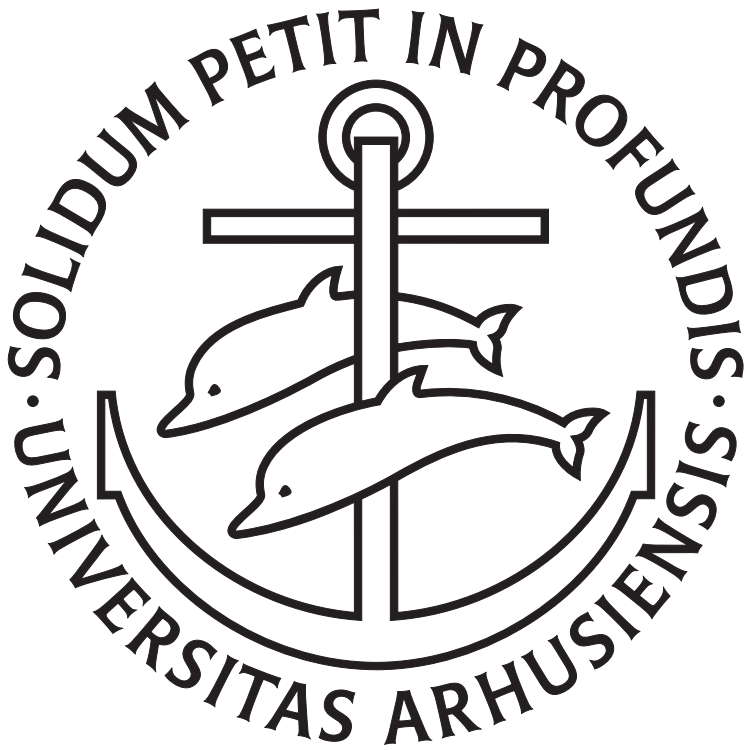
Aarhus University

Intrinsic Diophantine Approximation



PhD Thesis

Author
Morten Hein Tiljeset

Advisor
Simon Kristensen

Abstract

The theory of intrinsic Diophantine approximation concerns the problem of approximating points on a variety by rational points lying on the same variety. We first consider this problem from a metric point of view, where we try to derive results regarding almost all points in the sense of measure. In this direction, we derive a zero-infinity law for Hausdorff measure on certain varieties using a projection argument. The key novelty here is the use of algebraic geometry to control the complexity of the rational points under the projection. Following this, we turn to the problem of finding algorithms for Diophantine approximation on varieties. This is inspired by a problem of constructing efficient universal quantum computers. We consider continued fractions in terms of a certain tree, and use this description to describe the problems in constructing continued fractions for the unit circle. Finally, we consider a problem of finding transcendental numbers which behave like Pisot numbers. We use finite automata to construct transendetal numbers with known Diophantine properties and do a computer search through these.

Resumé

Teorien for intrinsisk Diofantisk approksimation omhandler problemet om at tilnærme punkter på en varitet med rationelle punkter der ligger på den samme varitet. Vi betragter først dette problem fra et metrisk synspunkt, hvor vi prøver at udlede egenskaber for næsten alle punkter i en målteoretisk forstand. I denne retning udleder vi en nul-uendelig lov for Hausdorffmål på visse variteter ved at bruge et projektionsargument. Hovedidéen er her at bruge algebraisk geometri til at styre kompleksiteten af de rationelle punkter under projektionen. Herefter kigger vi på problemet med at finde algoritmer til Diofantisk approksimation på variteter. Dette er inspireret af problemet med at konstruere effektive universelle kvantecomputere. Vi betragter kædebrøker i termer af et vist træ, og bruger denne beskrivelse til at beskrive problemet med at konstruere kædebrøker på enhedscirklen. Endeligt betragter vi spørgsmålet om hvorvidt der findes transcendente tal der opfører sig som Pisottal. Vi bruger endelige automater til at konstruere transcendente tal med kendte Diofantiske egenskaber og søger igennem disse med en computer.

PREFACE

This thesis is the culmination of my work as a graduate student at the Department of Mathematics, Aarhus University. The main subject matter is Diophantine approximation, which roughly concerns the problem of approximating real numbers by simple rational numbers.

After introducing the subject matter in Chapter 1, the thesis naturally splits into three parts: *Metric Theory*, *Continued Fractions* and *Experimental Mathematics*. The unifying theme for the first two parts, is that of *intrinsic Diophantine Approximation*, from which the thesis derives its title. In here, we consider approximation of points by rational points in the same space. The metric theory seeks to quantify, in terms of measure, the size of the "well-approximable" points. The theory of continued fractions, at least from our point of view, seeks to derive algorithms for finding these approximations.

Historically, the theory of continued fractions precedes the metric theory by several millennia. But with our modern technology, it is possible to derive results in the metric direction much more readily than in the algorithmic direction.

In Chapter 2, we introduce the very important notion of Hausdorff measure which generalize the usual notions of length, area and volume, and will be used throughout. The metric theory proper is introduced in Chapter 3, where we discuss the fundamental theorems of Khintchine and Jarník, which provide zero-infinity laws for the size of the set of sufficiently well-approximable points in $\mathbb{R}^n$. Chapter 4 surveys the theory of metric approximation on manifolds. In particular, we discuss the particular problems of the intrinsic theory which is not present in the ambient theory.

The main result of the thesis is Theorem 6.1, which provides an analogue of Jarník's theorem for certain varieties given as a graph of integer polynomials. This result led to the publication [Til17]. In order to derive Theorem 6.1, we need to be able to control the complexity of rational points under certain maps. This is done using projective methods of algebraic geometry and the Nullstellensatz. This theory is covered in Chapter 5. Chapter 6 is dedicated to the proof and discussion of the main result. Compared to the published version, the discussion of Hausdorff measures in Chapter 2 allows us to slightly weaken some assumptions.

In the second part, *Continued Fractions*, we delve into the problem of generating algorithms for approximation. This is motivated by a problem of constructing efficient universal quantum computers, which is discussed in Chapter 7. We take some time to study the classical continued fractions in Chapter 8. We do so from a slightly unorthodox perspective, which more closely aligns the fundamental definition to the question of Diophantine approximation. In Chapter 9, we try to apply this definition to constructing a continued fraction algorithm on the unit circle, unfortunately without much success.

Finally, the third part of the thesis, *Experimental Mathematics*, is somewhat disjoint from the rest. It concerns the distribution of numbers modulo one, and in particular an attempt at finding transcendental numbers with exceptional behavior. In a joint work with my advisor, Simon Kristensen, we generate transcendental numbers with known Diophantine properties by using automatic sequences. We then use a computer to search through such examples, unfortunately without finding any likely candidates.

Notation

Throughout we use Vinogradov notation, that is, for $a, b > 0$, $a \ll b$ means that there exists some constant $c > 0$ such that $a \leq cb$.

We will also make use of Big-O notation, also known as Landau notation. Thus, we say that $f(x) = O(g(x))$ if there exists a constant $c > 0$ and a point x_0 such that $f(x) \leq cg(x)$ for $x > x_0$. We say that $f(x) = o(g(x))$ if the constant $c > 0$ can be made arbitrarily small, or equivalently, if $f(x)/g(x) \to 0$ as $x \to \infty$.

CONTENTS

Chapter 1

INTRODUCTION

Diophantine approximation concerns the problem of approximating arbitrary real numbers by simple rational numbers. There are several ways of measuring the complexity (also known as the height) of a rational number, but the most common choice is to take the size the denominator when the fraction is written in lowest terms. Concretely, the problem is to find the parameters ε and M for which we may solve the inequalities

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon, \quad q \leq M.$$

A good starting point for this theory is the approximation theorem of Dirichlet from the 1800s.

Theorem 1.1 (Dirichlet) *Let $\alpha \in \mathbb{R}$ be a real number. For any natural number N, there exists a fraction p/q with $1 \leq q \leq N$ such that*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qN}.$$

Proof. By multiplying the above inequality with q, we find that we need to solve

$$|q\alpha - p| \leq \frac{1}{N}.$$

For $q = 0, 1, \ldots, N$ consider the fractional part $\{q\alpha\}$ in the intervals

$$\left[0, \frac{1}{N}\right), \left[\frac{1}{N}, \frac{2}{N}\right), \ldots, \left[\frac{N-1}{N}, 1\right).$$

Since we have $N + 1$ numbers $\{q\alpha\}$ in N intervals, the pigeonhole principle implies that there exist two numbers $q_1 > q_2$ such that $\{q_1\alpha\}$ and $\{q_2\alpha\}$ lie in the same interval. Put $p_1 = \lfloor q_1\alpha \rfloor$ and $p_2 = \lfloor q_2\alpha \rfloor$, then

$$|\{q_1\alpha\} - \{q_2\alpha\}| = |(q_1 - q_2)\alpha - (p_1 - p_2)| \leq \frac{1}{N}.$$

So choosing $q = q_1 - q_2$ and $p = p_1 - p_2$ yields the desired result. □

The estimate $q \leq N$ immediately yields the following non-uniform corollary.

Corollary 1.2 *Let $\alpha \in \mathbb{R}$ be a real number. There are infinitely many rational points, such that*

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

It turns out that this result is essentially optimal, as it does not hold if we replace the exponent by $2 + \varepsilon$. The constant of 1 however, is not optimal. The optimal value was found by Hurwitz to be $1/\sqrt{5}$.

While Dirichlet's theorem has a neat and beautiful proof and is essentially optimal, it has one important defect: It provides no method of actually finding the fractions! It turns out, that an algorithm does exist and that it has been known since antiquity: the process of *continued fractions*, which is an extension of the Euclidean algorithm. We delay a full discussion of this process to the second part.

The questions raised by Diophantine application may at first seem quaint, but they are in fact connected to natural problems arising in applied mathematics. Probably the first application was in ease of calculations. The well-known approximation of $\pi \approx 22/7$ comes from this theory, and makes many calculations much easier. But there are also many applications which are much more intrinsically tied to the theory.

A very simple example of a completely rational phenomenon is the ratio produced by mechanical gear trains. The ratio produced by a set of gears is always the ratio of number of teeth. A more complex fraction requires more teeth, and is hence also mechanically more complex to produce. If you were to construct an analog clock with an indicator for the year, or perhaps a mechanical model of the solar system, the problem of approximating complex ratios by simpler ratios while minimizing the error is very natural. A further twist to this problem, is that gears' ratios multiply when put together. Thus, it is mechanically feasible to produce a high gear ratio if the numbers are sufficiently *smooth* (have many small prime divisors). An example of a gear train producing the ratio $1 : 60$, as might be found in an ordinary clock, is given in figure 1.1. This in turn motivates us to extend the mathematical theory. We will see another example of applications motivating the mathematical theory in the second part of the thesis.

Finally, a very important application which is of current interest is to resonances. The oldest case of this, are the harmonics of music. When you pluck a string, it will resonate at some frequency ν and additionally at $2\nu, 3\nu, \ldots$ known as the *overtones*. It was known already by the Pythagoreans that frequencies which share overtones are harmonious, or phrased differently, that simple proportions are harmonious. Thus, when designing music, one should use simple ratios like $1 : 2$ and $3 : 2$ and their inverses. The

problem here, is that starting with one base note and using these two rules, it is possible to arrive slightly off from the original note. This makes it impossible to make a correct musical scale. Mathematically, the problem is that $2^a = 3^b$ has no solutions in the integers. By taking the base two logarithm, we see that this is equivalent to finding a rational expression for $\log_2(3)$. The 5-note and 12-note scales we know today, arise from the Diophantine approximations $\log_2(3) \approx 8/5$ and $\log_2(3) \approx 19/12$. Fore more details on this example see [DM99].

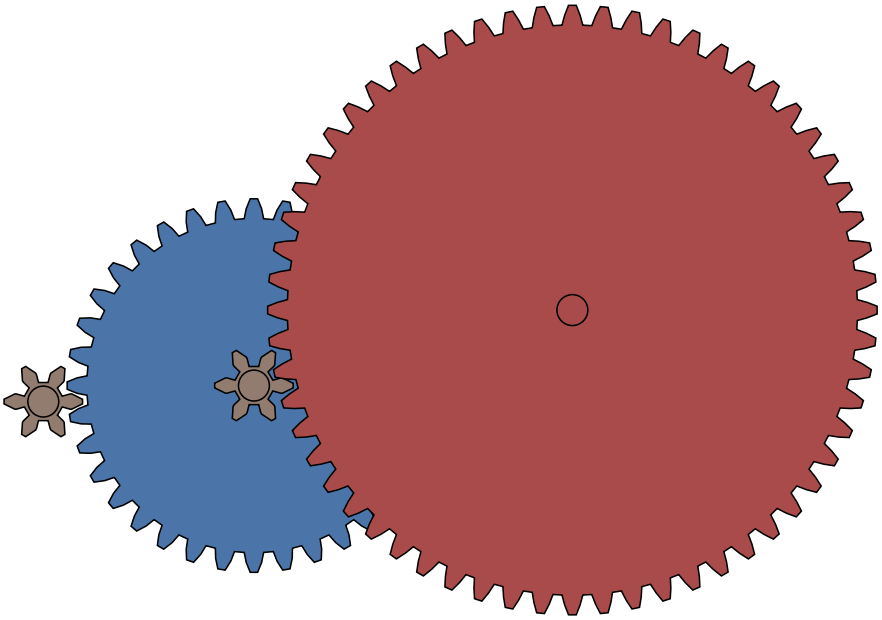


Figure 1.1: A gear train with total ratio $1/60 = 1/6 \times 1/10$.

Diophantine Approximation in Higher Dimensions

The theory of Diophantine approximation can be extended to higher dimensions. There are several ways of doing this, but perhaps the most natural is that of *simultaneous approximation*. Here we try to approximate an arbitrary vector $\boldsymbol{x} \in \mathbb{R}^n$ be a rational vector $\boldsymbol{p}/q$ where $\boldsymbol{p} \in \mathbb{Z}^n$ is an integer vector and $q \in \mathbb{N}$ is a natural number. Alternatively, we may phrase this as approximating n real numbers by rational numbers with the same denominator.

It is possible to generalize Dirichlet's theorem to this setting. In order to do this, we need a geometric analogue of the pigeon hole principle. The

analogue is known as Minkowski's theorem and forms the beginning of the field of *geometry of numbers*, see [Cas97].

Theorem 1.3 (Minkowski) *Let $S \in \mathbb{R}^n$ be a convex set which is centrally symmetric, i.e.*

$$-S \coloneqq \{-x : x \in S\} = S.$$

Suppose that $\mathrm{Vol}(S) > 2^n$*, then S contains a non-zero integer point.*

Proof. Consider the set

$$S' \coloneqq \tfrac{1}{2}S = \left\{\tfrac{1}{2}x : x \in S\right\}$$

with volume $\mathrm{Vol}(S') > 1$. Divide this into disjoint sets by

$$S'_{\boldsymbol{u}} \coloneqq \{\boldsymbol{x} \in S' : u_i \leq x_i < u_i + 1\}, \quad \boldsymbol{u} \in \mathbb{Z}^n.$$

Now consider the sets

$$S''_{\boldsymbol{u}} = S'_{\boldsymbol{u}} - \boldsymbol{u} \subseteq [0,1)^n, \quad \boldsymbol{u} \in \mathbb{Z}^n.$$

The sum of the volumes of these sets is strictly greater than 1, so they must overlap. Hence, we may find point $\boldsymbol{x'}, \boldsymbol{x''} \in S'$ and $\boldsymbol{u'}, \boldsymbol{u''} \in \mathbb{Z}^n$ such that

$$\boldsymbol{x'} - \boldsymbol{x''} = \boldsymbol{u'} - \boldsymbol{u''} =: \boldsymbol{u} \in \mathbb{Z}^n \setminus \{\boldsymbol{0}\}.$$

Now by convexity of S we get

$$\tfrac{1}{2}\boldsymbol{x'} - \tfrac{1}{2}\boldsymbol{x''} = \tfrac{1}{2}\boldsymbol{u} \in S' = \tfrac{1}{2}S$$

so $\boldsymbol{u} \in S$ as required. □

With this tool, it is easy to generalize Dirichlet's theorem to the case of simultaneous approximation.

Theorem 1.4 *Let $x_1, \ldots, x_n \in \mathbb{R}$. For any $N \in \mathbb{N}$ there exists $p_1, \ldots, p_n \in \mathbb{Z}$ and $q \in \mathbb{N}$ with $1 \leq q \leq N^n$ such that*

$$\left| x_i - \frac{p_i}{q} \right| \leq \frac{1}{qN}, \quad i = 1, \ldots, n.$$

Proof. This is equivalent to solving $|qx_i - p_i| \leq 1/N$ for $i = 1, \ldots, n$. Put

$$S \coloneqq \left\{(q, p_1, \ldots, p_n) \in \mathbb{R}^{n+1} : |q| \leq N^n + \tfrac{1}{2}, |qx_i - p_i| \leq \tfrac{1}{N}\right\} \subset \mathbb{R}^{n+1}.$$

Note that

$$\mathrm{Vol}(S) = 2(N^n + \tfrac{1}{2})\frac{2^n}{N^n} = 2^{n+1}\left(1 + \frac{1}{2N^n}\right) > 2^{n+1}.$$

So by Minkowski's theorem there is a non-zero integer point $(q, p_1, \ldots, p_n) \in S$. By symmetry we may choose $q > 0$. This proves the claim. □

Corollary 1.5 *Let $x_1, \ldots, x_n \in \mathbb{R}$. There are infinitely many integers $p_1, \ldots, p_n \in \mathbb{Z}$ and $q \in \mathbb{N}$ such that*

$$\left| x_i - \frac{p_i}{q} \right| \leq \frac{1}{q^{1+1/n}}.$$

As in the one-dimensional version of Dirichlet's theorem, the proof gives no algorithm for actually *finding* such solutions. In fact, there is no known efficient algorithm in this case.

Part I

Metric Theory

Chapter 2

HAUSDORFF MEASURE AND DIMENSION

In this chapter, we introduce the Hausdorff measures which greatly generalize the usual notions of length, area, volume and so forth. The standard introduction to this is [Fal03], while a much more technical treatment is given in [Rog70]. While we are not striving for utmost generality in our definitions (for instance, we will work exclusively over $\mathbb{R}^n$), we do take care to prove all theorems in the general case, as some non-trivial issues arise here.

§ 2.1 Fundamental Definitions

Recall that for any subset $E \subseteq \mathbb{R}^n$, the *diameter* of E is defined by $\operatorname{diam}(E) = \sup\{|x - y| : x, y \in E\}$. A collection $\{U_i\}$ of subsets of $\mathbb{R}^n$ is called a *δ-cover* of E if $\operatorname{diam}(U_i) < \delta$ for all i and $E \subseteq \bigcup U_i$. For any $s \geq 0$ and $\delta > 0$ we define the *(outer) Hausdorff s-δ-measure* by

$$\mathcal{H}^s_\delta(E) = \inf\Big\{\sum \operatorname{diam}(U_i)^s : \{U_i\} \text{ is a } \delta\text{-cover of } E\Big\}.$$

Note that as δ decreases, the number of possible δ-covers decrease and hence $\mathcal{H}^s_\delta$ increases and the limit as $\delta \to 0$ exists.

Definition 2.1 For $s > 0$, the *(outer) Hausdorff s-measure* of a set E is

$$\mathcal{H}^s(E) = \lim_{\delta \to 0} \mathcal{H}^s_\delta(E).$$

When we restrict to the Borel subsets of $\mathbb{R}^n$, the outer Hausdorff measure does indeed restrict to a proper measure by the usual Carathéodory construction.

A very special case of the Hausdorff measure is the case of $\mathcal{H}^n$ where n is an integer. In this case, the Hausdorff measure will agree with the Lebesgue measure up to scaling by a factor equal to the volume of the n-dimensional sphere. The advantages of the Hausdorff measure are twofold: First, the usual construction of the n-dimensional Lebesgue measure is tied intrinsically to $\mathbb{R}^n$, which makes it inconvenient for measuring e.g. surface area in space. The Hausdorff measure does not have this limitation. Second,

the Hausdorff measure is defined for all $s \geq 0$, not just integers. This opens the door for a measure-theoretic approach to "fractals". For instance, the middle-third Cantor set C is uncountable but with length 0. However, for $s = \log 2/\log 3$ we have $\mathcal{H}^s(C) = 1$.

It turns out that there is always a correct choice for s in the following sense: If E is some set and $\{U_i\}$ is a δ-cover, then for any $t > s$

$$\sum_i \operatorname{diam}(U_i)^t = \sum_i \operatorname{diam}(U_i)^s \operatorname{diam}(U_i)^{t-s} \leq \delta^{t-s} \sum_i \operatorname{diam}(U_i)^s.$$

Hence $\mathcal{H}^t_\delta(E) \leq \delta^{t-s}\mathcal{H}^s_\delta(E)$. So if $\mathcal{H}^s(E) < \infty$ letting $\delta \to 0$ we find that $\mathcal{H}^t(E) = 0$. We thus see that there exists a point $t \geq 0$ with the property that $\mathcal{H}^s(E) = \infty$ for $s < t$ (which is an empty set if $t = 0$), and $\mathcal{H}^s(E) = 0$ if $s > t$. This number is called the *Hausdorff dimension* of E. A perhaps more convenient way of stating this, is the following definition.

Definition 2.2 For any set E the *Hausdorff dimension* of E is given by

$$\dim_H E = \inf\{s \geq 0 : \mathcal{H}^s(E) = 0\} = \sup\{s \geq 0 : \mathcal{H}^s(E) = \infty\}.$$

Note that the Hausdorff measure may be (and frequently is) 0 or ∞ at this critical value.

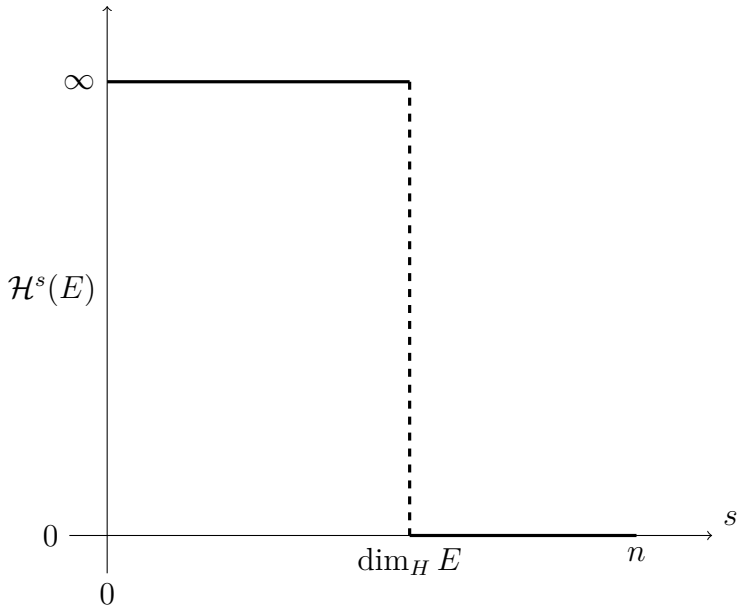


Figure 2.1: The Hausdorff s-measure of a set E as a function of s. The dimension is at the critical value.

A very nice way to think about the Hausdorff dimension is in analogy with a microscope, which we borrow from [DK04]: When you zoom in to dimension 0, points are sharp while larger objects like lines and planes are blurry. Adjusting the scale to 1 makes points blurry, while lines are now sharp. When the "microscope" is set to $\log 2/\log 3$, the Cantor set is in focus while both points and lines are blurry.

§ 2.2 Arbitrary Dimension Functions

More generally, let $h : [0, \infty) \to [0, \infty)$ be an increasing and continuous function, which we will refer to as a *dimension function*. With exactly the same construction as above, we define the (outer) Hausdorff h-measure.

Definition 2.3 For any set E and dimension function h, the *(outer) Hausdorff h-measure* is defined by

$$\mathcal{H}^h(E) = \lim_{\delta \to 0} \inf\Big\{\sum h(\operatorname{diam}(U_i)) : \{U_i\} \text{ is a } \delta\text{-cover of } E\Big\}.$$

The Hausdorff s-measure is recovered as the Hausdorff h-measure with $h(r) = r^s$.

The classical example of the usefulness of Hausdorff h-measures is the case of Brownian motion in $\mathbb{R}^3$. Any Brownian motion has Hausdorff dimension 2, but $\mathcal{H}^2$-measure equal to 0. However, if we put $h(r) = r^2 \log\log(1/r)$, it turns out that the Hausdorff h-measure of the path is both positive and finite.

§ 2.3 Hausdorff Measure and Lipschitz Mappings

A very important property of the Hausdorff measures, is the fact their measure is changed by at most a constant under a bi-Lipschitz mapping. We first show this for Hausdorff s-measures, and then extend this proof to cover the case of Hausdorff measures for general dimension functions. To the author's knowledge, the generalization (while probably well-known) has not appeared in the literature.

Theorem 2.4 *Let $E \subseteq \mathbb{R}^n$ be some set, and suppose that $f : E \to \mathbb{R}^m$ is a Lipschitz mapping, so there exists some $K > 0$ such that*

$$|f(x) - f(y)| \leq K|x - y| \quad \textit{for all } x, y \in E.$$

Then

$$\mathcal{H}^s(f(E)) \leq K^s \mathcal{H}^s(E).$$

Proof. Let $\{U_i\}$ be a δ-cover of E. Now

$$\operatorname{diam}(f(U_i)) \leq K \operatorname{diam}(U_i)$$

so $\{f(U_i)\}$ is a $K\delta$-cover of $f(E)$. Since

$$\sum_i \operatorname{diam}(f(U_i))^s \leq K^s \sum_i \operatorname{diam}(U_i)^s$$

we have

$$\mathcal{H}^s_{K\delta}(E) \leq K^s \mathcal{H}^s_\delta(E).$$

Letting $\delta \to 0$ yields the desired result. □

Corollary 2.5 *If $f : E \to \mathbb{R}^m$ is bi-Lipschitz with*

$$K_1|x-y| \leq |f(x)-f(y)| \leq K_2|x-y|,$$

then

$$K_1^s \mathcal{H}^s(E) \leq \mathcal{H}^s(f(E)) \leq K_2^s \mathcal{H}^s(E).$$

Proof. The second inequality follows directly from the theorem. The first inequality follows from the theorem applied to f^{-1}. □

In order to formulate the above theorems in the general case, we introduce the concept of a *doubling* dimension function.

Definition 2.6 A dimension function h is called *doubling* if there exists a constant $C > 0$ such that for all sufficiently small $x \geq 0$

$$h(2x) \leq Ch(x).$$

It is quite easy to see that not all dimension functions are doubling. For instance, it is readily verified that $h(r) = 2^{-1/r}$ is not doubling. However, it turns out that such dimension functions do not cause problems as they lead to degenerate measures.

Lemma 2.7 *If there exists a $C > 0$ such that $h(2^{-n}) \leq Ch(2^{-(n+1)})$ for all n, then h is doubling.*

Proof. Suppose such a C exists. Then for any $x \in [0,1]$ we may find n such that

$$2^{-(n+1)} \leq x \leq 2^{-n}.$$

Now

$$h(2x) \leq h(2^{-(n-1)}) \leq C^2 h(2^{-(n+1)}) \leq C^2 h(x).$$ □

Lemma 2.8 *If h is a non-doubling dimension function, then*

$$\mathcal{H}^h(\mathbb{R}^n) = 0.$$

Proof. Let $F \subset \mathbb{R}^n$ be a compact set. We show that $\mathcal{H}^h(F) = 0$, since then $\mathcal{H}^h(\mathbb{R}^n) = 0$ by σ-compactness.

Let K be a number such that any ball of radius r may be covered by K balls of radius $r/2$. This number only depends on the dimension n. Let $\{B_i\}_{i\in I}$ be a finite cover of F by balls of radius 1. Since h is not doubling, there exists a sequence $\{C_k\}$ of positive numbers, such that $h(2^{-(k-1)}) \geq C_k h(2^{-k})$ and $C_k \to \infty$ as $k \to \infty$.

Now, for any $k \in \mathbb{N}$ we may cover F by $K^k|I|$ balls of radius 2^{-k} and we get the estimate

$$\mathcal{H}^h(F) \leq K^k \sum_{i\in I} h(2^{-k}) \leq \frac{K^k}{C_1 C_2 \dots C_k} \sum_{i\in I} h(1)$$

which tends to 0 as $C_k \to \infty$ when $k \to \infty$. □

Theorem 2.9 *Let $h : [0,\infty) \to [0,\infty)$ be an arbitrary dimension function. Let $E \subset \mathbb{R}^n$ be some subset of $\mathbb{R}^n$ and let $f : E \to \mathbb{R}^m$ be a Lipschitz function such that*

$$|f(x) - f(y)| \leq K|x - y|, \quad x, y \in E.$$

Then there exists a constant $C = C(K, h)$ depending only on K and h such that

$$\mathcal{H}^h(f(E)) \leq C\mathcal{H}^h(E).$$

Proof. If h is not doubling, the measure $\mathcal{H}^h$ is identically 0 and there is nothing to prove. Now suppose that h is doubling. Then there exists a constant $C > 0$ such that

$$h(Kx) \leq Ch(x)$$

when x is sufficiently small.

Now let $\delta > 0$ be given and let $\{U_i\}_{i\in I}$ be a δ-cover of E. We have

$$\operatorname{diam}(f(U_i)) = \sup_{x,y} |f(x) - f(y)| \leq K \operatorname{diam}(U_i).$$

When δ is sufficiently small, we get the estimate

$$h(\operatorname{diam}(f(U_i))) \leq h(K \operatorname{diam}(U_i)) \leq Ch(\operatorname{diam}(U_i))$$

and hence

$$\sum_i h(\mathrm{diam}(f(U_i))) \le C \sum_i h(\mathrm{diam}(U_i)).$$

Since $\{f(U_i)\}$ is a δK-cover of $f(E)$ we get

$$\mathcal{H}^h_{\delta K}(f(E)) \le C\mathcal{H}^h_\delta(E).$$

Letting $\delta \to 0$ gives the desired result. □

Corollary 2.10 *If $f : E \to \mathbb{R}^m$ is bi-Lipschitz with*

$$K_1|x-y| \le |f(x)-f(y)| \le K_2|x-y|,$$

then there exists constants $C_1 = C_1(h, K_1)$ and $C_2 = C_2(h, K_2)$ such that

$$C_1\mathcal{H}^h(E) \le \mathcal{H}^h(f(E)) \le C_2\mathcal{H}^h(E).$$

Chapter 3

THE THEOREMS OF KHINTCHINE AND JARNÍK

The metric theory of Diophantine approximation allows us to make more general statements, at the cost of some precision as to what happens on a nullset. The theory begins with Khintchine's theorem. Let $\psi : \mathbb{N} \to \mathbb{R}^+$ be a decreasing function, which we will refer to as an *approximation function*. We say that $\boldsymbol{x} \in \mathbb{R}^n$ is *(simultaneously) ψ-approximable* if there exists infinitely many rational points $\boldsymbol{p}/q$ with $\boldsymbol{p} \in \mathbb{Z}^n$ and $q \in \mathbb{N}$ such that

$$\|\boldsymbol{x} - \boldsymbol{p}/q\|_\infty \leq \psi(q).$$

Denote the set of ψ-approximable vectors by $\mathcal{S}_\psi$. For the particular approximation function $\psi_\tau(r) \coloneqq r^{-\tau}$ put $\mathcal{S}_\tau = \mathcal{S}_{\psi_\tau}$.

Theorem 3.1 (Khintchine) *Let $\psi : \mathbb{N} \to \mathbb{R}^+$ be a decreasing approximation function. Let λ_n denote the n-dimensional Lebesgue measure. Then*

$$\lambda_n(\mathcal{S}_\psi) = \begin{cases} 0 & \text{if } \sum_{r=1}^{\infty} r^n \psi(r)^n < \infty \\ \infty & \text{if } \sum_{r=1}^{\infty} r^n \psi(r)^n = \infty. \end{cases}$$

In particular, this theorem recovers up to a nullset the statement of Dirichlet's theorem. Furthermore, it shows that the exponent in Dirichlet's theorem is optimal in the sense that the set of $\psi_{1+1/n+\varepsilon}$-approximable vectors is a nullset. Finally, it gives complete metric answers not only for the particular approximation function $\psi_\tau(r) = r^{-\tau}$ but for arbitrary approximation functions.

The proof of Khintchine's theorem naturally splits into two parts: the case of convergence and the case of divergence. The convergence part is easy, and is essentially just an application of the first Borel-Cantelli lemma. The key realization is that the set of ψ-approximable vectors is a limsup set:

$$\mathcal{S}_\psi = \bigcap_{N=1}^{\infty} \bigcup_{q>N} \bigcup_{\boldsymbol{p}\in\mathbb{Z}} B\left(\frac{\boldsymbol{p}}{q}, \psi(q)\right),$$

where $B(\boldsymbol{x}, r) = \{\boldsymbol{y} \in \mathbb{R}^n : \|\boldsymbol{x} - \boldsymbol{y}\|_\infty \leq r\}$ denotes the ball centered at $\boldsymbol{x}$ of radius r in the supremum norm.

Proof (Convergence part). Let $I \subset \mathbb{R}$ be some bounded interval. For any fixed $N \in \mathbb{N}$ we have

$$\begin{aligned}\lambda_n(S_\psi \cap I^n) &\ll \sum_{q>N} \sum_{\boldsymbol{p}/q \in I^n} \lambda_n\left(B\left(\frac{\boldsymbol{p}}{q}, \psi(q)\right)\right) \\ &\ll \sum_{q>N} q^n \psi(q)^n,\end{aligned}$$

which is the tail of a convergent series and hence tends to 0 as $N \to \infty$. Since N was arbitrary we conclude that $\lambda_n(\mathcal{S}_\psi \cap I^n) = 0$. Now we can write $\mathcal{S}_\psi$ as a countable union of nullsets and we hence conclude that $\lambda_n(\mathcal{S}_\psi) = 0$.□

Like in the case of the Borel Cantelli lemmas, the divergence case is much harder as we need to make sure that the sets in question do not overlap too much. In probability theory, this is done by assuming that the sets (events) are independent. This is neither a natural nor a true condition in our setting. To solve this problem, various weaker notions of independence have been found, which allow us to reclaim the conclusion of the second Borel-Cantelli lemma. The modern version of this is the notion of *ubiquity*, which is a very general framework for deriving theorems of this kind (see [BDV06]).

We remark that Khintchine's theorem also holds when intersecting with an arbitrary ball. In this case, the measure is either null or the full measure of the ball. The method of proof outlined above works precisely the same.

There is an analogue of Khintchine's theorem for Hausdorff measures, known as *Jarník's theorem*. The history of this theorem is rather complicated, and many early versions had unnecessary technical conditions attached to them. A modern version is the following (see [BDV06, Theorem DV]).

Theorem 3.2 (Jarník; Dickinson, Velani) *Let h be a dimension function such that $r^{-n}h(r) \to \infty$ as $r \to 0$ and $r \mapsto r^{-n}h(r)$ is decreasing. Then*

$$\mathcal{H}^h(\mathcal{S}_\psi) = \begin{cases} 0 & \text{if } \sum_{r=1}^{\infty} h(\psi(r))r^n < \infty \\ \infty & \text{if } \sum_{r=1}^{\infty} h(\psi(r))r^n = \infty. \end{cases}$$

When $h(r) = r^n$ this theorem morally generalizes Khintchine's theorem, however note that the theorem is strictly not true in this case as h does not satisfy the growth condition. It is perhaps somewhat surprising then, that Khintchine's theorem in fact implies Jarnik's theorem by the mass transference principle of Beresnevich and Velani [BV06]. This principle relies on the beautiful observation that when we are rescaling the measure,

we should simply rescale the balls in our limsup set. To be more precise, we need to introduce some notation.

Given a dimension function h and a ball $B = B(\boldsymbol{x}, r) \subset \mathbb{R}^n$, define

$$B^h := B(\boldsymbol{x}, h(r)^{1/n}).$$

For real numbers $s > 0$ we put $B^s = B^{(r \mapsto r^s)}$. Note that $B^n = B$.

Theorem 3.3 (Mass Transference Principle) *Let $\{B_i\}_{i=1}^{\infty}$ be a sequence of balls in $\mathbb{R}^n$. Let h be a dimension function such that $r^{-n}h(r)$ is decreasing and suppose that for any ball B in $\mathbb{R}^n$ we have*

$$\mathcal{H}^n\left(B \cap \limsup_{i\to\infty} B_i^h\right) = \mathcal{H}^n(B).$$

Then, for any ball B in $\mathbb{R}^n$

$$\mathcal{H}^h\left(B \cap \limsup_{i\to\infty} B_i^n\right) = \mathcal{H}^h(B).$$

Assuming Khintchine's theorem and the mass transference principle, it is now easy to derive Jarnik's theorem.

Proof of Jarnik's theorem. The proof of the convergence part is exactly the same as in the case of Khintchine's theorem, so we skip it.

Now suppose that

$$\sum_{r=1}^{\infty} h(\psi(r))r^n = \infty.$$

Let $\{B_i\}_{i=1}^{\infty}$ be some ordering of the balls

$$B\left(\frac{\boldsymbol{p}}{q}, \psi(q)\right), \quad \boldsymbol{p} \in \mathbb{Z}^n, q \in \mathbb{N}$$

and recall that

$$S_\psi = \limsup_{i\to\infty} B_i.$$

Now $\{B_i^h\}_{i=1}^{\infty}$ consists of balls of the form

$$B\left(\frac{\boldsymbol{p}}{q}, h(\psi(q))^{1/n}\right)$$

so by Khintchine's theorem we have

$$\mathcal{H}^n\left(\limsup_{i\to\infty} B_i^h\right) = \mathcal{H}^n\left(S_{r\mapsto h(\psi(r))^{1/n}}\right) = \infty.$$

And in fact, the proof of Khintchine's theorem extends to give that

$$\mathcal{H}^n\left(B \cap \limsup_{i\to\infty} B_i^h\right) = \mathcal{H}^n(B).$$

The mass transference principle now implies that

$$\mathcal{H}^h\left(B \cap \limsup_{i\to\infty} B_i\right) = \mathcal{H}^h\left(B \cap \mathcal{S}_\psi\right) = \mathcal{H}^h(B).$$

The condition that $r^{-n}h(r) \to \infty$ as $r \to 0$ implies that $\mathcal{H}^h(B) = \infty$, which proves the theorem. $\square$

Chapter 4

METRIC APPROXIMATION ON MANIFOLDS

Recall once again that Dirichlet's theorem shows that $\mathcal{S}_{1+1/n} = \mathbb{R}^n$. We say that $\boldsymbol{x} \in \mathbb{R}^n$ is *very well approximable* if $\boldsymbol{x} \in \mathcal{S}_\tau$ for some $\tau > 1 + 1/n$. Otherwise we say that $\boldsymbol{x}$ is not very well approximable or *extremal*.

Consider a manifold $M \subset \mathbb{R}^n$. We say that M is extremal if almost all points on M (with respect to the Hausdorff s-measure where $s = \dim M$) are extremal. By Khintchine's theorem we saw that $\mathbb{R}^n$ is extremal.

The theory of Diophantine approximation on manifolds begins with the question of whether there exists non-extremal manifolds in $\mathbb{R}^n$. Intuitively, we're asking whether the well-approximable points somehow "clump together". We note that we have a class of degenerate counterexamples: on the manifold given by the natural embedding $\mathbb{R} \hookrightarrow \mathbb{R}^n$ which puts all but one coordinate constant, almost all points are $\psi_\tau = r^{-\tau}$ approximable where $\tau = 2$.

This problem was originally considered by Mahler in 1932 [Mah32] in the context of approximating transcendental numbers by algebraic numbers. Mahler conjectured that the Veronese curve

$$\mathcal{V} = \{(x, x^2, \ldots, x^n) : x \in \mathbb{R}\}$$

is extremal. This conjecture was verified by Sprindžuk in 1964, which led to development of this theory of Diophantine approximation on manifolds. The culmination of this investigation, was the seminal paper of Kleinbock and Margulis [KM98], which shows that all smooth manifolds which are non-degenerate in a sense of not lying infinitesimally in an affine hyperplane, are extremal. Their proof used a dynamical approach to Diophantine approximation via the so-called Dani-Margulis correspondence. We briefly sketch the correspondence for simultaneous approximation.[1]

[1] Kleinbock and Margulis used another form of approximation called *dual approximation*, but for the question of extremality, this is equivalent to simultaneous approximation.

For $\boldsymbol{x} \in \mathbb{R}^n$ associate a lattice in $\mathbb{R}^{n+1}$ by

$$\Lambda_{\boldsymbol{x}} = \begin{pmatrix} 1 & 0 & \dots & 0 & x_1 \\ & 1 & \dots & 0 & x_2 \\ & & \ddots & & \vdots \\ & & & 1 & x_n \\ & & & & 1 \end{pmatrix} \mathbb{Z}^{n+1} = \left\{ \begin{pmatrix} p_1 + qx_1 \\ p_2 + qx_2 \\ \vdots \\ p_n + qx_n \\ q \end{pmatrix} \right\}.$$

It is intuitively clear, that good approximations correspond to small vectors in $\Lambda_{\boldsymbol{x}}$. The insight is to act on the lattice $\Lambda_{\boldsymbol{x}}$ by elements of the form

$$g_{\boldsymbol{t}} = \begin{pmatrix} e^{t_1} & & & \\ & \ddots & & \\ & & e^{t_n} & \\ & & & e^{-t} \end{pmatrix}$$

where $\boldsymbol{t} = (t_1, \dots, t_n)$ and $t = t_1 + \dots + t_n$. It can be shown that small vectors along this flow correspond to good approximation. By realizing that the set of unimodular lattices in $\mathbb{R}^{n+1}$ is isomorphic to the space $\mathrm{SL}_{n+1}(\mathbb{R})/\mathrm{SL}_{n+1}(\mathbb{Z})$, this turns the problem into one of studying the dynamics on this homogeneous space.

The result of Kleinbock and Margulis shows that the correct exponent for Diophantine approximation on a non-degenerate manifold M is the same as that of the ambient space. Two natural problems now emerge.

(i) To obtains a Khintchine-type theory for manifolds, which allow us to replace the approximation functions $\psi_\tau(r) = r^{-\tau}$ by more general approximation functions.

(ii) To give a more detailed account of the size null sets, by establishing Hausdorff measure and dimension of the set of ψ-approximable points on M.

The Khintchine-type theory is very well developed, and the question was essentially completely answered by Beresnevich in 2012 [Ber12].

It is very tempting to think that a Jarník-type theorem should follow from the Khintchine-type theory, by using the mass transference principle as in the classical case. However, this is not so. We are approximating by points outside the manifold, so on rescaling the balls, we may not hit anything at all. In fact, it turns out that the Jarník-type theory is completely different from the Khintchine-type theory and depends intricately on the subtle arithmetical nature of the manifold itself. The reason for this, is that for

many manifolds, if the approximation is sufficiently good, the approximating points must eventually lie *on* the manifold itself. This was first observed in the case of the circle by Dickinson and Dodson [DD01]. We give a slightly generalized version of their argument.

Lemma 4.1 *Let $r, n \in \mathbb{N}$ be natural numbers and consider the manifold*

$$M \coloneqq \{(x, y) \in \mathbb{R}^n : x^n + y^n = r\}.$$

Suppose $(x_1, x_2) \in M$ satisfies $|x_1 - p_1/q|, |x_2 - p_2/q| = o\left(1/q^n\right)$ for integers $p_1, p_2 \in \mathbb{Z}$ and $q \in \mathbb{N}$. Then, for q sufficiently large, we have $(p_1/q, p_2/q) \in M$.

Proof. Let $(x_1, x_2) \in M$ so $x_1^n + x_2^n = r$. Put $\varepsilon_1 \coloneqq qx_1 - p_1$, $\varepsilon_2 \coloneqq qx_2 - p_2$. We have $\varepsilon_1, \varepsilon_2 = o(1/q^{n-1})$ and $p_1, p_2 = O(q)$. Now we find

$$\begin{aligned} q^n(r - x_1^n) = (qx_2)^n &= (\varepsilon_2 + p_2)^n \\ q^n x_1^n &= (\varepsilon_1 + p_1)^n. \end{aligned}$$

Adding these two equations we get

$$\begin{aligned} q^n r &= (\varepsilon_2 + p_2)^n + (\varepsilon_1 + p_1)^n \\ &= p_1^n + p_2^n + \sum_{k=1}^{n} \binom{n}{k} \left(\varepsilon_1^k p_1^{n-k} + \varepsilon_2^k p_2^{n-k}\right) \\ &= p_1^n + p_2^n + o(1). \end{aligned}$$

So we find that

$$|q^n r - p_1^n - p_2^n| = o(1) < 1$$

for q large. Since there is only one integer satisfying this, we get that

$$q^n r = p_1^n + p_2^n$$

and $(p_1/q, p_2/q) \in M$. □

In the case of the circle of radius 1, we have a dense set of rational points, while the circle of radius 3 has no only finitely many rational points and the question of Diophantine approximation is meaningless.

This gives rise to a new form of Diophantine approximation on manifolds: the question of *intrinsic Diophantine approximation* in which we consider approximation by rational points on the manifold. In contrast, we refer to

the previous form of Diophantine approximation as *ambient approximation*. We introduce the notation

$$\mathcal{I}_\psi(M) \coloneqq \\ \{\boldsymbol{x} \in M : \|\boldsymbol{x} - \boldsymbol{p}/q\|_\infty \leq \psi(q) \text{ for infinitely many } \boldsymbol{p}/q \in \mathbb{Q}^n \cap M\}$$

for the set of intrinsically ψ-approximable points on M. For $\psi_\tau(r) = r^{-\tau}$ we put $\mathcal{I}_\tau = \mathcal{I}_{\psi_\tau}$.

In order for the question of intrinsic Diophantine approximation to make sense, we need to have a dense set of rational points on the manifold. However, there is no known method for determining if a variety, much less a manifold, has infinitely many rational points. Indeed, even determining the number of rational points on $\{(x, y) : x^n + y^n = 1\}$ for $n \geq 3$ is the content of a famous theorem of Wiles[2]. Thus, a general theory for intrinsic Diophantine approximation is very much out of reach. However, some important progress has been made in special cases.

In the case of the unit circle, the Hausdorff dimension of $\mathcal{I}_\tau$ is computed in [DD01] using the concept of ubiquity. This is extended to a Jarník-type theorem in [BDV06, Theorem 19].

In [BDL10] a projection argument is used to derive a Jarník-type theorem for intrinsic approximation for graphs of polynomial curves of the form

$$\Gamma = \{(x, P_1(x), \ldots, P_n(x)) : x \in \mathbb{R}\}$$

where $P_1, \ldots, P_n \in \mathbb{Z}[x]$. In the paper, this is expressed as a result as a result on ambient approximation when the approximation is suitably fast and the two questions coincide. In chapter 6 we generalize their approach to the case of certain polynomials in several variables. The case of several variables, where each polynomial still only depends on one variable is considered in [Sch15].

Recently, a lot of progress has been made using dynamical methods. Complete answers for spheres are obtained in a paper by Kleinbock and Merrill from 2015 [KM15]. Their approach uses a analogue of the Dani-Margulis correspondence, where the space $\mathrm{SL}_{n+1}(\mathbb{R})/\mathrm{SL}_{n+1}(\mathbb{Z})$ is replaced by the space $\mathrm{SO}_{n+1}(\mathbb{R})/\mathrm{SO}_{n+1}(\mathbb{Z})$. This approach has been generalized to the case of quadratic hypersurface [FKMS14].

Another angle of the dynamic approaches, is the work of Ghosh, Gorodnik and Nevo on homogeneous varieties [GGN14, GN15]. Their results are applicable not only for approximation by rationals, but also by S-algebraic

[2]the fact that it has only finitely many points follows from a theorem of Faltings

integers. Their approach is to use an analogue of the Dani-Margulis correspondence along with quantitative ergodic theorems to control the dynamics. The quantitative ergodic theorems depend on a *spectral gap* property for the Laplacian of the associated homogeneous space. This relates their work to spectral theory and representation theory.

Chapter 5

PRELIMINARIES ON ALGEBRAIC GEOMETRY

In this chapter we cover the basics of algebraic geometry. The goal is to obtain a theorem which will allow us to control the height of rational points under certain maps. This theorem provides the crucial step in the proof of the main theorem of the next chapter.

There are many books on algebraic geometry, many of which are quite technical and abstract. For a broader picture, we recommend the introduction of Smith et. al. [SKKT00] and for the Diophantine aspects we recommend the book of Hindry and Silverman [HS00].

In the following, let k be an arbitrary field of characteristic 0.

§ 5.1 Affine Varieties

The most basic object in algebraic geometry is the affine n-space $\mathbb{A}^n = \mathbb{A}^n(k) = k^n$. There are two reasons for introducing this notation. Firstly, it hints at the fact that we consider k^n in the category of affine varieties and not, for example, as a vector space. More importantly, it's useful to think of the affine n-space as living independently of the ground field k, though this doesn't make sense in a strictly set-theoretical sense. We will make use of this technique shortly.

A set $V \subseteq \mathbb{A}^n$ is called an *affine variety* if it is given as the common set of vanishing for a collection of polynomials[1] $\{f_i\}_{i\in I} \subset k[x_1, \ldots, x_n]$, i.e.

$$V = \mathbb{V}(\{f_i\}_{i\in I}) = \{x \in \mathbb{A}^n : f_i(x) = 0 \text{ for all } i \in I\}.$$

In general we allow the variety to be defined by infinitely many polynomials, but finitely many suffice by Hilbert's basis theorem. We define a topology on $\mathbb{A}^n$ called the *Zariski topology* by taking the affine varieties as a basis for the closed sets.

If a variety is given as the vanishing of some polynomials, it will also be given as the vanishing of the ideal generated by these polynomials. Hence,

[1] It is customary to assume that varieties are indecomposable, i.e., they cannot be written as the proper union of other varieties. This is not important for our purposes, so we do not make this distinction.

for any variety V we may write $V = \mathbb{V}(I)$ for some ideal I. On the other hand, we can associate an ideal to each variety by

$$\mathbb{I}(V) = \{f \in k[x_1, \ldots, x_n] : f(x) = 0 \text{ for all } x \in V\}.$$

It is readily verified that if $I \subset J$ are ideals, then $\mathbb{V}(I) \supset \mathbb{V}(J)$ and if $V \subset W$ are varieties, then $\mathbb{I}(V) \supset \mathbb{I}(W)$ so the correspondence is order-reversing. Furthermore, it is seen that if V is a variety, then $\mathbb{V}(\mathbb{I}(V)) = V$. However it is not true that if I is an ideal, then $\mathbb{I}(\mathbb{V}(I)) = I$. A counterexample is given by the ideal $I = \langle x^2 \rangle \subset \mathbb{C}[x]$ as $\mathbb{I}(\mathbb{V}(I)) = \langle x \rangle$. In general the answer is given by Hilbert's nullstellensatz.

Theorem 5.1 (Hilbert's Nullstellensatz) *Suppose that k is algebraically closed. Let $I \subset k[x_1, \ldots, x_n]$ be some ideal. We have*

$$\begin{aligned}\mathbb{I}(\mathbb{V}(I)) &= \operatorname{rad} I \\ &\coloneqq \{f \in k[x_1, \ldots, x_n] : \textit{there exists } m > 0 \textit{ such that } f^m \in I\}.\end{aligned}$$

The assumption that k is algebraically closed is crucial: for $f \in \mathbb{C}[x]$ the Nullstellensatz asserts that the polynomial is given up to a scalar factor and multiplicity by its roots. In this way, the Nullstellensatz is a generalization of the fundamental theorem of algebra. The proof is an entirely algebraic consequence of the fundamental theorem of algebra and can be found in many books on commutative algebra (e.g. [Eis95]).

As a corollary we have the following version of the Nullstellensatz, which relates the statement to one of solving equations.

Corollary 5.2 *A system of polynomial equations*

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ f_2(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_m(x_1, \ldots, x_n) &= 0 \end{aligned}$$

over an algebraically closed field k has no solution in k^n if and only if 1 can be expressed as a linear combination of the form

$$1 = \sum_{i=1}^{m} p_i f_i$$

with $p_i \in k[x_1, \ldots, x_n]$.

Proof. Let $I = \mathbb{I}(\{f_i\}_{i=1}^m)$ be the ideal generated by the polynomials.

Suppose the system has no solutions. Then

$$\mathbb{V}(I) = \emptyset = \mathbb{V}(k[x_1, \ldots, x_n]) = \mathbb{V}(\langle 1 \rangle).$$

By the Nullstellensatz we have $\operatorname{rad} I = \langle 1 \rangle$ so $1^p = 1 \in I$ for some p, but then 1 is given a linear combination as desired.

On the other hand, if 1 is given as a linear combination of the polynomials, then $1 \in I$ and $I = k[x_1, \ldots, x_n]$ and $\mathbb{V}(I) = \emptyset$. □

The natural maps on varieties are polynomials, so the morphisms should preserve that structure. A map $F : \mathbb{A}^n \to \mathbb{A}^m$ is called a polynomial map if F is given as $F(x) = (f_1(x), \ldots, f_m(x))$ for some polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$. if $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ are affine varieties, we say that $F : V \to W$ is a *morphism of affine varieties* if F is the restriction of a polynomial map.

As an aside, we are now in a position to make the connection between algebra and geometry more precise, at least for algebraically closed fields. For a variety V define the *coordinate ring of* V by

$$k[V] = \{f : V \to k : f \text{ is a polynomial map}\}.$$

We can think of this object as an analogue of the dual of a vector space. It is not too hard to see that

$$k[V] \simeq \frac{k[x_1, \ldots, x_n]}{\mathbb{I}(V)}.$$

The coordinate ring is a finitely generated reduced k-algebra. The generators are (equivalence classes of) the functions $x_1, \ldots, x_n$ and, since $\mathbb{I}(V)$ is radical, the quotient has no zero divisors so $k[V]$ is reduced.

Conversely, every finitely generated reduced k-algebra R is given as a coordinate ring of some variety. To see this, fix a set of generators $\sigma_1, \ldots, \sigma_n$ of R and let I be the kernel of

$$k[x_1, \ldots, x_n] \to R, \quad x_i \mapsto \sigma_i.$$

Then $R \simeq k[x_1, \ldots, x_n]/I$ and as R is reduced, I is a radical ideal, and $\mathbb{V}(I) \subseteq \mathbb{A}^n$ defines a variety whose coordinate ring is isomorphic R.

In fact, this equivalence extends to an (arrow-reversing) equivalence of categories between the category of affine varieties and the category finitely generated, reduced k-algebras.

§ 5.2 Projective Varieties

It turns out that the natural setting for algebraic geometry is in a larger space than the affine space: the projective space. Intuitively, the projective space is given as the compactification of the affine space, by adding points "at infinity" in all directions. More precisely, we define the *projective n-space* as the set of all lines through the origin in $\mathbb{A}^{n+1}$. We can represent these as non-zero points in $\mathbb{A}^{n+1}$ modulo scaling, i.e.,

$$\mathbb{P}^n = \mathbb{P}^n(k) = \left(\mathbb{A}^{n+1} \setminus \{0\}\right) / \sim$$

where $(x_0 : \cdots : x_n) \sim (\lambda x_0 : \cdots : \lambda x_n)$ for any $\lambda \in k^*$. The scaling-invariant coordinates are called *homogeneous coordinates*.

The *Zariski topology* on $\mathbb{P}^n$ is given as in the affine case by taking the projective varieties as a basis for the closed sets. The relationship between projective and affine varieties can now be made precise. For $i = 0, \ldots, n$ let $H_i \subset \mathbb{P}^n$ be the hypersurface given by the vanishing of x_i. We see that

$$\mathbb{P}^n \setminus H_i = \left\{\left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, 1, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right)\right\} \simeq \mathbb{A}^n.$$

Hence, $\mathbb{P}^n$ is covered by $n+1$ copies of $\mathbb{A}^n$ which are open subsets of $\mathbb{P}^n$. We can thus think of affine varieties as local charts of the global projective space.

Recall that a polynomial is called *homogeneous* if all terms have the same (total) degree. A subset $V \subseteq \mathbb{P}^n$ is called a projective variety if it given as the common vanishing of a set of homogeneous polynomials $\{f_i\}_{i \in I} \subset k[x_0, \ldots, x_n]$. We write

$$V = \mathbb{V}(\{f_i\}_{i \in I}) = \{x \in \mathbb{P}^n : f_i(x) = 0 \text{ for all } i \in I\}.$$

This is well-defined since if $f \in k[x_0, \ldots, x_n]$ is a homogeneous polynomial of degree d, we have

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$$

for all $\lambda \in k^*$, so the question of whether f vanishes or not is independent on the choice of homogeneous coordinates.

We say that an ideal is *homogeneous* if it is generated by homogeneous polynomials. To each homogeneous ideal $I \subseteq k[x_0, \ldots, x_n]$ we associate a projective variety

$$\mathbb{V}(I) = \{x \in \mathbb{P}^n : f(x) = 0 \text{ for all } f \in I\},$$

where by $f(x) = 0$ we mean that f vanishes for all representations of x in $\mathbb{A}^{n+1}$. On the other hand we may associate a homogeneous ideal to each projective variety $V \subseteq \mathbb{P}^n$ by:

$$\mathbb{I}(V) = \{f \in k[x_0, \ldots, x_n] : f(x) = 0 \text{ for all } x \in V\}.$$

This is easily seen to be a radical ideal and by Hilbert's basis theorem, it is seen to be finitely generated. It can be checked, that if $f \in \mathbb{I}(V)$ then each of the homogeneous components must also be in $\mathbb{I}(V)$, so it is a homogeneous ideal.

Given a homogeneous ideal $I \subseteq k[x_0, \ldots, x_n]$, care should be taken to distinguish between the affine variety $\mathbb{V}(I) \subset \mathbb{A}^{n+1}$ and the projective variety $\mathbb{V}(I) \subset \mathbb{P}^n$. The affine variety defined by the same polynomials is called the *affine cone* over the projective variety. The standard way of working with projective space is to go to the associated affine cone. For example, we can use it to derive the following correspondence between projective varieties and homogeneous ideals.

Theorem 5.3 (Projective Nullstellensatz) *The projective varieties in $\mathbb{P}^n$ are in one-to-one correspondence with the radical homogeneous ideals in the ring $k[x_0, \ldots, x_n]$ with the exception of the ideal $\langle x_0, \ldots, x_n \rangle$. The correspondence is given by the maps $\mathbb{I}$ and $\mathbb{V}$.*

The ideal $\langle x_0, \ldots, x_n \rangle$ corresponds to the affine variety $\{0\}$ which of course does not correspond to any projective points. It is sometimes known as the *irrelevant ideal*.

Proof. The only hard thing to show, is that if I is an ideal then $\mathbb{I}(\mathbb{V}(I)) = \operatorname{rad} I$. If $I = \langle x_0, \ldots, x_n \rangle$ then $\mathbb{V}(I) = \emptyset$ in $\mathbb{P}^n$ and $\mathbb{I}(\mathbb{V}(I)) = k[x_0, \ldots, x_n]$. Now for any other ideal, the polynomials vanishing on the projective variety $\mathbb{V}(I)$ are precisely the polynomials vanishing on the affine cone $\mathbb{V}(I)$. The result now follows from the affine nullstellensatz. □

A map $F : \mathbb{P}^n \supseteq V \to W \subseteq \mathbb{P}^m$ is called a *(projective) morphism* if it is given locally as a polynomial map. That is, if for each $p \in V$ there exists a (Zariski) open neighborhood U of p such that $F|_U$ is given by

$$F|_U(q) = (F_0(q), \ldots, F_m(q)), \quad (q \in U)$$

for some homogeneous polynomials $F_0, \ldots, F_m \in k[x_0, \ldots, x_n]$. In order for the homogeneous coordinates to be well-defined, it is implicit that the polynomials are all of the same degree and do not vanish at the same time. We say that $F : \mathbb{P}^n \to \mathbb{P}^m$ is a *global morphism* of projective varieties if we

may use the same polynomials everywhere, that is if we may choose $U = \mathbb{P}^n$. A partial map $F : V \to W$ is called a *rational map* if it is a morphism on a (Zariski) open subset $U \subset V$.

§ 5.3 Heights and Morphisms

We introduce the notion of a *height* for rational points in projective space $\mathbb{P}^n(\mathbb{Q})$, which measures the complexity of the rational point. In the introduction we took the height of a rational in reduced terms to be the size of denominator. More generally, for a rational vector in $\mathbb{Q}^n$, we took the height to be the size of least common denominator of the entries. For $P \in \mathbb{P}^n(\mathbb{Q})$ we may write P uniquely up to a sign as

$$P = (x_0 : \cdots : x_n)$$

where $x_0, \ldots, x_n \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$. The projective height is defined by

$$H_{\text{proj}}(p) = \max\{|x_0|, \ldots, |x_n|\}.$$

This is not quite the same notion of complexity as we defined in the introduction. If $p/q \in \mathbb{Q}$ is a rational vector, the natural ways of embedding it in $\mathbb{P}^n(\mathbb{Q})$ are as $P = (p/q : 1) = (p : q)$ and as $P = (1 : p/q) = (q : p)$. In either case, the projective height is $\max\{|p|, |q|\}$.

We are now in a position to derive arithmetic information from the (algebraic) geometry.

Theorem 5.4 *Let $\phi : \mathbb{P}^n \to \mathbb{P}^m$ be a global morphism of degree d defined over $\overline{\mathbb{Q}}$ but with coefficients in $\mathbb{Q}$. For all rational points $P \in \mathbb{P}^n(\mathbb{Q})$ we have*

$$H_{\text{proj}}(P)^d \ll H_{\text{proj}}(\phi(P)) \ll H_{\text{proj}}(P)^d.$$

The implied constants depend on ϕ but not on P.

Proof. As ϕ is a global morphism with rational coefficients, we may write

$$\phi = (\phi_0 : \cdots : \phi_m)$$

for some homogeneous polynomials $\phi_0, \ldots, \phi_m \in \mathbb{Q}[X_0, \ldots, X_n]$ of degree d. Write out each ϕ_i explicitly as

$$\phi_i(X_0, \ldots, X_n) = \sum_{e_0 + \cdots + e_n = d} c_{i,e_0,\ldots,e_n} X_0^{e_0} \cdots X_n^{e_n}.$$

We now establish the upper bound. Consider $P \in \mathbb{P}^n(\mathbb{Q})$ and write $P = (x_0 : \cdots : x_n)$ for $x_0, \ldots, x_n \in \mathbb{Z}$ coprime integers. We find that

$$\begin{aligned} |\phi_i(x_0, \ldots, x_n)| &= \left| \sum_{e_0+\cdots+e_n=d} c_{i,e_0,\ldots,e_n} x_0^{e_0} \cdots x_n^{e_n} \right| \\ &\ll \max |x_j|^d. \end{aligned}$$

Taking the maximum and clearing possible denominators coming from the ϕ_i's yields

$$H(\phi(P)) \ll H(P)^d.$$

We now turn to the lower bound. The polynomials $\phi_0, \ldots, \phi_m$ have no common point of vanishing other than 0. Thus, as affine varieties, we have

$$\mathbb{V}(\phi_0, \ldots, \phi_m) = \{0\} = \mathbb{V}(X_0, \ldots, X_n).$$

The affine Nullstellensatz (Theorem 5.1) yields the following equality of ideals in the ring $\overline{\mathbb{Q}}[X_0, \ldots, X_n]$:

$$\operatorname{rad}\left(\langle \phi_0, \ldots, \phi_m \rangle\right) = \langle X_0, \ldots, X_n \rangle.$$

Hence there exists polynomials $g_{ij} \in \overline{\mathbb{Q}}[X_0, \ldots, X_n]$ and a natural number $p \in \mathbb{N}$ such that

$$X_j^p = \sum_{i=0}^{n} g_{ij} \phi_i \quad (0 \leq j \leq n).$$

We may further take the g_{ij}'s to be homogeneous polynomials with coefficients in $\mathbb{Q}$.

Now consider $P \in \mathbb{P}^n(\mathbb{Q})$ and write $P = (x_0 : \cdots : x_n)$ for $x_0, \ldots, x_n \in \mathbb{Z}$ coprime integers. Evaluating the above in the affine point $(x_0, \ldots, x_n)$ we find

$$x_j^p = \sum_{i=0}^{n} g_{ij}(x_0, \ldots, x_n) \phi_i(x_0, \ldots, x_n)$$

As the ϕ_i's are homogeneous of degree d the g_{ij}'s must have degree $p - d$ so

$$|g_{ij}(x_0, \ldots, x_n)| \ll \max_j |x_j|^{p-d}, \quad (0 \leq j \leq n).$$

So we get the estimate

$$\max_j |x_j|^p \ll \max_j |x_j|^{p-d} \max_i |\phi_i(x_0, \ldots, x_n)|.$$

Since the only possible denominators are those coming from the ϕ_i's, we find that

$$H(\phi(P)) \gg H(P)^d. \qquad \square$$

It is possible to generalize the theorem to number fields, as well as the case of subvarieties and sufficiently nice rational maps see [HS00, Theorem B.2.5]. The constants may also be made effective by using an effective version of the Nullstellensatz.

The upper bound holds even if ϕ is only a rational map, but the lower bound depends both on the fact that the morphism is global and that it is defined over an algebraically closed field. To see this, consider the affine map $(x, y) \mapsto x^2 + y^2$. Since there are infinitely many Pythagorean triples, we have rationals of arbitrarily large height which map to 1. A projective version of this map is that map $F : \mathbb{P}^2 \to \mathbb{P}^1$ given by

$$F(X, Y, Z) = (X^2 + Y^2, Z^2).$$

Note that it restricts to the map above in the affine chart given by $Z = 1$. It is easy to see that this is a morphism over $\mathbb{Q}$ and it also restricts to a morphism over $\overline{\mathbb{Q}}$ in the affine chart $Z = 1$. But it is not a global morphism over $\overline{\mathbb{Q}}$ as it is not defined at the point $(1 : i : 0)$. It is thus very close to satisfying the conditions of the theorem, and yet the upper bound fails to hold in a spectacular way: For any Pythagorean triple $p^2 + r^2 = q^2$ we have $H_{\text{proj}}(p : r : q) = q$ while

$$H_{\text{proj}}(F(p : r : q)) = H_{\text{proj}}(p^2 + r^2 : q^2) = H_{\text{proj}}(1 : 1) = 1.$$

This shows a quite remarkable interplay between geometry and arithmetic. The local arithmetical properties are governed by the geometry at "infinity" over a larger field!

It would be quite interesting to know if we could go the other way. That is, given a rational map $\phi : \mathbb{P}^n \to \mathbb{P}^m$ which satisfies the conclusion of Theorem 5.4, what can be said about the geometry of ϕ?

§ 5.4 Diophantine Approximation and Algebraic Geometry

The most basic question in algebraic geometry is the problem of classifying all varieties up to isomorphism. Similarly, we might frame the problem of metric Diophantine approximation on varieties as one of classifying all varieties by the quality of approximation possible on them. From the previous section is seems obvious to suggest that the answer lies in the classification of projective varieties.

However, it turns out that the question of Diophantine approximation relies not just on the projective variety, but also by the "coordinate system"

given in terms of its embedding into projective space. To see this, consider the morphism $\phi : \mathbb{P}^1 \to \mathbb{P}^2$ given by $(x : y) \mapsto (x^2 : xy : y^2)$. The image of $\mathbb{P}^1$ under ϕ is the curve

$$C = \mathbb{V}(xz - y^2)$$

and in fact, ϕ provides an isomorphism $C \simeq \mathbb{P}^1$. The inverse morphism is given by

$$\begin{aligned} C &\to \mathbb{P}^1 \\ (x : y : z) &\mapsto \begin{cases} (x : y) \text{ if } x \neq 0, \\ (x : z) \text{ if } z \neq 0. \end{cases} \end{aligned}$$

The map is defined everywhere since if $z = x = 0$ then $zx = y^2 = 0$ and $y = 0$, which is impossible. It is well-defined since if both x and z are non-zero, then y is non-zero, and

$$(x : y) = (yx : y^2) = (xy : xz) = (y : z).$$

Furthermore, it is easily seen to be an inverse.

We thus see that Diophantine aspects are not *intrinsic* to the algebraic variety. That is not to say that algebraic geometry is not useful, but that more care is needed. The field of *Diophantine geometry* concerns how to do this, but it requires some substantial technical baggage, even for something as simple as defining a good intrinsic notion of height. The idea here is to consider the functions on the variety (algebraically known as divisors) and using these to construct a *canonical* morphism into projective space in which a height can be measured. For more information see [HS00].

Chapter 6

A JARNÍK-TYPE THEOREM FOR VARIETIES

Let $P_1, \dots, P_m \in \mathbb{Z}[X_1, \dots, X_n]$ be integer polynomials in n variables, and consider the variety given as the graph of the polynomials:

$$\Gamma = \{(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{R}^n \times \mathbb{R}^m : y_1 = P_1(\boldsymbol{x}), \dots, y_m = P_m(\boldsymbol{x})\}.$$

Let $d = \max_j \deg P_j$ be the maximum degree of the polynomials. For an approximation function ψ, we consider the set of ambiently ψ-approximable vectors $\mathcal{S}_\psi(\Gamma) = \mathcal{S}_\psi \cap \Gamma$ as well as the set of intrinsically ψ-approximable vectors $\mathcal{I}_\psi(\Gamma)$ as introduced in Chapter 4. Our main result is the following Jarník-type theorem which appeared in [Til17]. It generalizes the main theorem of [BDL10], which considered the case $n = 1$ where the variety is a curve.

Theorem 6.1 *Let ψ be a decreasing approximation function and let h be a dimension function such that for all $\delta > 0$ we have $h(\psi(\delta r)) \ll h(\psi(r))$ when r is large. Suppose that $r^{-n}h(r) \to \infty$ as $r \to 0$ and $r \mapsto r^{-n}h(r)$ is decreasing. Write*

$$P_i = P_{i,0} + \cdots + P_{i,d}$$

where $P_{i,k}$ are homogeneous polynomials of degree k, and suppose that the only common point of vanishing for $\{P_{i,d}\}_{i=1}^m$ over $\overline{\mathbb{Q}}$ is 0. The Hausdorff h measure of $\mathcal{I}_\psi(\Gamma)$ satisfies

$$\mathcal{H}^h(\mathcal{I}_\psi(\Gamma)) = \begin{cases} 0 & \text{if } \sum_{r=1}^{\infty} r^n h(\psi(r^d)) < \infty, \\ \infty & \text{if } \sum_{r=1}^{\infty} r^n h(\psi(r^d)) = \infty. \end{cases}$$

Furthermore, if $r^d\psi(r) \to 0$ as $r \to \infty$ we have $\mathcal{I}_\psi(\Gamma) = \mathcal{S}_\psi(\Gamma)$.

As a corollary, we derive the following statement on the Hausdorff dimension.

Corollary 6.2 *Suppose that the polynomials defining* Γ *satisfy the condition of the theorem. For* $\tau > (n+1)/nd$*, the Hausdorff dimension of* $\mathcal{I}_\tau(\Gamma)$ *is given by*

$$\dim \mathcal{I}_\tau(\Gamma) = \frac{1+n}{d\tau}.$$

Proof of corollary. Put $\psi(r) = r^{-\tau}$ and $h(r) = r^s$ where $s = (1+n)/d\tau$. We see that

$$r^{-n}h(r) = r^{s-n} \to \infty \text{ as } r \to 0$$

precisely when

$$s - n = \frac{1+n}{d\tau} - n < 0.$$

But this is satisfied as $\tau > (1+n)/d\tau$.

By the strict inequality, the condition of the theorem is satisfied for dimension functions $h(r) = r^t$ where t is in some small interval around s. It follows that $\mathcal{H}^t(\mathcal{I}_\tau(\Gamma)) = \infty$ when $t \leq s$ and $\mathcal{H}^t(\mathcal{I}_\tau(\Gamma)) = 0$ when $t > s$. $\square$

We now turn to the proof of the theorem. The strategy is the same as in [BDL10]: Project down to $\mathbb{R}^n$ where we may apply Jarník's theorem and estimate how the projection changes the distribution and height of the rationals. The only novelty in our argument is the use of algebraic geometry to control the height of the rationals, which in the case of curves was done explicitly. We prove the theorem through three lemmas, which establish the cases of convergence and divergence as well as the equality of ambient and intrinsic approximation separately. This also highlights which assumptions are used in the different parts.

We begin by making some reductions in order to write the set $\mathcal{I}_\psi(\Gamma)$ as a more manageable limsup set. Since we are aiming for a zero-infinity law, it suffices to show that the Hausdorff measure of the ψ-approximable points is either full or null for sets of the form

$$\Gamma_I = \{(\boldsymbol{x}, P_1(\boldsymbol{x}), \dots, P_m(\boldsymbol{x})) \in I^n \times \mathbb{R}^m\}$$

where $I \subset \mathbb{R}$ is some arbitrary bounded interval. In order to make the notation simpler, we take $I = [0,1]$ to be the unit interval, although the argument does not make use of this in any essential way.

Define the function $F : \mathbb{R}^n \to \Gamma$ by

$$F(\boldsymbol{x}) = (\boldsymbol{x}, P_1(\boldsymbol{x}), \dots, P_m(\boldsymbol{x})).$$

By the mean value theorem, we may find a constant $K \geq 1$ such that for any $\boldsymbol{x_1}, \boldsymbol{x_2} \in I^n$, we have

$$\|\boldsymbol{x_1} - \boldsymbol{x_2}\|_\infty \leq \|F(\boldsymbol{x_1}) - F(\boldsymbol{x_2})\|_\infty \leq K\|\boldsymbol{x_1} - \boldsymbol{x_2}\|_\infty$$

and we see that F is bi-Lipschitz on I^n. By Corollary 2.10 the Hausdorff measure is changed by at most a constant under a bi-Lipschitz mapping. It hence suffices to show that the Hausdorff measure is full or null for the set

$$V_\psi(\Gamma_I) = \{\boldsymbol{x} \in I^n : F(\boldsymbol{x}) \in \mathcal{I}_\psi(\Gamma)\}.$$

For a rational vector $\boldsymbol{x} \in \mathbb{Q}^k$, the *affine height* is the least natural number D such that

$$\boldsymbol{x} = (r_1/D, \ldots, r_k/D) \quad \text{and} \quad \gcd(r_1, \ldots, r_n, D) = 1$$

for some integers $r_1, \ldots, r_k \in \mathbb{Z}$. Denote the height of $\boldsymbol{x} \in \mathbb{Q}^k$ by $H(\boldsymbol{x})$.

Recall that $V_\psi(\Gamma_I)$ consists of the set of $\boldsymbol{x} \in I^n$ such that

$$\|F(\boldsymbol{x}) - \boldsymbol{r}\|_\infty \leq \psi(H(\boldsymbol{r}))$$

for infinitely many rationals $\boldsymbol{r} \in \Gamma_I \cap \mathbb{Q}^{n+m}$. Such rationals are necessarily of the form $\boldsymbol{r} = F(\boldsymbol{p}/q)$ for some rational $\boldsymbol{p}/q$.

We may now write $V_\psi(\Gamma_I)$ as a limsup set. Put

$$L_q \coloneqq \{\boldsymbol{p} \in \mathbb{Z} : 0 \leq p_1, \ldots, p_n \leq q,\ \gcd(p_1, \ldots, p_n, q) = 1\}.$$

We have

$$\begin{aligned} &\bigcap_{N=1}^{\infty} \bigcup_{q>N} \bigcup_{\boldsymbol{p} \in L_q} B\left(\frac{\boldsymbol{p}}{q}, \frac{\psi(H(F(\boldsymbol{p}/q)))}{K}\right) \subseteq V_\psi(\Gamma_I), \\ &V_\psi(\Gamma_I) \subseteq \bigcap_{N=1}^{\infty} \bigcup_{q>N} \bigcup_{\boldsymbol{p} \in L_q} B\left(\frac{\boldsymbol{p}}{q}, \psi(H(F(\boldsymbol{p}/q)))\right). \end{aligned} \tag{6.1}$$

Lemma 6.3 (Divergence case) *Let ψ be a decreasing approximation function and let h be a dimension function. Suppose that $r^{-n}h(r) \to \infty$ as $r \to 0$ and $r \mapsto r^{-n}h(r)$ is decreasing. If $\sum_{r=1}^{\infty} r^n h(\psi(r^d)) = \infty$, then $\mathcal{H}^h(\mathcal{I}_\psi(\Gamma)) = \infty$.*

Proof. Let $\boldsymbol{p}/q \in I^n$ be some rational vector. It is clear that q^d is a common multiple of all denominators in $F(\boldsymbol{p}/q)$ so $H(F(\boldsymbol{p}/q)) \leq q^d$. As ψ is decreasing we have

$$\frac{\psi(H(F(\boldsymbol{p}/q)))}{K} \geq \frac{\psi(q^d)}{K}.$$

We thus have

$$\bigcap_{N=1}^{\infty} \bigcup_{q>N} \bigcup_{\boldsymbol{p} \in L_q} B\left(\frac{\boldsymbol{p}}{q}, \frac{\psi(q^d)}{K}\right) \subseteq V_\psi(\Gamma_I).$$

The set on the left is just the set of $\phi(q) \coloneqq \psi(q^d)/K$-approximable points in I^n. By Jarník's theorem (Theorem 3.2) this set has full measure if

$$\sum_{r=1}^{\infty} h(\phi(r))r^n = \infty.$$

By the discussion in chapter 2, without loss of generality, we may assume that h is doubling so that $h(\psi(r^d)/K) \gg h(\psi(r^d))$ when r is large. This gives

$$\sum_{r=1}^{\infty} h(\psi(r^d)/K)r^n \gg \sum_{r=1}^{\infty} h(\psi(r^d))r^n = \infty. \qquad \square$$

Lemma 6.4 (Convergence case) *Let ψ be a decreasing approximation function and let h be a dimension function such that $h(\psi(\delta r)) \ll h(\psi(r))$ when r is sufficiently large. Write*

$$P_i = P_{i,0} + \cdots + P_{i,d}$$

where $P_{i,k}$ are homogeneous polynomials of degree k, and suppose that the only common point of vanishing for $\{P_{i,d}\}_{i=1}^m$ over $\overline{\mathbb{Q}}$ is 0. If we have $\sum_{r=1}^{\infty} r^n h(\psi(r^d)) < \infty$, then $\mathcal{H}^h(\mathcal{I}_\psi(\Gamma)) = 0$.

Proof. We wish to apply Theorem 5.4 to control the height of the rationals under F. In order to do this, we need to extend F to projective space. For each of the defining polynomials $P_i \in \mathbb{Z}[X_1, \ldots, X_n]$ write $P_i = P_{i,0}+\cdots+P_{i,d}$ in homogeneous components and define the *degree-d homogenization* of P_i by

$$P_i^* = X_0^d P_{i,0} + X_0^{d-1} P_{i,1} + \cdots + P_{i,d}.$$

Now $P_i^* \in \mathbb{Z}[X_0, \ldots, X_n]$ is a homogeneous polynomial of degree d which is equal to P_i in the affine patch $X_0 = 1$. Define the (rational) map $F^* : \mathbb{P}^n \to \mathbb{P}^m$ by

$$\begin{aligned} &F^*(X_0 : \cdots : X_n) \\ &= (X_0^d : X_0^{d-1}X_1 : \cdots : X_0^{d-1}X_n : P_1^*(X_0, \ldots, X_n) : \cdots : P_n^*(X_0, \ldots, X_n)). \end{aligned}$$

In the affine patch $X_0 = 1$ this is just the map F from above. Furthermore, we claim that this map is a global morphism over $\overline{\mathbb{Q}}$. To see this, we just need to check that the defining polynomials do not have a common point of vanishing other than 0. For $X_0 \neq 0$ this is clearly true as then $X_0^d \neq 0$. If $X_0 = 0$, then the defining polynomials vanish if and only if the polynomials $P_{1,d}, \ldots, P_{m,d}$ has a common point of vanishing other than 0,

but the assumption of the theorem was precisely that this does not happen. We conclude that F^* is a global morphism of $\overline{\mathbb{Q}}$.

Now let $\boldsymbol{p}/q \in I^n$ be a rational vector. Since I is a bounded interval, the ratio of the projective height of and affine height is bounded by a constant. We now have

$$\begin{aligned} q^d \leq H_{\mathrm{proj}}((1 : p_1/q : \cdots : p_n/q))^d &\ll H_{\mathrm{proj}}(F^*(1 : p_1/q : \cdots : p_n/q)) \\ &\ll H(F(\boldsymbol{p}/q)). \end{aligned}$$

The implied constants here only depend on Γ and I. Let $\delta > 0$ be a constant such that $H(F(\boldsymbol{p}/q)) \geq \delta q^d$. Now, by the inclusion (6.1) and the estimate $h(\psi(\delta q^d)) \ll h(\psi(q^d))$ we get, for any $N \in \mathbb{N}$:

$$\begin{aligned} \mathcal{H}^h(V_\psi(\Gamma_I)) &\ll \sum_{q>N} \sum_{\boldsymbol{p} \in L_q} h(\psi(H(F(\boldsymbol{p}/q)))) \\ &\ll \sum_{q>N} q^n h(\psi(q^d)) < \infty. \end{aligned}$$

So we find that the Hausdorff measure of $V_\psi(\Gamma_I)$ is bounded by the tail of a convergent series, and hence that $\mathcal{H}^h(V_\psi(\Gamma_I)) = 0$. □

Finally, we need to establish the equivalence of ambient and intrinsic approximation. This was already shown in full generality in [BDL10, Lemma 1].

Lemma 6.5 *Let ψ be an approximation function satisfying the growth condition $r^d\psi(r) \to 0$ as $r \to \infty$. Let $(\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{S}_\psi(\Gamma)$. If*

$$\|(\boldsymbol{x}, \boldsymbol{y}) - (\boldsymbol{r}, \boldsymbol{t})\|_\infty \leq \psi(H(\boldsymbol{r}, \boldsymbol{t}))$$

for $(\boldsymbol{r}, \boldsymbol{t}) \in \mathbb{Q}^{n+m}$ with $H(\boldsymbol{r}, \boldsymbol{t})$ sufficiently large, then $(\boldsymbol{r}, \boldsymbol{t}) \in \Gamma$.

Proof. Define $D = H(\boldsymbol{r}, \boldsymbol{t})$ and put $\varepsilon_i = x_i - r_i$ and $\eta_j = y_j - t_j$. By assumption we have $|\varepsilon_i|, |\eta_j| \leq \psi(D)$.

We have

$$y_j = P_j(\boldsymbol{x}) = P_j(\boldsymbol{r} + \boldsymbol{\varepsilon})$$

so

$$y_j = t_j + \eta_j = P_j(\boldsymbol{r}) + R_j(\boldsymbol{\varepsilon})$$

for some polynomial R_j where $R_j(\boldsymbol{\varepsilon}) \ll \|\boldsymbol{\varepsilon}\|_\infty$ for $\boldsymbol{\varepsilon}$ small. Multiply by D^d and rearrange to obtain

$$\left|D^d t_j - D^d P_j(\boldsymbol{r})\right| = D^d |\eta_j + R_j(\boldsymbol{\varepsilon})|,$$

where we've cleared denominators, so the left hand side is seen to be an integer. The right hand side can be estimated by

$$D^d|\eta_j + R_j(\boldsymbol{\varepsilon})| \ll D^d\psi(D)$$

which tends to 0 as $D \to \infty$. Hence, for D sufficiently large, we have

$$t_j = P_j(\boldsymbol{r}).$$

We conclude that $(\boldsymbol{r}, \boldsymbol{t}) \in \Gamma$ as desired. □

The proof of the theorem is now just a formality.

Proof of Theorem 6.1. This follows immediately from Lemmas 6.3, 6.4 and 6.5. □

The most restrictive condition in the theorem is the assumption that the degree-d parts of the defining polynomials have no common point of vanishing away from 0 over $\overline{\mathbb{Q}}$. As we previously mentioned, this always holds in the case of curves where $n = 1$ as the terms would be of the form cx^d for some constant c. Examples in several variables include the Veronese varieties, where we have all possible forms of degree d. Another example is given by $\Gamma = \{(x, y, x^2 + y^2, x^2 - y^2)\}$. In the other direction, it never holds for hypersurfaces when $n > 1$: The zero locus of the highest degree part of the polynomial over an algebraically closed field would have dimension $n - 1$ and hence cannot be a point. In general we need at least as many polynomials as we have variables.

The obvious question is whether this theorem may be generalized further. The key ingredient is the estimate $H(F(\boldsymbol{r})) \gg H(\boldsymbol{r})^d$, which is derived from Theorem 5.4. It seems unlikely that this theorem can be generalized in the direction we need, so the estimate probably fails for other varieties. When the estimate fails we get additional rational points of low height on the variety. In order to do Diophantine approximation on such varieties, we would need new methods for controlling how many and how well-distributed these points are.

Part II

Continued Fractions

Chapter 7

A QUANTUM COMPUTATIONAL CONUNDRUM

In this chapter, we will explain how a problem of constructing universal quantum computers leads to new questions in Diophantine approximation, and links the metric and algorithmic aspects of the theory. This connection was pointed out by Peter Sarnak [Sar15].

We will briefly introduce the notions of quantum mechanical computers, the exposition will be short and we will omit most of the physics. The classical reference for this is Nielsen and Chuang [NC00].

§ 7.1 The Circuit Model for Computation

Before explaining what a quantum computer is, we will explain what we mean by a classical computer. There are many theoretical models for a classical computer, with the most famous probably being the Turing machine. For our purposes, we will introduce a somewhat more practical model called the *circuit* model.

The most basic unit of information in a classical computer is the *bit* consisting of 1 or 0, which we often think of as true or false. A *logical gate* is a Boolean function

$$f : \{0,1\}^m \to \{0,1\}^n$$

of m input bits and n output bits. A *circuit* is a collection of logical gates connected by wires, which connects outputs to inputs without loops.

There are only two gates with 1 input bit and 1 output bit: the trivial (identity) gate, and the `NOT` gate which takes 0 to 1 and 1 to 0. Examples of gates with 2 input bits and 1 output bit are the classical logical operations: `AND`, `OR`, exclusive-or `XOR` along with the inverted versions of these, for instance NOT-AND or `NAND`. Additionally we have the very important `FANOUT` gate, which simply copies the input to two outputs.

A set of gates $\mathcal{G}$ is called *universal* if any function can be constructed from a circuit of gates from $\mathcal{G}$ with wires, extra bits and the `FANOUT` operation. A classical result in computing is that the `NAND`-gate alone is universal, a fact that can be shown by small induction proof.

§ 7.2 Quantum Mechanical Computers

Quantum States

The smallest state in quantum computing is the *quantum bit* or *qubit*. A qubit $\boldsymbol{\psi}$ is a complex linear combination of the two classical states

$$\boldsymbol{\psi} = \alpha\mathbf{0} + \beta\mathbf{1}$$

normalized such that $|\alpha|^2 + |\beta|^2 = 1$. If we *measure* the quantum bit, we get 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$. Thus, we may describe a quantum bit as a unit vector in $\mathbb{C}^2$.

It would seem that the quantum bit contains an infinite amount of information, however this is not so. Unlike in the classical world, quantum measurements are not passive but *active*. After measuring either the state 1 or 0, the qubit *decays* to this state, and all subsequent measurements will give the same result. From an information theoretical perspective, a qubit thus carries at most the entropy of a coin-flip which is 1 bit.

Going further, an n-qubit state is a unit vector in the tensor product

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2 \cong \mathbb{C}^{2n}.$$

Note that we allow all possible states. So for instance, we might consider the state

$$\boldsymbol{\psi} = \frac{\mathbf{0} \otimes \mathbf{0} + \mathbf{1} \otimes \mathbf{1}}{\sqrt{2}}$$

which is known as the Bell state or EPR[1] pair. This state has the property, that if we measure just the first qubit it gives 0 and 1 with equal probability and then decays to the measured state. Now the second qubit must give the same result, so it also has to decay. This is an example of *quantum entanglement*.

Quantum Gates

We begin by describing 1-qubit quantum gates. Such a gate should be a function

$$f : \mathbb{C}^2 \to \mathbb{C}^2.$$

But not all such functions are allowed. It turns out that we need to require that f is linear. Secondly, the states were really unit vectors in $\mathbb{C}^2$ so we need to assume that f is an isometry. These are the only constrains we

[1] Einstein, Podolsky, Rosen

need, so we define the set of 1-bit quantum gates to be the group $U(2)$ of unitary 2×2 matrices. A good example of a 1-qubit quantum gate is the extension of the classical NOT gate given by

$$\texttt{NOT} : \alpha\mathbf{0} + \beta\mathbf{1} \mapsto \beta\mathbf{0} + \alpha\mathbf{1}$$

or as a matrix

$$U_{\texttt{NOT}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Similarly, a k-bit quantum gate is an element of $U(2k)$. Note that these restrictions mean that all quantum gates must be invertible, unlike in the case of classical gates, and hence there are no direct analogous of the AND-, OR- and NAND-gates. The prototypical example of a 2-qubit quantum gate is the controlled-NOT or CNOT-gate, which is defined by:

$$\begin{aligned} \mathbf{0} \otimes \mathbf{0} &\mapsto \mathbf{0} \otimes \mathbf{0} \\ \mathbf{0} \otimes \mathbf{1} &\mapsto \mathbf{0} \otimes \mathbf{1} \\ \mathbf{1} \otimes \mathbf{0} &\mapsto \mathbf{1} \otimes \mathbf{1} \\ \mathbf{1} \otimes \mathbf{1} &\mapsto \mathbf{1} \otimes \mathbf{0} \end{aligned}$$

or in matrix form

$$U_{\texttt{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

That is, if the first entry is 0, the second entry is the identity, if the first entry is 1, the second entry is a NOT-gate. Another way of describing it, is that it's the identity on the first output and XOR on the second output.

A quantum circuit is now constructed in much the same way as a classical circuit: We have gates connected with "wires" without loops. However, we do not allow combining "wires" through the OR-operation, as this is not an invertible operation. Additionally, there is no FANIN operation. In fact, copying an unknown quantum state is impossible, a fact known as the *No-Cloning Theorem*.

Universal Quantum Gates

A set of gates $\mathcal{G}$ is called *universal* if any quantum gate can be *approximated* arbitrarily well by a finite circuit with gates from $\mathcal{G}$. We would like to obtain a universality result analogous to the universality of NAND-gates for classical computers. It is a reasonable assumption that the time complexity of a

quantum circuit is proportional to the number of gates, hence we would also like the universal set to be *efficient*.

A *two-level unitary matrix* is a unitary matrix U which only acts non-trivial on at most two vectors. A little bit of linear algebra shows that any unitary matrix can be decomposed as a product of two-level unitary matrices. This shows that the set of 2-qubit quantum gates is universal. Furthermore, it can be shown that any two-level unitary transformation can be approximated by single-qubit gates and the `CNOT`-gate. This process is algorithmic and close to optimal. See [NC00, Chapter 4] for details.

This still leaves us with an infinite set of gates, which is not practical. We are then left with our main problem: Finding an efficient, universal set of 1-bit quantum gates.

§ 7.3 A Mathematical Framework

We begin by rephrasing the problem in a more mathematical setting, which unfortunately comes with quite a bit of notation. We replace the group $U(2)$ by $G := \mathrm{SU}(2)$ – the only difference is an unimportant phase factor. This group is equipped with a (left) Haar measure which we denote by μ and normalize such that $\mu(G) = 1$.

We consider a finite set of gates

$$S = \{s_1, \ldots, s_\nu\} \subset G$$

and the subgroup generated by this set

$$\Gamma = \langle S \rangle \subset G.$$

We assume that this set is a universal set of gates, such that $\langle S \rangle$ is dense in G. We allow each gate to have a cost associated with them, which we denote $w(s_i) \geq 0$. We now define the *height* on Γ by

$$h(\gamma) = \min\left\{ \sum_{k=1}^{l} w(s_{i_k}) : \gamma = s_{i_1} \cdots s_{i_l} \right\}.$$

For each natural number t put

$$V(t) = \{\gamma \in \Gamma : h(\gamma) \leq t\}.$$

For each $\varepsilon > 0$ let t_ε denote the smallest t such that the set of gates of height at most t cover G, i.e.

$$G \subseteq \bigcup_{\gamma \in V(t)} B_G(\gamma, \varepsilon).$$

Note that $|V(t_\varepsilon)|$ is essentially the number of gates we need to cover G with balls of size ε, so if the gates were optimally spread out, we would expect

$$|V(t_\varepsilon)| \sim \frac{1}{\mu(B_\varepsilon)}$$

where $\mu(B_\varepsilon)$ denotes the measure of a ball of radius ε. Now suppose we have $|V(t_\varepsilon)| \sim \mu(B_\varepsilon)^{-\kappa}$ for some $\kappa > 0$, then we would have

$$\kappa = \lim_{\varepsilon \to 0} \frac{\log|V(t_\varepsilon)|}{-\log \mu(B_\varepsilon)}.$$

Of course we have no reason to make this assumption nor do we have any reason to expect the limit to exist at all, however it motivates the following definition.

Definition 7.1 The number

$$\kappa := \limsup_{\varepsilon \to 0} \frac{\log|V(t_\varepsilon)|}{-\log \mu(B_\varepsilon)}$$

is called the (upper) *covering exponent* of the gate set S.

This number is a reasonable measure of how well-chosen our set of gates is.

Our problems are now the following:

(A) How small can we make the covering exponent κ by choosing S suitably?

(B) For a given (well-chosen) gate set, can we find an efficient approximation algorithm?

The first result towards the existence of a good universal gate set, is the following theorem known as the Solovay-Kitaev theorem see [NC00, App. 3] and [DN06].

Theorem 7.2 (Solovay-Kitaev) *Let S be a finite set of gates which contains its own inverses, such that $\langle S \rangle$ is dense in G. Let $\varepsilon > 0$ and $x \in G$ be given. There is an algorithm which finds $\gamma \in \Gamma$ with*

$$d_G(x, \gamma) \leq \varepsilon, \quad h(\gamma) = O(\log(1/\varepsilon)^{3.97})$$

in time $O(\log(1/\varepsilon)^{2.97}$.

The idea of the proof is to walk around randomly, until you reach a specified distance (say 1/10) from the identity I. Then, you go to the Lie algebra, and apply a process similar to Newton's method.

The Solovay-Kitaev theorem is very general and completely answers the question in a theoretical sense: any quantum circuit may be simulated on a quantum computer constructed from a gate set as above with at most a polynomial time cost. In this way, a computer constructed from these circuits is universal from a perspective of complexity classes.

From a more practical perspective, a polynomial time simulation cost is not acceptable and indeed the Solovay-Kitaev theorem does not even guarantee the existence of a gate set with $\kappa < \infty$. To get an idea of what we should expect, suppose that $|V(t)| \sim e^t$, then if $\kappa < \infty$ we have

$$t_\varepsilon \approx \log|V(t_\varepsilon)| \approx -\kappa \log \mu(B_\varepsilon) \approx -\log(\varepsilon^3) \approx \log(1/\varepsilon).$$

So the Solovay-Kitaev algorithm is off by up to a exponent of 4. In other words, the Solovay-Kitaev theorem might give an approximation using 10.000 gates where 10 might suffice, this is clearly not practical!

In order to do better, we need to be more specific in our construction. It turns out, almost magically, that all known good constructions (even those originating from physics) can be constructed from number theoretical methods. We now describe one such example.

§ 7.4 An Example of an Efficient Gate Set

The following example was originally used by Lubotzky et. al. [LPS86] to construct a well-distributed set of rotations from SO(3), and discussed in connection with universal quantum computers in Sarnak's letter [Sar15].

Consider the prime number $p = 5$. Let

$$S = \{s_1, s_1^{-1}, s_2, s_2^{-1}, s_3, s_3^{-1}\}$$

where

$$s_1 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1+2i & 0 \\ 0 & 1+2i \end{pmatrix}, \quad s_2 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}, \quad s_3 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}.$$

We take $w(s_i) = 1$ for $i = 1, 2, 3$. Here, Γ is the free group on s_1, s_2, s_3 and $h(\gamma)$ is the reduced word length, that is the length of the word without subwords of the form $s_i s_i^{-1}$ or $s_i^{-1} s_i$. We will see, that if we include some non-important phase factors this is a universal gate set.

It turns out, that these elements and their approximation properties have a very nice interpretation in terms of the quaternion algebra which we now review.

Quaternion Arithmetic

We consider the classical Hamilton quaternions

$$\mathbb{H}(\mathbb{R}) = \{a_0 + a_1 i + a_2 j + a_3 k : a_i \in \mathbb{R}\}$$

where i, j, k satisfy the relations $i^2 = j^2 = k^2 = -1$ and $ij = k$. If $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ is a quaternion, we define the *conjugate* by

$$\overline{\alpha} = a_0 - a_1 i - a_2 j - a_3 k$$

and define the *norm* by[2]

$$N(\alpha) = \alpha\overline{\alpha} = a_0^2 + a_1^2 + a_2^2 + a_3^2.$$

We can embed the quaternions into the space of complex 2×2 matrices by

$$a_0 + a_1 i + a_2 j + a_3 k \mapsto \begin{pmatrix} a_0 + a_1 i & a_2 + a_3 i \\ -a_2 + a_3 i & a_0 - a_1 i \end{pmatrix}.$$

In this way conjugation corresponds to the conjugate transpose matrix, and the norm corresponds to the determinant. In particular, if we restrict to the quaternions of unit norm $\mathbb{H}_1(\mathbb{R})$ we get an isomorphism $\mathbb{H}_1(\mathbb{R}) \cong \mathrm{SU}(2)$.

Now consider the integral quaternions (not to be confused with the Hurwitz integers)

$$\mathbb{H}(\mathbb{Z}) = \{a_0 + a_1 i + a_2 j + a_3 k : a_i \in \mathbb{Z}\}.$$

In general, these are not quite as nice as one could hope, but Dickson [Dic22] has shown that the odd elements (elements with $N(\alpha)$ odd) is a left- and right Euclidean ring. Furthermore, the prime elements are precisely the elements where $N(\alpha)$ is a rational prime. It is clear that the units in $\mathbb{H}(\mathbb{Z})$ are precisely $\pm 1, \pm i, \pm j, \pm k$. It is also clear the number of elements with $N(\alpha) = n$ is equal to the number of representations of n as a sum of four squares, which is well-known to be given by

$$r_4(n) = 8 \sum_{d|n,\, 4\nmid d} d. \tag{7.1}$$

Now let p be a prime number $p \equiv 1(4)$, for instance $p = 5$. We consider the set of integer quaternions $\alpha \in \mathbb{H}(\mathbb{Z})$ with $N(\alpha) = p$. By reduction modulo 4, we find that for such $\alpha = a_0 + a_1 i + a_2 j + a_3 k$, precisely one of

[2]For reasons which will be clear later, we omit the usual square root from the norm.

a_i, $i = 0, 1, 2, 3$ is odd. Thus, for each α' we may find a unit ε such that $\alpha = \varepsilon\alpha'$ satisfies

$$N(\alpha) = p, \quad a_0 \equiv 1(2), \quad a_1 \equiv a_2 \equiv a_3 \equiv 0(2), \quad a_0 > 0. \tag{7.2}$$

By (7.1) there are $p + 1$ elements of the form (7.2), which clearly split into $\sigma = \frac{1}{2}(p + 1)$ conjugate pairs

$$S_p = \{\alpha_1, \overline{\alpha_1}, \ldots, \overline{\alpha_\sigma}\}.$$

In particular, it is not too hard to see that

$$S_5 = \{1 \pm 2i, 1 \pm 2j, 1 \pm 2k\}.$$

Let $\mathbb{H}_p(\mathbb{Z})$ denote the set of integer quaternions with $N(\alpha) = p^k$ for some k. The following lemma shows that every elements of $\mathbb{H}_p(\mathbb{Z})$ can be written as a product of elements from S_p.

Lemma 7.3 *Every $\beta \in \mathbb{H}_p(\mathbb{Z})$ with $N(\beta) = p^k$ has a unique representation*

$$\beta = p^l \varepsilon R_m(\alpha_1, \ldots, \overline{\alpha_\sigma}),$$

where $l \leq \frac{1}{2}k$, $m + 2l = k$ and R_m is a reduced word (i.e. without subwords of the form $\alpha_j\overline{\alpha_j}$ or $\overline{\alpha_j}\alpha_j$) of length m.

Proof. Let β be such an element. Since the odd elements form a left- and right Euclidean ring, and the primes are exactly the numbers with prime norm, we may factor β as $\beta = \gamma\alpha$ with $N(\gamma) = p^{k-1}$ and $N(\alpha) = p$. Up to a unit we may choose $\alpha \in S_p$. By induction get the factorization

$$\beta = \varepsilon s_1 \ldots s_k, \quad s_i \in S_p$$

and carrying out the cancellations gives the desired factorization.

We now show uniqueness. The number of reduced words of length l in $\alpha_1, \ldots, \overline{\alpha_\sigma}$ is $(p + 1)p^{l-1}$, so the number of different factorizations is

$$8\left(\sum_{0 \leq l < k/2} (p + 1)p^{k-2l-1} + \delta(k)\right)$$

where $\delta(k) = 1$ if k is even and $\delta(k) = 0$ otherwise. We can rewrite this as the geometric sum

$$\begin{aligned} 8\left(\sum_{\substack{0\le m<k\\ m \text{ even}}} (p+1)p^{k-m-1} + \delta(k)\right) &= 8\left(\sum_{0\le m\le k} p^{k-m}\right) \\ &= 8\left(\sum_{0\le m\le k} p^{m}\right) \\ &= 8\,\frac{p^{k+1}-1}{p-1}. \end{aligned}$$

But this is precisely the number of elements of norm p^k as

$$r_4(p^k) = 8\sum_{d|p^k} d = 8(1+p+\cdots+p^k) = 8\,\frac{p^{k+1}-1}{p-1}.$$

This proves uniqueness. □

Note that the elements of $\mathbb{H}_p(\mathbb{Z})$ are in one-to-one correspondence with the integer solutions to

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = p^k.$$

The elements of the form $\beta = \varepsilon R_k(\alpha_1, \ldots, \overline{\alpha_\sigma})$ (without a term p^l) precisely correspond *primitive* solutions, that is those solutions where

$$\gcd(x_1, x_2, x_3, x_4, p) = 1.$$

We now define the *height* of an element of $\mathbb{H}_p(\mathbb{Z})$ to be the reduced word length in the representation given by the lemma.

Now consider the set $\mathbb{H}^*(\mathbb{Z}[\frac{1}{p}])$ quaternions with entries in the ring

$$\mathbb{Z}[\tfrac{1}{p}] = \left\{\frac{a}{b} : b = p^k\right\}$$

which are invertible, and whose inverse is also in $\mathbb{H}^*(\mathbb{Z}[\frac{1}{p}])$. These are exactly the $\alpha \in \mathbb{H}(\mathbb{Z}[\frac{1}{5}])$ with $N(\alpha) = p^k$ for some k. The map

$$\begin{gathered} \mathbb{H}^*\left(\mathbb{Z}[\tfrac{1}{5}] \to \mathrm{SU}(2)\right) \\ \alpha = a_0 + a_1 i + a_2 j + a_3 k \mapsto \frac{1}{\sqrt{N(\alpha)}} \begin{pmatrix} a_0 + a_1 i & a_2 + a_3 i \\ -a_2 + a_3 i & a_0 - a_1 i \end{pmatrix} \end{gathered}$$

is dense, and injective modulo scaling. Now note that the elements of $\mathbb{H}_p(\mathbb{Z})$ correspond to the primitive elements of $\mathbb{H}^*(\mathbb{Z}[\frac{1}{p}])$ with $N(\alpha) \geq 1$. The primitive elements in $\mathbb{H}^*(\mathbb{Z}[\frac{1}{p}])$ with $N(\alpha) \leq 1$ correspond to the inverses of those such elements. The image of S_5 in SU(2) is exactly the set S given above, and the phase factors mentioned are precisely those coming from the units in $\mathbb{H}(\mathbb{Z})$.

By using methods from harmonic analysis and spectral theory, Lubotzky et. al. [LPS86, LPS87] uses a spectral gap to show that

$$\frac{4}{3} \leq \kappa(S) \leq 2.$$

It is also useful to compare with the work of Ghosh et. al. [GGN14]. They consider approximation by points in $\mathbb{Z}[\frac{1}{5}]$ on a homogeneous space which we take to be S^3. These points correspond to solutions of

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = p^{2k}$$

which is almost the same as in our case. As in the case above, they get

$$\frac{4}{3} \leq \kappa \leq 2.$$

However, they also define a *local covering exponent* as follows: Let $x \in S^3$ and $\varepsilon > 0$ be given. Let $t_\varepsilon(x)$ be the smallest t such that $B_{S^3}(x, \varepsilon)$ contains an element of $S^3(\mathbb{Z}[\frac{1}{5}])$ of height at most 5^t. We define the local covering exponent at x in an analogous way by

$$\kappa(x, \mathbb{Z}[\tfrac{1}{5}]) = \limsup_{\varepsilon \to 0} \frac{\log|V_{t_\varepsilon}(x)|}{-\log(\mu(B_\varepsilon))}.$$

Remarkably, they show that for all $x \in S^3$ with respect to the induced Lebesgue measure we have

$$\kappa(x) = 1.$$

In other words, almost all points have optimal approximation properties with elements from $\mathbb{Z}[\frac{1}{5}]$.

§ 7.5 Problems in Diophantine Approximation

The above example illustrates an important point: the question is really one of Diophantine approximation in a suitable variety. While the historical development begins with an algorithm – the continued fraction algorithm,

in this case we begin by a much better understanding of the metric theory. This motivates us to further develop the algorithmic theory, and to try to extend the theory of continued fractions. In particular, we could ask for a solution to the following problems:

(1) Develop a continued fraction algorithm for the (unit) quaternions and the (unit) complex numbers.

(2) Develop a continued fraction algorithm on manifolds/varieties.

(3) Develop the algorithm over not just $\mathbb{Q}$ but also over $\mathbb{Z}[\frac{1}{p}]$.

In the following chapter, we will go into some details on the classical continued fraction algorithm, to see what makes it "tick". We will then try to extend these methods to the unit circle (or equivalently, the unit complex numbers).

Chapter 8

CLASSICAL CONTINUED FRACTIONS

We are going to describe a process for finding rational approximations to a given real number. This process is usually known as the *Continued Fraction Algorithm*, and a plethora of books exist on the subject. For a classical treatment see for example [HW08] and [Khi63]. Our treatment of this process starts from a somewhat different perspective akin to using Farey fractions. In [Niv63] Niven uses the Farey fractions as a simpler alternative to continued fractions, but with some loss of refinements. The point of this chapter, is to show that the two approaches are essentially the same, and to derive the classical theory "backwards", starting with a construction that puts the approximation aspects first.

The author does not claim much originality in this description, as the proofs quickly turn out to be the same. However, it is the author's belief that the theory should start from the most fundamental definitions, which should relate directly to the problem at hand. A grave defect of the classical approach, is that the central approximation aspects are not at all obvious, and appear only after much work.

Before proceeding, it is useful to introduce two notions of "best" rational approximations. If α is a real number, we say that p/q is a (weak) best approximation or a best approximation of the first kind, if every fraction $r/s \neq p/q$ with $s \leq q$ satisfies

$$\left|\alpha - \frac{p}{q}\right| \leq \left|\alpha - \frac{r}{s}\right|.$$

In other words, among all fractions with denominator at most q, the fraction p/q is the one closest to α.

Furthermore, we say that p/q is a strong best approximation or a best approximation of second kind, if every fraction $r/s \neq p/q$ with $s \leq q$ satisfies

$$|q\alpha - p| \leq |s\alpha - r|.$$

It is fairly easy to see that strong best approximations are also weak best approximants. The difference is that strong best approximants are not only the closest approximants, but also the best "value for money". Both are interesting from a practical perspective.

§ 8.1 The Construction

Without loss of generality, we will consider only the problem of approximating positive rationals. We are going to construct an infinite binary tree containing all positive reduced fractions, subject to the following conditions:

(i) For any node in the tree, all children have a greater denominator

(ii) For any node in the tree, all elements to the left are smaller than the node, and all elements to right are larger.

Our construction is known as the Stern-Brocot tree after the German mathematician Moritz Stern and the French clockmaker Achille Brocot. We follow the exposition of Knuth et. al. [GKP94]. We first introduce the mediant, which consists of adding fractions "the easy way":

$$\frac{p}{q} \oplus \frac{r}{s} = \frac{p+r}{q+s}.$$

The mediant has the following elementary property.

Lemma 8.1 *If $0 \leq p/q < r/s$ are two positive fractions, then*

$$\frac{p}{q} < \frac{p+r}{q+s} < \frac{r}{s}.$$

Proof. We prove the first inequality, and leave the second as an exercise to the reader. We have

$$\frac{p}{q} < \frac{p+r}{q+s} \iff (q+s)p < q(p+r) \iff sp < qr \iff \frac{p}{q} < \frac{r}{s}$$

and the lemma follows. □

The Stern-Brocot tree is now constructed inductively as follows: start with the "fractions"

$$\frac{0}{1} \quad \text{and} \quad \frac{1}{0} = \infty.$$

Take the mediant to obtain the first node of the tree: 1/1. Inductively, for each pair of adjacent nodes in the tree, insert the mediant between them. See Figure 8.1.

We need to show that this process includes all positive rationals, and that they are in reduced form. The key to realizing this, is the following technical lemma.

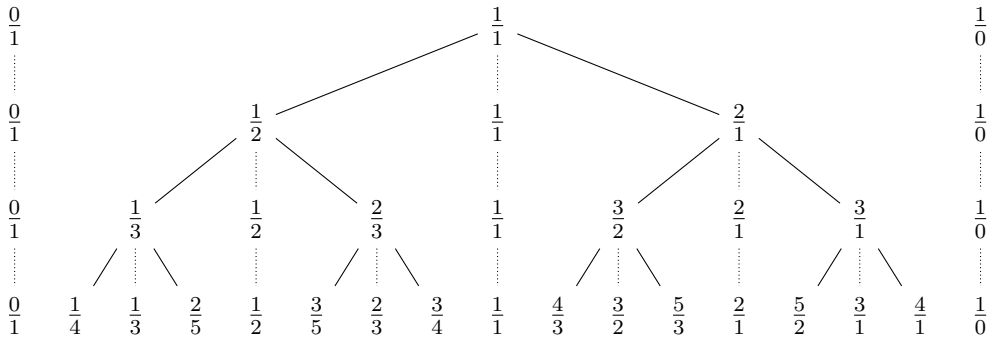


Figure 8.1: The Stern-Brocot Tree

Lemma 8.2 *For any pair of adjacent rationals $p/q < r/s$, we have*

$$qr - sp = 1.$$

Proof. The proof goes by induction in the tree. It is true for the fractions $0/1$ and $1/0$. Now suppose the relation is true at some point in the construction of the tree. Let $p/q < r/s$ be two adjacent fractions in the tree, so that $qr - sp = 1$. The successor to p/q is then $(p + r)/(q + s)$ and we must show

$$1 = q(p + r) - (q + s)p,$$

but this follows directly, since

$$q(p + r) - (q + s)p = qp + qr - qp - ps = qr - ps = 1.$$

Similarly, the successor to $(p + r)/(q + s)$ is r/s so we verify that

$$r(q + s) - s(p + r) = qr - sp = 1. \qquad \square$$

Corollary 8.3 *All fractions in the Stern-Brocot tree are in reduced form.*

Proof. Consider a fraction p/q in the tree and find an adjacent element r/s such that

$$\frac{p}{q} < \frac{r}{s}.$$

By the lemma, we have

$$qr - sp = 1$$

so any common divisor of p and q is also a divisor of 1. $\square$

Proposition 8.4 *All positive fractions appear in the Stern-Brocot tree.*

Proof. Let $a/b > 0$ be some positive fraction. We will show that a/b appears in the tree. Suppose we have

$$\frac{p}{q} < \frac{a}{b} < \frac{r}{s}$$

for two successive fractions $p/q < r/s$ in the tree. It is clear that such exist as we can simply start with $0/1$ and $1/0$.

The algorithm for finding a/b is now the following. Compute the median of p/q and r/s. We have three cases:

(i) If $(p+q)/(r+s) = a/b$ we are done.

(ii) If $(p+q)/(r+s) < a/b$ we replace p/q by the mediant.

(iii) If $(p+q)/(r+s) > a/b$ we replace r/s by the mediant.

We show that this process must eventually stop. The inequalities $p/q < a/b < r/s$ gives

$$qa - bp > 0 \quad \text{and} \quad br - as > 0.$$

Since this is an inequality in integers, we have

$$qa - bp \geq 1 \quad \text{and} \quad br - as \geq 1.$$

Now we find

$$a + b = (r+s)(qa - bp) + (p+q)(br - as) \geq p + q + r + s.$$

At each step of the algorithm, the right hand side must increase by at least one, so we must stop after at most $a + b$ iterations. □

As a corollary, we remark that this gives an alternative proof of the following classical theorem.

Corollary 8.5 (Bezout's identity) *For any pair of positive, coprime integers a and b, the equation*

$$ax + by = 1$$

has an integer solution.

Proof. The fraction a/b is in reduced form, so it is somewhere in the Stern-Brocot tree. Find a successor

$$\frac{a}{b} < \frac{r}{s}$$

then

$$ar - bs = 1$$

is a solution to the equation. □

Finally, we note that the Stern-Brocot tree contains the classical Farey fractions. The Farey fractions of order n is the sequence of reduced fractions between 0 and 1 with denominator less than n. Thus, the first few entries are

$$\begin{aligned}
\mathcal{F}_1 &= \left\{\frac{0}{1}, \frac{1}{1}\right\} \\
\mathcal{F}_2 &= \left\{\frac{0}{1}, \frac{1}{2}, \frac{1}{1}\right\} \\
\mathcal{F}_3 &= \left\{\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}\right\} \\
\mathcal{F}_4 &= \left\{\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}\right\} \\
\mathcal{F}_5 &= \left\{\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}\right\}.
\end{aligned}$$

The Farey fractions can be recovered from the Stern-Brocot tree by considering the subtree to the left of 1 and simply searching.

§ 8.2 Approximations of Real Numbers

A method for finding approximations to a given real number $\alpha > 0$ is now clear: simply search the tree. This will generate all best approximants of the first kind from above and below, i.e. fractions which are best approximations of the first kind if we only consider fractions greater than (resp. smaller than) α. Since the Stern-Brocot tree is constructed from the mediant process which only depends on the two adjacent numbers, finding the n'th best approximant from either above or below can be done in constant space and $O(n)$ arithmetical operations.

A more challenging problem is to find the strong best approximations. For this purpose, we will associate to α the path in the tree starting with 1 and going towards α. We will denote this with R and L for right and left respectively. Thus, we get a sequence

$$R \dots RL \dots LR \dots$$

where introduce the notation $R^n = R \dots R$ (n times) so that we may write the path as

$$R^{a_0} L^{a_1} R^{a_2} L^{a_3} \dots$$

For reasons which will become clear later, we will call this sequence of symbols the *continued fraction* of α.

For example, for Euler's number $e = 2.718\ldots$ we get the continued fraction

$$R^2L^1R^2L^1R^1L^4R^1L^1R^6\ldots$$

We now introduce the *convergents* of a continued fraction. They are the elements in the continued fraction which are closest to the number without crossing it, i.e. the elements just before we change direction when searching the tree. Formally, we may define them as follows.

Definition 8.6 For a given real number $\alpha > 0$, we define the convergents inductively by putting

$$\frac{p_{-1}}{q_{-1}} = \frac{0}{1}, \quad \frac{p_0}{q_0} = \frac{1}{0}$$

and for each $n \geq 0$

$$\frac{p_n}{q_n} = \frac{p_{n-1}}{q_{n-1}} \oplus^{a_n} \frac{p_n}{q_n} = \frac{p_{n-1} + a_n p_n}{q_{n-1} + a_n q_n}.$$

Note that the convergents are less than α when n is even, and greater than α when n is odd.

Proposition 8.7 *We have*

$$q_{n+1}p_n - q_{n+1}p_n = (-1)^n$$

Proof. We prove this by induction. For $n = -1$ we have

$$q_0 p_{-1} - q_{-1}p_0 = 1 \cdot 1 - 0 \cdot 0 = 1.$$

Inductively, we have

$$\begin{aligned} q_{n+1}p_n - q_n p_{n+1} &= (a_n q_n + q_{n-1})p_n - q_n(a_n p_n + p_{n-1}) \\ &= q_{n-1}p_n - q_n p_{n-1} = -(-1)^{n-1} = (-1)^n. \end{aligned}$$ □

Corollary 8.8 *The convergents satisfy*

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n q_{n+1}} \leq \frac{1}{q_n^2}.$$

Proof. The convergents are alternatively greater than and less than α and we have

$$\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} = \frac{(-1)^n}{q_n q_{n+1}}$$

so

$$\left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| = \frac{1}{q_n q_{n+1}} \leq \frac{1}{q_n^2}$$

and the statement follows. □

Theorem 8.9 *The convergents p_n/q_n for $n \geq 2$ of a real number $\alpha > 0$ are strong best approximants.*

Proof. Let $p/q \neq p_n/q_n$ be some fraction with $1 \leq q \leq q_n$. We must show that

$$|p_n - q_n\alpha| < |p - q\alpha|.$$

Without loss of generality, suppose that $\gcd(p, q) = 1$. The statement is clear if $q = q_n$, since then $|p_n/q_n - p/q| > 1/q_n$ and Corollary 8.8 gives that p_n/q_n is a better approximation.

Suppose that $q_{n-1} < q < q_n$. By Proposition 8.7 we may solve the equation

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} p \\ q \end{pmatrix}$$

in non-zero integers s, t. Note that $q = sq_n + tq_{n-1}$ so that $\operatorname{sign}(s) = -\operatorname{sign}(t)$ and $\operatorname{sign}(p_n - q_n\alpha) = -\operatorname{sign}(p_{n-1} - q_{n-1}\alpha)$ so that

$$\operatorname{sign}(s(p_n - q_n\alpha)) = \operatorname{sign}(t(p_{n-1} - q_{n-1}\alpha)).$$

Thus,

$$|p - q\alpha| = |s(p_n - q_n\alpha) + t(p_{n-1} - q_{n-1}\alpha)| \geq |p_{n-1} - q_{n-1}\alpha| > |p_n - q_n\alpha|.$$

Which was what we wanted. □

Theorem 8.10 *All strong best approximants of a real number $\alpha > 0$ appear as convergents.*

Proof. Let p/q be a strong best approximant to α. Observe that p/q must lie on the path of the continued fraction, since otherwise we have taken a wrong turn in the binary tree, and we can get a better approximation with a simpler fraction by backtracking.

Thus, there must exist two convergents p_{n-1}/q_{n_1} and p_{n+1}/q_{n+1} such that

$$\frac{p_{n-1}}{q_{n-1}} \leq \frac{p}{q} \leq \frac{p_{n+1}}{q_{n+1}}.$$

If p/q is equal to either of endpoints, we are done, so suppose the inequality is sharp. We now have,

$$\left|\frac{p}{q} - \frac{p_{n-1}}{q_{n-1}}\right| \geq \frac{1}{qq_{n-1}}$$

and

$$\left|\frac{p}{q} - \frac{p_{n-1}}{q_{n-1}}\right| \leq \left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| = \frac{1}{q_n q_{n-1}}$$

so $q > q_0$.

On the other hand,

$$\left|\alpha - \frac{p}{q}\right| \geq \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p}{q}\right| \geq \frac{1}{q q_{n+1}}$$

so

$$|qx - p| \geq \frac{1}{q_{n+1}}.$$

But now we have

$$|q_n\alpha - p_n| \leq \frac{1}{q_{n+1}} \leq |q\alpha - p|$$

which contradicts the fact that p/q is a strong best approximant. □

We may now formulate an efficient algorithm for finding the best approximants of a given real number. This is equivalent to computing the convergents, which we may do by finding the continued fraction. For some convergents with say,

$$\frac{p_{n-1}}{q_{n-1}} < \alpha < \frac{p_n}{q_n}$$

we may compute a_n as the largest number N such that

$$\frac{p_{n-1} + Np_n}{q_{n-1} + Nq_n} < \alpha,$$

but solving this is easy. Similarly for the case where

$$\frac{p_n}{q_n} < \alpha < \frac{p_{n-1}}{q_{n-1}}.$$

Thus, the n'th convergents of a real number $\alpha > 0$ may be computed in space equivalent to two integers and $O(n)$ arithmetical operations. This is very efficient indeed!

§ 8.3 A Geometric Approach

The observant reader will have noticed, that in this construction we never used the arithmetical properties of the fractions and only treated a fraction as a pair of numbers. It is natural to make this construction formal, by

considering the process in $\mathbb{R}^2$. Here, the mediant simply becomes vector addition.

Let $\alpha > 0$ be some real number. Start by drawing the line $y = \alpha x$ and define the vectors

$$e_{-1} = (1, 0)$$
$$e_0 = (0, 1).$$

Inductively, we define e_{i+1} by

$$e_{i+1} = e_{i-1} + a_i e_i$$

where a_i is taken to be the largest integer such that the sum does not cross the line y. This is precisely the same definition as in the case of the tree. This is illustrated in Figure 8.2. In this description, the crucial technicality of lemma 8.2 also gains a nice geometric interpretation: It states that the determinant of (e_{k+1}, e_k) is $(-1)^k$.

Another way of generating these vectors, is to take an infinite string fixed at the end of the line and pulling down (resp. up) until it is straight. The extremal points of this convex hull are precisely the convergents. This method is what Arnol'd calls "the algorithm of stretching the noses" [Arn88].

It is worth noting that this process works not only for the lattice $\mathbb{Z}^2$ but also for any sublattice of $\mathbb{Z}^2$. With this observation, we see that this process gives an efficient algorithm for Diophantine approximation by elements of $\mathbb{Z}[1/p]$. Of course, we already have a simpler algorithm for this: write up the base-p expansion of the number and truncate.

§ 8.4 The Classical Definition

The standard definition of the continued fraction is quite different from what we have described here, and we briefly recall it. Given a real number α we may put

$$\alpha = \lfloor \alpha \rfloor + \{\alpha\}$$

where $\lfloor \alpha \rfloor$ is the largest integer less than α and $\{\alpha\}$ is the remainder, called the fractional part of α. We define $a_0 = \lfloor \alpha \rfloor$ and get

$$\begin{aligned} \alpha &= a_0 + \{\alpha\} \\ &= a_0 + \frac{1}{\frac{1}{\{\alpha\}}}. \end{aligned}$$

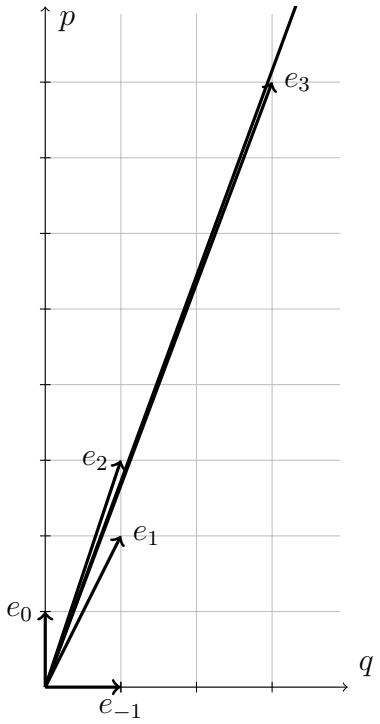


Figure 8.2: Geometric Continued Fraction of e.

By iterating this process on $1/\{\alpha\}$ we get an infinite sequence

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots}}$$

which turns out to have the property that the convergents are given by

$$\frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}.$$

This should explain why the process is known as the *continued fraction algorithm*.

Since this notation for continued fractions is rather cumbersome, we often write

$$\alpha = [a_0; a_1, a_2, \dots].$$

§ 8.5 What Are Continued Fractions?

On a slightly philosophical level, we might then ask, what is a continued fraction? In the classical case of approximation of the reals by rationals, all these are answers are the same, but that is not so when we try to generalize. We review some of the work done in order to extend continued fractions to higher dimensions.

One approach, which is quite close to the old definition from which the process derives its name, is to consider the *Gauss map* on the unit interval:

$$\begin{aligned} T :&[0,1] \to [0,1] \\ &x \mapsto \left\{\frac{1}{x}\right\}. \end{aligned}$$

With this map, the elements of the continued fraction are given as the integers parts of successive iterations of T.

One aspect, that becomes very clear from this point of view, is the periodicity. We can classify the rational numbers as those for which $T^n(x) = 0$ from some point on and Lagrange's theorem states that a number is a quadratic irrational if and only if there is some number p such that $T^{n+p}(x) = T^n(x)$ for sufficiently large n. Another very nice aspect is that the Gauss map turns out to be ergodic with respect to a certain measure. This allows us to derive statistical properties on the distribution of the entries in the continued fraction. This viewpoint is taken by Schweiger [Sch00], who generalize continued fractions to be (essentially) fractional linear transformations of the unit interval. Unfortunately, these algorithms fail to exhibit good convergence properties.

Another approach is to try to generalize the geometric viewpoint. This was originally done by Klein, but was abandoned due to the computational complexity. This has recently been taken up again, primarily by Russian mathematicians as the theory of sails. A comprehensive treatment of this idea is given by Karpenkov [Kar13] who describes this in terms of a synthetic geometry called *integer geometry*, which is created in analogy with the Euclidean geometry.

The book of Brentjes [Bre81] is a quite comprehensive survey of most continued fraction algorithms. The definition taken here is essentially based on the recursion formula. In this book, good algorithms from the point of view of Diophantine approximation are constructed in two dimensions.

Finally, one could take the Farey sequence (which as discussed above, is essentially the same as the Stern-Brocot tree). This approach is taken by A. Schmidt [Sch69], [Sch67] by generalizing the Farey sections to the quadratic fields $\mathbb{Q}(i\sqrt{m})$ for $m = 1, 2, 3, 7$ as well as the quaternions. This approach

yields good (if not necessarily efficient) approximation and in the paper this is used to obtain information on the spectrum of optimal approximation constants.

Chapter 9

CONTINUED FRACTIONS ON THE CIRCLE

In this section we consider the problem of constructing a continued fraction algorithm on the unit circle. In order to do this, we describe an analogue of the Stern-Brocot tree on the circle. Unfortunately, the non-linear circle turns out to be much more complicated, and we are unable to construct an efficient algorithm.

§ 9.1 The Rational Case

Consider the unit circle

$$\mathbb{S}^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}.$$

The stereographic projection to the real line puts the rational points on the circle in one-to-one correspondence with the rational numbers, so the set of rational numbers is dense on the unit circle and the question of Diophantine approximation makes sense.

Our first problem is to list all the fractions in a reduced form. Multiplying through by a common denominator, the rational points correspond to integral solution of the Pythagorean equation

$$x^2 + y^2 = z^2.$$

These are also known as *Pythagorean triples*. The classical way of generating all primitive triples (that is, triples with $\gcd(x, y, z) = 1$) is by Euclid's formula: if $m > n > 0$ positive integers coprime integers, which are not both odd, then

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2$$

is a primitive Pythagorean triple. Furthermore, up to interchanging x and y, all positive primitive triples are generated in this way. Note that this procedure does not guarantee $x < y < z$.

We would like to generate an analogue of the Stern-Brocot tree for the circle, and in order to do that, we would like to sort the triples by z. The primitive Pythagorean triples with $z < 100$ sorted by their z-value are the following:

(3, 4, 5)	(5, 12, 13)	(8, 15, 17)	(7, 24, 25)
(20, 21, 29)	(12, 35, 37)	(9, 40, 41)	(28, 45, 53)
(11, 60, 61)	(16, 63, 65)	(33, 56, 65)	(48, 55, 73)
(13, 84, 85)	(36, 77, 85)	(39, 80, 89)	(65, 72, 97).

Or alternatively in terms of the generating pair (m, n):

(2, 1)	(3, 2)	(4, 1)	(4, 3)
(5, 2)	(6, 1)	(5, 4)	(7, 2)
(6, 5)	(8, 1)	(7, 4)	(8, 3)
(7, 6)	(9, 2)	(8, 5)	(9, 4).

The author is not aware of, and has not been able to find, any structure in these pairs that would allow us to effectively compute the next entry. To generate the above, we used brute-force: compute all Pythagorean triples given by pairs (m, n) where $m < \sqrt{100}$ and sort them.

For the problem of approximating points on the circle it's useful to realize that we only need to consider the points in the first quadrant, as the other points are analogous up to choosing a sign. Furthermore, we have mirror symmetry around the angle $\pi/4$ by interchanging the x- and y-coordinates, so it suffices to consider the points (x, y) with $x < y$. For these points the analogue of the Stern-Brocot tree for the circle is given by Figure 9.1. In Figure 9.1 we give the same tree in terms of the generators of the associated Pythagorean triple.

As in the classical case, we might define the continued fraction to be the sequence in L and R of the path to our given point. In order to construct a good continued fraction algorithm, we would like to compute the next element in the tree using only finitely many of the previous elements. The trees below were again generated by brute force.

§ 9.2 The Case of Restricted Rationals

We now consider the problem of approximation on the unit circle by elements of $\mathbb{Z}[\frac{1}{p}]$. These correspond to solutions of

$$x^2 + y^2 = p^{2k}.$$

To be more concrete, we just consider the case $p = 5$.

To begin with, it is not even clear that there are infinitely many such rational points and if there are, that these points are dense. A clever trick, however, is to realize that we know one solution, namely

$$3^2 + 4^2 = 5^2.$$

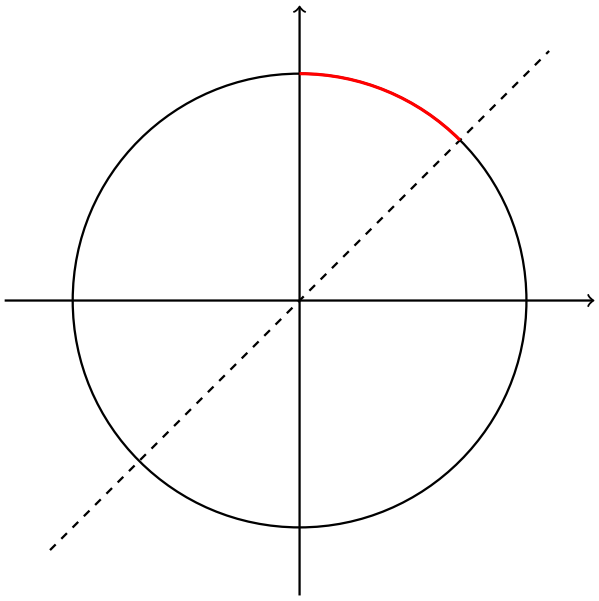


Figure 9.1: The octant of the circle which we consider.

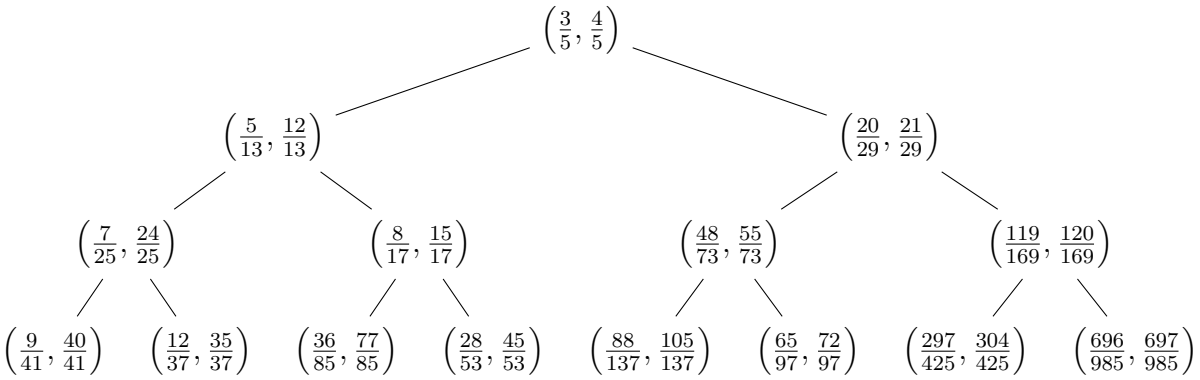


Figure 9.2: The Stern-Brocot tree on the circle.

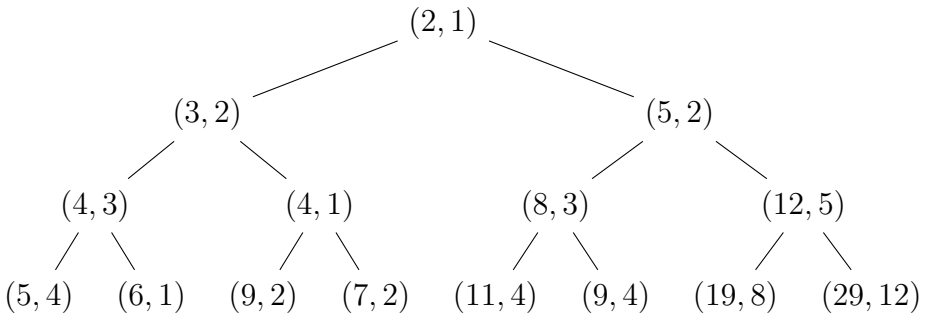


Figure 9.3: The Stern-Brocot on the circle in terms of generators of the Pythagorean triple.

In the complex plane this corresponds to $z = (3 + 4i)/5$ with $|z| = 1$. Note that z^n gives rise to a new solution for all integers n. Now, the argument of z is $\theta = \arccos(3/5)$ which is rationally independent on π, so the orbit of $\{z^n\}_{n=1}^{\infty}$ is dense in the unit circle. To see why θ is rationally independent on π, suppose to the contrary that

$$\theta = \frac{m}{m}\pi$$

so that $\cos(n\theta) = \pm 1$. Write $cos(n\theta) = T_n(\cos(\theta)) = T_n(3/5)$ where T_n is the n'th Chebyshev polynomial. The Chebyshev polynomial is an integer polynomial of the form

$$T_n(x) = 2^{n-1}x^n + O(x^{n-1}).$$

Plugging in our values we get

$$\pm 1 = T_n(3/5) = 2^{n-1}\left(\frac{3}{5}\right)^n + A_n/5^{n-1}$$

where $A_n \in \mathbb{Z}$ is some integer. Multiplying by 5^n and moving around we get

$$\pm 5(5^{n-1} - A_n) = 2^{n-1}3^n$$

which is clearly impossible.

Having shown that the question makes sense, we turn to the same question as before: Generating all the Pythagorean triples satisfying

$$x^2 + y^2 = p^{2k}$$

and putting them in the suitable tree. We begin with the problem of generating the associated Pythagorean triples. Generating all the Pythagorean

triples and filtering those where z is a power of p is very slow. A better approach is to fix $z = p^k$ and search through the possible generating pairs (m, n) of which the ones we need to try are those with $1 \leq n < \sqrt{(z)}$ and $m = \sqrt{(z - n^2)}$ which takes $O(p^k)$ time – extremely slow. Still, by a brute force process, we can write down the first entries in the Stern-Brocot tree here. This is done in Figure 9.2.

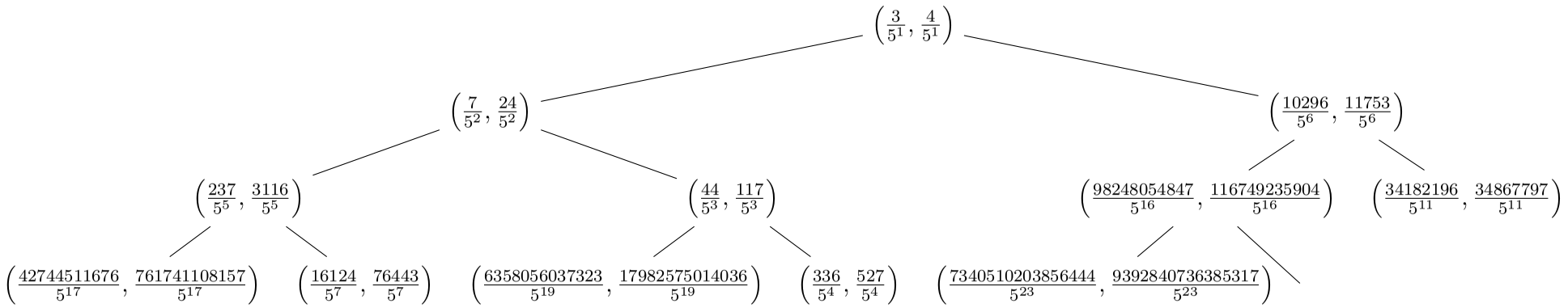


Figure 9.4: Stern-Brocot tree for $\mathbb{Z}[\frac{1}{5}]$ on the circle.

Part III

Experimental Mathematics

Chapter 10

ON A CONJECTURE RELATED TO PISOT NUMBERS

In this chapter, we describe an unsuccessful attempt at producing transcendental analogues of Pisot numbers through the use of finite automata. This is joint work with Simon Kristensen.

§ 10.1 Pisot Numbers

Let $\alpha \in (1, \infty)$. We consider the problem of how the sequence $(\{\alpha^n\})_{n=1}^{\infty}$ is the distributed modulo one. Here $\{\cdot\}$ denotes the fractional part, and we will let $\|\cdot\|_{\mathbb{Z}}$ denote the distance to the nearest integer. A very comprehensive survey of this problem is available in [Bug12].

A first step is the well-known result of Koksma that for almost all (in the sense of Lebesgue measure) $\alpha > 1$, the sequence $(\{\alpha^n\})_{n=1}^{\infty}$ is uniformly distributed modulo 1. Thus, the problem is almost solved. What remains, is to determine what kind of exceptional behavior we can get in a nullset.

Now suppose that $\alpha > 1$ is a *Pisot number*, that is, an algebraic integer whose Galois conjugates have norm strictly less than 1. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$ denote the Galois conjugates with associated embeddings $\sigma_1, \ldots, \sigma_d : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$. Recall that the trace of an algebraic integer

$$\mathrm{Tr}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_d(\alpha)$$

is a rational integer. In particular, since α^n is an algebraic integer for all $n \in \mathbb{N}$ we have $\mathrm{Tr}(\alpha^n) \in \mathbb{Z}$. We have the estimate

$$\begin{aligned} \|\alpha^n\|_{\mathbb{Z}} &\leq |\alpha^n - \mathrm{Tr}(\alpha^n)| \\ &= |\alpha_2^n + \alpha_3^n + \cdots + \alpha_d^n| \\ &\leq |\alpha_2^n| + \cdots + |\alpha_d^n| \end{aligned}$$

so since $|\alpha_2|, \ldots, |\alpha_d| < 1$ we find that $\|\alpha^n\|_{\mathbb{Z}} \to 0$ as $n \to \infty$.

Conversely, we have the following theorem due to Hardy and Pisot.

Theorem 10.1 *If $\alpha > 1$ is algebraic and*

$$\|\alpha^n\|_{\mathbb{Z}} \to 0, \quad n \to \infty$$

then α is a Pisot number.

This naturally leads to the following problem: Are there any transcendental numbers $\alpha > 1$ such that $\|\alpha^n\|_{\mathbb{Z}} \to 0$?

This question is currently out of reach. On the one hand, such transcendental numbers, if they exist, must be sparse. In fact, it can be shown that there are only countably many $\alpha > 1$ satisfying $\|\alpha^n\|_{\mathbb{Z}} \to 0$ as $n \to \infty$. On the other hand, there is no particular reason to expect algebraic numbers to be special in this regard. Furthermore, some "almost counterexamples" are abundant: Baker [Bak14] has shown that if n_k grows sufficiently rapidly, the numbers satisfying $\lim_{k\to\infty}\|\alpha^{n_k}\|_{\mathbb{Z}}$ is dense in the real line, and has Hausdorff dimension 1.

The problem in attempting to explicitly construct such numbers, is that we need to construct transcendental numbers whose Diophantine properties are well-understood. In practice, this means constructing transcendental numbers whose continued fraction expansion is known. In general, such numbers are hard to construct as the continued fraction expansion only allow us to classify fractions (finite continued fractions) and quadratic irrationals (ultimately periodic continued fractions).

Our approach to constructing transcendental numbers whose Diophantine properties are known, is through the recent work of Bugeaud [Bug13]: if $\{a_n\}$ is the continued fraction of an algebraic number, and $\{a_n\}$ is not ultimately periodic, then the complexity of the sequence is high. Thus, if we generate a simple sequence of numbers (a_n) which is not ultimately periodic, then $x = [a_0, a_1, \dots]$ is transcendental.

§ 10.2 Automatic Sequences

Before proceeding, we review the basics of finite automata and automatic sequences. The standard reference is [AS03].

We will need some notation. An alphabet Σ is a finite set, the elements are called letters. A *word* over an alphabet, is some concatenation of letters or the empty word. The set of all words is called the language over Σ and is denoted Σ^*.

A *deterministic finite automaton* (DFA) is a very simple model for a computer which takes a word over some alphabet Σ and return accepted or rejected to any input. Formally, we may define a DFA as a 5-tuple

$$M = (Q, \Sigma, \delta, q_0, F)$$

where Q is a finite set of states, Σ is an input alphabet, $\delta : Q \times \Sigma \to Q$ a transition function, $q_0 \in Q$ is the initial state and $F \subset Q$ is the set of accepted states. The process for determining whether some input is accepted

or rejected works like this: we start at the state q_0 and read the first letter of our input word l, then follow the transition function to get a new state $\delta(q_0, l)$ and continue. If the final state is in F, we accept the word, otherwise we reject it.

As an example, a DFA which accepts the words in $\{0,1\}^*$ with a positive even number of 1's is illustrated in Figure 10.2. The states are represented as nodes of the graph, with arrows for the transition function. The accepting states are denoted by double lines.

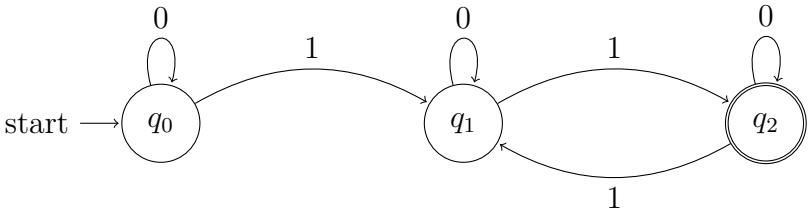


Figure 10.1: Example of a DFA.

In this way, we may think of a DFA as a function

$$f_M : \Sigma^* \to \{\text{accept}, \text{reject}\}.$$

An extension of this line of thought, is that rather than just outputting a binary value, we can output an arbitrary value of some output alphabet Δ. We call such an automaton a *deterministic finite automaton with output* (DFAO). Formally, we define a DFAO as a 6-tuple

$$M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$$

where Q, Σ, δ, q_0 are as in the definition of a DFA, and $\tau : Q \to \Delta$ is a function which takes a state and gives a number.

Now take the input alphabet to be

$$\Sigma = \Sigma_k = \{0, 1, 2, \ldots, k-1\}.$$

For each n denote by $[n]_k$ the base-k representation of the number. For a DFAO M on Σ_k we have an associated sequence given by $\{f_m([n]_k)\}_{n=0}^{\infty}$. We call a sequence *$k$-automatic* if it is generated by a DFAO in this way. A sequence is called *automatic* if it is k-automatic for some k.

The prototypical automatic sequence is the *Thue-Morse sequence* $\{t_n\}_{n=0}^{\infty}$ which counts the number of 1's in the base-2 representation of n. The first few terms are

$$\{t_n\}_{n=0}^{\infty} = \{0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, \ldots\}.$$

A graphical representation of the DFAO which generates the Thue-Morse sequence is given in figure 10.2.

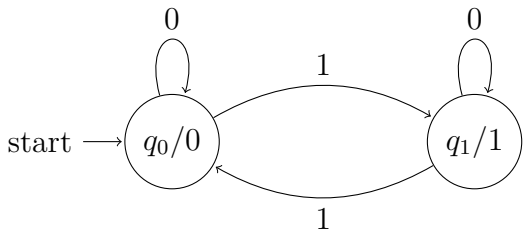


Figure 10.2: A finite automaton generating the Thue-Morse sequence

§ 10.3 Complexity of Words and Diophantine Approximation

Let $\boldsymbol{w} = \{w_n\}$ be some infinite word on an alphabet Σ. A natural measure of the complexity of the word, is the *block complexity* $p(n, \boldsymbol{w})$ which measures the number of distinct blocks of n successive letters in w. That is,

$$p(n, w) = |\{w_k w_{k+1} \cdots w_{k+n-1} : k \geq 1\}|.$$

It is easily seen the block complexity of an ultimately periodic word is bounded by some constant. Furthermore, it was shown by Cobham [Cob72, Theorem 2] that if the sequence $\boldsymbol{w} = \{w_n\}$ is automatic, then $p(n, \boldsymbol{w}) = O(n)$.

Now let $\boldsymbol{a} = \{a_n\}$ be a sequence of natural numbers, and consider the number

$$\begin{aligned} \alpha &\coloneqq [0; a_1, \dots] \\ &= \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots}}. \end{aligned}$$

Bugeaud has shown [Bug13, Theorem 1.1] that if $\boldsymbol{a}$ is not ultimately periodic and α is algebraic, then

$$\lim_{n \to \infty} \frac{p(n, \boldsymbol{a})}{n} = \infty.$$

This gives us a method for constructing transcendental numbers: If $\{a_n\} \subset \mathbb{N}$ is an automatic sequence which is not ultimately periodic then

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots}}$$

cannot be algebraic, and is hence transcendental.

§ 10.4 A Computer Search

Our approach to finding possible counterexamples of this form, was to do a computer search. For this purpose we used SageMath[1] software package. We chose Sage for several reasons. The most important reason, is that is allows us to use mathematical objects as if they were infinite by using lazy evaluation where only the terms requested are computed. Coupling this with built-in support for interval arithmetic, means that we can compute with real numbers given in various ways as if they were mathematical objects, and let the computer dynamically increase the number of digits used for computation behind the scenes. The downside of this is that it is very hard to reason about the complexity of the computation. Finally, Sage has library support for both continued fractions and finite automata, so we did not need to implement these ourselves.

The program works as follows. Start by generating a list of output labels for the DFAO, for example $[1, 2, 3, 4]$. Next, we generate all possible binary transition functions for DFA's starting in 1. For each of these, we generate the infinite word associated with the DFAO and use this to construct the associated continued fraction. Both are of course implemented as lazy objects. We check that the continued fraction is not ultimately periodic by the heuristic that it is ultimately periodic if after the first 35 entries, there exists a range of 25 letters for which we get the same subsequence by translating with a period between 1 and 10. This is very crude, but seems good enough for our purposes.

Finally, we need to figure out if the number α generated by the continued fraction satisfies $\{\alpha^n\} \to 0$ as $n \to \infty$. To do this, we compute the continued fraction of α^n. There are essentially two ways to do this. We first considered using the continued fraction arithmetic of Gosper [BGS72, Gos] which is further described in [LS98], however this was abandoned due to being fairly complex to implement and with unclear improvements. Instead we chose

[1] `http://www.sagemath.org`

the use interval arithmetic to compute the numbers α^n and compute their continued fractions by brute force. Here, it is important that α is not a quadratic irrational, and in particular that α^n is not rational, as it is impossible to conclude that α^n is rational from the interval approximations and the computation would result in an infinite loop of repeating with higher and higher precision.

Once the continued fraction has been computed, we need a criterion for deciding if $\{\alpha^n\}$ is close to 0. In terms of the continued fraction, there are two ways this can happen. Write

$$\alpha^n = a_{0,n} + \cfrac{1}{a_{1,n} + \cfrac{1}{a_{2,n} + \dots}}.$$

If $a_{1,n}$ is large, then α^n is close to $a_{0,n}$ from above. If $a_{1,n} = 1$ and $a_{2,n}$ is large, then α^n is very close $a_{0,n} + 1$ from below. To keep track of this, we associated a number $c(\alpha^n)$ by

$$c(\alpha^n) = \begin{cases} a_{1,n} & \text{if } a_{1,n} > 1 \\ a_{2,n} & \text{if } a_{1,n} = 1. \end{cases}$$

We now formulated the heuristic for $\{\alpha^n\} \to 0$ as $n \to \infty$, that for $n > 50$ we had $c(\alpha^n) > 3$.

Unfortunately, the only numbers we found with $\|\alpha^n\|_{\mathbb{Z}} \to 0$ were quadratic irrationals.

SAGE CODE

```
import itertools
cf = continued_fraction

class InfiniteLoopException(Exception):
    """ Exception to cast in case of possibly infinite loops."""
    def __init__(self, message, object):
        super(Exception, self).__init__(message)
        self.object = object

def cc(x):
    """For x > 1, compute the coefficient which should tend to infinity."""
    y = cf(x)
    if y[1] == 1:
        return y[2]
    return y[1]

def likely_increasing(mylist):
    """Return true if liminf of the list seems to tend to infinity,
    list must be at least 50 long."""

    return min(mylist[50:]) > 4

def mylabel(T):
    """ Proper labels for edges of transitions """
    return str(T.word_in[0])

def generator_automatons(N):
    """
    Genrator yielding all our chosen automatons with N states.
    """

    states = list(range(1,N+1))
    alphabet = [0,1]

    transition_functions = []
    for outputs in itertools.product(states, repeat=2*N):
        q = iter(outputs)
        transition_functions.append([(p,q.next(), a)
                                     for p in states
                                     for a in alphabet])

```

```
42      for transition in transition_functions:
43          tm = Automaton(transition,
44                         initial_states=[1],
45                         final_states=states,
46                         input_alphabet=alphabet
47          )
48
49          yield tm
50
51  def dfa_word(dfa, tau):
52      """Output the automatic word generated by the DFA.
53
54      Input: DFA with states labelled by integers with transitions for
55      {0,1}.
56
57      Output: Automatic word of Integers, given by the tau(label).
58      """
59      def word_gen(dfa):
60          # Generator processing each integer in turn
61          i = Integer(0)
62          while True:
63              # process the digits in reverse order
64              # Stop processing if we seem to be reaching an endless loop
65              if i > 1000:
66                  raise InfiniteLoopException("Maximum generation depth reached
    (i > 1000)", dfa)
67              out = dfa.process(i.digits(base=2)[::-1])
68
69              i += Integer(1)
70              # out contains (True, end_state), since all states are
71              # accepted, we discard unnessecary info.  Result is of
72              # type FSMState, label is of type 'int', so we turn it
73              # into a sage.rings.integer.Integer object.
74              yield tau[Integer(out[1].label())]
75
76      g = word_gen(dfa)
77      w = Word(g, length=Infinity)
78      return w
79
80  def likely_ultimately_periodic(w, max_period=10):
81      if w.is_finite():
82          return True
83
84      w = w[:1000]
85
86      offset = 35
87      test_range = 25
88
89      for p in range(1, max_period+1):
```

```
90          if w[offset:offset + test_range] == w[offset + p:offset + p +
    test_range]:
91              return True
92
93      return False
94
95  def find_likely_increasing(output_labels):
96      """ Find likely increasing sequences in automatic words
97
98      INPUT: A list of output labels.
99      """
100
101     n = len(output_labels)
102
103     # Create the tau function for the DFAO
104     states = [k for k in range(1, n+1)]
105     tau = dict(zip(states, output_labels))
106
107     count = 0
108     hits = 0          # count of number of possible candidates
109     discarded = 0     # count of quadratic irrationals, which we discard
110
111     generator = generator_automatons(n)
112     for dfa in generator:
113         count += 1
114
115         if not dfa.digraph().is_strongly_connected():
116             # Only strongly connected components are really interresting
117             continue
118
119         try:
120             w = dfa_word(dfa, tau)
121         except InfiniteLoopException as exception:
122             print "Skipping due to infinite loop. This should not happen!"
123             debug_information.append(dfa)
124             discarded += 1
125
126         if likely_ultimately_periodic(w):
127             discarded += 1
128             continue
129
130         x = continued_fraction(w)
131         v = x.value()
132
133         coefficients = []
134         for k in range(100):
135             coefficients.append(cc(v^k))
136
137         if likely_increasing(coefficients):
```

```
            print("Found candidate:", w)
            hits += 1
            candidates.append(dfa)

    print "Results for:", output_labels
    print "\tTried", count, "automatic sequences"
    print "\tDiscarded", discarded, "quadratic irrationals"
    print "\tFound", hits, "candidates"

if __name__ == "__main__":
    outputs = [[1,2],
               [2,3],
               [3,4],
               [1,2,3],
               [1,2,2],
               [2,3,4],
               [2,3,3],
               [2,4,5],
               [2,4,7],
               [1,1,2],
               [1,2,3,4],
               [2,2,3,4]
               ]

    print "Starting search..."

    error = Exception()

    candidates = []
    debug_information = []      # used when raising exceptions

    for x in outputs:
        for y in itertools.permutations(x):
            try:
                find_likely_increasing(list(y))
            except Exception as e:
                print("serious error.")
                error = e
```

BIBLIOGRAPHY

[Arn88] V. I. Arnold. *Geometrical methods in the theory of ordinary differential equations*, volume 250 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, second edition, 1988. Translated from the Russian by Joseph Szücs [József M. Szűcs].

[AS03] Jean-Paul Allouche and Jeffrey Shallit. *Automatic sequences*. Cambridge University Press, Cambridge, 2003. Theory, applications, generalizations.

[Bak14] Simon Baker. On the distribution of powers of real numbers modulo 1, 2014, arXiv:1411.4817.

[BDL10] Natalia Budarina, Detta Dickinson, and Jason Levesley. Simultaneous Diophantine approximation on polynomial curves. *Mathematika. A Journal of Pure and Applied Mathematics*, 56(1):77–85, 2010.

[BDV06] Victor Beresnevich, Detta Dickinson, and Sanju Velani. Measure theoretic laws for lim sup sets. *Memoirs of the American Mathematical Society*, 179(846):x–91, 2006.

[Ber12] Victor Beresnevich. Rational points near manifolds and metric Diophantine approximation. *Ann. of Math. (2)*, 175(1):187–235, 2012.

[BGS72] Michael Beeler, R. William Gosper, and Richard Schroeppel. *Hakmem*, chapter Continued Fractions. MIT, 1972. Digital version available at `http://home.pipeline.com/~hbaker1/hakmem/hakmem.html`.

[Bre81] A. J. Brentjes. *Multidimensional continued fraction algorithms*, volume 145 of *Mathematical Centre Tracts*. Mathematisch Centrum, Amsterdam, 1981.

[Bug12] Yann Bugeaud. *Distribution modulo one and Diophantine approximation*, volume 193 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2012.

[Bug13] Yann Bugeaud. Automatic continued fractions are transcendental or quadratic. *Ann. Sci. Éc. Norm. Supér. (4)*, 46(6):1005–1022, 2013.

[BV06] Victor Beresnevich and Sanju Velani. A mass transference principle and the Duffin-Schaeffer conjecture for Hausdorff measures. *Ann. of Math. (2)*, 164(3):971–992, 2006.

[Cas97] J. W. S. Cassels. *An introduction to the geometry of numbers*. Classics in Mathematics. Springer-Verlag, Berlin, 1997. Corrected reprint of the 1971 edition.

[Cob72] Alan Cobham. Uniform tag sequences. *Math. Systems Theory*, 6:164–192, 1972.

[DD01] H. Dickinson and M. M. Dodson. Simultaneous Diophantine approximation on the circle and Hausdorff dimension. *Math. Proc. Cambridge Philos. Soc.*, 130(3):515–522, 2001.

[Dic22] L. E. Dickson. Arithmetic of Quaternions. *Proc. London Math. Soc.*, S2-20(1):225, 1922.

[DK04] M. Maurice Dodson and Simon Kristensen. Hausdorff dimension and Diophantine approximation. In *Fractal geometry and applications: a jubilee of Benoît Mandelbrot. Part 1*, volume 72 of *Proc. Sympos. Pure Math.*, pages 305–347. Amer. Math. Soc., Providence, RI, 2004.

[DM99] Edward Dunne and Mark McConnell. Pianos and continued fractions. *Math. Mag.*, 72(2):104–115, 1999.

[DN06] Christopher M. Dawson and Michael A. Nielsen. The Solovay-Kitaev algorithm. *Quantum Inf. Comput.*, 6(1):81–95, 2006.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[Fal03] Kenneth Falconer. *Fractal geometry*. John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2003. Mathematical foundations and applications.

[FKMS14] Lior Fishman, Dmitry Kleinbock, Keith Merrill, and David Simmons. Intrinsic diophantine approximation on quadric hypersurfaces, 2014, arXiv: 1405:7650v4.

[GGN14] Anish Ghosh, Alexander Gorodnik, and Amos Nevo. Metric Diophantine approximation on homogeneous varieties. *Compos. Math.*, 150(8):1435–1456, 2014.

[GKP94] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete mathematics*. Addison-Wesley Publishing Company, Reading, MA, second edition, 1994. A foundation for computer science.

[GN15] Alexander Gorodnik and Amos Nevo. Quantitative ergodic theorems and their number-theoretic applications. *Bull. Amer. Math. Soc. (N.S.)*, 52(1):65–113, 2015.

[Gos] Ralph William Gosper. Continued fraction arithmetic. http://perl.plover.com/yak/cftalk/INFO/gosper.txt.

[HS00] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[HW08] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.

[Kar13] Oleg Karpenkov. *Geometry of continued fractions*, volume 26 of *Algorithms and Computation in Mathematics*. Springer, Heidelberg, 2013.

[Khi63] A. Ya. Khintchine. *Continued fractions*. Translated by Peter Wynn. P. Noordhoff, Ltd., Groningen, 1963.

[KM98] D. Y. Kleinbock and G. A. Margulis. Flows on homogeneous spaces and Diophantine approximation on manifolds. *Ann. of Math. (2)*, 148(1):339–360, 1998.

[KM15] Dmitry Kleinbock and Keith Merrill. Rational approximation on spheres. *Israel J. Math.*, 209(1):293–322, 2015.

[LPS86] A. Lubotzky, R. Phillips, and P. Sarnak. Hecke operators and distributing points on the sphere. I. *Comm. Pure Appl. Math.*, 39(S, suppl.):S149–S186, 1986. Frontiers of the mathematical sciences: 1985 (New York, 1985).

[LPS87] A. Lubotzky, R. Phillips, and P. Sarnak. Hecke operators and distributing points on S^2. II. *Comm. Pure Appl. Math.*, 40(4):401–420, 1987.

[LS98] Pierre Liardet and Pierre Stambul. Algebraic computations with continued fractions. *Journal of Number Theory*, 73(1):92 – 121, 1998.

[Mah32] Kurt Mahler. über das Maß der Menge aller S-Zahlen. *Math. Ann.*, 106(1):131–139, 1932.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.

[Niv63] Ivan Niven. *Diophantine approximations*. The Ninth Annual Series of Earle Raymond Hedrick Lectures of The Mathematical Association of America. Interscience Tracts in Pure and Applied Mathematics No. 14. Interscience Publishers, a division of John Wiley & Sons, New York- London, 1963.

[Rog70] C. A. Rogers. *Hausdorff measures*. Cambridge University Press, London-New York, 1970.

[Sar15] Peter Sarnak. Letter to scott aaronson and andy pollington on the solovay-kitaev theorem and golden gates. `https://publications.ias.edu/sarnak/paper/2637`, 2015.

[Sch67] Asmus L. Schmidt. Farey triangles and Farey quadrangles in the complex plane. *Math. Scand.*, 21:241–295 (1969), 1967.

[Sch69] Asmus L. Schmidt. Farey simplices in the space of quaternions. *Math. Scand.*, 24:31–65, 1969.

[Sch00] Fritz Schweiger. *Multidimensional continued fractions*. Oxford Science Publications. Oxford University Press, Oxford, 2000.

[Sch15] Johannes Schleischitz. Diophantine approximation on polynomial curves, 2015, arXiv:1503.01622.

[SKKT00] Karen E. Smith, Lauri Kahanpää, Pekka Kekäläinen, and William Traves. *An invitation to algebraic geometry*. Universitext. Springer-Verlag, New York, 2000.

[Til17] Morten Hein Tiljeset. Intrinsic Diophantine Approximation on General Polynomial Surfaces. *Mathematika. A Journal of Pure and Applied Mathematics*, 63(1):250–259, 2017.