Wesleyan University

Close Enough: a Dynamical Approach to the Littlewood Conjecture

by

Prayag George Singh Chatha

Advisor: Felipe A. Ramírez

Assistant Professor of Mathematics

A Thesis in Mathematics
submitted in partial fulfillment of the
requirements for the degree of Master of Arts
at Wesleyan University

Middletown, CT May, 2016

Acknowledgements

First and foremost, I would like to thank my advisor, Felipe Ramírez: ever generous with his time, he was a font of mathematical clarity, wise counsel, and corny (often funny) jokes, without which this thesis would never have been written. It has been a pleasure to work with and learn from him for over a year now; I couldn't have asked for a better advisor. I'd also like to single out my undergraduate advisors, Adam Fieldsteel, who welcomed me as a late-entry into the major and inducted me into the discipline of analysis, and Cameron Hill, who graciously mentored me for a summer research in 2015 and convinced me to pursue the BA/MA degree. Thank you both for placing your faith in a novice. Thanks of course to Caryn Canalia, the math department faculty, and my fellow grad students, for making the sixth floor such a fun place to be. To Helena, you have my gratitude for being the most agreeable of roommates. Together, we ran one heck of a victory lap. Shouts out to Throw Culture and the folks at 71 Lawn for keeping me young-at-heart. To Annie, Jaspal, and Nasim: I could not have gotten here without your support.

Abstract

Diophantine approximation is a branch of number theory that concerns the metric relationship of the rationals and irrationals. Much of the present-day research in the subject approaches problems of approximation via dynamics. We introduce the Littlewood Conjecture, a longstanding problem that was almost completely proven in 2006 by a theorem of Einsiedler, Katok, and Lindenstrauss. After giving an exposition of classical Diophantine approximation and fundamental ergodic theory, we set out a survey of the aforementioned theorem's context, particularly the motivation of the authors' dynamical approach, rich connections to linear algebra and hyperbolic geometry, an exploration of measure rigidity, and an interpretation of the paper's main conclusions.

Contents

Chapter 1

Introduction

For any $x \in \mathbb{R}$, let $\|x\|$ denote the distance from x to the nearest integer. We may reformulate the commonly-known fact that the rationals are densely distributed among the reals as follows: for every $\varepsilon > 0$, for some integer q, $\|qx\| < q \cdot \varepsilon$. In this case, q is the denominator of a rational approximation of x, and its numerator is some p, the nearest integer to qx. Whenever x is irrational, $\|qx\| \neq 0$ for all $q \in \mathbb{Z}$.

We can think of the analysis of $\|qx\|$ as the object of study in *Diophantine approximation*, a classical branch of number theory that yields unsolved problems to this day. How quickly does the infimum of $\|qx\|$ approach 0? Are there effective bounds we can place on the distance with respect to q? Do all irrational numbers behave equally? The answers are, in reverse order, "no," "yes," and "it depends." Another way to imagine Diophantine approximation is as the quantitative study of the density of $\mathbb{Q}$ in $\mathbb{R}$. We remark that because $\|x\| \leq 1$, we often work with the real line modded out by the integers, that is $\mathbb{R}/\mathbb{Z} = \mathbb{T}$, the one-dimensional torus. Virtually anything we might prove about approximation on this compact space we can generalize to all of $\mathbb{R}$.

Sometime in the 1930s, J. E. Littlewood (1885-1977) proposed one of the more

famous problems in the field.

Conjecture 1 (Littlewood's Conjecture)**.** For all $\alpha, \beta \in \mathbb{R}$,

$$\liminf_{n\to\infty} n\|n\alpha\|\|n\beta\| = 0.$$

In the words of Akshay Venkatesh, the Littlewood Conjecture (or the LC, from here on out) asserts that "α, β may be simultaneously approximated, moderately well, by rationals with the same denominator" ([Ven08]). It is generally believed, but not known, that the infimum of $\|n\alpha\| \cdot \|n\beta\|$ always approaches zero faster than $1/n$. This unsolved conjecture will serve as a focus and unifying thread throughout this survey of Diophantine approximation and contemporary methods of investigation.

In chapter two, we will cover some of the classical results of Diophantine approximation, leading to a presentation of Khinchine's result, which predates the LC and motivates the hypothesis.

Fact 1. *The set Ξ, comprising all $(\alpha, \beta) \in \mathbb{R}^2$ such that the Littlewood conjecture is not satisfied, has Lebesgue measure zero. Therefore, the LC is a problem about a set of zero measure.*

(If $\liminf_{n\to\infty} n\|n\alpha\| = 0$, then the LC holds. But one can find certain irrationals x such that $\liminf_{n\to\infty} n\|nx\| > 0$. Numbers with this property are the only possible exceptional points in the LC. Khinchin (1894 - 1959) proved that these numbers, the so-called *badly-approximables*, are a zero-measure set in $\mathbb{R}/\mathbb{Z}$.)

Despite our knowledge that the LC is, probabilistically, 'almost always true,' to find the above limit inferior via explicit calculation turns out to be rather difficult. Namely, a sequence (n_k) of integers (denominators) such that $\|n_k\alpha\|$

decreases might not lend itself to minimizing $\|n\beta\|$. Indeed, it is unknown (for instance) whether

$$\liminf_{n\to\infty} n\|\sqrt{2}n\|\|\sqrt{3}n\| = 0,$$

noting that both $\sqrt{2}$ and $\sqrt{3}$ are badly-approximable.

The intuition underlying the LC is that two (badly-approximable) numbers will always 'conspire' so that $\|n\alpha\|$ and $\|n\beta\|$ are not both large, infinitely often. Which is to say that their product is small, infinitely often.

The first significant contribution to the LC came from Cassels and Swinnerton-Dyer, who in 1955 proved that the Littlewood Conjecture is satisfied for α and β belonging to the same cubic field ([Cas55]). We shall not explore their work in any detail, for their proof is abstruse, and their result, while providing specific examples of successful Littlewood pairs, tells us little about the general truth of the LC. We should note, however, that Cassels and Swinnerton-Dyer appear to be the first mathematicians to treat the lefthand side of the formula of the LC as the product P of three linear forms, viz. n, $(n\alpha - m)$, and $(n\beta - l)$, where n, m, and l range over the integers and (we must be careful) $n \neq 0$. The question of Diophantine approximation becomes a *Diophantine inequality*, where we wish to find non-trivial solutions to $P(\vec{x}) < \varepsilon$ for $\vec{x} \in \mathbb{Z}^3$. This slight generalization of the problem allows for enormous flexibility in approaching the LC from the perspective of *homogeneous dynamics.*

In Chapter Three, we present a general introduction to the theory of dynamical systems and to ergodic theory–roughly speaking, the branch of dynamics studying transformations on spaces equipped with invariant measures–culminating in a discussion of *measure rigidity*, the extent to which the invariant measures of a system are fixed in a predictable manner, and *measure theoretic entropy*, which is

an important ingredient of the best result so far on the LC.

The seminal result in applications of dynamics to number theory comes from G. A. Margulis, who proved the Oppenheim Conjecture sixty years after the problem was first posed in 1929. The Oppenheim Conjecture posits that an indefinite quadratic form, not the multiple of a rational form, with three (or more) variables takes arbitrarily small values over the integers. The statement of the problem is evocative of the above formulation of the LC. For instance, for every $\varepsilon > 0$,

$$Q(\vec{x}) = x_1^2 + x_2^2 - \sqrt{2}x_3^2 < \varepsilon$$

is solvable for some solution $\vec{x} \in \mathbb{Z}^3$ ([Ven08]). His key observation, which we will explicate in Chapter Four, was to recast the density properties of forms in n variables as the density of orbits of certain flows in the n-dimension space of unimodular lattices $\mathcal{L}_n$, which we can naturally equate with the quotient $\mathrm{SL}(n,\mathbb{R})/\mathrm{SL}(n,\mathbb{Z})$. In the case of the Oppenheim conjecture, these flows were a parametrized group H of *unipotent* matrices corresponding to the symmetry (automorphism) group of Q. A bounded orbit in the space of lattices is one that stays away from its 'cusp' (a lattice is near the cusp of $\mathcal{L}_n$ if it contains a small non-zero vector), and a complete classification of all H-invariant closed sets (or equivalently, H-invariant measures) has the result of classifying all H-orbit types. If there are no H-invariant closed (proper) subsets of $\mathcal{L}_n$, the existence of bounded H-orbits is precluded. (Similarly, the fact that there are no H-invariant measures, up to composition, besides Haar ('algebraic') measures associated with some topological group containing H, has this same implication.)

The analogous approach to the Littlewood Conjecture proves more difficult because the symmetry group of Littlewood's form P is a group of *hyperbolic* ma-

trices, namely the set of diagonal matrices of determinant one, which we call A_n. Roughly speaking, the coefficients of hyperbolic matrices grow exponentially whereas those of unipotent, or 'parabolic' matrices (i.e. those whose complex eigenvalues are 1 alone) diverge only polynomial fast, and so we 'lose' information about the orbits of hyperbolic matrices much sooner ([Ven08]). Nonetheless, in 2006, Einsiedler, Katok, and Lindenstrauss proved the following:

Theorem 1. *Let μ be an A_n-invariant and ergodic measure on $X_n = SL(n,\mathbb{R})/SL(n,\mathbb{Z})$ for $n \geq 3$. Suppose that there exists a one-parameter subgroup of A_n acting on X_n with positive entropy (w.r.t μ). Then μ is algebraic: there is a closed, connected group $L > A_n$ so that μ is the L-invariant measure on a single, closed L-orbit.*

The group structure of A_n within $\mathrm{SL}(n,\mathbb{R})$ is well understood, giving us a classification of special linear subgroups L and their corresponding measures. In this way, the authors categorized all A_n-invariant measures that exhibit positively entropic behavior. We note that the statement of the above theorem mirrors quite closely a result of Daniel Rudolph, that partially answers Harry Furstenberg's $\times 2 \times 3$ Conjecture. It is commonly known that there exist many closed subsets of (and, accordingly, many invariant measures on) the circle that are invariant under a single-rank expansive action, such as $\times 2 : (x) \mapsto 2x \mod 1$: as we will see in Chapter Three, some of these are fractal Cantor sets. Furstenberg proved that, for co-prime p, q, the orbit closure $\overline{\{p^n q^m\}}_{n,m\geq 0}$ is either finite (for rational x) or otherwise the whole circle, $\mathbb{R}/\mathbb{Z}$. He conjectured, plausibly, that any measure that is invariant under the action $\times 2 \times 3$ on $\mathbb{R}/\mathbb{Z}$ is either Lebesgue measure or a Dirac measure supported on a finite set. Rudolph's 1990 theorem is the following [Rud90]:

Theorem 2. *Let μ be a probability measure on $\mathbb{R}/\mathbb{Z}$ that is invariant under and*

ergodic with respect to $\times 2$ *and* $\times 3$, *and assume that either* $\times 2$ *or* $\times 3$ *acts with positive entropy. Then* μ *is Lebesgue measure.*

Given that Lebesgue measure is the 'algebraic' measure up to a scalar constant, invariant with respect to multiplication (i.e., circle expansion), the parallels to the result of EKL are evident. Though both theorems require an entropic hypothesis, the methodology of the proofs differ greatly. But one may consider both EKL and Rudolph as facts about the rigidity of systems with "higher rank hyperbolic homogeneous actions" ([ME06]), those with transformations that take two or more parameters, which display expansive and/or contracting behavior. As we shall see in Chapter Four, the best two-dimensional analogue of A_n is the diagonal action (i.e., A_2) on $\mathcal{L}_2$, which comes with diverse invariant measures and closed invariant sets (similarly to $\times 2$ acting on $\mathbb{R}/\mathbb{Z}$.) Remarkably, the badly-approximable numbers may be embedded in these orbits.

The following is a direct corollary of Theorem 1, and is considered to be the state-of-the art of progress on the LC:

Theorem 3. *Let* Ξ, *as before, be the set of points for which the Littlewood conjecture does not hold. Then its Hausdorff dimension* $dim_H(\Xi) = 0$.

It is worth remarking that the $\dim_H(\mathbf{BA}) = 1$. We will discuss this fact and exposit Hausdorff dimension more generally in Chapter 4.5. Perhaps we could draw a loose analogy to a situation in which we had a conjecture that was open for a one-dimensional (in the common, Euclidean sense) set, such as a line, and we arrived at a result that reduces the uncertainty of the problem to a zero-dimensional set, like a point. This gives us some sense of the strength of Theorem 3. Also note that if we could obviate the assumption of positive entropy in Theorem 1, we would have the full proof of the LC ([Ven08]).

Chapter 2

Diophantine approximation

2.1 First Approach

Diophantus of Alexandria (lived c. 3rd Century CE) probably holds the distinction of being the first algebraist to publish. His treatise *Arithmetica* presented 130 algebraic problems, many of which did not see a solution until the early modern era and beyond (cf. Fermat's Last Theorem and the Hardy–Ramanujam numbers). Though he is the namesake of Diophantine approximation, Diophantus's work has little to do with number theory.

Rather, the mathematics of approximating numbers is called 'Diophantine' because it can inform the existence (or not) of solutions to types of Diophantine equations, namely polynomial equations for which only integer solutions are sought.

Definition 1 (Optimal Diophantine Approximations)**.** We say that the rational p/q, with p, q co-prime, is a best Diophantine approximation of $\alpha \in \mathbb{R}$ if

$$|q\alpha - p| < |q'\alpha - p'|$$

for all $p'/q' \in \mathbb{Q}$ such that $1 \leq q' \leq q$ and $p/q \neq p'/q.'$ In simpler terms, p/q is a best approximation if it 'beats' all other approximations, not a multiple of p/q, with smaller denominators. Whenever p/q is a best approximation of α, we find that $\|q\alpha\| = |q\alpha - p|$.

For instance, the first couple best approximations of π are $3, 22/7, 333/106, 355/113$, and $103993/33102$.

Remark. A common alternate definition of best Diophantine approximation replaces the above inequality with

$$\left|\alpha - \frac{p}{q}\right| < \left|\alpha - \frac{p'}{q'}\right|,$$

which is a weaker condition ([AMR92]) than the former. Throughout this paper I will stick by the first definition.

The following result (c. 1836) of Peter Gustav Lejeune Dirichlet (1805-1889) is considered to be the foundational theorem of Diophantine approximation.

Theorem 4 (Dirichlet's Approximation Theorem)**.** *For any $\alpha \in \mathbb{R}$, for every $N \in \mathbb{Z}_+$, there exists a pair $(p, q) \in \mathbb{Z} \times \{1, \ldots, N\}$ such that*

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

The proof is notable for being the first documented application of the *Schubfachprinzip*, or Pigeonhole Principle.

Proof. Fixing a positive integer N, we must find a q such that $\|q\alpha\| < \frac{1}{N}$. Having found such a q, our choice of p immediately follows: it's simply the integer nearest to $q\alpha$.

Consider the following sequence of integer multiples of α, $\mod 1$: $S := (\alpha, 2\alpha, \ldots, (N+1)\alpha)$. By the Pigeonhole Principle, it must be that for some pair $q_1\alpha, q_2\alpha \in S$, where $q_1 < q_2$,

$$q_1\alpha, q_2\alpha \in \Big[\frac{m-1}{N}, \frac{m}{N}\Big),$$

where $m \in 1, \ldots, N$. (Observe that S gives us $N+1$ points distributed across N slices of the unit interval: two multiples must occupy the same slice.) Hence

$$q_2\alpha - q_1\alpha \in \Big[0, \frac{1}{N}\Big),$$

implying

$$(q_2 - q_1)\alpha \in \Big[0, \frac{1}{N}\Big).$$

Letting $q = q_2 - q_1$, we have that

$$\|q\alpha\| < \frac{1}{N},$$

which proves the theorem. □

Notice that in the previous theorem, we can take $(p, q) = 1$, trivially: it's simply a matter of dividing out the pair by their greatest common factor.

Corollary 1. *When α is irrational,*

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

holds for infinitely many co-prime pairs (p, q).

Proof. Toward deriving a contradiction, assume that the corollary holds for only

n co-prime pairs, $\{(p_i, q_i)\}_{i=1}^{n}$. Since $\alpha \notin \mathbb{Q}$, for no i does $|q_i\alpha - p_i| = 0$. By the Archimedean property, there exists some $M \in \mathbb{N}$ such that $1/M < \min\{|q_i\alpha - p_i|\}_{i \leq N}$. From the previous theorem, we can furnish a $(p_{n+1}, q_{n+1}) \in \mathbb{Z} \times \{1, \ldots, M\}$ such that

$$|q_{n+1}\alpha - p_{n+1}| < \frac{1}{M},$$

a contradiction of our assumption that there are only n co-prime pairs satisfying the inequality. (If (p_{n+1}, q_{n+1}) aren't co-prime, we can force them to be by dividing them out by their greatest common divisor.) As n was arbitrarily chosen, we conclude that there are infinitely many co-prime pairs satisfying the inequality of the corollary. □

2.2 Mind Your p's and q's

The most familiar way by which we approximate irrational numbers is by truncating their (infinite) decimal expansion, such as '$2.7128\ldots$' for e. Though most of us have ten fingers, *continued fractions* offer a more intrinsic representation of a number than any base expansion.

Definition 2 (Continued Fraction)**.** A (simple) *finite continued fraction* is an expression

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}$$

on $n+1$ variables: $a_0, a_1, \ldots, a_n$. We stipulate that each a_i, also known as the ith partial quotient of α. be an integer and a positive integer for $i \neq 0$. $[a_0 : a_1, \ldots, a_n]$ is the conventional shorthand for the above expression. An *infinite continued fraction* is defined similarly, except for infinitely many inputs: i.e., $[a_0 : a_1, a_2, \ldots]$.

Though not the first to study continued fractions, Leonhard Euler (1707-1783) was the first to write about them in a systematic fashion. He proved the following in 1737:

Fact 2. *A finite continued fraction is rational; an infinite continued fraction is irrational.*

The insight for this proof comes from a well-known algorithm for converting a real number α into a continued fraction. Let $\lfloor x \rfloor$ denote the greatest integer less than or equal to x.

Definition 3 (the Continued Fraction Algorithm)**.** We obtain the continued fraction expansion of α in this way: Define $a_0 := \lfloor \alpha \rfloor$ and $r_0 := \alpha - a_0$. For $i \geq 1$, define $a_i := \lfloor \frac{1}{r_{i-1}} \rfloor$ and $r_i := \frac{1}{r_{i-1}} - a_i$. It is a straightforward exercise to show that if (and only if) α is rational, the algorithm terminates at some $k \in \mathbb{N}$ (i.e., $a_{k+1} = 0$). Then $\alpha = [a_0 : a_1, \ldots, a_k]$. Otherwise α is irrational and is equal to the limit $[a_0 : a_1, a_2, \ldots]$.

In either case, the algorithm provides us with some useful information at any given step.

Definition 4 (Convergents and Complete Quotients)**.** Let $\alpha \in \mathbb{R}$ and let $a_0, a_1, \ldots, a_k$ be the first $k+1$ terms of its continued fraction expansion. We say that the kth *convergent* of α is the rational $c_n = \frac{p_n}{q_n} = [a_0; a_1, \ldots, a_n]$. The algorithm for

computing the kth convergent is as follows: fix $c_0 = \frac{a_0}{1}$, $c_1 = \frac{a_1 a_0 + 1}{a_1}$, and for $k \geq 2$,

$$c_k = \frac{p_k}{q_k} = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}}$$

We say that the kth *complete quotient* of α is $\zeta_k = [a_k; a_{k+1}, \ldots]$. By definition,

$$\zeta_k = a_k + \frac{1}{\zeta_{k+1}} \implies \zeta_{k+1} = \frac{1}{\zeta_k - a_k}$$

The complete quotient of α terminates if and only if α is rational.

As an example, the first five convergents of π are $3, \frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \frac{103993}{332102}$. These are exactly the same as the first five best Diophantine approximations, a fact that generally holds true, which we shall later prove. We note that the 4th convergent, $\frac{355}{113}$, gives a remarkably good approximation to π for a relatively small denominator (it estimates π to 6 decimal places!). For reasons that we shall see, this fact corresponds to the fifth coefficient in its continued fraction expansion, $\pi = [3; 7, 15, 1, 292, 1, \ldots]$. 292 dwarfs the other partial quotients. We will see that larger coefficients in a number's expansion (conversely, smaller denominators in the convergents) correspond to better approximations.

Often, it's easier to work with convergents rather than partial quotients when proving things about continued fractions. We will present three somewhat technical lemmata that we require to prove the main theorems of this section, which follows [GH60]. These lemmata will allow us to calculate the distance between a real number and its nth convergent.

Lemma 5. *Let $\alpha \in \mathbb{R}$. Then $\alpha = \zeta_0$, $\alpha = \frac{\zeta_1 a_0 + 1}{\zeta_1}$, and for $n \geq 2$,*

$$\alpha = \frac{\zeta_{n+1} p_n + p_{n-1}}{\zeta_{n+1} q_n + q_{n-1}}$$

Proof. The case for $n = 0$ is obvious. For $n = 1$, we have $\alpha = a_0 + \frac{1}{\zeta_1} = \frac{\zeta_1 a_0 + 1}{\zeta_1}$. We proceed by induction: $n = 2$ is the base case:

$$\frac{\zeta_2 p_1 + p_0}{\zeta_2 q_1 + q_0} = \frac{\zeta_2(a_1 a_0 + 1) + a_0}{\zeta_2 a_1 + 1}.$$

Then, substituting our formula for the $(n+1)$th complete quotient, we obtain

$$\frac{\frac{1}{\zeta_1 - 1}(a_1 a_0 + 1) + a_0}{\frac{1}{\zeta_1 - 1} a_1 + 1} = \frac{a_1 a_0 + 1 + (\zeta_1 - a_1) a_0}{a_1 + \zeta_1 - a_1} = \frac{\zeta_1 a_0 + 1}{\zeta_1},$$

which we have shown is equal to α. We invite the reader to undertake the inductive step. □

Lemma 6. *For all $n \geq 1$,*

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

Proof. Converting the lefthand side of the equation to a common denominator and substituting for p_n, q_n, we get

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{p_{n-2} q_{n-1} + q_{n-1}(a_n p_{n-1}) - p_{n-1}(a_n q_{n-1}) - q_{n-1} p_{n-2}}{q_n q_{n-1}} = \frac{p_{n-2} q_{n-1} - p_{n-1} q_{n-2}}{q_n q_{n-1}}$$

It is a cumbersome but task to show, working inductively on the continued fraction algorithm, to show that $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}(p_1 q_0 - q_1 p_0) = (-1)^{n-1}$, which is sufficient to complete the proof. □

Lemma 7.

$$\left| \alpha - \frac{p_n}{q_n} \right| = \frac{1}{q_n(\zeta_{n+1} q_n + q_{n-1})}$$

As a corollary, we get the following inequality:

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

since $q_{n+1} = a_{n+1}q_n + q_{n-1}$.

Proof. By applying Lemma 5 and converting to a common denominator, we get

$$|\alpha - \frac{p_n}{q_n}| = |\frac{(\zeta_{n+1}p_n + p_{n-1})q_n}{(\zeta_{n+1}q_n + q_{n-1})q_n} - \frac{p_n(\zeta_{n+1}q_n + q_{n-1})}{q_n(\zeta_{n+1}q_n + q_{n-1})}| = |\frac{p_{n-1}q_n - q_{n-1}p_n}{q_n(\zeta_{n+1}q_n + q_{n-1})}|.$$

Substituting the formula from Lemma 6, we get

$$|\alpha - \frac{p_n}{q_n}| = |\frac{(-1)^{n-1}}{q_{n-1}q_n}| = \frac{1}{q_n(\zeta_{n+1}q_n + q_{n-1})},$$

which concludes the proof of our last continued fraction lemma. Incidentally, this lemma, plus the fact that irrational numbers have infinitely many convergents, give another proof of Dirichlet's theorem. □

Theorem 8 (Convergents are Best Diophantine Approximations)**.** *Let* p_n/q_n *be the* n*th convergent of* α*, where* $n > 1$*. Let* $p/q \neq p_n/q_n$ *be a rational and suppose that* $1 \leq q < q_{n+1}$*. Then*

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

Proof. We can assume that $(p, q) = 1$. From Lemma 7 , we have that

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

so we can further assume that $q_{n-1} < q < q_n$, which reduces the problem to showing that p_{n-1}/q_{n-1} is a best Diophantine approximation: the complete theorem

follows from a simple reverse-inductive argument. Now if $q = q_n$, then certainly $p \neq p_n$, so

$$\left|\frac{p_n}{q_n} - \frac{p}{q_n}\right| \geq \frac{1}{q_n}.$$

And from Lemma 7,

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

since for all n $q_n \geq n$. An application of the triangle inequality tells us that

$$\left|\frac{p}{q_n} - \alpha\right| > \frac{1}{2q_n}.$$

So

$$\left|\frac{p_n}{q_n} - \alpha\right| < \frac{1}{2q_n} < \left|\frac{p}{q_n} - \alpha\right|,$$

which proves the theorem for the case $q = q_n$.

Now suppose that $q_{n-1} < q < q_n$. Consider the following system of equations for suitable μ, ν:

$$\mu p_n + \nu p_{n-1} = p, \quad \mu q_n + \nu q_{n-1} = q.$$

We multiply the former by q_{n-1}, the latter by p_{n-1}, and subtract them, yielding

$$\mu(p_n q_{n-1} - p_{n-1} q_n) = p q_{n-1} - q p_{n-1},$$

giving us (after an application of Lemma 6)

$$\mu = \pm(p q_{n-1} - q p_{n-1}).$$

Similarly, multiplying the first equation by q_n, the second by p_n, and subtracting

them shows that

$$n = \pm(pq_n - qpn).$$

We conclude that μ and ν are non-zero integers, since $p/q \neq p_{n-1}/q_{n-1}, p_n/q_n$. Our equation for q tells us that $\mu q_n + \nu q_{n-1} = q < q_n$, which means μ and ν have opposite signs. Recall from Lemma 7 that

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

So

$$q_n\alpha - p_n = \frac{(-1)^{n-1}}{q_{n-1}}, \quad q_{n-1}\alpha - p_{n-1} = \frac{(-1)^n}{q_n}.$$

Since q_n, q_{n-1} are both positive, then $q_n\alpha - p_n, q_{n-1}\alpha - p_{n-1}$ are of opposite sign. Which is to say that $\mu(q_n\alpha - p_n), \nu(q_{n-1}\alpha - p_{n-1})$ have the same sign. Therefore:

$$|q\alpha - p| = |(\mu q_n + \nu q_{n-1})\alpha - \mu q_n + \nu q_n - 1| = |\mu(q_n\alpha - p_n) + \nu(q_{n-1}\alpha - p_{n-1})|.$$

Because the two summands have the same sign, we may break apart the inequality:

$$= |\mu||(q_n\alpha - p_n)| + |\nu||(q_{n-1}\alpha - p_{n-1})| > |\mu||(q_n\alpha - p_n)|.$$

Since μ is a non-zero integer,

$$|q\alpha - p| > |\mu||q_n\alpha - p_n| \geq |p_n\alpha - p_n|,$$

which is what needed to be shown. □

Adolf Hurwitz (1859-1919) proved what is the *tightest* bound of approximation we can apply to every irrational, giving the best refinement of Dirichlet's result.

His theorem also comes in two parts.

Theorem 9 (Hurwitz's Approximation Theorem)**.**

(a) For any irrational α, there exist infinitely many co-prime pairs $(p, q) \in \mathbb{Z} \times \mathbb{Z}_+$ such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

(b) Furthermore, if $c < \frac{1}{\sqrt{5}}$, then there exists some $x \in \mathbb{R}$ such that the inequality

$$\left|x - \frac{p}{q}\right| < \frac{c}{q^2}$$

holds for only finitely many co-prime pairs (p, q). In other words, $1/\sqrt{5}$ is the optimal bound for (a), for the general statement turns out to be false for any smaller value.

Remark. From Lemma 7,

$$|\alpha - \frac{p_n}{q_n}| = \frac{1}{q_n^2(\zeta_{n+1} + \frac{q_{n-1}}{q_n})} \lesssim \frac{1}{q_n^2 a_{n+1}}$$

since $a_{n+1} < \zeta_{n+1} < \zeta_{n+1} + \frac{q_{n-1}}{q_n}$. ("$\lesssim$" denotes less-than-but-approximately-equals.) The inequality above becomes tighter for large values of a_{n+1}, confirming our intuition that large coefficients in a number's continued fraction expansion correspond to closely-approximating convergents. Obversely, if the coefficients of a number's continued fraction expansion stay low, none of the convergents will approximate the number particularly well. This observation motivates the proof of Hurwitz's theorem.

Definition 5 (the Golden Ratio)**.** Let $\varphi = [1; 1, 1, 1, \ldots]$. Because its partial quotients are identicial, φ is equal to each of its complete quotients. Observe that

$1/\varphi = \varphi - 1 = [0; 1, 1, 1, \ldots]$. This is to say,

$$\varphi = 1 + \frac{1}{\varphi} \implies \varphi^2 - \varphi - 1 = 0.$$

Then the positive root of this polynomial is $\frac{1+\sqrt{5}}{2} \approx 1.618$.

The first few convergents of φ are:

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}.$$

Seeding the continued fraction algorithm with $a_i = 1$ for all i shows that the convergents of φ are f_{n+1}/f_n, where f_n is the nth Fibonacci number. From the previous remark, we have that

$$\left|\varphi - \frac{p_n}{q_n}\right| = \frac{1}{q_n(\zeta_{n+1}q_n + q_{n+1})} = \frac{1}{q_n(\varphi q_n + q_{n-1})} = \frac{1}{q_n^2(\varphi - \frac{q_{n-1}}{q_n})}$$

It follows from the Fibonacci sequence that $q_n = p_{n-1}$. So

$$\frac{1}{q_n^2(\varphi - \frac{q_{n-1}}{q_n})} = \frac{1}{q_n^2(\varphi - \frac{q_{n-1}}{p_{n-1}})}$$

Then, as n goes to infinity, the latter goes to

$$\frac{1}{q_n^2(\varphi - \frac{1}{\varphi})} = \frac{1}{q_n^2(2\varphi - 1)} = \frac{1}{q_n^2 2(\frac{1+\sqrt{5}}{2}) - 1} = \frac{1}{q_n^2\sqrt{5}}$$

So in some sense, this is the derivation of the bound in Hurwitz's theorem. While the continued fraction expansion of φ appears as simple as it gets, Hurwitz's theorem obliquely implies that ϕ is the least 'reasonably behaved' of all irrational numbers. In the words of Hardy and Wright, "[f]rom the point of view of rational

approximation, *the simplest numbers are the worst*" ([GH60], emphasis theirs).

Proof of Theorem 9.

(a) Let α be an irrational number. We will show that for any three successive convergents of α, at least one of them satisfies the inequality of Hurwitz's theorem. Let $b_{n+1} = q_{n-1}/qn$ for $n \geq 1$. Recall from Lemma 7 that

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n(\zeta_{n+1}q_n + q_{n-1})} = \frac{1}{\zeta_{n+1} + b_{n+1}}.$$

Therefore, it is sufficient to prove that

$$\sqrt{5} < \zeta_i + b_i$$

for some $i \in \{n-1, n, n+1\}$.

Now suppose that $\zeta_i + b_i \leq \sqrt{5}$ is true for $i = n-1, n$. Recall that

$$\frac{1}{\zeta_n} = \zeta_{n-1} - a_{n-1}$$

and, since $q_{n-1} = a_{n-1}q_{n-2} + q_{n-3}$,

$$\frac{1}{b_n} = \frac{q_{n-1}}{q_{n-2}} = a_{n-1} + \frac{q_{n-3}}{q_{n-2}} = a_{n-1} + b_{n-1}.$$

It follows from our supposition that

$$\frac{1}{\zeta_n} + \frac{1}{b_n} = \zeta_{n-1} + b_{n-1} \leq \sqrt{5}.$$

We have that $\frac{1}{\zeta_n} \leq \sqrt{5} - \frac{1}{b_n}$ from the above and $\zeta_n \leq \sqrt{5} - b_n$ by supposition.

Hence,

$$1 = \zeta_n \frac{1}{\zeta_n} \leq (\sqrt{5} - b_n)(\sqrt{5} - \frac{1}{b_n}) = 5 - (b_n + \frac{1}{b_n})\sqrt{5} + 1.$$

Therefore,

$$\sqrt{5}(b_n + \frac{1}{b_n}) \leq 5 \implies b_n + \frac{1}{b_n} \leq \sqrt{5}.$$

But b_n is rational, so we have strict inequality in the above. Also, the sequence (q_n) is increasing, so $b_n < 1$. First,

$$b_n^2 + 1 < \sqrt{5} b_n \implies b_n^2 + 1 - \sqrt{5} b_n < 0.$$

Adding 1/4 to both sides, we obtain

$$(\frac{1}{2}\sqrt{5} - b_n)^2 < \frac{1}{4}$$

Then

$$b_n > \frac{1}{2}\sqrt{5} - \frac{1}{2} = \frac{1}{2}(\sqrt{5} - 1) = \frac{1}{\varphi}.$$

If we had that $\zeta_i + b_i \leq \sqrt{5}$ were also true for $i = n + 1$, we could prove, *mutatis mutandi* that

$$b_{n+1} > \frac{1}{2}(\sqrt{5} - 1).$$

Now

$$a_n = \frac{1}{b_{n+1}} - b_n < \frac{1}{2}(\sqrt{5} + 1) - \frac{1}{2}(\sqrt{5} - 1) = 1.$$

But a_n is necessarily a positive integer, running us into a contradiction. We conclude that $\zeta_{n+1} + b_{n+1} > \sqrt{5}$, which finishes our proof.

(b) We will show that if $c > \frac{1}{\sqrt{5}}$, then there are only finitely many solutions p/q

to the following inequality, disproving its general veracity:

$$\left|\varphi - \frac{p}{q}\right| < \frac{c}{q^2}.$$

This shows that $\frac{1}{\sqrt{5}}$ is the best universal bound. To derive a contradiction, suppose that there are infinitely many co-prime (p, q) for which the inequality holds. Then there are infinitely many solutions p and q such that

$$\varphi = \frac{p}{q} + \frac{\delta}{q^2}$$

where $|\delta| < c < 1/\sqrt{5}$. We re-express the above equality for arbitrary δ.

$$\frac{\delta}{q} = q\varphi - p.$$

Since $\phi = \frac{1+\sqrt{5}}{2}$, we may split this:

$$\frac{\delta}{q} = \frac{1}{2}q + \frac{\sqrt{5}}{2}q - p \implies \frac{\delta}{q} - \frac{\sqrt{5}}{2}q = \frac{1}{2}q - p.$$

Squaring both sides,

$$\frac{\delta^2}{q^2} - \sqrt{5}\delta + \frac{5}{4}q = (\frac{1}{2}q - p)^2.$$

Then

$$\frac{\delta^2}{q^2} - \delta\sqrt{5} = (\frac{1}{2}q - p)^2 - \frac{5}{4}q^2 = \frac{1}{4}q^2 - pq + p^2 - \frac{5}{4}q^2 = p^2 - pq - q^2.$$

Now, the righthand side necessarily comes out to an integer. But for sufficiently large q, the lefthand side is less than 1, a contradiction. It could be

that $p^2 - pq - q^2 = 0$, but this would imply that $(4p^2 - 4pq + q^2) = 5q^2$, or $(2p-q)^2 = 5q^2$, which cannot be because $2p-q$ is rational. We conclude that there are only finitely many solutions to the above inequality.

□

Remark. Here is an elementary observation on the Littlewood Conjecture that derives from Hurwitz's Theorem. For all $\alpha, \beta \in \mathbb{R}$,

$$\liminf_{n\to\infty} n\,\|\alpha n\|\|\beta n\| < \liminf_{n\to\infty} n\|\alpha n\|\frac{1}{n\sqrt{5}}$$

since $|n\beta - b| = \|n\beta\| < 1/\sqrt{5}n$ infinitely often with respect to rationals b/n. But for $\|\alpha n\|$ is at most $1/2$, so

$$\liminf_{n\to\infty} n\,\|\alpha n\|\|\beta n\| < \liminf_{n\to\infty} \frac{1}{2}\frac{1}{\sqrt{5}} = \frac{1}{2\sqrt{5}}.$$

We can restate Dirichlet's theorem like so: for any α in $\mathbb{R}$, there exist infinitely many positive integers q such that

$$q\|qx\| \leq 1$$

In these terms, Hurwitz's theorem tells us, in fact

$$q\|qx\| \leq \frac{1}{\sqrt{5}}$$

infinitely often, and that we cannot replace $1/\sqrt{5}$ with some smaller c, or we can supply points (such as φ, its integer translates, and integer multiples) that contravene the new bound. There are, in fact, uncountably many numbers that share this property, the *badly-approximable* numbers.

Definition 6 (Badly Approximable Numbers)**.** We define the set of badly-approximable numbers, or **BA** to be

$$\mathbf{BA} = \{x \in \mathbb{R} : \inf_{n\in\mathbb{N}} n\|nx\| > 0\}$$

$$= \{x \in \mathbb{R} : c(x) := \liminf_{n\in\mathbb{N}} n\|nx\| > 0\}.$$

We can think of $c(x)$ as an approximation constant that is non-zero only for $x \in \mathbf{BA}$; Hurwitz's theorem tells us that $c(x) \leq 1/\sqrt{5}$. The complement of **BA** are the well-approximable numbers or $\mathbf{WA} = \{x \in \mathbb{R} : c(x) = 0\}$. An equivalent definition is

$$\mathbf{WA} = \{x \in \mathbb{R} : (\forall c > 0)\left|x - \frac{a}{n}\right| < \frac{c}{n^2} \text{ i.o.}\}.$$

(Throughout we use i.o. denotes 'infinitely often,' which in this case is taken with respect to $(a, n) \in \mathbb{Z} \times \mathbb{N}$.)

The only numbers α, β for which the Littlewood Conjecture can possibly hold false are pairs within **BA**: to wit, suppose that for some α, β, we have that

$$\inf_{n\in\mathbb{N}} n\|\alpha n\|\|\beta n\| = c > 0.$$

Recalling that $\|\alpha n\| \leq 1/2$, it follows that

$$\inf_{n\in\mathbb{N}} \|\beta n\| \leq \frac{2c}{n},$$

implying that β is badly-approximable. A similar argument shows that $\alpha \in \mathbf{BA}$ as well.

It turns out that there is a beautiful connection between the elements of **BA** (incidentally, an uncountable set, see [GH60]) and their characterizations as con-

tinued fractions . Our proof here follows [BRV16].

Lemma 10. *Let x be an irrational. Then x is badly-approximable if and only if the partial quotients of its continued fraction expansion $[a_0; a_1, a_2, \ldots]$ are bounded.*

Proof. We must show that

$$x \in \mathbf{BA} \iff (\exists M \in \mathbb{N})(\forall i)\ a_i \leq M.$$

Recall that Lemma 7 gives us the distance between x and its nth convergent:

$$\left| x - \frac{p_n}{q_n} \right| = \frac{1}{q_n(\zeta_{n+1}q_n + q_{n-1})}$$

The continued fraction algorithm tells us that $q_{n+1} = a_{n+1}q_n + q_{n-1}$, and we saw in Lemma 6 that $a_{n+1} + 1 \geq \zeta_{n+1}$. Therefore $a_{n+1}q_n + q_n + q_{n-1} \geq \zeta_{n+1}q_n + q_{n-1}$, which is to say that

$$q_{n+1} + q_n \geq \zeta_{n+1}q_n + q_{n-1}.$$

Thus

$$\frac{1}{q_n(q_{n+1} + q_n)} \leq \left| x - \frac{p_n}{q_n} \right|.$$

Putting the two bounds together,

$$\frac{1}{q_n(q_{n+1} + q_n)} \leq \left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}.$$

Some manipulation shows that

$$\frac{1}{q_n^2(\frac{q_n+1}{q_n} + 1)} < \left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n \frac{q_{n+1}}{q_n}},$$

implying

$$\frac{1}{q_n^2(a_{n+1}+2)} \leq \left| x - \frac{p_n}{q_n} \right| < \frac{1}{a_{n+1}q_n^2}.$$

First, suppose that $x \in \mathbf{BA}$. Then $c(x)$, as defined above, is greater than zero. The above implies that (multiplying through by q_n^2)

$$c(x) \leq q_n \|q_n x\| < \frac{1}{a_{n+1}}.$$

Taking reciprocals, we get that

$$a_{n+1} < \frac{1}{c(x)},$$

which is of course a bounded quantity. So for every number i, $|a_i| \leq \max\{|a_0|, 1/c(x)\}$.

Conversely, suppose that there exists $M \in \mathbb{N}$ bounding all partial quotients of x. Let $q \in \mathbb{N}$. Because convergents are best approximations (Theorem 8), there exists $n \geq 1$ such that $q_{n-1} \leq q < q_n$ and

$$\left| x - \frac{p}{q} \right| \geq \left| x - \frac{p_n}{q_n} \right| > \frac{1}{q_n^2(a_{n+1}+2)} > \frac{q^2}{q_n^2} \frac{1}{q^2(M+2)}.$$

Now, by supposition on q,

$$\frac{q}{q_n} \geq \frac{q_{n-1}}{q_n} = \frac{q_{n-1}}{a_n q_{n-1} + q_{n-2}},$$

from the CF algorithm. Thus

$$\frac{q}{q_n} \geq \frac{1}{M+1}.$$

We substitute it back in. Then,

$$\left| x - \frac{p}{q} \right| > \frac{1}{q^2(M+2)} \frac{1}{(M+2)^2},$$

implying that $c(x) > 0$ and that $x \in \mathbf{BA}$, completing the proof. □

One of the defining characteristic of φ is that it is equal to each of its complete quotients. That is,

$$\varphi = 1 + \frac{1}{\varphi},$$

which gives us the quadratic $\varphi^2 - \varphi - 1 = 0$. φ is the positive root of a quadratic (thence the root 5 in its evaluation and in Hurwitz's bound). That the archetypical badly-approximable number is a 'quadratic surd,' or irrational algebraic number of degree two, is no coincidence. In 1737, Leonhard Euler (1707 - 1783) proved that a periodic continued fraction is a quadratic surd, which is to say, a real solution to a second-degree polynomial. Joseph-Louis Lagrange (1736 - 1813) proved the converse in 1770. [AMR92] presents the proofs of these (intricate) theorems in full detail; we will satisfy ourselves with a crude heuristic that makes this fact plausible. Observe that if ξ is a periodic continued fraction, then

$$\xi = \frac{1}{\text{finite number of partial quotients} + \frac{1}{\xi}},$$

in which case, we would expect (after some manipulation) to be able to express ξ in terms of its reciprocal, a fundamentally *quadratic* relation. An elegant fact follows from this.

Fact 3. *Every quadratic irrational is badly-approximable. Because quadratic irrationals have periodic continued fraction expansions, their partial quotients are*

bounded, which implies their bad-approximability.

In Hurwitz's Theorem, we saw that φ, as a root of the polynomial $x^2 - x - 1$, is the 'pathological' point motivating bound in the inequality

$$q\|qx\| < \frac{1}{\sqrt{5}}.$$

The proof of part (b) would have worked had we substituted in the other root of $x^2 - x - 1$, namely $-\varphi + 1$. As it turns out, $\frac{1}{\sqrt{5}}$ is the first member of a fascinating set of numbers that further tie quadratic surds to approximation of continued fractions.

Definition 7 (the Lagrange Spectrum)**.** For all $x \in R$
$\{\varphi, -\varphi + 1\}$, the inequality

$$q\|qx\| < \frac{1}{\sqrt{8}}$$

holds for infinitely many integers q, and $\frac{1}{\sqrt{8}}$ cannot be decreased if x is a solution to the quadratic equation $x^2 + 2x - 1$. Otherwise, there are infinitely many integer solutions of

$$q\|qx\| < \frac{5}{\sqrt{221}},$$

a bound which cannot be improved for roots of $13x^2 + 29x - 13 = 0$, and so forth. This family of quadratic forms gives rise to the Lagrange Spectrum, $\{\frac{1}{\sqrt{5}}, \frac{1}{\sqrt{8}}, \frac{5}{\sqrt{221}}, \frac{13}{\sqrt{1517}}, \ldots\}$ which tends to $\frac{1}{3}$. A curious reader may consult [Cas57] and [AMR92] for the particulars on how these numbers arise.

Besides degree two surds, it is unclear which numbers belong to **BA**, which is nonetheless an uncountable set.

Conjecture 2 (the Folklore Conjecture)**.** The only algebraic irrationals in **BA**

are the quadratic irrationals [BRV16].

At any rate, it's unclear whether or not even cubic irrationals have any connection to periodic continued fractions. In this light, the 1955 result of Cassels and Swinnerton-Dyer, that numbers belonging to the same *cubic field* satisfy the Littlewood Conjecture, raises further questions.

2.3 Measure for Measure

Definition 8 (Very Well-Approximable Numbers)**.** We say that a number $x \in \mathbb{R}$ is very well-approximable if belongs to the set **VWA**, defined as follows: $\varepsilon > 0$ and infinitely many pairs (a, n) such that

$$\mathbf{VWA} := \{x \in \mathbb{R} : (\exists \varepsilon > 0)\left|x - \frac{a}{n}\right| < \frac{1}{n^{2+\varepsilon}} \text{ i.o.}\}.$$

Perhaps superficially, this doesn't seem like a very different set from **WA**. For any x in $\mathbf{WA} \cup \mathbf{VWA}$, $c(x) = 0$. But in **VWA**, the distance between a number and its approximations goes to zero particularly fast–faster than quadratically. This extra condition has the ramification that, whereas **WA** has full measure in $\mathbb{R}$, **VWA** is a zero-measure set. The remainder of this chapter will be dedicated to a proof of this fact.

(There is an even more stringent family of numbers (with no name that I am aware of), the set of irrational $x \in \mathbb{R}$ such that for every $n \in \mathbb{N}$, for some $p, q \in \mathbb{Z}$ with $q \neq 1$,

$$\left|x - \frac{p}{q}\right| < \frac{1}{q^n}.$$

Joseph Liouville (1809-1882) proved in 1844 that a number satisfying this inequality cannot be the root to a polynomial of degree > 0. In doing so, he proved the

existence of transcendental numbers, a set to which nearly every number belongs. See [GH60] for the proof of this fascinating and monumental theorem.)

We will assume that the reader has a basic grasp of measure theory.

Lemma 11 (the First Borel-Cantelli Lemma)**.** *Let (X, Σ, μ) be a measure space, and let $(E_n)_{n=1}^{\infty} =: (E_n)$ be a sequence of subsets in Σ. If the summed measure of (E_n) is finite, that is,*

$$\sum_{n=1}^{\infty} \mu(E_n) \leq M$$

for some $M \in \mathbb{R}_+$, then

$$\mu(\limsup_{n\to\infty} E_n) = \mu(\bigcap_{n\in\mathbb{N}} \bigcup_{k\geq n}^{\infty} E_k) = 0.$$

The limit supremum of a sequence of subsets are the points which appear in (E_n) infinitely often. Therefore, in less formal terms, the first Borel-Cantelli lemma tells us that the 'events' recurring infinitely in a sequence with finite summed measure must have zero measure.

Proof. Measure is monotone: if $A \subseteq B$ then $\mu(A) \leq \mu(B)$. Therefore, for every $n \in \mathbb{N}$,

$$\mu(\bigcap_{n\in\mathbb{N}} \bigcup_{k\geq n} E_k) \leq \mu(\bigcup_{k\geq n}^{\infty} E_k) \leq \sum_{k\geq n}^{\infty} \mu(E_k),$$

which is a bound on $\mu(\limsup_{n\to\infty}(E_n))$ holding true for any n. Now by assumption, $\sum_{n=1}^{\infty} \mu(E_n) \leq M$, so evidently the tail end of the series must go to zero as n goes to infinity. Then

$$\lim_{n\to\infty} \sum_{k\geq n}^{\infty} \mu(E_k) = 0,$$

which shows that $\mu(\limsup_{n\to\infty}(E_n)) = 0$. □

Does a direct converse of the first Borel-Cantelli lemma hold? One might *expect* that if a sequence of subsets in a measure space has unbounded measure, then the limit supremum of the sequence has full measure. As it turns out, this statement is false. Consider $(E_n) = ([0,1],[0,1/2],[0,1/3],\ldots)$ as a sequence on the unit interval I. The summed measure (length) of this harmonious sequence diverges, yet $\limsup_{n\to\infty} E_n = \{0\}$, a zero-measure singleton. However, if we strengthen the conditions on (E_n), we obtain a partial converse to the above lemma.

We say that two sets $A, B \in \Sigma$ are independent if

$$\mu(A \cap B) = \mu(A)\mu(B).$$

Note that the counterexample above does *not* possess this property.

Lemma 12 (the Second Borel-Cantelli Lemma)**.** *Let (E_n) be a sequence of independent subsets of a probability space (i.e., a finite measure space normalized to have a total measure of 1). In particular,*

$$\mu(\bigcap_{n\in\mathbb{N}}(E_n)) = \prod_{n\in\mathbb{N}} \mu(E_n).$$

If

$$\sum_{n=1}^{\infty} \mu(E_n) > M$$

for all $M > 0$, then

$$\mu(\limsup_{n\in\mathbb{N}}(E_n)) = 1.$$

Proof. We will show that the complement of $\limsup_{n\to\infty}(E_n)$ has zero measure. By

DeMorgan's Law,

$$(\limsup_{n\to\infty} E_n)^C = (\bigcap_{n\in\mathbb{N}} \bigcup_{k\geq n} E_k)^C = (\bigcup_{n\in\mathbb{N}} \bigcap_{k\geq n} E_k^C).$$

This latter set is the set of points that appear outside of E_n all but finitely often, which is to say, $\liminf_{n\to\infty} E_n^C$). With this in mind, toward our proof it suffices to show that $\mu(\bigcap_{k\geq n} E_k^C = 0$ for every n, since a countable union of zero-measure sets has measure zero. Now

$$\mu(\bigcap_{k\geq n} E_k^C) = \lim_{M\to\infty} \mu(\bigcap_{k=n}^{M} E_k^C),$$

which by assumption of independence comes out to

$$\lim_{M\to\infty} \prod_{k=n}^{M} \mu(E_K^C)$$

because (we assert) independence of (E_k) implies independence of (E_k^C). Given the inequality $1 - x \leq e^{-x}$, we deduce that

$$\lim_{M\to\infty} \prod_{k=n}^{M} \mu(E_k^C) \leq \lim_{M\to\infty} \prod_{k=m}^{M} e^{-\mu(E_k)} = \lim_{M\to\infty} e^{-\sum_{k=n}^{M} \mu(E_k)}.$$

By hypothesis, $\sum_{k=1}^{\infty} \mu(E_k)$ diverges, so certainly $\sum_{k=n}^{M} \mu(E_k)$ diverges as M goes to infinity. Hence

$$\mu(\bigcap_{k\geq n}^{\infty} E_k^C) = \lim_{M\to\infty} e^{-\sum_{k=n}^{M} \mu(E_k)} = 0,$$

which proves that $\liminf_{n\to\infty} E_k^C$ has measure zero, completing the proof. □

With these lemma, we can begin to prove some measure-theoretic properties of the sets **VWA** and **BA**.

Theorem 13. *The set of very well-approximable numbers has measure zero.*

Proof. For $\varepsilon > 0$, we define the set

$$V(\varepsilon) = \{x \in [0,1] : |x - \frac{a}{n}| < \frac{1}{n^{2+\varepsilon}} \text{ i.o.}\}$$

that is, infinitely often with respect to co-prime pairs (a, n). Then $\mathbf{VWA} = \bigcup_{k\in\mathbb{N}} V(1/k)$. So it suffices, toward finishing the proof, to show that $V(1/k)$ has measure zero for any choice of k. So we fix k, and define, for $n \in \mathbb{N}$,

$$E_n(k) = E_n := \bigcup_{a\leq n} \{x \in [0,1] : \left|x - \frac{a}{n}\right| < \frac{1}{n^{2+\frac{1}{k}}}\}$$

Then

$$V(1/k) = \limsup_{n\to\infty}(E_n).$$

Now for each n,

$$\mu(E_n) \leq \sum_{a\leq n} \frac{1}{n^{2+\frac{1}{k}}} = \frac{1}{n^{1+\frac{1}{k}}}.$$

Therefore,

$$\sum_{n=1}^{\infty} \mu(E_n) \leq \sum_{n=1}^{\infty} \frac{1}{n^{1+\frac{1}{k}}}.$$

But the latter series converges, so $\sum_{n=1}^{\infty} \mu(E_n)$ is bounded. By the first Borel-Cantelli Lemma,

$$\mu(V(1/k)) = \mu(\limsup_{n\to\infty} E_n) = \mu(\{x\}) = 0.$$

Thus $\mu(\mathbf{VWA} \cap [0,1]) = 0$. This is sufficient to conclude that almost every real number x is *not* very well approximable: $\mathbb{R}$ is a countable union of integer translates of $I = [0,1]$, and addition by an integer does not affect its Diophantine

properties. □

Theorem 14. *The set of well-approximable numbers has full measure and its complement, the set of badly-approximable numbers, has zero measure.*

Corollary 2 (Corollary to Theorem 14)**.** *The set of points in* $\mathbb{R}^2$ *that violate the Littlewood Conjecture has measure zero.*

Remark. Restricting our attention again to the unit interval, recall that

$$\mathbf{WA} \cap [0,1] = \bigcap_{k\in\mathbb{N}} \{x \in [0,1] : \left|x - \frac{a}{n}\right| < \frac{1}{kn^2} \text{ i.o.}\} =: \bigcap_{k\in\mathbb{N}} U_k.$$

It would be enough to show that for each n, $\mu(W_k) = 1$. Then

$$U_k = \limsup_{n\to\infty} \bigcup_{a\leq n} \{x \in [0,1] : \left|x - \frac{a}{n}\right| < \frac{1}{kn^2}\} =: \limsup_{n\to\infty} F_n.$$

We would want to be able to apply the second Borel-Cantelli Lemma, and it can be shown that $\sum_{n=1}^{\infty} F_n$ diverges. However, the successive F_n are not independent since, for $n' > n$, $F_n \subset F_{n'}$. We could attempt to prove instead that $\mu(\mathbf{BA}) = 0$, but this involves measuring the limit inferior of a sequence of sets, which we don't have any useful theorems about.

The following theorem is due to Aleksandr Ya. Khinchin ([BRV16]). As a preliminary, given a sequence $\psi : \mathbb{N} \to \mathbb{R}^+$, we define a number x to be ψ-approximable if there exist infinitely many $q \in \mathbb{N}$ such that $\|qx\| < \psi(q)$. Furthermore, we define

$$W(\psi) := \{x \in [0,1] : \|qx\| < \psi(q) \text{ i.o.}\}.$$

Theorem 15 (Khinchin's Approximation Theorem)**.** *Khinchin's theorem is the*

following: whenever ψ is monotone,

$$\mu(W(\psi)) = \begin{cases} 0 & \text{if} \quad \sum_{q=1}^{\infty} \psi(q) < \infty, \\ 1 & \text{if} \quad \sum_{q=1}^{\infty} \psi(q) = \infty. \end{cases}$$

These two branches of above expression are sometimes called the convergent and divergent case of Khinchin's Theorem. The convergent case follows immediately from the first Borel-Cantelli Lemma, but the proof of the divergent case is is too involved to be reproduced here. The latter case allows us to prove that $\mu(\mathbf{BA}) = 0$, but before we do so, we make two remarks.

First, in terms of this new notation, Dirichlet's Approximation Theorem implies that

$$W(q^{-1}) = [0, 1].$$

This fact certainly agrees with the convergent case of Khinchin's theorem: the harmonic series diverges, implying that $\mu(W(q^{-1})) = 1$. Another way to look at it is this: if ψ is of the form $\psi : q \mapsto q^{-\tau}$ for some $t > 0$, we define $W(\tau) := W(\psi)$, and call this set the *τ-well approximable numbers.* Dirichlet's theorem informs us that every number is 1-well approximable.

Secondly Khinchin's theorem tells us that for every $\tau > 1$, $W(\tau)$ is a set of zero measure (and **VWA** is a countable union of zero measure W-sets; therefore it has zero measure itself). But consider the pair $W(2), W(100)$. Clearly the former is contained in the latter, and we would intuitively expect $W(q^{-100})$ to be a smaller set, for its membership criterion is stricter. But Khinchin's theorem tells us nothing about the relative size of the two, only that both have zero measure. It turns out that there is a more refined notion of a set's size than Lebesgue measure, which affords us a refinement (of sorts) of Khinchin's theorem. In the very last

section of this paper (4.5), we will revisit this matter.

Proof of Theorem 14. Picking up where we left off, let

$$W_k = \limsup_{n\to\infty}\{x \in [0,1] : \|nx\| < \frac{1}{kn}\} = \limsup_{n\to\infty} F_n.$$

Observe that this set corresponds to $W(\psi)$ for $\psi(n) = \frac{1}{kn}$. Since $\sum_{n=1}^{\infty} \psi(n)$ diverges, Khinchin's theorem tells us that $\mu(W(\psi)) = 1$. But W_k is just a reformulation of U_k. So

$$\mu(\mathbf{WA}) = \mu(\bigcap_{k\in\mathbb{N}} U_k) = \mu(\bigcap_{k\in\mathbb{N}} W_k) = 1,$$

since the intersection of countably many sets with full measure has full measure. We conclude that **WA** has full measure in $[0,1]$, and by extension, full measure in $\mathbb{R}$. □

Chapter 3

Ergodic theory

3.1 A Dynamical Duo

In terms of classical mechanical physics, 'dynamical' refers to a system of equations of motion modeling the evolution of a working system. The mathematical study of dynamical systems arose in the late 19th century, particularly in the work of Poincaré and Lyapunov, as a method to investigate (respectively) the three-body problem in celestial mechanics and the stability of fluid particles. As one might expect, mathematical dynamics borrows much of its terminology from physics.

The barest definition of a dynamical system is a pair (X, T), where X is a nonempty set and $T : X \to X$ a map. We think of T as describing immediate change in the system, whereas change over the 'time' parameter t gives us the composition T^t, thus modeling the long-term behavior of X. For non-invertible mappings, t belongs to $\mathbb{Z}^+$ in discrete systems and to $\mathbb{R}^+$ is continuous systems, or flows. (if T is invertible, then the moving 'backwards in time' makes sense, and we draw t from $\mathbb{Z}$ and $\mathbb{R}$.) We can think of dynamical systems as a (semi-)group

action on their associated spaces. If G is the parametrizing (semi-)group, then

$$G \curvearrowright X : (t, x) \mapsto T^t(x).$$

Obviously the action is compatible ($T^s \circ T^t(x) = T^{s+t}(x)$) and has an identity ($T^0(x) = x$).

We'll introduce the the fundamental concepts of dynamics through two simple, canonical examples. Note that both of these examples will be *discrete* systems.

Example 1 (Circle Rotation). Let our space be the one-dimensional torus $\mathbb{T} = [0, 1]/\sim$, which is the circle obtained by gluing the ends of the unit interval together. Let $\alpha \in \mathbb{R}$. Then $R_\alpha : \mathbb{T} \to \mathbb{T}$ defines the map that rotates a point on the torus by an angle of $2\pi\alpha$ degrees. Equivalently,

$$R_\alpha x = x + \alpha \,(\text{mod } 1)$$

Note that R_α is an invertible map, which is not generally the case for dynamical systems.

We say that the *orbit* of a point x in a dynamical system (X, T) is the union of the positive (forward) and negative (backward) semiorbits of x, or

$$\mathcal{O}_T(x) = \mathcal{O}_T^+(x) \cup \mathcal{O}_T^-(x) = \bigcup_{t \geq 0} T^t(x) \cup \bigcup_{t \leq 0} T^t(x).$$

If $T^t(x) = x$ for some $m > 0$, then we say that x is m-periodic. x is fixed if $T^t(x) = x$ for all t. A subset $A \subset X$ is *forward invariant* if $T^t(A) \subset A$ for all $t \geq 0$ and *backward invariant* if $T^t(A) \subset A$ for all $t \leq 0$. In general, closures forward orbits are forward invariant and closures of backward orbits are backward

invariant.

Theorem 16. *Under circle rotation, the orbit of every $x \in \mathbb{T}$ is periodic whenever α is rational. If α is irrational, then every orbit is dense in $\mathbb{T}$ when α is irrational.*

Proof. First, suppose that α is some rational p/q. Then, for any $x \in \mathbb{T}$,

$$R_\alpha^q(x) = x + q(p/q) \,(\text{mod } 1) = x + p = x.$$

Therefore every x is q-periodic. In fact, the set

$$Y(x) = \{x + a/q \,:\, 1 \leq a \leq q\} = \mathcal{O}_{R_\alpha}(x)$$

is invariant with respect to R_α.

Now suppose α is irrational. Let $\varepsilon > 0$. By the Archimedean property, there exists a positive integer N such that $1/N < \varepsilon$. By Dirichlet's approximation theorem, there exists a pair of positive integers p, q such that

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

We may assume that p is optimally chosen, so that

$$|q\alpha - p| = \|q\alpha\| = q\alpha \bmod 1.$$

Then

$$R_\alpha^q(0) = 0 + q\alpha \bmod 1 < x + \frac{1}{N} < x + \varepsilon,$$

which implies that R_α^q is a rotation by some angle less than ε. As ε was arbitrarily chosen, it follows that that we can produce rotations via R_α that are as small as

we please. Therefore, for any x, $\mathcal{O}_{R_\alpha}(x)$ is dense in $\mathbb{T}$. $\square$

If α is a rational p/q, then any set Q of q points distributed evenly across $\mathbb{T}$ by arc length $2\pi/q$ is R_α invariant, both ways. Q is an example of a *minimal* invariant set, for there are no proper, non-empty, closed, and mapping-invariant subsets of Q. However, rotation by irrational α is dense in $\mathbb{T}$, so it follows that the only invariant subset (and thus, minimal) is $\mathbb{T}$ itself. In this sense, we can call the mapping given by irrational rotations of the circle minimal.

The following dynamical system is analogous to multiplication in the way that circle rotation was to addition. Its properties are generally more intricate.

Example 2 (Circle Expansion). Let $m \in \mathbb{Z}^+$. Letting $\mathbb{T}$ be our space as before, consider the map E_m where

$$E_m(x) = mx \,(\text{mod } 1).$$

Another way of notating this system is as $\times m$.

This map is not invertible, since for every $x \neq 0$, $E_m^{-1}(x)$ contains m points. For instance, when $m = 2$, $E_m^{-1}(1/2) = \{1/4, 3/4\}$. Additionally, E_m does not preserve the distance between points as it iterates, but rather increases (locally) them by a factor of m (mod 1). Whether or not a point x is fixed or periodic depends on its base-m expansion. We make use of the following observation: if $0.a_1a_2a_3\ldots$ is an arbitrary base m decimal, then $E_m(0.a_1a_2a_3\ldots) = a_1.a_2a_3\ldots \,(\text{mod } 1) = .a_2a_3\ldots$. In fact, circle expansions are isomorphic to the 'right shift' action on infinite strings in an alphabet of m characters, the latter being a *symbolic* dynamical system. Here's a concrete illustration. Fix the expansion factor as $m = 3$ and assume all decimals presented below are in base 3. An example of a fixed point under $\times 3$ is

$x_1 = 0.1111\ldots$. See that

$$E_3(x_1) = E_3(0.11\bar{1}) = 1.11\bar{1}\ldots \pmod 1 = 0.11\bar{1}\ldots = x_1$$

Similarly, for an example of a 2-periodic point, let $x_2 = 0.\overline{12}$. Observe,

$$E_3^2(x_2) = E_3 \circ E_3(.\overline{12}) = E_3(1.2\overline{12} \pmod 1) = E_3(.2\overline{12}) = .\overline{12} = x_2.$$

One striking difference between circle rotation and expansion is that in the latter, there exist both periodic points and points with dense orbit (as we shall see below) in the same mapping E_m, whereas in the former only on or the other is present (depending on whether rotation is rational). In this framework, R_α is the more *rigid* system of the two.

We construct a point with dense orbit under $\times m$ as follows. For each integer m, we define the *base-m enumeration* as follows:

$$\mathcal{F}_m = \bigcup_{k=1}^{\infty} \{0, 1, \ldots, m-1\}^k$$

In words, $\mathcal{F}_m$ is the (countable) set of all finite strings base m. We may enumerate its elements: $\mathcal{F}_m = w_0, w_1, w_2, \ldots$. For instance, the first few elements of $\mathcal{F}_2$ are

$$\{(0), (1), (0,0), (0,1), (1,0), (1,1), (0,0,0)\ldots\}.$$

A set A is dense in [0,1] if and only if for each $w \in \mathcal{F}_m$ there exists some $x(w) \in A$ whose base-m expansion begins with w. For instance,

$$A = \{0, 0.1, 0.01, 0.11, 0.001, 0.011, 0.101, 0.111, \ldots\}$$

is dense in $[0,1]$. (We have ommitted redundant expressions in $\mathcal{F}_m$ of the same number, namely those with trailing zeros.) Therefore we may construct a point $z \in [0,1]/\sim = \mathbb{T}$ with a dense orbit by *concatenating* each $x \in A$ into a single base-m expansion. That is,

Theorem 17.

$$z = \lim_{i\to\infty} 0.w_0 w_1 \dots w_i \in \mathbb{T},\ w_i \in \mathcal{F}_m$$

is dense in $\mathbb{T}$ *under the mapping* E_m.

Proof. Let $x \in \mathbb{T}$ and let $\varepsilon > 0$. We will show that for some positive integer n, $|E_m^n(z) - x| < \varepsilon$. For some k, it must be that $1/m^k < \varepsilon$. We consider the base-m expansion of x . Let l denote the (possibly infinite) length of the base-m expansion of x.

First, we suppose that $l \leq k$. We have that $x = 0.a_1 \dots a_l$, (where each term $a_i \in \{0, 1, \dots, m-1\}$) We define $\bar{x} = 0.a_1 \dots a_l *_{i=1}^{k-l} (0)1$, where $*_{i=1}^{k-l}(0)$ denotes 0 concatenated $k-l$ times. $\bar{x}$ is a finite base-m string, so for some j, $\bar{x} = w_j \in \mathcal{F}_m$. Then, by construction of our 'dense point' z, for some n, $E_m^n(z) = 0.w_j w_{j+1} w_{j+2} \dots$. It follows that

$$|E_m^n(z) - x| = |(0.w_j w_{j+1} \dots) - x| = |(0.a_1 \dots a_l *_{i=1}^{k-l} (0)1 w_{j+1} \dots) - 0.a_1 \dots a_l|$$

$$= |0. *_{i=1}^{k} (0)1 w_{j+1} \dots| \leq |0. *_{i=1}^{k-1} (0)1| = \frac{1}{m^k},$$

which is, by assumption, less than ε. Next, we suppose that $l > k$, which includes the case where x has an infinite base-m expansion. Then we define $\bar{x} = 0.a_1 \dots a_k$, where $(a_i)_{i=1}^{i=k}$ are the first k terms of the base-m expansion of x. Again, $\bar{x}$ is a finite sequence base-m, so for some j, $\bar{x} = w_j \in \mathcal{F}_m$. Thus for some n, $E_m^n(z) =$

$0.w_j w_{j+1} w_{j+2} \ldots$. Therefore

$$|E_m^n(z) - x| = |(0.w_j w_{j+1} \ldots) - x| = |0.a_1 \ldots a_k - 0.a_1 \ldots a_k a_{k+1} \ldots|$$

$$= |0. *_{i=1}^{k} (0) a_k a_{k+1} \ldots| \leq |0. *_{i=1}^{k-1} 1| = \frac{1}{m^k},$$

a value less than ε, thus completing our proof. □

We say that the circle expansion $(\mathbb{T}, E_m)$ is *topologically transitive* because there exists a point $z \in \mathbb{T}$ such that $\mathcal{O}_{E_m}(z)$ is dense in $\mathbb{T}$, as we just showed. The expansive $\times m$-orbit of z will eventually intersect any open set (union of arcs) we might define on the circle.

Just as with rational circle rotations, the closure of a periodic E_m-orbit is invariant. Unlike circle rotations, however, circle expansions have more exotic types of invariant sets. We'll demonstrate one in the case of $m = 3$.

Definition 9 (the Cantor ternary set)**.** Set $C_0 := [0, 1]$, and (for $i \geq 1$) define $C_i := T_L(C_{i-1}) \cup T_R(C_{i-1})$, where $T_L(x) = x/3$ and $T_R(x) = x/3 + 2$. Each set in the sequence (C_i) is a pair of copies of its predecessor, a left branch and a right branch, both shrunken down by a factor of three and translated apart. Each C_i has 2^i connected components. Another way to think of each C_i is a copy of its predecessor with the middle thirds of each component deleted.

We define $\mathcal{C}$, the Cantor ternary set, iteratively: $\mathcal{C} := \lim_{n\to\infty} C_n = \bigcap_{n=1}^{\infty} C_n$. (if you doubt that $C_0 \supset C_1 \supset C_2 \supset \ldots$ is a nested sequence of sets, the proof is an enjoyable exercise in recursive argument.) The Cantor set is a quintessential fractal, by virtue of its self-similarity. In the topology of $\mathbb{R}$, it serves as a remarkable example of a set that is both *perfect* (closed, but without isolated points) yet *nowhere dense* (the interior of its closure is empty).

Theorem 18. *The Cantor ternary set is an E_3-invariant set.*

Remark. We will shortly see that an equivalent construction of the Cantor set is $\mathcal{C} = \{x \in [0,1] : (\forall k) E_3^k(x) \notin (1/3, 2/3)\}$. Note that in base 3, $(1/3, 2/3) = (0.1, 0.2)$. If (and only if) a point $y \in [0,1]$ has a '1' in the kth position of its base-3 expansion does $E_3^k(y) = 0.1a_{k+1} \ldots \in (0.1, 0.2)$. Hence $\mathcal{C}$ is the subset of the unit interval of points whose base-3 expansion is comprised of 0's and 2's, union $\{0.1\}$. It follows readily from this new definition that $\mathcal{C}$ is E_3-invariant.

Proof. We show that $\mathcal{C} = \mathcal{A} := \{x \in [0,1] : (\forall k) E_3^k(x) \notin (1/3, 2/3)\}$, which is clearly E_3-invariant.

First, we set $A_0 := [0,1]$, and for $i \geq 1$ define $A_i := A_{i-1} - E_3^{-(n-1)}(1/3, 2/3)$. Observe that $\mathcal{A} = lim_{n\to\infty} A_n$. Furthermore, we have that $C_0 = A_0$. We proceed by induction. Let $n \in \mathbb{N}$ and suppose $C_n = A_n$. We must show that $C_{n+1} = A_{n+1}$, which is to say, that

$$T_L(C_n) \cup T_R(C_n) = A_n - E_3^{-n}(1/3, 2/3).$$

$\subseteq$: First, let $x \in T_L(C_n)$. Since $T_L(C_n) \subset C_{n+1}$, and (C_i) is a nested sequence, it follows that $x \in C_n = A_n$. Furthermore, $x \in T_L(C_n)$ implies that $3x = E_3(x) \in C_n$, which ensures that $E_3(x) \notin E_3^{-(n-1)}(1/3, 2/3)$. So $x \notin E_3^{-n}(1/3, 2/3)$, proving that $x \in A_{n+1}$. Thus $T_L(C_n) \subset A_{n+1}$, and a similar argument shows that $T_R(C_n) \subset A_{n+1}$ as well.

$\supseteq$: Let $x \in A_n - E_3^{-n}(1/3, 2/3)$. Since $A_n = C_n$, $x \in T_L(C_{n-1}) cup T_R(C_{n-1}$. Without loss of generality, assume $x \in T_L(C_{n-1})$. Then $3x \in C_{n-1} = A_{n-1}$. Furthermore, since $x \notin E_3^{-n}(1/3, 2/3)$, we know that $3x \notin E_3^{-(n-1)}(1/3, 2/3) + i$ for $i \in 0, 1, 2$. Hence $3x \in A_{n-1} - E_3^{-(n-1)}(1/3, 2/3) = A_n$. If $3x \in A_n$, then

$x \in T_L(A_n) = T_L(C_n) \subset C_{n+1}$. □

We remark that we could, with some modification to the procedure above, construct Cantoresque fractals that are invariant with respect to other factors of expansion. Also, by concatenating every base-3 word composed of only 0s and 2s into a single string, we obtain a number between 0 and 1 whose orbit is dense (and contained) in $\mathcal{C}$.

The rotation and expansion of circles are perhaps the two 'primitive' dynamical systems, simple enough to visualize but interesting enough to illustrate key dynamical concepts. We will return to these examples several times throughout the rest of this paper. To summarize what we have seen so far, the former mapping preserves distance between points while the latter increases it. The former is invertible, but the latter isn't. Orbits in the former system are either universally periodic or universally dense, whereas in the former system points can display radically different behavior. Rotations are rather rigid, expansions give rise to a wide range of invariant sets. In the language of 'higher-rank' actions, first seen in Chapter 1, we might call R_α a unipotent or *parabolic* system, whereas E_m is *hyperbolic*. We will see more of this particular dualism in Chapter 4.

3.2 Ergodic Theory for Dummies

Let $(X, \mathfrak{A}, \mu)$ be a measure space and $T : X \to X$ a map from the measure space back into itself. If T is *measurable*, meaning the preimage of any measurable set is also measurable, and *non-singular*, which requires that the pre-image of any zero-measure set also has measure zero, then we call T a transformation. A transformation is basically a dynamical system with extra measure-theoretic structure. One can check that both R_α and E_m are transformations with respect

to Lebesgue measure and the usual σ-algebra of $\mathbb{T}$.

Definition 10. We say that T is *measure-preserving* if $\mu(T^{-}1(A)) = \mu(A)$ for every $A \in \mathfrak{A}$. Accordingly, the measure μ is called *T-invariant.* A measurable f is *essentially T-invariant* if $\mu(\{x \in X : f(T^t x) \neq f(x)\}) = 0$ for every t. A measurable set A is *essentially T-invariant* if its indicator function is essentially T-invariant.

The general idea of ergodic theory is the study of dynamical systems equipped with invariant measure(s). Across the sciences, the 'ergodicity' of a stochastic process (such as a dynamical system) concerns the statistical correlation between time and space averages of its behavior. As a mathematical term, 'ergodic' is a borrowing from statistical mechanics, namely the ergodic hypothesis of Ludwig Boltzmann (1844-1906). We will present a version of his hypothesis in the inform language of measure and dynamics before giving a precise definition.

Let $(X, T : X \to X)$ be a transformation, μ a probability measure on X, and $f : X \to R$ a function. We can imagine that X is the phase space of some physical system and that T models the evolution of the system over time. The orbit $\mathcal{O}_T(x)$ gives the phase space trajectory with respect to some starting condition(s), viz. the phase $x \in X$. We think of f as an 'observable,' the outcome of a physical experiment (such as the measured pressure of a body of gas) and of $\int f d\mu$ as the expected value of the observable with respect to some statistical distribution μ. Boltzmann's hypothesis states that if μ is an equilibrium distribution (invariant with respect to time), then the time average of the observable f along a given phase space trajectory (excluding a negligible set of ill-behaved starting states) asymptotically approaches the expected value of f with respect to μ over all phases. In other words, virtually every phase space trajectory samples all possible

states if given enough time, and spends time in each of them proportional to the initial probabilistic distribution. Hence we say that the time average of an observable, under these vaguely-posed special conditions, tends to equal the space average.

Definition 11. A measure-preserving transformation T is *ergodic* if any essentially T-invariant measurable set has either zero or full measure. Equivalently, T is ergodic if any essentially T-invariant measurable function is constant $\mod 0$.

If a system is not ergodic, then it has a non-negligible invariant subset that does not interact with any other part of the system: effectively, there's another system contained within. The result of a system being ergodic is that it can't be decomposed into smaller pieces. We note that it is easy to prove one direction of the above equivalence. Suppose that every T-invariant measurable function is constant $\mod 0$. Let A be an essentially $T - invariant$ measurable set, and let $\mathbb{1}_A$ be the indicator function on A. Then $\mathbb{1}_A$ is essentially T-invariant, and by supposition, it's constant $\mod 0$. Therefore $\mathbb{1}_A$ is identically 0 or 1 on X, proving that A has either zero or full measure.

A useful fact that I will state, without proof, is that T is ergodic if and only if any essentially invariant $f \in L^p(X, \mu)$ (i.e., bounded f) is constant $\mod 0$ ([MB02]).

Theorem 19. *The circle rotation R_α is ergodic with respect to Lebesgue measure λ if and only if α is irrational.*

Proof. Let α be irrational. It suffices to show that an essentially R_α-invariant bounded function is constant $\mod 0$. Let f be an essentially R_α-invariant bounded function. It follows that f is square-integrable. Then f belongs to $L^2(\mathbb{T}, \lambda)$ a

Hilbert space with the following property: for some unique sequence $(a_n)_{n\in\mathbb{Z}}$, the Fourier series of f, $\sum_{n\in\mathbb{Z}} a_n e^{2n\pi ix}$, converges to f in the L^2 norm. Similarly, $\sum_{n\in\mathbb{Z}} a_n e^{2n\pi i(x+\alpha)}$ converges to $f \circ R_\alpha$. But by assumption, $f = f \circ R_\alpha \mod 0$, so $a_n = a_n e^{2n\pi i\alpha}$ for all n. If $n \neq 0$, then $e^{2n\pi i\alpha} \neq 1$, so $a_n = 0$. If $n = 0$, then $e^{2\pi i\alpha} = e^0 = 1$, so potentially a_0 is nonzero. Either way, f converges to a_0, so f is constant $\mod 0$. We conclude that R_α is ergodic.

If α is rational, then $\alpha = p/q$ for some integers p, q. We define an open arc

$$A(k) = (\frac{k - 1/4}{q}, \frac{k + 1/4}{q}))$$

and set

$$S = \bigcup_{1\leq k\leq q} A(k).$$

Observe that $R_\alpha^{-1}(A(k)) = A(k - p)$. So $R_\alpha^{-1}(S) = S$, which proves that S is R_α-invariant. But $\lambda(S) = \sum_{k=1}^{q} \lambda(A(k)) = q\lambda(\frac{k-1/4}{q}, \frac{k+1/4}{q})) = q(\frac{k+1/4-(k-1/4)}{q}) = q(\frac{1/2}{q}) = 1/2$, which implies that R_α is not λ-ergodic. □

Theorem 20. *The circle expansion E_m is ergodic with respect to Lebesgue measure for any m.*

Proof. Let $m \in \mathbb{N}$. Let f be an essentially E_m-invariant bounded function. Then for some unique sequence $(a_n)_{n\in\mathbb{Z}}$, the Fourier series $\sum_{n\in\mathbb{Z}} a_n e^{2n\pi ix}$ converges to f in the L^2 norm. Likewise, $\sum_{n\in\mathbb{Z}} a_n e^{2n\pi imx}$ converges to $f \circ E_m$ which is equal to $f \mod 0$. So for almost every x,

$$\sum_{n\in\mathbb{Z}} a_n e^{2n\pi ix} = \sum_{n\in\mathbb{Z}} a_n e^{2mn\pi ix}.$$

By uniqueness of the expansion, we may roup together terms of the same exponent

and conclude that $a_{mn}e^{2mn\pi ix} = a_n e^{2n\pi imx}$, which is to say that $a_n = a_{mn} = a_{m^2n} = \ldots$. If $n \neq 0$, then the series will not converge unless $a_n = 0$. Therefore f converges to a constant a_0 in the L^2 norm, so f is constant $\mod 0$. We conclude that E_m is λ-ergodic. □

For more information on the ergodic theorems and interesting applications of ergodicity to number theory, see [MB02] and [ME11].

3.3 Measure rigidity

Given a transformation $T : X \to X$, for some finite measure space on X, let $\mathcal{M}(T)$ be the set of T-invariant probability measures. The rigidity of $\mathcal{M}(T)$ is the extent to which the members of $\mathcal{M}(T)$ share an algebraic structure more predetermined than one might expect *a priori* ([Ein09]). Holomorphic functions in $\mathbb{C}$ are a classic example of a 'rigid' family of objects: every holomorphic function f can be expressed locally as a power series whose coefficients are a function of the (local) derivatives of f.

At one extreme end of the rigidity spectrum, one might be able to give no reasonable categorization of the invariant probability measures of T. At the other end, $\mathcal{M}(T)$ might contain only one element, in which case it is *uniquely ergodic.*

Theorem 21. *The circle rotation R_α is uniquely ergodic if and only if α is irrational. That is, Lebesgue measure λ on the circle is R_α-invariant and is the only invariant probability measure if and only if α is irrational.*

Proof. Any measurable set A on $\mathbb{T}$ may be approximated arbitrarily well by a finite union of intervals. This is because the set of intervals in $\mathbb{T}$ is a semi-algebra that generates the Lebesgue σ-algebra of measurable sets. The Lebesgue measure

of a generic compact interval $[a, b] \subset \mathbb{T}$ is $\int_a^b \mathbb{1} dx = b - a$ where $\mathbb{1}$ is the constant function that is identically 1. To prove that λ is R_α-invariant, it suffices to check then that $\int_a^b \mathbb{1} d\lambda = \int_a^b \mathbb{1} \circ R_\alpha^{-1} d\lambda$.

Assuming we are dealing with addition mod 1, we may write

$$\int_a^b \mathbb{1} \circ R_\alpha^{-1} d\lambda = \int_{T^{-1}(a)}^{T'^{-1}(b)} \mathbb{1}(T^{-1})'(x) d\lambda = \int_{a-\alpha}^{b-\alpha} \mathbb{1} d\lambda = (b - \alpha) - (a - \alpha) = b - a,$$

which shows that $\lambda([a, b]) = \lambda(R_\alpha[a, b])$, proving that Lebesgue measure is rotation-invariant.

Now, to prove our claim of unique ergodicity of α, we first assume that α is irrational. Let $\mu \in \mathcal{M}(T)$ be an unknown R_α-invariant measure. To show that μ and λ agree, it suffices to show that for any continuous function $f : \mathbb{T} \to \mathbb{R}$, $\int f d\mu = \int f d\lambda$. (again, 'agreement' of the two measures on continuous functions implies agreement on indicator functions, which implies that $\mu(X) = \lambda(X)$ for any measurable set X.)

Set $e_n(x) = e^{2n\pi ix}$ for $x \in \mathbb{T}$ and $n \in \mathbb{Z}$. By the Stone-Weierstrass theorem, f can be uniformly approximated by a linear combination of terms e_n (i.e. a Fourier series), so we will first check the integrals (over $\mathbb{T}$) that μ induces on each e_n. If μ is R_α-invariant, then

$$\int e_n d\mu = \int e_n \circ R_\alpha d\mu.$$

Now $e_0 = \mathbb{1}_{\mathbb{T}}$, so assume $n \neq 0$. Thus $e_n(R_\alpha(x)) = e^{2n\pi i(x+\alpha)} = e^{2n\pi i\alpha} e_n(x)$. Then

$$\int e_n d\mu = \int e_n \circ R_\alpha d\mu. = e^{2n\pi i\alpha} \int e_n(x) d\mu.$$

Since $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ we know that $e^{2n\pi i\alpha} \neq 1$, so $\int e_n d\mu = 0$ (for $n \neq 0$). Thus

$$\int f d\mu = \int a_0 e_0 d\mu = a_0 \int \mathbb{1} d\mu = a_0.$$

We'll show that λ defines the same integral on f. For each n, it follows that

$$\int_{\mathbb{T}} z^n dz = \int_0^1 e^{2\pi i t n}(2\pi i e^{2\pi i t}) dt = 2\pi i \int_0^1 e^{2\pi i t(n+1)} dt = 2\pi i \int_{\mathbb{T}} e_{n+1}$$

by parameterizing $z(t) = e^{2\pi i t}$. Therefore,

$$\int_0^1 e_n(t) dt = \frac{1}{2\pi i} \int_{\mathbb{T}} z^{n-1} dz.$$

When $n \neq 0$, $\int_{\mathbb{T}} z^{n-1}$ comes out to zero. When $n = 0$,

$$\frac{1}{2\pi i} \int_{\mathbb{T}} z^{-1} dz = \frac{1}{2\pi i} 2\pi i = 1.$$

This implies that under the Riemann integral (which is identical to Lebesgue measure for continuous functions),

$$\int_{\mathbb{T}} f d\lambda = \int_{\mathbb{T}} a_0 e_0 d\lambda = a_0.$$

We conclude that μ and λ define the same measure on $\mathbb{T}$.

Now suppose that α is rational. Then $\alpha = p/q$ for some integers p, q. Let $K = \{k/q : 1 \leq k \leq q\}$ be the set of points (*atoms*), evenly spaced by arc length $1/q$, that includes zero. Note that K is invariant with respect to rotation by p/q, and that for each $k \in K$, $R_\alpha^{-1}(k) \in K$. With this in mind, we'll define an 'atomic' probability measure (sometimes called a *Dirac measure*) ν as follows: for any

measurable $X \subset \mathbb{T}$, we set the measure

$$\nu(X) := \sum_{k \in K \cap X} 1/q.$$

Clearly ν is non-negative, assigns zero measure to the empty set, and is countably additive of disjoint sets.

Consider the interval $Y = [0, 1/q]$. Under Lebesgue measure, we have that $\lambda(Y) = 1/q$. But Y contains two atoms $k \in K$, (namely $1/q$ and $q/q = 0$) so $\nu(Y) = 2/q$. Hence ν disagrees with Lebesgue measure. All that remains to check is that ν is R_α-invariant. But for any measurable $X \subset \mathbb{T}$, if X contains n atoms of K, then $R_\alpha^{-1}(X)$ also contains n atoms, since rotation by $\alpha = p/q$ can only map atoms to atoms. So $\nu(X) = n/q = \nu(R_\alpha^{-1}(X)$, implying that ν is R_α-invariant. $\square$

The circle expansion map $E_m \curvearrowright \mathbb{T}$ also preserves Lebesgue measure. Given a generic interval $[a, b] \subset \mathbb{T}$,

$$E_m^{-1}([a, b]) = \{[\frac{a+i}{m}, \frac{b+i}{m}] : 0 \leq i < m\}.$$

Then

$$\lambda(E_m^{-1}([a, b])) = \sum_{i=0}^{m-1} \lambda([\frac{a+i}{m}, \frac{b+i}{m}]) = m(\frac{b}{m} - \frac{a}{m}) = b - a = \lambda([a, b]).$$

Because E_m preserves Lebesgue measure on intervals, it must preserve Lebesgue measure on all measurable sets. However, E_m, unlike R_α with irrational α, is not uniquely ergodic.

When we formed an invariant, non-Lebesgue probability measure ν for a rational circle rotation, we defined an 'atomic measure,' a measure in which the

smallest sets with positive measure were singletons, or atoms. The *support* of ν was the orbit closure of the point $0 \in \mathbb{T}$. One can think of the support of a measure space as the subspace where the measure is positive, or more precisely, as the closure of the maximal subset such that every open set within has positive measure. Hence atomic measures are measures whose supports are a countable collection of singletons.

Because orbit closures are (definitionally) closed, proper, and transformation-invariant subsets of their system spaces, they naturally lend themselves to constructing invariant atomic measures. In the case of E_m, we could build such a measure with respect to any point whose base-m is expansion is periodic. However, in the previous section we encountered a closed E_3-invariant proper subset of the circle that *isn't* the closure of a periodic orbit: the Cantor set. Indicating the relative complexity of circle expansions in comparison with rotations, we'll define an E_3-invariant measure on the unit interval that is neither atomic nor Lebesgue, suggesting that E_m is non-uniquely ergodic, and non-unique in a more significant way than R_α.

Lemma 22. *A necessary preliminary to defining the measure in question is the fact that the Cantor set is homeomorphic to the countably -infinite product of a two-element set with itself, each set endowed with the discrete topology:*

$$\mathcal{C} \cong 2^{\mathbb{N}}$$

Proof. There is a natural bijection between $\mathcal{C}$ and $2^{\mathbb{N}}$: any $x \in \mathcal{C}$ has a base-3 expansion $x = 0.x_1x_2\ldots$ where each $x_i \in \{0, 2\}$. Let $f(x) = (x_1, x_2, \ldots) \in \{0, 2\}^{\mathbb{N}}$. The natural topology of $2^{\mathbb{N}}$, as the product topology of countably infinite discrete topologies, has a basis generated by *cylinder sets* ([MB02]). We can define any

cylinder on $\{0,2\}^N$ as follows: let $n_1 < n_2 \ldots < n_k$ be some finite index in $\mathbb{N}$, and let $j_i \in \{0,2\}$ for $i \leq k$. These arguments define a cylinder,

$$K^{n_1,\ldots,n_k}_{j_1,\ldots,j_k} = \{x = (x_l) : x_{n_i} = j_i, i = 1,\ldots,k\},$$

which is the set of sequences in 2^N that 'agree' with a prescribed binary sequence (j_i). Observe that any such cylinder is actually the union of cylinders of the form

$$K_{j_1,\ldots,j_k} = \{x = (x_l) : x_i = j_i, i = 1,\ldots,k\},$$

thus allowing us to restrict our attention to prescribed sequences from 1 to some $k \in \mathbb{N}$. For reasons that should become apparent, we will call these sets 'connected cylinders.' An example would be $K_{0,0,2}$, the set of all sequences that begin as $(0,0,2,\ldots)$.

As it turns out, under the bijection f, the pre-image of a cylinder corresponds to one of the 'branches' of the recursive construction of $\mathcal{C}$. Recall that we could progressively 'refine' the unit interval into left and right branches (via the mappings T_L and T_R, which together act delete the middle third of successive connected components), and that the limit of this reductive process–in some sense, an infinite binary tree-gives the Cantor set. Though we never made it explicit, it's easy to check that $T_L([0,1]$ is the set of points whose base-3 expansion begins with a 0, and $T_R([0,1]$ is the set of points whose base-3 expansion begins with a 2. Generalizing this argument, we see that for any connected cylinder,

$$f^{-1}(K_{j_1,\ldots,j_k}) = \{x = 0.x_1x_2\ldots : x = .j_1\ldots j_k\ldots\} = T_{p_1,p_2,\ldots,p_k},$$

where

$$p_i = \begin{cases} L & \text{if } j_i = 0 \\ R & \text{if } j_i = 2, \end{cases}$$

and

$$T_{p_1,p_2,\ldots,p_k} = T_{p_k} \circ T_{p_{k-1}} \circ \ldots \circ T_{p_1}(0,1).$$

So, for example, $f^{-1}(K_{0,0,2}) = T_{L,L,R}$. Now each $T_{p_1,p_2,\ldots,p_k}$ corresponds to a connected component of C_k in the recursive construction of $\mathcal{C}$. This component is open (clopen, in fact), so f is continuous.

$\mathcal{C}$ is compact because it is closed and bounded. $2^{\mathbb{N}}$ is Hausdorff because it is the product of Hausdorff spaces. Given that $f : \mathcal{C} \to 2^{\mathbb{N}}$ is a continuous bijection, we can conclude that f is a homeomorphism: f is a closed mapping, so f^{-1} is continuous. □

Definition 12 (the Coin-Flipping Measure)**.** We have shown above that we can treat the Borel σ-algebra of $\mathcal{C}$ and of $2^{\mathbb{N}}$ as topologically equivalent under the above homeomorphism. The connected cylinders of the form $K_{j_1,\ldots,j_k}$ generate the topology of $2^{\mathbb{N}}$, so their pre-images under f generate the topology of $\mathcal{C}$. Hence we define $\tau(f^{-1}(K_{j_1,\ldots,j_k})) := 2^{-k}$. Effectively, we are treating the connected components of Cantor construction sets, $T_L(C_i)$ or $T_R(C_i)$ as generating the Borel-algebra of $\mathcal{C}$; the measure of these sets correspond (inversely) to their depth k in the binary tree that generates the Cantor set.

The measure τ is still, technically, a measure on the unit interval, but observe that its support is $\mathcal{C}$: an equivalent definition of the support of a measure space is the intersection of all sets with full measure. The sets of $[0,1]$ with full τ measure are exactly $C_0 = [0,1], C_1 = T_L([0,1]) \cup T_R([0,1]), C_2 = \ldots$, and their intersection is, by definition, $\mathcal{C}$. The support of Lebesgue measure on the unit interval is the

whole interval, so τ is a non-atomic, non-Lebesgue, probability measure.

Theorem 23. *The coin-flipping measure τ is E_3-invariant.*

Proof. Recall that Cantor construction sets generate the Borel-algebra of τ on $[0,1]$. Let X be such a set—then $X = [0,1]$, or for some $i \geq 0$, $X = T_L(C_i)$ or $X = T_R(C_i)$. In the former case,

$$\tau(E_3^{-1}([0,1])) = \tau([0,1/3] \cup [1/3,2/3] \cup [2/3,1]) = \tau([0,1/3]) + \tau([1/3,2/3]) + \tau([2/3,1])$$

by subadditivity of τ,

$$= \tau(T_L(C_0)) + 0 + \tau(T_R(C_0)) = 2^{-1} + 2^{-1} = 1 = \tau([0,1]),$$

proving τ-invariance of X in the first case. The argument for the latter case is quite similar, and I'll leave it as an exercise for the unconvinced. □

We should take away, from this discussion, the sense that there is a deep correspondence between the possible types of orbit closures in a transformation (be they dense, periodic, or dense in a particular subset) and the invariant measures associated with a system. We may classify such measures by their supports, which can be the whole space, a finite collection of atoms, or even a fractal, as we have seen with the Cantor set.

3.4 The $\times 2 \times 3$ Conjecture

We will now discuss a dynamical system obtained from the joint action of two expanding maps.

Example 3 ($\times 2 \times 3$). For $x \in \mathbb{T}$, let $F_{2,3}(x)$ denote the set (a rank-two semigroup) $\{2^k 3^l(x) : k, l \in \mathbb{Z}^+\}$. The $\times 2 \times 3$ map is the two-parameter dynamical system associated with the semigroup action of $F_{2,3}$ on $\mathbb{T}$

H. Furstenberg (b. 1935) was the first to study this system as an example of the 'product' (in a loose sense) of two semigroup actions with co-prime factors. He proved that $F_{2,3}(x)$ is dense in $[0,1]/\sim$ for irrational x ([Ein09]). In fact, we could generalize this to hold for any irrational orbit set $F_{m,n}$ where m and n are coprime. We are led to ask a natural question. Given that we have seen non-Lebesgue invariant probability measures for E_3–and by a small stretch of the imagination could imagine similar measures for E_2–are there any probability measure that are invariant with respect to both $\times 2$ and $\times 3$ (which is to say, $F_{2,3}$)? In the previous chapter, we have seen that closed, invariant sets dependably correspond to the set of possible invariant measures. Unlike in the case of E_2 or E_3 alone, there is no obvious way to define a Cantoresque fractal that is invariant under their joint action. The conjecture below is attributed to Furstenberg.

Conjecture 3 (the $\times 2 \times 3$ Conjecture)**.** The only probability measures on the circle that are invariant for both E_3 and E_2 are Lebesgue measure, atomic measures defined with respect to certain rational numbers (viz. those whose expansions are periodic in base 6), and convex combinations (averages) of the previous two. Stated equivalently, the only infinite, closed, $F_{2,3}$-invariant subset of the circle is the circle itself.

The conjecture is still unresolved, but Dan Rudolph (1949-2010) proved the fullest partial result ([Rud90]) in 1990:

Theorem 24. *If μ is an E_3, E_2-invariant measure with positive metric entropy, then μ is Lebesgue measure.*

But what is metric entropy, anyway?

3.5 The Most Glorious Number in Dynamics

(The title of this section is owed to an assertion of Anatole Katok (b. 1944). The discussion itself follows [Mor05].)

Entropy, in thermodynamics, is the quantification of the uncertainty of a physical system. The classic illustrating example is this: suppose that a sealed box were split into two connected compartments, each filled with a different type of gas, and that at will one could remove the dividing partition. The best case, in terms of certainty, is that the gases will remain segregated, but experience tells us that the intermingling of the gases is all but certain. Furthermore, once the gases are homogeneously distributed across the box, they will (almost certainly) not re-segregate without outside interference. This is the gist of physical entropy. Another analogy is that domestic spaces tend to get messier unless someone is making a conscious effort to clean up. These scenarios superficially adhere to the second law of thermodynamics, which is (roughly) that the entropy of an isolated system is either constant or increasing.

The mathematical concept of entropy builds on this notion.

Definition 13 (Entropy of a partition)**.** . First, we define the entropy of a partition. Let $(X, \mathfrak{A}, \mu)$ be a probability space. Suppose $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ is a *partition* of X, which is to say, a finite collection of essentially disjoint measurable sets, such that $\bigcup_{i \leq m} A_i = X \mod 0$. Furthermore, let $\mu(A_i) = p_i$ for each i. The *entropy* of $\mathcal{A}$ is

$$H_\mu(\mathcal{A}) = \sum_{i=1}^{m} p_i \log \frac{1}{p_i},$$

with log typically taken with base 2 or e. Fittingly enough, entropy as defined here can never take negative values.

We can think of a partition $\mathcal{A}$ of X as a set of mutually exclusive, exhaustive probabilistic events: an experiment with m distinct outcomes. In this framework, $H(\mathcal{A})$ represents the amount of uncertainty associated with the experiment, or perhaps the amount of new information to be gained from conducting the experiment. For instance, the entropy of the trivial partition $H(\{X\} = 1 \cdot \log 1 = 0$, which matches our expectation that an experiment with certain (just one) outcome can tell us nothing new. On the other hand, $H(\mathcal{A})$ is maximized when the probability of each event $p_i = 1/m$: an experiment of m equally likely outcomes is an uncertain thing.

We can extend this measurement of uncertainty to sample sets that change over time. As with our analogy for ergodicity, we might imagine again that X is a phase-space evolving under a transformation T. As the transformation progresses, the likelihood of experimental outcomes (i.e., the measures of sets in a partition of X) may change over time with more or less certainty. Hence we can speak of the entropy of the transformation itself.

Definition 14 (Entropy of a Transformation)**.** First, we denote the *refinement* of two partitions, $\mathcal{A}$ and $\mathcal{B}$, as

$$\mathcal{A} \vee \mathcal{B} = \{A \cap B : \, A \in \mathcal{A}, B \in \mathcal{B}\}.$$

Let (X, μ, T) be a transformation T on a space X equipped with measure μ. The entropy of this triple is

$$h_\mu(T) = \sup_{\mathcal{A}} \lim_{n \to \infty} \frac{H_\mu(\mathcal{A} \vee T^{-1}\mathcal{A} \vee \ldots \vee T^{-(n-1)}\mathcal{A})}{n},$$

where the supremum is taken with respect to finite partitions $\mathcal{A}$ of X, the vast number of which makes this definition unwieldy in practice. But suppose that $\mathcal{A}$ is a *generating partition* for T. That is, its orbit

$$\bigcup_{k=-\infty}^{\infty} T^k(\mathcal{A})$$

generates the σ-algebra associated with μ. Then

$$h_\mu(T) = h_\mu(T, \mathcal{A}) := \lim_{n\to\infty} \frac{H_\mu(\mathcal{A} \vee T^{-1}\mathcal{A} \vee \ldots \vee T^{-(n-1)}\mathcal{A})}{n}.$$

To see these definitions applied, we'll calculate entropy for circle rotations and circle expansions (assuming Lebesgue measure). Notably, we know *a priori* that the former is a predictable system, and the latter a rather unpredictable in the following sense. Thinking in terms binary expansions, let $x \in \mathbb{T}$ and let $\mathcal{A} = \{[0, 0.1), [0.1, 1)]\}$ partition $\mathbb{T}$, identified with $[0, 1)$. Let $\chi : [0, 1) \to \{0, 1\}$ be the indicator function for $[0.1, 1)$. Observe that $\chi(x)$ returns the first digit of the expansion of x. We consider the sequence

$$\ldots \chi(T^{-2}(x)), \chi(T^{-1}(x)), \chi(T^0(x)), \chi(T^1(x)), \chi(T^2(x)), \ldots,$$

where T stands for some transformation of the circle.

First, let T be $R_{\sqrt{17}}$. As $\sqrt{17} \approx 1/60$, we would expect the above sequence to consist of alternating strings of 30 0's and 30 1's: a point x spends about 30 iterations of $R_{\sqrt{17}}$ in each half of the partition. So if $\chi(R^{-1}_{\sqrt{17}}(x) = 0$ and $\chi(x) = 1$, we can say for certain that $\chi(R^k_{\sqrt{17}}(x)) = 1$ for $1 \leq k \leq 25$. And if we are given more 'data points', that is, the evaluation of $\chi(R^{-n}_{\sqrt{17}})$ for, say, $1 \leq n \leq 1000$, we can predict the forward orbit of x under $R_{\sqrt{17}}$ with extreme precision. We expect,

as n goes to infinity, that we can analyze the system's behavior with certainty, an expectation that matches the fact (that we shall prove below) that $R_{\sqrt{17}}$ has an entropy of zero.

However, if T stands for E_2, the picture gets more complicated. We've seen that points of the circle can show rather erratic behavior under expansion mappings. A point's orbit under E_2 is determined to the extent that its binary expansion is known. Given that E_2 corresponds to a left-shift on binary numbers, we see that

$$\chi(E_2^{-1000}(x)), \chi(E_2^{-999}(x)), \ldots \chi(E_2^{-1}(x))$$

is a sequence of the first 1000 digits of the binary expansion of x, which tells us next to nothing about the 1001st digit, $\chi(x)$! This is because almost every number is *normal*, which means that it has a random distribution of digits in any base. Thus, even with a great amount of prior information, E_2 is unpredictable, at least with respect to this partition. Different points might have a similar future trajectory, and two points that coincide in an observable past may diverge. This observation agrees with the fact that E_2 has positive entropy.

Theorem 25. *The (Lebesgue) entropy of R_α is 0 for all α.*

Proof. In the case where α is a rational p/q, first note that if $n \geq q$, then for any partition $\mathcal{A}$ of $\mathbb{T}$,

$$(\mathcal{A} \vee T^{-1}\mathcal{A} \vee \ldots \vee T^{-(n-1)}\mathcal{A}) = (\mathcal{A} \vee T^{-1}\mathcal{A} \vee \ldots \vee T^{-(q-1)}\mathcal{A}),$$

for $R_{p/q}$ is periodic with period q. Presumably $H(\mathcal{A} \vee T^{-1}\mathcal{A} \vee \ldots \vee T^{-(q-1)}\mathcal{A})$ is

a bounded quantity, δ. Then

$$h_\lambda(R_{p/q}) = \sup_{\mathcal{A}} \lim_{n\to\infty} \frac{\delta}{n} = \sup_{\mathcal{A}} 0 = 0.$$

Suppose next that $\alpha \in \mathbb{R} \setminus \mathbb{I}$. Let I be a proper, non-empty arc of the circle, and let $\mathcal{A} = \{I, \mathbb{T} \setminus I\}$. For any partition $\mathcal{B}$, $|\mathcal{A} \vee \mathcal{B}| \leq |\mathcal{A}| + |\mathcal{B}| = 2 + |\mathcal{B}|$. Furthermore, R_α preserves the cardinality of a partition. Hence

$$|\mathcal{A} \vee R_\alpha^{-1}(\mathcal{A}) \vee R_\alpha^{-2}(\mathcal{A}) \vee \ldots \vee R_\alpha^{-(n-1)}(\mathcal{A})| \leq 2n.$$

Recalling that the upper bound on the entropy of a partition of m constituent sets is when each set has measure $1/m$,, we find that

$$H_\lambda(\mathcal{A} \vee R_\alpha^{-1}(\mathcal{A}) \vee R_\alpha^{-2}(\mathcal{A}) \vee \ldots \vee R_\alpha^{-(n-1)}(\mathcal{A})) \leq \sum_{i=1}^{2k} \frac{1}{2k} \log(2k) = \log(2k).$$

If $\mathcal{A}$ is a generating partition, then

$$h_\lambda(R_\alpha, \mathcal{A}) = \lim_{k\to\infty} \frac{log(2k)}{k} = 0.$$

To see that $\mathcal{A}$ is indeed a generating partition of $\mathbb{T}$, let $I = [a, b]$. The orbits of a and b are λ-dense $\mathbb{T}$ because α is irrational, so $\mathcal{A}$ is a collection of disjoint intervals whose endpoints are a dense set, generating the standard Lebesgue sigma algebra: a generating partition. □

Theorem 26. *The (Lebesgue) entropy of E_2 is* $\log 2$.

Proof. Let $\mathcal{A} = \{[0, 1/2), [1/2, 1)\}$. Then

$$\mathcal{A} \vee T^{-1}\mathcal{A} \vee \ldots \vee T^{-(n-1)}\mathcal{A} = \{K_{j_1,\ldots,j_n} : (j_i)_1^n \in \{0, 1\}^n\},$$

which is the set of connected binary cylinders of length n, each of which has measure 2^{-n}. Then

$$h_\lambda(E_2, \mathcal{A}) = \lim_{n\to\infty} \frac{2^n \cdot (2^{-n} \log 2^n)}{n} = \frac{\log 2^n}{n} = \log 2.$$

The backward orbit $\bigcup_{i=1}^{k} E_2^{-k}(\mathcal{A})$ gives us 2^k disjoint half-open intervals each of length 2^{-n}: it's clear that the limit as k goes to infinity of this orbit gives us a collection of intervals whose endpoints are λ-dense. Then $\mathcal{A}$ is a generating partition, so $h_\lambda(T) = \log 2$. □

Chapter 4

The Littlewood conjecture and homogeneous dynamics

4.1 Reformulating the Littlewood Conjecture

We now return to the statement of the Littlewood Conjecture. We have reason to believe that

$$\liminf_{n\to\infty} n\|n\alpha\|\|n\beta\| = 0,$$

for all $\alpha, \beta \in \mathbb{R}$. The aim of this chapter is to contextualize and outline the 2006 theorem of Einsiedler, Katok, and Lindenstrauss, who proved that the LC's set of exceptions in $\mathbb{R}^2$ has Hausdorff dimension zero, which, we will see, improves considerably on the standing knowledge that the exceptions lie in a zero measure set. Their primary theorem entails a great deal of abstraction: rather than proving anything that recognizably pertains to classical Diophantine approximation, EKL (following Margulis) reframe the problem as a classification of measures on *spaces of lattices* that are invariant with respect to *diagonal* action. In this section and

the next, we will summarize how EKL reformulated the LC, a number theoretic problem, in terms of *homogeneous dynamics.*

We can think of a homogeneous space as one that looks the same when viewed from any local perspective: the surface of a sphere is homogeneous, but the surface of a cube is not. Formally, for any two points $x, y \in X$, a homogeneous space, there exists a *symmetry* g on X such that $gx = y$. The set of all symmetries of a space X form a group G that acts on X, acting *transitively* precisely when X is homogeneous. Homogeneous spaces are relatively nice objects to study because they afford dual characterizations, a geometric one (X) and an algebraic one (G modulo some stabilizing subgroup) each with useful structure.

The LC as it is usually written appears to be an analytic problem, but it's also a disguised Diophantine inequality: the LC holds if and only if the expression

$$|n(n\alpha - m)(n\beta - l)| < \varepsilon$$

is solvable for all $\varepsilon > 0$, with $(n, m, l) \in \mathbb{Z}^3$ and $n \neq 0$. (Without loss of generality, we can restrict our attention to $\alpha, \beta \mod 1$.) The lefthand side of the inequality is the product of three linear forms in $\mathbb{R}^3$, $P(\vec{x}) = P(x_1, x_2, x_3) = x_1(\alpha x_1 - x_2)(\beta x_1 - x_3)$. (Henceforth, we will sometimes refer to P as 'the Littlewood form.') We observe that, for a $\vec{x} \in \mathbb{R}^3$, when $|\vec{x}|$ is small, then $|P(\vec{x})|$ is small as well. Yet if we restrict our attention to integral vectors, with the first coordinate nonzero, the shortest one is $(1, 0, 0)$, at which P evaluates to $\alpha\beta$, which is not particularly small. The previous observation seems unhelpful, at least until we broaden our search.

Let a be an automorphism of $\mathbb{R}^3$ that preserves P. If $a\vec{x}$ is small, then $P(a\vec{x}) = P(\vec{x})$ is small as well. It turns out that $\mathrm{Aut}(P)$ (the 'symmetry' group of P) is

quite large, so this new approach gives us more to work with: to solve the LC, we now want to find an automorphism P that shrinks integral vectors. To be precise about what we mean by 'small,' for any linear transformation $f \in \mathrm{GL}(3,\mathbb{R})$ of $\mathbb{R}^3$, let $\delta(f.[\mathbb{Z}^3])$ denote the *least* length of the set of non-zero integral vectors transformed by f. (In the next section, we will see why we put $\mathbb{Z}^3$ in square braces.)

Thus if for any $\varepsilon > 0$, there exists an $a \in \mathrm{Aut}(P)$ such that

$$\delta(a.[\mathbb{Z}^3]) < \varepsilon,$$

we might expect the Littlewood conjecture to hold. But a pitfall remains: there is no guarantee that the shortest vector $\vec{x}$ generated by $a.[\mathbb{Z}^3]$ has a non-zero x_1 component.

We can circumvent this difficulty in the following way: we define the linear transformation $h_{\alpha\beta}$ as that which maps

$$(x_1, x_2, x_3) \mapsto (x_1, \alpha x_1 + x_2, \beta x_1 + x_3).$$

This transformation is a change in coordinates; it's a function of the initial choice of α and β, but for convenience's sake we will abbreviate it to h. We find that

$$P(h\vec{x}) = x_1(\alpha x_1 - (\alpha x_1 + x_2))(\beta x_1 - (\beta x_1 + x_3)) = x_1 x_2 x_3 =: Q(\vec{x}),$$

the latter being a variety on $\mathbb{R}^3$ that is simpler to work with than P. It follows that $\mathrm{Aut}(P) = h\mathrm{Aut}(Q)h^{-1}$. Observe that $\mathrm{Aut}(Q)$ contains the group of diagonal matrices of determinant one, which we call A_3. Note that A_3 is a subgroup of $\mathrm{SL}(3,\mathbb{R})$: we see that for $g \in A_3$, if $g(\vec{x}) = (y_1, y_2, y_3)$, then $Q(g\vec{x}) = y_1 y_2 y_3 =$

$\det(g) = 1$.

In fact, every element of $\mathrm{Aut}(Q)$ is basically some $g \in A_3$, discounting the 6 possible permutations of coordinates x_1, x_2, x_3, and $\mathrm{Aut}(P) = h\mathrm{Aut}(Q)h^{-1}$. So (ignoring permutations) every $a \in \mathrm{Aut}(P)$ is of the form hgh^{-1} for an appropriate $g \in A_3$. We can infer that $\delta(a.[\mathbb{Z}^3]) = \delta(hgh^{-1}.[\mathbb{Z}^3])$ may be made arbitrarily small by some clever choice of g. (Certainly $\delta(g.[\mathbb{Z}^3])$ is no greater than the magnitude of the smallest diagonal entry of g.) We can simplify this approach by narrowing our search field. We define a semi-subgroup of $\mathrm{Aut}(Q)$ as follows:

$$A_3^+ := \left\{ \begin{pmatrix} x & 0 & 0 \\ 0 & y & 0 \\ 0 & 0 & z \end{pmatrix} : xyz = 1, x \leq 1, y, z \geq 1 \right\}.$$

Proposition 1. *The Littlewood Conjecture is implied by the following statement: For all $\varepsilon > 0$, there exists some $g \in A_3^+$ such that*

$$\delta(gh^{-1}.[\mathbb{Z}^3]) < \varepsilon.$$

Proof. The above implies that for arbitrarily small ε, there are a $g \in A_3^+$ and an integral vector $\vec{x}$ such that$|gh^{-1}\vec{x}| < \varepsilon$. The x_1 component of $gh^{-1}\vec{x}$ is certainly no more than ε. Recalling that the transformation h is a translation along the second and third coordinates in proportion to the length of the first, we conclude that h translates $gh^{-1}\vec{x}$ by a distance no greater than

$$\sqrt{(\varepsilon\alpha)^2 + (\varepsilon\beta)^2} = \varepsilon\sqrt{\alpha + \beta}.$$

Therefore $|ghg^{-1}\vec{x}| \leq \varepsilon\sqrt{\alpha + \beta} + \varepsilon$: this is a bound that goes to 0 as ε goes to 0.

So $\delta(hgh^{-1}\mathbb{Z}^3)$ can be made arbitrarily small. Now hgh^{-1} is an automorphism of P, meaning that for some $\vec{x} \in \mathbb{Z}^3$, $P(\vec{x}) < \varepsilon$.

We must confirm that the x_1 component of $\vec{x}$ is non-zero. Let $\vec{y} = (0, m, n)$ be a (non-zero) vector in $\mathbb{Z}^3$. Observe that, for all $g \in A_3^+$, $gh^{-1}\vec{y} = g\vec{y} = (0, ym, zn)$, for some $y, z \geq 1$. The length of $\vec{y}$ is at least 1, so the length of $g\vec{y}$ is greater than 1. We see that if the x_1 component of an integer vector is zero, then the transformation induced by gh^{-1} in fact *increases* its length. So our assumption that $\delta(hg^{-}1\mathbb{Z}^3)$ gets arbitrarily small presupposes that the x_1 component of the least non-zero integral vector is itself non-zero. We conclude that if, for all $\varepsilon > 0$, there exists an $h \in A_3^+$ such that $\delta(gh^{-1}\mathbb{Z}^3) < \varepsilon$, then there exists an integral solution to $P(\vec{x}) < \varepsilon$, with $x_1 \neq 0$, thus implying the validity of the LC. □

The δ-notation used above is rather clunky because it refers to the length of some transformed integer vector, which we know nothing about explicitly. In the next chapter, we will see that we can condense the information pertaining to $\mathbb{Z}^3$ mapped under a linear transformation, which is a countably infinite collection of vectors, into a single object, a *lattice*.

4.2 The Space of Lattices

A lattice of dimension n is the image of $\mathbb{Z}^n$ under a linear transformation of $\mathbb{R}^n$; it's the set of integral combinations of a basis of $\mathbb{R}^n$, or a 'grid' containing the origin. A *unimodular lattice* $\lambda \in \mathcal{L}_n$ has a covolume of one, which is to say that the parallelepiped formed by its generating vectors (in algebraic terms, its 'fundamental domain') has volume one. We will see that we can think of $\mathcal{L}_n$ as the 'space' of unimodular lattices in n dimensions.

Note that there is a natural equivalence between $\mathcal{L}_n$ and the coset space $X_n =$

$\mathrm{SL}(n,\mathbb{R})/\mathrm{SL}(n,\mathbb{Z})$. (This is why we may regard $\mathcal{L}_n$ as a homogeneous space.) The set of volume-preserving linear transformations of $\mathbb{R}^n$ is simply $\mathrm{SL}(n,\mathbb{R})$, a group which defines a transitive action on $\mathcal{L}_n$. But any *integral* linear transformation $g \in \mathrm{SL}(n,\mathbb{Z})$ preserves $\mathbb{Z}^3$, so an application of the orbit-stabilizer theorem tells us that $\mathcal{L}_n$ and X_n are in bijective correspondence. Hence every unimodular n-lattice λ is of the form $g.[\mathbb{Z}^n]$ for some $g \in X^n$. This fact is useful because it explictily gives $\mathcal{L}_n$ a known algebraic and topological structure, while at the same time giving X_n a geometric interpretation. For instance...

Theorem 27 (Mahler's Compactness Criterion)**.** *We define* $\mathcal{L}_n(\varepsilon) := \{\lambda \in \mathcal{L}_n : \delta(\lambda) \geq \varepsilon\}$, *that is, the set of lattices that do not intersect an open* ε*-ball about the origin. A subset* $K \subseteq \mathcal{L}_n$ *has compact closure (is precompact) if and only if for some* $\varepsilon > 0$, $K \subseteq \mathcal{L}_n(\varepsilon)$ *([ME11]).*

Perhaps we can intuitively see that a sequence of unimodular lattices whose δ values approach zero 'degenerates' in a sense: as one dimension of the lattice's fundamental domain gets extremely small, the others get near-infinitely large. This is a sequence with no obvious limit point. In the two-dimensional case, we can imagine a sequence of parallelograms of area one that stretch out into something resembling a line.

With the compactness criterion in mind, we can actually restate the preceding restatement of the LC in dynamical terms. If we recast the modified diagonal group A^{3+} as a *flow* with two parameters, establishing that $\{gh_{\alpha,\beta}^{-1}.[\mathbb{Z}^n] : g \in A^{3+}\}$ is unbounded in $\mathcal{L}_n$ would be sufficient to prove the LC.

We first remarked in the introduction that the one-dimensional variant of the LC is false due to the existence of (infinitely many) badly-approximable numbers.

That is,

$$\liminf_{n\to\infty} n\|\alpha n\| > 0$$

whenever α is badly-approximable. As with the Littlewood conjecture, we can express this statement in terms of dynamics on the space of lattices. The one-variable Littlewood problem seeks to minimize the magnitude $|a-n\alpha|$ over integer pairs (a,n). Letting

$$h_\alpha := \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix},$$

we seek (a,n) such that

$$h_\alpha \begin{pmatrix} a \\ n \end{pmatrix} = \begin{pmatrix} a-n\alpha \\ n \end{pmatrix}$$

is close to the y-axis of $\mathbb{R}^2$. This formulation leads us to the simplest case of an elegant correspondence between lattice-dynamics and Diophantine approximation, proved in 1985 ([Kle98]) by S. Dani for unimodular lattice spaces of all finite dimension. First, we define an orbit on the point $\Gamma := \mathrm{SL}(2,\mathbb{Z}) \in X_2$ (corresponding to $[\mathbb{Z}^2] \in \mathcal{L}_2$) as follows. For $t \in \mathbb{R}^+$, let

$$g_t := \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix},$$

and let

$$\mathcal{O}_\alpha := \{g_t h_\alpha \Gamma\}_{t\geq 0}\,.$$

Theorem 28 (Dani's Correspondence Lite)**.** *$\alpha \in \mathbb{R}$ is badly-approximable if and only if $\mathcal{O}_\alpha$ is bounded in $SL(2,\mathbb{R})$.*

Proof. First, suppose that α is badly-approximable. Then for some $c > 0$, $n|n\alpha - a| \geq c$ for all integer pairs (a, n) with $n \neq 0$. Note that c is the area of the rectangle bounded by the vectors $(a - n\alpha, 0), (0, n)$. The set of $\{g_t\}_{t\in\mathbb{R}^+}$ defines an area-preserving flow because each g_t has determinant 1. Let $\lambda_t \in \mathcal{O}_\alpha$ be the state of the flow at time t. A rectangle (one corner on a point in the lattice, two sides on the x and y-axes) in λ_t has an area of at least c. Its far corner does not lie inside the square of area c placed at the origin, so $\lambda_t \in \mathcal{L}_2(\sqrt{2c})$, which implies its precompactness by Mahler's criterion. Thus $\mathcal{O}_\alpha$, the closure of the set of all λ_t, is bounded.

Conversely, suppose $\mathcal{O}_\alpha$ is bounded. Then for some ε, for every $\lambda_t \in \mathcal{O}_\alpha$, $\lambda_t \in \mathcal{L}_2(\varepsilon)$. Thus a rectangle in λ_t must have an area of at least $\varepsilon^2/2$. Every $x \in g_\alpha\Gamma$ is of the form $(a - n\alpha, n)$, for pair of integers (a, n) Assuming n to be positive, we have that $n|a-n\alpha| \geq \varepsilon^2/2$, proving that α is badly-approximable. □

Dani's correspondence theorem indicates that, in the case of the 1-parameter diagonal matrix flow, A_2 acting on $\mathcal{L}_2$, there exist infinitely many bounded orbits, corresponding to badly-approximable numbers. However, as we have seen in the preceding chapter, the Littlewood conjecture is logically equivalent to a conjecture that there are no bounded orbits of A_3^+ (almost a higher-dimensional version of A_2) acting on $\mathcal{L}_3$. Why should we expect the three-dimensional system, the 'trickier' of the two, to behave with more rigidity?

4.3 *Hyperbolic Isometries and Lattices*

[Note: this section is only marginally related to the rest of the chapter but is fascinating in its own right. I present it because it gives the 'flavor' of some of the deeper results in homogeneous dynamics while remaining easy to understand.]

Recall that a *Möbius transformation* (or *linear fractional transformation* is a function $f : \mathbb{C} \to \mathbb{C}$ of the form

$$f(z) = \frac{az + b}{cz + d}$$

with $ad - bc \neq 0$. If we restrict our focus to linear fractional transformations (LFTs) with real coefficients for which $ad - bc = 1$, we get an obvious bijection between those maps and $\mathrm{SL}(2, \mathbb{R})$; as such, it is common practice to represent LFTs in matrix form. We will see that $\mathrm{SL}(2, \mathbb{R})$ has a group action on a special subset of $\mathbb{C}$, defined as

$$M \cdot z \mapsto \frac{az + b}{cz + d},$$

where

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{R}).$$

For convenience's sake, we will often say that a LFT $f \in \mathrm{SL}(2, \mathbb{R})$, but bear in mind that the way it acts on complex numbers is via the Möbius transformation, *not* matrix multiplication.

Proposition 2. *Let f be a Möbius transformation with real coefficients such that $ad - bc = 1$. Then f maps the upper-half complex plane, $\mathbb{H} := \{x + iy : y > 0\}$, to itself. Thus $SL(2, \mathbb{R})$ gives a group action on $\mathbb{H}$.*

Proof. For $z \in \mathbb{C}$, let $\Im(z)$ denote its imaginary component. Suppose that $\Im(z) > 0$, which is equivalent to z lying in $\mathbb{H}$. Let $f \in SL(2, \mathbb{R})$ define an LFT. Then

$$f(z) = \frac{az + b}{cz + d} = \frac{(az + b)(c\bar{z} + d)}{|cz + d|^2}.$$

We know that $z \neq -d/c$ since the latter lies in $\mathbb{R}$, the boundary of $\mathbb{H}$. So $f(z)$ is a defined fraction with an entirely real denominator. The only contribution to $\Im(f(z))$ comes from $bc\bar{z} + daz$. Letting $z = x + iy$ for $x, y \in \mathbb{R}$, we find that $\Im(bc\bar{z} + daz) = bc(-y) + ad(y) = (ad - bc)y$. Since $ad - bc = 1$, we have that $\Im(f(z)) = y = \Im(z)$, which, by our initial supposition, is greater than zero. $\square$

The space $\mathbb{H}$ is often called the 'hyperbolic' plane: in Poincaré's plane model of a hyperbolic surface (i.e., one with constant negative curvature), the associated Riemannian metric scales distances down as one travels up on $\mathbb{H}$ and increases them as one approaches the boundary of $\mathbb{H}$, which is to say $\mathbb{R}$. As we shall see, this metric induces a non-Euclidean geometry in which the equivalent of Euclid's fifth, 'parallel' axiom fails to hold. It turns out (see [ME11]) that Möbius transformations corresponding to $SL(2, R)$ are, remarkably, both conformal (locally angle-preserving) and hyperbolically isometric.

Under the above action, the matrix

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

acts trivially on $\mathbb{H}$. For this reason we often consider instead the *projective* special linear group, $\mathrm{PSL}(2, \mathbb{R}) = \mathrm{SL}(2, \mathbb{R})/\{\pm I_2\}$, which acts transitively upon $\mathbb{H}$: fixing a reference point in the upper half-plane—i is the logical choice—for each $z \in \mathbb{H}$, there exists a Möbius transformation $f \in \mathrm{PSL}(2, \mathbb{R})$ such that $f(i) \mapsto z$. Infinitely many of them, actually: it is easy to verify that the stabilizer of i under this

action is the set of 'rotational' linear transformations, viz. matrices of the form

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

with $\theta \in \mathbb{R}$ corresponding to the angle of rotation. This set of matrices is also known as the special orthogonal group in two dimensions, SO(2).

Proposition 3. *The stabilizing group of the LFT-orbit of $i \in \mathbb{H}$ is the set of transformations coming from $SO(2)$. Furthermore, the action of $PSL(2,\mathbb{R})$ on $\mathbb{H}$ is transitive. Therefore, by the orbit stabilizer theorem, we have a set bijection*

$$\mathbb{H} \cong SL(2,\mathbb{R})/SO(2).$$

(Because $\{\pm I_2\} \in SO(2)$, we can drop the requirement of dealing with projective groups.)

Proof. First, let $f \in \mathrm{PSL}(2,\mathbb{R})$ and suppose that $f \cdot i = i$. Then, for the corresponding entries of f,

$$\frac{ai+b}{ci+d} = i,$$

which implies that

$$ai + b = -c + di.$$

Clearly $a = d$ and $b = -c$. Given that $ad - bc = 1$, we have that $a^2 + b^2 = 1$, so for some $\theta \in [0, 2\pi)$, $a = \cos(\theta)$ and $b = \sin(\theta)$. Thus $f \in \mathrm{SO}(2)$. Conversely, a straightforward but tedious calculation shows that transformations deriving from SO(2) map i to i.

It remains to show that the action of $\mathrm{SL}(2,\mathbb{R})$ of $\mathbb{H}$ is transitive. Let $z =$

$x + iy \in \mathbb{H}$. Consider the following Möbius transformation:

$$f = \begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & 1/\sqrt{y} \end{pmatrix}.$$

Note that $\det(f) = 1$ and that

$$f(i) \mapsto \frac{\sqrt{y}i + \frac{x}{\sqrt{y}}}{\frac{1}{\sqrt{y}}} = x + iy,$$

showing that $\mathrm{SL}(2, \mathbb{R})$ has transitive action. (In fact, we can find an element of the group mapping z to w for any $z, w \in \mathbb{H}$. Suppose that for $A, B \in \mathrm{SL}(2, \mathbb{R})$ we have $A(i) \mapsto z$ and $B(i) \mapsto w$. Then $A^{-1}B(z) \mapsto w$.) □

We can deduce a similar identification between $\mathrm{SL}(2, \mathbb{R})$ and the *unit tangent bundle* of the upper-half plane, $T^1\mathbb{H}$. The unit tangent bundle of $\mathbb{H}$ is a *twofer* space (my own terminology) comprising points of $\mathbb{H}$ each paired with some complex vector of unit length: letting C denote the boundary of the unit disc, we see that $T^1\mathbb{H} = \mathbb{H} \times C$. One might also think of the space as the collection of derivatives of curves (of normalized speed) passing through each $z \in \mathbb{H}$. When acting on $T^1\mathbb{H}$, $\mathrm{SL}(2, \mathbb{R})$ does the usual thing to $\mathbb{H}$, and performs the *derivative action* on $\mathbb{C}$: namely, mapping the associated Möbius transformation down to its derivative.

To wit, let $(z, v) \in T^1\mathbb{H}$. Then, for $f \in \mathrm{SL}(2, \mathbb{R})$, we define the derivative action as

$$\mathrm{D}f(z, v) \mapsto (\frac{az + b}{cz + d}, \frac{v}{(cz + d)^2}),$$

a fact we obtain from applying the quotient rule to f viewed as a complex-differentiable function of z. Given that any $f \in \mathrm{SL}(2, \mathbb{R})$ is a hyperbolic isometry,

the ensuing derivative vector $v/(cz+d)^2$ has (hyperbolic) length 1 if v has length one. Hence $\mathrm{PSL}(2,\mathbb{R})$ gives a well-defined action on $T^1\mathbb{H}$, and this action is 'free': for every $(z,v),(w,u) \in T^1\mathbb{H}$ there is a unique element that maps the former to the latter. Perhaps the easiest understanding of this is that $\mathrm{SO}(2)$, which stabilized elements of $\mathbb{H}$, is the natural symmetry group of C. If we do not mod out $\mathrm{SL}(2,\mathbb{R})$ by it, we regain a sense of 'directionality' that, along with position, uniquely defines a point in $T^1\mathbb{H}$. A remarkable conclusion we can draw from this discussion is that the space of unimodular two-dimensional lattices is isomorphic to two copies of the unit tangent bundle of the hyperbolic plane. And just as we chose i to be the representative element of $\mathbb{H}$, (every point $z \in \mathbb{H}$ is identified with the unique linear transformation in $\mathrm{SL}(2,\mathbb{R})/\mathrm{SO}(2)$ mapping i to z) we pick a new representative element of $T^1\mathbb{H}$: i paired with the upwards-pointing unit vector, or (i,i).

In a geometric space, *geodesics* refer, roughly speaking, to locally distance-minimizing curves. They can be uniquely determined by specifying that they pass either through two points or through one point along a certain direction. In ordinary Euclidean space, geodesics are simply straight lines. In global navigation, these are called 'great circles' or, occasionally, 'ortrodromes,' and though they appear to be curved lines on most flat projections of the globe's surface, actual travel along a great global circle would appear to an observer as movement in a straight line. In our planar model of hyperbolic geometry, geodesics look like lines or circles that intersect the boundary $\mathbb{R}$ orthogonally, but, similarly, they look like straight paths locally.

The matrices of $SL(2,\mathbb{R})$ that correspond to geodesics are the group of diagonal matrices, A_2 (!) and its conjugate copies. We can see a basic illustration of this fact if we consider how a familiar one-parameter matrix group acts on i. We define

the *geodesic flow* as follows:

$$\{\gamma\}_{t\in\mathbb{R}} := \left\{ \begin{pmatrix} e^{t/2} & 0 \\ 0 & e^{-t/2} \end{pmatrix} \right\}_{t\in\mathbb{R}}.$$

Observe that $\gamma_t \cdot i \mapsto e^t i$, and so the orbit $\{\gamma_t \cdot i\}_{t\in\mathbb{R}}$ parametrizes a path along the imaginary axis of $\mathbb{H}$. Since the hyperbolic metric scales down local distance for z with $\Im(z) > 1$ and increases it for $\Im(z) < 1$, it is that this 'exponentially accelerating' path moves at unit speed in $\mathbb{H}$.

Now let z_0, z_1 be any two points in H. We know that for some $f \in SL(2,\mathbb{R})$, $f(z_0) = i$. We don't know anything in particular about $f(z_1)$, but can infer that for some rotation $g \in \mathrm{SO}(2)$, $f(z_0) = i$ is stabilized, but $f(z_1)$ is rotated to a congruent vector lying on the imaginary axis. (A compelling analogy for the action of $\mathrm{SO}(2)$ on $\mathbb{H}$ is that i is like the center of a bizarre clock, and allowing a hand of the clock to extend from i to $z \in \mathbb{H}$, an element of $\mathrm{SO}(2)$ rotates the hand while preserving its hyperbolic length.) So the points $g \circ f(z_0) = i$ and $g \circ f(z_1) = y_1 i$ (for some $y_1 \in \mathbb{R}$) both lie on the imaginary axis. Then the flow $\{\gamma\}_{t\in[0,ln(y_1)]}$ parametrizes a path from i to $y_1 i$, which being a geodesic, is the shortest path possible. Thus the unique geodesic segment l running between z_0 and z_1 is given by

$$l = f^{-1}g^{-1}\{\gamma\}_{t\in[0,ln(y_1)]}gf.$$

The preceding discussion has afforded us another geometric interpretation of the space of 2-D lattices: it's a quotient of $T^1\mathbb{H} = \mathrm{SL}(2,\mathbb{R})$ by a certain discrete, 'spanning' subgroup, $\mathrm{SL}(2,\mathbb{Z})$, or X_2 (following the notation introduced in Section 4.2). In fact, the *quotient space* X_2 is a fundamental domain of $\mathrm{SL}(2,\mathbb{Z})$ acting on $\mathbb{H}$: for every $z \in \mathbb{H}$, there is a unique $f \in \mathrm{SL}(2,\mathbb{Z})$ such that z lies in the

coset $f \cdot X_2$. (The easiest analogy is to compare $\mathbb{T} = [0,1)/\sim$ as a fundamental domain for $\mathbb{Z}$ acting on $\mathbb{R}$.) When equipped with the hyperbolic metric, X_2, also known as the *modular surface*, is a locally-compact space of finite volume. One can visualize the modular surface as the surface of a teardrop whose narrowing cusp (corresponding to the area bordering $\mathbb{R}$ in $\mathbb{H}$) extends off to infinity. Compact (in the 'lattice' sense associated with MCC) subsets of the modular surface have boundaries that terminate somewhere along the cusp.

We will mention the *horocyclic flow*, which is in many ways the natural counterpart to the geodesic flow. Whereas geodesics are 'longitudinal' curves, the set of vertical lines and circles that approach the real line orthogonally, horocycles are lines of 'latitude': horizontal lines and circles that lie tangent to $\mathbb{R}$. A horocyclic flow has a conventional group parameterization:

$$\{\eta\}_{t\in\mathbb{R}} := \left\{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \right\}_{t\in\mathbb{R}}.$$

Observe that $\eta_t \cdot i \mapsto z + t$, so the orbit $\{\eta_t \cdot i\}_{i\in\mathbb{R}}$ gives a horizontal line passing through i.

Now recall that in the 2-D Dani correspondence, we began with a matrix,

$$h_\alpha = \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix}$$

multiplying integer vectors (a, n), which was itself multiplied on the left by a set of diagonal matrices belonging to the geodesic flow. We can interpret the Dani correspondence as a theorem concerning the boundedness of geodesic flows, adjusted by certain horocyclic shifts, on the modular surface. Recall that, under

ordinary matrix multiplication, $h_\alpha \cdot (a, n) = (a - n\alpha, n)$. Since the geodesic flow acts not on points in $T^1\mathbb{H}$ but rather their 'representative' linear transformations (namely, the ones mapping them to the reference point (i, i),) we find the consider the γ_t-orbit of the unique $f \in \mathrm{PSL}(2, \mathbb{R})$ associated with $(a - n\alpha, n)$. The Dani Correspondence tells us that the orbit of this f is bounded if and only if α is badly-approximable. When we turn to the modular surface, badly-approximable α give rise to γ_t-orbits that rise no higher than a certain point along the cusp of X_2, meaning that their closures are bounded sets. Remarkably, it can be seen ([Kle98]) that the maximum height attained by such flows corresponds to the magnitude of the largest denominator of convergents of the continued fraction expansion of α. It's worth remembering that the convergents of badly-approximable numbers are bounded.

4.4 Invariant Measures, Orbit Closures, and Rigidity Revisted

We have translated the LC into a problem of determining the (un)boundedness of orbits of points of the form $h_{\alpha,gb}.[\mathbb{Z}^n]$. Superficially, this conversion into a dynamical problem may seem pointless, but we may now draw upon the methodologies of related problems in dynamics. In general, dynamicists often prove things about the overall 'rigidity' of a system, which in turn informs our knowledge of the properties of individual points.

Suppose we were able to give a complete classification of every minimal, closed, A_3-invariant subset $C \subset \mathcal{L}_n$. As the closure of every $h_{\alpha,gb}.[\mathbb{Z}^n]$-orbit is such a C, with luck we might be able to prove that no such orbit is bounded. In his proof

of the Oppenheim Conjecture, which was a landmark application of dynamics to number theory, Margulis used this essentially 'topological' method. His approach (the first instance of a class of theorems codified by M. Ratner) does not simply recycle into a proof of the LC, largely because the Oppenheim Conjecture concerns unipotent flows whereas the dynamical approach to the LC concerns hyperbolic flows. The former behave more predictably over time.

The progress on the LC is an illustration of the heuristic that measures can be easier to work with than sets. In brief, measures on a space relate to special subsets thereof but come with a great deal more of applicable structure. For instance, *ergodic decomposition* gives a procedure for analyzing the smallest components of a measure invariant to some transformation T, whereas there is no similar method for determining the minimal subsets of a closed, T-invariant set.

In Chapter 3 we saw that a measure which is T-invariant indicates the existence of a certain T-invariant closed set: viz. the support, the maximal closed set on which a measure 'lives.' While this connection is a more tenuous one, a classification of all T-invariant ergodic measures approaches a classification of T-invariant minimal closed sets. If we had a measure classification of A_3 that implied the existence of diverse, non-rigid invariant measures, we would expect that there are diverse and non-rigid orbits. But a rigidity of measures suggests a rigidity of closed sets which suggests a rigidity of orbits. Think of this as a dogma for dynamicists; it is along these lines that the best result on the LC proceeds.

We will clarify what we mean by labelling the action of A_3 on $\mathcal{L}_3$ as hyperbolic. A dynamical system is called *hyperbolic* to indicate the presence of a transformation that expands distance between points in one direction and/or contracts in another, 'transverse' direction. Circle expansions are perhaps the simplest (quasi-)hyperbolic systems; diagonal matrix action on homogeneous lattice spaces gives

a more involved example. We will see that these two classes of systems evoke each other in interesting ways, especially regarding questions of rigidity. One first, elementary observation we can make is that the construction of $\mathbb{T}^n$ and $\mathcal{L}_n$ are quite similar: the spaces, both of which have finite volume, are the quotient of a connected topological group by a discrete, infinite subgroup: $\mathbb{R}^n/\mathbb{Z}^n$ and $\mathrm{SL}(n,\mathbb{R})/\mathrm{SL}(n,\mathbb{Z})$, respectively.

We recall that E_3 (or any circle expansion map) produces some weird orbits, in addition to everywhere-dense and periodic ones: by playing around with base 3-expansions of numbers, we found in section 3.1 that we could produce an orbit that was dense in the Cantor ternary set, a fractal. As per our (dogmatic) expectation, the diverse orbits of $(\mathbb{T}, E_3)$ correlate with a plethora of closed, invariant subsets and invariant measures.

One-parameter circle expansions compare quite nicely to one-parameter diagonal flows on the space of lattices. As the Dani correspondence shows, infinitely many orbits (corresponding to the badly-approximable numbers) of $\mathcal{L}_2$ under A_2 have bounded closure, being proper, non-discrete subsets of their space. In fact, these badly-approximable orbits are typically Cantoresque fractal sets (c.f. [Mor05]) rather than algebraically well-behaved subgroups. Hence we conclude that $(\mathcal{L}_2, A_2)$ is a non-rigid system—there are too many ergodic measures and minimal closed sets to count.

The analogy continues, albeit more tenuously, when we turn toward two-parameter problems in both system classes. Recall, from our discussion in section 3.4, that $\times 2 \times 3$ refers to the two-parameter semi-subgroup $\{2^m 3^n\}_{m,n\geq 0} \subset \mathbb{T}$. Furstenberg proved that the orbit closure $\overline{\{2^m 3^n x\}}_{m,n\geq 0}$ is either all of $\mathbb{T}$ when x is irrational or a finite set if x is not. He conjectured that the only $\times 2 \times 3$-invariant, ergodic probability measures derive from the two possible orbit types: Lebesgue

measure, or some Dirac measure supported on a finite set of rationals. Rudolph proved this measure-classification theorem under the assumption that either $\times 2$ or $\times 3$ acts with positive entropy with respect to the measure in question.

The semigroup of positive diagonal matrices A_3^+ is a two parameter flow on $\mathcal{L}_3$. Grigory Margulis conjectured (c. 2000) that a compact orbit closure $\overline{A_3 \cdot x}$ in $\mathcal{L}_3$ is of the form $H' \cdot x$ where $H' \geq A_3^+$ is a subgroup of Γ/G containing A_3^+ : in essence, any positive diagonal orbit closure has a tidy algebraic structure. In measure-theoretic terms, Margulis's conjecture posits that an A_3-invariant and ergodic probability measure on the space of unimodular lattices is 'algebraic' with respect to some H' (assigned with the properties above).

Remark (Algebraic measures). For any locally compact, Hausdorff topological group, there exists a unique probability measure that is invariant under (left) action, which gives finite measure to all compact sets. If the group itself is compact, then the associated measure is also right-invariant and is called *Haar measure.* For instance, the Haar measure on $\mathbb{R}/\mathbb{Z}$ (with a group action of either addition or multiplication) is just Lebesgue measure. Thus Furstenberg's $\times 2 \times 3$ measure classification conjecture posits that the only non-atomic invariant probability measure is 'algebraic' in the obvious sense. We also note that the special linear group, as a Lie group, is locally compact and passes down this property to its subgroups.

The 2006 theorem of Einsiedler, Katok, and Lindenstrauss, alluded to at the beginning of this chapter, evokes Rudolph's result on $\times 2 \times 3$ in terms of results, though the respective methodologies differ a great deal. One might classify both investigations as pertaining to the general question of the rigidity of higher-rank hyperbolic homogeneous actions. In full generality, their theorem is as follows:

Theorem 29 (Einsiedler-Katok-Lindenstrauss)**.** *Suppose $n \geq 3$ and let μ be an*

A_n-invariant, A_n-ergodic probability measure on $\mathcal{L}_n$ such that there exists an element of A_n acting with positive entropy. Then μ is algebraic, coinciding with the (unique) H'-invariant probability measure on a closed orbit $H'x_0$, where $x_0 \in \mathcal{L}_n$ and $A_n \leq H' \leq SL(n,\mathbb{R})$ is closed.

As $\mathrm{SL}(n,\mathbb{R})$ is a well-understood algebraic object, the above theorem almost gives a full measure classification of the system: to the extent that we know all the intermediate subgroups of $\mathrm{SL}(n,\mathbb{R})$ and A_n, we know all (positively entropic) A_n-invariant measures. Of course, if we could forgo the assumed condition of positive entropy, we would have the full measure classification of A_n on $\mathcal{L}_n$, and by extension, the full resolution of the LC.

In the case of $n = 3$, the only possible A_3^+-invariant measures are invariant on all of A_3 (because they are 'algebraic' with respect to some subgroup *containing* A_3), which precludes the existence of special bounded orbits $\{g_{s,t}h_{\alpha,\beta}x_0\}_{s,t\geq 0} \subseteq \mathcal{L}_3$. (Recall from 4.1 that $g_{s,t}$ is a two-parameter flow spanning A_3^+, and $h_{\alpha,\beta}$ is the change-of-coordinate matrix associated to the Littlewood form for irrational coefficients α, β.) We know that such bounded orbits won't exist, for if they did, then it would be possible to define an A_3^+-invariant measure that is not algebraic in the above sense. But an A_3^+-invariant measure should also be A_3-invariant: every element of A_3^+ is (up to permutation of coefficients) an element of A_n.

We can conclude that $A_3^+ h_{\alpha,\beta}.[\mathbb{Z}^3]$ is unbounded in $\mathcal{L}_3$, which implies (by MCC) that $\delta(A_3^+ h_{\alpha,gb}.[\mathbb{Z}^3]) < \varepsilon$ for all $\varepsilon > 0$, That is, one can obtain an arbitrarily small non-zero vector from the (positive) diagonal flow action on the Littlewood form. What's more, we have guaranteed that the first coordinate has positive magnitude. Knowing that diagonal matrices are automorphisms of Littlewood's form P, we find that $P(\vec{x}) < \varepsilon$ is solvable in the integers. Which is all a roundabout way to

say that

$$\liminf_{n\to\infty} n\|\alpha n\|\|\beta n\| = 0$$

for all α, β. Except that the 2006 theorem of EKL didn't prove that exactly—it was shown only that the Littlewood-exceptional set of $\alpha, \beta \in \mathbb{R}^2$ has Hausdorff dimension 0. As it turns out, this is a very strong statement, far stronger than saying that the exceptional set has zero measure (which was 'known' ever since Khinchine's theorem was published, even before the LC was posed). Consequently, we are led to believe that the above equation holds true for *even more* than almost every choice of α, β, but (perhaps) not always. But what does that actually mean?

4.5 Beyond the Zero

Motivating this final section will be the need for a refinement of Lebesgue measure, which is too crude an instrument to gauge minuscule sets: how does one distinguish between the size of two zero-measure sets? *Hausdorff dimension* provides us with a more delicate notion of size. We will arrive at this new conceptualization of dimension by first constructing a family of measures $\{\mu_d : d \geq 0\}$. These *Hausdorff measures* can be defined with respect to any subset X of a metric space M. Whenever d is an integer and $M = \mathbb{R}^d$, then μ_d coincides with Lebesgue measure. Furthermore, if X is bounded, we can assign a unique non-negative real number to X, $\dim_H(X)$, so that (i) if $d < \dim_H(X)$, then $\mu_d(X) = \infty$, and (ii) if $d > \dim_H(X)$, then $\mu_d(X) = 0$. As one might expect, this assigned threshold value is the Hausdorff dimension of X.

Before we introduce technicalities, we'll see some examples of this 'threshold' behavior playing out. First of all, Lebesgue measure only tells us something useful

about about a set when the dimension of measurement agrees with that of the set: for instance, a (2-D) disc has zero volume but infinite length (if we were to somehow roll it out into a line), for instance. But when a set has a dimension that, intuitively, must lie in between two positive integers, Lebesgue measure in general becomes problematic. These sets of 'fractional' dimension are fractals, of course. One commonly-encountered example is the von Koch snowflake, an iteratively-constructed form with finite area yet an infinitely long perimeter: its Hausdorff dimension is $\log(4)/\log(3)$, about 1.26. Another example, one that we've already seen, is the Cantor set: its (Lebesgue) length is

$$1 - 1/3 - 2/9 - 4/27 \ldots \to 0,$$

yet there are infinitely many points in the set (both Hausdorff and Lebesgue 0-dimensional measure correspond to counting points, as we shall see). The Cantor set's Hausdorff dimension is $\log(2)/\log(3)$.

Definition 15 (Hausdorff Measure)**.** With X, M, and $d \in \mathbb{R}_0^+$ as before, let

$$\mu_d^\varepsilon := \inf_{(U_i)} \sum_i (\mathrm{diam}(U_i))^d,$$

where the infimum is taken over all countable covers $(U_i)_{i\in\mathbb{N}}$ of X such that $\mathrm{diam}(U_i) < \varepsilon$ for all i. We call such covers *ε-covers.* Then the d-dimensional Hausdorff measure of X is

$$\mu_d(X) = \lim_{\varepsilon \to 0+} \mu_d^\varepsilon.$$

Notice how the set-up of Hausdorff measure evokes Lebesgue outer measure; the idea with both functions is to countably cover (with arbitrarily small ε-balls U_i) X as efficiently as possible. Again, if X is bounded, it has a Hausdorff dimension,

a non negative (possibly infinite) number d such that Hausdorff measure for d' less than d returns infinity and returns 0 for d' greater than d.

Calculating exact Hausdorff measure (and by extension, dimension) isn't typically easy. Because the measure depends on taking an infimum of sums, it's more common for mathematicians to find upper bounds, which only require one covering per ε, than lower bounds, which require computing all possible coverings. It is then fortunate for us that for self-similar fractals (such as the von Koch snowflake and Cantor set), Hausdorff dimension coincides with the simpler concept of *box dimension*, ([Sch07]) which in general gives an upper bound for $\dim_H(X)$.

Definition 16 (Box Dimension)**.** Let X be a subset of $\mathbb{R}^n$. For a partition of $\mathbb{R}^n$ into n-cubes (or dimension smaller than n if applicable) of side length s, let $N(s)$ denote the number of s-cubes that intersect X. Then the box-counting dimension of X is

$$\lim_{s\to 0} \log(N(s))/\log(1/s).$$

Its easier to see how this works on (bounded) self-similar sets, which obviates the need to take the limit as s gets small (if X is a self-similar set, it may be split into $N(s)$ congruent subsets, each of which is a copy of X scaled down by a factor of s. For instance, the unit square may be split into four squares of side-length 1/2. We find that its self similarity dimension, $\log(4)/\log(2) = 2$, agrees with its canonical dimension. In a less trivial example, the Cantor thirds set may be split into two copies of itself, both scaled down by a factor of 3. Its self-similarity dimension (i.e., box-counting and Hausdorff dimension) is $\log(2)/\log(3) \approx .631$, which matches our expectation that its 'true' dimension lies somewhere between 0 and 1. It should be apparent that one can find Cantoresque sets that take any dimension between 0 and 1.

With this new conception of the size of sets, we can now return to a matter first broached in section 2.3, regarding the existence of a refinement of the Lebesgue theory of Diophantine approximation. Recall that if $\psi : \mathbb{N} \to \mathbb{R}^+$ is a sequence, the family of ψ-approximable numbers is

$$W(\psi) = \{x \in [0,1] : \|qx\| < \psi(q) \text{ i.o.}\},$$

infinitely often with respect to q. This is of course a limsup set, so if we define (using standard ε-ball notation)

$$A_q(\psi) := \bigcup_{p=0}^{q} B(\frac{p}{q}, \frac{\psi(q)}{q}) \cap [0,1]$$

then

$$W(\psi) = \limsup_{q\to\infty} A_q(\psi) = \bigcap_{t=1}^{\infty}\bigcup_{q=t}^{\infty} A_q(\psi).$$

Unpacking this definition, we have that for every t, the collection of sets $A_q(\psi)$ over $q \geq t$ is a cover of $W(\psi)$. (Note that each $A_q(\psi)$ is itself a union of balls; we're dealing with a union of unions.) If ψ is monotonic and $\psi(q) < 1$ for all q large enough, then for each $\varepsilon > 0$ we may choose a t such that $\varepsilon > \psi(t)/t$. Therefore the collection $\{A_q(\psi)\}_{q\geq}$ gives a ε-cover of $W(\psi)$. Therefore

$$\mu_d^{\varepsilon} \leq \sum_{q=t}^{\infty} q(2\psi(q)/q)^d.$$

(The additional factor of 2 is due to the fact that we defined the balls in each A_q in terms of their radii, whereas our definition Hausdorff measure uses diameters.)

The above sum goes to zero as t goes to infinity if

$$\sum_{q=1}^{\infty} q^{1-d}(2\psi(q))^d < \infty,$$

for the limit of the tail of a convergent sum goes to zero. This calculation proves the convergent case of the following 1931 theorem of Jarník.

Theorem 30 (Jarník's Theorem)**.** *Let $\psi : \mathbb{N} \to \mathbb{R}^+$ be a monotonic function and $d \in (0, 1)$. Then*

$$\mu_d(W(\psi)) = \begin{cases} 0 & \text{if} \quad \sum_{q=1}^{\infty} q^{1-d}(\psi(q))^d < \infty, \\ \infty & \text{if} \quad \sum_{q=1}^{\infty} q^{1-d}(\psi(q))^d = \infty. \end{cases}$$

Jarník's theorem is an analogue to Khinchin's theorem in a fairly faithful sense. For both theorems, the 'divergent' case is far more difficult to prove, and we can forgo the requirement for monotonicity of ψ in the divergent case ([BRV16]).

To address a hanging matter from Section 2.3, suppose that $\psi(q) = q^{-\tau}$ for some $\tau > 0$. Then if $d > 2/(t+1)$,

$$\sum_{q=1}^{\infty} q^{1-d}(\psi(q))^d = \sum_{q=1}^{\infty} q^{-(td+d-1)} = \sum_{q=1}^{\infty} q^{-(1+\delta)} < \infty$$

for some $\delta > 0$. So for $t \geq 1$, we have that $\dim_H(W(\tau)) \leq 2/(\tau+1)$. In fact, it can be seen from Jarník's Theorem that $\dim_H(W(\tau)) = 2/(\tau+1)$: this result is known as the Jarník-Besicovitch theorem, and was proved by the former in 1928 and by the latter in 1931, using different methods. The result of this fact is that (e.g.) $\dim_H(W(2)) = 2/3$ and $\dim_H(W(100)) = 2/101$, confirming our intuition that the size of families of τ-well approximable numbers decrease with τ.

The numbers that lie outside of every $W(\tau)$, a set which has Hausdorff dimension of zero, are known as the *Liouville numbers*. In discovering the first such number (1844), Joseph Liouville was the first to prove the existence of transcendental numbers.

The following elegant formulation unites the theorems of Khintchin and Jarník by including the case where $d = 1$ (which, recall, is 1-D Lebesgue measure).

Theorem 31. *Let $\psi : \mathbb{N} \to \mathbb{R}^+$ be a monotonic function and $d \in (0, 1]$. Then*

$$\mu_d(W(\psi)) = \begin{cases} 0 \quad \textit{if} \quad \sum_{q=1}^{\infty} q^{1-d}(\psi(q))^d < \infty, \\ \mu_d([0,1]) \quad \textit{if} \quad \sum_{q=1}^{\infty} q^{1-d}(\psi(q))^d = \infty. \end{cases}$$

To conclude, we recapitulate the best progress yet made toward solving the Littlewood Conjecture. By classifying the A_3-invariant, ergodic measures on $\mathrm{SL}(3,\mathbb{R})/\mathrm{SL}(3,Z)$ (or rather, those which exhibit positive entropic behavior), Einsiedler, Katok, and Lindenstrauss proved the following:

Theorem 32. *Let*

$$\Xi = \left\{ (\alpha, \beta) \in \mathbb{R}^2 : \liminf_{n\to\infty} n\|n\alpha\|\|n\beta\| > 0 \right\}.$$

Then the Hausdorff dimension of Ξ is 0. In fact, Ξ is a countable union of compact sets with zero box dimension.

It readily follows that for any $d > 0$, $\mu_d(\Xi) = 0$.

What should we think of this result? The rationals, $\mod \mathbb{Z}$, have 0 Hausdorff dimension, as do any bounded countable set. These aren't the only ones, however: one can define a sufficiently 'thin' Cantor set whose (downward) scaling factors, rather than remaining constant, increase exponentially faster than 2^n. Such a set

has box-dimension zero yet (by the same argument that we made in chapter 3) is bijective with $\{0,1\}^{\mathbb{N}}$, therefore uncountable. While we may know little indeed about the characterization of Ξ, we can interpret its magnitude and distribution as comparable to either a countable collection of isolated points or an extremely sparse fractal. Alternatively, in light of the Jarník-Besicovitch theorem, Ξ is smaller than *every* class of τ-well approximable numbers. Even by the standards of the most discriminating measures available to us, Ξ is an unfathomably minuscule (albeit possibly infinite) set. Which is to say that the 2006 result of EKL, if not an unqualified and complete proof of the Littlewood Conjecture, comes pretty darn close. Close enough?

Bibliography

[AMR92] Peter Szüsz Andrew M. Rockett, *Continued fractions*, World Scientific Publishing, 1992.

[BRV16] Victor Beresnevich, Felipe Ramírez, and Sanju Velani, *Metric diophantine approximation: Aspects of recent work*, London Mathematical Society Lecture Note Series, pp. 1–95, Cambridge University Press, Nov 2016.

[Cas55] H.P.F. Cassels, J.W.S. & Swinnerton-Dyer, *On the product of three homogeneous linear forms and the indefinite ternary quadratic forms.*, Philosophical Transactions of the Royal Society A (1955), no. 248, 73–96.

[Cas57] J. W. S. Cassels, *An introduction to Diophantine approximation*, Cambridge University Press, 1957.

[Ein09] Manfred Einsiedler, *What is measure rigidity?*, Notices of the AMS **56** (2009), no. 5, 600–601.

[GH60] E.M. Wright G.H Hardy, *An introduction to the theory of numbers*, Oxford University Press, 1960.

[Kle98] Dmitry Kleinbock, *Bounded orbit conjecture and Diophantine approximation*, Proceeedings of the International Colloquium on Lie Groups and Ergodic Theory, TIFR, Mumbai (1998), 119–130.

[Mar97] G.A. Margulis, *Oppenheim conjecture*, Fields Medallists' Lectures, World. Sci. Ser. 20th Century Math. **5** (1997), 272.

[MB02] Garrett Stuck Michael Brin, *Introduction to dynamical systems*, Cambridge University Press, 2002.

[ME06] Elon Lindenstrauss Manfred Einsiedler, Anatole Katok, *Invariant meausres and the set of exceptions to Littlewood's conjecture*, Annals of Mathematics **164** (2006), 513–560.

[ME11] Thomas Ward Manfred Einsiedler, *Ergodic theory with a view toward number theory*, Springer, 2011.

[Mor05] Dave Witte Morris, *Ratner's theorems on unipotent flows*, The University of Chicago Press, 2005.

[Rud90] Daniel J. Rudolph, *2 and 3 invariant measures and entropy*, Ergodic Theory and Dynamical Systems **10** (1990), no. 2, 395–406.

[Sch07] Dierk Schleicher, *Hausdorff dimension, its properties, and its surprises*, The American Mathematical Monthly (2007), no. 114, 509–528.

[Ven08] Akshay Venkatesh, *The work of Einsiedler, Katok and Lindenstrauss on the Littlewood conjecture*, Bulletin of the American Mathematical Society **45** (2008), no. 1, 117–134.