FACTA UNIVERSITATIS
Series: **Physics, Chemistry and Technology** Vol. 14, N° 3, Special Issue, 2016, pp. 143 – 196
DOI: 10.2298/FUPCT1603143A

DISCRETENESS CAUSES WAVES †

UDC 535.145:519.1:519.7/.8

Vladimir S. Anashin*

Faculty of Computational Mathematics and Cybernetics,
Lomonosov Moscow State University, Moscow, Russia

Abstract. *In the paper, we show that matter waves can be derived from discreteness and causality. Namely we show that matter waves can naturally be ascribed to finite discrete causal systems, the Mealy automata having binary input/output which are bit sequences. If assign real numerical values ('measured quantities') to bit sequences, the waves arise as a correspondence between the numerical values of input sequences ('impacts') and output sequences ('system-evoked responses'). We show that among all discrete causal systems with arbitrary (not necessarily binary) inputs/outputs, only the ones with binary input/output can be ascribed to matter waves* $\psi(x,t) = e^{i(kx-\omega t)}$.

Key words: *matter waves, finite discrete causal systems, binary bit sequences*

To Professor Branko Dragovich on the occasion of his 70-th birthday

1. Introduction

Since 1980's, there can be observed a steadily strengthening belief among physicists that information-theoretic approach may play a crucial role in finding natural explanations of the origin of physical laws, especially in quantum mechanics, see e.g. [7] for discussion and references. Note that within this approach the very notion of information is understood by different authors in different meanings (even leaving apart specific and rapidly developing area of so-called quantum information). For

Received April 15^{th}, 2016; accepted June 6^{th}, 2016.
†**Acknowledgement:** The author was supported by Russian Foundation for Basic Research grant No 16-01-00470-a
***E-mail:** anashin@iisi.msu.ru; vladimir.anashin@u-picardie.fr

instance, some of the authors consider Fisher information (which is mathematically equivalent to Shannon's information) as a basis for physically meaningful conclusions, see e.g. [20], some insist that Shannon's information can not be applied for these purposes and other concept of information should be used in physics (or at least in quantum theory), see e.g. [61]. We refer to [9] for various definitions of information and applications in numerous sciences including physics. Numerous works are aimed to give a so-called informational interpretation of quantum mechanics (QM), i.e. to derive (or to explain) the laws of QM on informational base (note that within that approach information is usually considered as a physical entity, see e.g. [38]). Some of that works are developing an approach which can be judged as a 'calculating Universe'; in these works evolution of Universe (at some level) is considered like information processing, i.e. as if a certain program is being performed on a computer, see e.g. [62, 44]. Some other works are developing an approach which is called 'discrete physics' or 'digital physics'. The leading idea of that approach is to explain laws of evolution of a physical, especially quantum, system (which are usually represented as continuous functions over real or complex numbers) via some 'discrete' transformations of some 'discrete' structures. For instance, [27] claims that at a deeper level functions defined on integers only are capable to describe evolution of a physical system. Moreover, some authors develop what they are calling a 'bit-stream physics', see e.g. [6, 47, 48]. In that works it is assumed that interactions of physical systems can be reduced to (and explained via) exchange of bits, elementary two-state entities, or *urs* in terminology of [55]. The most general idea of that approach may be called 'it from bit' concept, following J. A. Wheeler who wrote (see [59]):

> 'It from bit' symbolizes the idea that every item of the physical world has at bottom — a very deep bottom, in most instances — an immaterial source and explanation; that which we call reality arises in the last analysis from the posing of yes-no questions and the registering of equipment-evoked responses; in short, that all things physical are information-theoretic in origin and that this is a participatory universe.

We stress that most works which belong to 'digital physics' are based on common assumptions which follow:

- at a deep level, Universe consists of discrete entities, and
- laws of its evolution are discrete and causal.

For instance, D. R. Finkelstein in his monograph [19] considers quantum world as a spacetime net, what he calls a 'causal spacetime network'; and G. 't Hooft develops a cellular automata approach in a series of works, see e.g. [28, 25, 26, 27].

In current paper, we are going to derive some physically meaningful expressions (mainly, of waves) from the above mentioned basic assumptions, discreteness and causality. Our basic model for causality is also an automaton; but contrasting to 't

Hooft's approach, we are consider Mealy automata rather than cellular automata. And this is a crucial difference which needs some extra explanations.

Mealy automaton may be thought of as transducer which transforms input discrete signal (i.e., a sequence of $\ldots\xi_2\xi_1\xi_0$ which consists of 'pulses' α_i taking discrete values which we enumerate via $0, 1, \ldots, p-1$) into output discrete signal. Automaton has a finite number of internal states; every input α_i switches the automaton to some other state and the automaton outputs γ_i which also takes values enumerated via $0, 1, \ldots, q-1$. At the moment $t = 0$, when the automaton is assumed to be in the initial state s_0, the automaton absorbs 'input pulse' ξ_0, goes to a new state s_1 which depends on the value of α_0 and produces 'output pulse' χ_0 whose value depends only of α_0 and s_0. At the moment $t = 1$ the automaton (which is now at the state $s_1 = s(s_0, \xi_0)$) absorbs ξ_1, goes to the state $s_2 = s(s_1, \xi_1)$, produces $\chi_1 = \chi(s_1, \xi_1)$, etc. The automaton is said to be *autonomous* if both state update and output do not depend on input; that is, $s_{j+1} = s(s_j)$, $\chi_j = \chi(s_j)$, for all $j = 0, 1, 2, \ldots$. Compared to Mealy automata, cellular automata are autonomous automata with no output but with a possibly infinite number of states. Therefore cellular automata models focus on evolution of a system 'by itself', in accordance with prescribed laws, whereas *our approach, which is based on Mealy automata, is aimed at modelling of a process of interaction of an observer with a physical system during measurements.*

Automata considered further in the paper are actually 'black boxes' of which we only know that they can be in a finite number of states and every measurement somehow changes a state the automaton has been in before the measurement. Under a measurement we mean a comparison of input signal (impact) with output signal (response): To every sequence $x = \ldots\xi_2\xi_1\xi_0$ of 'pulses' ξ_j we associate some numerical value $v(x)$ (assuming that every signal represented by the sequence can be measured with a certain accuracy); then having corresponding output sequence $y = \ldots\chi_2\chi_1\chi_0$ we associate to that single measurement a point $(v(x); v(y))$ on the real plane. We assume also that before every such measurement a system is prepared in some fixed state which we associate to the initial state s_0 of the automaton. Numerous measurements therefore give us a number of points on a real plane; by studying cluster points we then try to guess the law the system transfers input signals to output ones. This way we are modelling a process of measurements of a physical system when experimenter obtains an experimental curve which is (usually) assumed to be a smooth curve giving the best approximation of the cluster points. This is a *model of how numerical data obtained during a physical experiment are usually processed.* We stress once again that we are not aware of what 'really happens inside' a system during measurements, we only expose a system to impacts and watch for responses of the system. This drastically differs our approach from the G. 't Hooft's one which is based on cellular automata as models of evolution of a physical systems on a deep level.

Note however that both models, ours and 't Hooft's, are *causal*, i.e., *completely deterministic.* That is, depending on type of a model, the next state of a system is uniquely determined by previous state of the cellular automaton or, respectively, by the previous state and current input of Mealy automaton. Moreover, both these models are *discrete*; both assume a fundamental role of discreteness at the Planck scale. Finally, either of the models nonetheless has a 'real image',i.e., corresponding model that is based on real numbers. That is, both of these two models lead to models which are common for the world of human perception.

But compared to models based on cellular automata, models based on Mealy automata are *finite*, and as we will see further namely the finiteness of the number of states plays a crucial role in our conclusions about the 'real image' of the model. It turns out that *'real image' of Mealy automaton exhibit 'wave properties'* and is *not deterministic* any more. Namely, we will see that the 'real image' looks like a collection of wave functions $\psi_j(x,t) = e^{i(k_j x - \omega_j t)}$ $(j = 1, 2, \ldots, N)$ of free particles; but this happens *only when* there are *exactly two distinct values* the 'pulses' (which constitute input impact and output response) may have. Therefore the 'pulses' can naturally be associated to bits; so this is why we may say that *particular 'its', the waves, are 'from bits' indeed.*

In our model, we associate a real value $v(a)$ to the n-tuple $a = \alpha_{n-1}\ldots\alpha_2\alpha_1\alpha_0$ (where α_j , $j = 0, 1, 2, \ldots$, only take p distinct values) as follows.

Firstly without loss of generality we may assume that the values a 'pulse' α_j takes are $0, 1, \ldots, p-1$; that is, we just enumerate distinct values a 'pulse' may take by $0, 1, \ldots, p-1$.

Secondly, the value $v(a)$ must reflect time order the 'pulses' of the tuple a are absorbed/emitted by a system since every input 'pulse' (impact) forces the system to change its current state to a new one and every output 'pulse' (response) depends on the current state and on the input 'pulse'. Therefore we must assign some 'weight' to every position j of the tuple to make the $(j+1)$-st place 'heavier' than the j-th one. It is clear then the weight must be just a non-decreasing function of j. We will assume that every $(j+1)$-st position is 'β times heavier' than the j-th one, where $\beta > 1$ is a real number.

Finally, it is convenient to have all values normalized so that for every tuple a of arbitrary length n its value $v(a)$ lies in some real interval $[c, d]$. Without loss of generality we may assume that $v(a) \in [0, d]$ for all $n = 1, 2, 3, \ldots$ and all tuples $a = \alpha_{n-1}\ldots\alpha_2\alpha_1\alpha_0$. Having all this in mind, we put therefore

$$v(a) = \alpha_{n-1}\beta^{-1} + \alpha_{n-1}\beta^{-2} + \cdots + \alpha_2\beta^{-n+2} + \alpha_1\beta^{-n-1} + \alpha_0\beta^{-n}. \qquad (1)$$

That is, speaking loosely, we just associate a real number $v(a)$ whose base-β expansion is $0.\alpha_{n-1}\ldots\alpha_2\alpha_1\alpha_0$ to the n-tuple $a = \alpha_{n-1}\ldots\alpha_2\alpha_1\alpha_0$. For instance, if $\beta = p$ then $0 \le v(a) < 1$. Thus we just read the sequence of 'pulses' as a sequence of digits, *the latest (i.e., leftmost) 'pulses' correspond to digits of highest order.* That order is important since we assume that *'pulses' follow one after another very quickly, within time interval which is out of accuracy of measurements*; for instance, the next 'pulse' happens exactly after a Planck time after the preceding 'pulse'. This implies that lower order digits are out of accuracy of measurements; that is, *during a measurement the value $v(a)$ can be measured only within a certain accuracy*;

normally we can not get exact value $v(a)$ from measurements, but only some approximation, and only when the sequence a is long enough. For instance, if assume that a 'pulse' after a 'pulse' follows exactly after Planck time τ elapses, than taking into the account that $\tau \approx 10^{-43}$ sec and that the shortest measured time interval (as of 2010, see [36]) is $\approx 10^{-18}$ then the number n of 'pulses' in n-tuple a should be assumed to be greater than 10^{25}; i.e., *sequences which are that long only* constitute 'measured data' that determine cluster points among all points $(v(a); v(a')) \in \mathbb{I}^2$ in the unit[1] real square $\mathbb{I}^2 = [0,1] \times [0,1]$ where n-tuples a are input 'impacts' and n-tuples a' are corresponding 'responses' of the system. *The set of all points* $(v(a); v(a'))$ *can therefore be treated as the set of 'experimental points' obtained by measurement of impacts and responses of the system.* We focus on that set in the paper.

Note that the rule (1) according to which we assign a real number to a sequence of 'pulses' is a model of a standard process of assigning numerical value to a physical quantity: For instance, distances can be measured in femtometers, picometers, micrometers, millimeters, decimeters, meters, kilometers, etc., which are linear units in base 10. But if one measures a distance between two milestones, there is no need (and practically impossible) to do this within accuracy up to micrometers, not speaking of femtometers and picometers. So *rule* (1) *is just a reasonable model for standard common rule of 'figuring out' numerical results of a measurement, after a proper normalization.*

Note that we do not demand the base b to be an integer though the case $b = p$ will be a basic one in further considerations. Actually to derive the expression $\psi(x,t) = e^{i(kx-\omega t)}$ for a wavefunction, where t is *real* time, we will have to assume that $b = 1 + \tau$ for $0 < \tau \ll 1$. Namely *we will show that* $b = 1 + \tau$ *with* $0 < \tau \ll 1$ *is the only possible value for* b *when a discrete causal system, Mealy automaton, 'produces' wavefunctions* $\psi(x,t) = e^{i(kx-\omega t)}$ *with a real time* t*. Moreover, namely that value of* b *immediately implies that the 'pulses' can take only two possible values and so the 'pulses' can naturally be associated to bits*; see Subsections 6.2.–6.3. for details.

This conclusion implies some important consequences.

- Most likely, in p-adic mathematical physics it is reasonable (at least for models on Planckian scales) assume that $p = 2$; so at that level the p-adic physics is just the 2-adic physics. On the p-adic mathematical physics reader is referred to comprehensive monograph [54] by V. S. Vladimirov, I. V. Volovich, and E. I. Zelenov and expository paper [15].

- Being considered w.r.t. 2-adic metric, Mealy automata just perform continuous (actually, 1-Lipschitz) mappings, see e.g. [3]; and since it is usually assumed that a dynamical system which corresponds to a physical system must preserve volume, from this assumption it can be derived that discrete time can uniquely be expanded to continuous time, however, not w.r.t real

[1]For convenience, we normalize numerical values $v(a)$ of tuples a so that $v(a) \in [0,1]$

metric but w.r.t. 2-adic metric, [5, Subsection 4.8.1, Proposition 4.90]. We note that to our best knowledge the p-adic time was initially introduced by B. Dragovich and his co-workers, see e.g. [14].

- All the said volume-preserving dynamical systems then are just isometries w.r.t. 2-adic metric and thus they are invertible [5, Subsection 4.4.1]; therefore reversibility of a system just follows from volume-preservation in our model.

- It is proved that no smooth curves other than waves can be obtained as experimental curves of best approximation of cluster points of Mealy automata maps; actually it is proved that the only class smooth functions which can be calculated on Mealy automata are affine functions, and that might be a deeper reason for the linearity of mathematical formalism of quantum mechanics. The latter question was discussed by A. Khrennikov in a series of papers on the so-called Prequantum Classical Statistical Field theory, see e.g. [32, 31].

- Although our black-box models are strictly deterministic rather than probabilistic, randomness arises with necessity due to the limited accuracy of measurements; that is, since each wave function $\psi(x,t)=e^{i(kx-\omega t)}$ can be assigned to a quantum state of a system, the system will fall in each of that states with certain probabilities that depend on 'internal' (i.e., unknown) structure of Mealy automaton which corresponds to the system, and these probabilities can be estimated in the course of measurements.

- The case $\beta=1$ corresponds to classical rather than quantum systems since this implies that no smallest measurable time interval like Planck time exists and arbitrarily small time intervals can be measured; in the latter case by sending $\tau\to 0$ we show that, speaking loosely, our models correspond to solid bodies rather than to waves.

All the issues from the above list are discussed in Section 6.

We stress that models we consider further in the paper correspond to the case when during a single measurement the number of impacts ('pulses' in a sequence) a system is exposed to is much bigger than the number of states of the system; each input 'pulse' forces the system to change its state to another one; that new state (as well as response of the system) depends only on the preceding state and on the value of the impact. Under these conditions, numerical simulations produce pictures which are very much alike to that of interference pattern from the double slit experiment, cf. Figures 1–2 and Figure 5.

The paper is organized as follows:

- In Section 2. we introduce mathematical notions and results (mainly from automata theory and p-adic numbers) which are needed for description of our model.

- In Section 5. we state main mathematical results which constitute mathematical description of the model.

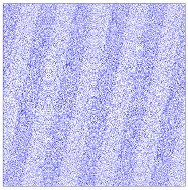

FIGURE 1: Approximate plot of an automaton at word length 16

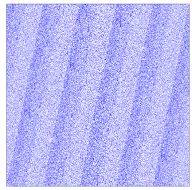

FIGURE 2: Approximate plot of the same automaton at word length 17

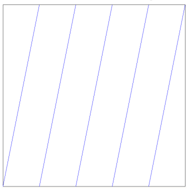

FIGURE 3: Cluster points of the plot of the same automaton

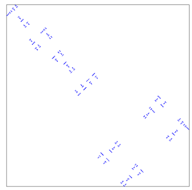

FIGURE 4: Monna graph of the same automaton

- In Section 6. we discuss possible physical interpretations of the model.

The paper is an extended version of the talk given by the author at the International Conference on p-adic mathematical physics and its applications (Belgrade, 7–12 September, 2015). The paper contains no (but few) proofs of mathematical results; for complete proofs reader is referred to [4].

Finishing introduction, we would like to make a remark about motivation of the research. Initially, the research was motivated by the need to explain empirical data obtained during intensive computer experiments with automata which represented various cryptographic primitives. Transformations performed by the automata where visualised, namely, represented by points of the unit square $\mathbb{I}^2 = [0,1] \times [0,1]$ in real plane $\mathbb{R}^2$ so that coordinates of the points relate numerical (radix) representations $0.\alpha_{N-1} \ldots \alpha_1$ of input words $\alpha_{N-1} \cdots \alpha_1 \alpha_0$ to the numerical representations of corresponding output words. It was noticed that once input words were taken sufficiently long compared to the number of states of the modelled system, some 'linear structures' may appear in the graph, cf. Figures 1–2, but more complicated structures like smooth curves of higher order had never been observed in that case although at shorter lengths the graphs may exhibit some 'smooth curve looking structures' (like the ones at Figure 6) which however disappear once input words become sufficiently long, cf. Figure 7. A particular goal of research was therefore to give mathematical explanation of the phenomenon and to characterize these 'linear structures'.

But during the research it became evident that the problem (which actually is a question what smooth real functions can be modelled on finite automata) has

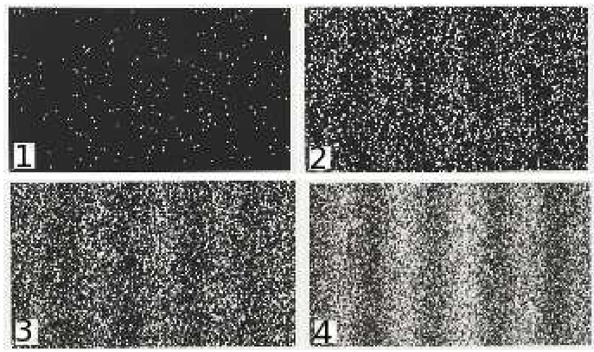

FIGURE 5: Interference pattern of the double slit experiment (from Wikimedia Commons, the free media repository http://commons.wikimedia.org/wiki/File:Double-slit experiment results Tanamura four.jpg)

applications not only to cryptography (see e.g. [5, Chapter 11]) but also may be related to mathematical formalism of quantum theory. The goal of current paper is to reveal these relations.

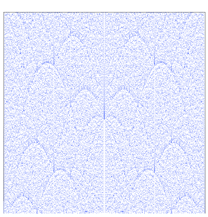

FIGURE 6: Layer 16 of the automaton plot (for wordlength 16)

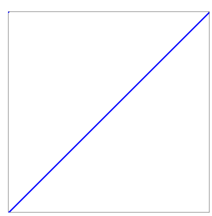

FIGURE 7: Layer 24 of the same automaton plot (for wordlength 24)

2. Preliminaries

Mathematically our results are based on examination of C^2-smooth real functions which can be computed (in some novel but natural meaning which is rigorously defined below) on finite automata, i.e., on sequential machines that have only finite number of states. All these functions turn out to be are affine and, moreover, they can be expressed as complex functions $e^{i(Ax+B)}$ and therefore can be ascribed (also in some natural rigorous meaning) to matter waves from quantum theory. Reader is referred to [4] for complete proofs (unfortunately, lengthy) of mathematical results. For reader's convenience, in the current Section we reproduce necessary definitions and state some of results which will be needed further.

2.1. Basic construction

In the paper, by a general automaton (whose set of states is not necessarily finite) we mean a machine which performs letter-by-letter transformations of words over input alphabet into words over output alphabet: Once a letter is fed to the automaton, the automaton updates its current state (which initially is fixed and so is the same for all input words) to the next one and produces corresponding output letter. Both the next state and the output letter depend on the current state as well as on the input letter. Therefore each letter of output word depends *only* on those letters of input word which have already been fed to the automaton. An input word is a finite sequence of letters; the letters can naturally be ascribed to 'causes' while letters of the corresponding output word can be regarded as 'effects'. *'Causality' just means that effects depend only on causes which 'already have happened'; therefore an automaton is an adequate mathematical formalism for a specific manifestation of causality principle once we assume that there exist only finitely many causes and effects*, cf., e.g.,[57, 58].

When speaking of real functions that can be computed by an automaton $\mathfrak{A}$ (whose input/output alphabets are $\mathcal{A} = \{0, 1, \ldots, p-1\}$, where $p > 1$ is an integer from $\mathbb{N} = \{1, 2, 3, \ldots\}$) we mean the following:

1. given a real number $x \in [0, 1]$, we represent x via base-p expansion $x = 0.\alpha_1\alpha_2\ldots\alpha_n\ldots$ (we take both expansions if x has two distinct ones);
2. from the base-p expansion $0.\alpha_1\alpha_2\ldots\alpha_n\ldots$ we derive corresponding sequence $\alpha_1, \alpha_1\alpha_2, \alpha_1\alpha_2\alpha_3, \ldots$ of words; then
3. feeding the automaton $\mathfrak{A}$ successively by the words $\alpha_1, \alpha_1\alpha_2, \alpha_1\alpha_2\alpha_3, \ldots$ so that *rightmost letters are fed to* $\mathfrak{A}$ *prior to leftmost ones*, we obtain corresponding output word sequence $\zeta_{11}, \zeta_{12}\zeta_{22}, \zeta_{13}\zeta_{23}\zeta_{33}, \ldots$;
4. to the output sequence we put into a correspondence the sequence $\mathcal{S}(x)$ of rational numbers whose base-p expansions are $0.\zeta_{11}, 0.\zeta_{12}\zeta_{22}, 0.\zeta_{13}\zeta_{23}\zeta_{33}, \ldots$ thus obtaining a point set $\mathfrak{X}(x) = \{(0.\alpha_1\ldots\alpha_i; 0.\zeta_{1i}\zeta_{2i}\ldots\zeta_{ii}) \colon i = 1, 2, \ldots\}$ in the real unit square $\mathbb{I}^2 = [0, 1] \times [0, 1]$; after that

5. we consider the set $\mathcal{F}(x)$ of *all* cluster points of the sequence $\mathcal{S}(x)$;
6. finally, we specify a *real plot* (or, briefly, a plot) of the automaton $\mathfrak{A}$ as a union $\mathbf{P}(\mathfrak{A}) = \cup_{x\in[0,1],y\in\mathcal{F}(x)}((x;y)\cup\mathcal{X}(x))$.

In other words, $\mathbf{P}(\mathfrak{A})$ is a closure in the unit square $\mathbb{I}^2$ of the union $\cup_{i=1}^{\infty}\mathbf{L}_i(\mathfrak{A})$ where $\mathbf{L}_i(\mathfrak{A}) = \{(0.\alpha_1\ldots\alpha_i; 0.\zeta_{1i}\zeta_{2i}\ldots\zeta_{ii})\colon x\in\mathbb{I}\}$ is the *i-th layer* of the plot $\mathbf{P}(\mathfrak{A})$. That is, the plot $\mathbf{P}(\mathfrak{A})$ can be considered as a 'limit' of the sequence of sets $\cup_{i=1}^{n}\mathbf{L}_i(\mathfrak{A})$, the *approximate plots* at word length N, while $N\to\infty$. For instance, Figures 6–7 show 16-th and 24-th layers of the plot of an automaton; Figures 1–2 are 16-th and 17-th approximate plots (of another automaton) respectively, whereas Figure 3 shows the set $\mathbf{AP}(\mathfrak{A})$ of all cluster points of the plot $\mathbf{P}(\mathfrak{A})$ and Figure 4 shows a counterpart of the real plot, a so-called *Monna graph* $\mathbf{M}(\mathfrak{A})$ obtained in a way similar to that the plot was constructed but with the only (however, crucial) difference: Digits of base-p expansion of a real number are fed to (and outputted from) the automaton $\mathfrak{A}$ in *inverse order*, more significant (i.e., leftmost) digits are fed to and read from the automaton prior to less significant (i.e., rightmost) ones. This results in a crucial difference in pictures since, loosely speaking, the plot better reflects a long-term behavior of the automaton, i.e., after a sufficiently long period of time has elapsed; whereas the Monna graph better reflects the behavior on short-time intervals: The Monna graph suggests that first (i.e., the earliest) income/outcome 'pulses' are the 'most accurately measured' while our plot-based model assumes that we are not possible to measure Planck-time interval and therefore the most accurately measured are the latest 'pulses'. We postpone more formal definitions for Subsection 2.6.

Note that according to automata 0-1 law (cf. [5, Proposition 11.15] and [3]) the plot $\mathbf{P}(\mathfrak{A})$ of arbitrary automaton $\mathfrak{A}$ can be of two kinds only: Either $\mathbf{P}(\mathfrak{A}) = \mathbb{I}^2$ or $\mathbf{P}(\mathfrak{A})$ is a (Lebesgue) measure-0 closed subset of $\mathbb{R}^2$. Moreover, if the number of states of the automaton $\mathfrak{A}$ is finite (further in the paper these automata are referred to as *finite* ones, or, which is the same, as *Mealy automata*), then the second case only takes place. That is, a plot of a finite automaton cannot contain 'figures', but it may contain 'lines'. While examining what the lines are we actually want to know what real functions can be 'computed' by a finite automaton.

In the sequel we refer real functions $g\colon G\to[0,1]$ with domain $G\subset[0,1]$ as to *finitely computable* if there exists a finite automaton $\mathfrak{A}$ whose real plot contains the graph of the function g; i.e., if $\mathbf{G}(g)\subset\mathbf{P}(\mathfrak{A})$. Theorem 5.1 characterizes all finitely computable C^2-functions g defined on a sub-segment $D=[a,b)\subset[0,1]$: The theorem yields that *if a finitely computable function $g\colon D\to[0,1]$ is twice differentiable and if its second derivative is continuous everywhere on D then g is necessarily affine of the form $g(x)=Ax+B$ for suitable rational p-adic A,B* (that is, for A, B which can be represented by irreducible fractions whose denominators are co-prime to p). Moreover, this is true in n-dimensional case as well (Theorem 5.2).

Theorem 5.1 reveals another important feature of smooth functions which can be computed on finite automata. From Figure 3 it can be clearly observed that accumulation points of the plot constitute a torus winding if one converts a unit square into a torus by gluing together opposite sides of the square. This is not occasional: Our Theorem 5.1 yields that *if the unit square $\mathbb{I}^2$ is mapped onto a torus $\mathbb{T}^2 \subset \mathbb{R}^3$, the smooth curves from the plot become torus windings*; and these *windings after being represented in cylindrical coordinates are described by complex-valued functions $e^{i(Ax+B)}$* ($x \in [0,1]$), see Corollary 3.2. But in quantum theory the latter exponential functions are ascribed to matter waves (cf., de Broglie waves); therefore, since automata can be considered as models for discrete casual systems, the *results of our paper give some mathematical evidence that matter waves are inherent in quantum systems merely due to causality principle and discreteness of matter.*

For not to overload the paper with technical details, we state Theorem 5.1 only for automata whose input and output alphabets consist of p letters $0, 1, \ldots, p-1$ where $p > 1$ is a prime number though our approach can be expanded to the case when p is arbitrary integer greater than 1 (and even to the case when p is not necessarily an integer, see Section 6.). For a prime p, we naturally associate when necessary letters of the alphabet $0, 1, \ldots, p-1$ to residues modulo p, i.e., to elements of finite field $\mathbb{F}_p$.

Technically our considerations are heavily based on interplay between real analysis and p-adic analysis since *automata maps are 1-Lipschitz functions w.r.t. p-adic metric which are defined on (and valuated in) the space $\mathbb{Z}_p$ of p-adic integers; and vice versa, every 1-Lipschitz map from $\mathbb{Z}_p$ to $\mathbb{Z}_p$ is an automaton map for a suitable automaton*, see Subsection 2.5.. This is why we first recall some facts about words over a finite alphabet, p-adic integers, and automata.

2.2. Few words about words

An *alphabet* is just a finite non-empty set $\mathcal{A}$; further in the paper usually $\mathcal{A} = \{0, 1, \ldots, p-1\} = \mathbb{F}_p$. Elements of $\mathcal{A}$ elements are called *symbols*, or *letters*. By the definition, a *word of length n over alphabet $\mathcal{A}$* is a finite sequence (stretching from right to left) $\alpha_{n-1} \cdots \alpha_1 \alpha_0$, where $\alpha_{n-1}, \ldots, \alpha_1, \alpha_0 \in \mathcal{A}$. The number n is called the *length* of the word $w = \alpha_{n-1} \cdots \alpha_1 \alpha_0$ and is denoted via $\Lambda(w)$. The *empty word* ϕ is a sequence of length 0, that is, the one that contains no symbols. Given a word $w = \alpha_{n-1} \cdots \alpha_1 \alpha_0$, any word $v = \alpha_{k-1} \cdots \alpha_1 \alpha_0$, $k \le n$, is called a *prefix* of the word w; whereas any word $u = \alpha_{n-1} \cdots \alpha_{i+1} \alpha_i$, $0 \le i \le n-1$ is called a *suffix* of the word w. Every word $\alpha_j \cdots \alpha_{i+1} \alpha_i$ where $n-1 \ge j \ge i \ge 0$ is called a *subword* of the word $w = \alpha_{n-1} \cdots \alpha_1 \alpha_0$. Given words $a = \alpha_{n-1} \cdots \alpha_1 \alpha_0$ and $b = \beta_{k-1} \cdots \beta_1 \beta_0$, the *concatenation* ab is the following word (of length $n+k$):

$$ab = \alpha_{n-1} \cdots \alpha_1 \alpha_0 \beta_{k-1} \cdots \beta_1 \beta_0.$$

Given a word w, its k-times concatenation is denoted via $(w)^k$:

$$(w)^k = \underbrace{ww \ldots w}_{k \text{ times}}.$$

We denote via $\mathcal{W}$ the set of all non-empty words over $\mathcal{A} = \{0, 1, \dots, p-1\}$ and via $\mathcal{W}_\phi$ the set of all words including the empty word ϕ. In the sequel the set of all n-letter words over the alphabet $\mathbb{F}_p$ we denote as $\mathcal{W}_n$; so $\mathcal{W} = \cup_{n=1}^{\infty}\mathcal{W}_n$. To every word $w = \alpha_{n-1}\cdots\alpha_1\alpha_0$ we put into the correspondence a non-negative integer $\mathsf{num}(w) = \alpha_0 + \alpha_1 \cdot p + \cdots + \alpha_{n-1}\cdot p^{n-1}$. Thus num maps the set $\mathcal{W}$ of all non-empty finite words over the alphabet $\mathcal{A}$ onto the set $\mathbb{N}_0 = \{0, 1, 2, \dots\}$ of all non-negative integers. We will also consider a map ρ of the set $\mathcal{W}$ into the real unit half-open interval $[0, 1)$; the map ρ is defined as follows: Given $w = \beta_{r-1}\dots\beta_0 \in \mathcal{W}$, put

$$\rho(w) = \mathsf{num}(w)\cdot p^{-\Lambda(w)} = \frac{\beta_0 + \beta_1 p + \cdots + \beta_{r-1}p^{r-1}}{p^r} = 0.\beta_{r-1}\dots\beta_0 \in [0, 1). \quad (2)$$

We also use notation $0.w$ for $0.\beta_{r-1}\dots\beta_0$.

Along with finite words we also consider (left-)infinite words over the alphabet $\mathcal{A}$; the ones are the infinite sequences of the form $\dots\alpha_2\alpha_1\alpha_0$ where $\alpha_i \in \mathcal{A}$, $i \in \mathbb{N}_0$. For infinite words the notion of a prefix and of a subword are defined in the same way as for finite words; whilst suffix is not defined. Let an infinite word w be eventually periodic, that is, let

$$w = \dots\beta_{t-1}\beta_{t-2}\dots\beta_0\beta_{t-1}\beta_{t-2}\dots\beta_0\alpha_{r-1}\alpha_{r-2}\dots\alpha_0$$

for $\alpha_i\beta_j \in \mathcal{A}$; then the subword $\beta_{t-1}\beta_{t-2}\dots\beta_0$ is called a *period* of the word w and the suffix $\alpha_{r-2}\dots\alpha_0$ is called the pre-period of the word w. Note that a pre-period may be an empty word while a period can not. We write the eventually periodic word w as $w = (\beta_{t-1}\beta_{t-2}\dots\beta_0)^\infty\alpha_{r-1}\alpha_{r-2}\dots\alpha_0$.

2.3. p-adic numbers

See [22, 29, 35] for introduction to p-adic analysis or comprehensive monographs [42, 51] for further reading.

Fix a prime number p and denote respectively via $\mathbb{N} = \{1, 2, \dots\}$ and $\mathbb{Z} = \{0, \pm1, \pm2, \dots\}$ the set of all positive rational integers and the ring of all rational integers. Given $n \in \mathbb{N} = \mathbb{N}_0 \setminus \{0\}$, the *$p$-adic absolute value* of n is $|n|_p = p^{-\operatorname{ord}_p n}$, where $p^{\operatorname{ord}_p n}$ is the largest power of p which is a factor of n; so $n = n' \cdot p^{\operatorname{ord}_p n}$ where $n' \in \mathbb{N}$ is co-prime to p. By putting $|0|_p = 0$, $|-n|_p = |n|_p$ and $|n/m|_p = |n|_p/|m|_p$ for $n, m \in \mathbb{Z}$, $m \neq 0$ we expand the p-adic absolute value to the whole field $\mathbb{Q}$ of rational numbers. Given an absolute value $|\ |_p$, we define a metric in a standard way: $|a-b|_p$ is a *p-adic metric* on $\mathbb{Q}$. The field $\mathbb{Q}_p$ of *p-adic numbers* is a completion of the field $\mathbb{Q}$ of rational numbers w.r.t. the p-adic metric while the ring $\mathbb{Z}_p$ of *p-adic integers* is a ring of integers of $\mathbb{Q}_p$; and the ring $\mathbb{Z}_p$ is a completion of $\mathbb{Z}$ w.r.t. the p-adic metric. The ring $\mathbb{Z}_p$ is compact w.r.t. the p-adic metric: Actually $\mathbb{Z}_p$ is a ball of radius 1 centered at 0; namely $\mathbb{Z}_p = \{r \in \mathbb{Q}_p : |r|_p \le 1\}$. Balls in $\mathbb{Q}_p$ are *clopen*; that is, both closed and open w.r.t. the p-adic metric.

A p-adic number $r \in \mathbb{Q}_p \setminus \{0\}$ admits a unique *p-adic canonical expansion* $r = \sum_{i=k}^{\infty}\alpha_i p^i$ where $\alpha_i \in \{0, 1, \dots, p-1\}$, $k \in \mathbb{Z}$, $\alpha_k \neq 0$. Note that then any

p-adic integer $z \in \mathbb{Z}_p$ admits a unique representation $z = \sum_{i=0}^{\infty} \alpha_i p^i$ for suitable $\alpha_i \in \{0, 1, \ldots, p-1\}$. The latter representation is called a *canonical form* (or, a *canonical representation*) of the p-adic integer $z \in \mathbb{Z}_p$; the i-th coefficient α_i of the expansion will be referred to as *the i-th p-adic digit* of z and denoted via $\alpha_i = \delta_i(z)$. It is clear that once $z \in \mathbb{N}_0$, the i-th p-adic digit $\delta_i(z)$ of z is just the i-th digit in the base-p expansion of z. Note also that a p-adic integer $z \in \mathbb{Z}_p$ is a *unity* of $\mathbb{Z}_p$ (i.e., has a multiplicative inverse $z^{-1} \in \mathbb{Z}_p$) if and only if $\delta_0(z) \neq 0$; so any p-adic number $z \in \mathbb{Q}_p$ has a unique representation of the form $z = z' \cdot |z|_p^{-1}$ where $z' \in \mathbb{Z}_p$ is a unity.

The p-adic integers may be associated to infinite words over the alphabet $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ as follows: Given a p-adic integer $z \in \mathbb{Z}_p$, consider its canonical expansion $z = \sum_{i=0}^{\infty} \alpha_i \cdot p^i$; then denote via $\mathsf{wrd}(z)$ the infinite word $\ldots \alpha_2 \alpha_1 \alpha_0$ (allowing some freedom of saying we will sometimes refer $\mathsf{wrd}(z)$ as to a *base-p expansion of* $z \in \mathbb{Z}_p$). Vice versa, given a left-infinite word $w = \ldots \alpha_2 \alpha_1 \alpha_0$ we denote via $\mathsf{num}(w) = \sum_{i=0}^{\infty} \alpha_i \cdot p^i$ corresponding p-adic integer whose base-p expansion is w thus expanding the mapping num defined in Subsection 2.2. to the case of infinite words as well. It is worth noticing here that addition and multiplication of p-adic integers can be performed by using the same school-textbook algorithms for addition/multiplication of non-negative integers represented via their base-p expansions with the only difference: The algorithms are applied to infinite words that correspond to p-adic canonical forms of summands/multipliers rather than to a finite words which are base-p expansions of summands/multipliers.

Given $n \in \mathbb{N}$ and a canonical expansion $z = \sum_{i=0}^{\infty} \alpha_i p^i$ for $z \in \mathbb{Z}_p$, denote $z \bmod p^n = \sum_{i=0}^{n-1} \alpha_i p^i$. The mapping $\mathsf{mod} p^n \colon z \mapsto z \bmod p^n$ is a ring epimorphism of $\mathbb{Z}_p$ onto the residue ring $\mathbb{Z}/p^n\mathbb{Z}$ (under a natural representation of elements of the residue ring by the least non-negative residues $\{0, 1 \ldots, p^n - 1\}$).

The series in the right-hand side of the canonical form converges w.r.t. the p-adic metric; that is, the sequence of partial sums $z \bmod p^n$ converges to z w.r.t. the p-adic metric: $\lim_{n\to\infty}^{p} (z \bmod p^n) = z$. It is worth noticing here that arbitrary infinite series $\sum_{i=0}^{\infty} r_i$ where $r_i \in \mathbb{Q}_p$ converges in $\mathbb{Q}_p$ (i.e., w.r.t. p-adic metric) if and only if $\lim_{i\to\infty} |r_i|_p = 0$ since p-adic metric is *non-Archimedean*; that is, it satisfies *strong triangle inequality* $|x - y|_p \leq \max\{|x - z|_p, |z - y|_p\}$ for all $x, y, z \in \mathbb{Q}_p$.

Note that $z \in \mathbb{N}_0$ if and only if all but a finite number of coefficients α_i in the canonical form are 0 while $z \in \{-1, -2, -3, \ldots\}$ if and only if all but a finite number of α_i are $p - 1$. Further we will need a special representation for *p-adic integer rationals*; that is, for those rational numbers z which at the same time are p-adic integers, i.e., for $z \in \mathbb{Z}_p \cap \mathbb{Q}$. Note that $z \in \mathbb{Z}_p \cap \mathbb{Q}$ if and only if z can be represented by an irreducible fraction $z = a/b$, $a \in \mathbb{Z}, b \in \mathbb{N}$ where b is co-prime to p. The following proposition is well known, cf., e.g., [21, Theorem 10]:

Proposition 2.1. *A p-adic integer z is rational* (i.e., $z \in \mathbb{Z}_p \cap \mathbb{Q}$) *if and only if* *the sequence of coefficients of its canonical form is eventually periodic:*

$$z=\alpha_0+\alpha_1p+\cdots+\alpha_{r-1}p^{r-1}+(\beta_0+\beta_1p+\cdots+\beta_{t-1}p^{t-1})p^r+ \\ (\beta_0+\beta_1p+\cdots+\beta_{t-1}p^{t-1})p^{r+t}+(\beta_0+\beta_1p+\cdots+\beta_{t-1}p^{t-1})p^{r+2t}+\cdots \quad (3)$$

for suitable $\alpha_j,\beta_i\in\{0,1,\dots,p-1\}$, $r\in\mathbb{N}_0$, $t\in\mathbb{N}$ (the sum $\alpha_0+\alpha_1p+\cdots+\alpha_{r-1}p^{r-1}$ is absent in the above expression once $r=0$).

In other words, once a p-adic integer z is represented in its canonical form, $z=\sum_{i=0}^{\infty}\gamma_ip^i$, the corresponding infinite word $\dots\gamma_1\gamma_0$ is eventually periodic: $\dots\gamma_1\gamma_0=(\beta_{t-1}\dots\beta_0)^\infty\alpha_{r-1}\dots\alpha_0$. It is clear that given $z\in\mathbb{Z}_p\cap\mathbb{Q}$, both r and t are not unique: For instance,

$$(\beta_{t-1}\dots\beta_0)^\infty\alpha_{r-1}\dots\alpha_0=(\beta_0\beta_{t-1}\dots\beta_1\beta_0\beta_{t-1}\dots\beta_1)^\infty\alpha_r\alpha_{r-1}\dots\alpha_0,$$

where $\alpha_r=\beta_0$. But once both pre-periodic and periodic parts (the prefix $\alpha_{r-1}\dots\alpha_0$ and the word $\beta_{t-1}\dots\beta_0$) are taken the shortest possible, both the *pre-period length* r and the *period length* t are unique for a given p-adic rational integer $z\in\mathbb{Z}_p\cap\mathbb{Q}$; we refer to $\alpha_{r-1}\dots\alpha_0$ and to $\beta_{t-1}\beta_{t-2}\dots\beta_1\beta_0$ as to *pre-period* of z and *period* of z accordingly.

Given $z\in\mathbb{Z}_p\cap\mathbb{Q}$ we mostly assume further that in the representation $z=\alpha_0+\cdots+\alpha_{r-1}p^{r-1}+(\beta_0+\cdots+\beta_{t-1}p^{t-1})\cdot\sum_{j=0}^{\infty}p^{r+tj}$ (respectively, in eventually periodic infinite word $\mathsf{wrd}(z)=(\beta_{t-1}\dots\beta_0)^\infty\alpha_{r-1}\dots\alpha_0$ that corresponds to z) r is a pre-period length and t is a period length. Note that a pre-period may be an empty word (i.e., of length 0) while a period can not.

Rational p-adic integers can also be represented as fractions of a special kind:

Proposition 2.2. *A p-adic integer $z\in\mathbb{Z}_p$ is rational if and only if there exist $t\in\mathbb{N}$, $c\in\mathbb{Z}$, $d\in\{0,1,\dots,p^t-2\}$ such that*

$$z=c+\frac{d}{p^t-1}. \quad (4)$$

Proof. Indeed, $z\in\mathbb{Z}_p\cap\mathbb{Q}$ if and only if z is of the form (3); therefore

$$z=(\alpha_0+\alpha_1p+\cdots+\alpha_{r-1}p^{r-1}-p^r)+p^r\left(1-\frac{\beta_0+\beta_1p+\cdots+\beta_{t-1}p^{t-1}}{p^t-1}\right)= \\ (\alpha_0+\alpha_1p+\cdots+\alpha_{r-1}p^{r-1}-p^r+q)+\frac{\zeta_0+\zeta_1p+\cdots+\zeta_{t-1}p^{t-1}}{p^t-1} \quad (5)$$

where $\zeta_0+\zeta_1p+\cdots+\zeta_{t-1}p^{t-1}$ is a base-p expansion of the least non-negative residue s of $p^r(p^t-1-(\beta_0+\beta_1p+\cdots+\beta_{t-1}p^{t-1}))=(p^t-1)q+s$ modulo p^t-1. $\square$

Remark 2.1. Recall that $(1-p^m)^{-1}=\sum_{i=0}^{\infty}p^{mi}\in\mathbb{Z}_p$, for every $m\in\mathbb{N}$.

Remark 2.2. Note that once in (5) r is a pre-period length and t is a period length of $z\in\mathbb{Z}_p\cap\mathbb{Q}$, the representation (4) is unique; that is, the choice of c and d in (4) is unique.

In the sequel we often use base-p expansions of p-adic rational integers reduced modulo 1 along with their p-adic canonical forms. Recall that if $y \in \mathbb{R}$ then by the definition $y \bmod 1 = y - \lfloor y \rfloor \in [0,1) \subset \mathbb{R}$, where $\lfloor y \rfloor$ is the biggest integer from $\mathbb{Z} = \{0, \pm 1, pm2, \ldots\}$ which does not exceed y.

For reader's convenience, we now summarize some facts on connections between these representations.

It is very well known that a base-p expansion of a rational number is eventually periodic; that is, given $x \in \mathbb{Q} \cap [0,1]$, the base-$p$ expansion for x is

$$
\begin{gathered}
x = 0.\chi_0 \ldots \chi_{k-1}(\xi_0 \ldots \xi_{n-1})^\infty = \\
\chi_0 p^{-1} + \chi_1 p^{-2} + \cdots + \chi_{k-1} p^{-k} + \xi_0 p^{-k-1} + \xi_1 p^{-k-2} + \cdots + \xi_{n-1} p^{-k-n} + \\
\xi_0 p^{-k-1-n} + \xi_1 p^{-k-2-n} + \cdots + \xi_{n-1} p^{-k-2n} + \cdots = \\
\frac{1}{p^k}(\chi_0 p^{k-1} + \chi_1 p^{k-2} + \cdots + \chi_{k-1}) + \frac{1}{p^k} \cdot \frac{\xi_0 p^{n-1} + \xi_1 p^{n-2} + \cdots + \xi_{n-1}}{p^n - 1}, \quad (6)
\end{gathered}
$$

where $\chi_i, \xi_j \in \{0, 1, \ldots, p-1\}$. Note that in base-$p$ expansions of rational integers from $[0,1]$ we use *right*-infinite words rather than left-infinite ones that correspond to canonical expansions of p-adic integers.

Proposition 2.3. *Given $z \in \mathbb{Z}_p \cap \mathbb{Q}$, represent z in the form* (3)*; then*

$$
z \bmod 1 = 0.(\hat\beta_{t-1-\bar r}\hat\beta_{t-2-\bar r} \ldots \hat\beta_0 \hat\beta_{t-1}\hat\beta_{t-2} \ldots \hat\beta_{t-\bar r})^\infty \bmod 1,
$$

where $\hat\beta = p - 1 - \beta$ for $\beta \in \{0, 1, \ldots, p-1\}$ and $\bar r$ is the least non-negative residue of r modulo t if $t > 1$ or $\bar r = 0$ if otherwise.

Proof. Indeed, by Note 2.1, $\sum_{j=0}^{\infty} p^{r+tj} = -p^r(p^t - 1)^{-1}$ in $\mathbb{Z}_p$; so $z = u - vp^r(p^t-1)^{-1}$ where $u = \alpha_0 + \alpha_1 p + \cdots + \alpha_{r-1}p^{r-1}$ and $v = \beta_0 + \beta_1 p + \cdots + \beta_{t-1}p^{t-1}$. Therefore

$$
z \bmod 1 = \left(-\frac{vp^r}{p^t - 1}\right) \bmod 1.
$$

But $(p^t - 1)^{-1} = p^{-t} + p^{-2t} + p^{-3t} + \cdots$ in $\mathbb{R}$; so

$$
(p^t - 1)^{-1} = 0.(\underbrace{00\ldots0}_{t-1}1)^\infty
$$

and thus $-v \cdot (p^t - 1)^{-1} = -0.(\beta_{t-1}\beta_{t-2} \ldots \beta_0)^\infty$.

Now just note that

$$
(p-1-\gamma_0) + (p-1-\gamma_1)p + \cdots + (p-1-\gamma_{s-1})p^{s-1} = p^s - 1 - (\gamma_0 + \gamma_1 p + \cdots + \gamma_{s-1}p^{s-1})
$$

for $\gamma_0, \gamma_1, \ldots \in \{0, 1, \ldots, p-1\}$, $s \in \mathbb{N}$; so

$$
\frac{(p-1-\gamma_0) + (p-1-\gamma_1)p + \cdots + (p-1-\gamma_{s-1})p^{s-1}}{p^s - 1} =
1 - \frac{\gamma_0 + \gamma_1 p + \cdots + \gamma_{s-1}p^{s-1}}{p^s - 1}
$$

and therefore

$$(-0.(\gamma_{s-1}\gamma_{s-2}\ldots\gamma_0)^\infty) \bmod 1 = (0.(\hat{\gamma}_{s-1}\hat{\gamma}_{s-2}\ldots\hat{\gamma}_0)^\infty) \bmod 1 \tag{7}$$

where $\hat{\gamma} = p-1-\gamma$ for $\gamma \in \{0,1,\ldots,p-1\}$. □Combining (6) with Proposition 2.2 we see that all real numbers whose base-p expansions are purely periodic must lie in $\mathbb{Z}_p \cap \mathbb{Q}$; therefore the following criterion is true:

Corollary 2.1. *A real number x is in $\mathbb{Z}_p \cap \mathbb{Q}$ if and only if base-p expansion of $x \bmod 1$ is purely periodic: $x \bmod 1 = 0.(\chi_0 \ldots \chi_{n-1})^\infty$ for suitable $\chi_0, \ldots, \chi_{n-1} \in \mathbb{F}_p$.*

The following corollary expresses base-p expansion of a p-adic rational integer via its representation in the form given by Proposition 2.2:

Corollary 2.2. *Once a p-adic rational integer $z \in \mathbb{Z}_p \cap \mathbb{Q}$ is represented in the form as of Proposition 2.2 then $z \bmod 1 = 0.(\zeta_{t-1}\zeta_{t-2}\ldots\zeta_0)^\infty$ where $d = \zeta_0 + \zeta_1 p + \cdots + \zeta_{t-1}p^{t-1}$.*

Now we can find a period length of $z \in \mathbb{Z}_p \cap \mathbb{Q}$ provided z is represented as an irreducible fraction $z = a/b$, where $a \in \mathbb{Z}$, $b \in \mathbb{N}$.

Proposition 2.4. *Once a p-adic rational integer $z \neq 0$ is represented as an irreducible fraction $z = a/b$, and if $b > 1$, then the period length t of z is equal to the multiplicative order of p modulo b* (i.e., to the smallest $\ell \in \mathbb{N}$ such that $p^\ell \equiv 1 \pmod{b}$)*.*

Now given $b \in \mathbb{N}$, b co-prime to p, we denote via $\mathrm{mult}_b\, p$ the multiplicative order of p modulo b if $b > 1$ or put $\mathrm{mult}_b\, p = 1$ once $b = 1$. Then $\mathrm{mult}_b\, p$ is the period length of $z \in \mathbb{Z}_p \cap \mathbb{Q}$ once z is represented as an irreducible fraction $z = a/b$ where $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Note that we consider here only infinite words that correspond to p-adic rational integers; thus to, e.g., 0 there corresponds a word $(0)^\infty$ (so a period of 0 is 0 and a pre-period is empty) and the respective base-p expansion of 0 is $0.(0)^\infty$. Also, $1 = 1 + 0\cdot p + 0\cdot p^2 + \cdots$, the corresponding infinite word is $(0)^\infty 1$; therefore 1 is a pre-period of 1, 0 is a period of 1, and the representation of 1 in the form (4) is $1 = 1 + (0/p-1)$.

Example 2.1. *Let $p = 2$; then $1/3 = 1\cdot 1 + 1\cdot 2 + 0\cdot 4 + 1\cdot 8 + 0\cdot 16 + \cdots = 1 - 2\cdot 3^{-1}$ is a canonical 2-adic expansion of $1/3$; so the corresponding infinite binary word is $(01)^\infty 1$. Therefore the period length of $1/3$ is 2 (and note that the multiplicative order of 2 modulo 3 is indeed 2), the period is 01, the pre-period is 1. Also, $c = 0$ and $d = 1$ once $1/3$ is represented in the form of Proposition 2.2; $1/3 = 0.(01)^\infty$ is a base-2 expansion of $1/3$, cf. Proposition 2.3 and Corollary 2.2.*

2.4. Automata: Basics

Here we recall some basic facts from automata theory (see e.g. monographs [8, 10, 18]).

By the definition, a (non-initial) automaton is a 5-tuple $\mathfrak{A} = \langle \mathcal{I}, \mathcal{S}, \mathcal{O}, S, O \rangle$ where $\mathcal{I}$ is a finite set, the *input alphabet*; $\mathcal{O}$ is a finite set, the *output alphabet*; $\mathcal{S}$ is a non-empty (possibly, infinite) set of *states*; $S\colon \mathcal{I} \times \mathcal{S} \to \mathcal{S}$ is a *state transition function*; $O\colon \mathcal{I} \times \mathcal{S} \to \mathcal{O}$ is an *output function*. An automaton where both input alphabet $\mathcal{I}$ and output alphabet $\mathcal{O}$ are non-empty is called a *transducer*, see e.g. [2, 10]. The *initial automaton* $\mathfrak{A}(s_0) = \langle \mathcal{I}, \mathcal{S}, \mathcal{O}, S, O, s_0 \rangle$ is an automaton $\mathfrak{A}$ where one state $s_0 \in \mathcal{S}$ is fixed; it is called the *initial state*. We stress that the definition of an initial automaton $\mathfrak{A}(s_0)$ is nearly the same as the one of *Mealy automaton* (see e.g. [8, 10]) with the only important difference: the set of states $\mathcal{S}$ of $\mathfrak{A}(s_0)$ is *not necessarily finite*. Note also that in literature the automata we consider in the paper are also referred to as *(letter-to-letter) transducers*; in the sequel we use terms 'automaton' and 'transducer' as synonyms.

Given an input word $w = \chi_{n-1} \cdots \chi_1 \chi_0$ over the alphabet $\mathcal{I}$, an initial transducer $\mathfrak{A}(s_0) = \langle \mathcal{I}, \mathcal{S}, \mathcal{O}, S, O, s_0 \rangle$ transforms w to output word $w' = \xi_{n-1} \cdots \xi_1 \xi_0$ over the output alphabet $\mathcal{O}$ as follows (cf. Figure 8): Initially the transducer $\mathfrak{A}(s_0)$ is at the state s_0; accepting the input symbol $\chi_0 \in \mathcal{I}$, the transducer outputs the symbol $\xi_0 = O(\chi_0, s_o) \in \mathcal{O}$ and reaches the state $s_1 = S(\chi_0, s_0) \in \mathcal{S}$; then the transducer accepts the next input symbol $\chi_1 \in \mathcal{I}$, reaches the state $s_2 = S(\chi_1, s_1) \in \mathcal{S}$, outputs $\xi_1 = O(\chi_1, s_1) \in \mathcal{O}$, and the routine repeats. This way the transducer $\mathfrak{A} = \mathfrak{A}(s_0)$ defines a mapping $\mathfrak{a} = \mathfrak{a}_{s_0}$ of the set $\mathcal{W}_n(\mathcal{I})$ of all n-letter words over the input alphabet $\mathcal{I}$ to the set $\mathcal{W}_n(\mathcal{O})$ of all n-letter words over the output alphabet $\mathcal{O}$; thus $\mathfrak{A}$ defines a map of the set $\mathcal{W}(\mathcal{I})$ of all non-empty words over the alphabet $\mathcal{I}$ to the set $\mathcal{W}(\mathcal{O})$ of all non-empty words over the alphabet $\mathcal{O}$. We will denote the latter map by the same symbol $\mathfrak{a}$ (or by $\mathfrak{a}_{s_0}$ if we want to stress what initial state is meant), and when it is clear from the context what alphabet $\mathcal{A}$ is meant we use notation $\mathcal{W}$ rather than $\mathcal{W}(\mathcal{A})$.

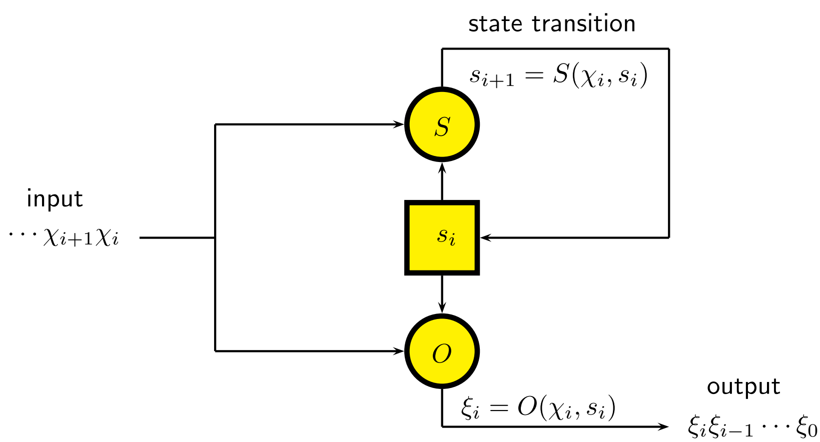

Figure 8: Initial transducer, schematically

Throughout the paper, 'automaton' mostly stands for 'initial automaton'; we make corresponding remarks if not. Further in the paper we mostly consider trans-

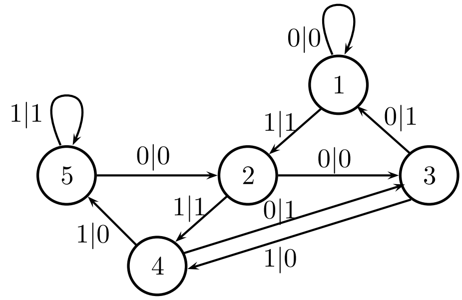

FIGURE 9: Example state diagram of a minimal automaton. Initial state is 1.

ducers. Furthermore, throughout the paper we consider *reachable transducers* only; that is, *we assume that all states of the initial transducer* $\mathfrak{A}(s_0)$ *are* reachable from *the initial state* s_0: Given $s \in \mathcal{S}$, there exists input word w over alphabet $\mathcal{I}$ such that after the word w has been fed to the automaton $\mathfrak{A}(s_0)$, the automaton reaches the state s. A reachable transducer is called *finite* if its set $\mathcal{S}$ of states is finite, and transducer is called *infinite* if otherwise.

It is convenient for illustrative purposes represent 'internal structure' of an automaton via its *state diagram*, a directed graph (*digraph*) whose vertices are states of the automaton, whose edges (arrows) are labelled by symbols $a|b$, where a (resp., b) is a letter of input (resp., output) alphabet, and arrow goes from i-th vertex to j-th vertex if for some input letter a the automaton goes from i-th state to j-th state; the arrow is labelled by $a|b$ if corresponding output symbol is b. Figure 9 shows example diagram of an automaton which performs multiplication by 5 of natural numbers represented by base-2 expansions; so both input and output alphabet of the automaton is $\{0, 1\}$, short bold arrow points to initial state.

To the initial automaton $\mathfrak{A}(s_0)$ we put into a correspondence a family $\mathcal{F}(\mathfrak{A})$ of all *sub-automata* $\mathfrak{A}(s) = \langle \mathcal{I}, \tilde{\mathcal{S}}, \mathcal{O}, \tilde{S}, \tilde{O}, s\rangle$, $s \in \mathcal{S}$, where $\tilde{\mathcal{S}} = \tilde{\mathcal{S}}(s) \subset \mathcal{S}$ is the set of all states that are reachable from the state s and $\tilde{S}, \tilde{O}$ are respective restrictions of the state transition and output functions S, O on $\mathcal{I} \times \tilde{\mathcal{S}}$. A sub-automaton $\mathfrak{A}(s)$ is called *proper* if the set $\tilde{\mathcal{S}}$ of all its states is a proper subset of $\mathcal{S}$. A sub-automaton $\mathfrak{A}(s)$ is called *minimal* if it contains no proper sub-automata; e.g., an automaton from Figure 9 is minimal.

It is obvious that a finite sub-automaton is minimal if and only if every its state is reachable from any other its state. The set of all states of a minimal sub-automaton of the automaton $\mathfrak{A}$ is called an *ergodic component* of the (set of all states) of the automaton $\mathfrak{A}$. It is clear that once the automaton is in a state that belongs to an ergodic component, all its further states will also be in the same ergodic component. Therefore all states of a finite automaton are of two types only: The *transient states* which belong to no ergodic component, and *ergodic states*

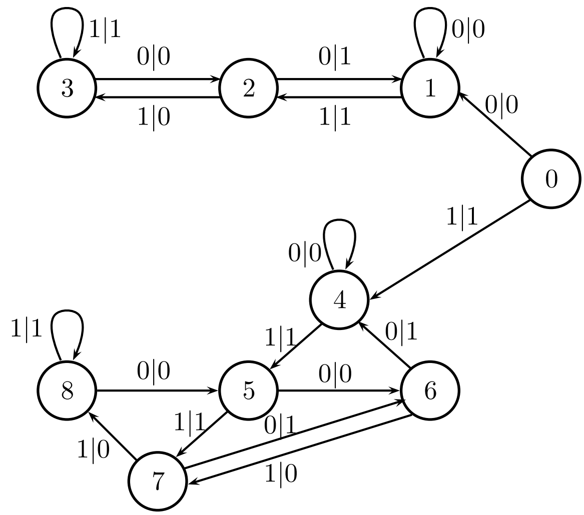

Figure 10: Example state diagram of an automaton with two minimal sub-automata. Initial state is 0.

which belong to ergodic components. It is clear that the set of all ergodic states is a disjoint union of ergodic components. Note that we use the term ‘minimal automaton’ in a different meaning compared to the one used in automata theory, see, e.g., [18]: Our terminology here is from the theory of Markov chains, see, e.g., [30] (since to the graph of state transitions of every automaton there corresponds a Markov chain). The automaton from Figure 10 has two minimal sub-automata; its ergodic components are respectively $\{1, 2, 3\}$ and $\{4, 5, 6, 7, 8\}$; 0 is its initial state. The sub-automaton whose set of states is $\{1, 2, 3\}$ performs multiplication by 3 of natural numbers represented via their base-2 expansions once state 1 is taken for the initial state. The sub-automaton with states $\{4, 5, 6, 7, 8\}$ is up to the numbering of states the same as in Figure 9; so it performs multiplication by 5 once state 4 is taken for the initial.

Hereinafter in the paper the word ‘automaton’ stands for a letter-to-letter initial transducer whose input and output alphabet consists of p symbols, and we mostly assume that p is a prime. Thus, for every $n = 1, 2, 3, \ldots$ the automaton $\mathfrak{A}(s_0) = \langle \mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, S, O, s_0\rangle$ maps n-letter words over $\mathbb{F}_p$ to n-letter words over $\mathbb{F}_p$ according to the procedure described above, cf. Figure 8. Given two such automata $\mathfrak{A} = \mathfrak{A}(s_0)$ and $\mathfrak{B} = \mathfrak{B}(t_0)$, their *sequential composition* (or briefly, a *composition*) $\mathfrak{C} = \mathfrak{B} \circ \mathfrak{A}$ can be defined in a natural way via sending output of the automaton $\mathfrak{A}$ to input of the automaton $\mathfrak{B}$ so that the mapping $\mathfrak{c}\colon \mathcal{W} \to \mathcal{W}$ the automaton $\mathfrak{C}$ performs is just a composite mapping $\mathfrak{b} \circ \mathfrak{a}$ (cf. any of monographs [8, 10, 18] for exact definition and further facts mentioned in the subsection). Note that a composition of finite automata is a finite automaton.

In a similar manner one can consider automata with multiply inputs/outputs; these can be also treated as automata whose input/output alphabets are Cartesian powers of $\mathbb{F}_p$: For instance, and automaton with m inputs and n outputs over alphabet $\mathbb{F}_p$ can be considered as an automaton with a single input over the alphabet $\mathbb{F}_p^m$ and a single output over the alphabet $\mathbb{F}_p^n$. Moreover, as the letters of the alphabet $\mathbb{F}_p^k$ are in a one-to-one correspondence with residues modulo p^k; the automaton with m inputs and n outputs can be considered (if necessary) as an automaton with a single input over the alphabet $\mathbb{Z}/p^m\mathbb{Z}$ and a single output over alphabet $\mathbb{Z}/p^n\mathbb{Z}$.

Compositions of automata with multiple inputs/outputs can also be naturally defined: For instance, given automata $\mathfrak{A}_1$, $\mathfrak{A}_2$, and $\mathfrak{A}_3$ with m_1, m_2, m_3 inputs and n_1, n_2, n_3 outputs respectively, in the case when $m_3 = n_1 + n_2$ one can consider a composition of these automata by connecting every output of automata $\mathfrak{A}_1$ and $\mathfrak{A}_2$ to some input of the automaton $\mathfrak{A}_3$ so that every input of the automaton $\mathfrak{A}_3$ is connected to a unique output which belongs either to $\mathfrak{A}_1$ or to $\mathfrak{A}_2$ but not to the both. This way one obtains various compositions of automata $\mathfrak{A}_1$ and $\mathfrak{A}_2$, with the automaton $\mathfrak{A}_3$, and either of these compositions is an automaton with $m_1 + m_2$ inputs and n_3 outputs. Moreover, either of the compositions is a finite automaton if all three automata $\mathfrak{A}_1$, $\mathfrak{A}_2$, $\mathfrak{A}_3$ are finite.

Automata can be considered as (generally) non-autonomous dynamical systems on different configuration spaces (e.g., $\mathcal{W}_n$, $\mathcal{W}$, etc.); the system is autonomous when neither the state transition function $\mathcal{S}$ nor the output function $\mathcal{O}$ depend on input; in this case the automaton $\mathfrak{A}$ is called *autonomous* as well. In the latter case the mapping $\mathfrak{a}$ is a constant map. An example state diagram of an autonomous automaton (whose input/output alphabet is $\{0,1\}$) is represented by Figure 11. Note that it produces different mappings depending on which state we choose to be initial.

For purposes of the paper it is convenient to consider automata with input/output alphabets $\mathcal{A} = \mathbb{F}_p$ as dynamical systems on the space $\mathbb{Z}_p$ of p-adic integers, i.e., to relate an automaton $\mathfrak{A}$ to a special map $f_{\mathfrak{A}} \colon \mathbb{Z}_p \to \mathbb{Z}_p$. In the next subsection we recall some facts about the map $f_{\mathfrak{A}}$.

2.5. Automata maps: p-adic view

We identify n-letter words over $\mathbb{F}_p$ with non-negative integers in a natural way: Given an n-letter word $w = \chi_{n-1}\chi_{n-2}\cdots\chi_0$ (i.e., $\chi_i \in \mathbb{F}_p$ for $i = 0, 1, 2, \ldots, n-1$), we consider w as a base-p expansion of the number $\mathsf{num}(w) = \chi_0 + \chi_1 \cdot p + \cdots + \chi_{n-1} \cdot p^{n-1} \in \mathbb{N}_0$. In turn, the latter number can be considered as an element of the residue ring $\mathbb{Z}/p^n\mathbb{Z}$ modulo p^n. We denote via wrd_n an inverse mapping to num. The mapping wrd_n is a bijection of the set $\{0, 1 \ldots, p^n - 1\} \subset \mathbb{N}_0$ onto the set $\mathcal{W}_n$ of all n-letter words over $\mathbb{F}_p$.

As the set $\{0, 1 \ldots, p^n - 1\}$ is the set of all non-negative residues modulo p^n , to *every automaton $\mathfrak{A} = \mathfrak{A}(s)$ there corresponds a map $f_{n,\mathfrak{A}}$ from $\mathbb{Z}/p^n\mathbb{Z}$ to $\mathbb{Z}/p^n\mathbb{Z}$*, for every $n = 1, 2, 3, \ldots$. Namely, for $r \in \mathbb{Z}/p^n\mathbb{Z}$ put $f_{n,\mathfrak{A}}(r) = \mathsf{num}(\mathfrak{a}(\mathsf{wrd}_n(r)))$, where

$\mathfrak{a}$ is a word transformation of $\mathcal{W}_n$ performed by the automaton $\mathfrak{A}$, cf. Subsection 2.4..

Speaking less formally, the mapping $f_{n,\mathfrak{A}}$ can be defined as follows: given $r \in \{0, 1, \ldots, p^n - 1\}$, consider a base-$p$ expansion of r, read it as a n-letter word over $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ (put additional zeroes on higher order positions if necessary) and then feed the word to the automaton so that letters that are on lower order positions ('less significant digits') are fed prior to ones on higher order positions ('more significant digits'). Then read the corresponding output n-letter word as a base-p expansion of a number from $\mathbb{N}_0$ keeping the same order, i.e. when the earliest outputted letters correspond to lowest order digits in the base-p expansion.

We stress the following determinative property of the mapping $f_{n,\mathfrak{A}}$ which follows directly from the definition: Given $a, b \in \{0, 1, \ldots, p^n - 1\}$, *whenever* $a \equiv b \pmod{p^k}$ *for some* $k \in \mathbb{N}$ *then necessarily* $f_{n,\mathfrak{A}}(a) \equiv f_{n,\mathfrak{A}}(b) \pmod{p^k}$. This implication may be re-stated in terms of p-adic metric as follows:

$$|f_{n,\mathfrak{A}}(a) - f_{n,\mathfrak{A}}(b)|_p \le |a - b|_p. \tag{8}$$

Furthermost, *every automaton* $\mathfrak{A} = \mathfrak{A}(s_0)$ *defines a mapping* $f_{\mathfrak{A}}$ *from* $\mathbb{Z}_p$ *to* $\mathbb{Z}_p$ which can be specified in a manner similar to the one of the mapping $f_{n,\mathfrak{A}}$: Given an infinite word $w = \ldots \chi_{n-1}\chi_{n-2} \cdots \chi_0$ (that is, an infinite sequence) over $\mathbb{F}_p$ we consider a p-adic integer whose p-adic canonical expansion is $z = z(w) = \chi_0 + \chi_1 \cdot p + \cdots + \chi_{n-1} \cdot p^{n-1} + \cdots$; so, by the definition, for every $z \in \mathbb{Z}_p$ we put

$$\delta_i(f_{\mathfrak{A}}(z)) = O(\delta_i(z), s_i) \qquad (i = 0, 1, 2, \ldots), \tag{9}$$

where $s_i = S(\delta_{i-1}(z), s_{i-1})$, $i = 1, 2, \ldots$, and $\delta_i(z)$ is the i-th p-adic digit of z; that is, the i-th term coefficient in the p-adic canonical representation of z: $\delta_i(z) = \chi_i \in \mathbb{F}_p$, $i = 0, 1, 2, \ldots$ (see Subsection 2.3.). The so defined map $f_{\mathfrak{A}}$ is called the *automaton function* (or, the *automaton map*) of the automaton $\mathfrak{A}$. Note that from (9) it follows that

$$\delta_i(f_{\mathfrak{A}}(z)) = \Phi_i(\delta_0(z), \ldots, \delta_i(z)), \tag{10}$$

where Φ_i is a map from the $(i+1)$-th Cartesian power $\mathbb{F}_p^{i+1}$ of $\mathbb{F}_p$ into $\mathbb{F}_p$.

More formally, given $z \in \mathbb{Z}_p$, define $f_{\mathfrak{A}}(z)$ as follows: Consider a sequence $(z \bmod p^n)_{n=1}^{\infty}$ and a corresponding sequence $(f_{n,\mathfrak{A}}(z \bmod p^n))_{n=1}^{\infty}$; then, as the sequence $(z \bmod p^n)_{n=1}^{\infty}$ converges to z w.r.t. p-adic metric (cf. Subsection 2.3.), the sequence $(f_{n,\mathfrak{A}}(z \bmod p^n))_{n=1}^{\infty}$ in view (8) also converges w.r.t. the p-adic metric (since the latter sequence is fundamental and $\mathbb{Z}_p$ is closed in $\mathbb{Q}_p$ which is a complete metric space). Now we just put $f_{\mathfrak{A}}(z)$ to be a limit point of the sequence $(f_{n,\mathfrak{A}}(z \bmod p^n))_{n=1}^{\infty}$. Thus, the mapping $f_{\mathfrak{A}}$ is a well-defined function with domain $\mathbb{Z}_p$ and values in $\mathbb{Z}_p$; by (8) the function $f_{\mathfrak{A}}$ satisfies Lipschitz condition with a constant 1 w.r.t. p-adic metric. For instance, for the automaton $\mathfrak{A}$ whose state diagram is represented by Figure 9, the automaton function $f_{\mathfrak{A}}$ is just multiplication by 5 in the space of all 2-adic integers; i.e., $f_{\mathfrak{A}}(z) = 5z$ for all $z \in \mathbb{Z}_2$. The automaton $\mathfrak{B}$ whose state diagram is represented by Figure 11 is an autonomous automaton; the domain and range of its automaton function are 2-adic integers; $f_{\mathfrak{B}}(z) = -\frac{1}{3} = \sum_{j=0}^{\infty} 2^{2j} =$

$(01)^\infty$ if we choose 1 as initial state, and $f_{\mathfrak{B}}(z) = -\frac{2}{3} = \sum_{j=0}^{\infty} 2^{2j+1} = (10)^\infty$ if we choose 2 as initial state. One more example of a state diagram of an autonomous automaton is given by Figure 14; its automaton function is a constant $2/7 \in \mathbb{Z}_2$.

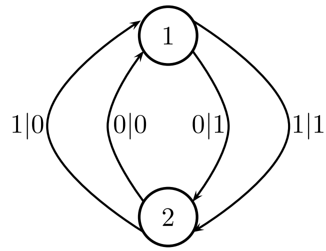

FIGURE 11: Example state diagram of autonomous automaton

The point is that *the class of all automata functions that correspond to automata with p-letter input/output alphabets coincides with the class of all maps from $\mathbb{Z}_p$ to $\mathbb{Z}_p$ that satisfy the p-adic Lipschitz condition with a constant 1* (the 1-Lipschitz maps, for brevity), cf., e.g., [3]. We note that the claim can also be derived from a more general result on asynchronous automata [23, Proposition 3.7]; for $p = 2$ the claim was proved in [56].

Further we need more detailed information about *finite automata functions*, that is, about functions $f_{\mathfrak{A}} \colon \mathbb{Z}_p \to \mathbb{Z}_p$ where $\mathfrak{A} = \mathfrak{A}(s_0)$ is a finite automaton (i.e., with a finite set $\mathcal{S}$ of states). It is well known (cf. previous subsection 2.4.) that *the class of finite automata functions is closed w.r.t. composition of functions and a sum of functions*: Once $f, g \colon \mathbb{Z}_p \to \mathbb{Z}_p$ are finite automata functions, either of mappings $x \mapsto f(g(x))$ and $x \mapsto f(x) + g(x)$ $(x \in \mathbb{Z}_p)$ is a finite automaton function. Another important property of finite automata functions is that *any finite automaton function maps $\mathbb{Z}_p \cap \mathbb{Q}$ into itself.* In view of (3), the latter property is just a re-statement of a a well-known property of finite automata which yields that any finite automaton fed by an eventually periodic sequence outputs an eventually periodic sequence, cf., e.g., [8, Corollary 2.6.9], [18, Chapter XIII, Theorem 2.2.]. Since further we often use that property of finite automata, we state it as a lemma for future references:

Lemma 2.1. *If a finite automaton $\mathfrak{A}$ is being fed by a left-infinite periodic word w^∞, where $w \in \mathcal{W}$ is a finite non-empty word, then the corresponding output left-infinite word is eventually periodic; i.e., it is of the form $u^\infty v$, where $u \in \mathcal{W}$, $v \in \mathcal{W}_\phi$. To put it in other words, if a finite automaton is being fed by an eventually periodic finite word $(w)^k t$, where $w \in \mathcal{W}$, $t \in \mathcal{W}_\phi$, and $k \in \mathbb{N}$ is sufficiently large, then the output word is of the form $r(u)^\ell v$, where $\ell \in \mathbb{N}$, $u \in \mathcal{W}$, $r, v \in \mathcal{W}_\phi$ and r is either empty or a prefix of u: $u = hr$ for a suitable $h \in \mathcal{W}_\phi$. Therefore the output word is of the form $(\bar{u})^\ell v'$, where $\bar{u}$ is a cyclically shifted word u.*

In literature, automata with multiple inputs and outputs over the same alphabet are also studied. We remark that in the case when the alphabet is $\mathbb{F}_p$, the automata can be considered as automata whose input/output alphabets are Cartesian powers $\mathbb{F}_p^n$ and $\mathbb{F}_p^m$, for suitable $m, n \in \mathbb{N}$. For these automata a theory similar to that of automata with a single input/output can be developed: Corresponding automata function are then 1-Lipshitz mappings from $\mathbb{Z}_p^n$ to $\mathbb{Z}_p^m$ w.r.t. p-adic metrics. Recall that p-adic absolute value on $\mathbb{Z}_p^k$ is defined as follows: Given $(z_1, \ldots, z_k) \in \mathbb{Z}_p^k$, put $|(z_1, \ldots, z_k)|_p = \max\{|z_i|_p : i = 1, 2, \ldots, k\}$. The so defined absolute value (and the corresponding metric) are non-Archimedean as well. Note that Theorem5.1 holds (after a proper re-statement) for these automata as well, see Theorem 5.2.

It is worth recalling here a well-known fact that *addition of two p-adic integers can be performed by a finite automaton with two inputs and one output*: Actually the automaton just finds successively (digit after digit) the sum by a standard addition-with-carry algorithm which is used to find a sum of two non-negative integers represented by base-p expansions thus calculating the sum with arbitrarily high accuracy w.r.t. the p-adic metric. On the contrary, *no finite automaton can perform multiplication of two arbitrary p-adic integers* since it is well known that no finite automaton can calculate a base-p expansion of a square of an arbitrary non-negative integer given a base-p expansion of the latter, cf., e.g., [8, Theorem 2.2.3].

The following properties of finite automata functions can be proved:

Proposition 2.5. *Let $\mathfrak{A}, \mathfrak{B}$ be finite automata, let $a, b \in \mathbb{Z}_p \cap \mathbb{Q}$ be p-adic rational integers. Then the following is true:*

1. *the mapping $z \mapsto f_{\mathfrak{A}}(z) + f_{\mathfrak{B}}(z)$ of $\mathbb{Z}_p$ into $\mathbb{Z}_p$ is a finite automaton function;*
2. *a composite function $f(z) = a \cdot f_{\mathfrak{A}}(z) + b$, $(z \in \mathbb{Z}_p)$, is a finite automaton function;*
3. *a constant function $f(z) = c$ is a finite automaton function if and only if $c \in \mathbb{Z}_p \cap \mathbb{Q}$;*
4. *an affine mapping $f(z) = c \cdot z + d$ is a finite automaton function if and only if $c, d \in \mathbb{Z}_p \cap \mathbb{Q}$.*

Concluding the subsection, we remark that in literature (finite) automata functions are also known under names of *(bounded) determinate functions*, or *(bounded) deterministic functions*, cf., e.g., [60].

2.6. Real plots of automata functions vs Monna graphs.

Further in the paper we consider special representation of automata functions by point sets of real and complex spaces. As we have already mentioned in previous section, two different representations of that sort may be considered: Via the Monna graphs (see e.g. [11, 12, 37, 40, 52]) and via real plots which were initially introduced in [5, Chapter 11]. In the paper we focus on real plots; however we will start this subsection with saying few words about Monna graphs since in some meaning they are counterpart of real plots and in literature they are used more often to represent automata maps on the real plane that real plots. But for our purposes we need automata plots rather than Monna graphs since the latter actually represent short-term behaviour of automaton while we need to study a long-term behaviour.

The Monna graphs are based on the Monna's representation of p-adic integers via real numbers of the unit closed segment $[0,1]$ originally suggested by Monna in [46]: Given a canonical expansion $z=\sum_{i=0}^{\infty}\alpha_ip^i$ of p-adic integer $z\in\mathbb{Z}_p$ (cf. Subsection 2.3.), consider a real number $\mathsf{mon}(z)=\sum_{i=0}^{\infty}\alpha_ip^{-i-1}\in[0,1]\subset\mathbb{R}$. It is clear that mon maps $\mathbb{Z}_p$ onto $[0,1]$, however, mon is not bijective: The only points from the open interval $(0,1)$ that have more than one (actually, exactly two) pre-image w.r.t. mon are rational numbers of the form $\sum_{i=0}^{\infty}\alpha_ip^{-i-1}$ where $\alpha_i=p-1$ for some $i\ge i_0$ since

$$\sum_{i=0}^{\infty}\alpha_ip^{-i-1}=\sum_{i=0}^{\infty}\beta_ip^{-i-1},\ \text{where} \tag{11}$$

$$\beta_j = \begin{cases}\alpha_j, & \text{if } j\le i_0-2;\\ (\alpha_{i_0-1}+1)\bmod p, & \text{if } j=i_0;\\ 0, & \text{if } j\ge i_0+1\end{cases}$$

where $\alpha_j=\beta_j$ for all $j\le i_0-2$, $\beta_j=0$ for all $j\ge i_0$ and $\beta_{i_0-1}=(\alpha_{i_0-1}+1)\bmod p$. We can naturally associate the segment $[0,1]$ (or a half-open interval $[0,1)$) to the real circle $\mathbb{S}$ by *reducing* $[0,1]$ *modulo 1*; that is, by taking fractional parts of reals from $[0,1]$: $\mathbb{S}=[0,1]\bmod 1$. Then in a similar manner we may consider a mapping of $\mathbb{Z}_p$ onto $\mathbb{S}$; we will denote the mapping also via mon since there is no risk of misunderstanding. Note that w.r.t. the latter mapping the point $0=1\in\mathbb{S}$ has exactly two pre-images since $\sum_{i=0}^{\infty}0\cdot p^{-i-1}=0=1=\sum_{i=0}^{\infty}(p-1)\cdot p^{-i-1}$ in $\mathbb{S}$.

Now, given an automaton $\mathfrak{A}=\mathfrak{A}(s_0)$, we define the *Monna graph* of $\mathfrak{A}$ as follows: Let $f=f_{\mathfrak{A}}$ be a corresponding automaton function, cf. Subsection 2.5. (that is, $f\colon\mathbb{Z}_p\to\mathbb{Z}_p$ is a 1-Lipschitz function w.r.t. p-adic metric). Then the Monna graph $\mathbf{M}(\mathfrak{A})=\mathbf{M}(f)$ (or, which is the same, of the automaton function f) is the point set $\mathbf{M}(\mathfrak{A})=\mathbf{M}(f)=\{(\mathsf{mon}(z),\mathsf{mon}(f(z)))\colon z\in\mathbb{Z}_p\}$. Note that we can consider the Monna graph when convenient either as a subset of the unit real square $\mathbb{I}^2$, a Cartesian square of a unit segment, $\mathbb{I}^2=[0,1]\times[0,1]$, or as a subset of a 2-dimensional real torus $\mathbb{T}^2=\mathbb{S}\times\mathbb{S}$, a Cartesian square of a real unit circle $\mathbb{S}$. A Monna graph can be considered as a graph of a real function $f^{\mathfrak{A}}$ defined on $[0,1]$ and valuated in $[0,1]$. Indeed, given a point $x\in[0,1]$, which is not of the form (11), there is a unique $z\in\mathbb{Z}_p$ such that $\mathsf{mon}(z)=x$. Therefore, $f^{\mathfrak{A}}$ is well defined at x since there exists a unique $y\in[0,1]$ such that $y=\mathsf{mon}(f_{\mathfrak{A}}(z))$; so we just put $f^{\mathfrak{A}}(x)=y$. Once x is of the form (11), then there exist exactly two $z_1,z_2\in\mathbb{Z}_p$, $z_1\ne z_2$ such that $\mathsf{mon}(z_1)=\mathsf{mon}(z_2)=x$. As $f_{\mathfrak{A}}(z_1)$ is not necessarily equal to $f_{\mathfrak{A}}(z_2)$, then $f^{\mathfrak{A}}$ may be not well defined at x: One have to assign to $f^{\mathfrak{A}}(x)$ both $\mathsf{mon}(f_{\mathfrak{A}}(z_1))$ and $\mathsf{mon}(f_{\mathfrak{A}}(z_2))$ which may happen to be non-equal. To make $f^{\mathfrak{A}}$

well defined on $[0,1]$ a usual way is to admit only representations of one (of two) types for x of the form (11); say, only those with finitely many non-zero terms, cf., e.g., [11, 12]. In this case the function $f^{\mathfrak{A}}$ becomes well-defined everywhere on $[0,1]$ and having points of discontinuity at maybe the points of type (11) only. A typical Monna graph of the function $f^{\mathfrak{A}}$ looks like the one represented by Figure 4.

Now we are going to introduce a notion of the *real plot* of an automaton function; the latter notion is somehow 'dual' to the notion of Monna graph. Given an automaton $\mathfrak{A} = \mathfrak{A}(s_0)$, we associate to an m-letter non-empty word $v = \gamma_{m-1}\gamma_{m-2}\cdots\gamma_0$ over the alphabet $\mathbb{F}_p$ a rational number $0.v$ whose base-p expansion is

$$0.v = 0.\gamma_{m-1}\gamma_{m-2}\ldots\gamma_0 = \sum_{i=0}^{m-1}\gamma_{m-i-1}p^{-i-1};$$

then to every m-letter input word $w = \alpha_{m-1}\alpha_{m-2}\cdots\alpha_0$ of the automaton $\mathfrak{A}$ and to the respective m-letter output word $\mathfrak{a}(w) = \beta_{m-1}\beta_{m-2}\cdots\beta_0$ (rightmost letters are fed to/outputted from the automaton prior to leftmost ones) there corresponds a point $(0.w; 0.\mathfrak{a}(w))$ of the real unit square $\mathbb{I}^2$; then we define $\mathbf{P}(\mathfrak{A})$ as a closure in $\mathbb{R}^2$ of the point set $(0.w; 0.\mathfrak{a}(w))$ where w ranges over the set $\mathcal{W}$ of all finite non-empty words over the alphabet $\mathbb{F}_p$.

Given an automaton function $f = f_{\mathfrak{A}}\colon \mathbb{Z}_p \to \mathbb{Z}_p$ define a set $\mathbf{P}(f_{\mathfrak{A}})$ of points of the real plane $\mathbb{R}^2$ as follows: For $k = 1, 2, \ldots$ denote

$$E_k(f) = \left\{\left(\frac{z \bmod p^k}{p^k}; \frac{f(z) \bmod p^k}{p^k}\right) \in \mathbb{I}^2 \colon z \in \mathbb{Z}_p\right\} \tag{12}$$

a point set in a unit real square $\mathbb{I}^2 = [0,1] \times [0,1]$ and take a union $E(f) = \cup_{k=1}^{\infty} E_k(f)$; then $\mathbf{P}(f)$ is a closure (in topology of $\mathbb{R}^2$) of the set $E(f)$. Note that if $z = \sum_{i=0}^{\infty}\gamma_i p^i$ is a p-adic canonical expansion of $z \in \mathbb{Z}_p$ then $p^{-m}(z \bmod p^m) = 0.\gamma_{m-1}\gamma_{m-2}\ldots\gamma_0$, c.f. (12); so $\mathbf{P}(\mathfrak{A}) \supset \mathbf{P}(f_{\mathfrak{A}})$. Moreover, $\mathbf{P}(\mathfrak{A}) = \mathbf{P}(f_{\mathfrak{A}})$, see further Note 2.4.

Definition 2.1. Automata plots *Given an automaton $\mathfrak{A}$, we call a* plot of the automaton $\mathfrak{A}$ *the set* $\mathbf{P}(\mathfrak{A})$. *We call a* limit plot *of the automaton $\mathfrak{A}$ the point set* $\mathbf{LP}(\mathfrak{A})$ *which is defined as follows: A point $(x; y) \in \mathbb{R}^2$ lies in* $\mathbf{LP}(\mathfrak{A})$ *if and only if there exist $z \in \mathbb{Z}_p$ and a strictly increasing infinite sequence $k_1 < k_2 < \ldots$ of numbers from $\mathbb{N}$ such that simultaneously*

$$\lim_{i\to\infty}\frac{z \bmod p^{k_i}}{p^{k_i}} = x; \ \lim_{i\to\infty}\frac{f_{\mathfrak{A}}(z) \bmod p^{k_i}}{p^{k_i}} = y. \tag{13}$$

Remark 2.3. Further in the paper we consider $\mathbf{LP}(\mathfrak{A})$ (as well as $\mathbf{P}(\mathfrak{A})$ and $\mathbf{P}(f)$) either as a subset of the unit square $\mathbb{I}^2 \subset \mathbb{R}^2$ or as a subset of the unit torus $\mathbb{T}^2 = \mathbb{R}^2/\mathbb{Z}^2$ when appropriate. Note that when considering the plot on the unit torus we reduce coordinates of the points modulo 1, that is, we just 'glue together' 0 and 1 of the unit segment $\mathbb{I}$ thus transforming it into the unit circle $\mathbb{S}$ (whose points we usually identify with the points of the half-open segment $[0,1)$ via a natural one-to-one correspondence, say, $\omega \leftrightarrow \sin^2(\omega/2)$).

Also, sometimes we consider $\mathbf{LP}(\mathfrak{A})$ (as well as $\mathbf{P}(\mathfrak{A})$ and $\mathbf{P}(f)$) as a subset of the cylinder $\mathbb{I}\times\mathbb{S}$ or of the cylinder $\mathbb{S}\times\mathbb{I}$ by reducing modulo 1 either y- or x-coordinate respectively. We denote the corresponding plot via $\mathbf{LP}_{\mathbb{M}}(\mathfrak{A})$ by using the subscript $\mathbb{M}\in\{\mathbb{I}^2,\mathbb{T}^2,\mathbb{I}\times\mathbb{S},\mathbb{S}\times\mathbb{I}\}$ and we omit the subscript when it is clear (or when it is no difference) on which of the surfaces the plot is considered.

We take a moment to recall some well-known topological notions and to introduce some notation. In the sequel, given a subset S of a topological (in particular, metric) space $\mathbb{M}$ which satisfies the Hausdorff axiom we denote via $\mathbf{AP}_{\mathbb{M}}(S)$ the set of all accumulation points of S. Recall that the point $x\in\mathbb{M}$ is called an *accumulation point of* $S\subset\mathbb{M}$ once every neighborhood of x contains infinitely many points from S; and a point $y\in\mathbb{M}$ is called *isolated point of* S (or, the point isolated from S; or, the point isolated w.r.t. S) once there exists a neighborhood $U\ni y$ such that U contains no points from S other than (maybe) y. We may omit the subscript and use notation $\mathbf{AP}(S)$ when it is clear from the context what metric space is meant.

We also write $\mathbf{AP}((a_i)_{i=0}^{\infty})$ (or briefly $\mathbf{AP}(a_i)$, or $\mathbf{AP}(\mathcal{C})$) for the set of all limit points of the sequence $\mathcal{C}=(a_i)_{i=0}^{\infty}$ over $\mathbb{M}$. Recall that a point $x\in\mathbb{M}$ is called a limit (or, cluster) point of the sequence $(a_i)_{i=0}^{\infty}$ if every neighbourhood of x contains infinitely many members of the sequence $(a_i)_{i=0}^{\infty}$; that is, given any neighborhood U of x, the number of i such that $a_i\in U$ is infinite (note that the very $a_i\in U$ are not assumed to be pairwise distinct points of $\mathbb{M}$; some, or even all of them may be identical). Note that in topology the terms 'accumulation point of a set' and 'limit point of a set' are used as synonyms; however to avoid possible misunderstanding we reserve the term 'limit point' only for sequences while for sets we use the term 'accumulation point'.

Remark 2.4. The definition of $\mathbf{P}(\mathfrak{A})$ immediately implies that $(x;y)\in\mathbf{P}(\mathfrak{A})$ if and only if there exists a sequence $(w_i)_{i=0}^{\infty}$ of finite non-empty words $w_i\in\mathcal{W}$ such that $\Lambda(w_i)=k_i$ for all $i=0,1,2,\dots$ and $\lim_{i\to\infty}\rho(w_i)=x$, $\lim_{i\to\infty}\rho(\mathfrak{a}(w_i))=y$. Note that once $(x;y)\in\mathbf{LP}(\mathfrak{A})$ then there exists a sequence $(w_i)_{i=0}^{\infty}$ of words such that the sequence $(\Lambda(w_i)=k_i)_{i=0}^{\infty}$ of their lengths is strictly increasing: One just may take $w_i=\mathsf{wrd}_{k_i}(z\bmod p^{k_i})$, cf. (2) and Subsection 2.5.. Therefore $\mathbf{LP}(\mathfrak{A})\subset\mathbf{AP}(\mathbf{P}(f_{\mathfrak{A}}))$. Moreover, from Definition 2.1 it readily follows that $\mathbf{AP}(\mathbf{P}(f_{\mathfrak{A}}))=\mathbf{AP}(E(f_{\mathfrak{A}}))=\mathbf{AP}(\mathbf{P}(\mathfrak{A}))$ since given a finite non-empty word w and taking any $z\in\mathbb{Z}_p$ such that the prefix of the corresponding infinite word is w (i.e., such that $w=\mathsf{wrd}_{\Lambda(w)}(z\bmod p^{\Lambda(w)})$) we see that $\rho(\mathfrak{a}(w))=((f_{\mathfrak{A}}(z))\bmod p^{\Lambda(w)})/p^{\Lambda(w)}$. This implies that $\mathbf{P}(\mathfrak{A})=\mathbf{P}(f_{\mathfrak{A}})$ since $\mathbf{P}(f_{\mathfrak{A}})=E(f_{\mathfrak{A}})\cup\mathbf{AP}(E(f_{\mathfrak{A}}))=\mathbf{P}(\mathfrak{A})$; so in the sequel we do not differ automata plots from the plots of automata functions and use both $\mathbf{P}(\mathfrak{A})$ and $\mathbf{P}(f_{\mathfrak{A}})$ as notation for the plot of the automaton $\mathfrak{A}$. Also we may use notation $\mathbf{LP}(f_{\mathfrak{A}})$ along with $\mathbf{LP}(\mathfrak{A})$ to denote the limit plot of the automaton $\mathfrak{A}$.

We stress here once again a crucial difference in the construction of plots and of Monna graphs of automata: Given a canonical expansion of p-adic integer $z=\sum_{i=0}^{\infty}\gamma_ip^i$ we put into correspondence to z a *single* real number $\mathsf{mon}(z)=\sum_{i=0}^{\infty}\gamma_ip^{-i-1}$ while constructing Monna graphs; whereas while constructing plots we associate to z a *whole set of all limit points* of the sequence $(p^{-m}(z\bmod p^m))_{m=1}^{\infty}$, and the latter set may not consist of a single point; moreover, 'usually' the set never consists of a single point since with a probability 1 the set is a whole segment $[0,1]$. Therefore to study structure of plots we need to work with sets of all limit points of (usually non-convergent) sequences rather than with limits of convergent sequences as in the case of Monna maps.

Theorem 2.1. *If automaton $\mathfrak{A}$ is finite and minimal then* $\mathbf{AP}(E(f_{\mathfrak{A}})) = \mathbf{LP}(\mathfrak{A})$.

It is well known (see e.g. [1, Ch.2, Exercise 2]) that the set of all accumulation points of a Hausdorff topological space (the *derived set* of the space) is a closed subset of the space. From Theorem 2.1 it follows that once a finite automaton is minimal then its limit plot is a derived set of its plot (whence, closed):

Corollary 2.3. *Let an automaton $\mathfrak{A}$ be finite and minimal; then the set $\mathbf{LP}(\mathfrak{A})$ is a derived set of $\mathbf{P}(\mathfrak{A})$ and therefore is closed in $\mathbb{R}^2$. A point $(x;y) \in \mathbb{R}^2$ belongs to $\mathbf{LP}(\mathfrak{A})$ if and only if there exists a sequence $\left(\alpha^{(i)}_{k_i-1}\dots\alpha^{(i)}_0\right)_{i=0}^{\infty}$ of finite non-empty words of strictly increasing lengths $k_0 < k_1 < k_2 < \cdots$ such that the sequence $\left(0.\alpha^{(i)}_{k_i-1}\alpha^{(i)}_{k_i-2}\dots\alpha^{(i)}_0\right)_{i=0}^{\infty}$ tends to x and the corresponding sequence $\left(0.\beta^{(i)}_{k_i-1}\beta^{(i)}_{k_i-2}\dots\beta^{(i)}_0\right)_{i=0}^{\infty}$ tends to y as $i\to\infty$, where $\beta^{(i)}_{k_i-1}\dots\beta^{(i)}_0$ are respective output words of the automaton $\mathfrak{A}$ that correspond to input words $\alpha^{(i)}_{k_i-1}\dots\alpha^{(i)}_0$* (i.e., $\beta^{(i)}_{k_i-1}\beta^{(i)}_{k_i-2}\dots\beta^{(i)}_0 = \mathfrak{a}(\alpha^{(i)}_{k_i-1}\alpha^{(i)}_{k_i-2}\dots\alpha^{(i)}_0)$, $i=0,1,2,\dots$).

We stress once again that words $\alpha_{k_i-1}\dots\alpha_0$ are fed to the automaton $\mathfrak{A}$ from right to left; i.e. the letter α_0 is fed to $\mathfrak{A}$ first, then the letter α_1 is fed to $\mathfrak{A}$, etc. It is worth noticing here that the limit plot of a finite minimal automaton does not depend on what state of the automaton is taken as initial:

Remark 2.5. If s,t are states of a finite minimal automaton $\mathfrak{A}$, $s\neq t$, then $\mathbf{LP}(\mathfrak{A}(s)) = \mathbf{LP}(\mathfrak{A}(t))$.

Indeed, due to the minimality, every state of $\mathfrak{A}$ is reachable from any other state of $\mathfrak{A}$. Therefore if $(x;y)\in\mathbf{LP}(\mathfrak{A}(t))$ then by Definition 2.1 there exist $z\in\mathbb{Z}_p$ and a strictly increasing infinite sequence $k_1<k_2<\dots$ of numbers from $\mathbb{N}$ such that (13) holds. By the minimality of $\mathfrak{A}$, there exists a finite word w of length $K>0$ such that after the automaton $\mathfrak{A}(s)$ has been fed by w, it reaches the state t. Now by substituting in Definition 2.1 $p^K\cdot z+\mathsf{num}(w)$ for z and $k_1+K<k_2+K<\dots$ for $k_1<k_2<\dots$ we see that (13) holds and therefore $(x;y)\in\mathbf{LP}(\mathfrak{A}(s))$.

Using an idea similar to that of Note 2.5 it can be easily demonstrated that if $\mathfrak{B}$ is a sub-automaton of $\mathfrak{A}$ then $\mathbf{P}(\mathfrak{B})\subset\mathbf{P}(\mathfrak{A})$ since every state of the automaton $\mathfrak{A}$ is reachable from its initial state:

Remark 2.6. Let $\mathfrak{B}=\mathfrak{B}(s)$ be a sub-automaton of the automaton $\mathfrak{A}$. As the initial state s of the automaton $\mathfrak{B}$ is reachable from the initial state s_0 of the automaton $\mathfrak{A}$, from the definition of the respective sets it immediately follows that $\mathbf{P}(\mathfrak{B})\subset\mathbf{P}(\mathfrak{A})$, $\mathbf{LP}(\mathfrak{B})\subset\mathbf{LP}(\mathfrak{A})$, and $\mathbf{AP}(\mathfrak{B})\subset\mathbf{AP}(\mathfrak{A})$.

The following useful lemma is a sort of a counter-part of Lemma 2.1 in terms of points from $\mathbf{LP}(\mathfrak{A})$ rather than in terms of words.

Lemma 2.2. *Given a finite automaton $\mathfrak{A}$ and a point $x \in \mathbb{Z}_p \cap \mathbb{Q}$, if $(x; y) \in \mathbf{LP}(\mathfrak{A})$ for some $y \in \mathbb{R}$ then $y \in \mathbb{Z}_p \cap \mathbb{Q}$.*

Yet one more property of automata plots is their invariance with respect to p-shifts. That is, *given a point $(x; y) \in \mathbf{P}(\mathfrak{A})$, take base-$p$ expansions $x = 0.\chi_1\chi_2\chi_3\ldots$, $y = 0.\xi_1\xi_2\xi_3\ldots$ of coordinates x, y; then $(0.\chi_2\chi_3\ldots; 0.\xi_2\xi_3\ldots) \in \mathbf{P}(\mathfrak{A})$*. To put it in other words, the following proposition is true:

Proposition 2.6. *For an arbitrary automaton $\mathfrak{A}$, if $(x; y) \in \mathbf{P}(\mathfrak{A}) \subset \mathbb{T}^2$ (resp., $(x; y) \in \mathbf{LP}(\mathfrak{A}) \subset \mathbb{T}^2$) then $((px) \bmod 1; (py) \bmod 1) \in \mathbf{P}(\mathfrak{A})$ (resp., $((px) \bmod 1; (py) \bmod 1) \in \mathbf{LP}(\mathfrak{A})$).*

It is known that the plot $\mathbf{P}(\mathfrak{A}) \subset \mathbb{I}^2$ of the automaton $\mathfrak{A}$ can be of two types only; namely, *given an automaton $\mathfrak{A}$, the set $\mathbf{P}(\mathfrak{A})$ either coincides with the whole unit square $\mathbb{I}^2$ or $\mathbf{P}(\mathfrak{A})$ is nowhere dense in $\mathbb{I}^2$*: Being closed in $\mathbb{R}^2$, the set $\mathbf{P}(\mathfrak{A})$ is measurable w.r.t. Lebesgue measure on $\mathbb{R}^2$, and the measure of $\mathbf{P}(\mathfrak{A})$ is 1 if and only if $\mathbf{P}(\mathfrak{A}) = \mathbb{I}^2$ and is 0 if otherwise: The later assertion is a statement of automata 0-1 law, cf. [5, Proposition 11.15] and [3]. Moreover, *once an automaton $\mathfrak{A}$ is finite, the measure of $\mathbf{P}(\mathfrak{A})$ is 0 and $\mathbf{P}(\mathfrak{A})$ is nowhere dense in $\mathbb{I}^2$* (cf. op. cit.). Therefore, *plots of finite automata are Lebesgue measure 0 nowhere dense closed subsets of the unit square $\mathbb{I}^2$*; thus they can not contain sets of positive measure, but they may contain lines. The goal of the paper is to prove that if $\mathfrak{A}$ is a finite automaton then smooth curves which lies completely in $\mathbf{P}(\mathfrak{A})$ (thus in $\mathbf{LP}(\mathfrak{A})$, cf. further Theorem 5.1) can only be straight lines. Moreover, we will prove that *if finite automata plots are considered as subsets of the unit torus $\mathbb{T}^2$ in $\mathbb{R}^3$ then smooth curves lying in the plots can only be torus windings.* For this purpose we will need some extra information (which follows) about torus knots.

2.7. Torus knots, torus links and linear flows on torus

Further in the paper we will need only few concepts concerning torus knots theory; details may be found in numerous books on knot theory, see e.g. [13, 43]. For our purposes it is enough to recall only two notions, the knot and the link. Recall that a knot is a smooth embedding of a circle $\mathbb{S}$ into $\mathbb{R}^3$ and a link is a smooth embedding of several disjoint circles in $\mathbb{R}^3$, cf. [43]. We will consider only special types of knots and links, namely, torus knots and torus links. Informally, a torus knot is a smooth closed curve without intersections which lies completely in the surface of a torus $\mathbb{T}^2 \subset \mathbb{R}^3$, and a link (of torus knots) is a collection of (possibly knotted) torus knots, see e.g. [17, Section 26] for formal definitions.

We also need a notion of a cable of torus. Formally, a cable of torus is any geodesic on torus. Recall that geodesics on torus $\mathbb{T}^2$ are images of straight lines in $\mathbb{R}^2$ under the mapping $(x; y) \mapsto (x \bmod 1; y \bmod 1)$ of $\mathbb{R}^2$ onto $\mathbb{T}^2 = \mathbb{R}^2/\mathbb{Z} \times \mathbb{Z}$, cf., e.g., [45, Section 5.4].

Definition 2.2. Cable of the torus *A* cable of the torus *is an image of a straight line in* $\mathbb{R}^2$ *under the map* $\mathsf{mod1}\colon (x;y) \mapsto (x \bmod 1; y \bmod 1)$ *of the Euclidean plain* $\mathbb{R}^2$ *onto the 2-dimensional real torus* $\mathbb{T}^2 = \mathbb{R}^2/\mathbb{Z}\times\mathbb{Z} = \mathbb{S}\times\mathbb{S}\subset\mathbb{R}^3$*. If the line is defined by the equation* $y = ax + b$ *we say that* a *is a* slope *of the cable* $\mathbf{C}(a,b)$*. We denote via* $\mathbf{C}(\infty,b)$ *a cable which corresponds to the line* $x = b$*, the* meridian*, and say that the slope is* ∞ *in this case. Cables* $\mathbf{C}(0,b)$ *of slope 0 (i.e., the ones that correspond to straight lines* $y = b$*) are called* parallels*.*

In dynamics, cables of torus $\mathbb{T}^2$ are viewed as orbits of *linear flows on torus*; that is, of dynamical systems on $\mathbb{T}^2$ defined by a pair of differential equations of the form $\frac{dx}{dt} = \beta; \frac{dy}{dt} = \alpha$ on $\mathbb{T}^2$, whence, by a pair of parametric equations $x = (\beta t + \tau) \bmod 1; y = (\alpha t + \sigma) \bmod 1$ in Cartesian coordinates, cf. e.g. [24, Subsection 4.2.3].

Remark 2.7. It is well known that a cable defined by the straight line $y = ax + b$ is dense in $\mathbb{T}^2$ if and only if $-\infty < a < +\infty$ and the slope $a = \frac{\alpha}{\beta}$ is irrational, see e.g. [24, Proposition 4.2.8] or [45, Section 5.4].

Given a Cartesian coordinate system XYZ of $\mathbb{R}^3$, a torus can be obtained by rotation around Z-axis of a circle which lies in the plain XZ. If a radius of the circle is r and the circle is centered at a point lying in X-axis at a distance R from the origin, then in cylindrical coordinates (r_0, θ, z) of $\mathbb{R}^3$ (where r_0 is a radius-vector in Cartesian coordinate system XY, θ is an angle of the radius-vector in coordinates XY, z is a Z-coordinate in Cartesian coordinate system XYZ) the torus is defined by the equation $(r_0 - R)^2 + z^2 = r^2$ and a cable (with a rational slope $\frac{\alpha}{\beta}$ where $\alpha \in \mathbb{Z}$ and $\beta \in \mathbb{N}$) of the torus is defined by the system of parametric equations (with parameter $s \in \mathbb{R}$) of the form

$$\begin{bmatrix} r_0 \\ \theta \\ z \end{bmatrix} = \begin{bmatrix} R + r\cos\left(\frac{\alpha}{\beta}s + \omega\right) \\ s \\ r\sin\left(\frac{\alpha}{\beta}s + \omega\right) \end{bmatrix}, \ s \in \mathbb{R}. \tag{14}$$

The cable defined by the above equations winds β times around Z-axis and $|\alpha|$ times around a circle in the interior of the torus (the sign of α determines whether the rotation is clockwise or counter-clockwise), see for an example of the corresponding torus knot Figures 15 and 16 where $\alpha = 5$ and $\beta = 3$. Letting ω in the above equations take a finite number of values we get an example of torus link, see e.g. Figures 18 and 19 which illustrate a link consisting of a pair of torus knots whose slopes are $\frac{3}{5}$. Note that Figures 20 and 21 illustrate a union of two distinct torus links (of two and of three knots respectively) rather than a single torus link of 5 knots. Finally, due to the above representation of a torus link in the form of equations in cylindrical coordinates, we naturally associate the torus link consisting of N cables with slopes $\frac{\alpha}{\beta}$ to a family of complex-valued functions $\psi_k\colon \mathbb{R} \to \mathbb{C}$ of real variable $s \in \mathbb{R}$

$$\left\{\psi_j(t) = e^{i(\frac{\alpha}{\beta}s + \omega_j)}\colon j = 0, 1, 2, \ldots, N-1\right\},$$

where i stands for imaginary unit $i \in \mathbb{C}$: $i^2 = -1$.

3. Plots of finite automaton functions: Constant and affine cases

In this section we completely describe limit plots of finite automata maps of the forms $z \mapsto c$ (constant maps), $z \mapsto az$ (linear maps) and $z \mapsto az + b$ (affine maps), where a, b, c are some (suitable) p-adic integers and the variable z takes values in $\mathbb{Z}_p$.

3.1. Limit plots of constants

Recall that an automaton $\mathfrak{A}(s_0) = \langle \mathcal{I}, \mathcal{S}, \mathcal{O}, S, O, s_0\rangle$ is called *autonomous* once neither its state update function S nor its output function O depend on input; i.e., when $s_{i+1} = S(s_i), \xi_i = O(\chi_i, s_i) = O(s_i)$ $(i = 0, 1, 2, \ldots)$, cf. Fig. 8.

It is clear that an autonomous automaton function is a constant; however a limit plot of this function is not necessarily a straight line. For instance, the limit plot of a constant $c \in \mathbb{Z}_p$ is the whole unit square $\mathbb{I}^2$ once $c = \sum_{i=0}^{\infty} \alpha_i p^i$ where the infinite word $u = \ldots \alpha_2\alpha_1\alpha_0$ over $\mathbb{F}_p$ is such that every non-empty finite word $w = \gamma_{k-1}\gamma_{k-2}\ldots\gamma_0$ over $\mathbb{F}_p$ occurs as a subword in u; that is, if there exist a finite word v and an infinite word s over $\mathbb{F}_p$ such that u is a concatenation of v, w and s: $u = swv$, cf. [3].

On the other hand, once an autonomous automaton $\mathfrak{A}$ is finite, the corresponding infinite output word must necessarily be eventually periodic. That is, $c = \alpha_0 + \alpha_1 p + \cdots + \alpha_{r-1}p^{r-1} + (\beta_0 + \beta_1 p + \cdots + \beta_{t-1}p^{t-1}) \cdot \sum_{j=0}^{\infty} p^{r+tj}$ for suitable $\alpha_i, \beta_j \in \mathbb{F}_p$; therefore a finite autonomous automaton function is a rational constant, i.e., $c \in \mathbb{Z}_p \cap \mathbb{Q}$, cf. Propositions 2.1 and 2.5.

Furthermore, the numbers that correspond to (sufficiently long) finite output words are then all the form

$$0.\beta_k\beta_{k-1}\ldots\beta_0\beta_{t-1}\beta_{t-2}\ldots\beta_0\beta_{t-1}\beta_{t-2}\ldots\beta_0\ldots\beta_{t-1}\beta_{t-2}\ldots\beta_0\alpha_{r-1}\alpha_{r-2}\ldots\alpha_0$$

for $k = 0, 1, \ldots, t-1$. Consequently, the limit plot of the automaton (in $\mathbb{R}^2$) consists of t pairwise parallel straight lines which correspond to the numbers

$$0.\beta_k\beta_{k-1}\ldots\beta_0\beta_{t-1}\beta_{t-2}\ldots\beta_0\beta_{t-1}\beta_{t-2}\ldots\beta_0\ldots = 0.\beta_k\beta_{k-1}\ldots\beta_0(\beta_{t-1}\beta_{t-2}\ldots\beta_0)^\infty$$

where $k = 0, 1, \ldots, t-1$, cf. Subsection 2.6.; or (which is the same) to the numbers $0.(\beta_k\beta_{k-1}\ldots\beta_0\beta_{t-1}\beta_{t-2}\ldots\beta_{k+1})^\infty$. That is, all the lines from the limit plot are $y = p^\ell h \bmod 1$, $\ell \in \mathbb{N}_0$, for any line $y = h$ belonging to the limit plot; thus the number of lines in the limit plot does not exceed t. Respectively, being considered as a point set on the torus $\mathbb{T}^2$, the limit plot consists of not more than t parallels, cf., e.g., Figures 12 and 13.

Now we present a more formal argument and derive a little bit more information about the number of lines in the limit plot. Given $q \in \mathbb{Z}_p \cap \mathbb{Q}$, represent q as an irreducible fraction $q = a/b$ for suitable $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Note that $p \nmid b$ since $q \in \mathbb{Z}_p$.

Denote

$$\mathbf{C}(a/b) = \text{limit points of}\left\{\left(p^{\ell}\cdot\left(1-\frac{a}{b}\right)\right) \mathsf{mod}\ 1\colon \ell=0,1,2,\dots\right\} = \text{limit points of}\left\{\left(-p^{\ell}\cdot\frac{a}{b}\right) \mathsf{mod}\ 1\colon \ell=0,1,2,\dots\right\}. \quad (15)$$

Since $a/b \in \mathbb{Z}_p \cap \mathbb{Q}$, by Proposition 2.1 a p-adic canonical form of a/b is

$$a/b = \alpha_0 + \alpha_1 p + \cdots + \alpha_{r-1}p^{r-1} + (\beta_0 + \beta_1 p + \cdots + \beta_{t-1}p^{t-1}) \cdot \sum_{j=0}^{\infty} p^{r+tj} \quad (16)$$

for suitable $\alpha_i, \beta_m \in \{0,1,\dots,p-1\}$, or, in other words, the infinite word that corresponds to a/b is $(\beta_{t-1}\dots\beta_0)^{\infty}\alpha_{r-1}\dots\alpha_0$. Then from Proposition 2.3 it follows that

$$(a/b)\ \mathsf{mod}\ 1 = (p^r \cdot 0.(\hat{\beta}_{t-1}\dots\hat{\beta}_0)^{\infty})\ \mathsf{mod}\ 1 = 0.(\hat{\beta}_{t-1-\bar{r}}\hat{\beta}_{t-2-\bar{r}}\dots\hat{\beta}_0\hat{\beta}_{t-1}\hat{\beta}_{t-2}\dots\hat{\beta}_{t-\bar{r}})^{\infty}\ \mathsf{mod}\ 1,$$

where $\hat{\beta}_i = p-1-\beta_i$, $i=0,1,2,\dots,t-1$, and $\bar{r}$ is the least non-negative residue of r modulo t if $t>1$ or $\bar{r}=0$ if otherwise. From here in view of (7) we deduce that

$$(-a/b)\ \mathsf{mod}\ 1 = 0.(\beta_{t-1-\bar{r}}\beta_{t-2-\bar{r}}\dots\beta_0\beta_{t-1}\beta_{t-2}\dots\beta_{t-\bar{r}})^{\infty}\ \mathsf{mod}\ 1$$

and thus

$$\mathbf{C}(a/b) = \{0.(\beta_{t-1-\ell}\beta_{t-2-\ell}\dots\beta_0\beta_{t-1}\beta_{t-2}\dots\beta_{t-\ell})^{\infty}\ \mathsf{mod}\ 1\colon \ell=0,1,2,\dots,t-1\} = \left\{\frac{\mathsf{num}(v)}{p^t-1}\colon v \in \{\hat{\zeta}_{t-1}\hat{\zeta}_{t-2}\dots\hat{\zeta}_0, \hat{\zeta}_{t-2}\hat{\zeta}_{t-3}\dots\hat{\zeta}_0\hat{\zeta}_{t-1}, \hat{\zeta}_{t-3}\hat{\zeta}_{t-4}\dots\hat{\beta}_0\hat{\zeta}_{t-1}\hat{\zeta}_{t-2},\dots\}\right\},$$

where $(a/b)\ \mathsf{mod}\ 1 = (\zeta_0 + \zeta_1\cdot p + \cdots + \zeta_{t-1}\cdot p^{t-1})(p^t-1)^{-1}$ (cf. Proposition 2.2 and Corollary 2.2). Now we can suppose that t is a period length of the rational p-adic integer $a/b \in \mathbb{Z}_p \cap \mathbb{Q}$ (cf. Subsection 2.3.); then in view of Proposition 2.4 we conclude that

$$\begin{aligned}\mathbf{C}(a/b) &= \{(-p^{\ell}\cdot(a/b))\ \mathsf{mod}\ 1\colon \ell=0,1,\dots,(\mathrm{mult}_b\, p)-1\} = \\ &\{0.(w)^{\infty}\ \mathsf{mod}\ 1\colon w \text{ runs through all cyclic shifts of the word } \beta_{(\mathrm{mult}_b\, p)-1}\dots\beta_0\} = \\ &\left\{0.(v)^{\infty}\ \mathsf{mod}\ 1\colon v \text{ runs through all cyclic shifts of the word } \hat{\zeta}_{(\mathrm{mult}_b\, p)-1}\dots\hat{\zeta}_0\right\} = \\ &\left\{\left(-p^{\ell}\cdot\frac{d}{p^{\mathrm{mult}_b\, p}-1}\right)\ \mathsf{mod}\ 1\colon \ell=0,1,\dots,(\mathrm{mult}_b\, p)-1\right\}\end{aligned} \quad (17)$$

since

$$1 - \frac{\zeta_0 + \zeta_1 p + \cdots + \zeta_{t-1}p^{t-1}}{p^t-1} = \frac{\hat{\zeta}_{t-1} + \hat{\zeta}_0 p + \hat{\zeta}_1 p^2 + \cdots + \hat{\zeta}_{t-2}p^{t-1}}{p^t-1} \text{ and}$$

$$p \cdot \frac{\hat{\zeta}_0 + \hat{\zeta}_1 p + \cdots + \hat{\zeta}_{t-1}p^{t-1}}{p^t-1} = \hat{\zeta}_{t-1} + \frac{\hat{\zeta}_{t-1} + \hat{\zeta}_0 p + \hat{\zeta}_1 p^2 + \cdots + \hat{\zeta}_{t-2}p^{t-1}}{p^t-1}.$$

Note that $0.(w)^\infty \bmod 1 = 0.(w)^\infty$ except of the case when $t = 1$ and w is a single-letter word that consists of the only letter $p-1$ (in the latter case $0.(w)^\infty = 1$ and thus $0.(w)^\infty \bmod 1 = 0$). Similarly, $0.(v)^\infty \bmod 1 = 0.(v)^\infty$ except of the case when $a/b \in \mathbb{Z}$ and thus $\zeta_0 = \ldots = \zeta_{t-1} = 0$ (so $\hat{\zeta}_0 = \ldots = \hat{\zeta}_{t-1} = p-1$ and $0.(v)^\infty = 1$). But this case happens if and only if $a/b \in \mathbb{Z}$; i.e., when $\mathbf{C}(a/b) = \{0\}$.

We now summarize all these considerations in a proposition:

Proposition 3.1. *Let $f_{\mathfrak{A}}\colon z \mapsto q$ be an automaton function of a finite automaton $\mathfrak{A}$* (therefore $q \in \mathbb{Z}_p \cap \mathbb{Q}$ by Proposition 2.5)*; then $\mathbf{LP}(\mathfrak{A}) \subset \mathbb{T}^2$ is a disjoint union of t parallels $\mathbf{C}(0,e)$, $e \in \mathbf{C}(q)$, and t is a period length of q* (cf. (15) and (17)).

Remark 3.1. In conditions of Proposition 3.1 the constant $q \in \mathbb{Z}_p \cap \mathbb{Q}$ can be represented as an irreducible fraction $q = a/b$ where $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $p \nmid b$ (we put $b = 1$ and $a = 0$ if $q = 0$). Then the limit plot $\mathbf{LP}(\mathfrak{A}) \subset \mathbb{T}^2$ is a torus link that consists of $t = \operatorname{mult}_b p$ trivial torus cables (parallels) with slopes 0; to the link there corresponds a collection of t complex constants (which are b-th roots of 1)

$$\left\{\psi_\ell = e^{-2\pi i p^\ell q} \colon \ell = 0, 1, \ldots, (\operatorname{mult}_b p) - 1\right\},$$

where i stands for imaginary unit $i \in \mathbb{C}$: $i^2 = -1$ (cf. Subsection 2.7.).

Being considered in the unit real square $\mathbb{I}^2$, the limit plot $\mathbf{LP}(\mathfrak{A})$ is a collection of $t = \operatorname{mult}_b p$ segments of straight lines $y = c(t,k,u)$ that cross $\mathbb{I}^2$, where

$$c(t,k,u) = \left(-p^k \cdot \frac{u}{p^t - 1}\right) \bmod 1 = \\ 0.(\hat{\zeta}_{t-1-k}\hat{\zeta}_{t-2-k}\ldots\hat{\zeta}_0\hat{\zeta}_{t-1}\hat{\zeta}_{t-2}\ldots\hat{\zeta}_{t-k})^\infty \bmod 1;\ k = 0, 1, \ldots, t-1. \tag{18}$$

Here $q \bmod 1 = u(p^t - 1)^{-1}$, $0 \le u \le p^t - 2$, and a base p-expansion of u is $u = \zeta_0 + \zeta_1 \cdot p + \cdots + \zeta_{t-1} \cdot p^{t-1}$ (cf. Proposition 2.2); $\hat{\zeta} = p - 1 - \zeta$ for $\zeta \in \{0, 1, \ldots, p-1\}$. In other words, all the constants $c(t,k,u)$ are of the form

$$c(t,k,u) = 0.v^\infty \bmod 1 = \frac{\mathsf{num}(v)}{p^t - 1} \bmod 1, \tag{19}$$

where v runs trough all cyclic shifts of the word $\hat{\zeta}_{t-1}\hat{\zeta}_{t-2}\ldots\hat{\zeta}_0$; that is,

$$v \in \{\hat{\zeta}_{t-1}\hat{\zeta}_{t-2}\ldots\hat{\zeta}_0, \hat{\zeta}_{t-2}\hat{\zeta}_{t-3}\ldots\hat{\zeta}_0\hat{\zeta}_{t-1}, \ldots\}.$$

If q is represented in a p-adic canonical form (16) rather than in a form of Proposition 2.2, then all the lines of the limit plot can be represented as

$$y = 0.(\beta_{t-1-\ell}\beta_{t-2-\ell}\ldots\beta_0\beta_{t-1}\beta_{t-2}\ldots\beta_{t-\ell})^\infty \bmod 1;\ \ell = 0, 1, 2, \ldots, t-1. \tag{20}$$

Note that we may omit $\mathsf{mod} 1$ in (19) and in (20) in all cases but the case when simultaneously the length t of the period is 1 and $\hat{\zeta}_0 = p - 1$ (respectively, $\beta_0 = p - 1$); but $q \in \mathbb{Z}$ in that case and therefore $\mathbf{C}(q) = \{0\}$.

The following property of the set $\mathbf{C}(q)$ shows that the set is uniquely determined by any of its elements.

Corollary 3.1. *Given $q_1, q_2 \in \mathbb{Z}_p \cap \mathbb{Q} \cap [0,1)$, the following alternative holds: Either $\mathbf{C}(q_1) = \mathbf{C}(q_2)$ or $\mathbf{C}(q_1) \cap \mathbf{C}(q_2) = \emptyset$.*

Example 3.1. *Let $p = 2$ and $q = 2/7$. Then $\operatorname{mult}_7 2 = 3$ and the limit plot consists of 3 lines. The binary infinite word that corresponds to the 2-adic canonical representation of $2/7$ is $(011)^\infty 10$, so the period of $2/7$ is 011, the pre-period is 01, and $u = 2 = 0 + 1 \cdot 2 + 0 \cdot 2^2$. Therefore the tree lines of the limit plot are: $y = 0.(101)^\infty = 5/7 = (-2/7) \bmod 1 = c(3,0,2)$, $y = 0.(011)^\infty = 6/7 = (-1/7) \bmod 1 = c(3,2,2)$, $y = 0.(110)^\infty = 3/7 = (-4/7) \bmod 1 = c(3,1,2)$. The limit plot (on the unit square and on the torus) is illustrated by Figures 12 and 13 accordingly; the state diagram is given by Figure 14. Note that the plot does not depend on what state is taken as initial; the plot is completely determined by the minimal sub-automaton whose set of states is $\{3,4,5\}$.*

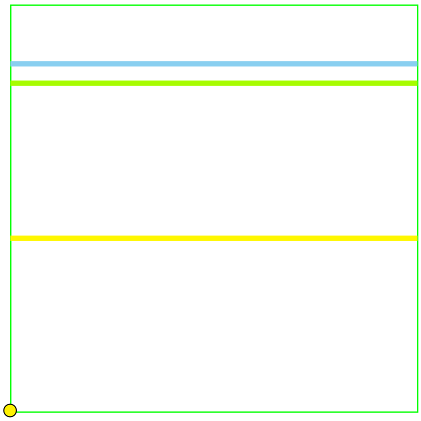

FIGURE 12: Limit plot of the constant function $f(z) = \frac{2}{7}$ ($z \in \mathbb{Z}_2$), in $\mathbb{R}^2$

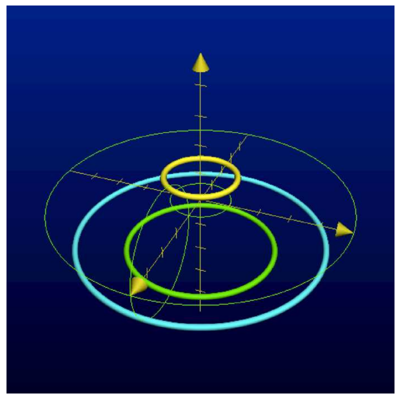

FIGURE 13: Limit plot of the same function on the torus $\mathbb{T}^2$

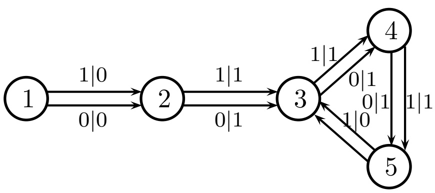

FIGURE 14: State diagram of autonomous automaton whose automaton function is a constant 2/7 when state 1 is taken as initial.

3.2. Limit plots of linear maps

In this subsection we consider limit plots of linear maps $z \mapsto cz$ $(z \in \mathbb{Z}_p)$ which are finite automaton functions. By Proposition 2.5, the latter takes place if and and only if $c \in \mathbb{Z}_p \cap \mathbb{Q}$.

Proposition 3.2. *Given $c \in \mathbb{Z}_p \cap \mathbb{Q}$, represent $c = a/b$, where $a \in \mathbb{Z}$, $b \in \mathbb{N}$, a, b are coprime, $p \nmid b$. If $\mathfrak{A}$ is an automaton such that $f_{\mathfrak{A}}(z) = cz$ $(z \in \mathbb{Z}_p)$ then $\mathbf{LP}(\mathfrak{A}) = \{(x \bmod 1; (cx) \bmod 1) \colon x \in \mathbb{R}\} = \mathbf{C}(c, 0)$ is a cable (with a slope c) of the unit 2-dimensional real torus $\mathbb{T}^2$. For every $c \in \mathbb{Z}_p \cap \mathbb{Q}$ the automaton $\mathfrak{A}$ may be taken a finite.*

Example 3.2. *Take $p = 2$ and $c = 5/3$. Figures 15 and 16 illustrate limit plot of the function $f(z) = (5/3) \cdot z$ in $\mathbb{I}^2$ and in $\mathbb{T}^2$ respectively. State diagram of corresponding automaton is given by Figure 17.*

FIGURE 15: Limit plot of the function $f(z) = \frac{5}{3}z$, $z \in \mathbb{Z}_2$, in $\mathbb{R}^2$

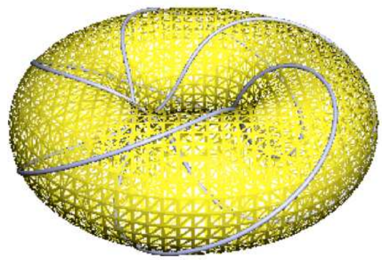

FIGURE 16: Limit plot of the same function on the torus $\mathbb{T}^2$

3.3. Limit plots of affine maps

In this subsection we combine the above two cases (constant maps and linear maps) into a single one to describe limit plots of finite automata whose functions are affine, i.e., of the form $z \mapsto c \cdot z + q$ $(z \in \mathbb{Z}_p)$. It is evident that the limit plot should be a torus link consisting of several disjoint cables with slopes c since the limit plot of the constant q is a collection of parallels, cf. Propositions 3.2 and 3.1. We will give a formal proof of this claim and find the number of knots in the link.

Recall that by Proposition 2.5 the map $z \mapsto c \cdot z + q$ of $\mathbb{Z}_p$ into itself is an automaton function of some finite automaton if and only if $c, q \in \mathbb{Z}_p \cap \mathbb{Q}$. The

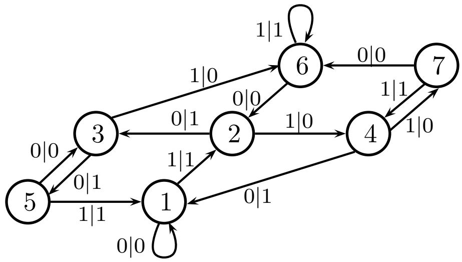

FIGURE 17: State diagram of the automaton whose function is $f(z) = \frac{5}{3}z$, $z \in \mathbb{Z}_2$ (state 1 is initial).

following proposition shows that we do not alter the limit plot of the map once we replace q by $q + n$ for arbitrary $n \in \mathbb{Z}$.

Proposition 3.3. *Given $f\colon z \mapsto cz + q$ $(z \in \mathbb{Z}_p)$ where $c, q \in \mathbb{Z}_p \cap \mathbb{Q}$, denote $\bar{q} = q \operatorname{\mathsf{mod}} 1$, $\bar{f}\colon z \mapsto cz + \bar{q}$. Then $\mathbf{LP}(f) = \mathbf{LP}(\bar{f})$.*

Note that the map $z \mapsto cz+\bar{q}$ from the statement of Proposition 3.3 is an automaton function for a suitable finite automaton $\mathfrak{B}$ and $\mathbf{LP}(\mathfrak{A}) = \mathbf{LP}(\mathfrak{B})$, where $\mathfrak{A}$ is a finite automaton whose automaton function is f.

Now we state main claim of the Section.

Theorem 3.1. *Given $c, q \in \mathbb{Z}_p$, a map $z \mapsto cz+q$ of $\mathbb{Z}_p$ into itself is an automaton function of a finite automaton if and only if $c, q \in \mathbb{Z}_p \cap \mathbb{Q}$. Given a finite automaton $\mathfrak{A}$ whose automaton function is $f(z) = cz + q$ for $c, q \in \mathbb{Z}_p \cap \mathbb{Q}$, represent c, q as irreducible fractions $c = a/b$, $q = a'/b'$, where $a, a' \in \mathbb{Z}$, $b, b' \in \mathbb{N}$ and $\gcd(a, b) = \gcd(a', b') = \gcd(b, p) = \gcd(b', p) = 1$; then the limit plot $\mathbf{LP}(\mathfrak{A}) \subset \mathbb{T}^2$ is a link of $\operatorname{mult}_m p$ torus knots, where $m = b'/\gcd(b, b')$, and every knot of the link is a cable $\mathbf{C}(c, e)$ for $e \in \mathbf{C}(q)$:*

$$\mathbf{LP}(\mathfrak{A}) = \{(y \operatorname{\mathsf{mod}} 1; (cy + e) \operatorname{\mathsf{mod}} 1) : y \in \mathbb{R}, e \in \mathbf{C}(q)\}. \tag{21}$$

Moreover, $\mathbf{C}(c, e_1) = \mathbf{C}(c, e_2)$ for $e_1, e_2 \in \mathbf{C}(q)$ if and only if $r_1 \equiv r_2 \pmod m$ where $e_i = (-p^{r_i} q) \operatorname{\mathsf{mod}} 1$, $i = 1, 2$, cf. (18).

Remark 3.2. Once $m = 1$, i.e., once $b' \mid b$, the congruence $r_1 \equiv r_2 \pmod m$ holds trivially, $\operatorname{mult}_1 p = 1$ and the link consists of a single knot; so in that case $\mathbf{C}(c, e_1) = \mathbf{C}(c, e_2)$ for all $e_1, e_2 \in \mathbf{C}(q)$.

We show here how to calculate the number of torus knots (cables) which constitutes the link $\mathbf{LP}(\mathfrak{A})$. Let for some $j_1, j_2 \in \{0, 1, \ldots, b - 1\}$, $(j_1 \neq j_2)$ and $e_1, e_2 \in \mathbf{C}(q)$ the following equality holds:

$$\left(\frac{j_1}{b} + e_1\right) \operatorname{\mathsf{mod}} 1 = \left(\frac{j_2}{b} + e_2\right) \operatorname{\mathsf{mod}} 1. \tag{22}$$

We see that $e_i = -p^{r_i}(\frac{a'}{b'}) \bmod 1$ for suitable $r_i \in \{0, 1, \ldots, (\mathrm{mult}_{b'} p) - 1\}$ by Note 3.1 ($i = 1, 2$). Therefore (22) is equivalent to the congruence

$$p^{r_1}\frac{a'}{b'} - p^{r_2}\frac{a'}{b'} \equiv \frac{j}{b} \pmod 1$$

for a suitable $j \in \{0, 1, \ldots, b-1\}$; but the latter congruence in turn is equivalent to the congruence

$$p^{r_2}\left(p^{r_1-r_2} - 1\right) a'n \equiv jm \pmod{nmd}, \tag{23}$$

where $d = \gcd(b', b)$, $m = b'/d$, $n = b/d$ (we assume that $r_1 > r_2$ since the case $r_1 = r_2$ is trivial). From here it follows that $p^{r_2}(p^{r_1-r_2} - 1)\, a'n \equiv 0 \pmod m$ once $m \neq 1$; therefore necessarily $r_1 \equiv r_2 \pmod{\mathrm{mult}_m p}$ since $\gcd(b', b) = \gcd(p, b) = \gcd(p, b') = 1$. So $(p^{r_1-r_2} - 1) = mh$ for a suitable $h \in \mathbb{N}$ and thus (23) is equivalent to the congruence $p^{r_2} ha'n \equiv j \pmod{nd}$, and the latter congruence gives the value of j (modulo $b = nd$) so that (22) is satisfied. This means that when $m \neq 1$, (22) holds if and only if $r_1 \equiv r_2 \pmod{\mathrm{mult}_m p}$. Thus, if $m \neq 1$ (that is, if b' is not a factor of b) then the number of pairwise distinct torus knots in the link is $\mathrm{mult}_m p$.

In the remaining case when $m = 1$ (i.e., when b' divides b) (23) always holds: If $p^{r_1-r_2} \equiv 1 \pmod d$ then we can take $j = 0$ to satisfy (23); otherwise the left-hand side of (23) just gives an expression for a unique residue j modulo $b = nd$ (which thus satisfies (23)). Therefore the link consists of a unique cable; so the number of pairwise distinct cables in the link is $1 = \mathrm{mult}_1 p$ in this case as well.

Remark 3.3. In conditions of Theorem 3.1 note that $b'|b$ is the only case when the link $\mathbf{LP}(\mathfrak{A})$ consists of a single cable . Note also that from the proof of Theorem 3.1 it is clear that if the number $\#\mathbf{C}(q)$ of points in $\mathbf{C}(q)$ is 1 then the link necessarily consists of a single cable. By note 3.1, $\#\mathbf{C}(q) = 1$ if and only if the period length of q is 1 and therefore $q \bmod 1 = 0.(\xi)^\infty \bmod 1$ for some $\xi \in \{0, 1, \ldots, p-1\}$).

Example 3.3. *Let $p = 2$ and $f(z) = (3/5) \cdot z + (1/3)$. Then in conditions of Theorem 3.1 we have that $m = 3$ and therefore the link consists of* $\mathrm{mult}_3 2 = 2$ *cables with slopes* $3/5$*, cf. Figures 18 and 19.*

Corollary 3.2. *There is a one-to-one correspondence between maps of the form $f\colon z \mapsto \frac{a}{b}z + \frac{a'}{b'}$ on $\mathbb{Z}_p$ (where $\frac{a}{b}, \frac{a'}{b'} \in \mathbb{Z}_p \cap \mathbb{Q}$; $a, a' \in \mathbb{Z}$; $b, b' \in \mathbb{N}$) and collections of* $\mathrm{mult}_m p$ *complex-valued exponential functions $\psi_k\colon \mathbb{R} \to \mathbb{C}$ of real variable $y \in \mathbb{R}$*

$$\left\{\psi_k(y) = e^{i(\frac{a}{b}y - 2\pi p^k \frac{a'}{b'})} \colon k = 0, 1, 2, \ldots, (\mathrm{mult}_m p) - 1\right\}.$$

Here $i \in \mathbb{C}$ is imaginary unit and $m = b'/\gcd(b, b')$.

Proof. Indeed, embedding the unit torus $\mathbb{T}^2$ into a 3-dimensional Euclidean space $\mathbb{R}^3$ and using cylindrical coordinates as in Note 2.7, in view of Theorem 3.1 every knot from the link can be expressed in the form (14) with $\omega = 2\pi e$ for

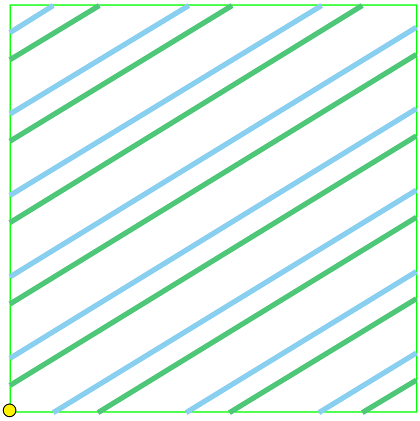

FIGURE 18: Limit plot of the function $f(z) = \frac{3}{5}z + \frac{1}{3}$, $z \in \mathbb{Z}_2$, in $\mathbb{R}^2$

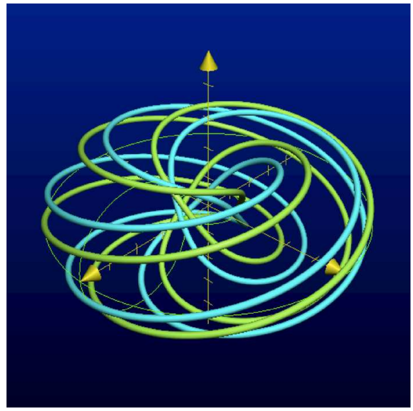

FIGURE 19: Limit plot of the same function on the torus $\mathbb{T}^2$

$e \in \mathbf{C}(q)$ since $\cos\omega$ and $\sin\omega$ specifies position of the point where the knot crosses zero meridian of the torus (i.e., when $\theta \equiv 0 \pmod{2\pi}$ in (14)). But $q = a'/b'$ and thus $\mathbf{C}(q) = \left\{(-p^\ell \cdot (a'/b')) \operatorname{mod} 1 \colon \ell = 0, 1, \ldots, (\mathrm{mult}_{b'}\, p) - 1\right\}$ by (17). As two such knots (with accordingly $\omega_i = 2\pi e_i$, $i = 1, 2$) coincide if an only if $\omega_1 \equiv \omega_2 \pmod{2\pi \cdot (a/b)}$ by (14), i.e., if and only if $e_1 \equiv e_2 \pmod{a/b}$. But the latter congruence is equivalent to (22); so finally the assertion follows from Theorem 3.1. □

4. FINITE COMPUTABILITY

In this section we introduce the notion of *finite computability*, and state some important properties of finitely computable functions.

Definition 4.1. *A non-empty point set $S \subset \mathbb{I}^2$ ($S \subset \mathbb{T}^2$, $S \subset \mathbb{I} \times \mathbb{S}$, $S \subset \mathbb{S} \times \mathbb{I}$) is called* (ultimately) finitely computable *(or, (ultimately) computable by a finite automaton) if there exists a finite automaton $\mathfrak{A}$ such that S is a subset of* $\mathbf{P}(\mathfrak{A})$ *(of* $\mathbf{LP}(\mathfrak{A})$*). We say that the automaton $\mathfrak{A}$* (ultimately) computes *the set S; and $\mathfrak{A}$ is called an* (ultimate) computing automaton *of the set S.*

In most further cases given a real function $g\colon D \to \mathbb{R}$ with the domain $D \subset \mathbb{R}$ by the *graph of the function* (on the torus $\mathbb{T}^2$) we mean the point subset $\mathbf{G}_D(g) = \{(x \operatorname{mod} 1; g(x) \operatorname{mod} 1) \colon x \in D\} \subset \mathbb{T}^2$. However, given a function $g\colon D \to T$ where either $D \subset [0,1]$ or $D \subset \mathbb{S}$ and T is either $[0,1]$ or $\mathbb{S}$, we call a graph $\mathbf{G}_D$ of the function g the set $\{(\bar{x}; \overline{g(x)}) \colon x \in D\}$ where either $\bar{x} = x$ if $D \subset [0,1]$ or $\bar{x} = x \operatorname{mod} 1$ if $D \subset \mathbb{S}$ and accordingly either $\overline{g(x)} = g(x)$ if $T = [0,1]$ or $\overline{g(x)} = (g(x)) \operatorname{mod} 1$ if $T = \mathbb{S}$. In the sequel we always explain what is meant by $\mathbf{G}_D(g)$ if this is not clear from the context. Also, we may omit the subscript D when it is clear what is the domain.

Definition 4.2. *Given a real function $g\colon D \to \mathbb{R}$ with domain $D \subset \mathbb{R}$ and an automaton $\mathfrak{A}$, the function g is called* (ultimately) computable by $\mathfrak{A}$ at the point $x \in D$ *if* $(x \bmod 1; g(x) \bmod 1) \in \mathbf{P}(\mathfrak{A}) \subset \mathbb{T}^2$ *($(x \bmod 1; g(x) \bmod 1) \in \mathbf{LP}(\mathfrak{A}) \subset \mathbb{T}^2$). Also, if either $D \subset [0,1]$ or $D \subset \mathbb{S}$ and $g\colon D \to T$ where either $T = \underline{[0,1]}$ or $T = \mathbb{S}$ we will say that* $\mathfrak{A}$ (ultimately) computes g at the point $x \in D$ *if* $(\bar{x}; \overline{g(x)}) \in \mathbf{LP}(\mathfrak{A})$ *where either $\bar{x} = x$ if $D \subset \underline{[0,1]}$ or $\bar{x} = x \bmod 1$ if $D \subset \mathbb{S}$ and accordingly either $\overline{g(x)} = g(x)$ if $T = [0,1]$ or $\overline{g(x)} = (g(x)) \bmod 1$ if $T = \mathbb{S}$ (cf. Note 2.3)*

Given a real function $g\colon D \to \mathbb{R}$ with domain $D \subset \mathbb{R}$, the function g is called (ultimately) finitely computable *(or,* (ultimately) computable by a finite automaton*) if there exists a finite automaton $\mathfrak{A}$ such that $\mathbf{G}(g) \subset \mathbf{P}(\mathfrak{A}) \subset \mathbb{T}^2$ ($\mathbf{G}(g) \subset \mathbf{LP}(\mathfrak{A}) \subset \mathbb{T}^2$). The automaton $\mathfrak{A}$ which* (ultimately) computes *the function g is called the* (ultimate) computing automaton *of the function g. In a similar manner we define these notions for the cases when $g\colon D \to T$ and D, T are as above.*

In loose terms, when assigning a real-valued function $f^{\mathfrak{A}}\colon [0,1] \to [0,1]$ to automaton $\mathfrak{A}$ via Monna map $\mathsf{mon} : \mathbb{Z}_p \to \mathbb{R}$ (cf. subsection 2.6.) one feeds the automaton by a base-p-expansion of argument $x \in [0,1]$ and considers the output as a base-p expansion of $f^{\mathfrak{A}}(x)$: A base-p expansion specifies a unique right-infinite word in the alphabet $\mathbb{F}_p$ and the automaton 'reads the word from head to tail', i.e., is fed by digits of the base-p expansion from left to right (i.e., digits on more significant positions are fed prior to digits on less significant positions); and the output word specifies a base-p expansion of a unique real number from $[0,1]$.

To examine functions computed by automata in the meaning of Definition 4.2 it would also be convenient to work with base-p expansions of real numbers; but the problem is that we need feed the automaton by a right-infinite word in the inverse order 'from tail (which is at infinity) to head': Digits on less significant positions (the rightmost ones) should be fed prior to digits on more significant positions (the leftmost ones). So straightforward inversion is impossible since it is unclear which letter should be the first when feeding the automaton this way; thus output word is undefined and so is the real number whose base-p expansion is the output word. So we proceed to rigorously specify that 'inversion'.

Let a function $g\colon D \to \mathbb{S}$ (or $g\colon D \to [0,1]$) whose domain D is either a subset of a real unit circle $\mathbb{S}$ or a subset of a unit segment $[0,1]$ be ultimately computable by a finite automaton $\mathfrak{A} = \mathfrak{A}(s_0)$; that is, for any $x \in D$ there exists $x \in \mathbb{Z}_p$ such that x is a limit point of the sequence $(z \bmod p^k/p^k)_{k=1}^{\infty}$ and $g(x)$ is a limit point of the sequence $((f_{\mathfrak{A}}(z)) \bmod p^k/p^k)_{k=1}^{\infty}$, where $f_{\mathfrak{A}}\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is automaton function of the automaton $\mathfrak{A}$, cf. Definition 4.2 and Definition 2.1. As said, further to examine finitely computable real functions it is however more convenient to work with automata maps as maps of reals into reals rather than to consider automata functions on p-adic integers and then represent $x \in \mathbb{R}$ and $g(x) \in \mathbb{R}$ as limit points of the sequences $(z \bmod p^k/p^k)_{k=1}^{\infty}$ and $((f_{\mathfrak{A}}(z)) \bmod p^k/p^k)_{k=1}^{\infty}$, respectively.

Further in this subsection we are going to show that once $x \in D$ and once $x = 0.\chi_1\chi_2\ldots$ is a base-p expansion of x, we can find a state $s = s(x) \in \mathcal{S}$ of the automaton $\mathfrak{A}$ and a strictly increasing infinite sequence of indices $1 \le k_1 < k_2 < \ldots$

such that the sequence $(0.\mathfrak{a}_s(\chi_1\chi_2\ldots\chi_{k_j}))_{j=1}^{\infty}$ tends to $(g(x))$ $\mathsf{mod}\ 1$ (recall that $\mathfrak{a}_s(\zeta_1\zeta_2\ldots\zeta_\ell)$ is an ℓ-letter output word of the automaton $\mathfrak{A}(s)$ whose initial state is s once the automaton has been fed by the ℓ-letter input word $\zeta_1\zeta_2\ldots\zeta_\ell$, cf. Subsection 2.4.). This means, loosely speaking, that once we feed the automaton $\mathfrak{A}(s)$ with approximations $0.\chi_1\chi_2\ldots\chi_{k_j}$ of x, the automaton outputs the sequence of approximations $0.\mathfrak{a}_s(\chi_1\chi_2\ldots\chi_{k_j})$ of $g(x)$, and these sequences tend to x and to $g(x)$ accordingly while $j\to\infty$. Moreover, we will show that if the function g is continuous then there exists a state $s\in\mathcal{S}$ such that all $x\in D$ for which $s(x)=s$ constitute a dense subset in D.

Recall that given $x\in(0,1)$, there exists a (right-)infinite word $w=\gamma_0\gamma_1\ldots$ over $\{0,1,\ldots,p-1\}$ such that

$$x=0.\gamma_0\gamma_1\ldots=0.w=\sum_{i=0}^{\infty}\gamma_i p^{-i-1}, \tag{24}$$

the *base-p expansion* of x. If x is not of the form $x=n/p^k$ for some $n=\alpha_0+\alpha_1p+\cdots+\alpha_\ell p^\ell\in\{0,1,\ldots,p^k-1\}$, where $\ell=\mathbf{le}(n)=\lfloor\log_p n\rfloor+1$ is the length of the base-p expansion of $n\in\mathbb{N}_0$ (recall that we put $\lfloor\log_p 0\rfloor=0$, cf. Subsection 2.5.), $\alpha_0,\alpha_1,\ldots\alpha_\ell\in\{0,1,\ldots,p-1\}$, then the right-infinite word $\mathsf{wrd}(x)=\gamma_0\gamma_1\ldots$ over $\{0,1,\ldots,p-1\}$ is uniquely defined (and the corresponding x is said to have a *unique* base-p expansion); else there are exactly two infinite words,

$$\mathsf{wrd}^r(x)=\alpha_0\alpha_1\ldots\alpha_{\ell-1}\alpha_\ell 00\ldots=\alpha_0\alpha_1\ldots\alpha_{\ell-1}\alpha_\ell(0)^\infty \tag{25}$$

$$\mathsf{wrd}^l(x)=\alpha_0\alpha_1\ldots\alpha_{\ell-1}(\alpha_\ell-1)(p-1)(p-1)\ldots=\alpha_0\alpha_1\ldots\alpha_{\ell-1}(\alpha_\ell-1)(p-1)^\infty, \tag{26}$$

where $\alpha_\ell\neq 0$, such that $x=0.\mathsf{wrd}_r(x)=0.\mathsf{wrd}_l(x)$. In that case x is said to have a *non-unique* base-p expansion; the corresponding base-p expansions are called *right* and *left* respectively. Both 0 and 1 are assumed to have unique base-p expansions since $0=0.00\ldots$, $1=0.(p-1)(p-1)\ldots$; so $\mathsf{wrd}(0)=00\ldots$, $\mathsf{wrd}(1)=(p-1)(p-1)\ldots$. This way we define $\mathsf{wrd}(x)$ for all $x\in[0,1]$; and to $x=n/p^k$ we will usually put into the correspondence both infinite words $\mathsf{wrd}^l(x)$ and $\mathsf{wrd}^r(x)$ if converse is not stated explicitly. The only difference in considering a unit circle $\mathbb{S}$ rather than the unit segment $\mathbb{I}=[0,1]$ is that we identify 0 and 1 and thus have two representations for 0, $0.(0)^\infty$ and $0=1\ \mathsf{mod}\ 1=0.(p-1)^\infty$.

Given a finite word $w=\alpha_{m-1}\alpha_{m-2}\cdots\alpha_0$, we denote via $\overrightarrow{w}$ the (right-)infinite word $\overrightarrow{w}=\alpha_{m-1}\alpha_{m-2}\cdots\alpha_0(0)^\infty$ and we put $0.\overrightarrow{w}=0.\alpha_{m-1}\alpha_{m-2}\cdots\alpha_0(0)^\infty\ldots$ (note that then $0.\overrightarrow{w}=\rho(w)$). Of course, $0.\overrightarrow{w}=0.w=\sum_{i=0}^{m-1}\alpha_i p^{-m+i}$; but we use notation $0.\overrightarrow{w}$ if we want to stress that we deal with infinite base-p expansion. To unify our notation, we also may write $\overrightarrow{w}=\zeta_1\zeta_2\ldots$ for a (right-)infinite word $w=\zeta_1\zeta_2\ldots$; then $0.\overrightarrow{w}=0.w=0.\zeta_1\zeta_2\ldots$.

Let $\overrightarrow{w}=\gamma_0\gamma_1\ldots$ be a (right-)infinite word over $\mathbb{F}_p=\{0,1,\ldots,p-1\}$. Given an automaton $\mathfrak{A}$ with the initial state s, we further denote via $\mathfrak{a}_s(\overrightarrow{w})$ the set of all limit points of the sequence $(\rho(\mathfrak{a}_s(\gamma_0\gamma_1\ldots\gamma_k)))_{k=0}^{\infty}$. We may omit the subscript s if it is clear from the context what is the initial state of the automaton.

Given $x \in [0,1]$ further $\mathfrak{a}_s(x)$ stands for $\mathfrak{a}_s(\overrightarrow{w}(x))$ if x admits a unique base-p expansion, and $\mathfrak{a}_s(x) = \mathfrak{a}_s(\overrightarrow{w}(x)_l) \cup \mathfrak{a}_s(\overrightarrow{w}(x)_r)$ if the expansion is non-unique (thus, if x admits both left and right base-p expansions). We also consider $\mathfrak{a}_s(x)$ for $x \in \mathbb{S}$ rather that for $x \in [0,1]$; in that case we take for 0 both base-p expansions $0.(0)^\infty$ and $0.(p-1)^\infty$ (since $0 = (0.(p-1)^\infty) \bmod 1$) and reduce modulo 1 all limit points of all sequences $(\rho(\mathfrak{a}_s(\gamma_0\gamma_1 \ldots \gamma_k)))_{k=0}^\infty$. We further use the same symbol $\mathfrak{a}_s(x)$ independently of whether we consider $x \in [0,1]$ or $x \in \mathbb{S}$; we make special remarks when this may cause a confusion.

We stress that $\mathfrak{a}_s(w)$ is a uniquely defined finite word whenever $w \in \mathcal{W}$ is a finite word (and therefore $\rho(\mathfrak{a}_s(w))$ consists of a single number), but in the case when w is an infinite word or w is a real number from $[0,1]$ (or $w \in \mathbb{S}$), the set $\mathfrak{a}_s(w)$ may contain more than one element.

Given $x \in \mathbb{Q} \cap [0,1]$, in view of Lemma 2.1 it is clear that if the automaton $\mathfrak{A}$ is finite then $\mathfrak{a}(x) \in \mathbb{Q} \cap [0,1]$ since a real number is rational if and only if its base-p expansion is eventually periodic. The following propositions reveals some more details about $\mathfrak{a}(x)$ for a rational x; and especially for $x = 0$.

Proposition 4.1. *If $\mathfrak{A}$ is finite, $x \in \mathbb{Q} \cap [0,1]$ then $\mathfrak{a}(x) \subset \mathbb{Q} \cap [0,1]$ and $\mathfrak{a}(x)$ is a finite set. Moreover, if $x \in \mathbb{Z}_p \cap \mathbb{Q} \cap [0,1]$ then $\mathfrak{a}(x) \subset \mathbb{Z}_p \cap \mathbb{Q} \cap [0,1]$. In particular, if $x = 0 \in \mathbb{S}$ then $\mathfrak{a}(x) = \mathbf{C}(q_1) \cup \mathbf{C}(q_2)$ for suitable $q_1, q_2 \in \mathbb{Z}_p \cap \mathbb{Q} \cap [0,1)$* (cf. Subsection 3.1.)*. Let a $\mathfrak{A}$-computable function $g\colon D \to \mathbb{S}$ be defined on the domain $D \subset \mathbb{S}$ and continuous at $0 \in D$. If the domain D is open then there exists $q \in \mathbb{Z}_p \cap \mathbb{Q} \cap [0,1)$ such that $\mathfrak{a}(0.(0)^\infty) = \mathfrak{a}(0.(p-1)^\infty) \in \mathbf{C}(q)$; and either $\mathfrak{a}(0.(0)^\infty) \in \mathbf{C}(q)$ or $\mathfrak{a}(0.(p-1)^\infty) \in \mathbf{C}(q)$ if the domain D is half-open and x is a boundary of D.*

Corollary 4.1. *Let $\mathfrak{A}$ be a finite automaton, let $(x;y) \in \mathbf{P}(\mathfrak{A}) \subset \mathbb{T}^2$, and let $x \in \mathbb{Z}_p \cap \mathbb{Q} \setminus \{0\}$; then $y \in \mathbb{Z}_p \cap \mathbb{Q}$. If $x = 0$ then $y \in [0,1) \cap \mathbb{Q}$; moreover, there exists $y \in \mathbb{Z}_p \cap \mathbb{Q}$ such that $(0;y) \in \mathbf{P}(\mathfrak{A})$.*

The following theorem shows that we may restrict our considerations of finitely computable continuous functions to the case when computing automata are minimal.

Theorem 4.1. *Given a continuous function $g\colon [a,b] \to [0,1]$, $[a,b] \subset [0,1]$ such that $\mathbf{G}(g) \subset \mathbf{P}(\mathfrak{A})$ for a finite automaton $\mathfrak{A}$, there exists a countable covering $\{[a'_j, b'_j] \subset [a,b] : j = 1,2,\ldots; a'_j < b'_j\}$ of the segment $[a,b]$ such that for every j the graph $\mathbf{G}(g_j)$ of the restriction g_j of the function g to the segment $[a'_j, b'_j]$ lies in $\mathbf{LP}(\mathfrak{A}_n)$ for a suitable minimal sub-automaton $\mathfrak{A}_n$ of $\mathfrak{A}$, $n = n(j)$.*

Remark 4.1. Theorem 4.1 remains true for a continuous function $g\colon [a,b] \to \mathbb{S}$ as well as for the case when $[a,b] \subset \mathbb{S}$.

The following proposition shows that we may if necessary consider only finitely computable continuous functions defined everywhere on the unit segment $[0,1]$ rather than on sub-segments of $[0,1]$.

Proposition 4.2. The similarity *If a continuous function* $g\colon [a,b] \to \mathbb{S}$, $[a,b] \subset [0,1]$, *is such that* $\mathbf{G}_{[a,b]}(g) \subset \mathbf{P}(\mathfrak{A})$ *for a suitable finite automaton* $\mathfrak{A} = \mathfrak{A}(s_0)$ *then for every* $n, m \in \mathbb{N}_0$ *such that* $m \geq \lfloor \log_p n \rfloor + 1$ *and* $n/p^m, (n+1)/p^m \in [a,b]$ *the function* $g_d(x) = (p^m g(d + p^{-m}x)) \bmod 1$, *where* $d = np^{-m}$, *is continuous on* $[0,1]$, *and* $\mathbf{G}_{[0,1]}(g_d) \subset \mathbf{P}(\mathfrak{A})$.

Corollary 4.2. *If a continuous function* $g\colon [a,b] \to \mathbb{S}$, $[a,b] \subset [0,1]$, *is such that* $\mathbf{G}_{(a,b)}(g) \subset \mathbf{P}(\mathfrak{A})$ *for a suitable finite automaton* $\mathfrak{A} = \mathfrak{A}(s_0)$ *then for every* $n, m \in \mathbb{N}_0$ *such that* $m \geq \lfloor \log_p n \rfloor + 1$ *and* $d = n/p^m \in [a,b)$

- *the function* $g_{d,M}(x) = (p^M g(d + p^{-M}x)) \bmod 1$ *is continuous on* $[0,1]$ *for all sufficiently large* $M \geq m$, *and*
- $\mathbf{G}_{[0,1]}(g_{d,M}) \subset \mathbf{P}(\mathfrak{A})$.

Remark 4.2. Corollary 4.2 shows that given any point $d' \in [a,b)$ and a rational approximation $d = np^{-m}$ of d', the graph of the function g on a sufficiently small closed neighbourhood $[a', b']$ of the point $d' \neq b'$ is similar to the graph of the function $g_{d,M}$ on $[0,1]$ where $d = np^{-m}$ and M is large enough.

Summarizing results of the subsection we may say that while considering a continuous function $g\colon [a,b] \to \mathbb{S}$ (where $[a,b] \subset [0,1]$ or $[a,b] \subset \mathbb{S}$) whose graph $\mathbf{G}(g)$ lies in $\mathbf{P}(\mathfrak{A})$ for some finite automaton $\mathfrak{A}$ one can if necessary assume that the function is defined and continuous on $[0,1]$ (or on $\mathbb{S}$ except for maybe a single point), the automaton $\mathfrak{A}$ is minimal, the function g is ultimately computable by $\mathfrak{A}$.

4.1. Finite computability of compositions

It is clear by intuition that a composition of finitely computable continuous functions should be a finitely computable continuous function. The following proposition states this formally and gives some extra information about the graph of a composite finitely computable function.

Proposition 4.3. *Let* $[a,b], [c,d] \subset [0,1]$ *and let* $g\colon [a,b] \to [0,1]$, $f\colon [c,d] \to [0,1]$ *be two continuous functions such that* $g([a,b]) \subset [c,d]$ *and there exist finite automata* $\mathfrak{A}$ *and* $\mathfrak{B}$ *such that* $\mathbf{G}_{[a,b]}(g) \subset \mathbf{P}(\mathfrak{A})$, $\mathbf{G}_{[c,d]}(f) \subset \mathbf{P}(\mathfrak{B})$. *Then there exists a covering* $\{[a'_j, b'_j] \subset [a,b] \colon j \in J\}$ *such that if* h_j *is a restriction of the composite function* $f(g)$ *to the sub-interval* $[a'_j, b'_j]$ *then* $\mathbf{G}_{[a'_j, b'_j]}(h_j) \subset \mathbf{P}(\mathfrak{C}_j)$ *for every* $j \in J$, *where* $\mathfrak{C}_j$ *is a sequential composition of the automaton* $\mathfrak{A}(s_j)$ *with the automaton* $\mathfrak{B}(t_j)$ *and* s_j, t_j *are suitable* (depending on j) *states of the automata* $\mathfrak{A}$, $\mathfrak{B}$ *accordingly.*

Remark 4.3. *Let* $[a,b] \subset [0,1]$, *let* $g\colon [a,b] \to \mathbb{S}$, $f\colon [a,b] \to \mathbb{S}$ *be two continuous functions, and let there exist finite automata* $\mathfrak{A}$ *and* $\mathfrak{B}$ *such that* $\mathbf{G}_{[a,b]}(g) \subset \mathbf{P}(\mathfrak{A})$, $\mathbf{G}_{[a,b]}(f) \subset \mathbf{P}(\mathfrak{B})$. *Then there exists a covering* $\{[a'_j, b'_j] \subset [a,b] \colon j \in J\}$ *such that if* h_j *is a restriction of the function* $(f+g) \bmod 1$ *to the sub-interval* $[a'_j, b'_j]$ *then* $\mathbf{G}_{[a'_j, b'_j]}(h_j) \subset \mathbf{P}(\mathfrak{C}_j)$ *for every*

$j \in J$, where $\mathfrak{C}_j$ is a sum of the automaton $\mathfrak{A}(s_j)$ with the automaton $\mathfrak{B}(t_j)$ and s_j, t_j are suitable (depending on j) *states of the automata $\mathfrak{A}$, $\mathfrak{B}$ accordingly.* Here by the sum of automata $\mathfrak{A}$ and $\mathfrak{B}$ we mean a sequential composition of the automata by automaton which has two inputs and a single output and performs addition of p-adic integers. The latter automaton is finite, see Subsection 2.5. and Proposition 2.5. Note also that we may assume that both f and g are defined on an arc of $\mathbb{S}$ rather than on $[a, b]$.

Corollary 4.3. *Given $A, B \in \mathbb{Z}_p \cap \mathbb{Q}$ and continuous finitely computable functions $f, g\colon [a, b] \to \mathbb{S}$, there exists a covering $\{[a'_j, b'_j] \subset [a, b]\colon j \in J\}$ such that the function $Af + Bg$ is finitely computable on every $[a'_j, b'_j]$.*

Comparing Theorem 4.1 with Proposition 4.3 we see that in the class of continuous functions there is no big difference between finite computability and ultimate finite computability since given a finitely computable continuous function on a segment there exists a covering of the segment by sub-segments such that the function is ultimately finitely computable on either of the sub-segments.

5. Main theorems

In this section we show that a graph of any C^2-smooth finitely computable function $g\colon [a, b] \to \mathbb{S}$, $[a, b] \subset [0, 1)$, lies (under a natural association of the half-open interval $[0, 1)$ with the unit circle $\mathbb{S}$) on a torus winding with a p-adic rational slope; and if $\mathfrak{A}$ is a finite automaton that computes g then necessarily the graph of the automaton contains the whole winding. Moreover, we prove a generalization of this theorem for multivariate functions.

5.1. The univariate case

Here we show that C^2-smooth finitely computable functions defined on $[a, b] \subset [0, 1)$ and valuated in $[0, 1)$ are only affine ones. Once we associate the half-open interval $[0, 1)$ with a unit circle $\mathbb{S}$ under a natural bijection we may consider graphs of the functions as subsets on a surface of the unit torus $\mathbb{T}^2 = \mathbb{S} \times \mathbb{S}$. We show that then the graphs lie only on cables of the torus $\mathbb{T}^2$, and the slopes of the cables must be p-adic rational integers (i.e., must lie in $\mathbb{Z}_p \cap \mathbb{Q}$), see Subsection 2.7. for definitions of torus knots, cables of torus, and links of knots.

Theorem 5.1. *Consider a finite automaton $\mathfrak{A}$ and a continuous function g with domain $[a, b] \subset [0, 1)$, valuated in $[0, 1)$. Let $\mathbf{G}(g) \subset \mathbf{P}(\mathfrak{A})$, let g be two times differentiable on $[a, b]$, and let the second derivative g'' of g be continuous on $[a, b]$. Then there exist $A, B \in \mathbb{Q} \cap \mathbb{Z}_p$ such that $g(x) = (Ax + B) \bmod 1$ for all $x \in [a, b]$; moreover, the graph $\mathbf{G}_{[a,b]}(g)$ of the function g lies completely in the cable $\mathbf{C}(A, B) \subset \mathbf{LP}(\mathfrak{A})$ and $\mathbf{C}(A, \bar{B}) \subset \mathbf{LP}(\mathfrak{A})$ for all $\bar{B} \in \mathbf{C}(B \bmod 1)$.*

Given a finite automaton $\mathfrak{A}$, there are no more than a finite number of pairwise distinct cables $\mathbf{C}(A, B)$ of the unit torus $\mathbb{T}^2$ such that $\mathbf{C}(A, B) \subset \mathbf{P}(\mathfrak{A})$ (note that *$A, B \in \mathbb{Z}_p \cap \mathbb{Q}$* then).

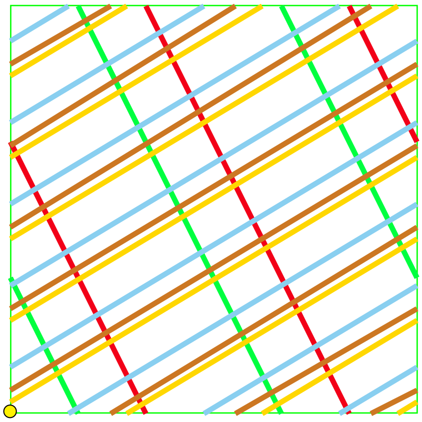

FIGURE 20: Limit plot in $\mathbb{R}^2$ of an automaton that has two affine subautomata $\mathfrak{A}$ and $\mathfrak{B}$; $f_{\mathfrak{A}}(z) = -2z + \frac{1}{3}$ and $f_{\mathfrak{B}}(z) = \frac{3}{5}z + \frac{2}{7}$, where $z \in \mathbb{Z}_2$.

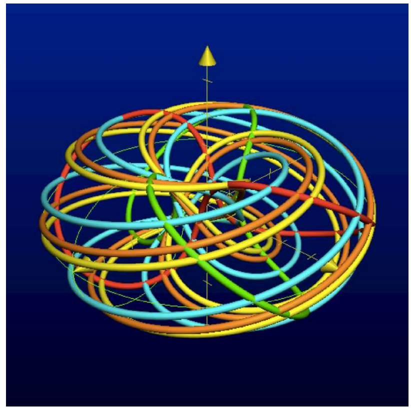

FIGURE 21: Limit plot of the same automaton on the torus $\mathbb{T}^2$ in $\mathbb{R}^3$. The plot consists of two torus links (of 2 and of 3 knots accordingly).

5.2. The multivariate case

In this subsection we extend Theorem 5.1 for the case of finite automata with multiply inputs/outputs. Note that actually an automaton over alphabet $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ with m inputs and n outputs can be considered as a letter-to-letter transducer with a single input over the alphabet $\{0, 1, \dots, p^m - 1\}$ and a single output over the alphabet $\{0, 1, \dots, p^n - 1\}$; therefore the plot of that automaton is a closed subset of the unit square $\mathbb{I}^2$. We however are going to consider plots of automata of that sort as subsets of multidimensional unit hypercube $\mathbb{I}^{m+n}$. Therefore automata functions of such automata are 1-Lipschitz mappings from $\mathbb{Z}_p^m$ to $\mathbb{Z}_p^n$, see Subsection 2.5.; and vice versa, every 1-Lipschitz mapping from $F\colon \mathbb{Z}_p^m \to \mathbb{Z}_p^n$ is an automaton function of a suitable automaton $\mathfrak{A}$ with m inputs and n outputs over the alphabet $\mathbb{F}_p$. Note that $F = (F_1; \dots; F_m)$ where $F_k\colon \mathbb{Z}_p^m \to \mathbb{Z}_p$ $(k = 1, 2, \dots, m)$ is 1-Lipschitz and therefore is an automaton function of an automaton with m inputs and a single output.

Now we re-state our definition of a (limit) plot for that case of automata with m inputs and n outputs.

Definition 5.1. Automata plots, the multivariate case *Given an automaton function $F = F_{\mathfrak{A}}\colon \mathbb{Z}_p^m \to \mathbb{Z}_p^n$ define a set $\mathbf{P}(F_{\mathfrak{A}})$ of points of $\mathbb{R}^{n+m}$ as follows: For $k = 1, 2, \dots$ denote*

$$E_k(F) = \left\{ \left(\frac{\mathbf{z} \bmod p^k}{p^k}; \frac{F(\mathbf{z}) \bmod p^k}{p^k} \right) \in \mathbb{I}^{m+n} \colon \mathbf{z} \in \mathbb{Z}_p^m \right\} \tag{27}$$

a point set in a unit real hypercube $\mathbb{I}^{m+n}$; here given $\mathbf{y}=(y_1;\dots;y_q)\in\mathbb{Z}_p^q$ we put

$$\frac{\mathbf{y} \bmod p^k}{p^k}=\left(\frac{y_1 \bmod p^k}{p^k};\dots;\frac{y_q \bmod p^k}{p^k}\right)\in(\mathbb{Z}/p^k\mathbb{Z})^q.$$

Then take a union $E(F)=\cup_{k=1}^{\infty}E_k(f)$ and denote via $\mathbf{P}(F)=\mathbf{P}(\mathfrak{A})$ a closure (in topology of $\mathbb{R}^{m+n}$) of the set $E(F)$.

Given an automaton $\mathfrak{A}$, we call a plot of the automaton $\mathfrak{A}$ *the set $\mathbf{P}(\mathfrak{A})$. We call a* limit plot *of the automaton $\mathfrak{A}$ the point set $\mathbf{LP}(\mathfrak{A})$ which is defined as follows: A point $(\mathbf{x};\mathbf{y})\in\mathbb{R}^{m+n}$ lies in $\mathbf{LP}(\mathfrak{A})$ if and only if there exist $\mathbf{z}\in\mathbb{Z}_p^m$ and a strictly increasing infinite sequence $k_1<k_2<\dots$ of numbers from $\mathbb{N}$ such that simultaneously*

$$\lim_{i\to\infty}\frac{\mathbf{z} \bmod p^{k_i}}{p^{k_i}}=\mathbf{x};\ \lim_{i\to\infty}\frac{F_{\mathfrak{A}}(\mathbf{z}) \bmod p^{k_i}}{p^{k_i}}=\mathbf{y}. \tag{28}$$

To put it in other words, at every step a letter-to-letter transducer $\mathfrak{A}$ (which has m inputs and n outputs over a p-symbol alphabet $\mathbb{F}_p$)

- obtains a vector $\mathbf{a}=(\alpha^{(1)};\dots,\alpha^{(m)})\in\mathbb{F}_p^m$ (each i-th letter $\alpha^{(i)}$ is sent accordingly to the i-th input of the automaton, $i=1,2,\dots,m$),
- outputs a vector $\mathbf{b}=(\beta^{(1)};\dots,\beta^{(n)})\in\mathbb{F}_p^n$ (each j-th output of the automaton outputs accordingly the letter $\beta^{(j)}$, $i=1,2,\dots,n$) which depends both on the current state and on the input vector $\mathbf{a}$,
- reaches the next state (which depends both on $\mathbf{a}$ and on the current state).

Then the routine repeats. Therefore after k steps the automaton $\mathfrak{A}$ transforms the input m-tuple $\mathbf{w}=(w_1;\dots;w_m)$ of k-letter words $w_i=\alpha_k^{(i)}\dots\alpha_1^{(i)}$ $(i=1,2,\dots,m)$ into the output n-tuple $\mathbf{v}=\mathfrak{a}(\mathbf{w})=(v_1;\dots;v_n)$ of k-letter words $v_j=\mathfrak{a}^{(j)}(\mathbf{w})=\beta_k^{(j)}\dots\beta_1^{(j)}$ $(j=1,2,\dots,n)$. For $\mathbf{w}$ running over all m-tuples of k-letter words, $k=1,2,\dots$ we consider the set $E(\mathfrak{A})$ of all points $(0.\mathbf{w};0.\mathfrak{a}(\mathbf{w}))\in\mathbb{R}^{m+n}$; here $0.\mathbf{u}$ stands for $(0.u_1;\dots;0.u_\ell)$ where $u_1,\dots,u_\ell$ are k-letter words. Then we define $\mathbf{P}(\mathfrak{A})$ as a closure in $\mathbb{R}^{m+n}$ of the set $E(\mathfrak{A})$. Following the lines of Note 2.4 it can be shown that $\mathbf{P}(\mathfrak{A})=\mathbf{P}(F_{\mathfrak{A}})$. We stress that $\mathfrak{A}$ is a synchronous letter-to-letter transducer; that is why in the definition of the plot all m input words as well as corresponding n output words of the automaton must have pairwise equal lengths.

Given a real function $G\colon D\to\mathbb{R}^n$ with the domain $D\subset\mathbb{R}^m$, by the *graph of the function* (on the torus $\mathbb{T}^{m+n}$) we mean the point subset $\mathbf{G}_D(g)=\{(\mathbf{x} \bmod 1; G(\mathbf{x}) \bmod 1)\colon \mathbf{x}\in D\}\subset\mathbb{T}^{m+n}$. Note that if $\mathbf{y}=(y_1;\dots;y_k)\in\mathbb{R}^k$ then $\mathbf{y} \bmod 1$ stands for $(y_1 \bmod 1;\dots;y_k \bmod 1)$.

Theorem 5.2. *Let $\mathfrak{A}$ be a finite automaton over the alphabet $\{0,1,\dots,p-1\}$, let $\mathfrak{A}$ have m inputs and n outputs, and let $G=(G_1;\dots;G_n)\colon[\mathbf{a},\mathbf{b}]=[a_1,b_1]\times\dots\times[a_m,b_m]\to[0,1)^n$ (where $[a_i,b_i]\subset[0,1)$, $G_i\colon[\mathbf{a},\mathbf{b}]\to[0,1)$, $i=1,2,\dots,m$) be* *a two times differentiable function such that all its second partial derivatives are continuous on* $[\mathbf{a}, \mathbf{b}]$. *If* $\mathbf{G}(G) \subset \mathbf{P}(\mathfrak{A}) \subset \mathbb{T}^{m+n}$ *then there exist an* $m \times n$ *matrix* $\mathbf{A} = (A_{ij})$ *and a vector* $\mathbf{B} = (B_1; \ldots; B_n)$ *such that* $A_{ij} \in \mathbb{Q} \cap \mathbb{Z}_p$, $B_j \in \mathbb{Q} \cap \mathbb{Z}_p \cap [0,1)$ $(i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n)$ *and* $G(\mathbf{x}) = (\mathbf{x}\mathbf{A} + \mathbf{B}) \bmod 1$ *for all* $\mathbf{x} \in [\mathbf{a}, \mathbf{b}]$. *There are not more than a finitely many* $\mathbf{A}$ *and* $\mathbf{B}$ *such that* $A_{ij} \in \mathbb{Q} \cap \mathbb{Z}_p$, $B_j \in \mathbb{Q} \cap \mathbb{Z}_p \cap [0,1)$ $(i = 1, 2, \ldots, m; j = 1, 2, \ldots, n)$ *and* $\mathbf{G}_{[\mathbf{a},\mathbf{b}]}((\mathbf{x}\mathbf{A} + \mathbf{B}) \bmod 1) \subset \mathbf{P}(\mathfrak{A})$ *for some* $[\mathbf{a}, \mathbf{b}] \subset [0,1)^m$*; moreover, if* $\mathbf{G}_{[\mathbf{a},\mathbf{b}]}(\mathbf{x}\mathbf{A} + \mathbf{B}) \subset \mathbf{P}(\mathfrak{A})$ *for some* $[\mathbf{a}, \mathbf{b}] \subset [0,1)^m$ *then* $\mathbf{G}_{\mathbb{R}^m}((\mathbf{x}\mathbf{A} + \mathbf{B}) \bmod 1) \subset \mathbf{P}(\mathfrak{A}) \subset \mathbb{T}^{n+m}$.

Remark 5.1. An automaton with a single input and a single output over respective alphabets $\{0, 1, \ldots, p^n - 1\}$ and $\{0, 1, \ldots, p^k - 1\}$, $(n, k \geq 1)$, can be considered as an automaton with n inputs and k outputs over an alphabet $\{0, 1, \ldots, p - 1\}$ and therefore Theorem 5.2 can be applied to automata of that sort as well.

6. *It from bit*, INDEED

Now we are going to outline possible relations of main results of preceding section to quantum theory. Although further physical interpretation of the results is highly speculative, it reveals deep analogies between automata and quantum systems and thus worth a short discussion to explain a direction in which it is reasonable to develop the results in order to derive some physically meaningful assertions (and maybe models) from mathematical theorems of the paper.

6.1. What is a physical law?

We start with some remarks on what is 'physical law'. Let us (somewhat naively) think of a physical law as of mathematical correspondence between quantities which express impacts a physical system is exposed to and quantities which express responses the system exhibits. Suppose for simplicity that both impacts and responses are scalars. As the measured experimental values of physical quantities are rational numbers (since there is no possibility to obtain during measurements an exact value of irrational number, cf. [54, 33, 34]) the result of measurements are points in $\mathbb{R}^2$, the experimental points. To find a particular physical law one seeks for a correspondence between cluster points (w.r.t. Euclidean metric in $\mathbb{R}^2$) of experimental values and tries to draw an experimental curve. The latter curve is a (piecewise) smooth curve (the C^2-smoothness is common) which is the best approximation of the set of the experimental points. A physical law is then a curve which approximate with the highest achievable accuracy (w.r.t. the said metric) the experimental curves obtained during series of measurements.

Let physical quantities which correspond to impacts and reactions be discrete; i.e, let they take only values (measured in suitable units and properly normalized), say, $0, 1, \ldots, p-1$, where $p > 1$ is an integer. Then, once the system is exposed to a sequence of k of impacts, it produces corresponding sequence of k reactions. Every impact changes current state of the system to a new one; therefore provided the systems is causal, both the next state and the reaction (effect) depend only on impacts (causes) the system has already been exposed to; so an automaton $\mathfrak{A}$ is an adequate model of the system[2]. Every finite sequence $\alpha_{k-1},\dots,\alpha_0$ of impacts/reactions corresponds to a base-p expansion of natural number $z=\alpha_{k-1}p^{k-1}+\cdots+\alpha_0$ to which after normalization there corresponds a rational number $\frac{z}{p^k}$. Every measurement is a sequence of interactions $\alpha_{k-1},\dots,\alpha_0$ of the measurement instrument with the system, and if the accuracy of the instrument is not better than p^{-N}, then the result of a single measurement lies within the segment $[\frac{z}{p^k}-p^{-N},\frac{z}{p^k}+p^{-N}]$. Assuming that $k\gg N$ we see that even if the system before every measurement has been prepared in a fixed state s_0 (the initial state of the automaton) during a single measurement the system $\mathfrak{A}(s_0)$ will be exposed to a random sequences of impacts $\alpha_{k-M-1},\dots,\alpha_0$ which switches the system to a new state $s=s(\alpha_{k-1},\dots,\alpha_0)$; so actually as a result of the measurement due to its limited accuracy we obtain an experimental point $(0.\alpha_k\dots\alpha_{k-M};0.\beta_k\dots\beta_{k-M})\in\mathbb{R}^2$ where $\beta_k\dots\beta_{k-M}$ is the output of the automaton $\mathfrak{A}(s)$ (whose initial state is $s=s(\alpha_{k-1},\dots,\alpha_0)$) fed by the sequence $\alpha_k,\dots,\alpha_{k-M}$.

Theorem 5.1 shows that if the number of states of the system $\mathfrak{A}$ is much less than the length of input sequence of impacts then experimental curves necessarily tend to straight lines (or torus windings, under a natural map of the unit square onto a torus), cf. Figures 1, 2, and 3. This may be judged as linearity of corresponding physical law and, what is even more important, the way experimental points are clustering on the unit square is very much alike to that of the points where electrons hit target screen in a double-slit experiment, cf. Figures 1–2 and Figure 5.

6.2. Can torus windings be wavefunctions?

By Theorem 5.1, the smooth curves from the plot of a finite automaton $\mathfrak{A}$ can be described by families of complex-valued exponential functions of the form $\psi_k(y)=e^{i(Ay-2\pi p^kB)}$, $k=0,1,2,\dots$, for suitable $A,B\in\mathbb{Z}_p\cap\mathbb{Q}$, cf. Corollary 3.2. The wave function of a particle is of the form $ce^{i(mx-t\omega)}$ where m is momentum, x position, ω angular frequency, and c is amplitude. Comparing the two expressions we see that p^k may serve as a time for the automaton $\mathfrak{A}$ since multiplication by p^k is a k-step shift of a base-p expansion of a number. But can we someway associate it to physical time t of quantum theory? In what follows we argue that yes, there is a natural way to do this.

Let us forget for a moment that p is a positive integer and suppose that $p=1+\tau$ where $1\gg\tau>0$ is a small real number; then $p^k\approx 1+k\tau$ if τ is a small time interval which is out of accuracy of measurements (e.g., let τ be Planck time which is approximately 10^{-43} s.). Therefore the torus link $\psi_k(y)=e^{i(Ay-2\pi p^kB)}$, $k=0,1,2,\dots$ can be approximately described by $\Psi(y,t)=e^{-i\cdot 2\pi B}e^{i(Ay-2\pi tB)}$,

[2]We stress that we are *not* speaking here about the so-called memory effect of the macroscopic measurement equipment which may 'remember' its previous interactions with particles, cf. [16]; we only say that every interaction (impact) forces the system (e.g. a particle) to change its state to some another one. We do *not* discuss the nature of these states which are *not* necessarily quantum states; we just say that every interaction changes something in a system and refer to this 'something' as to a 'state' of the system, and nothing more.

$y, t \in \mathbb{R}$ since it is reasonable to assume that $k\tau$ is just a time t as τ is a small time interval, a time quantum, the Planck time. But $\Psi(y,t)$ is a wave function of a particle with momentum A and angular frequency $2\pi B$. Is this mathematically correct to substitute $1+\tau$ for p in our reasoning? Yes, this is correct; but to explain why this is correct we need to recall a notion of *β-expansion* of a real number.

The β-expansions are radix expansions in non-integer bases; they were first introduced more than half-century ago, see [50, 49], and now β-expansions are a substantial part of dynamics, see e.g. survey [53]. Following [53], given $x \geq 0$ and $\beta \in \mathbb{R}$, $\beta > 1$ we call a sequence $(\chi_i)_{i=1}^{\infty}$ over the alphabet $\{0, 1, \ldots, \lfloor\beta\rfloor\}$ a *β-expansion* of x once $x = \sum_{i=-N}^{\infty} \chi_i \beta^{-i}$ for suitable $N \in \mathbb{Z}$ (here $\lfloor\beta\rfloor$ stands for the biggest integer from $\mathbb{Z}$ which does not exceed β). Note that sometimes the term β-expansion is used in a narrower meaning, when the 'digits' χ_i are obtained by the so-called 'greedy algorithm' only, cf. [41, Section 7.2] but this is not important at the moment: In what follows we just sketch the way how the results of current paper can be modified to handle the case of β-expansions rather than the case of base-p expansions only. We leave details and rigorous proofs for further paper.

From the definition we see that the notion of β-expansion is a generalization of the notion of base-p expansion: It is clear that for $\beta = p$ the β-expansion of x is just base-p expansion of x, and that is why both β-expansions and base-p expansions share some common properties. For instance, given β-expansion of reals it is possible to perform arithmetic operations with reals in a way similar to that of school-textbook algorithms for base-p expansions of reals. However, differences between base-p expansions and β-expansions should also be taken into the account since when β is not an integer, a β-expansion of a real number is generally not unique; moreover a real number may have a continuum of different β-expansions for β fixed. Nonetheless, we can perform arithmetic operations with numbers represented by β-expansions, i.e., with words over the alphabet $\{0, 1, \ldots, \lfloor\beta\rfloor\}$. These operations for some non-integer β may be represented by finite automata as well. For instance, if $\beta = \sqrt[n]{2}$ then arithmetic operations with numbers represented by $\sqrt[n]{2}$-expansions $\ldots\alpha_2\alpha_1\alpha_0$ and $\ldots\gamma_2\gamma_1\gamma_0$ (which are binary words over the alphabet $\{0,1\}$ since $\lfloor\sqrt[n]{2}\rfloor = 1$) can be performed in a manner similar to that when one applies school-textbook algorithms for base-p expansions, with the only difference: A 'carry' from i-th position should be added to $(n+i+1)$-th position; e.g. for $\beta = \sqrt{2}$ we have that $11 + 01 = 110$ while in the case $\beta = 2$ we have that $11 + 01 = 100$. Note that $01 = 1$, $11 = \sqrt{2}+1$ (and thus $110 = (\sqrt{2})^2 + (\sqrt{2})^1 + 0 = 2 + \sqrt{2}$) when $\beta = \sqrt{2}$; and $01 = 1$, $11 = 3$ when $\beta = 2$.

6.3. Bits come into play

When an automaton $\mathfrak{A}$ processes a word (or, a corresponding system responses to impacts) it just evaluates step-by-step a p-adic 1-Lipschitz function $f_{\mathfrak{A}}\colon \mathbb{Z}_p \to \mathbb{Z}_p$ (cf. Subsection 2.5.), and no β appears at that moment. But we need to specify β when we 'visualize' the function $f_{\mathfrak{A}}$ in $\mathbb{R}^2$: To every word $\alpha_{k-1}\ldots\alpha_0$ over the alphabet $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ we put into a correspondence a point

$\beta^{-k}(\alpha_{k-1}\beta^{k-1} + \cdots + \alpha_1\beta + \alpha_0) \in \mathbb{R}$; thus to every pair of input/output words of the automaton there corresponds a point in a square from $\mathbb{R}^2$(or, on a torus in $\mathbb{R}^3$). We then take a closure of all these points and obtain a *β-plot* of the automaton $\mathfrak{A}$ in a manner similar to one we have constructed a plot of the automaton (which corresponds to the case when $\beta = p$), cf. Definition 2.1. Note that if $\beta \in \mathbb{R}$ is not an integer then all real numbers represented by β-expansions $\sum_{i=1}^{\infty} \chi_i \beta^{-i}$ range from 0 to $\frac{\lfloor \beta \rfloor}{\beta - 1}$ and therefore β-plot lies in the square $[0, \frac{\lfloor \beta \rfloor}{\beta-1}] \times [0, \frac{\lfloor \beta \rfloor}{\beta-1}]$ rather than in the unit square $\mathbb{I}^2$. Note also that if $\beta = 1 + \tau$ where $0 < \tau \ll 1$ then the square tends to $[0, \infty) \times [0, \infty)$. Of course, after proper normalization the plot may be imbedded (if needed) into the unit square as well.

We then consider smooth curves in the β-plots of finite automata, in particular, the curves which correspond to affine automata functions $z \mapsto Az + B$. To these functions there correspond torus windings which can be expressed in a form of complex-valued functions $\psi_k(y) = e^{i(Ay - 2\pi\beta^k B)}$, $k = 0, 1, 2 \ldots$, $y \in \mathbb{R}$; and these functions can by approximated with arbitrarily high accuracy by functions $\Psi(y, t) = e^{-i\cdot 2\pi B} e^{i(Ay - 2\pi t B)}$, $t, y \in \mathbb{R}$, just by taking $\beta > 1$ sufficiently close to 1 (i.e., for $\beta = 1 + \tau$ with τ small, c.f. above). Moreover, the case when β is close to 1 is the only case when approximations are of the form of wavefunctions. But this means that the *corresponding automata must necessarily be binary*; i.e., their input/output alphabets are $\{0, 1, \ldots, \lfloor \beta \rfloor\} = \{0, 1\}$. So these automata (which are just models of causal discrete systems) indeed produce waves, the *its*, *from bits.*

From this view, main results of the current paper may be considered as a contribution to informational interpretation of quantum theory, namely, to J. A. Wheeler's *It from bit* doctrine which suggests that all things physical ('its') are information-theoretic in origin ('from bits'), [59]: We have given some evidence above that this is indeed so regarding particular 'its', the matter waves. We stress once again that our conclusion is based on the following assumptions only: *A quantum system is causal and discrete* (whence is an automaton) *and the number of states of the automaton is finite.*

6.4. More connections to physics

Also, from the above considerations it would be reasonable to conclude that p-adic mathematical physics should actually be 2-adic mathematical physics. Note that till now p is not still specified in p-adic mathematical physics, see e.g. [15].

It can be also of interest that the case $p = 2$ naturally leads to non-Archimedean (actually, 2-adic) time. Indeed, once automata (not necessarily finite) are considered as models of causal physical systems, usual condition of reversibility of evolution of a physical system implies that the automata must be reversible. This means that corresponding automata maps from $\mathbb{Z}_2$ to $\mathbb{Z}_2$ must be invertible. Since automata maps are 1-Lipschitz functions w.r.t. 2-adic metric, the invertibility is equivalent to measure-preservation w.r.t. normalized Haar measure, and moreover, that the functions are isometries of the space $\mathbb{Z}_2$, see [5, Subsection 4.4.1]. Note also that measure-preservation is just volume-preservation w.r.t. Haar measure, and when considering dynamical systems on configuration spaces which are models of physical systems it is usually assumed that dynamics must preserve volumes during evolution. Therefore standard demand of volume-preservation is equivalent to invertibility of automata maps; but for automata maps whose domain/range is 2-adic integers, invertibility implies that discrete time $0, 1, 2, \ldots$ can be uniquely expanded to 2-adic time so that the obtained dynamics will be continuous on both arguments, spatial and temporal. Namely, given a 1-Lipschitz (i.e., automaton) map $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$, for $j = 0, 1, 2, \ldots$ put as usual f^j to be j-th iterate of f; that is, $f^0(z) = z$, $f^{j+1}(z) = f(f^j(z))$ for all $z \in \mathbb{Z}_2$ and all $j \in \mathbb{N}_0 = \{0, 1, 2, \ldots\}$. Now consider a map $f^j(z)$ as a 2-variate function of $j \in \mathbb{N}_0$ and $z \in \mathbb{Z}_2$. In [5, Subsection 4.8.1, Proposition 4.90] it is shown that there exists a unique *continuous* function $F(t, z)\colon \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$ such that $F(j, z) = f^j(z)$ for all $z \in \mathbb{Z}_2$ and all $j = 0, 1, 2, \ldots$. It is worth noticing that p-adic time already has been considered in physics, see e.g. [14].

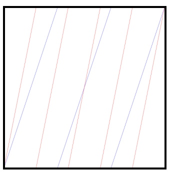

FIGURE 22: Figure 10 automaton plot for $\beta = 2$

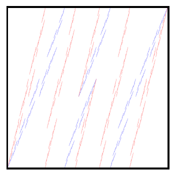

FIGURE 23: Same automaton plot for $\beta = 1.8$

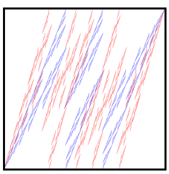

FIGURE 24: Same automaton plot for $\beta = 1.6$

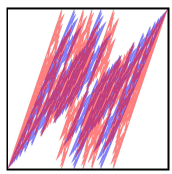

FIGURE 25: Same automaton plot for $\beta = 1.4$

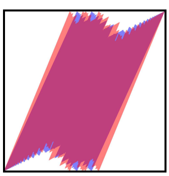

FIGURE 26: Same automaton plot for $\beta = 1.2$

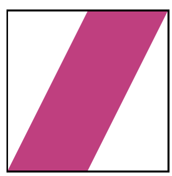

FIGURE 27: Same automaton plot for $\beta = 1$

There are more analogies between automata and physical systems, for instance:

- A *wavefunction of a free particle* can be associated to (linear) minimal automaton since the plot of the automaton is a torus winding which 'covers the whole space'. That is, once 'a part of winding' belongs to the plot, a whole winding belongs to the plot by Proposition 4.2.

- If the automaton function of the linear automaton is $f(z) = az+b$, the *helicity* corresponds to the sign of a since the sign defines direction of torus winding, clockwise or counter-clockwise.

- Automata with multiple inputs/outputs correspond to *finite-dimensional Hilbert spaces*; though it is possible to include into considerations infinite-dimensional Hilbert spaces: to do this one needs to consider automata of measure 0 rather then just finite ones.

- *Pure states* of a physical system correspond to ergodic linear sub-automata (actually to minimal sub-automata by Theorem 4.1) whereas *mixed states* correspond to those automata states which lead to more than 1 ergodic sub-automata. For instance, state 0 of the automaton whose state diagram is given by Figure 10 is mixed: depending on the first input symbol, the automaton will go to one pure state (which corresponds to multiplication by 5), or to another (which corresponds to multiplication by 3). Limit plot of the automaton is presented at Figure 22.

- Although our model is causal and deterministic, *randomness naturally arises with necessity due to the limited accuracy of measurements*; that is, since each wave function $\psi(x,t) = e^{i(kx-\omega t)}$ can be assigned to a minimal sub-automaton on the one hand, and to quantum state of a system on another hand, the system will fall in each of that states with certain probabilities which depend on the number of ways the automaton will reach an ergodic state, (i.e., the one belonging to some minimal sub-automaton) from the initial state. For instance, the system which corresponds to the automaton from Figure 10 will fall in either of two quantum states (which correspond to two minimal sub-automata) with equal probabilities, 1/2. Note that due to limited accuracy of measurements the very first input bit α_0 (that determines to which of two minimal sub-automata will belong the next state) is unknown and therefore it is impossible to say exactly in which of the states the system will occur even if we obtain during measurement an approximate numerical value $v(a) \approx 0.\alpha_{n-1}\dots\alpha_{n-k}$ of input bit string $\alpha_{n-1}\dots\alpha_2\alpha_1\alpha_0$.

Since we put $\beta = 1+\tau$ where τ is Planck time, it becomes reasonable in our model to interpret β^j as a time which is needed to acquire the next j-th bit of information; so the time T_k needed to acquire a k-bit information turns out to be exponential in k, namely

$$T_k = \frac{1}{\tau}(\beta^k - 1).$$

In classical models however it is usually assumed that the time needed to acquire a k-bit information is proportional to k. That is, classical case can be obtained from our model when $\tau \to 0$; i.e., when $\beta \to 1$ (since $T_k \to k$ then). As has recently shown by E. Lerner [39], when $\beta = 1$ the plot is not a torus winding any more but is a domain bounded by a polygon, cf., e.g., Figure 27. This may be treated so that a physical entity is a 'body' rather than a 'wave'. Figures 22–27 illustrate how the 'wave' is being transformed to 'body' when β decreases from 2 to 1; all the figures represent plots of the same automaton (actually the one whose state diagram is given by Figure 10) for β decreasing from 2 to 1 with step 0.2 (i.e., for $\beta = 2, \beta = 1.8, \ldots, \beta = 1.2, \beta = 1$). At our view, all these considerations show that our automata-based model of physical systems can be of physical meaning and worth further study.

REFERENCES

1. C. D. Aliprantis and O. Burkinshaw: *Principles of real analysis.* Academic Press, Inc., third ed., 1998.
2. J.-P. Allouche and J. Shallit: *Automatic Sequences. Theory, Applications, Generalizations.* Cambridge Univ. Press, 2003.
3. V. Anashin: *The non-Archimedean theory of discrete systems.* Math. Comp. Sci., **6** (2012), pp. 375–393.
4. ———: *Quantization causes waves: Smooth finitely computable functions are affine.* p-Adic Numbers, Ultrametric Analysis Appl., **7** (2015), pp. 169–227.
5. V. Anashin and A. Khrennikov: *Applied Algebraic Dynamics*, vol. 49 of de Gruyter Expositions in Mathematics. Walter de Gruyter GmbH & Co., Berlin—N.Y., 2009.
6. T. Bastin and C. W. Kilmister: *Combinatorial Physics*, vol. 9 of Series on Knots and Everything. World Scientific, Singapore, 1995.
7. A. Bokulich and G. Jaeger, eds.: *Philosophy of Quantum Information and Entaglement*, Cambridge Univ. Press, 2010.
8. W. Brauer: *Automatentheorie.* B. G. Teubner, Stuttgart, 1984.
9. M. Burgin: *Theory of Information*, vol. 1 of World Scientific Series in Information Studies. World Scientific, Singapore, 2010.
10. J. Carroll and D. Long: *Theory of Finite Automata.* Prentice-Hall Inc., 1989.
11. A. N. Cherepov: *On approximation of continuous functions by determinate functions with delay.* Discrete Math. Appl., **22** (2010), pp. 1–24.
12. ———: *Approximation of continuous functions by finite automata.* Discrete Math. Appl., **22** (2012), pp. 445–453.
13. R. Crowell and R. Fox: *Introduction to the Knot Theory.* Ginu and Co., Boston, 1963.
14. B. G. Dragović, P. H. Frampton, and B. V. Urošević: *Classical p-adic spacetime.* Mod. Phys. Lett., **A5** (1990), pp. 1521–1528.
15. B. Dragovich, A. Y. Khrennikov, S. V. Kozyrev, and I. V. Volovich: *On p-adic mathematical physics.* p-adic Numbers, Ultrametric Anal. Appl., **1** (2009), pp. 1–17.
16. D. Dubischar, V. M. Gundlach, O. Steinkamp, and A. Khrennikov: *The interference phenomenon, memory effects in the equipment and random dynamical systems over the fields of p-adic numbers.* Nuovo Cimento B, **114** (1999), pp. 373–382.
17. B. A. Dubrovin, A. T. Fomenko, and S. P. Novikov: *Modern Geometry - Methods and Applications*, vol. II. Springer-Verlag, NY–Berlin-Heidelberg-Tokyo, 1985.
18. S. Eilenberg: *Automata, Languages, and Machines*, vol. A. Academic Press, 1974.

19. D. R. Finkelstein: *Quantum Relativity.* Texts and Monographs in Physics, Springer, 1996.
20. B. R. Frieden: *Physics from Fisher Information.* Cambridge Univ. Press, 1998.
21. C. Frougny and K. Klouda: *Rational base number systems for p-adic numbers.* RAIPO Theor. Inform. Appl., **46** (2012), pp. 87–106.
22. F. Q. Gouvêa: *p-adic Numbers, An Introduction.* Springer-Verlag, Berlin–Heidelberg–New York, second ed., 1997.
23. R. I. Grigorchuk, V. V. Nekrashevich, and V. I. Sushchanskii: *Automata, dynamical systems, and groups.* Proc. Steklov Institute Math., **231** (2000), pp. 128–203.
24. B. Hasselblatt and A. Katok: *A First Course in Dynamics.* Cambridge Univ. Press, Cambridge, etc., 2003.
25. G. 't Hooft: *Determinism Beneath Quantum Mechanics.* In: Quo Vadis Quantum Mechanics? (A. Elitzur, S. Dolev, and N. Kolenda, eds.), Springer, 2005, pp. 99–111.
26. ———: *Classical cellular automata and quantum field theory*, in Proceedings of the Conference in Honor of Murray Gell-Mann's 80th Birthday "Quantum Mechanics, Elementary Particles, Quantum Cosmology and Complexity", H. Fritzsch and K. K. Phua, eds., Singapore, 2010, World Scientific, pp. 397–408.
27. ———: *Relating the quantum mechanics of discrete systems to standard canonical quantum mechanics*, Found. Phys., **44** (2014), pp. 406–425.
28. ———: *The Cellular Automaton Interpretation of Quantum Mechanics*, arXiv:1405.1548v3, December 2015.
29. S. Katok: *p-adic analysis in comparison with real.* Mass. Selecta, American Mathematical Society, 2003.
30. J. G. Kemeny and J. L. Snell: *Finite Markov Chains.* Springer-Verlag, 1976.
31. A. Khrennikov: *Quantum mechanics from time scaling and random fluctuations at the "quick time scale".* Nuovo Cimento B, **121** (2006), pp. 1005–1021.
32. ———: *To quantum averages through asymptotic expansion of classical averages on infinite-dimensional space.* Math. Phys., **48** (2007). Art. No. 013512.
33. ———: *Ultrametric Hilbert space representation of quantum mechanics with a finite exactness.* Found. Physics, **26** (1996), pp. 1033–1054.
34. ———: *Non-Archimedean Analysis: Quantum Paradoxes, Dynamical Systems and Biological Models.* Kluwer Academic Publishers, Dordrecht, 1997.
35. N. Koblitz: *p-adic numbers, p-adic analysis, and zeta-functions*, vol. 58 of Graduate texts in math. Springer-Verlag, second ed., 1984.
36. S. Koke, C. Grebing, H. Frei, A. Anderson, A. Assion, and G. Steinmeyer: *Direct frequency comb synthesis with arbitrary offset and shot-noise-limited phase noise.* Nature Photonic, **4** (2010), pp. 462–465.
37. M. Konečný: *Real functions computable by finite automata using affine representations.* Theor. Comput. Sci., **284** (2002), pp. 373–396.
38. R. Landauer: *Information is a physical entity.* Physica A, **263** (1999), pp. 63–67.
39. E. Lerner: *Private communication.* (Paper in preparation).
40. L. P. Lisovik and O. Y. Shkaravskaya: *Real functions defined by transducers.* Cybernetics and System Analysis, **34** (1998), pp. 69–76.
41. M. Lothaire: *Algebraic Combinatorics on Words.* Cambridge Univ. Press, 2002.
42. K. Mahler: *p-adic numbers and their functions.* Cambridge Univ. Press, 1981. (2nd edition).
43. V. Mansurov: *Knot theory.* Chapman & Hall/CRC, Boca Raton - London - NY - Washington, 2004.

44. N. Margolus: *Looking at nature as a computer.* Int. J. Theor. Phys., **42** (2003), pp. 309–327.
45. A. Mishchenko and A. Fomenko: *A course of differential geometry and topology.* Mir, Moscow, 1988.
46. A. F. Monna: *Sur une transformation simple des nombres p-adiques en nombres réels.* Indag. Math., **14** (1952), pp. 1–9.
47. H. P. Noyes: *Bit-String Physics*, vol. 27 of Series on Knots and Everything. World Scientific, Singapore, 2001.
48. A. F. Parker-Rhodes: *The Theory of Inditinguishables.* D. Reidel Publ. Co., Dordrecht, 1981.
49. W. Parry: *On the β-expansions of real numbers.* Acta Math. Acad. Sci. Hung., **11** (1960), pp. 401–416.
50. A. Rényi: *Representation for real numbers and their ergodic properties.* Acta Math. Acad. Sci. Hung., **8** (1957), pp. 477–493.
51. W. H. Schikhof: *Ultrametric calculus.* Cambridge University Press, 1984.
52. O. Y. Shkaravskaya: *Affine mappings defined by finite transducers.* Cybernetics and System Analysis, **34** (1998), pp. 781–783.
53. N. Sidorov: *Arithmetic dynamics.* In: Topics in dynamics and ergodic theory (S. Bezuglyi and S. Kolyada, eds.), vol. 310 of London Math. Soc. Lecture Note Series. Cambridge University Press, Cambridge, 2003, pp. 145–189.
54. V. S. Vladimirov, I. V. Volovich, and E. I. Zelenov: *p-adic Analysis and Mathematical Physics*, World Scientific, Singapore, 1994.
55. C. F. von Weizsäker: *The Structure of Physics*, vol. 154 of Fundamental Theories of Physics. Springer, 2006.
56. J. Vuillemin: *On circuits and numbers.* IEEE Trans. on Computers, **43** (1994), pp. 868–879.
57. ———: *Finite digital synchronous circuits are characterized by 2-algebraic truth tables.* In: Advances in computing science - ASIAN 2000, vol. 1961 of Lecture Notes in Computer Science, 2000, pp. 1–7.
58. ———: *Digital algebra and circuits.* In: Verification:Theory and Practice, vol. 2772 of Lecture Notes in Computer Science, 2003, pp. 733–746.
59. J. A. Wheeler: *Information, physics, quantum: The search for links.* In: Complexity, Entropy, and the Physics of Information (W. H. Zurek, ed.) Redwood City, Calif., 1990, Addison-Wesley Pub. Co., pp. 309–336.
60. S. V. Yablonsky: *Introduction to discrete mathematics.* Mir, Moscow, 1989.
61. A. Zeilinger: *A foundational principle of quantum mechanics.* Found. Phys., **21** (1999), pp. 631–643.
62. K. Zuce: *Calculating Space.* MIT, Cambridge, Mass., 1970. Translation from German of “Rechnender Raum”. Schr. Daten., Vol.1, Veiweg & Son, Braunschweig, 1969.

DISKRETNOST IZAZIVA TALASE

U ovom radu pokazujemo da talasi materije mogu biti izvedeni iz diskretnosti i kauzalnosti. Naime, pokazujemo da talasi materije mogu biti prirodno pripisani konačnim diskretnim kauzalnim sistemima, Mealy automatima kod kojih su ulaz/izlaz binarni nizovi bitova. Ako nizovi bitova imaju realne numeričke vrednosti (merljive veličine), tada talasi nastaju kao veza izmedju numeričkih vrednosti ulaznih ni-

zova (izazova) i izlaznih nizova (odgovora sistema). Pokazujemo da od svih diskretnih kauzalnih sistema sa proizvoljnim (ne obavezno binarnim) ulazima/izlazima, samo onima sa binarnim ulazom/izlazom mogu se pripisati talasi materije $\psi(x,t) = e^{i(kx-\omega t)}$.

Ključne reči: *talasi materije, konačni diskretni kauzalni sistemi, binarni nizovi bitova*