Counting Rational Points, Integral Points, Fields, and Hypersurfaces

Joseph Gunther

The Graduate Center, City University of New York

How does access to this work benefit you? Let us know!

Follow this and additional works at: http://academicworks.cuny.edu(gc_etds

Part of the Algebraic Geometry Commons, and the Number Theory Commons

Recommended Citation

http://academicworks.cuny.edu(gc_etds/2064

This Dissertation is brought to you by CUNY Academic Works. It has been accepted for inclusion in All Graduate Works by Year: Dissertations, Theses, and Capstone Projects by an authorized administrator of CUNY Academic Works. For more information, please contact deposit@gc.cuny.edu.
Counting rational points, integral points, fields, and hypersurfaces

by

Joseph William Gunther

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

2017
This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirements for the degree of Doctor of Philosophy.

Lucien Szpiro

Date

Chair of Examining Committee

Ara Basmajian

Date

Executive Officer

Lucien Szpiro (Chair)

Aise Johan de Jong

Alexander Gamburd

Victor Kolyvagin

Andrew Obus

THE CITY UNIVERSITY OF NEW YORK
Abstract

Counting rational points, integral points, fields, and hypersurfaces

by

Joseph William Gunther

Advisor: Lucien Szpiro

This thesis comes in four parts, which can be read independently of each other.

In the first chapter, we prove a generalization of Poonen’s finite field Bertini theorem, and use this to show that the obvious obstruction to embedding a curve in some smooth surface is the only obstruction over perfect fields, extending a result of Altman and Kleiman. We also prove a conjecture of Vakil and Wood on the asymptotic probability of hypersurface sections having a prescribed number of singularities.

In the second chapter, for a fixed base curve over a finite field of characteristic at least 5, we asymptotically count its degree three covers of given genus, as the genus increases. This gives an algebro-geometric proof of results of Datskovsky and Wright, as well as Bhargava, Shankar, and Wang, on asymptotically counting cubic field extensions.

In the third chapter, for $D$ a non-empty effective divisor on $\mathbb{P}^1$, we show that any set of $(D, S)$-integral points of bounded degree has relative density zero. We then apply this to arithmetic dynamics: let $\varphi(z) \in \overline{\mathbb{Q}}(z)$ be a rational function of degree at least two whose second iterate is not a polynomial. We show that as we vary over points $P \in \mathbb{P}^1(\overline{\mathbb{Q}})$ of bounded degree, the number of algebraic integers in the forward orbit of $P$ is absolutely bounded and zero on average.
In the fourth chapter, we count algebraic numbers. Masser and Vaaler have given an asymptotic formula for the number of algebraic numbers of given degree $d$ and increasing height. This problem was solved by counting lattice points (which correspond to minimal polynomials over $\mathbb{Z}$) in a homogeneously expanding star body in $\mathbb{R}^{d+1}$. The volume of this star body was computed by Chern and Vaaler, who also computed the volume of the codimension-one “slice” corresponding to monic polynomials – this led to results of Barroero on counting algebraic integers. We show how to estimate the volume of higher-codimension slices, which allows us to count units, algebraic integers of given norm, trace, norm and trace, and more. We also refine the lattice point-counting arguments of Chern-Vaaler to obtain explicit error terms with better power savings, which lead to explicit versions of some results of Masser-Vaaler and Barroero. Our results can be interpreted as counting rational points and integral points on $\mathbb{P}^d$. 
Acknowledgements

Material from the first chapter has previously appeared in an article in *Journal of Pure and Applied Algebra*. The third chapter represents joint work with Wade Hindes, which will appear in *Proceedings of the AMS*. The fourth chapter represents joint work with Robert Grizzard, which will appear in *Algebra & Number Theory*.

The support of my advisor, Lucien Szpiro, has been a source of encouragement throughout my time in graduate school. While I wandered pretty far off on my own mathematically, he was always happy to talk when I’d report back, and his vision and love of mathematics has been an inspiration.

Within CUNY, I’ve benefited from discussions with Wade Hindes, Ray Hoobler, and Jonah Leshin. (Thanks again for forwarding that email, Wade!) I would especially like to thank Alice Medvedev for her friendship and mentorship.

Johan de Jong was always willing to talk through ideas when I’d head up to Columbia and knock on his office door. I thank him for his generosity, enthusiasm, and rigor.

Graduate school would have been radically different, and far duller, without long conversations with my fellow graduate students, Joe Kramer-Miller and Lloyd West. During my semester at Wisconsin, I spent countless hours camped out in Bobby Grizzard’s office, devouring his candy and happily talking math.

I benefited from discussing this work with several mathematicians outside of CUNY, including Antoine Chambert-Loir, Nathan Clement, Moisés Herradón Cueto, Daniel Hast,
Aaron Levin, and Vlad Matei. Ravi Vakil helped put me on the scent of Chapter 2 and
more with an inspiring Arizona Winter School lecture series and project. Jordan Ellenberg
and David Zureick-Brown were sources of mathematical inspiration, kind advice, and music
recommendations.

Most of all, I am deeply grateful to Melanie Matchett Wood for her encouragement,
support, and mathematical guidance during my final two years of graduate school.

This thesis would not have been written without the love and support of my wonderful
family: Susie, Da, and Kitty. And lastly, thanks to everyone who made these years in New
York so incredible for me, especially Katy, Maria, Kate, Stu, Kaleigh, Will, Kat, Andrew,
John, and Miki.


### Contents

1. **Random hypersurfaces and embedding curves in surfaces over finite fields**  
   1.1 Introduction .......................................................... 1  
   1.2 Notation and conventions .......................................... 6  
   1.3 Embedding dimension theorem .................................... 7  
   1.4 The probability of a hypersurface section having a given number of singularities 13

2. **Counting cubic curve covers over finite fields**  
   2.1 Introduction .......................................................... 14  
   2.2 Vector bundles and ruled surfaces ................................ 15  
   2.3 Parametrization of cubic covers .................................. 18  
   2.4 Counting cubic covers ........................................... 23

3. **Integral points of bounded degree on \( \mathbb{P}^1 \) and in dynamical orbits**  
   3.1 Introduction .......................................................... 29  
   3.2 Notation and previous results ..................................... 33  
   3.3 Finiteness of integral images ...................................... 36  
   3.4 Upper bounds for orbits .......................................... 37  
   3.5 The relative density of integral points .......................... 38

4. **Slicing the stars: counting algebraic numbers, integers, and units of bounded**
degree and height

4.1 Introduction ................................................. 42
4.2 The unit star body ........................................... 53
4.3 Counting principles .......................................... 60
4.4 Volumes of slices of star bodies ............................ 61
4.5 Lattice points in slices: proof of Theorem 4.1.11 ......... 69
4.6 Proofs of Theorem 4.1.1 and corollaries ................. 70
4.7 Counting polynomials: explicit bounds .................. 72
4.8 Counting monic polynomials: explicit bounds .......... 76
4.9 Lattice points in slices: explicit bounds ................ 79
4.10 Reducible and imprimitive polynomials ................. 85
4.11 Explicit results ............................................. 94

Appendices

A Combinatorial estimates ...................................... 101

Bibliography ...................................................... 106
Chapter 1

Random hypersurfaces and embedding curves in surfaces over finite fields

1.1 Introduction

Poonen’s geometric closed point sieve was first introduced in [Poo04] to prove a finite field version of the classical Bertini smoothness theorem. The sieve has since been applied and adapted to a range of subjects, including point-counting distributions within families of curves [BDFL10, BK12, EW15] and arithmetic dynamics [Poo13]. In this chapter, we use it to prove embedding results for quasi-projective schemes over finite fields, as well as to prove a hypersurface stabilization conjecture of Vakil and Wood.

Given a curve, when does there exist some smooth surface into which it can be embedded? There is an obvious requirement: the curve must have no more than two tangent directions at any point, since this would be true on an ambient smooth surface. Altman and Kleiman proved that over an infinite perfect field, this local obstruction is the only obstruction [KA79]. In this chapter we prove the same for finite fields, thus removing their infinite hypothesis. The result follows from Corollary 1.1.3 of the following theorem. (Each $\zeta$ below indicates a zeta function, and for ease of notation we define the empty set to have dimension $-\infty$; see
THEOREM 1.1.1. Let $X$ be a smooth subscheme of $\mathbb{P}^n_{\mathbb{F}_q}$ of dimension $m$, $Z$ a closed subscheme of $\mathbb{P}^n_{\mathbb{F}_q}$, and $\mathcal{H}_{Z,d}$ the set of degree $d$ hypersurfaces in $\mathbb{P}^n_{\mathbb{F}_q}$ that contain $Z$. Let $V = X \cap Z$, and for any $e \geq 0$, let $V_e$ be the (locally closed) subset of $V$ whose closed points are exactly those of local embedding dimension $e$ in $V$. Then if $\max_e \{\dim(V_e) + e\} < m$, we have
\[
\lim_{d \to \infty} \frac{\# \{H \in \mathcal{H}_{Z,d} \mid X \cap H \text{ is smooth of dimension } m - 1\}}{\# \mathcal{H}_{Z,d}} = \frac{1}{\zeta_{X-V}(m+1) \prod_e \zeta_{V_e}(m-e)}.
\]
Conversely, if for some value of $e$ we have $\dim(V_e) + e \geq m$, then the limit is 0.

Roughly speaking, the above theorem says that, with positive probability, a hypersurface section of a smooth scheme $X$ containing a given subscheme $V$ is again smooth, provided that the dimension and singularities of the subscheme are adequately controlled. Furthermore, that positive probability is given by special values of zeta functions, which is what a naive point-by-point heuristic predicts.

Remark 1.1.2. In the case where the subscheme $V$ is smooth, Theorem 1.1.1 gives the central theorem of [Poo08]. While our result is more general, its proof is ultimately inspired by that paper. Over an infinite perfect field, under similar hypotheses on local embedding dimensions, the existence of smooth hypersurface sections was proved in [KA79, Theorem 7]. After submitting this chapter for publication as a paper, the author learned that Theorem 1.1.1 was independently obtained by Wutz in her recent thesis [Wut14, Theorem 2.1].

Corollary 1.1.3. Let $C$ be a reduced quasi-projective curve over $\mathbb{F}_q$, not necessarily smooth, irreducible, or projective. Then there exists a smooth $r$-dimensional scheme over $\mathbb{F}_q$ in which $C$ can be embedded if and only if the maximal ideal at each closed point of $C$ can be generated by $r$ elements. If $C$ is projective, the smooth scheme can be chosen projective as well.
Proof of Corollary 1.1.3 from Theorem 1.1.1. Necessity is clear. For sufficiency, consider $C$ embedded in $\mathbb{P}^n_{\mathbb{F}_q}$ for some $n$. If $n = r$, we’re done. If $n < r$, embed $\mathbb{P}^n_{\mathbb{F}_q}$ linearly into $\mathbb{P}^r_{\mathbb{F}_q}$, and we’re again done. Otherwise, let $Z = \bar{C}$ and $X = \mathbb{P}^n_{\mathbb{F}_q} - (\bar{C} - C)$. Applying Theorem 1.1.1 recursively $n - r$ times to find smooth hypersurface sections containing $X \cap Z$, we construct a smooth, $r$-dimensional $\mathbb{F}_q$-scheme $X \cap H_1 \cap \ldots \cap H_{n-r}$ containing $C$. It is projective if $C$ is.

Remark 1.1.4. Over an infinite perfect field, this corollary was proven in [KA79, Corollary 9], using methods inspired by Bloch’s thesis [Blo71, Proposition 1.2]. This chapter shows the corollary is in fact true over any perfect field. The starting idea of both proofs is the same: embed your curve in some large projective space, and then try to show there exist hypersurfaces that contain your curve and whose mutual intersection is smooth of the correct dimension. Altman and Kleiman’s proof in the infinite case proceeds via a Bertini-type argument that fails over finite fields since $\mathbb{F}_q$-points aren’t dense in a rational variety; instead, we adapt Poonen’s closed point sieve to prove the quantitative result in Theorem 1.1.1.

The local embedding dimension at a simple node or cusp on a reduced curve is 2, so we have the following special case.

Corollary 1.1.5. Let $C$ be a reduced, quasi-projective curve over $\mathbb{F}_q$ with only simple nodes and cusps. Then $C$ can be embedded in some smooth surface over $\mathbb{F}_q$.

Remark 1.1.6. In his thesis [Ngu05, Theorem 1.0.2], N. Nguyen proved a different embedding result, answering the question of when a smooth variety $X$ over $\mathbb{F}_q$ of dimension $m$ admits a closed immersion into $\mathbb{P}^n_{\mathbb{F}_q}$, for $n \geq 2m + 1$. In that case, the only obstruction is also an obvious one, though of an arithmetic nature: embedding fails exactly if, for some $e \geq 1$, $X$ has more closed points of degree $e$ than $\mathbb{P}^n_{\mathbb{F}_q}$ itself.
Theorem 1.1.1 also applies to higher-dimensional schemes, not just curves. In particular, we obtain some appealing probabilistic corollaries about subschemes $V \subset \mathbb{P}_{\overline{\mathbb{F}}}^n$ if we take $X = \mathbb{P}_{\overline{\mathbb{F}}}^n$ and $Z = \bar{V}$ in the theorem.

**Corollary 1.1.7.** Let $V \subset \mathbb{P}_{\overline{\mathbb{F}}}^n$ be an arbitrary subscheme. Then the probability that a random hypersurface containing $V$ will be smooth is

\[
\begin{cases} 
1/[[\mathbb{P}^n_{\mathbb{F}} - \bar{V}(n + 1)] \prod_e \zeta((\bar{V})_e) (n - e)], & \text{if } \max_e \{\dim((\bar{V})_e) + e\} < n, \\
0, & \text{otherwise.}
\end{cases}
\]

*Remark 1.1.8.* By rationality of the zeta function [Dwo60], the probabilities in Theorem 1.1.1 and Corollary 1.1.7 are always rational numbers.

**Example.** Let $C$ be the rational curve defined in $\mathbb{P}^3_{\overline{\mathbb{F}}}^3$ by $w = 0$ and $y^2z - x^3 + x^2z = 0$. Then $\zeta_V(s)^{-1} = \frac{1 - q^{-s}}{1 - q^{-s}}$, $\zeta_V(s)^{-1} = 1 - q^{-s}$, and $\zeta_{X-V}(s)^{-1} = (1 - q^{-s})(1 - q^{-2s})(1 - q^{-3s})$. So, for example, the probability that a hypersurface in $\mathbb{P}^3_{\overline{\mathbb{F}}}^3$ containing $C$ will be smooth is $[\zeta_{X-V}(4) \cdot \zeta_V(2) \cdot \zeta_V(1)]^{-1} = \frac{15}{128}$.

*Remark 1.1.9.* We should caution that just because an asymptotic probability in Theorem 1.1.1 or Corollary 1.1.7 is 0, this does not in general rule out the existence of any smooth hypersurface sections containing the given scheme. For example, the non-reduced scheme cut out by $y^2 = 0$ and $z = 0$ in $\mathbb{A}^3_{\overline{\mathbb{F}}} \subset \mathbb{P}^3_{\overline{\mathbb{F}}}$ is contained in smooth affine hypersurfaces of arbitrarily high degree (such as those given by $z - y^d = 0$); however, in accordance with Theorem 1.1.1, the proportion of smooth hypersurfaces decreases to 0 (exponentially with the degree, in fact). Conversely, a curve in $\mathbb{P}^3_{\overline{\mathbb{F}}}$ with a point of local embedding dimension 3 is contained in no smooth hypersurfaces at all.

The second main theorem of this chapter is also an application of Poonen’s sieve; we prove a recent conjecture of Vakil and Wood on hypersurface sections with a prescribed number of singularities. Before stating it, we provide some motivation.
Let $X$ be a smooth, quasi-projective, $m$-dimensional scheme over $\mathbb{F}_q$. Roughly speaking, [Poo04, Theorem 1.1] showed that a hypersurface section of $X$ has zero singularities with probability $\frac{1}{\zeta_X(m+1)}$. At the other extreme, [Poo04, Theorem 3.2] showed that a section has infinitely many singularities with probability 0. It is then natural to ask how the probabilities are distributed across the remaining possible numbers of singularities (one, two, etc.):

$$\frac{1}{\zeta_X(m+1)} + ? + ? + \ldots = 1.$$

To answer this question, we need a little notation. Let $X$ be a finite-type scheme over $\mathbb{F}_q$, and define $Z_X(t) = \sum_{n=0}^{\infty} |(\text{Sym}^n X)(\mathbb{F}_q)| t^n$. Then a standard computation shows that $Z_X(q^{-s}) = \zeta_X(s)$, as defined in the next section. The points of $\text{Sym}^n X$ correspond to formal sums of $n$ points on $X$, with possible repetition; let $\text{Sym}^n_{[\ell]} X$ be the natural subset comprising just those sums supported on exactly $\ell$ geometric points. Analogously, define $Z_X^{[\ell]}(t) = \sum_{n=0}^{\infty} |(\text{Sym}^n_{[\ell]} X)(\mathbb{F}_q)| t^n$, and let $\zeta_X^{[\ell]}(s) = Z_X^{[\ell]}(q^{-s})$. Based on their own motivic results about the Grothendieck ring of varieties, Vakil and Wood conjectured the following generalization of Poonen’s Bertini theorem [VW15, Conjecture A], which we prove in Section 1.4.

**Theorem 1.1.10.** Let $X$ be a smooth $m$-dimensional subscheme of $\mathbb{P}^n_{\mathbb{F}_q}$, $\ell \geq 0$ an integer, and $H_d$ the set of degree $d$ hypersurfaces in $\mathbb{P}^n_{\mathbb{F}_q}$. Then

$$\lim_{d \to \infty} \frac{\# \{ H \in H_d \mid X \cap H \text{ has exactly } \ell \text{ singular geometric points} \}}{\# H_d} = \frac{\zeta_X^{[\ell]}(m + 1)}{\zeta_X(m + 1)}.$$

**Remark 1.1.11.** This gives the distribution of probabilities over all possible numbers of singularities, in terms of a natural decomposition of the zeta function:

$$\frac{1}{\zeta_X(m + 1)} + \frac{\zeta_X^{[1]}(m + 1)}{\zeta_X(m + 1)} + \frac{\zeta_X^{[2]}(m + 1)}{\zeta_X(m + 1)} + \ldots = 1.$$

**Example.** What is the probability that a plane curve is singular at exactly one geometric point? For $X = \mathbb{P}^2_{\mathbb{F}_q}$, we have $\zeta_X^{[1]}(s) = \frac{s^2 + q^2 + 1}{q^2 - 1}$, and so the probability is $\frac{\zeta_X^{[1]}(3)}{\zeta_X(3)} = \frac{(q^3 - 1)(q^2 - 1)}{q^6 - 1}$. 


CHAPTER 1. RANDOM HYPERSURFACES

For $\mathbb{F}_2$, this probability is $\frac{21}{64}$. Coincidentally, by [Poo04, Section 3.5], this is the same as the probability that it’s smooth; thus over $\mathbb{F}_2$, a plane curve is precisely as likely to be smooth as it is to have exactly one singularity. Over any other finite field, a random plane curve is more likely to be smooth than singular.

1.2 Notation and conventions

Let $X$ be a scheme of finite type over $\mathbb{Z}$. The zeta function of $X$ is defined as

$$\zeta_X(s) = \prod_{\text{closed points } P \in X} \frac{1}{1 - |\kappa(P)|^{-s}},$$

where $\kappa(P)$ is the residue field of $P$. The product converges for $\text{Re}(s) > \dim X$ ([Ser65, Theorem 1]). In the particular case where $X$ is a scheme of finite type over $\mathbb{F}_q$, we have that

$$\zeta_X(s) = \prod_{\text{closed } P \in X} \frac{1}{1 - q^{-s \deg P}} = \exp \left( \sum_{n=1}^{\infty} \frac{|X(\mathbb{F}_q^n)|}{n} q^{-ns} \right).$$

Following [Poo04] and [Poo08], we wish to measure the density of sets of homogeneous $\mathbb{F}_q$-polynomials, within both the space of all such polynomials and just those vanishing on a given subscheme of $\mathbb{P}_q^n$. We’ll often speak informally of these densities as probabilities. Let $S = \mathbb{F}_q[x_0, x_1, \ldots, x_n]$, let $S_d$ be its degree $d$ homogeneous part, and let $S_{\text{homog}} = \bigcup_{d \geq 0} S_d$. For any $\mathcal{P} \subset S_{\text{homog}}$, we define the *density* of $\mathcal{P}$ to be

$$\mu(\mathcal{P}) = \lim_{d \to \infty} \frac{\# \mathcal{P} \cap S_d}{\# S_d}$$

if the limit exists.

To define the density relative to a closed subscheme $Z$ of $\mathbb{P}_q^n$, let $I_{\text{homog}}$ denote the homogeneous elements of $S$ that vanish on $Z$, and $I_d$ the degree $d$ part. For $\mathcal{P} \subset I_{\text{homog}}$, we define its *density relative to $Z$* as

$$\mu_Z(\mathcal{P}) = \lim_{d \to \infty} \frac{\# \mathcal{P} \cap I_d}{\# I_d}$$
if the limit exists.

Note that Theorem 1.1.1 is equivalent to a statement about $\mu_Z$; we’ll use this notation in its proof. Theorem 1.1.10 is technically a statement about $\mu$, but we will simply speak of probabilities in its proof. For $f \in S_d$, let $H_f = \text{Proj}(S/(f))$ be the associated hypersurface. All intersections and closures are scheme-theoretic, and a subscheme means a closed subscheme of an open subscheme. We use the convention that a product over an empty set is 1, and that the dimension of the empty set is $-\infty$.

Following [Har77, Section II.7], for a morphism $Y \to X$ and a sheaf of ideals $\mathcal{I}$ on $X$, we write $\mathcal{I} \cdot \mathcal{O}_Y$ for the inverse image ideal sheaf in $\mathcal{O}_Y$. For the definition of a simple singularity on a curve (also known as an ADE-singularity), we refer the reader to [GK90].

### 1.3 Embedding dimension theorem

Let $X$ and $Z$ be as in Theorem 1.1.1, with $I \subset S$ the vanishing ideal of $Z$. We define the **local embedding dimension** $e(P)$ of a closed point $P$ of a scheme to be the minimal number of generators for the maximal ideal $m_P$ in its stalk, or equivalently by Nakayama’s Lemma, the dimension of $m_P/m_P^2$ over the residue field $\kappa(P)$. In this section, $\mathbb{P}^n = \mathbb{P}^n_{\mathbb{F}_q}$, and the local embedding dimension of a point $P$ will always mean as a point of $V = X \cap Z$. For ease of comparison, we parallel the structure of [Poo08].

#### 1.3.1 Singular points of low degree

Fix any $c$ such that $S_1I_d = I_{d+1}$ for all $d \geq c$; for example, choose a finite homogeneous generating set for the ideal, and let $c$ be the maximal degree of its elements. The following interpolation lemma is [Poo08, Lemma 2.1].

**Lemma 1.3.1.** Let $Y$ be a finite subscheme of $\mathbb{P}^n$. Then the restriction map

$$\phi_d : I_d = H^0(\mathbb{P}^n, \mathcal{I}_Z(d)) \to H^0(Y, \mathcal{I}_Z \cdot \mathcal{O}_Y(d))$$
is surjective for \( d \geq c + h^0(Y, \mathcal{O}_Y) \).

**Lemma 1.3.2.** Suppose \( \mathfrak{m} \subset \mathcal{O}_X \) is the ideal sheaf of a closed point \( P \in X \). Let \( Y \subset X \) be the closed subscheme whose ideal sheaf is \( \mathfrak{m}^2 \subset \mathcal{O}_X \). Then for any \( d \in \mathbb{Z}_{\geq 0} \),

\[
\# H^0(Y, \mathcal{I}_Z \cdot \mathcal{O}_Y(d)) = \begin{cases} 
q^{(m-e(P)) \deg P}, & \text{if } P \in V, \\
q^{(m+1) \deg P}, & \text{if } P \notin V.
\end{cases}
\]

**Proof.** Because \( X \) is smooth, the space \( H^0(Y, \mathcal{O}_Y(d)) \) has a two-step filtration whose quotients have dimensions 1 and \( m \) over the residue field \( \kappa(P) \). Thus \( \# H^0(Y, \mathcal{O}_Y(d)) = q^{(m+1) \deg P} \). If \( P \in V = X \cap Z \), then \( H^0(Y, \mathcal{O}_{Z\cap Y}(d)) \) has a filtration whose quotients have dimensions 1 and \( e(P) \) over \( \kappa(P) \); if \( P \notin V \), then \( H^0(Y, \mathcal{O}_{Z\cap Y}(d)) = 0 \). Taking global sections for the exact sequence

\[
0 \to \mathcal{I}_Z \cdot \mathcal{O}_Y(d) \to \mathcal{O}_Y(d) \to \mathcal{O}_{Z\cap Y}(d) \to 0
\]

(taking global sections is exact on a zero-dimensional Noetherian scheme) gives

\[
\# H^0(Y, \mathcal{I}_Z \cdot \mathcal{O}_Y(d)) = \frac{\# H^0(Y, \mathcal{O}_Y(d))}{\# H^0(Y, \mathcal{O}_{Z\cap Y}(d))} = \begin{cases} 
q^{(m+1) \deg P}/q^{(e(P)+1) \deg P}, & \text{if } P \in V, \\
q^{(m+1) \deg P}, & \text{if } P \notin V.
\end{cases}
\]

For \( S \) a scheme of finite type over \( \mathbb{F}_q \), let \( S_{<r} \) be the set of closed points of \( S \) of degree less than \( r \). Define \( S_{>r} \) and \( S_{\geq r} \) similarly.

**Lemma 1.3.3 (Singularities of low degree).** Let notation and hypotheses be as in Theorem 1.1.1, and define

\[
\mathcal{P}_r = \{ f \in I_{\text{homog}} \mid X \cap H_f \text{ is smooth of dimension } m - 1 \text{ at all } P \in X_{<r} \}.
\]
CHAPTER 1. RANDOM HYPERSURFACES

Then

$$\mu_Z(P_r) = \left( \prod_{P \in (X-V)_<r} (1 - q^{-(m+1)\deg P}) \right) \cdot \prod_e \prod_{P \in (V_e)_<r} (1 - q^{-(m-e)\deg P}).$$

Proof. Let \( X_<r = \{ P_1, \ldots, P_k \} \). Let \( m_i \) be the ideal sheaf of \( P_i \) on \( X \). Let \( Y_i \) be the closed subscheme of \( X \) with ideal sheaf \( m_i^2 \subset O_X \), and let \( Y = \bigcup Y_i \). Then \( H_f \cap X \) is not smooth of dimension \( m - 1 \) at \( P_i \) exactly if the restriction of \( f \) to a section of \( O_{Y_i}(d) \) is zero.

By Lemma 1.3.1, the restriction map \( \phi_d : I_d \to H^0(Y, \mathcal{I}_Z \cdot O_Y(d)) \) is surjective for \( d >> 0 \), and as this is a linear map, its values are equidistributed. So \( \mu_Z(P_r) \) just equals the fraction of elements in \( H^0(\mathbb{P}^n, \mathcal{I}_Z \cdot O_Y(d)) \) which are nonzero when restricted to each \( Y_i \), which is constant. Thus, by Lemma 1.3.2,

$$\mu_Z(P_r) = \prod_{i=1}^s \frac{\#H^0(Y_i, \mathcal{I}_Z \cdot O_{Y_i}(d)) - 1}{\#H^0(Y_i, \mathcal{I}_Z \cdot O_{Y_i}(d))} = \left( \prod_{P \in (X-V)_<r} (1 - q^{-(m+1)\deg P}) \right) \cdot \prod_e \prod_{P \in (V_e)_<r} (1 - q^{-(m-e)\deg P}).$$

\[ \square \]

**Corollary 1.3.4.** If \( \dim(V_e) + e < m \) for all \( e \), then

$$\lim_{r \to \infty} \mu_Z(P_r) = \frac{1}{\zeta_{X-V}(m+1) \prod_e \zeta_{V_e}(m-e)}.$$

Proof. The products in Lemma 1.3.3 are the reciprocals of the partial products in the definition of the zeta functions. For convergence, we need \( m - e > \dim(V_e) \) for each \( e \) ([LW54, Corollary 5]), which is our hypothesis exactly. \( \square \)

**Corollary 1.3.5.** If \( \dim(V_e) + e \geq m \) for some \( e \), then \( \lim_{r \to \infty} \mu_Z(P_r) = 0 \).

Proof. By [LW54, Corollary 5], \( \zeta_{V_e}(s) \) has a pole at \( s = \dim(V_e) \), so the product in Lemma 1.3.3 converges to 0. This proves the second part of Theorem 1.1.1. \( \square \)
1.3.2 Singular points of medium degree

**Lemma 1.3.6.** Let \( P \in X \) be a closed point with \( \deg P \leq \frac{d-c}{m+1} \). Then the fraction of \( f \in I_d \) such that \( X \cap H_f \) is not smooth of dimension \( m-1 \) at \( P \) equals

\[
\begin{cases}
q^{-(m-e(P))\deg P}, & \text{if } P \in V \\
q^{-(m+1)\deg P}, & \text{if } P \notin V.
\end{cases}
\]

**Proof.** Let \( Y \) be as in Lemma 1.3.2. Then \( \#H^0(Y, I_Z \cdot \mathcal{O}_{Y_i}(d)) \) is given by the same lemma, which serves to calculate the desired fraction by Lemma 1.3.1. \( \square \)

Define the *upper density* \( \bar{\mu}_Z(\mathcal{P}) \) as the lim sup of the expression used to define \( \mu_Z \).

**Lemma 1.3.7 (Singularities of medium degree).** Define

\[
Q_r^{\text{medium}} = \bigcup_{d \geq 0} \{ f \in I_d \mid \text{there exists } P \in X \text{ with } r \leq \deg P \leq \frac{d-c}{m+1} \text{ such that } X \cap H_f \text{ is not smooth of dimension } m-1 \text{ at } P \}.
\]

Then \( \lim_{r \to \infty} \bar{\mu}_Z(Q_r^{\text{medium}}) = 0. \)

**Proof.** By Lemma 1.3.6, we have

\[
\frac{\#(Q_r^{\text{medium}} \cap I_d)}{\#I_d} \leq \sum_{e} \left( \sum_{P \in V_e \atop r \leq \deg P \leq \frac{d-c}{m+1}} q^{-(m-e)\deg P} \right) + \sum_{P \in X-V \atop r \leq \deg P \leq \frac{d-c}{m+1}} q^{-(m+1)\deg P}.
\]

By \([\text{LW54, Lemma 1}], a k\text{-dimensional variety has } \mathcal{O}(q^{kl}) \text{ closed points of degree } l; \) applied to each \( V_e \) and \( X - V \), we see as in \([\text{Poo08, Lemma 3.2}], that the above expression is \( \mathcal{O}(q^{-r}) \) as \( r \to \infty \), under our assumption that \( \dim(V_e) + e < m \) for each \( e \). \( \square \)
CHAPTER 1. RANDOM HYPERSURFACES

1.3.3 Singular points of high degree

Lemma 1.3.8 (Singularities of high degree off $V$). Define

$$Q^{\text{high}}_{X-V} = \bigcup_{d \geq 0} \{ f \in I_d \mid \exists P \in (X-V)_{d+\frac{c}{m+1}} \text{ s.t. } X \cap H_f \text{ isn't smooth of dimension } m-1 \text{ at } P \}.$$ 

Then $\bar{\mu}_Z(Q^{\text{high}}_{X-V}) = 0$.

Proof. The proof of [Poo08, Lemma 4.2] works without change. \qed

Lemma 1.3.9 (Singularities of high degree on $V_e$). For any $e$ such that $V_e$ is not empty, define

$$Q^{\text{high}}_{V_e} = \bigcup_{d \geq 0} \{ f \in I_d \mid \exists P \in (V_e)_{d+\frac{c}{m+1}} \text{ s.t. } X \cap H_f \text{ isn't smooth of dimension } m-1 \text{ at } P \}.$$ 

Then $\bar{\mu}_Z(Q^{\text{high}}_{V_e}) = 0$.

Proof. As the union of finitely many density 0 sets will be density 0, it suffices to prove the lemma with $X$ replaced by each of the sets in an open covering of $X$, so we may assume $X$ is contained in $\mathbb{A}^n_{\mathbb{F}_q} = \{ x_0 \neq 0 \} \subset \mathbb{P}^n$, and we may dehomogenize by setting $x_0 = 1$. This identifies $I_d \subset S_d \subset \mathbb{F}_q[x_0, \ldots, x_n]$ with subspaces $I'_d \subset S'_d \subset A = \mathbb{F}_q[x_1, \ldots, x_n]$.

Since $V$ isn’t assumed smooth, we can’t take it to be locally cut out by a system of local parameters, as is done in [Poo08]. Instead, fix a closed point $v \in V_e$. Recall the exact sequence of sheaves on $V$ [Har77, Section II.8]:

$$\mathcal{I}_V/\mathcal{I}_V^2 \to \Omega^1_X \otimes \mathcal{O}_V \to \Omega^1_V \to 0.$$ 

Thus we can choose a system of local parameters $t_1, \ldots, t_n \in A$ at $v$ on $\mathbb{A}^n_{\mathbb{F}_q}$ such that $t_{m+1} = t_{m+2} = \ldots = t_n = 0$ defines $X$ locally at $v$, while $t_1, \ldots, t_{m-e}$ vanish on $V$. In fact, since $V = X \cap Z$, we may choose $t_1, \ldots, t_{m-e}$ vanishing on $Z$.

Now $dt_1, \ldots, dt_n$ are an $\mathcal{O}_{\mathbb{A}^n_{\mathbb{F}_q},v}$-basis for the stalk $\Omega^1_{\mathbb{A}^n_{\mathbb{F}_q},v}$. Let $\partial_1, \ldots, \partial_n$ be the dual basis of the stalk $T_{\mathbb{A}^n_{\mathbb{F}_q},v}$ of the tangent sheaf. Choose $s \in A$ with $s(v) \neq 0$ to clear denominators so that $D_i = s \partial_i$ gives a global derivation $A \to A$ for $i = 1, \ldots, n$. Then there is a neighborhood $U$ of $v$ in $\mathbb{A}^n_{\mathbb{F}_q}$ such that $U \cap \{ t_{m+1} = t_{m+2} = \ldots = t_n = 0 \} = U \cap X$, $\Omega^1_U = \bigoplus_{i=1}^n \mathcal{O}_U dt_i$, and
CHAPTER 1. RANDOM HYPERSURFACES

For $f \in I'_d$, $H_f \cap X$ fails to be smooth of dimension $m - 1$ at a point $P \in V_e \cap U$ if and only if $f(P) = (D_1 f)(P) = \ldots = (D_m f)(P) = 0$.

Let $N = \dim(V_e)$, $\tau = \max_i \{\deg t_i\}$ and $\gamma = \lfloor \frac{d - \tau}{p} \rfloor$, where $p$ is the characteristic of $\mathbb{F}_q$. Given choices of $f_0 \in I'_d$, and $g_i \in S'_\gamma$ for $i = 1, \ldots, N + 1$, let $f = f_0 + g_1 t_1 + \ldots + g_{N+1}^d t_{N+1}$. By hypothesis, $N + 1 = \dim(V_e) + 1 \leq m - e$, so we have each $t_i \in I'_d$. Given all possible choices of $f_0, g_1, \ldots, g_{N+1}$, $f$ realizes every element of $I'_d$ the same number of times, because of $f_0$ (i.e. $f$ is a random element of $I'_d$).

This has served to make the derivatives partially independent of each other: note that for $i \leq N + 1$, $D_i f = D_i f_0 + s g_i^d$. Given choices of $f_0, g_1, \ldots, g_i$, let $W_i = V_e \cap \{D_1 f = \ldots = D_i f = 0\}$, which depends only on these choices. As in [Poo04, Lemma 2.6], for $1 \leq i \leq N$, the fraction of choices of $f_0, g_1, \ldots, g_i$ such that $\dim(W_i) \leq N - i$ goes to 1 as $d \to \infty$. In particular, for most choices, $W_N$ is finite.

Next, as in [Poo08, Lemma 4.3], given any choice of $f_0, g_1, \ldots, g_N$ such that $W_N$ is finite, the fraction of choices of $g_{N+1}$ such that $(V_e)_{d-c \choose m+1} \cap W_{N+1} = \emptyset$ goes to 1 as $d \to \infty$. In conclusion (the product of two quantities that both go to 1 itself goes to 1), $\bar{\mu}(\mathcal{Q}_{V_e}^{\text{high}}) = 0$.

Proof of Theorem 1.1.1. Let $\mathcal{P} = \{f \mid X \cap H_f \text{ is smooth of dimension } m - 1\}$. Then we have $\mathcal{P} \subset \mathcal{P}_r \subset \mathcal{P} \cup \mathcal{Q}^{\text{medium}} \cup \mathcal{Q}^{\text{high}}_{X-V} \cup (\cup_e \mathcal{Q}^{\text{high}}_{V_e})$, so by the preceding results

$$
\mu_Z(\mathcal{P}) = \lim_{r \to \infty} \mu_Z(\mathcal{P}_r) = \frac{1}{\zeta_{X-V}(m + 1) \prod_e \zeta_{V_e}(m - e)}.
$$

\qed
1.4 The probability of a hypersurface section having a given number of singularities

Proof of Theorem 1.1.10. Fix a value of $\ell \geq 1$. Suppose we have $r$ distinct closed points $\{P_1, \ldots, P_r\}$ of $X$, of any degrees $\lambda_1, \ldots, \lambda_r$ such that $\sum \lambda_i = \ell$. Then the contribution of zero-cycles supported on exactly this set to $Z_X^{[\ell]}(t)$ is $\prod_{i=1}^r \left( \frac{\sum_{n=1}^{\infty} t^{n\lambda_i}}{1-t^{n\lambda_i}} \right) = \prod_{i=1}^r \frac{t^{\lambda_i}}{1-t^{\lambda_i}}$. Plugging in $q^{-(m+1)}$ gives that their contribution to $\zeta_X^{[\ell]}(m+1)$ is $\prod_{i=1}^r \frac{q^{-\lambda_i(m+1)}}{1-q^{-\lambda_i(m+1)}}$.

On the other hand, consider the probability that an $\mathbb{F}_q$-hypersurface section $X \cap H$ of $X$ is singular at exactly the points $\{P_1, \ldots, P_r\}$. (Note that since $X$ and $H$ are both defined over $\mathbb{F}_q$, $X \cap H$ is singular at a geometric point if and only if it’s singular at all of the point’s $\mathbb{F}_q$-conjugates.) Let $m_i$ be the ideal sheaf of the point $P_i$, and let $Z_i$ be the subscheme of $X$ defined by $m_i^2$. Let $Z = \bigcup Z_i$. Then by Theorem 1.2 (Bertini with Taylor conditions) of [Poo04] applied to $T = \{0\} \times \ldots \times \{0\}$, the probability that an $\mathbb{F}_q$-hypersurface section of $X$ is singular at exactly the points $\{P_1, \ldots, P_r\}$ is

$$\frac{1}{q^{\sum \lambda_i(m+1)}} \cdot \frac{1}{\zeta_X-Z(m+1)} = \frac{1}{\zeta_X(m+1)} \cdot \prod_{i=1}^r \frac{q^{-\lambda_i(m+1)}}{1-q^{-\lambda_i(m+1)}}.$$ 

Note that there are only finitely many such $\{P_1, \ldots, P_r\}$, as their degree is bounded by $\ell$. Since our density definition of probability in Section 2 is finitely additive, the probabilities of being singular at each such set add to give the total probability in Theorem 1.1.10: the event of a hypersurface section being singular in precisely the points of one set is certainly disjoint from the event given by a different set of points. Meanwhile, the series contributions of each $\{P_1, \ldots, P_r\}$ add up to all of $\zeta_X^{[\ell]}(m+1)$. As the series terms and the probabilities were individually comparable, we’re done. □
Chapter 2

Counting cubic curve covers over finite fields

2.1 Introduction

Let $C$ be a nice curve over a finite field $\mathbb{F}_q$; here nice means smooth, geometrically irreducible, and projective. Let $g_C$ denote the genus of $C$, and let $N_3(C, m)$ denote the number of isomorphism classes of nice degree 3 covers $X$ of $C$, defined over $\mathbb{F}_q$, such that $X \rightarrow C$ has ramification divisor of degree $m$ (by Riemann-Hurwitz, $m$ is necessarily even). In this chapter we give an algebro-geometric proof that, for $\mathbb{F}_q$ of characteristic at least 5,

$$\lim_{m \to \infty} \frac{N_3(C, m)}{q^m} = \frac{|(\text{Pic}^0 C)(\mathbb{F}_q)|}{(q - 1)q^{g_C - 1} \zeta_C(3)}.$$ 

Phrased in terms of counting cubic field extensions of $\mathbb{F}_q(t)$, this theorem was originally proved by Datskovsky and Wright [DW88, Theorem 1.1], using adelic Shintani zeta functions. It was re-proved (and extended to all characteristics) by Bhargava, Shankar, and Wang, using geometry-of-numbers methods [BSW15, Theorem 1(b)]. The characteristic assumption isn’t strictly necessary for our algebro-geometric approach either, but does simplify the proof.

By Riemann-Hurwitz, counting covers with increasing ramification degree $m$ is equivalent to counting covers of increasing genus. Geometrically, this theorem can be viewed as saying...
that, for the natural sequence of (Hurwitz) moduli spaces parametrizing these covers, the point counts stabilize.

For the case $C = \mathbb{P}^1$, a geometric proof was given by Zhao in his recent thesis [Zha13] (he also made a more refined analysis and obtained a secondary term). Our approach is inspired by his, but over an arbitrary base curve, some new hurdles appear. Vector bundles on the base curve arise naturally in the geometric perspective, but while vector bundles on $\mathbb{P}^1$ are always direct sums of line bundles, the situation is more complicated for higher genus curves. However, this approach is still feasible (and elegant), when combined with a couple extra ingredients: some classical theory of ruled surfaces and the Siegel-Weil formula for vector bundles on curves over finite fields.

Our proof also shows that the Steinitz classes of cubic extensions equidistribute in the class group of the base curve (in the notation of Section 2.4, the Steinitz class corresponds to $\det \mathcal{E}$); this was also proved in [BSW15, Theorem 4].

## 2.2 Vector bundles and ruled surfaces

In Section 2.3, we’ll see that cubic covers of a base curve can be counted by embedding them into ruled surfaces. In this section, we collect various basic facts about these surfaces, all of which can be found in [Har77, V.2]. Throughout this section, except when otherwise noted, $C$ will be a nice curve over an arbitrary base field, and $\mathcal{E}$ will be a vector bundle of rank two on $C$.

### 2.2.1 Rank two vector bundles

Given such an $\mathcal{E}$, we can always write it in an exact sequence $0 \to \mathcal{N} \to \mathcal{E} \to \mathcal{M} \to 0$, with $\mathcal{N}$ and $\mathcal{M}$ line bundles, such that for any line bundle $\mathcal{L}$ with $\deg \mathcal{L} > \deg \mathcal{N}$, we have $h^0(C, \mathcal{E} \otimes \mathcal{L}^{-1}) = 0$. The integer $e = \deg \mathcal{N} - \deg \mathcal{M}$ is independent of the choice of line
bundles; we will call it the skew degree of \( E \).

We have that \( E \) is decomposable – i.e. splits as a direct sum of two line bundles – except possibly when \(-g_C \leq e \leq 2g_C - 2\). Thus an arbitrary \( E \) will always satisfy \( e \geq -g_C \). It will be important later that, when working over a finite field \( \mathbb{F}_q \), for any \( E \) with \( e > 2g_C - 2 \), we have \(|\text{Aut } E)(\mathbb{F}_q)| = (q - 1)^2 q^{e+1 - g_C} \). This follows directly from the fact that \( E \) splits as a direct sum.

Next we give conditions under which we know the dimension of global sections of certain vector bundles.

**Lemma 2.2.1.** Let \( E \) be a rank two vector bundle on a curve \( C \), and let \( L \) be a line bundle on \( C \). Let \( \ell \) and \( e \) be the degree of \( L \) and the skew degree of \( E \), respectively. For \( i \geq 0 \), if

\[
\min\{\ell + i \frac{\deg E + e}{2}, \ell + i \frac{\deg E - e}{2}\} > 2g_C - 2,
\]

then

\[
h^0(C, E^i \otimes L) = 2^i(\ell + 1 - g_C) + i 2^{i-1} \deg E,
\]

and \( h^1(C, E^i \otimes L) = 0 \).

**Proof.** We proceed by induction. When \( i = 0 \), this follows directly from Riemann-Roch for line bundles.

Suppose the lemma is true for \( i \), and that \( \min\{\ell + (i+1) \frac{\deg E + e}{2}, \ell + (i+1) \frac{\deg E - e}{2}\} > 2g_C - 2 \). Let \( 0 \to N \to E \to M \to 0 \) be as in the definition of skew degree. Note that we have \( \deg N = \frac{\deg E + e}{2} \) and \( \deg M = \frac{\deg E - e}{2} \). Since vector bundles are flat, there is an exact sequence

\[
0 \to E^i \otimes N \otimes L \to E^{i+1} \otimes L \to E^i \otimes M \otimes L \to 0.
\]

Applying the induction hypothesis with the line bundles \( N \otimes L \) and \( M \otimes L \), we have

\[
h^0(C, E^i \otimes N \otimes L) = 2^i(\ell + \deg N + 1 - g_C) + i 2^{i-1} \deg E
\]
and

$$h^0(C, \mathcal{E}^i \otimes \mathcal{M} \otimes \mathcal{L}) = 2^i(\ell + \deg \mathcal{M} + 1 - g_C) + i2^{i-1} \deg \mathcal{E}.$$  

Since furthermore $h^1(C, \mathcal{E}^i \otimes \mathcal{N} \otimes \mathcal{L}) = h^1(C, \mathcal{E}^i \otimes \mathcal{M} \otimes \mathcal{L}) = 0$, the lemma follows. \qed

**Lemma 2.2.2.** Let $\mathcal{E}$ be a rank two vector bundle on a curve $C$, and let $\mathcal{L}$ be a line bundle on $C$. Let $\ell$ and $e$ be the degree of $\mathcal{L}$ and the skew degree of $\mathcal{E}$, respectively. For $i \geq 0$, if

$$\min\{\ell + 3\frac{\deg \mathcal{E} + e}{2}, \ell + 3\frac{\deg \mathcal{E} - e}{2}\} > 2g_C - 2,$$

then

$$h^0(C, \text{Sym}^3 \mathcal{E} \otimes \mathcal{L}) = 6 \deg \mathcal{E} + 4(\ell + 1 - g_C),$$

and $h^1(C, \text{Sym}^3 \mathcal{E} \otimes \mathcal{L}) = 0$.

**Proof.** Since $\mathcal{E}$ is rank two, there is an exact sequence

$$0 \rightarrow (\mathcal{E} \otimes \text{det} \mathcal{E}) \oplus (\text{det} \mathcal{E} \otimes \mathcal{E}) \rightarrow \mathcal{E}^3 \rightarrow \text{Sym}^3 \mathcal{E} \rightarrow 0.$$

Tensoring with $\mathcal{L}$, using the fact that $\deg(\text{det} \mathcal{E}) = \deg \mathcal{E}$, and applying Lemma 2.2.1, the conclusion follows. \qed

### 2.2.2 Ruled surfaces

The Proj construction [Har77, II.7] takes as input $(C, \mathcal{E})$ and outputs $\mathbb{P}(\mathcal{E})$, a surface with a surjective map $\pi$ to $C$, whose geometric fibers are all isomorphic to $\mathbb{P}^1$ (hence the name *ruled surface*). Under this construction, two different vector bundles $\mathcal{E}$ and $\mathcal{E}'$ on $C$ give surfaces that are isomorphic over $C$ if and only if $\mathcal{E} \cong \mathcal{E}' \otimes \mathcal{L}$, with $\mathcal{L}$ a line bundle on $C$.

Given the map $\pi : \mathbb{P}(\mathcal{E}) \rightarrow C$, we can always find a section $C \rightarrow \mathbb{P}(\mathcal{E})$, with image $C_0 \cong C$, having certain useful properties. The Picard group of linear equivalence classes of divisors on $\mathbb{P}(\mathcal{E})$ decomposes as $\text{Pic} \mathbb{P}(\mathcal{E}) \cong \mathbb{Z}C_0 \oplus \pi^* \text{Pic} C$. The intersection product is given by $C_0^2 = -e$, $C_0 \cdot \pi^* D_1 = \deg D_1$, and $\pi^* D_1 \cdot \pi^* D_2 = 0$, for $D_i$ divisors on $C$. The
canonical divisor class is \(K_{P(E)} \sim -2C_0 + \pi^*(K_C + E)\), where \(E\) is a divisor on \(C\) of degree \(-e\), corresponding to \(\det \pi_* \mathcal{O}(C_0)\).

A final useful fact about divisors on ruled surfaces: for \(Z\) a divisor on \(\mathbb{P}(E)\) that intersects a fiber of \(\pi\) non-negatively, we have for all \(i \geq 0\),

\[
H^i(\mathbb{P}(E), \mathcal{O}(Z)) \cong H^i(C,\pi_* \mathcal{O}(Z)).
\]

Thus the cohomology of such line bundles on our surface is determined by the cohomology of vector bundles on our base curve.

### 2.2.3 Siegel-Weil formula

Lastly, we state the Siegel-Weil formula [DR75, Proposition 1.1], which gives a closed form for the automorphism-weighted count of vector bundles on a curve. For a curve \(C\) of genus \(g_C\) over a finite field \(\mathbb{F}_q\), \(r > 0\), and \(\mathcal{L}\) a line bundle on \(C\), let \(\text{VBun}_C(r, \mathcal{L})\) denote the set of isomorphism classes of vector bundles on \(C\) defined over \(\mathbb{F}_q\), of rank \(r\), and with determinant line bundle \(\mathcal{L}\). Then the Siegel-Weil formula says

\[
\sum_{\mathcal{E} \in \text{VBun}_C(r, \mathcal{L})} \frac{1}{|\text{Aut} \mathcal{E}(\mathbb{F}_q)|} = q^{(r^2-1)(g_C-1)} \frac{\zeta_C(2) \cdots \zeta_C(r)}{q-1}.
\]

We immediately have a projective bundle version:

\[
\sum_{\mathcal{E} \in \text{VBun}_C(r, \mathcal{L})} \frac{1}{|\text{Aut} \mathbb{P}(\mathcal{E})(\mathbb{F}_q)|} = q^{(r^2-1)(g_C-1)} \zeta_C(2) \cdots \zeta_C(r).
\]

### 2.3 Parametrization of cubic covers

We use a construction due to Miranda [Mir85], and later generalized considerably by Casnati and Ekedahl [CE96]. Given an integral cubic cover \(X \overset{\pi}{\rightarrow} C\), possibly singular, let

\[
\mathcal{E} = (\pi_* \mathcal{O}_X/\mathcal{O}_C)^\vee.
\]
This is a rank 2 vector bundle on $C$ called the Tschirnhausen bundle of the cover. Then the covering $X \xrightarrow{\pi} C$ factors naturally through an embedding of $X$ into $\mathbb{P}(\mathcal{E})$:

$$
\begin{array}{ccc}
X & \xrightarrow{\pi} & \mathbb{P}(\mathcal{E}) \\
& \downarrow & \\
& C & 
\end{array}
$$

If $X$ is smooth, and we define $N := g_X - 3g_C + 2$, then we have $\deg \mathcal{E} = N$. Furthermore, if we overload notation and let $\pi$ also denote the map from $\mathbb{P}(\mathcal{E})$ to $C$, we have that $\pi_* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(X) \cong \text{Sym}^3 \mathcal{E} \otimes \det \mathcal{E}^{-1}$. (Conversely, by the canonical nature of the Casnati-Ekedahl construction, for any nice $X \subset \mathbb{P}(\mathcal{E})$ with that pushforward property, $\mathcal{E}$ is its Tschirnhausen bundle.)

Given another cover $X' \to C$ that is isomorphic to $X \to C$ over $C$, its Tschirnhausen bundle $\mathcal{E}'$ will be isomorphic to $\mathcal{E}$, and the embedding of $X'$ into a fixed copy of $\mathbb{P}(\mathcal{E}') \cong \mathbb{P}(\mathcal{E})$ will differ only by a bundle automorphism of $\mathbb{P}(\mathcal{E})$.

This enables our approach to counting cubic covers, first employed in [Zha13] in the special case when the base curve is $\mathbb{P}^1$. We’ll count nice covers inside a given possible ruled surface, divide out by the surface’s automorphism group to identify isomorphic covers, and then sum up the contributions from all ruled surfaces.

By our characteristic assumption on $\mathbb{F}_q$, every cubic covering $X \xrightarrow{\pi} C$ is separable. The Riemann-Hurwitz theorem [Ros02, Theorem 7.16] gives us that, for such a cover,

$$2g_X - 2 = 3(2g_C - 2) + \deg R,$$

where $R$ is the ramification divisor of the map $\pi$, and $g_X$ and $g_C$ are the genus of $X$ and $C$, respectively. Thus we have

$$\deg R = 2g_X - 6g_C + 4 = 2N.$$
Given a rank two vector bundle \( E \) on \( C \), we fix a distinguished section \( C_0 \subset \mathbb{P}(E) \) as in Section 2.2.2. If \( E \) is the Tschirnhausen bundle of a nice cubic cover \( X \to C \), and we write \( \mathcal{O}(X) \cong 3\mathcal{O}(C_0) + \pi^*\mathcal{L} \), we can identify the degree \( \ell \) of \( \mathcal{L} \). Namely, adjunction tells us that for a curve \( X \) in a surface \( S \), we have

\[
g_X = 1 + \frac{1}{2}(X \cdot X + X \cdot K_S).
\]

Thus by the adjunction formula,

\[
g_X = 1 + \frac{1}{2}(-9e + 6\ell + 6e + 3(2g_C - 2 - e) - 2\ell) = 2\ell - 3e + 3g_C - 2.
\]

In other words, we have \( 2\ell - 3e = N \). This also gives the key fact that, for any separable irreducible cubic cover \( X \), we have

\[
0 \leq X \cdot C_0 = \frac{N - 3e}{2}.
\]  \hspace{1cm} (2.2)

In particular, we always have \( e \leq \frac{N}{3} \).

**Lemma 2.3.1.** Let \( E \) be a rank two vector bundle on a curve \( C \), of degree \( N \) and skew degree \( e \). If either \( e < 0 \) and \( N > 7g_C - 4 \), or \( e \geq 0 \) and \( \frac{N - 3e}{4} \geq g_C \), then

\[
h^0(C, \text{Sym}^3 E \otimes \det E^{-1}) = 2N + 4(1 - g_C).
\]

If \( e > 0 \) but \( 0 \leq \frac{N - 3e}{4} < g_C \), then for \( N \geq 10g_C - 6 \) we have the upper bound

\[
h^0(C, \text{Sym}^3 E \otimes \det E^{-1}) \leq 2N.
\]

**Proof.** Lemma 2.2.2 implies \( 2N + 4(1 - g_C) \) will be the dimension of the global sections whenever

\[
\min\{\frac{N + 3e}{2}, \frac{N - 3e}{2}\} > 2g_C - 2.
\]
CHAPTER 2. COUNTING CUBIC COVERS

If $N > 7g_C - 4$, this will automatically be satisfied for $e < 0$, because we know $e \geq -g_C$.

For $e \geq 0$, it suffices that $\frac{N - 3e}{4} \geq g_C$.

If $e > 0$ but $0 \leq \frac{N - 3e}{4} < g_C$, note first that this trivially implies $g_C > 0$. The condition $N \geq 10g_C - 6$ guarantees that $e > 2g_C - 2$, and thus that $\mathcal{E}$ is decomposable. So let $\mathcal{E} \cong \mathcal{N} \oplus \mathcal{M}$, with $\deg \mathcal{N} + \deg \mathcal{M} = N$ and $\deg \mathcal{N} - \deg \mathcal{M} = e$. Then $\text{Sym}^3 \mathcal{E} \cong \mathcal{N}^3 \oplus (\mathcal{N}^2 \otimes \mathcal{M}) \oplus (\mathcal{N} \otimes \mathcal{M}^2) \oplus \mathcal{M}^3$, and so $\text{Sym}^3 \mathcal{E} \otimes \det \mathcal{E}^{-1} \cong \text{Sym}^3 \mathcal{E} \otimes \mathcal{N}^{-1} \otimes \mathcal{M}^{-1} \cong (\mathcal{N}^2 \otimes \mathcal{M}^{-1}) \oplus \mathcal{N} \oplus \mathcal{M} \oplus (\mathcal{M}^2 \otimes \mathcal{N}^{-1})$.

Since $e \leq \frac{N}{3}$, the first three of those four line bundles all have degree greater than $2g_C - 2$, and so we know the dimension of their global sections by Riemann-Roch. As for $\mathcal{M}^2 \otimes \mathcal{N}^{-1}$, it has non-negative degree, so we have the trivial upper bound $h^0(C, \mathcal{M}^2 \otimes \mathcal{N}^{-1}) \leq \deg(\mathcal{M}^2 \otimes \mathcal{N}^{-1})$.

Thus overall we have

$$h^0(C, \text{Sym}^3 \mathcal{E} \otimes \det \mathcal{E}^{-1}) \leq 2N + 3(1 - g_C) \leq 2N.$$  

Our sieve will also require versions of this lemma in which we twist down by a line bundle of small degree. First we consider the case where $\mathcal{E}$ is semistable. This is equivalent to $\mathcal{E}$ having skew degree $e \leq 0$ (see [Har77, Ex. 2.8]).

**Lemma 2.3.2.** Let $\mathcal{E}$ be a semistable rank two vector bundle of degree $N$ on a curve $C$, over a field of characteristic not 2 or 3. Let $\mathcal{L}$ be a line bundle of degree $\ell$ on $C$. If $\frac{N}{2} - \ell > 2g_C - 2$, then we have

$$h^0(C, \text{Sym}^3 \mathcal{E} \otimes \det \mathcal{E}^{-1} \otimes \mathcal{L}^{-1}) = 2N - 4\ell + 4(1 - g_C).$$

If $0 \leq \frac{N}{2} - \ell \leq 2g_C - 2$, we have

$$h^0(C, \text{Sym}^3 \mathcal{E} \otimes \det \mathcal{E}^{-1} \otimes \mathcal{L}^{-1}) \leq N - 2\ell + 4.$$
Lastly, if \( 0 > \frac{N}{2} - \ell \), we have

\[
h^0(C, \text{Sym}^3 \mathcal{E} \otimes \text{det} \mathcal{E}^{-1} \otimes \mathcal{L}^{-1}) = 0.
\]

**Proof.** First, note that \( \text{Sym}^3 \mathcal{E} \) is semistable: in characteristic 0, every symmetric power of a semistable vector bundle is semistable, and this also holds in positive characteristic for a symmetric \( i \)-th power, when \( i \) is less than the field characteristic [RR84, Theorem 3.21]. We calculate that our bundle’s slope is

\[
\mu(\text{Sym}^3 \mathcal{E} \otimes \text{det} \mathcal{E}^{-1} \otimes \mathcal{L}^{-1}) = \frac{N}{2} - \ell.
\]

Then the lemma follows from standard results showing that semistable bundles behave roughly like line bundles [Tho15, Lemma 4.4], in that a semistable vector bundle has the expected number of global sections when its slope is not between 0 and \( 2g_C - 2 \), and that a form of Clifford’s theorem holds when it is.

\[\square\]

**Lemma 2.3.3.** Let \( \mathcal{E} \) be a non-semistable rank two vector bundle on a curve \( C \), of degree \( N \) and skew degree \( e \). Let \( \mathcal{L} \) be a line bundle on \( C \) with degree \( \ell \leq \frac{N-3e}{2} \). Then we have

\[
h^0(C, \text{Sym}^3 \mathcal{E} \otimes \text{det} \mathcal{E}^{-1} \otimes \mathcal{L}^{-1}) \leq 2N - 4\ell + 4.
\]

**Proof.** Let \( \mathcal{N} \) and \( \mathcal{M} \) be as in the definition of skew degree. Since \( \mathcal{E} \) is not semistable, we have \( e > 0 \), and so the Harder-Narasimhan filtration of \( \mathcal{E} \) is \( 0 \subset \mathcal{N} \subset \mathcal{E} \). The successive quotients in this filtration are line bundles, with degrees \( \text{deg} \mathcal{M} \) and \( \text{deg} \mathcal{N} \). Then \( \text{Sym}^3 \mathcal{E} \) also has line bundles for successive quotients in its Harder-Narasimhan filtration, with degrees \( 3 \text{deg} \mathcal{M} \), \( 2 \text{deg} \mathcal{M} + \text{deg} \mathcal{N} \), \( \text{deg} \mathcal{M} + 2 \text{deg} \mathcal{N} \), and \( 3 \text{deg} \mathcal{N} \) (see e.g. [Che12, Section 3.2]). After twisting down, we see that \( \text{Sym}^3 \mathcal{E} \otimes \text{det} \mathcal{E}^{-1} \otimes \mathcal{L}^{-1} \) has line bundles for successive quotients, with degrees \( 2 \text{deg} \mathcal{M} - \text{deg} \mathcal{N} - \ell \), \( \text{deg} \mathcal{M} - \ell \), \( \text{deg} \mathcal{N} - \ell \), and \( 2 \text{deg} \mathcal{N} - \text{deg} \mathcal{M} - \ell \).

Since by assumption, \( \ell \leq \frac{N-3e}{2} \), these four degrees are all non-negative. A quick exact sequences argument shows the \( h^0 \) of our bundle is bounded by the sum of the \( h^0 \)'s of its successive quotients. By using the trivial bound for the \( h^0 \) of a non-negative line bundle
(one more than its degree), we have that

\[ h^0(C, \text{Sym}^3 \mathcal{E} \otimes \text{det} \mathcal{E}^{-1} \otimes \mathcal{L}^{-1}) \leq 2N - 4\ell + 4. \]

\[ \square \]

\section{Counting cubic covers}

In this section, we work with a curve \( C \) defined over a finite field \( \mathbb{F}_q \), of characteristic at least 5. While we can now identify the line bundle inside a ruled surface corresponding to a nice cubic cover, some of the global sections of those line bundles will have smooth zero loci, while others will have singular loci. In order to count nice covers, we need to sieve for the sections with smooth zero loci.

Given a rank two vector bundle \( \mathcal{E} \) on \( C \) with degree \( N \) and skew degree \( e \), we denote by \( \mathcal{L}_\mathcal{E} \) the unique line bundle on \( \mathbb{P}(\mathcal{E}) \) such that \( \pi_* \mathcal{L}_\mathcal{E} = \text{Sym}^3 \mathcal{E} \otimes \text{det} \mathcal{E}^{-1} \), where \( \pi: \mathbb{P}(\mathcal{E}) \to C \) is the projective bundle map. We call \( \mathcal{E} \) \textit{good} if \( N \geq 3e \); by (2.2), any Tschirnhausen bundle of an integral cubic cover will be good. We say a curve in \( \mathbb{P}(\mathcal{E}) \) is \textit{horizontal} if it has positive intersection with a fiber of \( \pi \), and \textit{vertical} if not. By the \textit{isomorphism class} of an element of \( |\mathcal{L}_\mathcal{E}| \), we mean its orbit under the bundle automorphism group of \( \mathbb{P}(\mathcal{E}) \).

\textbf{Lemma 2.4.1.} Across all (isomorphism classes of) good \( \mathcal{E} \) with degree \( N \), the number of isomorphism classes of elements of \( |\mathcal{L}_\mathcal{E}| \) is \( O(q^{2N}) \).

\textit{Proof.} By Lemma 2.3.1 and (2.1), we can just apply the Siegel-Weil formula to

\[
\sum_{\mathcal{L} \in \text{Pic}^N(C)(\mathbb{F}_q) \text{ good}} \sum_{\mathcal{E} \in \text{VBun}_C(2, \mathcal{L})} \frac{q^{2N+4}}{(q-1)|\text{Aut}(\mathbb{P}(\mathcal{E}))(\mathbb{F}_q)|} \leq \sum_{\mathcal{L} \in \text{Pic}^N(C)(\mathbb{F}_q) \mathcal{E} \in \text{VBun}_C(2, \mathcal{L})} \frac{q^{2N+4}}{(q-1)|\text{Aut}(\mathbb{P}(\mathcal{E}))(\mathbb{F}_q)|}
\]
$\frac{|(\text{Pic}^0 C)(\mathbb{F}_q)|q^{2N+4}}{q-1}q^{3(g_C-1)}\zeta_C(2)$. 

\[ \square \]

Let $F_P$ be the fiber of $P$ under $\pi$, and $\mathcal{I}_{F_P}$ the associated sheaf of ideals, a line bundle. We denote by $F_p^{(2)}$ the subscheme of $\mathbb{P}(\mathcal{E})$ associated to $\mathcal{I}_{F_P}^2$, i.e. a doubled fiber. We’ll use the fact that smoothness of a global section of $\mathcal{L}_\mathcal{E}$ on the fiber above $P$ can be detected by considering its restriction to $F_p^{(2)}$. First, a local calculation.

**Lemma 2.4.2.** For a good $\mathcal{E}$ and a closed point $P$ of $C$, the probability of an element of $H^0(F_p^{(2)}, \mathcal{L}_\mathcal{E}|_{F_p^{(2)}})$ not vanishing on the fiber and being smooth is $(1 - q^{-2\deg P})(1 - q^{-3\deg P})$.

**Proof.** These sections on the doubled fiber can be written in the form $(a_0 + a_1x)u^3 + (b_0 + b_1x)u^2v + (c_0 + c_1x)uv^2 + (d_0 + d_1x)v^3$, where the coefficients $a_i$, $b_i$, $c_i$, and $d_i$ are drawn from $\mathbb{F}_{q^{\deg P}}$. We just need to count the sections that don’t have all of $a_0$, $b_0$, $c_0$, and $d_0$ equal to zero, and such that there is no point of the fiber where the section and its partial derivatives with respect to $u$, $v$, and $x$ all vanish. A simple calculation (see e.g. [EW15, Lemma 9.8] or [Zha13, Lemma 4.0.0.7]) gives the probability as $(1 - q^{-2\deg P})(1 - q^{-3\deg P})$. \[ \square \]

For a sum of distinct closed points $D = \sum P_i$ on the base $C$, let $F_D^{(2)} = \bigcup F_p^{(2)}$. The next lemma says we can interpolate local sections on a finite set of fibers whose combined degree isn’t too large.

**Lemma 2.4.3.** For a sum of distinct closed points $D = \sum P_i$ on the base $C$, the restriction map from $H^0(\mathbb{P}(\mathcal{E}), \mathcal{L}_\mathcal{E})$ to $H^0(F_D^{(2)}, \mathcal{L}_\mathcal{E}|_{F_D^{(2)}})$ is surjective if $\deg D \leq \min\{\frac{N-3e,N+3e}{4} - g_C\}$.

**Proof.** Consider the exact sequence

\[ 0 \to \mathcal{I}_{F_D^{(2)}} \to \mathcal{O}_{\mathbb{P}(\mathcal{E})} \to \mathcal{O}_{F_D^{(2)}} \to 0. \]
After tensoring this with $L_E$, it suffices to show that $H^1$ of the first term vanishes. Using (2.1) to interpret this as a cohomology group on the base curve, and noting that $\deg(O_C(-2D) \otimes \det E^{-1}) = -N - 2\deg D$, vanishing follows from the $h^1$ part of Lemma 2.2.2.

**Lemma 2.4.4.** Across all good $E$ with degree $N$, the number of isomorphism classes of elements of $|L_E|$ with more than one horizontal geometric component or with cyclic Galois group is $O(q^{2N})$.

**Proof.** If an element of $|L_E|$ reduces on some fiber to a degree 2 point and a degree 1 point, and reduces on another fiber to a degree 3 point, it’s horizontally geometrically irreducible with Galois group $S_3$. The set of elements that avoid one of these reduction types on every fiber has density 0.

We’ll call an element of $|L_E|$ horizontally irreducible if it has only one horizontal geometric component.

**Lemma 2.4.5.** For a good $E$ with degree $N$, and a closed point $P$ of $C$, the number of horizontally irreducible elements of $|L_E|$ containing the fiber over $P$ is $O(q^{2N-4\deg P})$.

**Proof.** First, note that for such an element, its intersection number with $C_0$ is at least $\deg P$. Since this intersection number is equal to $\frac{N-3\epsilon}{2}$ by (2.2), we have that $\deg P > \frac{N-3\epsilon}{2}$ would imply that the element of $|L_E|$ contains $C_0$ as a component, and thus is not horizontally irreducible. So we may restrict to $P$ such that $\deg P \leq \frac{N-3\epsilon}{2}$.

A global section of $L_E$ giving such an element factors as a fixed defining section for the fiber times a global section of $L_E \otimes I_{F_P}$, so we can just bound the number of global sections of the latter. We use (2.1) to transfer this to bounding $h^0(C, \text{Sym}^3 E \otimes \det E^{-1} \otimes O_C(-P))$, and then apply Lemmas 2.3.2 and 2.3.3.

**Lemma 2.4.6.** Across all good $E$ with degree $N$, the number of isomorphism classes of geometrically irreducible elements of $|L_E|$ singular above a point $P$ of $C$ is $O(q^{2N-2\deg P})$. 
Proof. This follows from Lemma 2.4.1 and the uniformity estimate in [GHM, Section 3].
Desingularizing such an element at its singular point above $P$ gives an irreducible cover of
lower genus, and the fibers of the map of sets sending a singular cover to its desingularization
are bounded in terms of $\deg P$, because there are not many ways to glue together points or
squish tangent vectors of a degree 3 cover on just one fiber.

Lemma 2.4.7. Let $r \geq 1$. Let $\Omega(N, r)$ be the number of isomorphism classes of elements of
$|L_{E}|$, across all good $E$ with degree $N$, that are smooth over the finitely many points of $C$ of
degree at most $r$. Then
$$
\lim_{N \to \infty} \frac{\Omega(N, r)}{q^{2N}} = \frac{|(\text{Pic}^{0}C)(\mathbb{F}_{q})|_{C}(2)}{(q-1)q^{g_{C}-1}} \prod_{P \in C \text{ s.t. } \deg P \leq r} (1 - q^{-2\deg P})(1 - q^{-3\deg P}).
$$

Proof. Pick a constant $\delta$ such that $0 < \delta < \frac{1}{3}$. We’re only going to look at $E$ such that
$e \leq \delta N$. So we’re losing all the curves that live on $\mathbb{P}(E)$’s with $\delta N < e \leq \frac{N}{3}$. But that’s
all right: on each one of these, by Lemma 2.3.1 and the automorphism fact in Section
2.2.1, we have at most
$$
\frac{q^{2N+4}}{(q-1)^{2}q^{e+1-g_{C}}} \sim q^{2N-e} < q^{2N-\delta N}
$$
isomorphism classes. There are $O((\frac{1}{3} - \delta)N)$ surfaces in this cusp, so the number of isomorphism classes we’re losing is
$O(Nq^{(2-\delta)N}) = O(q^{(2-\delta+\epsilon)N}) = o(q^{2N})$. Thus ignoring these surfaces won’t affect the limit
above.

So for a given value of $N$, we’re only looking at $\mathbb{P}(E)$’s with $e$ up to $\delta N$. Take $N$ such
that both $\frac{N-3g_{C}}{4} - g_{C}$ and $\frac{N-3N}{4} - g_{C} = \frac{(1-3\delta)N}{4} - g_{C}$ are bigger than the sum of the degrees
of all points of $C$ of degree at most $r$, and $N > 10g_{C} - 6$. Since by Lemma 2.4.3 we have
surjectivity onto doubled fibers over collections of points on $C$ whose degrees sum to at most
$\min\{\frac{N-3e,N+3e}{4}\} - g_{C}$, the number of elements of $|L_{E}|$ on one of our $\mathbb{P}(E)$’s smooth at these
points will be
$$
\frac{q^{2N+4(1-g_{C})}}{(q-1)^{2}} \prod_{P \in C \text{ s.t. } \deg P \leq r} (1 - q^{-2\deg P})(1 - q^{-3\deg P}).
$$
We just need to divide this by the automorphism group size and sum over the surfaces $\mathbb{P}(E)$ with $e$ up to $cN$.

So, on the nose for big enough $N$, the number of isomorphism classes in our $\delta$-range that
are smooth at all the points of degree at most \( r \) is

\[
\frac{q^{2N+4(1-gc)}}{q-1} \left( \prod_{P \in C \text{ s.t. } \deg P \leq r} (1 - q^{-2 \deg P})(1 - q^{-3 \deg P}) \right).
\]

\[
\sum_{\mathcal{L} \in \text{Pic}^N(C)(\mathbb{F}_q)} \sum_{\text{good } \mathcal{E} \in \text{VBun}_{C,2}(\mathcal{L}) \text{ with } e \leq \delta N} \frac{1}{|\text{Aut } \mathcal{P}(\mathcal{E})(\mathbb{F}_q)|}
\]

\[
= \frac{q^{2N}|(\text{Pic}^0 C)(\mathbb{F}_q)|\zeta_C(2)}{(q-1)q^{gc-1}} \left( \prod_{P \in C \text{ s.t. } \deg P \leq r} (1 - q^{-2 \deg P})(1 - q^{-3 \deg P}) \right) + O(q^{(2-\delta)N}).
\]

Dividing by \( q^{2N} \) and letting \( N \) tend to infinity gives us what we wanted. \( \square \)

**Lemma 2.4.8.** Let \( \Omega(N) \) be the number of isomorphism classes of smooth elements of \( |\mathcal{L}\mathcal{E}| \) across all good \( \mathcal{E} \) with degree \( N \). Then

\[
\lim_{N \to \infty} \frac{\Omega(N)}{q^{2N}} = \frac{|(\text{Pic}^0 C)(\mathbb{F}_q)|}{(q-1)q^{gc-1}\zeta_C(3)}.
\]

**Proof.** Given a value of \( r \), we have

\[
\lim_{N \to \infty} \frac{\Omega(N)}{q^{2N}} \leq \lim_{N \to \infty} \frac{\Omega(N,r)}{q^{2N}} = \frac{|(\text{Pic}^0 C)(\mathbb{F}_q)|\zeta_C(2)}{(q-1)q^{gc-1}} \left( \prod_{P \in C \text{ s.t. } \deg P \leq r} (1 - q^{-2 \deg P})(1 - q^{-3 \deg P}) \right).
\]

Taking \( r \to \infty \) gives us that

\[
\lim_{N \to \infty} \frac{\Omega(N)}{q^{2N}} \leq \frac{|(\text{Pic}^0 C)(\mathbb{F}_q)|}{(q-1)q^{gc-1}\zeta_C(3)}.
\]

So we’ve bounded the limit from above; now let’s bound it from below. By Lemmas 2.4.4, 2.4.5, and 2.4.6, we have

\[
\frac{\Omega(N)}{q^{2N}} \geq \frac{\Omega(N,r)}{q^{2N}} - O\left( \sum_{P \in C \text{ s.t. } \deg P > r} \frac{q^{2N-2 \deg P}}{q^{2N}} \right).
\]
\[ \frac{\Omega(N, r)}{q^{2N}} - o(1) - O \left( \sum_{P \in C \text{ s.t. } \deg P > r} q^{-2 \deg P} \right) \]

That sum is bounded above by the tail of the sum that gives \( \zeta_C(2) \) (multiply out the Euler product). Since the zeta function converges at \( s = 2 \), the tail goes to 0 as \( r \to \infty \), so we have

\[ \lim_{N \to \infty} \frac{\Omega(N)}{q^{2N}} \geq \lim_{N \to \infty} \lim_{r \to \infty} \frac{\Omega(N, r)}{q^{2N}} = \frac{|(\text{Pic}\,^0 C)(\mathbb{F}_q)|}{(q-1)q^{gC-1} \zeta_C(3)}. \]

We’re now in a position to conclude the theorem in the introduction. By Section 2.3, we have \( N_3(C, m) = \Omega(\frac{m}{2}) \), so we’re done by Lemma 2.4.8.
Chapter 3

Integral points of bounded degree on $\mathbb{P}^1$ and in dynamical orbits

This chapter represents joint work with Wade Hindes.

3.1 Introduction

Let $K/\mathbb{Q}$ be a number field and let $S$ be a finite set of places of $K$ containing the archimedean ones. Siegel’s theorem is a fundamental result in the study of integral points on curves (we use below the modern language of $(D, S)$-integral points; see Section 2 for more details):

**Theorem 3.1.1** (Siegel). Let $C$ be a curve defined over $K$ and let $D$ be a non-empty effective divisor on $C$, also defined over $K$. Then if $D$ contains at least 3 distinct (geometric) points, any set of $(D, S)$-integral points in $C(K)$ is finite.

More classically, one can state this (and later results of this introduction) in terms of an affine embedding: if $C_K \subseteq \mathbb{A}^n$ is an affine curve with at least three points at infinity, then $C$ has only finitely many $K$-points whose coordinates are $S$-integers.

In fact, a curve $C$ can have infinitely many integral $K$-points only if $D$ comprises one or two points and $C$ has genus zero. Even in this infinite case, integral points are still known to be rare, in the following sense: when we order the $K$-points of $C$ by a Weil height $H(\cdot)$
on $C$, any set of integral points has density zero within the rational points of $C$.

**Theorem 3.1.2.** Let $D$ be a non-empty effective divisor on $\mathbb{P}^1$ defined over $K$, and let $\mathcal{R}$ be any set of $(D, S)$-integral points in $\mathbb{P}^1(K)$. Then

$$
\lim_{B \to \infty} \frac{\# \{ P \in \mathcal{R} \mid H(P) \leq B \}}{\# \{ P \in \mathbb{P}^1(K) \mid H(P) \leq B \}} = 0.
$$

See [Ser97, Chapter 9] for a proof in the case where $S$ is exactly the set of archimedean places; it also shows the proportion of integral points decreases to zero relatively fast.

More recently, Siegel’s theorem has been generalized, beyond integral points defined over a fixed number field, to integral points defined over varying number fields of bounded degree. This deep finiteness result [Lev09, Corollary 14.14] follows from work of Vojta [Voj92] and of Song and Tucker [ST99]:

**Theorem 3.1.3** (Levin). Let $d \geq 1$ be an integer, let $C$ be a curve defined over $K$, and let $D$ be a non-empty effective divisor on $C$, also defined over $K$. Then if $D$ contains at least $2d + 1$ points, any set of $(D, S)$-integral points contained in $\{ P \in C(\overline{Q}) \mid [K(P) : K] \leq d \}$ is finite.

**Remark 3.1.4.** Note that when $d = 1$, this recovers Siegel’s theorem. See [Lev16] for an elegant converse, which shows that in one sense, integral points of bounded degree on curves behave better than rational points. Some special cases of Theorem 3.1.3 were known earlier: if $C = \mathbb{P}^1$, it follows from the Thue-Siegel-Roth-Wirsing theorem [Wir71] on Diophantine approximation. For arbitrary curves, Corvaja and Zannier proved the theorem [CZ04, Corollary 1] in the case $d = 2$.

Given this finiteness result, it’s reasonable to ask if a higher-degree analogue of Theorem 3.1.2 holds. In other words: in the cases where $C$ has infinitely many integral points of degree $d$, are they still density zero within the rational points of degree $d$? Our first theorem
shows this is indeed true if $C$ has genus zero and the base field is $\mathbb{Q}$. For $d \geq 1$, let $\mathbb{P}^1(\overline{\mathbb{Q}}, d) = \{P \in \mathbb{P}^1(\overline{\mathbb{Q}}) \mid [\mathbb{Q}(P) : \mathbb{Q}] \leq d\}.$

**Theorem 3.1.5.** Let $D$ be a non-empty effective divisor on $\mathbb{P}^1$ defined over $K$, and let $\mathcal{R} \subset \mathbb{P}^1(\overline{\mathbb{Q}}, d)$ be a set of $(D, S)$-integral points. Then

$$\lim_{B \to \infty} \frac{\# \{P \in \mathcal{R} \mid H(P) \leq B \}}{\# \{P \in \mathbb{P}^1(\overline{\mathbb{Q}}, d) \mid H(P) \leq B \}} = 0.$$ 

**Remark 3.1.6.** If $d = 1$ this is a special case of Theorem 3.1.2, while if $D$ contains a $\mathbb{Q}$-point, it follows from [Bar15, Theorem 1.2] or [CLT12, Theorem 3.5.6]. However, in its full generality, Theorem 3.1.5 appears to be new.

To briefly sketch some of the main ideas in the proof of Theorem 3.1.5, consider the case where $d = 1$ and $S$ is the archimedean place. In this special case, there are stronger proofs available [Ser97, Chapter 9], but the following argument generalizes better.

By Lemma 3.2.2 below, it (roughly) suffices to prove that a set of the form

$$\mathcal{R} = \{P \in \mathbb{P}^1(\mathbb{Q}) : f(P) \in \mathbb{Z}\},$$

for some non-constant rational function $f(z) \in \mathbb{Q}(z)$, has relative density zero in $\mathbb{P}^1(\mathbb{Q})$. To do this, we consider the set of rational primes $\mathcal{P}_f$ such that $f$ has at least one pole $a_p \in \mathbb{P}^1(\mathbb{F}_p)$. Note that $\mathcal{P}_f$ has positive Dirichlet density by the Chebotarev density theorem. For each such prime $p \in \mathcal{P}_f$, we consider the reduction map $\pi_p : \mathbb{P}^1(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{F}_p)$ and look at the set

$$\mathcal{I}_p = \{P \in \mathbb{P}^1(\mathbb{Q}) : \pi_p(P) = a_p\}.$$ 

The density of $\mathcal{I}_p$ in $\mathbb{P}^1(\mathbb{Q})$ is $\frac{1}{p+1}$; that is, the residue classes modulo $p$ equidistribute with respect to the Weil height (each choice of residue class is equally likely). On the other hand, our set of interest $\mathcal{R}$ must be contained in the complement of $\mathcal{I}_p$ by construction, and moreover, the sets $\mathcal{I}_p$ and $\mathcal{I}_q$ are “independent” for distinct primes $p$ and $q$. Hence, the
density of $\mathcal{R}$ is bounded above by the product $\prod_{p \in \mathcal{P}_f} (1 - \frac{1}{p+1})$, which is zero since $\mathcal{P}_f$ is a set of positive density.

The argument becomes more complicated when $d > 1$, especially if $D$ doesn’t contain a point of $\mathbb{P}^1(\mathbb{Q})$, but still proceeds similarly.

While Theorem 3.1.5 is of independent interest, our original motivation for proving it was an application to arithmetic dynamics, which we’ll now explain.

In [Sil93], Silverman established the following dynamical corollary to Siegel’s theorem (here $\varphi^n = \varphi \circ \cdots \circ \varphi$ denotes the $n$th iterate of $\varphi$):

**Theorem 3.1.7** (Silverman). Let $\varphi(z) \in K(z)$ be a rational function of degree at least two. If $\varphi^2(z)$ is not a polynomial, then the forward orbit of $P \in \mathbb{P}^1(K)$,

$$\text{Orb}_\varphi(P) := \{P, \varphi(P), \varphi^2(P), \ldots\},$$

contains only finitely many $S$-integral points.

In light of Theorem 3.1.7, it is natural to ask if the number of integral points in an orbit of $\varphi$ can be uniformly bounded. We show that the answer is yes, and in fact we strengthen the statement in two ways: first, we allow $\varphi$ to be defined with arbitrary $\mathbb{Q}$-coefficients, and second, our bound depends only on the degree of the number field.

Some notation: for $S$ a finite set of places of $\mathbb{Q}$ containing $\infty$, let $\mathcal{O}_S$ denote the integral closure of $\mathbb{Z}_S$ within $\overline{\mathbb{Q}}$. When $S = \{\infty\}$, this is simply the ring of all algebraic integers; the reader is welcome to keep this intuitive example in mind throughout the chapter. Whenever we write $P \in \mathcal{O}_S$ for a point of $\mathbb{P}^1(\overline{\mathbb{Q}})$, that means $P$ is of the form $[\alpha : 1]$, for $\alpha \in \mathcal{O}_S$.

**Theorem 3.1.8.** Let $\varphi(z) \in \overline{\mathbb{Q}}(z)$ be a rational function of degree at least two and let $S$ be a finite set of places of $\mathbb{Q}$ containing the archimedean one. Then if $\varphi^2(z)$ is not a polynomial, there exists a constant $N = N(\varphi, d, S)$ such that for any point $P \in \mathbb{P}^1(\overline{\mathbb{Q}}, d)$, we have $\#(\text{Orb}_\varphi(P) \cap \mathcal{O}_S) \leq N$. 
CHAPTER 3. INTEGRAL POINTS OF BOUNDED DEGREE

Although it’s nice to have an upper bound on the number of integral points of \(\text{Orb}_\varphi(P)\), one expects that most orbits contain no integers at all. To test this intuition, we study the average number of integral points in orbits as we vary over \(P \in \mathbb{P}^1(\overline{\mathbb{Q}})\) of degree at most \(d\) and height at most \(B\). In particular, we show that this average tends to zero as the height grows. Moreover, since the choice of \(d\) is arbitrary, the following result can be roughly interpreted as: “a random algebraic number has no integral points in its orbit.”

For \(P \in \mathbb{P}^1(\overline{\mathbb{Q}})\), let \(H(P)\) denote its absolute multiplicative Weil height. Let \(\mathbb{P}^1(\overline{\mathbb{Q}}, d, B) = \{P \in \mathbb{P}^1(\overline{\mathbb{Q}}) \mid [\mathbb{Q}(P) : \mathbb{Q}] \leq d \text{ and } H(P) \leq B\}\); by Northcott’s theorem, this is a finite set. Then we have:

**Theorem 3.1.9.** Let \(\varphi(z) \in \overline{\mathbb{Q}}(z)\) be a rational function of degree at least two and let \(S\) be a finite set of places of \(\mathbb{Q}\) containing the archimedean one. Then if \(\varphi^2(z)\) is not a polynomial,

\[
\lim_{B \to \infty} \frac{\sum_{P \in \mathbb{P}^1(\overline{\mathbb{Q}}, d, B)} \#(\text{Orb}_\varphi(P) \cap \mathcal{O}_S)}{\#\mathbb{P}^1(\overline{\mathbb{Q}}, d, B)} = 0
\]

for all \(d \geq 1\).

The idea behind these dynamical results is that the set of points with integral image under a map is itself integral with respect to the divisor obtained by pulling back the point at infinity. Our Theorem 3.1.8 then follows quickly from Theorem 3.1.3 (or even just the older result of Wirsing for \(\mathbb{P}^1\) [Wir71]), along with some standard properties of dynamical heights. Theorem 3.1.9 in turn follows from our density result in Theorem 3.1.5.

The dynamical results in this chapter generalize [Hin15, Theorem 1.2], which studies averages over a fixed number field.

### 3.2 Notation and previous results

In this section, we establish some notation for the rest of the chapter, and state known results that we’ll use.
There are various roughly equivalent definitions of integral points on a variety, so we’ll fix a convenient one for our purposes. For a number field $K$, a variety $X$ defined over $K$, a divisor $D$ on $X$ defined over $K$, and a finite set $S$ of places of $K$ containing the archimedean ones, we say that $\mathcal{R} \subset (X \setminus D)(\overline{\mathbb{Q}})$ is a set of $(D, S)$-integral points if there exists a global Weil function $\lambda_D$ such that for all places $v$ of $K$ not in $S$, we have $\lambda_{D,v}(P) \leq 0$ for all $P \in \mathcal{R}$. We refer the reader to [Voj11, Chapter 1] and [Lan83, Chapter 10] for the definition of a global Weil function as a suitable collection of local Weil functions; we’ll simply cite the properties relevant to us as needed.

Remark 3.2.1. This use of Weil functions gives a notion of integral points that is perhaps more general than one’s intuitive definition. For example, when $D$ is the point at infinity, and $S$ is the archimedean place of $\mathbb{Q}$, both the integers $\mathbb{Z}$ and the half-integers $\frac{1}{2}\mathbb{Z}$, viewed inside of $\mathbb{P}^1$ via $\alpha \mapsto [\alpha : 1]$, are sets of $(D, S)$-integral points. Loosely, any set such that denominators can be simultaneously cleared to yield a set with integral coordinates is $(D, S)$-integral.

The following “clearing denominators” lemma [Voj11, Lemma 1.4.6] will be of particular use:

**Lemma 3.2.2.** Let $\mathcal{R}$ be a $(D, S)$-integral set of points on $X$, and let $f$ be a rational function with no poles outside of $D$. Then there is some constant $b \in K^\times$ such that $b \cdot f(P)$ is integral for all $P \in \mathcal{R}$.

With the exception of Theorem 3.1.5, however, the above general notion of integrality is only used within the proofs, not in stating our dynamical results. For that, we need only the simpler definition of $\mathcal{O}_S$ given above Theorem 3.1.8.

We’ll use two different notions of height. First, for a point $P \in \mathbb{P}^1(\overline{\mathbb{Q}})$, let $H(P)$ denote the absolute multiplicative Weil height of $P$, for which there are various equivalent definitions. One of them: let $H([1 : 0]) = 1$, while for $\alpha \in \overline{\mathbb{Q}}$, let $H([\alpha : 1]) =$
\[ (a_d \prod_{\text{conjugates } \alpha'} \max\{1, |\alpha'|\})^{\frac{1}{[\mathbb{Q} : \mathbb{Q}]}}, \] where \( a_d \) is the leading coefficient of \( \alpha \)'s minimal polynomial over \( \mathbb{Z} \); here we obtain the minimal polynomial over \( \mathbb{Z} \) from the minimal monic polynomial over \( \mathbb{Q} \) by multiplying by the smallest positive integer that clears denominators.

Second, to a non-constant rational map \( \varphi \in \mathbb{Q}(z) \) of degree \( r \geq 2 \), we can associate another height function \( \hat{h}_{\varphi} \) on \( \mathbb{P}^1(\mathbb{Q}) \) called the (logarithmic) canonical height:

\[ \hat{h}_{\varphi}(P) = \lim_{n \to \infty} \frac{\log H(\varphi^n(P))}{r^n}; \]

see, for instance [Sil07, §3.4]. The canonical height behaves well under iteration: \( \hat{h}_{\varphi}(\varphi^n(P)) = r^n \hat{h}_{\varphi}(P) \). Moreover, a point \( P \) has canonical height 0 if and only if it is a preperiodic point for \( \varphi \), i.e., its forward orbit is finite.

Both of these heights satisfy the Northcott property [Sil07, Theorems 3.7 and 3.12]: for fixed values of \( d \) and \( B \), there are only finitely many points of \( \mathbb{P}^1(\mathbb{Q}) \) of degree at most \( d \) and height at most \( B \).

Next, for \( d, B \geq 1 \), we defined in the introduction \( \mathbb{P}^1(\mathbb{Q}, d) = \{ P \in \mathbb{P}^1(\mathbb{Q}) \mid [\mathbb{Q}(P) : \mathbb{Q}] \leq d \} \), as well as the (finite) subset \( \mathbb{P}^1(\mathbb{Q}, d, B) = \{ P \in \mathbb{P}^1(\mathbb{Q}) \mid [\mathbb{Q}(P) : \mathbb{Q}] \leq d \text{ and } H(P) \leq B \} \). While an easy crude bound on the size of \( \mathbb{P}^1(\mathbb{Q}, d, B) \) would suffice for our purposes, it’s clarifying to state some recent stronger results. For \( d \) fixed and \( B \) increasing, Masser and Vaaler [MV08] determined its asymptotic size:

**Theorem 3.2.3** (Masser-Vaaler). As \( B \) grows, the number of elements \( \alpha \in \mathbb{Q} \) such that \( [\mathbb{Q}(\alpha) : \mathbb{Q}] = d \) and \( H(\alpha) \leq B \) is asymptotic to \( c_{Q,d} \cdot B^{d(d+1)} \), for \( c_{Q,d} \) an explicit positive constant.

More generally, they established an asymptotic for points of degree \( d \) over arbitrary number fields [MV07], as well as a power-saving error term, but we won’t need that here. If we restrict attention to \( S \)-integral points, Barroero [Bar15, Theorem 1.2] showed:
Theorem 3.2.4 (Barroero). Let $S$ be a finite set of places of $\mathbb{Q}$ containing the archimedean one. Then as $B$ grows, the number of elements $\alpha \in \mathcal{O}_S$ such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ and $H(\alpha) \leq B$ is asymptotic to $a_{\mathbb{Q},d,S} \cdot B^d (\log B)^{|S|-1}$, for $a_{\mathbb{Q},d,S}$ an explicit positive constant.

Barroero also obtained an error term, as well as the asymptotic over an arbitrary base number field rather than just over $\mathbb{Q}$, but again we won’t need that full generality.

3.3 Finiteness of integral images

Lemma 3.3.1. Let $\varphi(z) \in \mathbb{C}(z)$ be a rational map of degree $r \geq 2$. If $\varphi^2(z)$ is not a polynomial, then the number of distinct poles of $\varphi^n(z)$ goes to $\infty$ as $n \to \infty$.

Proof. If $\infty$ is not a periodic point for $\varphi$, then $\varphi^n$ has at least $r^{n-2}$ poles; see [Sil07, Ex. 3.37(a)]. On the other hand, if $\infty$ is a periodic point of exact order $m$, then note that by our assumption on $\varphi^2$ and [Sil07, Theorem 1.7], $\infty$ is a fixed point of $\varphi^m$ but not totally ramified. Hence $\varphi^m$ has at least $r^{n-2} + 2$ poles by [Sil07, Ex. 3.37(b)]. In either case, the statement follows. \qed

We’ll write $x_0$ and $x_1$ for the natural coordinates on the projective line.

Proposition 3.3.2. Let $\varphi(z) \in \overline{\mathbb{Q}}(z)$ be a rational map with at least $2d + 1$ distinct poles and let $S$ be a finite set of places of $\mathbb{Q}$ containing the archimedean one. Then there are only finitely many points $P \in \mathbb{P}^1(\overline{\mathbb{Q}}, d)$ such that $\varphi(P) \in \mathcal{O}_S$.

Proof. Let $\mathcal{R} = \varphi(\mathbb{P}^1(\overline{\mathbb{Q}}, d)) \cap \mathcal{O}_S$, let $K$ be the smallest number field over which the coefficients of $\varphi$ can be defined, and let $S'$ be the set of places of $K$ lying over $S$. By [Voj11, (1.3.5)], setting $\lambda_{\{\infty\}, v} = \frac{1}{|K: \mathbb{Q}|} \log \max(1, \|[x_0 : x_1]\|_v)$ for $v \notin S'$ gives a global Weil function $\lambda_{\{\infty\}}$, which thus shows $\mathcal{R}$ to be a set of $(\{\infty\}, S')$-integral points. By [Voj11, Lemma 1.3.3(d)], $\lambda_{\{\infty\}} \circ \varphi$ is a global Weil function for the divisor $\varphi^*\{\infty\}$ on $\mathbb{P}^1$. From our earlier definition of
integral points in Section 2, the subset of $\mathbb{P}^1(\overline{\mathbb{Q}}, d)$ as in the proposition is immediately seen to be $(\varphi^*\{\infty\}, S')$-integral. By Theorem 3.1.3, there can only be finitely many such points of degree at most $d$, since $\varphi^*\{\infty\}$ contains at least $2d + 1$ distinct points by assumption. 

3.4 Upper bounds for orbits

**Proposition 3.4.1.** Let $\varphi(z) \in \overline{\mathbb{Q}}(z)$ be a rational map of degree $r \geq 2$ such that $\varphi^2(z)$ is not a polynomial, and let $S$ be a finite set of places of $\mathbb{Q}$ containing the archimedean one. Then there exists a constant $N' = N'(\varphi, d, S)$ such that for any non-preperiodic point $Q \in \mathbb{P}^1(\overline{\mathbb{Q}}, d)$, we have that $\varphi^n(Q) \in \mathcal{O}_S$ implies $n \leq N'$.

**Proof.** By Lemma 3.3.1, there exists $N_1$ such that $\varphi^{N_1}$ has at least $2d + 1$ distinct poles. By Proposition 3.3.2, there are only finitely many points $P \in \mathbb{P}^1(\overline{\mathbb{Q}}, d)$ such that $\varphi^{N_1}(P) \in \mathcal{O}_S$. Let $C$ be the maximum of the canonical heights $\hat{h}_\varphi(P)$ of these points. If $\varphi^n(Q) \in \mathcal{O}_S$ for $Q$ as in the proposition and $n \geq N_1$, then $\varphi^{n-N_1}(Q)$ has height at most $C$. Thus

$$r^n \hat{h}_\varphi(Q) = \hat{h}_\varphi(\varphi^n(Q)) = \hat{h}_\varphi(\varphi^{N_1}(\varphi^{n-N_1}(Q))) = r^{N_1} \hat{h}_\varphi(\varphi^{n-N_1}(Q)) \leq r^{N_1} C.$$

So if $M = M(\varphi, d)$ is the minimal positive value of the canonical height $\hat{h}_\varphi$ on $\mathbb{P}^1(\overline{\mathbb{Q}}, d)$ (which immediately exists by the Northcott property), then we must have $r^n \leq \frac{r^{N_1} C}{M}$, which proves the proposition.

(Proof of Theorem 3.1.8). Proposition 3.4.1 immediately reduces this to finding a uniform bound just for such points $P$ that are preperiodic. But those points have canonical height 0, so by Northcott there are finitely many of them, since their degree is bounded by assumption. Thus any bound bigger than the orbit lengths of all the preperiodic $P$’s will suffice. 

**Remark 3.4.2.** If $\varphi^2(z) \in \overline{\mathbb{Q}}[z]$ and $\varphi(z)$ is not itself a polynomial, then after a change of variables $\varphi(z)$ has the form $1/\zeta^r$; see [Sil93, Proposition 1.1].
3.5 The relative density of integral points

(Proof of Theorem 3.1.5). Recall that as $B$ grows, $\#\mathbb{P}^1(\overline{\mathbb{Q}}, d, B)$ is asymptotic to $c_{Q,d}B^{d(d+1)}$ by Theorem 3.2.3.

First, suppose that $D$ contains $\infty = [1:0]$. Then $\frac{x_0}{x_1}$ is a regular function on the complement of $D$, so by Lemma 3.2.2, there is a constant $b \in \overline{\mathbb{Q}}^\times$ such that $\frac{bx_0}{x_1}(P) \in \mathcal{O}_{S'}$ for all $P \in \mathcal{R}$, where $S'$ is the finite set of places of $\mathbb{Q}$ that the places of $S$ lie over. If we expand $S'$ to a possibly larger finite set of places $T$ of $\mathbb{Q}$ such that it contains all the places above which $b$ has absolute value less than 1, we see that $\mathcal{R} \subset \mathcal{O}_T$. Thus $\#\mathcal{R} \cap \mathbb{P}^1(\overline{\mathbb{Q}}, d, B)$ is bounded above by $\#\mathcal{O}_T \cap \mathbb{P}^1(\overline{\mathbb{Q}}, d, B)$. Since $\#\mathcal{O}_T \cap \mathbb{P}^1(\overline{\mathbb{Q}}, d, B)$ is asymptotic to $a_{Q,d,T}B^{d^2}(\log B)^{|T|-1}$ as $B$ grows, the limit in the theorem statement is zero.

Now suppose instead that $D$ doesn’t contain $\infty$. Then it has a finite point $[\beta : 1]$. Consider the rational function $\frac{x_1}{x_0 - \beta x_1}$; this is a regular function on the complement of $D$, so by Lemma 3.2.2, there is again a constant $b \in \overline{\mathbb{Q}}^\times$ such that $\frac{bx_1}{x_0 - \beta x_1}(P) \in \mathcal{O}_{S'}$ for all $P \in \mathcal{R}$. In particular, for all non-infinite $[\alpha : 1] \in \mathcal{R}$, we see that $\frac{1}{\alpha - \beta} \in \mathcal{O}_T$, where $T$ is the finite set of places containing $S'$ and all places above which $b$ can have absolute value less than 1. Hence, to prove Proposition 3.1.5 it suffices to show that the set of points $\alpha \in \overline{\mathbb{Q}}$ satisfying $\frac{1}{\alpha - \beta} \in \mathcal{O}_T$ and $[Q(\alpha) : Q] \leq d$ has relative density zero inside $\mathbb{P}^1(\overline{\mathbb{Q}}, d)$. In the special case where one can choose $\beta$ to lie in $\mathbb{Q}$, we again get an asymptotic bound of a constant times $B^{d^2}(\log B)^{|T|-1}$ from Theorem 3.2.4. But for the general case, this doesn’t work; instead we’ll show relative density zero by sieving out a family of local conditions.

First we make a couple reductions. Since $\#\mathbb{P}^1(\overline{\mathbb{Q}}, d - 1, B)$ is asymptotic to $c_{Q,d-1}B^{d(d-1)}$, one need only handle the set where $[Q(\alpha) : Q] = d$. Furthermore, we may restrict attention to the subset of $\alpha$’s where $[Q(\alpha, \beta) : Q(\beta)] = [Q(\alpha) : Q] = d$. To see this, let $L = Q(\beta)$, and let $g(x) = t_d x^d + \ldots + t_1 x + t_0$ be a polynomial with indeterminate coefficients. Then [DF04, §14.6
Theorem 32] implies that \( g \) is irreducible over \( L(t_0, \ldots, t_d) \). By [Coh81, Theorem 2.1], the polynomial remains irreducible over \( L \) for most choices of \( t_0, \ldots, t_d \in \mathbb{Z} \), when integer vectors are ordered by sup norm. However, for an algebraic number \( \alpha \) satisfying \([\mathbb{Q}(\alpha) : \mathbb{Q}] = d \) and \([\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)] < d\), its minimal polynomial over \( \mathbb{Z} \) will be reducible over \( L \). Thus it follows from Cohen’s result above, [BG06, Lemma 1.6.7], and Theorem 3.2.3 that the set of such \( \alpha \)'s has relative density zero in \( \mathbb{P}^1(\overline{\mathbb{Q}}, d) \).

To outline the argument going forward, let \( \mathcal{P} \) be the set of rational primes that split completely in the Galois closure of \( \mathbb{Q}(\beta) \). By the Chebotarev density theorem, \( \mathcal{P} \) has positive Dirichlet density. We may discard finitely many primes of \( \mathcal{P} \) and assume that \( \beta \) is integral at all \( p \in \mathcal{P} \) and that \( \mathcal{P} \) does not meet \( T \). Next, for each \( p \in \mathcal{P} \), we can fix a prime ideal \( p \) of \( \mathbb{Q}(\beta) \) lying over \( p \), and since there is no residue field extension we may choose an integer \( 0 \leq r_p \leq p - 1 \) such that \( |r_p - \beta|_p < 1 \). Now, consider the set

\[ \mathcal{I}_p := \{ \alpha \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] = d, \ |\alpha - r_p| < 1 \text{ for some absolute value } |\cdot| \text{ of } \overline{\mathbb{Q}} \text{ lying over } |\cdot|_p \}. \]

For an element \( \alpha \) of \( \mathcal{I}_p \), we have \( |\frac{1}{\alpha - \beta}| = |\frac{1}{(\alpha - r_p) + (r_p - \beta)}| > 1 \), and therefore \( \frac{1}{\alpha - \beta} \notin \mathcal{O}_T \). Thus \( \mathcal{R} \cap \mathcal{I}_p = \emptyset \), and so we’ll be done if we show that the complement of \( \bigcup_{p \in \mathcal{P}} \mathcal{I}_p \) has density zero. Rather than counting elements of the complement directly, we’ll instead bound its size from above, by counting polynomials whose roots lie in the complement.

To make this precise, let \( f(x) = a_dx^d + a_{d-1}x^{d-1} + \cdots + a_0 \) be a primitive irreducible polynomial with integer coefficients and write \( f(x) = a_d \prod(x - \alpha_i) \) in \( \mathbb{C}[x] \). Then we define \( \hat{H}(f) := \max\{|a_i|\} \) to be the naive height of \( f \). For \( \alpha \) a root of \( f \), the height of \( \alpha \) and the naive height of \( f \) are known to be comparable in the following sense:

\[
\frac{1}{\sqrt{d + 1}} H(\alpha)^d \leq \hat{H}(f) \leq \left(\frac{d}{|d/2|}\right)H(\alpha)^d,
\]

see, for instance [BG06, Lemma 1.6.7]. Now let \( p_1, \ldots, p_k \) be the first \( k \) primes in \( \mathcal{P} \). Let \( \text{Pol}^+(d, B) \) be the set of integer polynomials of degree \( d \), with positive leading coefficient,
and naive height at most $B$. Lastly, for any $m|p_1 \cdots p_k$, let

$$\mathcal{F}_m(d, B) := \# \{ f \in \text{Pol}^+(d, B) \mid \text{for each } p|m, \ a_d \not\equiv 0 \pmod{p}, \ f(r_p) \equiv 0 \pmod{p} \}. \quad (3.2)$$

By counting the number of integers in a residue class in a box (at each prime we’re excluding a single congruence class for the leading coefficient, and enforcing one condition on the remaining terms), we see that as $B$ grows,

$$\mathcal{F}_m(d, B) = \prod_{p|m} \left( \frac{p-1}{p^2} \right) 2^d B^{d+1} + O(B^d)$$

On the other hand, the irreducible polynomials counted by $\mathcal{F}_m(d, B)$ give rise to elements of $\cap_{p|m} \mathcal{I}_p$; to see this, suppose that $\alpha \in \overline{Q}$ is a root of an irreducible integer polynomial $f(x)$ of this type. Then considering the equation

$$0 = a_d \alpha^d + a_{d-1} \alpha^{d-1} + \ldots + a_0 = a_d (\alpha - r_p + r_p)^d + a_{d-1} (\alpha - r_p + r_p)^{d-1} + \ldots + a_0$$

we see, dividing by $a_d$ to obtain the minimal polynomial equation for $\alpha - r_p$ over $Q$, that the norm $N_{Q(\alpha)/Q}(\alpha - r_p) = \frac{(-1)^d f(r_p)}{a_d}$. Let $|\cdot|$ be an absolute value of $\overline{Q}$ lying over $|\cdot|_p$. Since the norm, which is the product of the Galois conjugates of $\alpha - r_p$, has absolute value less than 1 under $|\cdot|$, we must have, for some automorphism $\sigma \in \text{Gal}(\overline{Q}/Q)$, that $\sigma(\alpha - r_p) = \sigma(\alpha) - r_p$ satisfies $|\sigma(\alpha) - r_p| < 1$, and thus $\sigma(\alpha) \in I_p$. Now, by our earlier reduction to the case $[Q(\alpha, \beta) : Q(\beta)] = [Q(\alpha) : Q] = d$, we have that $\text{Gal}(\overline{Q}/Q(\beta))$ acts transitively on the conjugates of $\alpha$, so in fact we can choose $\sigma$ to lie in $\text{Gal}(\overline{Q}/Q(\beta))$. Thus the absolute value $|\cdot|'$ of $\overline{Q}$ given by $|\cdot|' = |\cdot| \circ \sigma$ also lies over $|\cdot|_p$, and we have $|\alpha - r_p|' < 1$. So we in fact have $\alpha \in I_p$.

Next, let $\mathcal{G}_k(d, B)$ be the number of polynomials in $\text{Pol}^+(d, B)$ not contained in any of the subsets defining $\mathcal{F}_{p_i}(d, B)$ for $i = 1, \ldots, k$. By inclusion-exclusion, we have

$$\mathcal{G}_k(d, B) = \sum_{m|p_1 \cdots p_k} \mu(m) \mathcal{F}_m(d, B)$$
\[
= \prod_{i=1}^{k} \left( 1 - \frac{p_i - 1}{p_i^2} \right) 2^d B^{d+1} + O(B^d).
\]

Now we count algebraic numbers. Let \( \alpha \in \overline{\mathbb{Q}} \) have degree \( d \), and let \( f \) be its minimal polynomial over \( \mathbb{Z} \). If \( \alpha \) has height at most \( B \), then by (3.1), we see \( f \) has naive height
\[
\tilde{H}(f) \leq \binom{d}{[d/2]} B^d.
\]
Thus the number of such \( \alpha \) not contained in \( \cup_{p \in \mathcal{P}} \mathbb{Z}_p \) is bounded above by
\[
d \cdot G_k(d, \binom{d}{[d/2]} B^d)
= \prod_{i=1}^{k} \left( 1 - \frac{p_i - 1}{p_i^2} \right) 2^d \binom{d}{[d/2]} B^{d+1} + O(B^{d^2}).
\]

We see that the relative density of \( \mathcal{R} \) is at most \( \frac{1}{c_{Q,d}} \) times the constant on \( B^{d(d+1)} \) above. However, now we can let \( k \) grow. Since \( \mathcal{P} \) had positive density in the primes, the product above converges to 0 as \( k \to \infty \): recall that an infinite product \( \prod (1 - a_i) \), with \( 0 \leq a_i < 1 \), converges to 0 if and only if \( \sum a_i \) diverges. In our case, \( a_i \) is on the order of \( \frac{1}{p_i} \); since the sum of the reciprocals of the primes diverges [Eul44, Theorema 19], the infinite product converges to 0.

\[\text{Corollary 3.5.1.} \quad \text{If } \varphi(z) \in \overline{\mathbb{Q}}(z) \text{ is a non-constant rational function, then}
\lim_{B \to \infty} \frac{\# \{ P \in \mathbb{P}^1(\overline{\mathbb{Q}}, d, B) \mid \varphi(P) \in \mathcal{O}_S \}}{\# \mathbb{P}^1(\overline{\mathbb{Q}}, d, B)} = 0.
\]

\[\text{Proof.} \quad \text{This follows directly from Theorem 3.1.5: as noted in the proof of Proposition 3.3.2, we have that } \{ P \in \mathbb{P}^1(\overline{\mathbb{Q}}, d) \mid \varphi(P) \in \mathcal{O}_S \} \text{ is a } (\varphi^*\{\infty\}, S') \text{-integral set of points.} \]

\[\text{(Proof of Theorem 3.1.9).} \quad \text{By Proposition 3.4.1, after discarding the finitely many preperiodic points, the numerator is at most}
\sum_{n=0}^{N'} \# \{ P \in \mathbb{P}^1(\overline{\mathbb{Q}}, d, B) \mid \varphi^n(P) \in \mathcal{O}_S \},
\]

so we’re done by Corollary 3.5.1.
Chapter 4

Slicing the stars: counting algebraic numbers, integers, and units of bounded degree and height

This chapter represents joint work with Robert Grizzard.

4.1 Introduction

A classical theorem of Northcott states that there are only finitely many elements of $\overline{\mathbb{Q}}$ of bounded degree and height. It’s then natural to ask, for interesting subsets $S \subset \overline{\mathbb{Q}}$ of bounded degree, how the number of elements of bounded height grows as we let the height bound increase. More precisely, one considers the asymptotics of

$$N(S, H) = \#\{x \in S \mid H(x) \leq H\},$$

where $H(x)$ is the absolute multiplicative Weil height of $x$ (see for example [BG06, p. 16]).

Many of the oldest instances of such asymptotic statements concern elements of a fixed number field. Schanuel [Sch79, Corollary] proved that, for any number field $K$, as $H$ grows,

$$N(K, H) = c_K \cdot H^{2[K:Q]} + O \left( H^{2[K:Q]-1} \log H \right),$$

where the constant $c_K$ involves all the classical invariants of the number field $K$, and the log $H$ factor disappears for $K \neq \mathbb{Q}$. 

42
Lang states analogous asymptotics for the ring of integers $\mathcal{O}_K$ and its unit group $\mathcal{O}_K^\ast$ [Lan83, Chapter 3, Theorem 5.2]:

\[
N(\mathcal{O}_K, \mathcal{H}) = \gamma_K \cdot \mathcal{H}^{[K:Q]}(\log \mathcal{H})^r + O(\mathcal{H}^{[K:Q]}(\log \mathcal{H})^{r-1}) ;
\]

\[
N(\mathcal{O}_K^\ast, \mathcal{H}) = \gamma_K^\ast \cdot (\log \mathcal{H})^r + O((\log \mathcal{H})^{r-1}) ,
\]

where $r$ is the rank of $\mathcal{O}_K^\ast$ and $\gamma_K$ and $\gamma_K^\ast$ are unspecified constants. That first count was later refined to a multi-term asymptotic by Widmer [Wid16, Theorem 1.1].

More recently, natural subsets that aren’t contained within a single number field have been examined. Masser and Vaaler [MV08, Theorem] determined the asymptotic for the entire set $\overline{\mathbb{Q}}_d = \{ x \in \overline{\mathbb{Q}} | [\mathbb{Q}(x) : \mathbb{Q}] = d \}$:

\[
N(\overline{\mathbb{Q}}_d, \mathcal{H}) = \frac{d \cdot V_d}{2\zeta(d+1)} \cdot \mathcal{H}^{d(d+1)} + O(\mathcal{H}^{d^2}(\log \mathcal{H})) ,
\]

(4.1)

where the log $\mathcal{H}$ factor disappears for $d \geq 3$, and $V_d$ is an explicit positive constant that we’ll define shortly.

This asymptotic was deduced from results of Chern and Vaaler [CV01] (discussed at length in section 4.2), which also imply an asymptotic for the set $\mathcal{O}_d$ of all algebraic integers of degree $d$, as noted by Widmer [Wid16, (1.2)]. It was sharpened by Barroero [Bar14, Theorem 1.1, case $k = \mathbb{Q}$]:

\[
N(\mathcal{O}_d, \mathcal{H}) = d \cdot V_{d-1} \cdot \mathcal{H}^{d^2} + O(\mathcal{H}^{d(d-1)}(\log \mathcal{H})) ,
\]

(4.2)

where again the log $\mathcal{H}$ factor disappears for $d \geq 3$.

After algebraic numbers and integers, it’s natural to turn to the problem of counting units and other interesting sets of algebraic numbers. It’s also desirable to obtain versions of these estimates with explicit error terms. These are the two purposes of this chapter.

We establish counts of units, algebraic integers of given norm, given trace, and given norm and trace in Corollaries 4.1.2-4.1.5, which follow from the more general Theorem 4.1.1.
stated below. As for explicit error bounds, we have made several improvements to the existing literature. The lack of explicit error terms in the results (4.1) and (4.2) is inherited from results of Chern and Vaaler on counting polynomials. Specifically, Chern and Vaaler mention (see [CV01, p. 6]) that it would be of interest to make the implied constant in [CV01, Theorem 3] explicit, but they were unable to do so. In this chapter we are able to make this constant explicit (Theorem 4.7.1 below), and we also prove an analogous result for monic polynomials (Theorem 4.8.1). We use these to obtain versions of (4.1) and (4.2) that are uniform in both \( H \) and \( d \). These, along with an explicit version of our result on counting units, are summarized below in Theorem 4.1.10.

4.1.1 Results

Throughout the chapter, we will understand the minimal polynomial of an algebraic number to be its minimal polynomial over \( \mathbb{Z} \); we obtain this by multiplying the minimal monic polynomial over \( \mathbb{Q} \) by the smallest positive integer such that all its coefficients become integers.

Counting algebraic integers, as in (4.2), is equivalent to counting only those algebraic numbers whose minimal polynomial has leading coefficient 1. Our primary goal in this chapter is to count algebraic numbers of fixed degree and bounded height subject to specifying any number of the leftmost and rightmost coefficients of their minimal polynomials. Besides specializing to the cases of algebraic numbers and algebraic integers above, this will allow us to count units, algebraic integers with given norm, algebraic integers with given trace, and algebraic integers with given norm and trace.

To state our theorem, we need a little notation. Our asymptotic counts will involve the Chern-Vaaler constants

\[
V_d = 2^{d+1}(d + 1)^s \prod_{j=1}^s \frac{(2j)^{d-2j}}{(2j + 1)^{d+1-2j}},
\]  

(4.3)
CHAPTER 4. SLICING THE STARS

where \( s = \lfloor (d - 1)/2 \rfloor \). These constants are volumes of certain star bodies discussed later.

For integers \( m, n, \) and \( d \) with \( 0 < m, 0 \leq n, \) and \( m + n \leq d, \) and integer vectors \( \vec{\ell} \in \mathbb{Z}^m \) and \( \vec{r} \in \mathbb{Z}^n \), we write \( \mathcal{N}(d, \ell, r, H) \) for the number of algebraic numbers of degree \( d \) and height at most \( H \), whose minimal polynomial is of the form

\[
f(z) = \ell_0 z^d + \cdots + \ell_{m-1} z^{d-(m-1)} + x_m z^{d-m} + \cdots + x_{d-n} z^n + r_{d-n+1} z^{n-1} + \cdots + r_d.
\]

Lastly, we set \( g = d - m - n \). In the statements below, the implied constants depend on all parameters stated other than \( H \).

**Theorem 4.1.1.** Fix \( d, \vec{\ell} \in \mathbb{Z}^m \), and \( \vec{r} \in \mathbb{Z}^n \) as above. Assume that \( \ell_0 > 0, \) that

\[
\gcd(\ell_0, \ldots, \ell_{m-1}, r_{d-n+1}, \ldots, r_d) = 1,
\]

and that \( r_d \neq 0 \) if \( n > 0 \). Then as \( H \to \infty \) we have

\[
\mathcal{N}(d, \ell, r, H) = d \cdot V_g \cdot H^{d(g+1)} + O \left( H^{d(g+\frac{1}{2})} \log H \right).
\]

This generalizes the situation one faces when counting algebraic integers, whose minimal polynomials are monic \((m = 1, n = 0, \vec{\ell} = (1))\). Certain special cases are of particular interest, and we prove stronger power savings terms for them.

**Corollary 4.1.2.** Let \( d \geq 2, \) and let \( \mathcal{N}(O_d^*, H) \) denote the number of units in the algebraic integers of height at most \( H \) and degree \( d \) over \( \mathbb{Q} \). Then as \( H \to \infty \) we have

\[
\mathcal{N}(O_d^*, H) = 2d \cdot V_{d-2} \cdot H^{d(d-1)} + O \left( H^{d(d-2)} \right).
\]

**Corollary 4.1.3.** Let \( \nu \neq 0 \) be an integer, \( d \geq 2, \) and let \( \mathcal{N}_{Nm=\nu}(d, H) \) denote the number of algebraic integers with norm \( \nu, \) of height at most \( H \) and degree \( d \) over \( \mathbb{Q} \). Then as \( H \to \infty \) we have

\[
\mathcal{N}_{Nm=\nu}(d, H) = d \cdot V_{d-2} \cdot H^{d(d-1)} + O \left( H^{d(d-2)} \right).
\]
Corollary 4.1.4. Let $\tau$ be an integer, $d \geq 2$, and let $N_{\text{Tr}=\tau}(d, H)$ denote the number of algebraic integers with trace $\tau$, of height at most $H$ and degree $d$ over $\mathbb{Q}$. Then as $H \to \infty$ we have

$$N_{\text{Tr}=\tau}(d, H) = d \cdot V_{d-2} \cdot H^{d(d-1)} + \begin{cases} O(H), & \text{if } d = 2 \\ O(H^3 \log H), & \text{if } d = 3 \\ O(H^{d(d-2)}), & \text{if } d \geq 4. \end{cases}$$

Corollary 4.1.5. Let $\nu \neq 0$ and $\tau$ be integers, $d \geq 3$, and let $N_{\text{Nm}=\nu, \text{Tr}=\tau}(d, H)$ denote the number of algebraic integers with norm $\nu$, trace $\tau$, of height at most $H$ and degree $d$ over $\mathbb{Q}$. Then as $H \to \infty$ we have

$$N_{\text{Nm}=\nu, \text{Tr}=\tau}(d, H) = d \cdot V_{d-3} \cdot H^{d(d-2)} + O(H^{d(d-3)}).$$

Remark 4.1.6. For two real-valued functions $f$ and $g$ with the same domain, we write $f = O(g)$ to mean there exists a constant $C > 0$ such that $|f(x)| \leq C|g(x)|$ for all $x$. In Theorem 4.1.1, the implied constant depends on $d$, $\ell$, and $\bar{\tau}$; in Corollary 4.1.2 on $d$; in Corollary 4.1.3 on $d$ and $\nu$; in Corollary 4.1.4 on $d$ and $\tau$; and in Corollary 4.1.5 on $d$, $\nu$, and $\tau$.

Remark 4.1.7. In Corollaries 4.1.3 through 4.1.5, the main term of the asymptotic doesn’t depend on the specific coefficients being enforced. Thus these may be interpreted as results on the equidistribution of norms and traces.

Remark 4.1.8. The type of counts found in this chapter are related to Manin’s conjecture, which addresses the asymptotic number of rational points of bounded height on Fano varieties. Counting points of degree $d$ and bounded height in $\overline{\mathbb{Q}}$, or equivalently, on $\mathbb{P}^1$, can be transferred to a question of counting rational points of bounded height on the $d$-th symmetric product of $\mathbb{P}^1$, which is $\mathbb{P}^d$. This is what Masser and Vaaler implicitly do when they count algebraic numbers by counting their minimal polynomials (as does this chapter; see the Methods subsection below). However, one needs to use a non-standard height on $\mathbb{P}^d$; Le Rudulier takes this approach explicitly [LR14, Théorème 1.1], thereby re-proving and
CHAPTER 4. SLICING THE STARS

generalizing (the main term of) the result of Masser and Vaaler. It should be noted, though, that while the shape of the main term – a constant times the appropriate power of the height – follows from known results on Manin’s conjecture, explicitly determining the constant in front relies ultimately on an archimedean volume calculation of Chern and Vaaler.

Barroero’s count of algebraic integers of degree $d$ corresponds to counting rational points on $\mathbb{P}^d$ that are integral with respect to the hyperplane at infinity. As noted in [LR14, Remarque 5.3], the shape of his count’s main term then follows from general results of Chambert-Loir and Tschinkel on counting integral points of bounded height on equivariant compactifications of affine spaces [CLT12, Theorem 3.5.6].

Our own units count corresponds to counting points on $\mathbb{P}^d$ integral with respect to two hyperplanes, and does not appear to follow from any results currently in the literature.

Remark 4.1.9. The algebraic number and integer counts of (4.1) and (4.2) have also been extended to arbitrary base number fields [MV07, Bar14] and to vectors of algebraic numbers [Sch95, Gao95, Wid09, Wid16, Gui17]. We expect there should be extensions of our new counts to these contexts as well.

The second goal of this chapter is to give explicit error terms, which we feel is especially justified in this context, beyond general principles of error-term morality. Namely, it’s natural to ask questions about properties of “random algebraic numbers” (or random algebraic integers, random units, etc.). For example: “What’s the probability that a random element of $\mathbb{Q}$ generates a Galois extension of $\mathbb{Q}$?”

How to make sense of a question like this? There are models from other arithmetic contexts; for example, if we’re asked “What’s the probability that a random positive integer is square-free?” we know what to do: count the number of square-free integers from 1 to $N$, divide that by $N$, and ask if that proportion has a limit as $N$ grows (Answer: Yes, $\frac{6}{\pi^2}$). Note that the easiest part is dividing by $N$, the number of elements in your finite box. In order
to make sense of probabilistic statements in the context of $\overline{\mathbb{Q}}$, one would like to first take a box of bounded height and degree (which will have only finitely many algebraic numbers by Northcott), determine the relevant proportion within that finite box, and then let the box size grow. But now the denominator in question is far from trivial; unlike counting the number of integers from 1 to $N$, estimating how many algebraic numbers are in a height-degree box is a more delicate matter.

In the context of $\overline{\mathbb{Q}}$, where there are two natural parameters to increase (the height and the degree), the gold standard for a "probabilistic" result would be that it holds for any increasing set of height-degree boxes such that the minimum of the height and degree goes to infinity. To prove results that even approach this standard (e.g. one might require that the height of the boxes grows at least as fast as some function of the degree), one likely needs good estimates for how many numbers are in a height-degree box to begin with. Without an estimate that holds uniformly in both $H$ and $d$, one would be justified in making statements about random elements in $\overline{\mathbb{Q}}$ of fixed degree $d$, but not random elements of $\overline{\mathbb{Q}}$ overall. Thus controlling the error terms in the theorems above is crucial.

To that end, in this chapter we give explicit error bounds for the algebraic number counts of Masser and Vaaler, the algebraic integer counts of Barroero, and our own unit counts. Below $p_d(T)$ is a polynomial defined in Section 4.2 whose leading term is $V_{d-1}T^d$, so our result is consistent with (4.2).

**Theorem 4.1.10.** Let $\overline{\mathbb{Q}}_d$ denote the set of algebraic numbers of degree $d$ over $\mathbb{Q}$, let $\mathcal{O}_d$ denote the set of algebraic integers of degree $d$ over $\mathbb{Q}$, and let $\mathcal{O}_d^*$ denote the set of units of
degree $d$ over $\mathbb{Q}$ in the ring of all algebraic integers. For all $d \geq 3$ we have

\begin{align*}
(i) \quad & |N(\bar{\mathcal{O}}_d, \mathcal{H}) - \frac{dV_d}{2(d+1)} \mathcal{H}^{d(d+1)}| \leq 3.37 \cdot (15.01)^d \cdot \mathcal{H}^d, \quad \text{for } \mathcal{H} \geq 1; \\
(ii) \quad & |N(\mathcal{O}_d, \mathcal{H}) - dp_d(\mathcal{H}^d)| \leq 1.13 \cdot 4^d d^2 2^d \cdot \mathcal{H}^{d(d-1)}, \quad \text{for } \mathcal{H} \geq 1; \text{ and} \\
(iii) \quad & |N(\mathcal{O}_d, \mathcal{H}) - 2dV_{d-2} \cdot \mathcal{H}^{d(d-1)}| \leq 0.000126 \cdot d^3 4^d (15.01)^d \cdot \mathcal{H}^{d(d-1)-1}, \quad \text{for } \mathcal{H} \geq d^{2d+1/d}.
\end{align*}

### 4.1.2 Methods

The starting point of all our proofs is the relationship between the height of an algebraic number and the Mahler measure of its minimal polynomial. Recall that the Mahler measure $\mu(f)$ of a polynomial with complex coefficients

\[ f(z) = w_0 z^d + w_1 z^{d-1} + \cdots + w_d = w_0(z - \alpha_1) \cdots (z - \alpha_d) \in \mathbb{C}[z], \]

with $w_0 \neq 0$, is defined by

\[ \mu(f) = |w_0| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}, \]

and $\mu(0)$ is defined to be zero. It’s immediate that the Mahler measure is multiplicative: $\mu(f_1 f_2) = \mu(f_1) \mu(f_2)$.

Crucially for our purposes, if $f(z)$ is the minimal polynomial of an algebraic number $\alpha$, then we have (see for example [BG06, Proposition 1.6.6])

\[ \mu(f) = H(\alpha)^d. \]

Thus, in order to count degree $d$ algebraic numbers of height at most $\mathcal{H}$, we can instead count minimal integer polynomials of Mahler measure at most $\mathcal{H}^d$.

We identify a polynomial with its vector of coefficients, so that counting integer polynomials amounts to counting lattice points. To do this we employ techniques from the geometry of numbers, which make rigorous the idea that, for a reasonable subset of Euclidean space, the number of integer lattice points in the set should be approximated by its volume. So for
example, the number of integer polynomials with degree at most $d$ and Mahler measure at most $T$ should be roughly the volume of the set of such real polynomials

$$\{ f \in \mathbb{R}[z]_{\deg \leq d} \mid \mu(f) \leq T \} \subset \mathbb{R}^{d+1}.$$  

Note that by multiplicativity of the Mahler measure, this set is the same as $Tu_d$, where

$$u_d := \{ f \in \mathbb{R}[z]_{\deg \leq d} \mid \mu(f) \leq 1 \}.$$  

The set $u_d$ will be our primary object of study. It is a closed, compact “star body,” i.e. a subset of euclidean space closed under scaling by numbers in $[0, 1]$. Chern and Vaaler [CV01, Corollary 2] explicitly determined the volume of $u_d$. In a rather heroic calculation, they showed that $V_d := \text{vol}_{d+1}(u_d)$ is given by the positive rational number in (4.3)*. Thus by geometry of numbers, and noting that $\text{vol}(Tu_d) = T^{d+1} \cdot \text{vol}(u_d)$, one expects the number of integer polynomials of degree at most $d$ and Mahler measure at most $T$ to be approximately $T^{d+1} \cdot V_d$. Chern and Vaaler proved this is indeed the case. Masser and Vaaler then showed how to refine this count of all such polynomials to just minimal polynomials, which let them prove the algebraic number count in (4.1).

What if you only want to count algebraic integers? Again, the above approach suggests you should do that by counting their minimal polynomials. Algebraic integers are characterized by having monic minimal polynomials. Thus one is naturally led to seek the volume of the “monic slice” of $Tu_d$ consisting of those real polynomials with leading coefficient 1.

However, these slices are no longer dilations of each other, so their volumes aren’t determined by knowing the volume of one such slice. Still, Chern and Vaaler were able to compute the volumes of monic slices of $Tu_d$; rather than a constant times a power of $T$, they are given by

---

*Our $u_d$ is the same as what would be denoted by $\mathcal{S}_{d+1}$ in the notation of [CV01], and our $V_d$ matches their $V_{d+1}$. Our subscripts correspond to the degree of the polynomials being counted rather than the dimension of the space.
a polynomial in $T$, whose leading term is $V_{d-1}T^d$. Geometry of numbers can then be applied again to obtain the algebraic integer count in (4.2).

In order to count units of degree $d$, or algebraic integers with given norm and/or trace, one needs to take higher-codimension slices. For example, the minimal polynomial of a unit will have leading coefficient 1 and constant coefficient $\pm 1$. But one quickly discovers that these higher-dimensional slices have volumes that are, in general, no longer polynomial in $T$. Rather than trying to explicitly calculate these volumes, we depart from the methods of earlier works, and instead approximate the volumes of such slices.

When we cut a dilate $TU_d$ by a certain kind of linear space, then as $T$ grows the slices look more and more like a lower-dimensional unit star body; this will be explained in Section 4.4. This explains the appearance of the volume $V_d$ in all of our asymptotic counts. We also use a careful analysis of the boundary of $U_d$ to show that the above convergence happens relatively fast; this makes our approximations precise enough to obtain algebraic number counts with good power-saving error terms.

We state here our main result on counting polynomials. For non-negative integers $m$, $n$, and $d$ with $0 < m + n \leq d$, and integer vectors $\vec{\ell} \in \mathbb{Z}^m$ and $\vec{r} \in \mathbb{Z}^n$, let $\mathcal{M}(d, \vec{\ell}, \vec{r}, T)$ denote the number of polynomials $f$ of the form

$$f(z) = \ell_0 z^d + \cdots + \ell_{m-1} z^{d-(m-1)} + x_m z^{d-m} + \cdots + x_{d-n} z^n + r_{d-n+1} z^{n-1} + \cdots + r_d$$

with Mahler measure at most $T$, where $x_m, \ldots, x_{d-n}$ are integers. Let $g = d - m - n$.

Combining our volume estimates with a counting principle of Davenport, we obtain the following.

**Theorem 4.1.11.** For all $0 < m + n \leq d$, $\vec{\ell} \in \mathbb{Z}^m$, and $\vec{r} \in \mathbb{Z}^n$, as $T \to \infty$ we have

$$\mathcal{M}(d, \vec{\ell}, \vec{r}, T) = V_g \cdot T^{g+1} + O(T^g).$$
Here the implied constant depends on $d, \tilde{\ell},$ and $\tilde{r}$.

Now we briefly discuss the methods used in the second half of the chapter to prove our explicit results, and how these results fit in with the literature. Chern and Vaaler’s [CV01, Theorem 3], which is the main ingredient in (4.1), gives an asymptotic count of the number of integer polynomials of given degree $d$ and Mahler measure at most $T$. The error term in this result contains a full power savings – order $T^d$ against a main term of order $T^{d+1}$ – but the implied constant in the error term is not made explicit. They do produce an explicit error term of order $T^{d+1-1/d}$ in [CV01, Theorem 5] using [CV01, Theorem 4], which is a quantitative statement on the continuity of the Mahler measure.

Our Theorem 4.7.1 below makes the constant in the error term of [CV01, Theorem 3] explicit, using a careful study of the boundary of $\mathcal{U}_d$. We apply the classical Lipschitz counting principle in place of the Davenport principle; the latter is not very amenable to producing explicit bounds. Theorem 4.8.1 is the analogous result to Theorem 4.7.1 for monic polynomials, and is obtained in a similar manner. However, the application of the Lipschitz principle is more delicate in this case. We also prove an explicit version of our Theorem 4.1.11 counting polynomials with specified coefficients (Theorem 4.9.3). For this result we also apply [CV01, Theorem 4], and, reminiscent of Chern and Vaaler’s application, this method yields an inferior power savings.

We now describe the organization of the chapter. In Section 4.2 we collect key facts about the unit star body $\mathcal{U}_d$, including a detailed discussion of its boundary. In Section 4.3 we describe the counting principles we use to estimate the difference between the number of lattice points in a set and the set’s volume. In Section 4.4 we estimate the volume of the sets in which we must count lattice points to prove Theorem 4.1.11; this theorem is then proved in Section 4.5. In Section 4.6 we transfer our counts for polynomials to counts for various kinds of algebraic numbers, thereby proving Theorem 4.1.1 and Corollaries 4.1.2-
4.1.5. This involves using a version of Hilbert’s irreducibility theorem to account for reducible polynomials.

The rest of the chapter is devoted to obtaining explicit versions of these counts. In Section 4.7 we prove the aforementioned explicit version of [CV01, Theorem 3] on counting polynomials of given degree and bounded Mahler measure, and in Section 4.8 we do the same for the count of monic polynomials. Section 4.9 contains a version of the general Theorem 4.1.11 with an explicit error term, at the cost of weaker power savings. In Section 4.10 we begin to convert our explicit counts of polynomials to explicit counts of minimal polynomials. The main piece of this is showing that the reducible polynomials are negligible. We follow the techniques for this used by Masser and Vaaler (sharper than the more general Hilbert irreducibility method described above), obtaining explicit bounds. In Section 4.11 we prove our final explicit results on counting algebraic numbers, including explicit versions of Masser and Vaaler’s result (4.1), Barroero’s result (4.2), and Corollaries 4.1.2 and 4.1.3. Finally, we include an appendix with some estimates for various expressions involving binomial coefficients which occur in our explicit error terms throughout the chapter.

4.2 The unit star body

In this section we discuss some properties of the unit star body

\[ \mathcal{U}_d := \{ \overline{w} \in \mathbb{R}^{d+1} \mid \mu(\overline{w}) \leq 1 \}. \]

Since for all \( f \in \mathbb{R}[x] \) and \( t \in \mathbb{R} \) we have

\[ \mu(tf) = |t| \mu(f), \]  \hspace{1cm} (4.4)

it’s easy to see that \( \mathcal{U}_d \) is in fact a (symmetric) star body. Furthermore, \( \mathcal{U}_d \) is compact; it is closed because \( \mu \) is continuous [Mah61, Lemma 1], and we can see it is bounded by
classical results that bound the coefficients of a polynomial in terms of its Mahler measure, for example the following (see [Mah76, p. 7] and [BG06, Lemma 1.6.7 and its proof]).

**Lemma 4.2.1 (Mahler).** Every polynomial \( f(z) = w_0 z^d + w_1 z^{d-1} + \cdots + w_0 \in \mathbb{C}[z] \) has coefficients satisfying
\[
|w_i| \leq \binom{d}{i} \mu(f), \ i = 0, \ldots, d.
\]

Furthermore, we have the following double inequality comparing Mahler measure with the sup-norm of coefficients:
\[
\left( \frac{d}{[d/2]} \right)^{-1} \|\bar{w}\|_\infty \leq \mu(\bar{w}) \leq \sqrt{d+1} \|\bar{w}\|_\infty, \ \forall \ \bar{w} \in \mathbb{R}^{d+1}.
\]

### 4.2.1 Volumes

As mentioned in the introduction, the exact volume of \( \mathcal{U}_d \) was determined by Chern and Vaaler [CV01, Corollary 2]:
\[
V_d := \text{vol}_{d+1}(\mathcal{U}_d) = 2^{d+1}(d+1)^s \prod_{j=1}^{s} \frac{(2j)^d}{(2j+1)^{d+1-2j}},
\]
where \( s = [(d-1)/2] \). (Here \( \text{vol}_N \) denotes Lebesgue measure on \( \mathbb{R}^N \).)

We record some numerical information about the volume of \( \mathcal{U}_d \). We note that a result like Lemma 4.2.2 below would follow quite easily from the asymptotic formula for \( \log V_d \) given in [CV01, (1.31)]. However, this formula was given without proof and contains an error. The correct version of [CV01, (1.31)] is apparently (using our notation):
\[
\log V_d = -\frac{1}{2} d \log d + \left( \frac{1}{2} \log 2\pi + 1 \right) d - \frac{5}{4} \log d + \left( 3\zeta'(-1) + \frac{1}{2} + \frac{1}{3} \log 2 \right) + \frac{19\theta_2}{12d},
\]
where \( |\theta_2| \leq 1 \). In this corrected version, the constant term differs from what was printed in [CV01] by \( \log 2 \). Since we are mainly interested in an upper bound on \( V_d \), we settle for the following simpler result that can be proved quickly.
Lemma 4.2.2. We have

\[ V_d \leq V_{15} = \frac{2658455991569831745807614120560689152}{1390487258770848957579157123046875} = \frac{2^{121}}{3^{20} \cdot 5^9 \cdot 7^9 \cdot 11^6 \cdot 13^4} \approx 191.1888 \]

for all \( d \geq 0 \), and

\[ \lim_{d \to \infty} V_d = 0. \]

Proof. Note using Stirling’s estimates (see (A.1) in the appendix) that for any positive integer \( s \), we have

\[
\prod_{j=1}^{s} \frac{2j}{2j+1} = \frac{2^s s!}{(2s+1)/!(2^s)!} = \frac{4^s s!}{(2s+1)!} \\
\leq \frac{4^s (e^{1-s} s^{s+1/2})^2}{\sqrt{2\pi} e^{-2s-1}(2s+1)^{2s+3/2}} \leq \frac{4^s (e^{-2s} s^{2s+1})}{\sqrt{2\pi} e^{-2s-1}(2s+1)^{2s+3/2}} \\
\leq \frac{e^{3} e^{s} (2s)^{2s+1}}{4\sqrt{\pi} s}.
\]

Suppose that \( d \) is odd, so we may take \( s = \left\lceil \frac{d-1}{2} \right\rceil = \left\lceil \frac{(d+1)-1}{2} \right\rceil \). Then we have

\[
\frac{V_{d+1}}{V_d} = \frac{2^{d+2}(d+2)^{s} s}{2^{d+1}(d+1)^{s}} \prod_{j=1}^{s} \left\{ \frac{(2j)^{d+1-2j}}{(2j)^{d-2j}} \right\} \prod_{j=1}^{s} \left\{ \frac{(2j+1)^{d+1-2j}}{(2j+1)^{d-2j}} \right\} \\
= 2 \left( \frac{d+2}{d+1} \right)^{s} \prod_{j=1}^{s} \left\{ \frac{2j}{2j+1} \right\} \leq \left( \frac{d+2}{d+1} \right)^{s} \cdot \frac{e^{3}}{2\sqrt{\pi} s}.
\]

If \( d \) is even and \( s = \left\lfloor \frac{d-1}{2} \right\rfloor = \frac{d}{2} - 1 \), then \( \left\lceil \frac{(d+1)-1}{2} \right\rceil = s + 1 \), and then we have

\[
\frac{V_{d+1}}{V_d} = \frac{2^{d+2}(d+2)^{s+1}}{2^{d+1}(d+1)^{s}} \cdot \frac{d}{(d+1)^{2}} \prod_{j=1}^{s} \left\{ \frac{(2j)^{d+1-2j}}{(2j)^{d-2j}} \right\} \prod_{j=1}^{s} \left\{ \frac{(2j+1)^{d+1-2j}}{(2j+1)^{d-2j}} \right\} \\
= \frac{2(d+2)^{s}}{(d+1)^{s}} \cdot \frac{d^2 + 2d}{d^2 + 2d + 1} \cdot \prod_{j=1}^{s} \left\{ \frac{2j}{2j+1} \right\} \leq \left( \frac{d+2}{d+1} \right)^{s} \cdot \frac{e^{3}}{2\sqrt{\pi} s}.
\]
In either case, the ratio of successive terms tends to zero, so in fact $V_d$ decays to zero faster than exponentially, proving the second claim of our lemma. For the first claim, it suffices to compute enough values of $V_d$. We see the maximum is attained at $d = 15$, as advertised.

For any $T \geq 0$, by (4.4) we have that
\[
\operatorname{vol}_{d+1}\left(\{\bar{w} \in \mathbb{R}^{d+1} \mid \mu(\bar{w}) \leq T\}\right) = \operatorname{vol}_{d+1}(TU_d) = V_d \cdot T^{d+1}.
\]

Chern and Vaaler (see [CV01, equation (1.16)], corrected as in [Bar14, footnote on p. 38]) also computed the volume of the “monic slice”
\[
W_{d,T} := \{(w_0, \ldots, w_d) \in TU_d \mid w_0 = 1\}. \tag{4.7}
\]

They showed:
\[
\operatorname{vol}_d(W_{d,T}) = p_d(T) := C_d 2^{-s}s!^{-1} \sum_{m=0}^{s} (-1)^m (d-2m)^s \binom{s}{m} T^{d-2m}, \tag{4.8}
\]
where again
\[
s = \left\lfloor \frac{d-1}{2} \right\rfloor, \quad \text{and} \quad C_d = 2^d \prod_{j=1}^{s} \left(\frac{2j}{2j+1}\right)^{d-2j}.
\]

Note that, since $p_d(T)$ is a polynomial in $T$, we automatically have (carefully inspecting the leading term):
\[
\operatorname{vol}_d(W_{d,T}) = V_{d-1} \cdot T^d + O(T^{d-1}).
\]

For other slices besides the monic one, we will have to work harder (in Section 4.4) to obtain such power savings. Along the way, it will become clear why the leading coefficient takes the form it does.

Remark 4.2.3. Above, and throughout the chapter, for a measurable set $S \subset \mathbb{R}^N$ and $n < N$, we will sometimes write $\operatorname{vol}_n(S)$. In this case, $S$ will always be a subset contained in an affine space defined by fixing $N-n$ coordinates of $\mathbb{R}^N$, and then $\operatorname{vol}_n(S)$ will always denote
the Lebesgue measure of the projection of $S$ to $\mathbb{R}^n$ given by simply forgetting the fixed coordinates. For ease of notation, we will sometimes drop the subscript when it is clear from context.

### 4.2.2 Semialgebraicity

Next we establish a qualitative result we will need in proving Theorem 4.1.11. A (real) *semialgebraic set* is a subset of euclidean space which is cut out by finitely many polynomial equations and/or inequalities, or a finite union of such subsets. Recall that the class of semialgebraic sets is closed under finite unions and intersections, and also closed under projections by the Tarski-Seidenberg theorem [BM88, Theorem 1.5].

**Lemma 4.2.4.** The set $U_d \subset \mathbb{R}^{d+1}$ is semialgebraic.

**Proof.** Our proof is similar to that of [Bar14, Lemma 4.1]. For $j = 0, \ldots, d$, we wish to define a semialgebraic set $S_j \subset \mathbb{R}^{d+1}$ corresponding to degree $j$ polynomials in $U_d$. We start by constructing auxiliary subsets of $\mathbb{R}^{d+1} \times \mathbb{C}^j$ corresponding to the polynomials’ coefficients and roots, where $\mathbb{C}$ is identified with $\mathbb{R}^2$ in the obvious way. We define

$$S_j^0 = \{(0, \ldots, 0, w_{d-j}, \ldots, w_d, \alpha_1, \ldots, \alpha_j) \in \mathbb{R}^{d+1} \times \mathbb{C}^j \mid w_{d-j} \neq 0, \text{ and}$$

$$w_{d-j}z^j + w_{d-j+1}z^{j-1} + \cdots + w_d = w_{d-j}(z - \alpha_1) \cdots (z - \alpha_j)\},$$

where the equalities defining the set are given by equating the real part of each elementary symmetric function in the roots $\alpha_1, \ldots, \alpha_j$ with the corresponding coefficient $w_i$, and setting the imaginary part to zero. To enforce $\mu((0, \ldots, 0, w_{d-j}, \ldots, w_d)) \leq 1$, we define $S_j^1$ to comprise those elements of $S_j^0$ such that all products of subsets of $\{\alpha_1, \ldots, \alpha_j\}$ are less than or equal to $1/|w_{d-j}|$ in absolute value. Finally, we let $S_j$ be the projection of $S_j^1$ onto $\mathbb{R}^{d+1}$. Now simply note that

$$U_d = \{0\} \cup \bigcup_{j=0}^d S_j.$$
Remark 4.2.5. Note that for any $T > 0$ the dilation $T \mathcal{U}_d$ is also semialgebraic, and is defined by the same number of polynomials (and of the same degrees) as is $\mathcal{U}_d$.

### 4.2.3 Boundary parametrizations

Next we describe the parametrization of the boundary of $\mathcal{U}_d$, which consists of vectors corresponding to polynomials with Mahler measure exactly 1. The simple idea behind the parametrization is that such a polynomial is the product of a monic polynomial with all its roots inside (or on) the unit circle, and a polynomial with constant coefficient $\pm 1$ and all its roots outside (or on) the unit circle. Recall that $\mathcal{U}_d$ is a compact, symmetric star body in $\mathbb{R}^{d+1}$. The parametrization is described in [CV01, Section 10]. We briefly summarize the key points here. The boundary $\partial \mathcal{U}_d$ is the union of $2d + 2$ “patches” $\mathcal{P}_{k,d}^\varepsilon$, $k = 0, \ldots, d$, $\varepsilon = \pm 1$.

The patch $\mathcal{P}_{k,d}^\varepsilon$ is the image of a certain compact set $\mathcal{J}_{k,d}^\varepsilon$ under the map

$$b_{k,d}^\varepsilon : \mathbb{R}^k \times \mathbb{R}^{d-k} \to \mathbb{R}^{d+1},$$

defined by

$$b_{k,d}^\varepsilon((x_1, \ldots, x_k), (y_0, \ldots, y_{d-k-1})) = B_{k,d}((1, x_1, \ldots, x_k), (y_0, \ldots, y_{d-k-1}, \varepsilon)), \quad (4.9)$$

$$B_{k,d}((x_0, x_1, \ldots, x_k), (y_0, \ldots, y_d)) = (w_0, \ldots, w_d),$$

with

$$w_i = \sum_{l=0}^{k} \sum_{\substack{m = 0 \\text{ to } d-k \\text{ with } l + m = i}} x_l y_m, \quad i = 0, \ldots, d. \quad (4.10)$$

Note that this simply corresponds to the polynomial factorization

$$w_0 z^d + \cdots + w_d = (x_0 z^k + \cdots + x_k) \cdot (y_0 z^{d-k} + \cdots + y_{d-k}).$$
The sets $\mathcal{J}_{k,d}^\varepsilon$ are given by

$$\mathcal{J}_{k,d}^\varepsilon = J_k \times K_{d-k}^\varepsilon \subseteq \mathbb{R}^k \times \mathbb{R}^{d-k},$$

where

$$J_k = \{ \bar{x} \in \mathbb{R}^k \mid \mu(1, \bar{x}) = 1 \}, \text{ and} \quad (4.11)$$

$$K_{d-k}^\varepsilon = \{ \bar{y} \in \mathbb{R}^{d-k} \mid \mu(\bar{y}, \varepsilon) = 1 \}.$$

It will also be useful in Section 4.8 to have a parametrization of $\partial \mathcal{W}_{d,T}$, the boundary of a monic slice (see (4.7)), along the lines of that given for $\partial \mathcal{U}_d$ above. Consider a monic polynomial

$$f(z) = z^d + w_1 z^{d-1} + \cdots + w_d \in \mathbb{R}[z],$$

having Mahler measure equal to $T \geq 0$ and roots $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$. We note that such a polynomial can be factored as $f(z) = g_1(z)g_2(z)$, where $g_1$ and $g_2 \in \mathbb{R}[z]$ are monic, $\mu(g_1) = 1$ (forcing $\mu(g_2) = T)$, the constant coefficient of $g_2$ is $\pm T$, and where $\deg(g_1) = k \in \{0, \ldots, d-1\}$. To do this, we simply let

$$g_1(z) = \prod_{|\alpha_i| \leq 1} (z - \alpha_i), \text{ and } g_2(z) = \prod_{|\alpha_i| > 1} (z - \alpha_i).$$

It is easy to check that $g_1$ and $g_2$ have the desired properties when $T > 1$. For $k = 0, \ldots, d-1$, we let $J_k$ be as in (4.11), and let

$$Y_{d-k}^\varepsilon = \{ \bar{y} \in \mathbb{R}^{d-k-1} \mid \mu(1, \bar{y}, \varepsilon) = 1 \}, \text{ and}$$

$$\mathcal{L}_{k,d}^\varepsilon = J_k \times Y_{d-k}^\varepsilon \subseteq \mathbb{R}^k \times \mathbb{R}^{d-k-1},$$

for each $k = 0, \ldots, d-1, \varepsilon = \pm 1$. We also define

$$\beta_{k,d}^\varepsilon((x_1, \ldots, x_k), (y_1, \ldots, y_{d-k-1})) = B_{k,d}^\varepsilon((1, x_1, \ldots, x_k), (1, y_1, \ldots, y_{d-k-1}, \varepsilon T)), \quad (4.12)$$
similarly to (4.9).

We have that $\partial W_{d,T}$ is covered by the $2d$ “patches”

$$\beta_{k,d}^T \left( \mathcal{L}_k^T \right).$$

(4.13)

4.3 Counting principles

We’ll need a counting principle of Davenport to estimate the number of lattice points in semialgebraic sets.

**Theorem 4.3.1** (Davenport). Let $S$ be a compact, semialgebraic subset of $\mathbb{R}^n$ defined by at most $k$ polynomial equalities and inequalities of degree at most $l$. Then the number of integer lattice points contained in $S$ is equal to

$$\text{vol}_n(S) + O(\max\{\text{vol}(S), 1\}),$$

where $\text{vol}(S)$ denotes the maximum, for $m = 1, \ldots, n - 1$, of the volume of the projection of $S$ on the $m$-dimensional coordinate space given by setting any $n - m$ coordinates equal to zero. The implicit constant in the error term depends only on $k, l$, and $n$.

**Remark 4.3.2.** This follows from the main theorem of [Dav51], as described immediately after its statement. (The argument for this reduction was corrected in [Dav64].) Davenport’s principle has been generalized in a couple directions, to allow for lattices other than the standard integer lattice [BW14, (1.2)], and to apply to sets definable in any $o$-minimal structure [BW14, Theorem 1.3], of which semialgebraic sets are but one example. However, the above version will suffice for our purposes.

For our explicit error estimates we will use a different counting principle, namely a refinement of the classical Lipschitz counting principle due to Spain [Spa95]. The classical principle allows one to estimate the difference between the number of lattice points in a set
and the set’s volume: one uses that the boundary is parametrized by finitely many Lipschitz maps, and that a Lipschitz map sends a cube in the domain into a cube in the codomain. In our case it will be convenient to use “tiles” other than cubes in the domain. This could be achieved by precomposing the maps with other maps which cover our tiles with the images of cubes, but we feel the following alternative formulation is intuitive and less awkward in application.

**Theorem 4.3.3.** Let $S \subset \mathbb{R}^n$ be a set whose boundary $\partial S$ is contained in the images of finitely many maps $\phi_i : J_i \to \mathbb{R}^n$, where $\mathcal{I}$ is a finite set of indices and each $J_i$ is a set. For each $i \in \mathcal{I}$, assume that $J_i$ can be covered by $m_i$ sets $T_{i,1}, \ldots, T_{i,m_i}$, with the property that for each $j$ the image $\phi_i(T_{i,j})$ is contained in a translate of $[0,1]^n$ inside $\mathbb{R}^n$. Then

$$|\#(S \cap \mathbb{Z}^n) - \text{vol}_n(S)| \leq 2^n \sum_{i \in \mathcal{I}} m_i.$$ 

**Proof.** We follow the “every other tile” approach of [Spa95]. The number of lattice points in $S$ differs from the volume of $S$ by at most the number of integer vector translates of the half-open unit tile $[0,1]^n \subseteq \mathbb{R}^n$ that meet the boundary $\partial S$. Consider the set $\mathcal{E}$ of tiles which are *even* integer vector translates of $[0,1]^n$; it is clear that any translate of $[0,1]^n$ meets exactly one such tile. Since $\partial S$ is contained in at most $\sum_{i \in \mathcal{I}} m_i$ translates of $[0,1]^n$, this means that at most that many tiles from $\mathcal{E}$ meet $\partial S$. But $\mathbb{R}^n$ is partitioned by $2^n$ sets of tiles which, like $\mathcal{E}$, are made up of “every other tile.” (Explicitly, these sets are of the form $\mathcal{E} + \vec{v}$, where $\vec{v}$ is a vector of 0’s and 1’s.) The bound claimed in the theorem follows. \qed

### 4.4 Volumes of slices of star bodies

We keep all the notation established just before Theorem 4.1.11 in the introduction, so $d, m, n, \vec{\ell} = (\ell_0, \ldots, \ell_{m-1}) \in \mathbb{Z}^m$, and $\vec{r} = (r_{d-n+1}, \ldots, r_d) \in \mathbb{Z}^n$ are fixed, and again we set

\footnote{For this section we could take $\vec{\ell}$ and $\vec{r}$ to be *real* vectors, but this will not be important for our results.}
\( g = d - m - n \). Let \( T \) be a positive real number. We continue to use the volume convention of Remark 4.2.3. The primary step in proving Theorem 4.1.11 is to estimate the volume of the slice

\[
S(T) = S_{\tilde{w}(T)}(T) := \{ \tilde{w} = (w_0, \ldots, w_d) \in \mathbb{R}^{d+1} \mid \mu(\tilde{w}) \leq T \};
\]

\[
w_i = \ell_i, \text{ for } i = 0, \ldots, m - 1; \text{ and } \]

\[
w_j = r_j, \text{ for } j = d - n + 1, \ldots, d
\]

as \( T \) grows. Specifically, we show the following.

**Theorem 4.4.1.** We have

\[
\vol_{g+1}(S(T)) = V_g T^{g+1} + O(T^g), \text{ as } T \to \infty.
\]

We won’t obtain an explicit error estimate of this strength, but in Section 4.9 we will discuss how to obtain an explicit error term of order \( T^{g+1-\frac{1}{2}} \).

The idea of the proof of Theorem 4.4.1 is as follows. Because \( \mu(T \tilde{w}) = T \mu(\tilde{w}) \) for all \( T \geq 0 \), and all \( \tilde{w} \in \mathbb{R}^{d+1} \), we have

\[
\{ \tilde{w} \in \mathbb{R}^{d+1} \mid \mu(\tilde{w}) \leq T \} = T \{ \tilde{w} \in \mathbb{R}^{d+1} \mid \mu(\tilde{w}) \leq 1 \} = T \mathcal{U}_d.
\]

Let

\[
\tilde{v} = (\ell_0, \ldots, \ell_{m-1}, 0, \ldots, 0, r_{d-n+1}, \ldots, r_d) \in \mathbb{R}^{d+1},
\]

and for each \( t \in [0, \infty) \), set

\[
W_t := t \tilde{v} + \text{Span}\{e_m, e_{m+1}, \ldots, e_{d-n}\} \subset \mathbb{R}^{d+1},
\]

where \( e_0, e_1, \ldots, e_d \) are standard basis vectors for \( \mathbb{R}^{d+1} \). Then for \( T > 0 \) we have

\[
S(T) = W_1 \cap \mathcal{U}_d = T \left( W_1/T \cap \mathcal{U}_d \right),
\]
and since $W_{1/T}$ is $(g+1)$-dimensional, this means

$$\text{vol}_{g+1}(S(T)) = T^{g+1} \text{vol}_{g+1}(W_{1/T} \cap \mathcal{U}_d).$$

(4.17)

Letting $t = 1/T$, we should expect that

$$\text{vol}_{g+1}(W_{1/T} \cap \mathcal{U}_d) = \text{vol}_{g+1}(\mathcal{U}_d \cap (W_0 + t\vec{v})) \to \text{vol}_{g+1}(\mathcal{U}_d \cap W_0), \text{ as } t \to 0,$$

unless the boundary of $\mathcal{U}_d$ were to intersect with $W_0$ in an unusual way; for example, if $\mathcal{U}_d$ were a cube and $W_0$ was a plane containing one of the faces. This basic idea of using continuity of volumes of slices appears in the proof of [Sin08, Theorem 1.5]. We will show below that $\text{vol}_{g+1}(\mathcal{U}_d \cap W_0) = V_g$, whence the main term in the statement of Theorem 4.4.1. We'll obtain a full power savings by showing that the boundary of $\mathcal{U}_d$ is never tangent to $W_0$.\footnote{As an exercise to see why tangency is a problem, consider the length of cross-sections of a disk as the cross-sections slide toward a tangent line.}

**Proposition 4.4.2.** Let $S \subset \mathbb{R} \times \mathbb{R}^N$ be a compact set bounded by finitely many smooth hypersurfaces $H_i, i = 1, \ldots, m$. Assume each boundary component $H_i \cap \partial S$ has smooth intersection with (i.e. is not tangent to) the hyperplane $\{0\} \times \mathbb{R}^N$, and that these boundary components $H_i \cap \partial S$ have pairwise disjoint interiors. Then

$$V(t) := \text{vol}_{N}(S \cap (\{t\} \times \mathbb{R}^N))$$

satisfies

$$V(t) = V(0) + O(t), \text{ as } t \to 0^+.$$

**Proof.** We denote points in $\mathbb{R} \times \mathbb{R}^N$ by $(x, y_1, \ldots, y_N)$. For each $t \geq 0$, let $S_{[0,t]} = S \cap ([0,t] \times \mathbb{R}^N)$, and let $S_t = S \cap (\{t\} \times \mathbb{R}^N)$. Let $F$ denote the constant vector field $(1,0,\ldots,0)$ on $\mathbb{R} \times \mathbb{R}^N$. By the divergence theorem, we have

$$\int_{\partial S_{[0,t]}} F \cdot d\vec{s} = \int_{S_{[0,t]}} \nabla \cdot F \; d\text{vol}_{N+1} = \int_{S_{[0,t]}} 0 \; d\text{vol}_{N+1} = 0,$$
where the first integral is with respect to the surface measure with outward normal. Note that our assumption that \( \{0\} \times \mathbb{R}^N \) is not tangent to any of the \( H_i \) means that neither is the parallel hyperplane \( \{t\} \times \mathbb{R}^N \) for \( t \) sufficiently small. Let \( R_t = ([0, t] \times \mathbb{R}^N) \cap \partial S \), and note that, as long as \( t \) is small enough to avoid the aforementioned tangencies, the boundary of \( S_{[0,t]} \) decomposes into three pieces with disjoint interiors as follows:

\[
\partial S_{[0,t]} = S_0 \cup S_t \cup R_t.
\]

and so we have

\[
0 = \oint_{\partial S_{[0,t]}} F \cdot d\vec{s} = \int_{S_0} F \cdot d\vec{s} + \int_{S_t} F \cdot d\vec{s} + \int_{R_t} F \cdot d\vec{s} = -V(0) + V(t) + \int_{R_t} F \cdot d\vec{s},
\]

where

\[
\int_{R_t} F \cdot d\vec{s} = \sum_i \int_{H_i \cap R_t} F \cdot d\vec{s}.
\]

Now we must show that

\[
|V(t) - V(0)| = \left| \int_{R_t} F \cdot d\vec{s} \right| = O(t). \tag{4.18}
\]

Since \( S \) is compact, the set \( R_t \) is contained in a “pizza box” \( [0, t] \times [-M, M]^N \) for some positive number \( M \) independent of \( t \). Fix \( i \in \{1, \ldots, m\} \). By assumption, \( H_i \cap \partial S \) is not tangent to the hyperplane \( \{x = 0\} \), but since \( H_i \) is smooth and we’re working in a compact set, we know \( H_i \cap \partial S \) is not tangent to \( \{x = t\} \) for any \( t \) sufficiently small. This means that, by the implicit function theorem, for \( t \) sufficiently small and any point \( P \in H_i \cap R_t \), we have that \( H_i \) coincides in an open subset \( U \subseteq H_i \cap R_t \) containing \( P \) with the graph of a function \( y_r = f(x, y_1, \ldots, \hat{y}_r, \ldots, y_N) \) for some \( r \in \{1, \ldots, N\} \) which depends on \( P \). So we have \( f : V \to [-M, M] \), where \( V \) is an open subset of \( [0, t] \times [-M, M]^{N-1} \). Letting \( \vec{n} \) denote
the outward unit normal, we have
\[ \int_U F \cdot d\mathbf{s} = \int_U F \cdot \mathbf{n} \, ds = \int_V \cdots \int_V \frac{\partial f}{\partial x} \, dxdy_1 \cdots \hat{y}_r \cdots dy_N, \] (4.19)
where the sign in the final integral is $-$ or $+$ depending on whether $\mathbf{n}$ is an upward or downward normal to the graph of $f$, respectively.

By our non-tangency assumption again, the partial derivative $\frac{\partial f}{\partial x}$ is bounded in absolute value inside our pizza box by a constant $K$ which does not depend on $U$, $i$, or $t$ as $t \to 0$.

By compactness, finitely many of these neighborhoods $U$ cover $H_i \cap R_t$, and the number of neighborhoods required -- call this number $n$ -- can be chosen independent of $t$ or $i$. Using (4.19), we estimate the integral in (4.18) as follows:

\[ \left| \int_{R_t} F \cdot d\mathbf{s} \right| \leq \sum_{i=1}^m \left| \int_{H_i \cap R_t} F \cdot d\mathbf{s} \right| \leq \sum_{i=1}^m \int_{H_i \cap R_t} |F \cdot \mathbf{n}| \, ds \leq \sum_{i=1}^m \sum_U \int_{U} |F \cdot \mathbf{n}| \, ds \\
\leq \sum_{i=1}^m \sum_U \int_{-M}^M \cdots \int_{-M}^M \int_0^t \left| \frac{\partial f}{\partial x} \right| dxdy_1 \cdots \hat{y}_r \cdots dy_N \\
\leq m \cdot n \cdot [(2M)^{N-1}t]K = O(t). \]

Now we verify that the boundary of $\mathcal{U}_d$ satisfies the hypotheses of Proposition 4.4.2. We refer to the parametrization of said boundary described in Section 4.2, and follow that notation. As noted in [CV01, Section 10], the condition of the boundary components having disjoint interiors is satisfied here -- this can be readily verified directly from the description of the parametrization. Let $H = H_{k,d}^\epsilon$ be one of the hypersurfaces which bound $\mathcal{U}_d$. The hypersurface $H$ is the image of $\mathbb{R}^k \times \mathbb{R}^{d-k}$ under the map $b = b_{k,d}^\epsilon$ described in (4.9).
CHAPTER 4. SLICING THE STARS

Proposition 4.4.3. Let \( \mathbf{v} = (\ell_0, \ldots, \ell_{m-1}, 0, \ldots, 0, r_{d-n+1}, \ldots, r_d) \in \mathbb{R}^{d+1} \), and let

\[
W_0 = \text{Span}\{e_m, e_{m+1}, \ldots, e_{d-n}\}, \quad \text{and}
\]

\[
W = \text{Span}\{\mathbf{v}, e_m, e_{m+1}, \ldots, e_{d-n}\},
\]

where \( e_0, e_1, \ldots, e_d \) are standard basis vectors for \( \mathbb{R}^{d+1} \). Then \( W_0 \) is not tangent to \( H \cap W \) at any point.

We will break up the proof of this proposition into three lemmas.

Lemma 4.4.4. The subspace \( W_0 \) does not meet \( H \) unless

\[
n \leq k \leq d - m.
\]

If those inequalities hold and \( P = (w_0, \ldots, w_d) = b(x_1, \ldots, x_k, y_0, \ldots, y_{d-k-1}) \) is a point in \( H \cap W_0 \), then we have

\[
y_0 = \cdots = y_{m-1} = x_{k-n+1} = \cdots = x_k = 0. \tag{4.20}
\]

Proof. Suppose the inequalities are satisfied. We'll prove vanishing of the parameters \( y_i \), by induction on \( 0 \leq i \leq m - 1 \). If \( m = 0 \), there's nothing to prove. Otherwise, for the base case \( i = 0 \), by the definition of \( W_0 \) we have \( w_0 = 0 \), but also \( w_0 = y_0 \) by the definition of \( b \) in (4.9). For arbitrary \( i \), we again have \( w_i = 0 \), while by the definition of \( b \), every summand in the formula for \( w_i \) is of the form \( x_{i-j}y_j \) for \( j < i \), except for the summand \( y_i \). Thus we're done by induction. Essentially the same proof works for the vanishing of \( x_{k-n+1}, \ldots, x_k \).

However, if \( n > k \), then the above argument would imply that \( x_0 = 0 \), but we know \( x_0 = 1 \), a contradiction. Similarly, if \( k > d - m \), the above would give \( 0 = y_{d-k} = \epsilon \), also a contradiction.

Lemma 4.4.5. The tangent space \( T_P(H) \) of \( H \) at \( P \) is the row space of the following \( d \times (d+1) \) matrix, where the first \( (d-k) \) rows represent the tangent vectors \( \left( \frac{\partial w_0}{\partial y_j}, \ldots, \frac{\partial w_d}{\partial y_j} \right) \), \( j = 0, \ldots, d-k \).
0, \ldots, d-k-1, and the last $k$ rows represent the tangent vectors \( \left( \frac{\partial u_0}{\partial x_i}, \ldots, \frac{\partial u_d}{\partial x_i} \right) \), \( i = 1, \ldots, k \).

Let \( q = d - k - 1 \) for ease of reading.

\[
(D_b)^T = \begin{bmatrix}
1 & x_1 & x_2 & \cdots & x_k & 0 & 0 & \cdots & 0 \\
0 & 1 & x_1 & x_2 & \cdots & x_k & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \cdots & \vdots \\
\vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \cdots & \vdots \\
0 & \cdots & \cdots & 0 & 1 & x_1 & x_2 & \cdots & x_k \\
0 & 0 & y_0 & y_1 & \cdots & y_q & \varepsilon & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \cdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \cdots & \vdots \\
0 & 0 & \cdots & \cdots & 0 & y_0 & y_1 & \cdots & y_q & \varepsilon
\end{bmatrix}.
\]

**Lemma 4.4.6.** The projection of \( T_p(H) \) onto \( W_0^\perp \) is surjective.

**Proof.** Using Lemma 4.4.4, the image of that projection contains the row space (in appropriate coordinates) of the following matrix, obtained by taking the first $m$ columns and first $m$ rows of the above matrix, as well as its last $n$ columns and last $n$ rows:

\[
C := \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix},
\]

where

\[
A = \begin{bmatrix}
1 & x_1 & x_2 & \cdots & x_{m-1} \\
0 & 1 & x_1 & \cdots & x_{m-2} \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
\vdots & \vdots & \ddots & \ddots & \ddots \\
\vdots & \vdots & \ddots & \ddots & x_1 \\
0 & \cdots & \cdots & 0 & 1
\end{bmatrix}
\]

is an $m \times m$-matrix, and

\[
B = \begin{bmatrix}
\varepsilon & 0 & \cdots & \cdots & 0 \\
y_q & \varepsilon & \cdots & \cdots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
y_{q-n+3} & \cdots & \cdots & \cdots & 0 \\
y_{q-n+2} & \cdots & y_{q-1} & y_q & \varepsilon
\end{bmatrix}
\]
is an $n \times n$-matrix.

Thus $C$ is a block diagonal matrix (we’ve used the vanishing of parameters described in (4.20) here) with determinant $\varepsilon^n \neq 0$, so its row space is all of $W_0^\perp$. \hfill \Box

**Proof of Proposition 4.4.3.** We seek a tangent vector to $H$ at $P$ which is contained in $W \setminus W_0$. By Lemma 4.4.6, $T_P(H)$ surjects onto the positive-dimensional space $W_0^\perp$. Since its kernel under this map is exactly $W_0$, a vector must exist as desired. \hfill \Box

**Proof of Theorem 4.4.1.** We begin by noting that we may identify $U_d \cap W_0 \subseteq \mathbb{R}^{d+1}$ with $U_g \subseteq \mathbb{R}^{g+1}$ as follows.

Define a map $\tau : \mathbb{R}^{g+1} \to \mathbb{R}^{d+1}$ by

$$
\tau(w_m, \ldots, w_{d-n}) = \begin{pmatrix} 0, \ldots, 0, w_m, \ldots, w_{d-n}, 0, \ldots, 0 \end{pmatrix} \in W_0,
$$

which corresponds to multiplying the polynomial corresponding to the input by $z^n$. Notice that this operation preserves the Mahler measure. It’s also clear that $\tau$ maps $U_g$ isometrically onto $U_d \cap W_0$, so we conclude that

$$
\text{vol}_{g+1}(U_d \cap W_0) = \text{vol}_{g+1}(U_g) = V_g. \quad (4.21)
$$

Using Proposition 4.4.3, we can apply Proposition 4.4.2 to the set $S = U_d \cap W$, considered as a subset of $W \cong \mathbb{R} \times \mathbb{R}^{g+1}$ (so we are setting $N = g + 1$). Here for $t \geq 0$ we have

$$
S \cap \{t\} \times \mathbb{R}^{g+1} = U_d \cap W_t.
$$

Then Proposition 4.4.2 gives

$$
\text{vol}_{g+1}(U_d \cap W_{1/T}) = \text{vol}_{g+1}(U_d \cap W_0) + O(1/T).
$$

Now by (4.17) and (4.21) we have

$$
\text{vol}_{g+1}(S(T)) = \left( \text{vol}_{g+1}(U_d \cap W_0) + O(1/T) \right) \cdot T^{g+1}
$$

$$
= V_g \cdot T^{g+1} + O(T^g),
$$
completing our proof.

4.5 Lattice points in slices: proof of Theorem 4.1.11

Now that we have an estimate for the volume of $S(T)$, we want to in turn estimate the number of integer lattice points in $S(T)$, via Theorem 4.3.1. Note that this is the same as the number of integer lattice points of $S'(T)$, which will denote the projection of $S(T)$ on $W_0 \cong \mathbb{R}^{g+1}$. Note that $\text{vol}(S(T)) = \text{vol}(S'(T))$.

Since $U_d$ is semialgebraic by Lemma 4.2.4 (and thus $T \cdot U_d$ as well), it is clear that the number and degrees of the polynomial inequalities and equalities needed to define $S'(T)$ are independent of $T$. Thus to apply Theorem 4.3.1, it remains only to bound the volumes of projections of $S'(T)$ on coordinate planes.

For $\bar{w} \in S'(T)$, by (4.6) we have

$$\|\bar{w}\|_\infty \leq \|\bar{\ell}, \bar{w}, \bar{r}\|_\infty \leq \left(\frac{d}{\lfloor d/2 \rfloor}\right) \mu(\bar{\ell}, \bar{w}, \bar{r}) \leq \left(\frac{d}{\lfloor d/2 \rfloor}\right) T,$$

so $S'(T)$ is contained inside a cube of side length $2\left(\frac{d}{\lfloor d/2 \rfloor}\right) T$ in $\mathbb{R}^{g+1}$. Thus for $j = 1, \ldots, g$, any projection of $S'(T)$ on a $j$-dimensional coordinate plane is contained inside a cube of side length $2\left(\frac{d}{\lfloor d/2 \rfloor}\right) T$ in $\mathbb{R}^j$, and thus has volume at most $\left(2\left(\frac{d}{\lfloor d/2 \rfloor}\right) T\right)^j$, which is certainly $O(T^g)$ for $j = 1, \ldots, g$.

By Theorem 4.3.1, we now get

$$\mathcal{M}(d, \bar{\ell}, \bar{r}, T) = \text{vol}(S'(T)) + O(T^g),$$

and so by Theorem 4.4.1 we have

$$\mathcal{M}(d, \bar{\ell}, \bar{r}, T) = V_g \cdot T^{g+1} + O(T^g).$$
4.6 Proofs of Theorem 4.1.1 and corollaries

In this section we transfer our counts for degree $d$ polynomials in Theorem 4.1.1 to the counts for degree $d$ algebraic numbers in Theorem 4.1.1. This only requires estimating the number of reducible polynomials, because the hypotheses of Theorem 4.1.1 (fixing a positive number of coefficients which must be coprime) ensure that the only irreducible polynomials we count are actually minimal polynomials of degree $d$. We’ll apply a version of Hilbert’s irreducibility theorem to achieve the most general result, which is the last ingredient needed to prove Theorem 4.1.1. However, in various special cases we work a little harder to improve the power savings, which will prove the sharper results of Corollaries 4.1.2 through 4.1.5.

We keep the notation and hypotheses of Theorem 4.1.1, fixing $d, m, n, \tilde{\ell} \in \mathbb{Z}^m$, and $\tilde{r} \in \mathbb{Z}^n$. Furthermore, we let $M_{\text{red}}(d, \tilde{\ell}, \tilde{r}, T)$ denote the number of reducible integer polynomials of the form

$$f(z) = \ell_0 z^d + \cdots + \ell_{m-1} z^{d-(m-1)} + x_m z^{d-m} + \cdots + x_{d-n} z^n + r_{d-n+1} z^{n-1} + \cdots + r_d,$$

and as before we set $g = d - m - n$.

**Proposition 4.6.1.** We have

$$M_{\text{red}}(d, \tilde{\ell}, \tilde{r}, T) = O \left( T^{g+\frac{1}{2}} \log T \right). \quad (4.22)$$

**Proof.** One of our hypotheses is that, if $n > 0$, then $r_d \neq 0$; that is, we don’t want $f(z)$ to be divisible by $z$. It’s not hard to see that, under this hypothesis, the “generic polynomial” $f(x_m, \ldots, x_{d-n}, z)$ defined above is irreducible in $\mathbb{Z}[x_m, \ldots, x_{d-n}, z]$, by the following argument. Suppose $f$ factors nontrivially as $f = f_1 f_2$. Since $f$ has degree 1 in $x_m$, without loss of generality $f_1$ has degree 1 in $x_m$ and $f_2$ has degree 0 in $x_m$. Let $f_1 = g_1 x_m + g_2$, where $g_1$ and $g_2$ are in $\mathbb{Z}[x_{m+1}, \ldots, x_{d-n}, z]$, so we have $f = f_2 g_1 x_m + f_2 g_2$, which means that $f_2 g_1 = z^{d-m}$. We discover that $f_2$ is (plus or minus) a power of $z$, and so $f$ was divisible by $z$ all along.
CHAPTER 4. SLICING THE STARS

Now our proposition follows immediately from a quantitative form of Hilbert’s irreducibility theorem due to Cohen [Coh81, Theorem 2.5]. In the notation of the cited theorem, we are setting \( r = 1 \), and \( s = g + 1 \). Cohen uses the \( \ell_\infty \) norm on polynomials rather than Mahler measure, but these are directly comparable by (4.6). It’s worth noting that, as can be inferred from [Coh81, Section 2], the implied constant in (4.22) depends only on \( d, g \), and \( \| (\bar{\ell}, \bar{r}) \|_\infty \), and could in principle be effectively computed. \( \square \)

In the situations of Corollaries 4.1.2 through 4.1.5, we can obtain stronger bounds.

**Proposition 4.6.2.** For \( d \geq 2 \), and \( r \in \mathbb{Z} \setminus \{0\} \), we have

\[
    \mathcal{M}^{\text{red}}(d, (1), (r), T) = O\left(T^{d-2}\right).
\]

For \( d \geq 3 \), \( t \in \mathbb{Z} \), and \( r \in \mathbb{Z} \setminus \{0\} \), we have

\[
    \mathcal{M}^{\text{red}}(d, (1, t), (r), T) = O\left(T^{d-3}\right).
\]

For \( d \geq 2 \), \( t \geq 1 \), and \( t \in \mathbb{Z} \), we have

\[
    \mathcal{M}^{\text{red}}(d, (1, t), (), T) = \begin{cases} 
        O\left(\sqrt{T}\right), & \text{if } d = 2, \\
        O\left(T \log T\right), & \text{if } d = 3, \text{ and} \\
        O\left(T^{d-2}\right), & \text{if } d > 3.
    \end{cases}
\]

We postpone the proof until Section 4.10, where we’ll prove it with explicit constants. For now, we show how Theorem 4.1.1 and Corollaries 4.1.2 through 4.1.5 follow from our results so far.

**Proof of Theorem 4.1.1 and Corollaries 4.1.2 through 4.1.5.** By Theorem 4.1.11 we have that

\[
    \mathcal{M}(d, \bar{\ell}, \bar{r}, T) = V_g \cdot T^{g+1} + O(T^g).
\]

We write \( \mathcal{M}^{\text{irr}}(d, \bar{\ell}, \bar{r}, T) \) for the corresponding number of *irreducible* degree \( d \) polynomials with specified coefficients. Since \( \bar{\ell} \) is non-empty and \( \ell_0 \neq 0 \), we have

\[
    \mathcal{M}^{\text{irr}}(d, \bar{\ell}, \bar{r}, T) = \mathcal{M}(d, \bar{\ell}, \bar{r}, T) - \mathcal{M}^{\text{red}}(d, \bar{\ell}, \bar{r}, T).
\]
Applying Theorem 4.1.11 and Proposition 4.6.1, we see that
\[
\mathcal{M}^{\text{irr}}(d, \tilde{\ell}, \tilde{r}, T) = V \cdot T^{g+1} + O(T^{g+\frac{1}{2}} \log T). \tag{4.23}
\]
By our assumption that the specified coefficients had no common factor, and that \( \ell_0 > 0 \), any irreducible polynomial counted will be a minimal polynomial. Thus each of the degree \( d \) irreducible polynomials \( f \) we count corresponds to exactly \( d \) algebraic numbers \( \alpha_1, \ldots, \alpha_d \) of degree \( d \) and height at most \( \mathcal{H} \), where \( \mathcal{H}^d = T \), since \( \mu(f) = H(\alpha_i)^d \) for \( i = 1, \ldots, d \). In other words, we have
\[
\mathcal{N}(d, \tilde{\ell}, \tilde{r}, \mathcal{H}) = d\mathcal{M}^{\text{irr}}(d, \tilde{\ell}, \tilde{r}, \mathcal{H}^d).
\]
Now Theorem 4.1.1 follows from (4.23).

Corollaries 4.1.3, 4.1.4, and 4.1.5 follow similarly, by replacing the general upper bound for reducible polynomials in Proposition 4.6.1 with the sharper bounds in Proposition 4.6.2. The count for units in Corollary 4.1.2 follows immediately from Corollary 4.1.3, since an algebraic number is a unit exactly if it is an algebraic integer with norm \( \pm 1 \). \( \square \)

### 4.7 Counting polynomials: explicit bounds

Let \( \mathcal{M}(\leq d, T) \) denote the number of polynomials in \( \mathbb{Z}[z] \) of degree at most \( d \) and Mahler measure at most \( T \). The following is an explicit version of [CV01, Theorem 3]. To condense notation, we define for each \( d \geq 0 \) the constants
\[
P(d) = \prod_{j=0}^{d} \binom{d}{j}, \quad \text{and} \quad A(d) = \sum_{k=0}^{d} P(k)P(d-k). \tag{4.24}
\]

**Theorem 4.7.1.** For \( d \geq 1 \) and \( T \geq 1 \) we have
\[
|\mathcal{M}(\leq d, T) - \text{vol}(U_d)T^{d+1}| \leq \kappa_0(d)T^d,
\]
where
\[
\kappa_0(d) = 4^{d+1} A(d) \left( \binom{d}{\lfloor d/2 \rfloor} + 1 \right)^d \leq 40 \sqrt[4]{2\pi^3} e^{-3} \cdot d^{-1/4} \cdot (4\sqrt{2}e^{3/2}\pi^{-3/2})^d \cdot (2\sqrt{e})^{d^2} \leq 5.59 \cdot (15.01)^{d^2}.
\]

Proof. We refer to the parametrization of the boundary of $U_d$ detailed in Section 4.2.3. The boundary $\partial(TU_d)$ is parametrized by $2d + 2$ maps of the form
\[
T_{b,k,d} : J_{k,d}^\varepsilon \to \partial(TU_d) \subseteq \mathbb{R}^{d+1},
\]
\[
T_{b,k,d}(\bar{x}, \bar{y}) = (T f_0(\bar{x}, \bar{y}), \ldots, T f_d(\bar{x}, \bar{y})),
\]
where
\[
f_i(\bar{x}, \bar{y}) := w_i((1, \bar{x}), (\bar{y}, \varepsilon)), \text{ for } i = 0, \ldots, d,
\]
and $w_i$ is as in (4.10).

Fix for the moment $k \in \{0, \ldots, d\}$ and $\varepsilon \in \{\pm 1\}$. If $(\bar{x}, \bar{y})$ lies in any $J_{k,d}^\varepsilon$, then $\mu(1, \bar{x}) = \mu(\bar{y}, \varepsilon) = 1$, and so by (4.5) we have $\|((\bar{x}, \bar{y}))\|_\infty \leq \left( \binom{d}{\lfloor d/2 \rfloor} \right)^d$, and so
\[
\|((\bar{x}, \bar{y}))\|_2 \leq \sqrt{d} \|((\bar{x}, \bar{y}))\|_\infty \leq \sqrt{d} \cdot \left( \binom{d}{\lfloor d/2 \rfloor} \right)^d.
\] (4.25)

Also, for any $i \in \{0, \ldots, d\}$, by (4.10) we have
\[
\|\nabla f_i(\bar{x}, \bar{y})\|_\infty \leq \max\{1, \|((\bar{x}, \bar{y}))\|_\infty\}.
\] (4.26)

Now for any $i \in \{0, \ldots, d\}$ and for any $(\bar{x}_1, \bar{y}_1), (\bar{x}_2, \bar{y}_2) \in J_{k,d}^\varepsilon$, using (4.25) and (4.26) we
CHAPTER 4. SLICING THE STARS

have

\[
|T f_i(\bar{x}_1, \bar{y}_1) - T f_i(\bar{x}_2, \bar{y}_2)| = T|f_i(\bar{x}_1, \bar{y}_1) - f_i(\bar{x}_2, \bar{y}_2)|
\]

\[
\leq T \cdot \sup_{(\bar{x}, \bar{y}) \in J} \|\nabla f_i(\bar{x}, \bar{y})\|_2 \cdot \|(\bar{x}_1, \bar{y}_1) - (\bar{x}_2, \bar{y}_2)\|_2
\]

\[
\leq T \cdot \sqrt{d} \cdot \sup_{(\bar{x}, \bar{y}) \in J} \|\bar{x}, \bar{y}\|_\infty \cdot \sqrt{d} \cdot \|(\bar{x}_1, \bar{y}_1) - (\bar{x}_2, \bar{y}_2)\|_\infty
\]

\[
\leq T \cdot \sqrt{d} \cdot \left(\frac{d}{\lfloor d/2 \rfloor}\right) \cdot \sqrt{d} \cdot \|(\bar{x}_1, \bar{y}_1) - (\bar{x}_2, \bar{y}_2)\|_\infty
\]

\[
= d \cdot \left(\frac{d}{\lfloor d/2 \rfloor}\right) \cdot T \cdot \|(\bar{x}_1, \bar{y}_1) - (\bar{x}_2, \bar{y}_2)\|_\infty.
\]

We obtain the Lipschitz estimate

\[
\|T b_{k,d}(\bar{x}_1, \bar{y}_1) - T b_{k,d}(\bar{x}_2, \bar{y}_2)\|_\infty \leq KT \cdot \|(\bar{x}_1, \bar{y}_1) - (\bar{x}_2, \bar{y}_2)\|_\infty,
\]

(4.27)

where \(K = K(d) := d \cdot \left(\frac{d}{\lfloor d/2 \rfloor}\right) \leq \sqrt{d} \cdot 2^d\).

We now apply the Lipschitz counting principle from Section 4.3. Fix \(T \geq 1\), so that \([KT] \leq KT + 1 \leq (K + 1)T\). Since \(T b_{k,d}\) satisfies the Lipschitz estimate (4.27), the image under \(T b_{k,d}\) of any translate of \([0, 1/[KT]]^d\) is contained in a unit cube in \(\mathbb{R}^{d+1}\).

Let \(Q_{k,d}(T)\) denote the number of \(d\)-cubes of side length \(1/[KT]\) required to cover \(J_{k,d}^e\). The easiest way to get an estimate for this quantity would be to note that each \(J\) is contained in a cube of side length \(2 \cdot \left(\frac{d}{\lfloor d/2 \rfloor}\right)^k\). However, we can do significantly better than this without too much effort, using the bounds on the individual coordinates (coefficients) from Lemma 4.2.1.

Using (4.5), we see that \(J_{k,d}^e\) is contained in the cuboid

\[
\left\{(x_1, \ldots, x_k, y_0, \ldots, y_{d-k-1}) \in \mathbb{R}^k \times \mathbb{R}^{d-k} \mid |x_\ell| \leq \left(\frac{k}{\ell}\right), |y_m| \leq \left(\frac{d-k}{m}\right), \forall \ell, m \right\},
\]

and therefore \(J_{k,d}^e\) can be covered by

\[
\prod_{\ell=1}^k 2\left(\frac{k}{\ell}\right) \cdot \prod_{m=0}^{d-k-1} 2\left(\frac{d-k}{m}\right) = 2^d P(k) \cdot P(d-k)
\]
CHAPTER 4. SLICING THE STARS

unit $d$-cubes. Hence surely we have

$$Q_{k,d}(T) \leq 2^d P(k) P(d - k) [KT]^d \leq 2^d P(k) P(d - k)((K + 1)T)^d. \quad (4.28)$$

Using Theorem 4.3.3 we conclude that

$$|M(\leq d, T) - \text{vol}(U_d)T^{d+1}| \leq 2^{d+1} \sum_{k,\varepsilon} Q_{k,d}(T)$$

$$\leq 2^{d+1} \cdot 2 \sum_{k=0}^d 2^d P(k) P(d - k)(K + 1)^dT^d$$

$$= 4^{d+1} A(d)(K + 1)^dT^d = \kappa_0(d)T^d.$$

We now estimate $\kappa_0(d)$ as in the statement of the theorem, using Lemma A.0.1 from the appendix:

$$\kappa_0(d) = 4^{d+1} A(d) \left( d \left( d \left\lfloor \frac{d}{d/2} \right\rfloor \right) + 1 \right)^d \leq 4^{d+1} A(d) \left( 2d \left( d \left\lfloor \frac{d}{d/2} \right\rfloor \right) \right)^d$$

$$\leq 4^{d+1} A(d) \left( \frac{2e}{\pi} \sqrt{d^2} \right)^d \leq \left( 40 \sqrt{2\pi^3/4} e^{-3} \right) d^{-1/4} \left( 4\sqrt{2\pi^3/2} \pi^{-3/2} / 2 \right) (2\sqrt{e})^d$$

$$= a \frac{b^d c^d}{d} \leq a(bc)^d = 40 \sqrt{2\pi^3/4} e^{-3} \cdot (8\sqrt{2\pi^{-3/2} e^2})^d \leq 5.59 \cdot (15.01)^d,$$

where $a = 40 \sqrt{2\pi^3/4} e^{-3}$, $b = 4\sqrt{2e^3/\pi - 3/2}$, and $c = 2\sqrt{e}$.

Remark 4.7.2. As each $J_{k,d}$ is measurable, it follows that for each $d$ we have

$$Q_{k,d}(T) \sim \text{vol}(J_{k,d}) \cdot ((K + 1)T)^d, \text{ as } T \to \infty. \quad (4.29)$$

Notice that

$$\text{vol}(J_{k,d}) = p_k(1) \cdot p_{d-k}(1),$$

where $p_d(T)$ is as defined in (4.8). The sharpest way to proceed would be to explicitly estimate the error in (4.29). Comparing (4.29) with (4.28): how much does $\text{vol}(J_{k,d})$ differ from $2^d P(k) P(d - k)$?
4.8 Counting monic polynomials: explicit bounds

Let $\mathcal{W}_{d,T}$ denote the subset of $\mathbb{R}^d$ corresponding to monic polynomials of degree $d$ in $\mathbb{R}[z]$ with Mahler measure at most $T$, i.e.,

$$\mathcal{W}_{d,T} = \{ \vec{w} = (w_1, \ldots, w_d) \in \mathbb{R}^d \mid \mu(1, \vec{w}) \leq T \}.$$ 

We want to estimate the number of lattice points $\mathcal{M}_1(d, T)$ in this region. Note that, in the notation of the introduction, we have $\mathcal{M}_1(d, T) = \mathcal{M}(d, (1), (), T)$. Recall that the volume of $\mathcal{W}_{d,T}$ is given by the Chern-Vaaler polynomial $p_d(T)$, as defined in (4.8).

We define, for $d$ a non-negative integer,

$$B(d) = \sum_{k=0}^{d-1} P(k) P(d-k) \gamma(k)^{d-k-1} \gamma(d-k)^{k},$$

where $P$ is as defined in (4.24), and $\gamma(k) := \binom{k}{\lfloor k/2 \rfloor}$.

**Theorem 4.8.1.** For all $d \geq 2$ and $T \geq 1$ we have

$$|\mathcal{M}_1(d, T) - p_d(T)| \leq \kappa_1(d) T^{d-1},$$

where

$$\kappa_1(d) = 4^d d^{d-1} B(d) \leq 4^d d^{d-1} 2^d.$$ 

**Proof.** Our starting point is the parametrization of the boundary $\partial \mathcal{W}_{d,T}$ given in Section 4.2, which consists of the patches described in (4.12) and (4.13). As opposed to the previous proof, we’ll need to be a bit more careful in our application of Theorem 4.3.3. Instead of a Lipschitz estimate of the form

$$\|\text{output}_1 - \text{output}_2\|_\infty \leq [\text{constant}] \cdot \|\text{input}_1 - \text{input}_2\|_\infty,$$
we’ll estimate each component of the parametrization separately, which will lead to an argument where the parameter space is tiled by “rectangles” instead of “squares.” We fix 

\( k \in \{0, \ldots, d - 1\} \) and \( \varepsilon \in \{\pm 1\} \), and set \( \mathcal{L} = \mathcal{L}_{k,d}^{\varepsilon T} \). We write

\[
\beta_{k,d}^{\varepsilon T}(\vec{x}, \vec{y}) = (1, g_1(\vec{x}, \vec{y}), \ldots, g_d(\vec{x}, \vec{y})).
\]

We have

\[
|g_i(\vec{x}_1, \vec{y}_1) - g_i(\vec{x}_2, \vec{y}_2)| \leq \sup_{(\vec{x}, \vec{y}) \in \mathcal{L}} |\nabla g_i(\vec{x}, \vec{y}) \cdot ((\vec{x}_1, \vec{y}_1) - (\vec{x}_2, \vec{y}_2))| \leq \sup_{(\vec{x}, \vec{y}) \in \mathcal{L}} \left( \sum_{\ell=1}^{k} \left| \frac{\partial g_i}{\partial x_\ell}(\vec{x}, \vec{y}) \right| |x_{1,\ell} - x_{2,\ell}| + \sum_{m=1}^{d-k-1} \left| \frac{\partial g_i}{\partial y_m}(\vec{x}, \vec{y}) \right| |y_{1,m} - y_{2,m}| \right).
\]

By (4.5), if \((\vec{x}, \vec{y}) \in \mathcal{L}\), then we must have \(|x_\ell| \leq (k \varepsilon) \leq \gamma(k)\), for each \( \ell = 1, \ldots, k \), and \(|y_m| \leq T(d-k)\), for each \( m = 1, \ldots, d - k - 1 \). Now notice that each partial derivative \( \frac{\partial g_i}{\partial x_\ell} \), as a function, is either equal to 1, \( \varepsilon T \), or \( y_{i-\ell} \), and thus has absolute value at most \( T(d-k) \leq T(d-k) \). By the same token, each \( \frac{\partial g_i}{\partial y_m} \) is equal to either 1 or \( x_{i-m} \), and thus has absolute value at most \( \min_{i-m} (k \varepsilon) \leq \gamma(k) \). Applying this to the inequality above gives

\[
|g_i(\vec{x}_1, \vec{y}_1) - g_i(\vec{x}_2, \vec{y}_2)| \leq k \gamma(d - k) T \|\vec{x}_1 - \vec{x}_2\|_\infty + (d - k - 1) \gamma(k) \|\vec{y}_1 - \vec{y}_2\|_\infty. \tag{4.30}
\]

Suppose for the moment that \( 0 < k < d - 1 \). Now if \( \frac{1}{p} + \frac{1}{q} = 1 \), and if

\[
\|\vec{x}_1 - \vec{x}_2\|_\infty \leq \frac{1}{pk \gamma(d - k) T}, \quad \text{and} \quad \|\vec{y}_1 - \vec{y}_2\|_\infty \leq \frac{1}{q(d - k - 1) \gamma(k)},
\]

then (4.30) will give

\[
|g_i(\vec{x}_1, \vec{y}_1) - g_i(\vec{x}_2, \vec{y}_2)| \leq 1.
\]

So, if \( \mathcal{P} \) is a cube in \( \mathbb{R}^k \) with sides parallel to the axes and side length

\[
\frac{1}{|p \gamma(d - k) k T|}, \tag{4.31}
\]
and if $Q$ is a cube in $\mathbb{R}^{d-k-1}$ with sides parallel to the axes and side length

$$
\frac{1}{|q(d-k-1)\gamma(k)|},
$$

(4.32)

then $\beta_{k,d}^{\ell T}(P \times Q)$ is contained in a unit $d$-cube with sides parallel to the axes in $\mathbb{R}^d$. If $k = 0$, we take $q = 1$ in (4.32), and $\beta_{k,d}^{\ell T}(Q)$ is contained in a unit $d$-cube with sides parallel to the axes in $\mathbb{R}^d$. Similarly, if $k = d - 1$, then we take $p = 1$ in (4.31), and we have the same result for $\beta_{k,d}^{T}(P)$.

This is the first part of preparing to apply Theorem 4.3.3. We let $R_{k,d}^{\varepsilon}(T)$ denote the minimum number of such “rectangles” $P \times Q$ required to cover $L$. As we argued in the previous section for the sets $\mathcal{J}_{k,d}^{\varepsilon}$, we see that $L$ can be covered by

$$
\prod_{\ell=1}^{k} 2 \binom{k}{\ell} \cdot \prod_{m=1}^{d-k-1} 2 T \binom{d-k}{m} = 2^{d-1} P(k) P(d-k) \cdot T^{d-k-1}
$$

unit cubes. Since each unit cube can be covered by

$$
[pk\gamma(d-k)T]^k \cdot [q(d-k-1)\gamma(k)]^{d-k-1}
$$

of our rectangles, we have

$$
R_{k,d}^{\varepsilon}(T) \leq 2^{d-1} P(k) P(d-k) [pk\gamma(d-k)T]^k \cdot [q(d-k-1)\gamma(k)]^{d-k-1} T^{d-k-1},
$$

for $0 < k < d - 1$. Similarly, when $k = 0$ we have

$$
R_{k,d}^{\varepsilon}(T) \leq 2^{d-1} P(k) P(d-k) \cdot [(d-k-1)\gamma(k)]^{d-k-1} T^{d-k-1},
$$

and when $k = d - 1$ we have

$$
R_{k,d}^{\varepsilon}(T) \leq 2^{d-1} P(k) P(d-k) [k\gamma(d-k)T]^k T^{d-k-1}.
$$
Following the proof in the previous section, by Theorem 4.3.3, we have

\[ |\mathcal{M}_1(d, T) - p_d(T)| \leq \sum_{k,e} 2^d p_{k,d}(T) \]

\[ \leq 2^d \cdot 2 \sum_{k=0}^{d-1} 2^{d-1} P(k) P(d - k) [p k \gamma(d - k) T]^k \cdot [q(d - k - 1) \gamma(k)]^{d-k-1} T^{d-k-1} \]

\[ = 4^d \sum_{k=0}^{d-1} P(k) P(d - k) [p k \gamma(d - k) T]^k \cdot [q(d - k - 1) \gamma(k)]^{d-k-1} T^{d-k-1}, \]

where we understand \([p k \gamma(d - k) T]^k = 1\) when \(k = 0\), and \([q(d - k - 1) \gamma(k)]^{d-k-1} = 1\) when \(k = d - 1\), and similarly below.

It will now be convenient to set \(p = \frac{d - 1}{k}\) and \(q = \frac{d - 1}{d - k - 1}\). Note that if \(k = 0\) we have \(q = 1\), and \(p\) does not appear; similarly if \(k = d - 1\) we have \(p = 1\), and \(q\) does not appear.

We conclude our proof, assuming \(T \geq 1\):

\[ |\mathcal{M}_1(d, T) - p_d(T)| \leq \]

\[ 4^d \sum_{k=0}^{d-1} P(k) P(d - k) (p k + 1)^k (q(d - k - 1) + 1)^{d-k-1} \gamma(k)^{d-k-1} \gamma(d - k)^k T^{d-k-1} \]

\[ = 4^d \sum_{k=0}^{d-1} P(k) P(d - k) d^k d^{d-k-1} \gamma(k)^{d-k-1} \gamma(d - k)^k T^{d-k-1} \]

\[ = 4^d d^{d-1} B(d) T^{d-1} = \kappa_1(d) T^{d-1}. \]

Finally, we note that \(B(d) \leq 2^d\) by Lemma A.0.2 from the appendix.

\[ \square \]

### 4.9 Lattice points in slices: explicit bounds

The goal of this section is to prove a version of the lattice point-counting result Theorem 4.1.11 with an explicit error term, albeit with worse power savings – Theorem 4.9.3 stated below. As a byproduct of the proof, we also obtain an explicit version of our volume estimate Theorem 4.4.1. Our explicit version of Theorem 4.1.11 makes it possible to estimate the quantities in Corollaries 4.1.2 through 4.1.5 with explicit error terms.
We start with some notation. Fix $d, m, n, \tilde{\ell}, \tilde{r},$ and $T > 0$ as in Section 4.1, and again set $g = d - m - n$. Let $\pi : \mathbb{R}^{d+1} \to \mathbb{R}^{g+1}$ denote the projection forgetting the first $m$ and last $n$ coordinates, given by

$$\pi(w_0, \ldots, w_d) = (w_m, \ldots, w_{d-n}).$$

Let $S(T)$ be as defined in (4.14). For $t \in [0, \infty)$, define $W_t$ as in (4.15), and set

$$B_t := \pi(W_t \cap \mathcal{U}_d).$$

By (4.16) we have

$$\pi(S(T)) = \pi(T(W_1/T \cap \mathcal{U}_d)) = T \pi((W_1/T \cap \mathcal{U}_d)) = TB_{1/T}. \quad (4.33)$$

Also note that by (4.21) we have

$$\text{vol}(B_0) = \text{vol}_{g+1}(\mathcal{U}_d \cap W_0) = V_g. \quad (4.34)$$

For subsets $A$ and $A'$ of a common set, we use the usual notation for a symmetric difference $A \triangle A' = (A \cup A') \setminus (A \cap A')$. Note that for $T > 0$ we have

$$T(A \triangle A') = (T A) \triangle (T A'),$$

for any two subsets $A$ and $A'$ of a common euclidean space.

The following lemma is the main tool of this section. We postpone its proof until the end.

**Lemma 4.9.1.** Let

$$k_1 = k_1(d, \tilde{\ell}, \tilde{r}) := 2^{d^2}d^d(m + n)\|\tilde{\ell}, \tilde{r}\|_\infty, \text{ and}$$

$$\delta_T := (k_1/T)^{1/d}.$$  

If $T \geq k_1$, then

$$B_0 \triangle B_{1/T} \subseteq \{ \bar{x} \in \mathbb{R}^{g+1} \mid 1 - \delta_T \leq \mu(\bar{x}) \leq 1 + \delta_T \}$$

$$= [(1 + \delta_T)\mathcal{U}_g] \setminus [(1 - \delta_T)\mathcal{U}_g]. \quad (4.35)$$
Using this result we take a brief detour to make the advertised explicit volume estimate. Compare the following with Theorem 4.4.1, in which we obtain a better power-savings in the error term, though in that theorem the error term is not made explicit.

**Theorem 4.9.2.** Let \( S(T) = S_{\ell, r}(T) \). If \( T \geq k_1 \), then

\[
| \text{vol}_{g+1} (S(T)) - V_g T^{g+1} | \leq c T^{g+1 - 1/d},
\]

where

\[
c = c(d, \ell, r) = 2^{d+1} \left( (m + n) \| (\ell, r) \|_\infty \right)^{1/d} \cdot d \cdot V_g.
\]

**Proof.** Using (4.33) and (4.34) we have

\[
\left| \frac{\text{vol}_{g+1}(S(T))}{T^{g+1}} - V_g \right| = |\text{vol}(B_{1/T} - \text{vol}(B_0)| \leq |\text{vol}(B_0 \triangle B_{1/T})|
\leq \text{vol}(\{ \bar{x} \in \mathbb{R}^{g+1} | 1 - \delta_T \leq \mu(\bar{x}) \leq 1 + \delta_T \}) \quad \text{(by Lemma 4.9.1)}
= 2\delta_T V_g = \frac{c}{T^{1/d}}.
\]

\( \square \)

In Section 4.4 we estimated the volume of \( S(T) \) in order to estimate the number of lattice points in that set. Here, by contrast, we actually don’t require a volume estimate; Lemma 4.9.1 allows us to directly estimate the number of lattice points in \( S(T) \), which we have denoted \( \mathcal{M}(d, \ell, r, T) \), as follows.

**Theorem 4.9.3.** Let \( k_1 = k_1(d, \ell, r) \) be as in Lemma 4.9.1, and \( \kappa_0 \) as defined in Theorem 4.7.1. For all \( T \geq k_1 \), we have

\[
| \mathcal{M}(d, \ell, r, T) - V_g \cdot T^{g+1} | \leq \kappa(d, \ell, r)(T^{g+1 - 1/d}),
\]

where

\[
\kappa(d, \ell, r) = (g + 1)2^{g+1}k_1^{1/d}V_g + (g2^g k_1^{1/d} + 1)\kappa_0(g).
\]
We note for later that $V_g \leq 2 \cdot 15^g$ for all $g \geq 0$, and so

$$
\kappa(d, \vec{\ell}, \vec{r}) \leq (g + 1)2^{g+1}k_1^{1/d} (V_g + \kappa_0(g))
$$

$$
\leq d(g + 1)2^{d+g+1}(m + n)^{1/d}\|\vec{\ell}, \vec{r}\|_{\infty} (V_g + \kappa_0(g))
$$

$$
\leq (2 + a) d(g + 1)2^{d+g+1}(m + n)^{1/d}\|\vec{\ell}, \vec{r}\|_{\infty}(bc)^g,
$$

(4.36)

where $a, b,$ and $c$ are the constants appearing in the end of the proof of Theorem 4.7.1 (note that $bc > 15$).

Proof. We let $Z(\Omega)$ denote the number integer lattice points in a subset $\Omega$ of euclidean space. Again applying (4.33), we have

$$
\mathcal{M}(d, \vec{\ell}, \vec{r}, T) = Z(S(T)) = Z(\pi(S(T)) = Z(TB_{1/T}).
$$

Also note that

$$
Z(TB_0) = \mathcal{M}(\leq g, T),
$$

which we estimated in Section 4.7. Therefore, using the triangle inequality and Theorem 4.7.1, we have

$$
\left|\mathcal{M}(d, \vec{\ell}, \vec{r}, T) - V_g \cdot T^{g+1}\right| = \left|Z(TB_{1/T}) - V_g \cdot T^{g+1}\right|
$$

$$
\leq \left|Z(TB_{1/T}) - Z(TB_0)\right| + \left|Z(TB_0) - V_g \cdot T^{g+1}\right|
$$

$$
\leq \left|Z(TB_{1/T}) - Z(TB_0)\right| + \kappa_0(g)T^g,
$$

(4.37)

Clearly

$$
\left|Z(TB_{1/T}) - Z(TB_0)\right| \leq Z\left( (TB_{1/T}) \triangle (TB_0) \right) = Z\left( T(B_{1/T} \triangle B_0) \right),
$$

and by Lemma 4.9.1 we have

$$
T(B_{1/T} \triangle B_0) \subseteq [(T + T\delta_T)U_g] \setminus [(T - T\delta_T)U_g].
$$
Hence, applying Theorem 4.7.1 a second time and using an elementary estimate from the mean value theorem, we find that

\[
\left| Z(TB_{1/T}) - Z(TB_0) \right| \leq Z((T + T\delta_T)U_g) - Z((T - T\delta_T)U_g) \\
\leq V_g \left[ (T + T\delta_T)^{g+1} - (T - T\delta_T)^{g+1} \right] \\
+ \kappa_0(g) [(T + T\delta_T)^g - (T - T\delta_T)^g] \\
\leq V_g(g + 1)(T + T\delta_T)^g(2T\delta_T) + \kappa_0(g)(T + T\delta_T)^{g-1}(2T\delta_T).
\]

Recall that \( \delta_T = k_1^{1/d}T^{-1/d} \). Assuming \( T \geq k_1 \) means that \( \delta_T \leq 1 \). Combining the estimate just obtained with (4.37), we achieve

\[
\left| \mathcal{M}(d, \ell^r, T) - V_g \cdot T^{g+1} \right| \leq V_g(g + 1)(2T)^g \cdot 2T^{1-1/d} \cdot k_1^{1/d} \\
+ g\kappa_0(g)(2T)^{g-1} \cdot 2T^{1-1/d} \cdot k_1^{1/d} + \kappa_0(g)T^g \\
\leq [(g + 1)2^{g+1}k_1^{1/d}V_g + (g2^gk_1^{1/d} + 1)\kappa_0(g)]T^{g+1-\frac{1}{d}}.
\]

\[\square\]

**Proof of Lemma 4.9.1.** We will require the following Lipschitz-type estimate for the Mahler measure [CV01, Theorem 4], which is a quantitative form of the continuity of Mahler measure:

**Theorem 4.9.4** (Chern-Vaaler). For any \( \vec{w}_1, \vec{w}_2 \in \mathbb{R}^{d+1} \), we have

\[
\left| \mu(\vec{w}_1)^{1/d} - \mu(\vec{w}_2)^{1/d} \right| \leq 2 \| \vec{w}_1 - \vec{w}_2 \|_1^{1/d},
\]

where \( \| \vec{w} \|_1 = \sum_{i=0}^{d} |w_i| \) is the usual \( \ell^1 \)-norm of a vector \( \vec{w} = (w_0, \ldots, w_d) \in \mathbb{R}^{d+1} \).

If \( \mu(\vec{w}_1) \) and \( \mu(\vec{w}_2) \) are both less than some constant \( k \), then applying (4.38) yields

\[
\left| \mu(\vec{w}_1) - \mu(\vec{w}_2) \right| = \left| \mu(\vec{w}_1)^{1/d} - \mu(\vec{w}_2)^{1/d} \right| \cdot \sum_{i=1}^{d} \left( \mu(\vec{w}_1)^{\frac{d-i}{d}} \mu(\vec{w}_2)^{\frac{i}{d}} \right) \leq 2 \| \vec{w}_1 - \vec{w}_2 \|_1^{1/d} \cdot dk^{\frac{d-1}{d}}.
\]

(4.39)
We will shortly apply this observation with \( k = 2^d \). We assume \( T \geq k_1 \).

Let \( \bar{x} \) be a vector in \( B_0 \triangle B_{1/T} \), and write

\[
\bar{x}_0 = \tau(\bar{x}) = (\bar{0}_m, \bar{x}, \bar{0}_n) \in \mathbb{R}^{d+1}, \quad \text{and} \quad \bar{x}_T = \left( \frac{\bar{\ell}}{T}, \frac{\bar{r}}{T}, \bar{x}_T \right) \in \mathbb{R}^{d+1}.
\]

Notice that \( \mu(\bar{x}_0) = \mu(\bar{x}) \) because \( \tau \) preserves Mahler measure, as noted in the proof of Theorem 4.4.1.

Since \( \bar{x} \in B_0 \triangle B_{1/T} \), it’s clear that either

\[
\mu(\bar{x}_0) \leq 1 < \mu(\bar{x}_T), \tag{4.40}
\]

or

\[
\mu(\bar{x}_T) \leq 1 < \mu(\bar{x}_0), \tag{4.41}
\]

must hold. In either case, we have

\[
1 - |\mu(\bar{x}_0) - \mu(\bar{x}_T)| \leq \mu(\bar{x}_0) \leq 1 + |\mu(\bar{x}_0) - \mu(\bar{x}_T)| \tag{4.42}
\]

First, suppose \( \bar{x} \) is in \( B_0 \), but not in \( B_{1/T} \), so (4.40) holds. Then, by (4.6) and our assumption that \( T \geq k_1 \), we have

\[
\mu(\bar{x}_T) \leq \|\bar{x}_T\|_\infty \sqrt{d+1} \leq \max\{\|\bar{x}_0\|_\infty, 1\} \sqrt{d+1} \leq \left( \frac{d}{|d/2|} \right) \sqrt{d+1} \max\{\mu(\bar{x}_0), 1\} \leq 2^d, \tag{4.43}
\]

as in the statement of the proposition. Here we have used that \( \left( \frac{d}{|d/2|} \right) \sqrt{d+1} \leq 2^d \) (see for example [BG06, Lemma 1.6.12]). Note that the second inequality in (4.43) follows because \( T \geq \|(\bar{\ell}, \bar{r})\|_\infty \). On the other hand, if \( \bar{x} \) is in \( B_{1/T} \), but not in \( B_0 \), so that (4.41) holds, then by applying (4.6) again, we have, in the same fashion as before:

\[
\mu(\bar{x}_0) \leq \|\bar{x}\|_\infty \sqrt{g+1} \leq \max\{\|\bar{x}_T\|_\infty, 1\} \sqrt{d+1} \leq \max\{\mu(\bar{x}_T), 1\} \leq 2^d.
\]
CHAPTER 4. SLICING THE STARS

Since in either case we have that both \( \mu(\tilde{x}_0) \) and \( \mu(\tilde{x}_T) \) are at most \( 2^d \), we may apply (4.39) to achieve

\[
|\mu(\tilde{x}_0) - \mu(\tilde{x}_T)| \leq 2\|\tilde{x}_0 - \tilde{x}_T\|_1^{1/d} \cdot d(2^d)^{d-1}. \tag{4.44}
\]

Note that

\[
\|\tilde{x}_0 - \tilde{x}_T\|_1 = \sum_{i=0}^{m-1} |\ell_i|/T + \sum_{i=d-n+1}^{d} |r_i|/T \leq (m + n)\|\tilde{e}, \tilde{r}\|_\infty/T,
\]

which, combined with (4.44), yields

\[
|\mu(\tilde{x}_0) - \mu(\tilde{x}_T)| \leq \delta_T.
\]

Now we combine with (4.42), and conclude that \( 1 - \delta_T \leq \mu(\tilde{x}) \leq 1 + \delta_T \). This completes our justification of (4.35), which concludes our proof of Lemma 4.9.1.

4.10 Reducible and imprimitive polynomials

In this section we begin to transfer our explicit counts for polynomials of degree at most \( d \) to explicit counts for algebraic numbers of degree \( d \), by counting their minimal polynomials. In most cases, this simply means bounding the number of reducible polynomials, because the hypotheses imposed in Theorem 4.1.1 don’t allow for any irreducible polynomials to be counted other than minimal polynomials of degree \( d \). We’ll apply a version of Hilbert’s irreducibility theorem to achieve the most general bound, which will finish off the proof of Theorem 4.1.1. However, in various special cases we work a little harder to improve the power savings.

In the one case we consider outside the hypotheses of Theorem 4.1.1, namely polynomials with no coefficients fixed, we must also address the presence of imprimitive degree \( d \) polynomials and lower-degree polynomials.
Several times in our arguments we use the following estimate: if \( a \geq 2 \), then
\[
\sum_{k=1}^{K} a^k = a^{K+1} - a \left( a^{K+1} \right) - 2a^K.
\]  
(4.45)

We write
\[
P(d) := \prod_{j=0}^{d} \binom{d}{j}, \text{ for } d \geq 0, \text{ and}
\]
\[
C_{m,n}(d) := \prod_{j=m}^{d-n} \left( 2 \binom{d}{j} + 1 \right), \text{ for } 0 \leq m + n \leq d.
\]

### 4.10.1 All polynomials

Let \( \mathcal{M}(d,T) \) denote the number of integer polynomials of degree exactly \( d \) and Mahler measure at most \( T \), and let \( \mathcal{M}^{\text{red}}(d,T) \) denote the number of such polynomials that are reducible. Recall that \( \mathcal{M}(\leq d,T) \) denotes the number of integer polynomials of degree at most \( d \) and Mahler measure at most \( T \). By (4.5), for all \( d \geq 0 \) and \( T > 0 \) we have
\[
\mathcal{M}(d,T) \leq \mathcal{M}(\leq d,T) \leq C_{0,0}(d)T^{d+1} \leq c_0 2^{d+1}P(d)T^{d+1},
\]  
(4.46)

where \( c_0 = 3159/1024 \), using Lemma A.0.3 from the appendix.

**Proposition 4.10.1.** We have
\[
\mathcal{M}^{\text{red}}(d,T) \leq \begin{cases} 
1758 \cdot T^2 \log T, & \text{if } d = 2, \ T \geq 2, \ \text{and} \\
16c_0^4dP(d-1) \cdot T^d, & \text{if } d \geq 3, \ T \geq 1.
\end{cases}
\]

**Proof.** For a reducible polynomial \( f \) of degree \( d \) and Mahler measure at most \( T \), there exist \( 1 \leq d_2 \leq d_1 \leq d - 1 \) such that \( f = f_1f_2 \), where each \( f_i \) is an integer polynomial with \( \deg(f_i) = d_i \). Of course we have \( d = d_1 + d_2 \). Let \( k \) be the unique integer such that \( 2^{k-1} \leq \mu(f_1) < 2^k \). We have \( 1 \leq k \leq K \), where \( K = \left\lfloor \frac{\log T}{\log 2} \right\rfloor + 1 \), and \( \mu(f_2) \leq 2^{1-k}T \).

Given such a pair \((d_1,d_2)\), by (4.46) there are at most \( c_0 2^{d_1+1}P(d_1)2^{k(d_1+1)} \) choices of such an \( f_1 \), and at most \( c_0 2^{d_2+1}P(d_2)(2^{1-k}T)^{d_2+1} \) choices for \( f_2 \). Assume first that \( d_1 > d_2 \).
We'll use below that $P(d_1)P(d_2)$ is always less than or equal to $P(d - 1)$, by Lemma A.0.4 in the appendix. Summing over all possible $k$ and applying (4.45), the number of pairs of polynomials is at most

$$
\sum_{k=1}^{K} c_0 2^{d_1+1} P(d_1)c_0 2^{d_2+1} P(d_2)2^{k(d_1+1)}(2^{d_2+1} - 2^{k-d_2}) = 4c_0^2 2^d P(d_1)P(d_2)(2T)^{d_2+1} \sum_{k=1}^{K} 2^{k(d_1-d_2)}
$$

$$
\leq 4c_0^2 2^d P(d - 1)(2T)^{d_2+1} \left[ 2 \cdot 2^{K(d_1-d_2)} \right] \leq 8c_0^2 2^d P(d - 1)(2T)^{d_1+1} \leq 16c_0^2 2^d 2d_1 P(d - 1)T^d.
$$

If instead $d_1 = d_2 = \frac{d}{2}$, (so in particular $d$ is even), then the first line above is at most

$$
4c_0^2 2^d P(d - 1)(2T)^{d_1+1} K.
$$

In the case $d = 2$, note that for $T \geq 2$ we have $K \leq \frac{2}{\log(2)} \log T$, and so

$$
\mathcal{M}^{red}(2, T) \leq 4c_0^2 2^2 P(1)(2T)^{1+1} \leq 64c_0^2 T^2 \frac{2}{\log(2)} \log T
$$

$$
= \frac{128c_0^2}{\log(2)} T^2 \log T \leq 1758 \cdot T^2 \log T.
$$

Whenever $T \geq 1$ we have $K \leq 2T$, and thus for even $d \geq 4$,

$$
4c_0^2 2^d P(d - 1)(2T)^{d_1+1} K \leq 8c_0^2 2^d 2d_1 P(d - 1)T^{\frac{d}{2}+1} \cdot 2T \leq 16c_0^2 2^d 2d_1 P(d - 1)T^d,
$$

so we have the same bound we had when we assumed $d_2 < d_1$.

Finally, for any $d \geq 3$, summing over the possible values of $d_1$ gives that

$$
\mathcal{M}^{red}(d, T) \leq \sum_{d_1=1}^{d} \sum_{d_1=1}^{d} 16c_0^2 2^d 2d_1 P(d - 1)T^d \leq 16c_0^2 2^d P(d - 1)T^d \sum_{d_1=1}^{d} 2^{d_1}
$$

$$
= 16c_0^2 2^d P(d - 1)T^d (2^d - 2) \leq 16c_0^2 4^d P(d - 1) \cdot T^d.
$$

We follow the proof of [MV08, Lemma 2] in counting primitive polynomials, but we’ll keep track of implied constants. For $n = 1, 2, \ldots$, let $\mathcal{M}'(\leq d, T)$ denote the number of nonzero
integer polynomials of degree at most \(d\) and Mahler measure at most \(T\), such that the greatest common divisor of the coefficients is \(n\). We let \(\mathcal{M}^n(d, T)\) denote the corresponding number of polynomials with degree \(\text{exactly } d\), so \(\mathcal{M}^1(d, T)\) is the number of primitive polynomials of degree \(d\) and Mahler measure at most \(T\). Recall that \(\kappa_0(d)\) is a function of \(d\) appearing in Theorem 4.7.1.

**Theorem 4.10.2.** For all \(d \geq 2\) and \(T \geq 1\) we have

\[
|\mathcal{M}^1(d, T) - \frac{V_d}{\zeta(d+1)} T^{d+1}| \leq \left(\frac{V_d}{d} + 1\right) T + (C_{0,0}(d-1) + \zeta(d)\kappa_0(d)) T^d,
\]

where \(\zeta\) is the Riemann zeta-function.

**Proof.** Being careful to account for the zero polynomial, we have

\[
\mathcal{M}(\leq d, T) - 1 = \sum_{1 \leq n \leq T} \mathcal{M}^n(\leq d, T) = \sum_{1 \leq n \leq T} \mathcal{M}^1(\leq d, T/n).
\]

By Möbius inversion (below we commit a sin of notation overloading and let \(\mu\) denote the Möbius function), this tells us that

\[
\mathcal{M}^1(\leq d, T) = \sum_{1 \leq n \leq T} \mu(n) [\mathcal{M}(\leq d, T/n) - 1].
\]

Combining this with Theorem 4.7.1 and (4.46), we have

\[
\begin{align*}
&\left|\mathcal{M}^1(d, T) - V_d T^{d+1} \sum_{1 \leq n \leq T} \frac{\mu(n)}{n^{d+1}}\right| \\
&= \left|\mathcal{M}^1(d, T) - \mathcal{M}^1(\leq d, T) + \sum_{n=1}^{T} \mu(n) [\mathcal{M}(\leq d, T/n) - 1] - V_d T^{d+1} \sum_{n=1}^{T} \frac{\mu(n)}{n^{d+1}}\right| \\
&\leq \mathcal{M}^1(\leq d - 1, T) + \sum_{n=1}^{T} |\mu(n)| + \sum_{n=1}^{T} |\mathcal{M}(\leq d, T/n) - V_d(T/n)^{d+1}| \\
&\leq \mathcal{M}(\leq d - 1, T) + T + \sum_{n=1}^{T} \kappa_0(d)(T/n)^d \leq C_{0,0}(d-1)T^d + T + \kappa_0(d)T^d \sum_{n=1}^{T} \frac{1}{n^d} \\
&\leq T + (C_{0,0}(d-1) + \zeta(d)\kappa_0(d)) T^d.
\end{align*}
\]
This in turn gives
\[
\left| \mathcal{M}_1(d, T) - \frac{V_d}{\zeta(d+1)} T^{d+1} \right| \leq V_d T^{d+1} \sum_{n=T+1}^{\infty} n^{-(d+1)} + T + (C_{0,0}(d-1) + \zeta(d)\kappa_0(d))T^d
\]
\[
\leq \left( \frac{V_d}{d} + 1 \right) T + (C_{0,0}(d-1) + \zeta(d)\kappa_0(d))T^d,
\]
by applying the integral estimate
\[
\sum_{n=T+1}^{\infty} n^{-(d+1)} \leq d^{-1}T^{-d}.
\]
This establishes the theorem.

4.10.2 Monic polynomials

Next, let \( \mathcal{M}_1(d, T) \) denote the number of monic integer polynomials of degree \( d \) and Mahler measure at most \( T \), and let \( \mathcal{M}_1^{\text{red}}(d, T) \) denote the number of such polynomials that are reducible. Using (4.5), we have for all \( d \geq 0 \) and \( T > 0 \) that
\[
\mathcal{M}_1(d, T) \leq C_{1,0}(d)T^d \leq c_1 2^d P(d)T^d,
\]
where \( c_1 = \frac{1053}{512} \), from Lemma A.0.3 in the appendix.

We’ll assume \( d \geq 2 \). In estimating the number of reducible monic polynomials, we follow the pattern of the proof of Proposition 4.10.1, noting that if a monic polynomial is reducible, its factors can be chosen to be monic. Using the same notation as in that proof, we have that the number of pairs of monic polynomials of degree \( d_1 \) and \( d_2 \), with \( d_1 > d_2 \), is at most
\[
\sum_{k=1}^{K} c_1 2^{d_1} P(d_1) c_1 2^{d_2} P(d_2) 2^{kd_1}(2^{1-k}T)^{d_2} = c_1^2 2^{d_1} P(d_1) P(d_2) (2T)^{d_2} \sum_{k=1}^{K} 2^{k(d_1-d_2)}
\]
\[
\leq c_1^2 2^{d_1} P(d-1)T^{d-1}.
\]
Noting that
\[
\frac{16 c_1^2}{\log 2} < 98,
\]
we continue almost exactly as in Proposition 4.10.1 and obtain the following.
Proposition 4.10.3. We have

\[
\mathcal{M}_1^{red}(d, T) \leq \begin{cases} 
98 \cdot T \log T, & \text{if } d = 2, \ T \geq 2, \ \text{and} \\
2c_1^2 4^d P(d - 1) \cdot T^{d-1}, & \text{if } d \geq 3, \ T \geq 1.
\end{cases}
\]

4.10.3 Monic polynomials with given final coefficient

Next we want to bound the number of reducible, monic, integer polynomials with fixed constant coefficient. For a nonzero integer, let \( \mathcal{M}^{red}(d, (1), (r), T) \) denote the number of reducible monic polynomials with constant coefficient \( r \), degree \( d \), and Mahler measure at most \( T \). Using (4.5), we have for all \( d \geq 0 \) and \( T > 0 \) that

\[
\mathcal{M}(d, (1), (r), T) \leq C_{1,1}(d)T^{d-1} \leq c_2 2^d P(d)T^{d-1},
\]

where \( c_2 = \frac{351}{256} \), from Lemma A.0.3 in the appendix.

Let \( \omega(r) \) denote the number of positive divisors of \( r \). We’ll assume \( d > 2 \); if \( d = 2 \), we easily have the constant bound \( \mathcal{M}^{red}(d, (1), (r), T) \leq \omega(r) + 1 \).

For a polynomial \( f \) counted by \( \mathcal{M}^{red}(d, (1), (r), T) \), there exist \( 1 \leq d_2 \leq d_1 \leq d - 1 \) such that \( f = f_1 f_2 \), where each \( f_i \) is an integer polynomial with \( \deg(f_i) = d_i \), and of course the constant coefficient of \( f \) is the product of those of \( f_1 \) and \( f_2 \). Define \( k \) as in the previous two cases. Given such a pair \( (d_1, d_2) \), summing over the \( 2\omega(r) \) possibilities for the final coefficient of \( f_1 \) there are at most \( 2\omega(r)c_2 2^{d_1-1} P(d_1)2^{k(d_1-1)} \) choices of such an \( f_1 \), and then at most \( c_2 2^{d_2-1} P(d_2)(2^{1-k}T)^{d_2-1} \) choices for \( f_2 \). The rest proceeds essentially as before, and we find that:

Proposition 4.10.4. For \( T \geq 1 \), we have

\[
\mathcal{M}^{red}(d, (1), (r), T) \leq \begin{cases} 
\omega(r) + 1, & \text{if } d = 2 \\
\frac{1}{2}\omega(r)c_2^2 4^d P(d - 1) \cdot T^{d-2}, & \text{if } d \geq 3.
\end{cases}
\]
4.10.4 Monic polynomials with a given second coefficient

For our next case, we want to bound the number of reducible, monic, integer polynomials with a given second leading coefficient. Let $\mathcal{M}^{\text{red}}(d, (1, t), (), T)$ denote the number of reducible monic polynomials of degree $d \geq 3$ (we’ll treat $d = 2$ separately at the end) with integer coefficients, second leading coefficient equal to $t$, and Mahler measure at most $T$.

**Proposition 4.10.5.** For all $t \in \mathbb{Z}$ we have

$$
\mathcal{M}^{\text{red}}(d, (1, t), (), T) \leq \begin{cases}
\frac{1}{2}\sqrt{t^2 + 4T} + 1, & \text{if } d = 2, \ T \geq 1; \\
\frac{96}{\log 2} \cdot T \log T, & \text{if } d = 3, \ T \geq 2; \text{ and} \\
d^{2d-1}P(d-1) \cdot T^{d-2}, & \text{if } d \geq 4, \ T \geq 1.
\end{cases}
$$

**Proof.** As before, we write such a polynomial as $f = f_1 f_2$, with

$$
f_1(z) = z^{d_1} + x_1 z^{d_1-1} + \cdots + x_{d_1}, \quad \text{and} \quad f_2(z) = z^{d_2} + y_1 z^{d_2-1} + \cdots + y_{d_2}.
$$

Also as before, we enforce $1 \leq d_2 \leq d_1 \leq d - 1$ to avoid double-counting, and we define $k$ as in the previous three cases. For $1 \leq i \leq d_1$ and $1 \leq j \leq d_2$, we have

$$
|x_i| \leq \binom{d_1}{i} 2^k, \quad \text{and} \quad |y_j| \leq \binom{d_2}{j} 2^{1-k} T. \tag{4.47}
$$

We also, of course, have

$$
x_1 + y_1 = t. \tag{4.48}
$$

First assume $d_1 > d_2 + 1$. Observe that the number of integer lattice points $(x_1, y_1)$ in $[-M_1, M_1] \times [-M_2, M_2]$ such that $x_1 + y_1 = t$ is at most $2 \min \{M_1, M_2\} + 1$. So the number of $(x_1, \ldots, x_{d_1}, y_1, \ldots, y_{d_2})$ satisfying (4.47) and (4.48) is at most

$$
(2 \min \{d_1 2^k, d_2 2^{1-k} T\} + 1) \prod_{j=2}^{d_1} \left(2 \binom{d_1}{j} 2^k + 1\right) \prod_{j=2}^{d_2} \left(2 \binom{d_2}{j} 2^{1-k} T + 1\right) \tag{4.49}
$$

\[
\leq (2 \min \{d_1 2^k, d_2 2^{1-k} T\} + 1) \cdot C_{2,0}(d_1) 2^{k(d_1-1)} \cdot C_{2,0}(d_2) (2^{1-k} T)^{d_2-1} \\
\leq (2d \cdot 2^{1-k} T) (2T)^{d_2-1} 2^{k(d_1-d_2)} \cdot 2^{d_1-1} P(d_1) \cdot 2^{d_2-1} P(d_2) \\
\leq d_2^{d-1} P(d-1)(2T)^{d_2} 2^{k(d_1-d_2)-1}.
\]
using Lemma A.0.3. Summing over all the possibilities $1 \leq k \leq K$, the number of possible pairs $f_1$ and $f_2$ of degrees $d_1$ and $d_2$, respectively, is at most
\[ d^{2d-1}P(d-1)(2T)^{d_2} \sum_{k=1}^{K} 2^{(d_1-d_2-1)k} \leq d^{2d-1}2^{d_2}P(d-1)T^{d_2} [2 \cdot 2^{K(d_1-d_2-1)}] \leq d^{2d-1}2^{d_1}P(d-1)T^{d-2}. \]

Now, if $d_1 = d_2 = \frac{d}{2}$ (in this case $d$ must be even), then the geometric sum above becomes $\sum_{k=1}^{K} 2^{-k} \leq 1$. So for $d \geq 4$ again we obtain the estimate (4.50) we achieved assuming $d_1 > d_2 + 1$. If $d_1 = d_2 + 1$ (so $d$ is odd), then the number of possible pairs is at most $d^{2d-1}P(d-1)(2T)^{d_2}K$, which does not exceed (4.50) for $d \geq 5$, and for $d = 3, T \geq 2$ is at most
\[ 3 \cdot 2^{3-1}P(2)(2T)^{1} \cdot \frac{2\log T}{\log 2} = \frac{96}{\log 2} \cdot T \log T, \]
which gives us the $d = 3$ case of the proposition. Finally, for $d \geq 4$ we sum over the at most $d/2$ possibilities for $(d_1, d_2)$, yielding
\[ M_{\text{red}}(d, (1, t), (), T) \leq d^{2d-1}P(d-1)T^{d-2}. \]

For the case $d = 2$, we’ll see that the error term is on the order of $\sqrt{T}$. Note that we are simply counting integers $c$ such that the polynomial
\[ f(z) = (z^2 + tz + c) = (z + x_1)(z + y_1) \]
has Mahler measure at most $T$. Since we know $|c| \leq T$, it suffices to control the size of \( \{x_1 \in \mathbb{Z} \mid |x_1(t - x_1)| \leq T\} \), which is itself bounded by the size of \( \{x_1 \in \mathbb{Z} \mid x_1^2 - tx_1 \leq T\} \).

By the quadratic formula, that last set is simply \( \{x_1 \in \mathbb{Z} \mid \frac{t - \sqrt{t^2 + 4T}}{2} \leq x_1 \leq \frac{t + \sqrt{t^2 + 4T}}{2}\} \), which has size at most $\sqrt{t^2 + 4T} + 1$. To better bound the number of $c$ of the form $x_1(t - x_1)$, note that such a $c$ can be written in this form for exactly two values of $x_1$, except for at most one value of $c$ for which $x_1$ is unique (this occurs when $t$ is even). So overall, the number of such $c$ with $|c| \leq T$ is at most $\frac{1}{2}\sqrt{t^2 + 4T} + 1$. \( \square \)
4.10.5 Monic polynomials with given second and final coefficient

For our final case, we want to bound the number of monic, reducible polynomials with a given second leading coefficient \( t \in \mathbb{Z} \) and given constant coefficient \( 0 \neq r \in \mathbb{Z} \). We can clearly assume that \( d \geq 3 \) since we’re imposing three coefficient conditions. We write \( \mathcal{M}^{\text{red}}(d, (1, t), (r), T) \) for the number of reducible monic polynomials of degree \( d \) with integer coefficients, second leading coefficient equal to \( t \), and constant coefficient equal to \( r \). We’ll show this is \( O(T^{d-3}) \) in all cases. While we don’t write an explicit bound for the error term, it should be clear from our proof that this is possible.

**Proposition 4.10.6.** For all \( d \geq 3, t \in \mathbb{Z}, \text{ and } r \in \mathbb{Z} \setminus \{0\}, \) we have

\[
\mathcal{M}^{\text{red}}(d, (1, t), (r), T) = O(T^{d-3}).
\]

**Proof.** As before, we write such a polynomial as \( f = f_1 f_2 \), with

\[
 f_1(z) = z^{d_1} + x_1 z^{d_1-1} + \cdots + x_{d_1}, \quad \text{and} \quad f_2(z) = z^{d_2} + y_1 z^{d_2-1} + \cdots + y_{d_2}.
\]

We always enforce \( 1 \leq d_2 \leq d_1 \leq d - 1 \) to avoid double-counting. We’ll consider the count in several different cases. First, if \( d_2 = 1 \), then \( f_2 = z + y_{d_2} \), so we must have \( y_{d_2} | r \) and \( y_{d_2} + x_1 = t \). Thus there are only \( 2\omega(r) \) possible choices of \( f_2 \); each choice will in turn determine \( x_{d_1} \) and \( x_1 \), so we have \( O(T^{d_1-2}) = O(T^{d-3}) \) choices of \( f_1 \) altogether, by Theorem 4.1.11. Note that this completely covers the case \( d = 3 \).

Now assume \( d_2 \geq 2 \), so \( d \geq 4 \). There are again only \( 2\omega(r) \) possible choices of \( y_{d_2} \), and each one will determine what \( x_{d_1} \) is (they must multiply to give \( r \)). Fix a choice of \( y_{d_2} \) for now.

Assume first that \( d_1 > d_2 + 1 \). Again we take \( k \) between 1 and \( K = \left\lfloor \frac{\log T}{\log 2} \right\rfloor + 1 \), and assume that \( 2^{k-1} \leq \mu(f_1) \leq 2^k \), so \( \mu(f_2) \leq 2^{1-k}T \). Almost exactly as in (4.49), we get that
CHAPTER 4. SLICING THE STARS

the number of \((x_1, \ldots, x_{d_1-1}, y_1, \ldots, y_{d_2-1})\) contributing to \(\mathcal{M}^{\text{red}}(d, (1, t), (r), T)\) is at most

\[
(2 \min\{d_1 2^k, d_2 2^{1-k} T\} + 1) \cdot \prod_{i=2}^{d_1-1} 2\left(\frac{d_1}{i}\right) 2^k + 1 \cdot \prod_{j=2}^{d_2-1} 2\left(\frac{d_2}{j}\right) (2^{1-k} T) + 1
\]

\[
\leq (2d \cdot 2^{1-k} T) \cdot 2^{k(d_1-2)} C_{2,1}(d_1) \cdot (2^{1-k} T)^{d_2-2} C_{2,1}(d_2)
\]

\[
= d^2 C_{2,1}(d_1) C_{2,1}(d_2) T^{d_2-1} 2^{(d_1-d_2-1)k}
\]

\[
\leq \frac{1}{64} d^2 2^{d_2} P(d-1) T^{d_2-1} 2^{(d_1-d_2-1)k},
\]

using Lemmas A.0.3 and A.0.4. Summing over all the possibilities \(1 \leq k \leq K\), the number of possible pairs \(f_1\) and \(f_2\) of degrees \(d_1\) and \(d_2\), respectively, is at most

\[
\frac{1}{64} d^2 2^{d_2} P(d-1) T^{d_2-1} \sum_{k=1}^{K} 2^{(d_1-d_2-1)k} \leq \frac{1}{32} d^2 2^{d_2} P(d-1) T^{d_1-2} \leq \frac{1}{32} d^2 2^{d_2} P(d-1) T^{d-3},
\]

(4.51)

which is certainly \(O(T^{d-3})\).

Next, if \(d_1 = d_2 = \frac{d}{2}\) (in this case \(d\) must be even), then the expression in (4.51), which contains a partial geometric sum that’s bounded by 1, is at most

\[
\frac{1}{64} d^2 2^{d_2} P(d-1) T^{d_2-2},
\]

which is certainly \(O(T^{d-3})\) since \(d \geq 4\). Lastly, if \(d_1 = d_2 + 1\), (so \(d \geq 5\)), then \(d_2 \leq d - 3\), and (using \(K \leq 2T\)) the expression in (4.51) is at most

\[
\frac{1}{64} d^2 2^{d_2} P(d-1) T^{d_2-1} K \leq \frac{1}{32} d^2 2^{d_2} P(d-1) T^{d_2} \leq \frac{1}{32} d^2 2^{d_2} P(d-1) T^{d-3},
\]

which is \(O(T^{d-3})\). Finally, we sum over the \(2\omega(r)\) possibilities for \(y_{d_2}\) and the at most \(d/2\) possibilities for \((d_1, d_2)\) and obtain overall that \(\mathcal{M}^{\text{red}}(d, (1, t), (r), T) = O(T^{d-3})\).

\[\square\]

4.11 Explicit results

Let \(N(\overline{\mathbb{Q}}_d, H)\) denote the number of algebraic numbers of degree \(d\) over \(\overline{\mathbb{Q}}\) and height at most \(H\). We give an explicit version of Masser and Vaaler’s main theorem of [MV08], which follows from Theorem 4.7.1, our explicit version of [CV01, Theorem 3].
**Theorem 4.11.1.** For all \( d \geq 2 \) and \( \mathcal{H} \geq 1 \), we have
\[
\left| N(\mathbb{Q}_d, \mathcal{H}) - \frac{d V_d}{2\zeta(d+1)} \mathcal{H}^{d(d+1)} \right| \leq \begin{cases} 
16690 \cdot \mathcal{H}^4 \log \mathcal{H}, & \text{if } d = 2 \text{ and } \mathcal{H} \geq \sqrt{2} \\
3.37 \cdot (15.01)^d \cdot \mathcal{H}^d, & \text{if } d \geq 3 \text{ and } \mathcal{H} \geq 1.
\end{cases}
\]

**Proof.** We combine Proposition 4.10.1 and Theorem 4.10.2 to estimate the number of irreducible, primitive (i.e. having relatively prime coefficients) polynomials of degree \( d \) and Mahler measure at most \( \mathcal{H}^d \), and relatively prime coefficients; we write \( \mathcal{M}^{\text{irr, prim}}(d, \mathcal{H}^d) \) for this number. Each pair of such a polynomial and its opposite corresponds to \( d \) algebraic numbers of degree \( d \) and height at most \( \mathcal{H} \) (the roots). So we have
\[
N(\mathbb{Q}_d, \mathcal{H}) = \frac{d}{2} \mathcal{M}^{\text{irr, prim}}(d, \mathcal{H}^d),
\]
and
\[
\left| N(\mathbb{Q}_d, \mathcal{H}) - \frac{d V_d}{2\zeta(d+1)} \mathcal{H}^{d(d+1)} \right| \leq \left| \frac{d}{2} \mathcal{M}^{\text{irr, prim}}(d, \mathcal{H}^d) - \frac{d \mathcal{M}^1(d, \mathcal{H}^d)}{2\zeta(d+1)} \mathcal{H}^{d^{d+1}} \right| + \left| \frac{d}{2} \mathcal{M}^1(d, \mathcal{H}^d) - \frac{d V_d}{2\zeta(d+1)} \mathcal{H}^{d(d+1)} \right|,
\]
and it follows from Proposition 4.10.1 and Theorem 4.10.2 that
\[
(d/2)^{-1} \left| N(\mathbb{Q}_d, \mathcal{H}) - \frac{d V_d}{2\zeta(d+1)} \mathcal{H}^{d(d+1)} \right| \leq \left( \frac{V_d}{d} + 1 \right) \mathcal{H}^d + \left( C_{1,0}(d - 1) + \zeta(d) \kappa_0(d) \mathcal{H}^{d^2} \right)
\]
\[
+ \begin{cases} 
1758 \mathcal{H}^4 \log(\mathcal{H}^2), & \text{if } d = 2 \text{ and } \mathcal{H}^2 \geq 2 \\
16 \kappa_0^2 \mathcal{H}^{2d} P(d - 1) \mathcal{H}^{d^2}, & \text{if } d \geq 3 \text{ and } \mathcal{H}^2 \geq 1.
\end{cases}
\]

Here \( \kappa_0(d) \) is the constant from Theorem 4.7.1, and \( c_0 = 3159/1024 \). The \( d = 2 \) case of our Theorem follows immediately, as
\[
\left( \frac{V_2}{2} + 1 \right) + C_{1,0}(1) + \zeta(2) \kappa_0(2) + 2 \cdot 1758 = \left( \frac{8}{2} + 1 \right) + 8000 \zeta(2) + 9 + 3516 < 16690.
\]

We now turn to \( d \geq 3 \), where we have
\[
\left| N(\mathbb{Q}_d, \mathcal{H}) - \frac{d V_d}{2\zeta(d+1)} \mathcal{H}^{d(d+1)} \right| \leq \theta_0(d) \cdot \mathcal{H}^{d^2}
\]
with
\[ \theta_0(d) = \frac{d}{2} \left( 1 + V_d/d + \zeta(d)\kappa_0(d) + C_{0,0}(d - 1) + 16c_2^24^dP(d - 1) \right) \]
\[ = \left[ \zeta(d) + \frac{1}{\kappa_0(d)} + \frac{V_d}{d\kappa_0(d)} + \frac{C_{0,0}(d - 1)}{\kappa_0(d)} + \frac{16c_2^24^dP(d - 1)}{\kappa_0(d)} \right] \frac{d\kappa_0(d)}{2}. \]

Note that the quantity in brackets above decreases for \( d \geq 3 \) (for this it may be helpful to consult Lemma 4.2.2 and compute a few values of \( V_d \)) so is no more than
\[ \lambda_0 := \zeta(3) + \frac{1}{\kappa_0(3)} + \frac{V_3}{3\kappa_0(3)} + \frac{C_{0,0}(2)}{\kappa_0(3)} + \frac{16c_2^24^3P(2)}{\kappa_0(3)}. \]

So, using the notation of the end of the proof of Theorem 4.7.1, we have
\[
\left| N(\mathcal{O}_d, \mathcal{H}) - \frac{dV_d}{2\zeta(d+1)} \mathcal{H}^{d+1} \right| \leq \theta_0(d) \cdot \mathcal{H}^{d^2} \leq \lambda_0 \frac{d\kappa_0(d)}{2} \cdot \mathcal{H}^{d^2} \leq \frac{\lambda_0}{2ad^{3/4}b^d c^{d^2}} \cdot \mathcal{H}^{d^2} \\
\leq \frac{\alpha_0}{2} (bc)^d \cdot \mathcal{H}^{d^2} \leq 3.37 \cdot (15.01)^d \cdot \mathcal{H}^{d^2}. \]

Next, we record an explicit version of [Bar14, Theorem 1.1] in the case \( k = \mathbb{Q} \), i.e., an explicit estimate for the number of algebraic integers of bounded height and given degree over \( \mathbb{Q} \). This explicit estimate follows from our Theorem 4.8.1, which improved the power savings of [CV01, Theorem 6]. We write \( N(\mathcal{O}_d, \mathcal{H}) \) for the number of algebraic integers of degree \( d \) over \( \mathbb{Q} \) and height at most \( \mathcal{H} \).

**Theorem 4.11.2.** We have
\[
\left| N(\mathcal{O}_d, \mathcal{H}) - d \cdot p_d(\mathcal{H}^d) \right| \leq \begin{cases} 
584 \cdot \mathcal{H}^2 \log \mathcal{H}, & \text{if } d = 2 \text{ and } \mathcal{H} \geq \sqrt{2} \\
1.13 \cdot 4^d d^d 2^d \cdot \mathcal{H}^{d(d-1)}, & \text{if } d \geq 3 \text{ and } \mathcal{H} \geq 1.
\end{cases}
\]

**Proof.** We follow the idea of the previous proof. Now that we require polynomials to be monic, we never count two irreducible polynomials with the same set of roots, and so combining Theorem 4.8.1 and Proposition 4.10.3 we obtain:
\[
d^{-1} \left| N(\mathcal{O}_d, \mathcal{H}) - d \cdot p_d(\mathcal{H}^d) \right| \leq \kappa_1(d) \mathcal{H}^{d(d-1)} + \begin{cases} 
98\mathcal{H}^2 \log(\mathcal{H}^2), & \text{if } d = 2, \mathcal{H}^2 \geq 2 \\
2c_1^24^dP(d-1)\mathcal{H}^{d(d-1)}, & \text{if } d \geq 3, \mathcal{H}^2 \geq 1.
\end{cases}
\]
where $c_1 = 1053/512$. We immediately have the $d = 2$ case of our theorem, as $\kappa_1(2) = 96$. Assuming $d \geq 3$, we have

$$
\left| N(O_d, \mathcal{H}) - d \cdot p_d(\mathcal{H}^d) \right| \leq \theta_1(d) \cdot \mathcal{H}^{d(d-1)},
$$

where

$$
\theta_1(d) = d\kappa_1(d) + 2c_1^2d4^dP(d - 1).
$$

The quantity in brackets decreases for $d \geq 3$, and so is no more than

$$
\lambda_1 := 1 + \frac{2c_1^24^3P(2)}{\kappa_1(3)} \leq 1.13,
$$

and the result follows from the estimate for $\kappa_1(d)$ stated in Theorem 4.8.1.

We can also prove an explicit version of our Corollary 4.1.3, albeit with worse power savings.

**Theorem 4.11.3.** For each $d \geq 2$, $\nu$ a nonzero integer, and $\mathcal{H} \geq d \cdot 2^{d+1/\nu}|\nu|^{1/d}$, we have

$$
|N_{Nm=\nu}(d, \mathcal{H}) - dV_{d-2} \cdot \mathcal{H}^{d(d-1)}| \leq \begin{cases} 
64\sqrt{2|\nu|} + 8 \cdot \mathcal{H} + 2\omega(\nu) + 2, & \text{if } d = 2 \\
0.0000063|\nu|\omega(\nu) \cdot d^34^d(15.01)^{d^2} \cdot \mathcal{H}^{d(d-1)-1}, & \text{if } d \geq 3,
\end{cases}
$$

where $\omega(\nu)$ is the number of positive integer divisors of $\nu$.

**Proof.** Our proof proceeds very similarly to the last two. Let $r = (-1)^d\nu$. Using Theorem 4.9.3 and Proposition 4.10.4, we have for all $\mathcal{H} \geq d \cdot 2^{d+1/\nu}|\nu|^{1/d}$:

$$
d^{-1}|N_{Nm=\nu}(d, \mathcal{H}) - d \cdot V_{d-2} \cdot \mathcal{H}^{d(d-1)}| \leq \begin{cases} 
\omega(r) + 1, & \text{if } d = 2 \\
\frac{1}{2}\omega(r)c_2^24^dP(d - 1) \cdot \mathcal{H}^{d(d-2)}, & \text{if } d \geq 3,
\end{cases}
$$
where \( \kappa(d, (1), (r)) \) is as defined in Theorem 4.9.3, and \( c_2 = \frac{351}{256} \). Consider the case \( d = 2 \). By definition (stated in Theorem 4.9.3) we have

\[
\kappa(2, (1), (r)) = (0 + 1)2^{0+1} \left[ 2^4 \cdot 2^2(1 + 1)|r| \right]^{1/2} V_0 + (0 + 1) \kappa_0(0) = 32\sqrt{2|r|} + 4,
\]

using \( V_0 = 2 \) and \( \kappa_0(0) = 4 \). Therefore

\[
|N_{N_m=\nu}(2H) - 2 \cdot V_0 \cdot H^2| \leq 2 \left( (32\sqrt{2|r|} + 4)H + \omega(r) + 1 \right) = \left( 64\sqrt{2|r|} + 8 \right) \cdot H + 2\omega(r) + 2.
\]

Now we assume \( d \geq 3 \), and we have

\[
|N_{N_m=\nu}(d, H) - d \cdot V_{d-2} \cdot H^{d-2}| \leq \theta_2(d, r)H^{d-2-d},
\]

where, using (4.36) and letting \( a, b, \) and \( c \) be as in the end of the proof of Theorem 4.7.1, we have

\[
\theta_2(d, r) = d \left( \kappa(d, (1), (r)) + \frac{1}{2} \omega(r)c_2^24^dP(d - 1) \right)
\]

\[
\leq d \cdot (2 + a)d(d - 1)2^{2d-1+1/d}|r|(bc)^{(d-1)^2} + \frac{d}{2} \omega(r)c_2^24^dP(d - 1)
\]

\[
\leq d^32^{2d-1}|r|\omega(r)(bc)^{d^2} \left[ \frac{(2 + a)d(d - 1)2^{1/d}}{(bc)^{2d-1}\omega(r)d^2} + \frac{c_2^2P(d - 1)}{d^2(bc)^{d^2}|r|} \right]
\]

\[
\leq d^32^{2d-1}|r|\omega(r)(bc)^{d^2} \left[ \frac{(2 + a)2^{1/d}}{(bc)^{2d-1}} + \frac{c_2^2P(d - 1)}{d^2(bc)^{d^2}} \right].
\]

As the quantity in brackets just above decreases for \( d \geq 3 \), it does not exceed

\[
\frac{(2 + a)2^{1/3}}{(bc)^5} + \frac{c_2^2P(2)}{3^2(bc)^9} \leq 0.0000126,
\]

completing our proof.

We can immediately state the following explicit unit count, since counting units amounts to counting algebraic integers of norm \( \pm 1 \).
Theorem 4.11.4. For each $d \geq 2$ and $H \geq d \cdot 2^{d+1/d}$, we have

$$\left| N(\mathcal{O}^*, \mathcal{H}) - 2dV_{d-2} \cdot \mathcal{H}^{d(d-1)} \right| \leq \begin{cases} 
(128\sqrt{10}) \mathcal{H} + 8, & \text{if } d = 2 \\
0.000126 \cdot d^34^d(15.01)^d \cdot \mathcal{H}^{d(d-1)-1}, & \text{if } d \geq 3.
\end{cases}$$

Finally, since Proposition 4.10.5 gives an explicit bound, it is also possible to obtain an explicit estimate for $N_{\mathcal{T}^*(d, \mathcal{H})}$ similar to that of Theorem 4.11.4; we leave this to the interested reader.
Appendix A

Combinatorial estimates

This appendix contains estimates for the combinatorial functions appearing in some of the constants in Chapter 4. For any integer \(d \geq 0\), define

\[
P(d) := \prod_{j=0}^{d} \binom{d}{j};
\]

\[
C_{m,n}(d) := \prod_{j=m}^{d-n} \left( 2 \binom{d}{j} + 1 \right), \text{ for } 0 \leq m + n \leq d;
\]

\[
A(d) := \sum_{k=0}^{d} P(k)P(d - k), \text{ and }
\]

\[
B(d) := \sum_{k=0}^{d-1} P(k)P(d - k)\gamma(k)^{d-k-1}\gamma(d - k)^{k}.
\]

where \(\gamma(k) := \left( \frac{k}{\lfloor k/2 \rfloor} \right)\).

Stirling’s inequality is the following estimate for factorials, which we will use several times:

\[
\sqrt{2\pi} \cdot k^{k+\frac{1}{2}}e^{-k} \leq k! \leq e \cdot k^{k+\frac{1}{2}}e^{-k}, \forall k \geq 1.
\]  

(A.1)

Using this we can easily see that

\[
\gamma(k) \leq \frac{e \cdot 2^k}{\pi \sqrt{k}}.
\]  

(A.2)

Lemma A.0.1. For all \(d \geq 1\) we have

\[
A(d) \leq \left( 10\sqrt{2\pi}^{3/4}e^{-3} \right) e^{\frac{1}{2}d^2+d(2\pi)^{-d/2}d^{-\frac{1}{2}d-\frac{1}{4}}}. 
\]

101
Proof. We write
\[
\Phi(d) := \sqrt{\frac{e^{d^2+d}}{(2\pi)^dd!}}.
\]
Note that of course the first and last factor appearing in the product \(P(d)\) are 1, so they may be omitted when convenient. Also notice that
\[
P(d) = \prod_{k=1}^{d} \frac{k^k}{k!}.
\]
Using Stirling’s inequality we have
\[
P(d) = \prod_{j=1}^{d} \frac{j^j}{j!} \leq \prod_{j=1}^{d} \frac{e^j}{\sqrt{2\pi j}} = \frac{\exp\left(\frac{1}{2}(d^2+d)\right)}{\sqrt{2\pi d^d d!}} = \frac{e^{d^2+d}}{(2\pi)^dd!}.
\]
We therefore have
\[
P(d) \leq \Phi(d), \ \forall d \geq 0. \quad (A.4)
\]
Now, for all \(d \geq 1\), we have
\[
A(d) = \sum_{k=0}^{d} P(k)P(d-k) \leq \sum_{k=0}^{d} \Phi(k)\Phi(d-k)
\]
\[
= \sum_{k=0}^{d} \sqrt{\frac{e^{k^2+k}}{(2\pi)^kk!}} \sqrt{\frac{e^{(d-k)^2+d-k}}{(2\pi)^{d-k}(d-k)!}}
\]
\[
= \Phi(d) \sum_{k=0}^{d} \sqrt{\left(\frac{d}{k}\right)e^{k^2-dk}} = \Phi(d) \left(2 + \sum_{k=1}^{d-1} \sqrt{\left(\frac{d}{k}\right)e^{k^2-dk}}\right). \quad (A.5)
\]
Now, since \(k^2 - dk = -k(d-k) \leq -(d-1)\) when \(1 \leq k \leq d-1\), we can easily estimate the sum
\[
\sum_{k=1}^{d-1} \sqrt{\left(\frac{d}{k}\right)e^{k^2-dk}} \leq 2^d \cdot e^{1-d} = e \cdot (2/e)^d. \quad (A.6)
\]
The interested reader will easily verify that
\[
\frac{A(d)}{\Phi(d)} \leq \frac{A(2)}{\Phi(2)} = 10\pi \sqrt{2}e^{-3} \approx 2.21198 \quad (A.7)
\]
for $0 \leq d \leq 8$, and by (A.5) and (A.6), we can easily check that

$$\frac{A(d)}{\Phi(d)} \leq 2 + e \cdot (2/e)^d < 2.2$$

for $d \geq 9$.

Finally, we estimate $\Phi(d)$ using Stirling’s inequality again:

$$\Phi(d) \leq \sqrt{\frac{e^{d^2+d}}{(2\pi)^d}} \cdot \frac{e^d}{\sqrt{2\pi d} \cdot d^d} = e^{\frac{1}{2}d^2+d}(2\pi d)^{-\frac{1}{2}d-\frac{1}{4}}. \quad (A.8)$$

Combining with (A.7) completes the proof. \hfill \Box

**Lemma A.0.2.** For all $d \geq 0$ we have

$$B(d) \leq 2^d.$$

**Proof.** We can readily verify the inequality for $d \leq 3$, so we’ll assume below that $d \geq 4$, and proceed by induction. Suppose that $B(d-1) \leq 2^{(d-1)^2}$. Notice that

$$P(d) = \frac{d^d}{d!} P(d-1), \quad (A.9)$$

and also that $\gamma(d) \leq 2\gamma(d-1)$ for all $d \geq 1$. We also easily have $P(d) \leq e^{\frac{1}{2}d^2+d}$ from the previous proof. Using these facts, we have

$$B(d) = P(d-1) + \sum_{k=0}^{d-2} P(k) P(d-k) \gamma(k)^{d-k-1} \gamma(d-k)^k$$

$$\leq P(d-1) + \sum_{k=0}^{d-2} P(k) \frac{(d-k)^{d-k}}{(d-k)!} P(d-k-1) \gamma(k)^{d-k-2} \gamma(d-k)^2 \gamma(d-k-1)^k$$

$$\leq P(d-1) + \sum_{k=0}^{d-2} \left[ \frac{e^{d-k} 2^{k}}{\sqrt{2\pi (d-k)}} \gamma(k+1) \right] P(k) P(d-k-1) \gamma(k)^{d-k-2} \gamma(d-k-1)^k$$

$$\leq P(d-1) + \sum_{k=0}^{d-2} \left[ \frac{e^{d-k} 2^{k}}{\sqrt{2\pi (d-k)}} e \cdot 2^{k+1} \right] P(k) P(d-k-1) \gamma(k)^{d-k-2} \gamma(d-k-1)^k$$

$$\leq P(d-1) + \sum_{k=0}^{d-2} \left[ \frac{\sqrt{2}}{\pi^{3/2}} \cdot \frac{e^d (4/e)^k}{\sqrt{(d-k)(k+1)}} \right] P(k) P(d-k-1) \gamma(k)^{d-k-2} \gamma(d-k-1)^k.$$
We note that \((d - k)(k + 1) \geq d\) for \(0 \leq k \leq d - 2\), and continue:

\[
B(d) \leq P(d - 1) + \left[ \frac{e \sqrt{2}}{\pi^{3/2}} \cdot \frac{e^{d}(4/e)^{d}}{\sqrt{d}} \right] \sum_{k=0}^{d-2} P(k)P(d - 1 - k)\gamma(k)\gamma(d - 1 - k)^{k}
\]

\[
= P(d - 1) + \left[ \frac{e \sqrt{2}}{\pi^{3/2}} \cdot \frac{4^{d}}{\sqrt{d}} \right] B(d - 1) \leq P(d - 1) + \left[ \frac{e \sqrt{2}}{\pi^{3/2}} \cdot \frac{4^{d}}{\sqrt{d}} \right] 2^{(d-1)^2}
\]

\[
= P(d - 1) + \left[ \frac{e \sqrt{2}}{\pi^{3/2}} \cdot \frac{4^{d}}{\sqrt{d}} \right] \frac{2}{4^{d}} 2^{d^2} = P(d - 1) + \left[ \frac{e \cdot 2^{3/2}}{\pi^{3/2} \sqrt{d}} \right] 2^{d^2}
\]

\[
= \left[ \frac{P(d) d!}{d^{d} 2^{d^2} \sqrt{d}} + \frac{e \cdot 2^{3/2}}{\pi^{3/2} \sqrt{d}} \right] 2^{d^2} \leq \left[ \frac{e^{d} d^{d+1} \cdot e \sqrt{d}}{e^{d} 2^{d^2}} + \frac{e \cdot 2^{3/2}}{\pi^{3/2} \sqrt{d}} \right] 2^{d^2}
\]

\[
= \left[ e \sqrt{d} \left( \frac{\sqrt{e}}{2} \right)^{d} + \frac{e \cdot 2^{3/2}}{\pi^{3/2} \sqrt{d}} \right] 2^{d^2} \leq 2^{d^2} \text{ for } d \geq 4.
\]

\[\square\]

**Lemma A.0.3.** We have

\[
C_{0,0}(d) \leq \frac{3159}{1024} \cdot 2^{d+1} P(d), \; \forall \; d \geq 0; \tag{A.10}
\]

\[
C_{1,0}(d) \leq \frac{1053}{512} \cdot 2^{d} P(d), \; \forall \; d \geq 0;
\]

\[
C_{1,1}(d) \leq \frac{351}{256} \cdot 2^{d-1} P(d), \; \forall \; d \geq 1;
\]

\[
C_{2,0}(d) \leq 2^{d-1} P(d), \; \forall \; d \geq 1; \text{ and}
\]

\[
C_{2,1}(d) \leq \frac{1}{2} \cdot 2^{d-2} P(d), \; \forall \; d \geq 2.
\]

**Proof.** We’ll prove the bound for \(C_{0,0}(d)\), and leave the other cases as exercises. The inequality (A.10) is easily verified for \(d \leq 3\), and we have equality for \(d = 4\). If we set

\[
R(d) := \frac{C_{0,0}(d)}{2^{d+1} P(d)} = \prod_{j=0}^{d} \frac{2^{d-j} + 1}{2^{d-j}},
\]

then to establish (A.10) it will suffice to show that

\[
\frac{R(d + 1)}{R(d)} \leq 1, \; \text{for } d \geq 4.
\]
We’ll use the standard identity
\[
\binom{d+1}{j} = \frac{d+1}{d+1-j} \binom{d}{j}.
\]

We have
\[
\frac{R(d+1)}{R(d)} = \frac{\prod_{j=0}^{d+1} \frac{2(d+1)_j}{2d_j+1}}{\prod_{j=0}^{d} \frac{2d_j+1}{2d_j+1}} = \frac{3}{2} \prod_{j=0}^{d} \frac{d_j}{2d_j+1} \cdot \frac{2(d+1)_j+1}{2d_j+1} = \frac{3}{2} \prod_{j=0}^{d} \frac{2d_j+1}{2d_j+1}
\]
\[
= \frac{3}{2} \prod_{j=0}^{d} \left[ 1 - \frac{j}{(d+1)(2d_j+1)} \right]
\]
\[
\leq \frac{3}{2} \prod_{j=d-2}^{d} \left[ 1 - \frac{j}{(d+1)(2d_j+1)} \right]
\]
\[
= \frac{3}{2} \cdot \frac{4d^6 + 10d^5 + 6d^4 + 8d^3 + 20d^2 + 24d + 18}{2d^6 + 5d^5 + 3d^4 + 4d^3 + 10d^2 + 12d + 9} \cdot \frac{2d^6 + 5d^5 + 4d^4 + 3d^3 + 5d^2 + 4d + 1}{2d^6 + 5d^5 + 4d^4 + 3d^3 + 5d^2 + 4d + 1} \leq 1, \text{ for } d \geq 4.
\]

\[\square\]

**Lemma A.0.4.** If \(d \geq 2\) and \(1 \leq k \leq d-1\), then
\[
P(k)P(d-k) \leq P(d-1).
\]

**Proof.** We have
\[
P(k)P(d-k) = \prod_{j=0}^{k-1} \binom{k}{j} \prod_{i=0}^{d-k-1} \binom{d-k-1}{i} \leq \prod_{j=0}^{k-1} \binom{d-1}{j} \prod_{i=0}^{d-1} \binom{d-1}{i}
\]
\[
= \prod_{j=0}^{k-1} \binom{d-1}{j} \prod_{i=0}^{d-1} \binom{d-1}{i} = \prod_{j=0}^{k-1} \binom{d-1}{j} \prod_{j=k}^{d-1} \binom{d-1}{j} = P(d-1).
\]
We have equality if and only if \(k = 1\) or \(k = d-1\). \[\square\]
Bibliography


BIBLIOGRAPHY


BIBLIOGRAPHY


[Tho15] Jack Thorne, *On the average number of 2-Selmer elements of elliptic curves over \( \mathbb{F}_q(X) \) with two marked points*, 2015, arXiv pre-print.


