Commun. Korean Math. Soc. **34** (2019), No. 3, pp. 967–979
https://doi.org/10.4134/CKMS.c180217
pISSN: 1225-1763 / eISSN: 2234-3024

A DEVANEY-CHAOTIC MAP WITH POSITIVE ENTROPY ON A SYMBOLIC SPACE

Shankar Bangalore Ramesh and Chetana Urva Vasu

Abstract. Chaotic dynamical systems, preferably on a Cantor-like space with some arithmetic operations are considered as good pseudo-random number generators. There are many definitions of chaos, of which Devaney-chaos and pos itive topological entropy seem to be the strongest. Let $A = \{0, 1, \ldots, p-1\}$. We define a continuous map on $A^{\mathbb{Z}}$ using addition with a carry, in combination with the shift map. We show that this map gives rise to a dynamical system with positive entropy, which is also Devaney-chaotic: i.e., it is transitive, sensitive and has a dense set of periodic points.

1. Introduction

We use the following notation: $\mathbb{N}$ - the set of all non-negative integers, $\mathbb{N}^+$ - the set of all positive integers, $\mathbb{Q}$ - the field of rational numbers, $\mathbb{Z}$ - the ring of all integers, $\mathbb{Q}_p$ - the field of p-adic numbers and $\mathbb{Z}_p$ - the ring of p-adic integers.

Chaotic dynamical systems, preferably on a Cantor-like space with some arithmetic operations are considered as good pseudo-random number generators. There are many definitions of chaos, of which Devaney-chaos and positive topological entropy seem to be the strongest. We construct a map that is Devaney chaotic and has positive entropy, on a symbolic space.

For any prime p, $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ in the p-adic norm [5]. Every p-adic number is represented uniquely as a sequence of the form

$$\cdots d_{-2}d_{-1}\overbrace{d_0}^{0^{\text{th}}}.d_1\cdots\underbrace{d_m}_{\neq 0},$$

where d_i are the p-adic digits $\in \{0, 1, 2, \ldots, p-1\}$. Its p-adic norm is p^m. The ring of p-adic integers, $\mathbb{Z}_p$, consists of elements with norm less than or equal to one. (If p is not a prime, then it is a pseudo-norm, which gives a ring $\mathbb{Q}_p$, not a field.) To add two p-adic numbers, align the zeroth coordinates (just before

Received May 16, 2018; Accepted August 29, 2018.
2010 *Mathematics Subject Classification.* Primary 54H20, 37B10.
Key words and phrases. discrete chaotic transitive positively expansive entropy.

the dot) and proceed with addition with the 'carry' moving from right to left. Here is an example of addition in $\mathbb{Q}_7$.

$$\begin{array}{r} \cdots 462535.354300\cdots \\ +\cdots 320656.4100\cdots \\ \hline \cdots 113525.064300\cdots \end{array}$$

Let $A = \{0, 1, \ldots, p-1\}$, where p is a prime, have discrete topology. Consider the symbolic space $A^{\mathbb{Z}}$, in the product topology. Its elements are bi-infinite sequences of the form

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

For any x and y in $A^{\mathbb{Z}}$, we define $d(x, y) = p^{-j}$ where $j=$ min $\{i \geq 0 \,|\, x_i \neq y_i$ or $x_{-i} \neq y_{-i}\}$. This metric induces the product topology. It is a compact, totally disconnected perfect space, or a Cantor space. The most important continuous self map on it is the shift map σ.

For any element $x = \ \cdots \ x_{-r-1} \ x_{-r} \ x_{-r+1} \ \cdots x_{-2} \ x_{-1} \ \overbrace{x_0}^{0^{\text{th}}} \ x_1 \ x_2 \ \cdots x_r \ \cdots$ of $A^{\mathbb{Z}}$, $\sigma(x)$ is given by $\sigma(x)_i = x_{i+1}$. As sets, $\mathbb{Z}_p \subset \mathbb{Q}_p \subset A^{\mathbb{Z}} = \mathbb{Z}_p \times \mathbb{Z}_p$.

We extend the addition operation in $\mathbb{Z}_p$ or $\mathbb{Q}_p$ to $A^{\mathbb{Z}}$, and in combination with the shift map obtain chaotic functions.

We can "add" a constant a in $\mathbb{Q}_p$ to any element of $A^{\mathbb{Z}}$ in the obvious way. For any $a \in \mathbb{Q}_p$ and $x \in A^{\mathbb{Z}}$, $x + a$ can be added as follows. If

$$\begin{aligned} a &= \ \cdots \ a_{-2} \ a_{-1} \ a_0. \ a_1 \ a_2 \ \cdots \ a_m, \\ x &= \ \cdots \ x_{-2} \ x_{-1} \ x_0. \ x_1 \ x_2 \ \cdots \ x_m \ x_{m+1} \ x_{m+2} \cdots , \end{aligned}$$

then $x+a = y$, where $y_i = x_i$ for $i > m$, $y_m = x_m + a_m \mod p$, $y_{m-1} = a_{m-1} + x_{m-1} +$ the carry $\mod p$, and so on. (This is similar to the well known adding machine.) The combination of this with a power of σ, say $f(x) = \sigma^k(x) + a$, gives a map conjugate to σ^k.

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

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

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

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

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

Let a_{-m} be the first non-zero digit of a on the left side (starting at the 0^{th} position), and let a_n be the first non-zero digit of a on the right side (starting at the 1^{st} position). That is, $a \ = \ \cdots a_{-m-1} \ \underbrace{a_{-m}}_{\neq 0} \ 0 \ 0 \ \cdots \ 0 \ \overbrace{0}^{0^{\text{th}}} \ 0 \cdots 0 \ \underbrace{a_n}_{\neq 0} \ a_{n+1} \cdots .$

Then we define

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

Using this addition operation in combination with the shift map we get some interesting chaotic maps.

2. Basic definitions

Let X be a topological space and f a continuous self map on X. We use the following standard definitions and results on a system (X, f) mostly from [7], [8] and [9]. Usually X is assumed to be a compact space.

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

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

A point $x \in X$ is a *non-wandering* point if for every open set U containing x, there is an $n > 0$ such that $f^n(U) \bigcap U \neq \varnothing$. If all points of X are non-wandering, then (X, f) is a *non-wandering system.*

The system (X, f) is *transitive* if for any nonempty open sets U and V in X, there exists $n > 0$ such that $f^n(U) \bigcap V \neq \varnothing$. A point x is *transitive* if its orbit under f is dense. It is known that (X, f) is transitive if and only if it has at least one transitive point. If (X, f^n) is transitive for all $n \in \mathbb{N}$, (X, f) is said to be *totally transitive.*

The system (X, f) is *weakly mixing* if the product system $(X \times X, f \times f)$ is transitive, and it is *strongly mixing* if for any two non-empty open sets U and V there is $N > 0$ such that $f^n(U) \bigcap V \neq \varnothing$ for all $n \geq N$.

The system (X, f) is called *minimal* if it contains no proper subsystem. A subset A of X is *minimal* if (A, f) forms a minimal subsystem. A closed invariant subset A of X is minimal if and only if the orbit of every point of A is dense in A. A point $x \in X$ is called *minimal* if it belongs to some minimal subset of X.

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

A point x is said to be *equicontinuous*, if for every $\epsilon > 0 \ \exists \ \delta > 0$ such that for any y, $d(x, y) < \delta \implies d(f^n(x), f^n(y)) < \epsilon, \ \forall \ n > 0$. The system (X, f) is *equicontinuous* if for every $\epsilon > 0 \ \exists \ \delta > 0$ such that for any x and y in X, $d(x, y) < \delta \implies d(f^n(x), f^n(y)) < \epsilon, \ \forall \ n > 0$. If X is compact, it means that every point is an equicontinuous point. (X, f) is *sensitive* (to initial conditions) if there exists $\epsilon > 0$ such that $\forall x \in X, \forall \ \delta > 0$, there exists y with $d(x, y) < \delta$ and $n \geq 0$ such that $d(f^n(x), f^n(y)) \geq \epsilon$. A sensitive system cannot have equicontinuous points. There are systems that are not sensitive and do not have equicontinuous points. But this cannot happen in a transitive system [2].

For $\delta > 0$, a δ-*pseudo orbit* or δ-*chain* is a finite or infinite sequence of points $(x_n)_{n=0}^{m}$, $m \in \mathbb{N} \bigcup \{\infty\}$, such that $d(f(x_n), x_{n+1}) < \delta$ for $n < m$. (X, f) has the *shadowing property* if for any $\epsilon > 0 \ \exists \ \delta > 0, \ \forall \ x_0, \ldots, x_n, (\ \forall i, \ d(f(x_i), x_{i+1})) < \delta \implies \exists \ x, \ \forall \ i, d(f^i(x), x_i) < \epsilon)$. It means that every finite δ-chain is ϵ-shadowed by some point. We say that (X, f) has the *pseudo-orbit tracing property* (POTP), if for each $\epsilon > 0$ there is a $\delta > 0$ such that every infinite δ-pseudo orbit is ϵ- shadowed by some point. If X is compact, the shadowing property implies the pseudo-orbit tracing property.

There are two types of expansiveness:

(i) (X, f) is said to be *expansive* if there exists an $\epsilon > 0$ such that for all x and y in X with $x \neq y$, there is $n \in \mathbb{Z}$ with $d(f^n(x), f^n(y)) \geq \epsilon$.
(ii) (X, f) is said to be *positively expansive* if there exists an $\epsilon > 0$ such that for all x and y in X with $x \neq y$, there is $n \geq 0$ with $d(f^n(x), f^n(y)) \geq \epsilon$.

If X is compact and infinite, it is well known that X cannot have a positively expansive homeomorphism into itself [4].

To quantify the complication of a dynamical system we associate a non-negative real number called *topological entropy* with it. The larger this number, the more complicated the dynamical system is. We measure the exponential growth rate of essentially different orbit segments.

For a compact dynamical system, entropy is defined using open covers as in [1]:

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

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

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

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

If the topological entropy of (X, f) is positive, (X, f) is said to be chaotic. (X, f) is said to be *Devaney chaotic* if it is transitive, sensitive and has a dense set of periodic points. Transitivity is irreducibility in a certain sense, sensitivity contributes towards irregularity, and density of periodic points towards regularity. (Actually transitivity and density of periodic points together imply sensitivity.)

Two systems (X, f) and (Y, g) are *conjugate* if there is a homeomorphism $h : X \to Y$ such that $g = hfh^{-1}$.

3. A Devaney chaotic map with positive entropy

Consider the addition operation defined in Section 1 on $A^{\mathbb{Z}}$. We can combine it with the shift map by taking $h(x) = \sigma^k(x) + a$, for some fixed element a of $A^{\mathbb{Z}}$. This turns out to be an expansive homeomorphism with positive entropy. It is not known whether it is Devaney chaotic. In order to get a map that is Devaney-chaotic and has positive entropy, we modify the above map as follows. Assume that k is positive, and first consider $g(x) = \sigma^k(x) + x$. This is not injective, hence cannot be modified to get an expansive homeomorphism. We modify it to get a positively expansive map f. For this, every application of f should increase the distance between any two points (if they are not already far apart).

Consider any two elements x and y of $A^{\mathbb{Z}}$. Suppose that $x_i = y_i$ for $0 \le i < j$, and $x_j \ne y_j$ for some $j > k$. That is, the first difference in the coordinates of x and y, towards the right side of 0^{th} position, appears at j^{th} position. Then for $\sigma^k(x)$ and $\sigma^k(y)$, the first difference appears at the $(j-k)^{\text{th}}$ position. It follows that for $g(x)$ and $g(y)$, the first difference appears at the $(j-k)^{\text{th}}$ position. In other words, if $d(x, y) = p^{-j}$, then $d(g(x), g(y)) = p^{-j+k}$, i.e., the distance is increased by a factor of p^k. But if there is no difference in the positively numbered coordinates of x and y, this cannot happen.

So we combine g with a map that we call a ‘reflection’, that transfers the left-hand-side coordinates to the right, and vice versa. The most natural map is r, the reflection about the central 0^{th} coordinate, given by $(r(x))_i = x_{-i}$. It is clearly an isometry. The map $f = r \circ g$ is positively expansive.

It is a surjective map with each element having exactly p^k pre-images. In fact, for any $y \in A^{\mathbb{Z}}$, and for any fixed k coordinates of x around the zero^{th} one, we can find a unique x with $f(x) = y$. Similarly if we can fix central nk coordinates to get a unique pre-image for y under f^n, we can get transitivity.

To achieve this we modify r by defining r' given by $(r'(x))_i = x_{-i+1}$. That is the 0^{th} coordinate is taken to the first, and vice versa. Now we take $f(x) = r'(\sigma^k(x) + x)$.

Proposition 3.1. *The function $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by $f(x) = r'(\sigma^k(x) + x)$ is continuous and positively expansive.*

Proof. Obviously, σ^k is a homeomorphism and $r' = \sigma^{-1} \circ r$ is a homeomorphism. Therefore it is enough to verify that the addition map given by $(x, y) \mapsto x + y$ is continuous from $A^{\mathbb{Z}} \times A^{\mathbb{Z}}$ to $A^{\mathbb{Z}}$. Then the function f is (uniformly) continuous on $A^{\mathbb{Z}}$.

For any (x, y) and (x', y') in $A^{\mathbb{Z}} \times A^{\mathbb{Z}}$, $d(x, x') < p^{-j}$ and $d(y, y') < p^{-j} \Rightarrow d(x + y, x' + y') < p^{-j}$. Thus the operation $+$ is continuous. To verify that f is positively expansive, choose an $\epsilon < p^{-k}$. Suppose that $x \neq y$, and $d(x, y) = p^{-j}$. If $j \leq k$, take $n = 0$.

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

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

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

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

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

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

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

Note that f is positively expansive implies f is sensitive, because $A^{\mathbb{Z}}$ is perfect [7]. Next we verify that f is transitive.

Proposition 3.2. *Let $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be given by $f(x) = r'(\sigma^k(x)+x)$, where k is a positive integer. Let $y = \cdots y_{-2}\, y_{-1} \overbrace{y_0}^{0^{\text{th}}} y_1\, y_2 \cdots$ be given from $A^{\mathbb{Z}}$, and let n be any positive integer. For any set of p-adic digits $a_{-nk+1}, a_{-nk+2}, \ldots, a_{nk}$, there is a unique x in $A^{\mathbb{Z}}$ with $x_i = a_i$ for $i = -nk+1, -nk+2, \ldots, nk$ and $f^{2n}(x) = y$.*

Proof. We use induction on n.

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

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

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

Note that in $\sigma^k(x) + x$, the coordinates from $(-k+1)^{\text{th}}$ to 0^{th} are fixed. Call these coordinates as $z_{-k+1}, \ldots, z_0$ respectively. We have to find z which is as follows:

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

Then $z' = r'(z)$ will be $\cdots \ * \ * \ * \cdots \overbrace{*}^{0^{\text{th}}} \ z_0\, z_{-1} \cdots z_{-k+1} \ * \ * \ * \cdots$, where the $*$s indicate that the corresponding coordinates are yet to be determined. $\sigma^k(z') = \ \cdots * \ * \ * \ z_0 \ \cdots \overbrace{z_{-k+1}}^{0^{\text{th}}} \ * \ * \ * \cdots$. The remaining coordinates of z' can be easily found so that $\sigma^k(z') + z' = y' = \ \cdots y_3\, y_2 \overbrace{y_1}^{0^{\text{th}}} y_0\, y_1 \ \cdots$.

We have to carry out the calculations for the left and right sides separately. For the left side first fix z'_0, which is the same as z_1, such that $z_1 + z_{-k+1} \equiv y_1 \bmod p$. If $z_1 + z_{-k+1} > p$, let c_0 (the carry) be 1, otherwise let c_0 be 0. Next choose $z'_{-1} = z_2$ such that $z_2 + z_{-k+2} + c_0 \equiv y_2 \mod p$, and call the carry as c_{-1}. Proceed similarly. At every step only the coordinate of $\sigma^k(z')$ is known, and the corresponding coordinate of z' has to be calculated.

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

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

Next we assume the result holds for $n-1$, and prove it for n.

Let p-adic digits $a_{-nk+1}, a_{-nk+2}, \ldots, a_{nk}$ and $y = \cdots\ y_{-2}\, y_{-1}\, \overbrace{y_0}^{0^{\text{th}}}\, y_1\, y_2\ \cdots$ be given. We have to find x such that $x_i = a_i$ for $i = -nk+1, -nk+2, \ldots, nk$, and $f^{2n}(x) = y$. Consider the following x, where x_i indicates a known coordinate $=a_i$, and a $*$ indicates that the corresponding coordinate is yet to be determined. $x = \cdots * * * x_{-nk+1} \cdots \overbrace{x_0}^{0^{\text{th}}}\ x_1\ \cdots x_{nk}\ * * * \cdots$. Then

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

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

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

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

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

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

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

Proposition 3.3. *The function $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by $f(x) = r'(\sigma^k(x) + x)$, where k is a positive integer, is transitive.*

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

By a similar argument, we see that f^2 is strongly mixing.

We now prove that the topological entropy is positive. We need the following result.

Proposition 3.4. *The map $f(x) = r'(\sigma^k(x) + x)$ is an open map.*

Proof. We use the following notation:

$$U(x, n) \text{ - the set of all points } z \text{ with } z_i = x_i \text{ for } -nk + 1 \leq i \leq nk \text{ for } n \in \mathbb{N}^+. \tag{1}$$

$$C(x, n, m) \text{ - the set of all points } z \text{ with } z_i = x_i \text{ for } -mk + 1 \leq i \leq nk \text{ for } n, m \in \mathbb{N}^+. \tag{2}$$

It is easily seen that cylinders of type (1) also form a basis for the product topology.

Now we prove that

$$f(U(x, n)) = C(f(x), n, n - 1). \tag{3}$$

Let $z \in U(x, n)$. Then $z_i = x_i$ for $-nk + 1 \leq i \leq nk$, and $\sigma^k(z)_i = \sigma^k(x)_i$ for $-nk+1 \leq i \leq (n-1)k$. It follows that $(\sigma^k(z)+z)_i = (\sigma^k(x)+x)_i$ for $-nk+1 \leq i \leq (n-1)k$, and so $(r'(\sigma^k(z) + z))_i = (r'(\sigma^k(x) + x))_i$, i.e., $(f(x))_i = f((z))_i$ for $-(n-1)k + 1 \leq i \leq nk$. Thus $f(U(x, n)) \subseteq C(f(x), n, n - 1)$.

Now let $y \in C(f(x), n, n-1)$. There is a unique pre-image z for this y under f such that $z_i = x_i$ for $1 \leq i \leq k$. We prove that $z_i = x_i$ for $-nk+1 \leq i \leq nk$.

Suppose that $z_i \neq x_i$ for some i with $-nk + 1 \leq i \leq nk$.

First let $z_i \neq x_i$ for some positive i, with $i \leq nk$, and choose the smallest such i. Then $k < i \leq nk$. Then $(\sigma^k(z))_{i-k} \neq (\sigma^k(x))_{i-k}$, and $(\sigma^k(z) + z)_{i-k} \neq (\sigma^k(x) + x)_{i-k}$, which implies $(r'(\sigma^k(z) + z))_{-i+k+1} \neq (r'(\sigma^k(x) + x))_{-i+k+1}$, i.e., $y_{-i+k+1} \neq f(x)_{-i+k+1}$. This is a contradiction because $-(n - 1)k + 1 \leq -i + k + 1 \leq 0$.

Now suppose that $z_i = x_i$ for $0 < i \leq nk$. Then $z_i \neq x_i$ for some negative i, with $-nk + 1 \leq i \leq 0$. Consider such i with minimum $|i|$. Now $(\sigma^k(z))_j = (\sigma^k(x))_j$, for $i \leq j \leq 0$, but $z_i \neq x_i$. Therefore $(\sigma^k(z) + z))_i \neq (\sigma^k(x) + x))_i$, and so $(r'(\sigma^k(z) + z))_{-i+1} \neq (r'(\sigma^k(x) + x))_{-i+1}$, or $y_{-i+1} \neq (f(x))_{-i+1}$, a contradiction because $0 < -i + 1 \leq nk$. Thus $f(U(x, n)) \supseteq C(f(x), n, n - 1)$.

As $C(f(x), n, n - 1)$ is a clopen cylinder, f is an open map. $\square$

Now we use a result from [10, p. 17, Theorem 1].

Theorem 3.5. *Let f be a positively expansive self map on a compact metrizable space. Then the following are equivalent.*

(1) *f is an open map.*
(2) *f has the shadowing property .*

It follows that the function $f(x) = r'(\sigma^k(x)+x)$ has the shadowing property. Finally, we use a result from [8, p. 6, Theorem 3.3].

Theorem 3.6. *Let (X, f) be a non-wandering dynamical system with the shadowing property. Then either (X, f) is equicontinuous or it has positive entropy.*

Proposition 3.7. *The function $f(x) = r'(\sigma^k(x) + x)$ has positive entropy.*

Proof. $(A^{\mathbb{Z}}, f)$ is transitive implies that it is non-wandering. It is positively expansive and $A^{\mathbb{Z}}$ is perfect implies it is sensitive, and therefore cannot be equicontinuous. By Theorem 3.6, it has positive entropy. □

4. Density of periodic points

To see that periodic points are dense, we use the following result from [3, Theorem 3.4.2].

Theorem 4.1. *Let (X, f) be a compact dynamical system. If f is a positively expansive surjection having the pseudo-orbit tracing property, then the set of periodic points of f is dense in $\Omega(f)$, the set of non-wandering points of f.*

Proposition 4.2. *The function $f(x) = r'(\sigma^k(x) + x)$ on $A^{\mathbb{Z}}$ has a dense set of periodic points.*

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

Thus, the system $(A^{\mathbb{Z}}, f)$ is Devaney-chaotic.

There are various kinds of chaos, some of which are compared in [9]. Among them we observe that positive entropy and Devaney-chaos are quite strong, that is, each of them implies many other types of chaos. Hence we can conclude that the function $f(x) = r'(\sigma^k(x) + x)$ is a good chaotic function.

We now find the fixed points of f.

Proposition 4.3. *For any elements $a_1, a_2, \ldots, a_k$ of A, there is a fixed point x of the function $f(x) = r'(\sigma^k(x) + x)$ with $x_i = a_i$ for $i = 1, 2 \ldots, k$.*

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

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

Then

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

We have to determine the remaining coordinates of x such that

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

Find x_0 such that $x_0 + x_k \equiv x_1 \mod p$, and let c_0 be the carry. Next find x_{-1} such that $x_{-1} + x_{k-1} + c_0 \equiv \ x_2 \mod p$, and let c_{-1} be the carry. Proceed similarly to find all coordinates on the left side.

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

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

Proposition 4.4. *For any elements $a_{-k+1}, a_{-k+2} \cdots a_1, a_2, \ldots, a_k$ of A, there is a periodic point x of the function $f(x) = r'(\sigma^k(x) + x)$ of period 2, with $x_i = a_i$ for $i = -k+1, -k+2, \ldots, 1, 2, \ldots, k$.*

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

$$x = \cdots * * * \; x_{-k+1} \; x_{-k+2} \cdots \; x_0 \; \overbrace{x_1}^{1^{\text{st}}} \; x_1 \; x_2 \cdots x_k \; * * * \cdots . \tag{4}$$

Then

$$\sigma^k(x) = \cdots * * * \; x_{-k+1} \; x_{-k+2} \cdots \; x_1 \; x_2 \cdots \overbrace{x_k}^{0^{\text{th}}} \; * * * \cdots . \tag{5}$$

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

$$z = \cdots * * * \; z_{-k+1} \; z_{-k+2} \cdots \overbrace{z_0}^{0^{\text{th}}} \; * * * \cdots . \tag{6}$$

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

$$z' = \cdots * * * \; \overbrace{z_0}^{1^{\text{st}}} \; z_{-1} \cdots z_{-k+1} * * * \cdots . \tag{7}$$

Or, denoting z' as

$$z' = \cdots * * * \; \overbrace{z'_1}^{1^{\text{st}}} \; z'_2 \cdots z'_k * * * \cdots . \tag{8}$$

$$\sigma^k(z') = \cdots * * * * z'_1 \; z'_2 \cdots z'_k \overbrace{*}^{1^{\text{st}}} * * * \cdots . \tag{9}$$

We have to find z and x such that $\sigma^k(z') + z' = x' = r'(x)$.

First find z'_{k+1} (i.e., z_{-k}), such that $z'_{k+1} + z'_1 \equiv x'_1 = x_0 \mod p$, and let c_1 be the carry. Substitute this value of z_{-k} in (6), so that x_{-k} is uniquely determined by (5) +(4) = (6).

Now find z'_0 (i.e., z_1), such that $z'_0 + z'_k \equiv x'_0 = x_1 \mod p$, and let c_0 be the carry. Substitute this z_1 in (6), to determine x_{k+1} uniquely by (5) +(4) = (6).

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

$\sigma^k(x) + x = z$. So $r'(\sigma^k(x) + x) = z'$, i.e., $f(x) = z'$, and $\sigma^k(z') + z' = x'$, or $r'(\sigma^k(z') + z') = x$, which means $f(z') = x$, $f^2(x) = f(f(x)) = f(z') = x$. $\square$

Remark 4.5.

- We cannot generalize this by imitating the proof of (3.2), and using induction, to get periodic points of period $2n$. We can start with x, whose middle $2nk$ coordinates are given. We can get $[-(n-1)k+1]$-th to $[(n-1)k]$-th coordinates of w. But in place of a fully known y, we have x, whose $2nk$ coordinates only are known. The remaining coordinates of x and w are to be determined simultaneously such that $f^{2(n-1)}(w') = x$ and $f^2(x) = w'$, for which we cannot use induction directly.
- We could as well define the addition without a carry, but then f^2 becomes just a Cellular Automaton [6], though f is not.

References

[1] R. L. Adler, A. G. Konheim, and M. H. McAndrew, *Topological entropy*, Trans. Amer. Math. Soc. **114** (1965), 309–319. https://doi.org/10.2307/1994177

[2] E. Akin, J. Auslander, and K. Berg, *When is a transitive map chaotic?*, in Convergence in ergodic theory and probability (Columbus, OH, 1993), 25–40, Ohio State Univ. Math. Res. Inst. Publ., 5, de Gruyter, Berlin, 1996.

[3] N. Aoki and K. Hiraide, *Topological Theory of Dynamical Systems*, North-Holland Mathematical Library, **52**, North-Holland Publishing Co., Amsterdam, 1994.

[4] E. M. Coven and M. Keane, *Every compact metric space that supports a positively expansive homeomorphism is finite*, in Dynamics & Stochastics, vol. 48 of IMS Lecture Notes Monogr. Ser., Inst. Math. Statist., Beachwood, OH, **2006** (2006), 304–305.

[5] S. Katok, *p-adic analysis compared with real*, Student Mathematical Library, **37**, American Mathematical Society, Providence, RI, 2007. https://doi.org/10.1090/stml/037

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

[7] ———, *Topological and Symbolic Dynamics*, Cours Spécialisés, **11**, Société Mathématique de France, Paris, 2003.

[8] J. Li and P. Oprocha, *Shadowing property, weak mixing and regular recurrence*, J. Dynam. Differential Equations **25** (2013), no. 4, 1233–1249. https://doi.org/10.1007/s10884-013-9338-x

[9] J. Li and X. D. Ye, *Recent development of chaos theory in topological dynamics*, Acta Math. Sin. (Engl. Ser.) **32** (2016), no. 1, 83–114. https://doi.org/10.1007/s10114-015-4574-0

[10] K. Sakai, *Various shadowing properties for positively expansive maps*, Topology Appl. **131** (2003), no. 1, 15–31. https://doi.org/10.1016/S0166-8641(02)00260-2

Shankar Bangalore Ramesh
Department of Mathematical and Computational Sciences
National Institute of Technology
Surathkal, 575025
Karnataka, India
Email address: shankarbr@gmail.com

Chetana Urva Vasu
Department of Mathematics
University College
Mangalore, 575001, Karnataka, India
Email address: chetanauv@gmail.com