Orbit Counting Far From Hyperbolicity

V.S. Stangoe

Abstract

We find a Prime Orbit Theorem and an analogue of Mertens' Theorem of analytic number theory for maps of interest in the field of dynamics. The maps studied are examples of S-Integer dynamical systems and are built as isometric extensions of hyperbolic maps. The results we obtain bear the same relationship to those known in a hyperbolic setting as Tchebyshev's Theorem does to the Prime Number Theorem. For the systems closest to hyperbolicity (those for which the set S is finite) the arguments proceed essentially by comparing orbit-counting problems for the $S-$integer system to the same problem for the hyperbolic base system. For the systems furthest from hyperbolicity (those for which the set S is co-finite) different and more direct methods are used. The $S-$ integer systems are constructed from arithmetic data and in this thesis both characteristic zero and positive characteristic examples are studied.

I would like to thank Tom Ward and Graham Everest, my supervisors for their help and support throughout this work. A special thank you to Tom for his time and patience with me and endless enthusiasm. I also thank my family for their support. Thanks to Scott Grandison for his help with the graphs. Finally, thank you to all friends who have helped me through this. You know who you are. Thank you for being there.

Contents

Chapter 1

Introduction

This work studies the counting of orbits in dynamical systems in a non-hyperbolic setting.

We look at how this has been done before for Axiom A flows and hyperbolic maps in [23] and ergodic (not necessarily hyperbolic) automorphisms in [29]. We consider such things as the topological entropy (Section 2.2), the growth rate of the periodic points (Section 3.3) and zeta functions (Section 3.6). These are the ingredients that contribute to the asymptotic formula for a Prime Orbit Theorem.

We first consider counting the number of orbits in a dynamical system as an analogue to the Prime Number Theorem. This work is a first step to extending [23] and [29] to non-hyperbolic maps and in particular S-integer systems, explained in Chapter 3.

We first study hyperbolic maps (Section 2.1) and see what the results in [23] say about them. We then consider if a hyperbolic map is perturbed (perturbed in an arithmetic sense) slightly, what effect will this have on the Prime Orbit Theorem? This small pertubation forms an S-integer dynamical system. We study the proof of the Prime Orbit Theorem in [29] and see if we can extend this to S-integer systems. Unfortunately, we find this cannot be done and have to look for other methods to count orbits. This results in an analogue to Tchebyshev's Theorem. This is done firstly by looking at the behaviour of the periodic points of these S-integer systems. We see that this is erratic and this causes the methods of proof for theorems in [23] and [29] to fail.

We then look at Mertens' theorem (Chapter 7), for prime numbers. In the same way as for the Prime Orbit Theorem we look at results already found in [26] and [22]. Here, we find it is easier to work with the logarithmic equivalent of Mertens' theorem. Again, we study the hyperbolic systems for which we know the results of from [26] and [22] and try to extend this to an S-integer setting. The knowledge we have from the Prime Orbit Theorem is used here.

1.1 Notation

The symbols O, $\sim$, $\asymp$, $\|$ are used often and are defined as follows for functions f, $\phi : \mathbb{R} \to \mathbb{R}$:

O : $f = O(\phi)$ means that there exists $A > 0$ such that $|f(x)| < A|\phi(x)|$ for all $x > 0$;

$\sim$: $f \sim \phi$ means that $f(x)/\phi(x) \to 1$ as $x \to \infty$;

$\asymp$: $f \asymp \phi$ means that there exist $A, B > 0$ such that $A\phi(x) < f(x) < B\phi(x)$ for all $x > 0$;

$\|$: $p^a \| n$ means that $p^a \mid n$ but $p^{a+1} \nmid n$.

Let A be a commutative ring with unit 1, and $S \subset A$ a multiplicative set. That is, $1 \in S$ and $a, b \in S \implies ab \in S$.

Definition 1.1. Suppose that $f : A \to B$ is a ring homomorphism with the properties that

1. $f(x)$ is a unit of B for all $x \in S$;
2. if $g : A \to C$ is a ring homomorphism taking every element of S to a unit of C then there exists a unique homomorphism $h : B \to C$ with $g = hf$.

Then B is uniquely determined up to isomorphism of rings, and B is called the *localisation* or *ring of fractions* of A with respect to S. Write $B = S^{-1}A$ or $B = A_S$ or sometimes $B = A_{(S)}$.

The ring B is constructed as follows. Define an equivalence relation $\sim$ on $A \times S$ by

$$(a, s) \sim (b, s') \iff \exists\, t \in S \text{ such that } t(s'a - sb) = 0.$$

Let B be the set of equivalence classes under $\sim$, and write a/s for the equivalence class of (a, s). Extend the ring operations to B by defining

$$a/s + b/s' = (as' + bs)/ss', \quad (a/s) \cdot (b/s') = ab/ss'.$$

The map f is defined to be $f(a) = a/1$. For example, for $x \in S$ the image is a unit since the multiplicative inverse of $x/1$ in B when $x \in S$ is simply $1/x$. For the uniqueness claim, if $g : A \to C$ is the given map, then we set $h(a/s) = g(a)g(s)^{-1}$.

If P is a prime ideal in A, then $S = A \backslash P$ is a multiplicative set. In this case we conventionally write $A_{(P)}$ for A_S.

Important example: Let $A = \mathbb{Z}$, and $P = 3\mathbb{Z}$. Then $\mathbb{Z} \backslash P$ is a multiplicative set consisting of all integers that are NOT divisible by 3. So there is a localisation in which all such integers become units, and you get that this localisation is $\mathbb{Z}[1/2, 1/5, 1/7, \ldots]$.

Thus, the ring $\mathbb{Z}_{(3)}$ consists of all the rationals whose denominators are not divisible by 3.

Chapter 2

Periodic points and dynamical systems

2.1 Periodic Points and Orbits

A dynamical system is an abstract mathematical model for the evolution over time of a physical system obeying fixed laws. This is conventionally modelled by a map whose iterates denote the passage of time.

Definition 2.1. A dynamical system (X, T) consists of a compact metric space X and a continuous mapping $T : X \to X$.

A point x in a dynamical system (X, T) is called a periodic point with *least period* n if $T^n(x) = x$ and $T^j(x) \neq x$ for $0 < j < n$. This means that after n iterations of the map T, the point x will come back to the same place for the first time. Define

$$\mathcal{L}_n(T) = \{x \in X : \#\{T^k(x)\}_{k \in \mathbb{N}} = n\}, \tag{1}$$

the set of points of least period n under T. Write $L_n(T) = |\mathcal{L}_n(T)|$ for the number of points of least period n. Define

$$\mathcal{F}_n(T) = \{x \in X : T^n(x) = x\}, \tag{2}$$

the set of points of period n under T. Write $F_n(T) = |\mathcal{F}_n(T)|$ for the number of points of *period* n.

The number of *orbits* of length n is then

$$O_n(T) = L_n(T)/n. \tag{3}$$

Notice that

$$\mathcal{F}_n(T) = \bigcup_{d|n} \mathcal{L}_d(T) \tag{4}$$

and since the $\mathcal{L}_n(T)$ are disjoint for distinct n, this implies that

$$F_n(T) = \sum_{d|n} L_d(T). \tag{5}$$

Example 2.2. Three of the following examples will arise again as special cases of S-integer dynamical systems.

1. Let X denote the unit interval with its end points identified, $X = \mathbb{R}/\mathbb{Z} = \mathbb{T}$. Define a continuous map $T : X \to X$ by $T(x) = 2x \bmod 1$ i.e.

   $$T(x) = \begin{cases} 2x & 0 \le x < 1/2; \\ 2x - 1 & 1/2 \le x \le 1 \ . \end{cases}$$

   This is called the *circle doubling map* since it locally doubles distances on the circle. Then

   $$F_1(T) = 1, F_2(T) = 3, F_3(T) = 7, \ldots,$$

   indeed $F_n(T) = 2^n - 1$, the Mersenne sequence. This may be seen as follows: $\mathcal{F}_n(T)$ is the kernel of the map $t \mapsto (2^n - 1)t \bmod 1$ on $\mathbb{T}$, which has the $2^n - 1$ elements, $\{0, \frac{1}{2^n-1}, \frac{2}{2^n-1}, \ldots, \frac{2^n-2}{2^n-1}\}$.

2. Let X denote the set of all doubly infinite strings of 0's and 1's, where any 0 is immediately followed by a 1. Define a continuous map $T : X \to X$ by $(Tx)_n = x_{n+1}$. This map is a left (or right) shift. Then

$$F_1(T) = 1, F_2(T) = 3, F_3(T) = 4, F_4(T) = 7 \ldots,$$

and $F_n(T) = F_{n-1}(T) + F_{n-2}(T) = L_n$, the Lucas sequence. This is known as the 'golden mean shift'; the formula for $F_n(T)$ may be found in [19, Prop. 2.2.12].

3. Let $\mathbb{S}^1$ denote the multiplicative circle. The map $T : z \to z^{-2}$ is an endomorphism of $\mathbb{S}^1$. The points of period n are given by

$$\mathcal{F}_n = \{z \in \mathbb{S}^1 \mid z^{(-2)^n} = z\},$$

so $F_n(T) = |(-2)^n - 1|$. Thus $(F_n(T))$ is the Jacobsthal-Lucas sequence (see [8, Example 11.1]).

Write $T_a : \mathbb{T} \mapsto \mathbb{T}$ for the map $x \mapsto ax \bmod 1$, $a \in \mathbb{Z}$. Thus the map in Example 2.2(1) is T_2, while that of Example 2.2(3) is isomorphic to T_{-2}. Since $(T_{-2})^2 = T_2^2$ we have that $F_n(T_{-2}) = F_n(T_2)$ whenever n is even. One of the issues that will arise later is this: what is the relationship between $O_n(T_2)$ and $O_n(T_{-2})$?

2.2 Topological Entropy

To measure how complicated the orbits in a dynamical system are, we use the *topological entropy*. There are several different equivalent definitions of topological entropy. We describe here the original definition of Adler, Konheim and McAndrew, which is closely analogous to the earlier measure-theoretic entropy of Kolmogorov and Sinai. The topological entropy of a dynamical system (X, T) is a non-negative real number or ∞ and is denoted by $h(T)$.

Definition 2.3. The collection $\alpha = \{A_\lambda\}_{\lambda\in\Lambda}$ is called an *open cover* of X if $X = \bigcup_{\lambda\in\Lambda} A_\lambda$, each A_λ is an open set and a *finite open cover* if Λ is finite. By compactness, an open cover has a finite subcover.

Definition 2.4. Let $N(\alpha)$ be the smallest number of sets in a finite subcover of α, and define the *entropy* of α to be $H(\alpha) = \log N(\alpha)$.

The *refinement* of two open covers $\alpha \bigvee \beta$, is defined to be the open cover comprising sets of the form $A \cap B$, where $A \in \alpha$ and $B \in \beta$. The following theorem and more detailed proof is found in [31, Chap. 7, §7.1]. Notice that

$$H(\alpha \bigvee \beta) \leq H(\alpha) + H(\beta),$$

and for any continuous map T,

$$H(T^{-1}\alpha) \leq H(\alpha).$$

Theorem 2.5. *If α is an open cover of X and $T : X \to X$ is continuous then the* topological entropy of T with respect to α *defined to be*

$$\lim_{n\to\infty} \frac{1}{n} H\left(\bigvee_{j=0}^{n-1} T^{-j}(\alpha)\right)$$

exists and is finite.

Proof. Recall that if $\{a_n\}_{n\geq 1}$ is a sequence of real numbers such that

$$a_{n+m} \leq a_n + \ a_m \forall\ n, m$$

then $\lim_{n\to\infty} a_n/n$ exists and equals $\inf_n a_n/n$. So if we set

$$a_n = H\left(\bigvee_{j=0}^{n-1} T^{-j}(\alpha)\right)$$

then it suffices to show that $a_{n+m} \leq a_n + a_m \forall\, n, m \geq 1$. We have

$$\begin{aligned} a_{n+m} &= H\left(\bigvee_{j=0}^{n+m-1} T^{-j}(\alpha)\right) \\ &\leq H\left(\bigvee_{j=0}^{n-1} T^{-j}(\alpha)\right) + H\left(T^{-n}\bigvee_{i=0}^{m-1} T^{-i}(\alpha)\right) \\ &\leq a_n + a_m. \end{aligned}$$

□

Definition 2.6. The topological entropy of T is

$$h(T) = \sup_{\alpha} h(T, \alpha),$$

where α ranges over all open covers of X.

Lemma 2.7. *$h(\varphi) = 0$, where φ is the identity map of X.*

Proof. Now $h(\varphi) := \sup h(\varphi, U)$, where the supremum is taken over all covers U.

$$h(\varphi, U) \;=\; \lim_{n\to\infty} H(U \vee \varphi^{-1}U \vee \cdots \vee \varphi^{-n+1}U)/n,$$

since φ is the identity map $\varphi^{-k}U = U, \forall k$, so $U \vee \varphi^{-1}U \vee \cdots \vee \varphi^{-n+1}U = U$. So

$$\begin{aligned} \lim_{n\to\infty} H(U \vee \varphi^{-1}U \vee \cdots \vee \varphi^{-n+1}U)/n &= \lim_{n\to\infty} \frac{1}{n} H(U) \\ &= 0. \end{aligned}$$

Hence $h(\varphi) = 0$. □

Definition 2.8. An open cover β is a *refinement* of an open cover α, written $\alpha \prec \beta$, if every member of β is a subset of a member of α.

If $\alpha \prec \beta$ then $H(\alpha) \leq H(\beta)$.

Theorem 2.9. *$h(T^k) = kh(T)$ for $k \geq 1$*

Proof.

$$\begin{aligned} h(T^k) &\geq h(T^k, U \vee T^{-1}U \vee \ldots \vee T^{-k+1}U) \\ &= k \lim_{n\to\infty} H(U \vee T^{-1}U \vee \cdots \vee T^{-k+1}U \vee T^{-k}U \vee \cdots \\ &\quad \vee T^{-2k+1}U \vee \cdots \vee T^{-(n-1)k}U \vee \cdots \vee T^{-nk+1}U)/nk \\ &= kh(T,U) \end{aligned}$$

for any open cover U. Thus $h(T^k) \geq kh(T)$. On the other hand, since

$$\begin{aligned} U \vee (T^k)^{-1}U \vee \cdots \vee (T^k)^{-n+1}U &\prec U \vee \cdots \vee T^{-nk+1}U, \\ h(T,U) &= \lim_{n\to\infty} H(U \vee T^{-1}U \vee \cdots \vee T^{-nk+1}U)/nk \\ &\geq \lim_{n\to\infty} H(U \vee (T^k)^{-1}U \vee \cdots \vee (T^k)^{-n+1}U)/nk \\ &= h(T^k, U)/k, \end{aligned}$$

for any open cover U; thus $kh(T) \geq h(T^k)$. □

In a metric space (X, d) define the diameter of a cover to be

$$diam(\alpha) = \sup_{A\in\alpha} diam(A),$$

where $diam(A)$ denotes the diameter of the set A.

We have that $\alpha = \{A_\lambda\}_{\lambda\in\Lambda}$ is an open cover. Define $diam(\alpha) = \sup_{\lambda\in\Lambda} diam(A_\lambda)$, where $diam(A) = \sup_{x,y\in A} d(x,y)$.

Theorem 2.10. *Let (X, d) be a compact metric space. If $\{\alpha_n\}_1^\infty$ is a sequence of open covers of X with diam $(\alpha_n) \to 0$ then if $h(T) < \infty, \lim_{n\to\infty} h(T, \alpha_n)$ exists and equals $h(T)$, and if $h(T) = \infty$ then $\lim_{n\to\infty} h(T, \alpha_n) = \infty$.*

The proof can be found in [31, Chap. 7, §7.2].

Theorem 2.11. *Let X and Y be two compact topological spaces. Let T be a continuous mapping of X into itself and S a continuous mapping of Y into itself. Then*

$$h(T \times S) = h(T) + h(S)$$

where $T\times S$ is the continuous mapping of $X\times Y$ into itself by $T\times S : (x, y) \to (Tx, Sy)$.

The proof of this can be found in [1].

Lemma 2.12. *For $K \in \mathbb{Z}\{0\}$,the topological entropy of the map $T : x \to Kx$ on $\mathbb{T}$ is $\log |K|$ when $|K| \geq 1$.*

Proof. If $K = \pm 1$ this is clear, so assume $K > 1$. The result may be seen using [1, Property 12]. Let α_r be the open cover of $\mathbb{T}$ consisting of all open intervals of length $1/r$, for some $r \in \mathbb{N}$. Then $\bigvee_{j=0}^{n-1} T^{-j}(\alpha_r)$ comprises intervals of length $1/rK^{(n-1)}$ so

$$rK^{(n-1)} - 1 \leq N\left(\bigvee_{j=0}^{n-1} T^{-j}(\alpha_r)\right) \leq rK^{(n-1)} + 1.$$

It follows that $h(T, \alpha_r) = \log K$; the sequence of covers α_r is refining, so we are done. The case for $K < 1$ is similar. $\square$

Example 2.13. Using Example (1) from Section 2.1, let α_r be the open cover of $\mathbb{T}$ consisting of all open intervals of length $1/r$, then $\bigvee_{j=0}^{n-1} T^{-j}(\alpha_r)$ contains intervals of length $1/r2^{(n-1)}$ so

$$\begin{aligned} h(T) &= h(T, \alpha) \\ &= \lim_{n\to\infty} \frac{1}{n} H\left(\bigvee_{j=0}^{n-1} T^{-j}(\alpha_r)\right) \\ &= \lim_{n\to\infty} \frac{1}{n} \log N\left(\bigvee_{j=0}^{n-1} T^{-j}(\alpha_r)\right) \\ &= \lim_{n\to\infty} \frac{1}{n} \log\left(2^n - 1\right) \\ &= \log 2. \end{aligned}$$

Define $\log^+ x = \max\{\log x, 0\}$, so that Lemma 2.12 may be written $h(T) = \log^+ |K|$. The topological entropy arises in the calculation of the number of orbits in a dynamical system.

2.3 Expansiveness

Expansiveness is a natural geometrical property a dynamical system may have. It influences the computation of topological entropy.

Definition 2.14. A continuous map T of a compact metric space (X, d) is said to be *forwardly expansive* if there exists a constant $\delta > 0$ such that for any $x \neq y$ there exists $n \in \mathbb{N}$ with $d(T^n(x), T^n(y)) > \delta$.

Lemma 2.15. *If $T : X \to X$ is a forwardly expansive homeomorphism then X is finite.*

See [2, Th. 3.9].

The following definition is from [31, Chap. 5, §5.6].

Definition 2.16. A homeomorphism T of a compact metric space (X, d) is said to be *expansive* if there exists a constant $\delta > 0$ with the property that if $x \neq y$ then there exists $n \in \mathbb{Z}$ with $d(T^n(x), T^n(y)) > \delta$.

In either case (Definition 2.14 or 2.16) we call δ an *expansive constant* for T.

The examples given in Example 2.1 are all expansive (or forwardly expansive) maps. The proofs follow.

Example 2.17. 1. The circle doubling map, Example 1, is forwardly expansive.
Let $\delta = 1/4$. Notice that $d(T^n x, T^n y) = d(T^n(x - y), 0)$, so it is enough to

show that there exists a $\delta > 0$ with the property that any $x \neq 0$ in $\mathbb{T}$ has $d(T^n x, 0) > 1/4$ for some $n \geq 0$. Write $x = 0.x_1 x_2 x_3 \ldots$ in base 2, then since $x \neq 0$, not all digits are 0 and $T(x) = 0.x_2 x_3 x_4 \ldots$. Therefore there exists an n such that $T^n(x) = 0.10 * \ldots$ so $d(T^n(x), 0) \geq 1/4$, as required.

2. Example 2, the Golden Mean shift map is expansive. Let $\delta = 1/4$. Define a metric on X to be $d(\underline{x}, \underline{y}) = \sum_{n \in \mathbb{Z}} 2^{-|n|} \cdot |x_n - y_n|$. When $\underline{x} \neq \underline{y}$ this implies there exists a k such that $x_k \neq y_k$. Therefore $d(T^{-k}\underline{x}, T^{-k}\underline{y}) \geq 1/4$.

3. The expansiveness of Example 3 can be proved in a similar way to Example 1.

The following Theorem and proof are found in [31, Ch. 5, §5.6].

Lemma 2.18. *Let $T : X \to X$ be an expansive homeomorphism of a compact metric space. For each integer $p > 0$ the homeomorphism T^p has only a finite number of fixed points.*

Proof. Let δ be an expansive constant for T^p. Suppose $T^p(x) = x$ and $T^p(y) = y$. Then either $x = y$ or $d(x, y) > \delta$. So $\{B_\delta(x) \mid T^p(x) = x\}$ is a set of disjoint $\delta-$balls in X, so must be a finite collection by compactness. $\square$

2.4 Möbius Inversion Formula

If $n > 1$, write $n = p_1^{a_1} \cdots p_k^{a_k}$, where $a_i \geq 1$ for the prime decomposition. The Möbius function $\mu(n)$ is defined as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } a_1 = a_2 = \cdots = a_k = 1 \\ 0 & \text{if } n \text{ has a square factor } > 1. \end{cases}$$

The Möbius function arises in the relationship between points of least period n and points of period n. It is useful because it eliminates values that will already have been counted.

Lemma 2.19.

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \textit{if} \quad n = 1 \\ 0 & \textit{if} \quad n > 1 \end{cases}$$

Proof. If $n = 1$ then $\mu(1) = 1$.

If $n > 1$, then take a prime p that divides n. Any squares of p give 0 by definition. For divisors that are square-free, arrange them into pairs d and dp, where $p \nmid d$. Then $\mu(dp) = -\mu(d)$, thus cancelling each other. Hence the result. □

Theorem 2.20. *Let A and B be functions on the positive integers.*

$$\textit{Then } A(n) = \sum_{d|n} B(d) \ \textit{ if and only if } \ B(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) A(d).$$

Proof. The proof is taken from [24, Chap.2 §2.1].

$$
\begin{aligned}
\sum_{d|n} A(d)\mu\left(\tfrac{n}{d}\right) &= \sum_{d|n} A\left(\tfrac{n}{d}\right)\mu(d) && \text{(this is simply the same sum in reverse order)} \\
&= \sum_{d_1 d_2 = n} \mu(d_1)A(d_2) && \text{(this sum is taken over all pairs } d_1, d_2 \text{ such that } d_1 d_2 = n\text{)} \\
&= \sum_{d_1 d_2 = n} \left[\mu(d_1)\sum_{d|d_2} B(d)\right] && \text{(by definition)} \\
&= \sum_{d_1 d|n} \mu(d_1)B(d) && \text{(by multiplying out the terms in the square brackets above, this new sum is taken over all pairs } d_1, d \text{ such that } d_1 d \mid n\text{)} \\
&= \sum_{d|n} B(d)\sum_{d_1|n/d} \mu(d_1) && \text{(by collecting together all multiples of } B(d) \text{ when } d \mid n\text{)} \\
&= B(n)
\end{aligned}
$$

□

This is known as the Möbius Inversion Formula.

Using the Möbius inversion formula equations (2) and (1) can be written as

$$F_n(T) = \sum_{d|n} L_d(T). \tag{6}$$

and

$$L_n(T) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F_d(T). \tag{7}$$

respectively. Also we can write equation (3) as

$$O_n(T) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) F_d(T). \tag{8}$$

Example 2.21. Using Example (1) from (2.1), let $F_n(T) = 2^n - 1$. Then

$$L_n(T) = \sum_{d|n} \mu\left(\frac{n}{d}\right)\left(2^d - 1\right).$$

Taking $n = 6$, we find

$$\begin{aligned}
\mathcal{L}_6(T) &= \mu(6)\cdot\mathcal{F}_1(T) + \mu(3)\cdot\mathcal{F}_2(T) + \mu(2)\cdot\mathcal{F}_3(T) + \mu(1)\cdot\mathcal{F}_6(T) \\
&= 1\cdot 1 + (-1)\cdot 3 + (-1)\cdot 7 + 1\cdot 63 \\
&= 54.
\end{aligned}$$

The following extract is taken from [3]. For any partially ordered set in which all the intervals are finite, there is a integer-valued Möbius function of two variables, $\mu(x, y)$, giving an inversion relation: if

$$A(x, y) = \sum_{x\le z\le y} B(x, z),$$

then

$$B(x, y) = \sum_{x\le z\le y} A(x, z)\mu(z, y),$$

and conversely. If we take the positive integers ordered by divisibility, then the function $\mu(1, n)$ is the 'classical' Möbius Function. The more general case can be applied to the lattice of subgroups of finite index in a countable group Γ, allowing (6) and (7) to be extended to periodic orbits for Γ-actions.

2.5 Zero and Positive Characteristic

Every field contains a unique prime subfield that is isomorphic to either $\mathbb{Q}$ or $\mathbb{F}_p$, where p is a prime number. We say that the characteristic of the field is either 0 or p.

A field of characteristic p has $px = 0$ for every element x, where $px = (1+1+\ldots+1)x$, where there are p elements 1, and p is the smallest positive integer such that $px = 0$. If a field has characteristic zero, and if $nx = 0$ for some non-zero element x, and integer n, then $n = 0$.

Chapter 3

S-integer dynamical systems

3.1 Non-Archimedean Valuations

Definition 3.1. Let K be a field. A *valuation* on K is a function $|\cdot| : K \to \mathbb{R}$ satisfying the properties:

1. $|x| \geq 0$ for all $x \in K$, with equality if and only if $x = 0$ (positive-definite);
2. $|xy| = |x| \cdot |y|$ for all $x, y \in K$ (multiplicative);
3. $|x + y| \leq |x| + |y|$ (triangle inequality).

A familiar valuation on the field $\mathbb{Q}$ is the absolute value $|x|$ that comes from the metric $d(x, y) = |x - y|$, the usual notion of distance on the number line. Any valuation defines a metric by $d(x, y) = |x - y|$.

The following definitions are taken from [15, Chap. 1, §2].

Definition 3.2. A valuation on a field K is called *non-Archimedean* if

$$|x + y| \leq \max\{|x|, |y|\}$$

for all $x, y \in K$. A metric is called non-Archimedean if

$$d(x,y) \le \max(d(x,z), d(z,y));$$

in particular, a metric is non-Archimedean if it is induced by a non-Archimedean norm, since in that case

$$d(x,y) = |x-y| = |(x-z)+(z-y)| \le \max(|x-z|, |z-y|) = \max(d(x,z), d(z,y)).$$

Definition 3.3. Let p be prime and let $\text{ord}_p a$ be the highest power of p which divides a. For example,

$$\text{ord}_3 15 = 1,\ \text{ord}_5 25 = 2,\ \text{ord}_2 16 = 4,\ \text{ord}_3 14 = 0.$$

For any rational number $x = a/b$, define $\text{ord}_p x = \text{ord}_p a - \text{ord}_p b$.

Define a map $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ as follows:

$$|x|_p = \begin{cases} \frac{1}{p^{\text{ord}_p x}}, & \text{if} \quad x \ne 0, \\ 0, & \text{if} \quad x = 0. \end{cases}$$

We claim that $|\cdot|_p$ is a non-Archimedean norm on $\mathbb{Q}$. It is known as the *p-adic* norm. The following proof is taken from [15, Chap.1, §2].

Proof. Properties 1 and 2 are straightforward to check. We now check Property 3. If $x = 0$ or $y = 0$, or if $x + y = 0$, Property 3 is trivial, so assume x, y and $x + y$ are all nonzero. Let $x = a/b$ and $y = c/d$ be written in lowest terms. Then we have

$$x + y = (ad + bc)/bd, \text{ and } \text{ord}_p(x+y) = \text{ord}_p(ad+bc) - \text{ord}_p b - \text{ord}_p d.$$

Now the highest power of p dividing the sum of two numbers is *at least* the minimum of the highest power dividing the first and the highest power dividing the second.

Hence

$$\begin{aligned}
\mathrm{ord}_p(x+y) &\geq \min(\mathrm{ord}_p ad, \mathrm{ord}_p bc) - \mathrm{ord}_p b - \mathrm{ord}_p d \\
&= \min(\mathrm{ord}_p a + \mathrm{ord}_p d, \mathrm{ord}_p b + \mathrm{ord}_p c) - \mathrm{ord}_p b - \mathrm{ord}_p d \\
&= \min(\mathrm{ord}_p a - \mathrm{ord}_p b, \mathrm{ord}_p c - \mathrm{ord}_p d) \\
&= \min(\mathrm{ord}_p x, \mathrm{ord}_p y).
\end{aligned}$$

Therefore $|x+y|_p = p^{-\mathrm{ord}_p(x+y)} \leq \max(p^{-\mathrm{ord}_p x}, p^{-\mathrm{ord}_p y}) = \max(|x|_p, |y|_p)$, and this is $\leq |x|_p + |y|_p$. $\square$

Example 3.4.

$$|15|_3 = \frac{1}{3},\ |25|_5 = \frac{1}{5^2},\ |16|_2 = \frac{1}{2^4},\ |14|_3 = 1.$$

Definition 3.5. Define $|\cdot|_\infty$ to be the usual absolute value on $\mathbb{R}$.

The following Lemma and proof is from [9, Chap. 3 §3.1].

Lemma 3.6. *(Artin-Whaples Product Formula) For any $x \in \mathbb{Q}^\times$, we have*

$$\prod_{p \leq \infty} |x|_p = 1,$$

where $p \leq \infty$ means that we take the product over all of the primes of $\mathbb{Q}$, including the 'prime at infinity'.

Proof. It is easy to see that we only need to prove the formula when x is a positive integer, and that the general case will then follow. So let x be a positive integer, which we can factor as $x = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$. Then we have

$$\begin{cases} |x|_q = 1 & \text{if } q \neq p_i \\ |x|_{p^i} = p_i^{-a_i} & \text{for } i = 1, 2, \ldots, k \\ |x|_\infty = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k} & \end{cases}$$

The result then follows. $\square$

3.2 S-Integer Dynamical Systems

The paper [4] associates to a set of data coming from an $\mathbb{A}$-field a compact group automorphism called an S-integer dynamical system.

Definition 3.7. An *algebraic number field* k is an extension of the rational field $\mathbb{Q}$ of finite degree. A *rational function field* is an extension of $\mathbb{F}_p(t)$ of finite degree. A field of either type is called an $\mathbb{A}$-*field*.

$\mathbb{A}$-fields have a well-understood set of locally compact completions; indeed their completions comprise the non-discrete locally compact fields (see [36, Chap. I, §3]).

In the following a *place* $w \in P$ of an $\mathbb{A}$-field k is an equivalence class of valuations on k, where valuations are equivalent if the corresponding completions are isomorphic (see [36, Chap.III, §1]). The following examples are taken from [4].

Example 3.8. 1. Let $k = \mathbb{Q}$, the rationals. The places of $\mathbb{Q}$ are in one-to-one correspondence with the set of rational primes $\{2, 3, 5, 7, \ldots\}$ together with one additional place ∞ at infinity. The corresponding valuations are $|r|_\infty = |r|$ (the usual archimedean valuation), and for each p, $|r|_p = p^{-\mathrm{ord}_p(r)}$, where $\mathrm{ord}_p(r)$ is the (signed) multiplicity with which the rational prime p divides the rational number r.

2. For $k = \mathbb{F}_q(t)$, the function field, there are no archimedean places. For each monic irreducible $v(t) \in \mathbb{F}_q[t]$ there is a distinct place v, with corresponding valuation given by

$$|f|_v = q^{-\mathrm{ord}_v(f)\cdot\deg(v)},$$

where $\mathrm{ord}_v(f)$ is the signed multiplicity with which v divides the rational function f. There is one additional place given by $v(t) = t^{-1}$, and this place will be called an infinite place even though the corresponding valuation is non-archimedean.

The product formula holds for any $\mathbb{A}-$field, with suitable normalization.

The set of places P contains a special set P_∞. In characteristic 0, the P_∞ corresponds to the Archimedean completions; in characteristic > 0 they are chosen arbitrarily as in Example 3.8 (2).

Definition 3.9. Let k be an $\mathbb{A}$-field. Given an element $\xi \in k^*$ (where k^* is the group of non-zero elements of k), and any set $S \subset P(k) \backslash P_\infty(k)$ with the property that $|\xi|_w \leq 1$ for all $w \notin S \cup P_\infty$, define a dynamical system $(X, \alpha) = (X^{(k,S)}, \alpha^{(k,S,\xi)})$ as follows. The compact abelian group X is the dual group to the discrete countable group of S-integers R_S in k, defined by

$$R_S = \{x \in k : |x|_w \leq 1 \text{ for all } w \notin S \cup P_\infty(k)\}.$$

The continuous group endomorphism $\alpha : X \to X$ is dual to the monomorphism $\widehat{\alpha} : R_S \to R_S$ defined by $\widehat{\alpha}(x) = \xi x$.

Dynamical systems of the form $(X^{(k,S)}, \alpha^{(k,S,\xi)})$ are called *S-integer dynamical systems*. These can be divided into two classes: *arithmetic systems* when k is a number field and *geometric* when k has positive characteristic.

The following examples are taken from [4].

Example 3.10. 1. Let $k = \mathbb{Q}, S = \emptyset$, and $\xi = 2$. Then

$$R_S = \{x \in \mathbb{Q} : |x|_p \leq 1 \text{ for all primes } p\} = \mathbb{Z},$$

so $X = \mathbb{T}$ and α is the circle doubling map.

2. Let $k = \mathbb{Q}, S = 2$, and $\xi = 2$. Then

$$R_S = \{x \in \mathbb{Q} : |x|_p \leq 1 \text{ for all primes } p \neq 2\} = \mathbb{Z}[\tfrac{1}{2}],$$

so X is the solenoid $\widehat{\mathbb{Z}[\frac{1}{2}]}$ and α is the automorphism of X dual to the automorphism $x \mapsto 2x$ of R_S. This is the natural invertible extension of the circle doubling map, see [5], Example (c).

3. Let $k = \mathbb{Q}, S = \{2, 3, 5, 7, 11, \ldots\}$, and $\xi = \frac{3}{2}$. Then $R_S = \mathbb{Q}$ and α is the automorphism of the full solenoid $\widehat{\mathbb{Q}}$ dual to multiplication by $\frac{3}{2}$ on $\mathbb{Q}$. This map has only one periodic point for any period by [20], Section 3, and has entropy $\log 3$ by [20], Section 2.

4. Let $k = \mathbb{F}_q(t), S = \emptyset$, and $\xi = t$. Then $R_S = \mathbb{F}_q[t]$ and so

$$X = \widehat{R_S} = \prod_{i=0}^{\infty} \{0, 1, \ldots, q-1\}.$$

The map α is therefore the full one-sided shift on q symbols.

5. Let $k = \mathbb{F}_q(t), S = \{t\}$, and $\xi = t$. Recall that the valuation corresponding to t is $|f|_t = q^{-\mathrm{ord}_t(f)}$, so $|t|_t = q^{-1}$. The ring of S-integers is

$$R_S = \{f \in \mathbb{F}_q(t) : |f|_w \leq 1 \text{ for all } w \notin t, t^{-1}\} = \mathbb{F}_q[t^{\pm 1}].$$

The dual of R_S is then $\prod_{-\infty}^{\infty} \{0, 1, \ldots, q-1\}$, and in this case α is the full two-sided shift on q symbols.

6. Let $k = \mathbb{F}_q(t), S = \{t, 1+t\}$, and $\xi = 1 + t$. Then α is the invertible extension of the cellular automaton defined by

$$(\alpha(x))_k = x_k + x_{k+1} \mod q.$$

Theorem 3.11. *The topological entropy of the S-integer system $(X^{(k,S)}, \alpha^{(k,S,\xi)})$ is given by*

$$h(\alpha^{(k,S,\xi)}) = \sum_{w \in S \cup P_\infty(k)} \log^+ |\xi|_w.$$

The proof of this can be found in [4]. The point is that there is a local isometry between $(X^{(k,S)}, \alpha^{(k,S,\xi)})$ and multiplication by ξ on $\prod_{w \in S \cup P_\infty(k)} k_w$, where k_w is the locally compact non-discrete completion of k with respect to the metric induced by the valuation w (see [36, Ch.3]). In each coordinate k_w, $x \to \xi x$ multiplies distance by $|\xi|_w$. So it is reasonable to expect the entropy to be

$$\sum_{w \in S \cup P_\infty(k)} \log^+ |\xi|_w.$$

The notion of expansiveness also makes sense on non-compact spaces (with the same definition).

Theorem 3.12. *Let K be a non-discrete field complete with respect to a valuation $|\cdot|$, and let $\overline{K}$ denote the algebraic closure of K with the uniquely extended absolute value from K. Let E be a finite dimensional vector space over K, and let u be an automorphism of E. Then u is expansive if and only if $|\lambda| \neq 1$ for each eigenvalue λ of u in $\overline{K}$.*

Proof. See Eisenberg's paper [7], Theorem 3.

Corollary 3.13. *Let $(X, \alpha) = (X^{(k,S)}, \alpha^{(k,S,\xi)})$ be an S-integer dynamical system. Then α is expansive if and only if $S \cup P_\infty \subseteq \{w \leq \infty : |\xi|_w \neq 1\}$.*

Again, the proof can be found in [4].

Lemma 3.14. *Let $(X, \alpha) = (X^{(k,S)}, \alpha^{(k,S,\xi)})$ be an S-integer dynamical system. Then the number of periodic points $n \geq 1$ is finite for all n if α is ergodic, and*

$$|\mathcal{F}_n(\alpha)| = \prod_{w \in S \cup P_\infty} |\xi^n - 1|_w.$$

The proof can be found in [4]. This is a generalization of Example 2.2(1) in Section 2.1: the group $\mathcal{F}_n(\alpha)$ is realized as the kernel of a certain map, whose size is computed using Haar measure in an adelic covering space.

3.3 Growth Rate of Periodic Points

Let $\theta : X \to X$ be a dynamical system. The quantity $\lim_{n\to\infty} \frac{1}{n} \log F_n(\theta)$, if it exists, gives the exponential growth rate of periodic points in a dynamical system.

Theorem 3.15. *Let $(X, \alpha) = (X^{(k,S)}, \alpha^{(k,S,\xi)})$ be an ergodic arithmetic S-integer dynamical system with S finite. Then the growth rate of the number of periodic points exists and is given by*

$$\liminf_{n\to\infty} \frac{1}{n} \log |\mathcal{F}_n(\alpha)| = \limsup_{n\to\infty} \frac{1}{n} \log |\mathcal{F}_n(\alpha)| = h(\alpha).$$

Theorem 3.16. *Let $(X, \alpha) = (X^{(k,S)}, \alpha^{(k,S,\xi)})$ be an ergodic geometric S-integer dynamical system with S finite. Then*

$$\limsup_{n\to\infty} \frac{1}{n} \log |\mathcal{F}_n(\alpha)| = h(\alpha).$$

For S non empty in the geometric case, the sequence behaves very badly, indeed for most geometric systems with $S \neq \emptyset$, $\{\frac{1}{n} \log F_n(\alpha)\}$ has infinitely many limit points. See [34].

Proofs of these theorems can be found in [4]. The following table shows the growth rate of periodic points and the topological entropy for some of the arithmetic systems we study here. The effects of Theorem 3.15 are shown.

ξ	S	Periodic points:$F_n(\alpha)$	$h(\alpha)$	$\lim_{n\to\infty}(1/n)\log F_n(\alpha)$
2	$\emptyset$	2^n-1	$\log 2$	$\log 2$
2	$\{3\}$	$(2^n-1)\lvert 2^n-1\rvert_3$	$\log 2$	$\log 2$
2	$\{3,5\}$	$(2^n-1)\lvert 2^n-1\rvert_3\lvert 2^n-1\rvert_5$	$\log 2$	$\log 2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	
2	$\{2,5,7,11,\ldots\}$	$(2^n-1)\prod_{p\neq 3}\lvert 2^n-1\rvert_p$	$\log 2$	0
2	$\{2,7,11,\ldots\}$	$(2^n-1)\prod_{p\neq 3,5}\lvert 2^n-1\rvert_p$	$\log 2$	0

Thus the growth rate of the number of periodic points when S is finite or co-finite is understood. The general case is not clear, but conjecturally, for a 'typical' set S of primes (for example, for a set of primes S chosen by a fair coin toss),

$$\limsup_{n\to\infty}\frac{1}{n}\log|F_n(\alpha)|=h(\alpha),\quad \liminf_{n\to\infty}\frac{1}{n}\log|F_n(\alpha)|=0.$$

This can be proved in certain geometric cases, and holds in general under the assumption that certain standard conjectures in number theory hold. See [32] and [33] for details.

3.4 Hyperbolic Toral Automorphism

A toral automorphism is a linear and bijective map $T:\mathbb{T}^n\to\mathbb{T}^n$. Such a map is called *hyperbolic* if it does not have any eigenvalues of modulus 1.

Example 3.17. Consider the linear map of $\mathbb{R}^2$ given by the matrix $A=\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}$.

The eigenvalues are $\lambda_+=\frac{3+\sqrt{5}}{2}$ and $\lambda_-=\frac{3-\sqrt{5}}{2}$. Thus A is hyperbolic since its eigenvalues are not of modulus 1. The matrix A has integer entries and preserves the integer lattice $\mathbb{Z}^2\subset\mathbb{R}^2$ and so generates a map of the torus $\mathbb{T}^2=\mathbb{R}^2/\mathbb{Z}^2$. The group

$\mathbb{T}^2$ is abelian and since A^{-1} is also an integer matrix, A induces an automorphism. T_A of $\mathbb{T}^2$.

The Mersenne sequence frequently used throughout this thesis arises from an expansive map, which is hyperbolic in a suitably generalized form, see [6]. We look to see what happens when it is perturbed slightly by an isometric extension.

Definition 3.18. Call a matrix A hyperbolic if all eigenvalues have modulus $\neq 1$. Then the toral map induced by T_A is expansive if and only if the corresponding matrix A is hyperbolic.

We use 'hyperbolic' loosely to include maps whose invertible extension is hyperbolic with respect to suitable valuations. In particular, $x \to 2x$ on $\mathbb{T}$ is 'hyperbolic'.

3.5 Ergodic Toral Automorphisms

Lemma 3.19. *A toral automorphism $T_A : \mathbb{T}^d \to \mathbb{T}^d$ is ergodic if and only if the matrix A has no roots of unity as eigenvalues.*

The proof of this can be found in [31, Chap. 1, §1.5].
Recall Kronecker's theorem.

Theorem 3.20. *If $\alpha_1, \ldots, \alpha_n$ are the roots of the polynomial*

$$P(x) = x^n + c_1 x^{n-1} + \cdots + c_n,$$

where $c_1, \ldots, c_n$ are integers with $P(0) \neq 0$, and if all the roots lie inside the closed unit disc, then they must all be roots of unity.

Lemma 3.21. *If $d \leq 3$ then any* ergodic *automorphism $T_A : \mathbb{T}^d \to \mathbb{T}^d$ is hyperbolic.*

Proof. Suppose T_A is ergodic but not hyperbolic. If $d = 1$, then since $A = [\pm 1]$, so T_A cannot be ergodic. If $d = 2$ or 3 then if λ is a unit modulus eigenvalue, it cannot be ± 1 since T_A is ergodic. Therefore λ is not real and so there exists a $\overline{\lambda} \neq \lambda$ that is also an eigenvalue.

So for the case $d = 2$, λ and $\overline{\lambda}$ are the eigenvalues. By Kronecker's Theorem above λ and $\overline{\lambda}$ are the roots of the characteristic polynomial relating to the matrix A and so are roots of unity, and so not ergodic. Therefore any other eigenvalue that is ergodic must also be hyperbolic.

For $d = 3$ then $|\det(A)| = |\mu| \cdot |\lambda| \cdot |\overline{\lambda}| = 1$, since $|\lambda|$ and $|\overline{\lambda}|$ both equal 1, then $|\mu|$ must also equal 1. So again by Kronecker's Theorem the three eigenvalues $\lambda, \overline{\lambda}, \mu$ are roots of unity and so not ergodic. Therefore any other eigenvalue that is ergodic must also be hyperbolic. So any ergodic but non-hyperbolic automorphism on $\mathbb{T}^d$ must have d equal to at least 4. $\square$

The following two examples are of ergodic (but non-hyperbolic) automorphisms on $\mathbb{T}^4$.

Example 3.22. This example is taken from [30]. Let

$$A = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 8 \\ 0 & 1 & 0 & -6 \\ 0 & 0 & 1 & 8 \end{pmatrix}.$$

This matrix has two real eigenvalues, $\alpha_1 = 0.1364697$ and $\alpha_2 = 7.32719$ and two complex eigenvalues of modulus 1. The topological entropy h of T_A is $\log \alpha_2$. T_A is not expansive since it has eigenvalues of modulus 1.

Example 3.23. Let α be the S-integer dynamical system corresponding to

$$S = \emptyset, \;\; \xi = \sqrt{2} - 1 + i\sqrt{2\sqrt{2} - 2}, \quad \text{and } k = \mathbb{Q}(\xi).$$

Then α is isomorphic to the automorphism of the 4-torus given by the matrix

$$B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -4 & 2 & -4 \end{pmatrix}$$

As discussed in [18] this automorphism is ergodic but not expansive. This matrix has two real eigenvalues of modulus 4.612 and 0.2168 and two complex with modulus 1.

3.6 Zeta Functions

The Artin-Mazur zeta function is defined as

$$\zeta_\alpha(z) = \exp \sum_{n=1}^{\infty} \frac{z^n \cdot F_n(\alpha)}{n},$$

where $F_n(\alpha)$ are the periodic points under α.

The following lemmas and examples are from [4].

Lemma 3.24. *Let X be a compact, connected group (necessarily abelian) and let α be an expansive automorphism of X. Then ζ_α is rational.*

Proof. By Theorem 6.1 in [14], X is isomorphic to

$$Y_{H(A)} = \{x = \{x_i\}_{-\infty}^{\infty} \in (\mathbb{T}^n)^{\mathbb{Z}} : (x_i, x_{i+1}) \in H(A) \text{ for all } i \in \mathbb{Z}\},$$

where $H(A) \subset \mathbb{T}^n \times \mathbb{T}^n$ is defined by

$$H(A) = \tau(\{(y, Ay) : y \in \mathbb{R}^n\})$$

for some $n \geq 1, A \in GL(n, \mathbb{Q})$ and τ is the quotient map

$$\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{T}^n \times \mathbb{T}^n.$$

The isomorphism carries α to T^A, the shift on $Y_{H(A)}$. The group $Y_{H(A)}$ is a *generalised solenoidal group* as studied by Lawton in [16]. Let d be the least positive integer for which dA has integer entries. Then the number of periodic points is given by

$$|\mathcal{F}_v(\alpha)| = d^v \prod |\lambda_i^v - 1|$$

where $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of dA. Expanding the finite product shows that the zeta function is rational. $\square$

Example 3.25. If $A = [3/2]$ then $(Y_{H(A)}, T^A)$ is homeomorphic to the one-dimensional solenoidal automorphism dual to multiplication by $3/2$ on $\mathbb{Z}[\frac{1}{6}]$ and the number of points of period n under T^A is $(3^n - 2^n)$.

Lemma 3.26. *Let X be a compact, zero-dimensional topological group and let α be an expansive automorphism. Then ζ_α is rational if α is ergodic.*

Proof. By Theorem 1(ii) in [13], (X, α) is homeomorphic to $(F, \psi) \times (G^{\mathbb{Z}}, \sigma)$ where F is a finite group, ψ is an automorphism, G is a finite group and σ is the shift. For $n \geq 1$,

$$|F_n(\alpha)| = |F_n(\psi \times \sigma)| = |F_n(\psi)| \cdot |G|^n,$$

which is finite. So the zeta function is given by

$$\zeta_\alpha(z) = \exp\left(\sum_{n=1}^{\infty} \frac{|F_n(\alpha)|}{n} z^n\right) = \exp\left(\sum_{n=1}^{\infty} \frac{|F_n(\psi)| \cdot |G|^n}{n} z^n\right).$$

Now α is ergodic if and only if $F = \{e\}$, in which case $|F_n(\psi)| = 1$ and the zeta function has the form $\frac{1}{1-|G|z}$. $\square$

The dynamical zeta function does characterize ergodicity in the setting of Lemma 3.26 (assuming the group X is infinite): α is ergodic if and only if the only pole of ζ_α in the closed unit disc is at $\exp\left(-h(\alpha)\right)$.

Clearly Lemma 3.26 cannot have a converse - the identity on $\{0,1\}$ has a rational zeta function but is not ergodic.

Example 3.27. This example is the same as Example 3.25 but presented in a different format. Let α be the expansive automorphism of $\widehat{\mathbb{Z}[\frac{1}{6}]}$ dual to $\times\frac{2}{3}$ on $\mathbb{Z}[\frac{1}{6}]$. The entropy of α is $\log 3$ and for each $n \geq 1$,

$$|F_n(\alpha)| = \left|\left(\frac{2}{3}\right)^n - 1\right|_\infty \left|\left(\frac{2}{3}\right)^n - 1\right|_2 \left|\left(\frac{2}{3}\right)^n - 1\right|_3 = 3^n - 2^n.$$

The zeta function is therefore given by

$$\zeta_\alpha(z) = \frac{1-2z}{1-3z}.$$

Example 3.28. Let α be the endomorphism of $\widehat{\mathbb{Z}[\frac{1}{30}]}$ dual to $\times\frac{3}{2}$ on $\mathbb{Z}[\frac{1}{30}]$. By Corollary 3.13 α is non-expansive (since $|\frac{3}{2}|_5 = 1|$). The number of points of period n is given by

$$|F_n(\alpha)| = \left|\left(\frac{3}{2}\right)^n - 1\right|_\infty \left|\left(\frac{3}{2}\right)^n - 1\right|_2 \left|\left(\frac{3}{2}\right)^n - 1\right|_3 \left|\left(\frac{3}{2}\right)^n - 1\right|_5 = (3^n - 2^n)|3^n - 2^n|_5,$$

the first few values of which are

$$1, 1, 19, 13, 211, 133, 2059, 1261, \ldots.$$

The exponential growth rate of this sequence is equal to $\log 3$ by Theorem 3.15, the entropy of α. We claim that ζ_α is irrational and will use the following theorem, the Hadamard Quotient Theorem, to prove this.

Theorem 3.29. *(Hadamard Quotient Theorem)*
Let $\mathbb{F}$ be a field of characteristic zero and (a'_n) a sequence of elements of a subring R of $\mathbb{F}$ which is finitely generated over $\mathbb{Z}$. Let $\sum b_n X^n$ and $\sum c_n X^n$ be formal series over $\mathbb{F}$ representing rational functions. Denote by J the set of integers $n \geq 0$ such that $b_n \neq 0$. Suppose that $a'_n = c_n/b_n$ for all $n \in J$. Then there is a sequence (a_n) with $a_n = a'_n$ for $n \in J$, such that the series $\sum a_n X^n$ represents a rational function.

Proof. This was proved by van der Poorten: see [27] and the lecture notes of [25] for a proof, and [28] for a general discussion. □

Thus the quotient (term by term) of two non-zero linear recurrence relations is a linear recurrence relation.

Proposition 3.30. *The number of values that a non-degenerate recurrence sequence can take on infinitely often is bounded by some integer that depends only on the poles of its generating rational function.*

Proof. See [21], Proposition 2. □

Proof of statement in Example 3.28. Suppose, for a contradiction, that ζ_α is rational. then by differentiating ζ_α, $\sum_{n=1}^{\infty} |F_n(\alpha)| z^n$ is also rational. The sequence defined by $a_n = 3^n - 2^n$ is a recurrence sequence since it satisfies the linear, homogeneous recurrence relation

$$a_{n+2} = 5a_{n+1} - 6a_n,$$

together with the initial conditions $a_0 = 0, a_1 = 1$. Hence $\sum_{n=1}^{\infty} a_n z^n$ represents the rational function

$$\frac{z}{1 - 5z + 6z^2}.$$

By Theorem 3.29, with $|F_n(\alpha)| \neq 0$,

$$\sum_{n=1}^{\infty} \frac{z^n}{|3^n - 2^n|_5}$$

is a rational function $P(z)/Q(z)$ and hence $b_n = |3^n - 2^n|_5^{-1}$ forms a recurrence sequence. The Taylor series coefficients are given by

$$b_n = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 5^{1+\mathrm{ord}_5(n)} & \text{if } n \text{ is even} \end{cases}$$

By the above Proposition the number of values that b_n can take on infinitely often is bounded by some integer depending on the roots of $Q(z)$. However, the set $\{1, 5, 5^2, \ldots\}$ is infinite, giving a contradiction. Hence ζ_α is irrational. □

Example 3.31. Let $k = \mathbb{F}_p(t)$ and $S = \{t\}$. Define α to be the endomorphism of $\widehat{R}_S = \mathbb{F}[t^{\pm 1}]$ dual to multiplication by t on $\mathbb{F}_p[t^{\pm 1}]$. The entropy of α is

$$h(\alpha) = \sum_{v \leq \infty} \log^+ |t|_v = \log p$$

and the number of periodic points is given by

$$|F_n(\alpha)| = |t^n - 1|_\infty |t^n - 1|_t = p^n.$$

Alternatively, we may note that $\widehat{R}_S \cong \widehat{\oplus_{\mathbb{Z}} \mathbb{F}_p} \cong \mathbb{F}_p^{\mathbb{Z}}$ and that α is the one-sided shift action on p symbols. Thus the entropy and the number of periodic points are as expected. The zeta function is rational and $\zeta_\alpha(z) = \frac{1}{1-pz}$.

Example 3.32. Let $k = \mathbb{F}_p(t)$ and $S = \{t-1\}$. Define α to be the endomorphism of $\widehat{R}_S = \widehat{\mathbb{F}_p[t][\frac{1}{t-1}]}$ dual to multiplication by t on $\mathbb{F}_p[t][\frac{1}{t-1}]$. The entropy of α is again $\log p$ and the number of periodic points is

$$|F_n(\alpha)| = |t^n - 1|_\infty |(1 + t - 1)^n - 1|_{t-1} = p^{n - p^{\mathrm{ord}_p(n)}}.$$

Suppose that ζ_α is rational, so $\sum_{n=1}^{\infty} |F_n(\alpha)| z^n$ is also rational. We know that $\sum_{n=1}^{\infty} p^n z^n = \frac{1}{1-pz}$ is rational. Using the method similar to that in Example 3.28 we see that

$$\frac{p^n}{|F_n(\alpha)|} = p^{p^{\mathrm{ord}_p(n)}}$$

is a recurrence sequence in $\mathbb{Z}$, and by Theorem 3.29

$$\sum_{n=1}^{\infty} p^{p^{\mathrm{ord}_p(n)}} z^n$$

would then be a rational function. However, the sequence $p^{p^{\mathrm{ord}_p(n)}}$ has an infinite number of values that it takes on infinitely often namely $\{p, p^p, p^{p^2}, \ldots\}$. This contradicts Proposition 3.30 and therefore implies that ζ_α is irrational, and so α is non-expansive.

Chapter 4

Counting Orbits

4.1 Prime Number Theorem

Let $\pi(x)$ denote the number of primes not exceeding x. Then the classical Prime Number Theorem states that

$$\pi(x) \sim \frac{x}{\log x}, \text{ as } x \to \infty.$$

This was conjectured by Gauss and Legendre and not proved until much later. There is an *analytic* proof of this in many books and an elementary proof has been found (see [12]). The analytic method uses complex analysis and the meromorphic extension of the Riemann Zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

Much earlier Chebyshev proved a weaker version of the Prime Number Theorem.

Theorem 4.1. *The order of magnitude of $\pi(x)$ is $x/\log(x)$:*

$$\pi(x) \asymp \frac{x}{\log(x)}.$$

That is, there exist constants $A, B \in (0, \infty)$ with

$$A \cdot \frac{x}{\log(x)} \leq \pi(x) \leq B \cdot \frac{x}{\log(x)},$$

for all x.

4.2 Prime Orbit Theorem

Parry and Pollicott [23] showed an analogy between the number of closed orbits of Axiom A flows (actions of $\mathbb{R}$ analogous to hyperbolic invertible maps viewed as $\mathbb{Z}$-actions) and the Prime Number Theorem. The main result was that if φ is an Axiom A diffeomorphism restricted to a non-trivial basic set Λ with topological entropy $h = h(\varphi|\Lambda)$, and τ denotes a generic prime closed orbit of $\varphi|\Lambda$ with least period $\lambda(\tau)$, then

$$|\{\tau : \lambda(\tau) \leq x\}| \sim \frac{e^{h(x+1)}}{(e^h - 1)x} \tag{9}$$

as $x \to \infty$ through the positive integers. The proof of this involves Markov partitions and the associated symbolic dynamics, together with a meromorphic extension of an associated zeta function. Similar results hold for hyperbolic maps. Waddington [29] later extended this analogy to the least periods of closed orbits of ergodic automorphisms of the N-torus. Examples of these can be found in Section 3.5. The main result of [29] is an asymptotic formula for the number of periodic orbits for quasi-hyperbolic toral automorphisms. The term 'quasihyperbolic' in his paper is used to describe ergodic automorphisms that are not hyperbolic.

Waddington's Prime Orbit Theorem is highly dependent on the behaviour of the dynamical zeta function on the circle at the radius of convergence and beyond.

Let $T : \mathbb{T}^n \to \mathbb{T}^n$ be an ergodic automorphism and let τ be a generic prime closed orbit with least period $\lambda(\tau)$. Set $\pi(x) = |\{\tau : \lambda(\tau) \leq x\}|$, that is, the number of orbits of least period not exceeding x. Then Waddington shows there is a finite set $U \subset \mathbb{S}^1$, and integers $K(\rho)$ for $\rho \in U$, such that

$$\pi(x) \sim \frac{e^{h(x+1)}}{x} \sum_{\rho \in U} K(\rho) \frac{\rho^{(x+1)}}{\rho e^h - 1}, \tag{10}$$

as $x \to \infty$ through the positive integers. The set U is comprised of the eigenvalues of modulus 1, together with 1, and so lie on the unit circle, and has:-

$$\text{(a)} 1 \in U \text{ and (b) if } u \in U \text{ then } \overline{u} \in U.$$

In the proof, the Artin-Mazur zeta function for dynamical systems is used in a similar way to the Riemann zeta function used in the analytic proof of the Prime Number Theorem in Section 4.1.

The proof relies on the fact that the Artin-Mazur zeta function can be meromorphically continued beyond the radius of convergence for these types of maps. A complete proof of the above formula can be found in [29].

4.3 Iterations of a Map

Recall that $O_n(T) = L_n(T)/n$ from (3) in Section 2.1. Then

$$F_n(T) = \sum_{d|n} L_d(T). \tag{11}$$

We can therefore determine the sequence of values of one of these quantities from the other. A consequence of this is a relationship between the number of orbits of a map and the number of orbits of its iterates which will be needed in particular cases further on.

Lemma 4.2. *Let $T : X \to X$ be a map. Define $O_n(T^k)$ to be the number of orbits under the map T^k of length n. Then*

$$O_n(T^k) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)\sum_{d'|dk} d' O_{d'}(T)$$

Proof. Let $a_n = F_n(T)$, then $F_n(T^k) = F_{nk}(T) = a_{nk}$. Then

$$\begin{aligned}
O_n(T^k) &= \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)F_d(T^k) \\
&= \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)a_{dk} \\
&= \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)\sum_{d'|dk} d' O_{d'}
\end{aligned}$$

$\square$

Example 4.3. Consider the expression for $O_n(T^2)$.

By (11) and (3),

$$O_n(T^2) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)F_{2d}(T).$$

First assume that n is odd, so all divisors d are odd. Then,

$$\begin{aligned}
O_n(T^2) &= \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)F_{2d}(T) - \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)F_d(T) + \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)F_d(T) \\
&= \frac{1}{n}\sum_{d|2n}\mu\left(\frac{2n}{d}\right)F_d(T) + \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)F_d(T) \\
&= 2\cdot\frac{1}{2n}\sum_{d|2n}\mu\left(\frac{2n}{d}\right)F_d(T) + \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)F_d(T) \\
&= 2O_{2n}(T) + O_n(T).
\end{aligned}$$

When n is even, notice that when a divisor d is odd $\mu\left(\frac{2n}{d}\right) = 0$.

So,

$$\begin{aligned} O_n(T^2) &= \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)F_{2d}(T) \\ &= 2\cdot\frac{1}{2n}\sum_{d|2n}\mu\left(\frac{2n}{d}\right)F_d(T) \\ &= 2O_{2n}(T). \end{aligned}$$

So we can deduce that,

$$O_n(T^2) = \begin{cases} 2O_{2n}(T) + O_n(T) & \text{if } n \text{ is odd ;} \\ 2O_{2n}(T) & \text{if } n \text{ is even} \end{cases}$$

4.4 Natural Boundary

Let D be a domain in $\mathbb{C}$, and ∂D be the boundary of D. Let g be a function such that $g : D \to \mathbb{C}$. If g cannot be analytically continued beyond ∂D, then we say that ∂D is the natural boundary of g.

Example 4.4. Let $g(z) = \sum_{n=0}^{\infty} z^{2^n} = z + z^2 + z^4 + \ldots$. Then $g(z)$ converges for $|z| < 1$. It is clear that $\lim_{z\to\xi} g(z) = \infty$ for any ξ with $\xi^{2^n} = 1$. So the boundary ∂D of the circle, radius 1 is a natural boundary for the function g.

4.5 The Prime Orbit Theorem for other maps

We want to try and apply the Prime Orbit Theorems of [23] and [29] to Example (1) in Section 2.1 and to see if it would be possible to obtain a similar Prime Orbit Theorem to maps from Section 3.2.

Example (1) from Section 2.1 is the circle doubling map. Let X denote the unit interval with its end points identified, $X = \mathbb{R}/\mathbb{Z} = \mathbb{T}$. Define a continuous map

$T : X \to X$ by $T(x) = 2x \bmod 1$ i.e.

$$T(x) = \begin{cases} 2x & 0 \le x < 1/2; \\ 2x - 1 & 1/2 \le x \le 1 \ . \end{cases}$$

The sequence of periodic points is $F_n(T) = 2^n - 1$, the Mersenne sequence. This map is non-invertible as every point has 2 pre-images but it is a forwardly expanding map since it doubles distances locally on X. This map behaves like a hyperbolic automorphism and so we can apply the Prime Orbit Theorem of Parry and Pollicott in [23]. The topological entropy of the system is $h(T) = \log 2$. The Artin-Mazur zeta function for this map is

$$\zeta(z) = \exp \sum_{n=1}^{\infty} \frac{z^n}{n}(2^n - 1) = \frac{1-z}{1-2z}.$$

This is a rational function and has a singularity at $z = \exp(-h(T)) = 1/2$ and a zero at $z = 1$. Following the argument in [23], we arrive at the asymptotic

$$\pi(x) \sim \frac{2^{(x+1)}}{x}, \tag{12}$$

where $\pi(x)$ is the number of orbits less than the given number x.

Let

$$T_a(x) : x \to ax \pmod 1,$$

be a map, where $a > 1$ is an integer, then $F_n(T) = a^n - 1$. This is a generalization of the doubling map. The Artin-Mazur zeta function is rational,

$$\zeta(z) = \exp \sum_{n=1}^{\infty} \frac{z^n}{n}(a^n - 1) = \frac{1-z}{1-az},$$

and the Prime Orbit Theorem is

$$\pi(x) \sim \frac{a^{(x+1)}}{x} \frac{1}{(a-1)}.$$

Chapter 5

S-Integer Dynamical Systems: Zero Characteristic

5.1 An S-Integer Dynamical System

Consider the map $\phi : x \to 2x$ on the ring $\mathbb{Z}[\frac{1}{3}]$. We cannot use the Prime Orbit Theorem of Parry and Pollicott since the dual of ϕ does not behave like a hyperbolic function in the way the 'circle doubling map' does. Is is possible to use Waddington's method in [29] to find a Prime Orbit Theorem for this map? Write $X = \widehat{\mathbb{Z}[\frac{1}{3}]}$ for the dual (character) group, and $f = \widehat{\phi}$ for the dual map. Then the topological entropy is $\log 2$ and the number of points of period n under f is $F_n(\phi) = (2^n - 1)|2^n - 1|_3$. This can be thought of as an extension of the circle doubling map by a cocycle taking values in $\mathbb{Z}_3$, the 3-adic integers. This extension kills certain periodic orbits.

n	1	2	3	4	5	6	7	8	9	10
Periodic points $2^n - 1$	1	3	7	15	31	63	127	255	511	1023
Periodic points $(2^n-1)\vert 2^n-1\vert_3$	1	1	7	5	31	7	127	85	511	341
#Orbits in Circle Doubling Map	1	1	2	3	6	9	18	30	56	99
#Orbits under ϕ	1	0	2	1	6	0	18	10	56	31

From the table we expect that for odd n, the number of periodic points and orbits for 2^n-1 is equal to those for $(2^n-1)|2^n-1|_3$. When n is even the number of periodic points seems to be reduced by a factor of a power of 3. (This is dependent on how divisible by 3 n is.) The rationality of the Artin-Mazur zeta function is crucial in the method of Waddington's prime orbit theorem.

First, notice that

$$\begin{aligned} |2^n-1|_3 &= |(3-1)^n-1|_3 \\ &= |3^n - n3^{n-1} + \cdots + (-1)^{n-1}3n + (-1)^n - 1|_3 \\ &= \begin{cases} \frac{1}{3}|n|_3 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd} \end{cases} \end{aligned}$$

In particular

$$|4^n-1|_3 = |2^{2n}-1|_3 = \frac{1}{3}|2n|_3 = \frac{1}{3}|n|_3. \tag{13}$$

Since $|n|_3 = 3^{-\mathrm{ord}_3(n)} \geq 3^{-\log_3(n)} \geq 1/n$, it follows that

$$\frac{1}{3n} \leq |2^n-1|_3 \leq 1 \text{ for all } n \geq 1, \tag{14}$$

so just as for the circle doubling map, Example (2.2)(1) in Section 2.1, the logarithmic growth rate of periodic points gives the topological entropy,

$$\frac{1}{n}\log F_n(f) \longrightarrow \log 2 = h(f).$$

The Artin-Mazur zeta function for the map f is

$$\zeta(z) = \exp \sum_{n=1}^{\infty} \frac{z^n}{n}(2^n - 1)|2^n - 1|_3,$$

and so the radius of convergence is $\exp(-h(f)) = 1/2$.

From the bound in (14) we can see that the number of periodic points for the circle doubling map is only polynomially larger than the number of periodic points for f. This makes a real difference though unlike the circle doubling map, a hyperbolic case, $\frac{F_{n+1}(f)}{F_n(f)}$ does not converge as $n \to \infty$.

We will see that the dynamical zeta function of f has a natural boundary and so cannot be meromorphically continued, and has a natural boundary at $|z| = 1/2$.

Proposition 5.1. *The dynamical zeta function of f has a natural boundary at $|z| = 1/2$.*

Proof. Let $\xi(z) = \sum_{n=1}^{\infty} \frac{z^n}{n}(2^n - 1)|2^n - 1|_3$ so $\zeta(z) = \exp(\xi(z))$.

$$
\begin{aligned}
\xi(z) &= z + \frac{z^2}{2} + \frac{7z^3}{3} + \frac{5z^4}{4} + \frac{31z^5}{5} + \frac{7z^6}{6} + \frac{127z^7}{7} + \frac{85z^8}{8} + \ldots \\
&= (z + \frac{7z^3}{3} + \frac{31z^5}{5} + \frac{127z^7}{7} + \ldots) + (\frac{z^2}{2} + \frac{5z^4}{4} + \frac{7z^6}{6} + \frac{85z^8}{8} + \ldots) \\
&= \sum_{n=0}^{\infty} \frac{z^{2n+1}}{2n+1}(2^{2n+1}-1) + \sum_{n=1}^{\infty} \frac{z^{2n}}{2n}(2^{2n}-1)|2^{2n}-1|_3 \\
&= \sum_{n=0}^{\infty} \frac{z^{2n+1}}{2n+1}(2^{2n+1}-1) + \sum_{n=1}^{\infty} \frac{z^{2n}}{2n}(2^{2n}-1) - \sum_{n=1}^{\infty} \frac{z^{2n}}{2n}(2^{2n}-1) + \\
&\qquad \sum_{n=1}^{\infty} \frac{z^{2n}}{2n}(2^{2n}-1)|2^{2n}-1|_3 \\
&= \sum_{n=1}^{\infty} \frac{z^n}{n}(2^n-1) - \frac{1}{2}\sum_{n=1}^{\infty} \frac{z^{2n}}{n}(2^{2n}-1) + \sum_{n=1}^{\infty} \frac{z^{2n}}{2n}(2^{2n}-1)|2^{2n}-1|_3 \\
&= \sum_{n=1}^{\infty} \frac{(2z)^n}{n} - \sum_{n=1}^{\infty} \frac{z^n}{n} - \frac{1}{2}\sum_{n=1}^{\infty} \frac{(4z^2)^n}{n} + \frac{1}{2}\sum_{n=1}^{\infty} \frac{(z^2)^n}{n} + \\
&\qquad \sum_{n=1}^{\infty} \frac{z^{2n}}{2n}(2^{2n}-1)|2^{2n}-1|_3 \\
&= -\log(1-2z) + \log(1-z) + \log(1-4z^2)^{1/2} - \log(1-z^2)^{1/2} + \\
&\qquad \sum_{n=1}^{\infty} \frac{z^{2n}}{2n}(2^{2n}-1)|2^{2n}-1|_3 \\
&= \log\left(\frac{1-z}{1-2z}\right) + \frac{1}{2}\log\left(\frac{1-4z^2}{1-z^2}\right) + \sum_{n=1}^{\infty} \frac{z^{2n}}{2n}(2^{2n}-1)|2^{2n}-1|_3.
\end{aligned}
$$

Write $\frac{1}{6}\xi_1(z)$ for the term $\sum_{n=1}^{\infty} \frac{z^{2n}}{2n}(2^{2n}-1)|2^{2n}-1|_3$, so

$$
\begin{aligned}
\xi_1 &= 3\sum_{n=1}^{\infty} \frac{z^{2n}}{n}(4^n-1)|4^n-1|_3 \\
&= \sum_{n=1}^{\infty} \frac{z^{2n}}{n}(4^n-1)|n|_3
\end{aligned}
$$

by (13). The following shows that $\xi_1(z)$ has infinitely many logarithmic singularities on the circle $|z| = \frac{1}{2}$. Each of these zeros correspond to a zero of $\zeta(z)$. Recall from

Section 1.1 that $3^a \parallel n$ means that $3^a \mid n$ but $3^{a+1} \nmid n$. Notice that $3^a \parallel n$ if and only if $|n|_3 = 3^{-a}$. This means we can split up ξ_1 in terms of $|n|_3$ since

$$\begin{aligned} \xi_1 &= \sum_{j=0}^{\infty} \frac{1}{3^j} \sum_{3^j \parallel n} \frac{z^{2n}}{n}(4^n - 1) \\ &= \sum_{j=0}^{\infty} \frac{1}{3^j} \eta_j^{(4)}(z), \end{aligned}$$

where

$$\eta_j^{(a)}(z) = \sum_{3^j \parallel n} \frac{z^{2n}}{n}(a^n - 1).$$

Then

$$\begin{aligned} \eta_0^{(a)}(z) &= \sum_{3^0 \parallel n} \frac{z^{2n}}{n}(a^n - 1) \\ &= \sum_{n=1}^{\infty} \frac{z^{2n}}{n}(a^n - 1) - \sum_{n=1}^{\infty} \frac{z^{6n}}{3n}(a^{3n} - 1) \\ &= \log\left(\frac{1 - z^2}{1 - az^2}\right) - \frac{1}{3}\log\left(\frac{1 - z^6}{1 - a^3 z^6}\right), \end{aligned}$$

$$\eta_1^{(4)}(z) = \sum_{3^1 \parallel n} \frac{z^{2n}}{n}(4^n - 1) = \sum_{3^0 \parallel n} \frac{z^{6n}}{3n}(4^{3n} - 1) = \frac{1}{3}\eta_0^{(4^3)}(z^3),$$

$$\eta_2^{(4)}(z) = \frac{1}{9}\eta_0^{(4^9)}(z^9),$$

and so on. Therefore

$$\xi_1(z) = \log\left(\frac{1 - z^2}{1 - (2z)^2}\right) + 2\sum_{j=1}^{\infty} \frac{1}{9^j} \log\left(\frac{1 - (2z)^{2\times 3^j}}{1 - z^{2\times 3^j}}\right),$$

so we have

$$|\zeta(z)| = \left|\frac{1 - z}{1 - 2z}\right| \cdot \left|\frac{1 - (2z)^2}{1 - z^2}\right|^{1/2} \cdot \left|\frac{1 - z^2}{1 - (2z)^2}\right|^{1/6} \cdot \prod_{j=1}^{\infty} \left|\frac{1 - (2z)^{2\times 3^j}}{1 - z^{2\times 3^j}}\right|^{1/3\times 9^j}.$$

So the series defining $\zeta(z)$ has a zero at all points of the form $\frac{1}{2}\exp(2\pi i j/3^r)$. Thus $|z| = \frac{1}{2}$ is a natural boundary for $\zeta(z)$. $\square$

By Section 4.4, a function that has a natural boundary such as $\zeta(z)$ cannot be analytically continued. Section 4.2 explains that for Waddington's Prime Orbit Theorem proof to work it is necessary for the dynamical zeta function to be meromorphically continued beyond the radius of convergence. As this is not possible for our function f we are unable to use this method.

5.2 Numerical Evidence

Since we were unable to find an asymptotic using Waddington's methods it was necessary to study the actual numerics of the number of orbits in the map $\phi : x \to 2x$ on the dual of the ring $\mathbb{Z}[\frac{1}{3}]$.

For this we had to use the orbit counting method described in Section 2.4 . To count the number of orbits for the function f we use the formula

$$\sum_{n\leq x} \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right)(2^d - 1)|2^d - 1|_3.$$

The pattern of this sequence using the GP/Pari program was studied and compared to that of

$$\sum_{n\leq x} \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right)(2^d - 1),$$

the number of orbits less than x for the circling doubling map from Example (1) Section 2.1, whose asymptotics are well-known.

Let

$$\pi_f(x) = \sum_{n\leq x} \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right)(2^d - 1)|2^d - 1|_3$$

and

$$\pi_g(x) = \sum_{n\leq x} \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right)(2^d - 1),$$

where $\pi_a(x)$ is the number of orbits of a map a with length up to a given number x. It appears that while $\pi_g(x)$ grows very steadily, $\pi_f(x)$ is very erratic in its growth. By comparing $\pi_f(x)$ to the asymptotic $\frac{2^{(x+1)}}{x}$ we can see that a pattern emerges. The values alternate between high and low values, so appear not to converge. Numerically, $\pi_f(x)/\frac{2^{(x+1)}}{x}$ has its lowest value of approximately 0.41 and a highest value of approximately 0.79. The following graph shows a sample of values from $x = 0$ to 100. We see that the lowest values occur when x is even and the higher values occur when x is odd.

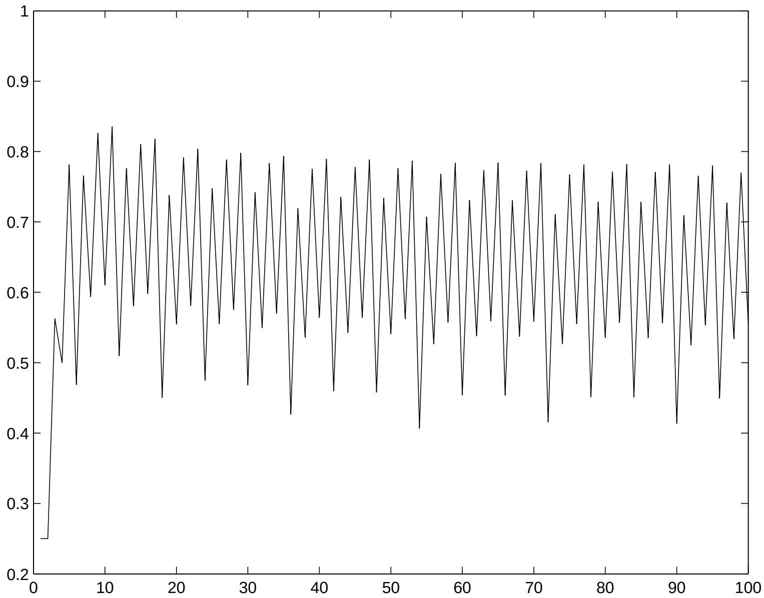

Figure 1: Graph of $(\pi_f(x) * x)/2^{(x+1)}$

5.3 Prime orbit theorem: one prime

Since we could not use Waddington's methods we looked for other ways to see how we could approximate $\pi_f(x)$. We looked at Tchebyshev's Prime Number Theorem and how he obtained upper and lower bounds. From Section 5.2 we expect upper and lower limits.

The first theorem shows some asymptotic bounds for $\pi_f(x)$. The results for this are reached by comparing this function with the asymptotics for the circle-doubling map from Section 2.1. This we already understand from Parry and Pollicott. In the circle-doubling map g, let $F_n(g) = 2^n - 1, O_n(g) = \frac{1}{n}\sum_{d|n}\mu(n/d)(2^d - 1)$, and (12) in Section 4.5 shows that

$$\pi_g(x) = \sum_{n\leq x}\frac{1}{n}\sum_{d|n}\mu(n/d)(2^d - 1) \sim \frac{2^{x+1}}{x}. \tag{15}$$

Theorem 5.2. *Let f be the endomorphism dual to $x \to 2x$ on $\mathbb{Z}[\frac{1}{3}]$. Then*

$$\pi_f(x) \leq \pi_g(x) \textit{ for all } x \geq 1,$$

and

$$\limsup_{x\to\infty}\frac{x\cdot\pi_f(x)}{2^{x+1}} \leq 1, \ \liminf_{x\to\infty}\frac{x\cdot\pi_f(x)}{2^{x+1}} \geq \frac{1}{3}.$$

Proof. Let $F_n(g) = 2^n - 1$ and let $F_n(f) = (2^n - 1)|2^n - 1|_3$, so

$$\pi_g(x) = \sum_{n\leq x} O_n(g) = \sum_{n\leq x}\frac{1}{n}\sum_{d|n}\mu(n/d)F_d(g)$$

and

$$\pi_f(x) = \sum_{n\leq x} O_n(f) = \sum_{n\leq x}\frac{1}{n}\sum_{d|n}\mu(n/d)F_d(f).$$

We first claim that

$$\pi_f(x) \leq \pi_g(x) \text{ for all } x \geq 1, \tag{16}$$

When n is odd, $F_n(f) = F_n(g)$ so $O_n(f) = O_n(g)$, since all factors of n are odd.

Now assume that n is even and note that

$$\sum_{d|n, d<n} (2^d - 1) \leq \frac{2}{3}(2^n - 1), \text{ for all } n \geq 1. \tag{17}$$

It follows that

$$\begin{aligned}
L_n(f) &= \sum_{d|n} \mu(n/d) F_d(f) \\
&\leq F_n(f) \\
&\leq \frac{1}{3} F_n(g) \\
&\leq F_n(g) - \sum_{d|n, d<n} F_d(g) \\
&\leq \sum_{d|n} \mu(n/d) F_d(g) = L_n(g).
\end{aligned}$$

Thus, $O_n(f) \leq O_n(g)$ for all $n \geq 1$ so (16) is proved and hence the upper bound is proved.

Now, turning to the lower bound, we know from (16) above that $O_n(f) \leq O_n(g)$. Therefore $\pi_f(x) + \Delta_x = \pi_g(x)$, hence, $\pi_g(x) - \Delta_x = \pi_f(x)$, where

$$\Delta_x = \left| \sum_{n \leq x} (O_n(g) - O_n(f)) \right| = \left| \sum_{2|n \leq x} (O_n(g) - O_n(f)) \right| \leq \sum_{2|n \leq x} O_n(g).$$

How big is $\sum_{2|n \leq x} O_n(g)$? Notice that

$$\sum_{2|n \leq x} O_n(g) = \sum_{n \leq [x/2]} O_{2n}(g) \leq \frac{1}{2} \sum_{n \leq [x/2]} O_n(g^2), \text{ and}$$

$$O_{2n}(g) = \frac{1}{2n} \sum_{d|2n} \mu(2n/d) \mathcal{F}_d(g), \text{ so}$$

$$O_{2n}(g) = \frac{1}{2n} \sum_{d|2n} \mu\left(\frac{2n}{d}\right)(2^d - 1) \text{ and } F_n(g^2) = 2^{2n} - 1 = 4^n - 1.$$

Since g^2 is the map $x \to 4x \bmod 1$ on the circle and is hyperbolic, we have

$$\sum_{n\leq x} O_n(g^2) \sim \frac{4^{(x+1)}}{3x}.$$

By Lemma 4.2

$$O_n(g^2) = \begin{cases} 2O_{2n}(g) + O_n(g) & \text{if } n \text{ is odd ;} \\ 2O_{2n}(g) & \text{if } n \text{ is even.} \end{cases}$$

So,

$$O_{2n}(g) = \begin{cases} \frac{(O_n(g^2) - O_n(g))}{2} & \text{if } n \text{ is odd ;} \\ \frac{O_n(g^2)}{2} & \text{if } n \text{ is even.} \end{cases}$$

Hence,

$$\begin{aligned} \sum_{n\leq x} O_{2n}(g) &= \sum_{2\nmid n\leq x} \frac{1}{2}\left(O_n(g^2) - O_n(g)\right) + \sum_{2|n\leq x} \frac{1}{2}\left(O_n(g^2)\right) \\ &= \sum_{n\leq x} \frac{1}{2}\left(O_n(g^2)\right) - \sum_{2\nmid n\leq x} \frac{1}{2}\left(O_n(g)\right). \end{aligned}$$

Since $\sum_{n\leq x} O_n(g^2) \sim \frac{4^{(x+1)}}{3x}$,

$$\sum_{n\leq x} O_{2n}(g) \sim \frac{1}{2}\cdot\frac{4^{(x+1)}}{3x} - \sum_{2\nmid n\leq x} \frac{1}{2}(O_n(g)).$$

The last term, $O_n(g) \sim \frac{2^{x+1}}{x}$, is of lower order and as it will not effect the term of higher order, we can for our purposes ignore it. It follows that,

$$\sum_{n\leq x} O_{2n}(g) \sim \frac{1}{2}\cdot\frac{4^{(x+1)}}{3x} = \frac{2}{3}\cdot\frac{4^x}{x}$$

so

$$\sum_{2|n\leq x} O_n(g) = \sum_{n\leq[x/2]} O_{2n}(g) \sim \frac{2}{3}\cdot\frac{4^{x/2}}{x/2} = \frac{2}{3}\cdot\frac{2^{x+1}}{x}.$$

Thus, we have

$$\sum_{n\leq x} O_n(g) - \sum_{2|n\leq x} O_n(g) \sim \frac{2^{x+1}}{x} - \frac{2}{3}\cdot\frac{2^{x+1}}{x} = \frac{1}{3}\cdot\frac{2^{x+1}}{x} \leq \sum_{n\leq x} O_n(f) = \pi_f(x).$$

So we have

$$\limsup_{x\to\infty} \frac{x \cdot \pi_f(x)}{2^{x+1}} \leq 1, \ \ \liminf_{x\to\infty} \frac{x \cdot \pi_f(x)}{2^{x+1}} \geq \frac{1}{3},$$

the required result. $\square$

Is the lim sup is greater than the lim inf? The numerics in Section 5.2 certainly suggest that this is the case and moreover that the sequence $\left(\frac{x \cdot \pi_f(x)}{2^{x+1}}\right)_{x \geq 1}$ has more than two limit points. However, I have been unable to provide a proof of this, and at this stage can only show that this appears to be true from the graph, see Figure 1, Section 5.2.

Theorem 5.2 has an analogue for any prime p and the proof can be adapted accordingly. In general,

Theorem 5.3. *Let f be the endomorphism dual to $x \to 2x$ on $\mathbb{Z}[\frac{1}{p}]$. Let*

$$\pi_g(x) = \sum_{n \leq x} \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right)(2^d - 1)$$

and

$$\pi_f(x) = \sum_{n \leq x} \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right)(2^d - 1)|2^d - 1|_p$$

then

$$\pi_f(x) \leq \pi_g(x) \text{ for all } x \geq 1,$$

and

$$\limsup_{x\to\infty} \frac{x\pi_f(x)}{2^{x+1}} \leq 1, \ \ \liminf_{x\to\infty} \frac{x\pi_f(x)}{2^{x+1}} \geq 1 - \frac{2^{(p-2)}}{2^{(p-1)} - 1}.$$

For a finite set of primes we would expect similar results to hold with different constants, but the arguments become much more complex.

5.4 Prime orbit theorem: infinitely many primes

The maps in Section 5.3 are small perturbations of the circle doubling map in the sense of [33]. At the opposite extreme, if S contains all the primes, then the corresponding map f has $\pi_f(x) = 1$ for all x. A small perturbation of this (highly non-hyperbolic) map includes all but one prime.

Consider the map $\phi : x \to 2x$ on the ring $\mathbb{Z}[\frac{1}{2}, \frac{1}{5}, \frac{1}{7}, \frac{1}{11}, \ldots] = \mathbb{Z}_{(3)}$, see Definition 1.1. Write $X = \widehat{\mathbb{Z}[\frac{1}{2\cdot5\cdot7\cdot11\cdots}]}$ for the dual (character) group, and $h = \widehat{\phi}$ for the dual map. By Theorem 3.11, the topological entropy is $\log 2$. The number of points of period n under h is calculated as follows:

n	1	2	3	4	5	6	7	8	9	10
$2^n - 1$	1	3	7	15	31	63	127	255	511	1023
$\lvert 2^n - 1\rvert_5$	1	1	1	1/5	1	1	1	1/5	1	1
$\lvert 2^n - 1\rvert_7$	1	1	1/7	1	1	1/7	1	1	1/7	1
$\lvert 2^n - 1\rvert_{11}$	1	1	1	1	1	1	1	1	1	1/11
$\vdots$						$\vdots$				
$(2^n - 1)\lvert 2^n - 1\rvert_5 \lvert 2^n - 1\rvert_7 \cdots$	1	3	1	3	1	9	1	3	1	3

So the number of periodic points is $(2^n - 1)|2^n - 1|_5|2^n - 1|_7 \cdots = |2^n - 1|_3^{-1}$, as all values are reduced by powers of all other primes.

This can be thought of as an extension of the circle doubling map by a cocycle taking values in $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{11} \times \ldots$. This extension kills all periodic orbits except those of period $n = 2 \cdot 3^k$. From the table above we expect that

$$F_n(h) = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 3^k \quad \text{for } k > 0 & \text{if } n \text{ is even.} \end{cases}$$

The following example shows this.

Example 5.4. Let $F_n = |2^n - 1|_3^{-1}$ and $O_n = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right)|2^d - 1|_3^{-1}$ then when $n = 2 \cdot 3^k$, $O_n = 1$.

Proof. When n is odd, $n = 2k - 1$ for some integer k, so

$$\begin{aligned}
2^n - 1 &= 2^{2k-1} - 1 \\
&= \frac{1}{2} \cdot 4^k - 1 \\
&= \frac{1}{2}\left((3+1)^k\right) - 1 \\
&= \frac{1}{2}(1 + 3k + \frac{k \cdot (k-1)}{2}3^2 + \ldots) - 1 \\
&= \frac{1}{2}(3c_1) - \frac{1}{2} \\
&= \frac{1}{2}(3c_1 - 1), \text{ for some integer } c_1.
\end{aligned}$$

Since $\frac{1}{2}(3c_1 - 1)$ is not a multiple of 3, $|2^n - 1|_3^{-1} = 1$ for all odd n. So

$$O_{2k-1} = \frac{1}{2k-1}\sum_{d|2k-1} \mu\left(\frac{2k-1}{d}\right)|2^d - 1|_3^{-1} = \frac{1}{2k-1}\sum_{d|2k-1} \mu\left(\frac{2k-1}{d}\right) = 0,$$

by Section 2.4.

When n is even, but not equal to $2 \cdot 3^k$, then $n = 2k$, for some integer k.

$$\begin{aligned}
2^n - 1 &= 2^{2k} - 1 \\
&= 4^k - 1 \\
&= \left((3+1)^k\right) - 1 \\
&= (1 + 3k + \frac{k \cdot (k-1)}{2}3^2 + \ldots) - 1 \\
&= 3c_2 \text{ for some constant } c_2.
\end{aligned}$$

So when n is even, $|2^n - 1|_3^{-1} \geq 3$ and by Section 2.4 the sum over the divisors all cancel each other out, so $O_n = 0$.

When $n = 2 \cdot 3^k$ for some integer k,

$$\begin{aligned}
O_{2\cdot 3^k} &= \frac{1}{2\cdot 3^k}\sum_{d|2\cdot 3^k}\mu\left(\frac{2\cdot 3^k}{d}\right)|2^d-1|_3^{-1} \\
&= \frac{1}{2\cdot 3^k}\left(\mu(3)\cdot 3^k+\mu(1)\cdot 3^{k+1}\right), \text{ by Section 2.4,} \\
&= \frac{1}{2\cdot 3^k}\left(-1\cdot 3^k+1\cdot 3^{k+1}\right) \\
&= \frac{1}{2\cdot 3^k}\left(3^k(-1+3)\right) \\
&= \frac{2\cdot 3^k}{2\cdot 3^k}=1.
\end{aligned}$$

□

The sum of the orbits grows very slowly. This meant that we could find an explicit formula for the number of orbits, as they only change when $n = 2 \cdot 3^k$.

The following theorem shows the formula for the number of orbits less than x for the above system.

Theorem 5.5. *Let h be the endomorphism dual to $x \to 2x$ on $\mathbb{Z}[\frac{1}{2}, \frac{1}{5}, \frac{1}{7}, \frac{1}{11}, \ldots]$. Then*

$$\pi_h(x) = \sum_{n\le x}\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)\prod_{p\ne 3}(2^d-1)|2^d-1|_p$$

$$= \sum_{n\le x}\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)\frac{1}{|2^d-1|_3}$$

and

$$\left|\pi_h(x) - \frac{\log(\frac{x}{2})}{\log 3}\right| \le 2.$$

Proof.

$$\text{Let } O_n(h) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)\prod_{p\ne 3}(2^d-1)|2^d-1|_p$$

$$= \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) \frac{1}{|2^d - 1|_3}$$

$$\text{then } O_n(h) = \begin{cases} 1 & n = 1 ; \\ 0 & \text{if } n \neq 2 \cdot 3^k ; \\ 1 & \text{if } n = 2 \cdot 3^k . \end{cases}$$

So, $O_n(h)$ increases by 1 each time $n = 2 \cdot 3^k$. When $x = 2 \cdot 3^k$, $k = \frac{\log(\frac{x}{2})}{\log 3}$.
Define $\pi_h(x) = \sum_{n \leq x} O_n(h)$ then

$$\pi_h(x) = \begin{cases} 1 & x = 1; \\ \pi_h(x-1) & \text{if } x \neq 2 \cdot 3^k ; \\ k+2 & \text{if } x = 2 \cdot 3^k . \end{cases}$$

When $x = 2, k = 0$ hence $\pi_h(x) = k + 2$. Since $\pi_h(x)$ is increasing, when $x \neq 2 \cdot 3^k$, $\pi_h(x) = \pi_h(2 \cdot 3^{k-1}) = k + 1 < k + 2$. Hence $|\pi_h(x) - \frac{\log(\frac{x}{2})}{\log 3}| \leq 2$. $\square$

5.5 Prime orbit theorem: finitely many primes

The maps in Sections 5.3 and 5.4 are the opposite extremes of perturbations of the circle doubling map. What would happen if S contained a finite number of primes? Consider, for example, the map $\phi : x \to 2x$ on the ring $\mathbb{Z}[\frac{1}{3}, \frac{1}{5}]$. Write $X = \widehat{\mathbb{Z}[\frac{1}{15}]}$ for the dual (character) group, and $b = \widehat{\phi}$ for the dual map. Then the topological entropy is $\log 2$ and the number of points of period n under b is $(2^n - 1)|2^n - 1|_3|2^n - 1|_5$. This can be thought of as an extension of the circle doubling map by a cocycle taking values in $\mathbb{Z}_3 \times \mathbb{Z}_5$.

By applying the method used for the dynamical system in Section 5.3, with periodic points $(2^n - 1)|2^n - 1|_3$, a similar prime orbit theorem is expected.

We can certainly say that

$$\pi_b(x) \leq \pi_g(x) \text{ for all } x \geq 1,$$

where $\pi_g(x)$ is the same as in Section 5.3 and

$$\limsup_{x\to\infty} \frac{x_{\pi_b}(x)}{2^{x+1}} \leq 1,$$

the proof of which follows the same arguments as before. It is, however, more difficult to obtain a lower limit bound for this case. The reason for this is because the method used in the proof for one prime in Section 5.3 does not work well for finitely many primes. In the proof for 'one prime' we are able to 'ignore' part of the calculation as it is of lesser order and will not affect the end result. However, with more than one prime, the parts of lesser order contribute too much to the result and we cannot simply 'ignore' them as we did before. The numerics showed this and for this reason we could not produce a result as before.

Chapter 6

S-Integer Dynamical Systems: Positive Characteristic

6.1 Prime orbit theorem for S-Integer systems of positive characteristic: one isometric direction

We now look at S-integer systems for positive characteristic to see what form the Prime Orbit Theorem takes in this setting.

We first consider a simple case that matched the criteria of Parry and Pollicott i.e. a hyperbolic map.

Example 6.1. Let p be a prime, let $k = \mathbb{F}_p(t)$ and $S = \{t\}$. Define g to be the endomorphism of $\hat{R}_S = \mathbb{F}_p^{\mathbb{Z}}$ dual to multiplication by t on $\mathbb{F}_p[t^{\pm 1}]$. The entropy of g is

$$h(g) = \sum_{v \leq \infty} \log^+ |t|_v = \log p \tag{18}$$

and the number of periodic points is given by

$$F_n(g) = |t^n - 1|_\infty |t^n - 1|_t = p^n. \tag{19}$$

In fact, g is the two-sided shift action on p symbols, so (18) and (19) are clear. The map g is an expansive ergodic automorphism and fits the model in [23]. The dynamical zeta function is rational: $\zeta_g(z) = \frac{1}{1-pz}$. By using the same techniques in Parry and Pollicott's Prime Orbit Theorem, (9) in Section 4.2 gives

$$\pi_g(x) \sim \frac{1}{p-1}\frac{p^{(x+1)}}{x},$$

where $\pi_g(x)$ is the number of orbits less than x.

So what happens if this dynamical system is perturbed slightly?

Example 6.2. Let $k = \mathbb{F}_p(t)$ and $S = \{t-1\}$. Define f to be the endomorphism of $\hat{R}_S = \widehat{\mathbb{F}_p[t][\frac{1}{t-1}]}$ dual to multiplication by t on $\mathbb{F}_p[t][\frac{1}{t-1}]$. The entropy of f is $\log p$ and the number of periodic points is given by

$$F_n(f) = |\mathcal{F}_n(f)| = |t^n - 1|_\infty |t^n - 1|_{t-1} = p^{n - p^{\mathrm{ord}_p(n)}}.$$

The dynamical zeta function is irrational and is explained in Example 8.5 in [4].

To study the numerics for a particular case, let $p = 2$. Then the number of periodic points in Example 6.1 is

$$F_n(g) = |t^n - 1|_\infty |t^n - 1|_t = 2^n,$$

so the dynamical zeta function $\zeta_g(z) = \exp \sum_{n=1}^{\infty} \frac{z^n}{n} \cdot 2^n = \frac{1}{1-2z}$ and the Prime Orbit Theorem is

$$\pi_g(x) \sim \frac{2^{(x+1)}}{x}.$$

The number of periodic points in Example 6.2 is

$$F_n(f) = |t^n - 1|_\infty |t^n - 1|_{t-1} = 2^{n - 2^{\mathrm{ord}_2(n)}}.$$

The dynamical zeta function $\zeta_f(z) = \exp \sum_{n=1}^{\infty} \frac{z^n}{n} 2^{n-2^{\mathrm{ord}_2(n)}}$, which we know from above that ζ_f is irrational and the topological entropy is $\log 2$. We are therefore, unable to use the same techniques in [23] or [29] to find a prime orbit theorem. The table below compares the the periodic points and number of orbits for Examples 6.1 and 6.2 using the counting method described in Section 2.4.

n	1	2	3	4	5	6	7	8	9	10
Periodic points 2^n	2	2	8	16	32	64	128	256	512	1024
Periodic points $2^{n-2^{\mathrm{ord}_2(n)}}$	1	1	4	1	16	16	64	1	256	256
#Orbits 2^n	2	1	2	3	6	9	18	30	56	99
#Orbits $2^{n-2^{\mathrm{ord}_2(n)}}$	1	0	1	0	3	2	9	0	28	24

By using the GP/Pari program and comparing Example 6.2 with Example 6.1 whose asymptotics are well known, the numerics suggest that $\pi_g(x)$ grows steadily but $\pi_f(x)$ grows erratically. By plotting the graph of $\frac{\pi_f(x) \cdot x}{2^{(x+1)}}$ you can see that it alternates in a similar way to that in the example in Section 5.2. The lowest value is approximately 0.2 and the highest value is approximately 0.4. The following graph shows a sample from $x = 0$ to 100. We see that the lowest values occur when x is even and the higher values occur when x is odd.

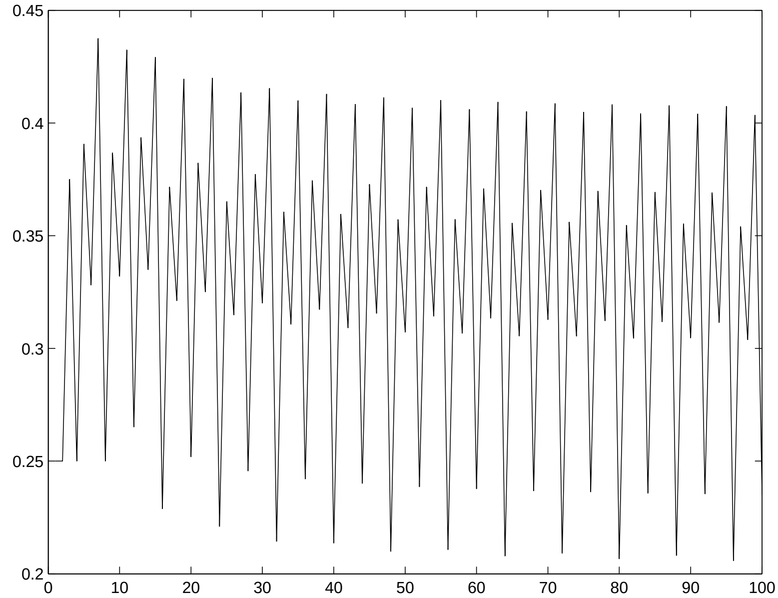

Figure 2: Graph of $(\pi_f(x) \cdot x)/2^{(x+1)}$

This is certainly a smaller span than that in Section 5.2 but there is no evidence of convergence. There are bounds for any prime p as shown in the following theorem.

Theorem 6.3. *Let f be the endomorphism of $\hat{R}_S = \widehat{\mathbb{F}_p[t][\frac{1}{t-1}]}$ dual to multiplication by t on $\mathbb{F}_p[t][\frac{1}{t-1}]$, and let g be the endomorphism of $\hat{R}_S = \mathbb{F}_p^{\mathbb{Z}}$ dual to multiplication by t on $\mathbb{F}_p[t^{\pm 1}]$. Then*

$$\pi_f(x) \leq \pi_g(x) \text{ for all } x \geq 1,$$

and

$$\limsup_{x\to\infty} \frac{x_{\pi_f}(x)}{p^x} \leq \frac{p}{p-1}, \ \liminf_{x\to\infty} \frac{x_{\pi_f}(x)}{p^x} \geq \frac{1}{p-1} - \frac{p^{p-1}}{p^p-1}.$$

For $p = 2$ as above, $\limsup \leq 2$ *and* $\liminf \geq 1 - \frac{2}{3} = \frac{1}{3}$.

Proof. Let $\pi_g(x) = \sum_{n \leq x} O_n(g)$ and $\pi_f(x) = \sum_{n\leq x} O_n(f)$, where

$$O_n(g) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$$

and

$$O_n(f) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)p^{d-p^{\mathrm{ord}_p(d)}}.$$

First consider, $\pi_f(x) \leq \pi_g(x)$ for all $x \geq 1$. When $p \nmid n$, $\mathrm{ord}_p(n) = 0$, so $p^{\mathrm{ord}_p(n)} = 1$.

Therefore,

$$O_n(f) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)p^{d-1} = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)\frac{1}{p}p^d = \frac{1}{p}O_n(g).$$

When $p \mid n$ then $n = pk$ that is not a power of p or $n = p^k$ for some $k \geq 1$.

Consider $n = p^k$, the divisors of n are $d = p^0, p^1, \ldots, p^k$.

Therefore,

$$O_n(f) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)p^{d-p^{\mathrm{ord}_p(d)}} = \frac{1}{n}\sum_{\substack{d|n\\ j=0,\ldots,k}}\mu\left(\frac{n}{d}\right)p^{p^j-p^j} = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right) = 0.$$

When $n = pk$, $p \mid n$ at least once.

Hence,

$$\begin{aligned} O_n(f) &= \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)p^{d-p^{\mathrm{ord}_p(d)}} \\ &\leq \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)p^{d-p} \\ &= \frac{1}{p^p}\sum_{n\leq x}\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)p^d \\ &= \frac{1}{p^p}O_n(g). \end{aligned}$$

So, $\pi_n(f) \leq \frac{1}{p^p}\pi_n(g) < \frac{1}{p}\pi_n(g) < \pi_n(g)$.

Therefore, $\pi_n(f) \leq \pi_n(g)$.

By Parry and Pollicott [23], $\pi_n(g) \sim (\frac{p}{p-1})\frac{p^x}{x}$ and hence

$$\limsup_{x\to\infty}\frac{x\cdot\pi_f(x)}{p^x} \leq \frac{p}{p-1}.$$

Consider the lower bound. We know

$$\begin{aligned}
\sum_{n\le x} O_n(f) &\le \frac{1}{p}\sum_{n\le x} O_n(g) \\
\Rightarrow \frac{1}{p}\sum_{n\le x} O_n(g) - \triangle_x &= \sum_{n\le x} O_n(f) \\
\Rightarrow \qquad\qquad \triangle_x &= \left| \frac{1}{p}\sum_{p|n\le x} O_n(g) - \sum_{p|n\le x} O_n(f) \right| \\
&\le \frac{1}{p}\sum_{p|n\le x} O_n(g),
\end{aligned}$$

since when $p \nmid n$, $\sum_{n\le x} O_n(f) = \frac{1}{p}\sum_{n\le x} O_n(g)$.

How big is $\frac{1}{p}\sum_{n\le x} O_n(g)$?

$$\sum_{p|n\le x} O_n(g) = \sum_{n\le[x/p]} O_{pn}(g)$$

Now g^p is the full shift on p symbols and in a similar way to Theorem 5.2, we can apply Parry and Pollicott's prime orbit theorem. So by [23],

$$\sum_{n\le x} O_n(g^p) \sim \frac{p^{p(x+1)}}{(p^p-1)x},$$

and

$$O_n(g^p) = \begin{cases} pO_{pn}(g) + O_n(g) & \text{if } n \ne pk; \\ pO_{pn}(g) & \text{if } n = pk \end{cases}$$

Hence,

$$\begin{aligned}
\sum_{n\le x} O_{pn}(g) &= \frac{1}{p}\sum_{p\nmid n\le x} O_n(g^p) - \sum_{p\nmid n\le x} O_n(g) + \frac{1}{p}\sum_{p|n\le x} O_n(g^p) \\
&= \sum_{n\le x} \frac{1}{p} O_n(g^p) - \sum_{p\nmid n\le x} \frac{1}{p} O_n(g).
\end{aligned}$$

Since, $\sum_{n\leq x} O_n(g^p) \sim \frac{p^{p(x+1)}}{(p^p-1)x}$,

$$\sum_{n\leq x} O_{pn}(g) \sim \frac{1}{p}\frac{p^{p(x+1)}}{(p^p-1)x} - \sum_{p\nmid n\leq x} \frac{1}{p} O_n(g).$$

The last term is of lower order and so for our purposes we can ignore it.

It follows that

$$\sum_{n\leq x} O_{pn}(g) \sim \frac{1}{p}\frac{p^{p(x+1)}}{(p^p-1)x} = \frac{p^{(p-1)}}{(p^p-1)} \cdot \frac{(p^p)^x}{x}.$$

So,

$$\sum_{p|n\leq x} O_n(g) = \sum_{n\leq[x/p]} O_{pn}(g) \sim \frac{p^{(p-1)}}{(p^p-1)} \cdot \frac{(p^p)^{x/p}}{x/p} = \frac{p^p}{(p^p-1)}\frac{p^x}{x}.$$

Hence, $\frac{1}{p}\sum_{p|n\leq x} O_n(g) \sim \frac{p^{(p-1)}}{(p^p-1)} \cdot \frac{p^x}{x}$.

So,

$$\frac{1}{p}\sum_{n\leq x} O_n(g) - \frac{1}{p}\sum_{p|n\leq x} O_n(g) \sim \left(\frac{1}{p-1} - \frac{p^{(p-1)}}{(p^p-1)}\right)\frac{p^x}{x}.$$

Thus,

$$\limsup_{x\to\infty} \frac{x\cdot\pi_f(x)}{p^x} \leq \frac{p}{p-1}, \quad \liminf_{x\to\infty} \frac{x\cdot\pi_f(x)}{p^x} \geq \frac{1}{p-1} - \frac{p^{p-1}}{p^p-1}.$$

□

6.2 Prime Orbit Theorem: infinitely many isometric directions

Now look at the other extreme where $S = \{$all irreducible polynomials except $(t-1)\}$.

Example 6.4. Let

$$k = \mathbb{F}_p(t) \text{ and } S = \{ \text{ all irreducible polynomials except } (t-1).$$

Define α to be the endomorphism of
$\hat{R}_S = \mathbb{F}_p[t][\text{ all irreducible }\widehat{\text{polynomials}}\text{ except }(t-1)]$ dual to multiplication by t on $\mathbb{F}_p[t][$ all irreducible polynomials except $(t-1)\}]$. The entropy of α is $\log p$ and the number of periodic points is given by

$$F_n(\alpha) = |\mathcal{F}_n(\alpha)| = |t^n - 1|_\infty \prod_{q \neq t-1} |t^n - 1|_q = p^{p^{\mathrm{ord}_p(n)}}.$$

Again the ζ_α function is irrational and α is not expansive, the growth rate of the orbits is very slow and we can obtain an asymptotic.

Theorem 6.5. *Let*

$$k = \mathbb{F}_p(t) \text{ and } S = \{\text{all irreducible polynomials except } (t-1)\}.$$

Let p be any prime and let α to be the endomorphism of
$\hat{R}_S = \mathbb{F}_p[t][\textit{ all irreducible }\widehat{\textit{polynomials}}\textit{ except }(t-1)$ *dual to multiplication by t on* $\mathbb{F}_p[t][$ *all irreducible polynomials except* $(t-1)]$, *then*

$$\limsup_{x\to\infty} \frac{x \cdot \pi_\alpha(x)}{p^x} = 1 \text{ and } \liminf_{x\to\infty} \frac{x \cdot \pi_\alpha(x)}{p^x} = 0.$$

Proof. Let $O_n(\alpha) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d}) p^{p^{\mathrm{ord}_p(d)}}$ and $\pi_\alpha(x) = \sum_{n \le x} O_n(\alpha)$.
Then

$$O_n(\alpha) = \begin{cases} p & \text{if } n = 1\ ; \\ 0 & \text{if } n \neq p^k; \\ \frac{1}{n}(p^n - p^{(\frac{n}{p})}) & \text{if } n = p^k \end{cases}$$

Now, $\pi_\alpha(x)$ only increases when $x = p^k$, so we only need to consider this case since for all other x, $\pi_\alpha(x) \le \frac{p^x}{x}$. When $x = p^k$,

$$\pi_\alpha(x) = \pi_\alpha(p^k) = \pi_\alpha\left(\frac{p^k}{p}\right) + \frac{1}{p^k}\left(p^{p^k} - p^{(\frac{p^k}{p})}\right) = \pi_\alpha(p^{k-1}) + p^{(p^k - k)} - p^{(p^{k-1} - k)}.$$

Now $\pi_\alpha(p^{k-1})$ and $p^{(p^{k-1}-k)}$ will contain terms of smaller order than $p^{(p^k-k)}$, and for our purposes we can ignore these as $x \to \infty$.

When $x = p^k$, $\frac{p^x}{x} = \frac{p^{p^k}}{p^k} = p^{(p^k-k)}$.

Hence as $x \to \infty$, $\pi_\alpha(x) \sim \frac{p^x}{x}$. $\square$

Chapter 7

Mertens' Theorem

7.1 Mertens' Theorem for prime numbers

For primes p the following asymptotic formula

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log x},$$

where γ is Euler's constant, is known as Mertens' theorem of analytic number theory. An elementary proof of this can be found in [10, pages 351-353]. The logarithmic equivalent of Mertens' theorem is

$$\sum_{n \leq x} \frac{1}{p} = \log \log x + B_1 + O\left(\frac{1}{\log x}\right),$$

where Mertens' constant $B_1 = \gamma + \sum_p \{\log(1 - \frac{1}{p}) + \frac{1}{p}\}$ has the value $0.2614972128\ldots$.

7.2 Mertens' Theorem for orbits

Sharp shows an analogy between the closed orbits of Axiom A flows and Mertens' theorem for prime numbers in [26]. Let ϕ be an Axiom A flow, let τ be a closed orbit for ϕ and let $\lambda(\tau)$ be its least period. Let $N(\tau) = e^{h\lambda(\tau)}$ where h is the entropy of ϕ. Then for an Axiom A flow φ,

$$\prod_{N(\tau)\leq x} \left(1 - \frac{1}{N(\tau)}\right) \sim \frac{e^{-\gamma}}{\mathrm{Res}(\zeta_\varphi, 1)\log(x)}$$

where ζ_φ is the Ruelle zeta function for φ. The proof of this in [26] relies on symbolic dynamics and follows analogous methods to the proof of Mertens' theorem for prime numbers in [10, pages 351-353].

This formula also holds for Axiom A diffeomorphisms like hyperbolic automorphisms of the finite dimensional torus.

Noorani [22] later extended Sharp's results to ergodic (not necessarily hyperbolic) toral automorphisms, (see Section 3.5) and provided the following theorem.

Theorem 7.1. *Let A be an ergodic (not necessarily hyperbolic) toral automorphism and let h be the topological entropy of A and for each closed orbit τ of A, let $\lambda(\tau)$ be its period. Also let $\zeta(z)$ be the zeta function of A. Then*

$$\prod_{\lambda(\tau)\leq x} \left(1 - \frac{1}{e^{h\lambda(\tau)}}\right) \sim \frac{e^{-m\gamma}}{x^m} v, \ \text{as } x \to \infty$$

where $m = 2^{d/2}$, d is the number of eigenvalues of A of modulus 1, γ is Euler's constant and v is the value of the non-zero and analytic function $\zeta(z)(1 - e^h z)^m$ at $z = e^{-h}$.

The proof is modelled on Sharp's paper which in turn is analogous to the number theoretic proof. The result for the toral automorphism can be derived directly without the need for symbolic models unlike the Axiom A diffeomorphisms which rely on the associated symbolic dynamics and zeta functions. This is because the corresponding zeta function, the Artin-Mazur zeta function, has a closed form that is readily understood.

Again using Example (1) from Section 2.1, the circle doubling map, we have the analogue of Mertens' theorem in Noorani's paper.

Firstly we have to write the formula

$$\prod_{\lambda(\tau)\leq x}\left(1-\frac{1}{e^{h\lambda(\tau)}}\right) \tag{20}$$

from [22] in a way that we can apply our counting method using the Möbius Inversion Formula.

For a hyperbolic toral automorphism A, let h be the topological entropy, let τ be a closed orbit of A, $\lambda(\tau)$ its least period and $\zeta(z)$ the dynamical zeta function. If O_n is the number of orbits of length n, then there are O_n number of $\tau's$ with $\lambda(\tau) = n$. Therefore we can express (20) in the form

$$\prod_{n\leq x}\left(1-\frac{1}{e^{hn}}\right)^{O_n}. \tag{21}$$

For computational purposes it is easier for us to use the logarithmic equivalent of Mertens' theorem, which from the formula above is

$$\sum_{n\leq x}\frac{O_n}{e^{hn}} = \log(x) + O(1). \tag{22}$$

So, for the circle doubling map, let $O_n(g) = \frac{1}{n}\sum_{n\leq\infty}\mu(\frac{n}{d})(2^d-1)$ and $h = \log 2$. So (22) becomes $\sum_{n\leq x}\frac{O_n(g)}{2^n} = \log(x) + O(1)$.

7.3 Mertens' Theorem in Zero Characteristic

Our purpose is to extend this analogue of Mertens' theorem to S-integer dynamical systems. However, we know the Artin-Mazur zeta function is typically irrational for these systems from Section 5.1 unlike the Axiom A flows and toral automorphisms. So, again, I look for other methods to find upper and lower asymptotics.

So again we want to look at what happens to Mertens' Theorem when a sequence like $2^n - 1$ is perturbed slightly. We look at the 3-adic example from Section 4.2. The theorem depends a lot on how 'well-behaved' the number of orbits are. From previous experience we are already aware of how badly behaved the sequence $(2^n - 1)|2^n - 1|_3$ is and as a consequence the orbits behave in a similarly erratic way.

Theorem 7.2. *Let f be the endomorphism dual to $x \to 2x$ on $\mathbb{Z}[\frac{1}{3}]$ and let g be the endomorphism dual to $x \to 2x$ on $\mathbb{Z}$. Let $O_n(g) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})(2^d - 1)$ and $O_n(f) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})(2^d - 1)|2^d - 1|_3$. Then*

$$\frac{1}{2}\log(x) + O(1) \leq \sum_{n \leq x} \frac{O_n(f)}{2^n} \leq \log(x) + O(1)$$

Proof. From [26] we know that $\sum_{n\leq x} \frac{O_n(g)}{2^n} = \log(x) + c$, where c is a constant. We can write this as $\sum_{n\leq x} \frac{O_n(g)}{2^n} = \log(x) + O(1)$. Since we know from Theorem 5.2 in Section 5.3 that $O_n(f) \leq O_n(g)$ for all $n \geq 1$, we can say that

$$\sum_{n\leq x} \frac{O_n(f)}{2^n} \leq \sum_{n\leq x} \frac{O_n(g)}{2^n} = \log(x) + O(1).$$

To get a lower bound, note that

$$\sum_{n\leq x} \frac{O_n(f)}{2^n} = \sum_{2\nmid n\leq x} \frac{O_n(f)}{2^n} + \sum_{j=0}^{\infty} \sum_{2.3^j \| n\leq x} \frac{O_n(f)}{2^n} \geq \sum_{2\nmid n\leq x} \frac{O_n(g)}{2^n} = A(x).$$

Now, $A(x) + \sum_{2|n\leq x} \frac{O_n(g)}{2^n} = \sum_{n\leq x} \frac{O_n(g)}{2^n} = \log(x) + O(1)$.

Consider $\sum_{2|n\leq x}\frac{O_n(g)}{2^n}=\sum_{m\leq x/2}\frac{O_{2m}(g)}{2^{2m}}$, then by Lemma 4.2

$$\begin{aligned}
2\sum_{2|n\leq x}\frac{O_n(g)}{2^n} &= 2\sum_{m\leq x/2}\frac{O_{2m}(g)}{2^{2m}}\\
&= \sum_{2\nmid m\leq x/2}\frac{O_n(g^2)-O_n(g)}{2^{2m}}+\sum_{2|m\leq x/2}\frac{O_m(g^2)}{2^{2m}}\\
&= \sum_{m\leq x/2}\frac{O_m(g^2)}{2^{2m}}-\sum_{2\nmid m\leq x/2}\frac{O_m(g)}{2^{2m}}\\
&\geq \log\frac{x}{2}+O(1)=\log x+O(1)
\end{aligned}$$

since

$$\sum_{2\nmid m\leq x/2}\frac{O_m(g)}{2^{2m}}\leq\sum_{m\leq x/2}\frac{O_m(g)}{2^{2m}}<\infty$$

because

$$\sum_{m\leq x/2}\frac{O_m(g)}{2^m}=\log x+O(1),$$

so

$$\sum_{m=1}^{\infty}\frac{1}{2^m}\cdot\frac{O_m(g)}{2^m}\text{ converges.}$$

□

7.4 Mertens' Theorem: Zero Characteristic, infinitely many primes

Again, in a similar way to the Prime Orbit Theorem we want to look at maps at the other extreme of the section above, if S contains all but one prime.

So consider the map from Section 5.4, i.e. $\phi : x \to 2x$ on the ring

$$\mathbb{Z}\left[\frac{1}{2},\frac{1}{5},\frac{1}{7},\frac{1}{11},\ldots\right]=\mathbb{Z}_{(3)}.$$

Write $X = \widehat{\mathbb{Z}[\frac{1}{2}, \frac{1}{5}, \frac{1}{7}, \frac{1}{11}, \ldots]}$ for the dual (character) group, and $f = \widehat{\phi}$ for the dual map. The topological entropy, $h = \log 2$ and the number of points of period n under f is $\frac{1}{|2^n-1|_3}$.

Theorem 7.3. *Let* $O_n(f) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})(2^d - 1)\prod_{p\neq 3} |2^d - 1|_p$. *Then*

$$\prod_{n\leq x}\left(1 - \frac{1}{e^{hn}}\right)^{O_n(f)} \leq \frac{1}{2} \textit{ for all } x.$$

Proof. Let $O_n(f) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})(2^d - 1)\prod_{p\neq 3} |2^d - 1|_p$
then from Section 5.4, $O_n(f) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})\frac{1}{|2^d-1|_3}$ and,

$$O_n(f) = \begin{cases} 1 & \text{if } n = 1\ ; \\ 0 & \text{if } n \neq 2\cdot 3^k; \\ 1 & \text{if } n = 2\cdot 3^k. \end{cases}$$

The prime orbit equivalent to Mertens' Theorem is

$$\prod_{\lambda(\tau)\leq x}\left(1 - \frac{1}{e^{h\lambda(\tau)}}\right) = \prod_{n\leq x}\left(1 - \frac{1}{2^n}\right)^{O_n(f)}.$$

Now

$$\left(1 - \frac{1}{2^n}\right)^{O_n(f)} = \begin{cases} \frac{1}{2} & \text{if } n = 1\ ; \\ 1 & \text{if } n \neq 2\cdot 3^k; \\ (1 - \frac{1}{2^n}) & \text{if } n = 2\cdot 3^k \end{cases}$$

So,

$$\begin{aligned} \prod_{n\leq x}\left(1 - \frac{1}{2^n}\right)^{O_n(f)} &= \prod_{2\cdot 3^k\leq x}\left(1 - \frac{1}{2^{2\cdot 3^k}}\right)^{O_{2\cdot 3^k}(f)}\cdot\frac{1}{2} \\ &= \prod_{2\cdot 3^k\leq x}\left(1 - \frac{1}{4^{3^k}}\right)\cdot\frac{1}{2} \\ &= \prod_{k\leq\frac{\log(x/2)}{\log(3)}}\left(1 - \frac{1}{4^{3^k}}\right)\cdot\frac{1}{2} \\ &< \frac{1}{2}. \end{aligned}$$

□

7.5 Mertens' Theorem: Positive Characteristic - one isometric direction

In a similar way to the Prime orbit theorem, we now want to look at S-integer systems for positive characteristic to see what form Mertens' theorem for orbits takes in this setting.

Example 7.4. We first look at a case that will match the setting of Sharp [26]. Consider Example 6.1 from Section 6.1 where the number of periodic points is given by

$$|\mathcal{F}_n(\alpha)| = |t^n - 1|_\infty |t^n - 1|_t = p^n.$$

and the dynamical zeta function is rational: $\zeta_\alpha(z) = \frac{1}{1-pz}$.
Let $O_n(g) = \frac{1}{n}\sum_{n \le x} \mu(\frac{n}{d})p^d$. From previous experience we know that in this particular case $O_n(g)$ is a smooth growing function and lends itself well to Noorani's theorem. Let $p = 2$ and $O_n(g) = \frac{1}{n}\sum_{n \le x} \mu(\frac{n}{d})2^d$ then the logarithmic equivalent of Mertens' theorem says that $\sum_{n \le x} \frac{O_n(g)}{2^n} = \log(x) + O(1)$.

We want to see what happens for Example 6.2 in Section 6.1.
Let $|\mathcal{F}_n(\theta)| = |t^n - 1|_\infty |t^n - 1|_{t-1} = p^{n - p^{\mathrm{ord}_p(n)}}$ as in Section 6.1, and consider the case where $p = 2$, so $|\mathcal{F}_n(\theta)| = 2^{n - 2^{\mathrm{ord}_2(n)}}$.
Then we know from Section 6.1 the growth of the periodic points is very erratic and hence so is the growth of the orbits. This has a big effect on the analogue of Mertens' theorem and again, we are unable to find an asymptotic growth rate.

Theorem 7.5. *Let f be the endomorphism of $\hat{R}_S = \widehat{\mathbb{F}_p[t][\frac{1}{t-1}]}$ dual to multiplication by t on $\mathbb{F}_p[t][\frac{1}{t-1}]$, and let g be the endomorphism of $\hat{R}_S = \mathbb{F}_p^{\mathbb{Z}}$ dual to multiplication by t on $\mathbb{F}_p[t^{\pm 1}]$. Then*

$$\frac{1}{4}\log(x) + O(1) \leq \sum_{n \leq x} \frac{O_n(f)}{2^n} \leq \log(x) + O(1).$$

Proof. Let $O_n(g) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})(2^d)$ and $O_n(f) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})(2^{d-2^{\mathrm{ord}_2(d)}})$. We know that $\sum_{n\leq x} \frac{O_n(g)}{2^n} = \log(x) + O(1)$, and since $\sum_{n\leq x} \frac{O_n(f)}{2^n} \leq \sum_{n\leq x} \frac{O_n(g)}{2^n}$ we can say that $\sum_{n\leq x} \frac{O_n(f)}{2^n} \leq \log(x) + O(1)$.

Now for the lower bound.

When n is odd

$$O_n(g) = 2O_n(f).$$

When $2^k \parallel n$,

$$O_n(g) \sim 2^{2^k} O_n(f).$$

So

$$\sum_{n\leq x} \frac{O_n(f)}{2^n} = \sum_{2\nmid n\leq x} \frac{O_n(f)}{2^n} + \sum_{k=1}^{\infty} \sum_{2^k \parallel n \leq x} \frac{O_n(f)}{2^n} \sim \frac{1}{2}\sum_{2\nmid n\leq x} \frac{O_n(g)}{2^n} + \frac{1}{2^{2^k}} \sum_{2^k\parallel n\leq x} \frac{O_n(g)}{2^n}.$$

So

$$\sum_{n\leq x} \frac{O_n(f)}{2^n} \geq \frac{1}{2}\sum_{2\nmid n\leq x} \frac{O_n(g)}{2^n}.$$

Now

$$\sum_{2\nmid n\leq x} \frac{O_n(g)}{2^n} + \sum_{2|n\leq x} \frac{O_n(g)}{2^n} = \sum_{n\leq x} \frac{O_n(g)}{2^n} \sim \log(x) + O(1).$$

What is $\sum_{2|n\leq x} \frac{O_n(g)}{2^n}$? First,

$$\sum_{2|n\leq x} \frac{O_n(g)}{2^n} = \sum_{n\leq x/2} \frac{O_{2n}(g)}{2^{2n}}.$$

Again using Lemma 4.2 from Section 4.3,

$$O_n(g^2) = \begin{cases} 2O_{2n}(g) + O_n(g) & \text{if } n \text{ is odd ;} \\ 2O_{2n}(g) & \text{if } n \text{ is even.} \end{cases}$$

In a similar way to the zero characteristic case,

$$\sum_{2|n\leq x} \frac{O_n(g)}{2^n} = \frac{1}{2}\sum_{n\leq x/2} \frac{O_n(g^2)}{2^{2n}} + O(1) = \frac{1}{2}\log(x/2) + O(1) = \frac{1}{2}\log(x) + O(1).$$

So

$$\sum_{2\nmid n\leq x} \frac{O_n(g)}{2^n} = \frac{1}{2}\log(x) + O(1)$$

and so

$$\frac{1}{2}\sum_{2\nmid n\leq x} \frac{O_n(g)}{2^n} = \frac{1}{4}\log(x) + O(1).$$

Hence,

$$\sum_{n\leq x} \frac{O_n(f)}{2^n} \geq \frac{1}{4}\log(x) + O(1).$$

□

7.6 Mertens' Theorem: Positive Characteristic and infinitely many isometric directions

So we now look at the other extreme where

$$S = \{\text{all irreducible polynomials except } (t-1)\}.$$

We use the same case as in Section 6.2. So we have that the number of periodic points is given by

$$F_n(\alpha) = |\mathcal{F}_n(\alpha)| = |t^n - 1|_\infty \prod_{q\neq t-1} |t^n - 1|_q = p^{p^{\mathrm{ord}_p(n)}}.$$

Let $p = 2$ then $F_n(\alpha) = 2^{2^{\mathrm{ord}_2(n)}}$, and

$$O_n(\alpha) = \begin{cases} 2 & \text{if } n = 1 \ ; \\ 0 & \text{if } n \neq 2^k; \\ \frac{1}{n}(2^n - 2^{(\frac{n}{2})}) & \text{if } n = 2^k. \end{cases}$$

Theorem 7.6. *Let* α *to be the endomorphism of* $\hat{R}_S = \mathbb{F}_2[t][\widehat{\frac{1}{t^2+t+1} \ldots}]$ *dual to multiplication by* t *on* $\mathbb{F}_2[t][\frac{1}{t^2+t+1} \ldots]$, *then*

$$\prod_{n \leq x} \left(1 - \frac{1}{2^n}\right)^{O_n(\alpha)} \leq \frac{1}{4}.$$

Proof. Let $O_n(\alpha) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) 2^{2^{\mathrm{ord}_2(d)}}$

$$\left(1 - \frac{1}{2^n}\right)^{O_n(\alpha)} = \begin{cases} \frac{1}{4} & \text{if } n = 1 \ ; \\ 1 & \text{if } n \neq 2^k; \\ \frac{1}{n}(2^n - 2^{(\frac{n}{2})}) & \text{if } n = 2^k \end{cases}$$

So,

$$\begin{aligned} \prod_{n \leq x} (1 - \frac{1}{2^n})^{O_n(\alpha)} &= \prod_{1 < 2^k \leq x} (1 - \frac{1}{2^{2^k}})^{O_{2^k}(\alpha)} \cdot \frac{1}{4} \\ &= \prod_{1 < 2^k \leq x} (1 - \frac{1}{4^k})^{O_{2^k}(\alpha)} \cdot \frac{1}{4} \\ &\leq \frac{1}{4}. \end{aligned}$$

□

Chapter 8

Infinite-dimensional Groups

All our work relates to endomorphisms of finite dimensional groups. What would happen for (say), automorphisms of $\mathbb{T}^\infty$. By [11] these are never expansive, so it is not reasonable to expect good asymptotics. In addition, there is a subtle problem with them: Lind [17] has shown that there exists an ergodic automorphism of an infinite torus with finite entropy if and only if there exists for every $\epsilon > 0$ an automorphism of a finite dimensional torus with entropy $< \epsilon$. Thus the expected answer to Lehmer's (open) problem suggests all ergodic automorphisms of $\mathbb{T}^\infty$ have infinite entropy (see [35]). The next example shows that it is impossible to seek general results on orbit-counting for automorphisms of infinite-dimensional groups.

Theorem 8.1. *Given any sequence $a_1, a_2, \dots$ in $\mathbb{N}$, there exists an automorphism T of an (infinite-dimensional) compact connected group with*

$$a_n \leq F_n(T) < \infty \textit{ for all } n \geq 1.$$

Proof. We need to construct an automorphism T such that

$$a_n < F_n(T) < \infty, \text{ for all } n > 1.$$

We first construct maps V_k that can be used as building blocks for T.

First we fix k and find a map V_k such that

$$\begin{aligned} F_1(V_k) &= 1 \\ F_2(V_k) &= 1 \\ &\vdots \\ F_{k-1}(V_k) &= 1 \\ \infty > F_k(V_k) &> 1 \end{aligned}$$

so that

$$T = \underbrace{(V_1 \times V_1 \times \cdots V_1)}_{\text{enough terms to make } \infty > F_1(T) > a_1} \times \underbrace{(V_2 \times V_2 \times \cdots V_2)}_{\text{enough terms to make } \infty > F_2(T) > a_2} \times \ldots.$$

For the case $k = 1$, let V_1 be the map $\times 3$ on $\widehat{\mathbb{Z}}$, then $F_1(V_1) = 2 > 1$, and we are done.

For $k = 2$, let V_2 be the map $\times 2$ on $\widehat{\mathbb{Z}}$, then $F_1(V_2) = 1,\ F_2(V_2) = 3 > 1$.

For $k = 3$, let V_3 be the map $\times 3$ on $\widehat{\mathbb{Z}[\frac{1}{2}]}$, then

$F_1(V_3) = 1,\ F_2(V_3) = 1,\ F_3(V_3) = (27-1) \cdot \mid 27 - 1 \mid_2 = 26 \cdot \frac{1}{2} = 13 > 1.$

By the classical Zsigmondy Theorem we can say that

$$\{p \mid (p \mid 3^n - 1) \text{ for some } n \leq k\} \subsetneq \{p \mid (p \mid 3^n - 1) \text{ for some } n \leq k+1\} \text{ unless } k = 1.$$

So let V_4 be $\times 3$ on $\widehat{\mathbb{Z}[\frac{1}{2}, \frac{1}{13}]}$, i.e.inverting the set of all earlier primes.

Similarly, V_k will be $\times 3$ on $\widehat{\mathbb{Z}[\frac{1}{s_1}, \ldots, \frac{1}{s_t}]}$, where

$$\{s_1, \ldots, s_t\} = \{\text{all primes already used}\}.$$

So

$$F_{1,2,3,\ldots,k-1}(V_k) = 1 \text{ and } F_k(V_k) > 1,$$

because it will be divisible by a new prime.

So all but finitely many terms in this product are 1, showing that $F_n(T)$ is always finite but exceeds a_n. $\square$

The construction above is quite profligate, and with a little more effort a more precise kind of statement can be made – at the expense of passing to compact groups that are not connected.

The following result appears in [35].

Theorem 8.2. *For any $C \in [0, \infty]$, there is a compact group automorphism T with $|\mathcal{F}_n(T)| < \infty$ for all n and with*

$$\frac{1}{n} \log |\mathcal{F}_n(T)| \longrightarrow C.$$

What kind of constructions are possible for automorphisms of the infinite torus is less clear.

Bibliography

[1] R. L. Adler, A. G. Konheim, and M. H. McAndrew. Topological entropy. *Trans. Amer. Math. Soc.*, 114:309–319, 1965.

[2] M. Boyle and D. A. Lind. Expansive subdynamics. *Trans. Amer. Math. Soc.*, 349(1):55–102, 1997.

[3] P. J. Cameron. *Permutation groups*, volume 45 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999.

[4] V. Chothi, G. Everest, and T. B. Ward. S-integer dynamical systems: periodic points. *J. Reine Angew. Math.*, 489:99–132, 1997.

[5] J. Conze. Points périodiques et entropie topologique. *C. R. Acad. Sci. Paris Sér. A-B*, 267:A149–A152, 1968.

[6] M. Einsiedler and D. A. Lind. Algebraic $\mathbb{Z}^d$ actions of entropy rank one. *Trans. Amer. Math. Soc.*, to appear.

[7] M. Eisenberg. Expansive automorphisms of finite-dimensional vector spaces. *Fund. Math.*, 59:307–312, 1966.

[8] G. Everest, A. van der Poorten, I. Shparlinski, and T. B. Ward. *Recurrence sequences*, volume 104 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2003.

[9] F. Q. Gouvêa. *p-adic numbers*. Universitext. Springer-Verlag, Berlin, second edition, 1997. An introduction.

[10] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford, at the Clarendon Press, 1954. 3rd ed.

[11] H. M. Hastings. On expansive homeomorphisms of the infinite torus. In *The structure of attractors in dynamical systems (Proc. Conf., North Dakota State Univ., Fargo, N.D., 1977)*, volume 668 of *Lecture Notes in Math.*, pages 142–149. Springer, Berlin, 1978.

[12] G. J. O. Jameson. *The prime number theorem*, volume 53 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2003.

[13] B. P. Kitchens. Expansive dynamics on zero-dimensional groups. *Ergodic Theory Dynam. Systems*, 7(2):249–261, 1987.

[14] B. P. Kitchens and K. Schmidt. Automorphisms of compact groups. *Ergodic Theory Dynam. Systems*, 9(4):691–735, 1989.

[15] N. Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1984.

[16] W. Lawton. The structure of compact connected groups which admit an expansive automorphism. In *Recent advances in topological dynamics (Proc. Conf.,*

Yale Univ., New Haven, Conn., 1972; in honor of Gustav Arnold Hedlund), pages 182–196. Lecture Notes in Math., Vol. 318. Springer, Berlin, 1973.

[17] D. A. Lind. Ergodic automorphisms of the infinite torus are Bernoulli. *Israel J. Math.*, 17:162–168, 1974.

[18] D. A. Lind. Ergodic group automorphisms and specification. In *Ergodic theory (Proc. Conf., Math. Forschungsinst., Oberwolfach, 1978)*, volume 729 of *Lecture Notes in Math.*, pages 93–104. Springer, Berlin, 1979.

[19] D. A. Lind and B. Marcus. *An introduction to symbolic dynamics and coding.* Cambridge University Press, Cambridge, 1995.

[20] D. A. Lind and T. B. Ward. Automorphisms of solenoids and p-adic entropy. *Ergodic Theory Dynam. Systems*, 8(3):411–419, 1988.

[21] G. Myerson and A. J. van der Poorten. Some problems concerning recurrence sequences. *Amer. Math. Monthly*, 102(8):698–705, 1995.

[22] M. S. Md. Noorani. Mertens theorem and closed orbits of ergodic toral automorphisms. *Bull. Malaysian Math. Soc. (2)*, 22(2):127–133, 1999.

[23] W. Parry and M. Pollicott. An analogue of the prime number theorem for closed orbits of Axiom A flows. *Ann. of Math. (2)*, 118(3):573–591, 1983.

[24] H. E. Rose. *A course in number theory.* Oxford Science Publications. The Clarendon Press Oxford University Press, New York, second edition, 1994.

[25] R. Rumely. Notes on van der Poorten's proof of the Hadamard quotient theorem. I, II. In *Séminaire de Théorie des Nombres, Paris 1986–87*, volume 75 of *Progr. Math.*, pages 349–382, 383–409. Birkhäuser Boston, Boston, MA, 1988.

[26] R. Sharp. An analogue of Mertens' theorem for closed orbits of Axiom A flows. *Bol. Soc. Brasil. Mat. (N.S.)*, 21(2):205–229, 1991.

[27] A. J. van der Poorten. Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles. *C. R. Acad. Sci. Paris Sér. I Math.*, 306(3):97–102, 1988.

[28] A. J. van der Poorten. Some facts that should be better known, especially about rational functions. In *Number theory and applications (Banff, AB, 1988)*, volume 265 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 497–528. Kluwer Acad. Publ., Dordrecht, 1989.

[29] S. Waddington. The prime orbit theorem for quasihyperbolic toral automorphisms. *Monatsh. Math.*, 112(3):235–248, 1991.

[30] P. Walters. Topological conjugacy of affine transformations of tori. *Trans. Amer. Math. Soc.*, 131:40–50, 1968.

[31] P. Walters. *An introduction to ergodic theory*, volume 79 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.

[32] T. B. Ward. An uncountable family of group automorphisms, and a typical member. *Bull. London Math. Soc.*, 29(5):577–584, 1997.

[33] T. B. Ward. Almost all S-integer dynamical systems have many periodic points. *Ergodic Theory Dynam. Systems*, 18(2):471–486, 1998.

[34] T. B. Ward. Dynamical zeta functions for typical extensions of full shifts. *Finite Fields Appl.*, 5(3):232–239, 1999.

[35] T. B Ward. Group automorphisms with few and with many periodic points. *Proc. Amer. Math. Soc.*, to appear.

[36] A. Weil. *Basic number theory.* Springer-Verlag, New York, third edition, 1974. Die Grundlehren der Mathematischen Wissenschaften, Band 144.