Automata as $p$-Adic Dynamical Systems

Livat B. Tyapaev

e-mail: TiapaevLB@info.sgu.ru

National Research Saratov State University

Abstract

The automaton transformation of infinite words over alphabet $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$, where $p$ is a prime number, coincide with the continuous transformation (with respect to the $p$-adic metric) of a ring $\mathbb{Z}_p$ of $p$-adic integers. The objects of the study are non-Archimedean dynamical systems generated by automata mappings on the space $\mathbb{Z}_p$. Measure-preservation (with the respect to the Haar measure) and ergodicity of such dynamical systems plays an important role in cryptography (e.g. for pseudo-random generators and stream cyphers design). The possibility to use $p$-adic methods and geometrical images of automata allows to characterize of a transitive (or, ergodic) automata. We investigate a measure-preserving and ergodic mappings associated with synchronous and asynchronous automata. We have got criterion of measure-preservation for an $n$-unit delay mappings associated with asynchronous automata. Moreover, we have got a sufficient condition of ergodicity of such mappings.

Key words: $p$-adic integers, automata, transitivity, geometrical images of automata, $p$-adic dynamical systems, $n$-unit delay mappings, measure-preserving maps, ergodic maps.

1 Introduction

Speaking about a (synchronous) automaton $\mathfrak{A}$, we always understand the letter-to-letter transducer (not necessarily with a finite number of states) with fixed initial state. Input and output alphabets $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ of an automaton consist of $p$ symbols, where $p$ is a prime number. The automaton naturally defines the mapping of the set $\mathbb{Z}_p$ of all (one-sided) infinite sequences in $\mathbb{Z}_p$. As is known, such maps are called deterministic functions (or, automata functions). The set $\mathbb{Z}_p$ is naturally endowed with the structure of the ring of a $p$-adic integers, i.e. turn into the metric space by specifying the metric $|a - b|_p$, $a, b \in \mathbb{Z}_p$, where $| \cdot |_p$ is the $p$-adic (that is, non-Archimedean) norm. All deterministic functions $f : \mathbb{Z}_p \to \mathbb{Z}_p$ satisfy the $p$-adic Lipschitz condition with constant 1, i.e. $|f(a) - f(b)|_p \leq |a - b|_p$ for all $a, b \in \mathbb{Z}_p$, see [1]. In particular, all deterministic functions are continuous with respect to the $p$-adic metric. For example, all functions defined by polynomials with $p$-adic integers coefficients (in particular, rational integers) are deterministic. Note, that in the case of $p = 2$, the standard processor commands, such as AND, OR, XOR, NOT, etc. naturally extend to functions from $\mathbb{Z}_2 \times \mathbb{Z}_2$ in $\mathbb{Z}_2$. Hence, in particular, it follows that all functions obtained with the compositions of arithmetic and coordinate-wise logical operations of the processor can be considered as 2-adic deterministic functions. By
the above, $p$-adic analysis can prove to be a very effective “analytical” tool for research the properties of deterministic functions and the behavior of automata.

\section{Transitivity of automata}

We consider only automata, where every state $s$ from the set $\mathcal{S}$ of all internal states of an automaton is accessible from the initial state $s_0$, that is, the automaton will pass from $s_0$ to $s$ by reading of some finite input word. Every automaton $\mathfrak{A}$ defines a family of automata $\mathfrak{A}_s$, where $\mathfrak{A}_s$ differs from $\mathfrak{A}$ only in that it has a different initial state, $s$ instead of $s_0$. An automaton $\mathfrak{A}$ is said to be \textit{transitive} (or, \textit{ergodic}) if the family of deterministic functions defined by the family of automata $\mathfrak{A}_s$, $s \in \mathcal{S}$ is transitive on every set $\mathbb{Z}/p^n\mathbb{Z}$ for all $n = 1, 2, \ldots$ (that is, for all finite words $u$ and $v$ of the same length there exists an automaton $\mathfrak{A}_s$ that transforms $u$ into $v$). We associate the automaton $\mathfrak{A}$ with the closure $\mathcal{E}_\mathfrak{A}$ of all points of the form $(\frac{c}{p^m}, \frac{d}{p^n}) \in [0, 1] \times [0, 1]$ in the topology of the Euclidean plane, where $u$ is the input word of length $n$, and $v$ is the corresponding output word, $n = 1, 2, \ldots$. The set $\mathcal{E}_\mathfrak{A}$ is measurable with respect to the Lebesgue measure $\lambda$. The following “law 0-1” holds: \textit{for any automaton $\mathfrak{A}$, $\lambda(\mathcal{E}_\mathfrak{A}) = 0$ or $\lambda(\mathcal{E}_\mathfrak{A}) = 1$. Moreover, $\lambda(\mathcal{E}_\mathfrak{A}) = 1$ if and only if $\mathfrak{A}$ is transitive, see [1].}

Let us enumerate symbols $\alpha_i$ of the alphabet $\mathbb{F}_p$ by natural numbers $c(\alpha_i) \in \{1, 2, \ldots p\}$, and we associate with the word $u = \alpha_{k-1} \ldots \alpha_1 \alpha_0$ over the alphabet $\mathbb{F}_p$ the rational number $\overline{u} = c(\alpha_0)+c(\alpha_1)\cdot(p+1)^{-1}+\ldots+c(\alpha_{k-1})\cdot(p+1)^{-(k-1)}$. We consider all points of the Euclidean square $[1, p+1] \times [1, p+1] \subset \mathbb{R}^2$ of the form $(\overline{u}, f(\overline{u}))$, where $u$ runs through all finite words over $\mathbb{F}_p$. The set of these points $\Omega(\mathfrak{A})$ is called a \textit{geometrical image} (or, \textit{graph}) of an automaton $\mathfrak{A}$, see [4] [5]. For every state $s \in \mathcal{S}$ of an automaton $\mathfrak{A}$ we associate a map $R_s: \mathbb{F}_p \to \mathbb{F}_p$ that transforms input symbol into output symbol. If we consider an automaton $\mathfrak{A}$ and the family $\{R_s: s \in \mathcal{S}\}$, then a correspondence for every state $s \in \mathcal{S}$ of a some map $R_s$ creates a new automaton $\mathcal{B}$ (and a set $K(\mathfrak{A})$ of an automata that is constructed this way). \textit{Then automaton $\mathfrak{A}$ is transitive if and only if there exists the automaton $\mathcal{B} \in K(\mathfrak{A})$ and such a geometrical images $\Omega(\mathfrak{A})$, $\Omega(\mathcal{B})$, that are affine equivalents} [6] [8].

\section{Dynamical systems}

A \textit{dynamical system} on a measurable space $\mathcal{S}$ is understood as a triple $(\mathcal{S}, \mu, f)$, where $\mathcal{S}$ is a set endowed with a measure $\mu$, and $f: \mathcal{S} \to \mathcal{S}$ is a measurable function. A dynamical system is also topological since configuration space $\mathcal{S}$ are not only measurable space but also metric space, and corresponding transformation $f$ are not only measurable but also continuous.

We consider a $p$-adic dynamical system $(\mathbb{Z}_p, \mu_p, f)$ [2]. The space $\mathbb{Z}_p$ is equipped with a natural probability measure, namely, the Haar measure $\mu_p$ normalized so that $\mu_p(\mathbb{Z}_p) = 1$. Balls $B_{p^{-k}}(a)$ of nonzero radii constitute the base of the corresponding $\sigma$-algebra of measurable subsets, $\mu_p(B_{p^{-k}}(a)) = p^{-k}$.
A measurable mapping \( f: \mathbb{Z}_p \to \mathbb{Z}_p \) is called measure-preserving if \( \mu_p(f^{-1}(S)) = \mu_p(S) \) for each measurable subset \( S \subseteq \mathbb{Z}_p \). 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.

We can consider an automaton function \( f: \mathbb{Z}_p \to \mathbb{Z}_p \) as an algebraic dynamical system on a measurable and a metric space \( \mathbb{Z}_p \) of \( p \)-adic integers, which, actually, 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.

4 Measure-preserving and ergodic an \( n \)-unit delay mappings

We assume that an asynchronous automaton (letter-to-word transducer) \( C \) 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 generalizations of synchronous transducers, which are required to output exactly one symbol for every symbol read. A mapping \( f_C: \mathbb{Z}_p \to \mathbb{Z}_p \) is called \( n \)-unit delay whenever given an asynchronous automaton \( C \) translated infinite input string \( \alpha = \ldots \alpha_n\alpha_{n-1} \ldots \alpha_1\alpha_0 \) (viewed as \( p \)-adic integer) into infinite output string \( \beta = \ldots \beta_{n+1}\beta_n \) (viewed as \( p \)-adic integer). An \( n \)-unit delay transducer 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 finite automaton, that produces no output for the first \( n \) times slots; after that, the automaton outputs the incoming words without changes. An \( n \)-unit delay mapping \( f_C: \mathbb{Z}_p \to \mathbb{Z}_p \) is continuous on \( \mathbb{Z}_p \) [8].

Let \( F_k \) be a reduction of function \( f \) modulo \( p^\alpha k \mathbb{Z} \) on the elements of the ring \( \mathbb{Z}/p^\alpha k \mathbb{Z} \) for \( k = 2, 3, \ldots \). The following criterion of measure-preservation for \( n \)-unit delay mappings is valid: An \( n \)-unit delay mapping \( f: \mathbb{Z}_p \to \mathbb{Z}_p \) preserves the measure if and only if the number \( \# F_k^{-1}(x) \) of \( F_k \)-pre-images of the point \( x \in \mathbb{Z}/p^\alpha k \mathbb{Z} \) is equal \( p^\alpha \), \( k = 2, 3, \ldots \) [7, 8].

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 a \( r \)-periodic point \( x_0 \) is \( \{x_0, x_1, \ldots, x_{r-1}\} \), where \( x_j = f^j(x_0), 0 \leq j \leq r - 1 \). 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

\[
x_j = (f \mod p^k)^j(x_0),
\]
\[0 \leq j \leq r(k) - 1, \ k = 1, 2, 3, \ldots\] The following condition of ergodicity holds: A measure-preserving an \(n\)-unit delay mapping \(f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p\) is ergodic if \(\gamma(k)\) is an unique cycle, for all \(k \in \mathbb{N}\) [9].

References

[1] V. Anashin and A. Khrennikov, *Applied Algebraic Dynamics*, de Gruyter Expositions in Mathematics (de Gruyter GmbH & Co., Berlin–N.Y., 2009).

[2] V. Anashin, “Ergodic transformations in the space of \(p\)-adic integers,” Proc. Int. Conf. on \(p\)-adic Mathematical Physics, AIP Conference Proceedings 826, 3–24 (2006).

[3] R. I. Grigorchuk, V. V. Nekrashevich, and V. I. Sushchanskii, “Automata, dynamical systems, and groups,” Proc. Steklov Math. Inst. 231, 128–203 (2000).

[4] L. B. Tyapaev, “The geometrical model of behavior of automata and their indistinguishability,” Mathematics, Mechanics 1, 139-143 (1999) [in Russian].

[5] L. B. Tyapaev, “Solving some problems of automata behaviour analysis,” Izv. Saratov Univ. (N.S.), Ser. Math. Mech. Inform. 6:1-2, 121-133 (2006).

[6] L. B. Tyapaev, “Transitive families of automata mappings,” in *Proceedings of the 9th International Conference on Discrete Models in the Theory of Control Systems* (May 20-22 2015, Moscow), eds. V. B. Alekseev, D. S. Romanov, B. R. Danilov, 244-247 (Lomonosov Moscow State University, Maks Press, 2015) [in Russian].

[7] L.B. Tyapaev, “Measure-preserving and ergodic asynchronous automata mappings,” in *Proceedings of the 12th International Workshop on Discrete Mathematics and its Applications* (June 20-26 2016, Moscow), edited by O.M. Kasim-Zade, 398-400 (published by Faculty of Mechanics and Mathematics, Lomonosov Moscow State University, 2016) [in Russian].

[8] L.B. Tyapaev, “Transitive families and measure-preserving an \(n\)-unit delay mappings,” in *Proceedings of the International Conference on Computer Science and Information Technologies* (June 30-July 2 2016, Saratov), 425-429 (Publishing Center Nauka, Saratov, 2016).

[9] L.B. Tyapaev, “Ergodic automata mappings with delay,” in *Proceedings of the International Conference on Problems of theoretical cybernetics* (June 19-23 2017, Penza), edited by Yu. I. Zhuravlev, 242-244, (Moscow, Maks Press, 2017) [in Russian].