

# The Lyapunov Exponents of Reversible Cellular Automata Are Uncomputable<sup>\*</sup>

Johan Kopra<sup>[0000-0002-6401-6795]</sup>

Department of Mathematics and Statistics, FI-20014 University of Turku, Finland  
jtjkop@utu.fi

**Abstract.** We will show that the class of reversible cellular automata (CA) with right Lyapunov exponent 2 cannot be separated algorithmically from the class of reversible CA whose right Lyapunov exponents are at most  $2 - \delta$  for some absolute constant  $\delta > 0$ . Therefore there is no algorithm that, given as an input a description of an arbitrary reversible CA  $F$  and a positive rational number  $\epsilon > 0$ , outputs the Lyapunov exponents of  $F$  with accuracy  $\epsilon$ .

**Keywords:** Cellular automata · Lyapunov exponents · Reversible computation · Computability.

## 1 Introduction

A cellular automaton (CA) is a model of parallel computation consisting of a uniform (in our case one-dimensional) grid of finite state machines, each of which receives input from a finite number of neighbors. All the machines use the same local update rule to update their states simultaneously at discrete time steps. The following question of error propagation arises naturally: If one changes the state at some of the coordinates, then how long does it take for this change to affect the computation at other coordinates that are possibly very far away? Lyapunov exponents provide one tool to study the asymptotic speeds of error propagation in different directions. The concept of Lyapunov exponents originally comes from the theory of differentiable dynamical systems, and the discrete variant of Lyapunov exponents for CA was originally defined in [11].

The Lyapunov exponents of a cellular automaton  $F$  are interesting also when one considers  $F$  as a topological dynamical system, because they can be used to give an upper bound for the topological entropy of  $F$  [12]. In [2] a closed formula for the Lyapunov exponents of linear one-dimensional cellular automata is given, which is a first step in determining for which classes of CA the Lyapunov exponents are computable. It is previously known that the entropy of one-dimensional cellular automata is uncomputable [7] (and furthermore from [4] it follows that there exists a single cellular automaton whose entropy is uncomputable), which

---

<sup>\*</sup> The work was partially supported by the Academy of Finland grant 296018 and by the Vilho, Yrjö and Kalle Väisälä Foundation.

gives reason to suspect that also the Lyapunov exponents are uncomputable in general.

The uncomputability of Lyapunov exponents is easy to prove for (not necessarily reversible) cellular automata by using the result from [8] which says that nilpotency of cellular automata with a spreading state is undecidable. We will prove the more specific claim that the Lyapunov exponents are uncomputable even for reversible cellular automata. In the context of proving undecidability results for reversible CA one cannot utilize undecidability of nilpotency for non-reversible CA. An analogous decision problem, the (local) immortality problem, has been used to prove undecidability results for reversible CA [10]. We will use in our proof the undecidability of a variant of the immortality problem, which in turn follows from the undecidability of the tiling problem for 2-way deterministic tile sets.

## 2 Preliminaries

For sets  $A$  and  $B$  we denote by  $B^A$  the collection of all functions from  $A$  to  $B$ .

A finite set  $A$  of *letters* or *symbols* is called an *alphabet*. The set  $A^{\mathbb{Z}}$  is called a *configuration space* or a *full shift* and its elements are called *configurations*. An element  $c \in A^{\mathbb{Z}}$  is interpreted as a bi-infinite sequence that contains the symbol  $c(i)$  at position  $i$ . A *factor* of  $c$  is any finite sequence  $c(i)c(i+1)\cdots c(j)$  where  $i, j \in \mathbb{Z}$ , and we interpret the sequence to be empty if  $j < i$ . Any finite sequence  $w = w(1)w(2)\cdots w(n)$  (also the empty sequence, which is denoted by  $\epsilon$ ) where  $w(i) \in A$  is a *word* over  $A$ . If  $w \neq \epsilon$ , we say that  $w$  *occurs* in  $c$  at position  $i$  if  $c(i)\cdots c(i+n) = w(1)\cdots w(n)$  and we denote by  $w^{\mathbb{Z}} \in A^{\mathbb{Z}}$  the configuration in which  $w$  occurs at all positions of the form  $in$  ( $i \in \mathbb{Z}$ ). The set of all words over  $A$  is denoted by  $A^*$ , and the set of non-empty words is  $A^+ = A^* \setminus \{\epsilon\}$ . More generally, for  $L, K \subseteq A^*$  we denote  $LK = \{w_1w_2 \mid w_1 \in L, w_2 \in K\}$ ,  $L^* = \{w_1\cdots w_n \mid n \geq 0, w_i \in L\}$  and  $L^+ = \{w_1\cdots w_n \mid n \geq 1, w_i \in L\}$ . The set of words of length  $n$  is denoted by  $A^n$ . For a word  $w \in A^*$ ,  $|w|$  denotes its length, i.e.  $|w| = n \iff w \in A^n$ .

If  $A$  is an alphabet and  $C$  is a countable set, then  $A^C$  becomes a compact metrizable topological space when endowed with the product topology of the discrete topology of  $A$  (in particular a set  $S \subseteq A^{\mathbb{Z}}$  is compact if and only if it is closed). In our considerations  $C = \mathbb{Z}$  or  $C = \mathbb{Z}^2$ . We define the *shift*  $\sigma : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$  by  $\sigma(c)(i) = c(i+1)$  for  $c \in A^{\mathbb{Z}}$ ,  $i \in \mathbb{Z}$ , which is a homeomorphism. We say that a closed set  $X \subseteq A^{\mathbb{Z}}$  is a *subshift* if  $\sigma(X) = X$ .

Occasionally we consider configuration spaces  $(A_1 \times A_2)^{\mathbb{Z}}$  and then we may write  $(c_1, c_2) \in (A_1 \times A_2)^{\mathbb{Z}}$  where  $c_i \in A_i^{\mathbb{Z}}$  using the natural bijection between the sets  $A_1^{\mathbb{Z}} \times A_2^{\mathbb{Z}}$  and  $(A_1 \times A_2)^{\mathbb{Z}}$ . We may use the terminology that  $c_1$  is on the upper layer or on the  $A_1$ -layer, and similarly that  $c_2$  is on the lower layer or on the  $A_2$ -layer.

**Definition 1.** A (*one-dimensional*) cellular automaton (or a CA) is a 3-tuple  $(A, N, f)$ , where  $A$  is a finite state set,  $N = (n_1, \dots, n_m) \in \mathbb{Z}^m$  is a neighborhood vector (containing distinct integers) and  $f : A^m \rightarrow A$  is a local rule. A

given CA  $(A, N, f)$  is customarily identified with a corresponding CA function  $F : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$  defined by

$$F(c)(i) = f(c(i + n_1), \dots, c(i + n_m))$$

for every  $c \in A^{\mathbb{Z}}$  and  $i \in \mathbb{Z}$ .  $F$  is a radius- $r$  CA ( $r \in \mathbb{N}$ ) if it can be defined with the neighborhood vector  $(-r, \dots, 0, \dots, r)$  and it is a radius- $\frac{1}{2}$  CA if it can be defined with the neighborhood vector  $(0, 1)$ . If  $X \subseteq A^{\mathbb{Z}}$  is a subshift and  $F(X) \subseteq X$ , the restriction map  $F : X \rightarrow X$  is a cellular automaton on  $X$ . In the case we consider only the restriction  $F : X \rightarrow X$ , it is sometimes sufficient that the local rule  $f$  is a partial function.

The *space-time diagram* of  $c \in X$  (with respect to a CA  $F : X \rightarrow X$ ) is the map  $\theta \in A^{\mathbb{Z}^2}$  defined by  $\theta(i, j) = F^j(c)(i)$ . These are occasionally represented pictorially. The CA-functions on  $X$  are characterized as those continuous maps on  $X$  that commute with the shift [5]. We say that a CA  $F : X \rightarrow X$  is *reversible* if it is bijective as a CA function. Reversible CA are homeomorphisms on  $X$ . The book [9] is a standard reference for subshifts and cellular automata on them.

The definition of Lyapunov exponents is from [11, 12]. For a fixed subshift  $X \subseteq A^{\mathbb{Z}}$  and for  $c \in X$ ,  $s \in \mathbb{Z}$ , denote  $W_s^+(c) = \{e \in X \mid \forall i \geq s : e(i) = c(i)\}$  and  $W_s^-(c) = \{e \in X \mid \forall i \leq s : e(i) = c(i)\}$ . Then for given cellular automaton  $F : X \rightarrow X$ ,  $c \in X$ ,  $n \in \mathbb{N}$ , define

$$\begin{aligned} A_n^+(c, F) &= \min\{s \geq 0 \mid \forall 1 \leq i \leq n : F^i(W_{-s}^+(c)) \subseteq W_0^+(F^i(c))\} \\ A_n^-(c, F) &= \min\{s \geq 0 \mid \forall 1 \leq i \leq n : F^i(W_s^-(c)) \subseteq W_0^-(F^i(c))\}. \end{aligned}$$

Finally, the quantities

$$\lambda^+(F) = \lim_{n \rightarrow \infty} \max_{c \in A^{\mathbb{Z}}} \frac{A_n^+(c, F)}{n}, \quad \lambda^-(F) = \lim_{n \rightarrow \infty} \max_{c \in A^{\mathbb{Z}}} \frac{A_n^-(c, F)}{n}$$

are called respectively the right and left *Lyapunov exponents* of  $F$ . These limits exist by an application of Fekete's lemma (e.g. Lemma 4.1.7 in [9]). We write  $A_n^+(c)$ ,  $A_n^-(c)$ ,  $\lambda^+$  and  $\lambda^-$  when  $F$  is clear by the context.

### 3 Tilings and Undecidability

In this section we recall the well-known connection between cellular automata and tilings on the plane. We use this connection to prove an auxiliary undecidability result for reversible cellular automata.

**Definition 2.** A Wang tile is formally a function  $t : \{N, E, S, W\} \rightarrow C$  whose value at  $I$  is denoted by  $t_I$ . Informally, a Wang tile  $t$  should be interpreted as a unit square with edges colored by elements of  $C$ . The edges are called north, east, south and west in the natural way, and the colors in these edges of  $t$  are  $t_N, t_E, t_S$  and  $t_W$  respectively. A tile set is a finite collection of Wang tiles.

**Definition 3.** A tiling over a tile set  $T$  is a function  $\eta \in T^{\mathbb{Z}^2}$  which assigns a tile to every integer point of the plane. A tiling  $\eta$  is said to be valid if neighboring tiles always have matching colors in their edges, i.e. for every  $(i, j) \in \mathbb{Z}^2$  we have  $\eta(i, j)_N = \eta(i, j + 1)_S$  and  $\eta(i, j)_E = \eta(i + 1, j)_W$ . If there is a valid tiling over  $T$ , we say that  $T$  admits a valid tiling.

We say that a tile set  $T$  is NE-deterministic if for every pair of tiles  $t, s \in T$  the equalities  $t_N = s_N$  and  $t_E = s_E$  imply  $t = s$ , i.e. a tile is determined uniquely by its north and east edge. A SW-deterministic tile set is defined similarly. If  $T$  is both NE-deterministic and SW-deterministic, it is said to be *2-way deterministic*.

The *tiling problem* is the problem of determining whether a given tile set  $T$  admits a valid tiling.

**Theorem 1.** [10, Theorem 4.2.1] *The tiling problem is undecidable for 2-way deterministic tile sets.*

**Definition 4.** Let  $T$  be a 2-way deterministic tile set and  $C$  the collection of all colors which appear in some edge of some tile of  $T$ .  $T$  is complete if for each pair  $(a, b) \in C^2$  there exist (unique) tiles  $t, s \in T$  such that  $(t_N, t_E) = (a, b)$  and  $(s_S, s_W) = (a, b)$ .

A 2-way deterministic tile set  $T$  can be used to construct a complete tile set. Namely, let  $C$  be the set of colors which appear in tiles of  $T$ , let  $X \subseteq C \times C$  be the set of pairs of colors which do not appear in the northeast of any tile and let  $Y \subseteq C \times C$  be the set of pairs of colors which do not appear in the southwest of any tile. Since  $T$  is 2-way deterministic, there is a bijection  $p : X \rightarrow Y$ . Let  $T^{\mathbb{C}}$  be the set of tiles formed by matching the northeast corners  $X$  with the southwest corners  $Y$  via the bijection  $p$ . Then the tile set  $A = T \cup T^{\mathbb{C}}$  is complete.

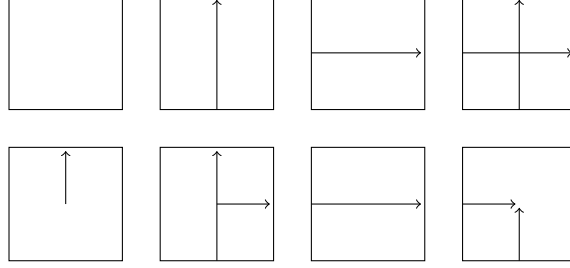
Every complete 2-way deterministic tile set  $A$  determines a reversible CA  $(A, (0, 1), f)$  with the local rule  $f : A^2 \rightarrow A$  defined by  $f(a, b) = c \in A$ , where  $c$  is the unique tile such that  $a_E = c_W$  and  $b_N = c_S$ . If we denote the corresponding CA function by  $F$ , the space-time diagram of a configuration  $c \in A^{\mathbb{Z}}$  corresponds to a valid tiling  $\eta$  via  $\theta(i, j) = F^j(c)(i) = \eta(i + j, -i)$ , i.e. configurations  $F^j(c)$  are diagonals of  $\eta$  going from northwest to southeast.

**Definition 5.** A cellular automaton  $F : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$  is  $(x, y)$ -locally immortal ( $x, y \in \mathbb{N}$ ) with respect to a subset  $B \subseteq A$  if there exists a configuration  $c \in A^{\mathbb{Z}}$  such that  $F^{iy+j}(c)(ix) \in B$  for all  $i \in \mathbb{Z}$  and  $0 \leq j \leq y$ . Such a configuration  $c$  is an  $(x, y)$ -witness.

Generalizing the definition in [10], we call the following decision problem the  $(x, y)$ -local immortality problem: given a reversible CA  $F : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$  and a subset  $B \subseteq A$ , is  $F$   $(x, y)$ -locally immortal with respect to  $B$ ? In Theorem 5.1.5 of [10] it is shown that the  $(0, 1)$ -local immortality problem is undecidable for reversible CA. We adapt the proof to get the following result.

**Lemma 1.** *The  $(1, 5)$ -local immortality problem is undecidable for reversible radius- $\frac{1}{2}$  CA.*

*Proof.* We will reduce the problem of Theorem 1 to the  $(1, 5)$ -local immortality problem. Let  $T$  be a 2-way deterministic tile set and construct a complete tile set  $T \cup T^{\mathbb{C}}$  as indicated above. Then also  $A_1 = (T \times T_1) \cup (T^{\mathbb{C}} \times T_2)$  ( $T_1$  and  $T_2$  as in Figure 1) is a complete tile set<sup>1</sup>. We denote the blank tile of the set  $T_1$  by  $t_b$  and call the elements of  $R = A_1 \setminus (T \times \{t_b\})$  arrow tiles. As indicated above, the tile set  $A_1$  determines a reversible radius- $\frac{1}{2}$  CA  $G_1 : A_1^{\mathbb{Z}} \rightarrow A_1^{\mathbb{Z}}$ .



**Fig. 1.** The tile sets  $T_1$  (first row) and  $T_2$  (second row) from [10].

Let  $A_2 = \{0, 1, 2\}$ . Define  $A = A_1 \times A_2$  and natural projections  $\pi_i : A \rightarrow A_i$ ,  $\pi_i(a_1, a_2) = a_i$  for  $i \in \{1, 2\}$ . By extension we say that  $a \in A$  is an arrow tile if  $\pi_1(a) \in R$ . Let  $G : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$  be defined by  $G(c, e) = (G_1(c), e)$  where  $c \in A_1^{\mathbb{Z}}$  and  $e \in A_2^{\mathbb{Z}}$ , i.e.  $G$  simulates  $G_1$  in the upper layer. We define, using the notation of Definition 1, involutive CA  $J_1, J_2$  and  $H$  by tuples  $(A_2, (0), j_1), (A_2, (0, 1), j_2)$  and  $(A_1 \times A_2, (0), h)$  where

$$j_1(0) = 0 \quad j_1(1) = 2 \quad j_1(2) = 1 \quad j_2(a, b) = \begin{cases} 1 & \text{when } (a, b) = (0, 2) \\ 0 & \text{when } (a, b) = (1, 2) \\ a & \text{otherwise} \end{cases}$$

$$h((a, b)) = \begin{cases} (a, 1) & \text{when } a \in R \text{ and } b = 0 \\ (a, 0) & \text{when } a \in R \text{ and } b = 1 \\ (a, b) & \text{otherwise.} \end{cases}$$

If  $\text{id} : A_1^{\mathbb{Z}} \rightarrow A_1^{\mathbb{Z}}$  is the identity map, then  $J = (\text{id} \times J_2) \circ (\text{id} \times J_1)$  is a CA on  $A^{\mathbb{Z}} = (A_1 \times A_2)^{\mathbb{Z}}$ . We define the radius- $\frac{1}{2}$  automaton  $F = H \circ J \circ G : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$  and select  $B = (T \times \{t_b\}) \times \{0\}$ . We will show that  $T$  admits a valid tiling if and only if  $F$  is  $(1, 5)$ -locally immortal with respect to  $B$ .

Assume first that  $T$  admits a valid tiling  $\eta$ . Then by choosing  $c \in A^{\mathbb{Z}}$  such that  $c(i) = ((\eta(i, -i), t_b), 0) \in A_1 \times A_2$  for  $i \in \mathbb{Z}$  it follows that  $F^j(c)(i) \in B$  for all  $i, j \in \mathbb{Z}$  and in particular that  $c$  is a  $(1, 5)$ -witness.

Assume then that  $T$  does not admit any valid tiling and for a contradiction assume that  $c$  is a  $(1, 5)$ -witness. Let  $\theta$  be the space-time diagram of  $c$  with

<sup>1</sup> The arrow markings are used as a shorthand for some coloring such that the heads and tails of the arrows in neighboring tiles match in a valid tiling.

respect to  $F$ . Since  $c$  is a  $(1, 5)$ -witness, it follows that  $\theta(i, j) \in B$  whenever  $(i, j) \in N$ , where  $N = \{(i, j) \in \mathbb{Z}^2 \mid 5i \leq j \leq 5(i+1)\}$ . There is a valid tiling  $\eta$  over  $A_1$  such that  $\pi_1(\theta(i, j)) = \eta(i+j, -i)$  for  $(i, j) \in \mathbb{Z}^2$ , i.e.  $\eta$  can be recovered from the upper layer of  $\theta$  by applying a suitable linear transformation on the space-time diagram. In drawing pictorial representations of  $\theta$  we want that the heads and tails of all arrows remain properly matched in neighboring coordinates, so we will use tiles with “bent” labelings, see Figure 2. Since  $T$  does not admit valid tilings, it follows by a compactness argument that  $\eta(i, j) \notin T \times T_1$  for some  $(i, j) \in D$  where  $D = \{(i, j) \in \mathbb{Z}^2 \mid j < -\lfloor i/6 \rfloor\}$  and in particular that  $\eta(i, j)$  is an arrow tile. Since  $\theta$  contains a “bent” version of  $\eta$ , it follows that  $\theta(i, j)$  is an arrow tile for some  $(i, j) \in E$ , where  $E = \{(i, j) \in \mathbb{Z}^2 \mid j < 5i\}$  is a “bent” version of the set  $D$ . In Figure 3 we present the space-time diagram  $\theta$  with arrow markings of tiles from  $T_1$  and  $T_2$  replaced according to the Figure 2. In Figure 3 we have also marked the sets  $N$  and  $E$ . Other features of the figure become relevant in the next paragraph.

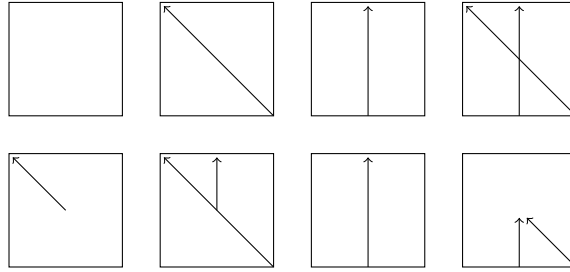
The minimal distance between a tile in  $N$  and an arrow tile in  $E$  situated on the same horizontal line in  $\theta$  is denoted by  $d_1 > 0$ . Then, among those arrow tiles in  $E$  at horizontal distance  $d_1$  from  $N$ , there is a tile with minimal vertical distance  $d_2 > 0$  from  $N$  (see Figure 3). Fix  $x, y \in \mathbb{Z}$  so that  $\theta(x, y+2)$  is one such tile and in particular  $(x-d_1, y+2), (x, y+2+d_2) \in N$ . Then  $\theta(x, y+j)$  contains an arrow for  $-2 \leq j \leq 2$ , because if there is a  $j \in [-2, 2)$  such that  $\theta(x, y+j)$  does not contain an arrow and  $\theta(x, y+j+1)$  does, then  $\theta(x, y+j+1)$  must contain one of the three arrows on the left half of Figure 2. These three arrows continue to the northwest, so then also  $\theta(x-1, y+j+2)$  contains an arrow. Because  $\theta(i', j') \in B$  for  $(i', j') \in N$ , it follows that  $(x-1, y+j+2) \notin N$  and thus  $(x-1, y+j+2) \in E$ . Since  $(x-d_1, y+2) \in N$ , it follows that one of the  $(x-d_1-1, y+j+2), (x-d_1, y+j+2)$  and  $(x-d_1+1, y+j+2)$  belong to  $N$ . Thus the horizontal distance of the tile  $\theta(x-1, y+j+2)$  from the set  $N$  is at most  $d_1$ , and is actually equal to  $d_1$  by the minimality of  $d_1$ . Since  $N$  is invariant under translation by the vector  $-(1, 5)$ , then from  $(x, y+2+d_2) \in N$  it follows that  $(x-1, y-3+d_2) \in N$  and that the vertical distance of the tile  $\theta(x-1, y+j+2)$  from  $N$  is at most  $(y-3+d_2) - (y+j+2) \leq d_2 - 3$ , contradicting the minimality of  $d_2$ . Similarly,  $\theta(x-i, y+j)$  does not contain an arrow for  $0 < i \leq d_1, -2 \leq j \leq 2$  by the minimality of  $d_1$  and  $d_2$ .

Now consider the  $A_2$ -layer of  $\theta$ . For the rest of the proof let  $e = F^y(c)$ . Assume that  $\pi_2(\theta(x-i, y)) = \pi_2(e(x-i))$  is non-zero for some  $i \geq 0, (x-i, y) \in E$  and fix the greatest such  $i$ , i.e.  $\pi_2(e(z)) = 0$  for  $z$  in the set

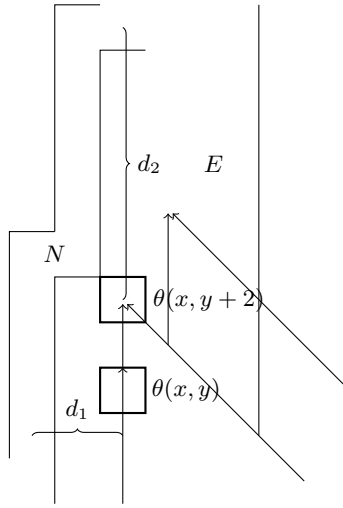
$$I_0 = \{x' \in \mathbb{Z} \mid x' < x-i, (x', y) \in N \cup E\}.$$

We start by considering the case  $\pi_2(e(x-i)) = 1$ . Denote

$$I_1 = \{x' \in \mathbb{Z} \mid x' < x-i, (x', y+1) \in N \cup E\} \subseteq I_0.$$



**Fig. 2.** The tile sets  $T_1$  and  $T_2$  presented in a “bent” form.



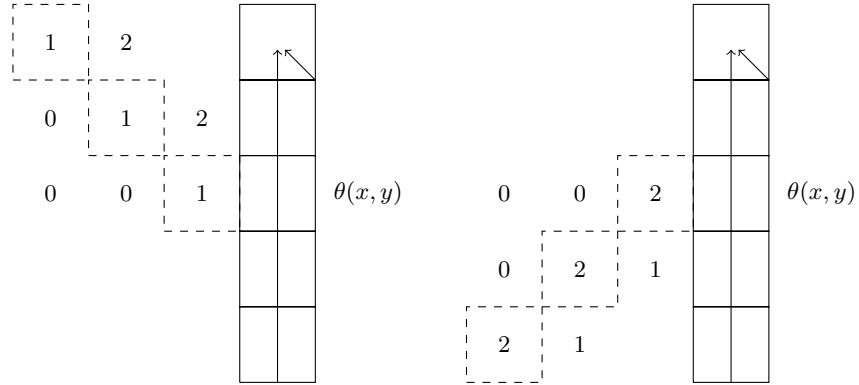
**Fig. 3.** The space-time diagram  $\theta$  with “bent” arrow markings. An arrow tile  $\theta(x, y+2)$  in  $E$  with minimal horizontal and vertical distances to  $N$  has been highlighted.

From the choice of  $(x, y)$  it follows that  $\pi_1(\theta(z, y+1)) = \pi_1(G(e)(z))$  are not arrow tiles for  $z \in I_1$ , and therefore we can compute step by step that

$$\begin{aligned} \pi_2((\text{id} \times J_1)(G(e))(x-i)) &= 2, & \pi_2((\text{id} \times J_1)(G(e))(z)) &= 0 \text{ for } z \in I_0 \subseteq I_1, \\ \pi_2(J(G(e))(x-(i+1))) &= 1, & \pi_2(J(G(e))(z)) &= 0 \text{ for } z \in I_1 \setminus \{x-(i+1)\}, \\ \pi_2(F(e))(x-(i+1)) &= 1, & \pi_2(F(e)(z)) &= 0 \text{ for } z \in I_1 \setminus \{x-(i+1)\} \end{aligned}$$

and  $\pi_2(\theta(x-(i+1), y+1)) = 1$ . By repeating this argument inductively we see that the digit 1 propagates to the upper left in the space-time diagram as indicated by Figure 4 and eventually reaches  $N$ , a contradiction. If on the other hand  $\pi_2(\theta(x-i, y)) = 2$ , a similar argument shows that the digit 2 propagates to the lower left in the space-time diagram as indicated by Figure 4 and eventually reaches  $N$ , also a contradiction.

Assume then that  $\pi_2(\theta(x-i, y))$  is zero whenever  $i \geq 0$ ,  $(x-i, y) \in E$ . If  $\pi_2(\theta(x+1, y)) = \pi_2(e(x+1)) \neq 1$ , then  $\pi_2((\text{id} \times J_1)(G(e))(x+1)) \neq 2$



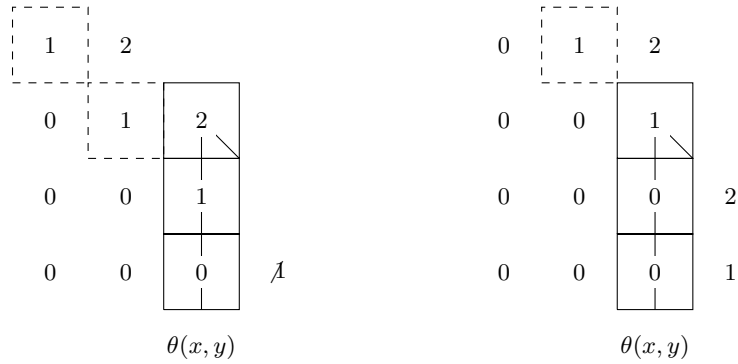
**Fig. 4.** Propagation of digits to the left of  $\theta(x, y)$ .

and  $\pi_2(J(G(e))(x)) = 0$ . Since  $\pi_1(\theta(x, y + 1))$  is an arrow tile, it follows that  $\pi_2(\theta(x, y + 1)) = \pi_2(H(J(G(e)))(x)) = 1$ . The argument of the previous paragraph shows that the digit 1 propagates to the upper left in the space-time diagram as indicated by the left side of Figure 5 and eventually reaches  $N$ , a contradiction.

Finally consider the case  $\pi_2(\theta(x + 1, y)) = \pi_2(e(x + 1)) = 1$ . Then

$$\begin{aligned} \pi_2(J(G(e))(x))\pi_2(J(G(e))(x + 1)) &= 12 \text{ and} \\ \pi_2(F(e))(x)\pi_2(F(e))(x + 1) &= 02. \end{aligned}$$

As in the previous paragraph we see that  $\pi_2(\theta(x, y + 2)) = 1$ . This occurrence of the digit 1 propagates to the upper left in the space-time diagram as indicated by the right side of Figure 5 and eventually reaches  $N$ , a contradiction.



**Fig. 5.** Propagation of digits at  $\theta(x, y)$ .

□



## 4 Uncomputability of Lyapunov exponents

In this section we will prove our main result saying that there is no algorithm that can compute the Lyapunov exponents of a given reversible cellular automaton on a full shift to an arbitrary precision.

To achieve greater clarity we first prove this result in a more general class of subshifts. For the statement of the following theorem, we recall for completeness that a sofic shift  $X \subseteq A^{\mathbb{Z}}$  is a subshift that can be represented as the set of labels of all bi-infinite paths on some labeled directed graph. This precise definition will not be of any particular importance, because the sofic shifts that we construct are of very specific form. We will appeal to the proof of the following theorem during the course of the proof of our main result.

**Theorem 2.** *For reversible CA  $F : X \rightarrow X$  on sofic shifts such that  $\lambda^+(F) \in [0, \frac{5}{3}] \cup \{2\}$  it is undecidable whether  $\lambda^+(F) \leq \frac{5}{3}$  or  $\lambda^+(F) = 2$ .*

*Proof.* We will reduce the decision problem of Lemma 1 to the present problem. Let  $G : A_2^{\mathbb{Z}} \rightarrow A_2^{\mathbb{Z}}$  be a given reversible radius- $\frac{1}{2}$  cellular automaton and  $B \subseteq A_2$  some given set. Let  $A_1 = \{0, \parallel, \leftarrow, \rightarrow, \swarrow, \nearrow\}$  and define a sofic shift  $Y \subseteq A_1^{\mathbb{Z}}$  as the set of those configurations containing a symbol from  $Q = \{\leftarrow, \rightarrow, \swarrow, \nearrow\}$  in at most one position. We will interpret elements of  $Q$  as particles going in different directions at different speeds and which bounce between walls denoted by  $\parallel$ . Let  $S : Y \rightarrow Y$  be the reversible radius-2 CA which does not move occurrences of  $\parallel$  and which moves  $\leftarrow$  (resp.  $\rightarrow, \swarrow, \nearrow$ ) to the left at speed 2 (resp. to the right at speed 2, to the left at speed 1, to the right at speed 1) with the additional condition that when an arrow meets a wall, it changes into the arrow with the same speed and opposing direction. More precisely,  $S$  is determined by the tuple  $(A_1, \{-2, -1, 0, 1, 2\}, f)$  where the local rule  $f : A_1^5 \rightarrow A_1$  is defined as follows (where  $*$  denotes arbitrary symbols):

$$\begin{aligned} f(\rightarrow, 0, 0, *, *) &= \rightarrow & f(*, \nearrow, 0, *, *) &= \nearrow \\ f(*, \rightarrow, 0, \parallel, *) &= \leftarrow & f(*, *, \nearrow, \parallel, *) &= \swarrow, \\ f(*, *, 0, \rightarrow, \parallel) &= \leftarrow \\ f(*, \parallel, \rightarrow, \parallel, *) &= \rightarrow \end{aligned}$$

with symmetric definitions for arrows in the opposite directions at reflected positions and  $f(*, *, a, *, *) = a$  ( $a \in A_1$ ) otherwise. Then let  $X = Y \times A_2^{\mathbb{Z}}$  and  $\pi_1 : X \rightarrow Y$ ,  $\pi_2 : X \rightarrow A_2^{\mathbb{Z}}$  be the natural projections  $\pi_i(c_1, c_2) = c_i$  for  $c_1 \in Y, c_2 \in A_2^{\mathbb{Z}}$  and  $i \in \{1, 2\}$ .

Let  $c_1 \in Y$  and  $c_2 \in A_2^{\mathbb{Z}}$  be arbitrary. We define reversible CA  $G_2, F_1 : X \rightarrow X$  by  $G_2(c_1, c_2) = (c_1, G^{10}(c_2))$ ,  $F_1(c_1, c_2) = (S(c_1), c_2)$ . Additionally, let  $F_2 : X \rightarrow X$  be the involution which maps  $(c_1, c_2)$  as follows:  $F_2$  replaces an occurrence of  $\rightarrow 0 \in A_1^2$  in  $c_1$  at a coordinate  $i \in \mathbb{Z}$  by an occurrence of  $\swarrow \parallel \in A_1^2$  (and vice versa) *if and only if*

$$G^j(c_2)(i) \notin B \text{ for some } 0 \leq j \leq 5 \quad \text{or} \quad G^j(c_2)(i+1) \notin B \text{ for some } 5 \leq j \leq 10,$$

and otherwise  $F_2$  makes no changes. Finally, define  $F = F_1 \circ G_2 \circ F_2 : X \rightarrow X$ . The reversible CA  $F$  works as follows. Typically particles from  $Q$  move in the upper layer in the intuitive manner indicated by the map  $S$  and the lower layer is transformed according to the map  $G^{10}$ . There are some exceptions to the usual particle movements: If there is a particle  $\rightarrow$  which does not have a wall immediately at the front and  $c_2$  does not satisfy a local immortality condition in the next 10 time steps, then  $\rightarrow$  changes into  $\nearrow$  and at the same time leaves behind a wall segment  $\parallel$ . Conversely, if there is a particle  $\nearrow$  to the left of the wall  $\parallel$  and  $c_2$  does not satisfy a local immortality condition,  $\nearrow$  changes into  $\rightarrow$  and removes the wall segment.

We will show that  $\lambda^+(F) = 2$  if  $G$  is  $(1, 5)$ -locally immortal with respect to  $B$  and  $\lambda^+(F) \leq \frac{5}{3}$  otherwise. Intuitively the reason for this is that if  $c, e \in X$  are two configurations that differ only to the left of the origin, then the difference between  $F^i(c)$  and  $F^i(e)$  can propagate to the right at speed 2 only via an arrow  $\rightarrow$  that travels on top of a  $(1, 5)$ -witness. Otherwise, a signal that attempts to travel to the right at speed 2 is interrupted at bounded time intervals and forced to return at a slower speed beyond the origin before being able to continue its journey to the right. We will give more details.

Assume first that  $G$  is  $(1, 5)$ -locally immortal with respect to  $B$ . Let  $c_2 \in A_2^{\mathbb{Z}}$  be a  $(1, 5)$ -witness and define  $c_1 \in Y$  by  $c_1(0) = \rightarrow$  and  $c_1(i) = 0$  for  $i \neq 0$ . Let  $c = (0^{\mathbb{Z}}, c_2) \in X$  and  $e = (c_1, c_2) \in X$ . It follows that  $\pi_1(F^i(c))(2i) = 0$  and  $\pi_1(F^i(e))(2i) = \rightarrow$  for every  $i \in \mathbb{N}$ , so  $\lambda^+(F) \geq 2$ . On the other hand,  $F$  has a neighborhood vector  $(-2, -1, 0, 1, \dots, 10)$  so necessarily  $\lambda^+(F) = 2$ .

Assume then that there are no  $(1, 5)$ -witnesses for  $G$ . Let us denote

$$C(n) = \{c \in A_1^{\mathbb{Z}} \mid G^{5i+j}(c)(i) \in B \text{ for } 0 \leq i \leq n, 0 \leq j \leq 5\} \text{ for } n \in \mathbb{N}.$$

Since there are no  $(1, 5)$ -witnesses, by a compactness argument we may fix some  $N \in \mathbb{N}_+$  such that  $C(2N) = \emptyset$ . We claim that  $\lambda^+(F) \leq \frac{5}{3}$ , so let us assume that  $(c^{(n)})_{n \in \mathbb{N}}$  with  $c^{(n)} = (c_1^{(n)}, c_2^{(n)}) \in X$  is a sequence of configurations such that  $A_n^+(c^{(n)}, F) = s_n n$  where  $(s_n)_{n \in \mathbb{N}}$  tends to  $\lambda^+$ . There exist  $e^{(n)} = (e_1^{(n)}, e_2^{(n)}) \in X$  such that  $c^{(n)}(i) = e^{(n)}(i)$  for  $i > -s_n n$  and  $F^{t_n}(c)(i_n) \neq F^{t_n}(e)(i_n)$  for some  $0 \leq t_n \leq n$  and  $i_n \geq 0$ .

First assume that there are arbitrarily large  $n \in \mathbb{N}$  for which  $c_1^{(n)}(i) \in \{0, \parallel\}$  for  $i > -s_n n$  and consider the subsequence of such configurations  $c^{(n)}$  (starting with sufficiently large  $n$ ). Since  $G$  is a radius- $\frac{1}{2}$  CA, it follows that  $\pi_2(F^{t_n}(c^{(n)}))(j) = \pi_2(F^{t_n}(e^{(n)}))(j)$  for  $j \geq 0$ . Therefore the difference between  $c^{(n)}$  and  $e^{(n)}$  can propagate to the right only via an arrow from  $Q$ , so without loss of generality (by swapping  $c^{(n)}$  and  $e^{(n)}$  if necessary)  $\pi_1(F^{t_n}(c^{(n)}))(j_n) \in Q$  for some  $0 \leq t_n \leq n$  and  $j_n \geq i_n - 1$ . Fix some such  $t_n, j_n$  and let  $w_n \in Q^{t_n+1}$  be such that  $w_n(i)$  is the unique state from  $Q$  in the configuration  $F^i(c^{(n)})$  for  $0 \leq i \leq t_n$ . The word  $w_n$  has a factorization of the form  $w_n = u(v_1 u_1 \cdots v_k u_k) v$  ( $k \in \mathbb{N}$ ) where  $v_i \in \{\rightarrow\}^+$ ,  $v \in \{\rightarrow\}^*$  and  $u_i \in (Q \setminus \{\rightarrow\})^+$ ,  $u \in (Q \setminus \{\rightarrow\})^*$ . By the choice of  $N$  it follows that all  $v_i, v$  have length at most  $N$  and by the definition of the CA  $F$  it is easy to see that each  $u_i$  contains at least  $2(|v_i| - 1) + 1$  occurrences of  $\nearrow$  and at least  $2(|v_i| - 1) + 1$  occurrences of  $\searrow$  (after  $\rightarrow$  turns into

$\nwarrow$ , it must return to the nearest wall to the left and back and at least once more turn into  $\nwarrow$  before turning back into  $\rightarrow$ . If  $\rightarrow$  were to turn into  $\leftarrow$  instead, it would signify an impassable wall on the right). If we denote by  $x_n$  the number of occurrences of  $\rightarrow$  in  $w_n$ , then  $x_n \leq |w_n|/3 + \mathcal{O}(1)$  (this upper bound is achieved by assuming that  $|v_i| = 1$  for every  $i$ ) and

$$s_n n \leq |w_n| + 2x_n \leq |w_n| + \frac{2}{3}|w_n| + \mathcal{O}(1) \leq \frac{5}{3}n + \mathcal{O}(1).$$

After dividing this inequality by  $n$  and passing to the limit we find that  $\lambda^+ \leq \frac{5}{3}$ .<sup>2</sup>

Next assume that there are arbitrarily large  $n \in \mathbb{N}$  for which  $c_1^{(n)}(i) \in Q$  for some  $i > -s_n n$ . The difference between  $c^{(n)}$  and  $e^{(n)}$  can propagate to the right only after the element from  $Q$  in  $c^{(n)}$  reaches the coordinate  $-s_n n$ , so without loss of generality there are  $0 < t_{n,1} < t_{n,2} \leq n$  and  $i_n \geq 0$  such that  $\pi_1(F^{t_{n,1}}(c^{(n)}))(-s) \in Q$  for some  $s \geq s_n n$  and  $\pi_1(F^{t_{n,2}}(c^{(n)}))(i_n) \in Q$ . From this the contradiction follows in the same way as in the previous paragraph.  $\square$

We are ready to prove our main result.

**Theorem 3.** *For reversible CA  $F : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$  such that  $\lambda^+(F) \in [0, \frac{5}{3}] \cup \{2\}$  it is undecidable whether  $\lambda^+(F) \leq \frac{5}{3}$  or  $\lambda^+(F) = 2$ .*

*Proof.* Let  $G : A_2^{\mathbb{Z}} \rightarrow A_2^{\mathbb{Z}}$ ,  $A_1$ ,  $F = F_1 \circ G_2 \circ F_2 : X \rightarrow X$ , etc. be as in the proof of the previous theorem. We will adapt the conveyor belt construction from [3] to define a CA  $F'$  on a full shift which simulates  $F$  and has the same right Lyapunov exponent as  $F$ .

Denote  $Q = \{\leftarrow, \rightarrow, \nwarrow, \nearrow\}$ ,  $\Sigma = \{0, \parallel\}$ ,  $\Delta = \{-, 0, +\}$ , define the alphabets

$$\Gamma = (\Sigma^2 \times \{+, -\}) \cup (Q \times \Sigma \times \{0\}) \cup (\Sigma \times Q \times \{0\}) \subseteq A_1 \times A_1 \times \Delta$$

and  $A = \Gamma \times A_2$  and let  $\pi_{1,1}, \pi_{1,2} : A^{\mathbb{Z}} \rightarrow A_1^{\mathbb{Z}}$ ,  $\pi_{\Delta} : A^{\mathbb{Z}} \rightarrow \Delta^{\mathbb{Z}}$ ,  $\pi_2 : A^{\mathbb{Z}} \rightarrow A_2^{\mathbb{Z}}$  be the natural projections  $\pi_{1,1}(c) = c_{1,1}$ ,  $\pi_{1,2}(c) = c_{1,2}$ ,  $\pi_{\Delta}(c) = c_{\Delta}$ ,  $\pi_2(c) = c_2$  for  $c = (c_{1,1}, c_{1,2}, c_{\Delta}, c_2) \in A^{\mathbb{Z}} \subseteq (A_1 \times A_1 \times \Delta \times A_2)^{\mathbb{Z}}$ . For arbitrary  $c = (c_1, c_2) \in (\Gamma \times A_2)^{\mathbb{Z}}$  define  $G'_2 : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$  by  $G'_2(c) = (c_1, G^{10}(c_2))$ .

Next we define  $F'_1 : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$ . Every element  $c = (c_1, c_2) \in (\Gamma \times A_2)^{\mathbb{Z}}$  has a unique decomposition of the form  $(c_1, c_2) = \cdots (w_{-2}, v_{-2})(w_{-1}, v_{-1})(w_0, v_0)(w_1, v_1)(w_2, v_2) \cdots$  where

$$w_i \in (\Sigma^2 \times \{+\})^* ((Q \times \Sigma \times \{0\}) \cup (\Sigma \times Q \times \{0\})) (\Sigma^2 \times \{-\})^* \\ \cup (\Sigma^2 \times \{+\})^* (\Sigma^2 \times \{-\})^*$$

with the possible exception of the leftmost  $w_i$  beginning or the rightmost  $w_i$  ending with an infinite sequence from  $\Sigma^2 \times \{+, -\}$ .

Let  $(x_i, y_i) \in (\Sigma \times \Sigma)^* ((Q \times \Sigma) \cup (\Sigma \times Q)) (\Sigma \times \Sigma)^* \cup (\Sigma \times \Sigma)^*$  be the word that is derived from  $w_i$  by removing the symbols from  $\Delta$ . The pair  $(x_i, y_i)$  can

<sup>2</sup> By performing more careful estimates it can be shown that  $\lambda^+ = 1$ , but we will not attempt to formalize the argument for this.

be seen as a conveyor belt by gluing the beginning of  $x_i$  to the beginning of  $y_i$  and the end of  $x_i$  to the end of  $y_i$ . The map  $F'_1$  will shift arrows like the map  $F_1$ , and at the junction points of  $x_i$  and  $y_i$  the arrow can turn around to the opposite side of the belt. More precisely, define the permutation  $\rho : A_1 \rightarrow A_1$  by

$$\begin{array}{llll} \rho(0) = 0 & \rho(\parallel) = \parallel & & \\ \rho(\leftarrow) = \rightarrow & \rho(\rightarrow) = \leftarrow & \rho(\nwarrow) = \nearrow & \rho(\nearrow) = \nwarrow \end{array}$$

and for a word  $u \in A_1^*$  let  $\rho(u)$  denote the coordinatewise application of  $\rho$ . For any word  $w = w(1) \cdots w(n)$  define its reversal by  $w^R(i) = w(n+1-i)$  for  $1 \leq i \leq n$ . Then consider the periodic configuration  $e = [(x_i, v_i)(\rho(y_i), v_i)^R]^\mathbb{Z} \in (A_1 \times A_2)^\mathbb{Z}$ . The map  $F_1 : X \rightarrow X$  extends naturally to configurations of the form  $e$ :  $e$  can contain infinitely many arrows, but they all point in the same direction and occur in identical contexts. By applying  $F_1$  to  $e$  we get a new configuration of the form  $[(x'_i, v_i)(\rho(y'_i), v_i)^R]$ . From this we extract the pair  $(x'_i, y'_i)$ , and by adding plusses and minuses to the left and right of the arrow (or in the same coordinates as in  $(x_i, y_i)$  if there is no occurrence of an arrow) we get a word  $w'_i$  which is of the same form as  $w_i$ . We define  $F'_1 : A^\mathbb{Z} \rightarrow A^\mathbb{Z}$  by  $F'_1(c) = c'$  where  $c' = \cdots (w'_{-2}, v_{-2})(w'_{-1}, v_{-1})(w'_0, v_0)(w'_1, v_1)(w'_2, v_2) \cdots$ . Clearly  $F'_1$  is shift invariant, continuous and reversible.

We define the involution  $F'_2 : A^\mathbb{Z} \rightarrow A^\mathbb{Z}$  as follows. For  $c \in A^\mathbb{Z}$  and  $j \in \{1, 2\}$   $F'_2$  replaces an occurrence of  $\rightarrow 0$  in  $\pi_{1,j}(c)$  at coordinate  $i \in \mathbb{Z}$  by an occurrence of  $\nwarrow \parallel$  (and vice versa) if and only if  $\pi_\Delta(c)(i+1) = -$  and

$$G^j(\pi_2(c))(i) \in B \text{ for } 0 \leq j \leq 5 \quad \text{and} \quad G^j(\pi_2(c))(i+1) \in B \text{ for } 5 \leq j \leq 10,$$

and otherwise  $F'_2$  makes no changes.  $F'_2$  simulates the map  $F_2$  and we check the condition  $\pi_\Delta(c)(i+1) = -$  to ensure that  $F'_2$  does not transfer information between neighboring conveyor belts.

Finally, we define  $F' = F'_1 \circ G'_2 \circ F'_2 : A^\mathbb{Z} \rightarrow A^\mathbb{Z}$ . The reversible CA  $F'$  simulates  $F : X \rightarrow X$  simultaneously on two layers and it has the same right Lyapunov exponent as  $F$ .  $\square$

The following corollary is immediate.

**Corollary 1.** *There is no algorithm that, given a reversible CA  $F : A^\mathbb{Z} \rightarrow A^\mathbb{Z}$  and a rational number  $\epsilon > 0$ , returns the Lyapunov exponent  $\lambda^+(F)$  within precision  $\epsilon$ .*

## 5 Conclusions

We have shown that the Lyapunov exponents of a given reversible cellular automaton on a full shift cannot be computed to arbitrary precision. Ultimately this turned out to follow from the fact that the tiling problem for 2-way deterministic Wang tile sets reduces to the problem of computing the Lyapunov exponents of reversible CA. In our constructions we controlled only the right exponent  $\lambda^+$  and let the left exponent  $\lambda^-$  vary freely. Controlling both Lyapunov exponents would be necessary to answer the following.

*Problem 1.* Is it decidable whether the equality  $\lambda^+(F) + \lambda^-(F) = 0$  holds for a given reversible cellular automaton  $F : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$ ?

We mentioned in the introduction that there exists a single CA whose topological entropy is an uncomputable number. We ask whether a similar result holds also for the Lyapunov exponents.

*Problem 2.* Does there exist a single cellular automaton  $F : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$  such that  $\lambda^+(F)$  is an uncomputable number?

We are not aware of a cellular automaton on a full shift that has an irrational Lyapunov exponent (see Question 5.7 in [1]), so constructing such a CA (or proving the impossibility of such a construction) should be the first step. This problem has an answer for CA  $F : X \rightarrow X$  on general subshifts  $X$ , and furthermore for every real  $t \geq 0$  there is a subshift  $X_t$  and a reversible CA  $F_t : X_t \rightarrow X_t$  such that  $\lambda^+(F_t) = \lambda^-(F_t) = t$  [6].

## References

1. Cyr, V., Franks, J., Kra, B.: The spacetime of a shift endomorphism. Transactions of the American Mathematical Society (2017)
2. D’Amico, M., Manzini G., Margara, L: On computing the entropy of cellular automata. Theoretical Computer Science **290**, 1629–1646 (2003)
3. Guillon, P., Salo, V.: Distortion in One-Head Machines and Cellular Automata. In: Cellular Automata and Discrete Complex Systems, volume 10248 of Lecture Notes in Comput. Sci. pp. 120–138. Springer, Cham (2017)
4. Guillon, P., Zinoviadis, Ch.: Densities and entropies in cellular automata. In: How the world computes, volume 7318 of Lecture Notes in Comput. Sci. pp. 253–263. Springer, Heidelberg (2012)
5. Hedlund, G.: Endomorphisms and automorphisms of the shift dynamical system. Math. Systems Theory **3**, 320–375 (1969)
6. Hochman, M.: Non-expansive directions for  $\mathbb{Z}^2$  actions. Ergodic Theory and Dynamical Systems, **31**(1), 91–112 (2011)
7. Hurd, L. P., Kari, J., Culik K.: The topological entropy of cellular automata is uncomputable. Ergodic Theory Dynamical Systems **12** 255–265 (1992)
8. Kari, J.: The nilpotency problem of one-dimensional cellular automata. SIAM Journal on Computing **21** 571–586 (1992)
9. Lind, D., Marcus, B.: An introduction to symbolic dynamics and coding. Cambridge University Press, Cambridge (1995)
10. Lukkarila, V.: On undecidable dynamical properties of reversible one-dimensional cellular automata (Ph.D. thesis). Turku Centre for Computer Science (2010)
11. Shereshevsky, M. A.: Lyapunov exponents for one-dimensional cellular automata. J. Nonlinear Sci. **2**(1), 1–8 (1992)
12. Tisseur, P.: Cellular automata and Lyapunov exponents. Nonlinearity **13**(5), 1547–1560 (2000)