reducible, Proposition 20 implies that there exists $\gamma \in \mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)$ such that $\gamma \cdot B \in W_{\mathscr{A}_n}(\mathbb{Z}_p)_0$. By the $p$-adic Iwasawa decomposition (see [89]), we have that $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p) = \mathcal{P}(\mathbb{Q}_p) \cdot \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)$. Thus, $\gamma = \pi \cdot \gamma'$ for some $\pi \in \mathcal{P}_n(\mathbb{Q}_p)$ and $\gamma' \in \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)$, and since $\mathcal{P}_n(\mathbb{Q}_p)$ acts on $W_{\mathscr{A}_n}(\mathbb{Q}_p)_0$, it follows that $\gamma' \cdot B \in \mathcal{O}_0$. □

The group $\mathcal{P}_n(\mathbb{Z}_p)$ acts on $\mathcal{O}_0$, which is nonempty by Lemma 206. The next lemma gives a parametrization of the orbits of $\mathcal{P}_n(\mathbb{Z}_p)$ on $\mathcal{O}_0$:

**Lemma 207.** *Let $B \in \mathcal{O}_0$. Then the set $\mathcal{P}_n(\mathbb{Z}_p)\backslash\mathcal{O}_0$ is in bijection with the quotient group* $\mathrm{Stab}_{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)}(B) / \mathrm{Stab}_{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)}(B)$.

*Proof of Lemma 207.* Let $B' \in \mathcal{O}_0$. Then there exists $\gamma \in \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)$ such that $B' = \gamma \cdot B$. Moreover, by the proof of Lemma 183, there exists $\pi' \in \mathcal{P}_n(\mathbb{Q}_p)$ such that $B' = \pi' \cdot B$. Then we have that $\pi'^{-1} \cdot \gamma \in \mathrm{Stab}_{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)}(B)$, and the map $\Phi\colon \mathcal{P}_n(\mathbb{Z}_p)\backslash\mathcal{O}_0 \to \mathrm{Stab}_{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)}(B) / \mathrm{Stab}_{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)}(B)$ defined by sending $B' \mapsto \pi'^{-1} \cdot \gamma$ is readily seen to be both well-defined and injective. To see that $\Phi$ is surjective, take $\gamma \in \mathrm{Stab}_{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)}(B)$, and write

$\gamma = \pi \cdot \gamma'$ for $\pi \in \mathcal{P}_n(\mathbb{Q}_p)$ and $\gamma' \in \mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)$. Then $B'' := \pi^{-1} \cdot B = \gamma' \cdot B \in W_{\mathscr{A}_n}(\mathbb{Q}_p)_0 \cap \mathcal{O} = \mathcal{O}_0$, and we evidently have $\Phi(B'') = \gamma$. □

Since $n$ is odd, we have isomorphisms $R_f^\times[2] \simeq R_f^\times[2]_{\mathrm{N}\equiv 1} \times \{\pm 1\}$ and $K_f^\times[2] \simeq \overline{R}_f^\times[2]_{\mathrm{N}\equiv 1} \times \{\pm 1\}$. Thus, by Theorem 13, we have that

$$\mathrm{Stab}_{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Q}_p)}(B) / \mathrm{Stab}_{\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)}(B) = K_f^\times[2]_{\mathrm{N}\equiv 1} / R_f^\times[2]_{\mathrm{N}\equiv 1} \simeq \overline{R}_f^\times[2] / R_f^\times[2], \tag{5.70}$$

Combining the parametrization of pre-projective reducible $\mathcal{G}_{\mathscr{A}_n}(\mathbb{Z}_p)$-orbits in (5.69), the parametrization of $\mathcal{P}_n(\mathbb{Z}_p)$-orbits in Lemma 207, and the equality (5.70) yields that the number of pre-projective $\mathcal{P}_n(\mathbb{Z}_p)$-orbits of elements $B \in W_{\mathscr{A}_n}(\mathbb{Z}_p)_0$ with $\iota(\mathscr{A}_n, B) = f$ is

$$\#(\overline{R}_f^\times[2] / R_f^\times[2]) \cdot \#\ker(R_f^\times / R_f^{\times 2} \to \overline{R}_f^\times / \overline{R}_f^{\times 2}) = 2^{\mathrm{rk}_2(\overline{R}_f^\times / R_f^\times)}. \qquad \square$$

The statement on 2-torsion in ideal groups in Theorem 174 now follows upon substituting the result of Proposition 205 into each of the local factors on the right-hand side of (5.64). As in the proof of Theorem 173, the statement on 2-torsion in class groups in Theorem 174 then follows by applying Siad's determination in [108, Theorem 9] of the average size of the quantity (5.2). □

# Bibliography


[1] A. Afshar and S. Porritt. The function field Sathe-Selberg formula in arithmetic progressions and 'short intervals'. *Acta Arith.*, 187(2):101–124, 2019.

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

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

[4] A. Ash, J. Brakenhoff, and T. Zarrabi. Equality of polynomial and field discriminants. *Experiment. Math.*, 16(3):367–374, 2007.

[5] M. Bhargava. The factorial function and generalizations. *Amer. Math. Monthly*, 107(9):783–799, 2000.

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

[7] M. Bhargava. Higher composition laws. III. The parametrization of quartic rings. *Ann. of Math. (2)*, 159(3):1329–1360, 2004.

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

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

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

[11] M. Bhargava. Most hyperelliptic curves over $\mathbb{Q}$ have no rational points. *arXiv preprint arXiv:1308.0395*, 2013.

[12] M. Bhargava. The geometric sieve and the density of squarefree values of invariant polynomials. *arXiv preprint arXiv:1402.0031*, 2014.

[13] M. Bhargava, J. Cremona, and T. Fisher. The proportion of genus one curves over $\mathbb{Q}$ defined by a binary quartic that everywhere locally have a point. *Int. J. Number Theory*, 17(4):903–923, 2021.

[14] M. Bhargava, J.-H. Evertse, K. Győry, L. Remete, and A. A. Swaminathan. Hermite equivalence of polynomials. *arXiv preprint arXiv:2109.02932v2*, 2022.

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

[16] M. Bhargava, B. H. Gross, and X. 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.

[17] M. Bhargava, B. H. Gross, and X. Wang. A positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ have no point over any odd degree extension. *J. Amer. Math. Soc.*, 30(2):451–493, 2017. With an appendix by T. Dokchitser and V. Dokchitser.

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

[19] M. Bhargava and W. Ho. Coregular spaces and genus one curves. *Camb. J. Math.*, 4(1):1–119, 2016.

[20] M. Bhargava, D. M. Kane, H. W. Lenstra, Jr., B. Poonen, and E. Rains. Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves. *Camb. J. Math.*, 3(3):275–321, 2015.

[21] M. Bhargava and B. Poonen. The local-global principle for stacky curves. 2019. In preparation, exact title to be determined.

[22] M. Bhargava and A. Shankar. The average number of elements in the 4-selmer groups of elliptic curves is 7. *arXiv preprint arXiv:1312.7333*, 2013.

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

[24] M. Bhargava and A. Shankar. The average size of the 5-selmer group of elliptic curves is 6, and the average rank is less than 1. *arXiv preprint arXiv:1312.7859*, 2013.

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

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

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

[28] M. Bhargava, A. Shankar, and A. Swaminathan. The second moment of the size of the 2-Selmer group of elliptic curves. *arXiv preprint arXiv:2110.09063*, 2021.

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

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

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

[32] B. J. Birch and J. R. Merriman. Finiteness theorems for binary forms with given discriminant. *Proc. London Math. Soc. (3)*, 24:385–394, 1972.

[33] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. I. *J. Reine Angew. Math.*, 212:7–25, 1963.

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

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

[36] B. Breen. The 2-Selmer group of $S_n$-number fields of even degree. *arXiv preprint arXiv:2110.00197*, 2021.

[37] N. Bruin and E. V. Flynn. Towers of 2-covers of hyperelliptic curves. *Trans. Amer. Math. Soc.*, 357(11):4329–4347, 2005.

[38] N. R. Bruin. *Chabauty methods and covering techniques applied to generalized Fermat equations*, volume 133 of *CWI Tract*. Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 2002. Dissertation, University of Leiden, Leiden, 1999.

[39] N. R. Bruin and M. Stoll. Two-cover descent on hyperelliptic curves. *Math. Comp.*, 78(268):2347–2370, 2009.

[40] L. Candelori and F. Cameron. Vector bundles and modular forms for Fuchsian groups of genus zero. *arXiv preprint arXiv:1704.01684*, 2017.

[41] Y. Cao, C. Demarche, and F. Xu. Comparing descent obstruction and Brauer-Manin obstruction for open varieties. *Trans. Amer. Math. Soc.*, 371(12):8625–8650, 2019.

[42] M. Car. Factorisation dans $F_q[X]$. *C. R. Acad. Sci. Paris Sér. I Math.*, 294(4):147–150, 1982.

[43] L. Carlitz. The arithmetic of polynomials in a Galois field. *Amer. J. Math.*, 54(1):39–50, 1932.

[44] J. W. S. Cassels. The Mordell-Weil group of curves of genus 2. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 27–60. Birkhäuser, Boston, Mass., 1983.

[45] S. Cho. Group schemes and local densities of quadratic lattices in residue characteristic 2. *Compos. Math.*, 151(5):793–827, 2015.

[46] 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.

[47] H. Cohen and J. Martinet. Class groups of number fields: numerical heuristics. *Math. Comp.*, 48(177):123–137, 1987.

[48] J. H. Conway. *The sensual (quadratic) form*, volume 26 of *Carus Mathematical Monographs*. Mathematical Association of America, Washington, DC, 1997. With the assistance of Francis Y. C. Fung.

[49] 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.

[50] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[51] J. E. Cremona and T. A. Fisher. On the equivalence of binary quartics. *J. Symbolic Comput.*, 44(6):673–682, 2009.

[52] H. Darmon. Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation. *C. R. Math. Rep. Acad. Sci. Canada*, 19(1):3–14, 1997.

[53] H. Darmon and A. Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

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

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

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

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

[58] 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.

[59] I. Del Corso, R. Dvornicich, and D. Simon. Decomposition of primes in non-maximal orders. *Acta Arith.*, 120(3):231–244, 2005.

[60] A. Dembo, B. Poonen, Q.-M. Shao, and O. Zeitouni. Random polynomials having few or no real zeros. *J. Amer. Math. Soc.*, 15(4):857–892, 2002.

[61] J. S. Ellenberg. Comment in response to blog post of Emerton. MathOverflow, 2011. URL: `https://mathoverflow.net/q/52815` (version: 2011-01-22).

[62] M. Emerton. Does (the ideal class of) the different of a number field have a canonical square root? MathOverflow, 2011. URL: `https://mathoverflow.net/questions/28776/does-the-ideal-class-of-the-different-of-a-number-field-have-a-canonical-squar/` (version: 2011-01-22).

[63] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[64] E. Fouvry and J. Klüners. On the 4-rank of class groups of quadratic number fields. *Invent. Math.*, 167(3):455–513, 2007.

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

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

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

[68] F. Gundlach. *Parametrizing extensions with fixed Galois group*. ProQuest LLC, Ann Arbor, MI, 2019. Thesis (Ph.D.)–Princeton University.

[69] D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. *Invent. Math.*, 111(1):171–195, 1993.

[70] E. Hecke. *Lectures on the theory of algebraic numbers*, volume 77 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1981. Translated from the German by G. U. Brauer, J. R. Goldman, and R. Kotzen.

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

[72] M. Hochster. Module-finite extensions of complete local rings. `http://www.math.lsa.umich.edu/ hochster/615W14/ModFinComp.pdf`, 2014.

[73] B. W. Jones. A canonical quadratic form for the ring of 2-adic integers. *Duke Math. J.*, 11:715–727, 1944.

[74] D. Kane. On the ranks of the 2-Selmer groups of twists of a given elliptic curve. *Algebra Number Theory*, 7(5):1253–1279, 2013.

[75] Y. Kitaoka. *Arithmetic of quadratic forms*, volume 106 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1993.

[76] Z. Klagsbrun, B. Mazur, and K. Rubin. Disparity in Selmer ranks of quadratic twists of elliptic curves. *Ann. of Math. (2)*, 178(1):287–320, 2013.

[77] Z. Klagsbrun, B. Mazur, and K. Rubin. A Markov model for Selmer ranks in families of twists. *Compos. Math.*, 150(7):1077–1106, 2014.

[78] V. Kovaleva. A note on the distribution of equivalence classes of random symmetric $p$-adic matrices. *arXiv preprint arXiv:2008.10732*, 2020.

[79] J. Laga. The average size of the 2-selmer group of a family of non-hyperelliptic curves of genus 3. *arXiv preprint arXiv:2008.13158*, 2021.

[80] 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.

[81] A. Lei and A. Poulin. On certain probabilistic properties of polynomials over the ring of $p$-adic integers. *Amer. Math. Monthly*, 127(6):519–529, 2020.

[82] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983. With a foreword by P. M. Cohn.

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

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

[85] J. Milnor and D. Husemoller. *Symmetric bilinear forms*. Springer-Verlag, New York-Heidelberg, 1973. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73.

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

[87] J. Nakagawa. Binary forms and orders of algebraic number fields. *Invent. Math.*, 97(2):219–235, 1989.

[88] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[89] nfdc23 (https://mathoverflow.net/users/81332/nfdc23). Non-archimedean QR factorization (Iwasawa decomposition). MathOverflow. URL: https://mathoverflow.net/q/255714 (version: 2016-11-27).

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

[91] B. Poonen and E. Rains. Self cup products and the theta characteristic torsor. *Math. Res. Lett.*, 18(6):1305–1318, 2011.

[92] B. Poonen and E. Rains. Random maximal isotropic subspaces and Selmer groups. *J. Amer. Math. Soc.*, 25(1):245–269, 2012.

[93] B. Poonen and E. F. Schaefer. Explicit descent for Jacobians of cyclic covers of the projective line. *J. Reine Angew. Math.*, 488:141–188, 1997.

[94] B. Poonen and M. Stoll. Most odd degree hyperelliptic curves have only one rational point. *Ann. of Math. (2)*, 180(3):1137–1166, 2014.

[95] M. Reid. *The complete intersection of two or more quadratics*. PhD thesis, University of Cambridge, 1972.

[96] I. Reiner. On the two-adic density of representations by quadratic forms. *Pacific J. Math.*, 6:753–762, 1956.

[97] B. Romano and J. A. Thorne. On the arithmetic of simple singularities of type $E$. *Res. Number Theory*, 4(2):Paper No. 21, 34, 2018.

[98] B. Romano and J. A. Thorne. $E_8$ and the average size of the 3-Selmer group of the Jacobian of a pointed genus-2 curve. *Proc. Lond. Math. Soc. (3)*, 122(5):678–723, 2021.

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

[100] P. Sarnak and A. Strömbergsson. Minima of Epstein's zeta function and heights of flat tori. *Invent. Math.*, 165(1):115–151, 2006.

[101] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[102] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[103] A. Shankar, A. Siad, A. Swaminathan, and I. Varma. Average 2-torsion in the ideal groups of rings associated to binary forms. 2020. In preparation.

[104] A. Shankar and J. Tsimerman. Counting $S_5$-fields with a power saving error term. *Forum Math. Sigma*, 2:Paper No. e13, 8, 2014.

[105] A. Shankar and X. Wang. Rational points on hyperelliptic curves having a marked non-Weierstrass point. *Compos. Math.*, 154(1):188–222, 2018.

[106] A. N. Shankar. 2-Selmer groups of hyperelliptic curves with marked points. *Trans. Amer. Math. Soc.*, 372(1):267–304, 2019.

[107] T. Shintani. On Dirichlet series whose coefficients are class numbers of integral binary cubic forms. *J. Math. Soc. Japan*, 24:132–188, 1972.

[108] A. Siad. Monogenic fields with odd class number part I: odd degree. *arXiv preprint arXiv:2011.08834*, 2020.

[109] A. Siad. Monogenic fields with odd class number part II: even degree. *arXiv preprint arXiv:2011.08842*, 2020.

[110] C. L. Siegel. The average measure of quadratic forms with given determinant and signature. *Ann. of Math. (2)*, 45:667–685, 1944.

[111] D. Simon. A "class group" obstruction for the equation $Cy^d = F(x, z)$. *J. Théor. Nombres Bordeaux*, 20(3):811–828, 2008.

[112] A. Smith. $2^\infty$-selmer groups, $2^\infty$-class groups, and Goldfeld's conjecture. *arXiv preprint arXiv:1702.02325*, 2017.

[113] M. Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.*, 98(3):245–277, 2001.

[114] M. Stoll and J. E. Cremona. Minimal models for 2-coverings of elliptic curves. *LMS J. Comput. Math.*, 5:220–243, 2002.

[115] M. Stoll and R. van Luijk. Explicit Selmer groups for cyclic covers of $\mathbb{P}^1$. *Acta Arith.*, 159(2):133–148, 2013.

[116] A. Swaminathan. Average 2-torsion in class groups of rings associated to binary $n$-ic forms. *arXiv preprint 2011.13578*, 2020.

[117] A. Swaminathan. Most integral odd-degree binary forms fail to properly represent a square. *arXiv preprint arXiv:1910.12409*, 2020.

[118] H. P. F. Swinnerton-Dyer. The effect of twisting on the 2-Selmer group. *Math. Proc. Cambridge Philos. Soc.*, 145(3):513–526, 2008.

[119] J. A. Thorne. $E_6$ and the arithmetic of a family of non-hyperelliptic curves of genus 3. *Forum Math. Pi*, 3:e1, 41, 2015.

[120] L. Y. Vulakh. Units in some families of algebraic number fields. *Trans. Amer. Math. Soc.*, 356(6):2325–2348, 2004.

[121] X. Wang. *Pencils of quadrics and Jacobians of hyperelliptic curves*. ProQuest LLC, Ann Arbor, MI, 2013. Thesis (Ph.D.)–Harvard University.

[122] X. Wang. Maximal linear spaces contained in the based loci of pencils of quadrics. *Algebr. Geom.*, 5(3):359–397, 2018.

[123] M. M. Wood. *Moduli spaces for rings and ideals*. ProQuest LLC, Ann Arbor, MI, 2009. Thesis (Ph.D.)–Princeton University.

[124] M. M. Wood. Rings and ideals parameterized by binary $n$-ic forms. *J. Lond. Math. Soc. (2)*, 83(1):208–231, 2011.

[125] M. M. Wood. Quartic rings associated to binary quartic forms. *Int. Math. Res. Not. IMRN*, (6):1300–1320, 2012.

[126] M. M. Wood. Parametrization of ideal classes in rings associated to binary forms. *J. Reine Angew. Math.*, 689:169–199, 2014.