Non-Archimedean Dynamics: Ergodic Transformations in the Space of p-Adic Integers

Livat Tyapaev

Chernyshevsky Saratov State University

Saratov, July 2nd-3rd, 2018

СГУ

Motivation

We study measure-preserving (in particular, ergodic) transformations of the space of p-adic integers; within this context the talk is a contribution to the theory of non-Archimedean dynamical systems. The latter are of growing interest now because of their possible applications in different areas: For instance, applications of the p-adic dynamics to physics, cognitive sciences, and neural networks. Recently ergodic transformations of the space of 2-adic integers were successfully applied to pseudorandom number generation for computer simulations and especially for cryptography (stream cipher design, homomorphic encryption).

Outline

1. Reminders and Preliminaries
   - Space of words
   - Space of p-adic numbers
2. Automata functions
   - Compatible functions
   - Locally compatible functions
3. Dynamics
   - Measure-preservation and ergodicity
   - Mahler series
   - Plots of p-adic dynamical systems in Euclidean space
   - Open problems

Outline

1. Reminders and Preliminaries
   - Space of words
   - Space of p-adic numbers

2. Automata functions
   - Compatible functions
   - Locally compatible functions

3. Dynamics
   - Measure-preservation and ergodicity
   - Mahler series
   - Plots of p-adic dynamical systems in Euclidean space
   - Open problems

Space of words

Let X be a finite set; we call this set an *alphabet*. Given alphabet X, we denote by X^* a free monoid generated by the set X. The elements of the monoid X^* are expressed as words $x_0x_1\dots x_{n-1}$ (including the empty word $\varnothing$).
If $u = x_0x_1\dots x_{n-1} \in X^*$, then $|u| = n$ is the length of the word u. The length of $\varnothing$ is equal to zero. Along with finite words from X^* we also consider infinite words of the form $x_0x_1x_2\dots$, where $x_i \in X$. The set of such infinite words is denote by X^∞.

Space of wors

For arbitrary $u \in X^*$ and $v \in X^* \cup X^\infty$, we naturally defines the product (concatenation) $uv \in X^\infty$. A word $u \in X^*$ is the *beginning*, or *prefix* of a word $w \in X^*$ $(\in X^\infty)$ if $w = uv$ for a certain $v \in X^*$ $(\in X^\infty)$. The set X^∞ is an infinite Cartesian product $X^{\mathbb{N}}$. We can introduce on the $X^{\mathbb{N}}$ the topology of the direct Tikhonov product of finite discrete topological spaces X.

In this topology X^∞ is homeomorphic to the Cantor set. Given finite word $u \in X^*$, the set uX^∞ of all words beginning with u is closed and open simultaneously (i.e. is *clopen*) in the given topology; the family of all such sets $\{uX^\infty : u \in X^*\}$ is the base of the topology.

Space of words

We put a metric d_π on X^∞ by fixing a number $\pi > 1$ and setting $d_\pi(u,v) = \pi^{-\ell}$, where ℓ is the length of the longest common prefix of the words u and v. The distance between identical words is equal to zero.

Thus the more that the initial terms of u and v agree, the closer they are to one another. It is easy to check that d_π is a metric, and indeed a *non-Archimedean metric*, i.e. for any $u, v, w \in X^\infty$:

$$0 \leq d_\pi(u,v) \leq 1;$$

$$d_\pi(u,v) = 0 \Leftrightarrow u = v;$$

$$d_\pi(u,w) \leq \max\{d_\pi(u,v), d_\pi(v,w)\}.$$

The set uX^∞ of infinite words beginning with u is a ball $B_{\pi^{-|u|}}(w)$ of radius $\pi^{-|u|}$ centered at arbitrary $w \in uX^\infty$.

Space of words

Speaking about an *asynchronous automaton* we always understand the "letter-to-word" transducer $\mathfrak{A} = (\mathbb{X}, \mathcal{S}, \mathbb{Y}, h, g, s_0)$, where

1) $\mathbb{X}$ and $\mathbb{Y}$ are finite sets (the *input and output alphabets*, respectively);
2) $\mathcal{S}$ is a set (*the set of internal states of automaton*);
3) $h\colon \mathbb{X} \times \mathcal{S} \to \mathcal{S}$ is a mapping (*transition function*);
4) $g\colon \mathbb{X} \times \mathcal{S} \to \mathbb{Y}^*$ is a mapping (*output function*), and
5) $s_0 \in \mathcal{S}$ is fixed (*initial state*).

We assume that an asynchronous automaton $\mathfrak{A}$ works in a framework of discrete time steps. The automaton reads one symbol at a time, changing its internal state and outputting a finite sequence of symbols at each step.

Space of words

Speaking about an *asynchronous automaton* we always understand the "letter-to-word" transducer $\mathfrak{A} = (\mathbb{X}, \mathcal{S}, \mathbb{Y}, h, g, s_0)$, where

1) $\mathbb{X}$ and $\mathbb{Y}$ are finite sets (the *input and output alphabets*, respectively);
2) $\mathcal{S}$ is a set (*the set of internal states of automaton*);
3) $h\colon \mathbb{X} \times \mathcal{S} \to \mathcal{S}$ is a mapping (*transition function*);
4) $g\colon \mathbb{X} \times \mathcal{S} \to \mathbb{Y}^*$ is a mapping (*output function*), and
5) $s_0 \in \mathcal{S}$ is fixed (*initial state*).

We assume that an asynchronous automaton $\mathfrak{A}$ works in a framework of discrete time steps. The automaton reads one symbol at a time, changing its internal state and outputting a finite sequence of symbols at each step.

Space of words

For example, the asynchronous automaton represented by Moor diagram: Starting in initial state, automaton converts any first input symbol to empty word.

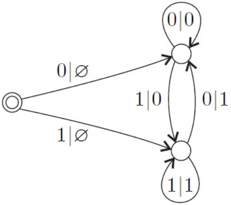


Figure: Example of an asynchronous automaton

Space of words

The cardinality $\#\mathcal{S}$ of the set of states $\mathcal{S}$ of an automaton $\mathfrak{A}$ is called the cardinality of the automaton. In particular, automaton $\mathfrak{A}$ is finite if $\#\mathcal{S} < \infty$.

If every value of the output function $g(\cdot, \cdot)$ is a one-letter word, then automaton $\mathfrak{A}$ is called a *synchronous* automaton. In the sequel denote a synchronous automaton via $\mathfrak{B}$.

The functions h and g can be continued to the set $\mathbb{X}^* \times \mathcal{S}$ ($\mathbb{X}^\infty \times \mathcal{S}$). The state $s \in \mathcal{S}$ of the automaton $\mathfrak{A}$ is called *accessible* if there exists a word $w \in \mathbb{X}^*$ such that $h(w, s_0) = s$. An automaton is called *accessible* if all its states are accessible. In the sequel, we consider only accessible automata.

An asynchronous automaton $\mathfrak{A}$ is *nondegenerate* if and only if there do not exist any accessible state $s \in \mathcal{S}$ and an infinite word $u \in \mathbb{X}^\infty$ such that, for an arbitrary prefix w of the word u, the word $g(w, s)$ is empty.

Space of words

A mapping $f\colon \mathbb{X}^\infty \to \mathbb{Y}^\infty$ is said to be defined a nondegenerate automaton $\mathfrak{A}$ if $f(u) = g(u, s_0) \in \mathbb{Y}^\infty$ for any $u \in \mathbb{X}^\infty$.

Theorem (Grigorchuk, Nekrashevich, Sushchanskii, 2000).

The mapping $f\colon \mathbb{X}^\infty \to \mathbb{Y}^\infty$ is continuous if and only if it is defined by a certain nondegenerate asynchronous automaton.

In the general case an asynchronous automaton defining a continuous mapping is infinite.

If the mapping $f\colon \mathbb{X}^\infty \to \mathbb{Y}^\infty$ is bijective, then this mapping is a homeomorphism, and the inverse mapping f^{-1} is also defined by a certain asynchronous automaton.

Space of words

A mapping $f\colon \mathbb{X}^\infty \to \mathbb{Y}^\infty$ is said to be defined a nondegenerate automaton $\mathfrak{A}$ if $f(u) = g(u, s_0) \in \mathbb{Y}^\infty$ for any $u \in \mathbb{X}^\infty$.

Theorem (Grigorchuk, Nekrashevich, Sushchanskii, 2000).

The mapping $f\colon \mathbb{X}^\infty \to \mathbb{Y}^\infty$ is continuous if and only if it is defined by a certain nondegenerate asynchronous automaton.

In the general case an asynchronous automaton defining a continuous mapping is infinite.
If the mapping $f\colon \mathbb{X}^\infty \to \mathbb{Y}^\infty$ is bijective, then this mapping is a homeomorphism, and the inverse mapping f^{-1} is also defined by a certain asynchronous automaton.

Space of p-adic numbers

Let p be a fixed prime number. By the fundamental theorem of arithmetics, each non-zero integer n can be written uniquely as

$$n = p^{\mathrm{ord}_p n}\hat{n},$$

where $\hat{n}$ is a non-zero integer, $p \nmid \hat{n}$, and $\mathrm{ord}_p n$ is a unique non-negative integer. The function $\mathrm{ord}_p n \colon \mathbb{Z}\backslash\{0\} \to \mathbb{N}_0$ is called the *p-adic valuation*. If $n, m \in \mathbb{Z}$, $m \neq 0$, then the p-adic valuation of $x = n/m \in \mathbb{Q}$ as

$$\mathrm{ord}_p x = \mathrm{ord}_p n - \mathrm{ord}_p m.$$

The p-adic valuation on $\mathbb{Q}$ is well defined; i.e., that $\mathrm{ord}_p x$ of x does not depend on the fractional representation of x.

Space of p-adic numbers

By using the p-adic valuation we will define a new absolute value on the field $\mathbb{Q}$ of rational numbers. The p-adic absolute value of $x \in \mathbb{Q}\backslash\{0\}$ is given by

$$|x|_p = p^{-\mathrm{ord}_p x}$$

and $|0|_p = 0$. The p-adic absolute value is non-Archimedean. It induces the *p-adic metric*

$$d_p(x, y) = |x - y|_p$$

which is non-Archimedean. The completion of $\mathbb{Q}$ w.r.t. p-adic metric is a field, the *field of p-adic numbers,* $\mathbb{Q}_p$. The p-adic absolute value is extended to $\mathbb{Q}_p$, and $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. The space $\mathbb{Q}_p$ is locally compact as topological space.

Space of p-adic numbers

As the absolute value $|\cdot|_p$ may be only p^k for some $k \in \mathbb{Z}$, for p-adic balls (i.e., for balls in $\mathbb{Q}_p$) we see that

$$B^-_{p^k}(x) = \{z \in \mathbb{Q}_p : d_p(z, x) < p^k\} = B_{p^{k-1}}(x) = \{z \in \mathbb{Q}_p : d_p(z, x) \leq p^{k-1}\}$$

Thus, we conclude that p-adic balls (of non-zero radii) are open and closed simultaneously; so $B_{p^k}(x)$ is a clopen ball of radius p^k centered at $x \in \mathbb{Q}_p$. Balls are compact; the set of all balls (of non-zero radii) form a topological base of a topology of a metric space. Thus, $\mathbb{Q}_p$ is a totally disconnected topological space.

Space of p-adic numbers

The ball $B_1(0) = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ is *the ring of p-adic integers* and denoted via $\mathbb{Z}_p$. The space $\mathbb{Z}_p$ is a compact clopen totally disconnected metric subspace of $\mathbb{Q}_p$.

The ball $B_1^-(0) = \{x \in \mathbb{Z}_p : |x|_p < 1\} = B_{p^{-1}}(0) = p\mathbb{Z}_p$ is a maximal ideal of the ring $\mathbb{Z}_p$. The factor ring

$$\mathbb{Z}_p / B_1^-(0) = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$$

is then a finite field $\mathbb{F}_p$ of p elements; it is called *the residue (class) field* of $\mathbb{Q}_p$.

$$\mathbb{Z} \underset{\neq}{\subseteq} \mathbb{Z}_p \cap \mathbb{Q} \underset{\neq}{\subseteq} \mathbb{Z}_p \underset{\neq}{\subseteq} \mathbb{Q}_p$$

Space of p-adic numbers

The ball $B_1(0) = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ is *the ring of p-adic integers* and denoted via $\mathbb{Z}_p$. The space $\mathbb{Z}_p$ is a compact clopen totally disconnected metric subspace of $\mathbb{Q}_p$.

The ball $B_1^-(0) = \{x \in \mathbb{Z}_p : |x|_p < 1\} = B_{p^{-1}}(0) = p\mathbb{Z}_p$ is a maximal ideal of the ring $\mathbb{Z}_p$. The factor ring

$$\mathbb{Z}_p/B_1^-(0) = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$$

is then a finite field $\mathbb{F}_p$ of p elements; it is called *the residue (class) field* of $\mathbb{Q}_p$.

$$\mathbb{Z} \subsetneqq \mathbb{Z}_p \cap \mathbb{Q} \subsetneqq \mathbb{Z}_p \subsetneqq \mathbb{Q}_p$$

Space of p-adic numbers

Every p-adic number has a unique representation as a sum of a special convergent p-adic series which is called a *canonical representation*, or a *p-adic expansion*.

For $x \in \mathbb{Z}_p$ there exist a unique sequence $\delta_0(x), \delta_1(x), \ldots \in \{0, 1, \ldots, p-1\}$ such that

$$x = \sum_{i=0}^{\infty} \delta_i(x) \cdot p^i = \delta_0(x) + \delta_1(x) \cdot p + \delta_2(x) \cdot p^2 + \ldots.$$

The function $\delta_i(x)$ is called the *i-th coordinate function*.

Space of p-adic numbers

Let $x = \delta_0(x) + \delta_1(x) \cdot p + \delta_2(x) \cdot p^2 + \ldots$ be a p-adic integer in its canonical representation. The map

$$\mathrm{mod} p^k : x = \sum_{i=0}^{\infty} \delta_i(x) \cdot p^i \mapsto x \bmod p^k = \sum_{i=0}^{k-1} \delta_i(x) \cdot p^i$$

is a *continuous ring epimorphism* of the ring $\mathbb{Z}_p$ onto the ring $\mathbb{Z}/p^k\mathbb{Z}$ of residues modulo p^k; it is called *reduction map modulo p^k*.
The kernel of the epimorphism $\mathrm{mod} p^k$ is a ball $p^k\mathbb{Z}_p = B_{p^{-k}}(0)$ of radius p^{-k} around 0. The rest $p^k - 1$ balls of radii p^{-k} are co-sets with respect to this epimorphism, e.g., $B_{p^{-k}}(1) = 1 + p^k\mathbb{Z}_p$, is a co-set of 1, i.e. the sets of all p-adic integers that are congruent to 1 modulo p^k.

Space of p-adic numbers

A p-adic integer $x \in \mathbb{Z}_p$ is *invertible* in $\mathbb{Z}_p$, that is, has a *multiplicative inverse* $x^{-1} \in \mathbb{Z}_p$, $x \cdot x^{-1} = 1$, if and only if $\delta_0(x) \neq 0$; that is, if and only if x is *invertible modulo p*, meaning $x \bmod p$ is invertible in $\mathbb{F}_p$. Invertible p-adic integer is also called a *unit*. The set $\mathbb{Z}_p^*$ of all units of $\mathbb{Z}_p$ is a group with respect to multiplication, called a *group of units*, or a *multiplicative subgroup* of $\mathbb{Z}_p$. The group of units $\mathbb{Z}_p^*$ is a p-adic *sphere* $S_1(0)$ of radius 1 around 0:

$$\mathbb{Z}_p^* = \{z \in \mathbb{Z}_p : |z|_p = 1\} = \mathbb{Z}_p \setminus p\mathbb{Z}_p = B_1(0) \setminus B_{p^{-1}}(0) = S_1(0).$$

Outline

1. Reminders and Preliminaries
   - Space of words
   - Space of p-adic numbers
2. Automata functions
   - Compatible functions
   - Locally compatible functions
3. Dynamics
   - Measure-preservation and ergodicity
   - Mahler series
   - Plots of p-adic dynamical systems in Euclidean space
   - Open problems

Automata maps

We identify n-letter words over $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ with non-negative integers in a natural way: Given an n-letter word $u = x_0 x_1 \dots x_{n-1}$, $x_i \in \mathbb{F}_p$, we consider u as a base-p expansion of the number $\alpha(u) = x_{n-1} \dots x_1 x_0 = x_0 + x_1 \cdot p + \dots + x_{n-1} \cdot p^{n-1}$. In turn, the latter number can be considered as an element of the residue ring $\mathbb{Z}/p^n\mathbb{Z} = \{0, 1, \dots, p^n - 1\}$ modulo p^n. Thus, every (synchronous) automaton $\mathfrak{B} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$ corresponds a *map from $\mathbb{Z}/p^n\mathbb{Z}$ to $\mathbb{Z}/p^n\mathbb{Z}$*, for every $n = 1, 2, 3 \dots$.

Moreover, given an infinite word $u = x_0 x_1 x_2 \dots$ over $\mathbb{F}_p$ we consider u as the p-adic integer $x = \alpha(u) = \dots x_2 x_1 x_0$ whose canonical expansion is $x = \alpha(u) = x_0 + x_1 \cdot p + x_2 \cdot p^2 + \dots = \sum_{i=0}^{\infty} x_i \cdot p^i$. Then every (synchronous) automaton $\mathfrak{B} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$ *defines a map $f_{\mathfrak{B}}$ from the ring of p-adic integers $\mathbb{Z}_p$ to itself*: For every $x \in \mathbb{Z}_p$ we put $\delta_i(f_{\mathfrak{B}}(x)) = g(\delta_i(x), s_i)$, $i = 0, 1, 2, \dots$ where $s_i = h(\delta_{i-1}(x), s_{i-1})$, $i = 1, 2, \dots$. We say then that map $f_{\mathfrak{B}}$ is *synchronous automaton function* (or, *automaton map*) of the synchronous automaton $\mathfrak{B}$.

Automata maps

We identify n-letter words over $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ with non-negative integers in a natural way: Given an n-letter word $u = x_0x_1 \ldots x_{n-1}$, $x_i \in \mathbb{F}_p$, we consider u as a base-p expansion of the number $\alpha(u) = x_{n-1} \ldots x_1x_0 = x_0 + x_1 \cdot p + \ldots + x_{n-1} \cdot p^{n-1}$. In turn, the latter number can be considered as an element of the residue ring $\mathbb{Z}/p^n\mathbb{Z} = \{0, 1, \ldots, p^n - 1\}$ modulo p^n. Thus, every (synchronous) automaton $\mathfrak{B} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$ corresponds a *map from $\mathbb{Z}/p^n\mathbb{Z}$ to $\mathbb{Z}/p^n\mathbb{Z}$*, for every $n = 1, 2, 3 \ldots$.

Moreover, given an infinite word $u = x_0x_1x_2 \ldots$ over $\mathbb{F}_p$ we consider u as the p-adic integer $x = \alpha(u) = \ldots x_2x_1x_0$ whose canonical expansion is $x = \alpha(u) = x_0 + x_1 \cdot p + x_2 \cdot p^2 + \ldots = \sum_{i=0}^{\infty} x_i \cdot p^i$. Then every (synchronous) automaton $\mathfrak{B} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$ *defines a map $f_{\mathfrak{B}}$ from the ring of p-adic integers $\mathbb{Z}_p$ to itself*: For every $x \in \mathbb{Z}_p$ we put $\delta_i(f_{\mathfrak{B}}(x)) = g(\delta_i(x), s_i)$, $i = 0, 1, 2, \ldots$ where $s_i = h(\delta_{i-1}(x), s_{i-1})$, $i = 1, 2, \ldots$. We say then that map $f_{\mathfrak{B}}$ is *synchronous automaton function* (or, *automaton map*) of the synchronous automaton $\mathfrak{B}$.

Automata maps

Similarly way, a (nondegenerate) asynchronous automaton $\mathfrak{A} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$ naturally defines a *continuous mapping* (w.r.t. p-adic metric) $f_{\mathfrak{A}} \colon \mathbb{Z}_p \to \mathbb{Z}_p$.

Theorem (Lunts, 1965; Grigorchuk et al., 2000; Anashin, 2009).

The automaton map $f_{\mathfrak{B}} \colon \mathbb{Z}_p \to \mathbb{Z}_p$ of the (synchronous) automaton $\mathfrak{B} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$ *satisfy the p-adic Lipschitz condition with constant* 1 (is a 1-Lipschitz, for brevity), i.e.

$$|f_{\mathfrak{B}}(x) - f_{\mathfrak{B}}(y)|_p \leq |x - y|_p$$

for all $x, y \in \mathbb{Z}_p$. Conversely, *for every 1-Lipschitz function $f \colon \mathbb{Z}_p \to \mathbb{Z}_p$ there exists an automaton $\mathfrak{B} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$ such that $f = f_{\mathfrak{B}}$*.

For example, every function $f \in \mathbb{Z}_p[x]$ defined by polynomial with p-adic integers coefficients (in particular, with rational integers) is a 1-Lipschitz map, hence it is an automaton map.

Automata maps

Similarly way, a (nondegenerate) asynchronous automaton $\mathfrak{A} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$ naturally defines a *continuous mapping* (w.r.t. p-adic metric) $f_{\mathfrak{A}} \colon \mathbb{Z}_p \to \mathbb{Z}_p$.

Theorem (Lunts, 1965; Grigorchuk et al., 2000; Anashin, 2009).

The automaton map $f_{\mathfrak{B}} \colon \mathbb{Z}_p \to \mathbb{Z}_p$ of the (synchronous) automaton $\mathfrak{B} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$ *satisfy the p-adic Lipschitz condition with constant* 1 (is a 1-Lipschitz, for brevity), i.e.

$$|f_{\mathfrak{B}}(x) - f_{\mathfrak{B}}(y)|_p \le |x - y|_p$$

for all $x, y \in \mathbb{Z}_p$. Conversely, *for every 1-Lipschitz function $f \colon \mathbb{Z}_p \to \mathbb{Z}_p$ there exists an automaton $\mathfrak{B} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$ such that $f = f_{\mathfrak{B}}$.*

For example, every function $f \in \mathbb{Z}_p[x]$ defined by polynomial with p-adic integers coefficients (in particular, with rational integers) is a 1-Lipschitz map, hence it is an automaton map.

Automata maps

Similarly way, a (nondegenerate) asynchronous automaton $\mathfrak{A} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$ naturally defines a *continuous mapping* (w.r.t. p-adic metric) $f_{\mathfrak{A}} \colon \mathbb{Z}_p \to \mathbb{Z}_p$.

Theorem (Lunts, 1965; Grigorchuk et al., 2000; Anashin, 2009).

The automaton map $f_{\mathfrak{B}} \colon \mathbb{Z}_p \to \mathbb{Z}_p$ of the (synchronous) automaton $\mathfrak{B} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$ *satisfy the p-adic Lipschitz condition with constant* 1 (is a 1-Lipschitz, for brevity), i.e.

$$|f_{\mathfrak{B}}(x) - f_{\mathfrak{B}}(y)|_p \leq |x-y|_p$$

for all $x, y \in \mathbb{Z}_p$. Conversely, *for every 1-Lipschitz function* $f \colon \mathbb{Z}_p \to \mathbb{Z}_p$ *there exists an automaton* $\mathfrak{B} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$ *such that* $f = f_{\mathfrak{B}}$.

For example, every function $f \in \mathbb{Z}_p[x]$ defined by polynomial with p-adic integers coefficients (in particular, with rational integers) is a 1-Lipschitz map, hence it is an automaton map.

Non-expansive maps (or, compatible functions)

Definition (Compatible function)

A map $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is called *compatible* iff $a \equiv b \pmod{p^k}$ implies $f(a) \equiv f(b) \pmod{p^k}$.

A map $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is compatible iff f commutes with modp^k for all $k = 1, 2, 3, \ldots$; that is, iff all the following diagrams commutes:

$$\begin{tikzcd}
\mathbb{Z}_p \arrow[r, "f"] \arrow[d, "\text{mod } p^k"] & \mathbb{Z}_p \arrow[d, "\text{mod } p^k"] \\
\mathbb{Z}/p^k\mathbb{Z} \arrow[r, "f \text{ mod } p^k"] & \mathbb{Z}/p^k\mathbb{Z}
\end{tikzcd}$$

Therefore all induced maps $f \bmod p^k\colon u \bmod p^k \mapsto f(u) \bmod p^k$ of residue rings $\mathbb{Z}/p^k\mathbb{Z}$ modulo p^k are well defined.

Non-expansive maps (or, compatible functions)

Compatibility = 1-Lipschitz propety = non-expansiveness:

A map $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is compatible iff it satisfies p-adic Lipschitz condition with a constant 1: $|f(a) - f(b)|_p \leq |a - b|_p$ for all $a, b \in \mathbb{Z}_p$.

Compatibility = triangularity

A map $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is called triangular iff it is of the form

$$\ldots + \chi_2 \cdot p^2 + \chi_1 \cdot p + \chi_0 \overset{f}{\mapsto} \cdots + \psi_2(\chi_0, \chi_1, \chi_2) \cdot p^2 + \psi_1(\chi_0, \chi_1) \cdot p + \psi_0(\chi_0),$$

where $\chi_0, \chi_1, \ldots \in \mathbb{F}_p = \{0, 1, \ldots, p-1\}$, $\psi_i\colon \mathbb{F}_p^{i+1} \to \mathbb{F}_p$, $i = 0, 1, 2, \ldots$.

For $p = 2$ this class of functions has practical importance for computer science since it includes all mappings combined of standard microprocessor instructions, such as arithmetic ones (integer addition, multiplication, etc.) and bitwise logical ones (such as AND, OR, XOR, etc.).

Non-expansive maps (or, compatible functions)

Compatibility = 1-Lipschitz propety = non-expansiveness:

A map $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is compatible iff it satisfies p-adic Lipschitz condition with a constant 1: $|f(a) - f(b)|_p \le |a - b|_p$ for all $a, b \in \mathbb{Z}_p$.

Compatibility = triangularity

A map $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is called triangular iff it is of the form

$$\ldots + \chi_2 \cdot p^2 + \chi_1 \cdot p + \chi_0 \overset{f}{\mapsto} \cdots + \psi_2(\chi_0, \chi_1, \chi_2) \cdot p^2 + \psi_1(\chi_0, \chi_1) \cdot p + \psi_0(\chi_0),$$

where $\chi_0, \chi_1, \ldots \in \mathbb{F}_p = \{0, 1, \ldots, p-1\}$, $\psi_i\colon \mathbb{F}_p^{i+1} \to \mathbb{F}_p$, $i = 0, 1, 2, \ldots$.

For $p = 2$ this class of functions has practical importance for computer science since it includes all mappings combined of standard microprocessor instructions, such as arithmetic ones (integer addition, multiplication, etc.) and bitwise logical ones (such as AND, OR, XOR, etc.).

Locally compatible functions

The function $F\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is called locally compatible function (or, locally 1-Lipschitz function) if F satisfies inequality

$$|F(a) - F(b)|_p \leq |a - b|_p$$

locally; that is, given $a \in \mathbb{Z}_p$, there exists an open neighbourhood $\mathbf{O}_a$ of a such that this inequality holds for all $b \in \mathbf{O}_a$.

As $\mathbb{Z}_p$ is compact, the function $F\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is locally compatible if and only if such that

$$|F(a) - F(b)|_p \leq |a - b|_p$$

holds for all $a, b \in \mathbb{Z}_p$ which are sufficiently close to one another, that is, there exists $r \in \mathbb{N}_0$ such that this inequality is true once $|a - b|_p \leq p^{-r}$.

Locally compatible functions

The function $F\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is called locally compatible function (or, locally 1-Lipschitz function) if F satisfies inequality

$$|F(a) - F(b)|_p \leq |a - b|_p$$

locally; that is, given $a \in \mathbb{Z}_p$, there exists an open neighbourhood $\mathbf{O}_a$ of a such that this inequality holds for all $b \in \mathbf{O}_a$.

As $\mathbb{Z}_p$ is compact, the function $F\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is locally compatible if and only if such that

$$|F(a) - F(b)|_p \leq |a - b|_p$$

holds for all $a, b \in \mathbb{Z}_p$ which are sufficiently close to one another, that is, there exists $r \in \mathbb{N}_0$ such that this inequality is true once $|a - b|_p \leq p^{-r}$.

Locally compatible functions

Now we characterize multivariate compatible functions in terms of the coordinate functions; the latter are functions $\delta_i(f(x_1,\dots,x_m))$ defined on $\mathbb{Z}_p^m$ and valuated in $\{0,1,\dots,p-1\}$: The i-th coordinate function is merely a value of coefficient of the i-th term in a canonical p-adic expansion of $f(x_1,\dots,x_m)$.

Proposition 1.

A function $f\colon \mathbb{Z}_p^m \to \mathbb{Z}_p$ is compatible if and only if for every $i = 1,2,\dots$ the i-th coordinate function $\delta_i(f(x_1,\dots,x_m))$ does not depend on $\delta_{i+k}(x_s)$, for all $s = 1,2,\dots,m$ and $k = 1,2,\dots$.

Proposition 2.

A function $f\colon Z_p^m \to \mathbb{Z}p$ is locally compatible if and only if there exists $N \in \mathbb{N}_0$ such that for every $i = N, N+1, N+2, \dots$ the i-th coordinate function $\delta_i(f(x_1,...,x_m))$ does not depend on $\delta_{i+k}(x_s)$, for all $s = 1,2,\dots,m$ and $k = 1,2,\dots$.

Locally compatible functions

Now we characterize multivariate compatible functions in terms of the coordinate functions; the latter are functions $\delta_i(f(x_1,\dots,x_m))$ defined on $\mathbb{Z}_p^m$ and valuated in $\{0,1,\dots,p-1\}$: The i-th coordinate function is merely a value of coefficient of the i-th term in a canonical p-adic expansion of $f(x_1,\dots,x_m)$.

Proposition 1.

A function $f\colon \mathbb{Z}_p^m \to \mathbb{Z}_p$ is compatible if and only if for every $i=1,2,\dots$ the i-th coordinate function $\delta_i(f(x_1,\dots,x_m))$ does not depend on $\delta_{i+k}(x_s)$, for all $s=1,2,\dots,m$ and $k=1,2,\dots$.

Proposition 2.

A function $f\colon Z_p^m \to \mathbb{Z}p$ is locally compatible if and only if there exists $N \in \mathbb{N}_0$ such that for every $i=N,N+1,N+2,\dots$ the i-th coordinate function $\delta_i(f(x_1,...,x_m))$ does not depend on $\delta_{i+k}(x_s)$, for all $s=1,2,\dots,m$ and $k=1,2,\dots$.

n-Unit delay

Let $n \in \mathbb{N}$ be a natural number and let $\mathfrak{C}^{(n)} = (\mathbb{X}, \mathcal{S}, \mathbb{Y}, h, g, s_0)$ be a nongenerate asynchronous automaton, which is translated the infinite input word $u = x_0 x_1 \dots x_{n-1} \dots$ into infinite output word $w = \underbrace{\varnothing\varnothing\dots\varnothing}_{n \text{ times}} y_n y_{n+1}\dots$; So, we have

$$y_i = g(x_i, s_i) = \varnothing \text{ for } i = 0, 1, 2 \dots, n-1,$$

$$s_i = h(x_{i-1}, s_{i-1}) \text{ for } i = 1, 2, \dots, n-1, \text{ and}$$

$$y_i = g(x_i, s_i), s_{i+1} = h(x_i, s_i)$$

for all $i = n, n+1, \dots$.

Unilateral shift

Example.

A *unilateral shift* is the transformation of the space of infinite words over alphabet $\mathbb{X}$ defined by the rule

$$x_0x_1x_2\ldots \mapsto x_1x_2x_3\ldots.$$

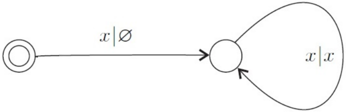
Unilateral shift

Example.

A *unilateral shift* is the transformation of the space of infinite words over alphabet $\mathbb{X}$ defined by the rule

$$x_0x_1x_2\ldots \mapsto x_1x_2x_3\ldots.$$

Note that, a unilateral shift is defined by an asynchronous automaton $\mathfrak{C}^{(1)} = (\mathbb{X}, \mathcal{S}, \mathbb{X}, h, g, s_0)$, whose output function g is expressed as follows $g(x_0, s_0) = \varnothing$, and $g(x_i, s_i) = x_i$ for $i = 1, 2, \ldots$.



Shifts

In the case $\mathbb{X} = \mathbb{Y} = \mathbb{F}_p$, the automaton $\mathfrak{C}^{(1)} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$ naturally defines the p-adic shift (or, *the one-sided Bernoulli shift*); that is, the p-adic shift $\sigma\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is expressed as follows. If $x = \ldots x_2 x_1 x_0 = x_0 + x_1 p + x_2 p^2 + \ldots$, where $x_i \in \mathbb{F}_p$, we let

$$\sigma(x) = \frac{x - x_0}{p} = \ldots x_3 x_2 x_1 = x_1 + x_2 p + x_3 p^2 + \cdots .$$

In other words, the shift σ cuts off the first digit term in the p-adic expansion of $x \in \mathbb{Z}_p$.We see that if σ^n denotes the n-fold iterate of σ, then we have

$$\sigma^n(x) = \frac{x - (x_0 + x_1 p + \ldots + x_{n-1} p^{n-1})}{p^n} = x_n + x_{n+1} p + \ldots .$$

Moreover, for $x \in \mathbb{Z}$, it is the case that $\sigma^n(x) = \lfloor \frac{x}{p^n} \rfloor$ were $\lfloor \cdot \rfloor$ is the greatest integer function.

Locally constant functions

A function $T\colon \mathbb{Z}_p \to \mathbb{Q}_p$ is called a *locally constant* if for every $x \in \mathbb{Z}_p$ there exist an open neighbourhood U_x (e.g., a ball of radius p^{-N} for some $N \in \mathbb{N}$ centered at x, $U_x = \{z \in \mathbb{Z}_p : |x - z|_p < p^{-N}\}$) such that T is a constant on U_x.

For example, for arbitrary $i \in \mathbb{N}$ a function $\delta_i(x)$ is locally constant, because δ_i remains unchanged if we replace x by any y, such that $|x - y|_p < p^{-i}$.

Let $D \subset \mathbb{Z}_p$, not necessarily compact. A function $T\colon \mathbb{Z}_p \to \mathbb{Q}_p$ is called a *step function* on D if there exists a positive integer ℓ such that $T(x) = T(y)$ for all $x, y \in D$ with $|x - y|_p \le p^{-\ell}$. The smallest integer ℓ with this property is called the *order* of the step function T.

It is clear from the definition that a step function is a locally constant on D. On $\mathbb{Z}_p$ it also holds, that any locally constant function is a step function.

Locally constant functions

A function $T\colon \mathbb{Z}_p \to \mathbb{Q}_p$ is called a *locally constant* if for every $x \in \mathbb{Z}_p$ there exist an open neighbourhood U_x (e.g., a ball of radius p^{-N} for some $N \in \mathbb{N}$ centered at x, $U_x = \{z \in \mathbb{Z}_p : |x - z|_p < p^{-N}\}$) such that T is a constant on U_x.

For example, for arbitrary $i \in \mathbb{N}$ a function $\delta_i(x)$ is locally constant, because δ_i remains unchanged if we replace x by any y, such that $|x - y|_p < p^{-i}$.

Let $D \subset \mathbb{Z}_p$, not necessarily compact. A function $T\colon \mathbb{Z}_p \to \mathbb{Q}_p$ is called a *step function* on D if there exists a positive integer ℓ such that $T(x) = T(y)$ for all $x, y \in D$ with $|x - y|_p \leq p^{-\ell}$. The smallest integer ℓ with this property is called the *order* of the step function T.

It is clear from the definition that a step function is a locally constant on D. On $\mathbb{Z}_p$ it also holds, that any locally constant function is a step function.

Locally constant functions

A function $T\colon \mathbb{Z}_p \to \mathbb{Q}_p$ is called a *locally constant* if for every $x \in \mathbb{Z}_p$ there exist an open neighbourhood U_x (e.g., a ball of radius p^{-N} for some $N \in \mathbb{N}$ centered at x, $U_x = \{z \in \mathbb{Z}_p : |x - z|_p < p^{-N}\}$) such that T is a constant on U_x.

For example, for arbitrary $i \in \mathbb{N}$ a function $\delta_i(x)$ is locally constant, because δ_i remains unchanged if we replace x by any y, such that $|x - y|_p < p^{-i}$.

Let $D \subset \mathbb{Z}_p$, not necessarily compact. A function $T\colon \mathbb{Z}_p \to \mathbb{Q}_p$ is called a *step function* on D if there exists a positive integer ℓ such that $T(x) = T(y)$ for all $x, y \in D$ with $|x - y|_p \leq p^{-\ell}$. The smallest integer ℓ with this property is called the *order* of the step function T.

It is clear from the definition that a step function is a locally constant on D. On $\mathbb{Z}_p$ it also holds, that any locally constant function is a step function.

Complex (or, generalized) shift

Let $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function. Given natural $n \in \mathbb{N}$, for all $x \in \mathbb{Z}_p$ we can represent f as

$$f(x) = (f(x \bmod p^n)) \bmod p^n + p^n G_z(t),$$

where $t = p^{-n}(x - (x \bmod p^n)) \in \mathbb{Z}_p$, $z = x \bmod p^n$, and $G_z\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is a 1-Lipschitz function. It is clear that f is the automaton map of a synchronous automaton $\mathfrak{B} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$, and G_z is an automaton map of the automaton $\mathfrak{B}_z = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s(z))$, where $s(z) \in \mathcal{S}$ is the accessible state of the automaton $\mathfrak{B}$, i.e. $s(z)$ was reached after being feeded by the input word $z = x \bmod p^n$.

Similarly, for map $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ that defined by an asynchronous automaton $\mathfrak{C}^{(n)}$, we can see that

$$f(x) = G_z(t) + T(x),$$

where for any $z = x \bmod p^n$, the map $G_z\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is a 1-Lipschitz, $T(x)$ is a step function of order not greater than n, and $t = p^{-n}(x - (x \bmod p^n))$; and we say that f is a *complex shift*.

Complex (or, generalized) shift

Let $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function. Given natural $n \in \mathbb{N}$, for all $x \in \mathbb{Z}_p$ we can represent f as

$$f(x) = (f(x \bmod p^n)) \bmod p^n + p^n G_z(t),$$

where $t = p^{-n}(x - (x \bmod p^n)) \in \mathbb{Z}_p$, $z = x \bmod p^n$, and $G_z\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is a 1-Lipschitz function. It is clear that f is the automaton map of a synchronous automaton $\mathfrak{B} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$, and G_z is an automaton map of the automaton $\mathfrak{B}_z = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s(z))$, where $s(z) \in \mathcal{S}$ is the accessible state of the automaton $\mathfrak{B}$, i.e. $s(z)$ was reached after being feeded by the input word $z = x \bmod p^n$.
Similarly, for map $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ that defined by an asynchronous automaton $\mathfrak{C}^{(n)}$, we can see that

$$f(x) = G_z(t) + T(x),$$

where for any $z = x \bmod p^n$, the map $G_z\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is a 1-Lipschitz, $T(x)$ is a step function of order not greater than n, and $t = p^{-n}(x - (x \bmod p^n))$; and we say that f is a *complex shift*.

Complex (or, generalized) shift

For a complex shift f a following condition holds: There exist positive integer $M \in \mathbb{N}$ such that for every $i \geq M$ the i-th coordinate function $\delta_i(f(x))$ does not depend on $\delta_{i+k}(x)$ for $k = 1, 2, \ldots$. Hence, a complex shift is a locally 1-Lipschitz function.

By the definition, a function F is a locally 1-Lipschitz if for a given $x \in \mathbb{Z}_p$, there exist an open neighbourhood U_x of x such that the inequality

$$|F(x) - F(y)|_p \leq |x - y|_p$$

holds for all $y \in U_x$. As $\mathbb{Z}_p$ is compact, the function $F\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is a locally 1-Lipschitz if and only if the latter inequality holds for all $x, y \in \mathbb{Z}_p$ which are sufficiently close to one another.

Complex (or, generalized) shift

For a complex shift f a following condition holds: There exist positive integer $M \in \mathbb{N}$ such that for every $i \geq M$ the i-th coordinate function $\delta_i(f(x))$ does not depend on $\delta_{i+k}(x)$ for $k = 1, 2, \ldots$. Hence, a complex shift is a locally 1-Lipschitz function.

By the definition, a function F is a locally 1-Lipschitz if for a given $x \in \mathbb{Z}_p$, there exist an open neighbourhood U_x of x such that the inequality

$$|F(x) - F(y)|_p \leq |x - y|_p$$

holds for all $y \in U_x$. As $\mathbb{Z}_p$ is compact, the function $F \colon \mathbb{Z}_p \to \mathbb{Z}_p$ is a locally 1-Lipschitz if and only if the latter inequality holds for all $x, y \in \mathbb{Z}_p$ which are sufficiently close to one another.

Outline

1. Reminders and Preliminaries
   - Space of words
   - Space of p-adic numbers
2. Automata functions
   - Compatible functions
   - Locally compatible functions
3. Dynamics
   - Measure-preservation and ergodicity
   - Mahler series
   - Plots of p-adic dynamical systems in Euclidean space
   - Open problems

Dynamics

A *dynamical system* on a measurable space $\mathbb{S}$ is understood as a triple $(\mathbb{S}, \mu, f)$, where $\mathbb{S}$ is a set endowed with a measure μ and $f\colon \mathbb{S} \to \mathbb{S}$ is a measurable function; that is, the f-preimage $f^{-1}(T)$ of any μ-measurable subset $T \subset \mathbb{S}$ is a μ-measurable subset of $\mathbb{S}$.

An iteration of a function $f_{\mathfrak{A}}\colon \mathbb{Z}_p \to \mathbb{Z}_p$ which is defined by (asynchronous) automaton $\mathfrak{A} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$ generates a dynamical system $(\mathbb{Z}_p, \mu_p, f_{\mathfrak{A}})$ on the space $\mathbb{Z}_p$.

The space $\mathbb{Z}_p$ is equipped with a natural probability measure, namely, the *Haar measure* μ_p normalized so that the measure of the whole space is 1, $\mu_p(\mathbb{Z}_p) = 1$. Balls $B_{p^{-k}}(a)$ of nonzero radii constitute the base of the corresponding σ-algebra of measurable subsets of $\mathbb{Z}_p$. That is, every element of the σ-algebra, the measurable subset of $\mathbb{Z}_p$, can be constructed from the elementary measurable subsets by taking complements and countable unions. We put $\mu_p(B_{p^{-k}}(a)) = p^{-k}$.

Dynamics

A *dynamical system* on a measurable space $\mathbb{S}$ is understood as a triple $(\mathbb{S}, \mu, f)$, where $\mathbb{S}$ is a set endowed with a measure μ and $f\colon \mathbb{S} \to \mathbb{S}$ is a measurable function; that is, the f-preimage $f^{-1}(T)$ of any μ-measurable subset $T \subset \mathbb{S}$ is a μ-measurable subset of $\mathbb{S}$.

An iteration of a function $f_{\mathfrak{A}}\colon \mathbb{Z}_p \to \mathbb{Z}_p$ which is defined by (asynchronous) automaton $\mathfrak{A} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, h, g, s_0)$ generates a dynamical system $(\mathbb{Z}_p, \mu_p, f_{\mathfrak{A}})$ on the space $\mathbb{Z}_p$.

The space $\mathbb{Z}_p$ is equipped with a natural probability measure, namely, the *Haar measure μ_p* normalized so that the measure of the whole space is 1, $\mu_p(\mathbb{Z}_p) = 1$. Balls $B_{p^{-k}}(a)$ of nonzero radii constitute the base of the corresponding σ-algebra of measurable subsets of $\mathbb{Z}_p$. That is, every element of the σ-algebra, the measurable subset of $\mathbb{Z}_p$, can be constructed from the elementary measurable subsets by taking complements and countable unions. We put $\mu_p(B_{p^{-k}}(a)) = p^{-k}$.

Dynamics

We remind that if a measure space $\mathbb{S}$ endowed with a probability measure μ is also a topological space, the measure μ is called *Borel* if all Borel sets in $\mathbb{S}$ are μ-measurable. Recall that a *Borel set* is any element of σ-algebra generated by all open subsets of $\mathbb{S}$; that is, a Borel subset can be constructed from open subsets with the use of complements and countable unions. A probability measure μ is called *regular* if for all Borel sets X in $\mathbb{S}$

$$\mu(X) = \sup\{\mu(A) : A \subseteq X, A \text{ closed}\} = \inf\{\mu(B) : X \subseteq B, B \text{ open}\}.$$

The probability measure μ_p is Borel and regular.

Dynamics

A dynamical system $(\mathbb{Z}_p, \mu_p, f_{\mathfrak{A}})$ is also *topological* since $\mathbb{Z}_p$ are not only measurable space but also metric space, and corresponding transformation $f_{\mathfrak{A}}$ are not only measurable but also continuous. Moreover, this dynamical system is non-Archimedean, due to the fact that the space $\mathbb{Z}_p$ is non-Archimedean space.

Measure-preservation and ergodicity

A measurable mapping $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is called *measure-preserving* if $\mu_p(f^{-1}(S)) = \mu_p(S)$ for each measurable subset $S \subset \mathbb{Z}_p$.

A measure-preserving map f is said to be *ergodic* if for each measurable subset S such that $f^{-1}(S) = S$ holds either $\mu_p(S) = 1$ or $\mu_p(S) = 0$; so ergodicity of the map f just means that f has no proper invariant subsets; that is, invariant subsets whose measure is neither 0 nor 1.

The following question arises. What continuous (w.r.t. the metric d_p) transformations of $\mathbb{Z}_p$ are measure-preserving or ergodic (w.r.t. the measure μ_p)?

Measure-preservation and ergodicity

A measurable mapping $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is called *measure-preserving* if $\mu_p(f^{-1}(S)) = \mu_p(S)$ for each measurable subset $S \subset \mathbb{Z}_p$.

A measure-preserving map f is said to be *ergodic* if for each measurable subset S such that $f^{-1}(S) = S$ holds either $\mu_p(S) = 1$ or $\mu_p(S) = 0$; so ergodicity of the map f just means that f has no proper invariant subsets; that is, invariant subsets whose measure is neither 0 nor 1.

The following question arises. What continuous (w.r.t. the metric d_p) transformations of $\mathbb{Z}_p$ are measure-preserving or ergodic (w.r.t. the measure μ_p)?

Measure-preservation

For a given $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ and $n \in \mathbb{N}$, let f_k be a function defined on the ring $\mathbb{Z}/p^{n\cdot k}\mathbb{Z}$ and valuated in the ring $\mathbb{Z}/p^{n\cdot(k-1)}\mathbb{Z}$, where $k = 2, 3, \ldots$. The following criterion of measure-preservation for a complex shift f is valid.

Theorem (L.T., 2015).

A mapping $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is measure-preserving if and only if the number $\# f_k^{-1}(x)$ of f_k-preimages of the point $x \in \mathbb{Z}/p^{n\cdot(k-1)}\mathbb{Z}$ is equal to p^n.

Ergodicity

Given a map $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$, a point $z_0 \in \mathbb{Z}_p$ is said to be a *periodic point* if there exists $r \in \mathbb{N}$ such that $f^r(z_0) = z_0$. The least r with this property is called the *length* of period of z_0. If z_0 has period r, it is called an *r-periodic point*. The orbit of an r-periodic point z_0 is $\{z_0, f(z_0), \dots, f^{r-1}(z_0)\}$. This orbit is called an *r-cycle*.

For a given $n \in \mathbb{N}$, let $f \bmod p^{k\cdot n}\colon \mathbb{Z}/p^{k\cdot n}\mathbb{Z} \to \mathbb{Z}/p^{k\cdot n}\mathbb{Z}$, for $k = 1, 2, 3, \dots$; and let γ_k be an r_k-cycle $\{z_0, z_1, \dots, z_{r_k - 1}\}$, where $z_j = (f \bmod p^{k\cdot n})^j(z_0)$, $0 \le j \le r_k - 1$, $k = 1, 2, 3, \dots$.

The following condition of ergodicity holds.

Theorem (L.T., 2015).

Let $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ be a complex shift and let f be a measure-preserving map. Then f is ergodic if for every $k \in \mathbb{N}$ γ_k is a unique cycle.

Mahler Expansion

By Mahler's Theorem, any continuous function $F\colon \mathbb{Z}_p \to \mathbb{Z}_p$ can be expressed in the form of a uniformly convergent series, called its *Mahler Expansion* (or, *Mahler series*):

$$F(x) = \sum_{m=0}^{\infty} a_m \binom{x}{m},$$

where

$$a_m = \sum_{i=0}^{m} (-1)^{m+i} F(i) \binom{m}{i} \in \mathbb{Z}_p$$

and

$$\binom{x}{m} = \frac{x(x-m)\cdots(x-m+1)}{m!}, m = 1, 2, \ldots, \binom{x}{0} = 1.$$

Mahler series converges uniformly on $\mathbb{Z}_p$ if and only if

$$\lim\limits^{p}_{m\to\infty} a_m = 0.$$

Mahler Expansion

Hence uniformly convergent series defines a uniformly continuous function on $\mathbb{Z}_p$. The function f represented by the Mahler series is uniformly differentiable everywhere on $\mathbb{Z}_p$ if and only if

$$\overset{p}{\lim_{m\to\infty}} \frac{a_{m+k}}{m} = 0$$

for all $k \in \mathbb{N}$.
The function f is analytic on $\mathbb{Z}_p$ if and only if

$$\overset{p}{\lim_{m\to\infty}} \frac{a_m}{m!} = 0.$$

Various properties of the function f can be expressed via properties of coefficients of its Mahler expansion.

Mahler Expansion

Let $a_m^{(n)}$ be the n-th Mahler coefficient of the Bernoulli shift σ^n. We have

$$\sigma^n(x) = \sum_{m=0}^{\infty} a_m^{(n)} \binom{x}{m}.$$

Theorem (Kingsbery, Levin, Preygel, Silva, 2011).

The coefficients $a_m^{(n)}$ satisfy the following properties:

1. $a_m^{(n)} = 0$ *for* $0 \le m < p^n$;
2. $a_m^{(n)} = 1$ *for* $m = p^n$;
3. *Suppose* $j \ge 0$. *Then,* p^j *divides* $a_m^{(n)}$ *for* $m > jp^n - j + 1$ *(and so,* $|a_m^{(n)}|_p \le 1/p^j$*).*

Mahler series

The following statement gives a description of 1-Lipschitz measure-preserving (respectively, of 1-Lipschitz ergodic) transformations on $\mathbb{Z}_p$.

Theorem (Anashin, 2009).

The function f defines a 1-Lipschitz measure-preserving transformation on $\mathbb{Z}_p$ whenever the following conditions hold simultaneously:

$$a_1 \not\equiv 0 \pmod{p};$$

$$a_m \equiv 0 \pmod{p^{\lfloor \log_p m \rfloor + 1}},\ m = 2, 3, \ldots$$

The function f defines a 1-Lipschitz ergodic transformation on $\mathbb{Z}_p$ whenever the following conditions hold simultaneously:

$$a_0 \not\equiv 0 \pmod{p};$$

$$a_1 \equiv 1 \pmod{p} \text{ for } p \text{ odd};$$

$$a_1 \equiv 1 \pmod{4} \text{ for } p = 2;$$

$$a_m \equiv 0 \pmod{p^{\lfloor \log_p (m+1) \rfloor + 1}},\ m = 1, 2, 3, \ldots$$

Moreover, in the case $p = 2$ these conditions are necessary.

Mahler series

The following statement gives a description of complex shift in terms of Mahler expansion.

Theorem (L.T., 2017).

A function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is a complex shift if and only if

$$|a_m|_p \leq p^{-\lfloor \log_{p^n} m \rfloor + 1},$$

where $n \in \mathbb{N}$, $m \geq 1$.

Measure-preservation and ergodicity in terms of Mahler expansion

Theorem (L.T., 2017).

A complex shift $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is measure-preserving whenever the following conditions hold simultaneously:

$$a_m \not\equiv 0 \pmod p \text{ for } m = p^n;$$

$$a_m \equiv 0 \pmod{p^{\lfloor \log_{p^n} m \rfloor}},\ m > p^n,$$

where $n \in \mathbb{N}$.

A complex shift $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is ergodic on $\mathbb{Z}_p$ whenever the following conditions hold simultaneously:

$$a_1 + a_2 + \ldots + a_{p^n-1} \equiv 0 \pmod p;$$

$$a_m \equiv 1 \pmod p \text{ for } m = p^n;$$

$$a_m \equiv 0 \pmod{p^{\lfloor \log_{p^n} m \rfloor}},\ m > p^n,$$

where $n \in \mathbb{N}$.

Maps of $\mathbb{Z}_p$ into $\mathbb{R}$

Let $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ be a complex shift, and let $E_k(f)$ be a set of all the following points $e_k^f(x)$ of Euclidean unit square $\mathbb{I}^2 = [0,1] \times [0,1] \subset \mathbb{R}^2$ for $k = 1, 2, 3, \ldots$:

$$e_k^f(x) = \Big(\frac{x \bmod p^k}{p^k}, \frac{f(x \bmod p^{n+k}) \bmod p^k}{p^k}\Big),$$

where $x \in \mathbb{Z}_p$, $n \in \mathbb{N}$. Note that $x \bmod p^{n+k}$ corresponds to the prefix of length $n+k$ of the infinite word $x \in \mathbb{Z}_p$, i.e., to the input word of length $n+k$ of the automaton $\mathfrak{C}^{(n)}$; while $f(x \bmod p^{n+k}) \bmod p^k$ corresponds to the respective output word of length k.

Maps of $\mathbb{Z}_p$ into $\mathbb{R}$

Let $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ be a complex shift, and let $E_k(f)$ be a set of all the following points $e_k^f(x)$ of Euclidean unit square $\mathbb{I}^2 = [0,1] \times [0,1] \subset \mathbb{R}^2$ for $k = 1, 2, 3, \ldots$:

$$e_k^f(x) = \Big(\frac{x \bmod p^k}{p^k}, \frac{f(x \bmod p^{n+k}) \bmod p^k}{p^k}\Big),$$

where $x \in \mathbb{Z}_p$, $n \in \mathbb{N}$.

Denote via *$\mathcal{E}(f)$ the closure of the set $E(f) = \bigcup_{k=1}^{\infty} E_k(f)$* in the topology of real plane $\mathbb{R}^2$. As $\mathcal{E}(f)$ is closed, it is measurable with respect to the Lebesgue measure on real plane $\mathbb{R}^2$. Let $\lambda(f)$ be the Lebesgue measure of $\mathcal{E}(f)$.

Theorem (L.T., 2018).

For a given complex shift $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ the closure $\mathcal{E}(f)$ is nowhere dense in $\mathbb{I}^2$, hence $\lambda(f) = 0$.

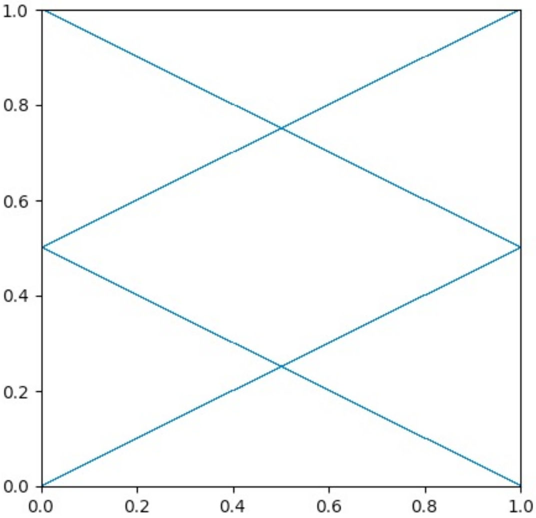


Figure: Example of complex shift, $n = 1$

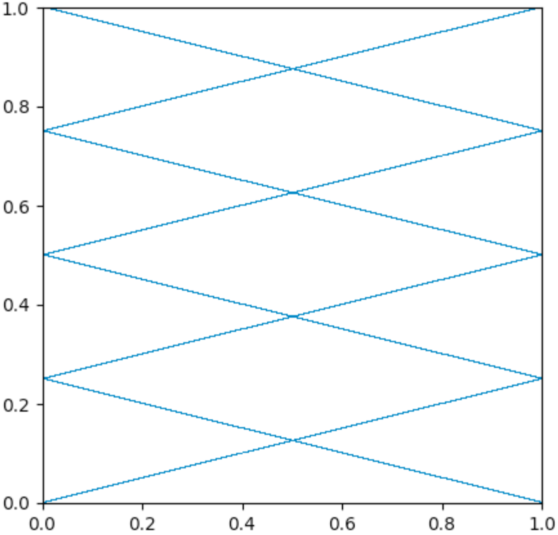


Figure: Example of complex shift, $n = 2$

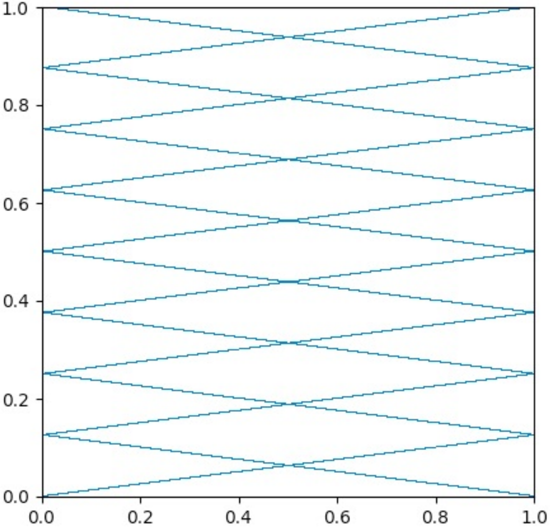


Figure: Example of complex shift, $n = 3$

Open problems

Problem 1 (Anashin). Consider the following map $g\colon x \mapsto \frac{x(x+1)}{2}$ with $x \in \{0, ..., 2^n - 1\}$. Calculate $x \mapsto g(x) \mod 2^n$. For all $n \in \mathbb{N}$ this is a permutation.
Does there exist a polynomial (or rational function) $f(x) \in \mathbb{Z}_2[x]$ such that $x \mapsto f(g(x)) \mod 2^n$ is a single cycle permutation for all n?
Motivation: (Woodcock-Smart 1998, Yurov 1998).

Problem 2 (Grigorchuk *et al.*). An important class of transformations of a Cantor set is represented by the homeomorphisms defined by finite automata, which called rational homeomorphisms. Examples of rational homeomorphisms are given by the adding machines and the Bernoulli shifts.
Give a topological and metric classification of rational homeomorphisms.

...

Open problems

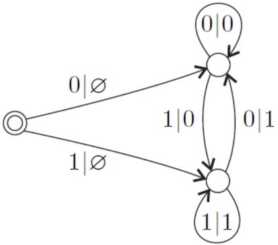
Problem 1 (Anashin). Consider the following map $g\colon x \mapsto \frac{x(x+1)}{2}$ with $x \in \{0, ..., 2^n - 1\}$. Calculate $x \mapsto g(x) \mod 2^n$. For all $n \in \mathbb{N}$ this is a permutation.
Does there exist a polynomial (or rational function) $f(x) \in \mathbb{Z}_2[x]$ such that $x \mapsto f(g(x)) \mod 2^n$ is a single cycle permutation for all n?
Motivation: (Woodcock-Smart 1998, Yurov 1998).

Problem 2 (Grigorchuk *et al.*). An important class of transformations of a Cantor set is represented by the homeomorphisms defined by finite automata, which called rational homeomorphisms. Examples of rational homeomorphisms are given by the adding machines and the Bernoulli shifts.
Give a topological and metric classification of rational homeomorphisms.

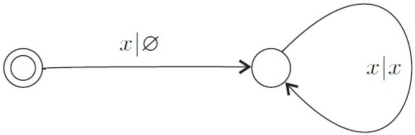
...

Thank you!

Asynchronous automaton



Unilateral shift


$x|\varnothing$
$x|x$