Approximation Constants for Closed Subschemes of Projective Varieties

by

Nickolas Rollick

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

Waterloo, Ontario, Canada, 2019

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

Dr. David McKinnon (Supervisor)
Dr. Dragos Ghioca (External Examiner)
Dr. Matthew Satriano (Internal Member)
Dr. Jerry Xiao Heng Wang (Internal Member)
Dr. David Jao (Internal-External Member)

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

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

Abstract

Diophantine approximation is a branch of number theory with a long history, going back at least to the work of Dirichlet and Liouville in the 1840s. The innocent-looking question of how well an arbitrary real algebraic number can be approximated by rational numbers (relative to the size of the denominator of the approximating rational number) took more than 100 years to resolve, culminating in the definitive Fields Medal-winning work of Klaus Roth in 1955.

Much more recently, David McKinnon and Mike Roth have re-phrased and generalized this Diophantine approximation question to apply in the setting of approximating algebraic points on projective varieties defined over number fields. To do this, they defined an "approximation constant", depending on the point one wishes to approximate and a given line bundle. This constant measures the tradeoff between the closeness of the approximation and the arithmetic complexity of the point used to make the approximation, as measured by a height function associated to the line bundle.

In particular, McKinnon and Roth succeeded in proving lower bounds on the approximation constant in terms of the "Seshadri constant" associated to the given point and line bundle, measuring local positivity of the line bundle around the point. Appropriately interpreted, these results generalize the classical work of Liouville and Roth, and the corresponding McKinnon-Roth theorems are therefore labelled "Liouville-type" and "Roth-type" results.

Recent work of Grieve and of Ru-Wang have taken the Roth-type theorems even further; in contrast, we explore results of Liouville-type, which are more elementary in nature. In Chapter 2, we lay the groundwork necessary to define the approximation constant at a point, before generalizing the McKinnon-Roth definition to approximations of arbitrary closed subschemes. We also introduce the notion of an essential approximation constant, which ignores unusually good approximations along proper Zariski-closed subsets. After verifying that our new approximation constant truly does generalize the constant of McKinnon-Roth, Chapter 3 establishes a fundamental lower bound on the approximation constants of closed subschemes of projective space, depending only on the equations cutting out the subscheme.

In Chapter 4, we provide a series of explicit computations of approximation constants, both for subschemes satisfying suitable geometric conditions, and for curves of low degree in projective 3-space. We will encounter difficulties computing the approximation constant exactly for general cubic curves, and we spend some time showing why some of the more evident approaches do not succeed. To conclude the chapter, we take up the question of large gaps between the ordinary and essential approximation constants, by considering approximations to a certain rational point on a diagonal quartic surface. Finally, in Chapter 5, we generalize the Liouville-type results of McKinnon-Roth.

Acknowledgements

Of course, the lion's share of the credit goes to my advisor, David McKinnon. In those occasional moments where I doubted my abilities, you were always there to remind me just how far I had really come. I deeply appreciate your support of my career aspirations and all the advice you have provided. You always left me plenty of space to explore the mathematical unknown, and yet you were never far away if I needed some guidance.

Next, I would like to thank the amazing group of graduate students in the Pure Mathematics department. The kindness and warmth you all showed me created an environment in which I could grow and thrive. The conversations we shared (often over lunch, dinner, or a hot beverage) helped keep me grounded and focused during the marathon known as graduate school. The friendly atmosphere was what attracted me to Waterloo in the first place, but I could never have realized how crucial those social connections would be for my overall wellbeing as a graduate student. In particular, I want to thank Bahaa Khaddaj, my office mate during the first year of my PhD. Not only was it a blast doing coursework with you, but you provided support and advice at a crucial time, when I was seriously questioning what my future might hold. It was a sad day when you moved back to Ottawa, but I know our friendship will stand the test of time.

Dedication

This thesis is dedicated to my parents, Joyce Rollick and Donald Rollick, and to my brother, Alex Rollick. None of you ever doubted that I could achieve whatever I set my mind to, and you have always been my biggest cheerleaders. For all the conversations we shared, all the advice you have provided, and all the loving support you have extended: this thesis is for you.

Table of Contents

Chapter 1

Introduction

1.1 Classical Diophantine Approximation

Diophantine approximation, in its simplest form, is the branch of mathematics concerned with approximating real numbers by rational numbers. In particular, we seek to measure the trade-off between the closeness of the approximation and the "complexity" of the rational number used to make the approximation. In this case, the complexity of a rational number is captured by the size of its denominator.

Intuitively, for a fixed real number x, the closer a rational number approximates x (in terms of the usual absolute value), the larger its denominator must grow. This follows because there are only finitely many rational numbers within bounded distance of x and with bounded denominator. We would like to measure the growth in the size of the denominator as the approximations get closer to x.

More precisely, given a real number x, we want to find the smallest exponent $\tau_x > 0$ such that for every $\delta > 0$, the inequality

$$\left|\frac{p}{q} - x\right| \leq \frac{1}{q^{\tau_x+\delta}}$$

has only finitely many solutions in rational numbers p/q. Given the existence of such a number τ_x, it follows that for every exponent $e < \tau_x$, there are infinitely many rational numbers p/q satisfying

$$\left|\frac{p}{q} - x\right| \leq \frac{1}{q^{e}},$$

which means we can find a sequence of such rational approximations converging to x. The bigger we are allowed to take e, the "better" the approximations become. This motivates us to try computing τ_x for a given real number x.

The simplest case is when x itself is rational. In that case, we may write $x = \frac{r}{s}$ for some choice of relatively prime integers r and s (with $s > 0$). Firstly, it is easy to see that there are infinitely many rational numbers p/q such that

$$\left|\frac{p}{q} - \frac{r}{s}\right| \leq \frac{1}{q}. \tag{1.1}$$

Indeed, clearing denominators, the inequality is equivalent to $|ps - rq| \leq s$, and so it is enough to arrange that $|ps - rq| = 1$. Since $\gcd(r, s) = 1$, the linear Diophantine equation $ps - rq = 1$ has infinitely many integer solutions (p, q), all of which necessarily satisfy $\gcd(p, q) = 1$, hence induce distinct rational numbers p/q.

Moreover, for any $\delta > 0$, there are only finitely many rational numbers p/q such that

$$\left|\frac{p}{q} - \frac{r}{s}\right| \leq \frac{1}{q^{1+\delta}}. \tag{1.2}$$

Indeed, multiplying both sides by sq, the inequality is equivalent to

$$|ps - rq| \leq \frac{s}{q^{\delta}}.$$

If $q^{\delta} > s$, the only integer solutions to the inequality occur when $ps - rq = 0$, i.e. $\frac{p}{q} = \frac{r}{s}$. Hence all solutions to inequality (1.2) have bounded denominator q. For any fixed q, there are clearly finitely many choices for p making the inequality true, establishing that (1.2) indeed has finitely many rational solutions.

This elementary argument shows that $\tau_x = 1$ when x is a rational number. When x is irrational, the first breakthrough dates back to 1842, when Dirichlet showed that for every irrational real number x, there are infinitely many rational solutions p/q to

$$\left|\frac{p}{q} - x\right| \leq \frac{1}{q^2}. \tag{1.3}$$

As a consequence, one deduces that $\tau_x \geq 2$ for all $x \in \mathbb{R} \setminus \mathbb{Q}$. Dirichlet's theorem can be deduced via a pigeonhole principle argument (see [9], §D.1). Alternatively, the theorem follows from the theory of continued fractions, since it is well-known that every convergent in the continued fraction expansion of x satisfies inequality (1.3).

This lower bound on τ_x was quickly complemented by an elementary upper bound, at least in the case where x is an algebraic number. In 1844, Liouville showed that if x is algebraic of degree $d \geq 2$ over $\mathbb{Q}$, then $\tau_x \leq d$, i.e. for every $\delta > 0$, there are finitely many rational solutions p/q to

$$\left|\frac{p}{q} - x\right| \leq \frac{1}{q^{d+\delta}}. \tag{1.4}$$

In outline, Liouville's argument proceeds by taking a rational solution to (1.4) and showing that q must be bounded above. To do this, one takes the integer minimal polynomial for x, say $f(X) \in \mathbb{Z}[X]$, and uses the Taylor expansion of $f(X)$ around the point x to show that if q is sufficiently large and p/q satisfies (1.4), then $f(p/q) = 0$. Since f is irreducible over $\mathbb{Q}$ of degree at least 2, this produces a contradiction. For more details, see [9], §D.1.

For real quadratic x, the theorems of Dirichlet and Liouville combine to say that $\tau_x = 2$. The next natural question to ask is: for general algebraic numbers, is it possible to narrow the gap between Liouville's upper bound on τ_x and Dirichlet's lower bound? The investigation of this question led to a series of gradual improvements on Liouville's theorem throughout the first half of the 20th century.

In 1909, Thue took the first step, showing that $\tau_x \leq \frac{1}{2}d+1$ when x is algebraic of degree d. This was refined by Siegel in 1921 ($\tau_x \leq 2\sqrt{d}$), by Gelfand and Dyson independently in 1947 ($\tau_x \leq \sqrt{2d}$), and culminated in the celebrated 1955 theorem of Klaus Roth:

Theorem 1.1.1 (Roth's Theorem, [16])**.** *For every irrational algebraic number x and every $\delta > 0$, there are finitely many rational solutions p/q to*

$$\left|\frac{p}{q} - x\right| \leq \frac{1}{q^{2+\delta}}.$$

In other words, if x is real algebraic of degree at least 2, then $\tau_x \leq 2$.

Hence Roth's theorem and Dirichlet's theorem combine to show that $\tau_x = 2$ for all real, algebraic, irrational numbers x. Roth earned the Fields Medal for his work on this theorem, completing a century-long quest to answer this innocuous-looking approximation question (at least for algebraic numbers x). Roth's theorem also holds for approximation with respect to the non-archimedean absolute values on $\mathbb{Q}$, and a version of the theorem remains true when the approximations are chosen from a more general number field. However, these generalizations fit more naturally into the "geometric" context described in the next section, and so we will immediately jump ahead to these more recent developments.

1.2 Modern Diophantine Approximation

The classical approximation problem discussed in the previous section can be phrased in a more geometric context, by considering both x and its rational approximations to be points on the projective line. In the setting encompassed by Roth's theorem, we treat the algebraic number x as the point $(x : 1) \in \mathbb{P}^1(\overline{\mathbb{Q}})$, and the rational approximations p/q can be treated as points $(p/q : 1) = (p : q) \in \mathbb{P}^1(\mathbb{Q})$.

In such a setting, we are interested in the trade-off between the distance from the point $(x : 1)$ to its approximations and the "complexity" of the approximating projective point $(p : q)$. This requires us to define a distance function $d_v(\cdot, \cdot)$ between projective points, dependent on some place v of the rational numbers. As for the "complexity" of a point, there is a well-studied theory of *height functions* on projective varieties, which are commonly used to measure this kind of complexity. Indeed, for every linear equivalence class of divisors (alternatively, every line bundle) L on a projective variety, there is such a height function $H_L(\cdot)$, assigning a positive real number to every point on the variety defined over $\overline{\mathbb{Q}}$. In "good" situations, such as when the line bundle is ample, a larger height indicates a greater complexity.

We will define and discuss these distance and height functions more carefully in the next section, but they do indeed generalize the classical notions of distance and complexity used above. Indeed, when x is fixed, it turns out that $d_v((x:1),(p:q))$ can be taken to be $\frac{|x-p/q|_v}{\max(|p/q|_v,1)}$. When restricting to a sequence of rational numbers converging v-adically to x, this agrees with the ordinary v-adic distance $|x-p/q|_v$ up to bounded multiplicative constants. Likewise, if we take the standard height function H associated to a hyperplane section in $\mathbb{P}^1$ (i.e. a point), we have $H(p:q) = \max(|p|,|q|)$, provided that we chose the rational number p/q so that $\gcd(p,q) = 1$. When considering a sequence of such rational numbers p/q converging to x with respect to the archimedean absolute value (and assuming that $q > 0$), the quantity $H(p:q)$ thus agrees with the denominator q up to bounded multiplicative constants.

In this reformulated setting, we fix a distance function d_v and height function H ahead of time. For appropriate choices of distances and heights, our classical problem can be stated as follows. Given a point $x \in \mathbb{P}^1(\overline{\mathbb{Q}})$, we look at the positive real numbers γ for which we can find infinitely many rational approximations $y \in \mathbb{P}^1(\mathbb{Q})$ such that

$$d_v(x,y)H(y)^\gamma \leq 1. \tag{1.5}$$

In analogy with the approximation exponent τ_x above, we would seek to locate the largest such real number γ. In fact, in order to ensure that various pleasant formal properties hold, we will prefer to shift the exponent γ to the distance function. Furthermore, it is essentially immaterial whether we use 1 as our upper bound in inequality (1.5), or any other positive constant.

Because we shift the exponent to the distance function, we now seek to find the values of γ for which there are infinitely many $y \in \mathbb{P}^1(\mathbb{Q})$ such that $d_v(x,y)^\gamma H(y)$ is bounded above. If L is the line bundle giving rise to the height function H, the infimum over all such γ (if it exists) is denoted by $\alpha_x(L)$ and called the *approximation constant for x with respect to L*. In general, the approximation constant also depends on the place v used to make the approximation, but this is usually suppressed in the notation.

In this generalized setting, there is nothing sacred about using $\mathbb{P}^1$ as the ambient projective variety, nor about insisting that our approximations come from $\mathbb{Q}$. Formally, the same questions may be asked when the approximations come from any number field k, and when working on any projective variety X defined over k. The question was first formulated and studied in this setting by McKinnon in his 2007 paper [12], before being refined and studied further by McKinnon and Mike Roth ([13], [14]) in work published nearly 10 years later.

In this new language, the theorems of Liouville and Klaus Roth may be formulated in terms of certain inequalities on approximation constants. Taking L to be the line bundle $\mathcal{O}(1)$ on $\mathbb{P}^1$, Liouville's theorem translates into the assertion that $\alpha_x(L) \geq \frac{1}{d}$ for all $x \in \mathbb{P}^1(\overline{\mathbb{Q}})$ of degree d over $\mathbb{Q}$, and Roth's theorem becomes the claim that $\alpha_x(L) \geq \frac{1}{2}$ for all $x \in \mathbb{P}^1(\overline{\mathbb{Q}}) \setminus \mathbb{P}^1(\mathbb{Q})$. Note how these theorems have translated into *lower* bounds on the approximation constants, owing to our insistence on moving the exponent from the height to the distance.

Both of these theorems have been generalized to arbitrary projective varieties and arbitrary number fields by McKinnon and Mike Roth. These generalized results may be expressed as lower bounds on the approximation constant of a point in terms of a geometric invariant known as the *Seshadri constant.* This constant also depends on a choice of point x and line bundle L on a projective variety. The resulting constant $\epsilon_x(L)$ was introduced by Demailly in the early 1990s [3] and has been used to study the "local positivity" of the line bundle L around the point x (for instance, see Chapter 5 of [10]).

In [13], McKinnon and Mike Roth prove a generalized Roth-type theorem, which states the following. For any projective variety X defined over a number field k, any point $x \in X(\overline{k})$, and all ample line bundles L, we have $\alpha_x(L) \geq \frac{1}{2}\epsilon_x(L)$. Since $\epsilon_x(L) = 1$ for any point x on the projective line when $L = \mathcal{O}_{\mathbb{P}^1}(1)$, their result immediately retrieves Roth's theorem.

Likewise, in [14], McKinnon and Mike Roth derive a generalized Liouville-type theorem, claiming that for any projective variety X defined over a number field k, any point $x \in X(\overline{k})$ whose field of definition has degree d over k, and all ample line bundles L, we have $\alpha_x(L) \geq \frac{1}{d}\epsilon_x(L)$. Again, knowing that $\epsilon_x(L) = 1$ for all points on the projective line when $L = \mathcal{O}_{\mathbb{P}^1}(1)$, this result immediately implies our reformulated version of Liouville's theorem.

While there are many ways in which the Roth-type theorem is "better" than the Liouville-type theorem (such as being independent of the field over which x is defined), the Liouville result is actually strictly better when approximating points defined over the base number field.

In the past few years, other work has appeared, taking the work of McKinnon and Roth even further. In one direction, Grieve [6] has proved a similar Roth-type theorem in the setting where the base number field k is replaced with the function field of a smooth projective curve defined over an algebraically closed field of characteristic zero. In another direction, Ru and Wang [17] proved a certain height inequality that recovers and generalizes the Roth-type theorem of McKinnon-Roth. In particular, the approach taken there suggests the possibility of considering approximations to an arbitrary closed subscheme of the ambient projective variety X.

1.3 Layout of the Thesis

Defining and studying these more general approximation constants is the primary goal of this thesis. In the next chapter, we begin by laying the groundwork necessary to define approximation constants $\alpha_Z(L)$, depending on a closed subscheme Z and line bundle L on some ambient projective variety X defined over a number field k. Just like the point-approximation case, this constant will measure the tradeoff between closely approximating Z with k-rational points not lying on Z, and the complexity of the points needed to make the approximation (as measured by the height function corresponding to the line bundle L).

This project will require us to adopt a definition of the v-adic distance to Z, $d_v(\cdot, Z)$, for each place v. At first glance, this definition will seem to clash with the function d_v used by McKinnon and Roth (specializing to the case where Z is a closed point). Hence, one of our first tasks in Chapter 3 is to show that our new notion of distance (and the resulting approximation constant) truly does generalize the one used by McKinnon and Roth.

At the same time, we will define and study an "essential approximation constant" $\alpha_Z^{\mathrm{ess}}(L)$ attached to a closed subscheme Z and line bundle L, which ignores unusually good approximations along proper closed subsets of X. Thus, the essential approximation constant measures how well we can approximate Z "generically", using a Zariski-dense sequence of points.

In Chapter 3, we establish fundamental lower bounds on these more general approximation constants. Unlike the work of Grieve and Ru-Wang, our results throughout this thesis are more of the "Liouville-type" than of the "Roth-type". In particular, we often work with bounds that follow from elementary properties of the distance and height functions, and depend quite directly on the equations used to cut out the closed subscheme in projective space.

Chapter 4 applies the foundational results of the preceding chapter to explicitly compute the approximation constant and essential approximation constant for a selection of different closed subschemes of projective space, with respect to the line bundle $\mathcal{O}(1)$. Since every ample line bundle on projective space is a multiple of $\mathcal{O}(1)$, we will see that this computes the approximation constants for all ample line bundles at once.

We begin Chapter 4 by proving a general geometric result, allowing for computation of the approximation constant in any situation where the closed subscheme Z is defined over $\mathbb{Q}$ and has a tangent line intersecting Z with the highest possible multiplicity. With the help of this result, we will be able to compute the approximation constant for irreducible subschemes cut out by integer polynomials of degree at most 2 (including rational normal curves of any degree) and for cubic curves in $\mathbb{P}^3$ defined over $\mathbb{Q}$ and having a rational flex. It will turn out that we run into obstructions computing the approximation constant for *arbitrary* cubic curves in $\mathbb{P}^3$, and taking one specific example, we investigate those obstructions in some detail. By other means, we also compute the ordinary approximation constants for all linear subvarieties and all conics in $\mathbb{P}^3$.

Supplementing this, we provide computations of the essential approximation constant for any closed subscheme contained in a proper linear subvariety of projective space, any conic curve in $\mathbb{P}^3$, and for the twisted cubic curve. To wrap up this computational chapter, we then take up the question of producing large gaps between the ordinary approximation constant and essential approximation constant, studying approximations of the point $(1 : 0 : 1 : 0)$ on the diagonal quartic surface $x^4 + y^4 = z^4 + w^4$.

Finally, in Chapter 5, we prove generalized versions of the Liouville-type results in [14]. In particular, we apply our results to give another proof of the diagonal quartic surface result at the end of Chapter 4. Furthermore, after formally defining the Seshadri constant, we use it to derive a theorem directly generalizing the Liouville bound of 1844.

Chapter 2

Definitions and Notation

2.1 Approximation Constant of a Point

As discussed in the introduction, McKinnon and Mike Roth have defined the notion of an approximation constant for a point on a projective variety defined over a number field; a notion we will be generalizing to apply to arbitrary closed subschemes.

We will begin by laying out the original definitions provided in [13], since our generalization requires only a minor variation on those definitions. Let k denote a number field, and fix a place v of k, extended in some way to its algebraic closure $\overline{k}$. Suppose that X is a projective variety defined over k, and fix a line bundle L on X. The definition of the approximation constant depends upon a choice of distance function $d_v(\cdot,\cdot)$ on X with respect to the place v, as well as a height function $H_L(\cdot)$ on $X(\overline{k})$ depending on the line bundle L.

To define the distance function, we choose an embedding $X \hookrightarrow \mathbb{P}^n$. Given points x and y on X, we let $(x_0 : \cdots : x_n)$ and $(y_0 : \cdots : y_n)$ denote homogeneous coordinates for these points under this embedding. If v is an archimedean place, we let σ denote the field embedding $k \hookrightarrow \mathbb{C}$ corresponding to v. Furthermore, we let k_v denote the completion of k with respect to v, so that $k_v = \mathbb{R}$ if σ is a real embedding, and $k_v = \mathbb{C}$ otherwise. We define

$$d_v(x,y) := \left(1 - \frac{\left|\sum_{i=0}^{n} \sigma(x_i)\overline{\sigma(y_i)}\right|^2}{\left(\sum_{i=0}^{n} |\sigma(x_i)|^2\right)\left(\sum_{i=0}^{n} |\sigma(y_i)|^2\right)}\right)^{[k_v:\mathbb{R}]/2}.$$

Above, $|\cdot|$ denotes the usual absolute value on $\mathbb{C}$. We will also have occasion to use a normalized absolute value corresponding to the archimedean place v. Namely, for $\alpha \in k$, we take $\|\alpha\|_v := |\sigma(\alpha)|$ if σ is a real embedding, and $\|\alpha\|_v := |\sigma(\alpha)|^2$ if σ is a complex embedding.

If v is a non-archimedean place, we define d_v slightly differently. We fix an absolute value $\|\cdot\|_v$ on k associated with v, normalized as follows. If π is a uniformizer for the local ring associated with v and κ is the residue field, we choose the absolute value such that $\|\pi\|_v = \frac{1}{\#\kappa}$. We then consider some extension of $\|\cdot\|_v$ to $\overline{k}$.

For each pair of points $x, y \in X(\overline{k})$, we take homogeneous coordinates $(x_0 : \cdots : x_n)$ and $(y_0 : \cdots : y_n)$, and set

$$d_v(x,y) := \frac{\max_{0\le i<j\le n} \|x_i y_j - x_j y_i\|_v}{\max_{0\le i\le n}(\|x_i\|_v)\max_{0\le j\le n}(\|y_j\|_v)}.$$

In either case, it is easy to verify that $d_v(x, y)$ is well defined on projective points. Moreover, it is not hard to check that $0 \le d_v(x, y) \le 1$ for all points x and y, and that $d_v(x, y) = 0$ if and only if $x = y$ as projective points. Likewise, it is immediate from the definitions that $d_v(x, y) = d_v(y, x)$ for all x and y.

While the notation suggests that d_v is a metric, this function does not satisfy the triangle inequality in general. We can see this in the simple case where v corresponds to the identity embedding on any non-real number field k and $X = \mathbb{P}^1_k$. We consider the identity embedding of X, and we take $x = (1 : 1), y = (1 : 2), z = (0 : 1)$. One computes that $d_v(x, z) = \frac{1}{2}$, $d_v(y, z) = \frac{1}{5}$, and $d_v(x, y) = \frac{1}{10}$. Therefore,

$$d_v(x,z) = \frac{1}{2} > \frac{3}{10} = d_v(x,y) + d_v(y,z),$$

showing that the triangle inequality does not hold.

Even though the triangle inequality might be violated, this need not be a source of concern for our purposes. Lemma 2.6 of [13] states that for any $x \in X(\overline{k})$, if K is a finite extension of k over which x is defined, there is an affine open neighbourhood U of x in $X \times_k K$ and generators $u_1, \ldots, u_m$ for the maximal ideal of x in U such that $d_v(x, \cdot)$ is equivalent to $\min(1, \max(\|u_1(\cdot)\|_v, \ldots, \|u_m(\cdot)\|_v))$ on $U(K_v)$. The equivalence holds in the sense of metric equivalence, i.e. each function is bounded above and below by positive multiples of the other. Since this latter function defines the usual v-adic distance in an affine neighbourhood of x, our "distance" function d_v still induces a topology on X, equivalent to the usual v-adic topology. In particular, the notion of a sequence of points $\{x_i\}$ converging to a point x with respect to d_v still makes sense.

Another concern is that the distance functions just defined depend upon the choice of embedding of X into projective space. However, it is proved in Proposition 2.5 of [13] that if d_v and d'_v are two distance functions coming from different embeddings of X, the two functions are *equivalent*, again in the sense that there are positive constants $c \le C$ for which $cd'_v \le d_v \le Cd'_v$. Hence, the two choices of distance function define the same topology, and convergence with respect to one distance is the same as convergence with respect to the other.

Next, we discuss height functions. For every linear equivalence class of Cartier divisors (or every line bundle) L on X, Weil's Height Machine gives us a height function H_L, which is a function $X(\overline{k}) \to (0, \infty)$. These functions have several important properties, which are stated in [9], §B.3. Some minor differences should be noted: we will often favour the multiplicative height H_L over the logarithmic height h_L, and our height functions will be normalized relative to the base field k, rather than using the absolute multiplicative height.

Given our conventions on heights, we state some properties of these functions that will come in handy. First, we can take

$$H_{\mathcal{O}_{\mathbb{P}^n_k}(1)}(x_0 : \cdots : x_n) = \prod_v \max\{\|x_0\|_v, \ldots, \|x_n\|_v\},$$

where the product runs over all places v of the number field k. As mentioned, this height is defined relative to k, so that if k' is a finite extension of k, then $H_{\mathcal{O}_{\mathbb{P}^n_{k'}}(1)} = H^{[k':k]}_{\mathcal{O}_{\mathbb{P}^n_k}(1)}$ (see [9], Lemma B.2.1(c)).

If $\phi : X \to Y$ is a morphism of projective varieties and L is a line bundle on Y, then $H_{X,\phi^*L}(x)$ is equivalent to $H_{Y,L}(\phi(x))$ as a function on $X(k)$. Additionally, if L_1 and L_2 are line bundles on X, then $H_{L_1+L_2}$ is equivalent to $H_{L_1}H_{L_2}$. Next, if L is effective, and B is the base locus for L, the function H_L is bounded below on $(X \setminus B)(k)$ by some positive constant. Finally, if L is an ample line bundle, then for any finite extension k' of k and any constant M, the set

$$\{x \in X(k') : H_L(x) \leq M\}$$

is finite. This is the sense in which H_L measures the "complexity" of a point (when L is ample).

Now, we put these two concepts together to define the approximation constant of a point, as given in [13]. With notation as above, fix a point $x \in X(\overline{k})$, and choose a sequence $\{x_i\}$ of distinct points in $X(k)$. If $\{x_i\}$ converges to x, in the sense that $d_v(x_i, x) \to 0$ as $i \to \infty$, we define the set

$$A(\{x_i\}, L) := \{\gamma \in \mathbb{R} : d_v(x_i, x)^\gamma H_L(x_i) \text{ is bounded from above}\}.$$

If $\{x_i\}$ does not converge to x, we set $A(\{x_i\}, L) = \varnothing$. Note that replacing either d_v or H_L with an equivalent distance or height function does not change the set $A(\{x_i\}, L)$, and hence this set does not depend on any choices that alter d_v or H_L up to equivalence. Notice also that $A(\{x_i\}, L)$, when nonempty, is an interval unbounded to the right. This follows because $0 \leq d_v(x_i, x) \leq 1$ for all x_i, so that $d_v(x_i, x)^{\gamma+\delta} \leq d_v(x_i, x)^\gamma$ for any $\delta > 0$. Thus, for a given sequence $\{x_i\}$, we set

$$\alpha_x(\{x_i\}, L) = \inf A(\{x_i\}, L),$$

and call this quantity the *approximation constant of* $\{x_i\}$ *with respect to* L. In turn, the *approximation constant of* x *with respect to* L is taken to be the infimum of all approximation constants over all sequences $\{x_i\}$ of points in $X(k)$ converging to x and is denoted by $\alpha_x(L)$.

2.2 Approximation Constant of a Closed Subscheme

Next, we present our generalized definition, going beyond the work in [13]. Instead of a point $x \in X(\overline{k})$, we fix a closed subscheme Z of X, where Z may be defined over any algebraic extension of k. The important change is to define the distance $d_v(x, Z)$ from a point x to the subscheme Z in an appropriate way. In this setting, local Weil functions give rise to the most useful notion, or more generally, arithmetic distance functions as defined in [19].

Given a place v of k and a divisor D on X, we may associate a real-valued function $\lambda_{D,v}$, defined on points of $X(k_v)$ not lying in the support of D. For fixed D, the function $\lambda_{D,\cdot}(\cdot)$ is referred to as a *local Weil function* for D. This function satisfies several pleasant functorial properties, similar to the height functions described earlier.

Firstly, suppose D represents a hypersurface in $\mathbb{P}^n_k$ defined by the vanishing of a single homogeneous polynomial $P(x_0, \ldots, x_n)$ of degree d. We normalize so that for any point $x = (x_0 : \cdots : x_n)$ in $\mathbb{P}^n(k_v)$ with $P(x_0, \ldots, x_n) \neq 0$, we may take

$$\lambda_{D,v}(x) = \log \max_{0 \leq i \leq n} \left\| \frac{x_i^d}{P(x_0, \ldots, x_n)} \right\|_v .$$

These local Weil functions are related to the height functions introduced earlier by the so-called *local/global property*. If we set $h_D = \log H_D$, where H_D is a height function associated to the linear equivalence class of D (as defined above), then our choice of normalizations yields

$$h_D(x) = \sum_v \lambda_{D,v}(x) + O(1),$$

where the sum runs over all places v of k and $x \in X(k)$ does not lie in the support of D.

If $\phi : X \to Y$ is a morphism of projective varieties and D is a divisor on Y, then $\lambda_{\phi^* D,v}$ is equal to $\lambda_{D,v} \circ \phi$ up to $O(1)$. Furthermore, if D_1 and D_2 are divisors on X, then $\lambda_{D_1+D_2,v}$ is equal to $\lambda_{D_1,v} + \lambda_{D_2,v}$ up to $O(1)$. Finally, if D is an effective divisor, then $\lambda_{D,v}$ is bounded below by some constant. Notice that all of these properties are the additive counterparts to similar properties involving the height functions.

It is desirable to extend the definition of local Weil functions to all closed subschemes of X. This is done in detail in Silverman's paper [19]. For any closed subscheme Z, Lemma 2.2 of [19] states that there is a collection of effective divisors $D_1, \ldots .D_r$ on X for which $Z = \bigcap_{i=1}^r D_i$ (this being a scheme-theoretic intersection). The local Weil function is then defined to be

$$\lambda_{Z,v} := \min_{1 \leq i \leq r} \lambda_{D_i,v}.$$

This function shares the property that for any morphism of varieties $\phi : X \to Y$ and any closed subscheme Z of Y, we have $\lambda_{\phi^* Z,v} = \lambda_{Z,v} \circ \phi$. To define the pullback $\phi^* Z$, one takes the ideal sheaf $\mathcal{I}_Z$ corresponding to Z and looks at the closed subscheme of X with ideal sheaf $\phi^{-1}\mathcal{I}_Z \otimes_{\phi^{-1}\mathcal{O}_Y} \mathcal{O}_X$.

Finally, we use these local Weil functions to define the distance to a closed subscheme. Given our fixed place v, a closed subscheme Z, and $x \in X(k_v)$, we define

$$d_v(x, Z) := \exp(-\lambda_{Z,v}(x)),$$

with the interpretation that $d_v(x, Z) = 0$ if x actually lies on Z. In particular, if Z is a hypersurface in $\mathbb{P}^n_k$ defined by the vanishing of a single polynomial $P(x_0, \ldots, x_n)$ of degree

d (so that Z is actually a Cartier divisor), we can choose the distance function so that for $x = (x_0 : \cdots : x_n)$, we have

$$d_v(x, Z) = \min_{0 \le i \le n} \left\| \frac{P(x_0, \ldots, x_n)}{x_i^d} \right\|_v = \frac{\|P(x_0, \ldots, x_n)\|_v}{\max_{0 \le i \le n} \|x_i\|_v^d}.$$

We will use this fact frequently without further comment.

Keeping with the notation above, suppose we have fixed a closed subscheme Z that we wish to approximate. We will say that a sequence of points $\{x_i\}$ in $X(k)$ *converges to* Z (with respect to a place v) if:

- None of the points lie on Z.
- We have $d_v(x_i, Z) \to 0$ as $i \to \infty$.

Note that the first condition is present to rule out the trivial case of approximation of Z from *within* Z. Given a sequence $\{x_i\} \subseteq X(k)$ converging to Z, we define the set

$$A(\{x_i\}, L) := \{\gamma \in \mathbb{R} : d_v(x_i, Z)^\gamma H_L(x_i) \text{ is bounded from above}\}.$$

If $\{x_i\}$ does not converge to Z, we set $A(\{x_i\}, L) = \varnothing$. As before, changing d_v and H_L up to equivalence does not affect the definition of this set. Since $d_v(x_i, Z)$ is always nonnegative, we also see that when $d_v(x_i, Z) \to 0$, the distance $d_v(x_i, Z)$ is eventually bounded between 0 and 1, and from there we deduce as before that $A(\{x_i\}, L)$ is an interval unbounded to the right.

We take $\alpha_Z(\{x_i\}, L) = \inf A(\{x_i\}, L)$, and set the *approximation constant of Z with respect to L* to be the infimum of the $\alpha_Z(\{x_i\}, L)$ over all sequences of points of $X(k)$ converging to Z. This constant will be denoted by $\alpha_Z(L)$.

At this stage, it will be useful to make a number of elementary remarks about approximation constants.

- For any line bundle L and positive integer m, we have $\alpha_Z(mL) = m\alpha_Z(L)$. Indeed, the height function H_{mL} is equivalent to H_L^m, by the properties above. Therefore, $d_v(x_i, Z)^\gamma H_{mL}(x_i)$ is bounded from above if and only if $d_v(x_i, Z)^{\gamma/m} H_L(x_i)$ is bounded from above. From this observation, the claim immediately follows. Since every ample line bundle on $\mathbb{P}^n$ is a positive multiple of $\mathcal{O}(1)$, this reduces the computation of approximation constants for all ample line bundles to the computation of $\alpha_Z(\mathcal{O}(1))$ in this case.
- If L is an ample line bundle, then $\alpha_Z(L) \ge 0$. Indeed, since L is ample, the set of points in $X(k)$ of height bounded by any fixed constant is finite. Thus for any sequence $\{x_i\}$ converging to Z, we have $H_L(x_i) \to \infty$ as $i \to \infty$. It follows that $d_v(x_i, Z)^\gamma H_L(x_i) \to \infty$ for $\gamma \le 0$, so $\alpha_Z(L) \ge \gamma$ for any such γ. In particular, $\alpha_Z(L) \ge 0$.

- For any real number $\gamma > \alpha_Z(\{x_i\}, L)$, we have $d_v(x_i, Z)^\gamma H_L(x_i) \to 0$ as $i \to \infty$. Indeed, under this assumption, we can find $\epsilon > 0$ such that $\gamma - \epsilon > \alpha_Z(\{x_i\}, L)$. Consequently, $d_v(x_i, Z)^{\gamma-\epsilon} H_L(x_i)$ is bounded above by some constant M. Since $d_v(x_i, Z) \to 0$ as $i \to \infty$, we have $d_v(x_i, Z)^\epsilon \to 0$ as well. Then

$$0 \leq d_v(x_i, Z)^\gamma H_L(x_i) = d_v(x_i, Z)^\epsilon (d_v(x_i, Z)^{\gamma-\epsilon} H_L(x_i)) \leq d_v(x_i, Z)^\epsilon M,$$

and taking limits as $i \to \infty$ shows $d_v(x_i, Z)^\gamma H_L(x_i) \to 0$, as claimed.

- Given $\gamma \in \mathbb{R}$ such that $d_v(x_i, Z)^\gamma H_L(x_i)$ is bounded below by a positive constant, we have $\alpha_Z(\{x_i\}, L) \geq \gamma$. Indeed, this follows directly from the previous remark.

2.3 Essential Approximation Constants

When computing approximation constants in practice, it will often happen that some key geometric feature of the closed subscheme causes the approximation constant to be smaller than it "should" be. In order to disregard such behavior, we will find it useful to define and study a refined approximation constant, one that prohibits consideration of sequences lying in any given Zariski-closed subset of our ambient variety X.

For any nonempty Zariski-open set $U \subseteq X$, we define the approximation constant $\alpha_Z(U, L)$ to be the infimum of the sequence approximation constants $\alpha_Z(\{x_i\}, L)$, ranging over all sequences of k-points $\{x_i\}$ lying inside of U and converging to Z. In particular, $\alpha_Z(X, L) = \alpha_Z(L)$. We take the *essential approximation constant of Z with respect to L* to be the quantity

$$\alpha_Z^{\mathrm{ess}}(L) := \sup_U \alpha_Z(U, L),$$

with the supremum running over all nonempty Zariski-open subsets of X. It is immediate from the definition that $\alpha_Z(L) \leq \alpha_Z^{\mathrm{ess}}(L)$. Moreover, we expect the essential approximation constant to be strictly larger than the ordinary one if Z has geometric features allowing for particularly good approximations along certain Zariski-closed subsets of X (e.g. along tangent lines to Z).

With the definition given, computing $\alpha_Z^{\mathrm{ess}}(L)$ requires us to consider all the open subsets of X at once. Our first goal is to prove a proposition giving us a different conceptual perspective on this. Before giving the proof, we will need to establish a certain lemma, one that we will invoke whenever we need to show that a closed subscheme is "defined over k". The argument we give is adapted from the proof of Proposition A.2.2.10 in [9].

Lemma 2.3.1. *Let k be a number field, and let X be a projective subvariety of $\mathbb{P}^n_k$ defined over k, corresponding to some homogeneous ideal $I(X)$ in $k[x_0, \ldots, x_n]$. Let Z be a closed subscheme of $X_{\overline{k}} := X \times_k \overline{k}$, corresponding to some homogeneous ideal $I(Z)$ inside the homogeneous polynomial ring $\overline{k}[x_0, \ldots, x_n]$.*

Suppose $I(Z) = (f_1, \ldots, f_m)$, and let ℓ be a finite Galois extension of k over which all of $f_1, \ldots, f_m$ are defined. For each $\sigma \in \mathrm{Gal}(\ell/k)$, let Z^σ be the closed subscheme defined *by the ideal* $(f_1^\sigma, \ldots, f_m^\sigma)$*, where* f_i^σ *denotes the polynomial obtained by applying* σ *to all coefficients of* f_i*. If*

$$Z' = \bigcap_{\sigma \in \mathrm{Gal}(\ell/k)} Z^\sigma,$$

then the homogeneous ideal corresponding to Z' *is generated by elements in* $k[x_0, \ldots, x_n]$*.*

Proof. By definition of scheme-theoretic intersection, the ideal of Z' may be generated by the polynomials $f_1^\sigma, \ldots, f_m^\sigma$, as σ ranges over all of $\mathrm{Gal}(\ell/k)$. Now, fix a basis $\alpha_1, \ldots, \alpha_N$ for ℓ over k. Since ℓ/k is a Galois extension, the group $\mathrm{Gal}(\ell/k)$ also has N elements, say $\sigma_1, \ldots, \sigma_N$.

For $1 \leq i \leq N$ and $1 \leq j \leq m$, we define the following polynomials:

$$g_{i,j} = \sum_{r=1}^{N} \sigma_r(\alpha_i f_j).$$

Clearly, each of the polynomials $g_{i,j}$ is $\mathrm{Gal}(\ell/k)$-invariant, which means $g_{i,j} \in k[x_0, \ldots, x_n]$ for each i and j. It is immediate from the construction that each $g_{i,j}$ is in the $\overline{k}$-span of the polynomials $f_1^\sigma, \ldots, f_m^\sigma$ as σ ranges over $\mathrm{Gal}(\ell/k)$, so the ideal generated by the $g_{i,j}$ is contained in the one generated by all the polynomials $f_1^\sigma, \ldots, f_m^\sigma$.

On the other hand, it is a well-known fact that the matrix $(\sigma_r(\alpha_i))$ is invertible (as stated in the proof of Proposition A.2.2.10 of [9]). So, for a fixed j, the polynomial f_j^σ is likewise in the $\overline{k}$-span of the polynomials $g_{i,j}$, $1 \leq i \leq N$. This implies that the ideal generated by all the $f_1^\sigma, \ldots, f_m^\sigma$ is contained in the ideal generated by the $g_{i,j}$, and in turn implies that the homogeneous ideal of the closed subscheme Z' is generated by these $g_{i,j}$, which are polynomials with coefficients in k. □

Now we are ready to provide a characterization of the essential approximation constant:

Proposition 2.3.1. *Let* X *be a projective variety defined over a number field* k*, and let* Z *be a closed subscheme of* X*. Let* S *denote the set of Zariski-dense sequences of* k*-points of* X *converging to* Z*. If* L *is an ample line bundle on* X*, then*

$$\alpha_Z^{ess}(L) = \inf_{\{x_i\} \in S} \alpha_Z(\{x_i\}, L).$$

Proof. For the moment, we will use $\tilde{\alpha}_Z(L)$ to denote the quantity on the right-hand side of the equality above. First, we will show $\alpha_Z^{\mathrm{ess}}(L) \leq \tilde{\alpha}_Z(L)$. This is obvious if $\tilde{\alpha}_Z(L) = \infty$, so we will assume that $\tilde{\alpha}_Z(L)$ is finite.

Now, let $\{x_i\}$ be an arbitrary Zariski-dense sequence of k-points on X converging to Z. By the Zariski-dense condition, for every nonempty open $U \subseteq X$, we can extract a subsequence $\{y_i\}$ that is contained inside of U. Indeed, by density, the original sequence intersects U in some point $y_1 = x_{i_1}$. Throwing away the points $x_1, \ldots, x_{i_1}$ from U, we get a new open subset, which must contain a sequence element $y_2 = x_{i_2}$, with $i_2 > i_1$. Proceeding in this manner, we obtain the desired subsequence.

It follows immediately from the definition of approximation constants that $\alpha_Z(\{y_i\}, L) \leq \alpha_Z(\{x_i\}, L)$, since $\{y_i\}$ is a subsequence of $\{x_i\}$. On the other hand, since $\{y_i\}$ is a sequence contained inside of U, we have $\alpha_Z(U, L) \leq \alpha_Z(\{y_i\}, L)$. Putting this all together, we see that

$$\alpha_Z(U, L) \leq \alpha_Z(\{x_i\}, L).$$

But U was an arbitrary nonempty open set, so we deduce that

$$\alpha_Z^{\text{ess}}(L) \leq \alpha_Z(\{x_i\}, L).$$

Finally, $\{x_i\}$ was an arbitrary sequence from S, so we arrive at

$$\alpha_Z^{\text{ess}}(L) \leq \tilde{\alpha}_Z(L).$$

To prove the other inequality, we may likewise assume that $\alpha_Z^{\text{ess}}(L)$ is finite. Notice that there are only countably many closed subsets of X cut out by polynomials defined over k. This follows because each closed subset is cut out by finitely many polynomials with coefficients in a number field, and the collection of such polynomials is countable. Taking complements, there are also countably many open subsets whose complements are cut out by polynomials over k. We will enumerate all the nonempty ones, say $U_1, U_2, U_3, \ldots$.

Now, fix $\epsilon > 0$. Certainly, for every open set U_m, we have $\alpha_Z(U_m, L) < \alpha_Z^{\text{ess}}(L) + \frac{\epsilon}{2}$. In particular, for each m, we can find a sequence $\{x_i^{(m)}\}$ of k-points of X, converging to Z and contained in U_m, such that

$$\alpha_Z(\{x_i^{(m)}\}, L) < \alpha_Z^{\text{ess}}(L) + \frac{\epsilon}{2}.$$

By our earlier remarks, for each m, the sequence $d_v(x_i^{(m)}, Z)^{\alpha_Z^{\text{ess}}(L)+\epsilon} H_L(x_i^{(m)})$ converges to 0. Taking any constant $C > 0$, we replace $\{x_i^{(m)}\}$ with a suitably chosen tail of the sequence for each m in order to assume that

$$d_v(x_i^{(m)}, Z)^{\alpha_Z^{\text{ess}}(L)+\epsilon} H_L(x_i^{(m)}) \leq C$$

for all choices of i and m.

Next, consider the diagonal sequence $\{x_i^{(i)}\}$. This is a sequence of k-points on X disjoint from Z, because each sequence $\{x_i^{(m)}\}$ is disjoint from Z by our definition of convergence. Furthermore, we claim the diagonal sequence is Zariski-dense.

Indeed, if it were not, then the whole sequence would be contained in some proper closed subset $W \subsetneq X$. Now, we appeal to Lemma 2.3.1, which says that intersecting W with all of its $\text{Gal}(\overline{k}/k)$-conjugates yields another proper closed subset W' cut out by polynomials with coefficients in k. Since every element of the diagonal sequence is defined over k, W' also contains the whole sequence. If we set U to be the complement of W', we must have $U = U_m$ for some positive integer m. On the other hand, we know that $x_m^{(m)} \in U_m$, so this element of the sequence cannot belong to W', a contradiction.

Finally, we argue that $\{x_i^{(i)}\}$ converges to Z. Indeed, we know by construction that there is some positive constant C such that for all i,

$$d_v(x_i^{(i)}, Z)^{\alpha_Z^{\text{ess}}(L)+\epsilon} H_L(x_i^{(i)}) \leq C.$$

On the other hand, since L is an ample line bundle, the heights $H_L(x_i^{(i)})$ tend to ∞, so it must be true that $d_v(x_i^{(i)}, Z)^{\alpha_Z^{\mathrm{ess}}(L)+\epsilon} \to 0$ as $i \to \infty$. Again, since L is ample, we know that $\alpha_Z^{\mathrm{ess}}(L) \geq \alpha_Z(L) \geq 0$, so it follows that $d_v(x_i^{(i)}, Z) \to 0$. In other words, $\{x_i^{(i)}\}$ converges to Z.

We have now verified that $\{x_i^{(i)}\}$ is a Zariski-dense sequence of k-points on X converging to Z, for which $d_v(x_i^{(i)}, Z)^{\alpha_Z^{\mathrm{ess}}(L)+\epsilon} H_L(x_i^{(i)})$ is bounded above. Putting this all together, we deduce that

$$\tilde{\alpha}_Z(L) \leq \alpha_Z(\{x_i^{(i)}\}, L) \leq \alpha_Z^{\mathrm{ess}}(L) + \epsilon.$$

Since $\epsilon > 0$ was arbitrary, we get $\tilde{\alpha}_Z(L) \leq \alpha_Z^{\mathrm{ess}}(L)$, as desired. $\square$

Chapter 3

Basic Results

3.1 Reconciling the Definitions

Before doing anything else, we should verify that when the closed subscheme Z is a reduced closed point $\{z\}$, the approximation constant $\alpha_{\{z\}}(L)$, as we just defined it, agrees with the approximation constant $\alpha_z(L)$ as defined in [13]. That way, we can rest assured that our new approximation constants are truly generalizations of previous work.

Proposition 3.1.1. *Let X be a projective variety defined over a number field k, let L be a line bundle on X, and let z be any point in $X(\overline{k})$. Then we have*

$$\alpha_z(L) = \alpha_{\{z\}}(L),$$

where $\{z\}$ refers to the point z considered as a (reduced) closed subvariety of X.

Proof. It will suffice to show that $d_v(\cdot, z)$ and $d_v(\cdot, \{z\})$ are equivalent, in the sense that there are positive constants $c < C$ for which

$$cd_v(\cdot, z) \leq d_v(\cdot, \{z\}) \leq Cd_v(\cdot, z).$$

Indeed, two things follow immediately from this. First, given any sequence $\{x_i\}$ of k-points on X, we have $d_v(x_i, \{z\}) \to 0$ if and only if $d_v(x_i, z) \to 0$. Second, for any real number γ, the sequence $d_v(x_i, z)^\gamma H_L(x_i)$ is bounded above if and only if $d_v(x_i, \{z\})^\gamma H_L(x_i)$ is bounded above. Combined with the first point, this implies $\alpha_z(\{x_i\}, L) = \alpha_{\{z\}}(\{x_i\}, L)$ for any sequence $\{x_i\} \subseteq X(k)$. From this, the conclusion of the proposition follows immediately.

Thus, we are reduced to showing that $d_v(\cdot, z)$ and $d_v(\cdot, \{z\})$ are equivalent functions in the sense described above. Since the two distance functions scale up by the same amounts when normalized with respect to different fields, we may assume that z is defined over k without loss of generality.

To produce an explicit formula for $d_v(\cdot, \{z\})$, we use the fact that for all choices of divisors $D_1, \ldots, D_m$ satisfying $\{z\} = \bigcap_{i=1}^m D_i$, the resulting distance functions $d_v(\cdot, \{z\})$

are equivalent (see the proof of Theorem 2.1 in [19]). Hence, we may use whichever choice of divisors we find most convenient.

Given some embedding of X into projective space $\mathbb{P}_k^n$, suppose that z has projective coordinates $(z_0 : \cdots : z_n)$, and suppose we have normalized so that $\max_{0\le k\le n} \|z_k\|_v = 1$. Certainly, $\{z\}$ may be cut out in X by the equations $z_j t_i - z_i t_j = 0$ for $i < j$. If we let D_{ij} denote the divisor given by the hyperplane section $z_j t_i - z_i t_j = 0$ in X, we see that $\{z\} = \bigcap_{i<j} D_{ij}$. Hence, for any $y \in X(k)$, we may take

$$d_v(y, \{z\}) = \max_{i<j} d_v(y, D_{ij}),$$

and in turn, if y has homogeneous coordinates $(y_0 : \cdots : y_n)$, we have

$$d_v(y, D_{ij}) = \min_{0\le k\le n} \left\| \frac{z_j y_i - z_i y_j}{y_k} \right\|_v = \frac{\|z_j y_i - z_i y_j\|_v}{\max_{0\le k\le n}(\|y_k\|_v)}.$$

Since we selected the homogenous coordinates of z so that $\max_{0\le k\le n} \|z_k\|_v = 1$, we may write

$$d_v(y, D_{ij}) = \frac{\|z_j y_i - z_i y_j\|_v}{\max_{0\le k\le n}(\|z_k\|_v) \cdot \max_{0\le k\le n}(\|y_k\|_v)}.$$

Consequently,

$$\begin{aligned} d_v(y, \{z\}) &= \max_{i<j} d_v(y, D_{ij}) \\ &= \max_{i<j} \frac{\|z_j y_i - z_i y_j\|_v}{\max_{0\le k\le n}(\|z_k\|_v) \cdot \max_{0\le k\le n}(\|y_k\|_v)} \\ &= \frac{\max_{i<j} \|z_j y_i - z_i y_j\|_v}{\max_{0\le k\le n}(\|z_k\|_v) \cdot \max_{0\le k\le n}(\|y_k\|_v)}. \end{aligned}$$

In the case that v is non-archimedean, we recognize the last expression above as being $d_v(y, z)$, so that we in fact have $d_v(y, \{z\}) = d_v(y, z)$ in this case. In the case v is an archimedean place (corresponding to some embedding $\sigma : k \hookrightarrow \mathbb{C}$), it only remains to prove that

$$\frac{\max_{i<j} \|z_j y_i - z_i y_j\|_v}{\max_{0\le k\le n}(\|z_k\|_v) \cdot \max_{0\le k\le n}(\|y_k\|_v)}$$

is equivalent to

$$d_v(y, z) = \left(1 - \frac{\left| \sum_{i=0}^n \sigma(y_i) \overline{\sigma(z_i)} \right|^2}{\left(\sum_{i=0}^n |\sigma(y_i)|^2\right) \left(\sum_{i=0}^n |\sigma(z_i)|^2\right)} \right)^{[k_v:\mathbb{R}]/2}.$$

Using the complex number identity $|\alpha|^2 = \alpha \cdot \overline{\alpha}$, we compute

$$\begin{aligned}
1 - \frac{\left|\sum_{i=0}^n \sigma(y_i)\overline{\sigma(z_i)}\right|^2}{\left(\sum_{i=0}^n |\sigma(y_i)|^2\right)\left(\sum_{i=0}^n |\sigma(z_i)|^2\right)} &= \frac{\left(\sum_{i=0}^n |\sigma(y_i)|^2\right)\left(\sum_{i=0}^n |\sigma(z_i)|^2\right) - \left|\sum_{i=0}^n \sigma(y_i)\overline{\sigma(z_i)}\right|^2}{\left(\sum_{i=0}^n |\sigma(y_i)|^2\right)\left(\sum_{i=0}^n |\sigma(z_i)|^2\right)} \\
&= \frac{\sum_{i,j=0}^n \sigma(y_i)\overline{\sigma(y_i)}\sigma(z_j)\overline{\sigma(z_j)} - \sum_{i,j=0}^n \sigma(y_i)\overline{\sigma(z_i)\sigma(y_j)}\sigma(z_j)}{\left(\sum_{i=0}^n |\sigma(y_i)|^2\right)\left(\sum_{i=0}^n |\sigma(z_i)|^2\right)} \\
&= \frac{\sum_{i\neq j}(\sigma(y_i)\overline{\sigma(y_i)}\sigma(z_j)\overline{\sigma(z_j)} - \sigma(y_i)\overline{\sigma(z_i)\sigma(y_j)}\sigma(z_j))}{\left(\sum_{i=0}^n |\sigma(y_i)|^2\right)\left(\sum_{i=0}^n |\sigma(z_i)|^2\right)} \\
&= \frac{\sum_{0\leq i<j\leq n} |\sigma(y_i)\sigma(z_j) - \sigma(y_j)\sigma(z_i)|^2}{\left(\sum_{i=0}^n |\sigma(y_i)|^2\right)\left(\sum_{i=0}^n |\sigma(z_i)|^2\right)}.
\end{aligned}$$

Now, we split into two cases. If v is a complex place, we see immediately that

$$d_v(y,z) = \frac{\sum_{0\leq i<j\leq n} \|y_i z_j - y_j z_i\|_v}{\left(\sum_{i=0}^n \|y_i\|_v\right)\left(\sum_{i=0}^n \|z_i\|_v\right)}.$$

For any collection of numbers $\alpha_0, \ldots, \alpha_n \in k$, we have $\max_{0\leq i\leq n} \|\alpha_i\|_v \leq \sum_{i=0}^n \|\alpha_i\|_v \leq (n+1)\max_{0\leq i\leq n} \|\alpha_i\|_v$. Applying this to the numerator and denominator of the identity above shows that

$$c \cdot \frac{\max_{0\leq i<j\leq n} \|y_i z_j - y_j z_i\|_v}{\max_{0\leq i\leq n}(\|y_i\|_v) \cdot \max_{0\leq i\leq n}(\|z_i\|_v)} \leq d_v(y,z) \leq C \cdot \frac{\max_{0\leq i<j\leq n} \|y_i z_j - y_j z_i\|_v}{\max_{0\leq i\leq n}(\|y_i\|_v) \cdot \max_{0\leq i\leq n}(\|z_i\|_v)},$$

where $c = \frac{1}{(n+1)^2}$ and $C = \frac{n(n+1)}{2}$. As for the case where v is a real place, our computation shows that

$$d_v(y,z) = \left(\frac{\sum_{0\leq i<j\leq n} \|y_i z_j - y_j z_i\|_v^2}{\left(\sum_{i=0}^n \|y_i\|_v^2\right)\left(\sum_{i=0}^n \|z_i\|_v^2\right)}\right)^{1/2}.$$

Here, the inequalities $\max_{0\leq i\leq n} \|\alpha_i\|_v^2 \leq \sum_{i=0}^n \|\alpha_i\|_v^2 \leq (n+1)\max_{0\leq i\leq n} \|\alpha_i\|_v^2$ lead to the result that

$$\sqrt{c}\frac{\max_{0\leq i<j\leq n} \|y_i z_j - y_j z_i\|_v}{\max_{0\leq i\leq n}(\|y_i\|_v) \cdot \max_{0\leq i\leq n}(\|z_i\|_v)} \leq d_v(y,z) \leq \sqrt{C}\frac{\max_{0\leq i<j\leq n} \|y_i z_j - y_j z_i\|_v}{\max_{0\leq i\leq n}(\|y_i\|_v) \cdot \max_{0\leq i\leq n}(\|z_i\|_v)},$$

where c and C are as above. Hence, in the archimedean case we also have that $d_v(\cdot, z)$ is equivalent to $d_v(\cdot, \{z\})$. As such, our proof is complete. □

When performing computations with approximation constants, it will be helpful to know that we can apply any convenient automorphism of our projective variety without affecting the approximation constant (though perhaps changing the line bundle). We prove this formally below:

Lemma 3.1.1. *Let X be a projective variety defined over a number field k, let v be a place of k extended in some way to $\overline{k}$, let L be a line bundle on X, and let Z be a closed subscheme of X. If $\phi : X \to X$ is an automorphism of X defined over k, then we have*

$$\alpha_Z(\phi^*(L)) = \alpha_{\phi(Z)}(L)$$

and
$$\alpha_Z^{ess}(\phi^*(L)) = \alpha_{\phi(Z)}^{ess}(L).$$

Proof. Noting that Z is the pullback of $\phi(Z)$ under the automorphism ϕ, functoriality gives us
$$\lambda_{Z,v} = \lambda_{\phi(Z),v} \circ \phi,$$
up to $O(1)$. Therefore, the values $d_v(x_i, Z)$ and $d_v(\phi(x_i), \phi(Z))$ agree up to bounded constants. Notice also that $\{x_i\}$ is a sequence of k-points if and only if $\{\phi(x_i)\}$ is a sequence of k-points, since the automorphism is defined over k. In particular, $\{x_i\}$ is a sequence of k-points converging to Z if and only if $\{\phi(x_i)\}$ is a sequence of k-points converging to $\phi(Z)$. By the functoriality property of global height functions, we likewise deduce that $H_L(\phi(x))$ and $H_{\phi^*L}(x)$ agree up to equivalence. Thus, if $d_v(x_i, Z)^\gamma H_{\phi^*L}(x_i)$ is bounded above, the same will be true of $d_v(\phi(x_i), \phi(Z))^\gamma H_L(\phi(x_i))$, and conversely. It follows that $\alpha_Z(\{x_i\}, \phi^*(L)) = \alpha_{\phi(Z)}(\{\phi(x_i)\}, L)$. Since the set of sequences used to define $\alpha_Z(\phi^*(L))$ is in one-to-one correspondence with the set of sequences used to define $\alpha_{\phi(Z)}(L)$, we get $\alpha_{\phi(Z)}(L) = \alpha_Z(\phi^*(L))$.

As for the essential approximation constant, by Proposition 2.3.1, it suffices to verify that a sequence $\{x_i\}$ of k-points on X is Zariski-dense if and only if $\{\phi(x_i)\}$ is Zariski-dense. But since ϕ is an automorphism of X, in particular it is a homeomorphism with respect to the Zariski topology, so that a subset U of X is open if and only if $\phi(U)$ is open. Consequently, the sequence $\{x_i\}$ intersects every nonempty open subset of X if and only if $\{\phi(x_i)\}$ does, which completes the proof. □

We will apply this lemma frequently when $L = \mathcal{O}_{\mathbb{P}^n}(1)$, $X = \mathbb{P}^n_k$, and ϕ is a linear automorphism of $\mathbb{P}^n_k$ defined over k. In such cases, $\phi^*(L)$ is always isomorphic to L, making the result particularly useful.

3.2 The Fundamental Lower Bound

Our next result will be the key tool behind all our computational examples. It is in the spirit of Liouville's theorem from Diophantine approximation, giving a lower bound on the approximation constant with respect to $\mathcal{O}_{\mathbb{P}^n_k}(1)$ for any closed subscheme, depending only on the degrees of the defining equations.

Proposition 3.2.1. *Let L denote the line bundle $\mathcal{O}_{\mathbb{P}^n_k}(1)$ on the projective space $\mathbb{P}^n_k$. Suppose Z is a closed subscheme of $\mathbb{P}^n_k$ defined by the equations*

$$\begin{cases} F_1(x_0, \ldots, x_n) = 0 \\ \vdots \\ F_m(x_0, \ldots, x_n) = 0, \end{cases}$$

where $F_1, \ldots, F_m$ are homogeneous polynomials in $k[x_0, \ldots, x_n]$. If $d_{max} = \max(\deg(F_1), \ldots, \deg(F_m))$, then for any place v of k, we have

$$\alpha_Z(L) \geq \frac{1}{d_{max}}.$$

Furthermore, suppose $\{x_i\}$ is a sequence of k-points converging to Z, and suppose that the sequence eventually lies off of the hypersurfaces $F_\ell = 0, F_{\ell+1} = 0, \ldots, F_m = 0$. If $d = \min(\deg(F_\ell), \ldots, \deg(F_m))$, then

$$\alpha_Z(\{x_i\}, L) \geq \frac{1}{d}.$$

In particular, if $d_{min} = \min(\deg(F_1), \ldots, \deg(F_m))$, then

$$\alpha_Z^{ess}(L) \geq \frac{1}{d_{min}}.$$

Proof. First, we prove that $\alpha_Z(L) \geq \frac{1}{d_{\max}}$ in the case $m = 1$. Here, Z is a divisor D representing a hypersurface $F(x_0, \ldots, x_n) = 0$ in $\mathbb{P}_k^n$. Setting $\deg(F) = d$, we claim that for all points x not lying on D, there is a positive constant M (independent of x) for which

$$d_v(x, D)^{1/d} H_L(x) \geq M. \tag{3.1}$$

From this, $\alpha_D(L) \geq \frac{1}{d}$ will follow directly, since all points in a sequence converging to D lie off of D by definition, and therefore obey the above inequality.

Taking logarithms in equation (3.1), we are reduced to finding a real constant $M_1 = \log M$ such that

$$\frac{1}{d}(-\lambda_{D,v}(x)) + h_L(x) \geq M_1.$$

Rearranging again, we seek a constant M_2 for which

$$\lambda_{D,v}(x) \leq d h_L(x) + M_2.$$

By the local-global property, we know that for all $x \notin \operatorname{Supp} D$, we have

$$h_D(x) = \sum_w \lambda_{D,w}(x) + O(1),$$

with the sum running over all places of k. Furthermore, since D is an effective divisor, we have $\lambda_{D,w}(x) \geq O(1)$ for all places w. Thus we find that

$$h_D(x) \geq \lambda_{D,v}(x) + O(1).$$

Finally, since D is a divisor representing the vanishing of a homogeneous form of degree d, it is linearly equivalent to dL on $\mathbb{P}_k^n$. By the properties of heights, $h_D(x) = h_{dL}(x) + O(1) = d h_L(x) + O(1)$. All in all, we see that

$$d h_L(x) \geq \lambda_{D,v}(x) + O(1).$$

Moving the $O(1)$ term to the other side, we conclude there is a real number M_2 such that

$$dh_L(x) + M_2 \geq \lambda_{D,v}(x),$$

for all $x \notin \operatorname{Supp} D$. We have now proved the first part of the proposition in the case $m = 1$.

Now, we proceed to show that $\alpha_Z(L) \geq \frac{1}{d_{\max}}$ in general. If D_i is the divisor represented by the hypersurface $F_i(x_0, \dots, x_n) = 0$, notice that $Z = \bigcap_{i=1}^m D_i$. It follows immediately from the definition of $d_v(x, Z)$ that for any point $x \in \mathbb{P}^n(k_v)$, we have

$$d_v(x, Z) = \max(d_v(x, D_1), \dots, d_v(x, D_m)).$$

Thus, for any constant $\gamma \geq 0$ and $1 \leq i \leq m$, we have $d_v(x, Z)^\gamma \geq d_v(x, D_i)^\gamma$. Setting $d_i = \deg(F_i)$, the first part of the proof says that there is a positive constant M_i such that for all points x not lying on D_i, we have $d_v(x, D_i)^{1/d_i} H_L(x) \geq M_i$.

Suppose we are given a sequence $\{x_j\} \subseteq \mathbb{P}^n(k)$ converging to Z. Let $M = \min(M_1, \dots, M_m)$, and suppose we take j sufficiently large so that $d_v(x_j, D_i) \leq 1$ for all i. For each x_j in the sequence, there is at least one divisor D_i for which $d_v(x_j, D_i) \neq 0$. Applying the above,

$$\begin{aligned}
d_v(x_j, Z)^{1/d_{\max}} H_L(x_j) &\geq d_v(x_j, D_i)^{1/d_{\max}} H_L(x_j) \\
&\geq d_v(x_j, D_i)^{1/d_i} H_L(x_j) \\
&\geq M_i \\
&\geq M.
\end{aligned}$$

In other words, for j sufficiently large, $d_v(x_j, Z)^{1/d_{\max}} H_L(x_j)$ is bounded below by M, which means the entire sequence $d_v(x_j, Z)^{1/d_{\max}} H_L(x_j)$ is bounded below by a positive constant. Since the sequence $\{x_j\}$ was arbitrary, we conclude that $\alpha_Z(L) \geq \frac{1}{d_{\max}}$.

Now, assume that the sequence $\{x_j\}$ of k-points approximating Z is chosen so that eventually it avoids the supports of the divisors $D_\ell, \dots, D_m$. By the above, we know that for all sufficiently large j, and for $\ell \leq i \leq m$, we have $d_v(x_j, D_i)^{1/d_i} H_L(x_j) \geq M_i$. In particular, setting $M' = \min(M_\ell, \dots, M_m)$,

$$d_v(x_j, Z)^{1/d_i} H_L(x_j) \geq d_v(x_j, D_i)^{1/d_i} H_L(x_j) \geq M',$$

so that $\alpha_Z(\{x_i\}, L) \geq \frac{1}{d_i}$ for $\ell \leq i \leq m$. In particular, $\alpha_Z(\{x_i\}, L) \geq \frac{1}{d}$, where $d = \min(d_\ell, \dots, d_m)$.

Finally, let U be the open set given by $F_1(x_0, \dots, x_n) \neq 0, \dots, F_m(x_0, \dots, x_n) \neq 0$. Applying the above in the case $\ell = 1$, we find that for any sequence of k-points $\{x_i\}$ lying in U and converging to Z, we have $\alpha_Z(\{x_i\}, L) \geq \frac{1}{d_{\min}}$. By definition it follows that $\alpha_Z(U, L) \geq \frac{1}{d_{\min}}$, and then $\alpha_Z^{\mathrm{ess}}(L) \geq \alpha_Z(U, L) \geq \frac{1}{d_{\min}}$ follows immediately. $\square$

3.3 A Necessary Condition for Approximation

Based on the numerous examples that we discuss below, one is led to conjecture that the inequalities in Proposition 3.2.1 are actually equalities, barring the "evident" obstructions.

One of the requirements is that the subscheme Z contains points defined over k_v. If this condition does not hold, the lower bound of Proposition 3.2.1 is extremely far from optimal, as the following theorem shows:

Theorem 3.3.1. *Let X be a projective variety defined over a number field k, and let Z be any closed subscheme of X. If v is a place of k such that $Z(k_v) = \varnothing$, then with respect to the place v and any line bundle L we have*

$$\alpha_Z(L) = \alpha_Z^{ess}(L) = \infty.$$

Proof. To establish our result, it suffices to show that for all sequences $\{x_i\} \subseteq X(k)$, it is *not* true that $d_v(x_i, Z) \to 0$. This will mean that all the sets $A(\{x_i\}, L)$ are empty, so they all have ∞ as their infimum, which forces $\alpha_Z(L) = \alpha_Z^{\text{ess}}(L) = \infty$.

First, we invoke the fact that Z may be written as the scheme-theoretic intersection of finitely many effective divisors $D_1, \ldots, D_r$ on X. Then, by definition, for any point $x \in X(k)$, we may take

$$d_v(x, Z) = \max(d_v(x, D_1), \ldots, d_v(x, D_r)).$$

Now, without loss of generality, assume that $d_v(x_n, D_1) = d_v(x_n, Z)$ for infinitely many positive integers n. We replace the original sequence $\{x_n\}$ with a subsequence for which $d_v(x_n, D_1) = d_v(x_n, Z)$, and we will bound $d_v(x_n, Z)$ away from 0 on this subsequence. This will be enough to conclude that the original sequence $d_v(x_n, Z)$ does not converge to 0. From this point on, we write D for the divisor D_1.

We want to look at the sequence of numbers $d_v(x_n, D)$ and prove it is bounded away from 0. To do this, we write down a formula for $d_v(\cdot, D)$ and observe that it is continuous with respect to the v-adic topology on $X(k_v)$. We use the description of local Weil functions sketched in [21], §1.3, but re-normalized to match our conventions here. One can choose the function so that whenever D has local equation f on some open subset U, we can take

$$\lambda_{D,v}(x) = -\log \|f(x)\|_v + \alpha(x)$$

for all $x \in U(k_v)$ at which $f(x)$ is defined, where α is a v-adically continuous function on $U(k_v)$. In terms of distance functions, this says

$$d_v(x, D) = \exp(-\alpha(x)) \cdot \|f(x)\|_v$$

on $U(k_v)$. In particular, when D is effective, f can be chosen to be a regular function on each open set U, so that $d_v(x, D)$ is defined everywhere on this open set. Since regular functions are v-adically continuous, it follows that $d_v(\cdot, D)$ is continuous on each such open set $U(k_v)$, which may be chosen to form an open cover of $X(k_v)$ in the v-adic topology.

Now, since X is a projective variety, $X(k_v)$ is v-adically compact. The closure $\overline{\{x_n\}}$ of our sequence in the v-adic topology is a v-adically closed subset of $X(k_v)$ (notice all limit points of the sequence are defined over k_v because the metric topology on k_v is complete). As such, $\overline{\{x_n\}}$ is compact in the v-adic topology, so that the continuous function $d_v(\cdot, D)$ attains a minimum value M on $\overline{\{x_n\}}$. We claim that $M \neq 0$. Indeed, if there were a point

$y \in \overline{\{x_n\}}$ for which $d_v(y, D) = 0$, then certainly y is not a member of the sequence. Thus y is a limit of some subsequence of the x_n; in particular, it is defined over k_v. Without loss of generality, we may replace our sequence with this further subsequence. By continuity, for all values of i we get $d_v(y, D_i) = \lim_{n\to\infty} d_v(x_n, D_i) \le \lim_{n\to\infty} d_v(x_n, D_1) = d_v(y, D_1) = 0$, so that $d_v(y, D_i) = 0$ for all i. It follows that $d_v(y, Z) = 0$, so that $y \in Z(k_v)$, a contradiction.

We conclude that $d_v(\cdot, D)$ is bounded below by $M > 0$ on $\overline{\{x_n\}}$, and in particular on the sequence itself. Hence $d_v(x_n, Z)$ does not converge to 0, as we needed to show. □

A refinement on the style of argument in the theorem above allows us to be more precise about the circumstance when there is a sequence $\{x_n\}$ of points in $X(k)$ for which $d_v(x_n, Z) \to 0$. When this happens, we can always find a smaller closed subscheme Z' defined over a finite extension of k, contained in k_v, for which it is also true that $d_v(x_n, Z') \to 0$.

Proposition 3.3.1. *Let X be a projective variety defined over a number field k, let v be a fixed place of k extended in some way to $\overline{k}$, and let Z be a closed subscheme of X (defined over some algebraic extension of k). If there is a sequence of points $\{x_i\}$ in $X(k)$ converging to Z, then there is a closed subscheme Z' contained in Z, defined over a finite extension ℓ/k such that $\ell \subseteq k_v$, for which $d_v(x_i, Z') \to 0$.*

Moreover, given any line bundle L on X, we have $\alpha_Z(L) = \alpha_{Z'}(L)$, and $\alpha_Z^{ess}(L) = \alpha_{Z'}^{ess}(L)$, where all approximation constants are normalized with respect to k.

Proof. First, we let K denote any finite Galois extension of k over which Z is defined. By the primitive element theorem, we have $K = k(\alpha)$ for some algebraic number α. If K_v denotes the completion of K with respect to the topology induced by v, it is easy to verify that $K_v = k_v(\alpha)$.

It immediately follows that K_v is also a Galois extension of k_v. Indeed, since K is a Galois extension of k, the minimal polynomial of α over k splits completely in K. Since the minimal polynomial of α over k_v divides the minimal polynomial of α over k, and K_v contains K, we see that the minimal polynomial of α over k_v also splits completely in K_v. Consequently, $k_v(\alpha) = K_v$ is Galois over k_v.

Now, for each $\sigma \in \mathrm{Gal}(K_v/k_v)$, we consider the closed subscheme Z^σ of X obtained by applying σ to all the coefficients of the equations defining Z. We let

$$Z' = \bigcap_{\sigma \in \mathrm{Gal}(K_v/k_v)} Z^\sigma.$$

By Lemma 2.3.1, the homogeneous ideal of Z' is generated by elements of k_v, and clearly Z' is contained in Z.

Next, given $\sigma \in \mathrm{Gal}(K_v/k_v)$, we consider its restriction to K. Knowing that σ fixes k_v, it also fixes the subfield k. Additionally, the automorphisms $\sigma \in \mathrm{Gal}(K_v/k_v)$ all send the primitive element α to one of its Galois conjugates over K_v, which are also Galois conjugates of α over K. It follows right away that σ restricts to an automorphism of K fixing k.

Knowing that $K_v = k_v(\alpha)$, we can choose a basis for K_v over k_v consisting entirely of powers of α, hence elements of K. Thus the argument of Lemma 2.3.1 shows that the equations for Z' that we select all have coefficients in K as well, so Z' is cut out by equations with coefficients in $\ell := K \cap k_v$. In particular, ℓ is a finite extension of k and also contained in k_v.

The last thing to verify is that $d_v(x_i, Z') \to 0$. First, we observe that $d_v(x_i, Z^\sigma) = d_v(x_i, Z)$ for each $\sigma \in \mathrm{Gal}(K_v/k_v)$. This follows because there is only one extension of $\|\cdot\|_v$ from k_v to K_v up to equivalence (see [15], §2.3.3–2.3.4 for an argument in the non-archimedean case), so that $\|\sigma(\beta)\|_v = \|\beta\|_v$ for each $\beta \in K_v$ and $\sigma \in \mathrm{Gal}(K_v/k_v)$. Note that we can take our distance function $d_v(\cdot, Z')$ to be the maximum of the quantities $d_v(\cdot, Z^\sigma)$ as σ ranges over $\mathrm{Gal}(K_v/k_v)$, because Z' is the intersection of the subschemes Z^σ. Thus, $d_v(x_i, Z') = d_v(x_i, Z) \to 0$. As such, Z' is the subscheme that we seek.

As for the statement about approximation constants, we noted above that $d_v(x_i, Z) = d_v(x_i, Z')$, provided that x_i is defined over k. Hence, a sequence of k-points converges to Z if and only if it converges to Z', and given any such sequence $\{x_i\}$ and any $\gamma \in \mathbb{R}$, we have $d_v(x_i, Z)^\gamma H_L(x_i) = d_v(x_i, Z')^\gamma H_L(x_i)$. It follows immediately that $\alpha_Z(L) = \alpha_{Z'}(L)$ and $\alpha_Z^{\mathrm{ess}}(L) = \alpha_{Z'}^{\mathrm{ess}}(L)$. $\square$

Chapter 4

Computational Examples

4.1 Geometric Generalities

Our next goal is to compute the approximation constants in a variety of different cases. Mostly, our computations will focus on closed subschemes of $\mathbb{P}^n$, using $\mathcal{O}_{\mathbb{P}^n}(1)$ as the line bundle L. In this case, having computed $\alpha_Z(L)$ for a given subscheme Z, a computation of $\alpha_Z(L')$ for any other ample line bundle L' is immediate, since L' must be of the form nL for some integer $n \geq 1$, and then $\alpha_Z(L') = n\alpha_Z(L)$. Thus, at least when working with closed subschemes of $\mathbb{P}^n$, we are justified in dealing exclusively with $\mathcal{O}_{\mathbb{P}^n}(1)$.

Initially, we restrict to the case where $\mathbb{Q}$ is our base number field. We begin with a general result, which will be of great use in many of the examples detailed below. For the remainder of this section, L will always denote the line bundle $\mathcal{O}(1)$ on $\mathbb{P}^n$.

Theorem 4.1.1. *Suppose Z is a closed subscheme of $\mathbb{P}^n$ cut out by the equations*

$$\begin{cases} F_1(x_0, \ldots, x_n) = 0 \\ \vdots \\ F_m(x_0, \ldots, x_n) = 0, \end{cases}$$

with the $F_i \in \mathbb{Z}[x_0, \ldots, x_n]$ homogeneous of degree d_i. Let $d = \max_{1 \leq i \leq m} d_i$, and without loss of generality, assume that the forms $F_1, \ldots, F_j$ have degree d, while $F_{j+1}, \ldots, F_m$ have degree smaller than d. Assume that for some choice of integers $\ell_1, \ldots, \ell_j$, not all zero, the subset V of $\mathbb{P}^{n+1}$ cut out by the equations

$$\begin{cases} F_1(x_0, \ldots, x_n) = \ell_1 t^d \\ F_2(x_0, \ldots, x_n) = \ell_2 t^d \\ \vdots \\ F_j(x_0, \ldots, x_n) = \ell_j t^d \\ F_{j+1}(x_0, \ldots, x_n) = 0 \\ \vdots \\ F_m(x_0, \ldots, x_n) = 0 \end{cases}$$

contains a genus zero curve C_0 defined over $\mathbb{Q}$. Set $t=0$ to be the hyperplane at infinity. If C_0 has exactly one place at infinity and a smooth point integral with respect to $t=0$, then $\alpha_Z(L)=\frac{1}{d}$ for all places of $\mathbb{Q}$. If C_0 has two real quadratic places at infinity and a smooth point integral with respect to the hyperplane at infinity, then $\alpha_Z(L)=\frac{1}{d}$ with respect to the archimedean place of $\mathbb{Q}$.

Proof. The inequality $\alpha_Z(L)\geq\frac{1}{d}$ is immediate from Proposition 3.2.1, so it only remains to show that $\frac{1}{d}$ is also an upper bound on $\alpha_Z(L)$. We will do this by exhibiting a sequence of rational points $y_i\in\mathbb{P}^n(\mathbb{Q})$ for which $d_v(y_i,Z)H_L(y_i)^d$ (equivalently, $d_v(y_i,Z)^{1/d}H_L(y_i)$) is bounded above as $i\to\infty$.

We begin with the archimedean place of $\mathbb{Q}$. For a given point $x\in\mathbb{P}^n(\mathbb{Q})$, we can always normalize so that it has coordinates $(x_0:x_1:\cdots:x_n)$ with $x_0,x_1,\dots,x_n$ relatively prime integers. If we do this, then $H_L(x)=\max(|x_0|,|x_1|,\dots,|x_n|)$. Now, for $1\leq i\leq j$, we let Y_i denote the hypersurface of $\mathbb{P}^n$ defined by $F_i(x_0,\dots,x_n)=0$. Supposing that we choose x such that $F_{j+1}(x)=\cdots=F_m(x)=0$, it follows from the definitions that

$$d_v(x,Z)=\max_{1\leq i\leq j}d_v(x,Y_i)=\frac{\max_{1\leq i\leq j}|F_i(x_0,x_1,\dots,x_n)|}{(\max(|x_0|,|x_1|,\dots,|x_n|))^d}.$$

Consequently, $d_v(x,Z)H_L(x)^d=\max_{1\leq i\leq j}|F_i(x_0,x_1,\dots,x_n)|$. So, provided we select our sequence $\{y_i\}$ to satisfy $F_{j+1}(y_i)=\cdots=F_m(y_i)=0$, asking that $d_v(y_i,Z)H_L(y_i)^d$ is bounded above as $i\to\infty$ with none of the y_i lying on Z is equivalent to asking for infinitely many coprime integer solutions $(x_0,x_1,\dots,x_n)$ to the system of Diophantine equations

$$\begin{cases}F_1(x_0,x_1,\dots,x_n)=\ell_1\\ F_2(x_0,x_1,\dots,x_n)=\ell_2\\ \vdots\\ F_j(x_0,x_1,\dots,x_n)=\ell_j\\ F_{j+1}(x_0,x_1,\dots,x_n)=0\\ \vdots\\ F_m(x_0,x_1,\dots,x_n)=0\end{cases}$$

for some integers $\ell_1,\dots,\ell_j$, not all zero.

In fact, the assumption that $x_0,x_1,\dots,x_n$ are coprime can be dropped. Indeed, if we have infinitely many integer solutions $(x_0,x_1,\dots,x_n)$ to the system of equations above for fixed values of $\ell_1,\dots,\ell_j$, then if $g=\gcd(x_0,x_1,\dots,x_n)$, it is necessary that $g^d\mid\ell_i$ for each i. Thus, g can only take on finitely many values over the infinite family of solutions. In particular, there is an infinite subfamily of solutions for which g is fixed. Replacing the infinitely many solutions $(x_0,x_1,\dots,x_n)$ with $(x_0/g,x_1/g,\dots,x_n/g)$, we get infinitely many coprime integer solutions to the system of equations above, but with $\ell_1,\dots,\ell_j$ replaced by $\ell_1/g^d,\dots,\ell_j/g^d$.

Now, suppose we have fixed values of $\ell_1, \ldots, \ell_j$ such that the closed subscheme $V \subseteq \mathbb{P}^{n+1}$ given by

$$\begin{cases} F_1(x_0, \ldots, x_n) = \ell_1 t^d \\ F_2(x_0, \ldots, x_n) = \ell_2 t^d \\ \vdots \\ F_j(x_0, \ldots, x_n) = \ell_j t^d \\ F_{j+1}(x_0, \ldots, x_n) = 0 \\ \vdots \\ F_m(x_0, \ldots, x_n) = 0 \end{cases}$$

contains a genus zero curve C_0 defined over $\mathbb{Q}$ with a smooth integral point and satisfying either hypothesis on its places at infinity. We invoke the result (as stated in [20]) that such a curve C_0 necessarily contains infinitely many points integral with respect to $t = 0$. Since the curve is contained in V, we immediately deduce the existence of infinitely many integer tuples $(x_0, \ldots, x_n)$ such that $(x_0 : \cdots : x_n : 1)$ lies on V, hence satisfying the required system of equations. Putting everything together, we now conclude that $\alpha_Z(L) = \frac{1}{d}$ with respect to the archimedean place of $\mathbb{Q}$.

Now, we specialize to the case where C_0 has exactly one place at infinity, and prove that $\alpha_Z(L) = \frac{1}{d}$ for all the p-adic absolute values as well. Fixing a prime p, we carry out a refined analysis of the infinite family of integral points that we just obtained. This argument is adapted from part of Lemma 2 in [1].

The existence of a genus 0 curve C_0 inside of V containing an integral (hence rational) point means we can consider the normalization morphism $\phi : \mathbb{P}^1 \to V$ defined over $\mathbb{Q}$ with image C_0. Suppose it is given by $\phi(a : b) = (G_0(a, b) : G_1(a, b) : \cdots : G_n(a, b) : H(a, b))$, where $G_0, G_1, \ldots, G_n, H$ are all homogeneous polynomials in $\mathbb{Z}[a, b]$ with the same degree and no common factors (without loss of generality). Composing with a projective automorphism of $\mathbb{P}^1$ defined over $\mathbb{Q}$, we can assume the coordinates on $\mathbb{P}^1$ are such that $\phi(0 : 1)$ is the smooth integral point on C_0 guaranteed in the hypothesis of the theorem, and $\phi(1 : 0)$ is the unique point at infinity on C_0.

Since $\phi(1 : 0)$ is the only point at infinity, we immediately deduce that $H(1, 0) = 0$ and that $H(a, b) \neq 0$ for all other points $(a : b) \in \mathbb{P}^1(\overline{\mathbb{Q}})$. This is only true if $H(a, b) = Cb^e$ for some integer C, where e denotes the common degree of all the polynomials $G_0, G_1, \ldots, G_n, H$. Furthermore, since $\phi(0 : 1)$ is an integral point on C_0, we deduce that C divides $G_0(0, 1), G_1(0, 1), \ldots, G_n(0, 1)$ in $\mathbb{Z}$. It is then easy to see that C divides $G_0(CN, 1), G_1(CN, 1), \ldots, G_n(CN, 1)$ for any integer N, giving a parametrization of an infinite family of integral points on C_0. Translating back to our original setting, we find that for $(x_0, x_1, \ldots, x_n, t) = (G_0(CN, 1)/C, G_1(CN, 1)/C, \ldots, G_n(CN, 1)/C, 1)$, all the equations of V are satisfied for each choice of integer parameter N. Indeed, the same is true if N is replaced with any rational number.

This leads us to consider the sequence of points $y_i = (G_0(Cp^{-i}, 1)/C : G_1(Cp^{-i}, 1)/C : \cdots : G_n(Cp^{-i}, 1)/C)$, for which we know $|F_r(y_i)|_p = |\ell_r|_p$ for $1 \leq r \leq j$ and $F_r(y_i) = 0$ for $r \geq j + 1$. Now, without loss of generality, assume that $G_0(Ct, 1)/C$ has the largest degree as a polynomial in t out of all polynomials $G_0(Ct,1)/C, G_1(Ct,1)/C, \ldots, G_n(Ct,1)/C$, and suppose this largest degree is e. Furthermore, if more than one of these polynomials is of largest degree, assume that the leading coefficient A of $G_0(Ct,1)/C$ has largest p-adic absolute value. It is easily checked that for sufficiently large i, we have

$$\max(|G_0(Cp^{-i},1)/C|_p, |G_1(Cp^{-i},1)/C|_p, \ldots, |G_n(Cp^{-i},1)/C|_p) = |A|_p \cdot p^{ei},$$

Consequently, we have $d_v(y_i, Z) = \frac{\max_{1\leq r\leq j}|\ell_r|_p}{|A|_p^d \cdot p^{dei}}$.

Finally, to compute $H_L(y_i)$, we multiply through all coordinates of y_i by Cp^{ei}, to make them integers. Then $H_L(y_i)$ is bounded above by the largest (archimedean) absolute value appearing in these new coordinates. But it is easy to see that after the coordinates have been multiplied by Cp^{ei}, all the resulting expressions are integer polynomials in p of degree at most ei. Hence $H_L(y_i)^d/p^{dei}$ converges to some finite constant as $i \to \infty$, which is enough to guarantee that $d_v(y_i, Z)H_L(y_i)^d$ is bounded above as $i \to \infty$. In conclusion, provided C_0 has only one place at infinity, we have shown that $\alpha_Z(L) = \frac{1}{d}$ for all the non-archimedean places of $\mathbb{Q}$. □

Aside from being a great tool for computational examples, Theorem 4.1.1 gives an affirmative answer to the question of whether $\alpha_Z(L)$ can be made arbitrarily close to zero for appropriate choices of Z:

Corollary 4.1.1. *For any $\epsilon > 0$, there exists a curve C in $\mathbb{P}^3$ defined over $\mathbb{Q}$ for which $\alpha_C(L) < \epsilon$, with respect to all places of $\mathbb{Q}$.*

Proof. Given $\epsilon > 0$, choose an integer $n > 0$ such that $\frac{1}{n} < \epsilon$, and consider the curve C defined by the equations

$$\begin{cases} x_0^n + x_1^n - x_2^n = 0 \\ x_3 = 0. \end{cases}$$

The surface $x_0^n + x_1^n - x_2^n = t^n$, $x_3 = 0$ in $\mathbb{P}^4$ with homogeneous coordinates $(x_0 : x_1 : x_2 : x_3 : t)$ contains the projective line defined by the equations $x_0 - t = 0$, $x_3 = 0$, and $x_1 - x_2 = 0$. This is a smooth genus zero curve, and its only intersection with the hyperplane $t = 0$ is the point $(0 : 1 : 1 : 0 : 0)$. Since this curve contains the integral point $(1 : 1 : 1 : 0 : 1)$, we conclude that $\alpha_C(L) = \frac{1}{n} < \epsilon$ for all places of $\mathbb{Q}$ by Theorem 4.1.1. □

Along different lines, Theorem 4.1.1 can be invoked when a certain geometric criterion is satisfied. This new theorem will be an important tool throughout the rest of the chapter.

Theorem 4.1.2. *Let Z be a closed subscheme of $\mathbb{P}^n$ cut out by equations*

$$\begin{cases} F_1(x_0, \ldots, x_n) = 0 \\ \vdots \\ F_m(x_0, \ldots, x_n) = 0, \end{cases}$$

with the $F_i \in \mathbb{Z}[x_0, \ldots, x_n]$ homogeneous of degree d_i. Without loss of generality, suppose we have ordered the polynomials so that $d_1 = d_2 = \cdots = d_j > d_{j+1} \geq \cdots \geq d_m$, and set

$d = d_1$. *Suppose there is a point* $a = (a_0 : \cdots : a_n) \in Z(\mathbb{Q})$ *and a projective line* ℓ *defined over* $\mathbb{Q}$ *intersecting* Z *only at* a*, with multiplicity exactly* d*. In other words, if* $\mathcal{O}_{\ell,a}$ *is the local ring of* ℓ *at* a*, and* I *is the ideal cut out by* Z *in this local ring, the dimension of the quotient* $\mathcal{O}_{\ell,a}/I$ *as a* $\mathbb{Q}$*-vector space is exactly* d*. Then* $\alpha_Z(L) = \frac{1}{d}$ *for all places of* $\mathbb{Q}$*.*

Proof. Since a and the line passing through it are defined over $\mathbb{Q}$, we can apply a linear automorphism of $\mathbb{P}^n$ defined over $\mathbb{Q}$ (which preserves the degrees of the equations cutting out Z), and assume that ℓ is given by $x_2 = \cdots = x_n = 0$. Furthermore, we can arrange that a has projective coordinates $(1 : 0 : 0 : \cdots : 0)$. With this change of coordinates, the local ring $\mathcal{O}_{\ell,a}$ can be identified with $\mathbb{Q}[x_1]_{(x_1)}$, by considering the affine coordinate ring for the affine piece $x_0 \neq 0$ and imposing the conditions that $x_2 = \cdots = x_n = 0$.

The ideal of Z inside this local ring is then generated by $F_1(1, x_1, 0, \ldots, 0), \ldots, F_m(1, x_1, 0, \ldots, 0)$. Since we are now dealing with a polynomial ring in one indeterminate, the ideal generated by these polynomials in $\mathbb{Q}[x_1]$ is the same as that generated by their greatest common divisor $G(x_1) \in \mathbb{Q}[x_1]$. Furthermore, since a is the only point of intersection of ℓ and Z over any field extension of $\mathbb{Q}$, we deduce that $G(x_1) = x_1^e$ for some exponent $e \geq 1$.

Our assumption about the intersection multiplicity means that $\mathbb{Q}[x_1]_{(x_1)}/(x_1^e)$ has dimension d as a $\mathbb{Q}$-vector space. On the other hand, it is easy to see that this quotient ring is e-dimensional as a $\mathbb{Q}$-vector space, with basis $1, x_1, \cdots, x_1^{e-1}$. Therefore, the greatest common divisor of $F_1(1, x_1, 0, \ldots, 0), \ldots, F_m(1, x_1, 0, \ldots, 0)$ is x_1^d.

Notice that for any $i > j$, the polynomial $F_i(1, x_1, 0, \ldots, 0)$ has degree smaller than d, but is divisible by x_1^d, so it must be identically zero. On the other hand, for $1 \leq i \leq j$, $F_i(1, x_1, 0, \ldots, 0)$ has degree at most d and is divisible by x_1^d, so we may write $F_i(1, x_1, 0, \ldots, 0) = b_i x_1^d$ for some integer b_i, which may be zero. However, since x_1^d is indeed the greatest common divisor of these polynomials, some b_i is non-zero. Re-homogenizing, we have $F_i(x_0, x_1, 0, \ldots, 0) = b_i x_1^d$ for $1 \leq i \leq j$ as well.

Now, we consider the subset V of $\mathbb{P}^{n+1}$ with homogeneous coordinates $(x_0 : x_1 : \cdots : x_n : t)$ cut out by the equations

$$\begin{cases} F_1(x_0, \ldots, x_n) = b_1 t^d \\ F_2(x_0, \ldots, x_n) = b_2 t^d \\ \vdots \\ F_j(x_0, \ldots, x_n) = b_j t^d \\ F_{j+1}(x_0, \ldots, x_n) = 0 \\ \vdots \\ F_m(x_0, \ldots, x_n) = 0. \end{cases}$$

From what we said above, the projective line with equations $x_2 = \cdots = x_n = 0$, $x_1 - t = 0$ is contained in V, and the point $(1 : 1 : 0 : \cdots : 0 : 1)$ is an integral point on this line. By Theorem 4.1.1, we deduce that $\alpha_Z(L) = \frac{1}{d}$ for all places of $\mathbb{Q}$. $\square$

4.2 Linear Subvarieties and Beyond

4.2.1 Subschemes Contained in Linear Subvarieties

Arguably, the simplest subvarieties of $\mathbb{P}^n$ are the ones cut out by linear equations, hence isomorphic to $\mathbb{P}^m$ for some $m < n$. As such, these will be among the first computational examples we consider. In fact, we will work in a slightly more general setting, computing essential approximation constants for closed subschemes *contained in* proper linear subvarieties, for *any* base number field k. Our result applies in two cases: when the closed subscheme contains a k-rational point, and when the closed subscheme contains a pair of k_v-points quadratic over k, where v is the place we use to conduct the approximation. In the first case, we will appeal to the proof of Lemma 2.14 of [13], to approximate a fixed k-point along a dense set of k-rational lines. In the second case, we will instead invoke the following lemma to approximate one of the quadratic k_v-points along a dense set of k-rational conics:

Lemma 4.2.1. *Let k be a number field, and suppose we are given two Galois-conjugate points y, y^σ in $\mathbb{P}^n_k$, quadratic over k. Let x be a k-point of $\mathbb{P}^n_k$ not collinear with y and y^σ. Then there is a conic curve defined over k passing through all of y, y^σ, and x, contained in the plane determined by these three points.*

Proof. Any three non-collinear points in $\mathbb{P}^n$ determine a unique plane, so let Y denote the plane determined by y, y^σ, and x. Since $\{y, y^\sigma, x\}$ is a $\mathrm{Gal}(\overline{k}/k)$-invariant set of points, we see that the equations of Y may be defined over k, courtesy of Lemma 2.3.1. Now, select two other k-points x_1, x_2 in Y, such that no three of the five points y, y^σ, x, x_1, x_2 are collinear. Given any five points in a projective plane, there is a (possibly singular) conic in that plane that contains them all, so we choose one. By assuming that no three of our five points are collinear, the conic is forced to be smooth. Indeed, the only other alternative is that the conic factors as a product of two lines, in which case three of the five points are necessarily collinear. Since the collection of five points used to define the conic is $\mathrm{Gal}(\overline{k}/k)$-invariant, we can make a choice of conic with coefficients defined over k. $\square$

In order to ensure that we construct a *dense* sequence, the Hilbert Irreducibility Theorem will be our main tool. The version of this theorem we will use requires us to define *thin sets*. Here, we borrow heavily from the exposition in [18], §9. For any field k of characteristic 0, a subset Ω of $\mathbb{P}^n(k)$ is called *thin* if we can find an algebraic variety X defined over k and a morphism $\pi : X \to \mathbb{P}^n$ such that:

1. $\Omega \subseteq \pi(X(k))$
2. The fibre of π over the generic point is finite and π has no rational section over k.

We will not actually require this formal definition in the arguments that follow; rather, we will be using properties related to thin sets. In particular, the next fact tells us that when k is a number field, thin subsets are small.

Theorem 4.2.1 (Hilbert's Theorem, §9.6, [18])**.** *Every number field k is* Hilbertian*, i.e. for all $n \geq 1$, $\mathbb{P}^n(k)$ is not thin.*

In §9.5 of [18], it is observed that for every Hilbertian field k, the complement of a thin set in $\mathbb{P}^n(k)$ is Zariski dense. It is this fact that features in the argument below.

Now, we are ready to state and prove the promised result on essential approximation constants:

Theorem 4.2.2. *Given a number field k, let Z be a closed subscheme of $\mathbb{P}^n_k$, and let $L = \mathcal{O}_{\mathbb{P}^n}(1)$. Suppose that Z is contained in a proper linear subvariety of $\mathbb{P}^n_k$. We have the following:*

(1) If $Z(k) \neq \varnothing$, then $\alpha_Z^{ess}(L) = 1$ for all places of k.

(2) If Z contains a k_v-point quadratic over k, then $\alpha_Z^{ess}(L) = 1$ with respect to the place v.

Proof. Let Y be a proper linear subvariety of $\mathbb{P}^n_k$ containing Z. By making Y larger if necessary, we can always assume that Y is a hyperplane. By Lemma 3.1.1, we can apply a linear automorphism of $\mathbb{P}^n_k$ and assume that Y is cut out by the equation $x_n = 0$. Without changing the subscheme Z, we can assume that $x_n = 0$ is one of the equations cutting out Z, from which we get $\alpha_Z^{\text{ess}}(L) \geq 1$, courtesy of Proposition 3.2.1.

First, assume we are in case (1), so that $Z(k) \neq \varnothing$. Fix a point $a \in Z(k)$. Given an arbitrary point $b \in \mathbb{P}^n(k) \setminus Y(k)$, we will construct a sequence $\{x_i\}$ of k-points converging to Z for which $\alpha_Z(\{x_i\}, L) = 1$, avoiding Y but lying on the line between b and a. In fact, if the sequence avoids Y, it is enough to verify that $\alpha_Z(\{x_i\}, L) \leq 1$, since $\alpha_Z(\{x_i\}, L) \geq 1$ follows from Proposition 3.2.1 and the fact that Y is cut out by the linear equation $x_n = 0$.

Since the closed point $\{a\}$ is contained in Z, we have $d_v(x_i, a) \geq d_v(x_i, Z)$ for any sequence $\{x_i\}$. Hence, to show $\alpha_Z(\{x_i\}, L) \leq 1$, it suffices to find such a sequence $\{x_i\}$ for which $d_v(x_i, a)H_L(x_i)$ is bounded above. In turn, this is a consequence of the argument of Lemma 2.14 in [13]. In that result, it is shown that the approximation constant $\alpha_a(L)$ is equal to 1 for any point $a \in \mathbb{P}^n(k)$, by approximating a along an arbitrary k-rational line through a. More specifically, a sequence $\{x_n\}$ of k-points is constructed, taken from the given line, with the property that $d_v(x_i, a)H_L(x_i)$ is bounded above as $i \to \infty$.

For each point $b \in \mathbb{P}^n(k) \setminus Y(k)$, the line through a and b is k-rational and intersects Y only at the point a. Thus we can apply the construction above to find the desired sequence of points, lying on the line through a and b, but avoiding Y.

Now, assume instead we are in case (2), and let $a \in Z(k_v)$ be quadratic over k. Then a has a unique Galois conjugate a^σ, different from a and also contained in the linear subvariety Y. Given an arbitrary point $b \in \mathbb{P}^n(k) \setminus Y(k)$, we construct a sequence of k-points $\{x_i\}$ converging to a for which $\alpha_Z(\{x_i\}, L) = 1$, avoiding Y but lying on a conic curve through b and a.

Since b does not lie in Y, it is not collinear with a and a^σ, so Lemma 4.2.1 guarantees the existence of a conic $C_{a,b}$ defined over k, passing through a, a^σ, and b, contained in the plane defined by these points.

Because $C_{a,b}$ is a degree 2 curve, it must intersect Y at only the points a and a^σ, so any sequence $\{x_i\}$ of k-points on $C_{a,b}$ automatically avoids Y. Thus $\alpha_Z(\{x_i\}, L) \geq 1$ automatically holds, by Proposition 3.2.1. Again, it suffices to construct the sequence in such a way that

$$d_v(x_i, Z)H_L(x_i)$$

is bounded above. Knowing that $d_v(x_i, Z) \leq d_v(x_i, a)$, it will be enough to find a sequence where

$$d_v(x_i, a)H_L(x_i)$$

is bounded above. If $\iota : C_{a,b} \hookrightarrow \mathbb{P}^n$ is the given embedding of $C_{a,b}$ into projective space, we know that $H_L(\iota(\cdot))$ is equivalent to $H_{\iota^* L}(\cdot)$. Since $C_{a,b}$ is a degree 2 curve in $\mathbb{P}^n$, we know that $\iota^* L \sim \mathcal{O}(2)$ on $C_{a,b}$, so that $H_L(\iota(\cdot))$ is equivalent to $H_{\mathcal{O}_{C_{a,b}}(1)}(\cdot)^2$. On the other hand, the distance function $d_v(\cdot, a)$ remains the same regardless of whether it is computed in the ambient projective space or restricted to $C_{a,b}$. Hence, we have reduced to proving that on $C_{a,b}$,

$$d_v(y_i, a)^{1/2} H_{\mathcal{O}_{C_{a,b}}(1)}(y_i)$$

is bounded for some sequence $\{y_i\} \in C_{a,b}(k)$.

To finish things off, notice that since $C_{a,b}$ is a smooth genus zero curve with a point defined over k, it is isomorphic to $\mathbb{P}^1$ over k. Let $\pi : \mathbb{P}^1 \to C_{a,b}$ be such an isomorphism. Since $\pi^{-1}(a) \in \mathbb{P}^1(k_v) \setminus \mathbb{P}^1(k)$, a generalized version of Dirichlet's theorem [2] says we can find an infinite sequence of k-points $\{m_i\} \in \mathbb{P}^1(k)$ for which

$$d_v(m_i, \pi^{-1}(a))^{1/2} H_{\mathcal{O}_{\mathbb{P}^1}(1)}(m_i)$$

is bounded above, where everything is computed in $\mathbb{P}^1$. Now, since π is an isomorphism, $H_{\mathcal{O}_{\mathbb{P}^1}(1)}(m_i)$ and $H_{\mathcal{O}_{C_{a,b}}(1)}(\pi(m_i))$ agree up to bounded constants, so we just need to check that the distances $d_v(m_i, \pi^{-1}(a))$ on $\mathbb{P}^1$ and $d_v(\pi(m_i), a)$ on $\mathbb{P}^n$ agree up to bounded constants as well. For this, we first invoke the proof of Proposition 3.1.1, where we showed that our distance function is equivalent to the distance function considered in [13]. Then, Proposition 2.5 of [13] tells us that the functions $d_v(\cdot, \pi^{-1}(a))$ and $d_v(\pi(\cdot), a)$ are equivalent on $C_{a,b}(k_v)$, since they are distances computed with respect to two different embeddings of $C_{a,b}$ in projective space. This means

$$d_v(\pi(m_i), a)^{1/2} H_{\mathcal{O}_{C_{a,b}}(1)}(\pi(m_i))$$

is also bounded as $i \to \infty$. Taking $x_i = \iota \circ \pi(m_i)$ for each i, we have found our desired sequence.

The rest of the argument proceeds identically in case (1) and (2). Because k is a number field, $\mathbb{P}^n(k) \setminus Y(k)$ is a countable set, so we can enumerate the points in it, say $b_1, b_2, b_3, \ldots$. For each point b_j, we take a sequence $\{x_i^{(j)}\}$ converging to Z, satisfying $\alpha_Z(\{x_i^{(j)}\}, L) = 1$, as described above in the respective cases.

Now, fix any $\epsilon > 0$. By construction, for each $j \in \mathbb{N}$, the sequence $d_v(x_i^{(j)}, Z)^{1+\epsilon} H_L(x_i^{(j)})$ converges to 0 as $i \to \infty$. In particular, given any constant $C > 0$, we can replace $\{x_i^{(j)}\}$ with a suitable tail of the sequence for each j to arrange that

$$d_v(x_i^{(j)}, Z)^{1+\epsilon} H_L(x_i^{(j)}) \leq C$$

for *all* positive integers i and j.

The union of the sequences $\{x_i^{(j)}\}$ over all j is a countable set, and therefore we can enumerate the points, say $y_1, y_2, \ldots$. This gives us a new sequence of k-points $\{y_i\}$. Notice that none of these points lies in Y, so *a fortiori* these points do not lie on Z. Furthermore, we know that

$$d_v(y_i, Z)^{1+\epsilon} H_L(y_i) \leq C$$

for all i. Since L is ample, the heights $H_L(y_i)$ are unbounded as $i \to \infty$, and so we must have $d_v(y_i, Z)^{1+\epsilon} \to 0$, from which $d_v(y_i, Z) \to 0$ immediately follows. In other words, $\alpha_Z(\{y_i\}, L) \leq 1 + \epsilon$. Finally, we argue that the sequence $\{y_i\}$ is Zariski dense.

For any positive integer j, our new sequence $\{y_i\}$ contains the sequence $\{x_i^{(j)}\}$ as a subset, and so the Zariski closure of $\{y_i\}$ contains the Zariski closure of $\{x_i^{(j)}\}$, which is either a line or a conic through a and b_j (according to whether we are in case (1) or (2)). In particular, the Zariski closure of $\{y_i\}$ contains each point b_j, and so it contains all the points in $U(k)$, where $U = \mathbb{P}_k^n \setminus Y$.

We now show that $U(k)$ is Zariski dense. First, we invoke Hilbert's theorem (Theorem 4.2.1), which tells us k is Hilbertian. As remarked above, this means the complement of a thin subset in $\mathbb{P}^n(k)$ is Zariski dense. It is a fact that every proper Zariski-closed subset of $\mathbb{P}_k^n$ has a thin set of k-points, and so we deduce immediately that $U(k)$ is Zariski dense. Thus $\{y_i\}$ is a dense sequence.

We have now produced a Zariski-dense sequence $\{y_i\}$ of k-points, converging to Z, for which $\alpha_Z(\{y_i\}, L) \leq 1 + \epsilon$, which implies $\alpha_Z^{\text{ess}}(L) \leq 1 + \epsilon$. But $\epsilon > 0$ was arbitrary, so we conclude that $\alpha_Z^{\text{ess}}(L) \leq 1$. Having already noted that $\alpha_Z^{\text{ess}}(L) \geq 1$, our proof is complete. $\square$

The previous theorem immediately implies something stronger in the case Z is a linear subvariety:

Theorem 4.2.3. *For any number field k, let Z denote the subvariety of $\mathbb{P}_k^n$ cut out by equations*

$$\begin{cases} F_1(x_0, \ldots, x_n) = 0 \\ \vdots \\ F_m(x_0, \ldots, x_n) = 0, \end{cases}$$

where $F_1, \ldots, F_m \in k[x_0, \ldots, x_n]$ are linearly independent linear forms (and $m \leq n$). Then for any place of k, we have $\alpha_Z(L) = \alpha_Z^{ess}(L) = 1$.

Proof. Any subvariety of the type described in the theorem is trivially contained in a proper linear subvariety of $\mathbb{P}_k^n$, namely itself. Since $Z(k)$ is obviously nonempty in this case, we deduce that $\alpha_Z^{\text{ess}}(L) = 1$ for all places of k by Theorem 4.2.2, case (1). Using the inequality $\alpha_Z^{\text{ess}}(L) \geq \alpha_Z(L)$, we get $\alpha_Z(L) \leq 1$ for each place of k. On the other hand, since all equations cutting out Z are linear, Proposition 3.2.1 guarantees that $\alpha_Z(L) \geq 1$, so in fact $\alpha_Z(L) = 1$ for all places of k. $\square$

4.2.2 Subschemes Cut Out by Quadrics

Having dealt with linear subvarieties, we now allow the equations cutting out Z to have degree either 1 or 2. In this case, we restrict to the case where the base field is $\mathbb{Q}$, so that we can utilize Theorem 4.1.2.

Proposition 4.2.1. *Let Z denote an irreducible subscheme of $\mathbb{P}^n_{\mathbb{Q}}$ cut out by the equations*

$$\begin{cases} F_1(x_0,\dots,x_n) = 0 \\ \vdots \\ F_m(x_0,\dots,x_n) = 0, \end{cases}$$

where $F_1,\dots,F_m \in \mathbb{Z}[x_0,\dots,x_n]$ are homogeneous of degree at most 2, and at least one has degree 2. If $Z(\mathbb{Q}) \neq \varnothing$, then $\alpha_Z(L) = \frac{1}{2}$ for all places of $\mathbb{Q}$.

Proof. Choose any point $a \in Z(\mathbb{Q})$ and let T denote the projective tangent space to Z at a. Since a is defined over $\mathbb{Q}$ and the equations for Z are also defined over $\mathbb{Q}$, T is a linear subvariety of $\mathbb{P}^n$ defined over $\mathbb{Q}$. We claim that $T \not\subseteq Z$. Indeed, if a is a singular point of Z, then T has larger dimension than Z. On the other hand, if a is a smooth point of Z, the containment $T \subseteq Z$ would imply $T = Z$ by irreducibility of Z, contradicting our assumption that Z is not a linear subvariety.

Since $T \not\subseteq Z$, there must be a line $\ell \subseteq T$ passing through a, defined over $\mathbb{Q}$ and not contained in Z. As usual, we can compose with a linear automorphism of $\mathbb{P}^n$ defined over $\mathbb{Q}$ to assume that $a = (1 : 0 : \cdots : 0)$, that T is given by $x_{r+1} = x_{r+2} = \cdots = x_n = 0$ for some positive integer r, and that ℓ is given by $x_2 = \cdots = x_n = 0$.

When set up this way, the fact that T is given by the equations just mentioned means $\frac{\partial F_i}{\partial x_j}(1,0,\dots,0) = 0$ for $0 \leq j \leq r$ and all i, as follows from consideration of the Jacobian matrix at the point a. In turn, if F_i is a linear form, this is only possible if F_i depends only on $x_{r+1},\dots,x_n$, which means $F_i(x_0,x_1,0,\dots,0) = 0$ identically. On the other hand, if F_i is quadratic, this can only occur if F_i does not contain any monomials of the form x_0x_j for $0 \leq j \leq r$. In this case, $F_i(x_0,x_1,0,\dots,0) = b_i x_1^2$ for some integer b_i. Since ℓ is not contained in Z, we deduce that $b_i \neq 0$ for at least one value of i.

These facts imply immediately that a is the only point of intersection of ℓ with Z, and that the quotient $\mathcal{O}_{\ell,a}/I$ of the local ring of ℓ at a by the ideal of Z is 2-dimensional as a $\mathbb{Q}$-vector space, with basis elements 1 and x_1/x_0. Appealing to Theorem 4.1.2, we conclude that $\alpha_Z(L) = \frac{1}{2}$ for all places of $\mathbb{Q}$. □

There is one particularly notable family of curves in projective space to which the above proposition can be applied:

Corollary 4.2.1. *Let C denote the rational normal curve of degree $m \geq 2$ in $\mathbb{P}^m$, i.e. the image of $\mathbb{P}^1$ under the mth Veronese embedding $(s : t) \mapsto (s^m : s^{m-1}t : \cdots : st^{m-1} : t^m)$. With respect to all places of $\mathbb{Q}$, we have $\alpha_C(L) = \frac{1}{2}$.*

Proof. It is well-known that every rational normal curve of degree $m \geq 2$ is cut out by quadrics in $\mathbb{P}^m$. Since these curves are irreducible and clearly contain rational points (for instance, $(1 : 0 : 0 : \cdots : 0)$), Proposition 4.2.1 immediately gives us the desired conclusion. $\square$

We wrap up this section with one more example, closely related to the rational normal curves. Consider the quartic curve in $\mathbb{P}^3$ parametrized by the morphism $(s : t) \mapsto (s^4 : s^3t : st^3 : t^4)$. In projective coordinates $(x : y : z : w)$, this curve is cut out by

$$\begin{cases} xw - yz = 0 \\ z^3 - w^2y = 0 \\ y^3 - x^2z = 0. \end{cases}$$

Proposition 4.2.2. *Let C denote the quartic curve in $\mathbb{P}^3$ cut out by the equations above. For all places of $\mathbb{Q}$, we have $\alpha_C(L) = \frac{1}{3}$.*

Proof. It is easy to verify that the tangent line to C at $a = (0 : 0 : 0 : 1)$ is cut out by $x = 0$ and $y = 0$. Computing the scheme-theoretic intersection of C with this tangent line yields the closed subscheme of $\mathbb{P}^1$ in projective coordinates $(z : w)$ cut out by z^3. Thus, if we look at the local ring of $\mathbb{P}^1$ at $(0 : 1)$ and quotient out by the ideal of C in this local ring, we are looking at $\mathbb{Q}[z]_{(z)}/(z^3)$, which is 3-dimensional as a $\mathbb{Q}$-vector space. Since C clearly intersects the tangent line set-theoretically only at a, the conclusion $\alpha_C(L) = \frac{1}{3}$ is immediate from Theorem 4.1.2. $\square$

4.3 Conics in $\mathbb{P}^3$

Taking degree as our measure of complexity, the next most complicated subschemes after the linear ones are the curves of degree 2, i.e. conics. In our discussion, we will embed them in $\mathbb{P}^3$, rather than the apparently more natural choice of the projective plane. In fact, we will often prefer to approximate subschemes of codimension at least 2 throughout this thesis. In cases where the closed subscheme is necessarily contained in a proper subvariety, like a plane, this opens the door to comparing approximations *within* that subvariety to approximations *outside* it. In this section and certain other places, some of the arguments will work in codimension 1 as well with little modification. However, another reason for focusing on subschemes of codimension at least 2 is that the history of Roth's theorem tells us that determining the approximation constant can be very difficult in the codimension 1 case.

To get an idea of what conics in $\mathbb{P}^3$ look like, we will use a lemma that is well-known in the field of algebraic geometry. The substance of the lemma's statement appears as part of Exercise IV.3.4 in Hartshorne's book [7].

Lemma 4.3.1. *Let C be a conic in $\mathbb{P}^3$. Then C is contained in some plane in $\mathbb{P}^3$, and consequently may be given as the intersection of that plane with a quadric surface.*

Thus, we know how to describe the equations of all conics in $\mathbb{P}^3$ exactly, which will aid us computationally. We will fix a base number field k and deal with the case where the linear form and quadratic form are defined over k. Composing with a linear automorphism of $\mathbb{P}^3_k$ (which does not affect the approximation constant, thanks to Lemma 3.1.1), we may assume that our conic is given by the equations $w = 0$ and $F(x, y, z) = 0$, where $F \in k[x, y, z]$ is homogeneous of degree 2 (here, we let $(x : y : z : w)$ denote the projective coordinates on $\mathbb{P}^3$).

4.3.1 Algebraic Preliminaries

Not surprisingly, the behavior of the approximation constant with respect to a place v depends entirely on whether the conic has a point defined over the completion k_v. Our first goal is to show that the existence of k_v-points on the conic implies the existence of k_v-points quadratic over k. In order to do this, we require an auxiliary lemma regarding the subset of k_v for which we can take a square root in k_v. This uses a version of Hensel's lemma, which we state here for convenience. Up to notation, it appears in [4] as Theorem 1.3.1, along with a proof.

Lemma 4.3.2. *Let K be a field complete with respect to a non-archimedean absolute value v, and let $\mathcal{O}_v$ denote the valuation subring of K, consisting of those $a \in K$ such that $|a|_v \leq 1$. Let $f \in \mathcal{O}_v[x]$ be a polynomial, and let $a_0 \in \mathcal{O}_v$ be such that $|f(a_0)|_v < |f'(a_0)|_v^2$. Then there is some $a \in \mathcal{O}_v$ with $f(a) = 0$ and $|a - a_0|_v < |f'(a_0)|_v$.*

Hensel's lemma will help us greatly in dealing with the non-archimedean case of the next result:

Lemma 4.3.3. *Let k be a number field, let v be a place of k, and let S denote the subset of k_v consisting of numbers having a square root in k_v. Then $S \setminus \{0\}$ is open in the v-adic topology on k_v.*

Proof. In the case where v is an archimedean place of k, we either have $k_v = \mathbb{R}$, or $k_v = \mathbb{C}$. In the former case, $S \setminus \{0\}$ is the positive real line, which is open in the ordinary metric topology on $\mathbb{R}$. In the latter case, S is the entire complex plane, so $S \setminus \{0\}$ is the punctured plane, which is also clearly open in the metric topology on $\mathbb{C}$.

Given a non-archimedean absolute value v, we must likewise show that the set of nonzero elements of k_v having a square root in k_v is open. Thus, we take an arbitrary $\alpha \in S \setminus \{0\}$. We know that the valuation subring $\mathcal{O}_v$, given by the closed unit disc in k_v, is a discrete valuation ring. Letting π denote a uniformizer, we may write $\alpha = \pi^n \alpha_0$, where n is an integer and $\alpha_0 \in \mathcal{O}_v^*$. Since α has a square root in k_v, we deduce that n is even and α_0 has a square root (necessarily belonging to $\mathcal{O}_v^*$).

Now, suppose we manage to prove that there is an open ball B contained in $\mathcal{O}_v$ and centered at α_0 for which $B \subseteq S \setminus \{0\}$. Then $\pi^n B$ is an open ball in k_v centered at $\pi^n \alpha_0 = \alpha$, and we claim that $\pi^n B \subseteq S \setminus \{0\}$. Indeed, we observed that n is even, and every element of B has a square root by hypothesis. Thus for any $\pi^n\beta \in \pi^n B$, this element has a square root $\pi^{n/2}\sqrt{\beta}$ in k_v. Hence, our proof is complete as soon as we establish the result for α_0.

We consider the open ball $B = \{\beta \in k_v : |\beta - \alpha_0|_v < |2|_v^2\}$. For any $\beta \in B$, we consider the polynomial $f(x) = x^2 - \beta \in \mathcal{O}_v[x]$. We know that $\sqrt{\alpha_0}$ exists in $\mathcal{O}_v$, and $|f(\sqrt{\alpha_0})|_v = |\alpha_0 - \beta|_v < |2|_v^2$. On the other hand, since $\sqrt{\alpha_0} \in \mathcal{O}_v^*$, we have $|f'(\sqrt{\alpha_0})|_v = |2\sqrt{\alpha_0}|_v = |2|_v \cdot |\sqrt{\alpha_0}|_v = |2|_v$. Thus $|f(\sqrt{\alpha_0})|_v < |f'(\sqrt{\alpha_0})|_v^2$, so that $f(x) = x^2 - \beta$ has a root in $\mathcal{O}_v$ by Lemma 4.3.2. In other words, $\beta \in S$. Finally, $0 \notin B$ since $|\alpha_0|_v = 1 \geq |2|_v^2$, so we conclude that $B \subseteq S \setminus \{0\}$, as desired. □

At this point, we require one more number-theoretic fact:

Lemma 4.3.4. *Let k be a number field and let v be a place of k. For infinitely many rational primes p, $\sqrt{p}$ lies in k_v, but not in k.*

Proof. First, we claim only finitely many rational primes have square roots in k. Since number fields have finite degree, the claim will follow immediately from the fact that for any m distinct rational primes $p_1, \ldots, p_m$, we have $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m}) : \mathbb{Q}] = 2^m$.

To establish that $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m}) : \mathbb{Q}] = 2^m$, we argue based on ramification in these extensions. Certainly, for any fixed prime p, the absolute discriminant of $\mathbb{Q}(\sqrt{p})$ is either p or $4p$, so 2 and p are the only possible ramified primes. Now we appeal to the standard fact that the only primes ramifying in a compositum of two number fields k_1 and k_2 are the primes ramifying in either k_1 or k_2. This is equivalent to Hilbert's Theorem 85 (see [8]), which says that the discriminant of the compositum k_1k_2 is divisible by all and only the rational primes dividing the discriminants of k_1 and k_2.

Applying this result, we see that for $1 \leq i \leq m$, the primes ramifying in $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_i})$ are $p_1, \ldots, p_i$ (and possibly 2), and nothing else. If $2 \in \{p_1, \ldots, p_m\}$, we may assume without loss of generality that $p_1 = 2$. Then, we conclude that $\mathbb{Q}(\sqrt{p_{i+1}}) \not\subseteq \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_i})$ for each i, since p_{i+1} ramifies in $\mathbb{Q}(\sqrt{p_{i+1}})$, but not $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_i})$. We immediately deduce that $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_i}, \sqrt{p_{i+1}}) : \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_i})] = 2$ for each i, from which $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m}) : \mathbb{Q}] = 2^m$ follows.

We conclude that only finitely many rational primes have square roots in k. To finish the proof, we show that *infinitely* many rational primes have square roots in k_v. This is obvious if v is an archimedean place, so we restrict to the non-archimedean case.

Let q denote the characteristic of the residue field of k_v. Notice that infinitely many primes p have a square root in the finite field $\mathbb{F}_q$; indeed, any prime $p \equiv 1 \pmod{q}$ has this property, and by Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many such primes. Consequently, we can apply the traditional form of Hensel's lemma to the polynomials $x^2 - p \in \mathcal{O}_v[x]$, where $\mathcal{O}_v$ denotes the valuation subring of k_v. The residue field of $\mathcal{O}_v$ is a finite extension of $\mathbb{F}_q$, and in particular, $x^2 - p$ splits as a product of distinct linear factors there. By Hensel lifting, $x^2 - p$ has a root in $\mathcal{O}_v$. Altogether, there are infinitely many rational primes p such that $\sqrt{p} \in k_v$.

Since k_v contains the square root of infinitely many rational primes, but k only contains finitely many such square roots, there must be an infinite collection of such rational primes with square roots lying in k_v but not k. □

Now, we can prove that any conic defined over k and possessing a k_v-point necessarily has infinitely many such points with field of definition equal to a quadratic extension of k:

Lemma 4.3.5. *Suppose that C is a conic in the projective plane defined over a number field k, and suppose that C has a k_v-point for some place v of k. Then C has infinitely many k_v-points quadratic over k.*

Proof. The k_v-point on C lies in one of the affine pieces of C, which we restrict to. Hence, we are looking at the set of solutions to an equation

$$ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

with $a, b, c, d, e, f \in k$. We are also given a solution (x_0, y_0) to this equation, with $x_0, y_0 \in k_v$. First, we argue that without loss of generality, we have either $a \neq 0$ or $c \neq 0$. If both coefficients are zero, it is necessary that $b \neq 0$ (since the conic has degree 2), and then the linear automorphism given in this affine piece by $x \mapsto x + y$, $y \mapsto y$ is defined over k and takes our conic to one where $c \neq 0$. By interchanging x and y if necessary, we can just assume that $a \neq 0$.

We treat the affine equation of C as a quadratic equation in x with coefficients in $k[y]$:

$$ax^2 + (by + d)x + (cy^2 + ey + f) = 0.$$

The quadratic formula then allows us to formally write x in terms of y:

$$x = \frac{-(by + d) \pm \sqrt{(by + d)^2 - 4a(cy^2 + ey + f)}}{2a}.$$

In particular, we are told that (x_0, y_0) is a k_v-point, so we find that $(by_0 + d)^2 - 4a(cy_0^2 + ey_0 + f)$ has a square root in k_v.

We now reduce to the case $(by_0 + d)^2 - 4a(cy_0^2 + ey_0 + f) \neq 0$. Indeed, if we have $(by_0 + d)^2 - 4a(cy_0^2 + ey_0 + f) = 0$, then y_0 satisfies a fixed polynomial over k, of degree at most 2, having at most 2 roots. The polynomial is not identically 0, because that would mean the equation for C factors over k, contradicting the irreducibility of the conic. Since $C(k_v) \neq \varnothing$, the conic C is isomorphic to the projective line over k_v, and in particular, has infinitely many k_v-points. Thus we can replace our given point with one where $(by_0 + d)^2 - 4a(cy_0^2 + ey_0 + f) \neq 0$, if necessary.

Hence, we may assume $\alpha = (by_0 + d)^2 - 4a(cy_0^2 + ey_0 + f) \neq 0$, and that α has a square root in k_v. By Lemma 4.3.3, there is some open neighbourhood U of α in k_v for which every element of U is nonzero and has a square root in k_v. Now, notice that $F(y) = (by + d)^2 - 4a(cy^2 + ey + f)$ is a continuous function of y, and therefore $F^{-1}(U)$ is an open neighbourhood of y_0, such that for all $y \in F^{-1}(U)$, $F(y)$ is nonzero and has a square root in k_v.

Since k is dense in its completion k_v, there are infinitely many elements $y_1 \in k \cap F^{-1}(U)$. For each such y_1, we deduce that

$$x_1 := \frac{-(by_1 + d) + \sqrt{(by_1 + d)^2 - 4a(cy_1^2 + ey_1 + f)}}{2a}$$

is defined over a quadratic extension of k contained in k_v. If $x_1 \notin k$ for each choice of y_1, then the points (x_1, y_1) give our desired infinite collection of points on C.

If $x_1 \in k$ for some choice of y_1, then (x_1, y_1) is a k-point on C, which means C is isomorphic to the projective line over k. If there are infinitely many k_v-points quadratic over k on the projective line, the same will be true for C via the isomorphism. By Lemma 4.3.4, there are infinitely many rational primes p such that the projective points $(\sqrt{p} : 1)$ have field of definition contained in k_v, but given by a quadratic extension of k, completing the proof. □

4.3.2 Computing the Approximation Constants

With this lemma in our hands, computing the approximation constant for conics in $\mathbb{P}^3$ with a k_v-point is straightforward.

Proposition 4.3.1. *Let C be a conic defined over a number field k, cut out in $\mathbb{P}^3$ by equations of the form*

$$\begin{cases} F(x, y, z) = 0 \\ w = 0, \end{cases}$$

where $F \in k[x, y, z]$ is homogeneous of degree 2. Let L denote the line bundle $\mathcal{O}_{\mathbb{P}^3}(1)$. If v is a place of k such that $C(k_v) \neq \varnothing$, then

$$\alpha_C(L) = \frac{1}{2}$$

and

$$\alpha_C^{ess}(L) = 1.$$

On the other hand, if $C(k_v) = \varnothing$, then

$$\alpha_C(L) = \alpha_C^{ess}(L) = \infty.$$

Proof. To start, assume $C(k_v) \neq \varnothing$. By Lemma 4.3.5, we may assume C has a k_v-point quadratic over k. Knowing that C is contained in a linear subvariety of $\mathbb{P}^3_k$, Theorem 4.2.2, case (2) implies immediately that $\alpha_C^{\text{ess}}(L) = 1$ with respect to the place v.

To compute the ordinary approximation constant, let $y \in C(k_v)$ be quadratic over k and let K denote the field of definition for y. Now let $\sigma \in \text{Gal}(K/k)$ be the non-trivial automorphism, and let y^σ denote the image of y under σ. Since y is not defined over k, we have $y^\sigma \neq y$. We let ℓ denote the projective line passing through y and y^σ. Since a line is determined by two points on it, and the set $\{y, y^\sigma\}$ is fixed by $\text{Gal}(\overline{k}/k)$, we see that ℓ is defined over k. Notice ℓ intersects C only at y and y^σ, since C has degree 2.

Now, since y is a point in $C(k_v \cap \overline{k})$ not belonging to $C(k)$ but lying on a projective line defined over k, we deduce that $\alpha_y(L) = \frac{1}{2}$ (see [13], p. 515). Finally, since y lies on C and any sequence of k-points approximating y along ℓ is disjoint from C, it follows immediately that $\alpha_C(L) \leq \frac{1}{2}$. The opposite inequality $\alpha_C(L) \geq \frac{1}{2}$ is immediate from Proposition 3.2.1, as usual.

As for the case $C(k_v) = \varnothing$, the desired conclusion $\alpha_C(L) = \alpha_C^{\mathrm{ess}}(L) = \infty$ follows directly from Theorem 3.3.1. $\square$

Now, we give explicit examples of conics illustrating the two alternatives presented in Proposition 4.3.1. Taking $F(x, y, z) = xy - z^2$, the resulting conic contains the rational point $(1 : 1 : 1 : 0)$. Hence $C(\mathbb{Q}_v)$ is nonempty for all places of $\mathbb{Q}$, with the conclusion that $\alpha_C(L) = \frac{1}{2}$ with respect to all places.

On the other hand, taking $F(x, y, z) = x^2 + y^2 + z^2$, the resulting conic has no real points, with the result that $\alpha_C(L) = \infty$ with respect to the archimedean place of $\mathbb{Q}$. But, there are points on C defined over other completions of $\mathbb{Q}$, for instance $\mathbb{Q}_5$, where we could take the point $(1 : i : 0 : 0)$. Here, i is a square root of -1, as usual. This tells us $\alpha_C(L) = \frac{1}{2}$ with respect to the 5-adic absolute value on $\mathbb{Q}$. Notice this is the first example presented so far where the approximation constant for the same curve and the same line bundle changes depending on the place used.

4.3.3 An Alternative Construction

Before leaving conics behind, we provide a counterpart to Proposition 4.3.1, at least in the case $k = \mathbb{Q}$. To be specific, if a conic C defined over $\mathbb{Q}$ has $\mathbb{Q}_v$-points, we provide a number-theoretic construction of a sequence $\{x_i\} \in \mathbb{P}^3(\mathbb{Q})$ not lying in the plane containing C, with $\alpha_C(\{x_i\}, L) = 1$. While the statement in the proposition is superseded by Proposition 4.3.1 and the geometric construction of Theorem 4.2.2 implicitly used in the result, the construction of the sequence below is different in nature and possibly of independent interest.

Proposition 4.3.2. *Let C be a conic defined over $\mathbb{Q}$, cut out in $\mathbb{P}^3$ by equations*

$$\begin{cases} F(x, y, z) = 0 \\ w = 0, \end{cases}$$

where $F \in \mathbb{Z}[x, y, z]$ is homogeneous of degree 2. Let Y denote the plane $w = 0$. If v is a place of $\mathbb{Q}$ such that $C(\mathbb{Q}_v) \neq \varnothing$, there is a sequence $\{x_i\} \in \mathbb{P}^3(\mathbb{Q})$, avoiding Y and converging to C for which

$$\alpha_C(\{x_i\}, L) = 1.$$

Proof. As usual, the lower bound $\alpha_C(\{x_i\}, L) \geq 1$ will follow immediately from Proposition 3.2.1, since the sequence we will be constructing avoids the linear subvariety Y. To construct an approximating sequence, we first deal with the case where v is associated to the p-adic absolute value for some prime p. Since $C(\mathbb{Q}_v) = C(\mathbb{Q}_p) \neq \varnothing$, we choose a point in $C(\mathbb{Q}_p)$, say $(\alpha_0 : \alpha_1 : \alpha_2 : 0)$, with $\alpha_0, \alpha_1, \alpha_2 \in \mathbb{Q}_p$. Multiplying all coordinates by a suitable power of p, we can arrange that $\alpha_0, \alpha_1, \alpha_2 \in \mathbb{Z}_p$, and in fact that $\alpha_i \in \mathbb{Z}_p^*$ for some i.

Now we write out the p-adic expansions:

$$\alpha_0 = \sum_{i=0}^{\infty} a_i p^i$$
$$\alpha_1 = \sum_{i=0}^{\infty} b_i p^i$$
$$\alpha_2 = \sum_{i=0}^{\infty} c_i p^i,$$

with $a_i, b_i, c_i \in \{0, 1, \ldots, p-1\}$ for each i. For a given integer $n \geq 1$, define $\alpha_{0,n} := \sum_{i=0}^{n-1} a_i p^i$, and define $\alpha_{1,n}$ and $\alpha_{2,n}$ analogously. Notice that for each n, $\alpha_{i,n}$ is an integer between 0 and $p^n - 1$. For each $n \geq 1$, we define the projective point $x_n = (\alpha_{0,n} : \alpha_{1,n} : \alpha_{2,n} : p^n)$. Our claim is that $\alpha_C(\{x_i\}, L) = 1$, for which it suffices to show that the sequence $d_v(x_n, C)H_L(x_n)$ is bounded above.

Because $\alpha_{i,n}$ is coprime to p for some fixed i and all $n \geq 1$, while each $\alpha_{i,n}$ is an integer, we find that $\max(|\alpha_{0,n}|_p, |\alpha_{1,n}|_p, |\alpha_{2,n}|_p, |p^n|_p) = 1$. Consequently, we compute directly that

$$d_v(x_n, Y) = \frac{|p^n|_p}{1} = \frac{1}{p^n}.$$

Likewise, letting Q denote the quadric surface $F(x, y, z) = 0$ containing C, we get

$$d_v(x_n, Q) = \frac{|F(\alpha_{0,n}, \alpha_{1,n}, \alpha_{2,n})|_p}{1^2} = |F(\alpha_{0,n}, \alpha_{1,n}, \alpha_{2,n})|_p.$$

To estimate this latter absolute value for a given n, we use the residue map $\mathrm{res}_{p^n} : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$. By construction, we know that $\mathrm{res}_{p^n}(\alpha_i) = \mathrm{res}_{p^n}(\alpha_{i,n})$. In particular, applying res_{p^n} to the known relation $F(\alpha_0, \alpha_1, \alpha_2) = 0$, we see that $F(\alpha_{0,n}, \alpha_{1,n}, \alpha_{2,n}) \equiv 0 \pmod{p^n}$, so that $|F(\alpha_{0,n}, \alpha_{1,n}, \alpha_{2,n})|_p \leq \frac{1}{p^n}$.

In summary, $d_v(x_n, Q) \leq \frac{1}{p^n}$. Putting these two computations together, we find that

$$d_v(x_n, C) = \max(d_v(x_n, Y), d_v(x_n, Q)) = \frac{1}{p^n}.$$

Finally, we compute the height of the point x_n with respect to L. By definition, we have

$$H_L(x_n) = \prod_w \max(|\alpha_{0,n}|_w, |\alpha_{1,n}|_w, |\alpha_{2,n}|_w, |p^n|_w),$$

where the product runs over all places of $\mathbb{Q}$. Since the coordinates of x_n are relatively prime integers by construction, all terms in the product corresponding to non-archimedean absolute values are equal to 1, and we are left with

$$H_L(x_n) = \max(|\alpha_{0,n}|, |\alpha_{1,n}|, |\alpha_{2,n}|, |p^n|),$$

where the absolute value is the archimedean one. By construction, $\alpha_{0,n}, \alpha_{1,n}, \alpha_{2,n}$ are nonnegative integers smaller than p^n, so we get $H_L(x_n) = p^n$. In conclusion,

$$d_v(x_n, C)H_L(x_n) = \frac{1}{p^n} \cdot p^n = 1,$$

which is bounded as $n \to \infty$. We deduce that $\alpha_C(\{x_i\}, L) \leq 1$, and the proof is complete in this case.

Now, the only case remaining is when v is the archimedean place of $\mathbb{Q}$ and C has a real point. For convenience, we consider two sub-cases: either C has a rational point, or it does not. If $C(\mathbb{Q}) \neq \varnothing$, then let $(\alpha_0 : \alpha_1 : \alpha_2 : 0)$ be a rational point on the conic, and without loss of generality, suppose that $\alpha_2 \neq 0$, so that we can scale coordinates such that $(\alpha_0 : \alpha_1 : 1 : 0)$ is a rational point on C. Applying the automorphism of $\mathbb{P}^3$ fixing z, w and replacing x and y with $x - \alpha_0 z$ and $y - \alpha_1 z$ in homogeneous coordinates, we can assume that $(0 : 0 : 1 : 0)$ is a rational point on C.

In this case, it is easy to produce an approximating sequence with the desired properties. Indeed, we let $x_n = (0 : 0 : n : 1)$. Notice that

$$d_v(x_n, Y) = \frac{1}{n},$$

while

$$d_v(x_n, Q) = \frac{|F(0, 0, n)|}{n^2} = 0,$$

because $F(0, 0, n) = n^2 F(0, 0, 1) = 0$ by homogeneity of F. Since $H_L(x_n) = n$, we get $d_v(x_n, C)H_L(x_n) = 1$, which is bounded as $n \to \infty$. Hence $\alpha_C(\{x_i\}, L) \leq 1$, and we are finished in this case as well.

Thus, it remains to consider the case where C has a real point, but no rational point. By Lemma 4.3.5, C has a point defined over a real quadratic extension of $\mathbb{Q}$. In fact, making the change of coordinates in the lemma and following the proof in the case $C(\mathbb{Q}) = \varnothing$, we see that this point can be taken to be of the form $(\alpha_0 : \alpha_1 : 1 : 0)$, where α_0 is a real quadratic irrational and $\alpha_1 \in \mathbb{Q}$.

For each positive integer n, we let $\frac{p_n}{q_n}$ be the nth convergent of the continued fraction expansion of α_0. As is well-known, these convergents are good approximations to α_0; in fact we have

$$\left| \frac{p_n}{q_n} - \alpha_0 \right| \leq \frac{1}{q_n^2}$$

for each $n \geq 1$. We consider the sequence of projective points $x_n = \left(\frac{p_n}{q_n} : \alpha_1 : 1 : \frac{1}{q_n} \right)$, all defined over $\mathbb{Q}$ and not lying on Y. Since $|p_n| \geq 1$ for all n, we know that $\left| \frac{p_n}{q_n} \right| \geq \frac{1}{q_n}$. Consequently, we have

$$d_v(x_n, Y) = \frac{1/q_n}{\max(|p_n/q_n|, |\alpha_1|, 1)}.$$

Analogously, we find that

$$d_v(x_n, Q) = \frac{|F(p_n/q_n, \alpha_1, 1)|}{\max(|p_n/q_n|, |\alpha_1|, 1)^2}.$$

To estimate the numerator, we use the fact that we can write

$$F(x, y, z) = ax^2 + bxy + cy^2 + dxz + eyz + fz^2$$

for some $a, b, c, d, e, f \in \mathbb{Z}$. Using this, along with $F(\alpha_0, \alpha_1, 1) = 0$, we explicitly compute

$$\begin{aligned}
|F(p_n/q_n, \alpha_1, 1)| &= |F(p_n/q_n, \alpha_1, 1) - F(\alpha_0, \alpha_1, 1)| \\
&= |a(p_n^2/q_n^2 - \alpha_0^2) + b(p_n/q_n - \alpha_0)\alpha_1 + d(p_n/q_n - \alpha_0)| \\
&= |p_n/q_n - \alpha_0| \cdot |a(p_n/q_n + \alpha_0) + b\alpha_1 + d| \\
&\le \frac{1}{q_n^2} \cdot |a(p_n/q_n + \alpha_0) + b\alpha_1 + d| \\
&\le \frac{|a||p_n/q_n + \alpha_0| + |b\alpha_1| + |d|}{q_n^2}.
\end{aligned}$$

Now, since $p_n/q_n \to \alpha_0$ as $n \to \infty$, the sequence $|p_n/q_n + \alpha_0|$ is bounded above, so there is some absolute constant $M > 1$ such that for all $n \ge 1$, we have

$$|F(p_n/q_n, \alpha_1, 1)| \le \frac{M}{q_n^2}.$$

In turn,

$$d_v(x_n, Q) \le \frac{M/q_n^2}{\max(|p_n/q_n|, |\alpha_1|, 1)^2}.$$

It only remains to show that $d_v(x_n, C)H_L(x_n)$ is bounded as $n \to \infty$. For this, we write $\alpha_1 = \frac{a}{b}$ for some coprime integers a and b. The projective point x_n may also be written $x_n = (bp_n : aq_n : bq_n : b)$, and the absolute value of all coordinates of this point with respect to non-archimedean places is at most 1. In particular, since p_n and q_n have archimedean absolute value at least 1, $H_L(x_n) \le \max(|bp_n|, |aq_n|, |bq_n|) \le M_1 \max(|p_n|, |q_n|)$, where $M_1 = \max(|a|, |b|)$.

To show that $d_v(x_n, C)H_L(x_n)$ is bounded, we will prove that $d_v(x_n, Y)H_L(x_n)$ and $d_v(x_n, Q)H_L(x_n)$ are both bounded.

First, we have

$$d_v(x_n, Y)H_L(x_n) \le \frac{M_1 \max(|p_n|, |q_n|)/q_n}{\max(|p_n/q_n|, |\alpha_1|, 1)} = \frac{M_1 \max(|p_n|, |q_n|)}{\max(|p_n|, |q_n\alpha_1|, |q_n|)} \le M_1,$$

so this sequence is bounded. Likewise,

$$\begin{aligned}
d_v(x_n, Q)H_L(x_n) &\le \frac{(M/q_n^2) \cdot (M_1 \max(|p_n|, |q_n|))}{\max(|p_n/q_n|^2, |\alpha_1|^2, 1)} \\
&= \frac{MM_1 \max(|p_n|, |q_n|)}{\max(|p_n|^2, |q_n\alpha_1|^2, |q_n|^2)} \\
&\le MM_1,
\end{aligned}$$

proving that this sequence is bounded as well. All in all, we certainly have $d_v(x_n, C)H_L(x_n) \le MM_1$ for all $n \ge 1$, so that $\alpha_C(\{x_i\}, L) \le 1$. This completes the proof in the final case. $\square$

4.4 Cubic Curves in $\mathbb{P}^3$

Having discussed curves of degree 2 in $\mathbb{P}^3$, we increase the degree once again and investigate cubic curves. Already, we will see that computing the exact approximation constants seems difficult in certain cases.

As usual, let L denote the line bundle $\mathcal{O}_{\mathbb{P}^3}(1)$ throughout this section. In parallel with the previous section, we begin with a structural result that narrows down the types of equations we must consider. The conclusion of the lemma in the smooth case appears as part of Exercise IV.3.4 in [7], and in the singular case, one can use an intersection-theoretic argument, with the help of a result such as Proposition 7.2 of [5], to establish the conclusion.

Lemma 4.4.1. *Every cubic curve in $\mathbb{P}^3$ is either contained in some plane of $\mathbb{P}^3$ or is the twisted cubic curve, up to linear automorphism.*

Therefore, we have essentially two types of cubic curves to discuss, and we treat each in turn.

4.4.1 Approximating the Twisted Cubic

The computation of the approximation constant for the twisted cubic follows directly from Corollary 4.2.1, because the twisted cubic curve is the rational normal curve of degree 3 in $\mathbb{P}^3$. Applying this result, we find that the approximation constant is $\frac{1}{2}$ for all places of $\mathbb{Q}$. On the other hand, the twisted cubic curve is *not* contained in a plane, so we cannot apply Theorem 4.2.2 to compute the essential approximation constant.

As such, a different argument is required. In outline, our strategy is to locate a Zariski-dense set of secant lines to the curve, such that approximating the curve along any one of these secant lines yields an approximation constant of $\frac{1}{2}$. Splicing together the sequences for each line into a Zariski-dense sequence will allow us to prove that the essential approximation constant is $\frac{1}{2}$ as well.

First, we prove a pair of computational lemmas that allow us to take a point in $\mathbb{P}^3(\mathbb{Q})$ not lying on the twisted cubic, and identify which secant line this point lies on. Before stating the first lemma, we recall that the twisted cubic curve may be described as the image of $\mathbb{P}^1$ under the embedding $(s : t) \mapsto (s^3 : s^2t : st^2 : t^3)$. Thus, all $\overline{\mathbb{Q}}$-points on this curve except $(1 : 0 : 0 : 0)$ are of the form $(\alpha^3 : \alpha^2 : \alpha : 1)$ for some $\alpha \in \overline{\mathbb{Q}}$.

Lemma 4.4.2. *Let C be the twisted cubic curve in $\mathbb{P}^3$, cut out by the equations*

$$\begin{cases} xw - yz = 0 \\ y^2 - xz = 0 \\ z^2 - yw = 0 \end{cases}$$

in projective coordinates $(x : y : z : w)$. *Fix two distinct points* $(\alpha^3 : \alpha^2 : \alpha : 1)$ *and* $(\beta^3 : \beta^2 : \beta : 1)$ *on* C, *where* $\alpha, \beta \in \overline{\mathbb{Q}} \setminus \{0\}$. *A point* $(a_0 : a_1 : a_2 : a_3) \in \mathbb{P}^3(\mathbb{Q}) \setminus C(\mathbb{Q})$ *is on the secant line through these points if and only if*

$$\det \begin{bmatrix} a_0 & a_1 & a_2 \\ \alpha^2 & \alpha & 1 \\ \beta^2 & \beta & 1 \end{bmatrix} = 0$$

and

$$\det \begin{bmatrix} a_1 & a_2 & a_3 \\ \alpha^2 & \alpha & 1 \\ \beta^2 & \beta & 1 \end{bmatrix} = 0.$$

Proof. Almost by definition, the point $(a_0 : a_1 : a_2 : a_3)$ is on the secant line through $(\alpha^3 : \alpha^2 : \alpha : 1)$ and $(\beta^3 : \beta^2 : \beta : 1)$ if and only if the vector (a_0, a_1, a_2, a_3) is in the linear span of $(\alpha^3, \alpha^2, \alpha, 1)$ and $(\beta^3, \beta^2, \beta, 1)$. Since $(\alpha^3, \alpha^2, \alpha, 1)$ and $(\beta^3, \beta^2, \beta, 1)$ are linearly independent, this holds if and only if the matrix

$$\begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ \alpha^3 & \alpha^2 & \alpha & 1 \\ \beta^3 & \beta^2 & \beta & 1 \end{bmatrix}$$

has rank 2. In turn, this is equivalent to the vanishing of all 3×3 minors of this matrix. We claim, in fact, that this is equivalent to the vanishing of just two minors:

$$\det \begin{bmatrix} a_0 & a_1 & a_2 \\ \alpha^3 & \alpha^2 & \alpha \\ \beta^3 & \beta^2 & \beta \end{bmatrix}$$

and

$$\det \begin{bmatrix} a_1 & a_2 & a_3 \\ \alpha^2 & \alpha & 1 \\ \beta^2 & \beta & 1 \end{bmatrix}.$$

Certainly, if all the 3×3 minors vanish, then these two vanish in particular. Conversely, if the two indicated determinants vanish, then on account of the linear independence of $(\alpha^2, \alpha, 1)$ and $(\beta^2, \beta, 1)$, as well as $(\alpha^3, \alpha^2, \alpha)$ and $(\beta^3, \beta^2, \beta)$, we know there must be scalars $\lambda_{11}, \lambda_{12}, \lambda_{21}, \lambda_{22}$ for which

$$(a_1, a_2, a_3) = \lambda_{11}(\alpha^2, \alpha, 1) + \lambda_{12}(\beta^2, \beta, 1)$$
$$(a_0, a_1, a_2) = \lambda_{21}(\alpha^3, \alpha^2, \alpha) + \lambda_{22}(\beta^3, \beta^2, \beta).$$

In particular, from the above we deduce that

$$\begin{cases} a_2 = \lambda_{11}\alpha + \lambda_{12}\beta = \lambda_{21}\alpha + \lambda_{22}\beta \\ a_1 = \lambda_{11}\alpha^2 + \lambda_{12}\beta^2 = \lambda_{21}\alpha^2 + \lambda_{22}\beta^2. \end{cases}$$

This gives us the matrix equation

$$\begin{bmatrix} \alpha & \beta \\ \alpha^2 & \beta^2 \end{bmatrix} \begin{bmatrix} \lambda_{11} \\ \lambda_{12} \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \alpha^2 & \beta^2 \end{bmatrix} \begin{bmatrix} \lambda_{21} \\ \lambda_{22} \end{bmatrix}.$$

Finally, the 2×2 matrix appearing on both sides of the equation is invertible, since its determinant is $\alpha\beta(\beta - \alpha) \neq 0$, so we deduce that $\lambda_{11} = \lambda_{21}$ and $\lambda_{12} = \lambda_{22}$. In turn, this means

$$(a_0, a_1, a_2, a_3) = \lambda_{11}(\alpha^3, \alpha^2, \alpha, 1) + \lambda_{12}(\beta^3, \beta^2, \beta, 1),$$

so that the other 3×3 minors of the matrix

$$\begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ \alpha^3 & \alpha^2 & \alpha & 1 \\ \beta^3 & \beta^2 & \beta & 1 \end{bmatrix}$$

vanish as well. In summary, the projective point $(a_0 : a_1 : a_2 : a_3)$ is on the secant line through $(\alpha^3 : \alpha^2 : \alpha : 1)$ and $(\beta^3 : \beta^2 : \beta : 1)$ if and only if

$$\det \begin{bmatrix} a_0 & a_1 & a_2 \\ \alpha^3 & \alpha^2 & \alpha \\ \beta^3 & \beta^2 & \beta \end{bmatrix} = 0$$

and

$$\det \begin{bmatrix} a_1 & a_2 & a_3 \\ \alpha^2 & \alpha & 1 \\ \beta^2 & \beta & 1 \end{bmatrix} = 0.$$

Since $\alpha, \beta \neq 0$, we may pull out common factors in the rows of the first determinant, so that the first condition is the same as

$$\det \begin{bmatrix} a_0 & a_1 & a_2 \\ \alpha^2 & \alpha & 1 \\ \beta^2 & \beta & 1 \end{bmatrix} = 0.$$

This completes the proof. □

Turning things around, we will now start with a given point $(a_0 : a_1 : a_2 : a_3) \in \mathbb{P}^3(\mathbb{Q})$ satisfying some mild assumptions, and identify points on the twisted cubic curve whose secant lines pass through the given point.

Lemma 4.4.3. *Let $(a_0 : a_1 : a_2 : a_3) \in \mathbb{P}^3(\mathbb{Q})$ be a point satisfying $a_1a_3 - a_2^2 \neq 0$, $a_0a_2 - a_1^2 \neq 0$ and $(a_1a_2 - a_0a_3)^2 - 4(a_1a_3 - a_2^2)(a_0a_2 - a_1^2) \neq 0$. If α is a root of the quadratic equation*

$$\det \begin{bmatrix} X^2 & X & 1 \\ a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \end{bmatrix} = 0,$$

or equivalently,

$$(a_1a_3 - a_2^2)X^2 + (a_1a_2 - a_0a_3)X + (a_0a_2 - a_1^2) = 0,$$

then $(a_0 : a_1 : a_2 : a_3)$ is on a secant line to C passing through the point $(\alpha^3 : \alpha^2 : \alpha : 1)$.

Proof. First, note that our assumptions on the coordinates a_0, a_1, a_2, a_3 in this lemma are there to make sure the leading coefficient of the quadratic equation is nonzero, and that the equation has two distinct roots, neither of which is 0.

Thus, suppose α is a root of the quadratic equation given in the lemma, and let β denote the other root. In particular, we know that

$$\det \begin{bmatrix} \alpha^2 & \alpha & 1 \\ a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \end{bmatrix} = 0$$

and

$$\det \begin{bmatrix} \beta^2 & \beta & 1 \\ a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \end{bmatrix} = 0.$$

Since $(a_0 : a_1 : a_2 : a_3)$ is not a point on the twisted cubic (for instance, $a_1 a_3 - a_2^2 \neq 0$), it is readily verified that (a_0, a_1, a_2) and (a_1, a_2, a_3) must be linearly independent vectors. Therefore, the determinant conditions say that both the vectors $(\alpha^2, \alpha, 1)$ and $(\beta^2, \beta, 1)$ are in the span of (a_0, a_1, a_2) and (a_1, a_2, a_3). Consequently, the matrix

$$\begin{bmatrix} \alpha^2 & \alpha & 1 \\ \beta^2 & \beta & 1 \\ a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \end{bmatrix}$$

has rank 2 as well, with row space spanned by (a_0, a_1, a_2) and (a_1, a_2, a_3). We deduce that the 3×3 minors of this matrix vanish, so that

$$\det \begin{bmatrix} a_0 & a_1 & a_2 \\ \alpha^2 & \alpha & 1 \\ \beta^2 & \beta & 1 \end{bmatrix} = \det \begin{bmatrix} a_1 & a_2 & a_3 \\ \alpha^2 & \alpha & 1 \\ \beta^2 & \beta & 1 \end{bmatrix} = 0.$$

By Lemma 4.4.2, this tells us $(a_0 : a_1 : a_2 : a_3)$ is on the secant line to C through $(\alpha^3 : \alpha^2 : \alpha : 1)$ and $(\beta^3 : \beta^2 : \beta : 1)$, as required. □

With the help of Lemma 4.4.3, we are in a position to construct a Zariski-dense set of secant lines to the twisted cubic, along which we will conduct our approximation. Our final lemma will be the key in verifying that the collection of secant lines we construct is indeed Zariski-dense.

Lemma 4.4.4. *For any fixed integer D, the surface S cut out by*

$$(yz - xw)^2 - 4(yw - z^2)(xz - y^2) - Dx^4 = 0$$

in $\mathbb{P}^3_{\mathbb{Q}}$ has a Zariski-dense set of $\mathbb{Q}$-points.

Proof. Let U be a nonempty open subset of S. We must prove that U contains at least one $\mathbb{Q}$-point. Notice that U must intersect at least one of the infinitely many hyperplane sections of S obtained by intersecting with $x = by + cz$ as b, c range over $\mathbb{Q}$. We will show that each such hyperplane section of S is a curve with infinitely many $\mathbb{Q}$-points. Having done this, the intersection of U with one of the hyperplane sections will be a nonempty open subset of the corresponding curve, hence must contain a $\mathbb{Q}$-point of S.

Expanding the equation of S yields

$$y^2z^2 - 2xyzw + x^2w^2 - 4xyzw + 4xz^3 + 4y^3w - 4y^2z^2 - Dx^4 = 0,$$

or more simply,

$$-3y^2z^2 - 6xyzw + x^2w^2 + 4xz^3 + 4y^3w - Dx^4 = 0.$$

Consequently, if we intersect S with $x = by + cz$ and restrict our attention to the projective plane in coordinates y, z, w, we are looking at

$$-3y^2z^2 - 6(by + cz)yzw + (by + cz)^2w^2 + 4(by + cz)z^3 + 4y^3w - D(by + cz)^4 = 0.$$

Since $x = by + cz$ with $b, c \in \mathbb{Q}$, if this quartic curve in the projective plane has infinitely many rational points, then the hyperplane section does too. One immediately checks that $(y : z : w) = (0 : 0 : 1)$ is a singular point on this curve. If this hyperplane section is not irreducible, this singular point is either at the intersection of two components, or it is a singular point of just one component (necessarily of smaller degree). In the former case, since at most one irreducible component of this curve is not a line or conic, the rational point $(0 : 0 : 1)$ lies on some line or conic, which is then isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$. In such a case, this hyperplane section automatically admits infinitely many $\mathbb{Q}$-points.

The only remaining cases to investigate are when the plane curve is an irreducible quartic with singular point $(0 : 0 : 1)$, or else that there is a unique cubic component with singular point $(0 : 0 : 1)$. Either way, the unique component containing this singular point must have geometric genus 0. Consequently, the normalization of that component is isomorphic to the projective line. Provided this normalization has a $\mathbb{Q}$-point, it will have infinitely many such points.

We restrict our attention to the affine piece $w \neq 0$, which results in the de-homogenized equation

$$-3y^2z^2 - 6(by + cz)yz + (by + cz)^2 + 4(by + cz)z^3 + 4y^3 - D(by + cz)^4 = 0.$$

Looking at the tangent cone to this curve at the singular point $(0, 0)$, we see it is given by $(by + cz)^2 = 0$, which tells us the singular point is a cusp. Since we have chosen $b, c \in \mathbb{Q}$, the cusp may be approached along a line with rational slope. Since we can normalize the curve by blowing up the projective plane at $(y : z : w) = (0 : 0 : 1)$, we see that the place over this cusp is rational, so that the normalization of the component containing $(0 : 0 : 1)$ has a rational point and is isomorphic to the projective line. This means the normalized curve has infinitely many points defined over $\mathbb{Q}$. Since the blow-up map is an isomorphism away from the single point $(0 : 0 : 1)$ in the projective plane, the original curve also has infinitely many rational points, as desired. $\square$

At last, we are ready to put all these pieces together to compute the essential approximation constant for the twisted cubic curve.

Proposition 4.4.1. *Let C be the twisted cubic curve in $\mathbb{P}^3$, cut out by the equations*

$$\begin{cases} xw - yz = 0 \\ y^2 - xz = 0 \\ z^2 - yw = 0 \end{cases}$$

in projective coordinates $(x : y : z : w)$. Then $\alpha_C^{ess}(L) = \frac{1}{2}$ for all places of $\mathbb{Q}$.

Proof. Since C is cut out entirely by equations of degree 2, Proposition 3.2.1 says that $\alpha_C^{\mathrm{ess}}(L) \geq \frac{1}{2}$. Thus it only remains to show that $\alpha_C^{\mathrm{ess}}(L) \leq \frac{1}{2}$.

Fix any place v of $\mathbb{Q}$. Regardless of our choice of place, there are infinitely many integers D such that $\sqrt{D}$ is a quadratic irrational defined over $\mathbb{Q}_v$. Fixing such an integer D, choose any point $(a_0 : a_1 : a_2 : a_3) \in \mathbb{P}^3(\mathbb{Q})$ such that $a_0 \neq 0$, $a_1a_3 - a_2^2 \neq 0$, $(a_1a_2 - a_0a_3)^2 - 4(a_1a_3 - a_2^2)(a_0a_2 - a_1^2) \neq 0$, and $a_0a_2 - a_1^2 \neq 0$, and choose it to lie on the surface $(yz - xw)^2 - 4(yw - z^2)(xz - y^2) - Dx^4 = 0$. By Lemma 4.4.4, such a point necessarily exists.

By Lemma 4.4.3, the point $(a_0 : a_1 : a_2 : a_3)$ is on a secant line ℓ to C passing through the point $(\alpha^3 : \alpha^2 : \alpha : 1)$, where α is a root of the quadratic equation $(a_1a_3 - a_2^2)X^2 + (a_1a_2 - a_0a_3)X + (a_0a_2 - a_1^2) = 0$. Using the quadratic formula, we may take

$$\alpha = \frac{(a_0a_3 - a_1a_2) + \sqrt{(a_1a_2 - a_0a_3)^2 - 4(a_1a_3 - a_2^2)(a_0a_2 - a_1^2)}}{2(a_1a_3 - a_2^2)}.$$

By our choice of $(a_0 : a_1 : a_2 : a_3)$, the number $\sqrt{(a_1a_2 - a_0a_3)^2 - 4(a_1a_3 - a_2^2)(a_0a_2 - a_1^2)} = \sqrt{Da_0^4} = a_0^2\sqrt{D}$ is a quadratic irrational defined over $\mathbb{Q}_v$, which means the point $z := (\alpha^3 : \alpha^2 : \alpha : 1)$ is likewise quadratic over $\mathbb{Q}$ and contained in $\mathbb{P}^3(\mathbb{Q}_v)$.

Let $z^\sigma = (\sigma(\alpha)^3 : \sigma(\alpha)^2 : \sigma(\alpha) : 1)$ denote the Galois conjugate point, where σ is the non-trivial automorphism of $\mathbb{Q}(\alpha)$. Notice that the secant line ℓ described above passes through z^σ as well. Hence, ℓ is defined over $\mathbb{Q}$, because the set $\{z, z^\sigma\}$ is Galois invariant.

Applying the Dirichlet-type result in [2] (Theorem 1), since ℓ is defined over $\mathbb{Q}$ and z is an irrational point defined over $\mathbb{Q}_v$, we can find a sequence of points $\{x_n\} \in \mathbb{P}^3(\mathbb{Q})$, all lying on the secant line ℓ, for which

$$d_v(x_n, z)^{1/2} H_L(x_n)$$

is bounded above as $n \to \infty$. But since z is a point on C, we have that $d_v(x_n, C) \leq d_v(x_n, z)$, so that

$$d_v(x_n, C)^{1/2} H_L(x_n)$$

is likewise bounded above as $n \to \infty$. Consequently, $\alpha_C(\{x_n\}, L) \leq \frac{1}{2}$. To prove that $\alpha_C^{\mathrm{ess}}(L) \leq \frac{1}{2}$, we only need to show that the collection of secant lines of the type just described are Zariski dense in $\mathbb{P}^3_{\mathbb{Q}}$.

Let U be a nonempty open subset of $\mathbb{P}^3$. Shrinking U if necessary, we may assume it is contained in the open subset where $z^2 - yw \neq 0$, $y^2 - xz \neq 0$, and $x \neq 0$. As mentioned above, there are infinitely many integers D for which $\sqrt{D}$ is a quadratic irrational defined over $\mathbb{Q}_v$. Hence, there is at least one such D for which U intersects the surface

$$(yz - xw)^2 - 4(yw - z^2)(xz - y^2) - Dx^4 = 0.$$

The resulting intersection of U with this surface is a nonempty open subset of the surface, which means U contains some $\mathbb{Q}$-point on the surface by Lemma 4.4.4. In particular, U intersects the family of secant lines of the type described above, proving those lines are Zariski-dense.

Proceeding as in the proof of Theorem 4.2.2, for any $\epsilon > 0$, we can find a sequence approximating C along each of the secant lines with approximation constant smaller than $\frac{1}{2} + \epsilon$. By taking the union of these countably many sequences, we construct a Zariski-dense sequence approximating C and also with approximation constant smaller than $\frac{1}{2} + \epsilon$. Since $\epsilon > 0$ was arbitrary, this proves that $\alpha_C^{\mathrm{ess}}(L) \leq \frac{1}{2}$, completing the proof. $\square$

4.4.2 Cubics Contained in a Plane

Now, we discuss cubic curves situated inside a plane in $\mathbb{P}^3$ with equations defined over $\mathbb{Q}$. After a linear automorphism of $\mathbb{P}^3$, these will have equations of the form

$$\begin{cases} F(x, y, z) = 0 \\ w = 0, \end{cases}$$

where $F \in \mathbb{Q}[x, y, z]$ is a homogeneous form of degree 3. Proposition 3.2.1 tells us that we will always have $\alpha_C(L) \geq \frac{1}{3}$ for such curves, and indeed, Theorem 3.3.1 tells us $\alpha_C(L) = \infty$ whenever $C(\mathbb{Q}_v) = \varnothing$. It should be noted that computing the *essential* approximation constant for many of these curves is immediate, thanks to Theorem 4.2.2. Indeed, all these curves are contained in a proper linear subvariety of $\mathbb{P}^3_{\mathbb{Q}}$, namely $w = 0$, and so for any such cubic curve C satisfying $C(\mathbb{Q}) \neq \varnothing$, that theorem tells us $\alpha_C^{\mathrm{ess}}(L) = 1$ for all places of $\mathbb{Q}$.

As we will see, computing the standard approximation constants for these curves is a bit more complicated. Fortunately, Theorem 4.1.2 allows us to deal with all cubics satisfying a simple geometric condition, including two particular, well-known families.

Proposition 4.4.2. *Let C be a cubic curve in $\mathbb{P}^3$ cut out by equations of the form*

$$\begin{cases} F(x, y, z) = 0 \\ w = 0, \end{cases}$$

with $F(x, y, z) \in \mathbb{Z}[x, y, z]$ homogeneous of degree 3, and assume that C has a rational flex. In other words, assume we have a point $a \in C(\mathbb{Q})$ for which the tangent line to C at a (in the plane $w = 0$) intersects C with multiplicity 3. Then for all places of $\mathbb{Q}$, we have $\alpha_C(L) = \frac{1}{3}$.

Proof. We are given a rational flex $a \in C(\mathbb{Q})$, so by definition, the tangent line ℓ to C at the point a meets C with intersection multiplicity at least 3. Since C is a cubic curve in the plane $w = 0$, the multiplicity must be exactly 3 by Bézout's theorem. In particular, ℓ does not intersect C at any other point, and the local intersection multiplicity of ℓ with C at a may be computed by taking the dimension of $\mathcal{O}_{\ell,a}/(f)$ as a $\mathbb{Q}$-vector space, where f is an appropriately de-homogenized version of $F(x, y, z)$. Since this dimension is exactly 3, the conclusion $\alpha_C(L) = \frac{1}{3}$ follows immediately from Theorem 4.1.2. □

In particular, Proposition 4.4.2 applies to elliptic curves in short Weierstrass form (taking $F(x, y, z) = zy^2 - x^3 - Az^2x - Bz^3$ for $A, B \in \mathbb{Q}$). Here, the rational flex can be found at the point at infinity, $(x : y : z : w) = (0 : 1 : 0 : 0)$.

The proposition also applies to certain diagonal cubics $F(x, y, z) = ax^3 + by^3 + cz^3$, with $a, b, c \in \mathbb{Z}$ relatively prime. Namely, if $F(X, Y, 0) = 0$ for some relatively prime integers X and Y, and $abc \neq 0$, then $(x : y : z : w) = (X : Y : 0 : 0)$ is a rational flex of the curve. In particular, this is applicable to the Fermat cubic, with $F(x, y, z) = x^3 + y^3 + z^3$, since $F(1, -1, 0) = 0$.

However, not every cubic curve contained in a plane is encompassed in the above proposition, and indeed, it seems more difficult to compute the approximation constant for any cubic curve contained in a plane that does not meet the criteria of either Proposition 4.4.2 or Theorem 3.3.1.

As a motivating case, suppose we let $F(x, y, z) = x^3 + 2y^3 + 7z^3$. First, note that the curve in $\mathbb{P}^3$ cut out by $F(x, y, z) = 0$ and $w = 0$ has no rational points, and hence no rational flex. Indeed, such a point would lead (after multiplying by an appropriate scalar) to a nonzero triple (a, b, c) of coprime integers such that $a^3 + 2b^3 + 7c^3 = 0$.

If we reduce this equation modulo 7, we find that $a^3 + 2b^3 \equiv 0 \pmod 7$. However, one can easily check that the only nonzero cubes modulo 7 are 1 and -1, and from this we see that $a^3 + 2b^3 \equiv 0 \pmod 7$ if and only if $a \equiv b \equiv 0 \pmod 7$. In other words, a and b must both be divisible by 7. But since $a^3 + 2b^3 + 7c^3 = 0$, we find that $7^3 \mid 7c^3$, so that c is also divisible by 7. We have now reached a contradiction to the assumption that a, b, c were relatively prime.

Thus, the curve C under discussion has no rational points, rendering Proposition 4.4.2 ineffective. Moreover, a minor modification of the above argument proves that $C(\mathbb{Q}_7) = \varnothing$, so that $\alpha_C(L) = \infty$ with respect to the 7-adic absolute value. However, the archimedean absolute value is of more interest to us, since C clearly possesses points defined over $\mathbb{R}$. In keeping with every other example considered so far, we would conjecture that $\alpha_C(L) = \frac{1}{3}$ with respect to this place. Certainly, Proposition 3.2.1 tells us that $\alpha_C(L) \geq \frac{1}{3}$.

However, the best upper bound we can offer is $\alpha_C(L) \leq \frac{1}{2}$. To arrive at this, we can apply the Dirichlet-type approach in [2], approximating along the line $y = w = 0$. This line intersects the curve in the real irrational algebraic point $a = (\sqrt[3]{7} : 0 : -1 : 0)$, and so this Dirichlet-style approach guarantees the existence of a sequence of points $\{x_i\} \subseteq \mathbb{P}^3(\mathbb{Q})$, all on the line $y = w = 0$, with the property that

$$d_v(x_i, a)^{1/2} H_L(x_i)$$

is bounded above as $i \to \infty$. Since a lies on C, this immediately yields $\alpha_C(L) \leq \frac{1}{2}$.

Attempts to show that $\alpha_C(L) \leq \frac{1}{3}$ using another familiar approach run into new difficulties. Ideally, we would find an integer $d \neq 0$ such that

$$x^3 + 2y^3 + 7z^3 = d$$

has infinitely many (coprime) integer solutions (x, y, z). Appending a 0 in the last coordinate and taking a sequence of such points $\{x_n\}$ would give us $d_v(x_n, C)H_L(x_n)^3 = |d|$ for all positive integers n. The conclusion $\alpha_C(L) = \frac{1}{3}$ would then follow immediately.

One way to go about finding infinitely many integer points is to identify a rational curve on the corresponding cubic surface $x^3 + 2y^3 + 7z^3 = dw^3$ for some integer d. If this rational curve has at most two places at infinity of the right form and a smooth integral point, we could apply Theorem 4.1.1 and be finished immediately. The problem is that the obvious candidates for such curves cannot be found, as illustrated in the following proposition:

Proposition 4.4.3. *For all integers $d \neq 0$, the cubic surface $x^3 + 2y^3 + 7z^3 + dw^3 = 0$ does not contain any of the following:*

(1) Lines defined over $\mathbb{Q}$.

(2) Conics defined over $\mathbb{Q}$.

(3) Curves of odd degree defined over $\mathbb{Q}$ and possessing at most two places at infinity.

Proof.

(1) To fix notation, let S denote the cubic surface in the statement of the proposition. It is well-known that there are 27 lines on every smooth cubic surface. For the diagonal cubic surface $x^3 + y^3 + z^3 + w^3 = 0$, these are easy to write down directly. They come in three families:

$$\begin{cases} x + \zeta_1 y = 0 \\ z + \zeta_2 w = 0 \end{cases} \quad \begin{cases} x + \zeta_1 z = 0 \\ y + \zeta_2 w = 0 \end{cases} \quad \begin{cases} x + \zeta_1 w = 0 \\ y + \zeta_2 z = 0, \end{cases}$$

where ζ_1 and ζ_2 are cube roots of unity. There are three choices for each of ζ_1 and ζ_2 in each of the three families, giving the desired 27 lines. It is easy to check that each of these lines is indeed distinct from the rest, for instance by checking their Plücker coordinates in the Grassmannian $\mathbf{Gr}(2, 4)$.

The surface S is obtained from the cubic surface mentioned above by scaling y, z, w by factors of $\sqrt[3]{2}$, $\sqrt[3]{7}$, $\sqrt[3]{d}$, respectively. This means the 27 lines on S are given by

$$\begin{cases} x + \zeta_1 \sqrt[3]{2} y = 0 \\ \sqrt[3]{7} z + \zeta_2 \sqrt[3]{d} w = 0 \end{cases} \quad \begin{cases} x + \zeta_1 \sqrt[3]{7} z = 0 \\ \sqrt[3]{2} y + \zeta_2 \sqrt[3]{d} w = 0 \end{cases} \quad \begin{cases} x + \zeta_1 \sqrt[3]{d} w = 0 \\ \sqrt[3]{2} y + \zeta_2 \sqrt[3]{7} z = 0, \end{cases}$$

again with ζ_1 and ζ_2 varying through the cube roots of unity.

Checking that S contains no lines defined over $\mathbb{Q}$ reduces to checking that none of these 27 lines are defined over $\mathbb{Q}$. None of the lines in the first family is of this type, because they contain points of the form $(\zeta_1\sqrt[3]{2} : -1 : 0 : 0)$. To see why this is enough, we fix a primitive cube root of unity ζ and consider the element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q})$ given by $\sigma(\zeta) = \zeta$ and $\sigma(\sqrt[3]{2}) = \zeta\sqrt[3]{2}$. The image of $(\zeta_1\sqrt[3]{2} : -1 : 0 : 0)$ under this automorphism is $(\zeta_1\zeta\sqrt[3]{2} : -1 : 0 : 0)$, which no longer lies on the line. If this line *were* defined over $\mathbb{Q}$, then the image of any point on the line under such an automorphism would again lie on the line.

For similar reasons, none of the lines in the second family are defined over $\mathbb{Q}$, considering a point of the form $(\zeta_1\sqrt[3]{7} : 0 : -1 : 0)$. Finally, none of the lines in the last family is defined over $\mathbb{Q}$, by considering the point $(0 : \zeta_2\sqrt[3]{7} : -\sqrt[3]{2} : 0)$ on the line and an automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2}, \sqrt[3]{7})/\mathbb{Q})$ fixing ζ and $\sqrt[3]{7}$ and mapping $\sqrt[3]{2}$ to $\zeta\sqrt[3]{2}$. Here, as before, ζ is some fixed primitive cube root of unity. The image of the point in question under σ is $(0 : \zeta_2\sqrt[3]{7} : -\zeta\sqrt[3]{2} : 0)$, which does not lie on the line.

This completes the proof that S does not contain any lines defined over $\mathbb{Q}$.

(2) Suppose to the contrary that there is a conic C defined over $\mathbb{Q}$ and contained in S. Appealing to Lemma 4.3.1, we deduce that C is contained in a (unique) plane of $\mathbb{P}^3$, which we denote by Y.

Since C is not a line, we can find three non-collinear points on C, which necessarily span the plane Y. The image of these three points under any automorphism in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ will again be three non-collinear points on C, spanning another projective plane, because C is invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Since this new plane intersects C in at least three points and C has degree 2, this new plane contains C as well. But Y is the unique plane containing C, so it follows that Y is invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. By Lemma 2.3.1, Y can be defined by equations with coefficients in $\mathbb{Q}$.

The intersection of Y with S must be a degree 3 curve C', because S is a cubic surface. But C is a degree 2 component of C', so we deduce that C' has two irreducible components, namely C and a line. Since C' is the intersection of two surfaces defined over $\mathbb{Q}$, it is likewise defined over $\mathbb{Q}$. So, we claim that the line contained in C' is also defined over $\mathbb{Q}$. Again, considering any element $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we know that σ fixes C' and also fixes C, from which it follows that the line is fixed by σ as well. Hence, if S contains a conic defined over $\mathbb{Q}$, then S also contains a line defined over $\mathbb{Q}$, which we previously showed is impossible.

(3) To show that there are no curves of odd degree $d \geq 3$ on S defined over $\mathbb{Q}$ and having at most two places at infinity, we prove that any such curve C of odd degree must have at least three points at infinity.

Since C is a curve of degree d, there are d points of intersection with the hyperplane $w = 0$, counting multiplicity. We claim that the intersection cannot consist of a single point with multiplicity d. Indeed, the intersection of $w = 0$ with C is defined over $\mathbb{Q}$, hence fixed by any element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If there were only a single point in that intersection, it would have to be a rational point. In particular, there would be a rational point lying on S in the hyperplane $w = 0$. But this intersection is the curve $x^3 + 2y^3 + 7z^3 = 0$, which we saw has no rational points.

Now, suppose there are exactly two points of intersection of C with the locus at infinity, say P and Q. The intersection of C with the plane at infinity has odd multiplicity, so the locus must be represented by a Weil divisor $a_1(P) + a_2(Q)$ on C for which $a_1 \neq a_2$. Since this locus is defined over $\mathbb{Q}$, the divisor must be Galois invariant. On the other hand, the image of this divisor under $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is $a_1(P^\sigma) + a_2(Q^\sigma)$, where P^σ and Q^σ are the images of P and Q under σ. Comparing divisors, we see that we must have $P = P^\sigma$ and $Q = Q^\sigma$, which implies that P and Q are actually defined over $\mathbb{Q}$. We have now reached the same contradiction as above, since S does not have any rational points at infinity.

□

Much of the work we've just done can be replicated in another way (and expanded upon), using an entirely different method of proof. It starts with the observation that any curve on our target surface S cuts out a divisor class in $\mathrm{Pic}(S)$. Since S is a smooth cubic surface, the structure of this Picard group (over $\overline{\mathbb{Q}}$ or $\mathbb{C}$, say) is well-known. Indeed, every smooth cubic surface is isomorphic to a blowup of the projective plane at six points in general position, and the Picard group of such a blowup is free of rank 7, generated by the six exceptional divisors of the blowup and the proper transform of any line not passing through the six points at which we blew up. As previously mentioned, such a cubic surface contains 27 lines. Under the isomorphism with the blown-up projective plane, these lines are divided up as follows:

(1) The six exceptional divisors of the blow-up, say $E_1, \ldots, E_6$.

(2) The proper transforms of lines in the plane through any two of the points at which we blew up (15 such lines in all).

(3) The proper transforms of conics in the plane through five out of the six points at which we blew up (6 such lines in all).

Furthermore, if $P_1, \ldots, P_6$ are the points where we blew up the plane, corresponding to the exceptional divisors $E_1, \ldots, E_6$, then the divisor class of a line of type (2) corresponding to the proper transform of a line through P_i and P_j is given by $\ell - E_i - E_j$, where ℓ is the proper transform of a line not passing through $P_1, \ldots, P_6$. Consequently, a basis for the Picard group may be obtained consisting exclusively of divisor classes of lines (for instance, the six exceptional divisors and any line of type (2) above). As an immediate corollary, $\mathrm{Pic}(S)$ is generated by the divisor classes of its 27 lines. Further details can be found in [7], §V.4.

Combining these facts with some tools from representation theory, we can establish the following result, overlapping with Proposition 4.4.3.

Theorem 4.4.1. *Let S denote the cubic surface*

$$x^3 + 2y^3 + 7z^3 + dw^3 = 0,$$

where $d \neq 0$ is an integer with cube-free part divisible by a prime different from 2, 3, and 7. If C is a curve on S defined over $\mathbb{Q}$, then the degree of C (in $\mathbb{P}^3$) is divisible by 3. In particular, S does not contain any lines, conics, or quartics defined over $\mathbb{Q}$.

Proof. First, note there is a natural action of the group $G := \mathrm{Gal}(k/\mathbb{Q})$ on the Picard group of S, where $k = \mathbb{Q}(\zeta, \sqrt[3]{2}, \sqrt[3]{7}, \sqrt[3]{d})$ is the field of definition for the set of 27 lines on S. The action is induced by the natural action of the automorphisms in G on those 27 lines, and thus each element of G induces a linear map on the $\overline{\mathbb{Q}}$-vector space $V = \mathrm{Pic}(S) \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}$. Since $\mathrm{Pic}(S)$ is free of rank 7, V is a 7-dimensional vector space, with a basis consisting of some collection of 7 lines on S.

By standard facts from representation theory, we can give V the structure of a $\overline{\mathbb{Q}}[G]$-module. The curve C in the statement of the theorem has an associated divisor class in $\mathrm{Pic}(S)$, and the corresponding element of V must be invariant under the G-action, because C is defined over $\mathbb{Q}$. By considering the decomposition of V into irreducible subrepresentations, it is easy to check that finding the G-invariant vectors in V reduces to determining the number of copies of the trivial representation appearing in this decomposition of V. Any G-invariant vector is necessarily the sum of vectors belonging to these copies of the trivial representation.

In turn, the number of copies of the trivial representation can be computed as the inner product of characters $\langle \chi_G, \chi_{\mathrm{triv}} \rangle$, where χ_G is the character attached to the given representation of G on V, and χ_{triv} is the character of the trivial representation of G.

Since

$$\langle \chi_G, \chi_{\mathrm{triv}} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_G(g) \overline{\chi_{\mathrm{triv}}(g)} = \frac{1}{|G|} \sum_{g \in G} \chi_G(g),$$

this computation reduces to determining the value of χ_G on the various elements of G. The bulk of the proof consists of two tasks:

(1) Determine an explicit basis for $\mathrm{Pic}(S)$ (and hence, for V) consisting of 7 lines on S.

(2) Let the elements of G act on this basis, and use this data to compute the values of χ_G on the elements of G.

At this point, it will be helpful to introduce some notation for the 27 lines on S. Fix a primitive cube root of unity ζ. For $1 \leq i, j \leq 3$, we set L_{1ij} to be the line

$$\begin{cases} x + \zeta^{i-1}\sqrt[3]{2}y = 0 \\ \sqrt[3]{7}z + \zeta^{j-1}\sqrt[3]{d}w = 0. \end{cases}$$

Likewise, for $1 \leq i, j \leq 3$, we set L_{2ij} and L_{3ij}, respectively, to be the lines

$$\begin{cases} x + \zeta^{i-1}\sqrt[3]{7}z = 0 \\ \sqrt[3]{2}y + \zeta^{j-1}\sqrt[3]{d}w = 0 \end{cases} \qquad \begin{cases} x + \zeta^{i-1}\sqrt[3]{d}w = 0 \\ \sqrt[3]{2}y + \zeta^{j-1}\sqrt[3]{7}z = 0. \end{cases}$$

In the Appendix, we carry out the computations necessary to show that the divisor classes of $L_{112}, L_{121}, L_{133}, L_{222}, L_{311}, L_{322}, L_{333}$ form a basis for $\mathrm{Pic}(S)$. A table is also given there indicating exactly how to write the other 20 lines as linear combinations of these seven in $\mathrm{Pic}(S)$.

Moreover, under the assumptions on d given in the statement of the theorem, the Appendix contains the remaining computations necessary to verify that $\langle \chi_G, \chi_{\mathrm{triv}} \rangle = 1$. This means V contains exactly one copy of the trivial representation in its direct-sum decomposition into irreducible subrepresentations. Hence, all the G-invariant elements of V are scalar multiples of some fixed non-zero vector in V. Once we exhibit a single nonzero G-invariant vector, all the elements of $\mathrm{Pic}(S)$ defined over $\mathbb{Q}$ (including the class of our target curve C) are multiples of this fixed vector.

It is easy to find such a G-invariant vector, because divisors defined over $\mathbb{Q}$ are easy to exhibit. For instance, $\mathrm{div}(x^3 + 2y^3)$ is the divisor of a homogeneous polynomial with coefficients in $\mathbb{Q}$, and so it must yield a Galois-invariant divisor class in $\mathrm{Pic}(S)$. Using our notation for the lines on S, one quickly checks that

$$\begin{aligned}\mathrm{div}(x^3 + 2y^3) &= \mathrm{div}(x + \sqrt[3]{2}y) + \mathrm{div}(x + \zeta\sqrt[3]{2}y) + \mathrm{div}(x + \zeta^2\sqrt[3]{2}y)\\ &= (L_{111} + L_{112} + L_{113}) + (L_{121} + L_{122} + L_{123}) + (L_{131} + L_{132} + L_{133}).\end{aligned}$$

Using the table of relations in the Appendix to re-write this in terms of our basis for $\mathrm{Pic}(S)$, we find that

$$\mathrm{div}(x^3 + 2y^3) \sim -3L_{112} - 3L_{121} + 6L_{133} + 9L_{222} - 3L_{311} + 6L_{322} - 3L_{333}.$$

Dividing out the common factor of 3, we deduce that all G-invariant elements of $\mathrm{Pic}(S)$ may be expressed as integer multiples of

$$D := -L_{112} - L_{121} + 2L_{133} + 3L_{222} - L_{311} + 2L_{322} - L_{333}.$$

Now, suppose the degree of the curve C is equal to δ. To prove the theorem, we must show δ is a multiple of 3. By definition of degree, if H is any hyperplane in $\mathbb{P}^3$ not containing C, the intersection number $H \cdot C$ is equal to δ. On the other hand, since C lies on S, we can also compute this intersection number on S as $H_0 \cdot C$, where H_0 is the pullback of H via the embedding $S \hookrightarrow \mathbb{P}^3$. Now, knowing that C is associated to a G-invariant divisor class in $\mathrm{Pic}(S)$, we have $C \sim mD$ for some integer m. On the other hand, we know that $H_0 \cdot L_{ijk} = 1$ for any of the 27 lines L_{ijk}, because the intersection multiplicity is the same as that of a hyperplane and a line in $\mathbb{P}^3$. In conclusion,

$$\begin{aligned}\delta &= H_0 \cdot C\\ &= H_0 \cdot mD\\ &= m(H_0 \cdot D)\\ &= m(H_0 \cdot (-L_{112} - L_{121} + 2L_{133} + 3L_{222} - L_{311} + 2L_{322} - L_{333}))\\ &= m(-1 - 1 + 2 + 3 - 1 + 2 - 1)\\ &= 3m.\end{aligned}$$

Thus, the degree of C is divisible by 3. $\square$

Because the curve $x^3 + 2y^3 + 7z^3 = 0, w = 0$ has no rational points, one might be led to guess that this is the source of the computational obstruction. However, the same kind of issues arise with the curve given by $x^3+2y^3+3z^3 = 0$, $w = 0$, which has the trivial rational point $(1 : 1 : -1 : 0)$. None of the equations $x^3 + 2y^3 = 0$, $x^3 + 3z^3 = 0$, $2y^3 + 3z^3 = 0$ have nonzero integer solutions (to see this, reduce modulo 7 and argue as in the case of the previous curve), so Proposition 4.4.2 cannot be applied to the "usual" rational flexes. Proposition 3.2.1 again tells us $\alpha_C(L) \geq \frac{1}{3}$, and approximating $(\sqrt[3]{3} : 0 : -1 : 0)$ along the line $y = w = 0$ will give $\alpha_C(L) \leq \frac{1}{2}$ with respect to the archimedean place. However, bridging the gap between the upper and lower bounds in cases like these seems to require a new technique.

Finally, it is worth remarking that Theorem 4.2.2 is also not applicable when computing the essential approximation constant for the curve given by $x^3 + 2y^3 + 7z^3 = 0$ and $w = 0$, because the curve does not have any rational points, nor points quadratic over $\mathbb{Q}$ (to see this latter fact, use the fact that every line in $w = 0$ intersects the curve in three places counting multiplicity). Insofar as Theorem 4.2.2 *is* applicable to $x^3 + 2y^3 + 3z^3 = 0, w = 0$, our ability to use the tools at hand on these curves does differ.

4.5 Approximation Constants for a Diagonal Quartic Surface

One interesting question we have not yet addressed is: can we exhibit a projective variety X over a number field k, line bundle L on X, and point $x \in X(k)$, for which the approximation constant $\alpha_x(L)$ is finite, but yet the essential approximation constant $\alpha_x^{\text{ess}}(L)$ is infinite? Furthermore, we want to avoid accomplishing this in the trivial way, where one selects X for which $X(k)$ is not Zariski-dense.

To make some initial progress on this question, we will take X to be the diagonal quartic surface

$$x^4 + y^4 = z^4 + w^4$$

in $\mathbb{P}^3_{\mathbb{Q}}$, and our line bundle will be $\iota^*(\mathcal{O}_{\mathbb{P}^3}(1))$, where $\iota : X \hookrightarrow \mathbb{P}^3$ is the given embedding of X.

Firstly, we argue that $X(\mathbb{Q})$ is Zariski-dense in X. This will follow from the fact that the quartic surface contains non-trivial rational points, i.e. points not lying on any of the 48 lines on the surface and where none of the coordinates are 0. The problem of writing a number as a sum of fourth powers in two distinct ways has a long history, tying in with the famous "taxi cab number" story, in which Ramanujan pointed out 1729 is the smallest number expressible as a sum of two cubes in two different ways. When Hardy relayed this story, he added that Euler had made a similar observation involving fourth powers, namely

$$59^4 + 158^4 = 133^4 + 134^4.$$

For our purposes, this says $(59 : 158 : 133 : 134)$ is a non-trivial rational point on X. Thus, we may invoke the following theorem to conclude that $X(\mathbb{Q})$ is Zariski dense:

Theorem 4.5.1 (Theorem 1.1, [11]). *Let $a, b, c, d \in \mathbb{Q}$ be nonzero rational numbers with abcd square. Let $P = (x_0 : y_0 : z_0 : w_0)$ be a rational point on the surface $ax^4 + by^4 + cz^4 + dw^4 = 0$, and suppose that $x_0y_0z_0w_0 \neq 0$ and that P does not lie on any of the 48 lines of the surface. Then the set of rational points of the surface is dense in both the Zariski and the real analytic topology.*

Thus, if the essential approximation constant is ∞ for a given point on X, we can rest assured it is not for trivial reasons. Here is what we *can* say:

Theorem 4.5.2. *Let X and L be as above, and choose the point $x_0 = (1 : 0 : 1 : 0) \in X(\mathbb{Q})$. Furthermore, let U denote the open subset of X given by $x - z \neq 0$. With respect to all places of $\mathbb{Q}$, we have $\alpha_{x_0}(L) = 1$, while $\alpha_{x_0}(U, L) \geq 4$. In particular, $\alpha^{ess}_{x_0}(L) \geq 4$ for all places of $\mathbb{Q}$.*

Proof. By approximating x_0 along the $\mathbb{Q}$-rational line $x-z = 0$, $y-w = 0$ (which is entirely contained in S), it follows easily that $\alpha_{x_0}(L) \leq 1$ with respect to each place of $\mathbb{Q}$. From here, $\alpha_{x_0}(L) = 1$ follows almost immediately. Indeed, by Theorem 4.2.3, approximating x_0 in $\mathbb{P}^3$ with respect to $\mathcal{O}_{\mathbb{P}^3}(1)$ results in an approximation constant of exactly 1 for all places of $\mathbb{Q}$. Since the distance and height functions we use on S are identical to the ones we would use in $\mathbb{P}^3$ (being pulled back from those corresponding functions on $\mathbb{P}^3$), and the sequences approximating x_0 on X are a subset of those sequences approximating x_0 in $\mathbb{P}^3$, we conclude there can be no sequence $\{x_n\} \subseteq X(\mathbb{Q})$ approximating x_0 with $\alpha_{x_0}(\{x_n\}, L) < 1$ for any place of $\mathbb{Q}$.

Now, we turn to the second part of the theorem. We begin with the archimedean place of $\mathbb{Q}$. In this case, we have

$$d_v((x : y : z : w), x_0) = \frac{\max(|y|, |w|, |x - z|)}{\max(|x|, |y|, |z|, |w|)},$$

since x_0 may be cut out in S by the equations $y = w = x - z = 0$. Fix a real number $\gamma > 0$ and suppose we have a sequence $\{x_n\} \subseteq U(\mathbb{Q})$ for which $\alpha_{x_0}(\{x_n\}, L) < \gamma$. We will show that $\gamma \geq 4$.

Writing each element of the sequence with coprime integer coordinates and applying the definitions, there is some positive constant M for which there are infinitely many different coprime integer tuples (x, y, z, w), satisfying $x^4 + y^4 = z^4 + w^4$ and

$$d_v((x : y : z : w), x_0)^\gamma H_L((x : y : z : w)) = \frac{\max(|y|, |w|, |x - z|)^\gamma}{\max(|x|, |y|, |z|, |w|)^{\gamma - 1}} \leq M.$$

This implies there are infinitely many integer tuples (x, y, z, w) satisfying the equation of X, and such that

$$\begin{aligned} |y|^\gamma &\leq M \max(|x|, |y|, |z|, |w|)^{\gamma-1} \\ |w|^\gamma &\leq M \max(|x|, |y|, |z|, |w|)^{\gamma-1} \\ |x - z|^\gamma &\leq M \max(|x|, |y|, |z|, |w|)^{\gamma-1}. \end{aligned}$$

Since y and w are integers, the first two conditions imply that there can only be finitely many tuples in this infinite collection for which $\max(|x|,|y|,|z|,|w|) = |y|$ or $\max(|x|,|y|,|z|,|w|) = |w|$. Throwing away those finitely many tuples, we may assume $\max(|x|,|y|,|z|,|w|) = \max(|x|,|z|)$.

Furthermore, either $|x| \geq |z|$ or $|z| \geq |x|$ holds for infinitely many of these points, so without loss of generality, we may assume that $\max(|x|,|y|,|z|,|w|) = |x|$ for this infinite collection of integer tuples. Finally, replacing x with $-x$ and z with $-z$ if necessary in each of these tuples, we can always assume $x > 0$. Now it follows from the third estimate above that $z > 0$ as well; otherwise $|x-z|^\gamma \geq x^\gamma$, and x^γ grows faster than $Mx^{\gamma-1}$.

Since all of these infinitely many tuples (x,y,z,w) satisfy $x^4+y^4 = z^4+w^4$, we rewrite and factor this expression to yield the relation

$$(x-z)(x+z)(x^2+z^2) = (w-y)(w+y)(w^2+y^2). \tag{4.1}$$

Keeping in mind $x = \max(|x|,|y|,|z|,|w|)$, it follows immediately from the inequalities above that

$$\begin{aligned} |w-y| &\leq 2M^{1/\gamma}x^{(\gamma-1)/\gamma} \\ |w+y| &\leq 2M^{1/\gamma}x^{(\gamma-1)/\gamma} \\ |w^2+y^2| &\leq 2M^{2/\gamma}x^{2(\gamma-1)/\gamma} \end{aligned}$$

for each of the infinitely many integer tuples. On the other hand, we have the trivial estimates

$$\begin{aligned} (x+z) &\geq x \\ (x^2+z^2) &\geq x^2. \end{aligned}$$

Taking absolute values of both sides of (4.1) and applying these estimates leads to

$$|x-z| \cdot x^3 \leq M_1 x^{4(\gamma-1)/\gamma}$$

for some absolute constant M_1. Simplifying, this means

$$|x-z| \leq M_1 x^{(\gamma-4)/\gamma}$$

for all of these infinitely many integer tuples (x,y,z,w). But x must grow without bound over this infinite collection, being the largest coordinate. So, if $\gamma < 4$, eventually the upper bound is smaller than 1. This forces $x - z = 0$, since $x - z \in \mathbb{Z}$. But our sequence was chosen from the open set U, so we have a contradiction. Since $\{x_n\}$ was an arbitrary sequence from U, we conclude that $\alpha_{x_0}(U,L) \geq 4$ when v is the archimedean place.

Next, assume v is non-archimedean, associated to some p-adic absolute value. As above, suppose we have a sequence of points $\{x_n\} \subseteq U(\mathbb{Q})$ for which $\alpha_{x_0}(\{x_n\},L) < \gamma$. Again, we choose the coordinates of each point x_n to be relatively prime integers.

This leads to the existence of infinitely many integer tuples (x,y,z,w) with $\gcd(x,y,z,w) = 1$ satisfying the equation of X and an absolute constant $M > 0$ such that

$$d_v((x:y:z:w),x_0)^\gamma H_L((x:y:z:w)) = \frac{\max(|y|_p,|w|_p,|x-z|_p)^\gamma}{\max(|x|_p,|y|_p,|z|_p,|w|_p)^\gamma}\max(|x|,|y|,|z|,|w|) \leq M$$

for each tuple. Since $\gcd(x, y, z, w) = 1$ always holds, it follows that $\max(|x|_p, |y|_p, |z|_p, |w|_p) = 1$, so the condition above is simplified to

$$\max(|y|_p, |w|_p, |x - z|_p)^\gamma \max(|x|, |y|, |z|, |w|) \leq M.$$

Even more than that, for each of the infinitely many tuples (x, y, z, w), at least one entry is not divisible by p. Therefore, we can extract an infinite sub-collection for which some fixed coordinate is *never* divisible by p. Notice that this cannot be true for either the y- or w-coordinate. Indeed, for such tuples, $\max(|y|_p, |w|_p, |x - z|_p) = 1$, so that

$$\max(|y|_p, |w|_p, |x - z|_p)^\gamma \max(|x|, |y|, |z|, |w|) = \max(|x|, |y|, |z|, |w|),$$

which is necessarily unbounded over an infinite set of integer tuples.

Therefore, without loss of generality, we may assume z is never divisible by p. Furthermore, by replacing x and z with $-x$ and $-z$ if necessary, we may assume that $x - z > 0$. At this point, we know that

$$\begin{aligned} |y|_p &\leq \frac{M^{1/\gamma}}{\max(|x|, |y|, |z|, |w|)^{1/\gamma}} \\ |w|_p &\leq \frac{M^{1/\gamma}}{\max(|x|, |y|, |z|, |w|)^{1/\gamma}} \\ |x - z|_p &\leq \frac{M^{1/\gamma}}{\max(|x|, |y|, |z|, |w|)^{1/\gamma}}. \end{aligned}$$

In turn, the first two bounds imply that

$$\begin{aligned} |w - y|_p &\leq \frac{M^{1/\gamma}}{\max(|x|, |y|, |z|, |w|)^{1/\gamma}} \\ |w + y|_p &\leq \frac{M^{1/\gamma}}{\max(|x|, |y|, |z|, |w|)^{1/\gamma}} \\ |w^2 + y^2|_p &\leq \frac{M^{2/\gamma}}{\max(|x|, |y|, |z|, |w|)^{2/\gamma}}. \end{aligned}$$

Going back to Equation (4.1), taking p-adic absolute values of both sides, and applying the bounds above, we arrive at an absolute constant M_1 such that

$$|x - z|_p |x + z|_p |x^2 + z^2|_p \leq \frac{M_1}{\max(|x|, |y|, |z|, |w|)^{4/\gamma}}. \tag{4.2}$$

To finish the argument, we recall the bound $|x - z|_p \leq \frac{M^{1/\gamma}}{\max(|x|,|y|,|z|,|w|)^{1/\gamma}}$. Since $\max(|x|, |y|, |z|, |w|)$ increases without bound over our infinite family, we can extract an infinite subfamily for which $x = z + ap^m$, where $\gcd(a, p) = 1$ and $m \geq 2$ (and where m may vary between tuples).

In turn, $x + z = 2z + ap^m$. Since $|z|_p = 1$, note that $|2z|_p = 1$ unless $p = 2$, in which case $|2z|_p = \frac{1}{p}$. Either way, $|ap^m|_p = \frac{1}{p^m} < |2z|_p$. We immediately conclude that

$$|x + z|_p = |2z + ap^m|_p = \max(|2z|_p, |ap^m|_p) = |2z|_p \geq \frac{1}{p}.$$

Similarly, $|x^2 + z^2|_p = |2z^2 + 2azp^m + a^2p^{2m}|_p \geq \frac{1}{p}$. Combining this with inequality (4.2), we find that

$$|x - z|_p \leq \frac{p^2 M_1}{\max(|x|, |y|, |z|, |w|)^{4/\gamma}}.$$

Written differently, there is an absolute constant M_2 such that

$$|x - z|_p^\gamma \max(|x|, |y|, |z|, |w|)^4 \leq M_2.$$

Now, recall that $x = z + ap^m$, where $\gcd(a, p) = 1$. Since $x - z > 0$, we see that $a > 0$. It immediately follows that either $|x| \geq \frac{ap^m}{2}$ or $|z| \geq \frac{ap^m}{2}$. Either way, we have

$$\max(|x|, |y|, |z|, |w|) \geq \frac{ap^m}{2} \geq \frac{p^m}{2}.$$

Therefore,

$$|x - z|_p^\gamma \max(|x|, |y|, |z|, |w|)^4 \geq \left(\frac{1}{p^{m\gamma}}\right)\left(\frac{p^{4m}}{16}\right) = \frac{p^{m(4-\gamma)}}{16}.$$

Unless $\gamma \geq 4$, we immediately deduce that $|x - z|_p^\gamma \max(|x|, |y|, |z|, |w|)^4$ is unbounded above (since $m \to \infty$ over this infinite family).

Thus, in the non-archimedean case, $\alpha_{x_0}(U, L) \geq 4$ as well. As an immediate consequence, $\alpha_{x_0}^{\text{ess}}(L) \geq 4$ for all places of $\mathbb{Q}$. $\square$

In the next chapter, we will discuss a Liouville-type result (Lemma 5.1.1), which will allow us to supply another, more conceptual proof that $\alpha_{x_0}(U, L) \geq 4$. There, we will blow up the diagonal quartic at x_0 and analyze the effectivity of a certain divisor class.

Chapter 5

Liouville-Type Theorems

5.1 A Liouville Lemma

Our next goal is to prove a more versatile counterpart to Proposition 3.2.1. Specifically, we aim to generalize Lemma 3.2 in [14] and its consequences. As always, X is a fixed projective variety, Z a closed subscheme, and k is our base number field. Recall that the *base locus* of a line bundle L on a variety X is the collection of points in X where all the global sections of L vanish simultaneously. The *stable base locus* of a line bundle L is the intersection of the base loci of the line bundles mL as m runs over all positive integers. One fact we will need is that we can find an $m \geq 1$ such that the stable base locus of L is the base locus of mL, which follows from Proposition 2.1.21 of [10].

Lemma 5.1.1. *Suppose that Z is a closed subscheme of X defined over k and let $\pi : \tilde{X} \to X$ be the blow up at Z with exceptional divisor E. Let L be a line bundle on X and $\gamma > 0$ a rational number such that $L_\gamma := \pi^*L - \gamma E$ is effective on $\tilde{X}$. Let B' be the stable base locus of L_γ and set $B = \pi(B')$.*

Then there is a positive real constant M (depending only on Z and L) such that for any sequence of k-points $\{x_j\} \to Z$ disjoint from B, we have

$$d_v(x_j, Z)^\gamma H_L(x_j) \geq M.$$

In particular, $\alpha_Z(\{x_j\}, L) \geq \gamma$.

Proof. By the remark preceding this lemma, there is some positive integer m such that B' is the base locus of mL_γ. Since L_γ is effective, so is mL_γ, which means there is a positive constant c such that $H_{mL_\gamma}(x) \geq c$ for all $x \in \tilde{X}(\overline{k})$ lying away from the base locus B', by Theorem B.3.2 of [9]. By the additivity property of height functions, H_{mL_γ} is equivalent to $H_{L_\gamma}^m$, so there is a constant c_1 (depending only on L and Z) for which $H_{L_\gamma}(x) \geq c_1$ for all points x lying outside of B'.

For convenience, set $U = \tilde{X} \setminus B'$. Since the sequence $\{x_j\}$ lies off of Z and B, and the blow-up map π is an isomorphism away from Z, we may write each x_j as $\pi(\tilde{x_j})$ for some

$\tilde{x_j} \in U$. Using the additivity and functoriality properties of height functions, we have the following inequality up to equivalence:

$$c_1 \leq H_{L_\gamma}(\tilde{x_j}) = H_{\pi^* L}(\tilde{x_j}) H_E(\tilde{x_j})^{-\gamma} = H_L(x_j) H_E(\tilde{x_j})^{-\gamma}.$$

We now wish to convert this into a problem about local Weil functions. Taking logarithms and using the local-global property tells us there is some constant C such that

$$C \leq h_L(x_j) - \gamma \sum_w \lambda_{E,w}(\tilde{x_j})$$

for all of our sequence elements $\tilde{x_j}$, with the sum running over all places of k. If we use the fact that $E = \pi^* Z$ and invoke the functoriality property of local Weil functions, we now have

$$C \leq h_L(x_j) - \gamma \sum_w \lambda_{Z,w}(x_j)$$

up to $O(1)$, for all x_j in our sequence. Now, for each place w, we claim that $\lambda_{Z,w} \geq O(1)$. Since Z is a closed subscheme, it can be described as the intersection of effective divisors $D_1, \ldots, D_m$ on X. By the positivity property of local Weil functions with respect to effective divisors, each $\lambda_{D_i,w}(x_j)$ is bounded below by a function that is $O(1)$, so that $\lambda_{Z,w}(x_j)$, the minimum of these values, is also bounded below by a $O(1)$ function. In other words, up to $O(1)$ we have $\sum_w \lambda_{Z,w}(x_j) \geq \lambda_{Z,v}(x_j)$ for any fixed place v. The end result of this is that up to $O(1)$, we have

$$C \leq h_L(x_j) - \gamma \lambda_{Z,v}(x_j).$$

Taking exponentials and applying the definition of the distance function $d_v(x_j, Z)$, we get a positive constant M such that

$$M \leq H_L(x_j) d_v(x_j, Z)^\gamma,$$

where M depends only on Z and L. In particular, the definition of $\alpha_Z(\{x_j\}, L)$ automatically forces $\alpha_Z(\{x_j\}, L) \geq \gamma$. $\square$

5.2 Application: Alternative Proof of Theorem 4.5.2

As a first application of this lemma, we can use it to give an alternative proof of the non-trivial statement in Theorem 4.5.2. There, we were working with the diagonal quartic $x^4 + y^4 = z^4 + w^4$ in $\mathbb{P}^3_{\mathbb{Q}}$, which we denoted by X, and were approximating the rational point $x_0 = (1 : 0 : 1 : 0)$ on X. If L denotes the pullback of $\mathcal{O}_{\mathbb{P}^3}(1)$ to the diagonal quartic, we showed that $\alpha_{x_0}(U, L) \geq 4$, where U is the open subset $x - z \neq 0$.

To see how to prove this another way using Lemma 5.1.1, we consider the point $\{x_0\}$ as a (reduced) closed subscheme of X, and let $\pi : \tilde{X} \to X$ be the blow-up at $\{x_0\}$ with exceptional divisor E. Our goal is to show that $\pi^* L - 4E$ is effective on $\tilde{X}$. Firstly, notice that if we choose the plane $x - z = 0$ as our representative of the divisor class on $\mathbb{P}^3$

corresponding to $\mathcal{O}_{\mathbb{P}^3}(1)$, then the pullback of this plane to X is the sum of four lines, say L_0, L_1, L_2, L_3, where L_m is the line given by $x - z = 0$, $y - i^m w = 0$, and i represents a fourth root of unity.

To show that $\pi^* L - 4E$ is effective, it will be enough to show that $\pi^* L_m - E$ is an effective divisor for each m, since $\pi^* L - 4E$ is the sum of these divisors. This is perhaps most easily seen by noting that the support of $\pi^* L_m$ is equal to the set-theoretic pre-image of L_m under π. Clearly, $\pi^{-1}(L_m)$ contains $\widetilde{L_m} := \overline{\pi^{-1}(L_m \setminus \{x_0\})}$. Moreover, $\pi^{-1}(L_m)$ also contains E, since all points in E map to x_0, which lies on L_m. These two components of $\pi^{-1}(L_m)$ must then both be zeros of the pullback divisor $\pi^*(L_m)$. In fact, $\mathrm{Supp}(\pi^*(L_m)) = E \cup \widetilde{L_m}$, since π is an isomorphism away from x_0 and maps E onto x_0. Consequently, when treated as a Weil divisor, $\pi^* L_m$ is of the form $a\widetilde{L_m} + bE$, where $a, b > 0$. In any case, since $\widetilde{L_m}$ and E are effective, $\pi^* L_m - E = a\widetilde{L_m} + (b-1)E$ is also effective.

Now that we are assured $\pi^* L - 4E$ is an effective divisor on $\tilde{X}$, let B' denote the stable base locus of $\pi^* L - 4E$. In particular, B' is the base locus of some multiple of $\pi^* L - 4E$, and any such multiple is effective and supported on the divisors $\widetilde{L_0}, \widetilde{L_1}, \widetilde{L_2}, \widetilde{L_3}$, and E. Thus, $B := \pi(B')$ is contained in the union of the four lines L_0, L_1, L_2, L_3, which is exactly the locus on X given by $x - z = 0$. If $U \subseteq X$ denotes the open set $x - z \neq 0$, it follows that any sequence of $\mathbb{Q}$-points in U is disjoint from B, with the immediate consequence that $\alpha_{x_0}(U, L) \geq 4$, thanks to Lemma 5.1.1.

5.3 Application: Liouville-Type Theorems

As another application of Lemma 5.1.1, we may generalize Theorem 3.3 of [14].

Theorem 5.3.1. *Let X be a projective variety defined over k, let Z be a closed subscheme of X defined over some algebraic extension of k, and let $d = [K : k]$, where K is the field of definition of the equations defining the subscheme Z. Additionally, set $m_v = [K_v : k_v]$, where v is a chosen place of k, extended in some way up to $\overline{k}$.*

Let X_K denote the base change of X to K, let $\tilde{X}$ denote the blowup of X_K at Z with exceptional divisor E, and let π denote the composition of the blowup map $\tilde{X} \to X_K$ with the base change map $X_K \to X$. Let L be an ample line bundle on X and let $\gamma > 0$ be a rational number such that $L_\gamma := \pi^* L - \gamma E$ is effective on $\tilde{X}$. Finally, let B' be the stable base locus of L_γ and set $B = \pi(B')$. Then:

1. *For any sequence of k-points $\{x_i\} \to Z$, if infinitely many points in the sequence lie outside B then $\alpha_Z(\{x_i\}, L) \geq \gamma m_v / d$.*

2. *If $\alpha_Z(L) < \gamma m_v / d$ then $Z \cap B \neq \varnothing$ and $\alpha_Z(L) = \alpha_{Z \cap B}(L|_B)$.*

3. *If $Z \cap B \neq \varnothing$ and $\alpha_{Z \cap B}(L|_B) \geq \gamma m_v / d$ then $\alpha_Z(L) \geq \gamma m_v / d$.*

Proof. Proof of (1): Let $\{x_i\}$ be a sequence of k-points approximating Z such that infinitely many points lie outside of B. If we drop to the subsequence of points not in B, the approximation constant for this new sequence cannot get larger, so to establish the lower bound, we may assume that the entire sequence $\{x_i\}$ is disjoint from B. After the base change, we may consider this sequence to be a sequence $\{y_i\}$ of distinct K-points approximating the subvariety Z of X_K. If we apply Lemma 5.1.1 to X_K and its closed subscheme Z, we find that there is a positive constant M such that $d_v(y_i, Z)^\gamma H_L(y_i) \geq M$ and $\alpha_Z(\{y_i\}, L)_K \geq \gamma$, where the subscript K means the approximation constant is measured with height functions and distances normalized with respect to K.

Now, when normalizing with respect to K rather than k, the height function gets raised to the power of d, while the distance function gets raised to the power m_v. Putting this information together, we find that $\alpha_Z(\{x_i\}, L)_k = \frac{m_v}{d}\alpha_Z(\{y_i\}, L)_K \geq \gamma m_v/d$, which proves (1).

Proof of (2): Assuming that $\alpha_Z(L) < \gamma m_v/d$, we can find a sequence $\{x_i\}$ of distinct k-points on X approximating Z such that $\alpha_Z(\{x_i\}, L) < \gamma m_v/d$. Applying part (1), we see that all but finitely many x_i lie inside B. Since omitting finitely many terms of a sequence has no impact on the approximation constant, we may assume that all x_i lie inside B. At this point, we claim that $Z \cap B \neq \varnothing$. Indeed, if we consider the closure C of the sequence $\{x_i\}$ in the v-adic topology on projective space over K_v, then since B is Zariski-closed in X, it is also v-adically closed, so it contains C. On the other hand, since $\{x_i\} \to Z$, the proof of Theorem 3.3.1 implies that $C \cap Z \neq \varnothing$, and so *a fortiori* $Z \cap B \neq \varnothing$.

Notice that the sequence $\{x_i\}$ is disjoint from the closed subset $Z \cap B$ of B, while lying entirely on the closed subset B. Furthermore, we notice that $\{x_i\} \to Z \cap B$ (within B). Indeed, to pick out $Z \cap B$ as an intersection of effective divisors on B, we can just use the same divisors defining Z, but restricted to B, which will not change the resulting distance functions.

Conversely, given a sequence $\{x_i\}$ of points lying in B and converging to $Z \cap B$, it may be treated as a sequence of distinct points lying on X, necessarily disjoint from Z (by definition of convergence). Convergence of this sequence to Z in X follows from the fact that $d_v(x_i, Z \cap B) \geq d_v(x_i, Z)$.

Finally, since $\alpha_Z(L)$ may be obtained by taking the infimum of the approximation constants for sequences $\{x_i\}$ with $\alpha_Z(\{x_i\}, L) < \gamma m_v/d$, it follows that $\alpha_Z(L) = \alpha_{Z\cap B}(L|_B)$, proving (2).

Proof of (3): Suppose that $Z \cap B \neq \varnothing$ and $\alpha_{Z\cap B}(L|_B) \geq \gamma m_v/d$. Taking the contrapositive of the statement in part (2) tells us that if $\alpha_Z(L) \neq \alpha_{Z\cap B}(L|_B)$, then $\alpha_Z(L) \geq \gamma m_v/d$. On the other hand, if $\alpha_Z(L) = \alpha_{Z\cap B}(L|_B)$, then our desired conclusion follows because $\alpha_{Z\cap B}(L|_B) \geq \gamma m_v/d$. □

Our generalized result features an apparently different lower bound than the one obtained in [14] for approximation constants of points, since we have obtained a bound of $\frac{\gamma m_v}{d}$, rather than $\frac{\gamma}{d}$.

The reason the m_v factor does not appear in [14] is that we must have $m_v = 1$ in the case where the subscheme is a point. Indeed, we can deduce this directly from Proposition 3.3.1. Applying that proposition in the case where Z is a single point x, we find that if there is a sequence of points x_i such that $d_v(x_i, x) \to 0$, there is a closed subscheme Z' of $\{x\}$ defined over a finite extension ℓ of k with $\ell \subseteq k_v$, for which $d_v(x_i, Z') \to 0$. But since x is a single reduced point, this is only true if $Z' = \{x\}$, so that x is already defined over an extension ℓ for which $\ell \subseteq k_v$, which amounts to claiming that $m_v = [\ell_v : k_v] = 1$.

When working with subvarieties of larger dimension, it is possible to approximate the subvariety even when m_v is larger than 1. To illustrate this, we give an example. We take $k = \mathbb{Q}$, $X = \mathbb{P}^2$, and $v = v_5$, the 5-adic absolute value on $\mathbb{Q}$. Consider the subvariety Z of the projective plane defined by

$$\sqrt{2}x + (1 + \sqrt{2})y - z = 0,$$

where x, y, z are the homogenous coordinates on $\mathbb{P}^2$. Certainly Z is defined over $\mathbb{Q}(\sqrt{2})$, and we claim this is indeed the field of definition of Z. The only proper subfield of $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Q}$ itself, and if we look at the projective point $(\sqrt{2} : 0 : 2)$ on Z, its image under the non-trivial automorphism in $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is $(-\sqrt{2} : 0 : 2)$, which does not lie on Z. Hence, Z is not defined over $\mathbb{Q}$.

Next, we observe that $m_v = [\mathbb{Q}(\sqrt{2})_{v_5} : \mathbb{Q}_{v_5}] = 2$. Indeed, note that $\mathbb{Q}(\sqrt{2})_{v_5} = \mathbb{Q}_5(\sqrt{2})$. Now $x^2 - 2$ is irreducible over $\mathbb{Q}_5$ (since $x^2 - 2$ is irreducible over the residue field $\mathbb{F}_5$), so that $\mathbb{Q}_5(\sqrt{2})$ is a degree-two extension of $\mathbb{Q}_5$.

Even though $m_v = 2$, we can easily concoct a sequence of projective points defined over $\mathbb{Q}$, not lying on Z, but still converging to Z with respect to v_5. Explicitly, if we fix a positive integer n, notice that the projective points $y_n := (-2 + 5^n : 2 : 2)$ approximate Z with respect to the 5-adic absolute value. Indeed, we observe that $|\sqrt{2}|_5 = |(\sqrt{2})(-\sqrt{2})|_5^{1/2} = |-2|_5^{1/2} = 1$, so that with our normalization with respect to $\mathbb{Q}(\sqrt{2})$, $\|\sqrt{2}\|_5 = |\sqrt{2}|_5^2 = 1$ as well. Noting that $5^n - 2$ is never divisible by 5 for any positive integer n, we immediately see $\|5^n - 2\|_5 = \|-2\|_5 = 1$. Finally, we have $\|\sqrt{2}(5^n - 2) + (1 + \sqrt{2})(2) - 2\|_5 = \|5^n\sqrt{2}\|_5 = \|5^n\|_5 \cdot \|\sqrt{2}\|_5 = \frac{1}{5^{2n}}$ with our choice of normalization. Thus $d_{v_5}(y_n, Z) = (5^{-2n})^{1/2} = 5^{-n} \to 0$ as $n \to \infty$ (re-normalizing with respect to the base field $\mathbb{Q}$). So, despite the fact that the completion of the field of definition for Z is a proper extension of the completion of $\mathbb{Q}$, nonetheless we can find a sequence of points defined over $\mathbb{Q}$ that approximates Z.

In some sense, however, an example like this obscures the truth: indeed, we know by Proposition 3.3.1 that there must be some closed subscheme Z' contained in Z, defined over an extension of $\mathbb{Q}$ contained in $\mathbb{Q}_5$, also approximated by the same sequence of points. For the subscheme Z', we will have $m_v = 1$, and it is "really" Z' that is being approximated, in the sense that $\alpha_Z(L) = \alpha_{Z'}(L)$ for any line bundle L.

In our example, it is easy to see by inspection that we can take Z' to be the projective point $\{(-2 : 2 : 2)\}$ lying on Z, and take $\ell = \mathbb{Q}$, since one can immediately check (for instance, using the definition of projective distance in [13]) that $(-2 + 5^n : 2 : 2)$ converges 5-adically to $(-2 : 2 : 2)$ as $n \to \infty$.

We can arrive at the same result by following the proof of Proposition 3.3.1 as well. In this case, $K = \mathbb{Q}(\sqrt{2})$ is a finite Galois extension over which Z is defined, and $K_{v_5} = \mathbb{Q}_5(\sqrt{2})$ is the corresponding finite Galois extension of $k_{v_5} = \mathbb{Q}_5$. The non-trivial automorphism interchanges $\sqrt{2}$ and $-\sqrt{2}$, and of course descends to an automorphism of K over

$\mathbb{Q}$. Applying Lemma 2.3.1, the subscheme Z' is defined via the two equations

$$\begin{cases}(\sqrt{2}x+(1+\sqrt{2})y-z)+(-\sqrt{2}x+(1-\sqrt{2})y-z)=0\\ (2x+(\sqrt{2}+2)y-\sqrt{2}z)+(2x+(-\sqrt{2}+2)y+\sqrt{2}z)=0.\end{cases}$$

Simplifying, this amounts to

$$\begin{cases}2y-2z=0\\ 4x+4y=0.\end{cases}$$

In other words, we deduce that $y = z$ and $x = -y$. The only projective point satisfying both relations simultaneously is $(-1 : 1 : 1) = (-2 : 2 : 2)$, so our result agrees with what we obtained by inspection.

In order to get more mileage out of Theorem 5.3.1, we now introduce the notion of the Seshadri constant, which plays a central role in the approximation results in [13], [14], and [6].

Definition 5.3.1. Let X be a projective variety defined over k, let Z be a closed subscheme of X defined over $\overline{k}$, and let L be an ample line bundle on X. The *Seshadri constant* $\epsilon_Z(L)$ is defined to be

$$\epsilon_Z(L) := \sup\{\gamma \geq 0 : \pi^*L - \gamma E \text{ is ample}\}$$

where $\pi : \tilde{X} \to X_{\overline{k}}$ is the blowup of $X_{\overline{k}} := X \times_k \overline{k}$ at Z with exceptional divisor E. Here, by abuse of notation, we also use L for the base change of L to $X_{\overline{k}}$.

The definition of the Seshadri constant for points, as used in [13], for instance, is given in slightly more generality. There, L is allowed to be a nef line bundle, and the supremum taken in the definition ranges over those $\gamma \geq 0$ for which $L_\gamma := \pi^*L - \gamma E$ is nef. (Recall that a Cartier divisor D is *nef* if its intersection number $D \cdot C$ is nonnegative for all irreducible curves C. The definition applies to line bundles via the Cartier divisor–line bundle correspondence).

However, when L is an ample line bundle and Z is a single point, taking the supremum over those γ for which L_γ is nef is the same as taking the supremum over those γ for which L_γ is ample. Indeed, in Demailly's original paper [3] defining the Seshadri constant, it is established that when Z is a single point x, for all rational $\gamma \in (0, \epsilon_x(L))$, the line bundle L_γ is itself ample. As noted in [14], this appears on page 98 of [3] as a special case of the statement "$F_{p,q}$ is ample whenever $p > q/\epsilon_x(L)$".

In turn, this implies that when using "ample" instead of "nef" in the definition of the Seshadri constant for an ample line bundle at a point, the value of the constant is at least as large. Conversely, since all ample line bundles are nef, the "ample" Seshadri constant cannot be larger than the "nef" one, so we see that our definition agrees with the conventional one in the case of ample line bundles.

The reason for making this definition is that we get the following slick corollary of Theorem 5.3.1:

Corollary 5.3.1. *Let X be a projective variety defined over k and let Z be a closed subscheme of X with field of definition K. If $[K:k]=d$, $[K_v:k_v]=m_v$, and L is an ample line bundle on X, then $\alpha_Z(L) \geq (m_v/d)\cdot \epsilon_Z(L)$.*

Proof. We set notation to match what is given in Theorem 5.3.1. By definition of the Seshadri constant, for all $\gamma \in (0, \epsilon_Z(L))$, the line bundle $L_\gamma := \pi^*L - \gamma E$ is ample on $\tilde{X}$. Therefore, the stable base locus of L_γ is empty. Applying part (1) of Theorem 5.3.1, we see that for *every* sequence $\{x_i\}$ of k-points approximating Z, we have $\alpha_Z(\{x_i\}, L) \geq \gamma m_v/d$, so that $\alpha_Z(L) \geq \gamma m_v/d$. Since $\gamma < \epsilon_Z(L)$ is arbitrary, we get $\alpha_Z(L) \geq (m_v/d)\cdot\epsilon_Z(L)$. □

This is the natural generalization of the main Liouville-type result in [14] (Corollary 3.5), as well as Liouville's original 1844 theorem. To conclude, we will say a few words about the avenues left to explore. The main challenge is to test the conjecture that the lower bound in Proposition 3.2.1 is actually an equality, provided we rule out certain obstructions, such as those raised by Theorem 3.3.1.

Suppose we wanted to set out to show that the lower bound on $\alpha_Z(L)$ produced in Proposition 3.2.1 is also an upper bound. For simplicity, let's consider the case where all the hypersurfaces defining Z have the same degree, and we are working with the archimedean place of $\mathbb{Q}$. In other words, if Z is the intersection of hypersurfaces of degree d, we want to prove that $\alpha_Z(L) \leq \frac{1}{d}$. Note it is enough to produce a sequence $\{x_i\}$ of points in $\mathbb{P}^n(\mathbb{Q})$ not lying on Z for which $d_v(x_i, Z)^{1/d} H_L(x_i)$ is bounded above. Since exponentiating a sequence by a positive integer does not affect its boundedness, it is enough to find a sequence such that $d_v(x_i, Z) H_L(x_i)^d$ is bounded above.

Now, we know that Z is the intersection of finitely many hypersurfaces, all of degree d. If D is the divisor of one of those hypersurfaces, then it follows by the definition of the distance function that we need to show $d_v(x_i, D) H_L(x_i)^d$ is bounded above for all such D. On the other hand, since dL is linearly equivalent to each such divisor D on $\mathbb{P}^n$, our task is really to prove that $d_v(x_i, D) H_D(x_i)$ is bounded above. If x_i belongs to the support of D, we automatically have $d_v(x_i, D) = 0$, so we may assume that x_i does not belong to $\operatorname{Supp} D$. In this case, we take logarithms, and we study when $-\lambda_{D,v}(x_i) + h_D(x_i)$ is bounded above.

Because we have assumed that x_i does not belong to $\operatorname{Supp} D$, we can apply the local-global formula for the height function $h_D(x_i)$ to find that

$$h_D(x_i) = \sum_w \lambda_{D,w}(x_i) + O(1),$$

where the sum runs over all places of $\mathbb{Q}$. Consequently, we are reduced to proving that $\sum_{w \neq v} \lambda_{D,w}(x_i)$ is bounded above for some choice of sequence x_i. Rephrasing, it is enough to find an infinite collection of D-*integral points*, in the sense defined in §1.4 of [21]. In other words, our task reduces to finding an infinite collection of points not lying on $\operatorname{Supp} D$ for which $\lambda_{D,w}$ is bounded above for all non-archimedean places of $\mathbb{Q}$ and for which the upper bound is 0 for all but finitely many places. This illustrates the close connection between the fundamental questions of Diophantine geometry and the subject matter of this thesis.

References

[1] Frits Beukers. *Integral points on cubic surfaces*, volume 19 of *Number theory (Ottawa, ON 1996)*, pages 25–33. Amer. Math. Soc., Providence, RI, 1999.

[2] Kwok-Kwong Choi and Jeffrey D. Vaaler. *Diophantine approximation in projective space*, volume 19 of *Number theory (Ottawa, ON 1996)*, pages 55–65. Amer. Math. Soc., Providence, RI, 1999.

[3] Jean-Pierre Demailly. *Singular Hermitian metrics on positive line bundles*, volume 1507 of *Complex algebraic varieties (Bayreuth, 1990)*, pages 87–104. Springer, Berlin, 1992.

[4] Antonio J. Engler and Alexander Prestel. *Valued fields*. Springer-Verlag, Berlin, 2005.

[5] William Fulton. *Intersection theory*, volume 2. Springer-Verlag, Berlin, second edition, 1998.

[6] Nathan Grieve. Diophantine approximation constants for varieties over function fields. *Michigan Mathematical Journal*, 67(2):371–404, 2018.

[7] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977.

[8] David Hilbert. *The theory of algebraic number fields*. Springer-Verlag, Berlin, 1998.

[9] Marc Hindry and Joseph H. Silverman. *Diophantine geometry: An Introduction*, volume 201. Springer-Verlag, New York, 2000.

[10] Robert Lazarsfeld. *Positivity in algebraic geometry. I*, volume 48. Springer-Verlag, Berlin, 2004.

[11] Adam Logan, David McKinnon, and Ronald van Luijk. Density of rational points on diagonal quartic surfaces. *Algebra & Number Theory*, 4(1):1–20, 2010.

[12] David McKinnon. A conjecture on rational approximations to rational points. *Journal of Algebraic Geometry*, 16(2):257–303, 2007.

[13] David McKinnon and Mike Roth. Seshadri constants, Diophantine approximation, and Roth's theorem for arbitrary varieties. *Inventiones Mathematicae*, 200(2):513–583, 2015.

[14] David McKinnon and Mike Roth. An analogue of Liouville's Theorem and an application to cubic surfaces. *European Journal of Mathematics*, 2(4):929–959, 2016.

[15] Alain M. Robert. *A course in p-adic analysis*, volume 198. Springer-Verlag, New York, 2000.

[16] K. F. Roth. Rational approximations to algebraic numbers. *Mathematika.A Journal of Pure and Applied Mathematics*, 2:1–20, 1955.

[17] Min Ru and Julie Tzu-Yueh Wang. A subspace theorem for subvarieties. *Algebra & Number Theory*, 11(10):2323–2337, 2017.

[18] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem.* Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997.

[19] Joseph H. Silverman. Arithmetic distance functions and height functions in Diophantine geometry. *Mathematische Annalen*, 279(2):193–216, 1987.

[20] Joseph H. Silverman. On the distribution of integer points on curves of genus zero. *Theoretical Computer Science*, 235(1):163–170, 2000.

[21] Paul Vojta. *Diophantine approximations and value distribution theory*, volume 1239. Springer-Verlag, Berlin, 1987.

Appendix A

Details from the Proof of Theorem 4.4.1

In this appendix, we fill in some of the computational details required to prove Theorem 4.4.1. For convenience, we recall it here:

Theorem 4.4.1. *Let S denote the cubic surface*

$$x^3 + 2y^3 + 7z^3 + dw^3 = 0,$$

where $d \neq 0$ is an integer with cube-free part divisible by a prime different from 2, 3, and 7. If C is a curve on S defined over $\mathbb{Q}$, then the degree of C (in $\mathbb{P}^3$) is divisible by 3. In particular, S does not contain any lines, conics, or quartics defined over $\mathbb{Q}$.

There are two computational gaps in the proof that need to be filled. Firstly, we must compute an explicit basis for $\mathrm{Pic}(S)$ consisting of 7 of the lines on S. Secondly, we must get a handle on the structure of the group $G = \mathrm{Gal}(k/\mathbb{Q})$, where $k = \mathbb{Q}(\zeta, \sqrt[3]{2}, \sqrt[3]{7}, \sqrt[3]{d})$ is the field of definition for the set of 27 lines on S (and ζ is a fixed primitive cube root of unity). Once we have the structure of G, we act on the basis lines for $\mathrm{Pic}(S)$ using the elements of G, in order to compute values of the character χ_G attached to the associated representation of G on the vector space $V = \mathrm{Pic}(S) \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}$.

A.1 An Explicit Basis for $\mathrm{Pic}(S)$

To compute the basis for $\mathrm{Pic}(S)$, it suffices to compute a basis for the Picard group of the diagonal cubic surface S_0 given by $x^3 + y^3 + z^3 + w^3 = 0$, since this surface is clearly isomorphic to S over $\overline{\mathbb{Q}}$. We begin by laying out some notation for the 27 lines, in agreement with our notation in the "main" proof of the theorem. Let ζ denote a fixed primitive cube root of unity. For $1 \leq i, j \leq 3$, we set L_{1ij} to be the line

$$\begin{cases} x + \zeta^{i-1} y = 0 \\ z + \zeta^{j-1} w = 0. \end{cases}$$

Likewise, for $1 \leq i, j \leq 3$, we set L_{2ij} and L_{3ij}, respectively, to be the lines

$$\begin{cases} x + \zeta^{i-1} z = 0 \\ y + \zeta^{j-1} w = 0 \end{cases} \quad \begin{cases} x + \zeta^{i-1} w = 0 \\ y + \zeta^{j-1} z = 0. \end{cases}$$

Our claim is that the divisor classes of the lines $L_{112}, L_{121}, L_{133}, L_{222}, L_{311}, L_{322}, L_{333}$ form a basis for this Picard group. Since we know *a priori* that $\mathrm{Pic}(S_0)$ is free of rank 7 and generated by the 27 lines on S_0, it suffices to express the remaining 20 lines as linear combinations of these 7 lines in $\mathrm{Pic}(S_0)$.

We claim that the following table gives the coefficients expressing all 27 lines as linear combinations of our purported basis lines:

Generator of $\mathrm{Pic}(S_0)$	L_{112}	L_{121}	L_{133}	L_{222}	L_{311}	L_{322}	L_{333}
L_{111}	-1	-1	2	2	-1	1	-1
L_{112}	1	0	0	0	0	0	0
L_{113}	-1	0	0	1	0	1	0
L_{121}	0	1	0	0	0	0	0
L_{122}	-1	-1	1	1	0	1	0
L_{123}	0	-1	1	2	-1	1	-1
L_{131}	0	-1	0	1	0	1	0
L_{132}	-1	0	1	2	-1	1	-1
L_{133}	0	0	1	0	0	0	0
L_{211}	0	0	0	1	-1	1	0
L_{212}	-1	0	1	1	0	1	-1
L_{213}	0	-1	1	1	0	0	0
L_{221}	0	-1	1	1	0	1	-1
L_{222}	0	0	0	1	0	0	0
L_{223}	-1	0	1	1	-1	1	0
L_{231}	-1	0	1	1	0	0	0
L_{232}	0	-1	1	1	-1	1	0
L_{233}	0	0	0	1	0	1	-1
L_{311}	0	0	0	0	1	0	0
L_{312}	0	0	1	1	-1	0	0
L_{313}	-1	-1	1	2	-1	2	-1
L_{321}	-1	-1	1	2	-1	1	0
L_{322}	0	0	0	0	0	1	0
L_{323}	0	0	1	1	0	0	-1
L_{331}	0	0	1	1	-1	1	-1
L_{332}	-1	-1	1	2	0	1	-1
L_{333}	0	0	0	0	0	0	1

To verify the relations in this table, we produce relations among these lines in the Picard group, obtained by taking a series of planes through subsets of these lines. For example, the divisor $\mathrm{div}(x + y)$ on S_0 is $L_{111} + L_{112} + L_{113}$, because these are exactly the lines forming the intersection of $x + y = 0$ with the surface S_0. We form relations by noting, for example, that $\mathrm{div}(x + y) \sim \mathrm{div}(x + z)$, because $\mathrm{div}(x + y) - \mathrm{div}(x + z) = \mathrm{div}((x+y)/(x+z))$ is the divisor of a rational function. In this particular case, we get the relation $L_{111} + L_{112} + L_{113} \sim L_{211} + L_{212} + L_{213}$.

The easiest non-trivial relations in the table to verify are the following:

$$\begin{aligned}
L_{113} &\sim -L_{112} + L_{222} + L_{322} \\
L_{131} &\sim -L_{121} + L_{222} + L_{322} \\
L_{211} &\sim L_{222} - L_{311} + L_{322} \\
L_{213} &\sim -L_{121} + L_{133} + L_{222} \\
L_{231} &\sim -L_{112} + L_{133} + L_{222} \\
L_{233} &\sim L_{222} + L_{322} - L_{333} \\
L_{312} &\sim L_{133} + L_{222} - L_{311} \\
L_{323} &\sim L_{133} + L_{222} - L_{333}.
\end{aligned}$$

These amount to rewritten versions of the following relations, respectively:

$$\begin{aligned}
\mathrm{div}(x + y) &\sim \mathrm{div}((x + \zeta z) + (y + \zeta w)) \\
\mathrm{div}(z + w) &\sim \mathrm{div}((x + \zeta z) + (y + \zeta w)) \\
\mathrm{div}((x + y) + (z + w)) &\sim \mathrm{div}((x + \zeta z) + (y + \zeta w)) \\
\mathrm{div}((x + \zeta y) + (z + w)) &\sim \mathrm{div}((x + \zeta z) + \zeta^2(y + \zeta w)) \\
\mathrm{div}((x + \zeta^2 z) + (y + w)) &\sim \mathrm{div}((x + \zeta^2 y) + \zeta(z + \zeta^2 w)) \\
\mathrm{div}((x + y) + \zeta^2(z + w)) &\sim \mathrm{div}((x + \zeta z) + (y + \zeta w)) \\
\mathrm{div}(x + w) &\sim \mathrm{div}((x + \zeta^2 y) + \zeta(z + \zeta^2 w)) \\
\mathrm{div}(y + \zeta^2 z) &\sim \mathrm{div}((x + \zeta^2 y) + \zeta(z + \zeta^2 w)).
\end{aligned}$$

Now, we look at the relations at the next level of difficulty to verify, namely

$$\begin{aligned}
L_{122} &\sim -L_{112} - L_{121} + L_{133} + L_{222} + L_{322} \\
L_{212} &\sim -L_{112} + L_{133} + L_{222} + L_{322} - L_{333} \\
L_{221} &\sim -L_{121} + L_{133} + L_{222} + L_{322} - L_{333} \\
L_{223} &\sim -L_{112} + L_{133} + L_{222} - L_{311} + L_{322} \\
L_{232} &\sim -L_{121} + L_{133} + L_{222} - L_{311} + L_{322} \\
L_{331} &\sim L_{133} + L_{222} - L_{311} + L_{322} - L_{333}.
\end{aligned}$$

In turn, these amount to simplified versions of the following relations:

$$\begin{aligned}
&\operatorname{div}(z+\zeta w)+\operatorname{div}((x+\zeta y)+(z+w))\\
&\sim \operatorname{div}((x+\zeta z)+\zeta^2(y+\zeta w))+\operatorname{div}((x+\zeta w)+\zeta^2(y+\zeta z))\\
&\operatorname{div}(x+y)+\operatorname{div}((x+\zeta^2 w)+\zeta(y+\zeta^2 z))\\
&\sim \operatorname{div}(z+\zeta^2 w)+\operatorname{div}((x+\zeta z)+(y+\zeta w))\\
&\operatorname{div}(z+w)+\operatorname{div}((x+\zeta^2 w)+\zeta^2(y+\zeta^2 z))\\
&\sim \operatorname{div}(x+\zeta^2 y)+\operatorname{div}((x+\zeta z)+(y+\zeta w))\\
&\operatorname{div}((x+w)+(y+z))+\operatorname{div}((x+\zeta^2 w)+(y+\zeta z))\\
&\sim \operatorname{div}((x+\zeta^2 w)+\zeta^2(y+\zeta z))+\operatorname{div}((x+\zeta z)+(y+\zeta w))\\
&\operatorname{div}(z+w)+\operatorname{div}((x+w)+\zeta^2(y+z))\\
&\sim \operatorname{div}(x+\zeta^2 y)+\operatorname{div}((x+\zeta z)+(y+\zeta w))\\
&\operatorname{div}(y+z)+\operatorname{div}((x+y)+\zeta^2(z+w))\\
&\sim \operatorname{div}((x+\zeta^2 y)+\zeta^2(z+\zeta^2 w))+\operatorname{div}((x+\zeta z)+(y+\zeta w)).
\end{aligned}$$

Now, we move up to the relations at the next level of complexity, which are

$$\begin{aligned}
L_{123} &\sim -L_{121}+L_{133}+2L_{222}-L_{311}+L_{322}-L_{333}\\
L_{132} &\sim -L_{112}+L_{133}+2L_{222}-L_{311}+L_{322}-L_{333}\\
L_{321} &\sim -L_{112}-L_{121}+L_{133}+2L_{222}-L_{311}+L_{322}\\
L_{332} &\sim -L_{112}-L_{121}+L_{133}+2L_{222}+L_{322}-L_{333}.
\end{aligned}$$

These four relations are simplified versions of the following:

$$\begin{aligned}
&\operatorname{div}(x+\zeta y)+\operatorname{div}(x+w)+\operatorname{div}((x+y)+\zeta^2(z+w))\\
&\sim \operatorname{div}((x+\zeta z)+(y+\zeta w))+\operatorname{div}((x+\zeta z)+\zeta^2(y+\zeta w))+\operatorname{div}((x+\zeta y)+\zeta^2(z+\zeta w))\\
&\operatorname{div}(x+y)+\operatorname{div}(x+w)+\operatorname{div}((x+\zeta^2 w)+\zeta^2(y+\zeta^2 z))\\
&\sim \operatorname{div}((x+\zeta z)+(y+\zeta w))+\operatorname{div}((x+\zeta z)+\zeta^2(y+\zeta w))+\operatorname{div}((x+y)+\zeta(z+\zeta^2 w))\\
&\operatorname{div}(x+y)+\operatorname{div}(y+z)+\operatorname{div}(x+\zeta y)\\
&\sim \operatorname{div}(z+\zeta^2 w)+\operatorname{div}((x+\zeta y)+\zeta(z+\zeta w))+\operatorname{div}((x+y)+\zeta(z+w))\\
&\operatorname{div}(x+y)+\operatorname{div}(x+\zeta^2 w)+\operatorname{div}((x+\zeta y)+(z+w))\\
&\sim \operatorname{div}((x+\zeta z)+(y+\zeta w))+\operatorname{div}((x+\zeta z)+\zeta^2(y+\zeta w))+\operatorname{div}((x+y)+(z+\zeta^2 w)).
\end{aligned}$$

Finally, we have two more relations of an even greater complexity:

$$\begin{aligned}
L_{111} &\sim -L_{112}-L_{121}+2L_{133}+2L_{222}-L_{311}+L_{322}-L_{333}\\
L_{313} &\sim -L_{112}-L_{121}+L_{133}+2L_{222}-L_{311}+2L_{322}-L_{333}.
\end{aligned}$$

These can be obtained by simplifying the following relations:

$$\begin{aligned}
&\operatorname{div}(x+y)+\operatorname{div}(x+\zeta y)+\operatorname{div}(x+w)+\operatorname{div}(x+\zeta^2 w)\\
&\sim \operatorname{div}(z+\zeta^2 w)+\operatorname{div}(y+\zeta z)+\operatorname{div}((x+\zeta z)+\zeta^2(y+\zeta w))+\operatorname{div}((x+\zeta z)+\zeta(y+\zeta w))\\
&\operatorname{div}(x+y)+\operatorname{div}(x+\zeta y)+\operatorname{div}(x+w)+\operatorname{div}(x+\zeta^2 w)\\
&\sim \operatorname{div}(z+\zeta^2 w)+\operatorname{div}(y+\zeta z)+\operatorname{div}((x+\zeta z)+(y+\zeta w))+\operatorname{div}((x+\zeta z)+\zeta(y+\zeta w)).
\end{aligned}$$

A.2 The Structure of G

Having proved all the relations in the table, we can now move on to the representation theory portion of the argument. For all values of d, the field of definition of the 27 lines on S is $k := \mathbb{Q}(\zeta, \sqrt[3]{2}, \sqrt[3]{7}, \sqrt[3]{d})$. In the theorem, we restrict to the case where the cube-free part of d is divisible by a prime other than 2, 3 and 7, which guarantees that $[k : \mathbb{Q}] = 54$ (by a ramification argument), and that k is a Galois extension of $\mathbb{Q}$ (in fact, it is the splitting field of the polynomial $(x^3-2)(x^3-7)(x^3-d)$ over $\mathbb{Q}$).

In this case, $G = \mathrm{Gal}(k/\mathbb{Q})$ is a group of order 54. We eventually want to compute $\langle \chi_G, \chi_{\mathrm{triv}} \rangle$. Since characters are class functions, constant on conjugacy classes, we will aim to compute the conjugacy classes of G and work out the value of χ_G at one representative of each class.

As with every group, the identity element of G forms a single conjugacy class. To describe the other classes, it will be helpful to describe the structure of G more completely. Since $54 = 2 \cdot 3^3$, Sylow theory tells us that the number of Sylow 3-subgroups of G is congruent to 1 mod 3 and also divides 2. Consequently, there is a unique (necessarily normal) Sylow 3-subgroup H, of order 27.

Necessarily, G/H is a cyclic group of order 2, and in particular, it is abelian. We deduce immediately that the commutator subgroup G' is contained in H. Our claim is that $G' = H$, but in order to show this, we should describe H more explicitly.

The fundamental theorem of Galois theory tells us that the index 2 subgroup H is of the form $\mathrm{Gal}(k/\ell)$, where ℓ is an intermediate quadratic extension of $\mathbb{Q}$. Obviously, $\mathbb{Q}(\zeta)$ is such a quadratic extension, so we conclude that $H = \mathrm{Gal}(k/\mathbb{Q}(\zeta))$ by uniqueness of H. In other words, the subgroup H consists of the automorphisms of k that leave ζ fixed.

On the other hand, we can immediately exhibit 27 such distinct automorphisms σ_{ijk}, where $i, j, k \in \{0, 1, 2\}$. These are given by the following four conditions:

$$\begin{cases} \sigma_{ijk}(\sqrt[3]{2}) = \zeta^i \sqrt[3]{2} \\ \sigma_{ijk}(\sqrt[3]{7}) = \zeta^j \sqrt[3]{7} \\ \sigma_{ijk}(\sqrt[3]{d}) = \zeta^k \sqrt[3]{d} \\ \sigma_{ijk}(\zeta) = \zeta. \end{cases}$$

It is easy to verify (using elementary Galois theory) that all of these do in fact give well-defined automorphisms of k fixing ζ. All the maps σ_{ijk} are clearly different from each other, and one can immediately check that

$$\sigma_{i_0,j_0,k_0} \circ \sigma_{i_1,j_1,k_1} = \sigma_{i_2,j_2,k_2},$$

where $i_2 \equiv i_0 + i_1 \pmod 3$, $j_2 \equiv j_0 + j_1 \pmod 3$, and $k_2 \equiv k_0 + k_1 \pmod 3$. These observations show that the collection of σ_{ijk} form a subgroup of G isomorphic to $C_3 \times C_3 \times C_3$, and by uniqueness, this is the Sylow 3-subgroup H.

Since we already know that G' is a subgroup of H, showing that $G' = H$ reduces to checking that every element of H is a commutator in G. For this, let $\pi \in G$ be the automorphism determined by the conditions

$$\begin{cases} \pi(\zeta) = \zeta^2 \\ \pi(\sqrt[3]{2}) = \sqrt[3]{2} \\ \pi(\sqrt[3]{7}) = \sqrt[3]{7} \\ \pi(\sqrt[3]{d}) = \sqrt[3]{d}. \end{cases}$$

We can immediately verify that for any i, j, k, we have $\pi \circ \sigma_{ijk} \circ \pi^{-1} \circ \sigma_{ijk}^{-1} = \sigma_{ijk}$, just by checking the action of both sides on the elements ζ, $\sqrt[3]{2}$, $\sqrt[3]{7}$, $\sqrt[3]{d}$. This demonstrates that every element of H is a commutator, completing the proof that $G' = H$.

Now, we are ready to discuss the conjugacy classes in G. Since H is an index 2 subgroup and $\pi \notin H$, every element of G is either of the form σ_{ijk} or $\pi\sigma_{ijk}$ for some choices of $i, j, k \in \{0, 1, 2\}$. Since our previous relation $\pi \circ \sigma_{ijk} \circ \pi^{-1} \circ \sigma_{ijk}^{-1} = \sigma_{ijk}$ can be simplified to $\pi \circ \sigma_{ijk} = \sigma_{ijk}^2 \circ \pi$, this essentially gives us the information needed to multiply any two elements of the group.

We claim that for any triples (i_0, j_0, k_0) and (i_1, j_1, k_1), the elements $\pi\sigma_{i_0,j_0,k_0}$ and $\pi\sigma_{i_1,j_1,k_1}$ are conjugate. Given the elements $\pi\sigma_{i_0,j_0,k_0}$ and $\pi\sigma_{i_1,j_1,k_1}$, if we take our subscripts modulo 3 (as we may), then

$$\begin{aligned} \sigma_{i_1-i_0,j_1-j_0,k_1-k_0}(\pi\sigma_{i_0,j_0,k_0})\sigma_{i_1-i_0,j_1-j_0,k_1-k_0}^{-1} &= \pi\sigma_{i_1-i_0,j_1-j_0,k_1-k_0}^2\sigma_{i_0,j_0,k_0}\sigma_{i_1-i_0,j_1-j_0,k_1-k_0}^{-1} \\ &= \pi\sigma_{i_0,j_0,k_0}\sigma_{i_1-i_0,j_1-j_0,k_1-k_0} \\ &= \pi\sigma_{i_1,j_1,k_1}, \end{aligned}$$

as needed. This gives us 27 elements in the same conjugacy class, and since the size of each conjugacy class divides the order of the group (and it is not possible for the entire group to be a conjugacy class), we conclude that these 27 elements form a complete conjugacy class in G.

So, it remains to sort the elements σ_{ijk}, with $(i, j, k) \neq (0, 0, 0)$, into conjugacy classes. Since H is abelian, conjugating σ_{ijk} by any element of H will give us σ_{ijk} again. On the other hand, if we conjugate σ_{ijk} by an element of the form $\pi\sigma_{i_0,j_0,k_0}$, then we get

$$(\pi\sigma_{i_0,j_0,k_0})\sigma_{ijk}(\pi\sigma_{i_0,j_0,k_0})^{-1} = \pi\sigma_{ijk}\pi = \sigma_{ijk}^{-1}.$$

Therefore, the conjugates of σ_{ijk} are exactly σ_{ijk} and σ_{ijk}^{-1}, which means these 26 remaining non-identity elements of G split into 13 more conjugacy classes, one for each subgroup of order 3 inside of $H \cong C_3 \times C_3 \times C_3$.

A.3 Computing Values of χ_G

For this part of the proof, we revert to the notation in the "main" argument, so that the lines L_{1ij}, L_{2ij}, L_{3ij} refer to lines on S, rather than the scaled surface S_0.

At last, we are ready to compute $\langle \chi_G, \chi_{\text{triv}} \rangle$. Based on the previous section, a complete set of conjugacy class representatives of G is:

$$\sigma_{000} = \text{id}, \pi, \sigma_{100}, \sigma_{010}, \sigma_{001}, \sigma_{110}, \sigma_{101}, \sigma_{011}, \sigma_{111}, \sigma_{120}, \sigma_{102}, \sigma_{012}, \sigma_{112}, \sigma_{121}, \sigma_{211}.$$

Taking the size of these classes into account, we have

$$\begin{aligned}
&\langle \chi_G, \chi_{\text{triv}} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_G(g) \\
&= \frac{1}{54}(\chi_G(\text{id}) + 27\chi_G(\pi) + 2\chi_G(\sigma_{100}) + 2\chi_G(\sigma_{010}) + 2\chi_G(\sigma_{001}) + 2\chi_G(\sigma_{110}) + 2\chi_G(\sigma_{101}) \\
&+ 2\chi_G(\sigma_{011}) + 2\chi_G(\sigma_{111}) + 2\chi_G(\sigma_{120}) + 2\chi_G(\sigma_{102}) + 2\chi_G(\sigma_{012}) + 2\chi_G(\sigma_{112}) + 2\chi_G(\sigma_{121}) \\
&+ 2\chi_G(\sigma_{211})).
\end{aligned}$$

Now, we just have to compute the action of each conjugacy class representative on our basis for $\text{Pic}(S)$ and take the traces of the corresponding matrices. Since our vector space is 7-dimensional, clearly $\chi_G(\text{id}) = 7$.

We check the action of the other conjugacy class representatives on our seven basis lines below:

Action of π:	Action of σ_{010}:	Action of σ_{110}:	Action of σ_{011}:	Action of σ_{120}:
$L_{112} \mapsto L_{113}$	$L_{112} \mapsto L_{111}$	$L_{112} \mapsto L_{121}$	$L_{112} \mapsto L_{112}$	$L_{112} \mapsto L_{123}$
$L_{121} \mapsto L_{131}$	$L_{121} \mapsto L_{123}$	$L_{121} \mapsto L_{133}$	$L_{121} \mapsto L_{121}$	$L_{121} \mapsto L_{132}$
$L_{133} \mapsto L_{122}$	$L_{133} \mapsto L_{132}$	$L_{133} \mapsto L_{112}$	$L_{133} \mapsto L_{133}$	$L_{133} \mapsto L_{111}$
$L_{222} \mapsto L_{233}$	$L_{222} \mapsto L_{232}$	$L_{222} \mapsto L_{231}$	$L_{222} \mapsto L_{233}$	$L_{222} \mapsto L_{211}$
$L_{311} \mapsto L_{311}$	$L_{311} \mapsto L_{312}$	$L_{311} \mapsto L_{311}$	$L_{311} \mapsto L_{322}$	$L_{311} \mapsto L_{312}$
$L_{322} \mapsto L_{333}$	$L_{322} \mapsto L_{323}$	$L_{322} \mapsto L_{322}$	$L_{322} \mapsto L_{333}$	$L_{322} \mapsto L_{323}$
$L_{333} \mapsto L_{322}$	$L_{333} \mapsto L_{331}$	$L_{333} \mapsto L_{333}$	$L_{333} \mapsto L_{311}$	$L_{333} \mapsto L_{331}$

Action of σ_{100}:	Action of σ_{001}:	Action of σ_{101}:	Action of σ_{111}:	Action of σ_{102}:
$L_{112} \mapsto L_{122}$	$L_{112} \mapsto L_{113}$	$L_{112} \mapsto L_{123}$	$L_{112} \mapsto L_{122}$	$L_{112} \mapsto L_{121}$
$L_{121} \mapsto L_{131}$	$L_{121} \mapsto L_{122}$	$L_{121} \mapsto L_{132}$	$L_{121} \mapsto L_{131}$	$L_{121} \mapsto L_{133}$
$L_{133} \mapsto L_{113}$	$L_{133} \mapsto L_{131}$	$L_{133} \mapsto L_{111}$	$L_{133} \mapsto L_{113}$	$L_{133} \mapsto L_{112}$
$L_{222} \mapsto L_{221}$	$L_{222} \mapsto L_{223}$	$L_{222} \mapsto L_{222}$	$L_{222} \mapsto L_{232}$	$L_{222} \mapsto L_{223}$
$L_{311} \mapsto L_{313}$	$L_{311} \mapsto L_{321}$	$L_{311} \mapsto L_{323}$	$L_{311} \mapsto L_{321}$	$L_{311} \mapsto L_{333}$
$L_{322} \mapsto L_{321}$	$L_{322} \mapsto L_{332}$	$L_{322} \mapsto L_{331}$	$L_{322} \mapsto L_{332}$	$L_{322} \mapsto L_{311}$
$L_{333} \mapsto L_{332}$	$L_{333} \mapsto L_{313}$	$L_{333} \mapsto L_{312}$	$L_{333} \mapsto L_{313}$	$L_{333} \mapsto L_{322}$

Action of σ_{012}:	Action of σ_{112}:	Action of σ_{121}:	Action of σ_{211}:
$L_{112} \mapsto L_{113}$	$L_{112} \mapsto L_{123}$	$L_{112} \mapsto L_{121}$	$L_{112} \mapsto L_{132}$
$L_{121} \mapsto L_{122}$	$L_{121} \mapsto L_{132}$	$L_{121} \mapsto L_{133}$	$L_{121} \mapsto L_{111}$
$L_{133} \mapsto L_{131}$	$L_{133} \mapsto L_{111}$	$L_{133} \mapsto L_{112}$	$L_{133} \mapsto L_{123}$
$L_{222} \mapsto L_{231}$	$L_{222} \mapsto L_{233}$	$L_{222} \mapsto L_{212}$	$L_{222} \mapsto L_{231}$
$L_{311} \mapsto L_{332}$	$L_{311} \mapsto L_{331}$	$L_{311} \mapsto L_{322}$	$L_{311} \mapsto L_{323}$
$L_{322} \mapsto L_{313}$	$L_{322} \mapsto L_{312}$	$L_{322} \mapsto L_{333}$	$L_{322} \mapsto L_{331}$
$L_{333} \mapsto L_{321}$	$L_{333} \mapsto L_{323}$	$L_{333} \mapsto L_{311}$	$L_{333} \mapsto L_{312}$

To compute the traces of these linear maps, we use the table of relations from the first section of this appendix to rewrite the image of each line as a linear combination of the seven basis lines, and then add up the "diagonal" contributions. For example, via the table of relations, the action of π can be written out as follows:

$$\begin{aligned}
L_{112} &\mapsto -L_{112} + L_{222} + L_{322} \\
L_{121} &\mapsto -L_{121} + L_{222} + L_{322} \\
L_{133} &\mapsto -L_{112} - L_{121} + L_{133} + L_{222} + L_{322} \\
L_{222} &\mapsto L_{222} + L_{322} - L_{333} \\
L_{311} &\mapsto L_{311} \\
L_{322} &\mapsto L_{333} \\
L_{333} &\mapsto L_{322}.
\end{aligned}$$

Summing up the diagonal contributions, we conclude that

$$\chi_G(\pi) = (-1) + (-1) + 1 + 1 + 1 + 0 + 0 = 1.$$

Similarly, one computes that

$$\begin{aligned}
\chi_G(\sigma_{100}) &= (-1) + (-1) + 0 + 1 + (-1) + 1 + (-1) = -2 \\
\chi_G(\sigma_{010}) &= (-1) + (-1) + 1 + 1 + (-1) + 0 + (-1) = -2 \\
\chi_G(\sigma_{001}) &= (-1) + (-1) + 0 + 1 + (-1) + 1 + (-1) = -2 \\
\chi_G(\sigma_{110}) &= 0 + 0 + 0 + 1 + 1 + 1 + 1 = 4 \\
\chi_G(\sigma_{101}) &= 0 + 0 + 2 + 1 + 0 + 1 + 0 = 4 \\
\chi_G(\sigma_{011}) &= 1 + 1 + 1 + 1 + 0 + 0 + 0 = 4 \\
\chi_G(\sigma_{111}) &= (-1) + (-1) + 0 + 1 + (-1) + 1 + (-1) = -2 \\
\chi_G(\sigma_{120}) &= 0 + 0 + 2 + 1 + (-1) + 0 + (-1) = 1 \\
\chi_G(\sigma_{102}) &= 0 + 0 + 0 + 1 + 0 + 0 + 0 = 1 \\
\chi_G(\sigma_{012}) &= (-1) + (-1) + 0 + 1 + 0 + 2 + 0 = 1 \\
\chi_G(\sigma_{112}) &= 0 + 0 + 2 + 1 + (-1) + 0 + (-1) = 1 \\
\chi_G(\sigma_{121}) &= 0 + 0 + 0 + 1 + 0 + 0 + 0 = 1 \\
\chi_G(\sigma_{211}) &= (-1) + (-1) + 1 + 1 + 0 + 1 + 0 = 1.
\end{aligned}$$

Altogether then, we find that

$$\begin{aligned}
\langle \chi_G, \chi_{\mathrm{triv}} \rangle &= \frac{1}{54}(\chi_G(\mathrm{id}) + 27\chi_G(\pi) + 2\chi_G(\sigma_{100}) + 2\chi_G(\sigma_{010}) + 2\chi_G(\sigma_{001}) + 2\chi_G(\sigma_{110}) \\
&+ 2\chi_G(\sigma_{101}) + 2\chi_G(\sigma_{011}) + 2\chi_G(\sigma_{111}) + 2\chi_G(\sigma_{120}) + 2\chi_G(\sigma_{102}) + 2\chi_G(\sigma_{012}) + 2\chi_G(\sigma_{112}) \\
&+ 2\chi_G(\sigma_{121}) + 2\chi_G(\sigma_{211})) \\
&= \frac{1}{54}(7 + 27 \cdot 1 + 2 \cdot (-2) + 2 \cdot (-2) + 2 \cdot (-2) + 2 \cdot 4 + 2 \cdot 4 + 2 \cdot 4 + 2 \cdot (-2) + 2 \cdot 1 \\
&+ 2 \cdot 1 + 2 \cdot 1 + 2 \cdot 1 + 2 \cdot 1 + 2 \cdot 1) \\
&= 1.
\end{aligned}$$