Some Results on Binary Forms and Counting Rational Points on Algebraic Varieties

by

Stanley Yao Xiao

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Pure Mathematics

Waterloo, Ontario, Canada, 2016

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

In this thesis we study several problems related to the representation of integers by binary forms and counting rational points on algebraic varieties. In particular, we establish an asymptotic formula for $R_F(Z)$, the number of integers of absolute value up to Z which can be represented by a binary form F with integer coefficients, degree $d \geq 3$, and non-zero discriminant. We give superior results when $d = 3$ or 4, which completely resolves the cases considered by Hooley. We establish an asymptotic formula for the number of pairs $(x, y) \in \mathbb{Z}^2$ such that $F(x, y)$ is k-free, whenever F satisfies certain necessary conditions and $k > 7d/18$. Finally, we give various results on the arithmetic of certain cubic and quartic surfaces as well as general methods to estimate the number of rational points of bounded height on algebraic varieties. In particular, we give a bound for the density of rational points on del Pezzo surfaces of degree 2. These results depend on generalizations of Salberger's global determinant method in various settings.

Acknowledgements

I would like to thank my thesis advisor, Professor Cameron Leigh Stewart, for his generous support over the course of my studies and for his meticulous and scrupulous efforts in improving the content of my results. Without his help this thesis surely would have been impossible. I also thank him for selecting the problem of power-free values of binary forms for me to work on initially; without this initial step none of the results contained in this thesis would have been possible.

I also thank the University of Waterloo and the Government of Ontario for providing funding for me during the course of my studies. The Ontario Graduate Scholarship in particular was very helpful for me and allowed me to be financially secure during my studies.

Next I thank the following individuals for their particular contributions to making my doctoral studies a success. I thank Dr. Shuntaro Yamagishi for always willing to be an enthusiastic participant in discussions regarding number theory and other topics during our time together as graduate students, Justin Scarfy for his companionship at various conferences and his partnership in writing the notes for the CRM program on the arithmetic of elliptic curves, and Professor David McKinnon who provided me with nice conversations and important support in the form of reference letters. I would also like to thank all other members of the Department of Pure Mathematics for helping to make my graduate studies a most excellent experience in my life.

Last but most certainly not least, I would like to thank my family and my wife Amy in particular for supporting me through the ups and downs of my life during the course of my PHD studies.

Dedication

This thesis is dedicated to my family. To my parents, whose lifetime of hard work and loving care to me was necessary for me to become the person I am today. To my wife, who showed me how wonderful life with someone could be.

Table of Contents

Chapter 1

Introduction

In this thesis we will record some progress made on several problems concerning binary forms and counting rational points on certain algebraic varieties. A *binary form* is a homogeneous polynomial in two variables. We will describe progress made on answering the following question: Given a binary form F with integer coefficients, how many integers n in an interval $[-Z, Z]$ can be written in the form $F(x, y) = n$ for some integers x and y? If $F(x, y) = n$ has a solution in integers x and y, we say that n is *representable* by F.

This question is difficult to answer. If instead we count the integers representable by F *with repetition*, then Gauss was able to prove an asymptotic formula in the case of positive definite binary quadratic forms. Let us write

$$N_F(Z) = \#\{(x, y) \in \mathbb{Z}^2 : |F(x, y)| \leq Z, F(x, y) \neq 0\}. \tag{1.0.1}$$

Gauss showed that for any positive definite binary quadratic form F, there exists a positive number $A_1(F)$ such that

$$N_F(Z) \sim A_1(F)Z. \tag{1.0.2}$$

Put

$$R_F(Z) = \#\{n \in \mathbb{Z} : |n| \leq Z, \exists (x, y) \in \mathbb{Z}^2 \text{ s.t. } F(x, y) = n\}. \tag{1.0.3}$$

Landau showed that for a positive definite binary quadratic form F, there exists a positive number $A_2(F)$ such that

$$R_F(Z) \sim A_2(F)Z(\log Z)^{-1/2}.$$

Thus, most integers cannot be represented by F, but on average each integer represented by F has many representations.

Mahler showed in [79] that there is an analogous asymptotic formula to (1.0.2) for forms of degree $d \geq 3$. He proved that for F an irreducible binary form of degree $d \geq 3$, we have

$$N_F(Z) = A_F Z^{\frac{2}{d}} + O_F\left(Z^{\frac{1}{d-1}}\right), \tag{1.0.4}$$

where A_F denotes the area of the region

$$\{(x, y) \in \mathbb{R}^2 : |F(x, y)| \leq Z\}. \tag{1.0.5}$$

Erdős and Mahler showed in [40] that contrary to the size difference between $N_F(Z)$ and $R_F(Z)$ for positive definite quadratic forms, the size of $R_F(Z)$ is not dramatically smaller than $N_F(Z)$. They showed that there exist positive numbers C_1, C_2 such that whenever $Z > C_1$, we have

$$R_F(Z) > C_2 Z^{\frac{2}{d}}.$$

A natural question to ask is whether an exact asymptotic formula holds for $R_F(Z)$. It would take almost thirty years after Erdős and Mahler's paper before the first instance of such an asymptotic formula was established. In [64], Hooley showed that for an irreducible binary cubic form F given by

$$F(x, y) = b_3x^3 + 3b_2x^2y + 3b_1xy^2 + b_0y^3,$$

where the discriminant $\Delta(F)$ of F is not a square, the asymptotic formula

$$R_F(Z) = A_F Z^{\frac{2}{3}} + O_F\left(Z^{\frac{2}{3}}(\log\log Z)^{-\frac{1}{600}}\right)$$

holds. In [68], Hooley showed that an asymptotic formula holds for $R_F(Z)$ when F is a binary quartic form of the shape

$$F(x, y) = ax^4 + 2bx^2y^2 + cy^4.$$

In particular, he showed that

$$R_F(Z) = \frac{1}{4}\begin{cases} A_F Z^{\frac{1}{2}} + O\left(Z^{\frac{18}{37}+\varepsilon}\right) & \text{if } a/c \text{ is not a perfect 4th power of a rational,} \\ \left(1 - \dfrac{1}{2AC}\right) A_F Z^{\frac{1}{2}} + O\left(Z^{\frac{18}{37}+\varepsilon}\right) & \text{if } a/c = A^4/C^4 \text{ for } A, C \in \mathbb{N}. \end{cases}$$

Moreover, he mentioned that the value of A_F is given in terms of complete elliptic integrals of the first kind. This point was expanded upon by M. A. Bean in [6].

In 2000, Hooley obtained in [69] the asymptotic formula for $R_F(Z)$ for binary cubic forms

$$F(x,y) = b_3x^3 + 3b_2x^2y + 3b_1xy^2 + b_0y^3$$

such that $\Delta(F) = k^2$ with k a positive integer. In this case we need to consider the Hessian $q_F(x,y)$ of F, which is given by

$$q_F(x,y) = (b_2^2 - b_3b_1)x^2 + (b_2b_1 - b_3b_0)xy + (b_1^2 - b_2b_0)y^2,$$

and we set

$$A = b^2 - b_3b_1, B = b_2b_1 - b_3b_0, C = b_1^2 - b_2b_0.$$

Put

$$m = \frac{k}{\gcd(A,B,C)}.$$

Then Hooley showed in [69] that there exists a positive number γ such that

$$R_F(Z) = \left(1 - \frac{2}{3m}\right) A_F Z^{\frac{2}{3}} + O\left(Z^{\frac{2}{3}}(\log Z)^{-\gamma}\right).$$

More specifically, he showed that A_F is given in terms of the discriminant $\Delta(F)$ of F and the Gamma function Γ; see Chapter 3.

Following Hooley's paradigm, one notices that in order to deduce an asymptotic formula for $R_F(Z)$ from Mahler's theorem (1.0.4) one has to do two things. First, one has to show that most integers represented by F are *essentially represented*. We say an integer n is essentially represented by F if whenever $F(u,v) = F(u',v') = n$, there exists a matrix

$$T = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})$$

such that

$$T\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} u' \\ v' \end{pmatrix},$$

and

$$F(t_1x + t_2y, t_3x + t_4y) = F(x,y) \tag{1.0.6}$$

for all $x, y \in \mathbb{R}$. Whenever (1.0.6) holds, we say that T is in $\operatorname{Aut} F$, the ($\mathrm{GL}_2(\mathbb{Q})$) *automorphism group* of F. This is very difficult and the bulk of Hooley's papers [64], [68], and [69] are dedicated to show that this is true for the cases he considered.

The second component, which is the most novel aspect of Hooley's second paper on binary cubic forms [69], is to determine the influence of the structure of the automorphism group $\operatorname{Aut} F$ on determining the asymptotic formula for $R_F(Z)$. Part of the reason for Hooley's success in [64], [68], and [69] is that the group structures of those $\operatorname{Aut} F$ he considered are relatively simple. In general, this can be quite complicated.

Heath-Brown, in [53], provided a pathway to establish an asymptotic formula for $R_F(Z)$ for all binary forms F by treating the difficult problem of bounding non-essential representations in great generality. He showed that for all binary forms with non-zero discriminant (in fact, his theorem even covers some cases where the discriminant vanishes) of degree $d \geq 3$, 100% of the integers representable by F are essentially represented. He did this using a geometric argument and remarked that the p-adic determinant method, which he introduced in the same paper for different purposes, can possibly be used to improve on this bound. This improvement was achieved by Salberger in [93], where he used his global determinant method in place of Heath-Brown's geometric arguments. Salberger's work helped us achieve the results in Chapter 2.

Combining Heath-Brown's argument to control the non-essentially represented integers and by determining the exact relation between $\operatorname{Aut} F$ and the asymptotic formula for $R_F(Z)$, C. L. Stewart and I in [100] were able to prove the following:

Theorem 1.0.1. *Let $d \geq 3$ be an integer and let $\mathcal{G}$ be a finite subgroup of $\mathrm{GL}_2(\mathbb{Q})$. Then there exists a positive number $\beta_d < 2/d$ and a positive rational number $W_{\mathcal{G}}$ such that for all positive numbers $\varepsilon > 0$ and binary forms F of degree d, integer coefficients, non-zero discriminant and $\operatorname{Aut} F = \mathcal{G}$, the asymptotic formula*

$$R_F(Z) = W_{\mathcal{G}} A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right)$$

holds.

The quantity β_d can be taken as in (2.0.7).

Observe that the number $W_{\mathcal{G}}$ depends only on the group $\mathcal{G}$ and not on F. If we put the asymptotic formula in Theorem 1.0.1 as

$$R_F(Z) \sim C_F Z^{\frac{2}{d}},$$

then whenever $F, \mathcal{F}$ are two binary forms with integer coefficients and non-zero discriminant such that $\operatorname{Aut} F = \operatorname{Aut} \mathcal{F}$, then the equality

$$C_F/A_F = C_{\mathcal{F}}/A_{\mathcal{F}}$$

holds. Note that we require *equality* of automorphism groups, not merely isomorphism.

Theorem 1.0.1 does not fully generalize Hooley's results in [64], [68], and [69]. In particular, we did not in [100] demonstrate a way to determine $\operatorname{Aut} F$ given F. We believe that for $d \geq 5$ it is genuinely difficult to determine $\operatorname{Aut} F$ for the generic binary form F of degree d, much like the computation of the Galois group of an arbitrary binary form F. In [106], we showed that one can fully generalize Hooley's results when the degree of F is 3 or 4. Indeed, we proved the following:

Theorem 1.0.2. *Let F be a binary form of degree $d = 3$ or 4. Then one can compute $\operatorname{Aut} F$ explicitly in terms of the invariants and covariants of the $\mathrm{GL}_2(\mathbb{Z})$-action on F via substitution. Moreover, the value of A_F in this case can be given explicitly in terms of the Gamma function and complete elliptic integrals of the first kind.*

Theorem 1.0.2 completely resolves the problem of finding asymptotic formula for $R_F(Z)$ for degree 3 and 4. The covariants and invariants of binary cubic and quartic forms will be discussed in detail in Chapter 3. For now, we shall note that the only invariant of cubic forms is the discriminant $\Delta(F)$, and that quartic forms have two basic invariants usually denoted by $I(F)$ and $J(F)$.

The key to proving Theorem 1.0.2 is to find explicit generators of $\operatorname{Aut}_{\mathbb{C}} F$, the subgroup of $\mathrm{GL}_2(\mathbb{C})$ which fixes F via substitution, and then determine when these generators lie in $\mathrm{GL}_2(\mathbb{Q})$. In doing so, we were able to prove the following result on certain cubic and quartic surfaces defined by binary cubic and quartic forms:

Theorem 1.0.3. *Let F be a binary cubic or quartic form with integer coefficients and non-zero discriminant. Let X be the surface in $\mathbb{P}^3$ defined by the equation*

$$F(x_1, x_2) - F(x_3, x_4) = 0.$$

Then we have:

(a) If F is a cubic form, then the 27 lines lying on X are all defined over a field of degree at most 12 over $\mathbb{Q}$.

(b) If F is a quartic form, then X contains:

1. *32 lines if $I(F), J(F)$ are both non-zero;*
2. *48 lines if $J(F) = 0$; and*
3. *64 lines if $I(F) = 0$.*

In all cases, the lines of the quartic surface X are all defined over a field of degree at most 192 over $\mathbb{Q}$.

The cubic case of Theorem 1.0.3 should be compared with the generic situation, where the field of definition of the 27 lines on a cubic surface defined over $\mathbb{Q}$ has Galois group isomorphic to the Weyl group of the E_6 root system, which has order $51,840$. In other words, these cubic surfaces are extremely special. The quartic case should be compared with the fact that the generic quartic surface contains no lines, so again, these surfaces are very special.

A significant portion of our thesis work is devoted to improving Heath-Brown's p-adic determinant method, which he introduced in [53]. It is a powerful method which gives good upper bounds for the density of rational points on algebraic varieties. It is especially useful in cases where other approaches, such as the circle method of Hardy and Littlewood, are of little use. Heath-Brown's p-adic version of the determinant method is itself an extension of the original real-analytic determinant method of Bombieri and Pila, introduced in 1989 in [14]. Heath-Brown's version can be applied to arbitrary projective varieties (as was shown later by Browning, Heath-Brown, and Salberger in [22]), whereas Bombieri and Pila's version seemed to rely heavily on the geometry of $\mathbb{R}^2$ and resisted generalization to higher dimensions. In [92] and [93], Salberger improved upon Heath-Brown's p-adic determinant method by introducing various machinery and language from algebraic geometry. The so-called *global determinant method*, introduced by Salberger in [93], is a particularly powerful improvement and is the most efficient version of the determinant method known so far. It has had some striking consequences in diophantine geometry; see [103] for example. Our contribution to the determinant method story is that we were able to generalize the p-adic determinant method to certain *weighted projective spaces*. Since the statement of these improvements are very technical and involved, we refer the interested reader to Chapter 4 for the details and instead introduce the three most interesting consequences of our improvements here.

The first consequence of our generalization of the p-adic determinant method is an improvement to the problem of proving that suitable binary forms F take on k-free values

infinitely often. We begin by discussing the square-free case. A long standing problem, dating back to Estermann [41], is the question of how often a given polynomial takes on square-free values. Certainly, some trivial obstructions have to be cleared in order for the question to be well-posed. We will say that a polynomial $f(x_1, \cdots, x_k)$ with integer coefficients is *admissible* if for all primes p, there exists an integer k-tuple $\mathbf{x}_p = (x_1^{(p)}, \cdots, x_k^{(p)})$ such that p^2 does not divide $f(\mathbf{x}_p)$. There are only a few cases where it is known unconditionally that f takes on infinitely many square-free values, which we summarize below:

- If $k = 1$, then it is known that $f(x)$ takes on infinitely many square-free values only when each irreducible component of f has degree at most 3. The case $f(x) = x^2 + 1$ was done by Estermann in [41] and the general degree 2 case by Ricci in [90], while the degree 3 case was first established by Erdős in [39] and later improved by Hooley in [63].

- If $k = 2$, then one can reduce to the single variable case by fixing one of x and y in $f(x, y)$. The cases where one can do better than the single variable case include admissible binary forms F such that each irreducible factor of F has degree at most 6; this was done by Greaves in [48], and those binary polynomials f which splits completely into linear factors over $\overline{\mathbb{Q}}$; this is due to Hooley in [70] and [71].

- If F is a highly symmetric polynomial, that is, if F is the *discriminant polynomial* of certain algebraic number fields, then it is known that F takes on square-free values infinitely often. The case of discriminant polynomials for cubic, quartic, and quintic fields is solved by Bhargava in [11].

Aside from the unconditional results noted above, it is known under the *abc*-conjecture that admissible f takes on infinitely many square-free values due to the work of Granville [47], Poonen [86], and Murty-Pasten [81]. Thus, the question is either resolved or widely open depending on the status of Mochizuki's purported proof of the *abc*-conjecture.

Nevertheless, we have made progress on a related and easier problem by considering *k-free values* instead. In this direction, we have improved upon a series of results due to Filaseta [43] and Browning [21]. In particular, we showed as a consequence of our extension of the global determinant method to weighted projective spaces, the following result concerning k-free values of binary forms:

Theorem 1.0.4. *Let $F(x, y)$ be a binary form with non-zero discriminant of degree $D \geq 2$ with integer coefficients. Let $k \geq 2$ be an integer. Suppose that for each prime p, there*

exists a pair of integers (x_0, y_0) *such that* p^k *does not divide* $F(x_0, y_0)$. *Let* d *denote the largest degree of an irreducible factor* f *of* F *over* $\mathbb{Q}$. *Then whenever*

$$k > \min\left\{\frac{7d}{18}, \left\lceil\frac{d}{2}\right\rceil - 2\right\}, \tag{1.0.7}$$

there exists a positive number $C_{F,k}$ *depending only on* F *and* k *such that the number of integer pairs* (x, y) *with* $\max\{|x|, |y|\} \leq B$ *such that* $F(x, y)$ *is* k*-free is asymptotic to*

$$C_{F,k}B^2 + O\left(\frac{B^2}{\log^{\delta} B}\right), \tag{1.0.8}$$

where $\delta = 0.7043$ *if* $k = 2, d = 6$ *and* $\delta = 1$ *otherwise.*

We were also able to extend a theorem of Stewart and Top in [99] in the cases where Theorem 1.0.4 holds. Namely we proved the following:

Theorem 1.0.5. *Let* $k \geq 2$. *Let* $F(x, y)$ *be a binary form of degree* $D \geq 3$ *with integer coefficients and non-zero discriminant, with no fixed* k*-th power prime divisor. Let* d *be the largest degree of an irreducible factor of* F *over* $\mathbb{Q}$ *and suppose that*

$$k > \min\left\{\frac{7d}{18}, \left\lceil\frac{d}{2}\right\rceil - 2\right\}.$$

Then there exist positive real numbers C_1 *and* C_2, *which depend on* F *and* k, *such that if* $B > C_1$, *then*

$$R_{F,k}(B) > C_2 B^{2/D}.$$

Theorem 1.0.5 can be thought of as an extension of the Erdős-Mahler theorem in [40] as it asserts that a positive proportion of integers represented by F are k-free, whenever an analogous result to Mahler's theorem (1.0.4) can be asserted. It would be of interest to establish a theorem analogous to Theorem 1.0.1 for k-free values represented by binary forms.

The last result we mention is unrelated to binary forms and is a consequence of our weighted version of the p-adic determinant method. It was noted by T.D. Browning, via personal communication, that our generalization of the p-adic determinant method may have consequences on bounding the density of rational points on certain algebraic surfaces, namely the so-called *del Pezzo surfaces*. It is known that del Pezzo surfaces have degree between 1 and 9, and for those del Pezzo surfaces of degree $3 \leq d \leq 9$, the

arithmetic information of rational points is fairly well understood, while knowledge of del Pezzo surfaces of degree 1 and 2 is scarce. We shall note our improvement in the case of degree 2 del Pezzo surfaces. By a del Pezzo surface of degree 2, we mean a surface defined by

$$X : y^2 = f(x_1, x_2, x_3), \tag{1.0.9}$$

where f is a ternary quartic form. We shall define the height $H(\mathbf{x})$ of a rational point $\mathbf{x} = (y, x_1, x_2, x_3)$ on X to be $\max\{H(x_1), H(x_2), H(x_3)\}$, where $H(q)$ is the naive height of a rational number. We then have the following:

Theorem 1.0.6. *Let X be a del Pezzo surface of degree 2 given by (1.0.9) for a ternary quartic form f with integer coefficients and irreducible over $\overline{\mathbb{Q}}$. Then the number of rational points $\mathbf{x}$ on X for which $H(\mathbf{x}) \leq B$ is at most*

$$O_{d,\varepsilon}\left(B^{\frac{36}{17}+\varepsilon}\right).$$

This is comparable to the result by Broberg [18], where he obtains the exponent $9/4$, and unpublished work of Salberger where he claims to have obtained the exponent $3/\sqrt{2}$.

Finally we mention that for the sake of brevity and thematic coherence we have made a few choices to curate the content of this thesis. One particular piece of work that we have done which did not make the final version of this thesis is our joint work with Dr. Shuntaro Yamagishi in [107].

Our work on classifying the automorphism groups of binary quartic forms in Chapter 3 (see also [106]) has enabled us to count binary quartic forms whose automorphism group contains an element which, up to scaling over $\mathbb{C}$, has co-prime integer entries. This allows us to count binary quartic forms whose Galois group is a subgroup of the dihedral group $\mathcal{D}_4$. Currently, this is an active joint project with Dr. Cindy Tsang which we hope to complete soon.

The content of Chapter 2 is roughly the same as that of our joint paper with Professor C. L. Stewart [100], where we established the asymptotic formula for $R_F(Z)$. Theorem 1.0.1 will be resolved there. Chapter 3 is devoted to binary cubic and quartic forms and contains the proofs of Theorems 1.0.2 and 1.0.3. The content of Chapter 3 is roughly the same as our preprint [106]. Chapter 4 contains expository material on the p-adic determinant method and the statements and proofs of the main theorems of the global

p-adic determinant method for weighted projective spaces. Finally, Chapter 5 gives several consequences of our generalization of the determinant method including consequences for k-free values of binary forms and del Pezzo surfaces of degree 2. Much of the content from Chapters 4 and 5 are in [105].

Chapter 2

Representation of integers by binary forms

The content of this chapter is joint work with my advisor Professor C. L. Stewart; see [100].

Let F be a binary form with integer coefficients, non-zero discriminant $\Delta(F)$, and degree d with $d \geq 2$. For any positive number Z let $\mathcal{R}_F(Z)$ denote the set of non-zero integers h with $|h| \leq Z$ for which there exist integers x and y with $F(x,y) = h$. For any set $\mathcal{S}$, denote the cardinality of $\mathcal{S}$ by $|\mathcal{S}|$, and put $R_F(Z) = |\mathcal{R}_F(Z)|$. There is an extensive literature, going back to the foundational work of Fermat, Lagrange, Legendre, and Gauss [45], on the set $\mathcal{R}_F(Z)$ and the growth of $R_F(Z)$ when F is a binary quadratic form; see [24], [25], and [27] for more recent treatments of these topics. For forms of higher degree much less is known. In 1938 Erdős and Mahler [40] proved that if F is irreducible over $\mathbb{Q}$ and $d \geq 3$, then there exist positive numbers c_1 and c_2, which depend on F, such that

$$R_F(Z) > c_1 Z^{\frac{2}{d}}$$

for $Z > c_2$.

Put

$$A_F = \mu(\{(x,y) \in \mathbb{R}^2 : |F(x,y)| \leq 1\}) \tag{2.0.1}$$

where μ denotes the area of a set in $\mathbb{R}^2$. In 1967 Hooley [64] determined the asymptotic growth rate of $R_F(Z)$ when F is an irreducible cubic binary form with discriminant which is not a square. He proved that

$$R_F(Z) = A_F Z^{\frac{2}{3}} + O\left(Z^{\frac{2}{3}}(\log\log Z)^{-\frac{1}{600}}\right). \tag{2.0.2}$$

In 2000 Hooley [69] treated the case when the discriminant is a perfect square. Suppose that

$$F(x,y) = b_3x^3 + b_2x^2y + b_1xy^2 + b_0y^3.$$

The Hessian covariant of F is

$$q_F(x) = Ax^2 + Bx + C,$$

where

$$A = b_2^2 - 3b_3b_1, \ , B = b_2b_1 - 9b_3b_0, \text{ and } C = b_1^2 - 3b_2b_0.$$

Put

$$m = \frac{\sqrt{\Delta(F)}}{\gcd(A,B,C)}. \tag{2.0.3}$$

Hooley proved that if F is cubic, irreducible, and $\Delta(F)$ is a square then there is a positive number γ such that

$$R_F(Z) = \left(1 - \frac{2}{3m}\right) A_F Z^{\frac{2}{3}} + O\left(Z^{\frac{2}{3}}(\log Z)^{-\gamma}\right). \tag{2.0.4}$$

We remark that if F is a binary cubic form then

$$|\Delta(F)|^{\frac{1}{6}} A_F = \begin{cases} \dfrac{3\Gamma^2(1/3)}{\Gamma(2/3)} & \text{if } \Delta(F) > 0, \\ \\ \dfrac{\sqrt{3}\Gamma^2(1/3)}{\Gamma(2/3)} & \text{if } \Delta(F) < 0, \end{cases}$$

where $\Gamma(s)$ denotes the gamma function. In [6] Bean gives a simple representation for A_F when F is a quartic form.

Hooley [69] also studied quartic forms of the shape

$$F(x,y) = ax^4 + 2bx^2y^2 + cy^4.$$

Let $\varepsilon > 0$. He proved that if a/c is not the fourth power of a rational number then

$$R_F(Z) = \frac{A_F}{4} Z^{\frac{1}{2}} + O_{F,\varepsilon}\left(Z^{\frac{18}{37}+\varepsilon}\right). \tag{2.0.5}$$

Further if $a/c = A^4/C^4$ with A and C co-prime positive integers then

$$R_F(Z) = \frac{A_F}{4}\left(1 - \frac{1}{2AC}\right) Z^{\frac{1}{2}} + O_{F,\varepsilon}\left(Z^{\frac{18}{37}+\varepsilon}\right). \tag{2.0.6}$$

In addition to these results, Browning [21], Greaves [48], Heath-Brown [55], Hooley [65], [66], [67], Skinner and Wooley [96] and Wooley [104] have obtained asymptotic estimates for $R_F(Z)$ when $F(x, y)$ is of the form $x^d + y^d$ with $d \geq 3$. Furthermore, Bennett, Dummigan, and Wooley [9] have obtained an asymptotic estimate for $R_F(Z)$ when $F(x, y) = ax^d + by^d$ with $d \geq 3$ and a and b non-zero integers for which a/b is not the d-th power of a rational number.

Put

$$\beta_d = \begin{cases} \dfrac{12}{19} & \text{if } d = 3 \\ \dfrac{3}{(d-2)\sqrt{d}+3} & \text{if } 4 \leq d \leq 8 \\ \dfrac{1}{d-1} & \text{if } d \geq 9. \end{cases} \tag{2.0.7}$$

We shall prove the following result.

Theorem 2.0.1. *Let F be a binary form with integer coefficients, non-zero discriminant, and degree $d \geq 3$. Let $\varepsilon > 0$. There exists a positive number C_F such that*

$$R_F(Z) = C_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right), \tag{2.0.8}$$

where β_d is given by (2.0.7).

Our proof of Theorem 2.0.1 depends on some results of Salberger in [93] and [94], which are based on a refinement of Heath-Brown's p-adic determinant method in [53], as well as a classical result of Mahler [79]. Indeed Heath-Brown remarks in [53] that Theorem 8 in [53] should enable one to deduce an asymptotic formula for $R_F(Z)$.

Let A be an element of $\mathrm{GL}_2(\mathbb{Q})$ with

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}.$$

Put $F_A(x, y) = F(a_1x + a_2y, a_3x + a_4y)$. We say that A fixes F if $F_A = F$. The set of $A \in \mathrm{GL}_2(\mathbb{Q})$ which fix F is the *automorphism group* of F and we shall denote it by $\mathrm{Aut}\, F$. Let G_1 and G_2 be subgroups of $\mathrm{GL}_2(\mathbb{Q})$. We say that they are equivalent under conjugation if there is an element $T \in \mathrm{GL}_2(\mathbb{Q})$ such that $G_1 = TG_2T^{-1}$.

The positive number C_F in (2.0.8) is a rational multiple of A_F and the rational multiple depends on $\mathrm{Aut}\, F$. There are 10 equivalence classes of finite subgroups of $\mathrm{GL}_2(\mathbb{Q})$ under $\mathrm{GL}_2(\mathbb{Q})$-conjugation to which $\mathrm{Aut}\, F$ might belong and we give a representative of each equivalence class together with its generators in Table 1.

Table 1

Group	Generators	Group	Generators
$\mathbf{C}_1$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\mathbf{D}_1$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$\mathbf{C}_2$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\mathbf{D}_2$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
$\mathbf{C}_3$	$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$	$\mathbf{D}_3$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$
$\mathbf{C}_4$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\mathbf{D}_4$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
$\mathbf{C}_6$	$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$	$\mathbf{D}_6$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$

Since the matrix $-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ is in $\mathrm{Aut}\, F$ if and only if the degree of F is even, we see from an examination of Table 1 that if the degree of F is odd then $\mathrm{Aut}\, F$ is equivalent

to one of $\mathbf{C}_1, \mathbf{C}_3, \mathbf{D}_1$, and $\mathbf{D}_3$ and if the degree of F is even then $\operatorname{Aut} F$ is equivalent to one of $\mathbf{C}_2, \mathbf{C}_4, \mathbf{C}_6, \mathbf{D}_2, \mathbf{D}_4$, and $\mathbf{D}_6$.

Note that the table has fewer entries than Table 1 of [98] which gives representatives for the equivalence classes of finite subgroups of $\mathrm{GL}_2(\mathbb{Z})$ under $\mathrm{GL}_2(\mathbb{Z})$-conjugation since for $i = 1, 2, 3$ the groups $\mathbf{D}_i$ and $\mathbf{D}_i^*$ are equivalent under conjugation in $\mathrm{GL}_2(\mathbb{Q})$ but not in $\mathrm{GL}_2(\mathbb{Z})$. Further every finite subgroup of $\mathrm{GL}_2(\mathbb{Q})$ is conjugate to a finite subgroup of $\mathrm{GL}_2(\mathbb{Z})$, see [84].

Let Λ be the sublattice of $\mathbb{Z}^2$ consisting of $(u, v) \in \mathbb{Z}^2$ for which $A\begin{pmatrix} u \\ v \end{pmatrix}$ is in $\mathbb{Z}^2$ for all $A \in \operatorname{Aut} F$, and put

$$m = d(\Lambda), \tag{2.0.9}$$

where $d(\Lambda)$ denotes the determinant of Λ. Note that $m = 1$ when $\operatorname{Aut} F$ is equal to either $\mathbf{C}_1$ or $\mathbf{C}_2$. Observe that since $\mathbf{C}_1$ and $\mathbf{C}_2$ contain only diagonal matrices, their conjugacy classes over $\mathrm{GL}_2(\mathbb{Q})$ consist only of themselves.

When $\operatorname{Aut} F$ is conjugate to $\mathbf{D}_3$ it has three subgroups G_1, G_2 and G_3 of order 2 with generators A_1, A_2, A_3, and one, G_4 say, of order 3 with generator A_4. Let $\Lambda_i = \Lambda(A_i)$ be the sublattice of $\mathbb{Z}^2$ consisting of $(u, v) \in \mathbb{Z}^2$ for which $A_i\begin{pmatrix} u \\ v \end{pmatrix}$ is in $\mathbb{Z}^2$ and put

$$m_i = d(\Lambda_i) \tag{2.0.10}$$

for $i = 1, 2, 3, 4$. We remark that m_4 is well defined since, by (2.2.7), Λ_4 does not depend on the choice of generator A_4.

When $\operatorname{Aut} F$ is conjugate to $\mathbf{D}_4$ there are three subgroups G_1, G_2, and G_3 of order 2 of $\operatorname{Aut} F/\{\pm I\}$. Let Λ_i be the sublattice of $\mathbb{Z}^2$ consisting of $(u, v) \in \mathbb{Z}^2$ for which $A\begin{pmatrix} u \\ v \end{pmatrix}$ is in $\mathbb{Z}^2$ for A in a generator of G_i and put

$$m_i = d(\Lambda_i) \tag{2.0.11}$$

for $i = 1, 2, 3$.

Finally when $\operatorname{Aut} F$ is conjugate to $\mathbf{D}_6$ there are three subgroups G_1, G_2, and G_3 of order 2 and one, G_4 say, of order 3 in $\operatorname{Aut} F/\{\pm I\}$. Let A_i be in a generator of G_i for

$i = 1, 2, 3, 4$, let $\Lambda_i = \Lambda(A_i)$ be the sublattice of $\mathbb{Z}^2$ consisting of $(u, v) \in \mathbb{Z}^2$ for which $A_i \begin{pmatrix} u \\ v \end{pmatrix}$ is in $\mathbb{Z}^2$ and put

$$m_i = d(\Lambda_i) \tag{2.0.12}$$

for $i = 1, 2, 3, 4$.

Theorem 2.0.2. *The positive number C_F in the statement of Theorem 2.0.1 is equal to $W_F A_F$ where A_F is given by (2.0.1) and W_F is given by the following table:*

Rep(F)	W_F	Rep(F)	W_F
$\mathbf{C}_1$	1	$\mathbf{D}_1$	$1 - \frac{1}{2m}$
$\mathbf{C}_2$	$\frac{1}{2}$	$\mathbf{D}_2$	$\frac{1}{2}\left(1 - \frac{1}{2m}\right)$
$\mathbf{C}_3$	$1 - \frac{2}{3m}$	$\mathbf{D}_3$	$1 - \frac{1}{2m_1} - \frac{1}{2m_2} - \frac{1}{2m_3} - \frac{2}{3m_4} + \frac{4}{3m}$
$\mathbf{C}_4$	$\frac{1}{2}\left(1 - \frac{1}{2m}\right)$	$\mathbf{D}_4$	$\frac{1}{2}\left(1 - \frac{1}{2m_1} - \frac{1}{2m_2} - \frac{1}{2m_3} + \frac{3}{4m}\right)$
$\mathbf{C}_6$	$\frac{1}{2}\left(1 - \frac{2}{3m}\right)$	$\mathbf{D}_6$	$\frac{1}{2}\left(1 - \frac{1}{2m_1} - \frac{1}{2m_2} - \frac{1}{2m_3} - \frac{2}{3m_4} + \frac{4}{3m}\right)$

Here Rep(F) *denotes a representative of the equivalence class of* Aut F *under* $\mathrm{GL}_2(\mathbb{Q})$ *conjugation and m, m_1, m_2, m_3, m_4 are defined in (2.0.9),(2.0.10), (2.0.11), and (2.0.12).*

We remark, see Lemma 2.2.2, that if Aut F is equivalent to $\mathbf{D}_4$ then $m = \mathrm{lcm}(m_1, m_2, m_3)$, the least common multiple of m_1, m_2, and m_3, and if Aut F is equivalent to $\mathbf{D}_3$ or $\mathbf{D}_6$ then $m = \mathrm{lcm}(m_1, m_2, m_3, m_4)$.

Observe that if F is a binary form with $F(1, 0) \neq 0$ and $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$ is in Aut F then A acts on the roots of F by sending a root α to $\dfrac{a_1\alpha + a_2}{a_3\alpha + a_4}$. If A fixes a root α then

$$a_3\alpha^2 + (a_4 - a_1)\alpha + a_2 = 0.$$

If F is an irreducible cubic then α has degree 3 and so

$$a_3 = a_4 - a_1 = a_2 = 0,$$

thus

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

But since F has degree 3 we see that $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Therefore the only element of $\operatorname{Aut} F$ which fixes a root of F is the identity matrix I.

If A in $\operatorname{Aut} F$ does not fix a root it must permute the roots cyclically and thus must have order 3. Further, since any element in $\operatorname{Aut} F$ of order 2 would fix a root of F, we find that $\operatorname{Aut} F$ is $\mathrm{GL}_2(\mathbb{Q})$-conjugate to $\mathbf{C}_3$, say $\operatorname{Aut} F = T\mathbf{C}_3T^{-1}$ with $T \in \mathrm{GL}_2(\mathbb{Q})$. Forms invariant under $\mathbf{C}_3$ are of the form

$$G(x, y) = ax^3 + bx^2y + (b - 3a)xy^2 - ay^3$$

with a and b integers; see (74) of [98]. Notice that

$$\Delta(G) = (b^2 - 3ab + 9a^2)^2.$$

Then $F = G_T$ for some G invariant under $\mathbf{C}_3$ and so

$$\Delta(F) = (\det T)^6 \Delta(G).$$

We conclude that if F is an irreducible cubic form with discriminant not a square then $\operatorname{Aut} F$ is $\mathbf{C}_1$ and so $W_F = 1$ and Hooley's result (2.0.2) follows from Theorems 2.0.1 and 2.0.2. When $\operatorname{Aut} F$ is equivalent to $\mathbf{C}_3$ then $W_F = 1 - \dfrac{2}{3m}$ where m is the determinant of the lattice consisting of $(u, v) \in \mathbb{Z}^2$ for which $A\begin{pmatrix} u \\ v \end{pmatrix}$ is in $\mathbb{Z}^2$ for all $A \in \operatorname{Aut} F$. By Lemma 2.2.2 it suffices to consider the lattice consisting of $(u, v) \in \mathbb{Z}^2$ for which $A\begin{pmatrix} u \\ v \end{pmatrix}$ is in $\mathbb{Z}^2$ for a generator A of $\operatorname{Aut} F$. Hooley has shown in [70] that the determinant of the lattice is m and so (2.0.4) follows from Theorems 2.0.1 and 2.0.2.

Now if $F(x, y) = ax^4 + bx^2y^2 + cy^4$ and the discriminant of F is non-zero then $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_2$ unless $a/c = A^4/C^4$ with A and C coprime positive integers. In this

case Aut F is equivalent to $\mathbf{D}_4$. In the first instance $m = 1$ and $W_F = \dfrac{1}{4}$ and so we recover Hooley's estimate (2.0.5). In the second case $m_1 = 1$ and $m_2 = m_3 = m = AC$ and so

$$W_F = \frac{1}{4}\left(1 - \frac{1}{2AC}\right).$$

which gives (2.0.6).

If follows from the analysis on page 818 of [98] that when F is a binary cubic form with non-zero discriminant Aut F is equivalent to $\mathbf{C}_1, \mathbf{C}_3$ or $\mathbf{D}_3$ whereas if F is a binary quartic form with non-zero discriminant Aut F is equivalent to $\mathbf{C}_2, \mathbf{C}_4, \mathbf{D}_2$ or $\mathbf{D}_4$. In Chapter 3 we will give a set of generators for Aut F in these cases and as a consequence it is possible to determine W_F explicitly in terms of the coefficients of F.

In the special case that F is a binomial form, so $F(x, y) = ax^d + by^d$, it is straightforward to determine Aut F; see Lemma 2.2.3. Then, by Theorems 2.0.1 and 2.0.2, we have the following result.

Corollary 2.0.3. *Let a, b and d be non-zero integers with $d \geq 3$ and let*

$$F(x, y) = ax^d + by^d.$$

Then (2.0.8) holds with $C_F = W_F A_F$. If a/b is not the d-th power of a rational number then

$$W_F = \begin{cases} 1 & \text{if } d \text{ is odd,} \\ \dfrac{1}{4} & \text{if } d \text{ is even.} \end{cases}$$

If $\dfrac{a}{b} = \left(\dfrac{A}{B}\right)^d$ with A and B coprime integers then

$$W_F = \begin{cases} 1 - \dfrac{1}{2|AB|} & \text{if } d \text{ is odd,} \\ \dfrac{1}{4}\left(1 - \dfrac{1}{2|AB|}\right) & \text{if } d \text{ is even.} \end{cases}$$

Further if d is odd then

$$A_F = \frac{1}{d|ab|^{1/d}}\left(\frac{2\Gamma(1-2/d)\Gamma(1/d)}{\Gamma(1-1/d)} + \frac{\Gamma^2(1/d)}{\Gamma(2/d)}\right)$$

while if d is even

$$A_F = \frac{2}{d|ab|^{1/d}} \frac{\Gamma^2(1/d)}{\Gamma(2/d)} \qquad \text{if } ab > 0$$

and

$$A_F = \frac{4}{d|ab|^{1/d}} \frac{\Gamma(1/d)\Gamma(1+2/d)}{\Gamma(1+3/d)} \qquad \text{if } ab < 0.$$

Finally we mention that there are other families of forms where one may readily determine W_F. For instance let a, b and k be integers with $a \neq 0$, $2a \neq \pm b$ and $k \geq 2$ and put

$$F(x, y) = ax^{2k} + bx^k y^k + ay^{2k}. \tag{2.0.13}$$

The discriminant of F is non-zero since $a \neq 0$ and $2a \neq \pm b$. Further, $\mathbf{D}_4$ is plainly contained in $\operatorname{Aut} F$ and there is no larger group which is an automorphism group of a binary form which contains $\mathbf{D}_4$. Therefore $\mathbf{D}_4$ is $\operatorname{Aut} F$. It now follows from Theorem 2.0.2 that $W_F = 1/8$ since $m_1 = m_2 = m_3 = m = 1$.

2.1 Preliminary lemmas

We shall require a result of Mahler [79] from 1933. For a positive number Z we put

$$\mathcal{N}_F(Z) = \{(x, y) \in \mathbb{Z}^2 : 0 < |F(x, y)| \leq Z\}$$

and

$$N_F(Z) = |\mathcal{N}_F(Z)|.$$

Lemma 2.1.1. *Let F be a binary form with integer coefficients, non-zero discriminant and degree $d \geq 3$. Then, with A_F defined by (2.0.1), we have*

$$N_F(Z) = A_F Z^{\frac{2}{d}} + O_F\left(Z^{\frac{1}{d-1}}\right).$$

In fact Mahler proved this result only under the assumption that F is irreducible. However, Lemma 2.1.1 can be deduced as a special case of Theorem 3 in [102].

Lemma 2.1.2. *Let F be a binary form with integer coefficients, non-zero discriminant and degree $d \geq 3$. Let Z be a positive real number and let γ be a real number larger than $1/d$. The number of pairs of integers (x, y) with*

$$0 < |F(x, y)| \leq Z \tag{2.1.1}$$

for which

$$\max\{|x|, |y|\} > Z^{\gamma}$$

is

$$O_F\left(Z^{\frac{1}{d}} \log Z + Z^{1-(d-2)\gamma}\right).$$

Proof. We shall follow Heath-Brown's proof of Theorem 8 in [53]. Accordingly put

$$S(Z; C) = |\{(x, y) \in \mathbb{Z}^2 : 0 < |F(x, y)| \leq Z, C < \max\{|x|, |y|\} \leq 2C, \gcd(x, y) = 1\}|$$

and suppose that $C \geq Z^{\gamma}$. Heath-Brown observes that by Roth's theorem $S(Z; C) = 0$ unless $C \ll Z^2$. Further,

$$S(Z; C) \ll 1 + \frac{Z}{C^{d-2}}. \tag{2.1.2}$$

Put

$$S^{(1)}(Z; C) = |\{(x, y) \in \mathbb{Z}^2 : 0 < |F(x, y)| \leq Z, C < \max\{|x|, |y|\}, \gcd(x, y) = 1\}|.$$

Therefore, on replacing C by $2^j C$ in (2.1.2) for $j = 1, 2, ...$ and summing we find that

$$S^{(1)}(Z; C) \ll \log Z + \frac{Z}{C^{d-2}}.$$

Next put

$$S^{(2)}(Z; C) = |\{(x, y) \in \mathbb{Z}^2 : 0 < |F(x, y)| \leq Z, C < \max\{|x|, |y|\}|.$$

Then

$$\begin{aligned} S^{(2)}(Z; C) &\ll \sum_{h \leq Z^{1/d}} S^{(1)}\left(\frac{Z}{h^d}, \frac{C}{h}\right) \\ &\ll \sum_{h \leq Z^{1/d}} \left(\log Z + \frac{Z}{h^2 C^{d-2}}\right) \\ &\ll Z^{\frac{1}{d}} \log Z + \frac{Z}{C^{d-2}} \end{aligned}$$

and our result follows on taking $C = Z^{\gamma}$.

We note that instead of appealing to Roth's theorem it is possible to treat the large solutions of (2.1.1) by means of the Thue-Siegel principle; see [15] and [98]. As a consequence all constants in the proof are then effective. □

We say that an integer h is *essentially represented* by F if whenever $(x_1, y_1), (x_2, y_2)$ are in $\mathbb{Z}^2$ and

$$F(x_1, y_1) = F(x_2, y_2) = h$$

then there exists A in $\operatorname{Aut} F$ such that

$$A\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}.$$

Observe that if there is only one integer pair (x_1, y_1) for which $F(x_1, y_1) = h$ then h is essentially represented since I is in $\operatorname{Aut} F$.

Put

$$\mathcal{N}_F^{(1)}(Z) = \{(x, y) \in \mathbb{Z}^2 : 0 < |F(x, y)| \leq Z \text{ and } F(x, y) \text{ is essentially represented by } F\}$$

and

$$\mathcal{N}_F^{(2)}(Z) = \{(x, y) \in \mathbb{Z}^2 : 0 < |F(x, y)| \leq Z \text{ and } F(x, y) \text{ is not essentially represented by } F\}.$$

Let $N_F^{(i)}(Z) = |\mathcal{N}_F^{(i)}(Z)|$ for $i = 1, 2$.

Let X be a smooth surface in $\mathbb{P}^3$ of degree d defined over $\mathbb{Q}$, and for a positive number B let $N_1(X; B)$ denote the number of integer points on X with height at most B which do not lie on any lines contained in X. Colliot-Thélène proved in the appendix of [53] that if X is a smooth projective surface of degree $d \geq 3$ then there are at most $O_d(1)$ curves of degree at most $d - 2$ contained in X. This, combined with Salberger's work in [93] and [94], implies that for any $\varepsilon > 0$, we have

$$N_1(X; B) = O_{\varepsilon}\left(B^{\frac{12}{7}+\varepsilon}\right) \text{ if } d = 3 \tag{2.1.3}$$

and

$$N_1(X; B) = O_{d,\varepsilon}\left(B^{\frac{3}{\sqrt{d}}+\varepsilon} + B^{1+\varepsilon}\right) \text{ if } d \geq 4. \tag{2.1.4}$$

We shall use (2.1.3) and (2.1.4) to prove the following result.

Lemma 2.1.3. *Let F be a binary form with integer coefficients, non-zero discriminant and degree $d \geq 3$. Then, for each $\varepsilon > 0$,*

$$N_F^{(2)}(Z) = O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right),$$

where β_d is given by (2.0.7).

Proof. Put

$$\eta_d = \begin{cases} \dfrac{7}{19} & \text{if } d = 3, \\ \dfrac{\sqrt{d}}{d\sqrt{d} - 2\sqrt{d} + 3} & \text{if } 4 \leq d \leq 8, \\ \dfrac{1}{d-1} & \text{if } d \geq 9. \end{cases}$$

We will give an upper bound for $N_F^{(2)}(Z)$ by following the approach of Heath-Brown in his proof of Theorem 8 of [53]. We first split $\mathcal{N}_F^{(2)}(Z)$ into two sets:

1. Those points $(x, y) \in \mathcal{N}_F^{(2)}(Z)$ which satisfy $\max\{|x|, |y|\} \leq Z^{\eta_d}$,
   and
2. Those points $(x, y) \in \mathcal{N}_F^{(2)}(Z)$ which satisfy $\max\{|x|, |y|\} > Z^{\eta_d}$.

We will use (2.1.3) and (2.1.4) to treat the points in category (1). Let us put

$$\mathcal{G}(\mathbf{x}) = F(x_1, x_2) - F(x_3, x_4).$$

We shall denote by X the surface defined by $\mathcal{G}(\mathbf{x}) = 0$. Notice that X is smooth since $\Delta(F) \neq 0$.

Let $N_2(X; B)$ be the number of integer points (x_1, x_2, x_3, x_4) in $\mathbb{R}^4$ with $\max\limits_{1 \leq i \leq 4} |x_i| \leq B$ for which (x_1, x_2, x_3, x_4), viewed as a point in $\mathbb{P}^3$, is on X but does not lie on a line in X; here we do not require $\gcd(x_1, x_2, x_3, x_4) = 1$. Then

$$N_2(X; B) \leq \sum_{t=1}^{B} N_1\left(X; \frac{B}{t}\right)$$

and so, by (2.1.3) and (2.1.4),

$$N_2(X;B) = O_\varepsilon\left(B^{\frac{12}{7}+\varepsilon}\right) \quad \text{if } d=3$$

and

$$N_2(X;B) = O_{d,\varepsilon}\left(B^{\frac{3}{\sqrt{d}}+\varepsilon} + B^{1+\varepsilon}\right) \quad \text{if } d \geq 4.$$

Therefore

$$N_2(X;Z^{\eta_d}) = O_{d,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right). \tag{2.1.5}$$

It remains to deal with integer points on X which lie on some line contained in X. Lines in $\mathbb{P}^3$ may be classified into two types. They are given by the pairs

$$u_1x_1 + u_2x_2 + u_3x_3 + u_4x_4 = 0, v_3x_3 + v_4x_4 = 0,$$

and by

$$x_1 = u_1x_3 + u_2x_4, x_2 = u_3x_3 + u_4x_4.$$

Suppose $\mathbf{x} = (x_1, x_2, x_3, x_4)$ lies on the first type of line. Then one of v_3, v_4 is non-zero, and we may assume without loss of generality that $v_3 \neq 0$. We thus have

$$x_3 = \frac{-v_4}{v_3}x_4.$$

Substituting this back into the first equation yields

$$u_1x_1 + u_2x_2 = -u_3\frac{-v_4}{v_3}x_4 - u_4x_4 = \frac{u_3v_4 - v_3u_4}{v_3}x_4.$$

Substituting this back into $F(x_1, x_2) = F(x_3, x_4)$ and assuming that $u_3v_4 - v_3u_4 \neq 0$, we see that

$$\begin{aligned} F(x_1,x_2) &= F\left(\frac{-v_4}{v_3}x_4, x_4\right) = x_4^d F(-v_4/v_3, 1) \\ &= F\left(\frac{-v_4}{v_3}, 1\right)\left(\frac{v_3u_1}{u_3v_4 - v_3u_4}x_1 + \frac{u_2v_3}{u_3v_4 - u_4v_3}x_2\right)^d. \end{aligned}$$

If $F(-v_4/v_3, 1) \neq 0$, then we see that F is a perfect d-th power, which is not possible since $\Delta(F) \neq 0$. Therefore we must have $F(x_1, x_2) = F(x_3, x_4) = 0$. Now suppose that $u_3v_4 = v_3u_4$. We see that u_1, u_2 cannot both be zero. Assume without loss of generality that $u_1 \neq 0$. Then

$$F(x_1, x_2) = x_2^d F(-u_2/u_1, 1),$$

which is not possible since $\Delta(F) \neq 0$. Therefore we must have $F(-u_2/u_1, 1) = 0$, so once again $F(x_1, x_2) = F(x_3, x_4) = 0$.

Now suppose that X contains a line of the second type. Suppose that $u_1u_4 = u_2u_3$. Since at least one of u_1, u_2 and one of u_3, u_4 is non-zero, we may assume that u_1 and u_3 are non-zero. Then we have

$$u_3x_1 = u_1u_3x_3 + u_2u_3x_4 = u_1(u_3x_3 + u_4x_4),$$

hence

$$x_1 = u_3x_3 + u_4x_4 = x_2.$$

Thus, $F(x_1, x_2) = F(x_3, x_4)$ implies that

$$F(x_3, x_4) = x_1^d F(1, 1) = (u_3x_3 + u_4x_4)^d F(1, 1).$$

As before we must have $F(x_1, x_2) = F(x_3, x_4) = 0$.

The last case is a line of the second type and for which $u_1u_4 \neq u_2u_3$. Such a line yields the equation

$$F(x_3, x_4) = F(u_1x_3 + u_2x_4, u_3x_3 + u_4x_4).$$

If (x_1, x_2) and (x_3, x_4) are in $\mathcal{N}_F^{(2)}(Z)$, then it follows that at least one of u_1, u_2, u_3 and u_4 is not rational. Therefore, $\mathbf{x} = (x_1, x_2, x_3, x_4)$ must lie on a line which is not defined over $\mathbb{Q}$ and hence has at most one primitive integer point on it. Thus there are at most $O\left(Z^{\eta_d}\right)$ integer points whose coordinates have absolute value at most Z^{η_d} which lie on it. Since X is smooth it follows from a theorem of Colliot-Thélène [53], or from [17], that there are at most $O_d(1)$ lines on X and so at most $O_d(Z^{\eta_d})$ integer points whose coordinates have absolute value at most Z^{η_d} on lines on X which are not defined over $\mathbb{Q}$. This, together with (2.1.5), shows that the number of points in category (1) is at most

$$O_{d,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right).$$

By Lemma 2.1.2 with $\gamma = \eta_d$ the number of points in category (2) is at most $O\left(Z^{\beta_d}\right)$ and the result now follows. □

In [53] Heath-Brown proved that for each $\varepsilon > 0$ the number of integers h of absolute value at most Z which are not essentially represented by F is

$$O_{F,\varepsilon}\left(Z^{\frac{12d+16}{9d^2-6d+16}+\varepsilon}\right), \tag{2.1.6}$$

whenever F is a binary form with integer coefficients and non-zero discriminant. This follows from the remark on page 559 of [53] on noting that the numerator of the exponent should be $12d + 16$ instead of $12d$. It follows from (2.1.6) that Lemma 2.1.3 holds, and indeed Theorem 2.0.1 holds, with β_d replaced by the larger quantity given by the exponent of Z in (2.1.6). To see this we denote, for any positive integer h, the number of prime factors of h by $\omega(h)$ and the number of positive integers which divide h by $\tau(h)$. By Bombieri and Schmidt [15] when F is irreducible and by Stewart [98] when F has non-zero discriminant, if h is a non-zero integer the Thue equation

$$F(x, y) = h, \tag{2.1.7}$$

has at most $2800d^{1+\omega(h)}$ solutions in coprime integers x and y. Therefore the number of solutions of (2.1.7) in integers x and y is at most

$$2800\tau(h)d^{1+\omega(h)}. \tag{2.1.8}$$

Our claim now follows from (2.1.6), (2.1.8) and Theorem 317 of [49].

Lemma 2.1.4. *Let F be a binary form with integer coefficients, non-zero discriminant and degree $d \geq 3$. Then with A_F defined as in (2.0.1),*

$$N_F^{(1)}(Z) = A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right)$$

where β_d is given by (2.0.7).

Proof. This is an immediate consequence of Lemmas 2.1.1 and 2.1.3 since $1/(d-1)$ is less than or equal to β_d . □

2.2 The automorphism group of F and associated lattices

For any element A in $\mathrm{GL}_2(\mathbb{Q})$ we denote by $\Lambda(A)$ the lattice of (u, v) in $\mathbb{Z}^2$ for which $A\begin{pmatrix} u \\ v \end{pmatrix}$ is in $\mathbb{Z}^2$.

Lemma 2.2.1. *Let F be a binary form with integer coefficients and non-zero discriminant. Let A be in $\mathrm{Aut}\, F$. Then there exists a unique positive integer a and coprime integers a_1, a_2, a_3, a_4 such that*

$$A = \frac{1}{a}\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \tag{2.2.1}$$

and

$$a = d(\Lambda(A)). \tag{2.2.2}$$

Proof. If $A = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{pmatrix}$ is in $\mathrm{GL}_2(\mathbb{Q})$, we write

$$\alpha_i = \frac{a_i}{a}$$

for $i = 1, 2, 3, 4$ where a is the least common denominator of the α_i's. This yields the form given in (2.2.1). Then $\Lambda(A)$ is the set of (u, v) in $\mathbb{Z}^2$ for which

$$a_1 u + a_2 v \equiv 0 \pmod{a}$$

and

$$a_3 u + a_4 v \equiv 0 \pmod{a}.$$

For each prime p let k be the largest power of p which divides a. We define the lattice $\Lambda^{(p)}(A)$ to be the set of (u, v) in $\mathbb{Z}^2$ for which

$$a_1 u + a_2 v \equiv 0 \pmod{p^k} \tag{2.2.3}$$

and

$$a_3 u + a_4 v \equiv 0 \pmod{p^k}. \tag{2.2.4}$$

Then

$$\Lambda(A) = \bigcap_p \Lambda^{(p)}(A), \tag{2.2.5}$$

where the intersection is taken over all primes p, or equivalently over primes p which divide a.

Since a_1, a_2, a_3 and a_4 are coprime at least one of them is not divisible by p. Suppose, without loss of generality, that p does not divide a_1. Then a_1^{-1} exists modulo p^k. Thus if (2.2.3) holds then

$$u \equiv -a_1^{-1} a_2 v \pmod{p^k}$$

and (2.2.4) becomes

$$(a_1 a_4 - a_2 a_3) v \equiv 0 \pmod{p^k}. \tag{2.2.6}$$

But A is in $\mathrm{Aut}\, F$ and so $|\det(A)| = 1$. Thus

$$|a_1 a_4 - a_2 a_3| = a^2$$

and (2.2.6) holds regardless of the value of v. Therefore the elements of the lattice $\Lambda^{(p)}(A)$ are determined by the congruence relation (2.2.3). It follows that

$$d(\Lambda^{(p)}(A)) = p^k$$

and by (2.2.5) and the Chinese Remainder Theorem we obtain (2.2.2). □

Lemma 2.2.2. *Let F be a binary form with integer coefficients, non-zero discriminant and degree $d \geq 3$. If A is an element of order 3 in $\operatorname{Aut} F$ then*

$$\Lambda(A) = \Lambda(A^2). \tag{2.2.7}$$

If $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_3, \mathbf{D}_4$ or $\mathbf{D}_6$ then

$$\Lambda_i \cap \Lambda_j = \Lambda \text{ for } i \neq j. \tag{2.2.8}$$

Further $m = \operatorname{lcm}(m_1, m_2, m_3)$ when $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_4$ and $m = \operatorname{lcm}(m_1, m_2, m_3, m_4)$ when $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_3$ or $\mathbf{D}_6$.

Proof. Let us first prove (2.2.7). Then either A or $-A$ is conjugate in $\mathrm{GL}_2(\mathbb{Q})$ to $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ or $\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ and since $\Lambda(A) = \Lambda(-A)$ we may assume we are in the former case. Further, then either A or A^2 is conjugate to $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ and we may assume we are in the former case. Let T be an element of $\mathrm{GL}_2(\mathbb{Q})$ with

$$T = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix}, \tag{2.2.9}$$

where t_1, t_2, t_3 and t_4 are coprime integers for which

$$A = T^{-1} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} T. \tag{2.2.10}$$

Put $t = t_1 t_4 - t_2 t_3$. Then

$$A = \frac{1}{t} \begin{pmatrix} t_1 t_2 + t_2 t_3 + t_3 t_4 & t_2^2 + t_4^2 + t_2 t_4 \\ -t_1 t_3 - t_3^2 - t_1^2 & -t_1 t_4 - t_3 t_4 - t_1 t_2 \end{pmatrix}$$

and

$$A^2 = \frac{1}{t} \begin{pmatrix} -t_1 t_2 - t_3 t_4 - t_1 t_4 & -t_2^2 - t_4^2 - t_2 t_4 \\ t_1^2 + t_3^2 + t_1 t_3 & t_1 t_2 + t_3 t_4 + t_2 t_3 \end{pmatrix},$$

hence $\Lambda(A)$ is the set of $(u,v) \in \mathbb{Z}^2$ for which

$$(t_1t_2 + t_2t_3 + t_3t_4)u + (t_2^2 + t_4^2 + t_2t_4)v \equiv 0 \pmod{t} \tag{2.2.11}$$

and

$$(t_1t_3 + t_3^2 + t_1^2)u + (t_1t_4 + t_3t_4 + t_1t_2)v \equiv 0 \pmod{t}. \tag{2.2.12}$$

Similarly, $\Lambda(A^2)$ is the set of $(u,v) \in \mathbb{Z}^2$ for which

$$(t_1t_2 + t_1t_4 + t_3t_4)u + (t_2^2 + t_4^2 + t_2t_4)v \equiv 0 \pmod{t} \tag{2.2.13}$$

and

$$(t_1^2 + t_3^2 + t_1t_3)u + (t_2t_3 + t_3t_4 + t_1t_2)v \equiv 0 \pmod{t}. \tag{2.2.14}$$

On noting that $t_1t_4 \equiv t_2t_3 \pmod{t}$ we see that the conditions (2.2.11) and (2.2.12) are the same as (2.2.13) and (2.2.14), hence

$$\Lambda(A) = \Lambda(A^2).$$

Suppose that $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_4$ under conjugation in $\mathrm{GL}_2(\mathbb{Q})$. Then there exists an element T in $\mathrm{GL}_2(\mathbb{Q})$ given by (2.2.9) with t_1, t_2, t_3 and t_4 coprime integers for which $\operatorname{Aut} F = T^{-1}\mathbf{D}_4T$. Put $t = t_1t_4 - t_2t_3$ and note that $t \neq 0$. The lattices Λ_1, Λ_2 and Λ_3 may be taken to be the lattices of (u,v) in $\mathbb{Z}^2$ for which

$$T^{-1}A_iT\begin{pmatrix} u \\ v \end{pmatrix} \in \mathbb{Z}^2,$$

where

$$A_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, A_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Thus Λ_1 consists of integer pairs (u,v) for which

$$(t_1t_2 + t_3t_4)u + (t_2^2 + t_4^2)v \equiv 0 \pmod{t} \tag{2.2.15}$$

and

$$(t_1^2 + t_3^2)u + (t_1t_2 + t_3t_4)v \equiv 0 \pmod{t}. \tag{2.2.16}$$

Λ_2 consists of integer pairs (u,v) for which

$$(t_1t_2 - t_3t_4)u + (t_2^2 - t_4^2)v \equiv 0 \pmod{t} \tag{2.2.17}$$

and

$$(t_1^2 - t_3^2)u + (t_1t_2 - t_3t_4)v \equiv 0 \pmod{t} \tag{2.2.18}$$

and Λ_3 consists of integer pairs (u, v) for which

$$2t_2t_3u + 2t_2t_4v \equiv 0 \pmod{t} \tag{2.2.19}$$

and

$$2t_1t_3u + 2t_2t_3v \equiv 0 \pmod{t}, \tag{2.2.20}$$

where in (2.2.19) and (2.2.20) we have used the observation that

$$t_1t_4 \equiv t_2t_3 \pmod{t}.$$

For each prime p dividing t we put $h = \operatorname{ord}_p t$. Define $\Lambda_i^{(p)}$ for $i = 1, 2, 3$ to be the lattice of (u, v) in $\mathbb{Z}^2$ for which the congruences (2.2.15) and (2.2.16), (2.2.17) and (2.2.18), and (2.2.19) and (2.2.20) respectively hold with t replaced by p^h and define $\Lambda^{(p)}$ to be the lattice for which all of the congruences hold. We shall prove that for some reordering (i, j, k) of $(1, 2, 3)$ we have

$$\Lambda_i^{(p)} \supset \Lambda_j^{(p)} = \Lambda_k^{(p)}. \tag{2.2.21}$$

It then follows that

$$\Lambda_r^{(p)} \cap \Lambda_s^{(p)} = \Lambda_1^{(p)} \cap \Lambda_2^{(p)} \cap \Lambda_3^{(p)} = \Lambda^{(p)} \tag{2.2.22}$$

for any pair $\{r, s\}$ from $\{1, 2, 3\}$. But since

$$\bigcap_p \left(\Lambda_r^{(p)} \cap \Lambda_s^{(p)}\right) = \Lambda_r \cap \Lambda_s \text{ and } \bigcap_p \Lambda^{(p)} = \Lambda, \tag{2.2.23}$$

we see that (2.2.8) holds. Further

$$\max\left\{d\left(\Lambda_1^{(p)}\right), d\left(\Lambda_2^{(p)}\right), d\left(\Lambda_3^{(p)}\right)\right\} = d\left(\Lambda^{(p)}\right)$$

and so $d(\Lambda)$ is the least common multiple of $d(\Lambda_1), d(\Lambda_2)$ and $d(\Lambda_3)$.

It remains to prove (2.2.21). Put

$$g_1 = \gcd(t_1t_2 + t_3t_4, t_1^2 + t_3^2, t_2^2 + t_4^2, t),$$

$$g_2 = \gcd(t_1t_2 - t_3t_4, t_1^2 - t_3^2, t_2^2 - t_4^2, t)$$

and

$$g_3 = \gcd(2t_2t_3, 2t_2t_4, 2t_1t_3, t).$$

We shall show that $\gcd(g_1, g_2)$ is 1 or 2 and that

$$\gcd(g_1, g_2) = \gcd(g_1, g_3) = \gcd(g_2, g_3). \tag{2.2.24}$$

Notice that if p divides g_1 then $t_1^2 \equiv -t_3^2 \pmod p$ and $t_2^2 \equiv -t_4^2 \pmod p$ while if p divides g_2 then $t_1^2 \equiv t_3^2 \pmod p$ and $t_2^2 \equiv t_4^2 \pmod p$ and if p divides g_3 then p divides $2t_2t_3, 2t_2t_4$ and $2t_1t_3$. Thus if p divides $\gcd(g_1, g_2)$ then p divides $2t_1^2, 2t_2^2, 2t_3^2$ and $2t_4^2$; whence $p = 2$ since $\gcd(t_1, t_2, t_3, t_4) = 1$. Next suppose that p divides $\gcd(g_1, g_3)$. Then p divides $2t_2t_4$ and $t_2^2 \equiv -t_4^2 \pmod p$ and p divides $2t_1t_3$ and $t_1^2 \equiv -t_3^2 \pmod p$. Since $\gcd(t_1, t_2, t_3, t_4) = 1$ we find that $p = 2$. Finally if p divides $\gcd(g_2, g_3)$ then, as in the previous case, $p = 2$. Observe that

$$0 = \operatorname{ord}_2 g_1 = \operatorname{ord}_2 g_2 \le \operatorname{ord}_2 g_3 \tag{2.2.25}$$

unless (t_1, t_2, t_3, t_4) is congruent to $(1, 0, 1, 0), (0, 1, 0, 1)$ or $(1, 1, 1, 1)$ modulo 2 and in these cases

$$1 = \operatorname{ord}_2 g_1 = \operatorname{ord}_2 g_3 \le \operatorname{ord}_2 g_2. \tag{2.2.26}$$

Thus (2.2.24) follows from (2.2.25) and (2.2.26).

For each prime p put $h_i = \operatorname{ord}_p g_i$ for $i = 1, 2, 3$. Then, by (2.2.24), for some rearrangement (i, j, k) of $(1, 2, 3)$ we have

$$h_i \ge h_j = h_k.$$

As in the proof of Lemma 2.2.1, $\Lambda_i^{(p)}$ is defined by a single congruence modulo p^{h-h_i} for $i = 1, 2, 3$. We check that t divides the determinant of any matrix whose rows are taken from the rows determined by the coefficients of the congruence relations (2.2.15), (2.2.16), (2.2.17), (2.2.18), (2.2.19), and (2.2.20). Furthermore $2t$ divides the determinant of such a matrix if (t_1, t_2, t_3, t_4) is congruent to $(1, 0, 1, 0), (0, 1, 0, 1)$ or $(1, 1, 1, 1)$ modulo 2. Since $h_j = h_k$ we see that the congruences modulo p^{h-h_j} define identical lattices $\Lambda_j^{(p)}$ and $\Lambda_k^{(p)}$. Further, since $h_i \ge h_j$, $\Lambda_j^{(p)}$ is a sublattice of $\Lambda_i^{(p)}$ and (2.2.8) follows when $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_4$.

Suppose now that $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_3$ under conjugation in $\mathrm{GL}_2(\mathbb{Q})$. There exists an element T in $\mathrm{GL}_2(\mathbb{Q})$, as in (2.2.9), with t_1, t_2, t_3 and t_4 coprime integers for which

$$\operatorname{Aut} F = T^{-1}\mathbf{D}_3 T.$$

Define $t = t_1t_4 - t_2t_3$. The lattices $\Lambda_1, \Lambda_2, \Lambda_3$ and Λ_4 may be taken to be the lattices of integer pairs (u, v) for which

$$T^{-1}A_iT\begin{pmatrix} u \\ v \end{pmatrix} \in \mathbb{Z}^2$$

where

$$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, A_3 = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \text{ and } A_4 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Thus Λ_1 consists of integer pairs (u, v) for which

$$(t_1t_2 - t_3t_4)u + (t_2^2 - t_4^2)v \equiv 0 \pmod{t} \tag{2.2.27}$$

and

$$(t_1^2 - t_3^2)u + (t_1t_2 - t_3t_4)v \equiv 0 \pmod{t}. \tag{2.2.28}$$

Λ_2 consists of integer pairs (u, v) for which

$$(t_1t_2 + t_2t_3 + t_1t_4)u + (t_2^2 + 2t_2t_4)v \equiv 0 \pmod{t} \tag{2.2.29}$$

and

$$(t_1^2 + 2t_1t_3)u + (t_1t_2 + t_2t_3 + t_1t_4)v \equiv 0 \pmod{t}. \tag{2.2.30}$$

Λ_3 consists of integer pairs (u, v) for which

$$(t_1t_4 + t_2t_3 + t_3t_4)u + (2t_2t_4 + t_4^2)v \equiv 0 \pmod{t} \tag{2.2.31}$$

and

$$(2t_1t_3 + t_3^2)u + (t_1t_4 + t_2t_3 + t_3t_4)v \equiv 0 \pmod{t}. \tag{2.2.32}$$

Λ_4 consists of integer pairs (u, v) for which

$$(t_1t_2 + t_2t_3 + t_3t_4)u + (t_2^2 + t_2t_4 + t_4^2)v \equiv 0 \pmod{t} \tag{2.2.33}$$

and

$$(t_1^2 + t_1t_3 + t_3^2)u + (t_1t_2 + t_1t_4 + t_3t_4)v \equiv 0 \pmod{t}. \tag{2.2.34}$$

For each prime p dividing t we put $h = \mathrm{ord}_p\, t$. Define $\Lambda_i^{(p)}$ for $i = 1, 2, 3, 4$ to be the lattice of (u, v) in $\mathbb{Z}^2$ for which the congruences (2.2.27) and (2.2.28), (2.2.29) and (2.2.30), (2.2.31) and (2.2.32), and (2.2.33) and (2.2.34) respectively hold with t replaced with p^h

and define $\Lambda^{(p)}$ to be the lattice for which all the congruences hold. We shall prove that for some reordering (i,j,k,l) of $(1,2,3,4)$ we have

$$\Lambda_i^{(p)} \supset \Lambda_j^{(p)} = \Lambda_k^{(p)} = \Lambda_l^{(p)}. \tag{2.2.35}$$

It then follows that

$$\Lambda_r^{(p)} \cap \Lambda_s^{(p)} = \Lambda_1^{(p)} \cap \Lambda_2^{(p)} \cap \Lambda_3^{(p)} \cap \Lambda_4^{(p)} = \Lambda^{(p)} \tag{2.2.36}$$

for any pair $\{r,s\}$ from $\{1,2,3,4\}$. But since

$$\bigcap_p \left(\Lambda_r^{(p)} \cap \Lambda_s^{(p)}\right) = \Lambda_r \cap \Lambda_s \text{ and } \bigcap_p \Lambda^{(p)} = \Lambda, \tag{2.2.37}$$

we conclude that (2.2.8) holds. Further

$$\max\left\{d\left(\Lambda_1^{(p)}\right), d\left(\Lambda_2^{(p)}\right), d\left(\Lambda_3^{(p)}\right), d\left(\Lambda_4^{(p)}\right)\right\} = d\left(\Lambda^{(p)}\right)$$

and so $d(\Lambda)$ is the least common multiple of $d(\Lambda_1), d(\Lambda_2), d(\Lambda_3)$ and $d(\Lambda_4)$.

It remains to prove (2.2.35). Put

$$g_1 = \gcd(t_1t_2 - t_3t_4, t_1^2 - t_3^2, t_2^2 - t_4^2, t),$$

$$g_2 = \gcd(t_1t_2 + t_2t_3 + t_1t_4, t_1^2 + 2t_1t_3, t_2^2 + 2t_2t_4, t),$$

$$g_3 = \gcd(t_1t_4 + t_2t_3 + t_3t_4, 2t_1t_3 + t_3^2, 2t_2t_4 + t_4^2, t),$$

and

$$g_4 = \gcd(t_1t_2 + t_2t_3 + t_3t_4, t_1^2 + t_1t_3 + t_3^2, t_2^2 + t_2t_4 + t_4^2, t).$$

Suppose that p is a prime which divides $\gcd(g_1, g_2)$. If p divides t_1 then since p divides $t_1^2 - t_3^2$ we see that p divides t_3. Similarly if p divides t_2 then since p divides $t_2^2 - t_4^2$ we see that p divides t_4. Since t_1, t_2, t_3 and t_4 are coprime either p does not divide t_1 or p does not divide t_2. In the former case since p divides $t_1^2 + 2t_1t_3$ we find that p divides $t_1 + 2t_3$. Thus $t_1^2 \equiv 4t_3^2 \pmod{p}$ and since $t_1^2 \equiv t_3^2 \pmod{p}$ we conclude that $p = 3$. In the latter case since p divides $t_2^2 + 2t_2t_4$ we again find that $p = 3$. In a similar fashion we prove that if p is a prime which divides $\gcd(g_i, g_j)$ for any pair $\{i,j\}$ from $\{1,2,3,4\}$ then $p = 3$.

Denote by E the set consisting of the 4-tuples $(1,1,1,1)$, $(-1,-1,-1,-1)$, $(1,-1,1,-1)$, $(-1,1,-1,1)$, $(1,0,1,0)$, $(-1,0,-1,0)$, $(0,1,0,1)$ and $(0,-1,0,-1)$. One may check that

if (t_1, t_2, t_3, t_4) is not congruent modulo 3 to an element of E then for some reordering (i, j, k, l) of $(1, 2, 3, 4)$ we have

$$0 = \operatorname{ord}_3 g_i = \operatorname{ord}_3 g_j = \operatorname{ord}_3 g_k \leq \operatorname{ord}_3 g_l. \tag{2.2.38}$$

If (t_1, t_2, t_3, t_4) is congruent modulo 3 to an element of E then there is some reordering (i, j, k, l) of $(1, 2, 3, 4)$ such that

$$1 = \operatorname{ord}_3 g_i = \operatorname{ord}_3 g_j = \operatorname{ord}_3 g_k \leq \operatorname{ord}_3 g_l. \tag{2.2.39}$$

To see this we make use of the fact that

$$\operatorname{ord}_3 g_1 \leq \operatorname{ord}_3(t_1^2 - t_3^2), \quad \operatorname{ord}_3 g_2 \leq \operatorname{ord}_3(t_1^2 + 2t_1 t_3), \tag{2.2.40}$$

$$\operatorname{ord}_3 g_3 \leq \operatorname{ord}_3(2t_1 t_3 + t_3^2) \text{ and } \operatorname{ord}_3 g_4 \leq \operatorname{ord}_3(t_1^2 + t_1 t_3 + t_3^2),$$

to deal with the first six cases. To handle the remaining two cases, so when (t_1, t_2, t_3, t_4) is congruent modulo 3 to $(0, 1, 0, 1)$ or $(0, -1, 0, -1)$, we appeal to (2.2.40) but with t_1 and t_3 replaced by t_2 and t_4 respectively.

It now follows from (2.2.38) and (2.2.39) that $\gcd(g_1, g_2)$ is 1 or 3 and

$$\gcd(g_1, g_2) = \gcd(g_1, g_3) = \gcd(g_1, g_4) = \gcd(g_2, g_3) = \gcd(g_2, g_4) = \gcd(g_3, g_4). \tag{2.2.41}$$

For each prime p put $h_i = \operatorname{ord}_p g_i$ for $i = 1, 2, 3, 4$. Then, by (2.2.41) for some reordering (i, j, k, l) of $(1, 2, 3, 4)$ we have

$$h_i \geq h_j = h_k = h_l.$$

As in the proof of Lemma 2.2.1, $\Lambda_i^{(p)}$ is defined by a single congruence relation modulo p^{h-h_i} and $\Lambda_j^{(p)}, \Lambda_k^{(p)}$ and $\Lambda_l^{(p)}$ are defined by single congruences modulo p^{h-h_j}. We check that t divides the determinant of any matrix whose rows are taken from the rows determined by the coefficients of the congruence relations (2.2.27), (2.2.28), (2.2.29), (2.2.30), (2.2.31), (2.2.32), (2.2.33), and (2.2.34) and that $3t$ divides the determinant of such a matrix if (t_1, t_2, t_3, t_4) is congruent to an element of E. Then since $h_j = h_k = h_l$ we see that the congruences modulo p^{h-h_j} define identical lattices so

$$\Lambda_j^{(p)} = \Lambda_k^{(p)} = \Lambda_l^{(p)}.$$

Further, since $h_i \geq h_j$, $\Lambda_j^{(p)}$ is a sublattice of $\Lambda_i^{(p)}$ and thus (2.2.35) holds and (2.2.8) follows when $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_3$.

Finally we remark that (2.2.8) holds when $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_6$ by the same analysis we used when $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_3$.

□

Lemma 2.2.3. *Let a and b be non-zero integers and let d be an integer with $d \geq 3$. Put*

$$F(x, y) = ax^d + by^d.$$

If a/b is not the d-th power of a rational number then when d is odd

$$\operatorname{Aut} F = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

and when d is even

$$\operatorname{Aut} F = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\}.$$

If $\dfrac{a}{b} = \dfrac{A^d}{B^d}$ with A and B coprime integers then when d is odd

$$\operatorname{Aut} F = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & A/B \\ B/A & 0 \end{pmatrix} \right\}$$

and when d is even

$$\operatorname{Aut} F = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} 0 & \pm A/B \\ \pm B/A & 0 \end{pmatrix} \right\}.$$

Proof. Let

$$U = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix}$$

be an element of $\operatorname{Aut} F$. Then u_1, u_2, u_3, u_4 are rational numbers with

$$u_1 u_4 - u_2 u_3 = \pm 1. \tag{2.2.42}$$

Since $F(u_1 x + u_2 y, u_3 x + u_4 y) = F(x, y)$ we see on comparing coefficients that

$$a u_1^d + b u_2^d = a, \ a u_3^d + b u_4^d = b \tag{2.2.43}$$

and

$$a u_1^j u_2^{d-j} = b u_3^j u_4^{d-j} \tag{2.2.44}$$

for $j = 1, \cdots, d-1$.

Suppose that $u_1u_2 \neq 0$. Then by (2.2.44), we have $u_3u_4 \neq 0$ as well. Therefore we may write

$$\left(\frac{u_3}{u_1}\right)\left(\frac{u_4}{u_2}\right)^{d-1} = \left(\frac{u_3}{u_1}\right)^2\left(\frac{u_4}{u_2}\right)^{d-2},$$

which implies that $u_1u_4 - u_2u_3 = 0$, contradicting (2.2.42). Therefore, $u_1u_2 = 0$ and similarly $u_3u_4 = 0$. Further, by (2.2.42), either $u_1u_4 = \pm 1$ and $u_2 = u_3 = 0$ or $u_2u_3 = \pm 1$ and $u_1 = u_4 = 0$. In the first case, by (2.2.43), we have $u_1^d = 1$ and $u_4^d = 1$, hence if d is odd we have $u_1 = u_4 = 1$ while if d is even we have $u_1 = \pm 1$ and $u_4 = \pm 1$. In the other case, by (2.2.43), we have $u_2^d = \dfrac{a}{b}$ and this is only possible if there exist coprime integers A and B with

$$\frac{a}{b} = \frac{A^d}{B^d}.$$

In that case $u_2 = A/B$ if d is odd and $u_2 = \pm A/B$ if d is even. Thus, by (2.2.42), $u_3 = B/A$ if d is odd and $u_3 = \pm B/A$ if d is even. Our result now follows. □

2.3 Proof of Theorems 2.0.1 and 2.0.2

If $\operatorname{Aut} F$ is conjugate to $\mathbf{C}_1$ then every pair $(x, y) \in \mathbb{Z}^2$ for which $F(x, y)$ is essentially represented with $0 < |F(x, y)| \leq Z$ gives rise to a distinct integer h with $0 < |h| \leq Z$. It follows from Lemma 2.1.3 and Lemma 2.1.4 that

$$R_F(Z) = A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right),$$

and we see that W_F in this case is 1. In a similar way we see that if $\operatorname{Aut} F$ is conjugate to $\mathbf{C}_2$ then

$$R_F(Z) = \frac{A_F}{2} Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right).$$

Next let us consider when $\operatorname{Aut} F$ is conjugate to $\mathbf{C}_3$. Then for A in $\operatorname{Aut} F$ with $A \neq I$ we have, by Lemma 2.2.2, $\Lambda(A) = \Lambda(A^2) = \Lambda$. Thus whenever $F(x, y) = h$ with (x, y) in $\mathcal{N}_F^{(1)}(Z) \cap \Lambda$ there are two other elements $(x_1, y_1), (x_2, y_2)$ for which $F(x_i, y_i) = h$ for $i = 1, 2$. When (x, y) is in $\mathbb{Z}^2$ but not in Λ and $F(x, y)$ is essentially represented then $F(x, y)$ has only one representation.

Let ω_1, ω_2 be a basis for Λ with $\omega_1 = (a_1, a_3)$ and $\omega_2 = (a_2, a_4)$. Put $F_\Lambda(x, y) = F(a_1x + a_2y, a_3x + a_4y)$ and notice that

$$|\mathcal{N}_F(Z) \cap \Lambda| = N_{F_\Lambda}(Z). \tag{2.3.1}$$

By Lemma 2.1.1

$$N_{F_\Lambda}(Z) = A_{F_\Lambda} Z^{\frac{2}{d}} + O_{F_\Lambda}\left(Z^{1/(d-1)}\right). \tag{2.3.2}$$

Since the quantity $|\Delta(F)|^{1/d(d-1)} A_F$ is invariant under $\mathrm{GL}_2(\mathbb{R})$

$$|\Delta(F)|^{1/d(d-1)} A_F = |\Delta(F_\Lambda)|^{1/d(d-1)} A_{F_\Lambda} \tag{2.3.3}$$

and we see that

$$A_{F_\Lambda} = \frac{1}{d(\Lambda)} A_F = \frac{A_F}{m}. \tag{2.3.4}$$

Therefore by (2.3.1), (2.3.2) and (2.3.4)

$$|\mathcal{N}_F(Z) \cap \Lambda| = \frac{A_F}{m} Z^{\frac{2}{d}} + O_F\left(Z^{1/(d-1)}\right). \tag{2.3.5}$$

Certainly $\mathcal{N}_F^{(2)}(Z) \cap \Lambda$ is contained in $\mathcal{N}_F^{(2)}(Z)$ and thus, by (2.3.5) and Lemma 2.1.3,

$$|\mathcal{N}_F^{(1)}(Z) \cap \Lambda| = \frac{A_F}{m} Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right). \tag{2.3.6}$$

Each pair (x, y) in $\mathcal{N}_F^{(1)}(Z) \cap \Lambda$ is associated with two other pairs which represent the same integer. Thus the pairs (x, y) in $\mathcal{N}_F^{(1)}(Z) \cap \Lambda$ yield

$$\frac{A_F}{3m} Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right) \tag{2.3.7}$$

integers h with $0 < |h| \le Z$. By Lemma 2.1.4 and (2.3.6) the number of pairs (x, y) in $\mathcal{N}_F^{(1)}(Z)$ which are not in Λ is

$$\left(1 - \frac{1}{m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right) \tag{2.3.8}$$

and each pair gives rise to an integer h with $0 < |h| \le Z$ which is uniquely represented by F. It follows from (2.3.7), (2.3.8) and Lemma 2.1.3 that when $\mathrm{Aut}\, F$ is equivalent to $\mathbf{C}_3$ we have

$$R_F(Z) = \left(1 - \frac{2}{3m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right).$$

A similar analysis applies in the case when $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_1, \mathbf{D}_2, \mathbf{C}_4$ or $\mathbf{C}_6$. These groups are cyclic with the exception of $\mathbf{D}_2$ but $\mathbf{D}_2/\{\pm I\}$ is cyclic and that is sufficient for our purposes.

We are left with the possibility that $\operatorname{Aut} F$ is conjugate to $\mathbf{D}_3, \mathbf{D}_4$ or $\mathbf{D}_6$. We first consider the case when $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_4$. In this case, recall (2.3.6), we have

$$|\mathcal{N}_F^{(1)}(Z) \cap \Lambda| = \frac{A_F}{m} Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right)$$

and since each h for which $h = F(x,y)$ with (x,y) in $\mathcal{N}_F^{(1)}(Z) \cap \Lambda$ is represented by 8 elements of $\mathcal{N}_F^{(1)}(Z)$ the pairs (x,y) of $\mathcal{N}_F^{(1)}(Z) \cap \Lambda$ yield

$$\frac{A_F}{8m} Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right) \tag{2.3.9}$$

terms h in $\mathcal{R}_F(Z)$. By Lemma 2.2.2 we have $\Lambda_i \cap \Lambda_j = \Lambda$ for $1 \le i < j \le 3$; whence the terms (x,y) in Λ_1, Λ_2 or Λ_3 but not in Λ for which (x,y) is in $\mathcal{N}_F^{(1)}(Z)$ have cardinality

$$\left(\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} - \frac{3}{m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right).$$

If (x,y) is in Λ_1, Λ_2 or Λ_3 but not in Λ and $h = F(x,y)$ is essentially represented then h has precisely four representations. Accordingly the terms in

$$\mathcal{N}_F^{(1)}(Z) \cap \Lambda_i, 1 \le i \le 3$$

which are not in Λ contribute

$$\frac{1}{4}\left(\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} - \frac{3}{m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right) \tag{2.3.10}$$

terms to $\mathcal{R}_F(Z)$. Finally the terms (x,y) in $\mathcal{N}_F^{(1)}(Z)$ but not in Λ_i for $i = 1,2,3$ have cardinality equal to

$$\left(1 - \frac{1}{m_1} - \frac{1}{m_2} - \frac{1}{m_3} + \frac{2}{m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right).$$

Each integer h represented by such a term has 2 representations and therefore these terms (x,y) contribute

$$\frac{1}{2}\left(1 - \frac{1}{m_1} - \frac{1}{m_2} - \frac{1}{m_3} + \frac{2}{m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right) \tag{2.3.11}$$

terms to $\mathcal{R}_F(Z)$. It now follows from (2.3.9), (2.3.10), (2.3.11) and Lemma 2.1.3 that

$$R_F(Z) = \frac{1}{2}\left(1 - \frac{1}{2m_1} - \frac{1}{2m_2} - \frac{1}{2m_3} + \frac{3}{4m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right),$$

as required.

We now treat the case when $\operatorname{Aut} F$ is conjugate to $\mathbf{D}_3$. As before the pairs (x, y) of $\mathcal{N}_F^{(1)}(Z) \cap \Lambda$ yield

$$\frac{A_F}{6m} Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right) \tag{2.3.12}$$

terms in $\mathcal{R}_F(Z)$. Since $\Lambda_i \cap \Lambda_j = \Lambda$ for $1 \le i < j \le 3$ by Lemma 2.2.2, the pairs (x, y) in $\mathcal{N}_F^{(1)}(Z) \cap \Lambda_i$ for $i = 1, 2, 3$ which are not in Λ contribute

$$\left(\frac{1}{2m_1} + \frac{1}{2m_2} + \frac{1}{2m_3} - \frac{3}{2m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right) \tag{2.3.13}$$

to $\mathcal{R}_F(Z)$. Further, the pairs (x, y) in $\mathcal{N}_F^{(1)}(Z) \cap \Lambda_4$ which are not in Λ contribute

$$\left(\frac{1}{3m_4} - \frac{1}{3m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right) \tag{2.3.14}$$

terms to $\mathcal{R}_F(Z)$. Furthermore the pairs (x, y) in $\mathcal{N}_F^{(1)}(Z)$ which are not in Λ_i for $i = 1, 2, 3, 4$ contribute, by Lemma 2.2.2,

$$\left(1 - \frac{1}{m_1} - \frac{1}{m_2} - \frac{1}{m_3} - \frac{1}{m_4} + \frac{3}{m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right) \tag{2.3.15}$$

terms to $\mathcal{R}_F(Z)$. It then follows from (2.3.12), (2.3.13), (2.3.14), (2.3.15), and Lemma 2.1.3 that

$$R_F(Z) = \left(1 - \frac{1}{2m_1} - \frac{1}{2m_2} - \frac{1}{2m_3} - \frac{2}{3m_4} + \frac{4}{3m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right)$$

as required.

When $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_6$ the analysis is the same as for $\mathbf{D}_3$ taking into account the fact that $\operatorname{Aut} F$ contains $-I$ and so the weighting factor W_F is one half of what it is when $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_3$. This completes the proof of Theorems 2.0.1 and 2.0.2.

2.4 Proof of Corollary 2.0.3

We first determine W_F. By Lemma 2.2.3, if a/b is not the d-th power of a rational then when d is odd $\operatorname{Aut} F$ is equivalent to $\mathbf{C}_1$ and, by Theorem 2.0.2, $W_F = 1$ while when d is even $\operatorname{Aut} F$ is equal to $\mathbf{D}_2$ and so by Theorem 2.0.2 we have $W_F = \frac{1}{4}$. Suppose that

$$\frac{a}{b} = \frac{A^d}{B^d}$$

with A and B coprime non-zero integers. If d is odd then $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_1$ by Lemma 2.2.3. Notice that

$$\begin{pmatrix} 0 & A/B \\ B/A & 0 \end{pmatrix} = \frac{1}{AB}\begin{pmatrix} 0 & A^2 \\ B^2 & 0 \end{pmatrix}$$

and that A^2 and B^2 are coprime integers. Therefore by Lemma 2.2.1 we have $m = |AB|$ and $W_F = 1 - \frac{1}{2|AB|}$ when d is odd. If d is even $\operatorname{Aut} F$ is equivalent to $\mathbf{D}_4$ with $m_1 = 1, m_2 = m_3 = m = |AB|$ and by Theorem 2.0.2 we have

$$W_F = \frac{1}{4}\left(1 - \frac{1}{2|AB|}\right).$$

We now determine A_F. We first consider the case $F(x,y) = ax^{2k} + by^{2k}$, with a and b positive. Then

$$A_F = \iint_{ax^{2k}+by^{2k}\le 1} dxdy.$$

Note that A_F is four times the area of the region with $ax^{2k} + by^{2k} \le 1$ and with x and y non-negative. Make the substitution $ax^{2k} = u, by^{2k} = uv, u, v \ge 0$. Then we see that

$$\begin{aligned}\frac{1}{4}A_F &= \int_0^\infty \int_0^{\frac{1}{v+1}} \frac{1}{4k^2(ab)^{1/2k}} u^{\frac{1}{k}-1} v^{\frac{1}{2k}-1} dudv \\ &= \frac{1}{4k(ab)^{1/2k}} \int_0^\infty \frac{v^{1/2k-1}}{(1+v)^{1/k}} dv\end{aligned}$$

The above integral is $B(1/2k, 1/2k)$ where $B(z,w)$ denotes the Beta function and thus, see 6.2.1 of [33],

$$A_F = \frac{1}{k(ab)^{1/2k}} \frac{\Gamma^2(1/2k)}{\Gamma(1/k)}.$$

Next, we treat the case $F(x,y) = ax^{2k} - by^{2k}$ with a and b positive. The region $\{(x,y) \in \mathbb{R}^2 : |F(x,y)| \leq 1\}$ has equal area in each quadrant, so it suffices to estimate the area assuming $x, y \geq 0$. We further divide the region into two, depending on whether $ax^{2k} - by^{2k} \geq 0$ or not. Let $A_F^{(1)}$ denote the area of the region satisfying $x, y \geq 0, 0 \leq F(x,y) \leq 1$. We make the substitutions $ax^{2k} = u, by^{2k} = uv$ with $u, v \geq 0$. Then

$$\begin{aligned}
\frac{1}{8}A_F = A_F^{(1)} &= \iint_{\substack{0 \leq ax^{2k} - by^{2k} \leq 1 \\ x,y \geq 0}} dxdy \\
&= \int_0^1 \int_0^{\frac{1}{1-v}} \frac{1}{4k^2(ab)^{1/2k}} u^{\frac{1}{k}-1} v^{\frac{1}{2k}-1} du dv \\
&= \frac{1}{4k(ab)^{1/2k}} \int_0^1 \frac{v^{1/2k-1}}{(1-v)^{1/k}} dv \\
&= \frac{1}{4k(ab)^{1/2k}} \frac{\Gamma(1/2k)\Gamma(1+1/k)}{\Gamma(1+3/2k)}.
\end{aligned}$$

Next, we treat the case when $F(x,y) = ax^{2k+1} + by^{2k+1}$. We put $ax^{2k+1} = u$ and $by^{2k+1} = uv$. We thus obtain

$$\begin{aligned}
\frac{A_F}{2}|ab|^{1/(2k+1)} &= \frac{1}{2(2k+1)} \int_{-\infty}^{\infty} \frac{v^{\frac{1}{2k+1}-1} dv}{(1+v)^{2/(2k+1)}} \\
&= \frac{1}{2(2k+1)} \left(\int_0^{\infty} \frac{v^{-2k/(2k+1)} dv}{(1+v)^{2/(2k+1)}} + \int_0^1 \frac{v^{-2k/(2k+1)} dv}{(1-v)^{2/(2k+1)}} + \int_1^{\infty} \frac{v^{-2k/(2k+1)} dv}{(1-v)^{2/(2k+1)}} \right) \\
&= \frac{1}{2(2k+1)} \left(\frac{\Gamma^2\left(\frac{1}{2k+1}\right)}{\Gamma\left(\frac{2}{2k+1}\right)} + \frac{\Gamma\left(\frac{1}{2k+1}\right)\Gamma\left(\frac{2k-1}{2k+1}\right)}{\Gamma\left(\frac{2k}{2k+1}\right)} + \frac{\Gamma\left(\frac{2k-1}{2k+1}\right)\Gamma\left(\frac{1}{2k+1}\right)}{\Gamma\left(\frac{2k}{2k+1}\right)} \right).
\end{aligned}$$

Chapter 3

Binary cubic and quartic forms

Let F be a binary form with integer coefficients, non-zero discriminant $\Delta(F)$, and degree d at least 3. Let $R_F(Z)$ denote the number of integers h with $|h| \leq Z$ for which the Thue equation

$$F(x, y) = h \tag{3.0.1}$$

has a solution in integers x and y. It is an old question, dating back to at least Erdős and Mahler [40], that there exists a positive number C_F for which the asymptotic formula

$$R_F(Z) \sim C_F Z^{\frac{2}{d}}$$

holds for $d \geq 3$. In [100], together with C. L. Stewart, we proved that this conjecture is true; see also the previous chapter.

One of the principal features of [100] is that we showed the constant C_F is a rational multiple W_F of A_F, where A_F is the area of the region

$$\{(x, y) \in \mathbb{R}^2 : |F(x, y)| \leq 1\}.$$

Let

$$T = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}).$$

Then T acts on F via substitution, namely $F_T(x, y) = F(t_1x + t_2y, t_3x + t_4y)$. Let $\mathcal{G} \subset \mathrm{GL}_2(\mathbb{Q})$ be the subgroup consisting of matrices $T \in \mathrm{GL}_2(\mathbb{Q})$ such that $F = F_T$. This group $\mathcal{G}$ is called the *automorphism group* of F and we denote it by $\mathrm{Aut}\, F$. More

generally, for any subfield $\mathbb{F}$ of $\mathbb{C}$ we can write $\mathrm{Aut}_{\mathbb{F}} F$ to be the subgroup of $\mathrm{GL}_2(\mathbb{F})$ consisting of $T \in \mathrm{GL}_2(\mathbb{F})$ such that $F = F_T$. We shall call $\mathrm{Aut}_{\mathbb{F}} F$ the $\mathbb{F}$-automorphism group of F.

It is known classically (see [85] for example) that a binary cubic form with non-zero discriminant is $\mathrm{GL}_2(\mathbb{C})$-equivalent to the form

$$xy(x+y)$$

and when that a binary quartic form with non-zero discriminant is equivalent to

$$x^4 + ux^2y^2 + y^4$$

for some $u \in \mathbb{C}$. This immediately shows, given the work of Stewart [98] and Lemma 3.2.1, that $\mathrm{Aut}_{\mathbb{C}} F$ contains a subgroup isomorphic to the dihedral group $\mathcal{D}_3$ when F is a binary cubic form and $\mathrm{Aut}_{\mathbb{C}} F$ contains a subgroup isomorphic to the dihedral group $\mathcal{D}_4$ when F is a binary quartic form. However, this classical approach is not explicit and does not produce easy criteria to determine the exact elements of $\mathrm{Aut}\, F$. In [100] we showed that the rational number W_F given by $C_F = W_F A_F$ depends only on the automorphism group $\mathrm{Aut}\, F$. More precisely, we showed that one needs to know the exact elements of $\mathrm{Aut}\, F$ in order to compute W_F and not just the isomorphism class. In [100] we did not attempt to determine $\mathrm{Aut}\, F$ given F. In general, this can be quite non-trivial.

Hooley, in [64], [68], and [70], showed that one can determine $\mathrm{Aut}\, F$ explicitly for irreducible binary cubic forms and certain binary quartic forms. Let

$$F(x,y) = b_3x^3 + b_2x^2y + b_1xy^2 + b_0y^3$$

be an irreducible binary cubic form with integer coefficients and discriminant $\Delta(F)$. Put

$$q_F(x) = (b_2^2 - 3b_3b_1)x^2 + (b_2b_1 - 9b_3b_0)x + (b_1^2 - 3b_2b_0), \tag{3.0.2}$$

for the *Hessian covariant* of F and put

$$A = b_2^2 - 3b_3b_1, B = b_2b_1 - 9b_3b_0, C = b_1^2 - 3b_2b_0, \tag{3.0.3}$$

with $D = B^2 - 4AC$. Consider the matrix

$$\mathcal{U}_{q_F} = \frac{1}{2D}\begin{pmatrix} B\sqrt{-3D} - D & 2C\sqrt{-3D} \\ -2A\sqrt{-3D} & -B\sqrt{-3D} - D \end{pmatrix}. \tag{3.0.4}$$

Put $\mathbf{C}_1 = \{I_{2\times 2}\}$. Hooley proved in [64] and [70] that

$$\operatorname{Aut} F = \begin{cases} \mathbf{C}_1 & \text{if } \Delta(F) \text{ is not a square;} \\ \{I_{2\times 2}, \mathcal{U}_{q_F}, \mathcal{U}_{q_F}^2\} & \text{if } \Delta(F) \text{ is a square.} \end{cases} \tag{3.0.5}$$

(3.0.5) is critical for Hooley's determination of the asymptotic growth of $R_F(Z)$ when F is cubic and irreducible in [64] and [70]. In addition to explicitly determining $\operatorname{Aut} F$, Hooley also obtained explicit values for A_F in his two papers. He proved

$$|\Delta(F)|^{\frac{1}{6}} A_F = \begin{cases} \dfrac{3\Gamma^2(1/3)}{\Gamma(2/3)} & \text{if } \Delta(F) > 0, \\ \\ \dfrac{\sqrt{3}\Gamma^2(1/3)}{\Gamma(2/3)} & \text{if } \Delta(F) < 0, \end{cases}$$

where

$$\Gamma(s) = \int_0^\infty x^{s-1} e^{-x} dx$$

is the Γ-function. If $\Delta(F)$ is a square, put

$$m = \frac{\sqrt{\Delta(F)}}{\gcd(A, B, C)}. \tag{3.0.6}$$

where A, B, C are as in (3.0.3) and D is as in (3.0.4). Then in [64] and [70] Hooley proved that there exists a positive number γ such that

$$R_F(Z) = \begin{cases} A_F Z^{\frac{2}{3}} + O\left(Z^{\frac{2}{3}} (\log\log Z)^{-\gamma}\right) & \text{if } \Delta(F) \text{ is not a square,} \\ \\ \left(1 - \dfrac{2}{3m}\right) A_F Z^{\frac{2}{3}} + O\left(Z^{\frac{2}{3}} (\log Z)^{-\gamma}\right) & \text{if } \Delta(F) \text{ is a square.} \end{cases} \tag{3.0.7}$$

In [68] Hooley considered bi-quadratic binary quartic forms of the shape

$$F(x, y) = a_4 x^4 + a_2 x^2 y^2 + a_0 y^4, a_4 a_0 \neq 0.$$

Put $\mathbf{D}_2 = \left\langle -I_{2\times 2}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$. If $\dfrac{a_4}{a_0} = \dfrac{A^4}{C^4}$ for non-zero integers A, C, put

$$\mathcal{G}_F^{(1)} = \begin{pmatrix} 0 & C/A \\ A/C & 0 \end{pmatrix}, \mathcal{G}_F^{(2)} = \begin{pmatrix} 0 & C/A \\ -A/C & 0 \end{pmatrix}.$$

Hooley proved in [68] that

$$\operatorname{Aut} F = \begin{cases} \mathbf{D}_2 & \text{if } a_4/a_0 \text{ is not the 4-th power of a rational number,} \\ \left\langle \mathcal{G}_F^{(1)}, \mathcal{G}_F^{(2)} \right\rangle & \text{if } a_4/a_0 = A^4/C^4 \text{ is a perfect 4-th power of a rational number.} \end{cases} \tag{3.0.8}$$

Using (3.0.8), Hooley showed that

$$R_F(Z) = \begin{cases} \dfrac{A_F}{4} Z^{\frac{1}{2}} + O_{F,\varepsilon}\left(Z^{\frac{18}{37}+\varepsilon}\right) & \text{if } a_4/a_0 \text{ is not the 4-th power of a rational,} \\ \dfrac{A_F}{4}\left(1 - \dfrac{1}{2AC}\right) Z^{\frac{1}{2}} + O_{F,\varepsilon}\left(Z^{\frac{18}{37}+\varepsilon}\right) & \text{if } a_4/a_0 = A^4/C^4 \text{ for } A, C \in \mathbb{Z}. \end{cases} \tag{3.0.9}$$

In this chapter, our main goal will be to explicitly determine $\operatorname{Aut} F$ in terms of the coefficients of F when the degree of F is 3 or 4. Specifically, we improve upon Hooley's work when $d = 3$ by addressing the case when F is reducible. For quartic forms, we will determine $\operatorname{Aut} F$ in all possible cases, generalizing Hooley's result in [68]. We will actually do more, namely we shall determine $\operatorname{Aut}_{\mathbb{F}} F$ for any subfield $\mathbb{F}$ of $\mathbb{C}$. Our result will depend on certain algebraic covariants of F when the degree of F is 3 or 4. We shall prove:

Theorem 3.0.1. *Let F be a binary form with integer coefficients and non-zero discriminant with degree d, where $d = 3, 4$. Then $\operatorname{Aut}_{\mathbb{F}} F$ can be given explicitly in terms of certain algebraic covariants of F for any subfield $\mathbb{F}$ of $\mathbb{C}$.*

As a consequence, we are able to refine Theorem 1.1 in [100] and thus extend Hooley's main theorems in [64], [68], and [70], given by (3.0.7) and (3.0.9):

Theorem 3.0.2. *Let $F(x, y)$ be a binary form of degree d with integer coefficients and non-zero discriminant. Then there exists an a positive number C_F such that for all $\varepsilon > 0$ we have*

$$R_F(Z) = C_F Z^{\frac{2}{3}} + O_{F,\varepsilon}\left(Z^{\frac{12}{19}+\varepsilon}\right)$$

if $d = 3$ and

$$R_F(Z) = C_F Z^{\frac{1}{2}} + O_{F,\varepsilon}\left(Z^{\frac{3}{7}+\varepsilon}\right)$$

if $d = 4$. Moreover, C_F can be explicitly determined from the coefficients of F.

Our explicit characterization of automorphism groups of binary cubic and quartic forms allows us to study lines on algebraic surfaces of the shape

$$X : F(x_1, x_2) - F(x_3, x_4) = 0. \tag{3.0.10}$$

It is a celebrated theorem of Cayley and Salmon that cubic surfaces contain exactly 27 lines over an algebraically closed field. For quartic surfaces, it is not known in general how many lines they contain. In the course of proving Theorems 2.0.1 and 2.0.2 (see Theorems 1.1 and 1.2 in [100]), we had to study lines on the surface X defined by (3.0.10). It is a consequence of Theorem 3.1 in [17] that this surface X contains exactly $d(d + \upsilon_F)$ many lines, where υ_F is the number of automorphisms of F in $\mathrm{PGL}_2(\mathbb{C})$. We shall prove that when $d = 3, 4$ that the number of lines defined over $\mathbb{C}$ is positive, and that the field of definition of these lines is very small.

Theorem 3.0.3. *Let F be a binary cubic or quartic form with non-zero discriminant and integer coefficients. Let X be the algebraic surface defined by (3.0.10). Then*

(a) for $d = 3$, X contains exactly 27 distinct lines over $\overline{\mathbb{Q}}$, and these lines are defined over a field of degree at most 12 over $\mathbb{Q}$.

(b) for $d = 4$, X contains exactly 32 distinct lines over $\overline{\mathbb{Q}}$ if the J-invariant $J(F)$ is non-zero, and 48 lines when $J(F) = 0$, and 64 lines when $I(F) = 0$. Further, these lines are defined over a field of degree at most 192 over $\mathbb{Q}$.

For cubic surfaces, this shows that those X which arise from (3.0.10) are highly atypical. In particular, for the generic cubic surface defined over $\mathbb{Q}$, the Galois group of its configuration of lines is isomorphic to $W(E_6)$, the Weyl group for the E_6 root system. This is also the field of definition of these lines, and so for the generic cubic surface, the lines are defined over a field of degree equal to $\#W(E_6) = 51840$. Ekedahl [38] found an explicit example of a cubic surface which realizes this bound.

3.1 Statement of main results

In [100], our Theorem 1.2 shows that for each binary form F of degree $d \geq 3$, integer coefficients and non-zero discriminant, there exists a positive rational number W_F which depends only on the automorphism group $\mathrm{Aut}\, F$ such that

$$C_F = W_F A_F.$$

We shall determine W_F when F is a binary cubic form with integer coefficients and non-zero discriminant in Theorem 3.1.4 and when F is a binary quartic form with integer coefficients and non-zero discriminant in Theorem 3.1.8. For the action of $\mathrm{GL}_2(\mathbb{Z})$ on the set of binary forms of a fixed degree d via substitution, we define a *covariant* of this action to be a function Φ which is a function of the coefficients of a binary form F of degree d and the variables x and y which satisfies

$$\Phi(F;(x,y)) = \Phi(F_T; T^{-1}(x,y)) \tag{3.1.1}$$

for all $T \in \mathrm{GL}_2(\mathbb{Z})$. When Φ is a polynomial in x and y, we see at once that Φ must be homogeneous. We then say Φ has degree k if it is a form of degree k in x and y.

The principal novelty of this work is the observation that for binary cubic and quartic forms, the structure of the automorphism group $\mathrm{GL}_2(\mathbb{C})$ is entirely determined by certain quadratic covariants of the form which are not in general defined over $\mathbb{Q}$. These covariants were originally discovered by Julia in his thesis and used extensively by Cremona [31] in his work on the reduction theory of binary cubic and quartic forms. Bhargava and Yang succeeded in using Julia's quadratic invariant to count binary forms of arbitrary degree in [13].

Let $f(x,y) = ax^2 + bxy + cy^2$ be a binary quadratic for with non-zero discriminant D. We put

$$\mathcal{M}_f = \frac{1}{\sqrt{|D|}} \begin{pmatrix} b & 2c \\ -2a & -b \end{pmatrix}. \tag{3.1.2}$$

Observe that this is always an element of finite order when f has real coefficients. Indeed, this is an element of order 4 in $\mathrm{GL}_2(\mathbb{R})$ if $D < 0$ and an element of order 2 with determinant -1 when $D > 0$. Moreover, for any binary quadratic form f with real coefficients, $\mathcal{M}_f \in \mathrm{Aut}_{\mathbb{R}} F$. Since for a given binary form F the elements of $\mathrm{Aut}_{\mathbb{R}} F$ also fix any covariant of F, we see that quadratic covariants f of F naturally give candidates for $\mathrm{Aut}_{\mathbb{R}} F$ via the map $f \mapsto \mathcal{M}_f$.

Another way to associate a matrix to a binary quadratic form $f(x,y) = ax^2 + bxy + cy^2$ with real coefficients of discriminant $D \neq 0$ is the following:

$$\mathcal{U}_f = \frac{1}{2D} \begin{pmatrix} b\sqrt{-3D} - D & 2c\sqrt{-3D} \\ -2a\sqrt{-3D} & -b\sqrt{-3D} - D \end{pmatrix}. \tag{3.1.3}$$

A quick calculation reveals that this matrix always has order 3 in $\mathrm{GL}_2(\mathbb{C})$, and when $D < 0$, this matrix has order 3 in $\mathrm{GL}_2(\mathbb{R})$. Further, one checks that $\mathcal{U}_f \in \mathrm{Aut}_{\mathbb{R}} f$ when $D < 0$ and

$\mathcal{U}_f \in \mathrm{Aut}_{\mathbb{C}}\, f$ otherwise.

If we consider the matrices in (3.1.2) and (3.1.3) not as elements in $\mathrm{GL}_2(\mathbb{C})$ but elements in $\mathrm{PGL}_2(\mathbb{C})$, then we can remove the weighting factor. Put

$$\mathcal{M}_f^* = \begin{pmatrix} b & 2c \\ -2a & -b \end{pmatrix} \tag{3.1.4}$$

and

$$\mathcal{U}_f^* = \begin{pmatrix} b\sqrt{-3D} - D & 2c\sqrt{-3D} \\ -2a\sqrt{-3D} & -b\sqrt{-3D} - D \end{pmatrix}. \tag{3.1.5}$$

We will show that certain explicit quadratic covariants of binary cubic and quartic forms completely determines the structure of the automorphism group. The nature of these quadratic covariants varies between the degree 3 and the degree 4 case, so we will introduce them separately below.

3.1.1 Binary cubic forms

Suppose

$$F(x, y) = b_3x^3 + b_2x^2y + b_1xy^2 + b_0y^3$$

is a binary cubic form with integer coefficients and non-zero discriminant. We shall assume, after applying a $\mathrm{GL}_2(\mathbb{Z})$-action if necessary, that $b_3 \neq 0$. The ring of polynomial invariants of binary cubic forms under $\mathrm{GL}_2(\mathbb{Z})$-action is generated by a single element, which we can take to be the discriminant given by

$$\Delta(F) = b_2^2b_1^2 - 4b_3b_1^3 - 4b_2^3b_0 - 27b_3^2b_0^2 - 18b_3b_2b_1b_0. \tag{3.1.6}$$

There is a single *rational* quadratic covariant of F, given by the Hessian (3.0.2). However, Julia identified three additional quadratic covariants with typically irrational coefficients which depend on the roots $\theta_1, \theta_2, \theta_3$ of F. We follow Cremona [31] and write the Julia covariant with respect to the root θ of $F(x, 1)$ as follows:

$$J_\theta(x, y) = \alpha_\theta x^2 + \beta_\theta xy + \gamma_\theta y^2, \tag{3.1.7}$$

where

$$\begin{aligned}
\alpha_\theta &= 9b_3^2\theta^2 + 6b_3b_2\theta + 6b_3b_1 - b_2^2, \\
\beta_\theta &= 6b_3b_2\theta^2 + 6(b_2^2 - b_3b_1)\theta + 2b_2b_1, \\
\gamma_\theta &= 3b_3b_1\theta^2 + 3(b_2b_1 - 3b_3b_0)\theta + 2b_1^2 - 3b_2b_0.
\end{aligned}$$

We will also require the so-called *cubicovariant* of F, which we call $F_3(x,y)$, given by

$$F_3(x,y) = (2b_2^3 + 27b_3^2b_0 - 9b_3b_2b_1)x^3 + 3(b_2^2b_1 + 9b_3b_2b_0 - 6b_3b_1^2)x^2y - \tag{3.1.8}$$
$$3(b_2b_1^2 + 9b_3b_1b_0 - 6b_2^2b_0)xy^2 - (2b_1^3 + 27b_3b_0^2 - 9b_2b_1b_0)y^3.$$

Cremona showed in [31] that the sextic covariant $F_6(x,y)$, given by

$$F_6(x,y) = \frac{1}{2}\left(F_3^2 - 27\Delta(F)F^2\right),$$

is the product of the Julia covariants. In particular, we have

$$F_6(x,y) = J_{\theta_1}(x,y)J_{\theta_2}(x,y)J_{\theta_3}(x,y). \tag{3.1.9}$$

An explicit calculation shows that each of the Julia covariants have discriminant equal to $12\Delta(F)$.

Even though our principal interest is in studying $\mathrm{Aut}_{\mathbb{Q}} F$, it is actually simpler to discuss the problem in full generality. Indeed, we shall study the group $\mathrm{Aut}_{\mathrm{PGL}_2(\mathbb{C})} F$, which is the finite subgroup of $\mathrm{PGL}_2(\mathbb{C})$ which fixes F under the substitution action. Recall the Hessian $q_F(x,y)$ from (3.0.2), with coefficients A, B, C. Define the element in $\mathrm{PGL}_2(\mathbb{C})$ given by

$$\mathcal{H}_F = M_{q_F} = \begin{pmatrix} B & 2C \\ -2A & -B \end{pmatrix}. \tag{3.1.10}$$

Similarly, for each Julia invariant J_θ, consider the associated matrix in $\mathrm{PGL}_2(\mathbb{C})$ given by

$$\mathcal{J}_\theta = M_{J_\theta} = \begin{pmatrix} \beta_\theta & 2\gamma_\theta \\ -2\alpha_\theta & -\beta_\theta \end{pmatrix}. \tag{3.1.11}$$

Put

$$\mathcal{T}_\theta = \frac{1}{2D}\mathcal{J}_\theta\mathcal{H}_F.$$

We shall prove the following:

Theorem 3.1.1. *Let F be a binary cubic form with complex coefficients and non-zero discriminant. Suppose that the leading coefficient b_3 of F is non-zero, and let $\theta_1, \theta_2, \theta_3$ be the roots of $F(x,1)$. Then the $\mathrm{GL}_2(\mathbb{C})$-automorphism group $\mathrm{Aut}_{\mathbb{C}} F$ of F is generated by $\mathcal{T}_{\theta_i}$ for $i = 1,2,3$, $\omega I_{2\times 2}$ where ω is a primitive third root of unity, and*

$$\mathcal{U}_{q_F} = \frac{1}{2D}\begin{pmatrix} B\sqrt{-3D} - D & 2C\sqrt{-3D} \\ -2A\sqrt{-3D} & -B\sqrt{-3D} - D \end{pmatrix}$$

with A, B, C given as in (3.0.3) and $D = B^2 - 4AC$.

We shall call $\mathcal{U}_{q_F}$ the *Hooley matrix* with respect to F. Specializing to $\mathrm{Aut}_{\mathbb{Q}} F$, we are able to completely characterize when binary cubic forms F with integer coefficients and non-zero discriminant may have non-trivial rational automorphism groups in terms of the reducibility and Galois structure of F. Indeed, we shall prove:

Theorem 3.1.2. *Let F be a binary cubic form with integer coefficients and non-zero discriminant. Then:*

1. $\mathrm{Aut}\, F = \mathbf{C}_1 = \{I_{2\times 2}\}$ *if and only if F is irreducible and $\Delta(F)$ is not a square.*
2. $\mathrm{Aut}\, F$ *is generated by $\mathcal{U}_{q_F} \in \mathrm{GL}_2(\mathbb{Q})$ and is isomorphic to $\mathcal{C}_3$ if and only if F is irreducible and $\Delta(F)$ is a square.*
3. $\mathrm{Aut}\, F$ *is generated by $\mathcal{T}_\theta$ for the unique rational root θ of $F(x,1)$ and is isomorphic to $\mathcal{C}_2$ if and only if F has exactly one rational linear factor over $\mathbb{Q}$, corresponding to the root θ.*
4. $$\mathrm{Aut}\, F = \{I_{2\times 2}, \mathcal{U}_{q_F}, \mathcal{U}_{q_F}^2, \mathcal{T}_{\theta_1}, \mathcal{T}_{\theta_2}, \mathcal{T}_{\theta_3}\} \cong \mathcal{D}_3$$
   if and only if F splits completely over $\mathbb{Q}$.

Theorems 3.1.1 and 3.1.2 can be used to deduce the following interesting consequence which characterizes $\mathrm{Aut}\, F$ in terms of the reducibility of the degree 6 covariant $F_6(x,y)$:

Theorem 3.1.3. *Let F be a binary cubic form with integer coefficients and non-zero discriminant. Then*

1. $\mathrm{Aut}\, F = \mathbf{C}_1 = \{I_{2\times 2}\}$ *if and only if $F_6(x,y)$ is irreducible and the discriminant of $q_F(x,y)$ is not -3 times a square;*
2. $\mathrm{Aut}\, F$ *is generated by $\mathcal{U}_{q_F} \in \mathrm{GL}_2(\mathbb{Q})$ and is isomorphic to $\mathcal{C}_3$ is irreducible and the discriminant of $q_F(x,y)$ is a square;*
3. $\mathrm{Aut}\, F$ *is generated by $\mathcal{T}_\theta$ for the unique rational root θ of $F(x,1)$ and is isomorphic to $\mathcal{C}_2$ if and only if $F_6(x,y)$ has exactly one quadratic factor over $\mathbb{Q}$ equal to the Julia covariant J_θ; and*
4. $$\mathrm{Aut}\, F = \{I_{2\times 2}, \mathcal{U}_{q_F}, \mathcal{U}_{q_F}^2, \mathcal{T}_{\theta_1}, \mathcal{T}_{\theta_2}, \mathcal{T}_{\theta_3}\} \cong \mathcal{D}_3$$
   if and only if $F_6(x,y)$ has three quadratic factors over $\mathbb{Q}$.

Theorem 3.1.2, combined with Theorem 1.2 of [100], has the following consequence. It can be checked that

$$\beta_\theta B - 4A\gamma_\theta = -\beta_\theta B + 4\alpha_\theta C,$$

where A, B, C are as in (3.0.3) and $\alpha_\theta, \beta_\theta, \gamma_\theta$ are as in (3.1.7). Now put

$$a_\theta = B\alpha_\theta + A\beta_\theta, b_\theta = B\beta_\theta - 4A\gamma_\theta, c_\theta = C\beta_\theta - \gamma_\theta B.$$

Then

$$\mathcal{T}_\theta = \frac{1}{2D}\begin{pmatrix} b_\theta & 2c_\theta \\ -2a_\theta & -b_\theta \end{pmatrix}.$$

If θ is rational, then write

$$m_\theta = \frac{2D}{\gcd(2a_\theta, b_\theta, 2c_\theta)}.$$

Now define m_1, m_2, m_3, m_4 as follows:

1. If $\Delta(F)$ is not a square and F is irreducible over $\mathbb{Q}$, then set $m_i = 1$ for $i = 1, 2, 3, 4$.
2. If $\Delta(F)$ is a square and F is irreducible over $\mathbb{Q}$, then set $m_i = 1$ for $i = 1, 2, 3$ and set m_4 as in (3.0.6).
3. If F has exactly one rational root, say θ_1, then set $m_1 = m_{\theta_1}$ and $m_i = 1$ for $i = 2, 3, 4$.
4. If F has three rational roots, then set $m_i = m_{\theta_i}$ for $i = 1, 2, 3$ and set m_4 as in (3.0.6).

In all cases, put $m = \mathrm{lcm}(m_1, m_2, m_3, m_4)$. We then obtain the following theorem:

Theorem 3.1.4. *Let $F(x, y)$ be an integral binary cubic form with non-zero discriminant $\Delta(F)$. Then*

1. *If $F(x, y)$ is irreducible and the discriminant $\Delta(F)$ of F is not a perfect square, then*
$$W_F = 1.$$
2. *If $F(x, y)$ is irreducible and $\Delta(F)$ is a square, then*
$$W_F = 1 - \frac{2}{3m}.$$
3. *If $F(x, y)$ has exactly one rational linear factor, then*
$$W_F = 1 - \frac{1}{2m}.$$

4. If $F(x,y)$ has three rational factors, then

$$W_F = 1 - \frac{1}{2m_1} - \frac{1}{2m_2} - \frac{1}{2m_3} - \frac{2}{3m_4} + \frac{4}{3m}.$$

Cases (1) and (2) of Theorem 3.1.4 are due to Hooley in [64] and [70] respectively.

3.1.2 Binary quartic forms

For a binary quartic form

$$F(x,y) = a_4x^4 + a_3x^3y + a_2x^2y^2 + a_1xy^3 + a_0y^4,$$

we may apply a $\mathrm{GL}_2(\mathbb{Z})$ element if necessary to obtain an equivalent form with non-zero leading coefficient. Therefore, we may factor F over $\mathbb{C}$ as

$$F(x,y) = a_4(x - \theta_1 y)(x - \theta_2 y)(x - \theta_3 y)(x - \theta_4 y).$$

Define $\chi(F)$ to be the number of real roots of F. We will label the roots of F as follows:

$$\begin{cases} \theta_1 > \theta_2 > \theta_3 > \theta_4, & \text{if } \chi(F) = 4, \\ \theta_1 > \theta_2, \theta_3 = \overline{\theta_4}, \Im(\theta_3) > 0, & \text{if } \chi(F) = 2, \\ \theta_1 = \overline{\theta_2}, \theta_3 = \overline{\theta_4}, \Im(\theta_1) > 0, \Im(\theta_3) < 0, & \text{if } \chi(F) = 0. \end{cases} \tag{3.1.12}$$

Here $\Im(z)$ refers to the imaginary part of the complex number z.

It is known that binary quartic forms F have two algebraically independent invariants, known as the I and J invariants, defined by

$$I(F) = 12a_4a_0 - 3a_3a_1 + a_2^2, \text{ and} \tag{3.1.13}$$

$$J(F) = 72a_4a_2a_0 + 9a_3a_2a_1 - 27a_4a_1^2 - 27a_0a_3^2 - 2a_2^3.$$

Write $\mathcal{Q}_F(x)$ for the *cubic resolvent* of F, defined by

$$\mathcal{Q}_F(x) = x^3 - 3I(F)x + J(F). \tag{3.1.14}$$

From the definition of $\mathcal{Q}_F(x)$ we see that the roots β_i's of $\mathcal{Q}_F(x)$ are given by

$$\beta_1 = 3a_4(\theta_1\theta_2 + \theta_3\theta_4) - a_2, \tag{3.1.15}$$

$$\beta_2 = 3a_4(\theta_1\theta_3 + \theta_2\theta_4) - a_2,$$

and

$$\beta_3 = 3a_4(\theta_1\theta_4 + \theta_2\theta_3) - a_2.$$

Furthermore, let us put

$$D_1 = 4(\theta_1 - \theta_3)(\theta_1 - \theta_4)(\theta_2 - \theta_3)(\theta_2 - \theta_4), \tag{3.1.16}$$
$$D_2 = 4(\theta_1 - \theta_2)(\theta_1 - \theta_4)(\theta_3 - \theta_2)(\theta_3 - \theta_4),$$

and

$$D_3 = 4(\theta_1 - \theta_2)(\theta_1 - \theta_3)(\theta_4 - \theta_2)(\theta_4 - \theta_3).$$

By (3.1.12), we see that β_1, D_1 are real for $\chi(F) = 0, 2, 4$. If $\chi(F) = 4$, then clearly β_i, D_i are real for $i = 1, 2, 3$. If $\chi(F) = 0$, then by noting that

$$\theta_1 - \theta_2, \theta_3 - \theta_4 \in \mathbb{R}$$

and

$$\theta_1 - \theta_4 = \overline{\theta_2 - \theta_3}, \theta_1 - \theta_3 = \overline{\theta_2 - \theta_4},$$

we see that D_i is real for $i = 1, 2, 3$. A similar argument yields that β_i is real for $i = 1, 2, 3$. When $\chi(F) = 2$, we see that $\beta_2, \beta_3, D_2, D_3$ are not real.

Now put

$$A_1 = \theta_1 + \theta_2 - \theta_3 - \theta_4, B_1 = 2(\theta_3\theta_4 - \theta_1\theta_2), C_1 = \theta_1\theta_2(\theta_3 + \theta_4) - \theta_3\theta_4(\theta_1 + \theta_2), \tag{3.1.17}$$

$$A_2 = \theta_1 + \theta_3 - \theta_2 - \theta_4, B_2 = 2(\theta_2\theta_4 - \theta_1\theta_3), C_2 = \theta_1\theta_3(\theta_2 + \theta_4) - \theta_2\theta_4(\theta_1 + \theta_3),$$

and

$$A_3 = \theta_1 + \theta_4 - \theta_2 - \theta_3, B_3 = 2(\theta_2\theta_3 - \theta_1\theta_4), C_3 = \theta_1\theta_4(\theta_2 + \theta_3) - \theta_2\theta_3(\theta_1 + \theta_4).$$

Cremona showed in [31] that the quadratic forms given by

$$\mathfrak{C}_i(x, y) = A_i x^2 + B_i xy + C_i y^2 \tag{3.1.18}$$

are covariants of F. We shall call the $\mathfrak{C}_i$'s *Cremona covariants*. Next put

$$U_i = \mathcal{M}_{\mathfrak{C}_i} = \frac{1}{\sqrt{|D_i|}} \begin{pmatrix} B_i & 2C_i \\ -2A_i & -B_i \end{pmatrix}. \tag{3.1.19}$$

Observe that $\det U_1 = -1$ for any binary quartic form F with real coefficients, and if $\Delta(F) > 0$, then $U_2 \in \mathrm{GL}_2(\mathbb{R})$ and $\det U_2 = 1$. Moreover, U_2 is an element of order 4 in $\mathrm{GL}_2(\mathbb{R})$.

We now state our main theorem characterizing the automorphism group $\mathrm{Aut}_{\mathbb{R}} F$ for binary quartic forms:

Theorem 3.1.5. *Let $F(x, y)$ be a binary quartic form with real coefficients and non-zero discriminant. Then*

(a) If $\Delta(F) > 0$, then $\mathrm{Aut}_{\mathbb{R}} F$ is generated by U_1, U_2, U_3.

(b) If $\Delta(F) < 0$, then $\mathrm{Aut}_{\mathbb{R}} F$ is generated by U_1 and $-I_{2\times 2}$.

Over $\mathbb{C}$, the group of automorphisms of a binary quartic form F can be strictly larger than over $\mathbb{R}$. Indeed, whenever the I or J invariant of F vanishes, the automorphism group of F in $\mathrm{PGL}_2(\mathbb{C})$ is larger than when $I(F)J(F) \neq 0$. The case $I(F) = 0$ was studied by Klein (see [8]), and these are called *Klein forms* of degree 4. In this case, it is known that the $\mathrm{PGL}_2(\mathbb{C})$-automorphism group of F is isomorphic to the alternating group $\mathcal{A}_4$. When $J(F) = 0$, the $\mathrm{PGL}_2(\mathbb{C})$-automorphism group of F contains a non-trivial element of order 8 which we denote by $\mathcal{G}_F$. We thus have:

Theorem 3.1.6. *Let $F(x, y)$ be a binary quartic form with complex coefficients and non-zero discriminant. Then*

$$\mathrm{Aut}_{\mathbb{C}} F = \langle U_1, U_2, U_3, \sqrt{-1} \cdot I_{2\times 2} \rangle$$

if $I(F) \cdot J(F) \neq 0$ and

$$\mathrm{Aut}_{\mathbb{C}} F = \langle U_1, U_2, U_3, \mathcal{G}_F, \sqrt{-1} \cdot I_{2\times 2} \rangle$$

if $J(F) = 0$. Moreover, when $I(F) = 0$ there exists an order 3 element in $\mathrm{Aut}_{\mathbb{C}} F$ and the $\mathrm{PGL}_2(\mathbb{C})$ automorphism group of F is isomorphic to the alternating group $\mathcal{A}_4$.

We note that Cremona and Fisher's work on equivalence of binary quartic forms in [32] allows us to determine $\mathrm{Aut}_{\mathbb{R}} F$ completely by examining the bilinear factors of the bihomogeneous form

$$F(x,y)F_4(u,v) - F(u,v)F_4(x,y).$$

However, their notion of an element in $\mathrm{Aut}_{\mathbb{R}} F$ being defined over a given field $\mathbb{F}$ is coarser than ours, and this is important for the present problem. A suitable refinement of Cremona and Fisher's work gives us another way to obtain $\mathrm{Aut}\, F$.

Theorem 3.1.5 allows us to determine $\mathrm{Aut}_{\mathbb{Q}} F$ from $\mathrm{Aut}_{\mathbb{R}} F$. In the cubic case of a cubic form F, the structure of $\mathrm{Aut}\, F$ is heavily influenced by how F factors over $\mathbb{Q}$. We will show that in the case of a quartic form F, it is not whether F factors over $\mathbb{Q}$ that is critical but rather the splitting properties of the cubic resolvent $\mathcal{Q}_F(x)$. In order to state our results, we will need to define several covariants of quartic forms F.

The Hessian covariant of the binary quartic form F is of degree 4, given by

$$\begin{aligned} F_4(x,y) = (3a_3^2 - 8a_4a_2)x^4 + 4(a_3a_2 - 6a_4a_1)x^3y + 2(2a_2^2 - 24a_4a_0 - 3a_3a_1)x^2y^2 \\ +4(a_2a_1 - 6a_3a_0)xy^3 + (3a_1^2 - 8a_2a_0)y^4 \end{aligned} \tag{3.1.20}$$

and the degree 6 covariant $F_6(x,y)$ of F, is given by (see [31]):

$$\begin{aligned} F_6(x,y) = {} & (a_3^3 + 8a_4^2a_1 - 4a_4a_3a_2)x^6 + 2(16a_4^2a_0 + 2a_4a_3a_1 - 4a_4a_2^2 + a_3^2a_2)x^5y \\ & + 5(8a_4a_3a_0 + a_3^2a_1 - 4a_4a_2a_1)x^4y^2 + 20(a_3^2a_0 - a_4a_1^2)x^3y^3 \\ & - 5(8a_4a_1a_0 + a_3a_1^2 - 4a_3a_2a_0)x^2y^4 - 2(16a_4a_0^2 + 2a_3a_1a_0 - 4a_2^2a_0 + a_2a_1^2)xy^5 \\ & - (a_1^3 + 8a_3a_0^2 - 4a_2a_1a_0)y^6. \end{aligned} \tag{3.1.21}$$

The Hessian covariant $F_4(x,y)$, $F(x,y)$ and $F_6(x,y)$ satisfy a syzygy:

$$F_4^3 - 3I(F)(-4F)^2F_4 + J(F)(-4F)^3 = 27F_6^2. \tag{3.1.22}$$

Let $\beta_1, \beta_2, \beta_3$ be the roots of $\mathcal{Q}_F(x)$. Then (3.1.22) implies that

$$F_6^2(x,y) = \tag{3.1.23}$$

$$\left(\frac{1}{3}(F_4(x,y) + 4\beta_1F(x,y))\right)\left(\frac{1}{3}(F_4(x,y) + 4\beta_2F(x,y))\right)\left(\frac{1}{3}(F_4(x,y) + 4\beta_3F(x,y))\right).$$

from (3.1.23).

Indeed, each of the forms

$$\frac{1}{3}\left(F_4(x,y)+4\beta_i F(x,y)\right)$$

is in fact a square of a quadratic form with complex coefficients. Moreover, we have the equation

$$a_4^2\mathfrak{C}_i^2(x,y)=\frac{1}{3}\left(F_4(x,y)+4\beta_i F(x,y)\right) \tag{3.1.24}$$

with $\mathfrak{C}_i(x,y)$ given as in (3.1.18). Note that the right hand side of (3.1.24) need not have non-negative leading coefficient, which means that it need not be the square of a real quadratic form. Thus, the leading coefficient of $\mathfrak{C}_i(x,y)$ is either real or purely imaginary. By multiplying by -1 we can take the right hand side of (3.1.24) to be the square of a quadratic form with integer coefficients, say $Q_i(x,y)$. We have

$$Q_i(x,y)=\begin{cases} a_4\mathfrak{C}_i(x,y), & \text{if the leading coefficient of } \mathfrak{C}_i(x,y) \text{ is real;} \\ a_4\sqrt{-1}\mathfrak{C}_i(x,y), & \text{if the leading coefficient of } \mathfrak{C}_i(x,y) \text{ is purely imaginary.} \end{cases} \tag{3.1.25}$$

We will write

$$Q_i(x,y)=\mathfrak{a}_i x^2+\mathfrak{b}_i xy+\mathfrak{c}_i y^2,$$

and

$$\mathfrak{d}_i=\mathfrak{b}_i^2-4\mathfrak{a}_i\mathfrak{c}_i.$$

Recall the roots β_i of the cubic resolvent $\mathcal{Q}_F(x)$ in (3.1.15). We may now state our next main theorem:

Theorem 3.1.7. *Let F be a binary quartic form with integer coefficients and non-zero discriminant. Then $U_i \in \mathrm{GL}_2(\mathbb{Q})$ if and only if β_i is an integer and $|\mathfrak{d}_i|$ is a square. Moreover, we have:*

1. $\mathrm{Aut}_{\mathbb{Q}} F=\langle U_1,U_2,U_3\rangle\cong\mathcal{D}_4$ *if and only if* $U_i\in\mathrm{GL}_2(\mathbb{Q})$ *for* $i=1,2,3$*;*
2. $\mathrm{Aut}_{\mathbb{Q}} F=\langle U_2\rangle\cong\mathcal{C}_4$ *if and only if* $U_2\in\mathrm{GL}_2(\mathbb{Q})$ *and* $U_1,U_3\notin\mathrm{GL}_2(\mathbb{Q})$*;*
3. $\mathrm{Aut}_{\mathbb{Q}} F=\langle U_1,I_{2\times 2}\rangle$ *or* $\langle U_3,I_{2\times 2}\rangle$ *and* $\mathrm{Aut}_{\mathbb{Q}} F\cong\mathcal{C}_2\times\mathcal{C}_2$ *if and only if there exists exactly one index* $i\in\{1,3\}$ *for which* $U_i\in\mathrm{GL}_2(\mathbb{Q})$*; and*
4. $\mathrm{Aut}_{\mathbb{Q}} F=\mathbf{C}_2$ *if and only if* U_i *is not in* $\mathrm{GL}_2(\mathbb{Q})$ *for* $i=1,2,3$.

Unlike the cubic case, the possibilities for $\operatorname{Aut} F$ are not drastically different for reducible forms. Indeed, all of the cases in Theorem 3.1.7 can occur for irreducible binary quartic forms. We can use Theorem 3.1.7 to deduce the value of W_F for binary quartic forms.

If $\beta_i \in \mathbb{Z}$, then U_i is given by

$$U_i = \frac{1}{\sqrt{|\mathfrak{d}_i|}} \begin{pmatrix} \mathfrak{b}_i & 2\mathfrak{c}_i \\ -2\mathfrak{a}_i & -\mathfrak{b}_i \end{pmatrix}.$$

If in addition $|\mathfrak{d}_i|$ is a square, then put $m_i = \dfrac{\sqrt{\mathfrak{d}_i}}{\gcd(2\mathfrak{a}_i, \mathfrak{b}_i, 2\mathfrak{c}_i)}$. If β_i is not an integer or $|\mathfrak{d}_i|$ is not a square, put $m_i = 1$. Set $m = \operatorname{lcm}(m_1, m_2, m_3)$. We then have:

Theorem 3.1.8. *Let $F(x, y)$ be a binary quartic form with integer coefficients and non-zero discriminant $\Delta(F)$. We have the following:*

1. *If the cubic resolvent $\mathcal{Q}_F(x)$ has three integral roots $\beta_1, \beta_2, \beta_3$ and the absolute value of the discriminant $\mathfrak{d}_i$ of $Q_i(x, y)$ is a square for $i = 1, 2, 3$, then*

$$W_F = \frac{1}{2}\left(1 - \frac{1}{2m_1} - \frac{1}{2m_2} - \frac{1}{2m_3} + \frac{3}{4m}\right).$$

2. *If there is exactly one integral root β of $\mathcal{Q}_F(x)$ such that $|\mathfrak{d}_\beta|$ is a square, then*

$$W_F = \frac{1}{2}\left(1 - \frac{1}{2m}\right).$$

3. *If $\mathcal{Q}_F(x)$ is irreducible over $\mathbb{Q}$ or for all integral roots β of $\mathcal{Q}_F(x)$ we have $|\mathfrak{d}_\beta|$ is not the square of an integer, then*

$$W_F = \frac{1}{2}.$$

Hooley's result (3.0.9) corresponds to case 1-(b) of Theorem 3.1.8 with $m = 1$, and 1-(a) of Theorem 3.1.8 with $m_2 = 1$ and $m_1 = m_3 = m = AC$ respectively.

Stewart provided many examples of binary quartic forms with large automorphism groups in [98], as well as giving all finite subgroups of $\mathrm{GL}_2(\mathbb{Z})$ up to conjugacy. We remark however that the situation changes when we replace $\mathrm{GL}_2(\mathbb{Z})$-conjugacy with $\mathrm{GL}_2(\mathbb{Q})$-conjugacy. Indeed, the groups $\mathbf{D}_i^*$ and $\mathbf{D}_i$ for $i = 1, 2, 3$ in Stewart's Table 1 are in fact

$\mathrm{GL}_2(\mathbb{Q})$ conjugate. See Table 1 of the present paper.

The final piece of the puzzle is the computation of the area A_F for binary quartic forms F. M.A. Bean gave an elegant method for calculating the value of A_F for binary quartic forms in [6]. Following [6], we label the roots as in (3.1.12). Bean stated his results in terms of the *cross ratio* of the roots of $F(x,1)$, given by

$$\lambda_F = \frac{(\theta_1-\theta_3)(\theta_2-\theta_4)}{(\theta_1-\theta_4)(\theta_2-\theta_3)}.$$

We then have

$$\lambda_F = \frac{\beta_3-\beta_1}{\beta_2-\beta_1},$$

where, as we recall, β_1,β_2,β_3 are the roots of the cubic resolvent $\mathcal{Q}_F(x)$ of F given as in (3.1.15). Thus, the computation of λ_F does not rely on finding the roots of $F(x,1)$ but only its resolvent cubic $\mathcal{Q}_F(x)$.

We now introduce, as in Bean's paper [6], the auxiliary quantity

$$\delta_F = \begin{cases} \lambda_F, & \text{if } \chi(F)=4, \\ \dfrac{1}{2}\left(1+\sqrt{\dfrac{1+\Re(\lambda_F)}{2}}\right), & \text{if } \chi(F)=2, \\ \left(\dfrac{\sqrt{\lambda_F}-1}{\sqrt{\lambda_F}+1}\right)^2, & \text{if } \chi(F)=0. \end{cases} \tag{3.1.26}$$

Here $\Re(z)$ refers to the real part of a complex number z. Bean showed that if one orders the the θ_i's in the manner as in (3.1.12), then the quantity δ_F always lies in the interval $(0,1)$ in [6], so we will assume that $0<\delta_F<1$.

The computation of A_F involves the evaluation of an elliptic integral. Indeed, it can be shown that one can reduce the computation of A_F to evaluating an *elliptic integral of the first kind* (see [26]). We will use the following representation for a complete elliptic integral of the first kind, with parameter α:

$$K(\alpha) = \int_0^1 \frac{dt}{\sqrt{t(1-t)(1-\alpha t)}},$$

where $\alpha \in (0,1)$. We now put

$$\begin{aligned}
\mathfrak{J}_4(\alpha) &= 2\alpha^{1/6}(1-\alpha)^{1/6}(K(\alpha)+K(1-\alpha)),\\
\mathfrak{J}_2(\alpha) &= 2^{1/3}\alpha^{1/12}(1-\alpha)^{1/12}(K(\alpha)+K(1-\alpha)),\\
\mathfrak{J}_0(\alpha) &= 2^{1/3}\alpha^{1/12}(1-\alpha)^{1/3}K(1-\alpha),
\end{aligned}$$

for $\alpha \in (0,1)$.

Bean's result in [6] can now be summarized as follows: for F a binary quartic form with real coefficients, we have

$$|\Delta(F)|^{\frac{1}{12}}A_F = \begin{cases} \mathfrak{J}_4(\delta_F) & \text{if } \chi(F)=4,\\ \mathfrak{J}_2(\delta_F) & \text{if } \chi(F)=2,\\ \mathfrak{J}_0(\delta_F) & \text{if } \chi(F)=0. \end{cases} \tag{3.1.27}$$

In [100], we have proved a general theorem which shows that the constant C_F in Theorem 3.0.2 is always a rational multiple of A_F, and this rational constant can be determined explicitly as a function of $\operatorname{Aut} F$. Thus, the main novelty of this paper is to show that $\operatorname{Aut} F$ can be obtained explicitly when $d = 3, 4$ and that there are simple criteria available that enables one to check immediately whether $\operatorname{Aut} F$ is trivial, and if it is not trivial, explicitly obtain it.

One of the main technical advances in this area that we shall mention once more is Heath-Brown's Theorem 8 in [53]. In particular, he proved that given a binary form F of degree $d \geq 3$ and such that no linear factor of F has multiplicity exceeding $d/2$, that the number of integers in a given interval $[1, Z]$ which can be *essentially represented*, meaning it has two representations which are not related by an element of $\operatorname{Aut} F$, is sufficiently small.

3.1.3 Lines on algebraic surfaces of degree 3 and 4 defined by binary cubic and quartic forms

In [17], it is proved that the surface X defined by (3.0.10) contains exactly $4(4+\upsilon_F)$ many lines when $d = 4$, where υ_F is the number of automorphisms of $\mathbb{P}^1(\mathbb{C})$ which permutes the roots of F. We shall prove that υ_F is equal to 4 or 8 when $d = 4$. More precisely, we will show that $\upsilon_F = 4$ when $J(F) \neq 0$, $\upsilon_F = 8$ when $J(F) = 0$, and $\upsilon_F = 12$ when $I(F) = 0$.

Further, our methods will show that $\upsilon_F = 6$ for all binary cubic forms F with non-zero discriminant.

For a given binary cubic form F with integer coefficients and non-zero discriminant, write K for the field of smallest degree for which all lines contained in the surface X defined by (3.0.10) is defined over K. We put $\mathbb{F}$ for the splitting field of F, and we shall denote by ω a primitive third root of unity. We will prove the following theorem for cubic surfaces X defined (3.0.10) and a binary cubic form $F(x, y)$:

Theorem 3.1.9. *Let F be a binary cubic form with integer coefficients and non-zero discriminant. Let X be the cubic surface defined by (3.0.10). Then*

1. *If F is irreducible and $\Delta(F)$ is a square, then $[K : \mathbb{Q}] = 6$ and K is obtained by adjoining a root of $F(x, 1)$ and ω.*
2. *If F is irreducible with positive non-square discriminant, then $[K : \mathbb{Q}] = 12$ and K is obtained by adjoining all roots of $F(x, 1)$ and ω.*
3. *If F is irreducible with negative discriminant, then $[K : \mathbb{Q}] = 6$ or 12, depending on whether or not the field $\mathbb{K}$ obtained by adjoining a root of $F(x, 1)$ is a pure cubic field or not. If $\mathbb{K}$ is a pure cubic field then $[K : \mathbb{Q}] = 6$ and if $\mathbb{K}$ is not a pure cubic field then $[K : \mathbb{Q}] = 12$.*
4. *If F has exactly one linear factor over $\mathbb{Q}$ and $\Delta(F) > 0$, then $[K : \mathbb{Q}] = 4$ and K is obtained by adjoining the roots of $F(x, 1)$ and ω.*
5. *If F has exactly one linear factor over $\mathbb{Q}$ and $\Delta(F) < 0$, then $[K : \mathbb{Q}] = 2$ or 4 depending on whether the splitting field $\mathbb{F}$ of F contains the third roots of unity. If so, then $K = \mathbb{Q}(\omega)$ and if not, then K is obtained by adjoining the roots of $F(x, 1)$ and ω.*
6. *If F splits completely over $\mathbb{Q}$, then $K = \mathbb{Q}(\omega)$.*

For a given binary quartic form F with integer coefficients and non-zero discriminant, write K for the field of smallest degree for which all lines contained in the surface X defined by (3.0.10) is defined over K. We put $\mathbb{F}$ for the splitting field of F. We will prove the following theorem for quartic surfaces X defined by (3.0.10) and a binary quartic form $F(x, y)$:

Theorem 3.1.10. *Let F be a binary quartic form with integer coefficients and non-zero discriminant. Let X be the quartic surface defined by (3.0.10). Then $K = \mathbb{F}(\sqrt{D_1}, \sqrt{D_2}, \sqrt{D_3}, \sqrt{-1})$. Further, the degree of K over $\mathbb{Q}$ is at most* 384.

In Sections 3.2 and 3.3, we will determine all possible automorphisms of a real binary cubic or quartic form respectively with non-zero discriminant in $\mathrm{GL}_2(\mathbb{R})$ and determine when these automorphisms lie in $\mathrm{GL}_2(\mathbb{Q})$. As an immediate corollary to our arguments, we will also be able to give a criteria to determine, for a given binary quartic form with real coefficients and any sub-field $\mathbb{F}$ of $\mathbb{R}$, the corresponding automorphism group $\mathrm{Aut}_{\mathbb{F}}(F)$ in $\mathrm{GL}_2(\mathbb{F})$. In Section 3.4, we will consider the arithmetical consequences of various possible rational automorphism groups of binary quartic forms with non-zero discriminant.

3.2 Automorphism groups of binary cubic forms from its quadratic covariants

In this section we shall prove that the $\mathrm{PGL}_2(\mathbb{C})$-automorphism group of a binary cubic form F can be given explicitly as a function of its quadratic covariants: the Hessian $q_F(x, y)$ and the Julia covariants J_{θ_i} for $i = 1, 2, 3$. We first prove a general result which holds for binary forms of any degree.

The following lemma shows that equivalent binary forms have conjugate automorphism groups:

Lemma 3.2.1. *Let F, G be binary forms with complex coefficients which are $\mathrm{GL}_2(\mathbb{C})$-equivalent, say $F_T(x, y) = G(x, y)$. Then*

$$\mathrm{Aut}_{\mathbb{C}} G = T^{-1}(\mathrm{Aut}_{\mathbb{C}} F)T.$$

Proof. Suppose that F, G are binary forms with complex coefficients and non-zero discriminant which are $\mathrm{GL}_2(\mathbb{C})$-equivalent, say $F_T(x, y) = G(x, y)$ with $T \in \mathrm{GL}_2(\mathbb{C})$. Suppose that $U \in \mathrm{Aut}_{\mathbb{C}} F$. Then

$$\begin{aligned} G_{T^{-1}UT}(x, y) &= F_{T(T^{-1}UT)}(x, y) \\ &= F_T(x, y) \\ &= G(x, y), \end{aligned}$$

hence $\mathrm{Aut}_{\mathbb{C}} G \subset T^{-1}(\mathrm{Aut}_{\mathbb{C}} F)T$. The reverse inclusion follows from the fact that $F(x, y) = G_{T^{-1}}(x, y)$. □

Our next result shows that under $\mathrm{GL}_2(\mathbb{C})$ action, there is just one orbit of binary cubic forms with non-zero discriminant. This follows from the fact that $\mathrm{PGL}_2(\mathbb{C})$ is 3-transitive on the projective line $\mathbb{P}^1(\mathbb{C})$. However, we shall give an explicit and elementary proof here.

Lemma 3.2.2. *Let F, G be two binary cubic forms with complex coefficients and non-zero discriminant. Then there exists $T \in \mathrm{GL}_2(\mathbb{C})$ for which $G(x, y) = F_T(x, y)$.*

Proof. It suffices to prove that every binary cubic form F with non-zero discriminant is equivalent to $F_0(x, y) = xy(x + y)$. Suppose that

$$F(x, y) = (\alpha_1 x - \beta_1 y)(\alpha_2 x - \beta_2 y)(\alpha_3 x - \beta_3 y), \alpha_i, \beta_i \in \mathbb{C} \text{ for } i = 1, 2, 3.$$

We first make the substitution

$$u = \alpha_1 x - \beta_1 y, \ v = \alpha_2 x - \beta_2 y. \tag{3.2.1}$$

This transformation is invertible, since $\Delta(F) \neq 0$. It follows that

$$F(u, v) = uv \left(\frac{(\alpha_3\beta_2 - \alpha_2\beta_3)u - (\alpha_3\beta_1 - \alpha_1\beta_3)v}{\alpha_1\beta_2 - \alpha_2\beta_1} \right).$$

From here, setting

$$s = \frac{\alpha_3\beta_2 - \alpha_2\beta_3}{\alpha_1\beta_2 - \alpha_2\beta_1} u \text{ and } t = -\frac{\alpha_3\beta_1 - \alpha_1\beta_3}{\alpha_1\beta_2 - \alpha_2\beta_1} v \tag{3.2.2}$$

shows that F is equivalent to a form of the shape

$$\mathcal{F}(x, y) = Axy(x + y)$$

for some non-zero complex number A. Finally, we can always normalize $\mathcal{F}$ by setting $u = A^{-1/3}x, v = A^{-1/3}y$, where the cube root can be taken with respect to any branch of the logarithm over $\mathbb{C}$. □

By Lemma 3.2.1 and the fact that J_{θ_i} for $i = 1, 2, 3$ and $\mathcal{H}_F$ are covariants of F, we have reduced the proof of Theorem 3.1.1 to just a single binary cubic form, which we take to be $F(x, y) = xy(x + y)$. In this case, we see that $\Delta(F) = 1$,

$$F_3(x, y) = 2x^3 + 3x^2y - 3xy^2 - 2y^3,$$

$$q_F(x, y) = x^2 + xy + y^2,$$

$$D = \Delta(q_F) = -3,$$

and

$$F_6(x,y) = (x^2 - 2xy - 2y^2)(2x^2 + 2xy - y^2)(x^2 + 4xy + y^2).$$

Thus, the Julia covariants are precisely

$$J_1(x,y) = x^2 - 2xy - 2y^2, J_2(x,y) = 2x^2 + 2xy - y^2, J_3(x,y) = x^2 + 4xy + y^2.$$

The associated matrices $\mathcal{J}_1, \mathcal{J}_2, \mathcal{J}_3$ are then given by

$$\mathcal{J}_1 = \begin{pmatrix} -2 & -4 \\ -2 & 2 \end{pmatrix}, \mathcal{J}_2 = \begin{pmatrix} 2 & -2 \\ -4 & -2 \end{pmatrix}, \mathcal{J}_3 = \begin{pmatrix} 4 & 2 \\ -2 & -4 \end{pmatrix}.$$

Next, we note that the matrix associated to the Hessian, $\mathcal{H}_F$, is given by

$$\mathcal{H}_F = \begin{pmatrix} 1 & 2 \\ -2 & -1 \end{pmatrix}.$$

Moreover, by [98], we know that the automorphism group of F even over $\mathbb{C}$ is given by

$$\mathbf{D}_3 = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle.$$

We then see that

$$\frac{1}{6}\mathcal{J}_1\mathcal{H}_F = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \frac{1}{6}\mathcal{J}_2\mathcal{H}_F = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \frac{1}{6}\mathcal{J}_3\mathcal{H}_F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

A quick calculation shows that all of these lie in $\mathbf{D}_3$, as desired. Moreover, by Hooley [64], we know that the order 3 element associated to the Hessian $x^2 + xy + y^2$, equal to $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, lies in $\operatorname{Aut} F$. This completes the proof of Theorem 3.1.1.

We shall now prove Theorem 3.1.2. We first show that if a Julia covariant J_θ of a binary cubic form F is rational, then the corresponding $\mathcal{T}_\theta$ is an element of $\mathrm{GL}_2(\mathbb{Q})$ of determinant -1 and order 2. Since the determinant of $\mathcal{J}_\theta$ is equal to the negative of the discriminant of J_θ, which by [31] has discriminant $12\Delta(F)$, we see that the determinant of $\mathcal{J}_\theta$ is $-12\Delta(F)$. Next, note that the determinant of $\mathcal{H}_F$ is equal to $3\Delta(F)$. It then follows that the determinant of $\mathcal{J}_\theta\mathcal{H}_F$ is equal to $-36\Delta(F)^2$. Further, since the Hessian is a rational covariant, $\mathcal{H}_F$ is always defined over $\mathbb{Q}$. Therefore, we see that

$$\mathcal{T}_\theta = \frac{1}{6\Delta(F)}\mathcal{J}_\theta\mathcal{H}_F$$

is an element of determinant -1 and order 2 whenever $\mathcal{J}_\theta$ is defined over $\mathbb{Q}$.

Now suppose that the roots $\theta_1, \theta_2, \theta_3$ of $F(x,1)$ are all rational. Then it is clear that the Julia covariants J_{θ_i} are rational for $i = 1, 2, 3$. Observe that (3.2.1) and (3.2.2) are all defined over the field $\mathbb{Q}(\theta_1, \theta_2, \theta_3)$. We then see that F is $\mathrm{GL}_2(\mathbb{Q})$-equivalent to a form of the shape $Axy(x+y)$ with A rational. Therefore, $\mathrm{Aut}_{\mathbb{R}} F$ is a rational conjugate of $\mathbf{D}_3$, so $\mathrm{Aut}_{\mathbb{R}} F = \mathrm{Aut}_{\mathbb{Q}} F \cong \mathcal{D}_3$.

Next, we deal with the case when $F(x,y)$ has exactly one rational linear factor $\alpha x + \beta y$, say

$$F(x,y) = (\alpha x + \beta y)(a_2 x^2 + a_1 xy + a_0 y^2)$$

where $a_2x^2 + a_1xy + a_0y^2$ is an irreducible quadratic form and $\alpha, \beta, a_2, a_1, a_0$ are integers. Put

$$u = x/\alpha, v = y/\beta. \tag{3.2.3}$$

We then have

$$F(u,v) = (u+v)(a_2' u^2 + a_1' uv + a_0' v^2),$$

where a_i' are rational. Observe that (3.2.3) is defined over $\mathbb{Q}$. Put $f(x,y) = a_2'x^2 + a_1'xy + a_0'y^2 = ax^2 + bxy + cy^2$. We wish to find another transformation

$$T = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})$$

such that $f_T(x,y)$ is symmetric while T fixes the sum $u+v$. Moreover, we shall assume that $t_1t_4 - t_2t_3 = 1$. These two conditions imply that there exist rational numbers s, t such that $t_1 = s, t_3 = 1-s, t_2 = t, t_4 = 1-t$. Further, we deduce by our assumptions that $s = t+1$. We then need to solve the equation

$$a(t+1)^2 b(t+1)(-t) + ct^2 = at^2 + bt(1-t) + c(1-t)^2.$$

Expanding both sides, we see that this is equivalent to

$$2at + a - bt = bt + c - 2ct.$$

Isolating for t, we have

$$2(a - b + c)t = c - a.$$

Observe that $a - b + c \neq 0$, otherwise f is reducible. Therefore we can put

$$t = \frac{c-a}{2a - 2b + 2c}.$$

Solving for T, we find that we can set

$$T = \frac{1}{2a-2b+2c}\begin{pmatrix} a-2b+3c & c-a \\ a-c & 3a-2b+c \end{pmatrix}.$$

Therefore, we see that if $F(x,y)$ has exactly one rational linear factor, then it is $\mathrm{GL}_2(\mathbb{Q})$-equivalent to a form of the shape

$$\mathcal{F}(x,y) = (x+y)(ax^2+bxy+ay^2), \tag{3.2.4}$$

which is symmetric, and hence is fixed by the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

We then note that when F has exactly one rational linear factor it does not have square discriminant, hence the Hooley matrix $\mathcal{U}_F$ cannot be in $\mathrm{GL}_2(\mathbb{Q})$. Further, the elements $\mathcal{T}_\theta$ for the two irrational roots of $F(x,1)$ are not rational, so $\mathrm{Aut}_{\mathbb{Q}} F$ is conjugate to $\mathbf{D}_1 \cong \mathcal{C}_2$.

If $F(x,y)$ is irreducible, then the only possible non-trivial element in $\mathrm{Aut}_{\mathbb{Q}} F$ is the Hooley matrix $\mathcal{U}_F$ and $\mathcal{U}_F^2$. The question is then completely answered by Hooley in [64] and [70].

We move on to prove Corollary 3.1.3. Suppose first that $F_6(x,y)$ is irreducible over $\mathbb{Q}$. Then in particular, none of the Julia covariants can be rational, since F_6 is the product of Julia covariants. Thus F itself is irreducible and the determination of $\mathrm{Aut}_{\mathbb{Q}} F$ goes back to the work of Hooley in [64] and [70]. Now suppose that $F_6(x,y)$ has exactly one rational quadratic factor, say $f(x,y)$. If $f = J_\theta$ for some root θ of $F(x,1)$, then we are done by Theorem 3.1.1. Otherwise, suppose f factors over a quadratic number field $\mathbb{Q}(\sqrt{k})$ as

$$f(x,y) = (ax+by)(\overline{a}x+\overline{b}y)$$

where $\overline{s}$ denotes the conjugate of s in $\mathbb{Q}(\sqrt{k})$. Since f is not a Julia covariant, there must exist distinct Julia covariants J_{θ_1} and J_{θ_2} of F such that $ax+by|J_{\theta_1}$ and $\overline{a}x+\overline{b}y|J_{\theta_2}$. This shows that θ_1, θ_2 are not cubic irrationalities. Hence, by (3.1.7), we see that at least one of the roots of $F(x,1)$ is rational. Suppose that θ_1 is rational. Then since J_{θ_1} and f share a common factor and are both rational, it follows that they are proportional. Moreover, this would imply that J_{θ_1} and J_{θ_2} are proportional; which shows that F_6 is singular. However, by the proof of Theorem 3.1.1 we see that there is just a single $\mathrm{GL}_2(\mathbb{C})$-orbit of possible F_6 such that F has non-zero discriminant, and it is not singular. We have thus arrived at

a contradiction and so θ_1 is irrational and thus must be a quadratic irrational. Likewise, θ_2 is irrational and is conjugate to θ_1. This implies that θ_3 is rational and thus J_{θ_3} is rational. We have thus found another rational quadratic factor of $F_6(x,y)$ distinct from f, contradicting our hypothesis. Therefore, if $F_6(x,y)$ has exactly one rational quadratic factor, it must be equal to a Julia covariant.

Now, we address the case when $F_6(x,y)$ has three rational quadratic factors. If these factors are exactly the Julia covariants, then again we are done by Theorem 3.1.2. We have shown in the previous case that if F_6 has an integral quadratic factor f which is not a Julia covariant, then in fact one of the Julia covariants co-prime to f, say J_{θ_3}, must be integral. Suppose that the factors of f divide $J_{\theta_1}, J_{\theta_2}$ as before, with θ_1, θ_2 quadratic irrationals. Note that the Galois group of F acts on F_6/J_{θ_3} by permuting J_{θ_1} to J_{θ_2}. Moreover, the Galois group of F_6/J_{θ_3} itself permutes the factors of J_{θ_1} and J_{θ_2} among themselves. Hence, the Galois group of F_6/J_{θ_3} is at least order 4. Now suppose that

$$F_6(x,y) = J_{\theta_3} f(x,y) g(x,y)$$

where g is also a rational quadratic form. Put

$$g(x,y) = (cx + dy)(\overline{c}x + \overline{d}y).$$

Notice that the linear factors of g must divide either J_{θ_1} or J_{θ_2}. Without loss of generality, suppose that $cx + dy | J_{\theta_1}$ so that

$$J_{\theta_1} = (ax + by)(cx + dy).$$

If the splitting field of f and g are distinct, then either ac or bd must be a quartic irrational, which is a contradiction on θ_1 being a quadratic rational. Therefore the splitting fields of f and g are the same. However, this implies that the Galois group of F_6/J_{θ_3} has order 2, which is a contradiction. Hence if F_6 has three rational quadratic factors, they must be each equal to a Julia covariant. We then see that each Julia covariant is rational, hence F is completely reducible and thus Theorem 3.1.3 follows from Theorem 3.1.2.

For the reverse direction, notice that if $\operatorname{Aut} F \cong \mathcal{D}_3$, then Theorem 3.1.2 asserts that F splits over $\mathbb{Q}$. Therefore, F_6 is $\mathrm{GL}_2(\mathbb{Q})$-conjugate to the form

$$(x^2 - 2xy - 2y^2)(2x^2 + 2xy - y^2)(x^2 + 4xy + y^2)$$

which manifestly has three rational quadratic factors.

If Aut $F \cong \mathcal{C}_2$, then Theorem 3.1.2 asserts that F has exactly one rational linear factor and is $\mathrm{GL}_2(\mathbb{Q})$-equivalent to a symmetric cubic form. It then suffices to check that the degree 6 covariant of any symmetric binary cubic form has exactly one rational quadratic factor. Indeed, let F be a symmetric cubic form, say

$$F(x, y) = ax^3 + bx^2y + bxy^2 + ay^3.$$

Then $\Delta(F) = b^4 - 8ab^3 - 27a^4 - 18a^2b^2$ and $F_3(x, y)$ is given by

$$F_3(x, y) = (2b^3 + 27a^3 - 9ab^2)x^3 + 3(b^3 + 9a^2b - 6ab^2)x^2y$$

$$-3(b^3 + 9a^2b - 6ab^2)xy^2 - (2b^3 + 27a^3 - 9ab^2)y^3.$$

Therefore, we have

$$\begin{aligned} F_6(x, y) &= \frac{1}{2}\left(F_3^2(x, y) - 27\Delta(F)F^2(x, y)\right) \\ &= ((3a + b)x^2 + 4bxy + (3a + b)y^2)G(x, y), \end{aligned}$$

where $G(x, y)$ is an irreducible quartic form.

The irreducible case follows the work of Hooley once again in [64] and [70].

Now that we have determined Aut F, we can use the redundancy lemmas in Section 2.2. To justify Theorem 3.1.4. We will defer this to Section 3.5.

3.3 Automorphism groups of binary quartic forms over subfields of $\mathbb{R}$

In this section, our primary aim is to compute, given a binary quartic form F with real coefficients and non-zero discriminant, the $\mathbb{R}$-automorphism group $\mathrm{Aut}_{\mathbb{R}} F$ and to determine when elements in $\mathrm{Aut}_{\mathbb{R}} F$ are defined over $\mathbb{Q}$. In particular, we shall give proofs to Theorems 3.1.5, 3.1.6. and 3.1.7.

We begin with the proof of Theorem 3.1.5. We shall show explicitly that $U_1, U_2, U_3 \in \mathrm{Aut}_{\mathbb{R}} F$ when $\Delta(F) > 0$ and $U_1 \in \mathrm{Aut}_{\mathbb{R}} F$ when $\Delta(F) < 0$. We then note that $\mathrm{Aut}_{\mathbb{R}} F$ is a

finite subgroup of $\mathrm{GL}_2(\mathbb{R})$, and we show that all finite subgroups of $\mathrm{GL}_2(\mathbb{R})$ are $\mathrm{GL}_2(\mathbb{R})$-conjugate to a subgroup of the orthogonal group $O_2(\mathbb{R})$. We show that in each case, $\mathrm{Aut}_{\mathbb{R}} F$ does not contain any other elements.

We first classify possible finite subgroups of $\mathrm{GL}_2(\mathbb{R})$. Let $G \subset \mathrm{GL}_2(\mathbb{R})$ be a finite subgroup, and let $q(x, y)$ be a positive definite binary quadratic form with real coefficients. Then for all $U \in G$ we have $q(U(x, y))$ is also positive definite. Moreover, the form given by

$$q_G(x, y) = \frac{1}{\#G} \sum_{U \in G} q(U(x, y))$$

is a positive definite quadratic form which is invariant under G. Let us put

$$q_G(x, y) = ax^2 + bxy + cy^2, b^2 - 4ac < 0.$$

Then by writing

$$q_G(x, y) = a\left(x + \frac{b}{2a}y\right)^2 + \frac{4ac - b^2}{4a}y^2,$$

we see that $q_G(x, y)$ is $\mathrm{GL}_2(\mathbb{R})$-equivalent to $x^2 + y^2$, say

$$q_G(T(x, y)) = x^2 + y^2$$

for some $T \in \mathrm{GL}_2(\mathbb{R})$. The form x^2+y^2 is invariant under the orthogonal group $O_2(\mathbb{R})$, and $O_2(\mathbb{R})$ is in fact the maximal subgroup of $\mathrm{GL}_2(\mathbb{R})$ which fixes $x^2 + y^2$. Moreover, $T^{-1}GT$ fixes $x^2 + y^2$. Therefore, $T^{-1}GT \subset O_2(\mathbb{R})$. We summarize this as the following lemma:

Lemma 3.3.1. *Let G be a finite subgroup of $\mathrm{GL}_2(\mathbb{R})$. Then G is $\mathrm{GL}_2(\mathbb{R})$-conjugate to a finite subgroup of the orthogonal group $O_2(\mathbb{R})$.*

It is well-known that all matrices in $O_2(\mathbb{R})$ are of the form

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix},$$

for some $\theta \in [0, 2\pi)$. The first type are rotations and the second type are reflections. Therefore, all finite subgroups of $O_2(\mathbb{R})$ are either cyclic or dihedral. We use the symbol $\mathcal{C}_n$ to denote the cyclic group of order n and $\mathcal{D}_n$ to denote the dihedral group of order $2n$.

We now prove the following lemma:

Lemma 3.3.2. *Let F be a binary quartic form with real coefficients and non-zero discriminant. Then $\mathrm{Aut}_{\mathbb{R}} F$ does not contain any elements of order different from $1, 2, 4$. If we further assume that $\Delta(F) < 0$, then $\mathrm{Aut}_{\mathbb{R}} F$ does not contain any elements of order 4.*

Proof. We first show that $\mathrm{Aut}_{\mathbb{R}} F$ does not contain any elements of odd prime order. By Cauchy's theorem, this implies that $\mathrm{Aut}_{\mathbb{R}} F$ does not contain any elements of order divisible by an odd prime.

For any

$$U = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}),$$

U acts on an element $\theta \in \mathbb{C}$ via the action

$$U : \theta \mapsto \frac{u_1\theta + u_2}{u_3\theta + u_4}. \tag{3.3.1}$$

Suppose $U \in \mathrm{GL}_2(\mathbb{C})$ permutes the roots of F via the action given in (3.3.1). Then U necessarily has finite order. If $p \geq 5$ is a prime and $U \in \mathrm{Aut}_{\mathbb{R}} F$ has order p, then for a given root θ of F, the orbit of θ under U must have size dividing p. Since F has at most 4 distinct roots, it follows that each orbit has size one and U fixes each root of F. In particular, for each root θ of $F(x, 1)$ we have

$$\theta = \frac{u_1\theta + u_2}{u_3\theta + u_4}.$$

Thus each root θ of F is a root of the quadratic polynomial

$$u_3x^2 + (u_4 - u_1)x - u_2 = 0.$$

If the coefficients $u_3, u_4 - u_1, -u_2$ are not all zero, then there are at most two choices for θ. However, the condition $u_3 = u_2 = 0, u_4 = u_1$ is only possible if $u_4 = u_1 = \pm 1$, since $U \in \mathrm{GL}_2(\mathbb{R})$ and has finite order. Since U has odd prime order, this is not possible, hence there are at most two choices for θ. However F has four roots, so each θ must be a root at least twice since there are only two non-parallel eigenvectors of U. This contradicts our assumption that $\Delta(F) \neq 0$.

If $p = 3$, then either U fixes all roots of F or fixes exactly one root θ of F. In the former case, we again derive that $\Delta(F) = 0$, contradicting our hypothesis. The latter is

impossible if F has real coefficients. This shows that $\mathrm{Aut}_{\mathbb{R}} F$ does not contain any elements whose order is divisible by an odd prime p.

Now consider a positive integer $k = 2^l$ with $l \geq 1$. Let $F(x, y)$ be a binary quartic form with real coefficients and non-zero discriminant such that $\mathrm{Aut}_{\mathbb{R}} F$ contains an element U of order k. By Lemma 3.3.1, upon considering a $\mathrm{GL}_2(\mathbb{R})$-action if necessary, we may assume

$$U = \begin{pmatrix} \cos(2\pi/k) & -\sin(2\pi/k) \\ \sin(2\pi/k) & \cos(2\pi/k) \end{pmatrix}.$$

If U fixes each of the roots of F and $l \geq 2$, then we may use the same argument to obtain a contradiction. Therefore, U must move at least one root θ of F. The orbit of θ under U has size at most 4 if $U \in \mathrm{Aut}_{\mathbb{R}} F$. Thus, U^4 fixes each root of F. If U^4 has two distinct eigenvalues, then we again conclude that $\Delta(F) = 0$. Hence, U^4 must have a single eigenvalue, so $U^4 = \pm I_{2\times 2}$. If $U^4 = I_{2\times 2}$ then U has order $1, 2, 4$, so we assume that $U^4 = -I_{2\times 2}$ and U has order 8. If the roots of F do not lie in a single orbit under U, then U^2 fixes all roots of F and has distinct eigenvalues, so $\Delta(F) = 0$ again. This implies that we may assume, without loss of generality, that the roots of F are

$$\theta, \frac{\theta - 1}{\theta + 1}, \frac{-1}{\theta}, \frac{1 + \theta}{1 - \theta}.$$

Therefore,

$$F(x, y) = a(x - \theta y)\left(x - \frac{\theta - 1}{\theta + 1} y\right)\left(x + \frac{y}{\theta}\right)\left(x + \frac{\theta + 1}{\theta - 1} y\right)$$

and

$$\begin{aligned}
F_U(x, y) &= \frac{a}{4}\left((x - y) - \theta(x + y)\right) \cdots \left((x - y) + \frac{\theta + 1}{\theta - 1}(x + y)\right) \\
&= \frac{a}{4}\left((1 - \theta)x - y(1 + \theta)\right)\left(x\left(\frac{2}{\theta + 1}\right) - y\left(\frac{2\theta}{\theta + 1}\right)\right) \\
&\times \left(x\left(\frac{\theta + 1}{\theta}\right) - y\left(\frac{\theta - 1}{\theta}\right)\right)\left(x\left(\frac{2\theta}{\theta - 1}\right) + y\left(\frac{2}{\theta - 1}\right)\right) \\
&= \frac{a(1 - \theta)(2)(\theta + 1)(2\theta)}{4(\theta + 1)(\theta)(\theta - 1)}\left(x + \frac{\theta + 1}{\theta - 1} y\right)\left(x - \frac{\theta - 1}{\theta + 1} y\right) \\
&\times \left(x - \frac{\theta - 1}{\theta + 1} y\right)\left(x + \frac{y}{\theta}\right) \\
&= -F(x, y).
\end{aligned}$$

This shows that U fixes the roots of F but not F, hence $U \notin \mathrm{Aut}_{\mathbb{R}} F$, a contradiction.

Any pair of elements $U, U' \in \mathrm{GL}_2(\mathbb{R})$ of order 4 are conjugate by Lemma 3.3.1. Thus, if $\mathrm{Aut}_{\mathbb{R}} F$ contains an element of order 4, say U, then there exists $T \in \mathrm{GL}_2(\mathbb{R})$ such that

$$U = T^{-1} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} T.$$

By [98] and Lemma 3.2.1, it follows that F is $\mathrm{GL}_2(\mathbb{R})$-equivalent to a form $\mathcal{F}$ of the shape

$$\mathcal{F}(x, y) = x^4 + bx^3y + cx^2y^2 - bxy^3 + y^4.$$

The discriminant of $\mathcal{F}$ is equal to

$$(b^2 - 4c - 8)^2(4b^2 + c^2 - 4c + 4) = (b^2 - 4c - 8)^2(4b^2 + (c - 2)^2).$$

Note that $\Delta(\mathcal{F}) \geq 0$. Thus, if $\Delta(F) < 0$, then $\mathrm{Aut}_{\mathbb{R}} F$ does not contain any elements of order 4. This concludes the proof. □

We now give a proof of Theorem 3.1.5.

Proof. (Theorem 3.1.5) By Theorem 8 of [53] we know that $\mathrm{Aut}_{\mathbb{R}} F$ is a finite group. Thus by Lemma 3.2.1, Lemma 3.3.1, and Lemma 3.3.2, we know that if $\Delta(F) > 0$ then $\mathrm{Aut}_{\mathbb{R}} F$ is contained in a group isomorphic to $\mathcal{D}_4$ and when $\Delta(F) < 0$, we have $\mathrm{Aut}_{\mathbb{R}} F$ is contained in a group isomorphic to $\mathcal{C}_2 \times \mathcal{C}_2$. It suffices to find explicit generators for $\mathrm{Aut}_{\mathbb{R}} F$ in both cases to show that equality holds.

3.3.1 The case $\Delta(F) > 0$

We will show that $U_1, U_2, U_3 \in \mathrm{Aut}_{\mathbb{R}} F$. We will use the following observation: if $U \in \mathrm{GL}_2(\mathbb{R})$ permutes the roots of F and fixes the leading coefficient of F, then $U \in \mathrm{Aut}_{\mathbb{R}} F$. Let us consider the action of U_1 on θ_1, via the action in (3.3.1). We have

$$U_1 : \theta_1 \mapsto \frac{B_1\theta_1 + 2C_1}{-2A_1\theta_1 - B_1}.$$

Expanding using (3.1.17), we obtain

$$\frac{-2\theta_2(\theta_1 - \theta_3)(\theta_1 - \theta_4)}{-2(\theta_1 - \theta_3)(\theta_1 - \theta_4)} = \theta_2.$$

Next we see that

$$\frac{B_1\theta_3 + 2C_1}{-2A_1\theta_3 - B_1} = \frac{2\theta_4(\theta_3 - \theta_1)(\theta_3 - \theta_2)}{2(\theta_3 - \theta_1)(\theta_3 - \theta_2)} = \theta_4.$$

A similar calculation shows that U_1 sends θ_2 to θ_1 and θ_4 to θ_3. This shows that U_1 permutes the roots of F.

Now we need to check that U_1 fixes the leading coefficient of F. This is equivalent to checking that

$$\frac{1}{D_1^2}\left(a_4B_1^4 + a_3B_1^3(-2A_1) + a_2B_1^2(-2A_1)^2 + a_1B_1(-2A_1)^3 + a_0(-2A_1)^4\right)$$

is equal to a_4. Using the fact that $a_4 \neq 0$ and the Vieta relations

$$\frac{a_3}{a_4} = -(\theta_1 + \theta_2 + \theta_3 + \theta_4),$$

$$\frac{a_2}{a_4} = \theta_1\theta_2 + \theta_1\theta_3 + \theta_1\theta_4 + \theta_2\theta_3 + \theta_2\theta_4 + \theta_3\theta_4,$$

$$\frac{a_1}{a_4} = -(\theta_1\theta_2\theta_3 + \theta_1\theta_2\theta_4 + \theta_1\theta_3\theta_4 + \theta_2\theta_3\theta_4),$$

and

$$\frac{a_0}{a_4} = \theta_1\theta_2\theta_3\theta_4,$$

this is equivalent to checking that

$$(\theta_3\theta_4 - \theta_1\theta_2)^4 + (\theta_1 + \theta_2 + \theta_3 + \theta_4)(\theta_3\theta_4 - \theta_1\theta_2)^3(\theta_1 + \theta_2 - \theta_3 - \theta_4)$$

$$+(\theta_1\theta_2 + \theta_1\theta_3 + \theta_1\theta_4 + \theta_2\theta_3 + \theta_2\theta_4 + \theta_3\theta_4)(\theta_3\theta_4 - \theta_1\theta_2)^2(\theta_1 + \theta_2 - \theta_3 - \theta_4)^2$$

$$+(\theta_1\theta_2\theta_3 + \theta_1\theta_2\theta_4 + \theta_1\theta_3\theta_4 + \theta_2\theta_3\theta_4)(\theta_3\theta_4 - \theta_1\theta_2)(\theta_1 + \theta_2 - \theta_3 - \theta_4)^3$$

$$+\theta_1\theta_2\theta_3\theta_4(\theta_1 + \theta_2 - \theta_3 - \theta_4)^4$$

is equal to

$$(\theta_1 - \theta_3)^2(\theta_1 - \theta_4)^2(\theta_2 - \theta_3)^2(\theta_2 - \theta_4)^2.$$

This can be done using any standard computer algebra package (in particular, we used Sage). Thus $U_1 \in \mathrm{Aut}_{\mathbb{R}} F$. The verification that $U_2, U_3 \in \mathrm{Aut}_{\mathbb{R}} F$ follows similarly.

Finally, it is immediate that $U_1^2 = U_3^2 = I_{2\times 2}$ and $U_2^2 = -I_{2\times 2}$. Thus, the group $\langle U_1, U_2\rangle \cong \mathcal{D}_4$ and therefore must equal $\mathrm{Aut}_{\mathbb{R}} F$.

3.3.2 The case $\Delta(F) < 0$

We can use the same argument to check that $U_1 \in \mathrm{Aut}_{\mathbb{R}} F$ in this case as well, which shows that $\mathrm{Aut}_{\mathbb{R}} F = \langle U_1, -I_{2\times 2}\rangle$ as desired.

This concludes the proof of Theorem 3.1.5. □

We move on to deal with $\mathrm{Aut}_{\mathbb{C}} F$ when F has real coefficients. Certainly $\mathrm{Aut}_{\mathbb{R}} F$ is contained in $\mathrm{Aut}_{\mathbb{C}} F$. Moreover, we see that the generators U_1, U_2, U_3 are always defined over $\mathrm{GL}_2(\mathbb{C})$ and thus $\mathrm{Aut}_{\mathbb{C}} F$ contains the subgroup generated by $U_1, U_2, U_3, \sqrt{-1}\cdot I_{2\times 2}$. We will show that in general, this is subgroup is equal to $\mathrm{Aut}_{\mathbb{C}} F$ unless $J(F) = 0$.

Proof. (Theorem 3.1.6) We first consider the case when $J(F) = 0$. By Theorem 3.1.5 and its proof, we see that it suffices to consider the possibility that $\mathrm{Aut}_{\mathbb{C}} F$ contains an element of order 8. Suppose that $U \in \mathrm{Aut}_{\mathbb{C}} F$ is an element of order 8. Let ϖ be a primitive 8-th root of unity. Then U is $\mathrm{GL}_2(\mathbb{C})$-conjugate to

$$V = \frac{\varpi}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix},$$

say via $T \in \mathrm{GL}_2(\mathbb{C})$. We thus have, by the proof of Lemma 3.3.2, that

$$\mathcal{F}(x,y) = F_T(x,y) = a(x-\theta y)\left(x - \frac{\theta-1}{\theta+1}y\right)\left(x+\frac{y}{\theta}\right)\left(x+\frac{\theta+1}{\theta-1}y\right).$$

Further, we see again from the proof of Lemma 3.3.2 that

$$\mathcal{F}_V(x,y) = \mathcal{F}(x,y),$$

so that V is an element of order 8 contained in $\mathrm{Aut}_{\mathbb{C}} \mathcal{F}$. Expanding $\mathcal{F}$ we see that

$$\mathcal{F}(x,y) = ax^4 + bx^3 - 6ax^2y^2 - bxy^3 + ay^4$$

for some $b \in \mathbb{C}$. Therefore the J-invariant of $\mathcal{F}$ is given by

$$J(\mathcal{F}) = -432a^3 + 54ab^2 - 27ab^2 - 27ab^2 - 2(-6a)^3 = 0.$$

Conversely, suppose that $J(F) = 0$. By [72], we know that F can be written as the sum of two perfect 4-th powers over $\mathbb{C}$ if and only if $J(F) = 0$. Therefore, there exist complex numbers u_1, u_2, u_3, u_4 such that

$$F(x,y) = (u_1x + u_2y)^4 + (u_3x + u_4y)^4.$$

By setting $s = u_1x + u_2y, t = u_3x + u_4y$ we see that F is $\mathrm{GL}_2(\mathbb{C})$ equivalent to $F_0(x, y) = x^4 + y^4$. Finally, we note that

$$F_0\left(\frac{\sqrt{-1}}{\sqrt{2}}x + \frac{1}{\sqrt{2}}y, \frac{\sqrt{-1}}{\sqrt{2}}x - \frac{1}{\sqrt{2}}y\right) = x^4 - 6x^2y^2 + y^4,$$

so we see that $\mathrm{Aut}_{\mathbb{C}} F_0$ contains an element of order 8.

Now we treat the case when F is a Klein form. It is known that if F is a Klein form, then it is $\mathrm{GL}_2(\mathbb{C})$-equivalent to the form

$$\mathcal{F}(x, y) = x(x^3 + y^3);$$

see [8]. We see that $I(\mathcal{F})$ is given by

$$I(\mathcal{F}) = 12(1)(0) - 3(0)(1) + 0^2 = 0.$$

We know from Klein [73] that $\mathrm{Aut}_{\mathbb{C}} \mathcal{F}$ indeed contains an element of order 3 and that $\mathrm{Aut}_{\mathrm{PGL}_2(\mathbb{C})} \mathcal{F} \cong \mathcal{A}_4$. By Lemma 3.2.1, we see that all forms whose automorphism group is isomorphic to $\mathcal{A}_4$ has I-invariant equal to zero. This completes the proof of Theorem 3.1.6. □

Finally, we move on to prove Theorem 3.1.7. If $\Delta(F) < 0$, then the only element in $\mathrm{Aut}_{\mathbb{R}} F$ aside from $\pm I_{2\times 2}$ which can be rational is U_1. We have shown in the proof of Theorem 3.1.5 that

$$U_1 = \frac{1}{\sqrt{|\mathfrak{d}_1|}} \begin{pmatrix} \mathfrak{b}_1 & 2\mathfrak{c}_1 \\ -2\mathfrak{a}_1 & -\mathfrak{b}_1 \end{pmatrix},$$

where $\mathfrak{C}_1(x, y) = A_1x^2 + B_1xy + C_1y^2$ is the Cremona covariant corresponding to the unique real root β_1 of $\mathcal{Q}_F(x)$. By (3.1.25), it follows that U_1 is rational if and only if $Q_1(x, y)$ is an integral quadratic form and $a_4^2 D_1 = \mathfrak{d}_1$ is a square. Similarly, when $\Delta(F) > 0$ we have $U_i \in \mathrm{GL}_2(\mathbb{Q})$ if and only if $Q_i(x, y)$ has integer coefficients and $|\mathfrak{d}_i|$ is a square. This completes the proof of Theorem 3.1.7.

To prove Theorem 3.1.8 from Theorem 3.1.7 we will require some results from [100], namely the so-called redundancy lemmas. We will state these lemmas in Section **??** and finish the proof of Theorem 3.1.8 in Section 3.4.

In the course of proving Theorem 3.1.5, we have discovered the following differences between conjugacy classes of finite subgroups of $\mathrm{GL}_2(\mathbb{Q})$ versus subgroups of $\mathrm{GL}_2(\mathbb{Z})$ as in Stewart's Table 1 in [98]; there are redundancies on that table if we consider $\mathrm{GL}_2(\mathbb{Q})$ conjugacy. Indeed, we find that the groups

$$\mathbf{D}_1 = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle, \mathbf{D}_1^* = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$$

which are not $\mathrm{GL}_2(\mathbb{Z})$-conjugate are $\mathrm{GL}_2(\mathbb{Q})$-conjugate by the matrix $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Indeed,

$$\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

This implies that the groups

$$\mathbf{D}_2 = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle, \mathbf{D}_2^* = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$$

are also $\mathrm{GL}_2(\mathbb{Q})$-conjugate. By noting that

$$\frac{-1}{3}\begin{pmatrix} 2 & -1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} -2 & 1 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

we see that the groups

$$\mathbf{D}_3 = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \right\rangle, \mathbf{D}_3^* = \left\langle \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \right\rangle$$

are $\mathrm{GL}_2(\mathbb{Q})$-conjugate.

We now prove that every finite subgroup of $\mathrm{GL}_2(\mathbb{Q})$ is conjugate to a finite subgroup of $\mathrm{GL}_2(\mathbb{Z})$. This argument is due to David Speyer, posted on Mathoverflow; see also [**?**]. Suppose that $\mathcal{G} \subset \mathrm{GL}_2(\mathbb{Q})$ is a finite subgroup. Consider the lattice

$$\Lambda = \sum_{\sigma \in \mathcal{G}} \sigma \cdot \mathbb{Z}^2 \subset \mathbb{Q}^2.$$

Plainly, we have $\mathcal{G}\Lambda = \Lambda$ and $\mathbb{Z}^2 \subset \Lambda$, since $\mathcal{G}$ contains the identity matrix. Therefore, we must have that Λ is of rank 2. Let $T \in \mathrm{GL}_2(\mathbb{Q})$ be a matrix that sends the standard basis to a basis of Λ. Then $T\mathbb{Z}^2 = \Lambda$, and $T^{-1}\Lambda = \mathbb{Z}^2$. Now for all $G \in \mathcal{G}$, we have

$$T^{-1}GT(\mathbb{Z}^2) = T^{-1}G\Lambda = T^{-1}\Lambda = \mathbb{Z}^2,$$

whence

$$T^{-1}\mathcal{G}T \subset \mathrm{GL}_2(\mathbb{Z}),$$

as desired. We state this as the following lemma:

Lemma 3.3.3. *All finite subgroups of* $\mathrm{GL}_2(\mathbb{Q})$ *are conjugate to a finite subgroup of* $\mathrm{GL}_2(\mathbb{Z})$.

3.4 Determining the value of W_F for integral binary quartic forms

In this section, we prove Theorem 3.1.8 by determining the value of W_F for given a binary quartic form

$$F(x, y) = a_4x^4 + a_3x^3y + a_2x^2y^2 + a_1xy^3 + a_0y^4,$$

with integer coefficients and non-zero discriminant. Much of what we do in this section is covered in [100] for general binary forms of degree $d \geq 3$, so we will be brief in our exposition here. We will recall the following definitions and lemmas. We say that an integer n is *essentially represented* by F if whenever $F(x, y) = F(u, v) = n$, then there exists an element $U \in \mathrm{Aut}\, F$ such that

$$U \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix}.$$

We will denote by $\mathcal{R}_F^{(1)}(Z)$ the set of integers n with $|n| \leq Z$ which are essentially represented by F. If $F(x, y)$ is essentially represented for $(x, y) \in \mathbb{Z}^2$, then we say that (x, y) is an *essential representative*. We denote by $\mathcal{N}_F^{(1)}(Z)$ the set of essential representatives (x, y) of F for which $|F(x, y)| \leq Z$. Put $R_F^{(1)}(Z) = \#\mathcal{R}_F^{(1)}(Z)$ and $N_F^{(1)}(Z) = \#\mathcal{N}_F^{(1)}(Z)$ respectively. We can now state the following lemma, which combined with the redundancy lemmas in Section 2.2 and Theorem 3.1.7 allow us to prove Theorem 3.1.8.

Lemma 3.4.1. *Let F be a binary form of degree $d \geq 3$ with integer coefficients and non-zero discriminant. Then there exists a number β_d which depends solely on d such that $0 < \beta_d < 2d^{-1}$ such that for all $\varepsilon > 0$, we have*

$$N_F^{(1)}(Z) = A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right).$$

Proof. This is essentially the content of Lemma 2.1.3; see Chapter 2. □

Proof. (Theorem 3.1.8) We first suppose that the roots β_i of $\mathcal{Q}_F(x)$ are integral for $i = 1, 2, 3$, and that the absolute value of the discriminant $\mathfrak{d}_i$ of $Q_i(x, y)$ is a square for $i = 1, 2, 3$. It then follows that U_1, U_2, U_3 are generators of $\mathrm{Aut}\, F/\{\pm I\}$, and from (2.0.11) we see that the determinant of the lattices Λ_i is equal to m_i for $i = 1, 2, 3$. Let us denote by $\mathcal{S}_0(Z)$ the set of points $(x, y) \in \mathbb{Z}^2$ in $\mathcal{N}_F^{(1)}(Z)$ which do not lie in Λ_i for $i = 1, 2, 3$, $\mathcal{S}_i(Z)$ for the set of points in $\mathcal{N}_F^{(1)}(Z)$ which lies in Λ_i but not in Λ_j for $j \neq i$, and $\mathcal{S}(Z)$ for the set of points $(x, y) \in \mathbb{Z}^2$ in $\mathcal{N}_F^{(1)}(Z)$ such that $(x, y) \in \Lambda_i$ for $i = 1, 2, 3$. Put $S(Z) = \#\mathcal{S}(Z)$ and $S_i(Z) = \#\mathcal{S}_i(Z)$ for $i = 0, 1, 2, 3$. By the inclusion-exclusion principle, Lemma 2.2.2 and Lemma 3.4.1 we have

$$S_0(Z) = \left(1 - \frac{1}{m_1} - \frac{1}{m_2} - \frac{1}{m_3} + \frac{2}{m}\right) N_F^{(1)}(Z) + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right),$$

$$S_i(Z) = \left(\frac{1}{m_i} - \frac{1}{m}\right) N_F^{(1)}(Z) + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right),$$

and

$$S(Z) = \frac{1}{m} N_F^{(1)}(Z) + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right).$$

Let

$$\mathcal{S}_i'(Z) = \{n \in \mathbb{Z} : |n| \leq Z, \exists (x, y) \in \mathcal{S}_i \text{ s.t. } F(x, y) = n\}$$

for $i = 0, 1, 2, 3$ and

$$\mathcal{S}'(Z) = \{n \in \mathbb{Z} : |n| \leq Z, \exists (x, y) \in \mathcal{S} \text{ s.t. } F(x, y) = n\}.$$

Put $S_i'(Z) = \#\mathcal{S}_i'(Z)$ for $i = 0, 1, 2, 3$ and $S'(Z) = \#\mathcal{S}'(Z)$. Then it follows that

$$S_0'(Z) = \frac{1}{2} S_0(Z)$$

since for each $n \in \mathcal{S}_0$ there are exactly two pairs in $\mathcal{S}_0$, namely (x, y) and $(-x, -y)$ such that $F(x, y) = F(-x, -y) = n$. Similarly, we have

$$S_i'(Z) = \frac{1}{4} S_i(Z)$$

for $i = 1, 2, 3$ and

$$S'(Z) = \frac{1}{8} S(Z).$$

Note that

$$R_F^{(1)}(Z) = S_0'(Z) + S_1'(Z) + S_2'(Z) + S_3'(Z) + S'(Z).$$

It thus follows that

$$R_F^{(1)}(Z) = \frac{1}{2}\left(1 - \frac{1}{2m_1} - \frac{1}{2m_2} - \frac{1}{2m_3} + \frac{3}{4m}\right) N_F^{(1)}(Z) + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right).$$

Lemma 3.4.1 then yields that

$$R_F^{(1)}(Z) = \frac{1}{2}\left(1 - \frac{1}{2m_1} - \frac{1}{2m_2} - \frac{1}{2m_3} + \frac{3}{4m}\right) A_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right),$$

and so

$$W_F = \frac{1}{2}\left(1 - \frac{1}{2m_1} - \frac{1}{2m_2} - \frac{1}{2m_3} + \frac{3}{4m}\right).$$

Next note that if there exist two integral roots, say β_1, β_2 of $\mathcal{Q}_F(x)$ such that $|\mathfrak{d}_1|, |\mathfrak{d}_2|$ are squares, then it follows that $U_3 \in \mathrm{GL}_2(\mathbb{Q})$ as well from Theorem 3.1.5. This implies that β_3 is integral and $|\mathfrak{d}_3|$ is a square. We now consider the case when $\mathcal{Q}_F(x)$ has exactly one integer root, say β, such that $|\mathfrak{d}_\beta|$ is a square. In this case we have

$$S_0(Z) = \left(1 - \frac{1}{m}\right) N_F^{(1)}(Z) + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right)$$

and

$$S(Z) = \frac{1}{m} N_F^{(1)}(Z) + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right).$$

Further, we have

$$S_0'(Z) = \frac{1}{2} S_0(Z)$$

and

$$S'(Z) = \frac{1}{4} S(Z),$$

and therefore

$$R_F^{(1)}(Z) = \frac{1}{2}\left(1 - \frac{1}{2m}\right) N_F^{(1)}(Z) + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right),$$

and by Lemma 3.4.1, we have

$$R_F^{(1)}(Z) = \frac{1}{2}\left(1 - \frac{1}{2m}\right) Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right).$$

This shows that in this case, we have

$$W_F = \frac{1}{2}\left(1 - \frac{1}{2m}\right).$$

Finally, if $\mathcal{Q}_F(x)$ is irreducible over $\mathbb{Z}$ or if for any integer root β of $\mathcal{Q}_F(x)$ we have $|\mathfrak{d}_\beta|$ is not the square of an integer, then $\operatorname{Aut} F = \mathbf{C}_2$ and so each integer represented by F is represented exactly twice. Therefore, we have

$$W_F = \frac{1}{2}$$

as desired. □

We now give examples of irreducible quartic forms which realizes each isomorphism class of automorphism groups. This demonstrates a significant difference between quartic and cubic forms. However, there is a connection between the automorphism group of F and the *Galois group* $\operatorname{Gal} F$ of the Galois closure of F; see Corollary 3.4.10.

3.4.1 Examples of irreducible quartic forms which realizes each possible automorphism group

By Theorem 3.1.7, the possible isomorphism classes of $\operatorname{Aut} F$ are $\mathcal{D}_4, \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_2$, and $\mathcal{C}_2 = \mathbf{C}_2$. While for each possible isomorphism class it is possible to find an irreducible form F which realizes that class, we note that the discriminant plays a key role. In particular, by Theorem 3.1.5 we see that $\operatorname{Aut}_{\mathbb{R}} F \cong \mathcal{C}_2 \times \mathcal{C}_2$ if $\Delta(F) < 0$, so whenever $\operatorname{Aut} F \cong \mathcal{D}_4$ or $\mathcal{C}_4$, the discriminant of F must be positive. Our examples show that this is the only obstruction.

Example 3.4.2.

$$F(x, y) = x^4 + y^4, \chi(F) = 0.$$

Note that $F(x, 1)$ is the 8-th cyclotomic polynomial, so it is irreducible. Also note that $\operatorname{Aut} F = \mathbf{D}_4$, as shown by Stewart in [98] in the proof of his Theorem 3.

Example 3.4.3.

$$F(x, y) = x^4 - 6x^2y^2 + y^4, \chi(F) = 4.$$

It is quickly verified that F is irreducible. Moreover, it can be seen to be fixed by $\mathbf{D}_4$, as argued by Stewart in [98].

We now show that there are forms F with signature 0 and 4 such that $\operatorname{Aut} F \cong \mathcal{C}_4$. By [98], all forms of the shape

$$\mathcal{F}(x, y) = Ax^4 + Bx^3y + Cx^2y^2 - Bxy^3 + Ay^4 \tag{3.4.1}$$

are fixed by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Any such $\mathcal{F}$ will satisfy $\operatorname{Aut}\mathcal{F} = \mathbf{C}_4$ as long as we can check that $\operatorname{Aut}\mathcal{F}$ contains no other elements except for those in $\mathbf{C}_4$. If there exists $U \in \mathrm{GL}_2(\mathbb{Q}) \setminus \mathbf{C}_4$ in $\operatorname{Aut} F$, then $\operatorname{Aut}\mathcal{F} \cong \mathcal{D}_4$, which implies that its cubic resolvent is completely reducible. Thus the discriminant $\Delta(\mathcal{Q}_\mathcal{F})$ of the cubic resolvent $\mathcal{Q}_\mathcal{F}$ must be a square. Moreover, $\Delta(\mathcal{Q}_\mathcal{F}) = 27\Delta(\mathcal{F})$. Therefore, if we find a form F of the shape (3.4.1) whose discriminant is not thrice a square, then $\operatorname{Aut} F = \mathbf{C}_4$.

Example 3.4.4.

$$F(x, y) = x^4 + 2x^3y + 3x^2y^2 - 2xy^3 + 1$$

has $\chi(F) = 0$ and $\Delta(F) = 4352$, which is not thrice a square in $\mathbb{Q}$. Further, one can check that $F(x, y)$ is irreducible over $\mathbb{Q}$. Hence, $\operatorname{Aut} F \ncong \mathcal{D}_4$ and contains $\mathbf{C}_4$, so it is exactly equal to $\mathbf{C}_4$.

Example 3.4.5.

$$F(x, y) = x^4 + 2x^3y - 3x^2y^2 - 2xy^3 + 1.$$

Then $\chi(F) = 4$ and $\Delta(F) = 2624$, which is not divisible by three. Again, it is easy to check that $F(x, y)$ is irreducible over $\mathbb{Q}$. Hence $\operatorname{Aut} F = \mathbf{C}_4$.

Next we show that there exist forms with $\chi(F) = 0, 2, 4$ such $\operatorname{Aut} F \cong \mathcal{C}_2 \times \mathcal{C}_2$.

Example 3.4.6.

$$F(x, y) = x^4 + 4x^2y^2 + 7y^4, \chi(F) = 0.$$

By Stewart [98], we know that $\operatorname{Aut} F$ contains $\mathbf{D}_2$. Thus, the cubic resolvent $\mathcal{Q}_F(x)$ will have a rational root. To show that it is exactly $\mathbf{D}_2$, it suffices to show that $\mathcal{Q}_F(x)$ has an irreducible quadratic factor. We explicitly find the factor

$$x^2 + 8x - 236$$

of $\mathcal{Q}_F(x)$. The quadratic formula yields the roots

$$\frac{-8 \pm \sqrt{1008}}{2} = -4 \pm 2\sqrt{63},$$

which are not rational. Therefore $\operatorname{Aut} F = \mathbf{D}_2$.

Example 3.4.7.

$$F(x, y) = x^4 - 7x^2y^2 + 7y^4, \chi(F) = 4.$$

In this case, we know that $\operatorname{Aut} F$ contains $\mathbf{D}_2$. The relevant quadratic polynomial is

$$x^2 - 14x + 203.$$

By Eisenstein's lemma applied to the prime $p = 7$, we see that the above is irreducible, whence $\operatorname{Aut} F = \mathbf{D}_2$.

Example 3.4.8.

$$F(x, y) = x^4 - 4y^4, \chi(F) = 2.$$

We have $\mathbf{D}_2 \subset \operatorname{Aut} F$. The relevant quadratic polynomial is

$$x^2 + 144,$$

which is irreducible by inspection since it has no real roots. Therefore $\operatorname{Aut} F = \mathbf{D}_2$.

The generic binary quartic form will have $\operatorname{Aut} F = \mathbf{C}_2$. A concrete example is, for instance,

Example 3.4.9.

$$F(x, y) = x^4 + 2x^3y + 3x^2y^2 + 4xy^3 + 5y^4.$$

It can be checked directly that $H_{\beta_i}(x)$ is not well-defined over $\mathbb{Q}$ for $i = 1, 2, 3$. However, we will adapt a more enlightened approach . It can be immediately verified using computer algebra programs that the Galois group of the Galois closure of F is isomorphic to $\mathcal{S}_4$, the full symmetric group on four letters. We may embed $\operatorname{Aut} F$ into $\mathcal{S}_4 = \operatorname{Gal} F$ via the action of $\operatorname{Aut} F$ on the roots of F. Now let $\sigma \in \operatorname{Gal} F$ be an element of the Galois group of the Galois closure of F and $U = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix}$. Then we see that for any root θ of F, we have

$$(\sigma U \sigma^{-1})\theta = \sigma\left(\frac{u_1\sigma^{-1}(\theta) + u_2}{u_3\sigma^{-1}(\theta) + u_4}\right) = \frac{u_1\theta + u_2}{u_3\theta + u_4},$$

since $U \in \mathrm{GL}_2(\mathbb{Q})$. Therefore, $U = \sigma U \sigma^{-1}$ for all $\sigma \in \mathcal{S}_4$, which implies that U lies in the center of $\mathcal{S}_4$. But $\mathcal{S}_4$ has trivial center, so $U = \pm I_{2\times 2}$, as desired.

In fact, this last example leads to the following corollary:

Corollary 3.4.10. *Suppose that $F(x, y)$ is an irreducible binary quartic form with integer coefficients. If* $\operatorname{Gal} F$ *is $\mathcal{S}_4$ or $\mathcal{A}_4$, then* $\operatorname{Aut} F$ *is trivial.*

Proof. This is the same as the argument given in Example 3.5.9. □

3.5 Computing W_F for integral binary cubic forms

Much like in Section 3.4, we shall apply the redundancy lemmas in Section **??** which were the main technical results in [100] to prove Theorem 3.1.4.

3.5.1 When F is irreducible and $\Delta(F)$ is not a square

In this case, we have shown in Section 3.2 that $\operatorname{Aut} F = \mathbf{C}_1$. Therefore, by Theorem 1.2 in [100] we see that $W_F = 1$.

3.5.2 When F is irreducible and $\Delta(F)$ is a square

Hooley showed that the Hooley matrix U_F lies in $\mathrm{GL}_2(\mathbb{Q})$ in this case and generates $\operatorname{Aut} F$. Let $\Lambda = \Lambda_{U_F}$ be the lattice associated to U_F. Then Lemma 2.2.1 shows that

$$d(\Lambda) = m,$$

as desired.

3.5.3 When F has exactly one rational root

We showed in Section 3.2 that $\operatorname{Aut} F \cong \mathcal{D}_2$ in this case. Moreover, $\operatorname{Aut} F$ is generated by the matrix

$$\frac{1}{2D}\mathcal{J}_\theta \mathcal{H}_F$$

where θ is the unique rational root of F. Lemma 2.2.1 applies and thus we are done by Theorem 1.2 in [100].

3.5.4 When F has three rational roots

In this case, $\operatorname{Aut} F \cong \mathcal{D}_3$. Then Lemma 2.2.2 and Theorem 1.2 in [100] shows that

$$W_F = 1 - \frac{1}{2m_1} - \frac{1}{2m_2} - \frac{1}{2m_3} - \frac{2}{3m_4} + \frac{4}{3m}.$$

This completes the proof of Theorem 3.1.4.

3.6 Proof of Theorems 3.1.9 and 3.1.10

3.6.1 Cubic surfaces

By the proof of Theorem 3.1 in [17], the lines contained in X are either of the form

$$L : [s, \theta_i s, t, \theta_j t] \tag{3.6.1}$$

where s, t are independent parameters and θ_i, θ_j are two roots of $F(x, 1)$ (not necessarily distinct), or of the shape

$$L : [s, t, \omega_j(u_1 s + u_2 t), \omega_j(u_3 s + u_4 t)] \tag{3.6.2}$$

where s, t are independent parameters,

$$U = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix} \in \mathrm{Aut}_{\mathbb{C}} F,$$

and ω_j is a third root of unity. The lines (3.6.1) are defined over the splitting field $\mathbb{F}$ of F. By Theorem 3.1.1, it follows that U can be chosen to be defined over the splitting field $\mathbb{F}$ of F. Thus, the lines in (3.6.2) are defined over the field $K = \mathbb{F}(\omega)$, where ω is a primitive third root of unity. Since $[\mathbb{F} : \mathbb{Q}]$ is $1, 2, 3$, or 6, the first part of Theorem 3.0.3 follows and a careful analysis of the cases yields Theorem 3.1.9.

3.6.2 Quartic surfaces

By the proof of Theorem 31 in [17], there are precisely $4(4+\upsilon_F)$ many lines contained in X. However, we must interpret υ_F to mean the number of automorphisms of the roots of F on the projective line, which means that these automorphisms are defined over $\mathrm{PGL}_2(\mathbb{C})$, not $\mathrm{GL}_2(\mathbb{C})$. By Theorem 3.1.6 and its proof, we see that every binary quartic form F with non-zero discriminant has exactly 4 automorphisms in $\mathrm{PGL}_2(\mathbb{C})$ if $J(F) \neq 0$ and there are 8 automorphisms otherwise. There are thus $4 \cdot 8 = 32$ lines contained in X over $\mathbb{C}$ when $I(F) \cdot J(F) \neq 0$, $4 \cdot 12 = 48$ lines when $J(F) = 0$ and $I(F) \neq 0$, and $4 \cdot 16 = 64$ lines when $I(F) = 0$ and $J(F) \neq 0$.

As before, we see that the lines L contained in X are of the shape

$$L : [s, \theta_i s, t, \theta_j t] \tag{3.6.3}$$

for two roots θ_i, θ_j of $F(x,1)$ and independent parameters $s,t \in \mathbb{C}$, or of the shape

$$L : [s, t, \nu_j(u_1 s + u_2 t), \nu_j(u_3 s + u_4 t)] \tag{3.6.4}$$

where

$$U = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix} \in \operatorname{Aut}_{\mathbb{C}} F$$

and ν_j is a 4-th root of unity. The lines (3.6.3) are defined over the splitting field $\mathbb{F}$ of F. By Theorem 3.1.6 and (3.1.19), we see that the lines in (3.6.4) are defined over $\mathbb{F}(\sqrt{D_1}, \sqrt{D_2}, \sqrt{D_3})$. We have that $[\mathbb{F} : \mathbb{Q}] \leq 24$. Moreover, since $a_4^3\sqrt{D_1 D_2 D_3} = \Delta(F)$, it follows that $\mathbb{F}(\sqrt{D_1}, \sqrt{D_2}, \sqrt{D_3} = \mathbb{F}(\sqrt{D_1}, \sqrt{D_2})$ so $[\mathbb{F}(\sqrt{D_1}, \sqrt{D_2}, \sqrt{D_3}) : \mathbb{Q}] \leq 96$. Finally, $K = \mathbb{F}(\sqrt{D_1}, \sqrt{D_2}, \sqrt{D_3}, \sqrt{-1})$, so $[K : \mathbb{Q}] \leq 192$.

We now refine our estimates when F has an almost rational stabilizer. In this case, $[K : \mathbb{Q}]$ is much smaller. The lines from (3.6.3) are defined over $\mathbb{F}$, which has either degree 4 or 8 over $\mathbb{Q}$. Without loss of generality, we shall assume that

$$U_1 = \frac{1}{\sqrt{\epsilon_1 D_1}} \begin{pmatrix} B_1 & 2C_1 \\ -2A_1 & -B_1 \end{pmatrix}$$

is almost rational, namely that the quadratic form $A_1 x^2 + B_1 xy + C_1 y^2$ is proportional over $\mathbb{C}$ to a quadratic form with integer coefficients. In this case the root β_1 of the cubic resolvent $\mathcal{Q}_F(x)$ is an integer, thus all elements in $\operatorname{Gal} F$ must fix β_1. One then sees that D_1 must be rational, since it is fixed under all elements in $\operatorname{Gal} F$. Moreover, we see that

$$64\Delta(F) = a_4^6 D_1 D_2 D_3,$$

and so $D_2 D_3$ is rational. Thus we only need to adjoin one of $\sqrt{D_2}, \sqrt{D_3}$. Therefore, $[\mathbb{F}(\sqrt{D_1}, \sqrt{D_2}) : \mathbb{Q}] \leq 32$ and $[K : \mathbb{Q}] \leq 64$.

Finally, if F is irreducible and has three almost rational stabilizers, then its Galois group is isomorphic to $\mathcal{C}_2 \times \mathcal{C}_2$. In this case, we claim that the lines in (3.6.4) are defined over at most a degree 4 extension of $\mathbb{F}$. To see this, observe that $D_i^2 | \Delta(F)$ for $i = 1, 2, 3$ and so for each prime factor p of D_1 which does not divide a_4, either $p^2 | D_1$ or $p | D_2 D_3$. Thus we see that $\mathbb{F}(\sqrt{D_1}, \sqrt{D_2}, \sqrt{D_3})$ is at most a degree 4 extension of $\mathbb{F}$. Thus, we see that $[K : \mathbb{Q}] \leq 32$.

We now give some examples of various K.

Example 3.6.1. Let $F(x,y) = x^4 + y^4$. Then it is clear that $\mathbb{F} = \mathbb{Q}(\varpi)$ and $\operatorname{Aut} F = \mathbf{D}_4$, where ϖ is a primitive 8-th root of unity. Moreover, in this case $D_1 = D_3 = -1$ and $D_2 = 1$. Moreover, $\sqrt{-1} \in \mathbb{F}$. Thus, in this case $K = \mathbb{Q}(\varpi)$ and $[K : \mathbb{Q}] = 4$, the smallest possible value.

Example 3.6.2. Let $F(x,y) = x^4 + 36xy^3 + 63y^4$. Then the Cremona covariants of F are given by

$$\mathcal{C}_1(x,y) = x^2 + 6xy + 3y^2, \mathcal{C}_2(x,y) = x^2 + 3xy + 6y^2, \text{ and } \mathcal{C}_3(x,y) = x^2 - 2xy - 9y^2.$$

This gives rise to

$$U_1 = \frac{1}{\sqrt{6}} \begin{pmatrix} 3 & 3 \\ -1 & -3 \end{pmatrix}, U_2 = \frac{1}{\sqrt{15}} \begin{pmatrix} 3 & 12 \\ -2 & -3 \end{pmatrix}, \text{ and } U_3 = \frac{1}{\sqrt{10}} \begin{pmatrix} 1 & 9 \\ 1 & -1 \end{pmatrix}.$$

This shows that $D_1 = -6, D_3 = -10, D_2 = 15$. One checks explicitly that $\mathbb{F} = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$. Thus, $\mathbb{F}(\sqrt{D_1}, \sqrt{D_2}, \sqrt{D_3}) = \mathbb{Q}(\sqrt{2}, \sqrt{-3}, \sqrt{-5})$. We see that this last field is missing $\sqrt{-1}$, so that $K = \mathbb{F}(\sqrt{-5}, \sqrt{-1})$ and so $[K : \mathbb{Q}] = 16$.

Chapter 4

The p-adic determinant method

In this chapter we give an overview of what is known presently of the so-called determinant method, originally formulated by Bombieri and Pila in [14] to bound the number of rational points on plane curves. Bombieri and Pila's original approach involved in a critical way the geometric properties of the Euclidean plane $\mathbb{R}^2$, which prevented their method from being generalized to higher dimensions for over a decade. In 2002, Heath-Brown found a way to formulate the determinant method in terms of p-adic valuations as opposed to the archimedean valuation in [53]. Heath-Brown's version of the determinant method, now known as the (local) p-adic determinant method, has proven to be immensely versatile and useful in studying problems involving counting rational points on algebraic varieties. One of the fantastic attributes of the determinant method is that the upper bound one gets from applying it only depends on the degree and dimension of an algebraic variety X and not on the coefficients of the polynomials defining X. Broberg and Salberger refined Heath-Brown's determinant method in [18] and [92] respectively, recasting Heath-Brown's argument in the language of algebraic geometry. Later, in [93], Salberger would give a much more efficient version of the p-adic determinant method which is now known as the *global determinant method*. Salberger gave a further refinement of the p-adic determinant method in [94], which improves the determinant method in a fundamental way. We dub this improvement the *Salberger improvement* to the p-adic determinant method.

We shall now briefly discuss the basic philosophy of the determinant method. Typically, the difficulty of counting rational points on an algebraic variety X increases rapidly with respect to the dimension of X. For instance, counting points on 0-dimensional varieties is almost trivial; since the count is bounded by the degree of the variety alone. Even the 1-dimensional case is highly non-trivial, as enumerating rational points on curves of positive

genus remains a challenging problem in general. Even though we have Faltings' theorem telling us that curves of genus at least two have only finitely many rational points on them, effective results are difficult and sporadic. For $\dim X \geq 2$ the problem of bounding the density of rational points is almost entirely unsolved.

Following the basic concept that lower dimensional algebraic varieties are easier to deal with, a reasonable strategy to count rational points on X of bounded height is to sort them into lower dimensional subvarieties. The most straightforward way to do so is to cut X using hyperplane sections. However, the number of hyperplanes needed to cover all rational points of height up to B is large. One might hope that there might be a more efficient way to count the points of height at most B if one allows coverings by subvarieties of higher degree, and this is precisely where the determinant method succeeds.

To be more clear, the objective of the determinant method is to produce a relatively small number of hypersurfaces $Y_1, Y_2, \cdots$ with respect to the parameter B such that the set $Y_1 \cup Y_2 \cdots$ covers the rational points on X of height at most B. The argument has a similar flavour to Roth's theorem: if there are few rational points to begin with, then we can trivially pick hypersurfaces in such a way that each hypersurface covers only one point. If there are a lot of rational points, then we shall show that there is a certain repulsion principle which prevents the existence of a greater number of points.

Heath-Brown [53], Broberg [18], and Salberger [92] [93] [94] worked in the setting of projective spaces (Heath-Brown also proved a version of the determinant method for affine spaces; see [54]). However, in order to study k-free values of binary forms or rational points on del Pezzo surfaces of degree 2, it is more natural to work over certain *weighted* projective spaces. Let K be a field. Then the projective space $\mathbb{P}^{r+1}_K$ is given by the Proj construction. In particular, the polynomial ring $K[x_0, \cdots, x_{r+1}]$ is a graded ring with respect to the degree. Moreover, there is a grading of the monomials provided by first comparing the degree of two monomials, and then when there is a tie, we follow the lexiographic ordering on $x_0, \cdots, x_{r+1}$; that is, x_i precedes x_j if $i < j$. We then have

$$\mathbb{P}^n_K = \operatorname{Proj} K[x_0, \cdots, x_n].$$

We can carry out the same construction, but we can assign a different grading to the ring $K[x_0, \cdots, x_{r+1}]$. Indeed, given an $(r+2)$-tuple of positive integers, say $\mathbf{w} = (w_0, \cdots, w_{r+1})$, we can define the *weighted degree with respect to* $\mathbf{w}$, $\deg_{\mathbf{w}}$, of a monomial $\mathbf{x}^{\boldsymbol{\alpha}} = x_0^{\alpha_1} \cdots x_{r+1}^{\alpha_{r+1}}$ by

$$\deg_{\mathbf{w}} \mathbf{x}^{\boldsymbol{\alpha}} = w_0\alpha_0 + \cdots + w_{r+1}\alpha_{r+1}.$$

This ordering turns $K[x_0, \cdots, x_{r+1}]$ into a graded ring, and the corresponding space is called the weighted projective space with weight vector $\mathbf{w}$, which we denote by $\mathbb{P}_K(\mathbf{w})$. We can define a similar monomial ordering $<$ by first comparing the weighted degree, then order $x_0, x_1, \cdots, x_{r+1}$ lexiographically. The usual projective space is then a weighted projective space with weight vector equal to $(1, 1, \cdots, 1)$.

From now on we will assume that the underlying field is $\mathbb{Q}$, unless otherwise stated. For brevity we put $\mathbb{P}(\mathbf{w}) = \mathbb{P}_{\mathbb{Q}}(w_0, \cdots, w_{r+1})$. We are not able to deal with general weighted projective spaces. Indeed, our arguments require at least two of the weights be equal to 1. We shall assume that $w_0 = w_1 = 1$. This will be made apparent in the proof of Theorem 4.2.1.

Let I be the weighted homogeneous ideal generated by a primitive weighted homogeneous form

$$F(x_0, \cdots, x_{r+1}) \in \mathbb{Z}[x_0, \cdots, x_{r+1}],$$

of weighted degree d, and let X be the corresponding hypersurface defined by F. Let the *height* of F, denoted by $\|F\|$, be the largest absolute value of the coefficients of F. Let $<$ be the monomial grading described earlier (see also Section 4.1), giving rise to the constants $a_{I,0}, \cdots, a_{I,r+1}$ as in (4.1.4). Let $\mathbf{B} = (B_0, \cdots, B_{r+1}) \in \mathbb{R}^{r+2}$ be an $(r+2)$-tuple of real numbers of size at least 1. Our goal is to count rational points $\mathbf{x} = (x_0, \cdots, x_{r+1})$ on the hypersurface X, defined over $\mathbb{P}(\mathbf{w})$, such that

$$|x_i| \leq B_i, \ 0 \leq i \leq r+1.$$

Let us write

$$\begin{aligned} w &= w_2 \cdots w_{r+1}, \\ V &= B_0 \cdots B_{r+1}, \end{aligned} \tag{4.0.1}$$

and

$$W = \left(B_0^{a_{I,0}} \cdots B_{r+1}^{a_{I,r+1}}\right)^{\frac{r+1}{r}\left(\frac{w}{d}\right)^{1/r}}. \tag{4.0.2}$$

Further, we will only be concerned with those rational points $\mathbf{x} \in X$ with integral representation $(x_0, \cdots, x_{r+1})$ satisfying $\gcd(x_0, x_1) = 1$. Note that any such integral representative is necessarily primitive. Let us write $X(\mathbb{Q}; B_0, \cdots, B_{r+1}) = X(\mathbb{Q}; \mathbf{B})$ for the set of rational points on X with an integral representative $(x_0, \cdots, x_{r+1})$ satisfying $|x_i| \leq B_i$ and $\gcd(x_0, x_1) = 1$. Sometimes we will wish to count a subset of $X(\mathbb{Q}; \mathbf{B})$ satisfying a certain set of congruence conditions. For each prime p, let us write X_p for the hypersurface defined

by reducing X modulo p, viewed as a variety over $\mathbb{F}_p$. Let $\mathcal{P} = \{p_1, \cdots, p_t\}$ be a set of primes, and let $\mathfrak{P} = (P_1, \cdots, P_t)$, with $P_j \in X_{p_j}$. Then we write

$$X(\mathbb{Q}; \mathbf{B}; \mathfrak{P}) = \{\mathbf{x} \in X(\mathbb{Q}; \mathbf{B}) : \mathbf{x} \equiv P_j \pmod{p_j}, 1 \leq j \leq t\}.$$

A hypersurface $X \subset \mathbb{P}(\mathbf{w})$ is *geometrically integral* if it is reduced and irreducible over the algebraic closure of $\mathbb{Q}$; see Hartshorne [50], p. 82 and p. 93.

We sketch the main ideas of the determinant method (and explaining its namesake) before moving on to stating our next theorem. The key idea is as follows. Suppose that $X(\mathbb{Q}; \mathbf{B}, \mathfrak{P})$ contains many S points. If S is small with respect to some a prior agreed upon function of $\mathbf{B}$, then we simply use S as a bound for $\#X(\mathbb{Q}; \mathbf{B}, \mathfrak{P})$. Otherwise, we choose a moderately large degree u and consider the set of monomials $\{\mathbf{x}^{\boldsymbol{\alpha}} : \deg_{\mathbf{w}} \boldsymbol{\alpha} = u\}$. The dimension of the span of these monomials is strictly smaller than the total number of monomials over X, since the vanishing of F induces non-trivial linear relations on X. We then consider the *Hilbert function* $H_{I(X)}(u)$ to be the number of linearly independent monomials of degree u over $I(X)$, the ideal generated by X (see the next section). We choose a subset of monomials $M_1, \cdots, M_s$ where $s = H_{I(X)}(u)$, each of weighted degree u. Our choice of u will be small enough so that $s < S$. Enumerate the points in $X(\mathbb{Q}; \mathbf{B}, \mathfrak{P})$ as $\mathbf{x}_1, \cdots, \mathbf{x}_S$. Now consider the $s \times S$ matrix $\mathcal{M}$ where the ij-th entry is $M_j(\mathbf{x}_i)$. If the rank of $\mathcal{M}$ is less than s, then we can take a non-trivial vector $\mathbf{g}$ from its kernel with integer entries which defines a form of weighted degree u vanishing on $X(\mathbb{Q}; \mathbf{B}, \mathfrak{P})$. By the linear independence of the monomials M_i, we see that this form cannot vanish identically on X, so it gives rise to a hypersurface satisfactory for our purposes. In order to force the rank of $\mathcal{M}$ to be less than s, we will show that every $s \times s$ sub-matrix of $\mathcal{M}$ has vanishing determinant. The quality of this result depends heavily on the number of linearly independent monomials we have available per degree u, a point which we will return to later when we discuss Salberger's improvement.

To show that the rank of any $s \times s$ sub-matrix of $\mathcal{M}$ is less than s, we use the fact that the points in $X(\mathbb{Q}; \mathbf{B}, \mathfrak{P})$ are congruent to each other modulo the primes $p_1, \cdots, p_t$. This means that given any $s \times s$ sub-matrix, say $\mathcal{M}'$, we can perform column operations to show that the determinant of $\mathcal{M}'$ is divisible by a large power of $p_1, \cdots, p_t$. The key to the argument is that after performing column operations, one can reach a state where there are few columns whose order of vanishing is small. This allows us a tremendous gain over the trivial estimate where $p_1, \cdots, p_t$ divides each column to the first power only. This in turn allows us to produce a very large divisor of $\det \mathcal{M}'$, and we recall that $\det \mathcal{M}'$ is an integer. By imposing conditions on $\mathfrak{P}$ so that this divisor is large with respect to the

upper bound for $\det \mathcal{M}'$ imposed by the bounds $\mathbf{B}$, we can force $\det \mathcal{M}' = 0$ and since the argument is uniform for any $s \times s$ sub-matrix $\mathcal{M}'$ of $\mathcal{M}$, we see that the rank of $\mathcal{M}$ is less than s, as desired.

We now state our generalization of the main theorem of the global determinant method to the case of weighted projective spaces where two of the weights are 1:

Theorem 4.0.1. *Let $\mathbf{B} = (B_0, \cdots, B_{r+1}) \in \mathbb{R}^{r+2}$ be a vector of positive numbers of size at least 1 and let $\mathbf{w} = (1, 1, w_2, \cdots, w_{r+1})$ be a vector of positive integers. Let X be a hypersurface in $\mathbb{P}(\mathbf{w})$ which is irreducible over $\mathbb{Q}$ and defined by a primitive weighted homogeneous form F in $\mathbb{Z}[x_0, \cdots, x_{r+1}]$ of weighted degree d with respect to $\mathbf{w}$. Let $I = \langle F \rangle$ be the weighted homogeneous ideal generated by F. Let $\mathcal{P}$ be a finite set of primes and put*

$$\mathcal{Q} = \prod_{p \in \mathcal{P}} p.$$

For each prime p in $\mathcal{P}$ let P_p be a non-singular point in X_p and put

$$\mathfrak{P} = \{P_p : p \in \mathcal{P}\}.$$

(a) Let $\varepsilon > 0$. If

$$WV^{\varepsilon} \leq \mathcal{Q} \leq WV^{2\varepsilon}$$

then there is a hypersurface $Y(\mathfrak{P})$ containing $X(\mathbb{Q}; \mathbf{B}, \mathfrak{P})$, not containing X and defined by a primitive form $G \in \mathbb{Z}[x_0, \cdots, x_{r+1}]$, whose weighted degree satisfies

$$\deg G = O_{d,r,\mathbf{w},\varepsilon}(1), \tag{4.0.3}$$

and whose height satisfies

$$\log \|G\| = O_{d,r,\mathbf{w},\varepsilon}\left(\log V\right). \tag{4.0.4}$$

(b) If X is geometrically integral, then there exists a hypersurface $Y(\mathfrak{P})$ containing $X(\mathbb{Q}; \mathbf{B}, \mathfrak{P})$, not containing X and defined by a primitive form $G \in \mathbb{Z}[x_0, \cdots, x_{r+1}]$, whose degree satisfies

$$\deg G = O_{\mathbf{w},d,r}\left((1 + \mathcal{Q}^{-1}W) \log V\mathcal{Q}\right).$$

The second part of Theorem 4.0.1 is a generalization of Salberger's Theorem 2.2 in [93] to the case of weighted projective hypersurfaces, and the first part is a generalization of

Salberger's Lemma 2.8 in [93]. Lemma 2.8 in [93] is itself an extension of Heath-Brown's Theorem 14 in [53]. In fact, both theorems are recovered if we set $\mathbf{w} = (1, 1, \cdots, 1)$. We note that, unlike earlier formulations when $\mathcal{Q} \geq WV^{\varepsilon}$, the dependence of the logarithm of the height of G on the degree d and the dependence of the degree of G on the degree d of F and the parameter ε is explicit with the remaining constant depending only on the dimension r and the weight vector $\mathbf{w}$.

M. Walsh was able to obtain an improved version of Theorem 1.1 of [93] in [103]. This corresponds to the case $\mathcal{P} = \emptyset$ in Theorem 4.0.1. His improvement was to show that one can obtain a saving of $\log(\|F\|+1)\|F\|^{-r^{-1}d^{-(r+1)/r}}$ on the estimate for the degree of the form G.

We will complete the proof of Theorem 4.0.1 in the next few sections.

In [94], Salberger devised an even more powerful version of the determinant method when the degree of X is small compared to its dimension r. We have named this modification of the determinant method the *Salberger improvement*. We have noticed that Salberger's improvement can be applied to weighted projective spaces as well, which allows us to obtain a stronger version of Theorem 4.0.1 in certain settings.

We will give a quick description of Salberger's improvement here. As we mentioned before, a bottleneck of the p-adic determinant method is finding many monomials which are linearly independent over X. In general, one cannot do better than the Hilbert function $H_{I(X)}(u)$ for each degree u. However, Salberger, in [94], gave a brilliant construction which yielded many more monomials in certain situations. In particular, he showed that whenever the degree of the variety X is sufficiently small with respect to its dimension, then one can construct more monomials than can be expected from the Hilbert function. We formalized his ideas and formulated the so-called *trading ratio* (see Section 4.5) λ, which depends only on the weight vector $\mathbf{w}$. For a given weight vector $\mathbf{w}$ and $w = w_0 \cdots w_{n+1}$ with associated trading ratio λ, we put

$$\mathfrak{S}(d, n, \mathbf{w}) = \left(\frac{w}{d}\right)^{1/n} \left(\left(\frac{d}{\lambda w}\right)^{1/(n-1)} (n-1) + \lambda \right).$$

We shall prove:

Theorem 4.0.2. *Let X be a weighted projective hypersurface in $\mathbb{P}(\mathbf{w})$ of degree $2 \leq d < 2^r w$. Let $\mathbf{B} = (B_0, \cdots, B_{n+1}) \in \mathbb{R}^{r+2}$ be a vector of positive numbers of size at least 1. Let*

$\varepsilon > 0$ and $p_1, \cdots, p_t$ be distinct primes with

$$\mathcal{Q} = p_1 \cdots p_t \geq W^{\frac{n}{\mathfrak{S}(d,n,\mathbf{w})}} V^{\varepsilon}.$$

For $i = 1, \cdots, t$, let P_i be a non-singular point on X_{p_i}. Then there exists a hypersurface $Y(\mathbf{B}, P_1, \cdots, P_t)$ of degree bounded solely in terms of ε which contains $X(\mathbb{Q}; \mathbf{B})$ but does not contain X.

4.1 Hilbert functions on weighted projective varieties

In this section, we work out some basic notions of Hilbert functions and weighted homogeneous ideals needed for the rest of the paper. Salberger relied on the analogous results in the projective case for his results in [92].

Let K be a fixed field of characteristic zero. We write $\boldsymbol{\alpha} = (\alpha_0, \cdots, \alpha_{r+1})$ to denote a sequence of non-negative integers, and for $\mathbf{x} = (x_0, \cdots, x_{r+1})$ we write

$$\mathbf{x}^{\boldsymbol{\alpha}} = x_0^{\alpha_0} \cdots x_{r+1}^{\alpha_{r+1}}.$$

Let $\mathbf{w} = (w_0, \cdots, w_{r+1})$ be a weight vector and let u be a non-negative integer. For a monomial $\mathbf{x}^{\boldsymbol{\alpha}} = x_0^{\alpha_0} \cdots x_{r+1}^{\alpha_{r+1}}$, define the *weighted degree* of $\mathbf{x}^{\boldsymbol{\alpha}}$ with respect to $\mathbf{w}$ to be

$$\boldsymbol{\alpha} \cdot \mathbf{w} = \alpha_0 w_0 + \cdots + \alpha_{r+1} w_{r+1}.$$

We say a polynomial $F \in K[x_0, \cdots, x_{r+1}]$ is *weighted homogeneous* (with respect to $\mathbf{w}$) of weighted degree u if for each monomial $\mathbf{x}^{\boldsymbol{\alpha}}$ that appears in F with a non-zero coefficient, the weighted degree of $\mathbf{x}^{\boldsymbol{\alpha}}$ is equal to u. This allows us to define the degree of a hypersurface X in $\mathbb{P}(\mathbf{w})$, but not necessarily the degree of a subvariety of codimension greater than one. This will not be an issue since in our main application, we will embed such subvarieties explicitly into a lower dimensional weighted projective space, in which they will have codimension equal to one and so the definition for the hypersurface case applies. In other situations, we will rely on a pullback to a straight projective space where the notion of degree is well understood.

Define the set $K[x_0, \cdots, x_{r+1}]_{\mathbf{w},u}$ to be the collection of weighted homogeneous polynomials with weight vector $\mathbf{w}$ whose weighted degree is equal to u. We say that $I \subset K[x_0, \cdots, x_{r+1}]$ is a *weighted homogeneous ideal* (with respect to $\mathbf{w}$) if I is generated

by a set of weighted homogeneous polynomials with respect to the weight vector $\mathbf{w}$. If $I \subset K[x_0, \cdots, x_{r+1}]_{\mathbf{w}}$ is a weighted homogeneous ideal with weight vector $\mathbf{w}$, then the set I_u given by

$$I_u = I \cap K[x_0, \cdots, x_{r+1}]_{\mathbf{w},u}$$

is a K-subspace of $K[x_0, \cdots, x_{r+1}]_{\mathbf{w},u}$. Like in the projective case, we can define the Hilbert function of I to be

$$\mathcal{H}_I(u) = \dim_K(K[x_0, \cdots, x_{r+1}]_{\mathbf{w},u}/I_u).$$

We can define a graded order $<$ on $K[x_0, \cdots, x_{r+1}]$ by the following: for $\boldsymbol{\alpha} = (\alpha_0, \cdots, \alpha_{r+1})$, $\boldsymbol{\beta} = (\beta_0, \cdots, \beta_{r+1}) \in \mathbb{Z}_{\geq 0}^{r+2}$ we have $\boldsymbol{\alpha} > \boldsymbol{\beta}$ if $w_0\alpha_0 + \cdots + w_r\alpha_r + w_{r+1}\alpha_{r+1} > w_0\beta_0 + \cdots + w_r\beta_r + w_{r+1}\beta_{r+1}$. If there is a tie, i.e. $w_0\alpha_0 + \cdots + w_{r+1}\alpha_{r+1} = w_0\beta_0 + \cdots + w_{r+1}\beta_{r+1}$, then we take $\boldsymbol{\alpha} > \boldsymbol{\beta}$ if $\alpha_{r+1} - \beta_{r+1} > 0$. If the weighted sums are equal and $\alpha_{r+1} = \beta_{r+1}$, then we compare α_r and β_r. This continues until we break the tie, so this ordering is a total order. Under this ordering, we can define the leading term of a given polynomial.

Definition 4.1.1. Suppose

$$F(x_0, \cdots, x_{r+1}) = \sum_{\mathbf{w}\cdot\boldsymbol{\beta}=u} c_{\boldsymbol{\beta}}\mathbf{x}^{\boldsymbol{\beta}} \in K[x_0, \cdots, x_{r+1}]$$

is a weighted homogeneous polynomial with respect to the weight vector $\mathbf{w}$ of weighted degree u. Suppose $\mathbf{x}^{\boldsymbol{\alpha}}$ is a monomial which appears in F with non-zero coefficient and which is maximal with respect to the total order $<$. Then, we say that $\mathbf{x}^{\boldsymbol{\alpha}}$ is the *leading monomial* of F. If we include the coefficient $c_{\boldsymbol{\alpha}}$ of $\mathbf{x}^{\boldsymbol{\alpha}}$, then $c_{\boldsymbol{\alpha}}\mathbf{x}^{\boldsymbol{\alpha}}$ is the *leading term* of F which we write as $\mathrm{LT}(F)$.

Write $\langle \mathrm{LT}(I) \rangle$ to denote the ideal generated by the leading terms of polynomials in I. Our first result is the following:

Proposition 4.1.2. *Let $I \subset K[x_0, \cdots, x_{r+1}]_{\mathbf{w}}$ be a weighted homogeneous ideal. Then I has the same Hilbert function as $\langle \mathrm{LT}(I) \rangle$.*

Proof. The argument is identical to Proposition 9 in Chapter 9 of [29]. □

Remark 4.1.3. The choice of the ordering $<$ does not matter in Proposition 4.1.2. Indeed, we will choose slightly different orderings when convenient.

We have

$$\mathcal{H}_I(u) = \mathcal{H}_{\mathrm{LT}(I)}(u).$$

With this characterization, we can define for each $i \in \{0, 1, \cdots, r+1\}$

$$\sigma_{I,i}(u) = \sum_{\substack{\boldsymbol{\beta}\cdot\mathbf{w}=u \\ \mathbf{x}^{\boldsymbol{\beta}} \notin \mathrm{LT}(I)}} \beta_i. \tag{4.1.1}$$

From the definition of the Hilbert function, there are $\mathcal{H}_I(u)$ many monomials that are not the leading monomial of any polynomial in I_u. Thus, it follows immediately that

$$w_0\sigma_{I,0}(u) + \cdots + w_r\sigma_{I,r}(u) + w_{r+1}\sigma_{I,r+1}(u) = u\mathcal{H}_I(u).$$

Now by Theorem 3.4.4 in [36], the Hilbert series of a hypersurface generated by a form F of weighted degree d with respect to the weight vector $\mathbf{w}$ is given by

$$\frac{(1-x^d)}{(1-x^{w_0})\cdots(1-x^{w_{r+1}})}. \tag{4.1.2}$$

From here on, we shall assume that our weight vector $\mathbf{w}$ has the property that the gcd of any $r+1$ of the weights is equal to 1. This distinction will be automatic in the relevant weight vectors in our paper; see Theorem 4.2.1. Thus, by examining the poles of the function above we conclude that there is only one pole of order $r+1$, we see that the u-th coefficient is of the form

$$\mathcal{H}_I(u) = \frac{du^r}{r!w_0\cdots w_{r+1}} + O_{\mathbf{w},r}(d^{r+1} + d^2u^{r-1}) = \frac{du^r}{r!w_0\cdots w_{r+1}} + O_{\mathbf{w},r}(d^{r+1}u^{r-1}), \tag{4.1.3}$$

where the constant in front of the big-O term depends only on $w_0, \cdots, w_{r+1}$ and r.

The argument in the proof of our next result, Proposition 4.1.4, was inspired by a discussion on MathOverflow with Richard Stanley [97]. In particular, the construction of the generating function used below was suggested by Stanley.

Proposition 4.1.4. *Let K be a field of characteristic zero and $<$ be the graded monomial ordering as before. Suppose $F(x_0, \cdots, x_{r+1}) \in K[x_0, \cdots, x_{r+1}]$ has weighted degree d with respect to $\mathbf{w}$ and leading monomial $\mathbf{x}^{\boldsymbol{\alpha}}$. Set $I = \langle F \rangle$. Define $\sigma_{I,m}(u)$ as in (4.1.1). Then*

$$\sigma_{I,m}(u) = a_{I,m}u\mathcal{H}_I(u) + O_{\mathbf{w},d,r}(u^r),$$

where

$$a_{I,m} = \frac{d - w_m\alpha_m}{(r+1)w_m d} \tag{4.1.4}$$

for $m = 0, 1, \cdots, r+1$.

Proof. Suppose that $\mathbf{x}^{\boldsymbol{\beta}}$ is a monomial of weighted degree u with respect to the weight vector $\mathbf{w}$. Then $\mathbf{x}^{\boldsymbol{\beta}} \in \langle \mathrm{LT}(I) \rangle$ if and only if $\mathbf{x}^{\boldsymbol{\alpha}} | \mathbf{x}^{\boldsymbol{\beta}}$. Hence, we need to count those monomials $\mathbf{x}^{\boldsymbol{\beta}} = x_0^{\beta_0} \cdots x_{r+1}^{\beta_{r+1}}$ of weighted degree u such that at least one of the exponents $\beta_i < \alpha_i$. Write $\sum^*$ to indicate a summation taken over those $\boldsymbol{\beta} = (\beta_0, \cdots, \beta_{r+1}) \in \mathbb{Z}_{\geq 0}^{r+2}$ such that $w_0\beta_0 + \cdots + w_{r+1}\beta_{r+1} = u$ and that $\beta_j < \alpha_j$ for some $0 \leq j \leq r+1$. Our goal, then, is to evaluate the sum

$$\sigma_{I,m}(u) = \sum{}^* \beta_m$$

for each $0 \leq m \leq r+1$. To do this, let us define:

$$T_m^j(u) = \sum_{\substack{\boldsymbol{\beta} \cdot \mathbf{w} = u \\ \beta_j < \alpha_j}} \beta_m.$$

We want to emphasize that the evaluation of $T_m^j(u)$ will vary based on whether $j \neq m$ or $j = m$. In fact, the terms $T_m^m(u)$ will be negligible. We address the former situation. Define the function

$$G_{j,m}(x,y) = \frac{1 + y^{w_j} + \cdots + y^{w_j(\alpha_j - 1)}}{[\prod_{t \neq j,m}(1 - y^{w_t})](1 - xy^{w_m})}$$

for $j \neq m$. We then take the derivative with respect to x and evaluate at $x = 1$ to obtain

$$\frac{d}{dx} G_{j,m}(x,y)|_{x=1} = \frac{(1 + y^{w_j} + \cdots + y^{(\alpha_j - 1)w_j}) y^{w_m}}{[\prod_{t \neq j,m}(1 - y^{w_t})](1 - y^{w_m})^2}. \tag{4.1.5}$$

Note that $T_m^j(u)$ is equal to the coefficient of y^u in the series expansion of (4.1.5) around 0. Since no $r+1$ of the weights have a common factor, it follows that for each root of unity ζ, ζ is a root of at most $r+1$ factors in the denominator of (4.1.5). Hence there is a single pole of order $r+2$ at $y = 1$.Since the highest order pole in (4.1.5) is $r+2$, its Laurent series around 0 is given by

$$c_{-r-2} y^{-r-2} + c_{-r-1} y^{-r-1} + \cdots$$

for complex coefficients $c_t \in \mathbb{C}$. Using Cauchy's integral formula, we can calculate the coefficient c_{-r-2}:

$$\frac{1}{2\pi i} \oint \frac{(1-z)^{r+1}(1 + z^{w_j} + \cdots + z^{w_j(\alpha_j - 1)}) z^{w_j}}{(1 - z^{w_m})^2 \prod_{t \neq j,m}(1 - z^{w_t})} dz,$$

and get that

$$c_{-r-2} = \frac{\alpha_j}{w_m^2 \prod_{t \neq j,m} w_t}.$$

Thus, $T_m^j(u)$ is asymptotically given by

$$\frac{\alpha_j}{w_m^2 \prod_{t \neq j,m} w_t} \frac{u^{r+1}}{(r+1)!}$$

for $j \neq m$, as $u \to \infty$. We now examine the contribution to $T_m^j(u)$ from other poles. From (4.1.5), it follows that each pole is a root of unity. Recall that there are no other poles of order $r+2$. The contribution from a pole ζ of order k less than $r+2$ is given by

$$\frac{1}{2\pi i} \oint \frac{(\zeta - z)^{k-1}(1 + z^{w_j} + \cdots + z^{w_j(\alpha_j - 1)}) z^{w_j}}{(1 - z^{w_m})^2 \prod_{t \neq j,m} (1 - z^{w_t})} dz.$$

The evaluation of this integral will depend on whether ζ is a w_t-th root of unity for $t \neq j$. To help us evaluate the integral, define

$$\mathfrak{f}_{\zeta,t}(z) = \begin{cases} \dfrac{1}{1 - z^{w_t}}, & \text{if } \zeta^{w_t} \neq 1, \\ \dfrac{\zeta - z}{1 - z^{w_t}}, & \text{if } \zeta^{w_t} = 1. \end{cases}$$

We now estimate $\mathfrak{f}_{\zeta,t}(\zeta)$ in both cases. Put $\zeta = e^{\frac{2\pi i l}{n}}$ with $\gcd(l, n) = 1$. Then

$$\begin{aligned} 1 - \zeta^{w_t} &= 1 - \cos\left(\frac{2\pi w_t l}{n}\right) - i \sin\left(\frac{2\pi w_t l}{n}\right) \\ &= 2 \sin\left(\frac{\pi w_t l}{n}\right) \left(\sin\left(\frac{\pi w_t l}{n}\right) - i \cos\left(\frac{\pi w_t l}{n}\right)\right). \end{aligned}$$

The term in the parentheses on the right has absolute value one, and we have

$$\left| 2 \sin\left(\frac{\pi w_t l}{n}\right) \right| \geq 2 \sin(\pi/n).$$

Moreover, $n \geq 2$, and on the interval $[0, \pi/2]$ $\sin(x)$ satisfies

$$\sin(x) \geq \frac{2x}{\pi},$$

whence

$$\left| 2 \sin\left(\frac{\pi w_t l}{n}\right) \right| \geq \frac{4}{n}.$$

Therefore, in this case, we have

$$|\mathfrak{f}_{\zeta,t}(\zeta)| \leq \frac{n}{4}.$$

In the second case, we put η for a primitive w_t-th root of unity, and put $\zeta = \eta^l$ for some $1 \leq l \leq w_t - 1$. Then we make the observation that

$$\prod_{\substack{1 \leq s \leq w_t \\ s \neq l}} (\zeta - \eta^s) = n\zeta^{n-1}.$$

Thus, in this case, we have $|\mathfrak{f}_{\zeta,t}(\zeta)| = n^{-1}$.

Next, we deal with the numerator $\mathfrak{g}(z) = 1 + z^{w_j} + \cdots + z^{w_j(\alpha_j - 1)}$. We note that if $\mathfrak{g}(\zeta) \neq 0$, then we can simply bound from above by the triangle inequality to obtain the upper bound α_j. Otherwise we make the observation that the contribution to the residue is equal to evaluating

$$\mathfrak{g}(z)(z - \zeta)^{-1}$$

at $z = \zeta$, which is equivalent to evaluating $\mathfrak{g}'(z) = w_j z^{w_j - 1} + \cdots + w_j(\alpha_j - 1)z^{w_j(\alpha_j - 1) - 1}$ at $z = \zeta$. The latter is readily seen to be bounded from above by $\dfrac{w_j \alpha_j (\alpha_j - 1)}{2}$.

Combining these estimates, we see that order of magnitude of the residue does not exceed

$$\frac{w_j \alpha_j (\alpha_j - 1)}{2} n^{r+2-2k}.$$

Therefore, the contribution to $T_m^j(u)$ from each pole of order k is at most

$$\frac{w_j \alpha_j (\alpha_j - 1) n^{r+2-2k}}{2} \frac{u^k}{k!}.$$

Note that n is bounded above by the maximum of the w_t's and bounded from below by the minimum of the w_t's and 2. Moreover, α_j is bounded from above by d. We have thus obtained an acceptable error term as stated in the proposition.

For the case $j = m$, we put

$$G_{m,m}(x, y) = \frac{1 + xy^{w_m} + \cdots + (xy^{w_m})^{\alpha_m - 1}}{\prod_{t \neq m}(1 - y^{w_t})},$$

so that

$$\frac{d}{dx} G_{m,m}(x, y)|_{x=1} = \frac{y + 2y^2 + \cdots + (\alpha_m - 1)y^{\alpha_m - 1}}{\prod_{t \neq m}(1 - y^{w_t})}. \tag{4.1.6}$$

The pole at $y = 1$ is only of order $r + 1$ as opposed to $r + 2$. By examining the Laurent series of (4.1.6) and evaluating the $-(r + 1)$-th coefficient, we see that the contribution from the pole of order $(r + 1)$ is equal to

$$\frac{\alpha_m(\alpha_m - 1)}{\prod_{t\neq m} w_t}\frac{u^r}{r!}.$$

Observe that the coefficient is bounded from above by d^2. The lower order poles can be analyzed as before, so we omit this step.

We now consider sums of the form

$$\sum\nolimits^{\natural} \beta_m$$

where the symbol $\sum^{\natural}$ indicates the sum is taken over those β such that there exist at least two indices i, j for which $\beta_i < \alpha_i$ and $\beta_j < \alpha_j$. Noting that $\alpha_j \leq d$ for $0 \leq j \leq r + 1$ we see that the contribution from these sums is at most $C_3(\mathbf{w}, r)d^2u^r$, where $C_3(\mathbf{w}, r)$ is a number which depends on $\mathbf{w}$ and r only. The existence of such a $C_3(\mathbf{w}, r)$ follows from analyzing the order of poles as above and applying Cauchy's integral formula as above. Thus, by the inclusion exclusion principle, we see that for $0 \leq m \leq r + 1$

$$\begin{aligned}\sigma_{I,m}(u) &= \sum_{0\leq j\leq r+1} T_m^j(u) + O_{\mathbf{w},d,r}\left(u^r\right)\\ &= \frac{1}{w_m\prod_{t=0}^{r+1} w_t}\left(\frac{w_0\alpha_0u^{r+1}}{(r+1)!} + \cdots + \frac{w_{r+1}\alpha_{r+1}u^{r+1}}{(r+1)!} - \frac{w_m\alpha_mu^{r+1}}{(r+1)!}\right) + O_{\mathbf{w},d,r}(u^r)\\ &= \frac{(d - w_m\alpha_m)u^{r+1}}{(r+1)!w_m\prod_{t=0}^{r+1} w_t} + O_{\mathbf{w},d,r}(u^r).\end{aligned}$$

Now, recall that $u\mathcal{H}_I(u) = \dfrac{du^{r+1}}{r!\prod_{t=0}^{r+1} w_t} + O_{\mathbf{w},d,r}(u^r)$, and hence we have, for $0 \leq m \leq r+1$,

$$\sigma_{I,m}(u) = \frac{d - w_m\alpha_m}{(r+1)w_md}u\mathcal{H}_I(u) + O_{\mathbf{w},d,r}\left(u^r\right).$$

This completes the proof of Proposition 4.1.4. □

4.2 Large divisors of the determinant

Our next theorem produces a prime power divisor of a determinant of the form $\det(M_j(\boldsymbol{\xi}_l))$, where $M_1, \cdots, M_s$ are monomials of the same weighted degree and where $\boldsymbol{\xi}_l \in \mathbb{Z}^{r+2}$,

$1 \leq l \leq s$ are all congruent to a point $P \in X_p$. The additional assumption that these tuples are congruent to some point $P \in X_p$ as opposed to the weaker assumption that they are merely congruent modulo p gives the extra geometric information that allows us to produce a divisor which is larger. Indeed, if we assume only that $\boldsymbol{\xi}_l \equiv \boldsymbol{\xi}_j \pmod{p}$ for $1 \leq j, l \leq s$, then by taking differences of columns we can produce a factor of p in each column, thereby allowing us to conclude that $p^{s-1} | \det(M_j(\boldsymbol{\xi}_l))$. However, our next theorem shows that for sufficiently large s, we can produce a larger power of p which divides $\det(M_j(\boldsymbol{\xi}_l))$. We aim to establish the following:

Theorem 4.2.1. *Let $\mathbf{w} = (1, 1, w_2, \cdots, w_{r+1})$ be a weight vector, p be a prime, X be a hypersurface of degree d in $\mathbb{P}(\mathbf{w})$, and P be an $\mathbb{F}_p$ point of multiplicity m_P on X_p. Suppose there are s distinct primitive $(r+2)$-tuples of integers on X*

$$\boldsymbol{\xi}_1, \cdots, \boldsymbol{\xi}_s$$

with reduction P, such that $\gcd(\xi_{0,l}, \xi_{1,l}) = 1$ for $1 \leq l \leq s$. If $M_1, \cdots, M_s$ are monomials in $(x_0, \cdots, x_{r+1})$ of the same weighted degree, then there exists a positive number $\kappa(d, r)$, depending on d and r, such that the determinant of the $s \times s$ matrix $(M_j(\boldsymbol{\xi}_l))$ is divisible by p^N, where

$$N > \left(\frac{r!}{m_P}\right)^{\frac{1}{r}} \cdot \frac{r}{r+1} \cdot s^{1+\frac{1}{r}} - \kappa(d, r)s.$$

If P is non-singular, so $m_P = 1$, then there exists a positive number $\kappa'(r)$, depending only on r, such that

$$N > (r!)^{1/r} \frac{r}{r+1} s^{1+\frac{1}{r}} - \kappa'(r)s.$$

We will prove Theorem 4.2.1 by means of the next two propositions; corresponding to Lemmas 2.3 and 2.4 respectively in [92]. We note here that for the proof of Theorem 4.2.1 we require that two of the weights be 1. This is the only part of the paper where we need to make such an assumption.

We remark that this restriction can be removed if we a priori pick monomials whose weighted degrees are a multiple of the least common multiple of all of the weights, and indeed this opens up the possibility to extend the determinant method to all weighted projective spaces. However the extra technical details take us too far afield in the present paper. We would like to return to this issue in the future.

Proposition 4.2.2. *Let $\mathbf{w} = (1, 1, \cdots, w_{r+1})$ be a weight vector, X a hypersurface of weighted degree d in $\mathbb{P}(\mathbf{w})$, p a prime and P an $\mathbb{F}_p$-point of multiplicity m_P on X_p. Write*

A for the local ring of regular functions at P and $\mathfrak{m}$ for the maximal ideal of A. For each positive integer t put $g_{X,P}(t) = \dim_{A/\mathfrak{m}} \mathfrak{m}^t/\mathfrak{m}^{t+1}$. Then, we have

$$g_{X,P}(t) = \frac{m_P t^{r-1}}{(r-1)!} + O_{d,r}(t^{r-2}).$$

If $m_P = 1$, then we obtain the more refined assertion that

$$g_{X,P}(t) = \frac{t^{r-1}}{(r-1)!} + O_r(t^{r-2}).$$

Proof. Write $\mathcal{B} = \bigoplus_{t\geq 0}(\mathfrak{m}^t/\mathfrak{m}^{t+1})$. By definition, the projectivized tangent cone at P is defined to be the $\mathrm{Proj}(\mathcal{B})$, see Exercise III-29 in [37]. Since $A/\mathfrak{m} \cong \mathbb{F}_p$ is a field, it follows that $g_{X,P}(t)$ is precisely the Hilbert function of the projectivized tangent cone at P, say W_P. Note that W_P is a subvariety of the Zariski tangent space of X at P, which is isomorphic to $\mathbb{P}^r_{\mathbb{F}_p}$. Hence, we can consider the homogeneous ideal of W_P, which is generated by $C_4(d,r)$ many forms; see III.3 of [80]. Note that this bound depends only on d and r. Following Lemma 1 of [18], we may choose a Groebner basis of forms of degree $C_5(d,r)$ for the homogeneous ideal of W_P. By Proposition 4.1.2, the Hilbert function does not change if we replace this ideal with the ideal generated by its leading terms. Hence, there are only finitely many candidates for Hilbert functions of W_P for points P of multiplicity $m_P = O_{\mathbf{w},d}(1)$. More precisely, the number of candidates is bounded by the number of monomials in $r-1$ variables of degree at most $C_5(d,r)$. Thus, there are at most $C_6(d,r)$ such functions.

Let us now fix a particular

$$g_{X,P}(t) = \frac{m_P t^{r-1}}{(r-1)!} + O_{P,r}(t^{r-2}).$$

To obtain the estimate for the coefficient in front of the big-O term, one notes that there exists a polynomial $Q(x)$ with integer coefficients with $Q(1) \neq 0$ such that the Hilbert series of the projectivized tangent cone is given by

$$\frac{Q(x)}{(1-x)^r},$$

see Chapter 9 of [29]. From here we see from Proposition 4.1.4 that the error term is at most an absolute constant times m_P^{r-1}. Since $m_P = O_{\mathbf{w},d}(1)$, the claim follows.

If $m_P = 1$, then it is known (see III.3 in [80]) that the ideal of the tangent cone at P is generated by a single polynomial of degree 1. Hence, we can replace $C_4(d,r), C_5(d,r)$, and $C_6(d,r)$ with numbers that depend at most on r. □

We shall denote by $\mathbb{Z}_p$ the ring of p-adic integers. Let R be a commutative noetherian local ring containing $\mathbb{Z}_p$ as a subring, $\mathcal{R} = R/pR$, and $\mathfrak{m}$ be the maximal ideal of $\mathcal{R}$. We then have the following proposition:

Proposition 4.2.3. *Let $(n_l(\mathcal{R}))_{l=1}^{\infty}$ be the non-decreasing sequence of integers $t \geq 0$, where t occurs exactly $\dim_{\mathcal{R}/\mathfrak{m}} \mathfrak{m}^t/\mathfrak{m}^{t+1}$ times. Let $r_1, \cdots, r_s$ be elements of R and $\varphi_1, \cdots, \varphi_s$ be ring homomorphisms from R to $\mathbb{Z}_p$. Then, the determinant of the $s \times s$ matrix $(\varphi_i(r_j))$ is divisible by $p^{A(s)}$ for $A(s) = n_1(\mathcal{R}) + \cdots + n_s(\mathcal{R})$.*

Proof. This is the same as the proof of Lemma 2.4 in [92]. □

Proof. (Theorem 4.2.1) Let R be the local ring of X over $\mathbb{Z}_p$ at the point P with respect to the weight vector $\mathbf{w} = (1, 1, w_2, \cdots, w_{r+1})$ and $\mathcal{R} = R/pR$. Since $\gcd(x_0, x_1) = 1$, there exists some index $j = 0, 1$ such that $p \nmid x_j$. Without loss of generality, suppose that $p \nmid x_0$. Then we can replace $M_j(x_0, \cdots, x_{r+1})$ with

$$M_j\left(1, \frac{x_1}{x_0}, \frac{x_2}{x_0^{w_2}}, \cdots, \frac{x_{r+1}}{x_0^{w_{r+1}}}\right)$$

without changing the p-adic valuation of $\det(M_j(\boldsymbol{\xi}_l))$. These rational functions are elements of R. We consider the evaluation maps at the points $\boldsymbol{\xi}_1, \cdots, \boldsymbol{\xi}_s$, which are homomorphisms from R to $\mathbb{Z}_p$. Since $\mathbb{Z}_p \subset R$, the conditions for the ring appearing in Proposition 4.2.3 is satisfied. Thus it follows that

$$p^{A(s)} | \Delta.$$

It remains to estimate $A(s)$. Let $g = g_{X,P}$ be as in proposition 4.2.2 and set $G(t) = g(0) + g(1) + \cdots + g(t)$. Since $g(t) = m_P t^{r-1}/(r-1)! + O_{d,r}(t^{r-2})$, it follows that

$$G(t) = \frac{m_P t^r}{r!} + O_{d,r}(t^{r-1}).$$

By the definition of g and $(n_l(\mathcal{R}))$, it follows that

$$A(G(t)) = g(1) + \cdots + tg(t) = \frac{m_P t^{r+1}}{(r+1)(r-1)!} + O_{d,r}(t^r),$$

and explicitly we have

$$\left(\frac{r!}{m_P}\right)^{\frac{1}{r}} G(t)^{1+\frac{1}{r}} = \left(\frac{r!}{m_P}\right)^{\frac{1}{r}} \left(\frac{m_P t^r}{r!} + O_{d,r}(t^{r-1})\right)^{1+\frac{1}{r}}$$
$$= \frac{m_P t^{r+1}}{r!} + O_{d,r}(t^r).$$

Multiplying by $r/(r+1)$ gives

$$A(G(t)) = \left(\frac{r!}{m_P}\right)^{\frac{1}{r}} \left(\frac{r}{r+1}\right) G(t)^{1+\frac{1}{r}} + O_{d,r}(G(t)),$$

since $t^r = O_{\mathbf{w},d,r}(G(t))$. The fact that

$$A(s) = \left(\frac{r!}{m_P}\right)^{\frac{1}{r}} \left(\frac{r}{r+1}\right) s^{1+\frac{1}{r}} + O_{d,r}(s)$$

follows from the observation that if t is the unique integer such that $G(t-1) < s \leq G(t)$, then

$$0 \leq A(G(t)) - A(s) \leq tg(t) \leq \frac{m_P t^r}{(r-1)!} + O_{d,r}(t^{r-1}) \leq rs + O_{d,r}(s^{1-\frac{1}{r}}),$$

and

$$0 \leq G(t)^{1+\frac{1}{r}} - s^{1+\frac{1}{r}} \leq G(t)^{1+\frac{1}{r}} - G(t-1)^{1+\frac{1}{r}} = O_{d,r}(t^r) = O_{d,r}(s).$$

If $m_P = 1$, then by Proposition 4.2.2 the constants in front of the error terms may be replaced with a number which depends on r only. □

We now proceed to give estimates for products of various 'bad' primes with respect to a geometrically integral hypersurface $X \subset \mathbb{P}(\mathbf{w})$.

Definition 4.2.4. Let X be a geometrically integral hypersurface in $\mathbb{P}(\mathbf{w})$ of degree d. We write π_X for the product of all primes p for which X_p is not geometrically integral.

Let us denote by $R_{r+1}(d)$ the number of distinct monomials in $x_0, \cdots, x_{r+1}$ of weighted degree d with respect to the weight vector $\mathbf{w} = (1, 1, w_2, \cdots, w_{r+1})$.

The next lemma allows us to capture whether a given polynomial is irreducible over $\overline{\mathbb{Q}}$ or not by considering a finite set of universal polynomials. This was first proved by Salberger in [92], and Lemma 4.2.5 below is essentially the same as Lemma 1.8 in [93], except

over weighted projective space.

Denote by $\mathcal{S}_d$ the set of vectors $\boldsymbol{\beta} \in \mathbb{Z}_{\geq 0}^{r+2}$ such that $\boldsymbol{\beta} \cdot \mathbf{w} = d$. Note that

$$\#\mathcal{S}_d = R_{r+1}(d).$$

Let the elements in $\mathcal{S}_d$ be enumerated by $\boldsymbol{\beta}_1, \cdots, \boldsymbol{\beta}_{R_{r+1}(d)}$.

Lemma 4.2.5. *Let d be a positive integer. Then there exists a finite set of universal forms*

$$\Phi_1(a_1, \cdots, a_{R_{r+1}(d)}), \cdots, \Phi_t(a_1, \cdots, a_{R_{r+1}(d)}),$$

with the following property. Whenever the variables a_j take values in a field K, the form

$$F(x_0, \cdots, x_{r+1}) = \sum_{j=1}^{R_{r+1}(d)} a_j \mathbf{x}^{\boldsymbol{\beta}_j}$$

is absolutely irreducible over K if and only if $\Phi_i(a_1, \cdots, a_{R_{r+1}(d)}) \neq 0$ in K for some $i \in \{1, \cdots, t\}$.

Proof. First, we remark that weighted projective space can be realized as an abstract projective scheme by considering a grading corresponding to its weight vector. See Miles Reid's course notes [88]. Thus, let $\mathbb{H}_k$ denote the Hilbert scheme of degree k hypersurfaces in $\mathbb{P}(\mathbf{w})$. Since these hypersurfaces are defined by polynomials of degree k, there is a natural morphism between $\mathbb{H}_k \times \mathbb{H}_{d-k}$ and $\mathbb{H}_d$. Let v_k denote this morphism. Then,

$$F(x_0, \cdots, x_{r+1}) = \sum_{j=1}^{R_{r+1}(d)} a_j \mathbf{x}^{\boldsymbol{\beta}_j}$$

has a factor over K of degree k if and only if the corresponding K-point on $\mathbb{H}_d$ lies in $v_k(\mathbb{H}_k \times \mathbb{H}_{d-k})$. Also, since $\mathbb{H}_k \times \mathbb{H}_{d-k}$ is a projective scheme, $v_k(\mathbb{H}_k \times \mathbb{H}_{d-k})$ must be a closed subset of $\mathbb{H}_d$ by the main theorem in elimination theory in Chapter 3, Section 1 of [29]. The union of $v_k(\mathbb{H}_k \times \mathbb{H}_{d-k})$ over $k = 1, \cdots, d-1$ must be a closed subset of $\mathbb{H}_d$ defined by a finite set of forms

$$\Phi_1(a_1, \cdots, a_{R_{r+1}(d)}), \cdots, \Phi_t(a_1, \cdots, a_{R_{r+1}(d)})$$

over $\mathbb{Z}$ such that F is absolutely irreducible over K if and only if $\Phi_i(a_1, \cdots, a_{R_{r+1}(d)}) = 0$ for all $1 \leq i \leq t$ in K. This completes the proof. □

The next lemma gives an upper bound for π_X in the case when $X(\mathbb{Q};\mathbf{B})$ is not contained in another hypersurface of the same degree as X.

Lemma 4.2.6. *Let $X \subset \mathbb{P}(\mathbf{w})$ be a geometrically integral hypersurface of degree d and $\mathbf{B} = (B_0, \cdots, B_{r+1}) \in \mathbb{R}_{\geq 1}^{r+2}$. Then one of the following statements hold:*

(a) $X(\mathbb{Q};\mathbf{B})$ lies in a hypersurface $Y \neq X$ of degree d,

(b) $\log \pi_X = O_{\mathbf{w},d,r}(1 + \log V)$.

Proof. Let $F(x_0, \cdots, x_{r+1}) = \sum_{j=1}^{R_{r+1}(d)} a_j \mathbf{x}^{\boldsymbol{\beta}_j}$ be a primitive integral form defining X and

$$\Phi_1(a_1, \cdots, a_{R_{r+1}(d)}), \cdots, \Phi_t(a_1, \cdots, a_{R_{r+1}(d)})$$

be the values of the universal forms in Lemma 4.2.5 of the coefficients a_j of F. Then $\Phi_i(a_1, \cdots, a_{R_{r+1}(d)}) \neq 0$ for some $i \in \{1, \cdots, t\}$, as X is geometrically integral. By applying Lemma 4.2.5 to F_p, which is F reduced modulo p, and setting $K = \overline{\mathbb{F}_p}$ for the prime factors p of $\Phi_i(a_1, \cdots, a_{R_{r+1}(d)})$, we see that π_X is a factor of $\Phi_i(a_1, \cdots, a_{R_{r+1}(d)})$. Note that the degree D of Φ_i and the height $\|\Phi_i\|$ are bounded in terms of d and r. Write $S = \#X(\mathbb{Q};\mathbf{B})$ and $s = R_{r+1}(d)$. Form the $S \times s$ matrix $\mathcal{M}$, where the rows correspond to the points $\mathbf{x}_1, \cdots, \mathbf{x}_S \in X(\mathbb{Q};\mathbf{B})$ and the columns correspond to the monomials of weighted degree d. Then the vector $\mathbf{f} \in \mathbb{Z}^s$ corresponding to the coefficients of F satisfies $\mathcal{M}\mathbf{f} = \mathbf{0}$, whence the rank of $\mathcal{M}$ is at most $s-1$. Let $s' \leq s-1$ denote the rank of $\mathcal{M}$. Then, for any $(s'+1) \times (s'+1)$ minor $\mathcal{M}'$ of $\mathcal{M}$, we have $\det \mathcal{M}' = 0$, while there exists some $s' \times s'$ minor $\mathcal{M}''$ of $\mathcal{M}$ such that $\det \mathcal{M}'' \neq 0$. Without loss of generality, assume that $\mathcal{M}''$ consisting of the first s' columns and s' rows of $\mathcal{M}$ is such that $\det \mathcal{M}'' \neq 0$. Then, by taking the $(s'+1) \times (s'+1)$ minor $\mathcal{M}'$ consisting of the first $s'+1$ columns and $s'+1$ rows of $\mathcal{M}$, we have that

$$\det \mathcal{M}' = 0. \tag{4.2.1}$$

Expanding $\det \mathcal{M}'$ along the right most column of $\mathcal{M}'$, we see that (4.2.1) implies that there exists an integral vector $\mathbf{g} \in \mathbb{Z}^s$, whose entries are at most V^{ds}, such that $\mathcal{M}\mathbf{g} = \mathbf{0}$. Let G be the corresponding weighted form. Note that G is not the zero form and has degree d. Further, G vanishes on $X(\mathbb{Q};\mathbf{B})$. Hence, if (a) does not hold, G must be a constant multiple of F. Thus, it follows that

$$\|F\| \ll (R_{r+1}(d))! V^{dR_{r+1}(d)} \tag{4.2.2}$$

where the implied constant is absolute. Therefore, there exists $C_7(\mathbf{w}, d, r)$ such that

$$|\Phi_i(a_1, \cdots, a_{R_{r+1}(d)})| = O_{\mathbf{w},d,r}(V^{C_7(\mathbf{w},d,r)}).$$

Since π_X divides $\Phi_i(a_1, \cdots, a_{R_{r+1}(d)})$, we have

$$\log \pi_X = O_{\mathbf{w},d,r}(1 + \log V)$$

if (a) does not hold, as desired. □

4.3 Proof of Theorem 4.0.1: Preliminaries

In the next two sections we complete the proof of Theorem 4.0.1. We have chosen to give arguments similar to those given by Salberger to prove his Lemma 1.4 in [93], which is stated as Lemma 4.3.1 below. The argument in the proof of Lemma 4.3.1 is essentially the same as the proof of Lemma 1.4 in [93]; Walsh also proved a similar result in [103].

For a given point P on X_p let m_P denote the multiplicity of P. Next, let us write $n_p = \sum_P m_P$, where the sum is over all points $P \in X_p$.

Lemma 4.3.1. *Let X be a geometrically integral hypersurface in $\mathbb{P}(\mathbf{w})$ of degree d defined by a primitive form F, and let p be a prime for which X_p is geometrically integral. Suppose there exist s primitive $(r+2)$-tuples of integers*

$$\boldsymbol{\xi}_1, \cdots, \boldsymbol{\xi}_s$$

representing elements of $X(\mathbb{Q}; \mathbf{B})$. Let $M_1, \cdots, M_s$ be monomials in $(x_0, \cdots, x_{r+1})$ with integer coefficients and the same weighted degree. Then, there is a positive number $\kappa(d, r)$ which depends on d and r, such that the determinant of the $s \times s$ matrix formed by the entries $M_j(\boldsymbol{\xi}_l)$ is divisible by p^N with

$$N > (r!)^{1/r} \frac{r}{r+1} \frac{s^{1+1/r}}{n_p^{1/r}} - \kappa(d, r)s.$$

Remark 4.3.2. The number $\kappa(d, r)$ is the same as in Theorem 4.2.1.

Proof. Let P be an $\mathbb{F}_p$-point on X_p. Write $I_P \subset \{1, \cdots, s\}$ for the set of indices l such that $\boldsymbol{\xi}_l + p\mathbb{Z}^{r+2}$ represents P, and write $s_P = \#I_P$. Then, by Theorem 4.2.1, there exists a non-negative integer

$$N_P > \left(\frac{r!}{m_P}\right)^{1/r} \frac{r}{r+1} s_P^{1+1/r} - \kappa(d, r)s_P, \tag{4.3.1}$$

such that $p^{N_P} | \det(\mathcal{M}_P)$, where $\mathcal{M}_P$ is a $s_P \times s_P$ submatrix of $\mathcal{M}$ with second indices $l \in I_P$. By Laplace expansion, we can express Δ as follows:

$$\Delta = \sum \operatorname{sgn}(\mathcal{M}_P, \mathcal{M}'_P) \det(\mathcal{M}_P) \det(\mathcal{M}'_P),$$

where the sum is over all $s_P \times s_P$ minors $\mathcal{M}_P$ along the indices in I_P and $\mathcal{M}'_P$ is the complementary minor of $\mathcal{M}_P$. We can iterate this process with each $\mathcal{M}'_P$, which consists of rows with indices in the set $\{1, \cdots, s\} \setminus I_P$. Each iteration yields a divisor of Δ which is independent of p^{N_P}. Hence, we get that $p^N | \Delta$, where

$$N = \sum_P N_P > (r!)^{1/r} \frac{r}{r+1} \sum_P \frac{s_P^{1+1/r}}{m_P^{1/r}} - \kappa(d,r)s.$$

By Hölder's inequality, we get that

$$s = \sum_P s_P \leq \left(\sum_P m_P \right)^{1/(r+1)} \left(\sum_P \frac{s_P^{1+1/r}}{m_P^{1/r}} \right)^{r/(r+1)}.$$

Re-arranging, we obtain

$$\sum_P \frac{s_P^{1+1/r}}{m_P^{1/r}} \geq \frac{s^{1+1/r}}{n_p^{1/r}}.$$

Thus, we have that

$$N \geq (r!)^{1/r} \frac{r}{r+1} \frac{s^{1+1/r}}{n_p^{1/r}} - \kappa(d,r)s,$$

as desired. □

We now draw on some results of Lang and Weil in [74] on the number of points of algebraic varieties over finite fields. Let us define $X_{p,\text{sing}}$ to be the singular locus of X_p. Let $X_{p,j}$ be the zero locus of the partial derivative $\dfrac{\partial F}{\partial x_j}$ over $\mathbb{F}_p$. Then $X_{p,\text{sing}} \subset X_p \cap X_{p,j}$ for each $j = 0, \cdots, r+1$. In particular, $X_{p,\text{sing}}$ has co-dimension at least one in X_p since the partial derivatives of F do not all vanish identically. By example 4 on page 130 of [7], both X_p and $X_{p,j}$ arise as quotients under the same action of hypersurfaces of degree d and $d-1$ respectively over $\mathbb{P}^{r+1}(\mathbb{F}_p)$, thus the usual Bézout's theorem gives an upper bound for the number of components in $X_{p,\text{sing}}$ as well as its degree. Therefore, the sum of the degrees of the irreducible components of $X_{p,\text{sing}}$ is bounded in terms of d and r. Hence, by

Lemma 1 in [74], we have $\#X_{p,\mathrm{sing}}(\mathbb{F}_p) = O_{\mathbf{w},d,r}(p^{r-1})$. Since the multiplicity of a point on X_p is bounded in terms of d, it follows that

$$\sum_P (m_P - 1) = O_{\mathbf{w},d,r}(p^{r-1}).$$

Theorem 1 of [74] states that $\#X_p(\mathbb{F}_p) = p^r + O(d^2 p^{r-1/2}) + O_{\mathbf{w},d,r}\left(p^{r-1}\right)$, hence

$$n_p = p^r + O(d^2 p^{r-1/2}) + O_{\mathbf{w},d,r}\left(p^{r-1}\right).$$

More specifically, the implied constant is at most d^2 by the argument in [74]. Note that for all real numbers $\alpha \in \mathbb{R}_{\geq 0}$, we have $\alpha - 1 = (\alpha^{1/r} - 1)(\alpha^{(r-1)/r} + \cdots + 1)$, and so $|\alpha^{1/r} - 1| \leq |\alpha - 1|$. Thus, $n_p^{1/r} = p + O_{\mathbf{w},d,r}(p^{1/2})$. We summarize this as a lemma:

Lemma 4.3.3. *If X_p is geometrically integral, then $n_p^{1/r} = p + O_{\mathbf{w},d,r}(p^{1/2})$.*

We are now ready to complete the proof of Theorem 4.0.1.

4.4 Proof of Theorem 4.0.1: Completion

Let $S = \#X(\mathbb{Q}; \mathbf{B}; \mathfrak{P})$, and let

$$\boldsymbol{\xi}_1, \cdots, \boldsymbol{\xi}_S \in X(\mathbb{Q}; \mathbf{B}, \mathfrak{P})$$

be primitive integral $(r+2)$-tuples representing elements of $X(\mathbb{Q}; \mathbf{B}; \mathfrak{P})$. Let I be the weighted homogeneous ideal generated by F in $\mathbb{Z}[x_0, \cdots, x_{r+1}]$. For a positive integer s, let u be the positive integer such that $\mathcal{H}_I(u-1) < s \leq \mathcal{H}_I(u)$. By (4.1.3), it follows that

$$s = \frac{du^r}{r!w} + O_{\mathbf{w},r}\left(d^{r+2} + d^2 u^{r-1}\right) = \frac{du^r}{r!w}\left(1 + O_{\mathbf{w},r}\left(d^{r+1}u^{-r} + du^{-1}\right)\right),$$

hence

$$\left(\frac{w \cdot r!}{d}\right)^{1/r} s^{1/r} = u\left(1 + O_{\mathbf{w},r}(d^{r+1}u^{-r} + du^{-1})\right)^{1/r}.$$

Let $C_8(\mathbf{w}, r)$ be a positive number that represents the coefficient in front of the big-O term above. We now choose our s so that

$$u > 3C_8(\mathbf{w}, r)(d + d^{r+1}). \tag{4.4.1}$$

Then

$$C_8(\mathbf{w}, r)(d^{r+1}u^{-r} + du^{-1}) < \frac{2}{3},$$

thus by the binomial theorem, we have

$$\left(\frac{w \cdot r!}{d}\right)^{1/r} s^{1/r} = u + O_{\mathbf{w},r}\left(d^{r+1}u^{-r+1} + d\right), \tag{4.4.2}$$

which then becomes

$$\left(\frac{w \cdot r!}{d}\right)^{1/r} s^{1/r} = u + O_{\mathbf{w},r}(d) \tag{4.4.3}$$

by (4.4.1). Rearranging, we obtain

$$u = \left(\frac{w \cdot r!}{d}\right)^{\frac{1}{r}} s^{\frac{1}{r}} + O_{\mathbf{w},r}\left(d\right). \tag{4.4.4}$$

Observe that

$$\mathcal{H}_I(u) - \mathcal{H}_I(u-1) = \frac{d(u^r - (u-1)^r)}{r!w} + O_{\mathbf{w},r}(d^{r+2} + d^2u^{r-1}) = O_{\mathbf{w},r}(d^{r+2} + d^2u^{r-1}),$$

hence by our choice of u with respect to s, we have

$$\mathcal{H}_I(u) - s = O_{\mathbf{w},r}\left(d^{r+2} + d^2u^{r-1}\right).$$

Therefore,

(4.4.5)

$$\begin{aligned} u\mathcal{H}_I(u) &= \left(\left(\frac{w \cdot r!}{d}\right)^{1/r} s^{1/r} + O_{\mathbf{w},r}(d)\right)\left(s + O_{\mathbf{w},r}(d^{r+2} + d^2u^{r-1})\right) \\ &= \left(\frac{w \cdot r!}{d}\right)^{1/r} s^{1+\frac{1}{r}} + O_{\mathbf{w},r}\left(ds\right). \end{aligned}$$

Let $M_1, M_2, \cdots, M_s$ be distinct monomials of weighted degree u which are not leading monomials of any element in $I = \langle F \rangle$. These monomials are linearly independent over $\mathbb{Q}$, and any $\mathbb{Q}$-linear combination of them is not a multiple of F.

Set

$$\mathfrak{M} = (M_j(\boldsymbol{\xi}_l))_{\substack{1 \le j \le s \\ 1 \le l \le S}}.$$

If $S < s$, then $\mathfrak{M}$ has rank at most $s-1$. Hence, $\mathfrak{M}$ has a non-trivial kernel, so there exists a vector $\mathbf{g} \in \mathbb{Z}^s$ such that

$$\mathfrak{M}\mathbf{g} = \mathbf{0}.$$

Such a $\mathbf{g}$ gives rise to a form G such that for all $\mathbf{x} \in X(\mathbb{Q}; \mathbf{B}; \mathfrak{P})$, we have $G(\mathbf{x}) = 0$. Thus G defines a hypersurface Y such that $X(\mathbb{Q}; \mathbf{B}; \mathfrak{P}) \subset Y$ and $\deg Y = u$.

We now assume that $S \geq s$. If we can prove that for any $s \times s$ minor $\mathcal{M}$ of $\mathfrak{M}$ has determinant equal to 0, then $\mathfrak{M}$ has rank at most $s-1$. This is the goal we devote the rest of this section to. We choose, as we may, $\mathcal{M}$ to be the $s \times s$ minor of $\mathfrak{M}$ composed of the first s rows, and consider

$$\Delta = \det \mathcal{M}.$$

We estimate Δ from above as follows:

$$|\Delta| \leq s! B_0^{\sigma_{I,0}(u)} \cdots B_{r+1}^{\sigma_{I,r+1}(u)},$$

where the $\sigma_{I,j}(u)$'s are as in equation (4.1.1). By Proposition 4.1.4, this is equivalent to

$$|\Delta| \leq s! \left(B_0^{a_{I,0}} \cdots B_{r+1}^{a_{I,r+1}}\right)^{u\mathcal{H}_I(u)} V^{O_{\mathbf{w},r}(d^{r+2}+d^2u^r)}.$$

Taking logarithms and recalling (4.0.2), this bound becomes

$$\log|\Delta| \leq u\mathcal{H}_I(u) \log(B_0^{a_{I,0}} \cdots B_{r+1}^{a_{I,r+1}}) + s\log s + O_{\mathbf{w},r}\left((d^{r+2}+d^2u^r)\log V\right). \tag{4.4.6}$$

We want to express everything in terms of s. By (4.0.2), (4.4.4), and (4.4.5), equation (4.4.6) becomes, for some positive $C_9(\mathbf{w}, r)$,

$$\log|\Delta| \leq (r!)^{1/r} \frac{r}{r+1} s^{1+1/r} \log W + s\log s + C_9(\mathbf{w}, r) ds \log V. \tag{4.4.7}$$

We proceed to prove the first part of the theorem. Let $\varepsilon > 0$ be as in the theorem, and recall the hypothesis

$$WV^{\varepsilon} \leq \mathcal{Q} \leq WV^{2\varepsilon}.$$

Choose s to be

$$s = \left\lceil C_{10}(\mathbf{w}, r) \left(\frac{d(r+1)}{\varepsilon r (r!)^{1/r}} \left(1 + 2\varepsilon + \left(\frac{w}{d}\right)^{1/r}\right)\right)^r \right\rceil + 1, \tag{4.4.8}$$

where $C_{10}(\mathbf{w}, r)$ is a positive number which will be chosen later. For each prime p, write $|\cdot|_p$ for the p-adic valuation on $\mathbb{Q}$, normalized so that $|p|_p = p^{-1}$. For convenience, let us write

$$\mathcal{P} = \{p_1, \cdots, p_t\}$$

and

$$\mathfrak{P} = (P_1, \cdots, P_t),$$

where P_i is a non-singular point on X_{p_i} for each i, $1 \le i \le t$. Theorem 4.2.1 gives that

$$-\log|\Delta|_{p_i} > \frac{(r!)^{1/r} r}{r+1} s^{1+1/r} \log p_i - \kappa'(r) s \log p_i.$$

Observe that

$$-\sum_{i=1}^{t} \log|\Delta|_{p_i} > \frac{(r!)^{1/r} r}{r+1} s^{1+1/r} \log \mathcal{Q} - \kappa'(r) s \log \mathcal{Q}. \tag{4.4.9}$$

By (4.4.7) and (4.4.9), there exists a positive number $C_{11}(\mathbf{w}, r)$ such that

$$\log|\Delta| + \sum_{i=1}^{t} \log|\Delta|_{p_i} \le \frac{r(r!)^{1/r}}{r+1} s^{1+1/r} \log \frac{W}{\mathcal{Q}} + C_{11}(\mathbf{w}, r) ds \log V\mathcal{Q}. \tag{4.4.10}$$

We choose $C_{10}(\mathbf{w}, r)$ to be $C_{11}(\mathbf{w}, r)^r$. Note that by (4.1.4), we have

$$a_{I,j} \frac{r+1}{r} \left(\frac{w}{d}\right)^{1/r} \le \left(\frac{w}{d}\right)^{1/r},$$

for $0 \le j \le r+1$, whence

$$\log W \le \left(\frac{w}{d}\right)^{1/r} \log V.$$

By the assumption that $\mathcal{Q} \ge WV^{\varepsilon}$, the right hand side of (4.4.10) then satisfies

$$\frac{r(r!)^{1/r}}{r+1} s^{1+1/r} \log \frac{W}{\mathcal{Q}} + C_{11}(\mathbf{w}, r) ds \log V\mathcal{Q} \le$$

$$-\varepsilon \frac{r(r!)^{1/r}}{r+1} s^{1+\frac{1}{r}} \log V + C_{11}(\mathbf{w}, r) ds \log V \left(1 + 2\varepsilon + \left(\frac{w}{d}\right)^{1/r}\right),$$

and upon dividing the right hand side by $s \log V$ we have

$$-\varepsilon \frac{r(r!)^{1/r}}{r+1} s^{\frac{1}{r}} + C_{11}(\mathbf{w}, r) d \left(1 + 2\varepsilon + \left(\frac{w}{d}\right)^{1/r}\right). \tag{4.4.11}$$

If (4.4.8) is satisfied, then

$$\varepsilon \frac{r(r!)^{1/r}}{r+1} s^{\frac{1}{r}} > C_{11}(\mathbf{w}, r) d \left(1 + 2\varepsilon + \left(\frac{w}{d}\right)^{1/r}\right),$$

whence (4.4.11) is negative. Therefore, we obtain

$$\log|\Delta| + \sum_{i=1}^{t} \log|\Delta|_{p_i} < 0. \tag{4.4.12}$$

Hence, for $WV^{\varepsilon} \le \mathcal{Q} \le WV^{2\varepsilon}$ and s satisfying (4.4.8), we have

$$\Delta = 0.$$

This implies that $X(\mathbb{Q}; \mathbf{B}, \mathfrak{P})$ is contained in a hypersurface $Y(P_1, \cdots, P_t)$ satisfying

$$\deg Y = O_{d,\mathbf{w},r}\left(s^{1/r}\right) = O_{d,\mathbf{w},r,\varepsilon}(1),$$

defined by a primitive form G. To estimate the height of G, we argue as in Lemma 4.2.6. Let $s' \le s-1$ denote the rank of $(M_j(\boldsymbol{\xi}_l))$. Then, from evaluating all $(s'+1)\times(s'+1)$ sub-determinants by expanding along a row, we see that the height of G is at most

$$\max|\det \mathcal{M}|$$

where the maximum is taken over all $s' \times s'$ minors of $(M_j(\boldsymbol{\xi}_l))$. This can be bounded just as in (4.4.7), so by (4.4.8) and (4.2.2), we obtain

$$\log\|G\| = O_{d,\mathbf{w},r,\varepsilon}\left(\log V\mathcal{Q}\right).$$

Further, since the monomials which appear in G with a non-zero coefficient are not leading monomials of I, F cannot divide G; and thus, X cannot be contained in $Y(\mathfrak{P})$. This completes the proof of the first part of Theorem 4.0.1.

For the second part, suppose that X is geometrically integral. Set

$$s = \left\lceil \max\left\{ \mathcal{Q}^{-r}W^r(1+\log V\mathcal{Q})^{C_{12}(\mathbf{w},d,r)}, (\log \mathcal{Q}V)^r \right\} \right\rceil + 1, \tag{4.4.13}$$

where $C_{12}(\mathbf{w}, d, r)$ is a number which depends on d, $\mathbf{w}$, and r, and will be specified later; see (4.4.17). By (4.4.13), it follows that

$$u = O_{\mathbf{w},d,r}\left((\mathcal{Q}^{-1}W+1)\log V\mathcal{Q}\right). \tag{4.4.14}$$

We now consider the two cases given by Lemma 4.2.6. If case (a) holds, we can produce a hypersurface Y of degree d, distinct from X, which contains $X(\mathbb{Q}; \mathbf{B}, \mathfrak{P})$. This is sufficient for the theorem. Thus, it remains to treat the case when $\pi_X = O_{\mathbf{w},d,r}(1+\log V)$. In this case, we have will have two separate divisors of Δ to estimate; one coming from the prime

factors of $\mathcal{Q}$, and one coming from primes which do not divide $\mathcal{Q}\pi_X$.

We now estimate the contribution coming from primes which are co-prime to $\mathcal{Q}\pi_X$. For each prime p such that X_p is geometrically integral, by Lemma 4.3.1 we have

$$-\log|\Delta|_p \geq \frac{(r!)^{1/r}r}{r+1}s^{1+1/r}\frac{\log p}{n_p^{1/r}} - \kappa(d,r)s\log p.$$

We write the sum over the primes p for which $p \nmid \mathcal{Q}\pi_X, p \leq s^{1/r}$ as $\sum_{p\leq s^{1/r}}^{*}$. By Lemma 4.2.6, we have

$$\sum_{p|\mathcal{Q}\pi_X}\frac{\log p}{p} = \log(1+\log V\mathcal{Q}) + O_{\mathbf{w},d,r}(1). \tag{4.4.15}$$

Then, by applying Lemma 4.3.3 and the prime number theorem, we have, for some positive numbers $C_{13}(\mathbf{w},d,r), C_{14}(\mathbf{w},d,r)$,

$$\begin{aligned}
-\sum_{p\leq s^{1/r}}^{*}\log|\Delta|_p &\geq \frac{(r!)^{1/r}r}{r+1}s^{1+1/r}\sum_{p\leq s^{1/r}}^{*}\frac{\log p}{n_p^{1/r}} - \kappa(d,r)s\sum_{p\leq s^{1/r}}\log p \\
&\geq \frac{(r!)^{1/r}r}{r+1}s^{1+1/r}\sum_{p\leq s^{1/r}}^{*}\frac{\log p}{p} - C_{13}(\mathbf{w},d,r)s^{1+1/r} \\
&\geq \frac{(r!)^{1/r}}{r+1}s^{1+1/r}\left(\log s - r\sum_{p|\mathcal{Q}\pi_X}\frac{\log p}{p}\right) - C_{14}(\mathbf{w},d,r)s^{1+1/r} \\
&\geq \frac{(r!)^{1/r}}{r+1}s^{1+1/r}\left(\log s - O_{\mathbf{w},d,r}(\log(1+\log V\mathcal{Q}))\right) - C_{14}(\mathbf{w},d,r)s^{1+1/r}.
\end{aligned}$$

We invoke the bound from equation (4.4.7) and obtain the inequality

$$\log|\Delta| + \sum_{i=1}^{t}\log|\Delta|_{p_i} + \sum_{p\leq s^{1/r}}^{*}\log|\Delta|_p \tag{4.4.16}$$

$$\leq \frac{(r!)^{1/r}}{r+1}s^{1+1/r}\log\left[\frac{W^r}{\mathcal{Q}^r s}\right] + C_{15}(\mathbf{w},d,r)\left(s^{1+1/r}(\log(1+\log V\mathcal{Q})) + s\log V\mathcal{Q}\right),$$

where $C_{15}(\mathbf{w},d,r)$ is a positive number which depends on d and r. Note that

$$\log V\mathcal{Q} \ll_{\mathbf{w},d,r} s^{1/r}$$

by (4.4.13). We may thus choose a positive number $C_{12}(\mathbf{w}, d, r)$ such that

$$C_{15}(\mathbf{w}, d, r)\left(s^{1+1/r} + s\log V\mathcal{Q}\right) < \frac{(r!)^{1/r}}{r+1}s^{1+1/r}\mathcal{C}_{12}(\mathbf{w}, d, r)\log(1+\log V\mathcal{Q}). \tag{4.4.17}$$

Then, equation (4.4.16) becomes

$$\log|\Delta| + \sum_{i=1}^{t}\log|\Delta|_{p_i} + \sum_{p\leq s^{1/r}}^{*}\log|\Delta|_p \leq \frac{(r!)^{1/r}}{r+1}s^{1+1/r}\log\left[\frac{(1+\log V\mathcal{Q})^{C_{12}(\mathbf{w},d,r)}W^r}{\mathcal{Q}^r s}\right]. \tag{4.4.18}$$

Hence,

$$\Delta = 0 \tag{4.4.19}$$

whenever

$$s > \max\left\{\mathcal{Q}^{-r}W^r(1+\log V\mathcal{Q})^{C_{12}(\mathbf{w},d,r)}, (\log V\mathcal{Q})^r\right\}.$$

By our choice of s and $C_{12}(\mathbf{w}, d, r)$, this is satisfied.

When s is of this size, any set of s $(r+2)$-tuples $\boldsymbol{\xi}_1, \cdots, \boldsymbol{\xi}_s \in X(\mathbb{Q}; \mathbf{B}; P_1, \cdots, P_t)$ satisfies

$$\Delta = 0,$$

so $(M_j(\boldsymbol{\xi}_l))$ has rank less than s. This implies that $(M_j(\boldsymbol{\xi}_l))$ has a non-trivial kernel, whence we may find an auxiliary form G of degree u defining a hypersurface $Y(P_1, \cdots, P_t)$ such that

$$X(\mathbb{Q}; \mathbf{B}, P_1, \cdots, P_t) \subset Y(P_1, \cdots, P_t).$$

Further, since the monomials which appear in G with non-zero coefficient are not leading monomials of I, it follows that F cannot divide G. Since X is geometrically integral, the hypersurface $Y(P_1, \cdots, P_t)$ satisfies the conditions of the theorem. This completes the proof of Theorem 4.0.1.

4.5 Salberger's Improvement to the Determinant Method

In this section we will establish an improved version of the determinant method for weighted projective spaces. The main input is an improvement to the exponent of prime powers which one can prove divides a certain determinant. This idea is due to Salberger; see [94]. Let us write, for a prime p,

$$\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbb{Q} : \gcd(a, b) = 1, p \nmid b\right\}.$$

We will need the following result, which is the same as Lemma 2.1 in [94]:

Lemma 4.5.1. *Let R be be a commutative noetherian regular local ring containing $\mathbb{Z}_{(p)}$ as a subring. Let $\varphi_1, \cdots, \varphi_s$ be ring homomorphisms from R to $\mathbb{Z}_{(p)}$ and $I = \ker \varphi_1$. Write $A = R_I$ for the localization of R at the prime ideal I, and let $\mathfrak{m} = IA$ be the maximal ideal of A. Let $r_1, \cdots, r_s$ be elements of R and write $\mathcal{W} \subset A$ for the $\mathbb{Q}$-vector space generated by $r_1, \cdots, r_s$. Write*

$$\nu = \sum_{k \geq 1} \dim_{\mathbb{Q}}(\mathcal{W} \cap \mathfrak{m}^k).$$

Then the determinant of the $s \times s$ matrix $(\varphi_i(r_j))$ is divisible by p^ν.

In the context of the p-adic determinant method, R will be the stalk of the structure sheaf of a non-singular point $\mathbf{x}$ on X, and $r_1, \cdots, r_s$ will be elements in a collection of monomials of the same (weighted) degree u. The key to Salberger's improvement is that some times it is possible to consider a collection of monomials $m_1, \cdots, m_s$ of degree *less* than u and by multiplying these by a linear form defining a tangent plane at P, obtain forms of degree u which vanish to high order at P. In the weighted projective setting, it is not always possible to find such a linear form, due to the differences in weights of the variables. However, it is still possible to find a form of low weighted degree (with respect to the weight vector $\mathbf{w}$) which vanishes to higher order than expected. We state this formally as follows.

Definition 4.5.2. Let $\mathbf{w} = (1, 1, w_2, \cdots, w_{n+1})$ be a vector of positive integers, and write $w = w_2 \cdots w_{n+1}$. We say that a positive integer γ is a *trading degree* of $\mathbb{P}(\mathbf{w})$ if the number of monomials of weighted degree γ exceed $\binom{n+\gamma}{n}$. We will refer to *the* trading degree as the smallest positive integer with this property. If no such integer exists, we write $\gamma = +\infty$.

If the trading degree is finite, define the *traditing ratio* to be

$$\lambda = \frac{\gamma + 1}{\gamma}.$$

Fortunately, the trading degree is always finite for weighted projective spaces.

Lemma 4.5.3. *Let $\mathbb{P}(\mathbf{w})$ be as in Definition 4.5.2. Then $\gamma < \infty$.*

Proof. It is known that the Hilbert function of $\mathbb{P}(\mathbf{w})$ satisfies

$$\mathcal{H}_{\mathbb{P}(\mathbf{w})}(u) = \frac{u^{n+1}}{w(n+1)!} + O_n(u^n);$$

see Dolgachev for example. Meanwhile, we have for a positive integer t

$$\binom{n+t}{n} = \frac{t^n}{n!} + O(t^{n-1}).$$

Thus the desired inequality holds provided that u is taken to be large with respect to w, n. □

If a hypersurface $X \subset \mathbb{P}(\mathbf{w})$ has degree d exceeding the trading ratio $\gamma(\mathbf{w})$, then the monomials of weighted degree γ will be $\mathbb{Q}$-linearly independent over X. In particular, $\mathcal{H}_X(\gamma)$ is equal to the number of all monomials of weighted degree γ. Thus, for any non-singular point P on X, we can find a form of weighted degree γ which vanishes to order $\gamma + 1$ at P. We make use of this fact in the following lemma, which is a generalization of Salberger's work in [94].

Lemma 4.5.4. *Let $\mathbf{w} = (1, 1, w_2, \cdots, w_{n+1})$ with $w = w_2 \cdots w_{n+2}$ be a vector of positive integers. Let X be an integral hypersurface in $\mathbb{P}(\mathbf{w})$ defined by the primitive form $\mathcal{F}$, and for a positive integer u, write $s = \mathcal{H}_X(u)$ and consider monomials $M_1, \cdots, M_s$ which are $\mathbb{Q}$-linearly independent over X. Let p be a prime, and let P be an $\mathbb{F}_p$-point on X_p. Consider a set of s of primitive $(n+2)$-tuples*

$$\boldsymbol{\xi}_i = (\xi_{i,0}, \cdots, \xi_{i,n+1}) \in \mathbb{Z}^{n+2}$$

which reduce to P modulo p. Write

$$\mathfrak{S}(d, n, \mathbf{w}) = \left(\frac{w}{d}\right)^{1/n} \left(\left(\frac{d}{\lambda w}\right)^{1/(n-1)} (n-1) + \lambda \right).$$

Then the determinant of the $s \times s$ matrix $(M_j(\boldsymbol{\xi}_i))$ is divisible by p^N, where for some positive number $C_1(n)$ depending at most on n, N satisfies

$$N \geq \mathfrak{S}(d, n, \mathbf{w}) \frac{(n!)^{1/n}}{n+1} s^{1+\frac{1}{n}} - C_1(n)s.$$

Proof. By Proposition 2.4 in [105], we have

$$s = \mathcal{H}_X(u) = \frac{du^n}{n!w} + O_n\left(d^n + d^2u^{n-1}\right).$$

Since $\gcd(x_0, x_1, x_2, \cdots, x_n, x_n) = 1$, we may assume without loss of generality that $x_0(P) \not\equiv 0 \pmod{p}$. Therefore, if we replace the $M_1, \cdots, M_s$ with

$$M_j(1, x_1/x_0, \cdots, x_n/x_0^{w_n}, x_{n+1}/x_0^{w_{n+1}}), j = 1, \cdots, s$$

without changing the p-adic valuation of $\det(M_j(\boldsymbol{\xi}_i))$. Thus, it suffices to deal with the affine variety Y defined by the equation

$$\mathcal{F}(1, x_1/x_0, \cdots, x_n/x_0^{w_n}, x_{n+1}/x_0^{w_{n+1}}) = 0.$$

Let P' be the point on X_1 corresponding to P, and let R be the stalk of the structure sheaf of Y at P'. Then it follows that $M_j/x_0^u \in R$ for $j = 1, \cdots, s$. Let $\varphi_i : R \to \mathbb{Z}_{(p)}$, $1 \le i \le s$ be the local ring homomorphisms at P' induced by evaluation maps by $\boldsymbol{\xi}_i$ for $1 \le i \le s$. Let $I = \ker \varphi_1$. Then $A = R_I$ is the stalk of the structure sheaf of Y at the non-singular rational point $\mathbf{x}$ defined by $\boldsymbol{\xi}_1$. It is thus an n-dimensional regular local ring with $\mathfrak{m} = IA$ as the maximal ideal and

$$\dim_{\mathbb{Q}}(A/\mathfrak{m}^k) = \binom{n+k}{k} = \frac{k^n}{n!} + O\left(k^{n-1}\right),$$

where the constant in the big-O term is absolute. Let $\mathcal{W}$ be the $\mathbb{Q}$-subspace of A generated by $r_1, \cdots, r_s$. Then $\dim_{\mathbb{Q}}(\mathcal{W}) = s$ as $M_1, \cdots, M_s$ are linearly independent on X. Further,

$$\dim_{\mathbb{Q}}(\mathcal{W}/\mathcal{W} \cap \mathfrak{m}^k)) \le \dim_{\mathbb{Q}}(A/\mathfrak{m}^k).$$

Hence, it follows that

$$\dim_{\mathbb{Q}}(\mathcal{W} \cap \mathfrak{m}^k) = \dim_{\mathbb{Q}}(\mathcal{W}) - \dim_{\mathbb{Q}}(\mathcal{W}/(\mathcal{W} \cap \mathfrak{m}^k)) \ge s - \binom{n+k}{k}. \tag{4.5.1}$$

We now set

$$g(d, n, \mathbf{w}) = (d/\lambda w)^{1/(n-1)}. \tag{4.5.2}$$

shall use (4.5.1) for the range $1 \le k \le g(d, n, \mathbf{w})u$ and establish a different estimate for the range $g(d, n, m)u < k \le \lambda u$. Indeed, if we use (4.5.1) for the full range of k, we would recover Theorem 4.2.1.

Let us write

$$\alpha = \frac{1}{\lambda - g(d, n, \mathbf{w})} \text{ and } \beta = \frac{g(d, n, \mathbf{w})}{\lambda - g(d, n, \mathbf{w})}. \tag{4.5.3}$$

Let us write $Q = Q_\alpha(k)$ for the largest non-negative integer lesser than or equal to $\alpha(\lambda u - k)$ such that $u - Q$ is a non-negative multiple of γ. Our goal is to use $\mathcal{H}_X(Q)$ weighted forms of degree Q to construct a family of $\mathcal{H}_X(Q)$ degree u forms which lie in $\mathfrak{m}^k$. Let us write

$$t_\alpha(k) = \frac{u - Q}{\gamma},$$

and $v(k) = k - (\gamma+1)t_\alpha(k)$. Observe that $t_\alpha(k), v(k) \in \mathbb{N} \cup \{0\}$. Further, note that $t_\alpha(k)$ satisfies

$$\frac{\alpha k - (\lambda\alpha - 1)u}{\gamma} - 1 < t_\alpha(k) \leq \frac{\alpha k - (\lambda\alpha - 1)u}{\gamma}.$$

Likewise, we have

$$\beta(\lambda u - k) - \gamma < v(k) \leq \beta(\lambda u - k).$$

Suppose we are given $\mathcal{G}_1, \cdots, \mathcal{G}_{\mathcal{H}_X(Q)}$ forms of weighted degree Q which are $\mathbb{Q}$-linearly independent over X. Let $\mathcal{W}_0$ be the $\mathbb{Q}$-subspace of A generated by $\mathcal{G}_j/x_0^Q$ for $1 \leq j \leq \mathcal{H}_X(Q)$. Then, we have

$$\dim_{\mathbb{Q}}(\mathcal{W}_0 \cap \mathfrak{m}^{v(k)}) \geq \dim_{\mathbb{Q}}(\mathcal{W}_0) - \dim_{\mathbb{Q}}(A/\mathfrak{m}^{v(k)})$$

and for some number $C_2(n, \mathbf{w})$ which depends only on n and $\mathbf{w}$, we have

$$\begin{aligned}\dim_{\mathbb{Q}}(\mathcal{W}_0 \cap \mathfrak{m}^{v(k)}) &\geq \left(\frac{dQ^n}{wn!} - \frac{v(k)^n}{n!}\right) - C_2(n, \mathbf{w})k^{n-1} \\ &= \left(\frac{d\alpha^n}{w} - \beta^n\right)\frac{(\lambda u - k)^n}{n!} - C_2(n, \mathbf{w})k^{n-1} \\ &= U(k).\end{aligned}$$

Hence, there are linearly independent $\mathbb{Q}$-linear combinations $G_1, \cdots, G_{\lceil U(k)\rceil}$ of the forms $\mathcal{G}_1, \cdots, \mathcal{G}_{\mathcal{H}_X(Q)}$ such that $G_j/x_0^Q \in \mathcal{W}_0 \cap \mathfrak{m}^{v(k)}$. Now, consider the monomials $\mathcal{H}_X(\gamma)$ monomials of weighted degree γ, which are $\mathbb{Q}$-linearly independent over X. By our definition of γ, λ, it follows that there exists a weighted form of degree γ such that $L/x_0^\gamma \in \mathfrak{m}^{\gamma+1}$. Now consider the forms $L^{t_\alpha(k)}G_j$. Since $G_j/x_0^Q \in \mathfrak{m}^{v(k)}$, it follows that

$$(L/x_0^\gamma)^{t_\alpha(k)})(G_j/x_0^Q) \in \mathfrak{m}^{v(k)+(\gamma+1)t_\alpha(k)} = \mathfrak{m}^k.$$

Let $\Phi_1, \cdots, \Phi_{\lceil U(k)\rceil}$ be linear combinations of $M_1, \cdots, M_s$ such that $\Phi_j - L^{t_\alpha(k)}G_j$ vanishes on X. Then $\Phi_1/x_0^u, \cdots, \Phi_{\lceil U(k)\rceil}/x_0^u$ are $\mathbb{Q}$-linearly independent elements of $\mathcal{W} \cap \mathfrak{m}^k$, whence

$$\dim_{\mathbb{Q}}(\mathcal{W} \cap \mathfrak{m}^k) \geq U(k) \tag{4.5.4}$$

for $k \in (g(d, n, \mathbf{w})u, \lambda u]$.

It remains to give an estimate for ν. For $1 \leq k \leq g(d, n, \mathbf{w})u$, we use (4.5.1). We

can approximate (4.5.1) with an integral, and see that for some positive numbers κ, κ' depending at most on n, that

$$\begin{aligned}\sum_{k=1}^{g(d,n,\mathbf{w})u} \dim_{\mathbb{Q}}(\mathcal{W} \cap \mathfrak{m}^k) &\geq \int_0^{g(d,n,\mathbf{w})u} \left(s - \frac{x^n}{n!}\right) dx - \kappa u^n \\ &\geq g(d,n,\mathbf{w}) \frac{du^{n+1}}{wn!} - \frac{(g(d,n,\mathbf{w})u)^{n+1}}{(n+1)!} - \kappa' u^n \\ &= \frac{dg(d,n,\mathbf{w})u^{n+1}}{wn!}\left(1 - \frac{g(d,n,\mathbf{w})}{\lambda(n+1)}\right) - \kappa' u^n.\end{aligned}$$

For the range $g(d,n,m) < k \leq \lambda u$, we have the estimate, for some non-negative κ'',

$$\begin{aligned}\sum_{g(d,n,\mathbf{w})u < k \leq \lambda u} \dim_{\mathbb{Q}}(\mathcal{W} \cap \mathfrak{m}^k) &\geq \frac{1}{n!}\left(\frac{d\alpha^n}{w} - \beta^n\right) \int_{g(d,n,\mathbf{w})u}^{\lambda u} (\lambda u - x)^n dx - \kappa'' u^n \\ &\geq \frac{d(\lambda - g(d,n,\mathbf{w}))^{n+1}}{w\lambda(\lambda - g(d,n,\mathbf{w}))^{n-1}(n+1)!} u^{n+1} - \kappa'' u^n \\ &= \frac{d(\lambda - g(d,n,\mathbf{w}))^2 u^{n+1}}{\lambda w(n+1)!} - \kappa'' u^n.\end{aligned}$$

Combining these estimates, we obtain

$$\begin{aligned}\sum_{k \geq 1} \dim_{\mathbb{Q}}(\mathcal{W} \cap \mathfrak{m}^k) &\geq \frac{du^{n+1}}{w(n+1)!}\left(g(d,n,\mathbf{w})(n-1) + \lambda\right) - C_1 u^n \\ &= \mathfrak{S}(d,n,\mathbf{w}) \frac{(n!)^{1/n}}{n+1} s^{1+1/n} - C_1 s.\end{aligned}$$

□

We now give a proof of Theorem 4.0.2.

Proof. (Theorem 4.0.2 Much of the proof follows from the proof of Theorem 4.0.1, with the exception that Theorem 4.2.1 has been replaced with Lemma 4.5.4. We write $|\cdot|_p$ for the p-adic valuation on $\mathbb{Q}$, normalized so that $|p|_p = p^{-1}$. We write the analogous equations to (6.6) in [105]:

$$\log|\Delta| \leq (n!)^{1/n} \frac{n}{n+1} s^{1+\frac{1}{n}} \log W + s \log s + C_2(n) ds \log V, \tag{4.5.5}$$

and observe that Lemma 4.5.4 implies

$$-\sum_{i=1}^{t}\log|\Delta|_{p_i} \geq \mathfrak{S}(d,n,\mathbf{w})\frac{(n!)^{1/n}}{n+1}s^{1+1/n}\log\mathcal{Q} - C_3(n)s\log\mathcal{Q}, \tag{4.5.6}$$

By our hypothesis, (4.5.6) satisfies (upon adjusting the value of ε if necessary)

$$-\sum_{i=1}^{t}\log|\Delta|_{p_i} \geq \mathfrak{S}(d,n,\mathbf{w})\frac{(n!)^{1/n}}{n+1}s^{1+\frac{1}{n}}\log\left(W^{n/\mathfrak{S}(d,n,\mathbf{w})}V^{\varepsilon}\right) - C_3(n)s\log V^{\varepsilon}W^{n/\mathfrak{S}(d,n,\mathbf{w})} \tag{4.5.7}$$

Therefore, in order for $\Delta = 0$ it suffices to insist that

$$\frac{n(n!)^{1/n}}{n+1}s^{1+\frac{1}{n}}\varepsilon\log V > s\log s + C_2(n)ds\log V + C_3(n)s\log V^{\varepsilon}W^{n/\mathfrak{S}(d,n,\mathbf{w})}. \tag{4.5.8}$$

By first choosing s to be large with respect to $C_2(n)d$ and ε, we see that the left hand side of (4.5.8) can be made to be arbitrarily large compared to the second and third terms on the right hand side. If s depends at most on n, d, ε, then the first term on the right hand side will be negligible when V is made to be large. Recall that

$$s = \mathcal{H}_X(u).$$

This shows that the degree u of our auxiliary polynomial can be bounded in terms of d, n, ε only. □

We will follow Salberger's approach in [94] instead of his approach in [93] (which was the method utilized in [105]). It seems that the argument in [94] avoids the issue of $\mathbb{F}_p$-points which have higher multiplicity more efficiently, but at the cost that the final estimate gains an exponent of ε instead of a power of a logarithm. Salberger called this version of the determinant method the *semi-global determinant method*. We will establish the following theorem:

Theorem 4.5.5. *Let $X \subset \mathbb{P}(\mathbf{w})$ be an integral hypersurface of degree $2 \leq d < 2^n w$. Let $\mathbf{B} = (B_0, \cdots, B_n, B_{n+1}) \in \mathbb{R}^{n+2}$ be a vector of positive numbers. Suppose that X is the only hypersurface containing $X(\mathbb{Q}; \mathbf{B})$. Then for each $\varepsilon > 0$ there exists a set $\Omega(\varepsilon, \mathbf{B})$ of primes, depending on ε and $\mathbf{B}$, and a set of surfaces*

$$Y(\mathbf{B}, P_1, \cdots, P_t)$$

indexed by t-tuples $(P_1, \cdots, P_t)$ of non-singular $\mathbb{F}_{p_i}$-points P_i on X_{p_i} for primes $p_1, \cdots, p_t \in \Omega(\varepsilon, \mathbf{B})$ with

$$\mathcal{Q}_t = p_1 \cdots p_t \geq 2W^{n/\mathfrak{S}(d,n,\mathbf{w})}V^{\varepsilon}$$

such that the following hold:

(a) There exists a number $C_4(\varepsilon)$ which depends only on ε such that whenever $p \in \Omega(\varepsilon, \mathbf{B})$, we have

$$V^{\varepsilon} < p \leq C_4(\varepsilon) V^{\varepsilon}.$$

(b) $\#\Omega(\varepsilon, \mathbf{B})$ depends only on ε.

(c) We have

$$X(\mathbb{Q}; \mathbf{B}, P_1, \cdots, P_t) \subset Y(\mathbb{Q}; \mathbf{B}, P_1, \cdots, P_t)$$

for each t-tuple $(P_1, \cdots, P_t)$ as above, and each hypersurface $Y(\mathbf{B}, P_1, \cdots, P_t)$ has the same degree $D(\varepsilon)$ which only depends on ε.

(d) For each non-singular $\mathbf{x} \in X(\mathbb{Q}; \mathbf{B})$, we have one of the following alternatives:

1. *There exist primes $p_0 < \cdots < p_t$ in $\Omega(\varepsilon, \mathbf{B})$ with*

$$p_0 \cdots p_t = O_{\varepsilon}\left(W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{3\varepsilon}\right)$$

and

$$p_0 \cdots p_{t_1} \geq W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{\varepsilon}$$

such that $\mathbf{x}$ specializes to a non-singular $\mathbb{F}_{p_i}$-point P_i on X_{p_i} for $i = 0, \cdots, t$ and where $\mathbf{x}$ lies on a component of $X \cap Y(\mathbf{B}, P_0, \cdots, P_{t-1})$ not contained in $X \cap Y(\mathbf{B}, P_0, \cdots, P_t)$.

2. *There exist primes $p_0 < \cdots < p_t$ in $\Omega(\varepsilon, \mathbf{B})$ with*

$$p_0 \cdots p_t = O_{\varepsilon}\left(W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{2\varepsilon}\right)$$

such that $\mathbf{x}$ specializes to a non-singular $\mathbb{F}_{p_i}$-point on X_{p_i} for $0 \leq i \leq t$ and that there exists $i \in \{0, \cdots, t\}$ with

$$p_0 \cdots p_{i-1} p_{i+1} \cdots p_t \geq W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{\varepsilon},$$

we have $\mathbf{x}$ lies on a component of $X \cap Y(\mathbf{B}, P_0, \cdots, P_t)$ not contained in

$$Y(\mathbf{B}, P_0, \cdots, P_{i-1}, P_{i+1}, \cdots, P_t).$$

3. *There are primes $p_1 < \cdots < p_t$ in $\Omega(\varepsilon, \mathbf{B})$ with*

$$W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{\varepsilon} \leq p_1 \cdots p_t = O_{\varepsilon}\left(W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{2\varepsilon}\right)$$

such that $\mathbf{x}$ to a non-singular $\mathbb{F}_{p_i}$-point on P_i on X for $1 \leq i \leq t$ and a component Z of $X \cap Y(\mathbf{B}, P_1, \cdots, P_t)$ containing $\mathbf{x}$ where $Z(\mathbb{Q}; \mathbf{B})$ such that either $\mathbf{x}$ is singular on Z or $\mathbf{x}$ specializes to a non-singular $\mathbb{F}_{p_i}$-point P_i on Z_{p_i} for each $1 \leq i \leq t$.

Proof. Consider a set of primes $p_1, \cdots, p_t$ such that

$$p_1 \cdots p_t \geq W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{\varepsilon}$$

and for each set of non-singular points $P_i \in X_{p_i}, 1 \leq i \leq t$, choose a hypersurface $Y(\mathbf{B}, P_1, \cdots, P_t)$ not containing X as in Theorem 5.1.2. Then all $Y(\mathbf{B}, P_1, \cdots, P_t)$ have the same degree, say $D(\varepsilon)$. By the theorem of Bezout, the components Z of $X \cap Y(\mathbf{B}, P_1, \cdots, P_t)$ have degree at most dD.

For a non-singular point $\mathbf{x} \in Z$, let us write $\pi_{\mathbf{x}}$ for the product of all primes such that $\mathbf{x}$ reduces to a singular point on Z. By the same argument as Lemma 4.7 in [**?**], except replacing the universal polynomial with a partial derivative which does not vanish at $\mathbf{x}$, we see that either $Z(\mathbb{Q}; \mathbf{B})$ is contained in a hypersurface Y' which does not contain Z as a subvariety or

$$\pi_{\mathbf{x}} = O_{d,n,\varepsilon}(1 + \log V);$$

and in particular, the bound is uniform for non-singular points on $Z(\mathbb{Q}; \mathbf{B})$. Let Ł be a constant which depends only on d, n, ε such that

$$\pi_{\mathbf{x}} \leq V^{L}$$

for all non-singular $\mathbf{x} \in Z(\mathbb{Q}; \mathbf{B})$. If we apply the same analysis to X, we can likewise obtain a constant $\mathcal{K}$ which depends only on d, n such that

$$\pi_{\mathbf{x}} \leq V^{\mathcal{K}}$$

for all non-singular $\mathbf{x}$ in $X(\mathbb{Q}; \mathbf{B})$. Now let m be the smallest positive integer such that

$$p_1 \cdots p_t \geq V^{\mathcal{K}+L} W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{\varepsilon}$$

and $V^{\varepsilon} \leq p_1 < \cdots < p_t$. Let

$$\Omega = \Omega(\varepsilon, \mathbf{B}) = \{p_1, \cdots, p_m\}.$$

Observe that

$$p_1 \cdots p_{m-1} < V^{\mathcal{K}+L} W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{\varepsilon} \leq V^{\mathcal{K}+L+n/\mathfrak{S}(d,n,\mathbf{w})+\varepsilon}$$

by the minimality of m. Since we had imposed $p \geq V^{\varepsilon}$ for all $p \in \Omega$, it follows that

$$V^{(m-2)\varepsilon} < V^{\mathcal{K}+L+n/\mathfrak{S}(d,n,\mathbf{w})},$$

whence

$$\#\Omega = m < 2 + \frac{\mathcal{K} + L + n/\mathfrak{S}(d, n, \mathbf{w})}{\varepsilon}.$$

We can also approximate the size of primes in Ω crudely via Bertrand's postulate; the refinements on the maximize of prime gaps are not necessary for our application. We therefore obtain

$$p \leq 2^m V^{\varepsilon} = O_{\varepsilon}(V^{\varepsilon})$$

for $p \in \Omega$. We have thusly justified items (a) to (c).

To prove (d), let $\mathbf{x}$ be a non-singular point in $X(\mathbb{Q}; \mathbf{B})$ and $\Omega(\mathbf{x}) \subset \Omega$ be the subset consisting of primes p such that $\mathbf{x}$ specializes to a non-singular $\mathbb{F}_p$-point on X_p. We shall also write, for square-free products

$$q_t = p_1 \cdots p_t \geq W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{\varepsilon}$$

of primes in $\Omega(\mathbf{x})$,

$$Y(\mathbf{x}, q_t) = Y(\mathbf{B}, P_1, \cdots, P_t)$$

where P_i is the specialization of $\mathbf{x}$ in X_{p_i}. By the definition of $\pi_{\mathbf{x}}$ and $\mathcal{K}$, we have

$$\prod_{p \in \Omega(\mathbf{x})} p \geq V^L W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{\varepsilon}. \tag{4.5.9}$$

Now list the primes in $\Omega(\mathbf{x})$ in increasing order and stop as soon as

$$p_1 \cdots p_t \geq W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{\varepsilon}.$$

Then

$$p_1 \cdots p_{t-1} < W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{\varepsilon},$$

with $p_1 \cdots p_{t-1} = 1$ if $t = 1$. Let q_t be the product $p_1 \cdots p_t$ of these primes and Z be a component of $X \cap Y(\mathbf{x}, q_t)$ containing $\mathbf{x}$. Further, let $\Omega(\mathbf{x}; Z)$ be the subset of primes p in $\Omega(\mathbf{x})$ where $\mathbf{x}$ specializes to a non-singular $\mathbb{F}_p$-point on Z_p. By (4.5.9) and the bound $\pi_{\mathbf{x}} \leq V^L$, we obtain the inequality

$$\prod_{p \in \Omega(\mathbf{x}; Z)} p \geq W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{\varepsilon}. \tag{4.5.10}$$

We now define a finite sequence $(\mathcal{Q}_0, \cdots, \mathcal{Q}_m)$ with $q_t = \mathcal{Q}_0$ of square-free integers recursively as follows. If Z is not a component of $X \cap Y(\mathbf{x}, \mathcal{Q}_i)$, we stop. If all prime factors of

of $\mathcal{Q}_i$ are in $\Omega(\mathbf{x}; Z)$ or if all primes in $\Omega(\mathbf{x}; Z)$ divide $\mathcal{Q}_i$, then we also stop. Otherwise, we replace the largest prime factor p of $\mathcal{Q}_i$ by the smallest prime $p' \in \Omega(\mathbf{x}; Z)$ which is not a prime factor of $\mathcal{Q}_i$ and let $\mathcal{Q}_{i+1} = \mathcal{Q}_i p'/p$. Then $\mathcal{Q}_i < \mathcal{Q}_{i+1}$ for all i as the prime factors of $\mathcal{Q}_0$ are smaller than the other primes in $\Omega(\mathbf{x})$. Further, $\mathcal{Q}_{i+1} \le C_4(\varepsilon)\mathcal{Q}_i$ by (a). Since

$$\mathcal{Q}_0 < W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{\varepsilon} p_t \le C_4(\varepsilon) W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{2\varepsilon},$$

we get that

$$\operatorname{lcm}(\mathcal{Q}_{i-1}, \mathcal{Q}_i) < C_4(\varepsilon)^{i+1} W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{3\varepsilon}$$

and

$$\mathcal{Q}_i < C_4(\varepsilon)^{i+1} W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{2\varepsilon}$$

for all $i \ge 1$.

This process will finish after at most $t \le \#\Omega$ steps and produce an integer $\mathcal{Q}_m$ with

$$W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{2\varepsilon} \le \mathcal{Q}_m < C_4(\varepsilon)^{t+1} W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{2\varepsilon}$$

satisfying one of the following alternatives:

(i) $m \ge 1$ and Z is a component of $X \cap Y(\mathbf{x}, \mathcal{Q}_{m-1})$, but not of $X \cap Y(\mathbf{x}, \mathcal{Q}_m)$,

(ii) Z is a component of $X \cap Y(\mathbf{x}, \mathcal{Q}_m)$ and all factors of $\mathcal{Q}_m$ are in $\Omega(\mathbf{x}; Z)$.

(iii) Z is a component of $X \cap Y(\mathbf{x}, \mathcal{Q}_m)$ and $\mathcal{Q}_m$ is divisible by all primes in $\Omega(\mathbf{x}; Z)$.

Since $\operatorname{lcm}(\mathcal{Q}_{m-1}, \mathcal{Q}_m) < C_4(\varepsilon)^{t+1} W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{3\varepsilon}$ all the conditions in (1) are satisfied if (i) holds. If (ii) holds, then the conditions of (3) will hold.

If (iii) holds, then we define a new sequence $(\mathcal{Q}_m, \cdots, \mathcal{Q}_{m+u})$ starting with $\mathcal{Q}_m$. If Z is not a component of $X \cap Y(\mathbf{x}, \mathcal{Q}_{m+j})$ or if all factors of $\mathcal{Q}_{m+j}$ are in $\Omega(\mathbf{x}; Z)$, then we stop. Otherwise, we let $\mathcal{Q}_{m+j+1} = \mathcal{Q}_{m+j}/p$, where p is the largest prime factor p of $\mathcal{Q}_{m+j}$ which is not in $\Omega(\mathbf{x}; Z)$. This process will finish after less than t steps and all integers in the sequence will be divisible by all primes in $\Omega(\mathbf{x}; Z)$. By (4.5.10) we have that

$$\mathcal{Q}_{m+u} \ge W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{\varepsilon}.$$

The last integer $\mathcal{Q}_{m+u}$ will also satisfy $\mathcal{Q}_{m+u} \le \mathcal{Q}_m < C_4(\varepsilon)^{t+1} W^{n/\mathfrak{S}(d,n,\mathbf{w})} V^{2\varepsilon}$ and one of the following conditions:

(iv) $u \geq 1$ and Z is a component of $X \cap Y(\mathbf{x}, \mathcal{Q}_{m+u-1})$ but not $X \cap Y(\mathbf{x}, \mathcal{Q}_{m+n})$.

(v) Z is a component of $X \cap Y(\mathbf{x}, \mathcal{Q}_{m+u})$ and all factors of $\mathcal{Q}_{m+u}$ are in $\Omega(\mathbf{x}; Z)$.

If (iv) holds, then (2) will hold. If instead (v) holds, then (3) holds. This exhausts all cases, so we are done. □

Remark 4.5.6. In the form given, Theorem 4.5.5 is not terribly useful because we have not really addressed case (3) properly. In the case $\mathbf{w} = (1, \cdots, 1)$, then one can, after projecting onto an appropriate hyperplane and then applying Theorem 5.1.2 to the corresponding variety, show that $Z(\mathbb{Q}; \mathbf{B}, P_1, \cdots, P_t)$ is in fact contained in a co-dimension one subvariety of Z. We do not know how to do this for general varieties in weighted projective space, but we will use a specific argument that works for the varieties we are dealing with.

In the balance of this section we prove an extended version of Theorem 3.1 in [105] and Main Lemma 3.2 in [93].

Theorem 4.5.7. *Let $X \subset \mathbb{P}(1, 1, w_2, \cdots, w_{n+1})$ be an integral hypersurface of degree d, defined by the primitive weighted homogeneous form $F(x_0, \cdots, x_{n+1})$. Let ε be a positive real number. Then the non-singular points in $X(\mathbb{Q}; \mathbf{B})$ is contained in the union*

$$\bigcup_{j=1}^{n} \bigcup_{Z \in \Gamma_n} Z(\mathbb{Q}; \mathbf{B}),$$

where Γ_j consists of co-dimension j subvarieties of X of degree at most $O_{d,n}\left((\log V)^j\right)$, and

$$\#\Gamma_j = O_{d,n,\varepsilon}\left(W^j V^{\varepsilon}\right)$$

for $j = 1, \cdots, n$.

Proof. The main tool to carry out this argument will be Theorem 3.1 in [105], and indeed is reminiscent of the argument given in Section 8 of [105]. It furnishes a hypersurface $Y(\emptyset)$ with the property that $X(\mathbb{Q}; \mathbf{B}) \subset Y(\emptyset)(\mathbb{Q})$, but X is not contained in $Y(\emptyset)$. Further, it satisfies

$$\deg Y(\emptyset) = O_{d,n}\left(W \log V\right).$$

We then consider a set of primes $p_1, \cdots, p_{t+1}$ as in Section 8 of [105]. We then furnish, for each point $P_1 \in X_{p_1}$, a hypersurface $Y(P_1)$ such that $X(\mathbb{Q}; \mathbf{B}, P_1) \subset Y(P_1)(\mathbb{Q})$ but X is not contained in $Y(P_1)$. We then examine the components Z_1 of $X \cap Y(\emptyset)$. Suppose that Z_1 is a component of $X \cap Y(\emptyset)$ which contains a non-singular point $\mathbf{x} \in X(\mathbb{Q}; \mathbf{B})$.

Then $\mathbf{x}$ also lies in $Y(P_1)$, where $\mathbf{x} \equiv P_1 \pmod{p_1}$. Suppose that Z_1 is not a component of $X \cap Y(P_1)$. Then $\mathbf{x}$ lies on a component $Z_2^{(1)}$ of $X \cap Y(\emptyset) \cap Y(P_1)$, which is a co-dimension two subvariety of X. We then discard Z_1 and put $Z_2^{(1)}$ in the set $\Gamma_2^\flat$. We then consider the hypersurface $Y(P_1, P_2)$, where P_2 is such that $\mathbf{x} \equiv P_2 \pmod{p_2}$. If Z_1 is not a component of $X \cap Y(P_1, P_2)$, then $\mathbf{x}$ lies on a co-dimension two subvariety $Z_2^{(2)}$ of X which is contained in $X \cap Y(P_1, P_2)$. We then discard Z_1 and place $Z_2^{(2)}$ in $\Gamma_2^\flat$. We repeat this process until we end up with a collection Γ_1 of co-dimension one subvarieties Z_1 of X, which are components of $X \cap Y(\emptyset)$ and $X \cap Y(P_1, \cdots, P_j)$ for $j = 1, \cdots, t+1$. In particular, we have

$$\#\Gamma_1 \leq \deg X \deg Y(\emptyset),$$

and for each $Z_1 \in \Gamma_1$, we have

$$\deg Z_1 \leq \deg X \cap Y(P_1, \cdots, P_{t+1}) = O_{d,n}(\log V).$$

Now we treat the co-dimension two subvarieties obtained in the above process. By construction, all of them lie in

$$X \cap Y(\emptyset) \cap Y(P_1),$$

and also

$$X \cap Y(\emptyset) \cap Y(P_1, \cdots, P_j)$$

for some $j \geq 1$. Again, since we have taken $Z_2^{(j)}$'s as irreducible components, we can ask the question whether it is contained in $Y(P_1, \cdots, P_{j+1})$. If not, then it intersects $Y(P_1, \cdots, P_{j+1})$ in a proper subvariety, which has co-dimension 3 in X. If this is the case, we discard $Z_2^{(j)}$ and put the corresponding co-dimension 3 subvariety in $\Gamma_3^\flat$. Otherwise, we continue to track $Z_2^{(j)}$ and continue to ask whether it lies in $Y(P_1, \cdots, P_k)$ with $k > j$, terminating at $k = t+1$ if it never intersects properly. If this happens, we put $Z_2^{(j)}$ in Γ_2. Otherwise, it is put into $\Gamma_3^\flat$. We then examine Γ_2. Since for all $Z_2 \in \Gamma_2$ we have that Z_2 is a co-dimension two subvariety of X lying in $X \cap Y(\emptyset) \cap Y(P_1)$, it follows from Bezout's theorem and Theorem 3.1 of [105] that

$$\#\Gamma_2 = O_{d,n}\left(p_1^{-1} W^2 (\log V)^2\right),$$

and since Z_2 is a component of $X \cap Y(P_1, \cdots, P_t) \cap Y(P_1, \cdots, P_{t+1})$, it follows that

$$\deg Z = O_{d,n}\left((\log V)^2\right).$$

Continuing in this fashion, we see that we obtain sets $\Gamma_1, \cdots, \Gamma_n$ with the following properties:

1. Γ_j contains irreducible co-dimension j subvarieties of X; and
2. If $Z_j \in \Gamma_j$, then $\deg Z_j = O_{d,n}\left((\log V)^j\right)$.

The desired conclusion then follows.

□

Chapter 5

Applications of the determinant method

in this chapter we give some applications to the p-adic determinant method. The most notable of which is our theorem which establishes that whenever F is an admissible binary form of degree d, then F takes on the expected density of k-free values whenever $k > 7d/18$. We shall also establish a bound for the density of rational points of bounded height on del Pezzo surfaces of degree 2. Finally, we give an argument which bounds the density of rational points on the open subset of a projective surface X of degree d consisting of the complement of curves of degree k.

5.1 k-free values of binary forms

Let $F(x, y)$ be a binary form with integer coefficients, non-zero discriminant, and degree $D \geq 3$, such that the largest degree of an irreducible factor f of F over $\mathbb{Q}$ is d. We say that an integer n is *k-free* if, for all primes p dividing n, we have $p^k \nmid n$. In general, when $k \geq 2$, we expect that for a positive proportion of integer tuples (x, y), that $F(x, y)$ is k-free; unless there is a reason for it not to be k-free.

For any set $\mathcal{S}$, we denote by $\#\mathcal{S}$ the cardinality of $\mathcal{S}$. Write

$$\rho_F(m) = \#\{(i, j) \in \{0, \cdots, m-1\}^2 : F(i, j) \equiv 0 \pmod{m}\} \tag{5.1.1}$$

and

$$C_{F,k} = \prod_p \left(1 - \frac{\rho_F(p^k)}{p^{2k}}\right). \tag{5.1.2}$$

As we will show in Section 5.1, and was shown by Filaseta in [43], the quantity $\rho_F(p^k) \ll p^{2k-2}$, whence the product in (5.1.2) converges absolutely since $k \geq 2$. Further, write

$$N_{F,k}(B) = \#\{(x,y) \in \mathbb{Z}^2 \cap [1,B]^2 : F(x,y) \text{ is } k\text{-free}\}.$$

Suppose that there is no prime p for which p^k divides $F(x,y)$ for all $(x,y) \in \mathbb{Z}^2$. In 1992, Greaves [48] showed that as (x,y) takes on values in $[1,B]^2 \cap \mathbb{Z}^2$, the binary form $F(x,y)$ as above takes on, asymptotically as B tends to ∞, $C_{F,k}B^2$ k-free values whenever $k \geq (d-1)/2$. Filaseta improved this for irreducible binary forms (in which case $D = d$ in the above notation) to $k \geq (2\sqrt{2}-1)d/4$ in [43]. Hooley, in 2009, showed in [71] that it suffices to take $k \geq (d-2)/2$. This improvement is significant for small degrees. In particular, it shows that suitable forms of degree 8 take on infinitely many cube-free values, a result unavailable until Hooley's paper. In 2011, Browning [21] was able to apply the so-called determinant method to obtain that irreducible binary forms satisfying the necessary non-degenerate conditions are k-free as soon as $k > 7d/16$. The determinant method was pioneered by Bombieri and Pila in [14] and greatly extended by Heath-Brown in [53]. The key to Browning's improvement is the so-called global determinant method introduced by Salberger in [93].

Granville showed, subject to the *abc*-conjecture, that appropriate binary forms $F(x,y)$ take on infinitely many square-free values in [47]. Poonen showed in [86] that general, not necessarily homogeneous, binary polynomials $F(x,y)$ with integer coefficients take on infinitely many square-free values assuming the *abc*-conjecture.

For a real number t, let $\lceil t \rceil$ denote the least integer u such that $t \leq u$. We obtain the following theorem:

Theorem 5.1.1. *Let $F(x,y)$ be a binary form with non-zero discriminant of degree $D \geq 2$ with integer coefficients. Let $k \geq 2$ be an integer. Suppose that for each prime p, there exists a pair of integers (x_0, y_0) such that p^k does not divide $F(x_0, y_0)$. Let d denote the largest degree of a factor f of F over $\mathbb{Q}$. Then whenever*

$$k > \min\left\{\frac{7d}{18}, \left\lceil\frac{d}{2}\right\rceil - 2\right\}, \tag{5.1.3}$$

we have

$$N_{F,k}(B) = C_{F,k}B^2 + O\left(\frac{B^2}{\log^{\delta} B}\right), \tag{5.1.4}$$

where $\delta = 0.7043$ *if* $k = 2, d = 6$ *and* $\delta = 1$ *otherwise.*

For example, we have that $F(x, y)$ takes on infinitely many 6-free values for $d \leq 15$.

The value of δ in Theorem 5.1.1 for the case $k = 2, d = 6$ is due to Helfgott [59]. He obtained a better error term in (5.1.4) for the cases $k = 2$ and $d = 3, 4, 5$ as well; see page 2 of [59]. The condition $k > 7d/18$ in (5.1.3) arises from the application of the global determinant method, and represents the main contribution of this paper. The condition $k > \lceil d/2 \rceil - 2$ is equivalent to the condition $d \leq 2k + 1$, which is exactly the condition required for Greaves' theorem in [48]. This result is superior for small degrees.

Mazur and Gouvêa showed in [46] that the problem of counting square-free values of binary forms can be applied to construct elliptic curves E that possess many quadratic twists with large rank. They adapted methods introduced by Hooley in [63] to the context of binary forms. They remarked in [46] that the sieve method developed by G. Greaves in [48] is more efficient at counting square-free values of binary forms and can be used to strengthen their result. Stewart and Top, in [99], were able to achieve this. In particular, they proved as Theorem 1 in [99] that for $F(x, y)$ a binary form with integral coefficients of degree $D \geq 3$ and non-zero discriminant, there exists a positive constant C for which F assumes at least $CB^{2/D}$ k-free values in the interval $[-B, B]$, provided that $k \geq (d-1)/2$ or if $k = 2, d \leq 6$. The condition $k \geq (d-1)/2$ or if $k = 2, d \leq 6$ corresponds precisely to the theorem of Greaves in [48]. The argument used to prove Theorem 1 [99] is mostly independent of the arguments used in Greaves [48], whence we can improve Theorem 1 in [99] by providing a better estimate for k-free values of binary forms. Analogous to [99], we define the counting function $R_{F,k}(B)$ as follows:

$$R_{F,k}(B) = \#\{t \in \mathbb{Z} : |t| \leq B, \exists (x, y) \in \mathbb{Z}^2 \text{ such that } F(x, y) = t, t \text{ is } k\text{-free}\}.$$

We then have the following result:

Theorem 5.1.2. *Let* $k \geq 2$. *Let* $F(x, y)$ *be a binary form of degree* $D \geq 3$ *with integer coefficients and non-zero discriminant, with no fixed* k*-th power prime divisor. Let* d *be the largest degree of an irreducible factor of* F *over* $\mathbb{Q}$ *and suppose that*

$$k > \min\left\{\frac{7d}{18}, \left\lceil\frac{d}{2}\right\rceil - 2\right\}.$$

Then there exist positive real numbers C_1 and C_2, which depend on F and k, such that if $B > C_1$, then

$$R_{F,k}(B) > C_2 B^{2/D}.$$

There is an analogous question for polynomials of a single variable. Suppose that $g(x)$ is a polynomial with integer coefficients and degree d which is irreducible over $\mathbb{Q}$ and has no fixed k-th power prime divisor. Then we expect that $g(x)$ should take on infinitely many k-free values for $k \geq 2$. Indeed, this was established conditionally assuming the *abc*-conjecture by Granville [47]; see also [81]. For larger values of k, the investigation goes back to Ricci in 1933 [90], who established that g takes on infinitely many k-free values for $k \geq d$. Erdős [39], in 1956, showed that $k \geq d-1$ suffices. However, Erdős only gave a lower bound and not an asymptotic formula. Hooley was able to obtain the exact asymptotic formula in terms of local densities in 1967 [63]. This point will be elaborated below.

For each positive integer m, define $\rho_g(m)$ to be the cardinality of the set $\{i \in \{0, \cdots, m-1\} : g(i) \equiv 0 \pmod{m}\}$. Put

$$c_{g,k} = \prod_p \left(1 - \frac{\rho_g(p^k)}{p^k}\right), \tag{5.1.5}$$

which is well defined (that is, the product converges) when $k \geq 2$. It is non-zero precisely when g does not have a fixed k-th power prime divisor. Write

$$N_{g,k}(B) = \#\{1 \leq x \leq B : g(x) \text{ is } k\text{-free}\}.$$

Then, one should expect that

$$N_{g,k}(B) \sim c_{g,k} B. \tag{5.1.6}$$

Indeed, this was the result obtained by Hooley, under the assumption that $k \geq d-1$. A similar asymptotic formula was obtained by all subsequent authors. Nair obtained (5.1.6) under the assumption $k \geq \left(\sqrt{2} - \frac{1}{2}\right) d$ in 1976 [82]. Heath-Brown obtained (5.1.6) under the assumption that $k \geq (3d+2)/4$ in 2006 [54], where he used the determinant method. Browning improved Heath-Brown's result to $k \geq (3d+1)/4$ in [21]. We will give another proof of Browning's result in Section 5.2 as an illustration of our method.

It should be noted that Heath-Brown obtained (5.1.6) for irreducible polynomials of the shape $f(x) = x^d + c, c \in \mathbb{Z}$ assuming $k \geq (5d+3)/9$ in [56]. His arguments are also inspired by weighted projective spaces, defined below, but are materially different from the

arguments presented in the present paper. It would be interesting to see whether Theorem 5.1.1 can be improved for diagonal forms of the shape $F(x,y) = Ax^d + By^d$.

In order to prove Theorem 5.1.1 and Theorem 5.1.2, we utilize the p-adic determinant method proved for the case of weighted projective spaces proved in the previous chapter. We shall apply the determinant method mentioned above which applies to the weighted projective space setting to the weighted projective surface X defined by the following equation:

$$f(x,y) = vz^k, \tag{5.1.7}$$

which is a surface in $\mathbb{P}_{\mathbb{Q}}(1,1,d-2k,2)$. Here f is an irreducible factor of degree d of the binary form F given in Theorem 5.1.1. Applying the determinant method in this way allows us to deal with a dimension two subvariety X inside the weighted projective space $\mathbb{P}_{\mathbb{Q}}(1,1,d-2k,2)$. This leads to a stronger result than we would obtain by dealing with a dimension three subvariety inside $\mathbb{A}^4$ or working with a surface in $\mathbb{A}^3$ by a priori fixing one variable, which was Browning's approach. We emphasize that viewing (5.1.7) as a surface in weighted projective space is critical to our improvement.

We now make a remark regarding the choice of weights $(1,1,d-2k,2)$. It seems a priori that the better weight choice is $(1,1,d-k,1)$, which is similar to Heath-Brown's approach in [56]. However the weight vector $(1,1,d-k,1)$ does not take into account the progress made by Greaves and will in fact produce results inferior to Greaves in [48]. Nevertheless, in our proof of Theorem 5.2.1 we will use $(1,1,d-k,1)$, precisely because Greaves' result does not apply in this context.

Moreover, we remark that our approach does not seem to generalize in an obvious way to subsequent work by Browning, Heath-Brown, and Salberger dealing with arbitrary projective varieties in [22], because we do not know how to deal with projections of arbitrary weighted projective varieties onto a hypersurface in a weighted projective space of lower dimension.

5.1.1 Preliminaries for dealing with binary forms

In this section and the next, we use our results from previous sections to prove Theorem 5.1.1. Suppose we have a binary form $F(x,y)$ of degree D with integer coefficients. Notice that if $k \geq d/2$, Theorem 5.1.1 follows from the work of Greaves [48]. Hence, we may

suppose that $k \geq 2$ is an integer which satisfies

$$\frac{7}{18} < \frac{k}{d} < \frac{1}{2}. \tag{5.1.8}$$

We turn our attention to the following central object

$$N_{F,k}(B) = \#\{(x,y) \in \mathbb{Z}^2 : 1 \leq x, y \leq B, F(x,y) \text{ is } k\text{-free}\}. \tag{5.1.9}$$

We assume that for all primes p, there exists a pair of positive integers (a,b), such that p^k does not divide $F(a,b)$. Our strategy will be to show that subject to (5.1.8), we have $N_{F,k}(B) = C_{F,k}B^2 + O(B^2(\log B)^{-\delta})$, where $C_{F,k}$ is as in (5.1.2). This would show that F takes on k-free values infinitely often. We also note the following observation, which follows easily from the definition of the Mobius function:

$$\sum_{b^k | F(x,y)} \mu(b) = \begin{cases} 1, & \text{if } F(x,y) \text{ is } k\text{-free}, \\ 0, & \text{otherwise.} \end{cases}$$

For any $\xi > 0$, we write

$$M_1(B) = \#\{(x,y) \in \mathbb{Z}^2 : 1 \leq x, y \leq B : p^k | F(x,y) \Rightarrow p > \xi\},$$

$$M_2(B) = \#\left\{(x,y) \in \mathbb{Z}^2, 1 \leq x, y \leq B : p^k | F(x,y) \Rightarrow p > \xi, \exists p \in \left(\xi, \frac{B^2}{\log B}\right] \text{ s.t. } p^k | F(x,y)\right\},$$

and

$$M_3(B) = \#\left\{(x,y) \in \mathbb{Z}^2, 1 \leq x, y \leq B : \exists p > \frac{B^2}{\log B}, v \in \mathbb{Z} \text{ s.t. } F(x,y) = vp^k\right\}.$$

Note that by their definitions we have

$$M_1(B) - M_2(B) - M_3(B) \leq N_{F,k}(B) \leq M_1(B),$$

so it suffices to show that $M_1(B)$ dominates the other two terms. Write

$$N(b,B) = \#\{(x,y) \in \mathbb{Z}^2 : |x|, |y| \leq B, b^k | F(x,y)\}.$$

We have that

$$\begin{aligned} M_1(B) &= \sum_{\substack{b \in \mathbb{N} \\ p|b \Rightarrow p \leq \xi}} \mu(b) N(b,B) \\ &= \sum_{\substack{b \in \mathbb{N} \\ p|b \Rightarrow p \leq \xi}} \mu(b) \rho_F(b^k) \left\{\frac{B^2}{b^{2k}} + O\left(\frac{B}{b^k} + 1\right)\right\}. \end{aligned}$$

When b is squarefree, we have the bound

$$b \leq \prod_{p \leq \xi} p = \exp\left(\sum_{p \leq \xi} \log p\right) \leq e^{2\xi},$$

by Theorem 4 of [91]. It is clear that the function ρ_F is multiplicative. Since F is a binary form, we see that if $F(x,0) \equiv 0 \pmod{p}$, then $a_D x^D \equiv 0 \pmod{p}$, where a_D is the coefficient of x^D in F. There can only be finitely many primes p such that $p|a_D$, and for all other primes we must have $x \equiv 0 \pmod{p}$. In other words, for all but finitely many primes, 0 is the only solution to $F(x,0) \equiv 0 \pmod{p}$. A similar argument applies for solutions of the form $(0,y)$. Now, suppose that (x,y) is a solution such that $x, y \not\equiv 0 \pmod{p}$. Then,

$$F(x,y) \equiv y^D F(x/y, 1) \equiv 0 \pmod{p},$$

and since $y \not\equiv 0 \pmod{p}$, it follows that this solution arises from a zero of $F(\gamma, 1)$ over the field of p elements. However, there can be at most D roots to this polynomial, which implies that $\rho_F(p) \ll p$. For $\rho_F(p^k)$, we refer the reader to Lemma 1 of [43] for the proof of the bound $\rho_F(p^k) \ll p^{2k-2}$. Hence, for any $\varepsilon > 0$ and b square-free, we have $\rho_F(b^k) \ll_\varepsilon b^{2k-2+\varepsilon}$. For $k \geq 2$, we have

$$M_1(B) = B^2 \prod_{p \leq \xi} \left(1 - \frac{\rho_F(p^k)}{p^{2k}}\right) + O\left(\sum_{b \leq e^{2\xi}} (Bb^{k-2+\varepsilon} + b^{2k-2+\varepsilon})\right).$$

Note that

$$\prod_{p \leq \xi} \left(1 - \frac{\rho_F(p^k)}{p^{2k}}\right)$$

is a partial product of an absolutely convergent product, $C_{F,k}$, and is therefore positive.

By setting $\xi = \dfrac{1}{2k} \log B$, we see that

$$M_1(B) = B^2 \prod_{p \leq \xi} \left(1 - \frac{\rho_F(p^k)}{p^{2k}}\right) + O\left(B^{2-\frac{1}{k}+\varepsilon}\right).$$

We now consider $M_2(B)$. We refer the reader to Lemma 2 in Greaves [48], where he obtained the bound

$$M_2(B) = O\left(B^2 (\log B)^{-1}\right),$$

for $k \geq d/2$ and

$$M_2(B) = O\left(B^2(\log B)^{-1/2}\right)$$

for $k = 2, d = 6$. Helfgott, in [59], obtained the error term

$$M_2(B) = O\left(B^2(\log B)^{-\delta}\right)$$

for $\delta = 0.7034\cdots$. We note that the argument in [48] deals with essentially one prime at a time, so it simultaneously deals with all numbers z divisible by some prime p in the interval $(\xi, B^2(\log B)^{-1}]$. An important feature of Greaves' estimate which is not present in the work of any subsequent author, except Hooley [70] [71], is that his estimate for $M_2(B)$ is *independent* of any relationship between k and d. All further estimates obtained by other authors require a relationship between k and d of the form $k \geq \upsilon_1 d + \upsilon_2$, where $0 < \upsilon_1 \leq 1/2$ and $\upsilon_2 \in \mathbb{R}$.

To complete the proof of the theorem, it will be enough to show that

$$M_3(B) \ll B^{2-\eta}$$

for some $\eta > 0$, which will be the focus of the next section.

5.1.2 Application of the determinant method: proof of Theorem 5.1.1

We estimate the remaining term $M_3(B)$ via the generalization of Salberger's global determinant method (see [93]) in the weighted projective case established in earlier sections. The argument given here is specialized for the binary form problem. We denote by

$$S_3^{(f)}(B) = \left\{(x,y) \in \mathbb{Z}^2 : 1 \leq x, y \leq B, \exists p > \frac{B^2}{\log B}, v \in \mathbb{Z} \text{ s.t. } f(x,y) = vp^k\right\}$$

for some irreducible factor f of F. Further, write $M_3^{(f)}(B) = \#S_3^{(f)}(B)$. Since F has non-zero discriminant, it follows that

$$M_3(B) \leq \sum_{f|F, f \text{ irreducible}} M_3^{(f)}(B).$$

Let us fix an irreducible factor $f(x,y) \in \mathbb{Z}[x,y]$ of F, such that f has maximal degree, and write $d = \deg f$. Note that if $p^k > d\|f\|B^d$, then $p^k > |f(x,y)|$ for all $(x,y) \in [1,B]^2 \cap \mathbb{Z}^2$.

Therefore, p^k cannot divide $f(x,y)$ unless $(x,y) = (0,0)$. Hence, we may assume that $p \leq (d\|f\|)^{1/k} B^{d/k}$. Thus, the relevant range of primes left to consider are

$$\frac{B^2}{\log B} < p \leq d\|f\|B^{\frac{d}{k}}.$$

Following Browning in [21] , we partition the above range into dyadic intervals of the form $(H/2, H]$ where

$$B^2/\log B \ll H \ll d\|f\|B^{\frac{d}{k}}.$$

Now write

$$R(f;H,B) = \#\{(x,y,v,z) \in \mathbb{Z}^4 : f(x,y) = vz^k, (x,y) \in S_3^{(f)}(B), \tag{5.1.10}$$
$$\gcd(x,y) = 1, H/2 < z \leq H, v \ll B^d/H^k, z \text{ prime}, v \neq 0\}.$$

Write $H = B^\beta$, so $B^d/H^k = B^{d-k\beta}$. Summing over these dyadic intervals, we then obtain:

$$M_3^{(f)}(B) \ll \log B \sup_{2-\frac{\log\log B}{\log B} < \beta \leq \frac{d}{k} + \frac{\log(d\|f\|)}{\log B}} R(f; B^\beta, B). \tag{5.1.11}$$

Therefore, it suffices to examine the maximum size of a single $R(f;B^\beta,B)$, as in [21]. Diverging from Browning's argument, we directly estimate $R(f;B^\beta,B)$ instead of passing to the single variable case. We are then left to count the number of integral solutions to

$$\mathcal{F}(x,y,v,z) = f(x,y) - vz^k = 0 \tag{5.1.12}$$

where (x,y,v,z) is subject to the constraints in (5.1.10) with $H = B^\beta$.

Let us denote by X the surface given by (5.1.12). We consider possible singular points in $X(\mathbb{Q};\mathbf{B})$. First, note that our ambient space $\mathbb{P}(1,1,2,d-2k)$ has singularities at $(0,0,1,0)$ and $(0,0,0,1)$. However, these points do not line in $X(\mathbb{Q};\mathbf{B})$ since we are only counting points whose first two coordinates are co-prime. Next recall that a point $\mathbf{z} = (x_0,y_0,v_0,z_0)$ on X is singular if

$$\frac{\partial\mathcal{F}}{\partial x}(\mathbf{z}) = \frac{\partial\mathcal{F}}{\partial y}(\mathbf{z}) = \frac{\partial\mathcal{F}}{\partial v}(\mathbf{z}) = \frac{\partial\mathcal{F}}{\partial z}(\mathbf{z}) = 0.$$

Suppose that $\dfrac{\partial\mathcal{F}}{\partial x}(\mathbf{z}) = \dfrac{\partial\mathcal{F}}{\partial y}(\mathbf{z}) = 0$, with $\mathbf{z} \neq \mathbf{0}$. Then, by Euler's formula, we have

$$\begin{aligned} 0 &= \left(x_0\frac{\partial\mathcal{F}}{\partial x}(\mathbf{z}) + y_0\frac{\partial\mathcal{F}}{\partial y}(\mathbf{z})\right) \\ &= \left(x_0\frac{\partial f}{\partial x}(\mathbf{z}) + y_0\frac{\partial f}{\partial y}(\mathbf{z})\right) \\ &= df(x_0,y_0). \end{aligned}$$

Since f is irreducible over $\mathbb{Q}$, it has no integral zeroes except $(0,0)$. Therefore, we see that all points in $X(\mathbb{Q};\mathbf{B})$ are non-singular, since it only counts those points where the first two coordinates are co-prime.

Let

$$X^{\beta}(\mathbb{Q};\mathbf{B}) = \{\mathbf{x} \in X : \mathbf{x} \text{ satisfies (5.1.10) }\}. \tag{5.1.13}$$

In view of Proposition 4.1.4, we need to compute the constants a_x, a_y, a_v, a_z with respect to the ideal $I = \langle \mathcal{F} \rangle$. By (5.1.10), we have

$$B_x = B_y = B, B_v = B^{d-k\beta}, B_z = B^{\beta}.$$

Note that with respect to reverse lexicographic ordering, the monomial vz^k is maximal in $\mathcal{F}$. Hence, it follows that

$$a_x = a_y = \frac{d-0}{3d},$$

$$a_v = \frac{d-(d-2k)}{3d(d-2k)} = \frac{2k}{3d(d-2k)},$$

and

$$a_z = \frac{d-2(k)}{3d(2)} = \frac{d-2k}{6d}.$$

Thus, we have

$$B_x^{a_x} B_y^{a_y} B_v^{a_v} B_z^{a_z} = B^{\frac{1}{3}\left(2+\frac{2k(d-k\beta)}{d(d-2k)}+\frac{\beta(d-2k)}{2d}\right)}.$$

Next, note that

$$1 + \frac{2k(d-k\beta)}{d(d-2k)} + \frac{\beta(d-2k)}{2d} = \frac{d-k\beta}{d-2k} + \frac{\beta}{2},$$

whence it follows

$$\left(B_x^{a_x} B_y^{a_y} B_v^{a_v} B_z^{a_z}\right)^{\frac{3}{2}\left(\frac{2(d-2k)}{d}\right)^{1/2}} = \left(B^{1+\frac{d-k\beta}{d-2k}+\frac{\beta}{2}}\right)^{\frac{1}{2}\left(\frac{2(d-2k)}{d}\right)^{1/2}}.$$

Let us write

$$\psi = \frac{1}{2}\left(1 + \frac{d-k\beta}{d-2k} + \frac{\beta}{2}\right)\left(\frac{2(d-2k)}{d}\right)^{1/2}. \tag{5.1.14}$$

Observe that B^{ψ} corresponds to W in Theorem 4.0.1.

It is clear that X is geometrically integral. Hence, by Theorem 4.0.1, there exists a surface $Y(\emptyset) \subset \mathbb{P}(1,1,d-2k,2)$ not containing X such that

$$\deg Y(\emptyset) = O_{d,\varepsilon}\left(B^{\psi+\varepsilon}\right) \tag{5.1.15}$$

and

$$X^{\beta}(\mathbb{Q};\mathbf{B}) \subset X(\mathbb{Q};\mathbf{B}) \subset Y(\emptyset).$$

We will now show that, in fact, X_p is geometrically integral except for those primes p which divide the coefficients of x^d and y^d in $f(x,y)$. Suppose that

$$\mathcal{F}(x,y,v,z) = f(x,y) - vz^k$$

admits a factorization into two weighted forms $\mathcal{F}_1, \mathcal{F}_2$ over the algebraic closure of $\overline{\mathbb{F}_p}$, where p does not divide the coefficient of x^d nor y^d in $f(x,y)$. By Lemma 8 in Chapter 2 of [29], it follows that the leading monomial of $\mathcal{F}$ is equal to the product of the leading monomials of $\mathcal{F}_1, \mathcal{F}_2$. Thus, under our ordering $>$, where vz^k is the leading monomial of $\mathcal{F}$, this implies that $\mathcal{F}_1, \mathcal{F}_2$ must take the forms

$$\mathcal{F}_1(x,y,v,z) = a_0 v z^l + \mathcal{G}_1(x,y,z),$$

$$\mathcal{F}_2(x,y,v,z) = b_0 z^{k-l} + \mathcal{G}_2(x,y,z)$$

for some non-negative integer $l \leq k$, since $\mathcal{F}_1, \mathcal{F}_2$ are both weighted homogeneous with respect to $(1,1,d-2k,2)$. By considering different orderings which order x and y respectively as the highest and applying Lemma 8 in Chapter 2 of [29], we see that

$$\mathcal{F}_1(x,y,v,z) = a_0 v z^l + a_1 x^{d-2k+2l} + a_2 y^{d-2k+2l} + \mathcal{G}_1'(x,y,z),$$

$$\mathcal{F}_2(x,y,v,z) = b_0 z^{k-l} + b_1 x^{2k-2l} + b_2 y^{2k-2l} + \mathcal{G}_2'(x,y,z)$$

where a_1, a_2, b_1, b_2 are non-zero in $\overline{\mathbb{F}_p}$. The terms

$$a_0 b_1 x^{2k-2l} v z^l, a_0 b_2 y^{2k-2l} v z^l, b_0 a_1 x^{d-2k+2l} z^{k-l}, b_0 a_2 y^{d-2k+2l} z^{k-l}$$

must appear in $\mathcal{F} = \mathcal{F}_1 \mathcal{F}_2$ with non-zero coefficient, which is plainly not the case. This contradiction implies that X_p is geometrically integral over $\mathbb{F}_p$ whenever p does not divide the coefficients of x^d and y^d.

Recall the definition of π_X (Definition 4.2.4) from Section 4.2. By the preceding argument, it follows that $\pi_X \leq \|f\|$. Let $0 < \varepsilon < 1/2$ be a positive number, and let $\{p_1, p_2, \cdots\}$ be the increasing sequence of consecutive primes larger than $\max\{\|f\|, \log B\}$ for which

$$p_1 \cdots p_t < B^{\psi+\varepsilon} \leq p_1 \cdots p_{t+1}. \tag{5.1.16}$$

We now give an estimate for p_{t+1}. Let

$$\theta(x) = \sum_{p \le x} \log p,$$

and let us write $\mathcal{Q}_j = p_1 \cdots p_j$ for $j = 1, 2, \cdots, t+1$, with $\mathcal{Q}_0 = 1$. By the Prime Number Theorem, there exists some absolute constant C_{16} such that

$$p_{t+1} < C_{16}\theta(p_{t+1}) = C_{16} \sum_{p \le p_{t+1}} \log p, \tag{5.1.17}$$

hence

$$\begin{aligned} p_{t+1} - C_{16} \log p_{t+1} &\ll \sum_{p \le \max\{\|f\|, \log B\}} \log p + \sum_{\max\{\|f\|, \log B\} < p \le p_t} \log p \\ &\le \theta(\log B) + \sum_{p \mid \pi_X} \log p + \sum_{j=1}^{t} \log p \\ &= \theta(\log B) + \sum_{p \mid \pi_X} \log p + \log \mathcal{Q}_t \\ &\ll \log B + \|f\|, \end{aligned}$$

since we know that $p_{t+1} > \max\{\log B, \|f\|\}$ and therefore we can, by choosing B sufficiently large, make sure that $C_{16} \log p_{t+1} < \frac{1}{2} p_{t+1}$. Thus, we have

$$\mathcal{Q}_{t+1} = O(B^{\psi+\varepsilon} \log B). \tag{5.1.18}$$

Since the partial derivative

$$\frac{\partial \mathcal{F}}{\partial v} = z^k$$

is only divisible by primes $\gg B^2 (\log B)^{-1}$, (5.1.17) implies that there is no point $\mathbf{x} \in X^\beta(\mathbb{Q}; \mathbf{B})$ which specializes to a singular point on X_{p_j} for $j = 1, \cdots, t+1$. Hence, every $\mathbf{x} \in X^\beta(\mathbb{Q}; \mathbf{B})$ reduces to a non-singular point on X_{p_j} for every prime $j = 1, \cdots, t+1$.

Our goal now is to construct a set of exceptional points $\mathcal{E}$ and a collection of curves Γ which cover $X^\beta(\mathbb{Q}; \mathbf{B})$. Consider an irreducible component $\mathcal{D}(\emptyset)$ of $X \cap Y(\emptyset)$. For each point $\mathbf{x} \in \mathcal{D}(\emptyset) \cap X^\beta(\mathbb{Q}; \mathbf{B})$, let $P_1(\mathbf{x}) = P_1$ be the $\mathbb{F}_{p_1}$-point on X_{p_1} such that $\mathbf{x} \equiv P_1 \pmod{p_1}$. By Theorem 4.0.1, there exists a surface $Y(P_1)$ which contains $X^\beta(\mathbb{Q}; \mathbf{B}, P_1)$. Thus, there exists an irreducible component $\mathcal{D}_{\mathbf{x}}(P_1)$ of $X \cap Y(P_1)$ which contains $\mathbf{x}$. If

$\mathcal{D}(\emptyset) \neq \mathcal{D}_{\mathbf{x}}(P_1)$, then put $\mathbf{x}$ in a set $Z(P_1)$. Repeat this process for each irreducible component $\mathcal{D}$ of $X \cap Y(\emptyset)$, to obtain sets $Z(P_1)$ for each $P_1 \in X_{p_1}$. Note that a surface in $\mathbb{P}(1,1,2,d-2k)$ of weighted degree d is the quotient of a certain action of a surface of degree d in the straight projective space $\mathbb{P}^3$, therefore Bézout's Theorem for straight projective spaces provides an upper bound for the cardinality of the sets $Z(P_1)$. Theorem 4.0.1 then shows that for each $P_1 \in X_{p_1}$, we have

$$\#Z(P_1) \ll_d \left(p_1^{-1}B^{\psi} + \log Bp_1\right)\left(B^{\psi} + \log B\right)(\log B)^2.$$

Write

$$Z(p_1) = \bigcup_{P_1 \in X_{p_1}} Z(P_1).$$

By Lang and Weil's theorem, we have $\#X_{p_1} = O_d(p_1^2)$, where it follows that

$$\#Z(p_1) = O_d\left(p_1^2\left(p_1^{-1}B^{2\psi} + \log Bp_1\right)(\log B)^2\right) = O_d\left(B^{2\psi}(\log B)^5\right).$$

What remains are irreducible components $\mathcal{C}$ of $X \cap Y(\emptyset)$ which are also irreducible components of $X \cap Y(P_1)$ for some $P_1 \in X_{p_1}$. Call this collection of curves $\Gamma^{(1)}$. For each surface $Y(P_1)$, suppose that G_{P_1} is a primitive form which defines $Y(P_1)$. Then, from (5.1.12) we see that we can substitute $v = f(x,y)/z^k$ into G_{P_1} to obtain

$$G_{P_1}(x,y,v,z) = G_{P_1}\left(x, y, \frac{f(x,y)}{z^k}, z\right). \tag{5.1.19}$$

If $G_{P_1}(x,y,v,z)$ has a v term, then we may replace the v's with $f(x,y)/z^k$ to obtain a form over $\mathbb{P}(1,1,2)$. If G does not have a term containing v, then no substitution is necessary and we again obtain a form over $\mathbb{P}(1,1,2)$. Since G_{P_1} is weighted homogeneous with respect to $(1,1,d-2k,2)$, it follows that each monomial that appears in G_{P_1} with a non-zero coefficient has the same weighted degree l with respect to the weight vector $(1,1,d-2k,2)$. Consider a monomial $x^{\alpha_1}y^{\alpha_2}v^{\alpha_3}z^{\alpha_4}$ that appears in G_{P_1} with non-zero coefficient. After the substitution, we obtain

$$x^{\alpha_1}y^{\alpha_2}\left(\frac{f(x,y)}{z^k}\right)^{\alpha_3} z^{\alpha_4}.$$

Expanding $f(x,y)$ and recalling that f is a binary form of degree d, it follows that each monomial which appears in the expansion $f(x,y)^{\alpha_3}$ has degree $d\alpha_3$. Now, we multiply by a large power of z, say z^L, so that

$$z^L G_{P_1}\left(x, y, \frac{f(x,y)}{z^k}, z\right)$$

is a polynomial in x, y, z. Each monomial that appears in $z^L x^{\alpha_1} y^{\alpha_2} (f(x,y)/z^k)^{\alpha_3} z^{\alpha_4}$ has weighted degree

$$2L + \alpha_1 + \alpha_2 + d\alpha_3 - 2k\alpha_3 + 2\alpha_4 = 2L + l,$$

so $z^L G_{P_1}(x, y, f(x,y)/z^k, z)$ is a polynomial over $\mathbb{P}(1,1,2)$. Further, if we choose L to be minimal, then $L \leq kl$. We call the new polynomial $\mathcal{G}_{P_1}(x,y,z)$. It is now clear that the degree of $\mathcal{G}_{P_1}$ is at most $2kl + l = l(2k+1)$, and thus Theorem 4.0.1 implies

$$\deg \mathcal{C} = \deg \mathcal{G}_{P_1} = O_d\left(\left(p_1^{-1} B^{\psi} \log B + \log B p_1\right)\right) \tag{5.1.20}$$

for each $\mathcal{C} \in \Gamma^{(1)}$. Observe that $\Gamma^{(1)}$ is a collection of irreducible components of $X \cap Y(\emptyset)$, hence

$$\#\Gamma^{(1)} = O_d\left(B^{\psi} \log B\right).$$

We have thus obtained a relatively small set of points $Z(p_1)$ and a collection of curves $\Gamma^{(1)}$ which together cover $X^{\beta}(\mathbb{Q}; \mathbf{B})$. Moreover, the curves in $\Gamma^{(1)}$ now have degrees bounded as in (5.1.20) and the number of curves in $\Gamma^{(1)}$ is bounded above by the degree of $Y(\emptyset)$. We can continue this process to continue to separate points in $X^{\beta}(\mathbb{Q}; \mathbf{B})$ into an exceptional set or onto a curve of relatively small degree.

Suppose we have obtained $Z(\mathcal{Q}_i)$ for $1 \leq i \leq j$ up to some positive integer j. In particular, $Z(\mathcal{Q}_i)$ is the set of points $\mathbf{x} \in X^{\beta}(\mathbb{Q}; \mathbf{B})$ such that $\mathbf{x} \notin Z(\mathcal{Q}_{i-1})$ and $\mathcal{D}(\emptyset) \neq \mathcal{D}_{\mathbf{x}}(P_1, \cdots, P_i)$. Notice that

$$\#Z(\mathcal{Q}_i) = O_d\left(\mathcal{Q}_i^2 (p_i^{-1} \mathcal{Q}_{i-1}^{-2} B^{2\psi} + \log B\mathcal{Q}_i)(\log B)^2\right).$$

Similarly, suppose we have obtained $\Gamma^{(i)}$, $1 \leq i \leq j$, where $\Gamma^{(i)}$ is the set of curves $\mathcal{C}$ of degree

$$O_d\left(\mathcal{Q}_i^{-1} B^{\psi} \log B + \log B\mathcal{Q}_i\right),$$

such that $\mathcal{C} \in \Gamma^{(i-1)}$ and

$$\mathcal{C} = \mathcal{D}(\emptyset) = \mathcal{D}_{\mathbf{x}}(P_1, \cdots, P_i)$$

for some $(P_1, \cdots, P_i)$. Observe that we have

$$X^{\beta}(\mathbb{Q}; \mathbf{B}) \subset \bigcup_{\mathcal{C} \in \Gamma^{(i)}} \mathcal{C} \cup Z(\mathcal{Q}_i).$$

We now construct $Z(\mathcal{Q}_{j+1})$ given $Z(\mathbb{Q}_j)$. Consider an irreducible curve $\mathcal{C} \in \Gamma^{(j)}$. For each point $\mathbf{x} \in \mathcal{C} \cap (X^{\beta}(\mathbb{Q}; \mathbf{B}) \setminus Z(\mathcal{Q}_j))$, we have

$$\mathcal{D}(\emptyset) = \mathcal{D}_{\mathbf{x}}(P_1) = \mathcal{D}_{\mathbf{x}}(P_1, P_2) = \cdots = \mathcal{D}_{\mathbf{x}}(P_1, \cdots, P_j) = \mathcal{C}.$$

There exists a point $P_{j+1} = P_{j+1}(\mathbf{x}) \in X_{p_{j+1}}$ such that $\mathbf{x} \equiv P_{j+1} \pmod{p_{j+1}}$. Hence, by Theorem 4.0.1, there exists a surface $Y(P_1, \cdots, P_{j+1})$ such that $\mathbf{x} \in X \cap Y(P_1, \cdots, P_{j+1})$, and

$$\deg Y(P_1, \cdots, P_{j+1}) = O_d\left(\mathcal{Q}_{j+1}^{-1} B^{\psi+\varepsilon} + \log B\mathcal{Q}_{j+1}\right).$$

Set $\mathcal{D}_{\mathbf{x}}(P_1, \cdots, P_{j+1})$ to be an irreducible component of $X \cap Y(P_1, \cdots, P_{j+1})$ which contains $\mathbf{x}$. Put $\mathbf{x}$ in the set $Z(P_1, \cdots, P_{j+1})$ if

$$\mathcal{D}_{\mathbf{x}}(P_1, \cdots, P_j) \neq \mathcal{D}_{\mathbf{x}}(P_1, \cdots, P_{j+1}),$$

then repeat this process for every point $\mathbf{x} \in \mathcal{C} \cap (X^{\beta}(\mathbb{Q}; \mathbf{B}) \setminus Z(\mathcal{Q}_j))$ and for every curve in $\Gamma^{(j)}$ to obtain our sets $Z(P_1, \cdots, P_{j+1})$ for $P_i \in X_{p_i}, i = 1, \cdots, j+1$. By Bézout's theorem, we have

$$\begin{aligned} \#Z(P_1, \cdots, P_{j+1}) &= O_d\left(\deg Y(P_1, \cdots, P_j) \deg Y(P_1, \cdots, P_{j+1}\right) \\ &= O_d\left(\mathcal{Q}_j^{-1}\mathcal{Q}_{j+1}^{-1} B^{2\psi} + (\mathcal{Q}_j^{-1} + \mathcal{Q}_{j+1}^{-1}) B^{\psi} \log B\mathcal{Q}_{j+1} + \log^2 B\mathcal{Q}_{j+1}\right) \\ &= O_d\left(\mathcal{Q}_{j+1}^{-2} B^{2\psi} \log B + \log^2 B\mathcal{Q}_{j+1}\right) \end{aligned} \tag{5.1.21}$$

Write $Z(\mathcal{Q}_{j+1})$ as

$$Z(\mathcal{Q}_{j+1}) = \bigcup_{\substack{P_i \in X_{p_i} \\ 1 \leq i \leq j+1}} Z(P_1, \cdots, P_{j+1}).$$

By Lemma 4.3.3, we have

$$\#X_{p_j} = p_j^2 + O(d^2 p_j^{3/2}) + O_d(p)$$

for $j = 1, \cdots, t+1$. We write this as

$$\#X_{p_j}/p_j^2 = 1 + O(d^2 p_j^{-1/2}) + O_d(p^{-1}).$$

Therefore, for some number $C_{17}(d) > 0$ depending on d, we have

$$\prod_{i=1}^{j+1} \frac{\#X_{p_i}}{p_i^2} \leq \left(\prod_{i=1}^{j+1}\left(1 + p_i^{-1/2}\right)\right)^{C_{17}(d)},$$

hence

$$\prod_{i=1}^{j+1} \#X_{p_i} \leq \mathcal{Q}_{j+1}^2 \left(\prod_{i=1}^{j+1}\left(1 + p_i^{-1/2}\right)\right)^{C_{17}(d)}.$$

Since $\mathcal{Q}_{t+1} = p_1 \cdots p_{t+1} \ll B^{\psi+\varepsilon} \log B$ and $p_i \geq \log B$, there exists a positive number $C_{18}(d)$ such that

$$t \leq \frac{C_{18}(d) \log B}{\log \log B}. \tag{5.1.22}$$

We now use the inequality

$$1 + \upsilon \leq e^{\upsilon}$$

which is valid for all $\upsilon \geq 0$, to obtain

$$\prod_{i=1}^{j+1}(1 + p_i^{-1/2}) \leq \prod_{i=1}^{j+1} \exp\left(p_i^{-1/2}\right).$$

Noting that $p_i \geq \log B$ for $i = 1, \cdots, j+1$, it follows that

$$\prod_{i=1}^{j+1}(1 + p_i^{-1/2}) \leq \exp\left((j+1)(\log B)^{-1/2}\right).$$

Hence, by (5.1.22), we have

$$\prod_{i=1}^{j+1}(1 + p_i^{-1/2}) \leq \exp\left(\frac{C_{18}(d)(\log B)^{1/2}}{\log \log B}\right),$$

so we obtain

$$\prod_{i=1}^{j+1} \#X_{p_i} \leq \mathcal{Q}_{j+1}^2 \exp\left(\frac{C_{19}(d)(\log B)^{1/2}}{\log \log B}\right), \tag{5.1.23}$$

where $C_{19}(d) = C_{17}(d)C_{18}(d)$. By (5.1.21), (5.1.23), and Theorem 4.0.1, it follows that:

$$\#Z(\mathcal{Q}_{j+1}) = O_d\left(\left(B^{2\psi} + \mathcal{Q}_{j+1}^2 \log^2 B \mathcal{Q}_{j+1}\right) \exp\left(\frac{C_{19}(d)(\log B)^{1/2}}{\log \log B}\right)\right). \tag{5.1.24}$$

We write $\Gamma^{(j+1)}$ to be the set of irreducible curves $\mathcal{C} \in \Gamma^{(j)}$ which are common irreducible components of $X \cap Y(P_1, \cdots, P_j)$ and $X \cap Y(P_1, \cdots, P_{j+1})$. For each curve $\mathcal{C} \in \Gamma^{(j+1)}$, we have

$$\deg \mathcal{C} = O_d\left(\mathcal{Q}_{j+1}^{-1} B^{\psi} \log B + \log B \mathcal{Q}_{j+1}\right).$$

By (5.1.18) and (5.1.24), we see that

$$\#Z(\mathcal{Q}_{t+1}) = O_{d,\varepsilon}\left(B^{2\psi+\varepsilon}(\log B)^2 \exp\left(\frac{C_{19}(d)(\log B)^{1/2}}{\log \log B}\right)\right) \tag{5.1.25}$$

We write $\Gamma = \Gamma^{(t+1)}$. If $\mathcal{C} \in \Gamma$, then the hypothesis of the first half of Theorem 4.0.1 applies, whence

$$\deg \mathcal{C} = O_{d,\varepsilon}(1).$$

We put the sets $Z(\mathcal{Q}_1), \cdots Z(\mathcal{Q}_{t+1})$ together to form the exceptional set:

$$\mathcal{E} = \bigcup_{j=1}^{t+1} Z(\mathcal{Q}_j).$$

Then (5.1.22) and (5.1.25) imply that:

$$\#\mathcal{E} = O_d\left(B^{2\psi+\varepsilon} \exp\left((\log B)^{1/2}/\log\log B\right)(\log B)^3(\log\log B)^{-1}\right). \tag{5.1.26}$$

We now turn our attention to the set Γ. Since $\#\Gamma$ does not exceed the number of irreducible components of $X \cap Y(\emptyset)$, it follows from (5.1.15) that

$$\#\Gamma = O_{d,\varepsilon}\left(B^{\psi+\varepsilon}\right). \tag{5.1.27}$$

By construction, it follows that

$$R(f; B^\beta, B) \leq \#\mathcal{E} + \#\bigcup_{\mathcal{C}\in\Gamma} \mathcal{C}(\mathbb{Q}; \mathbf{B}). \tag{5.1.28}$$

For $\mathcal{C} \in \Gamma$, $\mathcal{C}$ is a component of $Y(P_1, \cdots, P_{t+1})$ for some $(P_1, \cdots, P_{t+1})$. Moreover, since $\mathcal{Q}_{t+1} = p_1 \cdots p_{t+1}$ satisfies the hypothesis of part (a) of Theorem 4.0.1, it follows from Bézout's theorem that

$$\deg \mathcal{C} \leq \deg X \cdot \deg Y(P_1, \cdots, P_{t+1}) = O_{d,\varepsilon}(1). \tag{5.1.29}$$

Let G^* be a primitive form which defines $Y(P_1, \cdots, P_{t+1})$. By (5.1.16) and case a) of Theorem 4.0.1, we also have

$$\log\|G^*\| = \log(H(Y(P_1, \cdots, P_{t+1}))) = O_{d,\varepsilon}(\log B).$$

By following the same substitution as in (5.1.19), we obtain a form over $\mathbb{P}(1,1,2)$ by substituting (5.1.12) into G^*. We call the new polynomial $G(x,y,z)$. Observe that

$$\log\|G\| = \log\|G^*\| + O_d(l \log\|f\|).$$

We may now suppose that B is chosen sufficiently large so that $\log\|f\| < \log B$. Then we obtain

$$\log\|G\| = O_{d,\varepsilon}(\log B). \tag{5.1.30}$$

Note that the curve $\mathcal{C}$ corresponds naturally to a component $\mathcal{C}'$ of the curve $G(x,y,z)=0$. If $\mathcal{C}'$ is reducible, we consider each irreducible component separately, noting that there are at most $O_{d,\varepsilon}(1)$ components by Bézout's theorem and (5.1.29). Thus, we may consider each irreducible component $\mathcal{C}''$ of $\mathcal{C}'$. There are two situations. First, $\mathcal{C}''$ may be irreducible over $\mathbb{Q}$, but reducible over $\overline{\mathbb{Q}}$. In this case, the rational points on $\mathcal{C}''$ are preserved under the all elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, but $\mathcal{C}''$ has a conjugate which is also a component of $\mathcal{C}'$, whence $\mathcal{C}''(\mathbb{Q})$ corresponds to the rational points in the intersection of two curves each of degree $O_{d,\varepsilon}(1)$; so by Bézout's theorem, it follows that

$$\#\mathcal{C}''(\mathbb{Q}) = O_{d,\varepsilon}(1).$$

We suppose now that $\mathcal{C}$ corresponds to a $\mathbb{Q}$-defined and geometrically integral component of G, which we call $\mathcal{G}$. Hence we have

$$\mathcal{C} \leftrightarrow \mathcal{G}(x,y,z) = 0.$$

By Proposition B.7.3 in [62] and (5.1.30), we have

$$\log\|\mathcal{G}\| = O_{d,\varepsilon}\left(\log B\right).$$

We write

$$\mathcal{G}(x,y,z) = G_1(x,y) + zG_2(x,y,z),$$

where $G_1(x,y)$ consists of all monomials in $\mathcal{G}$ which only contains x and y. Observe that since $\mathcal{G} \in \mathbb{P}(1,1,2)$ that G_1 is homogeneous in x and y. We then consider several situations.

Let Γ_1 denote the set of curves $\mathcal{C} \in \Gamma$ such that $f(x,y)$ and $G_1(x,y)$ are coprime. If $xy=0$, say $y=0$, then

$$f(x,0) = a_d x^d = vz^k.$$

Since we have assumed that z is a prime by (5.1.10), it follows that we must have $z|a_d x^d$. However, since we assumed that $z \gg B^2(\log B)^{-1}$ and $B > \|f\|$, this is not possible. It follows that no point with $xy=0$ can lie in $X^{\beta}(\mathbb{Q};\mathbf{B})$. Write $f(x,y) = y^d f(x/y,1)$ and $G_1(x,y) = y^{\deg(G_1)}G_1(x/y,1)$. Further, write $h(x) = f(x,1)$ and $g(x) = G_1(x,1)$. There exist polynomials $a(x), b(x) \in \mathbb{Z}[x]$ and such that

$$a(x)h(x) + b(x)g(x) = \mathrm{Res}(h,g),$$

where $\mathrm{Res}(h,g)$ is the resultant of h and g, see [29]. Homogenizing the equation, we obtain

$$a'(x,y)f(x,y) + b'(x,y)G_1(x,y) = ny^e,$$

where e is the least positive integer such that the left hand side is a binary form.

Since $z|G_1(x,y)$ and $z|f(x,y)$, it follows that $z|ny^e$. However, recall from Section 5.1 that z is a prime not smaller than $B^2(\log B)^{-1}$, and since $y \in [1,B]$, it follows that $z|n$. The resultant $\mathrm{Res}(h,g)$ is bounded by

$$|\operatorname{Res}(h,g)| \leq (d+\deg \mathcal{G}+1)!(\|f\| \cdot \|\mathcal{G}\|)^{d+\deg \mathcal{G}+1}.$$

Hence, the number of prime divisors dividing n of size at least $B^2(\log B)^{-1}$ is at most

$$O\left(\frac{\deg \mathcal{G} \log\|\mathcal{G}\|}{\log B}\right) = O_{d,\varepsilon}(1). \tag{5.1.31}$$

We can now argue as in Greaves [48]. By (5.1.10), we have that z is in fact a prime. Thus, there are at most d solutions to the congruence

$$f(\omega,1) \equiv 0 \pmod{z}.$$

By (5.1.7), we have

$$f(x,y) \equiv 0 \pmod{z},$$

and since $xy \not\equiv 0 \pmod{z}$, there exists $\omega \neq 0$ such that $x \equiv \omega y \pmod{z}$. For each such ω, Lemma 1 in Greaves [48] gives that there are at most

$$\frac{B^2}{z} + O(B) = O(B)$$

such solutions. Thus for each z, there are at most $d \cdot O(B) = O_d(B)$ many points in $X^\beta(\mathbb{Q};\mathbf{B})$ corresponding to a point on a curve $\mathcal{C} \in \Gamma_1$. Since there are $O_\varepsilon(B^\varepsilon)$ choices for z and

$$O_{d,\varepsilon}\left(B^{\psi+\varepsilon}\right)$$

choices for $\mathcal{C} \in \Gamma_1$, it follows that

$$\#X^\beta(\mathbb{Q};\mathbf{B}) \cap \bigcup_{\mathcal{C}\in\Gamma_1} \mathcal{C} = O_{d,\varepsilon}\left(B^{\psi+1+\varepsilon}\right). \tag{5.1.32}$$

Next, consider the curves $\Gamma_2 \subset \Gamma$ consisting of those $\mathcal{C} \in \Gamma$ such that $f(x,y), G_1(x,y)$ are not co-prime. As we have chosen f to be irreducible, this implies that $f(x,y)$ divides $G_1(x,y)$. By our choice of $\mathcal{G}$, the degree of $\mathcal{G}$ is at least d and at most $O_{d,\varepsilon}(1)$. We write $l = \deg \mathcal{C} = \deg \mathcal{G}$. We calculate the corresponding quantities a_x, a_y, a_z with respect to the

monomial ordering $<$. Suppose that $x^{\alpha_x}y^{\alpha_y}z^{\alpha_z}$ is the leading monomial in $\mathcal{G}$ with respect to reverse lexicographic ordering. In particular, we must have

$$\alpha_x + \alpha_y + 2\alpha_z = l,$$

since $\mathcal{G}$ is a polynomial over $\mathbb{P}(1,1,2)$ of weighted degree l. Further, we have

$$a_x = \frac{l - \alpha_x}{2l},$$

$$a_y = \frac{l - \alpha_y}{2l},$$

and

$$a_z = \frac{l - 2\alpha_z}{4l}.$$

Hence,

$$\begin{aligned} B_x^{a_x} B_y^{a_y} B_z^{a_z} &= B^{\frac{1}{4}\left(\frac{(4+\beta)l - 2\alpha_x - 2\alpha_y - 2\beta\alpha_z}{l}\right)} \\ &= B^{\frac{1}{4}\left(\frac{(2+\beta)l + 2\alpha_z(2-\beta)}{l}\right)}. \end{aligned}$$

Write

$$\Psi = \frac{(2+\beta)l + 2\alpha_z(2-\beta)}{l^2}. \tag{5.1.33}$$

Observe that the W in Theorem 4.0.1 corresponds to the quantity B^{Ψ}.

Now we argue as in [53]. If $\mathbf{x} \in \mathbb{P}(1,1,2)$ is a singular point on $\mathcal{C}$, then $\mathbf{x}$ is a common zero of $\mathcal{G}$ and $\dfrac{\partial \mathcal{G}}{\partial x}$, hence $\mathbf{x}$ lies on the intersection

$$\mathcal{C} \cap \mathcal{C}',$$

where $\mathcal{C}'$ is the zero-locus of $\dfrac{\partial \mathcal{G}}{\partial x}$. By Bézout's theorem, the number of singular points on $\mathcal{C}$ is at most

$$O_{d,\varepsilon}(1). \tag{5.1.34}$$

It remains to consider non-singular points on $\mathcal{C}$. Suppose $\mathbf{z} \in \mathcal{C}^{\beta}(\mathbb{Q}; \mathbf{B})$ is non-singular, but reduces to a singular point modulo p for some prime p. Then, we must have p divides

$$\frac{\partial \mathcal{G}}{\partial x}(\mathbf{z}), \frac{\partial \mathcal{G}}{\partial y}(\mathbf{z}), \frac{\partial \mathcal{G}}{\partial z}(\mathbf{z}).$$

However, $\mathbf{z}$ is non-singular, so one of the partial derivatives above is non-zero. We may suppose, as we may, that $\dfrac{\partial \mathcal{G}}{\partial x}(\mathbf{z}) \neq 0$. Since

$$\left|\frac{\partial \mathcal{G}}{\partial x}(\mathbf{z})\right| \ll_d l\|\mathcal{G}\|B^{l-1},$$

it follows that

$$\#\left\{p > B^{\Psi+\varepsilon} : p|\frac{\partial \mathcal{G}}{\partial x}(\mathbf{z})\right\} \ll_{d,\varepsilon} \frac{l\log(\|\mathcal{G}\|B)}{\log 2 + \Psi \log B}.$$

Choose $C_{20}(d,\varepsilon)$ to be a number which depends on d, ε and gives an upper bound for the inequality above. Now set

$$n = \left\lceil \frac{C_{20}(d,\varepsilon) l \log(\|\mathcal{G}\|B)}{\log 2 + \Psi \log B} \right\rceil \ll \log B,$$

where the implied constant is absolute, and

$$q_1 < \cdots < q_n$$

to be the first n primes larger than $B^{\Psi+\varepsilon}$. Then there exists j with $1 \leq j \leq n$ such that $q_j \nmid \dfrac{\partial \mathcal{G}}{\partial x}(\mathbf{z})$, so $\mathbf{z}$ will reduce to a non-singular point on $\mathcal{C}_{q_j}$. By Theorem 4.0.1 and the theorem of Lang-Weil [74], there exist

$$R = O(nq_n) \ll_{d,\varepsilon} B^{\Psi+\varepsilon}$$

forms $\mathcal{G}_1, \cdots, \mathcal{G}_R$ of degree $O_{l,\varepsilon}(1) = O_{d,\varepsilon}(1)$, defining curves $\mathcal{Y}_1, \cdots, \mathcal{Y}_R$, such that $\mathcal{C} \not\subset \mathcal{Y}_j$ for $j = 1, \cdots, R$, and

$$\mathcal{C}^{\beta}_{\text{non-singular}}(\mathbb{Q}; \mathbf{B}) \subset \bigcup_{j=1}^{R} \mathcal{Y}_j.$$

By Bézout's Theorem, (5.1.34), and Theorem 4.0.1, we have the bound

$$\#\mathcal{C}^{\beta}(\mathbb{Q}; \mathbf{B}) = O_{d,\varepsilon}\left(B^{\frac{2+\beta}{l} + \frac{2\alpha_z(2-\beta)}{l^2} + \varepsilon}\right).$$

Further, we have

$$2 - \frac{\log\log B}{\log B} < \beta \leq \frac{d}{k} + \frac{\log(\|f\|d)}{\log B}.$$

If $\beta \geq 2$, then certainly

$$2 - \beta \leq 0,$$

hence

$$2\alpha_z(2-\beta) \le 0,$$

so we obtain the upper bound

$$\#\mathcal{C}^\beta(\mathbb{Q};\mathbf{B}) = O_{d,\varepsilon}\left(B^{\frac{2+\beta}{l}+\varepsilon}\right).$$

and if $\beta \le 2$, then

$$0 \le 2-\beta < \frac{\log\log B}{\log B}.$$

Therefore, we obtain

$$\begin{aligned} B^{\frac{2\alpha_z(2-\beta)}{\mathfrak{d}^2}} &\le B^{\frac{2\alpha_z(\log\log B/\log B)}{l^2}} \\ &= (\log B)^{\frac{2\alpha_z}{l^2}} \\ &\le (\log B)^{\frac{1}{l}}, \end{aligned}$$

as $2\alpha_z \le l$. This again implies that

$$\#\mathcal{C}^\beta(\mathbb{Q};\mathbf{B}) = O_{d,\varepsilon}\left(B^{\frac{2+\beta}{l}+\varepsilon}\right).$$

Since $l \ge d$ and $\beta \le d/k + \log(d\|f\|)/\log B$, it follows that

$$\#\mathcal{C}^\beta(\mathbb{Q};\mathbf{B}) = O_{d,\varepsilon}\left(B^{\frac{2}{d}+\frac{1}{k}+\varepsilon}\right).$$

Since $k \ge 2$, it follows that

$$\#\mathcal{C}^\beta(\mathbb{Q};\mathbf{B}) = O_{d,\varepsilon}\left(B^{\frac{2}{d}+\frac{1}{2}+\varepsilon}\right).$$

Combining these estimates, we obtain

$$\#X^\beta(\mathbb{Q};\mathbf{B}) \cap \bigcup_{\mathcal{C}\in\Gamma_2} \mathcal{C} = O_{d,\varepsilon}\left(B^\psi B^{\frac{2}{d}+\frac{1}{2}+\varepsilon}\right). \tag{5.1.35}$$

By (5.1.26), (5.1.27), (5.1.32), and (5.1.35), we have

$$\#X^\beta(\mathbb{Q};\mathbf{B}) = O_{d,\varepsilon}\left(B^{2\psi+\varepsilon} + B^{1+\psi+\varepsilon} + B^{\psi+\frac{2}{d}+\frac{1}{2}+\varepsilon}\right). \tag{5.1.36}$$

Since we may assume $d \ge 6$ by Greaves [48], we obtain

$$\#X^\beta(\mathbb{Q};\mathbf{B}) = O_{d,\varepsilon}\left(B^{2\psi+\varepsilon} + B^{1+\psi+\varepsilon}\right). \tag{5.1.37}$$

It remains to show that if $k/d > 7/18$ and β is in the range

$$2 - \frac{\log\log B}{\log B} < \beta \leq \frac{d}{k} + \frac{\log(\|f\|d)}{\log B},$$

then one can choose ε so that $\psi < 1$. Let us analyze the expression

$$\frac{d - k\beta}{d - 2k} + \frac{\beta}{2} \tag{5.1.38}$$

as a function of β. Its derivative is given by

$$\frac{-k}{d - 2k} + \frac{1}{2} = \frac{d - 4k}{2(d - 2k)},$$

which is negative whenever $k/d > 1/4$. Therefore, by (5.1.8), (5.1.38) viewed as a function of β, is decreasing. Thus, for any

$$0 < \eta < \frac{\log\log B}{\log B}$$

with

$$2 - \eta < \beta \leq 2,$$

we have

$$\begin{aligned}\frac{d - k\beta}{d - 2k} + \frac{\beta}{2} &\leq \frac{d - k(2 - \eta)}{d - 2k} + \frac{2}{2} \\ &= 2 + \frac{k\eta}{d - 2k} \\ &\leq 2 + \frac{k\log\log B}{(d - 2k)\log B}.\end{aligned}$$

Choose B sufficiently large so that

$$\left(\frac{2(d - 2k)}{d}\right)^{1/2} \frac{k\log\log B}{(d - 2k)\log B} < \varepsilon. \tag{5.1.39}$$

Let $\lambda = k/d$. Then, by (5.1.39), we have

$$\frac{1}{2}\left(2(1 - 2\lambda)^{1/2}\left(1 + \frac{d - 2k}{d - 2k} + \frac{2}{2}\right) + \varepsilon = \frac{3}{\sqrt{2}}\sqrt{1 - 2\lambda} + \varepsilon.\right.$$

To ensure that $\psi < 1$, we are left to consider the inequality

$$\frac{3\sqrt{1-2\lambda}}{\sqrt{2}} < 1.$$

This is equivalent to

$$1 - 2\lambda < \frac{2}{9},$$

which gives

$$\lambda > \frac{7}{18}.$$

Thus, whenever $k/d > 7/18$ and ε is sufficiently close to zero, we have $\psi < 1$. This completes the proof of Theorem 5.1.1, by virtue of (5.1.8).

5.2 Another proof of Browning's theorem

In this section, we give another proof of Browning's theorem in [21]. It illustrates the differences between our approaches to the determinant method. In [21], Browning combined elements of the "affine determinant method" introduced by Heath-Brown in [54] and Salberger's global determinant method in [93] to prove his result, which is stated below as Theorem 5.2.1. Heath-Brown had already shown in [54] that his affine determinant method could be applied to study integral points on the variety defined by

$$f(x) = yz^k,$$

where $f(x)$ is a polynomial with integral coefficients of degree d. More specifically, for irreducible $f(x) \in \mathbb{Z}[x]$ of degree d with no fixed k-th power divisor, Heath-Brown proved that f takes on infinitely many k-free values whenever $k \geq (3d+2)/4$. Browning improved on this slightly by showing that Salberger's arguments in [93] can be adopted to augment the affine determinant method to sharpen the above result to $k \geq (3d+1)/4$.

We show that our version of the determinant method, detailed in Sections 4.1 to 5.1.2, can also be used to obtain the same result. It is interesting that these two different versions of the determinant method lead to the same conclusion.

For convenience, we state Browning's theorem again:

Theorem 5.2.1. *(Browning, 2011) Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial of degree $d \geq 3$. Suppose that $k \geq (3d+1)/4$. Then, we have*

$$\#\{n \in \mathbb{Z} \cap [1, B] : f(n) \text{ is } k\text{-free}\} \sim c_{f,k} B$$

as $B \to \infty$, where $c_{f,k}$ is defined as in equation (5.1.5).

We first establish some preliminaries analogous to Section 5.1. Recall that we stated, in equation (5.1.6), the notation $N_{f,k}(B) = \#\{1 \leq x \leq B : f(x) \text{ is } k\text{-free}\}$. We define

$$N(f; b, B) = \#\{1 \leq x \leq B : b^k | f(x)\}.$$

From elementary properties of the Mobius function, we have

$$N_{f,k}(B) = \sum_{b=1}^{\infty} \mu(b) N(f; b, B).$$

We also have the formula

$$N(f; b, B) = \rho_f(b^k) \left(\frac{B}{b^k} + O(1) \right),$$

where as we recall, $\rho_f(m)$ counts the number of congruence classes modulo m for which f vanishes modulo m. Browning [21] obtains the estimate

$$\rho_f(b^k) = O(b^{\varepsilon})$$

whenever b is square-free, and so we obtain

$$N(f; b, B) = B \frac{\rho_f(b^k)}{b^k} + O(b^{\varepsilon}).$$

We thefore conclude that

$$N_{f,k}(B) = B \sum_{b \leq B^{1-\delta}} \frac{\mu(b)\rho_f(b^k)}{b^k} + \sum_{b > B^{1-\delta}} \mu(b) N(f; b, B) + o(B), \tag{5.2.1}$$

where δ is a small positive constant.

Define the quantity

$$E(\xi) = \#\{x \in \mathbb{Z} \cap [1, B] : \exists b > \xi \text{ s.t. } b^k | f(x) \text{ and } \mu^2(b) = 1\}$$

for any $\xi \geq 1$. Using the assumption of the theorem that $k > 3d/4 \geq 1$, we find

$$N_{f,k}(B) = c_{f,k} B + o(B) + O(E(B^{1-\delta})). \tag{5.2.2}$$

We now proceed with the proof of Theorem 5.2.1.

Proof. The discussion above essentially reduced the proof of Theorem 5.2.1 to obtaining a satisfactory upper bound for the quantity $E(B^{1-\delta})$. We first homogenize our polynomial f to obtain a binary form $F(x, y)$. As in the proof of Theorem 5.1.1, we write $H = B^{\beta}$, where

$$1 - \delta < \beta \ll d/k.$$

We then apply Theorem 4.0.1 with the weight vector $(1, 1, d-k, 1)$ and the box $\mathbf{B} = (B, 1, H, O(B^d/H^k))$ to the variety defined by

$$X : F(x, y) - vz^k = 0.$$

Note that this is a weighted projective surface. By Theorem 4.0.1 we obtain that all points counted by $E(B^{1-\delta})$ lie on an auxiliary curve $\mathcal{C}$ of degree

$$O_{d,\varepsilon}\left(B^{\frac{1}{2}\left(\frac{d-k}{d}\right)^{1/2}\left(\frac{d-k\beta}{d-k}+\beta\right)+\varepsilon}\right),$$

which assumes its maximum value at $\beta = 1 - \delta$. Then, as per our analysis in the binary form case in Section 5.1.2, we deduce that we can partition $\mathcal{C} \cap X$ into a collection of

$$O_{d,\varepsilon}\left(B^{\frac{1}{2}\left(\frac{d-k}{d}\right)^{1/2}\left(\frac{d-k\beta}{d-k}+\beta\right)+\varepsilon}\right)$$

geometrically irreducible curves Γ, and an exceptional set $\mathcal{E}$ consisting of

$$O_{d,\varepsilon}\left(B^{\left(\frac{d-k}{d}\right)^{1/2}\left(\frac{d-k\beta}{d-k}+\beta\right)+\varepsilon}\right)$$

points. By [63], we may assume that $d \geq 3$, and as we have shown in Section 5.1.2, the contribution from each irreducible curve $\mathcal{D} \in \Gamma$ is no more than

$$O_{d,\varepsilon}\left(B^{\frac{1}{3}+\varepsilon}\right),$$

hence it suffices to take d, k to satisfy

$$\left(\frac{d-k}{d}\right)^{1/2}\left(\frac{d-k\beta}{d-k}+\beta\right) < 1$$

for $\beta = 1 - \delta$, with $\delta > 0$ approaching zero. This is satisfied when $k/d > 3/4$, which is equivalent to $k \geq (3d+1)/4$. This completes the proof of Theorem 5.2.1. □

5.3 Representation of k-free numbers by binary forms

In this section, we give a proof of Theorem 5.1.2. Much of the argument remains unchanged from that given in [99].

Let A be a positive real number. For any value $0 < \theta \leq 1$ and for any non-zero integer h, let us write

$$\mathfrak{s}(h) = \prod_{\substack{p \leq A^{\theta} \\ |h|_p^{-1} \leq A^{\theta} \\ p \nmid \mathfrak{D}}} |h|_p^{-1},$$

where $\mathfrak{D}$ denotes the discriminant of f. Write U to be the set of pairs $(a, b) \in \mathbb{Z}^2$ such that $f(a, b) \neq 0$ and the only primes dividing $\gcd(a, b)$ are those that divide $\mathfrak{D}$. Now, define

$$S(\theta, A) = \prod_{(a,b) \in U} \mathfrak{s}(f(a, b)).$$

One can estimate $S(\theta, A)$ in exactly the same way as in [99] (note that in [99], they wrote u instead of A). In particular, by Section 6 of Stewart-Top [99], we have the estimate

$$S(\theta, A) \leq A^{5\theta d A^2}.$$

As a consequence, we see that the number of pairs $(a, b) \in U$ such that $|\mathfrak{s}(f(a, b))| \geq A^{1/8}$ is at most $40\theta d A^2$. Now, we may argue as in Lemma 2 of [40] that if h and b are integers such that $|h| \leq A^{1/2}$ and $1 \leq b \leq A$, then there are at most d integers a with $f(a, b) = h$. Hence, the number of pairs of integers (a, b) with $1 \leq a, b \leq A$ and $|f(a, b)| \leq A^{1/2}$ is at most

$$3dA^{3/2}.$$

Set $\theta = C_{f,k}/120d$. Define T to be the set of integers (a, b) with $1 \leq a, b \leq A$, $f(a, b)$ is k-free, $|f(a, b)| \geq A^{1/2}$, and $\mathfrak{s}(f(a, b)) < A^{1/8}$. By Theorem 5.1.1 and our choice of θ, we have that there exist constants $C_{22}, C_{23} > 0$, which depend on f and k, such that whenever $A > C_{22}$, we have

$$\#T > \frac{1}{2} C_{23} A^2. \tag{5.3.1}$$

We invoke the work of Stewart in [98] on estimating the number of solutions to Thue equations. Recall that for any integer h, $\omega(h)$ denotes the number of distinct prime factors of h. Let h be an integer for which there exists $(a, b) \in T$ such that

$$f(a, b) = h. \tag{5.3.2}$$

Write $h = \mathfrak{s}(f(a,b)) \cdot g$. Since by assumption we have $\mathfrak{s}(f(a,b)) \leq A^{1/8}$ and $|f(a,b)| \geq A^{1/2}$, it follows that $|\mathfrak{s}(f(a,b))| \leq |h|^{1/4}$ and consequently, $|g| \geq |h|^{3/4}$. If A is chosen to be greater than $|\mathfrak{D}|^{24}$ and $|h| \geq |\mathfrak{D}|^{12}$, then choosing $\varepsilon = 1/12$ and applying Corollary 1 of [**?**] we obtain that the number of solutions to equation (5.3.2) is at most

$$5600d^{1+\omega(g)}.$$

Observe that trivially we have the bound

$$|f(a,b)| \leq d\|f\|A^d. \tag{5.3.3}$$

Note that by construction, the prime divisors of g either divide $\mathfrak{D}$ or satisfy $|f(a,b)|_p^{-1} \geq A^\theta$. Hence, by choosing A so that $A^\theta \geq d\|f\|$, we have

$$\omega(g) \leq \omega(\mathfrak{D}) + (d+1)/\theta.$$

The second term on the right hand side in the above equation is from the worst case, where each prime p such that $|f(a,b)|_p^{-1} \geq A^\theta$ divides $f(a,b)$ with multiplicity one. If there are more than $(d+1)/\theta$ of such primes, then we will have $|f(a,b)| \geq A^{\theta\cdot(d+1)/\theta} = A^{d+1}$, which yields a contradiction to equation (5.3.3) as we chose $A \geq A^\theta \geq d\|f\|$. Hence, there exist constants C_{24}, C_{25} such that if $A > C_{24}$, then the number of distinct pairs $(a,b) \in T$ is at least $C_{25}A^2$.

To finish the proof of the theorem, let B be a real number with $B > d\|f\|C_{24}^d$ and write $A = (B/d\|f\|)^{1/d}$. Note that $A > C_{24}$. With this choice of A, we have that whenever $(a,b) \in T$, we have $|f(a,b)| \leq B$. Hence,

$$R_k(B) \geq \#T \geq C_{25}(B/d\|f\|)^{2/d},$$

which completes the proof of Theorem 5.1.2.

5.4 Del Pezzo surfaces of degree 2

In this section, we will prove the first part of Theorem 1.0.6. The main tool used will be Theorem 4.5.5. Recall that a del Pezzo surface of degree 2 is given by an equation of the form

$$y^2 = f(x_1, x_2, x_3), \tag{5.4.1}$$

where f is a quartic binary form. This variety naturally lives in the weighted projective space $\mathbb{P}_{\mathbb{Q}}(1,1,1,2)$. Let us denote the surface defined by (5.4.1) by X. We consider the vector

$$\mathbf{B} = (B, B, B, B^2)$$

for a positive real number B, which we think of as a parameter tending to infinity. We use the monomial order induced by choosing y^2 as the largest monomial in (5.4.1). Then we have

$$W = \left(B^{\frac{1}{3}} B^{\frac{1}{3}} B^{\frac{1}{3}} B^{\frac{4-2(2)}{24}}\right)^{\frac{3}{2}\left(\frac{2}{4}\right)^{1/2}} = B^{\frac{3}{2\sqrt{2}}}.$$

Let us now compute the trading ratio. One observes that the monomials

$$x_1^2, x_2^2, x_3^2, x_1x_2, x_1x_3, x_2x_3, y$$

are all of weighted degree 2, and they are $\mathbb{Q}$-linearly independent over X since the degree of X is 4. Further, there are seven of them, which exceeds $\binom{2+2}{2} = 6$. Hence the trading ratio is $3/2$. We then have

$$g(4,2,2) = \frac{4}{(3/2)2} = \frac{4}{3},$$

and

$$\mathfrak{S}(4,2,2) = \left(\frac{2}{4}\right)^{1/2}\left(\frac{4}{3}(2-1) + \frac{3}{2}\right) = \frac{17}{6\sqrt{2}}.$$

Hence we have

$$W^{2/\mathfrak{S}(4,2,2)} = B^{\frac{18}{17}}.$$

Observe that X is non-singular, by the Jacobian criterion. Hence, we may use Theorem 4.5.5, which counts non-singular points in $X(\mathbb{Q};\mathbf{B})$, to count the number of all points in $X(\mathbb{Q};\mathbf{B})$. The subset $X^{(1)}(\mathbb{Q};\mathbf{B})$ which consists of points in $X(\mathbb{Q};\mathbf{B})$ satisfying (d)-(1) is contained in the union of a collection $\mathcal{Z}^{(1)}$ of co-dimension two subvarieties of X, where if $Z \in \mathcal{Z}^{(1)}$, then

$$\deg Z \leq dD(\varepsilon)^2$$

by the theorem of Bezout. Further, we have

$$\#\mathcal{Z}^{(1)} = O_\varepsilon\left((p_0 \cdots p_t)^2\right) = O_\varepsilon\left(B^{\frac{36}{17}+6\varepsilon}\right).$$

Therefore, it follows that

$$\#X^{(1)}(\mathbb{Q};\mathbf{B}) \leq \# \bigcup_{Z \in \mathcal{Z}^{(1)}} \deg Z = O_\varepsilon\left(B^{\frac{36}{17}+6\varepsilon}\right).$$

The subset $X^{(2)}(\mathbb{Q};\mathbf{B})$ consisting of points $\mathbf{x} \in X(\mathbb{Q};\mathbf{B})$ satisfying (d)-(2) can be treated similarly.

It remains to treat the subset $X^{(3)}(\mathbb{Q};\mathbf{B})$ of $X(\mathbb{Q};\mathbf{B})$ satisfying (d)-(3). In this case, we consider two further sub-cases. In the first sub-case, we have $\mathbf{x}$ reduces to a singular point on Z. This case is easy to address because then $\mathbf{x}$ is forced to lie on a co-dimension one subvariety of Z, and the size of this set is bounded by $\deg Z \leq dD(\varepsilon)$. It suffices to consider the second sub-case, where $\mathbf{x}$ reduces to a non-singular point P_i on Z_{p_i} for $i = 1, \cdots, t$.

Recall that Z is a component of $X \cap Y(\mathbf{B}, P_1, \cdots, P_t)$. Let us consider an equation defining $Y = Y(\mathbf{B}, P_1, \cdots, P_t)$, say

$$\mathcal{G}(x_1, x_2, x_3, y) = 0. \tag{5.4.2}$$

We can further assume that $\mathcal{G}$ is a *primitive* form. By making use of (5.4.1), we can write (5.4.2) as

$$\mathcal{G}(x_1, x_2, x_3, y) = \mathcal{G}_1(x_1, x_2, x_3) + y\mathcal{G}_2(x_1, x_2, x_3) = 0.$$

This can be re-arranged to give

$$\mathcal{G}_1(x_1, x_2, x_3) = -y\mathcal{G}_2(x_1, x_2, x_3),$$

and if we square both sides of the equation and make use of (5.4.1) again, we obtain an equation of the form

$$\mathcal{G}_1^2(x_1, x_2, x_3) = \mathcal{G}_3(x_1, x_2, x_3),$$

which defines a curve in $\mathbb{P}^2_{\mathbb{Q}}$. Therefore, we can think of Z as a component of this curve, and so can be defined by a homogeneous equation. Indeed, suppose that Z is given by the equation

$$G(x_1, x_2, x_3) = 0. \tag{5.4.3}$$

Again, we insist that G is a primitive form. Since $\deg Z$ is bounded solely in terms of ε, we can apply Theorem 4.5.5 to Z and see that $Z(\mathbf{B}, P_1, \cdots, P_t)$ is contained in another curve Z' which does not contain Z of degree bounded solely in terms of ε. By Bézout's theorem, it follows that

$$\#Z(\mathbf{B}, P_1, \cdots, P_t) = O_\varepsilon(1).$$

Therefore, it follows that

$$\#X^{(3)}(\mathbb{Q};\mathbf{B}) = O_\varepsilon\left((p_1 \cdots p_t)^2 \# \bigcup_{Z \in \mathcal{Z}^{(3)}} Z(\mathbf{B}, P_1, \cdots, P_t)\right) = O_\varepsilon\left(B^{\frac{36}{17}+4\varepsilon}\right).$$

On re-adjusting our definition of ε if necessary, we therefore see that

$$N_X(B) = \#X(\mathbb{Q}; \mathbf{B}) = \sum_{j=1}^{3} \#X^{(j)}(\mathbb{Q}; \mathbf{B}) = O_\varepsilon\left(B^{\frac{36}{17}+\varepsilon}\right).$$

References

[1] S. Akhtari, *Upper bounds for the number of solutions to quartic Thue equations* International Journal of Number Theory, (2) **8** (2012), 335-360.

[2] S. Akhtari, *Representation of small integers by binary forms* To appear in Q.J.Math, Oxford.

[3] T. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, 1998.

[4] E. A. Bartolo, J. Martin-Morales, J. Ortigas-Galindo, *Q-Resolutions and intersection numbers*, Monografas Matemticas Garca de Galdeano **vv**, 1-10.

[5] M. A. Bean, *An isoperimetric inequality for the area of plane regions defined by binary forms*, Compositio Mathematica, (2) **92** (1994), 115-131.

[6] M. A. Bean, *The practical computation of areas associated with binary quartic forms*, Mathematics of Computation, (66) **219** (1997), 1269-1293.

[7] M. Beltramettii, L. Robbiano, *Introduction to the theory of weighted projective spaces*, Expo. Math, **4** (1986), 111-162.

[8] M. A. Bennett, S. R. Dahmen, *Klein forms and the generalized superelliptic equation*, Annals of Mathematics (1) **177** (2013), 177-239.

[9] M. A. Bennett, N. P. Dummigan, T. D. Wooley, *The representation of integers by binary additive forms*, Compositio Mathematica **111** (1998), 15-33.

[10] M. Bhargava, *Most hyperelliptic curves over $\mathbb{Q}$ have no rational points*, arXiv:1308.0395 [math.NT], http://arxiv.org/abs/1308.0395, retrieved 03 Dec 2014.

[11] M. Bhargava, *The geometric sieve and the density of squarefree values of invariant polynomials*, arXiv:1402.0031 [math.NT] https://arxiv.org/abs/1402.0031, retrieved 07 Jun 2016.

[12] M. Bhargava, A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Annals of Mathematics **181** (2015), 191-242.

[13] M. Bhargava, A. Yang, *On the number of binary n-ic forms with bounded Julia invariant*, arXiv:1312.7339 [math.NT] http://arxiv.org/abs/1312.7339

[14] E. Bombieri, J. Pila, *The number of integral points on arcs and ovals*, Duke Mathematical Journal, (2) **59** (1989), 337-357.

[15] E. Bombieri, W. Schmidt, *On Thue's equation*, Invent. Math. **88** (1987), 69-81.

[16] E. Bombieri, J. Vaaler, *On Siegel's lemma*, Inventiones Mathematicae, **73** (1983), 11-32.

[17] S. Boissire, A. Sarti, *Counting lines on surfaces*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (5) **6** (2007), 39-52.

[18] N. Broberg, *A note on a paper by R. Heath-Brown: "The density of rational points on curves and surfaces"*, J. reine angew. Math. **571** (2004), 159-178.

[19] T. D. Browning, *Equal sums of two kth powers*, J. Number Theory **96** (2002), 293-318.

[20] T. D. Browning, *Quantitative Arithmetic of Projective Varieties*, Progress in Mathematics, **277** (2009).

[21] T. D. Browning, *Power-free values of polynomials*, Arch. Math. (2) **96** (2011), 139-150.

[22] T. D. Browning, D. R. Heath-Brown, P. Salberger, *Counting rational points on algebraic varieties*, Duke Mathematical Journal, (3) **132** (2006), 545-578.

[23] T. D. Browning, M. Swarbrick Jones, *Counting rational points on del Pezzo surfaces with a conic bundle structure*, Acta Arithmetica **163** (2014), 271-298.

[24] J. Buchmann, U. Vollmer, *Binary Quadratic Forms: An Algebraic Approach*, Springer-Verlag, New York, Berlin, 2007.

[25] D. A. Buell, *Binary Quadratic Forms: Classical Theory and Modern Computations*, Springer-Verlag, New York, Berlin, 1989.

[26] P. F. Byrd, M. D. Friedman, *Handbook of Elliptic Integrals for Engineers and Scientists*, Second Edition, Revised, Springer-Verlag 1971.

[27] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication*, John Wiley and Sons, Hoboken, 1989.

[28] D. A. Cox, J. B. Little, D. O'Shea, *Using Algebraic Geometry*, Revised Second Edition (2005), Springer-Verlag.

[29] D. A. Cox, J. B. Little, D. O'Shea, *Ideals, Varieties, and Algorithms*, Third Edition (2007), Springer-Verlag.

[30] D. A. Cox, J. B. Little, H. K. Schenck *Toric Varieties*, Graduate Studies in Mathematics, **124** (2011), American Mathematical Society.

[31] J. Cremona, *Reduction of binary cubic and quartic forms*, LMS J. Comput. Math. **2** (1999), 64-94.

[32] J. E. Cremona, T. A. Fisher, *On the equivalence of binary quartics*, Journal of Symbolic Computation, **44** (2009), 673–682

[33] P. Davis, *Gamma function and related functions*, Handbook of Mathematical Functions (M. Abramowitz and I. Stegun, eds.), Dover Publications, New York, 1965.

[34] R. Dietmann, O. Marmon, *The density of twins of k-free numbers*, Bull. London Math.Soc., **46** (2014), 818-826.

[35] R. Dietmann, O. Marmon, *Random Thue and Fermat equations*, Acta. Arith., **167** (2015), 189-200.

[36] I. Dolgachev, *Weighted projective varieties*, Group Actions and Vector Fields (1982), Springer.

[37] D. Eisenbud, J. Harris, *The Geometry of Schemes*, (2000), Springer-Verlag.

[38] T. Ekedahl, *An effective version of Hilbert's irreducibility theorem*, Seminaire de Theorie des Nombres, Paris 1988-1989, 241-249, Progr. Math., 91, Birkhauser Boston, Boston, MA, 1990.

[39] P. Erdős, *Arithmetical properties of polynomials*, J. London Math. Soc. **28** (1953), 416-425.

[40] P. Erdős, K. Mahler, *On the number of integers which can be represented by a binary form*, J. London Math. Soc, **13** (1938), 134-139.

[41] T. Estermann, *Einige Satze uber quadratfeie Zahlen*, Math. Ann., **105** (1931), 653-662.

[42] J-H. Evertse, *The number of solutions of decomposable form equations*, Inventiones Mathematicae **122** (1995), 559-601.

[43] M. Filaseta, *Powerfree values of binary forms*, Journal of Number Theory **49** (1994), 250-268.

[44] W. Fulton, *Intersection Theory*, Springer-Verlag 1984.

[45] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801.

[46] F. Q. Gouvêa, B. Mazur, *The square-free sieve and the rank of elliptic curves*, Journal of the American Mathematical Society (1) **4** (1991), 1-23.

[47] A. Granville, *ABC allows us to count squarefrees*, International Mathematics Research Notices, **9** (1998).

[48] G. Greaves, *Power-free values of binary forms*, Q. J. Math, (2) **43** (1992), 45-65.

[49] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford Univ. Press, 1979.

[50] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics **52** (1977), Springer-Verlag.

[51] R. Hartshorne, *Deformation Theory*, Graduate Texts in Mathematics **257** (2010), Springer-Verlag.

[52] D. R. Heath-Brown, *Primes represented by* $x^3 + 2y^3$, Acta Mathematica **186** (2001), 1-84.

[53] D. R. Heath-Brown, *The density of rational points on curves and surfaces*, The Annals of Mathematics (2) **155** (2002), 553-598.

[54] D. R. Heath-Brown, *Counting rational points on algebraic varieties*, Analytic number theory, 5195, Lecture Notes in Math., 1891, Springer, Berlin, 2006.

[55] D. R. Heath-Brown, *Sums and differences of three k-th powers*, Journal of Number Theory, **129** (2009), 1579-1594.

[56] D. R. Heath-Brown, *Square-free values of* $n^2 + 1$, Acta. Arith.,

[57] D. R. Heath-Brown, *Powerfree values of polynomials*, Q. J. Math, (2) **64** (2013), 177-188.

[58] D. R. Heath-Brown, B. Z. Moroz, *Primes represented by binary cubic forms*, Proc. London Math. Soc. (2) **84** (2002), 257-288.

[59] H. A. Helfgott, *On the square-free sieve*, Acta Arithmetica, **115** (2004), 349-402.

[60] H. A. Helfgott, *Power-free values, large deviations and integer points on irrational curves*, J. Thor. Nombres Bordeaux **19** (2007), 433-472.

[61] H. A. Helfgott, *Square-free values of* $f(p)$*,* f *cubic*, Acta Math. (1) **213** (2014), 107-135.

[62] M. Hindry, J. Silverman, *Diophantine Geometry: An Introduction*, (2000), Springer-Verlag.

[63] C. Hooley, *On the power free values of polynomials*, Mathematika **14** (1967), 21-26.

[64] C. Hooley, *On binary cubic forms*, J. reine angew. Math. **226** (1967), 30-87.

[65] C. Hooley, *On the numbers that are representable as the sum of two cubes*, J. reine angew. Math. **314** (1980), 146-173.

[66] C. Hooley, *On another sieve method and the numbers that are a sum of two* h^{th} *powers*, Proc. London Math. Soc. **43** (1981), 73-109.

[67] C. Hooley, *On another sieve method and the numbers that are a sum of two* h^{th} *powers. II*, J. reine angew. Math. **475** (1996), 55-75.

[68] C. Hooley, *On binary quartic forms*, J. reine angew. Math. **366** (1986), 32-52.

[69] C. Hooley, *On binary cubic forms: II*, J. reine angew. Math. **521** (2000), 185-240.

[70] C. Hooley, *On the power-free values of polynomials in two variables*, Analytic number theory, 235-266, Camb. Univ. Press, 2009.

[71] C. Hooley, *On the power-free values of polynomials in two variables: II*, Journal of Number Theory, **129** (2009), 1443-1455.

[72] S. Janson, *Invariants of polynomials and binary forms*, arXiv:1102.3568 [math.HO], http://arxiv.org/abs/1102.3568

[73] F. Klein, *Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree*, Dover, New York, 1956 (revised edition).

[74] S. Lang, A. Weil, *Number of points of varieties over finite fields*, American Journal of Mathematics, (4) **76** (1954), 819-827.

[75] O. Marmon, *A generalization of the Bombieri-Pila determinant method*, Proceedings of the HIM trimester on Diophantine equations, Journal of Mathematical Sciences **171** (2010), 736-744.

[76] O. Marmon, *The density of integral points on hypersurfaces of degree at least four*, Acta. Arith. **141** (2010), 211-240.

[77] O. Marmon, *Sums and differences of four k-th powers*, Monatshefte fur Mathematik, (1) **164** (2011), 55-74.

[78] D. MacLagan, *Notes on Hilbert schemes*, http://homepages.warwick.ac.uk/staff/D.Maclagan/papers/HilbertSchemesNotes.pdf.

[79] K. Mahler, *Zur Approximation algebraischer Zahlen. I. (Uber den grossten Primteiler binarer Formen)*, Math. Ann. **107** (1933), 691-730.

[80] D. Mumford, *The Red Book of Varieties and Schemes*, Lect. Notes Math., **1358**, Springer-Verlag, 1988.

[81] R. Murty, H. Pasten, *Counting square free values of polynomials with error term*, International Journal of Number Theory, (7) **10** (2014), 1743-1760.

[82] M. Nair, *Power free values of polynomials*, Mathematika **23** (1976), 159-183.

[83] M. Nair, *Power free values of polynomials II*, Proceedings of the London Mathematical Society (3) **38** (1979), 353-368.

[84] M. Newman, *Integral matrices*, Pure and Appl. Math. (S. Eilenberg and P.A.Smith, eds.), vol.45, Academic Press, New York, 1972.

[85] P. J. Olver, *Classical Invariant Theory*, London Mathematical Society Student Texts **44**, Cambridge University Press (1999).

[86] B. Poonen, *Squarefree values of multivariate polynomials*, Duke Math. J., (2) **118** (2003), 353-373.

[87] J. Pila, *Integer points on the dilation of a subanalytic surface*, Q.J. Math., (2) **55** (2004), 207-223.

[88] M. Reid, *Graded rings and varieties in weighted projective space*, http://homepages.warwick.ac.uk/~masda/surf/more/grad.pdf.

[89] T. Reuss, *Power-free values of polynomials*, preprint.

[90] G. Ricci, *Riecenche aritmetiche sui polynomials*, Rend. Circ. Mat. Palermo **57** (1933), 433-475.

[91] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math., (1) **6** (1962), 64-94.

[92] P. Salberger, *On the density of rational and integral points on algebraic varieties*, J. reine angew. Math. **606** (2007), 123-147.

[93] P. Salberger, *Counting rational points on projective varieties*, Preprint 2009.

[94] P. Salberger, *Uniform bounds for rational points on cubic hypersurfaces*, Preprint 2015.

[95] W. M. Schmidt, *The number of solutions of norm form equations*, Transactions of the American Mathematical Society, (1) **317** (1990), 197-227.

[96] C. Skinner, T. D. Wooley, *Sums of two k-th powers*, J. reine angew. Math. **462** (1995), 57-68.

[97] R. Stanley, *Some restricted weighted sums*. MathOverflow, 2012. URL (accessed on 2014-05-22): http://mathoverflow.net/questions/90381/some-restricted-weighted-sums.

[98] C. L. Stewart, *On the number of solutions of polynomial congruences and Thue equations*, Journal of the American Mathematical Society, (4) **4** (1991), 793-835.

[99] C. L. Stewart, J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, Journal of the American Mathematical Society, (4) **8** (1995), 943-972.

[100] C. L. Stewart, S. Y. Xiao, *On the representation of integers by binary forms*, arXiv:1605.03427 [math.NT], http://arxiv.org/abs/1605.03427 .

[101] A. Thue, *Uber Annaherungswerte algebraischer Zahlen.* J. reine angew. Math, **135** (1909), 284-305.

[102] J. L. Thunder, *Decomposable form inequalities*, Annals of Mathematics (3) **153** (2001), 767-804.

[103] M. Walsh, *Bounded rational points on curves*, Int Math Res Notices, (2014),

[104] T. D. Wooley, *Sums of two cubes*, Int. Math. Res. Notices. **4** (1995), 181-185.

[105] S. Y. Xiao, *Power-free values of binary forms and the global determinant method*, arXiv:1505.05587 [math.NT] http://arxiv.org/abs/1505.05587.

[106] S. Y. Xiao, *On binary cubic and quartic forms*, Preprint.

[107] S. Y. Xiao, S. Yamagishi, *Zeroes of polynomials in many variables with prime inputs*, arXiv:1512.01258 [math.NT] http://arxiv.org/abs/1512.01258.