CHAOTIC DYNAMICAL SYSTEMS ON SYMBOLIC SPACES

Thesis

Submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

By

CHETANA U V

DEPARTMENT OF MATHEMATICAL AND
COMPUTATIONAL SCIENCES
NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA
SURATHKAL, MANGALORE - 575 025

May 2016

Dedicated to Prof. Juliet Britto

DECLARATION

By the Ph.D. Research Scholar

I hereby declare that the Research Thesis entitled **CHAOTIC DYNAMICAL SYSTEMS ON SYMBOLIC SPACES**, which is being submitted to the National Institute of Technology Karnataka, Surathkal in partial fulfillment of the requirements for the award of the Degree of **Doctor of Philosophy** in **Mathematics** is a *bonafide report of the research work carried out by me*. The material contained in this Research Synopsis has not been submitted to any University or Institution for the award of any degree.

Chetana U V

(Register No.: 123039MA12F05)

Department of Mathematical and Computational Sciences

Place: NITK, Surathkal.

Date: 30 /05/2016

CERTIFICATE

This is to *certify* that the Research Thesis entitled **CHAOTIC DYNAMICAL SYSTEMS ON SYMBOLIC SPACES** submitted by **CHETANA U V**, (Register Number: 123039MA12F05) as the record of the research work carried out by her, is *accepted as the Research Thesis submission* in partial fulfillment of the requirements for the award of degree of **Doctor of Philosophy**.

Dr. B R Shankar

Research Guide

Chairman - DRPC

(Signature with Date and Seal)

ACKNOWLEDGEMENT

I would like to take this opportunity to thank the people who supported me in one way or the other to pursue my Ph. D.

I am very grateful to the University Grants Commision, Mangalore University and University College, Mangalore, for giving me the opportunity to pursue full-time Ph. D. under the Faculty Development Program, and to NITK for accepting me as a full-time research scholar.

Dr. B. R. Shankar was not only my research guide, but was a well wisher, and helped me and guided me throughout my work. I am grateful to him for all his support.

I extend my thanks to my RPAC members, Prof. Santhosh George, Department of Mathematics And Computational Sciences, and Prof. M. B. Saidutta, Department of Chemical Engg., for their valuable suggestions, which helped me to improve my presentations and my work.

I am thankful to Prof. Murulidhar N. N., the former Head of the Department of MACS, and Prof. Santhosh George, the present Head of Department of MACS, for all the help. I extend my thanks to all the members of the teaching and non-teaching staff of the Department of MACS for their cooperation.

I am very grateful to Prof. Hisao Kato of University of Tsukuba, Ibaraki, Japan for sending the paper "Fractal metrics of ruelle expanding maps and expanding ratios".

I thank all the research scholars of the Department of MACS for making my stay in NITK pleasant and memorable.

Place: NITK, Surathkal Chetana U V

Date: 30/05/2016

Abstract

Chaotic dynamical systems, preferably on a Cantor-like space with some arithmetic operations are considered as good pseudo-random number generators. There are many definitions of chaos, of which Devaney-chaos and positive topological entropy seem to be the strongest. These two together imply several other kinds of chaos. For data hiding schemes, systems with more types of chaotic features are considered to be better. Let $A = \{0, 1, \cdots, p-1\}$. We define some continuous maps on $A^{\mathbb{Z}}$ using addition with a carry, in combination with the shift map. We get some dynamical systems that are conjugate to a power of the shift map, or have positive entropy. In one case we can give bounds for the topological entropy. We also obtain one system with positive entropy, which is also Devaney-chaotic: i.e., it is transitive, sensitive and has a dense set of periodic points.

Keywords : discrete ; chaotic ; transitive ; entropy.

Contents

Chapter 1

INTRODUCTION

A topological dynamical system is a pair (X, f) where f is a continuous self map of a topological space X. Topological Dynamics is the study of iterations $f^n : X \to X$. The **trajectories**, that is the sequences $\{f^n(x)\}_{n\geq 0}$ and **orbits**, that is the sets $\{f^n(x)|n > 0\}$ of elements x of X are of particular interest. Generally X is assumed to be a compact metric space with metric d. Many important theorems of Topological Dynamics hold only for compact spaces. Topological entropy is actually defined for compact spaces, but can be generalized to noncompact spaces. Some common questions are :

(i) Is the orbit of x finite (in which case x is an eventually periodic point for f)?

(ii) Is it dense ?

(iii) Does it have limit points? If so what are the limit points?

More generally we ask whether a point $y \in X$ can be "reached" from a point $x \in X$. Depending on the exact meaning of "reached" we get several relations $R \subseteq X \times X$. They are the **orbit relation, recurrence relation, non-wandering relation** and the **chain relation** (Kůrka, 2003), to be defined precisely later in Chapter 2. The **diagonal** of a relation $R \subseteq X \times X$ is $|R| = \{x \in X|(x,x) \in R\}$. The points of the diagonals of the above four relations are called **periodic, recurrent, non-wandering** and **chain-recurring** respectively. A point is non-wandering if it returns to each of its neighbourhoods at least once, recurring if it returns to all of its neighbourhoods infinitely many times, but not necessarily periodically. If the times between successive returns forms a bounded sequence, we say that x

is **almost periodic**. If x returns to all of its neighbourhoods periodically (the period may depend on the neighbourhood), then it is called **quasi-periodic** or **regularly recurrent**. We have

periodic $\implies$ quasi-periodic $\implies$ almost periodic $\implies$ recurrent $\implies$ non-wandering $\implies$ chain-recurrent.

The chain relation is defined in terms of pseudotrajectories or δ-chains. A (finite or infinite) sequence $\{x_n\}_{n\geq 0}$ is a δ-chain if $d(f(x_n), x_{n+1}) < \delta$ for all n. If a trajectory is computed numerically with round-off errors less than δ, we obtain a δ-chain rather than a trajectory. So a δ-chain is an approximation to a trajectory. In general such an approximation works only for a short term. Sometimes the approximation may work in the long run. A δ-chain may approximate the trajectory of its initial point, or of some other point. Then we say that the point shadows the δ-chain in question (Kůrka, 2003). It is desirable to have every δ- chain shadowed by some point. Then every δ chain is an approximation of some orbit.

Equicontinuity and sensitivity (to initial conditions) are two mutually opposite concepts. In a sensitive system there is a positive ε such that in any neighbourhood of a point there is another point such that the trajectories of the two points are eventually at least ε apart.

We may also study dynamical systems from the point of view of information sources. The amount of information which the dynamical system generates per step is called its topological entropy.

We are particularly interested in chaotic dynamical systems which are a source of randomness. Actually, the behaviour of a trajectory in a chaotic system is not really "random", but is "unpredictable" if we do not have enough information about the system.

Most studies in security aspects of data hiding schemes usually have used the theory of probability to measure unpredictability. Unpredictability related to some topological or ergodic aspects of a function f, taken from the mathematical theory of chaos offers an additional contribution to the variety of security evaluations. But, answer to the question " What chaotic properties are needed to achieve goals like robustness, security or authentication? " is not very clear. Generally sensitivity to initial conditions is referred to as chaos, or a simple use of the logistic map is done (Bahi and Guyeux, 2013) .

Chaos is defined in various ways. In common usage “chaos” means “a state of disorder”, but in the mathematical theory of chaos the term is defined precisely, in many ways (Li and Ye, 2015). Each notion of chaos offers a new light on the security of a data hiding scheme. A data hiding scheme may be considered to be more secure than another, if it presents a larger number of chaotic qualities and if its quantitative values are better.
Most defintions of chaos are based on one or more of the following aspects :

- Complex behaviour of trajectories of points, such as Li-Yorke chaos and distributional chaos.
- Sensitive dependence on initial conditions, such as Devaney chaos and Auslander-Yorke chaos.
- Fast growth of different orbits of length n, such as having positive topological entropy.
- Strong recurrence property, weakly mixing property.

The notion of topological entropy was introduced by Adler et al. in 1965 (Adler et al., 1965), and systems with positive entropy are considered as chaotic. Weak mixing was introduced by Furstenberg in 1967 (Furstenberg, 1967). The term “chaos” was first used by Li and Yorke in 1975 (Li and Yorke, 1975), in the paper titled “Period three implies chaos”. They proved that for a conituous self-map on [0,1], existence of point of period three implies existence of all periods greater than three, and also that there is an uncountable subset of points which are not even asymptotically periodic (see section 2.3). Later in 1989 Devaney defined a new kind of chaos (Devaney et al., 1989). It was based on the notion of sensitivity introduced by Guckenheimer (Guckenheimer, 1979). A system is Devaney chaotic if it is transitive (equivalent to having a dense orbit), has a dense set of periodic points and is sensitive. The transitive points contribute to “irregularity”, and the periodic points contribute to “regularity”. A combination of the two is considered as chaos. Distributional chaos was introduced by Schweizer and Smítal in 1994, of which there are three versions, DC1, DC2 and DC3. Uniform chaos was defined by Akin et al. (Akin et al., 1996).

All these definitions do not give the same type of chaos. It is known that each of weak mixing, Devaney chaos and positive topological entropy implies Li-Yorke chaos (Li and Ye, 2015). A dynamical system with positive entropy may not contain a weakly mixing subsystem. There are maps with zero entropy that are Devaney chaotic, and there are maps with positive entropy that are not Devaney chaotic (Balibrea et al., 2003). Positive entropy does not imply DC1 chaos, but it implies DC2 chaos. Devaney chaos implies uniform chaos.

Though classical chaotic maps defined on manifolds are plenty, they are not particularly suited for machine computation. Discrete functions are more suitable for computers. For ease of implementation, analysis etc., it would be helpful if X is a cantor-like set, preferably with some arithmetic structure, and f is given by a simple formula (Woodcock and Smart, 1998).

Let A be a finite set with at least two elements, in the discrete topology. Let $A^{\mathbb{Z}}$ have product topology. The shift map σ which shifts each coordinate of a point to the "left" by one position is a continuous map. The two-sided full shift, $(A^{\mathbb{Z}}, \sigma)$ is a very important dynamical system. A closed subspace of $A^{\mathbb{Z}}$, along with a continuous self map is a symbolic space. Symbolic dynamics originated as a tool for analyzing dynamical systems and flows by discretizing space as well as time. But, with the development of information theory, now symbolic sequences are being studied as objects in their own right. In spite of the simplicity of their spaces, symbolic dynamical sytems are in some sense universal compact dynamical systems. Every compact dynamical system is a factor of a symbolic dynamical system. Any trajectory of the original system comes from one or more trajectories of the symbolic system. In (Hedlund, 1969), Cellular Automata (CA), which form a special class of symbolic dynamical systems, are discussed. Some special cases of non-uniform CA are studied in (Dennunzio et al., 2012).

The field $\mathbb{Q}_p$ of p-adic numbers is the completion of the field $\mathbb{Q}$ of rational numbers in the p-adic norm, for a prime number p. Woodcock and Smart discuss some discrete dynamical systems based on p-adic numbers in (Woodcock and Smart, 1998). They discuss the properties of p-adic analogues of the logistic and Smale horseshoe maps, and adapt them to form possible practical pseudo-random number generators. The p-adic logistic map is

proved to be conjugate to the one sided full shift, and the p-adic horseshoe map conjugate to the twosided full shift. Hence both are Devaney- chaotic.
In (Bryk and Silva, 2005), measurable dynamics of some p-adic functions including translation and multiplication in the field $\mathbb{Q}_p$ of p-adic numbers are studied.

As a set, $\mathbb{Q}_p$ is contained in $A^{\mathbb{Z}}$, where $A = \{0,1,2\cdots, p-1\}$. The ring $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$, and as a set $A^{\mathbb{Z}} = \mathbb{Z}_p \times \mathbb{Z}_p$. Our aim is to extend the addition operation in $\mathbb{Q}_p$ and $\mathbb{Z}_p$ to $A^{\mathbb{Z}}$, and combine it with the shift map to get other dynamical systems.
In Chapter 2 some basic definitions and background matter regarding p-adic numbers, topological dynamics and symbolic dynamics along with some examples are given.
In Chapter 3, extending addition of a constant in $\mathbb{Q}_p$ to $A^{\mathbb{Z}}$ is discussed, and a conjugate to the two sided full shift is obtained. By considering the set $A^{\mathbb{Z}} = \mathbb{Z}_p \times \mathbb{Z}_p$, and using the addition in $\mathbb{Z}_p$, an expansive homeomorphism conjugate to a subshift, and two maps which are positively expansive with positive entropy are obtained.
In Chapter 4, a better version of the above maps is obtained. Besides having positive entropy, it is Devaney chaotic.
We observed that there is a slight difference in the definition of positively expansive maps given by different authors in different papers. In Chapter 5, some examples are are given to clarify the notion of positively expansive maps on non-compact spaces.

Chapter 2

BASIC DEFINITIONS AND EXAMPLES

We use the following notations : $\mathbb{N}$- set of non-negative integers, $\mathbb{N}^+$ - set of positive integers, $\mathbb{Q}$ - field of rational numbers, $\mathbb{Z}$ - ring of all integers, $\mathbb{C}$- field of complex numbers, $\mathbb{R}$- field of real numbers.

2.1 THE FIELD OF p-ADIC NUMBERS

Consider the field $\mathbb{Q}$ of rational numbers. It is not complete in the Euclidean norm, and its completion is $\mathbb{R}$. Some other norms can be defined on $\mathbb{Q}$ using prime numbers. For any fixed prime p, let p^α be the highest power of p that divides an integer a not equal to zero. Then $\|a\|_p$ is $p^{-\alpha}$. For a rational number $\frac{a}{b}$, $\|\frac{a}{b}\|_p$ is $\frac{\|a\|_p}{\|b\|_p}$ and $\|0\|_p$ is defined to be zero. With respect to this norm, $\mathbb{Q}$ is a normed field, but it is not complete in the metric topology induced by this norm. Its completion is denoted by $\mathbb{Q}_p$ (Katok, 2007). The Euclidean norm is denoted by $\| \ . \ \|_\infty$. In fact, these are the only norms that can be defined on $\mathbb{Q}$, as shown by Ostrowski (Katok, 2007):

Theorem 2.1.1. *(Ostrowski) : Every nontrivial norm $\| \ . \ \|$ on $\mathbb{Q}$ is equivalent to $\| \ . \ \|_p$ for some prime p or to $\| \ . \ \|_\infty$.*

The p-adic metric takes only discrete values, namely integer powers of p, and so all open balls are also closed in $\mathbb{Q}_p$. Surfaces of spheres, which are in general only closed, are also open here. Another important property is that $\|.\|_p$ is non-Archimedean, that is for any x, y in $\mathbb{Q}_p$, $\|x+y\|_p \leq max\{\|x\|_p \ , \ \|y\|_p\}$. The metric induced by this norm is an **ultrametric**. It satisfies the strong triangle inequality, $d(x,\ z) \leq \ max\{d(x,\ y),\ d(y,\ z)\}$, for all y in $\mathbb{Q}_p$. Here two open balls intersect if and only if one is contained in the other. Every point of a ball is its centre.

It can be shown that this field contains some elements like irrational numbers and complex numbers, in addition to many other elements. It is not an ordered field. It is not algebraically closed. For example, $\mathbb{Q}_5$ contains $\sqrt{6}$ and $\sqrt{-1}$, but does not contain a square root of 7. $\mathbb{Q}_3$ does not contain $\sqrt{-1}$. For $p \neq q$, $\mathbb{Q}_p$ and $\mathbb{Q}_q$ are not isomorphic (Katok, 2007).

2.2 REPRESENTATION OF p-ADIC NUMBERS

It can be shown that every p-adic number x can be canonically represented as $\sum_{i=-\infty}^{i=m} d_i p^{-i}$, where m is in $\mathbb{Z}$ and $d_i \ \in \ \{0,\ 1,\ 2,\ 3,\cdots,\ (p-1)\}$, and $d_m \neq 0$. This can be viewed as a *doubly infinite* series in powers of p, where the "digits" d_i are all zero for $i \ > \ m$. The p-adic norm of this number is p^m. It is also written as $x = \cdots d_{-2}\, d_{-1} \overbrace{d_0}^{0^{th}} .\, d_1\, d_2 \ \cdots \underbrace{d_m}_{(\neq 0)} \ 0\, 0 \cdots$

The numbers for which $m \leq \ 0$ are called *p-adic integers*. The set of p-adic integers is denoted by $\mathbb{Z}_p$. It is the set of p-adic numbers with norm less than or equal to one. Note that this contains all the positive integers, each represented by a finite sum, which is the same as the base-p expansion the positive integer. It contains negative integers also, but the sum is infinite. $-\sum_{i=-\infty}^{i=m} d_i p^{-i} \ = \ \sum_{i=-\infty}^{i=m-1}(p-1-d_i)p^{-i} + (p-d_m)p^{-m}$, where d_m is the last nonzero digit. Therefore for any $x \ \in \ \mathbb{Q}_p$, either x or $-x$ must have infinitely many nonzero digits (towards left) in the canonical p-adic expansion.

For example in $\mathbb{Q}_5$, $-(\cdots 234100.32200000\cdots) = \cdots 210344.123000\cdots$.

It is easy to see that a number x in $\mathbb{Q}_p$ is a rational number if and only if its canonical p-adic expansion is eventually periodic (Katok, 2007).

The arithmetical operations in $\mathbb{Q}_p$ are similar to arithmetical operations on natural numbers written in base p. Algorithms of addition and subtraction are pursued from right to left indefinitely, after aligning the "point" after the digit in the zeroth place. Multiplication also proceeds from right to left indefinitely, in the usual way. "Long division" proceeds

from right to left, unlike the usual long division of natural numbers (Katok, 2007).
Here is an example of addition in $\mathbb{Q}_7$.

$$\cdots 462535.354300\cdots$$

$$+\cdots 320656.4100\cdots$$

$$-------------$$

$$\cdots 113525.064300\cdots$$

2.3 DISCRETE DYNAMICAL SYSTEMS AND CHAOS

Let X be a topological space, and $f: X \to X$ be a continuous function. If Y is a closed subspace of X which is invariant under f, i.e., $f(Y) \subseteq Y$, then (Y, f) is a subsystem of (X, f). We use the following standard definitions, examples and results on a compact dynamical system (X, f), mostly from (Kůrka, 2003), (Li and Oprocha, 2013), (Vries, 2014) and (Li and Ye, 2015).

Definition 2.3.1. *(X, f) is called **minimal** if it contains no proper subsystem.*

Example 1. *Let $\mathbb{Z}(n)$ denote the set of integers modulo n, with discrete toplogy. Let f be given by $f(x) = (x+1) \mod n$. Then $(\mathbb{Z}(n), f)$ is a dynamical system with a single orbit, hence is minimal.*

An example of an infinite minimal system is Example 2.
A subset A of X is minimal if (A, f) forms a minimal subsystem. A closed invariant subset A of X is minimal if and only if the orbit of every point of A is dense in A. A point $x \in X$ is called minimal if it belongs to some minimal subset of X.

Definition 2.3.2. *A point $x \in X$ is called **periodic** if there exists an integer $n > 0$ such that $f^n(x) = x$.*

It is **eventually periodic** if $f^n(x)$ is periodic for some $n > 0$.

Definition 2.3.3. *A point $x \in X$ is called **quasi-periodic** or **regularly recurring** if for every neighbhourhood U of x, there is a $j > 0$ such that for any $n \geq 0$, $f^{nj}(x) \in U$.*

Definition 2.3.4. *A point $x \in X$ is called **almost periodic** if for every neighbhourhood U of x, there exists an integer $p > 0$ such that for $\forall n \geq 0$, there exists an integer $k < p$ such that $f^{nk}(x) \in U$.*

Definition 2.3.5. *A point $x \in X$ is called **asymptotically periodic** if $d(f^n(x), f^n(p)) \to 0$ as $n \to \infty$, for some periodic point p.*

Definition 2.3.6. *A point $x \in X$ is called **recurrent** if for every neighbhourhood U of x, there exists an integer $n > 0$ such that $f^n(x) \in U$.*

Definition 2.3.7. *$x \in X$ is a **non-wandering** point if for every open set U containing x, there is an $n > 0$ such that $f^n(U) \bigcap U \neq \varnothing$.*

Definition 2.3.8. *If all points of X are non-wandering, then (X, f) is a **non-wandering** system.*

Definition 2.3.9. *(X, f) is **transitive** if for any nonempty open sets U and V in X, there exists $n > 0$ such that $f^n(U) \bigcap V \neq \varnothing$.*

A point x is **transitive** if its orbit under f is dense. It follows that (X, f) is transitive if and only if it has at least one transitive point.
Clearly, periodic $\Longrightarrow$ quasi-periodic $\Longrightarrow$ almost periodic $\Longrightarrow$ recurrent $\Longrightarrow$ nonwandering. But none of the converse implications is true.

Example 2. *In $(\mathbb{S}, \varphi)$ where $\mathbb{S}$ is the unit circle and φ is rotation by an irrational multiple of 2π, every point has a dense orbit and hence is recurrent, but not periodic.*

On the other hand, a periodic point in an infinite system is an example of a non-transitive recurrent point.

Example 3. *Consider $\tau := \varphi \times Id : \mathbb{S}^2 \times \mathbb{S}^2$, where Id denotes the identity map. Each " horizontal" circle, i.e., the circle got by fixing the "vertical" coordinate, $\mathbb{S}_t := \mathbb{S} \times [t]$, $(0 \leq t < 1)$, is an invarient system conjugate (see Section 2.5) to $(\mathbb{S}, \varphi)$. Consequently no orbit is dense in $\mathbb{S}^2$, but every point is recurrent (and non-wandering) but not transitive and not periodic.*

Example 4. *Consider an infinite compact minimal system. It contains no periodic points. Therefore all its points are almost periodic, but not periodic.*

Example 5. *Let* $A = \{0,1\}$. *Consider* $(A^{\mathbb{N}}, \sigma)$, *where* σ *is the one sided full shift given by* $\sigma(x_1x_2x_3\cdots) = x_2x_3\ \cdots$. *(See Section (2.6)). Here, the Champernowne sequence* $x = 0100011011\cdots$, *which concatenates all finite binary words, is recurrent but not almost periodic (Kůrka, 2003).*

Example 6. *Any point of* $(\mathbb{S}, \varphi)$, *where* φ *is an irrational rotation of the circle, is almost periodic but not quasi-periodic (Kůrka, 2003).*

Definition 2.3.10. (X, f) *is* ***totally transitive*** *if* (X, f^n) *is transitive for all* $n \in \mathbb{N}$.

Definition 2.3.11. (X, f) *is* ***weakly mixing*** *if the product system* $(X \times X, f \times f)$ *is transitive.*

Definition 2.3.12. (X, f) *is* ***strongly mixing*** *if for every two non-empty open sets* U *and* V, *there is* $N > 0$ *such that* $f^n(U) \bigcap V \neq \varnothing$ *for all* $n \geq N$.

When X is a metric space, a few more definitions can be given.

Definition 2.3.13. *A point* x *is said to be* ***equicontinuous***, *if for every* $\varepsilon > 0\ \exists\ \delta > 0$ *such that for any* y, $d(x,y) < \delta \implies d(f^n(x), f^n(y)) < \varepsilon,\ \forall\ n > 0$.

Definition 2.3.14. (X, f) *is* ***equicontinuous*** *if for every* $\varepsilon > 0\ \exists\ \delta > 0$ *such that for any* x *and* y *in* X, $d(x,y) < \delta \implies d(f^n(x), f^n(y)) < \varepsilon,\ \forall\ n > 0$.

If X is compact, it means that every point is an equicontinuous point.

Equicontinuous systems have simple dynamical behaviour. It is well-known that a system (X, f), with f being surjective is equicontinuous if and only if there is a compatible metric ρ on X such that f is an isometry with respect to ρ.

Example 7. *Let* $\mathbb{I} = [0,1]$, *and* $Q_r(x) = rx(1-x)$ *for an* $r \in [0,4]$. *In the system* $(\mathbb{I}, Q_r)$, *if* $r \leq 1$, *all points are equicontinuous. For* $1 < r \leq 3$, *all points in* $(0,1)$ *are equicontinuous, and for* $r = 4$ *there are no equicontinuous points.*

Definition 2.3.15. (X,f) *is **sensitive** (to initial conditions) if there exists* $\varepsilon > 0$ *such that* $\forall x \in X, \forall\, \delta > 0$*, there exists y with* $d(x,y) < \delta$ *and* $n \geq 0$ *such that* $d(f^n(x), f^n(y)) \geq \varepsilon$.

The full shift in Section 2.6 is a sensitive sytem. A sensitive sytem cannot have equicontinuous points. There are systems that are not sensitive and do not have equicontinuous points. But this cannot happen in a transitive system (Akin et al., 1996).

Definition 2.3.16. *A pair* (x,y) *of points in X is called*

(i) ***asymptotic*** *if* $\lim\limits_{n\to\infty} d(f^n(x), f^n(y)) = 0$.

(ii) ***proximal*** *if* $\liminf\limits_{n\to\infty} d(f^n(x), f^n(y)) = 0$.

(iii) ***distal*** *if* $\liminf\limits_{n\to\infty} d(f^n(x), f^n(y)) > 0$.

The sytem (X,f) is is called **proximal** if any two points in X form a proximal pair, and **distal** if any two points form a distal pair.

Definition 2.3.17. *A pair* $(x,y) \in X \times X$ *is called **scrambled** if* $\liminf\limits_{n\to\infty} d(f^n(x), f^n(y)) = 0$ *and* $\limsup\limits_{n\to\infty} d(f^n(x), f^n(y)) > 0$*, that is (x,y) is proximal but not asymptotic. A subset C of X is called scrambled if any two points of X form a scrambled pair, and* (X,f) *is called **Li-Yorke chaotic** if there is an uncountable scrambled subset in X.*

The following is a characterization of a proximal system (Li and Ye, 2015).

Theorem 2.3.1. *A dynamical system* (X,f) *is proximal if and only if it has a fixed point which is the only minimal point of X.*

In 1996, Akin et. al. proposed the concept of uniform chaos (Akin et al., 1996).

Definition 2.3.18. *Let* (X,F) *be a transitive dynamical system. A subset K of X is said to be*

(i) ***uniformly recurrent*** *if for every* $\varepsilon > 0$ *there exists an* $n \in \mathbb{N}$ *with* $d(f^n(x), x) < \varepsilon$ *for all* $x \in K$;

(ii) ***recurrent*** *if every finite subset of K is uniformly recurrent;*

(iii) ***uniformly proximal*** *if for every* $\varepsilon > 0$ *there exists an* $n \in \mathbb{N}$ *with* $diam(f^n(K)) < \varepsilon$;

(iv) ***proximal*** *if every finite subset of* K *is uniformly proximal.*

Definition 2.3.19. *Let* (X, f) *be a transitive dynamical system. A subset* K *of* X *is called* ***uniformly chaotic*** *if there are Cantor sets* $C_1 \subset C_2 \subset \cdots$ *such that*

(i) *for each* $N \in \mathbb{N}$, C_N *is uniformly recurrent;*

(ii) *for each* $N \in \mathbb{N}$, C_N *is uniformly proximal;*

(iii) $K := \bigcup_{i=1}^{\infty} C_i$ *is a recurrent subset of* X *and also a proximal subset of* X.

The system (X, f) *is called (densely)* ***uniformly chaotic*** *if it has a (dense) uniformly chaotic subset of* X.

The following is a corollary of the main result of (Akin et al., 2010). (p.18, Corollary 5.17, (Li and Ye, 2015)).

Corollary 2.3.1. *Let* (X, f) *be a dynamical system without isolated points. Then,*

(i) *If* (X, f) *is transitive and has a fixed point, then it is densely uniformly chaotic.*

(ii) *If* (X, f) *is transitive and has a periodic point (of period* ≥ 2*), then it is uniformly chaotic.*

Definition 2.3.20. *Let* (X, f) *be a dynamical system. For* $\delta > 0$, *a* ***δ-pseudo orbit*** *or a* ***δ-chain*** *is a finite or infinite sequence of points* $(x_n)_{n=0}^{m}$, $m \in \mathbb{N} \bigcup \{\infty\}$, *such that* $d(f(x_n), x_{n+1}) < \delta$ *for* $n < m$.

Example 8. *Here is an example of a* δ*-pseudo orbit which not an orbit, in the system* $(A^{\mathbb{Z}}, \sigma)$ *(see Section 2.6).*
For agiven $\delta > 0$, *choose an integer* m *such that* $2^{-m} < \delta$. *Fix any* x *in* $(A^{\mathbb{Z}}, \sigma)$, *with all non-zero coordinates. Define a sequence* $\{a^{(n)}\}$, *for* $n \geq 0$, *as follows.*

$$a_i^{(n)} = \begin{cases} (\sigma^n(x))_i & \text{for} \quad |i| \leq m+1 \\ 0 & \text{for} \quad |i| > m+1 \end{cases}$$

Then $\{a^{(n)}\}$ is a δ-pseudo orbit, because $d(\sigma(a^{(n)}), a^{(n+1)}) < 2^{-m} < \delta$. It is obviously not an orbit.

Definition 2.3.21. *(X, f) has the **shadowing property** if*
for any $\varepsilon > 0 \; \exists \; \delta > 0, \; \forall \, x_0, \cdots x_n, (\; \forall i, \; d(f(x_i), x_{i+1}) < \delta \implies \exists \, x, \; \forall \, i, d(f^i(x), x_i) < \varepsilon)$.

It means that every finite δ-chain is ε-shadowed by some point.

Definition 2.3.22. *(X, f) has the **pseudo-orbit tracing property** if for each $\varepsilon > 0$ there is a $\delta > 0$ such that every infinite δ-pseudo orbit is ε- shadowed by some point.*

If X is compact, the shadowing property implies the pseudo-orbit tracing property (POTP).

Example 9. *The identity map on the interval $[0,1]$ does not have shadowing property. For any δ, divide the interval into n equal parts of length less than δ. Let $0 = x_0 < x_1 < \cdots x_n = 1$ be the end points of the subintervals. Then $x_0, x_1, \cdots x_n$ is a δ chain, which is not ε shadowed by any $y \in [0,1]$, for any $\varepsilon < \frac{1}{2}$.*

Example 10. *The identity map on $A^{\mathbb{N}}$ (see Section 2.6), for a finite set A has shadowing property. If $\delta = 2^{-n}$, and $(x_i)_{0 \leq i \leq m}$ is a δ-chain in $A^{\mathbb{N}}$, then $d(x_i, x_{i+1}) < 2^{-n}$ and so $(x_0)_{[0,n]} = (x_1)_{[0,n]} = \cdots = (x_n)_{[0,n]}$. Therefore x_0 δ-shadows $(x_i)_{0 \leq i \leq m}$.*

The following is a non-trivial example of shadowing property, from (Kůrka, 2003).

Example 11. *Let $\mathbb{T} = [0,1)$, and let $\mathbb{S}$ be the uinit circle. A point z on $\mathbb{S}$ is of the form $z = e^{2\pi ix}$, $x \in \mathbb{T}$. Every z in $\mathbb{S}$ may be identified with that x in $\mathbb{T}$. Define distance between two points as the length of the shortest arc which joins them.*
$d(x,y) = min\{|x-y|, 1-|x-y|\}$. Define

$$D(x) = \begin{cases} 2x & for \quad x < \frac{1}{2} \\ 2x-1 & for \quad x \geq \frac{1}{2} \end{cases}$$

Then $(\mathbb{S}, D)$ has shadowing property.

Example 12. *The quadratic map $Q(x) = x^2$ on $\mathbb{T}$ does not have shadowing property.*

Definition 2.3.23. *Let x, y be points in X, where (X, f) is a dynamical system.*

*(i) x and y are **chain related** if for every $\delta > 0$, there is a finite δ- chain from x to y, and from y to x.*

*(ii) x is called **chain recurrent** if for every $\delta > 0$, there is a finite δ- chain from x to x.*

*(iii) The map f is **chain recurrent** if every $x \in X$ is chain recurrent.*

*(iv) The map f is **chain transitive** if any two points of X are chain related.*

We denote by $CR(f)$ the set of all chain recurring points of f, and by $\omega(f)$, the set of all non-wandering points of f.

There are two versions of expansiveness associated with dynamical systems.

Definition 2.3.24. *A bijective dynamical system (X, f) is **expansive** if $\exists\, \varepsilon > 0,\ \forall\, x \neq y \in X,\ \exists\, n \in \mathbb{Z},\ d(f^n(x), f^n(y)) \geq \varepsilon$.*

Definition 2.3.25. *(X, f) is said to be **positively expansive** if there exists an $\varepsilon > 0$ such that for all x and y in X with $x \neq y$, there is $n \geq 0$ with $d(f^n(x), f^n(y)) \geq \varepsilon$.*

Every compact metric space that supports a positively expansive homeomorphism is finite (Coven et al., 2006). Positively expansive maps, under certain conditions, have positive topological entropy, which is discussed in the next section.

Definition 2.3.26. *(X, f) is said to be **Auslander_Yorke chaotic** if it is both transitive and sensitive.*

According to the definition of chaos given by R. L. Devaney (Devaney et al., 1989), there is one more condition, that is, existence of a dense set of periodic points.

Definition 2.3.27. *An infinite dynamical system (X, f) is **chaotic** if it is transitive, has a dense set of periodic points and is sensitive to initial conditions.*

Theorem 2.3.2. (Bank's Theorem) *(Kůrka, 2003) : If X is infinite, then (X, f) is transitive and X has a dense set of periodic points together imply that (X, f) is sensitive.*

By Corollary (2.3.1), every Devaney chaotic system is uniformly chaotic.

2.4 TOPOLOGICAL ENTROPY

We define **topological entropy** of a compact dynamical system using open covers as follows (Adler et al., 1965) :
Let $\mathscr{U}$ be an open covering of X. Let $N(\mathscr{U})$ be the minimum number of elements of $\mathscr{U}$ that are needed to cover X. Since X is compact, this number exists. If $\mathscr{U}$ and $\mathscr{V}$ are finite open covers of X, their joint open cover, denoted by $\mathscr{U} \vee \mathscr{V}$ is $\{U \cap V | U \in \mathscr{U}, V \in \mathscr{V}, U \cap V \neq \emptyset\}$. If f is a continuous function from X to itself,
$N_n(\mathscr{U}, f) = N(\mathscr{U} \vee f^{-1}(\mathscr{U}) \vee f^{-2}(\mathscr{U}) \cdots \vee f^{-(n-1)}(\mathscr{U}))$.
The **topological entropy** of the open cover $\mathscr{U}$ of X is

$$h(\mathscr{U}, f) = \lim_{n \to +\infty} \frac{logN_n(\mathscr{U}, f)}{n}$$

The topological entropy of (X, f), denoted by $h(X, f)$ is defined by

$$h(X, f) = \sup\{h(\mathscr{U}, f) | \mathscr{U} \ finite\ open\ cover\ of\ X\}$$

.

If the topological entropy of (X, f) is positive, (X, f) is said to be chaotic.
There is another equivalent definition of topological entropy when X is a compact metric space, due to Bowen (Bowen, 1971). Roughly speaking, we would like to equate “higher entropy” with “more” orbits. But the number of orbits is usually infinite, and so we fix a “resolution”, i.e., a scale below which we are unable to tell points apart. Suppose we are unable to distinguish between points that are $< \varepsilon$ apart. Then $N(n, \varepsilon)$ represents the number of distinguishable orbits of lenght n, and if this number grows like $\sim e^{nh}$, then h is the topological entropy.
Another way of counting the number of distinguishable orbits is to use (n, ε) **spanning sets**, or (n, ε) **dense sets** (Young, 2003).
Let (X, d) be a compact metric space and let f be a continuous self map of X.

For any two points x and y of X, and any $n \geq 1$, let

$$d_n^f(x,y) \;=\; \max_{0 \leq i \leq n-1} \{d(f^i(x), f^i(y))\}$$

We denote the open ball $\{y \in X |\; d_n^f(x,y) < \varepsilon\}$ by $B_f(x,\varepsilon,n)$.
A set $E \subseteq X$ is **ε-dense** with respect to d_f^n, or **(n,ε)-dense**, if $X \subseteq \bigcup_{x \in E} B_f(x,\varepsilon,n)$. The **$\varepsilon$-capacity** of d_f^n, denoted by $S_d(f,\varepsilon,n)$ is the minimal cardinality of an (n,ε)-dense set.
Consider the exponential growth rate

$$h_d(f,\varepsilon) \;:=\; \overline{\lim_{n\to\infty}} \frac{1}{n} log\; S_d(f,\varepsilon,n) \tag{2.1}$$

We define

$$h_d(f) \;:=\; \lim_{\varepsilon\to 0} \; h_d(f,\varepsilon) \tag{2.2}$$

For equivalent metrics d and d', $h_d(f) = h_{d'}(f)$, and both may be denoted by $h(X,f)$, which is the topological entropy. For a compact dynamical system (X,f), and for any positive integer n, $h(X,f^n) = nh(X,f)$ (Adler et al., 1965).
It is not possible to find the exact value of topological entropy always. To get estimates for topological entropy, some concepts of fractal dimensions are used. We make use of the upper box counting dimension. For a compact metric space (X,d), the **upper box counting dimension** is

$$D_d(X) = \overline{\lim_{\varepsilon\to\, 0}} \frac{log\; b(\varepsilon)}{|log\; \varepsilon|} \tag{2.3}$$

where $b(\varepsilon)$ is the number of ε-balls required to cover X.
Systems with positive entropy are considered to be chaotic.

2.5 TOPOLOGICAL CONJUGACY

In order to identify dynamical systems with similar behaviour, the concept of **topological conjugacy** is used.

Definition 2.5.1. *A system (X,f) is said to be* ***topologically conjugate*** *to (Y,g) if there exists a homeomorphism $h:\; X \;\to\; Y$ such that $h^{-1}gh \;=\; f$.*

Theorem 2.5.1. *Let (X, f) and (Y, g) be dynamical systems and h be a homeomorphism from X to Y such that $h^{-1}gh = f$. Let x be any point of X. Then*

(i) h (Orbit of x under f) = Orbit of $(h(x))$ under g.

(ii) If x is a periodic point of f with period k, then $h(x)$ is a periodic point of g with period k.

(iii) If the periodic points of f are dense in X, then the periodic points of g are also dense in Y.

(iv) If f is transitive, so is g.

(v) If f is Devaney-chaotic, so is g.

(vi) Topological entropy of f = Topological entropy of g.

However, if f is sensitive we cannot always say that g is sensitive (Grosse-Erdmann and Manguillot, 2011).
Sometimes, if a function f is difficult to analyze, a simpler conjugate of f can be studied. At one end we have equicontinuous functions, and at the other end we have chaotic functions. Between these extreme classes there are many other distinct types of dynamical behaviour.

2.6 SYMBOLIC DYNAMICAL SYSTEMS

The above basic concepts are discussed in (Kůrka, 2003), for a **Cantor space**. It is a metric space which is compact, totally disconnected and perfect. Any two Cantor spaces are homeomorphic. A **symbolic space** is a closed subset of a Cantor space. It is compact and totally disconnected. A **symbolic dynamical system**, denoted by SDS, is an ordered pair (X, f), where X is a symbolic space and $f : X \to X$ is a continuous function.
Let A be a finite set with m elements, where $m \geq 2$. A **word** over A is finite sequence $w =$

$w_0w_1w_2\cdots w_{l-1}$ of elements of A. The length of w is l, denoted by $|w|$. A^n denotes the set of all words of length n. The set of all words is denoted by $A^* : A^* = \bigcup_{n\geq 0} A^n$.
$A^{\mathbb{Z}}$ is the set of all two sided configurations or bi-infinite sequences over A. Its elements are of the type $x = \cdots x_{-2}x_{-1}x_0x_1x_2 \cdots$, where $x_i \in A \; \forall \; i$. The word $x_ix_{i+1}\cdots x_j$ is denoted by $x_{[i,j]}$. For any $w = w_0w_1w_2 \cdots w_{l-1} \in A^l$, $\overline{w} \in A^{\mathbb{Z}}$ is the infinite repetition of w defined by $(\overline{w})_{nl+i} = w_i$ for $i = 0,1,2,\cdots l-1$. That is,
$\overline{w} = \cdots w_0w_1 \cdots w_{l-1}\overbrace{w_0}^{0^{th}}w_1 \cdots w_{l-1}w_0w_1 \cdots w_{l-1} \cdots$.
Let A have discrete topology and $A^{\mathbb{Z}}$ have the product topology. It is induced by the metric $d(x,y) = 2^{-n}$ where $n = min\{i \geq 0, \; x_i \neq y_i, \; or \; x_{-i} \neq y_{-i}\}$. The shift map $\sigma : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by $\sigma(x)_i = x_{i+1}$ is continuous in this topology. $A^{\mathbb{Z}}$ is a Cantor space. The system $(A^{\mathbb{Z}}, \; \sigma)$ is called the **two sided full shift**. A **two sided subshift** is the dynamical system $(\Sigma, \sigma|_{\Sigma})$, where Σ is a closed subspace of $A^{\mathbb{Z}}$ such that $\sigma(\Sigma) = \Sigma$.
The topological entropy of the the full-shift $(A^{\mathbb{Z}}, \sigma)$ is $log \; p$, where p is the number of elements in A (see section 3.4), and so for $(A^{\mathbb{Z}}, \sigma^k)$ it is $k \; log \; p$.

Definition 2.6.1. *A map $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is **a cellular automaton (CA)** if there exists an $r \in \mathbb{N}^+$, and a local rule $g : A^{2r+1} \to A$ such that $f(x)_i = g(x_{i-r}, x_{i-r+1}, \cdots, x_i, x_{i+1}, \cdots, x_{i+r})$. Here r is called the radius of the CA.*

By a theorem of Hedlund (Hedlund, 1969), a map $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a CA if and only if f is continuous and commutes with the shift map σ.
A slight variation of a CA is a **nonuniform CA**. (Dennunzio et al., 2012). For a non-uniform CA, the radius is not uniform and the local function g is also not uniform. It is given by a rule

$$f(x)_i = g_i(x_{i-r_i}, x_{i-r_i+1}, \cdots, x_i, x_{i+1}, \cdots, x_{i+r_i}). \tag{2.4}$$

Here r_i ang g_i depend on i. A non-uniform CA is just a continuous function (Dennunzio et al., 2012). Generally, only some special types of nonuniform CA are studied.
We may not get conjugacy to a well-known function like the full shift always, so we use the concept of a **factor** map.

Definition 2.6.2. *A morphism $\pi : (X, f) \to (Y, g)$ between two dynamical systems s a continuous map π satsisfying $\pi f = g\pi$. If π is surjective we say that (Y, g) is a **factor** of (X, f)*

and (X, f) *is an* ***extension*** *of* (Y, g).

Every compact dynamical system is a factor of some subshift (Kůrka, 2003).
The **one-sided full shift** is the system $(A^{\mathbb{N}}, \sigma)$ where $\sigma(x_1x_2x_3x_4\cdots) = x_2x_3x_4\cdots$. Here σ is not a homeomorpism, but is Devaney-chaotic. The one sided full shift is positively expansive, whereas the two sided fullshift is an expansive homeomorphism.

Chapter 3

DYNAMICAL SYSTEMS FROM EXTENSION OF p-ADIC ADDITION

3.1 A DEVANEY-CHAOTIC DYNAMICAL SYSTEM USING p-ADIC ADDITION WITH A CARRY

Consider the sets $\mathbb{Z}_p \subset \mathbb{Q}_p \subset A^{\mathbb{Z}}$ where $A = \{0, 1, 2, \cdots, p-1\}$ and p is a prime number. The first question is whether we can extend the non-Archimedean topology of $\mathbb{Q}_p$ to $A^{\mathbb{Z}}$. The norm of x, or the "distance of x from 0" cannot be extended because $\|x\|_p$ is p^m where m is the largest integer such that m^{th} coordinate of x in the canonical representation of x is nonzero. There is no such m for elements outside $\mathbb{Q}_p$. So the metric cannot be extended in a natural way.

We can at most extend the topology to $A^{\mathbb{Z}}$, by defining open balls centred at x in a similar fashion. Let x_i denote the i^{th} coordinate of x, for any element of $A^{\mathbb{Z}}$. Define $\mathbf{B}_{p^r}(x) = \{ y \in A^{\mathbb{Z}} \mid x_i = y_i \ \forall \ i > r\}$. Then $\mathbb{Q}_p$ is an open subset of $A^{\mathbb{Z}}$ in this topology. In fact, $\mathbb{Q}_p = \bigcup_{i=-\infty}^{i=+\infty} \mathbf{B}_{p^i}(0)$. $\mathbb{Q}_p$ is complete implies that it is closed in $A^{\mathbb{Z}}$. Thus $\mathbb{Q}_p$ is both open and closed. Hence any element outside $\mathbb{Q}_p$ is in a different component, and any continuous function on $\mathbb{Q}_p$ cannot be extended naturally and uniquely to $A^{\mathbb{Z}}$.

Next consider $\mathbb{Q}_p$ as a subset of $A^{\mathbb{Z}}$. We denote the non-Archimedean topology of $\mathbb{Q}_p$ by T_1. Let A have discrete topology. Let T_2 denote the product topology on $A^{\mathbb{Z}}$ and its restrictions to $\mathbb{Z}_p$ and $\mathbb{Q}_p$.

We know that T_2 is induced by the metric $d(x,y) = 2^{-r}$ where $r = \min\{i \geq 0 \mid x_i \neq y_i \text{ or } x_{-i} \neq y_{-i}\}$. We can as well replace 2 by p, and define the distance as p^{-r}. Note that it will induce the same topology.

Proposition 3.1.1. *(i)* $\mathsf{T}_1 = \mathsf{T}_2$ *on* $\mathbb{Z}_p$.

(ii) T_1 *is finer than* T_2 *on* $\mathbb{Q}_p$.

(iii) $\mathbb{Q}_p$ *is dense in* $A^{\mathbb{Z}}$ *(with respect to* T_2 *)*

(iv) $\mathbb{Z}_p$ *is a closed subset of* $A^{\mathbb{Z}}$ *in* T_2

Proof. (i) If $x = \cdots x_{-2}\, x_{-1} \overbrace{x_0}^{0^{th}} 0\, 0 \cdots$ then $\mathrm{B}_{p^{-r}}(x)$, that is the ball of radius p^{-r}, for a positive integer r, centered at x is the same in both the topologies of $\mathbb{Z}_p$. It consists of elements of the type

$x = \cdots * \ * \ * \ x_{-r} \cdots x_{-2}\, x_{-1} \overbrace{x_0}^{0^{th}} 0\, 0 \cdots$.

(ii) Consider open balls of radius p^{-r} in both topologies. It is enough to consider $r > 1$. Let $\mathrm{B}^1_{p^{-r}}(x)$ be the ball of radius p^{-r} centered at x in T_1, and $\mathrm{B}^2_{p^{-r}}(x)$ the corresponding one in T_2 for $\mathbb{Q}_p$.

Let $x = \cdots x_{-2}\ x_{-1} \overbrace{x_0}^{0^{th}} x_1\ x_2\ \cdots x_m\ 0\ 0 \cdots$ be an element of $\mathbb{Q}_p$. Then $\mathrm{B}^1_{p^{-r}}(x)$ consists of elements of the type

$\cdots\ *\ *\ *\ x_{-r}\, x_{-r+1}\ \cdots x_{-2}\, x_{-1} \overbrace{x_0}^{0^{th}} x_1\, x_2\ \cdots x_m\, 0\, 0 \cdots$, whereas $\mathrm{B}^2_{p^{-r}}(x)$ consists of elements of the type

$\cdots\ *\ *\ x_{-r}\, x_{-r+1}\ \cdots x_{-2}\, x_{-1} \overbrace{x_0}^{0^{th}} x_1\, x_2\ \cdots x_r\ *\ *\ \cdots$.

Therefore $\mathrm{B}^1_{p^{-r}}(x) \subseteq \mathrm{B}^2_{p^{-r}}(x)$, and so T_1 is finer than T_2 on $\mathbb{Q}_p$.

(iii) Let

$a = \ \cdots\ x_{-r-1}\, x_{-r}\, x_{-r+1}\ \cdots x_{-2}\, x_{-1} \overbrace{x_0}^{0^{th}} x_1\, x_2\ \cdots x_r\ \cdots$ be an element of $A^{\mathbb{Z}}$.

Define

$$a_n = \cdots\ x_{-r-1}\, x_{-r}\, x_{-r+1}\ \cdots x_{-2}\, x_{-1} \overbrace{x_0}^{0^{th}} x_1\, x_2\ \cdots\ x_n\, 0\, 0\, 0\ \cdots \tag{3.1}$$

Then $d(a_m, a_n) \leq p^{-k}$ where k is min $\{m,n\}$, hence $\{a_n\}$ is a Cauchy sequence in T_2, which clearly converges to a in T_2. It is not Cauchy in T_1, unless $a \in \mathbb{Q}_p$.

(iv) We prove that the complement of $\mathbb{Z}_p$ is open. Take any element

$$x = \cdots x_{-2}\, x_{-1} \overbrace{x_0}^{0^{th}} x_1\, x_2 \cdots \underbrace{x_m}_{\neq 0} x_{m+1} * * \cdots$$

of $A^{\mathbb{Z}} \setminus \mathbb{Z}_p$, where $x_m \neq 0$ for some $m > 0$. Take $\delta = p^{-m}$. Then $\mathrm{B}^2_\delta(x) \subset A^{\mathbb{Z}} \setminus \mathbb{Z}_p$, because for all y in $\mathrm{B}^2_\delta(x)$, the m^{th} coordinate $y_m = x_m \neq 0$, and so $y \notin \mathbb{Z}_p$.

□

Our aim is to find what functions $\mathbb{Z}_p \to \mathbb{Z}_p$ and $\mathbb{Q}_p \to \mathbb{Q}_p$ can be extended to functions $A^{\mathbb{Z}} \to A^{\mathbb{Z}}$, to give rise to new dynamical systems, particulary chaotic.
In order to extend a function f on $\mathbb{Q}_p$ to a continuous function on $A^{\mathbb{Z}}$, f should be uniformly continuous in T_2, as $A^{\mathbb{Z}}$ is compact (by Tychonoff's theorem). We can see that any of the algebraic functions like polynomials, or even multiplication by a constant is not uniformly continuous. It is because when x and c, whose norms are say, p^m and p^j, are multiplied, the product has norm p^{m+j}, and the digits upto $m+j$ depend both on x and c. The "carry" travels from right to left; so even if x and y agree on a large range of coordinates around the 0^{th} postion, say $-j$ to j, xc and yc need not agree around the 0^{th} position. In other words, we cannot choose a j such that $d(x,y) < p^{-j}$ implies $d(xc,yc) < \varepsilon$, for small ε.
For example take $p = 2$, and consider the element $c = \cdots 1111 \cdots 11111.00000 \cdots$ in $\mathbb{Q}_p$. We see that multiplication by c is discontinuous at 0, in both T_1 and T_2. Clearly $0c = 0$. Let $\varepsilon < 1$ be given. Consider any $\delta > 0$. Take an integer m such that $2^{-m} < \delta$. Let

$$x = \cdots 00000 \cdots 0000.\underbrace{000 \cdots 000}_{m \text{ times}}1000 \cdots.$$ Then

$$xc = \cdots 1111 \cdots 11111.\underbrace{111 \cdots 1111}_{m+1 \text{ times}}00000000.$$ Thus $d(x,0) < \delta$, but $d(xc, x0) = 1 > \varepsilon$ in T_2, and $d(xc, x0) = 2^{m+1} > \varepsilon$ in T_1.
Consider adding a constant to any element of $\mathbb{Q}_p$. This gives a uniformly continuous function on $\mathbb{Q}_p$.

Proposition 3.1.2. *Let*

$$c = \cdots c_{-1} \overbrace{c_0}^{0^{th}} c_1 \cdots c_{n-1}\, c_n\, 0\, 0\, 0 \cdots$$ *be any fixed element of* $\mathbb{Q}_p$. *Let* $\varphi : \mathbb{Q}_p \to \mathbb{Q}_p$

be given by $\varphi(x) = x + c$. This can be extended to a function on $A^{\mathbb{Z}}$ that is continuous in the product topology.

Proof. For any

$x = \cdots x_{-2}x_{-1}\overbrace{x_0}^{0^{th}} x_1\, x_2 \cdots x_m\, 0\,0\,0 \cdots$, take $j > |n|$. Adding the constant c affects only the n^{th} coordinate and the coordinates to the left. If x and y agree from $-j^{th}$ to j^{th} coordinates, so do $\varphi(x)$ and $\varphi(y)$. This n depends only on the constant c and not on x. If $d(x,y) < p^{-j}$, then $d(\varphi(x),\varphi(y)) < p^{-j}$. Therefore adding a constant gives a uniformly continuous function on $\mathbb{Q}_p$. Therefore, if $\{a_n\}$ is a sequence in $\mathbb{Q}_p$ converging to x in $A^{\mathbb{Z}}$, then $\varphi(a_n)$ converges to a unique point $\varphi(x)$ in $A^{\mathbb{Z}}$. Therefore $\varphi : x \mapsto x + a$ extends to a continuous function on $A^{\mathbb{Z}}$. □

Note that $(A^{\mathbb{Z}}, \varphi)$ is similar to the adding machine in (Kůrka, 2003). Combining φ with powers σ^k of the shift map, we get maps that are chaotic in the sense of Devaney. We denote $\sigma^k(x)$ also by $p^k x$. Fix an element a of $\mathbb{Q}_p$ and define a function f on $A^{\mathbb{Z}}$ by

$$f : x \mapsto a + p^k x \tag{3.2}$$

This is chaotic according to the definition by Devaney, as we can see that it is conjugate to σ^k.

Proposition 3.1.3. *Let k be any nonzero integer, and let a be a p-adic number. Let f be the function $A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by $f : x \mapsto a + p^k x$. Then f is conjugate to σ^k.*

Proof. Let $b = \frac{a}{1-p^k}$. Define $\varphi : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ by $\varphi(x) = x - b$. Then

$$\begin{aligned} \varphi \circ f \circ \varphi^{-1}(x) &= \varphi \circ f(x+b) \\ &= \varphi(p^k x + p^k b + a) = p^k x + p^k b + a - b \\ &= p^k x + b(p^k - 1) + a = p^k(x) = \sigma^k(x). \end{aligned} \tag{3.3}$$

□

As 0 is the only fixed point of σ^k, it follows that b is the only fixed point of f. For f

restricted to $\mathbb{Q}_p$ and positive k it is an attractive fixed point. For negative k it is a repelling fixed point.

Proposition 3.1.4. *Let $f : \mathbb{Q}_p \to \mathbb{Q}_p$ be defined by $f(x) = p^k x + a$, for a constant a in $\mathbb{Q}_p$, and positive k. For all x in $\mathbb{Q}_p$, $f^n(x)$ converges to $b = \frac{a}{1-p^k}$.*

Proof. For any positive integer n, and any x in $\mathbb{Q}_p$,

$$\begin{aligned} f^n(x) &= xp^{nk} + a(1 + p^k + p^{2k} + \cdots + p^{(n-1)k}) \\ &= xp^{nk} + a\frac{1-p^{nk}}{(1-p^k)} \\ &= (x-b)p^{nk} + b \end{aligned} \tag{3.4}$$

For positive k, p^{nk} tends to zero as n tends to infinity, in the topology T_1 of $\mathbb{Q}_p$ and so in the coarser topology T_2 too. For any x in $\mathbb{Q}_p$, xp^{nk} also tends to zero in this topology, and so in the coarser topology T_2 too. Therefore $f^n(x)$ tends to b for any x in $\mathbb{Q}_p$. $\square$

(Note : For negative k, p^{nk} does not tend to zero when n tends to infinity, and so $f^n(x)$ cannot tend to b for $x \neq b$.)

The periodic points of f are $\overline{w} + b$, where w is a word of length $|nk|$ in $A^{\mathbb{Z}}$. For any transitive point y of σ^k, $y + b$ is a transitive point of f.

Clearly f is not a cellular automaton but is a non-uniform cellular automaton. However, it does not have any properties of the type non-uniform cellular automata defined in (Dennunzio et al., 2012).

3.2 AN EXPANSIVE MAP WITH POSITIVE ENTROPY

When the above function f is applied to x, the coordinates at the far right are affected only by the shift map. We try to look for a function that affects all the coordinates. For computational purposes, it is good if we can start calculating the digits of $f(x)$ at the centre, that is around the 0^{th} coordinate and proceed iteratively in both directions. We try to extend the above addition to an addition in $A^{\mathbb{Z}}$. It would be better if can add two elements of $A^{\mathbb{Z}}$, in a way different from the usual coordinate-wise addition mod p, ie., making use of the the "carry".

Let $a = \cdots a_{-2}\, a_{-1} \overbrace{a_0}^{0^{th}} a_1\, a_2 \cdots$ and $b = \cdots b_{-2}\, b_{-1} \overbrace{b_0}^{0^{th}} b_1\, b_2 \cdots$ be any two elements of $A^{\mathbb{Z}}$.

We define a new kind of "addition" as follows.

$a + b = c = \ldots c_{-2}\, c_{-1} \overbrace{c_0}^{0^{th}} c_1\, c_2 \cdots$ where

$\cdots c_{-2}\, c_{-1}\, c_0$ is the usual sum of the p-adic integers $\cdots a_{-2}\, a_{-1}\, a_0$ and $\cdots b_{-2}\, b_{-1}\, b_0$, with carries transferred to the left, and $\cdots c_2\, c_1$ is the usual sum of the p-adic integers $\cdots a_2\, a_1$ and $\cdots b_2\, b_1$. In other words, the given elements are split after the 0^{th} position, the two parts are considered as seperate p-adic integers and added in the usual way. For the left part, addition proceeds from right to left, and for the right part it proceeds from left to right. Actually this operation makes $A^{\mathbb{Z}}$ into a topological group. The additive identity of the group is the zero sequence. The additive inverse of an element a is defined in a similar fashion as that of p-adic integers.

Let a_{-m} be the first non-zero digit of a on the left side (starting at the 0^{th} position), and let a_n be the first non-zero digit of a on the right side (starting at the 1^{st} position).

That is, $a = \cdots a_{-m-1} \underbrace{a_{-m}}_{\neq 0} 0\, 0 \cdots 0 \overbrace{0}^{0^{th}} 0 \cdots 0 \underbrace{a_n}_{\neq 0} a_{n+1} \cdots$

Then we define $-a =$

$\cdots\ (p-1-a_{(-m-2)})\ (p-1-a_{(-m-1)})\ \overbrace{(p-a_{-m})}^{(-m)^{th}}\ 0 \cdots\ 0^{th}\ 0\ \cdots 0\ \overbrace{(p-a_n)}^{n^{th}}\ (p-1-a_{(n+1)})\ (p-1-a_{(n+2)})\ \cdots$

Using this operation in combination with the shift map we try to get some chaotic maps. First consider $f(x) = \sigma^k(x) + a$ for a constant a in $A^{\mathbb{Z}}$. This is clearly a homeomorphism. Now we prove that $(A^{\mathbb{Z}}, f)$ is conjugate to some subshift. For this, we use a result from (Kůrka, 2003)(p. 140, Proposition 3.68) for compact dynamical systems.

Proposition 3.2.1. *A bijective dynamical system (X, f) is conjugate to a two-sided subshift if and only if it is expansive and X is totally disconnected.*

Using the above result, we have

Proposition 3.2.2. *Let $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be given by $f(x) = \sigma^k(x) + a$. Then*

$(A^{\mathbb{Z}}, f)$ is conjugate to a subshift and $h(A^{\mathbb{Z}}, f) = h(A^{\mathbb{Z}}, \sigma^k) = k\ log\ p$.

Proof. To add a, to any elements x and y of $A^{\mathbb{Z}}$, we start at 1^{st} position and move towards right. So the first difference between coordinates of $x+a$ and $y+a$ towards right is encounterd exactly at the positon where the first difference between coordinates of x and y occurs. After that we cannot say anything about whether the coordinates are same or different. They may differ for x and y, but may be same for $x+a$ and $y+a$, and vice versa. The same is true for the left side also.
Let $d(x,y) = p^{-j}$. We make the following observations.

Case(i) Suppose that $x_i = y_i$ for all $i \geq 0$. Then $(\sigma^{nk}(x))_i = (\sigma^{nk}(y))_i$ for all $i \geq 0$, and $(f^n(x))_i = (f^n(y))_i$ for all $i \geq 0$. Any difference in the coordinates appears only for negative i. When we start from the central 0^{th} position and move left, the first position where the difference appears is same for f^n and σ^{nk}, and it keeps moving to the left with successive applications of f and σ^k. Therefore

$$d(f^n(x), f^n(y)) \ = \ d(\sigma^{nk}(x), \sigma^{nk}(y)) \text{ for all } n \geq 0. \tag{3.5}$$

Moreover, this distance decreases as n increases.

Case(ii) Let $x_i = y_i$ for $0 \leq i < mk+l$ and $x_{mk+l} \neq y_{mk+l}$ for some $m \geq 0$ and some l with $0 \leq l < k$. Clearly $j \leq mk+l$. Then for $n \leq m$,
$(f^n(x))_i = (f^n(y))_i$ and $(\sigma^{nk}(x))_i = (\sigma^{nk}(y))_i$ for $0 \leq i < (m-n)k+l$ and
$(f^n(x))_{(m-n)k+l} \neq (f^n(y))_{(m-n)k+l}$ and $(\sigma^{nk}(x))_{(m-n)k+l} \neq (\sigma^{nk}(y))_{(m-n)k+l}$.
Now $(m-n)k+l \geq 0$, and upto this n, any difference in the coordinates of x and y from the right side of 0^{th} position is not yet transferred to the left. At the left side, if at all there is a difference in the coordinates of x and y, it moves further to the left with successive applications of f and σ^k. Therefore we can say that

$$d(f^n(x), f^n(y)) = d(\sigma^{nk}(x), \sigma^{nk}(y)) \ for \ \ 0 \leq n \leq m. \tag{3.6}$$

For $n = m+1$, $(\sigma^{nk}(x))_{-k+l} \neq (\sigma^{nk}(y))_{-k+l}$. Therefore $d(\sigma^{nk}(x), \sigma^{nk}(y)) \geq p^{l-k}$.

For $f^n(x)$ and $f^n(y)$ there may be a difference in the coordinates at any of the positions $l-k,\ l-k+1,\cdots,-1,0$, or to the right side of 0^{th} position. In any case we can say that

$$d(f^n(x), f^n(y)) \geq p^{-k} \text{ and } d(\sigma^{nk}(x), \sigma^{nk}(y)) \geq p^{-k}. \tag{3.7}$$

We will prove that f is expansive, using the fact that σ^k is expansive. Take $\varepsilon = p^{-k}$. For $x \neq y$, we have to find $n \in \mathbb{Z}$ such that $d(f^n(x), f^n(y)) \geq \varepsilon$. If $d(x,y) \geq \varepsilon$, we are through.

Let $d(x,y) < \varepsilon$. Suppose that there is some positive j such that $d(\sigma^{jk}(x), \sigma^{jk}(y)) \geq \varepsilon$. It means that there was a difference in the coordinates of x and y at a position after k, which was brought to a position $\leq k$, after j applications of σ^k. So we are in Case(ii). We can find a positive n satisfying (3.7).

Next suppose that $d(\sigma^{jk}(x), \sigma^{jk}(y)) < \varepsilon$ for all positive j. Then we are in Case(i), and $x_i = y_i$ for all $i \geq 0$. We have to find a positive n such that $d(f^{-n}(x), f^{-n}(y)) \geq \varepsilon$.

$f^{-1}(x) = \sigma^{-k}(x-a)$. Let $j = mk+l$, with $m \geq 1$, and $0 \leq l < k$, be the smallest positive integer such that $x_{-j} \neq y_{-j}$. It follows that $(x-a)_i = (y-a)_i$ for all $i > -j$, and $(x-a)_{-j} \neq (y-a)_{-j}$. Therefore $(\sigma^{-k}(x-a))_i = (\sigma^{-k}(y-a))_i$ for $-j+k < i$ and $(\sigma^{-k}(x-a))_{-j+k} \neq (\sigma^{-k}(y-a))_{-j+k}$. Therefore $d(\sigma^{-k}(x-a), \sigma^{-k}(y-a)) = p^{-j+k}$. Thus by one application of f^{-1} the distance is increased by a factor of p^k. Successive applications of f^{-1}, m times gives $d(f^{-m}(x), f^{-m}(y) \geq \varepsilon$. Thus f is expansive, hence is conjugate to a subshift.

Now we find the topological entropy of f. We prove that $B_f(x,r,n) = B_{\sigma^k}(x,r,n)$ (see (2.4)), for sufficiently large n and sufficiently small r. Let $r < p^{-2k}$ and $n > 2$. Suppose that $y \in B_f(x,r,n)$ for some x. Then $d(f^i(x), f^i(y)) \leq r < p^{-2k}$, for $0 \leq i \leq n-1$. If x and y are as in Case(i), clearly $d(\sigma^{ik}(x), \sigma^{ik}(y)) \leq r$ for $0 \leq i \leq n-1$, and $y \in B_{\sigma^k}(x,r,n)$.

If x and y are not as in Case(i), then take m and l as in Case(ii). Then $n-1 \leq m$, because of (3.7), and from (3.6) it follows that $y \in B_{\sigma^k}(x,r,n)$. Therefore $B_f(x,r,n) \subseteq B_{\sigma^k}(x,r,n)$. By a similar argument $B_{\sigma^k}(x,r,n) \subseteq B_f(x,r,n)$. It follows that $S_d(f,r,n) = S_d(\sigma^k,r,n)$, and from (2.1) and (2.2) both f and σ^k have same topological entropy, that is $k\ log\ p$.

□

3.3 A POSITIVELY EXPANSIVE MAP

We try to modify the above map f to get a positively expansive map (2.3.25), with positive topological entropy.

For any $x = \cdots x_{-2}\, x_{-1} \overbrace{x_0}^{0^{th}} x_1\, x_2 \cdots$ in $A^{\mathbb{Z}}$, define the "reflection" about 0^{th} coordinate, $r(x)$, as $\cdots x_2\, x_1 \overbrace{x_0}^{0^{th}} x_{-1}\, x_{-2} \cdots$. That is $r(x)_i = x_{-i}$ for all $i \in \mathbb{Z}$.

Let x and y be two distinct points in $A^{\mathbb{Z}}$, separated by a distance p^{-j}. To get a positively expansive function f, we have to increase the distance between them at each application of f. If there is a difference in the j^{th} coordinates, for $j > k > 0$, application of σ^k brings the difference to $(j-k)^{th}$ position, and so the distance increases by a factor of p^k. But if there is no difference in the positively numbered coordinates, application of σ^k will not increase the distances. So we use the function r to transfer the difference in coordinates at the left side to the right side. We use a combination of σ, r and the addition. Now define $f(x) = r(\sigma^k(x) + x)$. It is enough to consider positive values of k.

Proposition 3.3.1. *The function $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by $f(x) = r(\sigma^k(x) + x)$, where k is a positive integer, is continuous and positively expansive.*

Proof. Obviously, σ^k is a homeomorphism and r is an isometry. Therefore it is enough to verify that the addition map given by $(x,y) \mapsto x + y$ is continuous from $A^{\mathbb{Z}} \times A^{\mathbb{Z}}$ to $A^{\mathbb{Z}}$. Then the function f is (uniformly) continuous on $A^{\mathbb{Z}}$.

For any(x,y) in $A^{\mathbb{Z}} \times A^{\mathbb{Z}}$, consider the p^{-j} neighbourhood of $x+y$ in $A^{\mathbb{Z}}$. Consider any x' in $A^{\mathbb{Z}}$ with $d(x,x') < p^{-j}$, and any y' in $A^{\mathbb{Z}}$ with $d(y,y') < p^{-j}$. The coordinates of x are same as those of x' for $-j,\ -j+1\ ,\ -j+2,\ \cdots 0,\ 1, \cdots\ j-1,\ j$. The same is true for y and y'. Therefore the coordinates of $x+y$ and $x'+y'$ agree from $-j$ to j.

So, $d(x,x') < p^{-j}$ and $d(y,y') < p^{-j} \Rightarrow d(x+y, x'+y') < p^{-j}$. Thus the operation $+$ is continuous.

Next, we verify that f is positively expansive.

Let $x = \cdots x_{-j}\, x_{-j+1} \cdots x_{-2}\, x_{-1} \overbrace{x_0}^{0^{th}} x_1\, x_2 \cdots x_{j-1}\, x_j \cdots$

$\sigma^k(x) = \cdots x_{k-j}\, x_{k-j+1} \cdots x_{k-2}\, x_{k-1} \overbrace{x_k}^{0^{th}} x_{k+1}\, x_{k+2} \cdots x_{k+j-1}\, x_{k+j} \cdots$

Choose an $\varepsilon < p^{-k}$. If $x \neq y$, let $d(x,y) = p^{-j}$. If $j \leq k$, take $n = 0$.

Let $d(x,y) = p^{-j}$, with $j > k$.

Then $x_i = y_i$ for $-j+1 \leq i \leq j-1$, and either $x_j \neq y_j$ or $x_{-j} \neq y_{-j}$. We denote $\sigma^k(x)+x$ by x' and $\sigma^k(y)+y$ by y'.

Case(i) Suppose that $x_j \neq y_j$. Then $\sigma^k(x)_{j-k} \neq \sigma^k(y)_{j-k}$ and $\sigma^k(x)_i = \sigma^k(y)_i$ for $0 \leq i < j-k$, on the right side. On the left side, $\sigma^k(x)_i = \sigma^k(y)_i$ for $(-j+1) \leq i \leq 0$. Therefore, $x'_i = y'_i$ for $-j+1 \leq i < j-k$, and $x'_{j-k} \neq y'_{j-k}$. When r is applied, $(r(x'))_i = (r(y'))_i$ for $-j+k < i \leq j-1$ and $(r(x'))_{-j+k} \neq (r(y'))_{-j+k}$. Therefore $d(f(x), f(y))$ is p^{-j+k}.

Case (ii) If $x_j = y_j$, then $x_{-j} \neq y_{-j}$. Then $\sigma^k(x)_i = \sigma^k(y)_i$ for $0 \leq i \leq j-k$, on the right side. On the left side, $\sigma^k(x)_i = \sigma^k(y)_i$ for $-j \leq i \leq 0$, and $x_{-j} \neq y_{-j}$. Therefore $x'_i = y'_i$ for $(-j+1) \leq i \leq (j-k)$ and $x'_{-j} \neq y'_{-j}$. When r is applied, $(r(x'))_i = (r(y'))_i$ for $(-j+k) \leq i \leq (j-1)$ and $(r(x'))_j \neq (r(y'))_j$. For $i < (-j+k)$ we cannot conclude anything about $(r(x'))_i$ and $(r(y'))_i$. Therefore $d(f(x), f(y))$ is either $> p^{-j}$, or $d(f(x), f(y)) = p^{-j}$ and we are back in case(i). Another application of f will increase the distance.

It follows that application of f once or twice increases the distances by a factor of atleast p^k. Repeating this process, we can bring the distance to a value $\geq p^{-k} > \varepsilon$. Thus the function is positively expansive. □

We use the following result from (Bahi and Guyeux, 2013)(p. 40, Proposition 21)

Proposition 3.3.2. *For a positively expansive system (X, f), topological entropy $h(X, f) > \sup\{\frac{p_n}{n}\}$, where p_n is the number of points with period n.*

It follows that $h(X, f) \geq 1$, because there is a fixed point 0.

3.4 A MAP THAT INCREASES SMALL DISTANCES

Let X be a metrizable space. We say that a self map f of X **increases small distances** if there is a compatible metric d, and there exists an $\varepsilon > 0$ such that $0 < d(x,y) < \varepsilon$ implies

$d(f(x), f(y)) > d(x,y)$. We can further modify the above map to a map that increases small distances, and give both upper and lower bounds for entropy.

We make use of the following result from (Fujita et al., 2010)(p. 627, Proposition 5.1).

Proposition 3.4.1. *Let $f : X \to X$ be a map of a compactum X with metric d. Suppose there exist positive numbers $\varepsilon > 0$ and $1 < \lambda_2 \leq \lambda_1$ such that if $x, y \in X$ and $0 < d(x,y) \leq \varepsilon$, then $\lambda_2 d(x,y) \leq d(f(x), f(y)) \leq \lambda_1 d(x,y)$. Then the following inequalities hold.*

$$D_d(X) \log \lambda_2 \leq h(f) \leq D_d(X) \log \lambda_1 \tag{3.8}$$

In the above map f given by $f(x) = r(\sigma^k(x) + x)$, to increase small distances, one or two applications of f are needed. If we replace the "reflection " r by r_1, which reflects x about the $(-1)^{th}$ position, rather than the 0^{th} position, we get a map that not only increases small distances, but satisfies conditions of Proposition 3.4.1.

If $x = \cdots x_{-3}\, x_{-2}\, x_{-1}\, \overbrace{x_0}^{0^{th}}\, x_1\, x_2\, x_3 \cdots$

$r_1(x) = \cdots x_2\, x_1\, x_0\, x_{-1}\, \overbrace{x_{-2}}^{0^{th}}\, x_{-3}\, x_{-4}\, x_{-5} \cdots$

As $r_1(x) = \sigma^2(r(x))$, r_1 is a homeomorphism.

Proposition 3.4.2. *Let $r_1 : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be given by $(r_1(x))_i = x_{-i-2}$. For $k > 2$, define $f(x) = r_1(\sigma^k(x) + x)$. Then for x and y with $0 < d(x,y) < p^{-k}$, $pd(x,y) \leq d(f(x), (y)) \leq p^k d(x,y)$.*

Proof. If $x = \cdots x_{-j}\, x_{-j+1} \cdots x_{-2}\, x_{-1}\, \overbrace{x_0}^{0^{th}}\, x_1\, x_2 \cdots x_{j-1}\, x_j \cdots$

$\sigma^k(x) = \cdots x_{k-j}\, x_{k-j+1} \cdots x_{k-2}\, x_{k-1}\, \overbrace{x_k}^{0^{th}}\, x_{k+1}\, x_{k+2} \cdots x_{k+j-1}\, x_{k+j} \cdots$

Let $d(x,y) = p^{-j}$, with $j > k$.

Then $x_i = y_i$ for $-j+1 \leq i \leq j-1$, and either $x_j \neq y_j$ or $x_{-j} \neq y_{-j}$. We denote $\sigma^k(x) + x$ by x' and $\sigma^k(y) + y$ by y'.

Case(i) Suppose that $x_j \neq y_j$. Then $\sigma^k(x)_{j-k} \neq \sigma^k(y)_{j-k}$ and $\sigma^k(x)_i = \sigma^k(y)_i$ for $0 \leq i < j-k$, on the right side. On the left side, $\sigma^k(x)_i = \sigma^k(y)_i$ for $(-j+1) \leq i \leq 0$. Therefore, $x'_i = y'_i$ for $-j+1 \leq i < j-k$, and $x'_{j-k} \neq y'_{j-k}$. When r_1 is applied,

$(r_1(x'))_i = (r_1(y'))_i$ for $-j+k-2 < i \leq j-3$ and $(r_1(x'))_{-j+k-2} \neq (r_1(y'))_{-j+k-2}$. Therefore $d(f(x), f(y))$ is at least p^{-j+k-2}.

Case(ii) If $x_j = y_j$, then $x_{-j} \neq y_{-j}$. So $\sigma^k(x)_i = \sigma^k(y)_i$ for $0 \leq i \leq (j-k)$, on the right side. On the left side, $\sigma^k(x)_i = \sigma^k(y)_i$ for $-j \leq i \leq 0$, and $x_{-j} \neq y_{-j}$. Therefore $x'_i = y'_i$ for $(-j+1) \leq i \leq (j-k)$ and $x'_{-j} \neq y'_{-j}$. When r_1 is applied, $(r_1(x'))_i = (r_1(y'))_i$ for $(-j+k-2) \leq i \leq (j-3)$ and $(r_1(x'))_{j-2} \neq (r_1(y'))_{j-2}$. Therefore $d(f(x), f(y))$ is at least p^{-j+2}.

In any case, we can conclude that $d(f(x), f(y)) \geq p^l d(x,y)$, where $l = min\{(k-2), 2\} \geq 1$. In both cases, we can verify that $d(f(x), f(y))$ cannot be more than p^{-j+k}.
In Case(i), for $-j+k-2 < i \leq j-3$, coordinates of $f(x)$ and $f(y)$ are equal, and for $-j+k-2$ they differ. So the distance is at least p^{-j+k-2}. If it is exacly p^{-j+k-2}, then

$$d(f(x), f(y)) = p^{-j+k-2} \leq p^{-j+k}. \tag{3.9}$$

If it is not exactly p^{-j+k-2}, then it is more, and so it must be due to the difference in some coordinates at the right side. That is, $f(x)_i \neq f(y)_i$ for some i with $\geq j-2$. Choose the smallest such i. Then

$$d(f(x), f(y)) = p^{-i} \leq p^{-j+2} \leq p^{-j+k}. \tag{3.10}$$

From (3.9) and (3.10), $d(f(x), f(y)) \leq p^{-j+k}$.
In Case(ii), for $-j+k-2 \leq i \leq j-3$, coordinates of $f(x)$ and $f(y)$ are equal, and for $j-2$ they differ. So the distance is at least p^{-j+2}. If it is exactly p^{-j+2}, then as $2 < k$,

$$d(f(x), f(y)) = p^{-j+2} < p^{-j+k}. \tag{3.11}$$

If it is not exactly p^{-j+2}, then it must be more, and so it must be due to the difference in some coordinates at the left side. That is, $f(x)_i \neq f(y)_i$ for some i with $i < -j+k+2$. Choose smallest $|i|$ among such i. Then

$$p^{-j+2} < d(f(x), f(y)) = p^i < p^{-j+k-2} < p^{-j+k}. \tag{3.12}$$

From (3.11) and (3.12), $d(f(x), f(y)) \leq p^{-j+k}$. Hence $d(f(x), f(y)) \leq p^k d(x,y)$. $\square$

For $X = A^{\mathbb{Z}}$, $B(x, p^{-m}) = \{y \in X | y_i = x_i \; for \; -m \leq i \leq m\}$. There are exactly p^{2m+1} balls of radius p^{-m}, and all of them are needed to cover $A^{\mathbb{Z}}$. Therefore

$$D_d(A^{\mathbb{Z}}) = \overline{\lim_{m\to\infty}} \frac{\log(p^{2m+1})}{|\log(p^{-m})|} = \overline{\lim_{m\to\infty}} \frac{(2m+1)\log\, p}{m\log\, p} = 2$$

Now applying Proposition 3.4.1, with $\lambda_2 = p$ and $\lambda_1 = p^k$, we get $2\, \log\, p \leq h(X, f) \leq 2k\, \log\, p$.

REMARKS

- Only in section (3.1) we need p to be prime, to get a field $\mathbb{Q}_p$, so that $b = \frac{a}{1-p^k}$ makes sense.
- When p is prime, every rational number has a unique p-adic expansion, whose digits can be got by iterative algorithms.

Chapter 4

A DEVANEY CHAOTIC MAP WITH POSITIVE ENTROPY

Consider a slight variation of the "reflection" functions r and r_1, which "reflect" about the 0^{th} and $(-1)^{th}$ coordinates respectively. We want a function f such that by fixing $2nk$ consecutive central coordinates, we can fix a unique pre-image under f^{2n} for any given element of $A^{\mathbb{Z}}$. It becomes necessary that the indices of the fixed coordinates remain same after the reflection. It is not possible with r or r_1. So we consider a different reflection, that is a function that maps x_0 to x_1 and vice versa.

$x = \cdots x_{-2}\, x_{-1} \overbrace{x_0}^{0^{th}} x_1\, x_2 \cdots$ is mapped to

$r'(x) = \cdots x_2 \overbrace{x_1}^{0^{th}} x_0\, x_{-1}\, x_{-2} \cdots$. In other words the map r' is given by $(r'(x))_i = x_{(-i+1)}$. It is clearly a homeomorphism.

We consider $f(x) = r'(\sigma^k(x) + x)$, and show below that it is positively expansive and transitive, and it has positive entropy and a dense set of periodic points.

4.1 POSITIVE EXPANSIVENESS

Proposition 4.1.1. *The function $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by $f(x) = r'(\sigma^k(x) + x)$, where k is a positive integer, is continuous and positively expansive.*

Proof. Continuity of f follows from continuity of r' and continuity of the addition in $A^{\mathbb{Z}}$. We only have to verify that f is positively expansive. Choose an $\varepsilon < p^{-k}$. Suppose that $x \neq y$, and $d(x,y) = p^{-j}$. If $j \leq k$, take $n = 0$.

Let $d(x,y) = p^{-j}$, with $j > k$.

Let $x = \cdots x_{-j}\, x_{-j+1} \cdots x_{-2}\, x_{-1} \overbrace{x_0}^{0^{th}} x_1\, x_2 \quad \cdots \quad x_{j-1}\, x_j \cdots$. Then

$\sigma^k(x) = \cdots x_{k-j}\, x_{k-j+1} \cdots x_{k-2}\, x_{k-1} \overbrace{x_k}^{0^{th}} x_{k+1}\, x_{k+2} \cdots x_{k+j-1}\, x_{k+j} \cdots$.

Then $x_i = y_i$ for $-j+1 \leq i \leq j-1$, and either $x_j \neq y_j$ or $x_{-j} \neq y_{-j}$. We denote $\sigma^k(x)+x$ by x' and $\sigma^k(y)+y$ by y'.

Case(i) Suppose that $x_j \neq y_j$. Then on the right side, $\sigma^k(x)_i = \sigma^k(y)_i$ for $0 \leq i < j-k$, and $\sigma^k(x)_{j-k} \neq \sigma^k(y)_{j-k}$. On the left side, $\sigma^k(x)_i = \sigma^k(y)_i$ for $-j+1 \leq i \leq 0$. Therefore, $x'_i = y'_i$ for $-j+1 \leq i < j-k$, and $x'_{j-k} \neq y'_{j-k}$. When r' is applied $(r'(x'))_i = (r'(y'))_i$ for $-j+k+1 < i \leq j$ and $(r'(x'))_{-j+k+1} \neq (r'(y'))_{-j+k+1}$. Therefore $d(f(x), f(y)) = p^{-j+k+1}$. The distance gets multiplied by a factor p^{k+1}, when f is applied.

Case(ii) If $x_j = y_j$, then $x_{-j} \neq y_{-j}$. Then on the right side, $(\sigma^k(x))_i = (\sigma^k(y))_i$ for $0 \leq i \leq j-k$. On the left side $(\sigma^k(x))_i = (\sigma^k(y))_i$ for $-j+1 \leq i \leq 0$. Therefore $x'_i = y'_i$ for $-j+1 \leq i \leq j-k$ and $x'_{-j} \neq y'_{-j}$. When r' is applied $(r'(x'))_i = r'(y')_i$ for $-j+k+1 \leq i \leq j$ and $(r'(x'))_{j+1} \neq r'(y')_{j+1}$. For $i < -j+k+1$ we cannot conclude anything about $(r'(x'))_i$ and $(r'(y'))_i$. Therefore $d(f(x), f(y))$ is atleast p^{-j-1}. Either the distance $d(f(x), f(y))$ is increased by a sufficiently large factor, or we are back in Case (i), and another application of f will increase the distance by a factor p^{k+1}.

Thus in both cases successive applications of f increase the distances till finally $d(f^n(x), f^n(y)) \geq \varepsilon$ for some n. □

Note that f is positively expansive implies f is sensitive, because $A^{\mathbb{Z}}$ is perfect (Kůrka, 2003).

4.2 TRANSITIVITY

Next we verify that f is transitive. First, we prove the following result, which is actually stronger than transitivity:

Proposition 4.2.1. *Let $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be given by $f(x) = r'(\sigma^k(x)+x)$, where k is a positive integer. Let any $y = \cdots y_{-2}\, y_{-1} \overbrace{y_0}^{0^{th}} y_1\, y_2 \cdots$ be given from $A^{\mathbb{Z}}$, and let n be any positive integer. For any set of p-adic digits $a_{-nk+1}, a_{-nk+2}, \cdots, a_{nk}$, there is a unique x in $A^{\mathbb{Z}}$ with $x_i = a_i$ for $i = -nk+1, -nk+2, \cdots, nk$ and $f^{2n}(x) = y$.*

Proof. We use induction on n.

Let $n=1$. Let $a_{-k+1}, a_{-k+2}, \cdots, a_k$ and $y = \cdots y_{-2}\, y_{-1} \overbrace{y_0}^{0^{th}} y_1\, y_2 \cdots$ be given. Consider $y' = r'(y) = \cdots y_3\, y_2 \overbrace{y_1}^{0^{th}} y_0\, y_{-1} \cdots$. Consider the following x where x_i indicates a known coordinate $x_i = a_i$, and a $*$ indicates that the corresponding coordinate is yet to be determined.

$$x = \cdots * * * x_{-k+1} \cdots \overbrace{x_0}^{0^{th}} x_1 \cdots x_k * * * \cdots.$$

$\sigma^k(x) = \cdots * * * x_{-k+1} \cdots x_0\, x_1 \cdots \overbrace{x_k}^{0^{th}} * * \cdots$. Note that in $\sigma^k(x)+x$, The coordinates from $(-k+1)^{th}$ to 0^{th} are fixed. Call these coordinates as $z_{-k+1}, \cdots, z_0$ respectively. We have to find z which is as follows :

$z = \cdots * * * z_{-k+1} \cdots \overbrace{z_0}^{0^{th}} * * * \cdots$. Then

$z' = r'(z)$ will be $\cdots * * * \cdots \overbrace{*}^{0th} z_0\, z_{-1} \cdots z_{-k+1} * * * \cdots$, where the $*$s indicate that the corresponding coordinates are yet to be determined. Here $z'_1 = z_0, z'_2 = z_{-1} \cdots z'_k = z_{-k+1}$. So,

$\sigma^k(z') = \cdots * * * z_0 \cdots \overbrace{z_{-k+1}}^{0^{th}} * * * \cdots$. The remaining coordinates of z' can be easily found so that

$$\sigma^k(z') + z' = y' = \cdots y_3\, y_2 \overbrace{y_1}^{0^{th}} y_0\, y_1 \cdots$$

We have to carry out the calculations for the left and right halves separately. For the left side first fix z'_0, which is the same as z_1, such that $z_1 + z_{-k+1} \equiv y_1 \; mod(p)$. If $z_1 + z_{-k+1} > p$, let c_0 (the carry) be 1, otherwise let c_0 be 0. Next choose $z'_{-1} = z_2$ such that $z_2 + z_{-k} + c_0 \equiv y_2 \; mod(p)$, and call the carry as c_{-1}. Proceed similarly. At every step only the coordinate of $\sigma^k(z')$ is known, and the corresponding coordinate of z' has to be calculated.

The same procedure applies to the right side also. First find $z'_{(k+1)} = z_{(-k)}$, next find $z_{(-k-1)}$, and so on. Here, at every step the coordinate of z' is known and the corresponding coordinate of $\sigma^k(z')$ has to be calculated. Thus z' is uniquely determined such that $\sigma^k(z') + z' = y'$, and $r'(\sigma^k(z') + z') = r'(y') = y$. Thus $f(z') = y$.

Now $z = r'(z')$ is known. Hence x can be determined such that $\sigma^k(x) + x = z$, or $r'(\sigma^k(x) + x) = z'$, i.e., $f(x) = z'$, and $f^2(x) = f(z') = y$.

Next assume the result for $n-1$, and prove it for n. Let p-adic digits $a_{-nk+1}, a_{-nk+2}, \cdots, a_{nk}$ and $y = \cdots y_{-2}\, y_{-1} \overbrace{y_0}^{0^{th}} y_1\, y_2 \cdots$ be given. We have to find x such that $x_i = a_i$ for $i = -nk+1, -nk+2, \cdots, nk$, and $f^{2n}(x) = y$. Consider the following x, where x_i indicates a known coordinate $=a_i$, and a $*$ indicates that the corresponding coordinate is yet to be determined.

$$x = \cdots * * * x_{-nk+1} \cdots \overbrace{x_0}^{0^{th}} x_1 \cdots x_{nk} * * * \cdots.$$ Then

$$\sigma^k(x) = \cdots * * * x_{-nk+1} \cdots \overbrace{x_{nk}}^{((n-1)k)^{th}} * * * \cdots.$$

Since $2nk$ coordinates of x , from $-nk+1$ to nk are fixed, it follows that in $\sigma^k(x)+x$, the $2nk-k$ coordinates from $(-nk+1)$ to $(n-1)k$ are fixed. Call these fixed coordinates as $z_{-nk+1}, \cdots, z_{(n-1)k}$. We have to determine z which has to be as follows :

$$z = \cdots * * * z_{-nk+1} \cdots \overbrace{z_0}^{0^{th}} z_1 \cdots z_{(n-1)k} * * * \cdots.$$

Consider $z' = r'(z)$.

$$z' = \cdots * * * \overbrace{z_{(n-1)k}}^{(-(n-1)k+1)^{th}} \cdots \overbrace{z_1}^{0^{th}} z_0 \cdots \overbrace{z_{-nk+1}}^{nk^{th}} * * * \cdots.$$

$$\sigma^k(z') = \cdots * * * \overbrace{z_{(n-1)k}}^{(-nk+1)^{th}} \cdots z_1 z_0 \cdots \overbrace{z_{-nk+1}}^{(n-1)k^{th}} * * * \cdots.$$ Thus we are fixing coordinates from $(-(n-1)k+1)^{th}$ to $(n-1)k^{th}$, in $\sigma^k(z')+z'$, which we call as w. Consider $w' = r'(w)$, in which coordinates from $(-(n-1)k+1)^{th}$ to $(n-1)k^{th}$ are fixed. By induction hypothesis the remaining coordinates of w' can be uniquely determined so that $f^{2(n-1)}(w') = y$. Now w is uniquely determined, so that we can find z' uniquely such that $\sigma^k(z')+z' = w$, which implies $r'(\sigma^k(z')+z') = w'$, or $f(z') = w'$. Since z is uniquely determined, we can find remaining coordinates of x such that $\sigma^k(x)+x = z$, which gives $r'(\sigma^k(x)+x) = f(x) = r'(z) = z'$. Then $f^2(x) = f(z') = w'$, and $f^{2n}(x) = f^{2(n-1)}(f^2(x)) = f^{2(n-1)}(w') = y$.

□

Proposition 4.2.2. *The function $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by $f(x) = r'(\sigma^k(x)+x)$, where k is a positive integer, is transitive.*

Proof. Let U and V be any nonempty open sets in $A^{\mathbb{Z}}$. Fix some element y in V. Consider an ε ball contained in U, centered at some point z. We may assume that $\varepsilon = p^{-j}$ for some positive integer j. Choose n such that $nk > j+1$. There is an x such that $x_i = z_i$ for $i = -nk+1, \cdots, nk$, and $f^{2n}(x) = y$. $d(x,z) \leq p^{-nk+1} < p^{-j}$, and so $x \in U$. Therefore $f^{2n}(U) \bigcap V$ is non-empty. □

By a similar argument, we see that f^2 is strongly mixing. (See defintion (2.3.12)).

4.3 POSITIVE ENTROPY

We now prove that the topological entropy of f is positive.

Proposition 4.3.1. *The map* $f(x) = r'(\sigma^k(x) + x)$ *is an open map.*

Proof. We use the following notations :

$$B_d(x, p^{-j}) \text{ - the open ball of radius } p^{-j} \text{ centered at } x, \text{ for any positive integer } j. \quad (4.1)$$

$$B(x, n) \text{ - the open ball of radius } p^{-nk} \text{ centered at } x, \text{ for any positive integer } n. \quad (4.2)$$

$$U(x, n) \text{ - the set of all points } z \text{ with } z_i = x_i \text{ for } -nk + 1 \le i \le nk \text{ for any positive integer } n. \quad (4.3)$$

$$C(x, n, m) \text{ - the set of all points } z \text{ with } z_i = x_i \text{ for } -mk + 1 \le i \le nk \text{ for any positive integers } n, m. \quad (4.4)$$

Here sets of type (4.1) and (4.2) are clopen (both open and closed) balls. Those of type (4.3) and (4.4) are clopen cylinders by (Kůrka, 2009). We know that balls of type (4.1), and the set of all clopen cylinders form bases for the product topology on $A^{\mathbb{Z}}$.

We prove that balls of type (4.2) and cylinders of type(4.3) also form bases.

For any x, we have to express $B_d(x, p^{-j})$ as a union of balls of type (4.2).

Let $j = nk + l$, where $0 < l < k$. Let $S = \{y \in A^{\mathbb{Z}} \mid y_i = x_i$ for $-nk - l \le i \le nk + l$, and $y_i = 0$ for $i < -(n+1)k$ and $(n+1)k < i\}$. For $-(n+1)k \le i < -nk - l$ and $nk + l < i \le (n+1)k$, y_i can be anything. There are $p^{2(k-l)}$ such y. Then $B_d(x, p^{-j}) = \bigcup_{y \in S} B(y, n+1)$.

By a similar argument we can express every subset of type (4.2) as a union subsets of type (4.3). For any x, let $S_1 = \{y \in A^{\mathbb{Z}} \mid y_i = x_i$ for $-nk \le i \le nk$, and $y_i = 0$ for $i < -(n+1)k + 1$ and $i > (n+1)k\ \}$. For $-(n+1)k + 1 \le i < -nk$, and $nk < i \le (n+1)k$, y_i can be anything. Then $B(x, n) = \bigcup_{y \in S_1} U(y, n+1)$. Therefore subsets of type (4.3) also form a basis.

Now it is enough to show that $f(U(x, n))$ is open for all $x \in A^{\mathbb{Z}}$ and all $n > 1$. We prove that

$$f(U(x, n)) = C(f(x), n, n-1) \quad (4.5)$$

Let $z \in U(x, n)$. Then $z_i = x_i$ for $-nk + 1 \le i \le nk$, and $\sigma^k(z)_i = \sigma^k(x)_i$ for $-nk + 1 \le i \le (n-1)k$. It follows that

$(\sigma^k(z) + z)_i = (\sigma^k(x) + x)_i$ for $-nk + 1 \le i \le (n-1)k$, and so

$(r'(\sigma^k(z) + z))_i = (r'(\sigma^k(x) + x))_i$, i.e., $f(x)_i = f(z)_i$ for $-(n-1)k + 1 \le i \le nk$. Thus $f(U(x, n)) \subseteq C(f(x), n, n-1)$.

Now let $y \in C(f(x),n,n-1)$. There is a unique pre-image z for this y under f such that $z_i = x_i$ for $1 \leq i \leq k$. We prove that $z_i = x_i$ for $-nk+1 \leq i \leq nk$.
Suppose that $z_i \neq x_i$ for some i with $-nk+1 \leq i \leq nk$.
First let $z_i \neq x_i$ for some positive i, with $i \leq nk$, and choose the smallest such i. Then $k < i \leq nk$. Then $\sigma^k(z)_{i-k} \neq \sigma^k(x)_{i-k}$, and $(\sigma^k(z)+z)_{i-k} \neq (\sigma^k(x)+x)_{i-k}$, which implies $r'(\sigma^k(z)+z)_{-i+k+1} \neq r'(\sigma^k(x)+x)_{-i+k+1}$, i.e., $y_{-i+k+1} \neq f(x)_{-i+k+1}$. This is a contradiction because $-(n-1)k+1 \leq -i+k+1 \leq 0$.
Now suppose that $z_i = x_i$ for $0 < i \leq nk$. Then $z_i \neq x_i$ for some negative i, with $-nk+1 \leq i \leq 0$. Consider such i with minimum $|i|$.
Now $\sigma^k(z)_j = \sigma^k(x)_j$, for $i \leq j \leq 0$, but $z_i \neq x_i$. Therefore $(\sigma^k(z)+z))_i \neq (\sigma^k(x)+x))_i$, and so $r'(\sigma^k(z)+z))_{-i+1} \neq r'(\sigma^k(x)+x))_{-i+1}$, or $y_{-i+1} \neq f(x)_{-i+1}$, a contradiction because $0 < -i+1 \leq nk$. Thus $f(U(x,n)) \supseteq C(f(x),n,n-1)$.
As $C(f(x),n,n-1)$ is a clopen cylinder, f is an open map. □

Now we use a result from (Sakai, 2003) (p. 17, Theorem 1).

Theorem 4.3.2. *Let f be a positively expansive self map on a compact metrizable space. Then the following conditions are equivalent.*

(1) f is an open map.

(2) f has shadowing property .

It follows that the function $f(x) = r'(\sigma^k(x)+x)$ has shadowing property. Finally, we use a result from (Li and Oprocha, 2013) (p. 6, Theorem 3.3).

Theorem 4.3.3. *Let (X,f) be a non-wandering dynamical system with the shadowing property. Then either (X,f) is equicontinuous or it has positive entropy.*

Proposition 4.3.4. *The function $f(x) = r'(\sigma^k(x)+x)$ has positive entropy.*

Proof. $(A^{\mathbb{Z}}, f)$ is transitive implies that it is non-wandering. It is positively expansive and $A^{\mathbb{Z}}$ is perfect implies it is sensitive, and therefore cannot be equicontinuous. By Theorem 4.3.3, it has positive entropy. □

4.4 DENSITY OF PERIODIC POINTS

To see that periodic points are dense, we use the following result from (Aoki and Hiraide, 1994) (Theorem 3.4.2)

Theorem 4.4.1. *Let (X, f) be a compact dynamical system. If f is a positively expansive surjection having the pseudo-orbit tracing property, then the set of periodic points of f is dense in $\Omega(f)$, the set of non-wandering points of f.*

Proposition 4.4.2. *The function $f(x) = r'(\sigma^k(x) + x)$, on $A^{\mathbb{Z}}$ has a dense set of periodic points.*

Proof. Since $(A^{\mathbb{Z}}, f)$ is transitive, it is non-wandering, i.e., $\Omega(f) = A^{\mathbb{Z}}$. It has the shadowing property, and the compactness of $A^{\mathbb{Z}}$ implies it has pseudo-orbit tracing property. therefore the set of periodic points is dense in $A^{\mathbb{Z}}$. □

Thus, the system $(A^{\mathbb{Z}}, f)$ is Devaney chaotic.
There are various kinds of chaos, some of which are defined in Chapter 2. Among them we observe that positive entropy and Devaney chaos are quite strong, that is each of them implies many other types of chaos. Hence we can conclude that the function $f(x) = r'(\sigma^k(x) + x)$ is a good enough chaotic function.

We now find the fixed points of f.

Proposition 4.4.3. *For any elements $a_1, a_2, \cdots, a_k$ of A, there is a fixed point x of the function $f(x) = r'(\sigma^k(x) + x)$ with $x_i = a_i$ for $i = 1, 2 \cdots, k$.*

Proof. Consider the following x, where $x_i = a_i$, for $i = 1, 2 \cdots, k$, and *s indicate that the corresponding coordinates are yet to be determined.

$$x = \cdots * * * \overbrace{x_1}^{1^{st}} x_2 \cdots x_k * * * \cdots.$$ Then

$$\sigma^k(x) = \cdots * * * x_1\, x_2 \cdots \overbrace{x_k}^{0^{th}} * * * \cdots.$$

We have to determine the remaining coordinates of x such that

$$\sigma^k(x) + x = * * * \cdots x_k x_{k-1} \cdots x_2 \overbrace{x_1}^{0^{th}} * * * \cdots.$$

Find x_0 such that $x_0 + x_k \equiv x_1 \ mod\ p$, and let c_0 be the carry. Next find x_{-1} such that $x_{-1} + +x_{k-1} + c_0 \equiv \ x_2 \ mod\ p$, and let c_{-1} be the carry. Proceed similarly to find all coordinates on the left side.
For the right side, first find x_{k+1} such that $x_1 + x_{k+1} \equiv \ x_0 \ mod\ p$, and let c_1 be the carry. Then find x_{k+2} such that $x_2 + x_{k+2} \equiv \ x_{-1} \ mod\ p$, and let c_2 be the carry. Proceed similarly to find all coordinates on the right side of 0^{th} position. Now $\sigma^k(x) + x = r'(x)$ or $f(x) = x$. □

Thus there are p^k fixed points. We can also construct points of period 2.

Proposition 4.4.4. *For any elements $a_{-k+1}, a_{-k+2} \cdots a_1, a_2, \cdots, a_k$ of A, there is a periodic point x of the function $f(x) = r'(\sigma^k(x) + x)$ of period 2, with $x_i = a_i$ for $i = -k+1, -k+2, \cdots, 1, 2 \cdots, k$.*

Proof. Consider the following x, where $x_i = a_i$, for $i = -k+1, -k+2, \cdots, 1, 2 \cdots, k$, and *s indicate that the corresponding coordinates are yet to be determined.

$$x = \qquad \cdots * * * x_{-k+1}\, x_{k+2} \cdots x_0 \overbrace{x_1}^{1^{st}} x_1\, x_2 \cdots x_k * * * \cdots . \tag{4.6}$$

Then

$$\sigma^k(x) = \cdots * * * x_{-k+1}\, x_{-k+2} \cdots x_1\, x_2 \cdots \overbrace{x_k}^{0^{th}} * * * \cdots . \tag{4.7}$$

Then $z = \sigma^k(x) + x$ is as follows, where $z_{-k+1}, z_{-k+2}, \cdots, z_0$ are the known coordinates and the *s indicate that the corresponding coordinates are yet to be determined.

$$z = \qquad \cdots * * * z_{-k+1}\, z_{-k+2} \cdots \overbrace{z_0}^{0^{th}} * * * \cdots . \tag{4.8}$$

So, $z' = r'(z)$ will look like

$$z' = \qquad \cdots * * * \overbrace{z_0}^{1^{st}} z_{-1} \cdots z_{-k+1} * * * \cdots . \tag{4.9}$$

Or

$$z' = \qquad \cdots * * * \overbrace{z'_1}^{1^{st}} z'_2 \cdots z'_k * * * \cdots . \tag{4.10}$$

$$\sigma^k(z') = \qquad \cdots * * * * z'_1\, z'_2 \cdots z'_k \overbrace{*}^{1^{st}} * * * \cdots . \tag{4.11}$$

We have to find z and x such that $\sigma^k(z') + z' = x' = r'(x)$.
First find z'_{k+1} i.e., z_{-k} such that $z'_{k+1} + z'_1 \equiv x'_1 = x_0$ *mod* p , and let c_1 be the carry. Subsitute this value of z_{-k} in (4.8), so that x_{-k} is uniquely determined by (4.7) +(4.6) = (4.8).
Now find z'_0, i.e., z_1 such that $z'_0 + z'_k \equiv x'_0 = x_{-1}$ *mod* p, and let c_0 be the carry. Substitute this z_1 in (4.8), to determine x_{k+1} uniquely by (4.7) +(4.6) = (4.8).

Next find z'_{k+2}, i.e., z_{-k-1} such that $z'_{k+2}+z'_2+c_1 \equiv x'_2 x_{-1}\ mod\ p$, and let c_2 be the carry. Proceed similarly on both sides. Now we have got $\sigma^k(x)+x=z$. So $r'(\sigma^k(x)+x)=z'$, i.e., $f(x)=z'$, and $\sigma^k(z')+z'=x'$, or $r'(\sigma^k(z')+z')=x$, which means $f(z')=x$, $f^2(x)=f(f(x))=f(z')=x$. □

We cannot generalize this by imitating the proof of (4.2.1), and using induction, to get periodic points of period $2n$. We can start with x, whose central $2nk$ coordinates are given. We can get $-(n-1)k+1^{th}$ to $(n-1)k^{th}$ coordinates of w. But in place of a fully known y, we have x, whose $2nk$ coordinates only are known. The remaining coordinates of x and w are to be determined simultaneously such that $f^{2(n-1)}(w')=x$ and $f^2(x)=w'$, for which we cannot use induction directly.

Example (1)

Let $p=5$, $k=3$ and $n=1$. Let w be the word 0 1 2 3 4. Let $y=\bar{w}$. That is,

$y =$ $\cdots$0 1 2 3 4 0 1 2 3 4 . 0 1 2 3 4 0 1 2 3 4 $\cdots$.

We put a dot after the zeroth coordinate to identify that position.

Suppose that $2nk=6$ coordinates of x, from x_{-2} to x_3 are given. Say, $x_i=1$ for $i=-2,-1,0,1,2,3$.

i.e., $x =$ $\cdots$ ∗ ∗ ∗ 1 1 1 . 1 1 1 ∗ ∗ ∗ $\cdots$.

We have to determine the remaining coordinates of x such that $f^2(x)=y$.

$x =$ $\cdots$ ∗ ∗ ∗ 1 1 1 . 1 1 1 ∗ ∗ ∗ $\cdots$

$\sigma^3(x) =$ $\cdots$ ∗ ∗ ∗ 1 1 1 1 1 1 . ∗ ∗ ∗ $\cdots$

Adding, $\cdots$ ∗ ∗ ∗ 2 2 2 . ∗ ∗ ∗ $\cdots$

Now $r'(\sigma^3(x)+x)=z$, say, is $\cdots$ ∗ ∗ ∗ ∗ ∗ ∗ . 2 2 2 ∗ ∗ ∗ $\cdots$

$\sigma^3(z) =$ $\cdots$ ∗ ∗ ∗ ∗ ∗ ∗ 2 2 2 . ∗ ∗ ∗ $\cdots$

Adding, we get $r'(y)$ $\cdots$ 4 3 2 1 0 4 3 2 1 0 . 4 3 2 1 0 4 3 2 1 0 $\cdots$

Comparing coordinates, we find z_0, z_{-1} and z_{-2} in that order.

$z_0+2 \equiv 0 \mod 5$ gives $z_0=3$ and $c_0=1$.

$z_{-1}+2+1 \equiv 1 \mod 5$ gives $z_{-1}=3$ and $c_{-1}=1$.

$z_{-2}+2+1 \equiv 2 \mod 5$ gives $z_{-2}=4$ and $c_{-2}=1$. This gives

$z =$ $\cdots$ ∗ ∗ ∗ ∗ ∗ 4 3 3 . 2 2 2 2 ∗ ∗ $\cdots$

$\sigma^3(z) =$ $\cdots$ ∗ ∗ ∗ ∗ 4 3 3 2 2 2 . 2 1 ∗ $\cdots$

$r'(y) =$ $\cdots$ 4 3 2 1 0 4 3 2 1 0 . 4 3 2 1 0 4 3 2 1 0 $\cdots$

Next find z_{-3}, z_{-4} and z_5.

$z_{-3}+3+1 \equiv 3 \mod 5$ gives $z_{-3}=4$, and $c_{-3}=1$.

$z_{-4}+3+1 \equiv 4 \mod 5$ gives $z_{-4}=0$, and $c_{-4}=0$.

$z_{-5}+4+1 \equiv 0 \mod 5$ gives $z_{-5}=1$, and $c_{-5}=1$. This gives

$z =$ $\cdots * * * * 1\ 0\ 4\ 4\ 3\ 3\ .\ 2\ 2\ 2\ * * * \cdots$

$\sigma^3(z) =$ $\cdots * * * 1\ 0\ 4\ 4\ 3\ 3\ 2\ 2\ 2\ .\ * * * \cdots$

$r'(y) =$ $\cdots 4\ 3\ 2\ 1\ 0\ 4\ 3\ 2\ 1\ 0\ .\ 4\ 3\ 2\ 1\ 0\ 4\ 3\ 2\ 1\ 0 \cdots$

Continuing similarly at the right side we get z_4, z_5, z_6, z_7 etc. in that order. So

$z = \cdots * * * * 1\ 1\ 1\ 0\ 4\ 4 3\ 3\ .\ 2\ 2\ 2\ 2\ 1\ 0\ 4\ 3\ 3\ 4\ 3\ 2\ * * * \cdots$ Substituting this z in the equation $\sigma^3(x)+x = r'(z)$, we get

$x =$ $\cdots * * * 1\ 1\ 1\ .\ 1\ 1\ 1 * * * \cdots$

$\sigma^3(x) =$ $\cdots * * * 1\ 1\ 1\ 1\ 1\ 1\ .\ * * * \cdots$

$r'(z) =$ $\cdots * * *\ 2\ 3\ 4\ 3\ 3\ 4\ 0\ 1\ 2\ 2\ 2\ 2\ .\ 3\ 3\ 4\ 4\ 0\ 1\ 1\ 1\ * * * \cdots$

By a similar argument, we find $x_{-3}, x_{-4}, x_{-5}, x_{-6}$, etc. in that order on the left side , and x_4, x_5, x_6, x_7, etc. in that order on the right side. We get

$x = \cdots * * *\ 3\ 0\ 1\ 4\ 3\ 2\ 4\ 0\ 1\ 1\ 1\ 1\ .\ 1\ 1\ 1\ 2\ 2\ 3\ 2\ 3\ 2\ 3\ 2 * * * \cdots.$

For this x, $f^2(x) = y$.

Example (2)

Let $p = 5$ and $k = 3$. We find a periodic point x with period 2, of the form

$x =$ $\cdots * * * 1\ 1\ 1\ .\ 2\ 2\ 2\ * * * \cdots$

$\sigma^3(x) =$ $\cdots * * * 1\ 1\ 1\ 2\ 2\ 2\ .\ * * * \cdots$

--- Adding, we get

$\cdots * * *\ 3\ 3\ 3\ .\ * * * \cdots.$

Let $r'(\sigma^3(x)+x) = z$. Then

$z =$ $\cdots * * * .\ 3\ 3\ 3 * * * \cdots$

$\sigma^3(z) =$ $\cdots * * *\ 3\ 3\ 3\ .\ * * * \cdots$

--- Adding, we have to get

$r'(x) =$ $\cdots * * * 2\ 2\ 2\ .\ 1\ 1\ 1\ * * * \cdots$

At the left side, we calculate z_0, z_{-1} and z_{-2} in that order.

$z_0+3 \equiv 2 \mod 5$, which gives $z_0 = 4$ and the carry $c_0 = 1$.

$z_{-1}+3+1 \equiv 2 \mod 5$, which gives $z_{-1} = 3$ and the carry $c_{-1} = 1$.

$z_{-2}+3+1 \equiv 2 \mod 5$, which gives $z_{-2} = 3$ and the carry $c_{-2} = 1$. Substituting these values,

$x =$ $\cdots * * * 1\ 1\ 1\ .\ 2\ 2\ 2\ * * * \cdots$

$\sigma^3(x) =$ $\cdots * * * 1\ 1\ 1\ 2\ 2\ 2\ .\ * * * \cdots$

--- Adding, we get

$r'(z) = \qquad \cdots * * * 3\ 3\ 3 . 4\ 3\ 3\ * * * \cdots.$

Now we can find x_4, x_5 and x_6 in that order.

$2 + x_4 \equiv 4 \mod 5$, so $x_4 = 2$ and the carry $c'_4 = 0$.

$2 + x_5 + 0 \equiv 3 \mod 5$, so $x_5 = 1$ and the carry $c'_5 = 0$.

$2 + x_6 + 0 \equiv 3 \mod 5$, so $x_6 = 1$ and the carry $c'_6 = 0$.

Now the situation is

$z = \qquad \cdots * * * 3\ 3\ 4 . 3\ 3\ 3 * * * \cdots$

$\sigma^3(z) = \qquad \cdots * * * 3\ 3\ 4\ 3\ 3\ 3 . * * * \cdots$

$r'(x) = \qquad \cdots * * * 1\ 1\ 2\ 2\ 2\ 2 . 1\ 1\ 1\ * * * \cdots$

Next calculate z_{-3}, z_{-4} and z_{-5}.

$z_{-3} + 4 + 1 \equiv 2 \mod 5$, which gives $z_{-3} = 2$, $c_{-3} = 1$.

$z_{-4} + 3 + 1 \equiv 1 \mod 5$, which gives $z_{-4} = 2$, $c_{-4} = 1$.

$z_{-5} + 3 + 1 \equiv 1 \mod 5$, which gives $z_{-5} = 2$, $c_{-5} = 1$. Substituting these values,

$x = \qquad \cdots * * * 1\ 1\ 1 . 2\ 2\ 2\ 2\ 1\ 1 * * * \cdots$

$\sigma^3(x) = \qquad \cdots * * * 1\ 1\ 1\ 2\ 2\ 2 . 2\ 1\ 1 * * * \cdots$

--- Adding, we get

$r'(z) = \qquad \cdots * * * 3\ 3\ 3 . 4\ 3\ 3\ 2\ 2\ 2 * * * \cdots.$

At this stage we can find x_7, x_8 and x_9. Proceeding similarly, we can find all coordinates of x on the right side of the dot. The same procedure is repeated with the right side to get x_0, x_{-1}, etc.

Remarks

- The basic map used here is the shift map. But just the shift map is not of much use in data hiding, as it does not alter any coordinate, but only shifts coordinates to one side, so it is used in combination with addition with a carry.
- Most of the basic dynamical properties of the shift map, like positive entropy and Devaney chaos are not changed after combining with the addition map. It is natural to guess that the behaviour of f^n should be similar whether n is even or odd. In particular, the result in 4.2.1, which could be proved only for even integers, may actually be true for all integers.

Chapter 5

A NOTE ON POSITIVELY EXPANSIVE MAPS ON NON-COMPACT SPACES

Expansive homeomorphisms and positively expansive maps occur frequently in dynamical systems. Consider the following commonly used definition :

Definition 5.0.1. *A dynamical system* (X, f) *is positively expansive if* $\exists\ \varepsilon > 0,\ \forall\ x \neq y \in X,\ \exists\ n \geq 0$ *such that* $d(f^n(x), f^n(y)) \geq \varepsilon$*.*

This concept is used usually with compact spaces ((Kůrka, 2003), (Bahi and Guyeux, 2013), (Sakai, 2003), (Sakai, 1985), (Reddy, 1982) and (Fujita et al., 2010)), and sometimes with non-compact spaces also. This property, sometimes along with some other properties like shadowing property, is used to determine other dynamical properties like topological entropy and set of periodic points ((Li and Oprocha, 2013), (Aoki and Hiraide, 1994), (Fujita et al., 2008)).
The above n cannot be zero for all x and y in X, with $x \neq y$, unless the topology is discrete, and is not of any interest. Therefore at least for some x and y, n should be greater than zero.
The question is whether we can find such n greater than zero for all x and y in X with $x \neq y$, or is a positively expansive map injective?
At least in the case of a compact metric space X it is well known that existence of a positively expansive homeomorphism from X onto X implies X is finite. In fact in (Coven et al., 2006), without assuming that $f : X \to X$ is onto, it is proved that, if X is compact and infinite, f can not be positively expansive and injective.
It is not true in the case of non-compact spaces. There, positively expansive maps can be,

but need not be, injective. Further we can prove that when not injective, it is possible for all points in the image to have any prescribed number of pre-images.

5.1 AN EXAMPLE IN THE NON-COMPACT CASE

When X is compact, some authors define (X, f) to be positively expansive if the condition in the above definition holds for some equivalent metric (Reddy, 1982). There any equivalent metric is also totally bounded (i.e., for every $\varepsilon > 0$, X can be covered by finitely many ε-balls). But a non-compact space, which is totally bounded in some metric may be unbounded in another equivalent metric.

For example, in the complex plane $\mathbb{C}$, consider the annulus $X = \{z \in \mathbb{C} \mid |z| > 1\}$ on the complex plane and the map $f(z) = z^n$. It multiplies angles by n and also increases the modulus, and so is positively expansive, and every element has exactly n pre-images.

To verify that it is positively expansive, first consider the map $f(z) = z^2$ on the anulus $X = \{z \in \mathbb{C} \mid |z| > 1\}$ of the complex plane. This map doubles angles on the unit circle. On the outer side of the unit circle, it not only doubles angles but increases the modulus also. It is clearly not injective because $z^2 = (-z)^2$.

It is positively expansive, with expansive constant 1. Consider two distinct elements $x = r_1 e^{i\theta_1}$ and $y = r_2 e^{i\theta_2}$. If $r_1 \neq r_2$, then

$$
\begin{aligned}
d(f^n(x), f^n(y)) &\geq |r_1^{2^n} - r_2^{2^n}| \\
&= |(r_1^{2^{n-1}})^2 - (r_2^{2^{n-1}})^2| \\
&= |r_1^{2^{n-1}} + r_2^{2^{n-1}}||r_1^{2^{n-1}} - r_2^{2^{n-1}}| \\
&\geq |r_1^{2^{n-1}} + r_2^{2^{n-1}}||r_1 - r_2|
\end{aligned}
$$

which is greater than 1 for sufficiently large n.

If $r_1 = r_2 = r$, then $\theta_1 \neq \theta_2$. We may assume $|\theta_1 - \theta_2| \leq \pi$. Distance between x and y is $2r\ sin(\frac{|\theta_1 - \theta_2|}{2})$. If $|\theta_1 - \theta_2| \geq \frac{\pi}{2}$, then $\frac{\pi}{4} \leq \frac{|\theta_1 - \theta_2|}{2} \leq \frac{\pi}{2}$ and we have $2r\ sin(\frac{|\theta_1 - \theta_2|}{2}) \geq 2r\frac{1}{\sqrt{2}} > 1$, and we may take $n = 0$.

If $|\theta_1 - \theta_2| < \frac{\pi}{2}$, apply f once, to get $f(x) = r^2 e^{2i\theta_1}$ and $f(y) = r^2 e^{2i\theta_2}$. If $2|\theta_1 - \theta_2| \geq \frac{\pi}{2}$, take $n = 1$. If not, apply f once more. By repeating this sufficiently many times, for some n we get $d(f^n(x), f^n(y)) = 2r^{2^n}\ sin(2^n\frac{|\theta_1 - \theta_2|}{2}) \geq 2r^{2^n}\frac{1}{\sqrt{2}} > 1$.

A similar argument can be applied to the function $f(x) = x^n$, to get n inverse images for any element of the annulus.

The annulus can be made totally bounded easily. Partition it into the annuli A_j, where $A_j = \{z \in \mathbb{C} \mid j < |z| \leq j+1\}$, for $j \geq 1$. $X = \bigcup_{j \geq 1} A_j$. Each A_j can be "shrunk" so that

difference between the outer and inner radius is $\frac{1}{2^j}$, instead of 1. Thus X becomes a disc Y of radius $\sum_{j=0}^{\infty}\frac{1}{2^j} < 2$ in $\mathbb{R}^2$ (or $\mathbb{C}$), and so is totally bounded. Let h be the homeomorphism that does this shrinking of X to the bounded annulus Y. Now, consider the conjugate $g = hfh^{-1}$ of f. For two points x and y of Y, with same argument, $d(g^n(x), g^n(y))$ tends to zero as n tends to infinity, and so g is not positively expansive.
But if we take the equivalent metric d' in Y, given by $d'(x,y) = d(h^{-1}(x), h^{-1}(y))$, then in this metric the map g on Y is positively expansive. So a map that does not actually increase distances, may do so if the metric is changed. In the case of unbounded spaces, it is easy to define positively expansive maps. For isolated points, any map is continuous and it is simple to define maps with required properties. Therefore interesting cases are only when X is totally bounded, and perfect (i.e., every point of X is a limit point).
Hence we consider only the case when X is totally bounded and perfect.
Consider the totally disconnected symbolic space $A^{\mathbb{N}}$ where $A = \{0, 1, 2, \ \cdots p-1\}$ for some positive integer p. If A is given discrete topology, $A^{\mathbb{N}}$ (where $\mathbb{N} = 0, 1, 2\cdots$), in the product topology is a totally disconnected, compact, perfect metric space (Kůrka, 2003). The distance between two points $x = x_0x_1x_2\cdots$ and $y = y_0y_1y_2\cdots$ may be defined by $d(x,y) = 2^{-j}$ where $j = min\{i|x_i \neq y_i\}$.

Consider the one sided full shift σ given by $(\sigma(x))_i = x_{i+1}$. It is a well known positively expansive map. Consider a point $x = x_0x_1\ x_2\ \cdots$, with a dense (forward) orbit, W. Then $W = \{x, \sigma(x), \sigma^2(x), \cdots\}$. For example, x can be taken as the Champernowne sequence, which is obtained by the concatenation of all words of length n, with letters in A, for all positive integers n (Kůrka, 2003). For example, for $p = 2$, x can be 0 1 00 01 10 11 000 001 010 100 011 101 110 111 $\cdots$. Assume that all length-n words appear before length-$(n+1)$ words, for $n > 0$. So, W consists of the elements

$x_0x_1x_2\cdots$

$x_1x_2x_3\cdots$

$x_2x_3x_4\cdots$

$\cdots$.

These elements are distinct, otherwise it follows that there are m and k, with $m > k \geq 0$ such that $x_{k+i} = x_{m+i}$ for all $i \geq 0$, and so x is eventually periodic under σ, which is not true.
Let $Y = \sigma^{-1}(W)$. Then $\sigma(Y) = W$. Both W and Y are non-compact, because they are proper dense subsets of of the compact space $A^{\mathbb{N}}$. They are totally bounded because $A^{\mathbb{N}}$ is. We verify that W has no isolated points. Let $w = x_kx_{k+1}\cdots$ be any point in W. In every open ball of radius 2^{-j} around w, we have to find a point of W, different from w. There is an n such that all words of length $n-1$ appear before x_k in x, and at least a part of a

length-n word appears after x_{k-1}. It is enough to consider 2^{-j} neighborhoods of w, where $j > n$. The word $x_k x_{k+1} \cdots x_{k+j}$, of length $j+1$ appears somewhere later in the orbit of x, i.e., there is $m > k$ such that $x_k x_{k+1} \cdots x_{k+j} = x_m x_{m+1} \cdots x_{m+j}$ for some $m > k$.
To verify that Y is perfect, we use a similar argument. Any element y of Y is of the form $a x_k x_{k+1} \cdots$, for some $a \in A$. For $\sigma(y) = x_k x_{k+1} \cdots \in W$, choose j and find $m > k$ as above. Then $y = a x_k x_{k+1} \cdots \neq a x_m x_{m+1} \cdots$, but $a x_m x_{m+1} \cdots$ belongs to the 2^{-j} -neighborhood of y. Thus Y is also prefect.
Now, $\sigma|_W$ is injective, $\sigma|_Y$ is not injective, and every element in the image has exactly p pre-images.
Here $\sigma|_W$ is not onto because the first element x, is not the image under σ for any element of W. So we may take W' to be a bi-infinite orbit of x, by including a backward orbit, say,
$0x_0x_1x_2\cdots$
$00x_0x_1x_2\cdots$
$000x_0x_1x_2\cdots$
$\cdots$.
Any two of these elements are also distinct.
So W' is
$\cdots$
$x_2x_3\cdots$
$x_1x_2\cdots$
$x_0x_1\cdots$
$0x_0x_1x_2\cdots$
$00x_0x_1x_2\cdots$
$000x_0x_1x_2\cdots$
$\cdots$.
Take $Y' = \sigma^{-1}(W')$. Both Y' and W' are perfect. $\sigma(Y') = \sigma(W') = W'$. Every element in W' has exactly one pre-image in W' and exactly p pre-images in Y'. Since σ is an open map, $\sigma|_{W'}$ is a homeomorphism.
These two examples are are just orbits of a single element. We can also have another pair of examples, which are also countable, but are not orbits of a single element.

Proposition 5.1.1. *The function $f: A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by $f(x) = r(\sigma^k(x) + x)$, where k is a positive integer, is continuous, positively expansive and surjective. Each element in $A^{\mathbb{Z}}$ has exactly p^k pre-images under f.*

Proof. We have already verified in (3.4) that the function is positively expansive. From the proof of (4.2.1) it follows that each y has exactly p^k pre-images under f. □

Now consider two subspaces of $X = A^{\mathbb{Z}}$, invariant under f given by

$$Y = \{y \in X | f(y) \text{ has only finitely many non–zero coordinates}\} \tag{5.1}$$

and

$$W = \{w \in X | w \text{ has only finitely many non–zero coordinates}\} \tag{5.2}$$

Clearly $f(W) \subseteq f(Y) \subseteq W \subseteq Y$. We prove that W and Y are not compact. Take an element $x = \cdots x_{-2}\, x_{-1} \overbrace{x_0}^{0^{th}} x_1\, x_2 \cdots$ in X, not in Y. Consider the sequence $\{a_n\}$ in W given by $a_n = \cdots 0\,0\,0\, x_{-n} x_{-n+1} \cdots x_{n-1}\, x_n\, 0\,0\,0 \cdots$. Each a_n is in W and so is in Y. The sequence $\{a_n\}$ converges to x. But $x \notin Y$ and hence $x \notin W$. It follows that W and Y are not comapct. We prove that $f|_Y$ is is not injective, but $f|_W$ is injective.

From Proposition 5.1.1, it follows that every element of $f(Y)$ has p^k pre-images under f in Y. Thus $f|_Y$ is not one-to-one.

For every element of W, we prove that it has atmost one pre-image in W. Recall $f(x) = r(\sigma^k(x) + x)$. Note that r is a homeomorphism. Hence it is enough to prove that for each w in W, there is atmost one x in W such that $\sigma^k(x) + x = w$.

Let

$$x = \quad \cdots 0\,0\,0\, x_{-j}\, x_{-j+1} \cdots\ x_{-1} \overbrace{x_0}^{0^{th}} x_1\, x_2\, \cdots x_m\, 0\,0\,0 \cdots\ \in W.$$

Then

$$\sigma^k(x) = \cdots 000\ \overbrace{x_{-j}}^{(-j-k)^{th}}\ x_{-j+1} \cdots x_0 \cdots\ \overbrace{x_k}^{0^{th}}\ x_{k+1}\, x_{k+2}\, \cdots x_m\, 0\,0\,0 \cdots.$$

Consider first the addition of the left part. Let a be the p-adic integer represented by $x_{-j} x_{-j+1} \cdots x_0$, i.e.,

$$x_0 + p x_{-1} + \cdots p^j x_{-j} = a \tag{5.3}$$

and b be the p-adic integer represented by $x_1 x_2 \cdots x_k$, i.e.,

$$x_k + p x_{k-1} \cdots p^{k-1} x_1 = b \tag{5.4}$$

Then the integer represented by $x_{-j} x_{-j+1} \cdots x_0 \cdots\ x_k$ is $ap^k + b$, i.e

$$x_k + p x_{k-1} \cdots p^{k-1} x_1 + p^k x_0 + p^{k+1} x_{-1} + \cdots + p^{j+k} x_{-j} = ap^k + b \tag{5.5}$$

Addition on the left side i.e., (5.3) + (5.5) gives $a + ap^k + b$.

The question is if $a + ap^k + b = a' + a' p^k + b'$ for some other such non-negative integers a' and b', then can we say $a = a'$ and $b = b'$?

The answer is yes, because $(1 + p^k)(a - a') = b' - b$ and $|b - b'| \leq p^k$. If $a - a' \neq 0$, then

$|(1+p^k)(a-a')| > p^k$. So $a=a'$ and $b=b'$. For the right side, once $x_1, x_2 \cdots, x_k$ are fixed, the remaining coordinates are also fixed. Hence $f|_W$ is injective.
Here we note that if $p=n$ is any number, not necessarily a prime, and if $k=1$, $f|_Y$ is not injective and any element of $f(Y)$ has n pre-images.

Chapter 6

CONCLUSION

The above arguments and discussions given in Chapter 3 and Chapter 4 carry through, if we replace the addition with a carry by addition without the carry. (In that case f^2 is a cellular automaton.)

The metric used here recognises only the coordinates for which the "first difference" appears. We may redefine the metric, for example, as

$$d(x,y) = \sum_{i, x_i \neq y_i} \frac{1}{p^{-|i|}} \tag{6.1}$$

This will take into consideration all coordinates where x and y differ. But it will not help much in distinguishing between the entropies of the function f that uses addition with a carry, and the corresponding function that uses addition without a carry.

Though all the differences in behaviour of the two functions cannot be measured mathematically, by intution we see that addtion with a carry should give more unpredictability.

Following are some points to be considered for future work.

- In Chapter 4, though we proved that periodic points are dense, we did not actually find the periodic points. Possible future work can be done to find some periodic points.

- To verify whether any of the functios in Chapter 3 are Devaney-chaotic.

- To study the behaviour of positively expansive maps on non-compact manifolds with boundary.

Bibliography

Adler, R. L., Konheim, A. G., and McAndrew, M. H. (1965). "Topological entropy." *Transactions of the American Mathematical Society*, 309–319.

Akin, E., Auslander, J., and Berg, K. (1996). "When is a transitive map chaotic." *Convergence in Ergodic Theory and Probability, Walter de Gruyter & Co*, 25–40.

Akin, E., Glasner, E., Huang, W., Shao, S., and Ye, X. (2010). "Sufficient conditions under which a transitive system is chaotic." *Ergodic Theory and Dynamical Systems*, 30(05), 1277–1310.

Aoki, N. and Hiraide, K. (1994). *Topological theory of dynamical systems: recent advances*, 52, Elsevier.

Bahi, J. M. and Guyeux, C. (2013). *Discrete dynamical systems and chaotic machines: theory and applications*. CRC Press.

Balibrea, F. et al. (2003). "Topological entropy of devaney chaotic maps." *Topology and its Applications*, 133(3), 225–239.

Bowen, R. (1971). "Entropy for group endomorphisms and homogeneous spaces." *Transactions of the American Mathematical Society*, 153, 401–414.

Bryk, J. and Silva, C. E. (2005). "Measurable dynamics of simple p-adic polynomials." *American Mathematical Monthly*, 212–232.

Coven, E. M., Keane, M., et al. (2006). "Every compact metric space that supports a positively expansive homeomorphism is finite." *Dynamics & stochastics*, 304–305.

Dennunzio, A., Formenti, E., and Provillard, J. (2012). "Non-uniform cellular automata: classes, dynamics, and decidability." *Information and Computation*, 215, 32–46.

Devaney, R. L., Devaney, L., and Devaney, L. (1989). *An introduction to chaotic dynamical systems*, 13046, Addison-Wesley Reading.

Grosse-Erdmann, K. G., and Manguillot, A. P. (2011). *Linear chaos*, Springer Science & Business Media.

Fujita, C., Kato, H., and Matsumoto, M. (2008). "Expanding ratios, box counting dimension and hausdorff dimension." *Mathematical Analysis Laboratory Proceedings*, 1578, 28–35.

Fujita, C., Kato, H., and Matsumoto, M. (2010). "Fractal metrics of ruelle expanding maps and expanding ratios." *Topology and its Applications*, 157(3), 615–628.

Furstenberg, H. (1967). "Disjointness in ergodic theory, minimal sets, and a problem in diophantine approximation." *Theory of Computing Systems*, 1(1), 1–49.

Guckenheimer, J. (1979). "Sensitive dependence to initial conditions for one dimensional maps." *Communications in Mathematical Physics*, 70(2), 133–160.

Hedlund, G. A. (1969). "Endomorphisms and automorphisms of the shift dynamical system." *Theory of computing systems*, 3(4), 320–375.

Katok, S. (2007). *p-adic Analysis Compared with Real*, 37, AMS Bookstore.

Kůrka, P. (2003). *Topological and symbolic dynamics*, 11, SMF.

Kůrka, P. (2009). "Topological dynamics of cellular automata." *Encyclopedia of Complexity and Systems Science*, 9246–9268.

Li, J. and Oprocha, P. (2013). "Shadowing property, weak mixing and regular recurrence." *Journal of Dynamics and Differential Equations*, 25(4), 1233–1249.

Li, J. and Ye, X. D. (2015). "Recent development of chaos theory in topological dynamics." *Acta Mathematica Sinica, English Series*, 1–32.

Li, T.-Y. and Yorke, J. A. (1975). Period three implies chaos. *American mathematical monthly*, 985–992.

Reddy, W. L. (1982). "Expanding maps on compact metric spaces." *Topology and its Applications*, 13(3), 327–334.

Sakai, K. (1985). "Periodic points of positively expansive maps." *Proceedings of the American Mathematical Society*, 94(3), 531–534.

Sakai, K. (2003). "Various shadowing properties for positively expansive maps." *Topology and its Applications*, 131(1), 15–31.

Vries, J. (2014). *Topological Dynamical Systems: An Introduction to the Dynamics of Continuous Mappings*, 59, Walter De Gruyter.

Woodcock, C. F. and Smart, N. P. (1998). “p-adic chaos and random number generation.” *Experimental Mathematics*, 7(4), 333–342.

Young, L.-S. (2003). “Entropy in dynamical systems.” *Entropy*, Princeton University Press Princeton, NJ., 313–327.

LIST OF PUBLICATIONS/COMMUNICATIONS BASED ON THE THESIS:

- Chetana U V and B R Shankar, A note on positively expansive maps on non-compact spaces, *Asian Journal of Mathematics and Computer Research*, Vol.11, No.1 (2016), 57-60.
- Chetana U V and B R Shankar, Chaotic dynamical systems on symbolic spaces, *Journal of Dynamical Systems and geometric Theories* (Communicated).
- Chetana U V and B R Shankar, A Devaney-chaotic map with positive entropy on a symbolic space, *Bulletin of the Venezuelan Mathematical Association* (Communicated).

PAPERS PRESENTED AT INTERNATIONAL CONFERENCES

- Chetana U V and B R Shankar, Chaotic Dynamical Systems from extension of p-adic numbers, 23^{rd} *International Conference of Forum for Interdisciplinary Mathematics, NITK Surathkal, December 18 - 20, 2014.*
- Chetana U V and B R Shankar, A Devaney-chaotic map with positive entropy on a symbolic space using addition with a carry, *International Conference in Engineering and material Science, March 17-19, 2016, Jaipur National University, Jaipur.*

BIODATA

Name	:	Chetana U V
Email	:	chetanauv@gmail.com
Date of Birth	:	20 April 1958.
Permanent address	:	Chetana U V, Door No. 10-94/6, “Makaranda“, Nalyapadavu, Shaktinagar, Mangalore-575 016

Educational Qualifications :

Degree	**Year**	**Institution / University**
B.Sc. Physics, Chemistry, Mathematics	1978	St. Agnes College, Mangalore.
M.Sc. Mathematics	1982	Mangalore University, Mangalore.

Work Experience

- Temp. Lecturer in Mathematics, Mangalore University - from Sept 1985 to June 1988.
- Asst. Lecturer in Mathematics, at KREC Suarthkal, from July 1988 to Dec 1990.
- Junior Technical Asst., Dept of FPDE, CFTRI, Mysore, from Dec 1990 to July 1994.
- Lecturer in Mathematics, University College, Mangalore from July 1994 to July 2008.
- Associate Professor in Mathematics, University College, Mangalore, from July 2008 todate.