Dynamical Systems Generated by Mappings with Delay over the p-adic Integers

Livat B. Tyapaev (National Research Saratov State University)
TiapaevLB@info.sgu.ru

The automaton transformation of infinite words over alphabet $\mathbb{F}_p = \{0, 1, \dots, p-1\}$, where p prime number coincide with the continuous transformation of a ring of p-adic integers $\mathbb{Z}_p$. The object of this study is dynamical system associated with automata maps that is important for cryptography. We prove criterion of measure-preserving for an n-unit-delay mappings associated with asynchronous automata. Moreover, we give a sufficient condition of ergodicity of such mappings.

Keywords: p-adic integers, dynamical systems, n-unit delay mappings, measure-preserving maps, ergodic maps, automata.

Introduction

An automaton (letter–to–letter transducer) is tuple $\mathcal{A} = (\mathfrak{I}, \mathcal{S}, \mathcal{O}, S, O, s_0)$ where $\mathfrak{I}$ is an input alphabet, $\mathcal{S}$ is a set of states, $\mathcal{O}$ is an output alphabet, $S\colon \mathfrak{I} \times \mathcal{S} \to \mathcal{S}$ is a state update map, $O\colon \mathfrak{I} \times \mathcal{S} \to \mathcal{O}$ is an output map, $s_0 \in \mathcal{S}$ is an initial state. Note that $\mathfrak{I}, \mathcal{O}$ are finite alphabets, however $\mathcal{S}$ could be an infinite set of states.

Let's consider only accessible automata: where any state $s \in \mathcal{S}$ of automaton $\mathcal{A}$ is reachable from initial state s_0 after a finite input word u was fed to the automaton. We assume further that $\mathfrak{I} = \mathcal{O} = \mathbb{F}_p = \{0, 1, \dots, p-1\}$, where p is prime. We identify n-letter words over $\mathbb{F}_p$ with non-negative integers: Given an n-letter word $u = \alpha_{n-1} \dots \alpha_1 \alpha_0$, $\alpha_i \in \mathbb{F}_p$ for $i = 0, 1, 2, \dots, n-1$, we consider u as a base-p expansion of the number $\alpha_0 + \alpha_1 \cdot p + \dots + \alpha_{n-1} \cdot p^{n-1}$. In turn, the latter number can be considered as an element of the residue ring $\mathbb{Z}/p^n\mathbb{Z}$ modulo p^n. Thus, every automaton $\mathcal{A}$ the 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, every automaton $\mathcal{A}$ *defines a map $f_{\mathcal{A}}$ from ring of p-adic integers $\mathbb{Z}_p$ to itself*: Given an infinite word $\alpha = \dots \alpha_{n-1} \dots \alpha_1 \alpha_0$ (that is, an infinite sequence) over $\mathbb{F}_p$ we consider a p-adic integer x whose canonical expansion is $x = x(\alpha) = \alpha_0 + \alpha_1 \cdot p + \dots + \alpha_{n-1} \cdot p^{n-1} + \dots = \sum_{i=0}^{\infty} \delta_i(x) \cdot p^i$, where $\delta_i(x) \in \mathbb{F}_p$; so, by the definition, for every $x \in \mathbb{Z}_p$ we put $\delta_i(f_{\mathcal{A}}(x)) = O(\delta_i(x), s_i)$, $i = 0, 1, 2, \dots$ where

$s_i = S(\delta_{i-1}(x), s_{i-1})$, $i = 1, 2, \ldots$. We say then that map $f_{\mathcal{A}}$ is *automaton function* (or, automaton map) of the automaton $\mathcal{A}$.

The automaton function $f_{\mathcal{A}}\colon \mathbb{Z}_p \to \mathbb{Z}_p$ of the automaton $\mathcal{A}$ is 1-Lipschitz. Conversely, for every 1-Lipschitz function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ there exists an automaton $\mathcal{A} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, S, O, s_0)$ such that $f = f_{\mathcal{A}}$, see [1]. The automata functions were studied in context of metric and affine equivalence of geometrical images of automata, see [4–9]. A transitive families of such mappings by means of geometrical images were described in [10].

Dynamical systems

Dynamics is a mathematical science that studies action of a semigroup H on a phase space $\mathbb{S}$, which is a *measure* space: that is, $\mathbb{S}$ is endowed with a measure μ, and H acts on $\mathbb{S}$ by transformations that are measurable with respect to μ. A transformation $f\colon \mathbb{S} \to \mathbb{S}$ is said to be *measurable* whenever given a measurable subset $S \subset \mathbb{S}$, the pre-image $f^{-1}(S)$ is also measurable. Often it is additionally assumed that $\mathbb{S}$ is endowed also with a *metric* ρ, and that H acts by transformations that are *continuous* with respect to ρ.

We speak about *algebraic* dynamics whenever we additionally assume that space $\mathbb{S}$ is endowed not only with a metric and with a measure, but also with a certain *algebraic structure* (i.e., $\mathbb{S}$ is a universal algebra).

A *dynamical system* on a measuarable spase $\mathbb{S}$ 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. A dynamical system is also topological since configuration space $\mathbb{S}$ are not only measure space but also metric space, and corresponding transformation f are not only measurable but also continuous.

The *orbit*(or, the *trajectory*) of a piont x_0 of the dynamical system is a sequense

$$x_0 = f^0(x_0), x_1 = f(x_0), x_2 = f(x_1) = f^2(x_0) \ldots, x_i = f(x_{i-1}) = f^i(x_0), \ldots$$

of points of the space $\mathbb{S}$; that is, the orbit of the point x_0 is just sequence of iterates $(f^i(x_0))_{i=0}^{\infty}$. The point x_0 is called an *initial* point of the trajectory. A mapping $F\colon \mathbb{S} \to \mathbb{S}$ of measurable space $\mathbb{S}$ into a measurable space $\mathbb{Y}$ endowed with probabilistic measure μ and ν, respectively, is said to be *measure-preserving* whenever $\mu(F^{-1}(S)) = \nu(S)$ for each measurable subset $S \subseteq \mathbb{S}$. Also in this case once $\mathbb{S} = \mathbb{Y}$ and $\mu = \nu$ the measure μ is said to be *invariant* with respect to F (or simply invariant when it is clear from the context what F is meant). In the case when $\mathbb{S} = \mathbb{Y}$ and $\mu = \nu$, a measure-preserving map F is said to be *ergodic* if for each measurable subset S such that $F^{-1}(S) = S$ holds either $\mu(S) = 1$ or $\mu(S) = 0$. A measurable subset $S \subset \mathbb{S}$ is called *invariant subset* of the map $F : \mathbb{S} \to \mathbb{S}$ (or, F-*invariant*) if $F^{-1}(S) = S$; 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.

We can consider an automaton function $f \colon \mathbb{Z}_p \to \mathbb{Z}_p$ of the automaton $\mathcal{A} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, S, O, s_o)$ as an algebraic dynamical system on a mesuarable and a metric space $\mathbb{Z}_p$ of p-adic integers, which, actally, is a profinite algebra with the structure of an inverse limit: The ring $\mathbb{Z}_p$ is an inverse limit of residue rings $\mathbb{Z}/p^k\mathbb{Z}$, $k = 1, 2, 3 \ldots$. As any profinite algebra can be endowed with a metric and a measure, it is reasonable to ask what continuous with respect to the metric transformations are measure-preserving or ergodic with respect to the mentioned measure. Besides, the same question can be asked in the case of mappings for asynchronous automata.

Measure-preserving an n-unit delay mappings

An *asynchronous automaton (transducer)* is a 6-tuple

$$\mathcal{B} = (\mathfrak{I}, \mathcal{S}, \mathcal{O}, S, O, s_o),$$

where $\mathfrak{I}$, $\mathcal{O}$ are finite alphabets, $\mathcal{S}$ is a set of states, $S \colon \mathfrak{I} \times \mathcal{S} \to \mathcal{S}$ is the state update function, $O \colon \mathfrak{I} \times \mathcal{S} \to \mathcal{O}^*$ is output function, where $\mathcal{O}^*$ denotes the set of all finite strings over $\mathcal{O}$, and s_0 is the initial state. Denote $\mathfrak{I}^\infty$ and $\mathcal{O}^\infty$ the sets of all infinite sequences over $\mathfrak{I}$ (over $\mathcal{O}$, resp.).

We assume that an asynchronous transducer works in a framework of discrete time steps. The transducer reads one symbol at a time, changing its internal state and outputting a finite sequence of symbols at each step. Asynchronous transducers are a natural generalization of synchronous transducers, which are required to output exactly one symbol for every symbol read.

Let's define a function of special type for asynchronous transducer where input and output alphabets are same. Moreover, let's $\mathfrak{I} = \mathcal{O} = \mathbb{F}_p = \{0, 1, \dots p-1\}$. A mapping $f_{\mathcal{B}}\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is called *n-unit delay* whenever given an asynchronous transducer $\mathcal{B} = (\mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, S, O, s_0)$ traslated input string $\alpha = \dots \alpha_n \alpha_{n-1} \dots \alpha_1 \alpha_0$ (viewed as p-adic integer) into infinite output string $\beta = \dots \beta_{n+1} \beta_n$ (viewed as p-adic integer): So, that is

$$O(\delta_i(\alpha_{n-1} \dots \alpha_1 \alpha_0), s_i) = e,$$

where e is empty word, for $i = 0, 1, 2 \dots, n-1$, and

$$s_i = S(\delta_i(\alpha_{n-1} \dots \alpha_1 \alpha_0), s_{i-1}),$$

$i = 1, 2, \dots, n-1$.

An n-unit delay transducer is one that produces the some output n times unit later. Note that usually the term n-unit delay is used in a narrower meaning, cf. [3] when n-unit delay transducer is defined by fininite automaton, that is the initial state of the automaton, irrespective of the incomming letter, outputs an empty word, that transducer produces no output for the first n times slots; after that, the automaton outputs the incoming words without changes. Specifically, if the transducer reads as input a symbol $\delta_i(\alpha)$ at time i, it will produce this symbol as output at time $i+1$. At time $i = 0$, the transducer outputs nothing. For example, an *unilateral shift*, see e.g. [2], is defined by finite asynchronous automaton with unit-delay, in the narrow sense.

Theorem. *An n-unit delay mapping $f_{\mathcal{B}}\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is a continuous.*

The ring of p-adic integers $\mathbb{Z}_p$ can be endowed with a probability measure μ, e.g. normalized *Haar measure*: The base of the corresponding σ-algebra of measurable subsets of $\mathbb{Z}_p$, the elementary measurable subsets, are all balls of non-zero radii. 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.

Recall, that *open* (resp., *closed*) *ball* of radius ϵ centered at the point $a \in M$ in a metric space (M, ρ) is a set $B^-_\epsilon(a) = \{x \in M\colon \rho(x, a) < \epsilon\}$ (resp., $B_\epsilon(a) = \{x \in M\colon \rho(x, a) \le \epsilon\}$).

As the absolute value $|\cdot|_p$ may be only $p^{-\ell}$ for some $\ell \in \mathbb{N} \bigcup \{0\}$, for p-adic balls (i.e., for balls of field $\mathbb{Q}_p$ of p-adic numbers) we see that $B^-_{p^{-\ell}}(a) = B_{p^{-\ell}}(a)$. We put $\mu(B_{p^{-\ell}}(a)) = p^{-\ell}$.

Let F_k be a reduction of function f modulo $p^{n\cdot(k-1)}$ on the elements of the ring $\mathbb{Z}/p^{n\cdot k}\mathbb{Z}$ for $k = 2, 3, \ldots$.

Theorem *An n-unit delay 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-pre-images of the point $x \in \mathbb{Z}/p^{n\cdot(k-1)}\mathbb{Z}$ is equal p^n, $k = 2, 3, \ldots$.*

A point $x_0 \in \mathbb{Z}_p$ is said to be a *periodic point* if there exists $r \in \mathbb{N}$ such that $f^r(x_0) = x_0$. The least r with this property is called the *length* of period of x_0. If x_0 has period r, it is called an *r-periodic point.* The orbit of an r-periodic point x_0 is $\{x_0, x_1, \ldots, x_{r-1}\}$, where $x_j = f^j(x_0)$, $0 \le j \le r - 1$. This orbit is called an *r-cycle.*

Let $\gamma(k)$ be an $r(k)$-cycle $\{x_0, x_1, \ldots, x_{r(k)-1}\}$, where

$$x_j = (f \mod p^{k\cdot n})^j(x_0),$$

$0 \le j \le r(k) - 1$, $k = 1, 2, 3, \ldots$.

Theorem. *A measure-preserving an n-unit delay mapping $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is ergodic if a $\gamma(k)$ is an unique cycle, for all $k \in \mathbb{N}$.*

References

1. V. Anashin and A. Khrennikov. Applied Algebraic Dynamics. volume 49 of de Gruyter Expositions in Mathematics. Walter de Gruyter GmbH & Co., Berlin–N.Y., 2009

2. R. I. Grigorchuk, V. V. Nekrashevich, and V. I. Sushchanskii. Automata, dynamical systems,and groups. Proc. Steklov Institute Math., 231:128—203, 2000.

3. P. Linz. An Introduction to Formal Languages and Automata. Jones and Bartlett Learning, 5th edition, 2011.

4. L. B. Tyapaev. The geometrical model of behavior of automata and their indistinguishability. Mathematics, Mechanics, Mathematical Cybernetics, Saratov Univ. Press, pages 139–143, 1999. (in Russian).

5. L. B. Tyapaev. Solution of some problems for finite automata based on the analysis of their behavior. Izv. Sarat. Univ. (N.S.), Ser. Mat. Mekh. Inform., 6(2):121–133, 2006. (in Russian).

6. L. B. Tyapaev. Geometrical images of automata and dynamical systems. Workshop on Discrete Mathematics and Applications. Moscow State University. Faculty of Mechanics and Mathematics, pages 510–513, 2010. (in Russian).

7. L. B. Tyapaev, D. V. Vasilenko, M. V. Karandashov. Discrete dynamical systems defined geometrical images of automata. Izv. Sarat. Univ.

(N.S.), Ser. Mat. Mekh. Inform., 13(2-2):73–78, 2013. (in Russian).

8. L. B. Tyapaev, D. V. Vasilenko. Discrete dynamical systems over geometrical images of automata. Intel. Systems, 17(1-4):196–201, 2013.

9. L. B. Tyapaev, D. O. Matov Bases of geometrical images for dynamical systems defined by some classes of automata. In Computer Science and Information Technologies. Proceedings of the Int'l Conference (Saratov, July, 2009), pages 201–204, Saratov State University, Saratov Univ. Press, 2009. (in Russian).

10. L. B. Tyapaev. Transitive families of automata mappings. In V. B. Alekseev, D. S. Romanov, B. R. Danilov, editors, Discrete models in the theory of control systems. Proceedings of the 9th Int'l Conference (Mocsow, May, 2015), pages 244–247, Moscow State Univesity, Maks Press, 2015. (in Russian).