On computing the Lyapunov exponents of reversible cellular automata

Johan Kopra[1]

Abstract

We consider the problem of computing the Lyapunov exponents of reversible cellular automata (CA). We show that the class of reversible 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 ϵ. We also compute the average Lyapunov exponents (with respect to the uniform measure) of the reversible CA that perform multiplication by p in base pq for coprime $p, q > 1$.

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 Shereshevsky (1992).

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 (Tisseur 2000). It is previously known that the entropy of one-dimensional cellular automata is uncomputable (Hurd et al. 1992) (and furthermore from (Guillon and Zinoviadis 2012) it follows that there exists a single cellular automaton whose entropy is uncomputable), which 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 Kari (1992) which says that nilpotency of cellular automata with a spreading state is undecidable. We will prove in Sect. 4 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 (Lukkarila 2010). We will use in our proof the undecidability of a variant of the immortality problem, presented in Sect. 3, which in turn follows from the undecidability of the tiling problem for 2-way deterministic tile sets.

In the other direction, there are interesting classes of cellular automata whose Lyapunov exponents have been computed. In D'amico et al. (2003) a closed formula for the Lyapunov exponents of linear one-dimensional cellular automata is given. In Sect. 5 we present results concerning the family of reversible multiplication automata that

✉ Johan Kopra
jtjkop@utu.fi

1   Department of Mathematics and Statistics, University of Turku, FI 20014 Turku, Finland

simulate multiplication by p in base pq for coprime $p, q > 1$. It is easy to find out their Lyapunov exponents and it is more interesting to consider a measure theorical variant, the average Lyapunov exponent. We compute the average Lyapunov exponents (with respect to the uniform measure) for these automata.

This is an extended version of the conference paper (Kopra 2019b) published in the proceedings of UCNC 2019. Section 3 is essentially the same as in Kopra (2019b), but Section 4 has been revised extensively. Section 5 is new, and the computations in it are originally from the author's Ph.D. thesis (Kopra 2019a).

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 $x \in A^{\mathbb{Z}}$ is interpreted as a bi-infinite sequence and we denote by $x[i]$ the symbol that occurs in x at position i. A *factor* of x is any finite sequence $x[i]x[i + 1] \cdots x[j]$ 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 ϵ) where $w[i] \in A$ is a *word* over A. If $w \neq \epsilon$, we say that w *occurs* in x at position i if $x[i] \cdots x[i + n - 1] = w[1] \cdots w[n]$ 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 $LK = \{w_1 w_2 \mid w_1 \in L, w_2 \in K\}$ and $L^* = \{w_1 \cdots w_n \mid n \geq 0, w_i \in L\}$. If $\epsilon \notin L$, define $L^+ = L^* \setminus \{\epsilon\}$ and if $\epsilon \in L$, define $L^+ = L^*$. The set of words of length n is denoted by A^n. For a word $w \in A^*$, $|w|$ denotes its length, i.e. $|w| = n \Longleftrightarrow w \in A^n$.

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 $S \subseteq A^C$ is compact if and only if it is closed). In our considerations $C = \mathbb{Z}$ or $C = \mathbb{Z}^2$. We define the *shift* $\sigma : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ by $\sigma(x)[i] = x[i + 1]$ for $x \in A^{\mathbb{Z}}$, $i \in \mathbb{Z}$, which is a homeomorphism. We say that a closed set $X \subseteq A^{\mathbb{Z}}$ is a *subshift* if $\sigma(X) = X$. Any $w \in A^+$ and $i \in \mathbb{Z}$ determine a *cylinder* of X

$$\mathrm{Cyl}_X(w, i) = \{x \in X \mid w \text{ occurs in } x \text{ at position } i\}.$$

Every cylinder is an open set of X and the collection of all cylinders

$$\mathcal{C}_X = \{\mathrm{Cyl}_X(w, i) \mid w \in A^+, i \in \mathbb{Z}\}$$

is a basis for the topology of X.

Occasionally we consider configuration spaces $(A_1 \times A_2)^{\mathbb{Z}}$ and then we may write $(x_1, x_2) \in (A_1 \times A_2)^{\mathbb{Z}}$ where $x_i \in A_i^{\mathbb{Z}}$ 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 x_1 is on the upper layer or on the A_1-layer, and similarly that x_2 is on the lower layer or on the A_2-layer.

Definition 1 Let $X \subseteq A^{\mathbb{Z}}$ be a subshift. We say that the map $F : X \to X$ is a *cellular automaton* (or a CA) on X if there exist integers $m \leq a$ (memory and anticipation) and a *local rule* $f : A^{a-m+1} \to A$ such that $F(x)[i] = f(x[i + m], \ldots, x[i], \ldots, x[i + a])$. If we can choose $m = 0$ we say that F is a *one-sided* CA. A one-sided CA with anticipation 1 is called a radius-$\frac{1}{2}$ CA.

Note that both memory and anticipation can be either positive or negative. For instance, a negative value of the memory m means that the value of $F(x)[i]$ can also depend on those values in the sequence x that are contained on the left side of the coordinate i.

We can extend any local rule $f : A^{a-m+1} \to B$ to words $w = w[1] \cdots w[a - m + n] \in A^{a-m+n}$ with $n \in \mathbb{N}_+$ by $f(w) = u = u[1] \cdots u[n]$, where $u[i] = f(w[i], \ldots, w[i + a - m])$.

The CA-functions on X are characterized as those continuous maps on X that commute with the shift (Hedlund 1969). We say that a CA $F : X \to X$ is *reversible* if it is bijective. Reversible CA are homeomorphisms on X. The book (Lind and Marcus 1995) is a standard reference for subshifts and cellular automata on them.

For a given reversible CA $F : X \to X$ and a configuration $x \in X$ it is often helpful to consider the *space-time diagram* of x with respect to F. Formally it is the map $\theta \in A^{\mathbb{Z}^2}$ defined by $\theta(i, -j) = F^j(x)[i]$: the minus sign in this definition signifies that time increases in the negative direction of the vertical coordinate axis. Informally the space-time diagram of x is a picture which depicts elements of the sequence $(F^i(x))_{i \in \mathbb{Z}}$ in such a way that $F^{i+1}(x)$ is drawn below $F^i(x)$ for every i.

The definition of Lyapunov exponents is from Shereshevsky (1992), Tisseur (2000). For a fixed subshift $X \subseteq A^{\mathbb{Z}}$ and for $x \in X$, $s \in \mathbb{Z}$, denote $W_s^+(x) = \{y \in X \mid \forall i \geq s : y[i] = x[i]\}$ and $W_s^-(x) = \{y \in X \mid \forall i \leq s : y[i] = x[i]\}$. Then for a given cellular automaton $F : X \to X$, $x \in X$, $n \in \mathbb{N}$, define

$$\Lambda_n^+(x, F) = \min\{s \geq 0 \mid \forall 1 \leq i \leq n : F^i(W_0^+(x)) \subseteq W_s^+(F^i(x))\}$$

$$\Lambda_n^-(x, F) = \min\{s \geq 0 \mid \forall 1 \leq i \leq n : F^i(W_0^-(x)) \subseteq W_{-s}^-(F^i(x))\}.$$

These have shift-invariant versions $\overline{\Lambda}_n^{\pm}(x, F) = \max_{i \in \mathbb{Z}} \Lambda_n^{\pm}(\sigma^i(x), F)$. The quantities

$$\lambda^+(x, F) = \lim_{n \to \infty} \frac{\overline{\Lambda}_n^+(x, F)}{n},$$

$$\lambda^-(x, F) = \lim_{n \to \infty} \frac{\overline{\Lambda}_n^-(x, F)}{n}$$

are called (when the limits exist) respectively the right and left *Lyapunov exponents of x* (with respect to F).

A global version of these are the quantities

$$\lambda^+(F) = \lim_{n \to \infty} \max_{x \in X} \frac{\Lambda_n^+(x, F)}{n},$$

$$\lambda^-(F) = \lim_{n \to \infty} \max_{x \in X} \frac{\Lambda_n^-(x, F)}{n}$$

that are called respectively the right and left *(maximal) Lyapunov exponents* of F. These limits exist by an application of Fekete's subadditive lemma (e.g. Lemma 4.1.7 in Lind and Marcus (1995)). We note that at least when F is a CA on some full shift $A^{\mathbb{Z}}$, there exists a configuration $x \in A^{\mathbb{Z}}$ such that $\lambda^{\pm}(x, F) = \lambda^{\pm}(F)$: for example, one can choose some x containing occurrences of all the words from A^*.

Occasionally we consider cellular automata from the measure theoretical point of view. For a subshift X we denote by $\Sigma(\mathcal{C}_X)$ the *sigma-algebra* generated by the collection of cylinders $\mathcal{C}_X$. It is the smallest collection of subsets of X which contains all the elements of $\mathcal{C}_X$ and which is closed under complement and countable unions. A *measure* on X is a countably additive function $\mu : \Sigma(\mathcal{C}_X) \to [0, 1]$ such that $\mu(X) = 1$, i.e. $\mu(\bigcup_{i=0}^{\infty} A_i) = \sum_{i=0}^{\infty} \mu(A_i)$ whenever all $A_i \in \Sigma(\mathcal{C}_X)$ are pairwise disjoint. A measure μ on X is completely determined by its values on cylinders. We say that a cellular automaton $F : X \to X$ preserves the measure μ if $\mu(F^{-1}(S)) = \mu(S)$ for all $S \in \Sigma(\mathcal{C})$.

On full shifts $A^{\mathbb{Z}}$ we are mostly interested in the *uniform measure* determined by $\mu(\mathrm{Cyl}\,(w, i)) = |A|^{-|w|}$ for $w \in A^+$ and $i \in \mathbb{Z}$. By Theorem 5.4 in Hedlund (1969) any surjective CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ preserves this measure. For more on measure theory of cellular automata, see Pivato (2009).

Measure theoretical variants of Lyapunov exponents are defined as follows. Given a measure μ on X (typically assumed to be preverved by F and σ) and for $n \in \mathbb{N}$, let $I_{n,\mu}^+(F) = \int_{x \in X} \Lambda_n^+(x, F) d\mu$ and $I_{n,\mu}^-(F) = \int_{x \in X} \Lambda_n^-(x, F) d\mu$. Then the quantities

$$I_{\mu}^+(F) = \liminf_{n \to \infty} \frac{I_{n,\mu}^+(F)}{n}, \qquad I_{\mu}^-(F) = \liminf_{n \to \infty} \frac{I_{n,\mu}^-(F)}{n}$$

are called respectively the right and left *average Lyapunov exponents* of F (with respect to the measure μ).

We will write $W_s^{\pm}(x)$, $\Lambda_n^{\pm}(x)$, $\lambda^+(x)$, $I_{n,\mu}^+$ and I_{μ}^+ when X and F are 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 $t : \{N, E, S, W\} \to C$ 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 η 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 [*Lukkarila* (2010), *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 $p : X \to Y$. Let $T^{\complement}$ 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 $A = T \cup T^{\complement}$ is complete.

Every complete 2-way deterministic tile set A determines a local rule $f : A^2 \to A$ defined by $f(a, b) = c \in A$, where c is the unique tile such that $a_S = c_N$ and $b_W = c_E$. This then determines a reversible radius-$\frac{1}{2}$ CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$

by $F(x)[i] = f(x[i], x[i+1])$ for $x \in A^{\mathbb{Z}}$, $i \in \mathbb{Z}$. The space-time diagram of a configuration $x \in A^{\mathbb{Z}}$ corresponds to a valid tiling η via $\theta(i, -j) = F^j(x)[i] = \eta(i, -i - j)$, i.e. configurations $F^j(x)$ are diagonals of η going from northwest to southeast and the diagonal corresponding to $F^{j+1}(x)$ is below the diagonal corresponding to $F^j(x)$.

Definition 5 A cellular automaton $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is (p, q)-locally immortal ($p, q \in \mathbb{N}$) with respect to a subset $B \subseteq A$ if there exists a configuration $x \in A^{\mathbb{Z}}$ such that $F^{iq+j}(x)[ip] \in B$ for all $i \in \mathbb{Z}$ and all j such that $0 \le j \le q$. Such a configuration x is a (p, q)-witness.

Generalizing the definition in Lukkarila (2010), we call the following decision problem the (p, q)-*local immortality problem*: given a reversible CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ and a subset $B \subseteq A$, find whether F is (p, q)-locally immortal with respect to B.

Theorem 2 *(Lukkarila 2010, Theorem 5.1.5) The $(0, 1)$-local immortality problem is undecidable for reversible CA.*

We now adapt the proof of Theorem 2 to get the following result, which we will use in the proof of Theorem 3.

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 $T \cup T^{\complement}$ as indicated above. Then also $A_1 = (T \times T_1) \cup (T^{\complement} \times T_2)$ (T_1 and T_2 as in Fig. 1) is a complete tile set.[1] 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 $G_1 : A_1^{\mathbb{Z}} \to A_1^{\mathbb{Z}}$.

Let $A_2 = \{0, 1, 2\}$. Define $A = A_1 \times A_2$ and natural projections $\pi_i : A \to A_i$, $\pi_i(a_1, a_2) = a_i$ for $i \in \{1, 2\}$. By extension we say that $a \in A$ is an arrow tile if $\pi_1(a) \in R$. Let $G : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ 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 construct involutive CA J_1, J_2 and H of memory 0 with local rules $j_1 : A_2 \to A_2$, $j_2 : A_2^2 \to A_2$ and $h : (A_1 \times A_2) \to (A_1 \times A_2)$ respectively defined by

---
[1] The arrow markings are used as a shorthand for some coloring such that in a valid tiling an arrowhead on the edge of one tile must connect with an arrow tail on the edge of the neighboring tile. Strictly speaking all the necessary information concerning the tiles is on the edges: the lines in the tile interiors are only a guide to intuition.
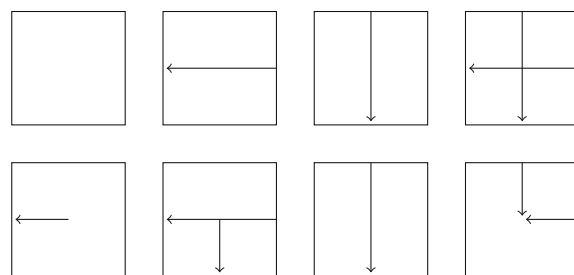
Fig. 1 The tile sets T_1 (first row) and T_2 (second row). These are originally from Lukkarila (2010) (up to a reflection with respect to the northwest - southeast diagonal)

$$j_1(0) = 0$$
$$j_1(1) = 2 \qquad j_2(a_2, b_2) = \begin{cases} 1 & \text{when } (a_2, b_2) = (0, 2) \\ 0 & \text{when } (a_2, b_2) = (1, 2) \\ a & \text{otherwise} \end{cases}$$
$$j_1(2) = 1$$

$$h((a_1, a_2)) = \begin{cases} (a_1, 1) & \text{when } a_1 \in R \text{ and } a_2 = 0 \\ (a_1, 0) & \text{when } a_1 \in R \text{ and } a_2 = 1 \\ (a_1, a_2) & \text{otherwise.} \end{cases}$$

If $\text{id} : A_1^{\mathbb{Z}} \to A_1^{\mathbb{Z}}$ 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 $F = H \circ J \circ G : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$, which is reversible because G is reversible and $H \circ J$ is a composition of involutions. We will show that T admits a valid tiling if and only if F is $(1, 5)$-locally immortal with respect to $B = (T \times \{t_b\}) \times \{0\}$.

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

Assume then that T does not admit any valid tiling and for a contradiction assume that x is a $(1, 5)$-witness. Let θ be the space-time diagram of x with respect to F. Since x is a $(1, 5)$-witness, it follows that $\theta(i, -j) \in B$ whenever $(i, -j) \in N$, where $N = \{(i, -j) \in \mathbb{Z}^2 \mid 5i \le j \le 5(i+1)\}$. There is a valid tiling η over A_1 such that $\pi_1(\theta(i, j)) = \eta(i, j - i)$ for $(i, j) \in \mathbb{Z}^2$, i.e. η can be recovered from the upper layer of θ by applying a suitable linear transformation on the space-time diagram. In drawing pictorial representations of θ 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 $D = \{(i, j) \in \mathbb{Z}^2 \mid j > -6i\}$ and in particular that $\eta(i, j)$ is an arrow tile. Since θ contains a "bent" version of η, 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 Fig. 3 we present the space-time diagram θ with arrow markings of tiles from T_1 and T_2

replaced according to the Fig. 2. In Fig. 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 θ 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 Fig. 3). Fix $p, q \in \mathbb{Z}$ so that $\theta(p, q - 2)$ is one such tile and in particular $(p - d_1, q - 2), (p, q - 2 - d_2) \in N$. We note that $\theta(p - i, q - j)$ does not contain an arrow for $0 < i \le d_1$, $-2 \le j \le 3$. Namely, assume to the contrary that it does contain an arrow for some fixed i and j (and in particular $(p - i, q - j) \notin N$). It is clear that at least in the case $i > 1$ the horizontal distance of $\theta(p - i, q - j)$ from N is strictly less than d_1, contradicting the minimality of d_1. If on the other hand $i = 1$, the tile $\theta(p - 1, q - j)$ could have horizontal distance from N equal to d_1, so assume that it is so. Since N is invariant under translation by the vector $-(1, -5)$, then from $(p, q - 2 - d_2) \in N$ it follows that $(p - 1, q + 3 - d_2) \in N$ and that the vertical distance of the tile $\theta(p - 1, q - j)$ from N is at most $(q - j) - (q + 3 - d_2) \le d_2 - 1$, contradicting the minimality of d_2.

Now it can be seen that $\theta(p, q - j)$ contains an arrow for $-2 \le j \le 2$, because if there is a $j \in [-2, 2)$ such that $\theta(p, q - j)$ does not contain an arrow and $\theta(p, q - j - 1)$ does, then $\theta(p, q - j - 1)$ must contain one of the three arrows on the left half of Fig. 2. These three arrows continue to the southwest, so then also $\theta(p - 1, q - j - 2)$ contains an arrow, but this contradicts the previous paragraph.

Now consider the A_2-layer of θ. For the rest of the proof let $y = F^{-q}(x)$. Assume that $\pi_2(\theta(i, q)) = \pi_2(y[i])$ is nonzero for some $-q/5 < i \le p$ (in other words, the coordinate (i, q) is to the left of (p, q) and $(i, q) \in E$), and fix the least such i, i.e. $\pi_2(y[s]) = 0$ for s in the set

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

We start by considering the case $\pi_2(y[i]) = 1$. Denote

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

From the choice of (p, q) it follows that $\pi_1(\theta(s, q - 1)) = \pi_1(G(y)[s])$ are not arrow tiles for $s \in I_1$, and therefore we can compute step by step that

$\pi_2((\mathrm{id} \times J_1)(G(y))[i]) = 2$, $\quad \pi_2((\mathrm{id} \times J_1)(G(y))[s]) = 0$ for $s \in I_0 \supseteq I_1$,
$\pi_2(J(G(y))[i - 1]) = 1$, $\quad \pi_2(J(G(y))[s]) = 0$ for $s \in I_1 \setminus \{i - 1\}$,
$\pi_2(F(y)[i - 1]) = 1$, $\quad \pi_2(F(y)[s]) = 0$ for $s \in I_1 \setminus \{i - 1\}$

and $\pi_2(\theta(i - 1, q - 1)) = 1$. By repeating this argument inductively we see that the digit 1 propagates to the lower left in the space-time diagram as indicated by Fig. 4 and

eventually reaches N, a contradiction. If on the other hand $\pi_2(\theta(i, q)) = 2$, a similar argument shows that the digit 2 propagates to the upper left in the space-time diagram as indicated by Fig. 4 and eventually reaches N, also a contradiction.

Assume then that $\pi_2(\theta(i, q))$ is zero whenever $-q/5 < i \le p$ (or equivalently, whenever (i, q) is to the left of (p, q) and $(i, q) \in E$). If $\pi_2(\theta(p + 1, q)) = \pi_2(y[p + 1]) \ne 1$, then $\pi_2((\mathrm{id} \times J_1)(G(y))[p + 1]) \ne 2$ and $\pi_2(J(G(y))[p]) = 0$. Since $\pi_1(\theta(p, q - 1))$ is an arrow tile, it follows that $\pi_2(\theta(p, q - 1)) = \pi_2(H(J(G(y)))[p]) = 1$. The argument of the previous paragraph shows that the digit 1 propagates to the lower left in the space-time diagram as indicated by the left side of Fig. 5 and eventually reaches N, a contradiction.

Finally consider the case $\pi_2(\theta(p + 1, q)) = \pi_2(y[p + 1]) = 1$. Then

$\pi_2(J(G(y))[p])\pi_2(J(G(y))[p + 1]) = 12$ and
$\pi_2(F(y)[p])\pi_2(F(y)[p + 1]) = 02$.

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

Remark 1 It is possible that for every choice of $p \in \mathbb{N}$ and $q \in \mathbb{N}_+$ the (p, q)-local immortality problem for reversible radius-$\frac{1}{2}$ CA is undecidable. We proved this in the case $(p, q) = (1, 5)$ but for our purposes it is sufficient to prove this just for some $p > 0$ and $q > 0$. The important (seemingly paradoxical) part will be that for $(1, 5)$-locally immortal radius-$\frac{1}{2}$ CA F the "local immortality" travels to the right in the space-time diagram even though in reality there cannot be any information flow to the right because F is one-sided.

Remark 2 The automaton of the previous lemma was found by a little bit of trial and error: $J_2 \circ J_1$ is one of the simplest nontrivial reversible radius-$\frac{1}{2}$ CA that comes to mind, and we just coupled its dynamics with the tile set of Lukkarila (2010) via the CA H. After that we chose to consider $(1, 5)$-local immortality to get at least five consecutive arrows in the space-time diagram that "shield" signals of non-zero digits from possible interference caused by other arrows (Figure 4) and generate new signals of non-zero digits (Figure 5). For these purposes a smaller number of consecutive arrows in the space-time diagram is probably sufficient and one could show the undecidability of $(1, q)$-local immortality also for some smaller q. Our proof cannot be used to show the undecidability of $(1, 1)$-local immortality, because then the signal of non-zero
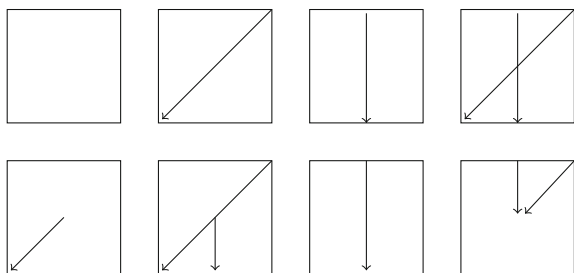
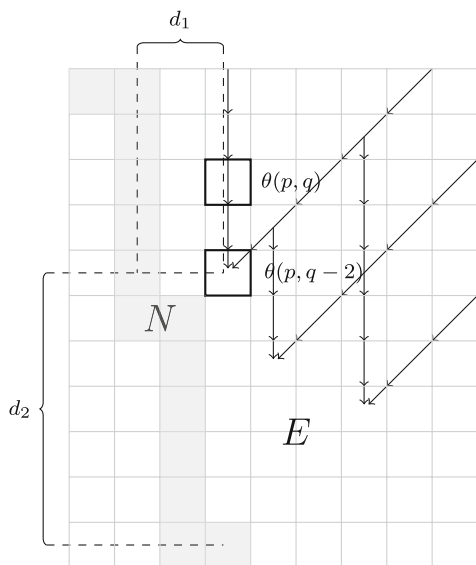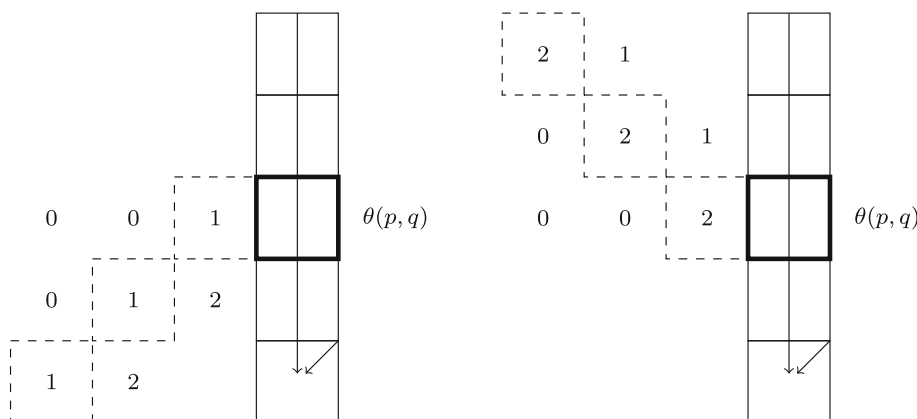**Fig. 2** The tile sets T_1 and T_2 presented in a "bent" form

Fig. 3 The space-time diagram θ with "bent" arrow markings. The set N is the infinite band colored in gray and the set E is the half-plane to the right of N. An arrow tile $\theta(p, q-2)$ in E with minimal horizontal and vertical distances to N has been highlighted

digits in the right side of Fig. 4 would travel at the same speed as the "local immortality", parallel to the infinite band N which we would now define to be at a 45 degree angle with respect to the vertical axis.

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. Specifically, we will show that the cases $\lambda^+(F) \leq \frac{5}{3}$ and $\lambda^+(F) = 2$ are algorithmically inseparable in the class of reversible CA. We first present simple examples of CA corresponding to these cases.

Example 1 Consider the shift map σ^{-t} for $t \geq 0$ over some full shift $A^{\mathbb{Z}}$. For any $i \in \mathbb{N}$ and $x \in A^{\mathbb{Z}}$ we see that $(\sigma^{-t})^i (W_0^+(x)) = W_{ti}^+((\sigma^{-t})^i(x))$ and thus $(\sigma^{-t})^i(W_0^+(x)) \subseteq W_s^+((\sigma^{-t})^i(x))$ for $s \in \mathbb{N}$ if and only if $s \geq ti$. For a fixed $n \in \mathbb{N}$ the inequality $s \geq ti$ holds for $1 \leq i \leq n$ if and only if $s \geq tn$ and therefore $\Lambda_n^+(x, \sigma^{-t}) = tn$. Using this we conclude that the right Lyapunov exponent is

$$\lambda^+(\sigma^{-t}) = \lim_{n \to \infty} \max_{x \in A^{\mathbb{Z}}} \frac{\Lambda_n^+(x, \sigma^{-t})}{n} = \lim_{n \to \infty} \frac{tn}{n} = t.$$

Some examples of reversible CA corresponding to the two cases noted above are σ^{-1} and σ^{-2}, whose right Lyapunov exponents are equal to 1 and 2 respectively.

To achieve greater clarity we first prove our result in Theorem 3 for a special class of subshifts, where the configurations contains at most one "particle". Cellular automata can then use this particle for easily controlled information propagation.

Definition 6 Let $Q, \Sigma, A_1 = Q \cup \Sigma$ and A_2 be alphabets such that $0 \in \Sigma$ and $Q \cap \Sigma = \emptyset$, let $\rho : A_1 \to A_1$ be an involution (i.e. $\rho^2 = \mathrm{id}$) acting as the identity on Σ and let

$$Y = \{y \in A_1^{\mathbb{Z}} \mid y[i] \in Q \text{ for at most one } i \in \mathbb{Z}\}.$$

Then $X = Y \times A_2^{\mathbb{Z}}$ is a $(Q, \Sigma, Y, A_2, \rho)$ *particle shift* (or just a particle shift), the elements of Q are called its *particles* and the map ρ is a *particle flip*.

Fig. 4 Propagation of digits to the left of $\theta(p, q)$. The tile $\theta(p, q)$ is denoted by thick edges and nearby tiles guaranteed to contain arrows are denoted by solid edges. The tiles on diagonals along which the "front" of non-zero digits propagates are denoted by dashed edges
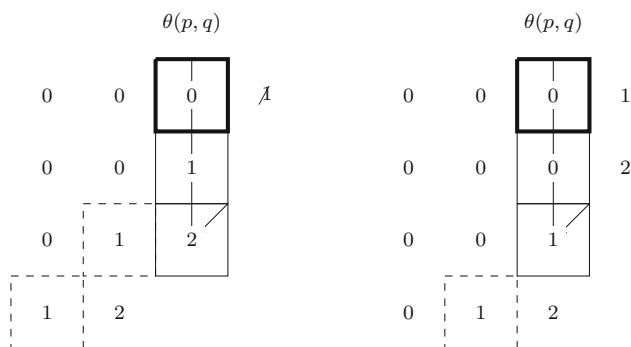
Fig. 5 Propagation of digits at $\theta(p,q)$. The tile $\theta(p,q)$ is denoted by thick edges and nearby tiles guaranteed to contain arrows are denoted by solid edges. The tiles on diagonals along which the "front" of non-zero digits propagates are denoted by dashed edges

We define the natural projections $\pi_1 : X \to Y$, $\pi_2 : X \to A_2^{\mathbb{Z}}$ by $\pi_1(y,z) = y$, $\pi_2(y,z) = z$ for $y \in Y, z \in A_2^{\mathbb{Z}}$.

For $y \in Y$ we will also denote by $\rho(y)$ the coordinate-wise application of ρ to y: equivalently, ρ is applied to the only symbol from Q in y (if there is such a symbol). The interpretation for the map ρ will be that it changes the "direction" of the particle symbol without changing its speed. We also define a few special classes of CA on particle shifts.

Definition 7 The reversal of a configuration $x \in A^{\mathbb{Z}}$ is the configuration x^R defined by $x^R[i] = x[-i]$ for all $i \in \mathbb{Z}$.

Definition 8 A reversible CA $F : X \to X$ on a $(Q, \Sigma, Y, A_2, \rho)$ particle shift X is a *particle rule* if there is a CA $S : Y \to Y$ such that

- $F(y,z) = (S(y), z)$ for all $y \in Y$, $z \in A_2^{\mathbb{Z}}$ (i.e. F only changes the top layer in a way that does not depend on the bottom layer)
- $S(y) = y$ for all $y \in \Sigma^{\mathbb{Z}}$ (i.e. S does nothing when y does not contain particles)
- If $y \in Y$ and $y[i] \in Q$ for some $i \in Z$, then either there is a $j \in \mathbb{Z}$ such that $y[j] = 0$ and $S(y)[i] = 0$, $S(y)[j] \in Q$ and $S(y)[k] = y[k]$ for $k \notin \{i,j\}$ (i.e. the particle in y moves to an empty position) or $S(y)[i] \in Q$ and $S(y)[k] = y[k]$ for $k \neq i$ (i.e. the particle in y possibly changes but remains in the same position)
- $S(\rho(y^R)) = \rho(S(y)^R)$ for all $y \in Y$ (i.e. S has a left-right symmetry).

Definition 9 A reversible one-sided CA $G : X \to X$ on a $(Q, \Sigma, Y, A_2, \rho)$ particle shift X is a *background rule* if there is a CA $G' : A_2^{\mathbb{Z}} \to A_2^{\mathbb{Z}}$ such that $G(y,z) = (y, G'(z))$ for all $y \in Y$, $z \in A_2^{\mathbb{Z}}$ (i.e. G only changes the bottom layer in a way that does not depend on the top layer or on symbols to the left).

Definition 10 Let X be a $(Q, \Sigma, Y, A_2, \rho)$ particle shift and let $w_1, w_2 \in \Sigma^n Q \Sigma^m$ for some $n, m \in \mathbb{N}$ be words of equal length such that none of the symbols of w_1 occur in w_2 and vice versa. Let $W \subseteq A_2^*$ and $j \in \mathbb{Z}$. A reversible CA $H : X \to X$ is a *coupling rule* (with parameters (w_1, w_2, W, j)) if for all $y \in Y$, $z \in A_2^{\mathbb{Z}}$ the configuration $H(y, z)$ is obtained by replacing an occurrence of w_1 by w_2 (and vice versa) at position i in y if and only if $z \in \text{Cyl}(w, i+j)$ for some $w \in W$.

Theorem 3 *For reversible CA $F : X \to X$ on particle shifts such that $\lambda^+(F) \in [0, \frac{5}{3}] \cup \{2\}$ and F is some composition of particle rules, background rules and coupling rules 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 $G' : A_2^{\mathbb{Z}} \to A_2^{\mathbb{Z}}$ be a given reversible radius-$\frac{1}{2}$ cellular automaton and $B \subseteq A_2$ some given set. Let $\Sigma = \{0, \|\}$, $Q = \{\leftarrow, \rightarrow, \nearrow, \searrow\}$, let $A_1 = Q \cup \Sigma$ and define the subshift $Y \subseteq A_1^{\mathbb{Z}}$ as the set of those configurations containing a symbol from Q in at most one position. Then X is a $(Q, \Sigma, Y, A_2, \rho)$ particle shift with the particle flip ρ defined by

$$\rho(0) = 0 \qquad \rho(\|) = \|$$
$$\rho(\leftarrow) = \rightarrow \qquad \rho(\rightarrow) = \leftarrow \qquad \rho(\nearrow) = \searrow \qquad \rho(\searrow) = \nearrow$$

We will interpret elements of Q as particles going in different directions at different speeds and which bounce between walls denoted by $\|$. Let $S : Y \to Y$ be the reversible CA which does not move occurrences of $\|$ and which moves $\leftarrow$ (resp. $\rightarrow$, $\nearrow$, $\searrow$) 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 opposite direction. More precisely, S is the CA with memory -2 and anticipation 2 determined by the local rule $f : A_1^5 \to A_1$ defined as follows (where $*$ denotes arbitrary symbols):

$$f(\rightarrow, 0, 0, *, *) = \rightarrow \qquad f(*, \searrow, 0, *, *) = \searrow$$
$$f(*, \rightarrow, 0, \|, *) = \leftarrow \qquad f(*, *, \searrow, 0, *) = 0,$$
$$f(*, *, \rightarrow, 0, *) = 0 \qquad f(*, *, \searrow, \|, *) = \nearrow,$$
$$f(*, 0, \rightarrow, \|, *) = 0$$
$$f(*, \|, \rightarrow, \|, *) = \rightarrow$$
$$f(*, *, 0, \rightarrow, \|) = \leftarrow$$

with symmetric definitions for arrows in the opposite directions at reflected positions and $f(*, *, a, *, *) = a$ ($a \in Q \cup \Sigma$) otherwise.

Let $x_1 \in Y$ and $x_2 \in A_2^{\mathbb{Z}}$ be arbitrary. We define reversible CA $G, F_1 : X \to X$ by $G(x_1, x_2) = (x_1, G'^{10}(x_2))$, $F_1(x_1, x_2) = (S(x_1), x_2)$. They are easily seen to be a

background rule and a particle rule respectively. Additionally, let $F_2: X \to X$ be the involution which maps (x_1, x_2) as follows: F_2 replaces an occurrence of $\to 0 \in Q\Sigma$ in x_1 at a coordinate $i \in \mathbb{Z}$ by an occurrence of $\diagup \| \in Q\Sigma$ (and vice versa) *if and only if*

$G'^j(x_2)[i] \notin B$ for some $0 \leq j \leq 5$

or $G'^j(x_2)[i+1] \notin B$ for some $5 \leq j \leq 10$,

and otherwise F_2 makes no changes. The map F_2 is then a coupling rule. Finally, define $F = F_1 \circ G \circ F_2 : X \to X$. 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 $\to$ which does not have a wall immediately at the front and x_2 does not satisfy a local immortality condition in the next 10 time steps, then $\to$ changes into $\diagup$ and at the same time leaves behind a wall segment $\|$. Conversely, if there is a particle $\diagup$ to the left of the wall $\|$ and x_2 does not satisfy a local immortality condition, $\diagup$ changes into $\to$ and removes the wall segment. The choice of the power 10 in G'^{10} is to make the "local immortality" in a potential $(1, 5)$-witness of G' to travel two steps to the right at each application of F, which is the same as the intended speed for the particle $\to$.

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 $x, y \in X$ are two configurations that differ only to the left of the origin, then the difference between $F^i(x)$ and $F^i(y)$ can propagate to the right at speed 2 only via an arrow $\to$ 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 $x_2 \in A_2^{\mathbb{Z}}$ be a $(1, 5)$-witness and define $x_1 \in Y$ by $x_1[0] = \to$ and $x_1[i] = 0$ for $i \neq 0$. Let $x = (0^{\mathbb{Z}}, x_2) \in X$ and $y = (x_1, x_2) \in X$. It follows that $\pi_1(F^i(x))[2i] = 0$ and $\pi_1(F^i(y))[2i] = \to$ for every $i \in \mathbb{N}$, so $\lambda^+(F) \geq 2$. On the other hand, F has memory -2 so necessarily $\lambda^+(F) = 2$.

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

$C(n) = \{x \in A_2^{\mathbb{Z}} \mid G'^{5i+j}(x)[i] \in B$ for $0 \leq i \leq n, 0 \leq j \leq 5\}$ 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 $(x^{(n)})_{n \in \mathbb{N}}$

with $x^{(n)} = (x_1^{(n)}, x_2^{(n)}) \in X$ is a sequence of configurations such that $\Lambda_n^+(x^{(n)}, F) = s_n n$ where $(s_n)_{n \in \mathbb{N}}$ tends to λ^+. There exist $y^{(n)} = (y_1^{(n)}, y_2^{(n)}) \in X$ such that $x^{(n)}[i] = y^{(n)}[i]$ for $i \geq 0$ and $F^{t_n}(x)[i_n] \neq F^{t_n}(y)[i_n]$ for some $0 \leq t_n \leq n$ and $i_n = s_n n - 1$. Since G' is a one-sided CA, it follows that $\pi_2(F^{t_n}(x^{(n)}))[j] = \pi_2(F^{t_n}(y^{(n)}))[j]$ for $j \geq 0$. Therefore the difference between $x^{(n)}$ and $y^{(n)}$ can propagate to the right only via an arrow from Q, which must at some time step first visit some position to the left of coordinate 0. Without loss of generality (by swapping $x^{(n)}$ and $y^{(n)}$ if necessary) there are $0 \leq t_{n,1} < t_{n,2} \leq n$ and $j_n \geq i_n - 1$ such that $\pi_1(F^{t_{n,1}}(x^{(n)}))[-s] \in Q$ for some $s > 0$ and $\pi_1(F^{t_{n,2}}(x^{(n)}))[j_n] \in Q$. Fix some such $t_{n,1}, t_{n,2}, j_n$ and let $w_n \in Q^{(t_{n,2} - t_{n,1}) + 1}$ be such that $w_n[i]$ is the unique state from Q in the configuration $F^{t_{n,1}+i}(x^{(n)})$ for $0 \leq i \leq t_{n,2} - t_{n,1}$.

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 $v_i \in \{\to\}^+$, $v \in \{\to\}^*$ and $u_i \in (Q \setminus \{\to\})^+$, $u \in (Q \setminus \{\to\})^*$. 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 $\diagup$ and at least $2(|v_i| - 1) + 1$ occurrences of $\diagdown$. Namely, $\to$ can only change into $\diagup$ via the map F_2, at which point a new wall is created on the right side of $\diagup$. The arrow $\diagup$ must return to the nearest wall to the left, then come back as $\diagdown$ to the new wall on the right, and then at least once more turn into $\diagup$ before turning back into $\to$ via the map F_2. If $\to$ were to turn into $\leftarrow$ instead, it would signify a wall on the right which cannot be removed at any time step by the map F_2 and which the arrow cannot therefore bypass.

If we denote by k_n the number of occurrences of $\to$ in w_n, then $k_n \leq |w_n|/3 + \mathcal{O}(1)$ (this upper bound is achieved by assuming that $|v_i| = 1$ for every i) and

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

After dividing this inequality by n and passing to the limit we find that $\lambda^+(F) \leq \frac{5}{3}$.[2] $\qquad \square$

To prove the uncomputability result for full shifts, we use the conveyor belt construction introduced in Kim and Roush (1990) (where it is called the bucket passing construction). The variant that we use follows closely the one in Guillon and Salo (2017).

Definition 11 Let X be a $(Q, \Sigma, Y, A_2, \rho)$ particle shift. Define alphabets $A_1 = Q \times \Sigma$, $\Delta = \{-, 0, +\}$ and

---

[2] By performing more careful estimates it can be shown that $\lambda^+(F) = 1$, but we will not attempt to formalize the argument for this.

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

Then the *belted version of X* is the full shift $X_\circ = A^\mathbb{Z}$ over the alphabet $A = \Gamma \times A_2$. The natural projections $\pi_{1,1}, \pi_{1,2} : A^\mathbb{Z} \to A_1^\mathbb{Z}$, $\pi_\Delta : A^\mathbb{Z} \to \Delta^\mathbb{Z}$, $\pi_2 : A^\mathbb{Z} \to A_2^\mathbb{Z}$ are defined as $\pi_{1,1}(x) = x_{1,1}$, $\pi_{1,2}(x) = x_{1,2}$, $\pi_\Delta(x) = x_\Delta$, $\pi_2(x) = x_2$ for $x = (x_{1,1}, x_{1,2}, x_\Delta, x_2) \in A^\mathbb{Z} \subseteq (A_1 \times A_1 \times \Delta \times A_2)^\mathbb{Z}$.

The configurations of $X_\circ$ can be decomposed into several disjoint "conveyor belts" with "junction points": this will become clearer after the next few definitions.

Definition 12 Every element $x = (x_1, x_2) \in (\Gamma \times A_2)^\mathbb{Z}$ on belted version $X_\circ$ of a $(Q, \Sigma, Y, A_2, \rho)$ particle shift X has a unique decomposition of the form

$$(x_1, x_2) = \cdots (w_{-2}, v_{-2})(w_{-1}, v_{-1})(w_0, v_0)$$
$$(w_1, v_1)(w_2, v_2)\cdots$$

where $v_i \in A_2^+$ and

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

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

$$\{j_i \in \mathbb{Z} \mid j_i \text{ is the coordinate of the leftmost letter of } w_i \text{ in } x\}$$

is the set of *junction points* of x.

The main reason for defining $X_\circ$ is to be able to "simulate" particle rules of X as reversible automata on some full shift similarly as in Guillon and Salo (2017). To be exact, let F be a particle rule on a $(Q, \Sigma, Y, A_2, \rho)$ particle shift X and let $S : Y \to Y$ be such that $F(y, z) = (S(y), x)$ for $(y, z) \in Y \times A_2^\mathbb{Z}$. We will define $F' : X_\circ \to X_\circ$ as follows. We first consider the decomposition of an arbitrary $x = (x_1, x_2) \in (\Gamma \times A_2)^\mathbb{Z}$ into words (w_i, v_i) in the sense of the previous definition. Let $(c_i, e_i) \in (\Sigma \times \Sigma)^*((Q \times \Sigma) \cup (\Sigma \times Q))(\Sigma \times \Sigma)^* \cup (\Sigma \times \Sigma)^*$ be the word that is derived from w_i by removing the symbols from Δ. The pair (c_i, e_i) can be seen as a conveyor belt by gluing the beginning of c_i to the beginning of e_i and the end of c_i to the end of e_i. The map F' will shift particles of Q like the map F on both layers c_i and e_i, and near the junction points of c_i and e_i the particle can turn around to the opposite side of the belt. More precisely, for a word $u \in A_1^*$ let $\rho(u)$ denote the coordinatewise application of ρ. For any word

$w = w[1] \cdots w[n]$ define its reversal by $w^R[i] = w[n+1-i]$ for $1 \le i \le n$. Then consider the periodic configuration $y = [(c_i, v_i)(\rho(e_i), v_i)^R]^\mathbb{Z} \in (A_1 \times A_2)^\mathbb{Z}$. The map $F : X \to X$ extends naturally to configurations of the form y: y can contain infinitely many particles, but they are all identical and occur in identical contexts. By applying F to y we get a new configuration of the form $[(c_i', v_i)(\rho(e_i'), v_i)^R]$. From this we extract the pair (c_i', e_i'), and by adding plusses and minuses to the left and right of the particle (or in the same coordinates as in (c_i, e_i) if there is no occurrence of a particle) we get a word w_i' which is of the same form as w_i. We define $F' : A^\mathbb{Z} \to A^\mathbb{Z}$ by $F'(x) = x'$ where $x' = \cdots (w_{-2}', v_{-2})(w_{-1}', v_{-1})(w_0', v_0)(w_1', v_1)(w_2', v_2)\cdots$. Clearly F' is shift invariant, continuous and reversible, so it is a reversible CA. We say that F' is a *belted version* of F.

It is important to note that the map F' above acts very similarly to the map F at those points of the configuration that are far away from the junction points and that F' does not transfer information over the junction points to neighboring belts. This is formalized as the following more general definition of a belted version of a reversible CA.

Definition 13 Let $F : X \to X$ be a reversible CA on a $(Q, \Sigma, Y, A_2, \rho)$ particle shift. We say that a reversible CA $F' : X_\circ \to X_\circ$ is a *belted version* of F if the following hold.

- For $z_{top} = (y, x_1, x_\Delta, x_2)$ and $z_{bot} = (x_1, y, x_\Delta, x_2)$ where $x_1 \in \Sigma^\mathbb{Z}$, $y \in Y$ is such that $y[i] \in Q$ for some $i \in \mathbb{Z}$, $x_2 \in A_2^\mathbb{Z}$ and x_Δ is defined by $x_\Delta[i] = 0$, $x_\Delta[i-j] = +$ and $x_\Delta[i+j] = -$ for $j > 0$ it holds that

$$(\pi_{1,1}(F'(z_{top})), \pi_2(F'(z_{top}))) = F(y, x_2)$$
$$\text{and } (\pi_{1,2}(F'(z_{bot})), \pi_2(F'(z_{bot}))) = F(y, x_2).$$

- For all $x \in X_\circ$ the configurations x and $F'(x)$ have the same set of junction points.
- For all $x, y \in X_\circ$ such that $\pi_2(x) = \pi_2(y)$ and any $i, j \in \mathbb{Z}$ such that $x[i, j-1] = y[i, j-1]$ and i, j form a pair of consecutive junction points of both x and y it holds that

$$\pi_{1,k}(F'(x))[i, j-1] = \pi_{1,k}(F'(y))[i, j-1] \text{ for } k \in \{1, 2\}.$$

It is easy to see that if $F', G' : X_\circ \to X_\circ$ are belted versions of reversible CA $F, G : X \to X$ then $F' \circ G'$ is a belted version of $F \circ G$. Belted versions of reversible CA are not necessarily unique.

Lemma 2 *Let $F : X \to X$ be a composition $F_k \circ \cdots \circ F_1$ of particle rules, background rules and coupling rules on a $(Q, \Sigma, Y, A_2, \rho)$ particle shift X such that belted versions F_i' exist for all $1 \le i \le k$. Then for $F' = F_k' \circ \cdots \circ F_1'$ it holds that $\lambda^+(F') = \lambda^+(F)$.*

Proof Assume that $r > 0$ is a common radius for F, F' and for all F_i, F_i'. We first show that $\lambda^+(F') \geq \lambda^+(F)$. For this let $x \in X$ be arbitrary and let $y \in Y, z \in A_2^{\mathbb{Z}}$ be such that $x = (y, z)$. Define a configuration $x_\Delta \in \Delta^{\mathbb{Z}}$ as follows: if y contains a symbol from Q at some position $i \in \mathbb{Z}$, then $x_\Delta[i] = 0$ and $x_\Delta[i - j] = +, x_\Delta[i + j] = -$ for $j > 0$. If y contains no symbols from Q, then $x_\Delta[i] = +$ for all $i \in \mathbb{Z}$. Finally define $z = (y, y, x_\Delta, z) \in X_\bigcirc$. The configuration x_Δ was chosen so that z essentially consists of two layers of conveyor belts without any junction points. The map F' simulates F on these layers in the sense of Definition 13 and so $\Lambda_n^+(z, F') \geq \Lambda_n^+(x, F)$ for all $n \in \mathbb{N}$. Because x was arbitrary, the inequality $\lambda^+(F') \geq \lambda^+(F)$ follows by the definition of Lyapunov exponents.

To show that $\lambda^+(F') \leq \lambda^+(F)$, assume to the contrary that $\lambda^+(F') > \lambda^+(F)$. By the definition of Lyapunov exponents we can choose $n' \in \mathbb{N}$ and $c > 0$ such that

$$\max_{z \in X_\bigcirc} \Lambda_n^+(z, F') > \max_{x \in X} \Lambda_n^+(x, F) + nc$$

for all $n \geq n'$. Fix some such $n \geq 4r \max\{1, 1/c\}$ and some $z \in X_\bigcirc$ such that

$$\Lambda_n^+(z, F') > \max_{x \in X} \Lambda_n^+(x, F) + nc.$$

Denote $d = \Lambda_n^+(z, F')$. There exists $z' \in X_\bigcirc$ such that $z[i] = z'[i]$ for $i \geq 0$ and $F'^t(z)[d-1] \neq F'^t(z')[d-1]$ for some $1 \leq t \leq n$. Since background rules are one-sided and particle rules and coupling rules can change configurations only near particles, the difference between z and z' can propagate to the right only via a symbol from Q which must at some time step first visit some position near the origin, and these configurations cannot have junction points on the interval $[0, d-1]$. Without loss of generality, within t time steps a particle in the upper conveyor belt layer of z first gets within distance r from the coordinate -1 and then gets withing distance r from the coordinate $d-1$ (by swapping z and z' if necessary and by swapping the upper and lower conveyor belt layers of the configurations if necessary). Also, after a sufficiently long time, the particle will remain at least at distance r from the origin. More precisely, there are $1 \leq t_1 < t_2 \leq t$ and $r \leq i_1 < 2r, d-1-r \leq i_2 \leq d-1$ such that for all $t_1 \leq t' \leq t_2$

$$\pi_{1,1}(F'^{t_1}(z))[i_1] \in Q, \quad \pi_{1,1}(F'^{t_2}(z))[i_2] \in Q \text{ and}$$

$$\pi_{1,1}(F'^{t'}(z))[i] \in Q \text{ for some } i \geq r.$$

Define configurations $x, x' \in X$ such that $\pi_2(x) = \pi_2(x') = \pi_2(F'^{t_1}(z))$ and

$\pi_1(x[i]) = 0$ for $i < 0$ and

$\pi_1(x[i]) = \pi_{1,1}(F'^{t_1}(z))[i]$ otherwise ,

$\pi_1(x'[i]) = 0$ for $i < 0$ and for $i = i_1$ and

$\pi_1(x[i]) = \pi_{1,1}(F'^{t_1}(z))[i]$ otherwise.

Consider now the configurations $y = \sigma^{i_1+1}(x)$ and $y' = \sigma^{i_1+1}(x')$. These agree at coordinates $i \geq 0$, y contains a particle at the coordinate -1 and y' contains no particles. Then $F^{t_2-t_1}(y)$ contains a particle at $i_2 - i_1 - 1$ but $F^{t_2-t_1}(y')$ does not. Since $t_2 - t_1 \leq n$, we reach a contradiction by computing

$$\max_{x \in X} \Lambda_n^+(x, F) \geq \Lambda_n^+(y, F) \geq i_2 - i_1 \geq$$

$$d - 1 - r - 2r \geq d - 4r \geq \Lambda^+(z, F') - nc.$$

$\square$

We are ready to prove the result for CA on full shifts.

Theorem 4 *For reversible CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ 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 We will reduce the decision problem of Theorem 3 to the present problem. Let therefore $F : X \to X$ be a reversible CA on a $(Q, \Sigma, Y, A_2, \rho)$ particle shift such that $\lambda^+(F) \in [0, \frac{5}{3}] \cup \{2\}$ and F is some composition of particle rules, background rules and coupling rules. We will show that the CA F' of the previous lemma can be effectively constructed. We then get the reduction, because F' is a CA on a full shift and $\lambda^+(F') = \lambda^+(F)$. To construct F' it is sufficient to show how to construct belted versions of background rules and coupling rules, since we saw earlier how to construct belted versions of particle rules. Throughout let Γ, Δ, A and the natural projections be as in Definition 11.

Let $G : X \to X$ be a background rule and let $G_1 : A_2^{\mathbb{Z}} \to A_2^{\mathbb{Z}}$ be such that $G(y, z) = (y, G_1(z))$ for $(y, z) \in Y \times A_2^{\mathbb{Z}}$. Define $G' : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ by $G'(x_1, x_2) = (x_1, G(x_2))$ for $(x_1, x_2) \in (\Gamma \times A_2)^{\mathbb{Z}}$. Clearly G' is a belted version of G.

Let then H be a coupling rule with parameters (w_1, w_2, W, j). For any $x \in A^{\mathbb{Z}}$ let $H'(x)$ be the configuration gotten from x by replacing an occurrence of w_1 by w_2 (and vice versa) at position i in $\pi_{1,1}(x)$ or $\pi_{1,2}(x)$ if and only if $\pi_2(x) \in \mathrm{Cyl}(w, i + j)$ for some $w \in W$ and $\pi_\Delta(x)[i, |w_1| - 1] \in {}^*0{}^-{}^*$ (and then automatically the symbol 0 occurs at the same coordinate as the symbol from Q in the occurrence of w_1 or w_2). Clearly H' is a belted version of H. $\square$

The following corollary is immediate.

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

5 Lyapunov exponents of multiplication automata

In this section we present a class of multiplication automata which perform multiplication by nonnegative numbers in some integer base. After the definitions and preliminary lemmas we compute their average Lyapunov exponents.

For this section denote $\Sigma_n = \{0, 1, \ldots, n-1\}$ for $n \in \mathbb{N}$, $n > 1$. To perform multiplication using a CA we need be able to represent a nonnegative real number as a configuration in $\Sigma_n^{\mathbb{Z}}$. If $\xi \geq 0$ is a real number and $\xi = \sum_{i=-\infty}^{\infty} \xi_i n^i$ is the unique base-n expansion of ξ such that $\xi_i \neq n-1$ for infinitely many $i < 0$, we define $\operatorname{config}_n(\xi) \in \Sigma_n^{\mathbb{Z}}$ by

$$\operatorname{config}_n(\xi)[i] = \xi_{-i}$$

for all $i \in \mathbb{Z}$. In reverse, whenever $x \in \Sigma_n^{\mathbb{Z}}$ is such that $x[i] = 0$ for all sufficiently small i, we define

$$\operatorname{real}_n(x) = \sum_{i=-\infty}^{\infty} x[-i]n^i.$$

For words $w = w[1]w[2]\cdots w[k] \in \Sigma_n^k$ we define analogously

$$\operatorname{real}_n(w) = \sum_{i=1}^{k} w[i]n^{-i}.$$

Clearly $\operatorname{real}_n(\operatorname{config}_n(\xi)) = \xi$ and $\operatorname{config}_n(\operatorname{real}_n(x)) = x$ for every $\xi \geq 0$ and every $x \in \Sigma_n^{\mathbb{Z}}$ such that $x[i] = 0$ for all sufficiently small i and $x[i] \neq n-1$ for infinitely many $i > 0$.

The fractional part of a number $\xi \in \mathbb{R}$ is

$$\operatorname{frac}(\xi) = \xi - \lfloor \xi \rfloor \in [0, 1).$$

For integers $p, q \geq 2$ let $g_{p,pq} : \Sigma_{pq} \times \Sigma_{pq} \to \Sigma_{pq}$ be defined as follows. Digits $a, b \in \Sigma_{pq}$ are represented as $a = a_1 q + a_0$ and $b = b_1 q + b_0$, where $a_0, b_0 \in \Sigma_q$ and $a_1, b_1 \in \Sigma_p$: such representations always exist and they are unique. Then

$$g_{p,pq}(a,b) = g_{p,pq}(a_1 q + a_0, b_1 q + b_0) = a_0 p + b_1.$$

An example in the particular case $(p, pq) = (3, 6)$ is given in Fig. 6.

We define the CA $\Pi_{p,pq} : \Sigma_{pq}^{\mathbb{Z}} \to \Sigma_{pq}^{\mathbb{Z}}$ by $\Pi_{p,pq}(x)[i] = g_{p,pq}(x[i], x[i+1])$, so $\Pi_{p,pq}$ is a radius-$\frac{1}{2}$ CA.

The CA $\Pi_{p,pq}$ performs multiplication by p in base pq in the sense of the following lemma.

Lemma 3 $\operatorname{real}_{pq}(\Pi_{p,pq}(\operatorname{config}_{pq}(\xi))) = p\xi$ for all $\xi \geq 0$.

We omit the proof of the lemma, which can be found for example in Kari (2012). The idea of the proof is to notice that the local rule $g_{p,pq}$ mimics the usual school multiplication algorithm. Because p divides pq, the carry digits cannot propagate arbitrarily far to the left.

It is well known that $\Pi_{p,pq}$ is reversible. Indeed, by the previous lemma the map $\Pi_{q,pq} \circ \Pi_{p,pq}$ agrees with σ on the dense set of configurations $\operatorname{config}_{pq}(\mathbb{R}_{\geq 0})$. Thus by continuity $\Pi_{q,pq} \circ \Pi_{p,pq} = \sigma$ and $\sigma^{-1} \circ \Pi_{q,pq}$ is the inverse of $\Pi_{p,pq}$.

For the statement of the following lemma, which can essentially be found from Kari and Kopra (2017), we define a function $\operatorname{int} : \Sigma_{pq}^+ \to \mathbb{N}$ by

$$\operatorname{int}(w[1]w[2]\cdots w[k]) = \sum_{i=0}^{k-1} w[k-i](pq)^i,$$

i.e. $\operatorname{int}(w)$ is the integer having w as a base-pq representation. We also write $\operatorname{Md}_n(m)$ to denote the remainder of m divided by n.

Lemma 4 *Let $t > 0$ and $w \in \Sigma_{pq}^k$ for some $k \geq t+1$. Then*

$$\operatorname{int}(g_{p,pq}^t(w)) = \operatorname{Md}_{(pq)^{k-t}}(\lfloor \operatorname{int}(w)/q^k \rfloor).$$

Proof Let $x \in \Sigma_{pq}^{\mathbb{Z}}$ be such that $x[-(k-1), 0] = w$ and $x[i] = 0$ for $i < -(k-1)$ and $i > 0$. From this definition of x it follows that $\operatorname{int}(w) = \operatorname{real}_{pq}(x)$. Denote $y = \Pi_{p,pq}^t(x)$. We have

$$\sum_{i=-\infty}^{\infty} y[-i](pq)^i = \operatorname{real}_{pq}(y) = p^t \operatorname{real}_{pq}(x) = p^t \operatorname{int}(w).$$

Dividing both sides of this equality by $(pq)^t$ we find that

$$\sum_{i=-\infty}^{\infty} y[-i](pq)^{i-t} = \operatorname{int}(w)/q^t$$

and

$a \backslash b$	0	1	2	3	4	5
0	0	0	1	1	2	2
1	3	3	4	4	5	5
2	0	0	1	1	2	2
3	3	3	4	4	5	5
4	0	0	1	1	2	2
5	3	3	4	4	5	5

Fig. 6 The values of $g_{3,6}(a, b)$

$$\text{int}\,(g_{p,pq}^t(w)) = \text{int}\,(y[-(k-1),-t])$$
$$= \sum_{i=t}^{k-1} y[-i](pq)^{i-t} = \text{Md}_{(pq)^{k-t}}(\lfloor \text{int}\,(w)/q^t \rfloor).$$

$\square$

We consider the Lyapunov exponents of the multiplication automaton $\Pi_{p,pq}$. Since $\Pi_{p,pq}$ is a radius-$\frac{1}{2}$ CA, it is easy to see that for any $x \in \Sigma_{pq}^{\mathbb{Z}}$ we must have $\lambda^+(x) = 0$ and $\lambda^-(x) \leq 1$ and therefore $\lambda^+(\Pi_{p,pq}) = 0$, $\lambda^-(\Pi_{p,pq}) \leq 1$.

Now consider a positive integer $m > 0$. Multiplying m by p^n yields a number whose base-pq representation has length approximately equal to $\log_{pq}(mp^n) = n(\log_{pq} p) + \log_{pq} m$. By translating this observation to the configuration space $\Sigma_{pq}^{\mathbb{Z}}$ it follows that $\lambda^-(0^{\mathbb{Z}}, \Pi_{p,pq}) = \log_{pq} p$. One might be tempted to conclude from this that $\lambda^-(\Pi_{p,pq}) = \log_{pq} p$. In Theorem 5 it turns out that this conclusion is not true. The intuition that the left Lyapunov exponent of $\Pi_{p,pq}$ "should be" equal to $\log_{pq} p$ is explained by the computation of the average Lyapunov exponent with respect to the uniform measure in Theorem 6. Recall that $\Pi_{p,pq}$ is a reversible CA and in particular it preserves the uniform measure.

Theorem 5 *For coprime $p, q > 1$ we have $\lambda^-(\Pi_{p,pq}) = 1$.*

Proof For every $n \in \mathbb{N}_+$ define $x_n = \text{config}_{pq}(q^n - 1)$ and $y_n = \text{config}_{pq}(q^n)$. Note that q^n isn't divisible by pq for any $n \in \mathbb{N}_+$, which means that x_n and y_n differ only at the origin. By Lemma 3, $\text{real}\,(\Pi_{p,pq}^n(x_n)) = p^n(q^n - 1) < (pq)^n$ and $\text{real}\,(\Pi_{p,pq}^n(y_n)) = p^n q^n = (pq)^n$, which means that $\Pi_{p,pq}^n(x_n)[-n] = 0$ and $\Pi_{p,pq}^n(y_n)[-n] = 1$. It follows that $\Lambda_n^-(\sigma^{-1}(x_n), \Pi_{p,pq}) \geq n$ and

$$\lambda^-(\Pi_{p,pq}) = \lim_{n \to \infty} \max_{x \in \Sigma_{pq}^{\mathbb{Z}}} \frac{\Lambda_n^-(x, \Pi_{p,pq})}{n}$$
$$\geq \lim_{n \to \infty} \frac{\Lambda_n^-(\sigma^{-1}(x_n), \Pi_{p,pq})}{n} \geq 1.$$

Since we already know that $\lambda^-(\Pi_{p,pq}) \leq 1$, we are done. $\square$

Theorem 6 *For coprime $p, q > 1$ we have $I_\mu^-(\Pi_{p,pq}) = \log_{pq} p$, where μ is the uniform measure on $\Sigma_{pq}^{\mathbb{Z}}$.*

Proof First note that for any $n \in \mathbb{N}_+$ and any $w \in \Sigma^{n+1}$ the equality $\Lambda_n^-(x) = \Lambda_n^-(y)$ holds for each pair $x, y \in \text{Cyl}\,(w, -n)$, so we may define the quantity $\Lambda_n^-(w) = \Lambda_n^-(x)$ for $x \in \text{Cyl}\,(w, -n)$. For any $i \in \mathbb{N}$ denote $(\Lambda_n^-)^{-1}(i) = \{x \in \Sigma_{pq}^{\mathbb{Z}} \mid \Lambda_n^-(x) = i\}$. Then, note that always $\Lambda_n^-(x) \leq n$ and define for $0 \leq i \leq n$

$$P_n(i) = \{w \in \Sigma_{pq}^{n+1} \mid \Lambda_n^-(w) = i\}$$

which form a partition of Σ_{pq}^{n+1}. From these definitions it follows that

$$I_{n,\mu}^- = \int_{x \in \Sigma_{pq}^{\mathbb{Z}}} \Lambda_n^-(x)$$
$$d\mu = \sum_{i=0}^{\infty} i\mu((\Lambda_n^-)^{-1}(i))$$
$$= (pq)^{-(n+1)} \sum_{i=0}^{n} i|P_n(i)|.$$

To compute $|P_n(i)|$ we define an auxiliary quantity

$$p_n(i) = \{w \in \Sigma_{pq}^{n+1} \mid i \leq \Lambda_n^-(w) \leq n\} :$$

then clearly $P_n(n) = p_n(n)$ and $P_n(i) = p_n(i) \setminus p_n(i+1)$ for $0 \leq i < n$. Note that $w \in p_n(i)$ $(0 \leq i \leq n)$ is equivalent to the existence of words $w' \in \Sigma_{pq}^{n+1-i}$, $u \in \Sigma_{pq}^i$, $v_1, v_2 \in \Sigma_{pq}^{n+1-i}$ such that $w = w'u$ and $g_{p,pq}^t(uv_1)[1] \neq g_{p,pq}^t(uv_2)[1]$ for some $i \leq t \leq n$. By denoting

$$d_n(i) = \{u \in \Sigma_{pq}^i \mid \exists v_1, v_2 \in A^{n+1-i},$$
$$t \in [i, n] : g_{p,pq}^t(uv_1)[1] \neq g_{p,pq}^t(uv_2)[1]\},$$

it follows that $|p_n(i)| = (pq)^{n+1-i}|d_n(i)|$. By Lemma 4, for a word $u \in \Sigma_{pq}^i$ the condition $u \in d_n(i)$ is equivalent to the existence of a number divisible by q^t on the open interval

$$J(u)_t = (\text{int}\,(u)(pq)^{t+1-i}, (\text{int}\,(u) + 1)(pq)^{t+1-i})$$

for some $t \in [i, n]$. Furthermore, if an integer m is divisible by q^t and $m \in J(u)_t$, then $m(pq)^{n-t} \in J(u)_n$ is divisible by q^n. Thus it is sufficient to consider only the interval $J(u)_n$. We use this to compute $|d_n(i)|$. The computation is divided into two cases that can be defined using the quantity $\kappa = \lfloor n - n\log_{pq} q + 1 \rfloor$.

In the case $(pq)^{n+1-i} > q^n$ (equivalently: $i \leq \kappa$) each interval $J(u)_n$ contains a number divisible by q^n and therefore $|d_n(i)| = (pq)^i$. Using this we can also compute $|P_n(i)|$ when $i < \kappa$:

$$|P_n(i)| = |p_n(i)| - |p_n(i+1)|$$
$$= (pq)^{n+1-i}|d_n(i)| - (pq)^{n-i}|d_n(i+1)|$$
$$= (pq)^{n+1} - (pq)^{n+1} = 0.$$

In the case $(pq)^{n+1-i} < q^n$ (equivalently: $i > \kappa$) each interval $J(u)_n$ contains at most one number divisible by q^n. Then $|d_n(i)|$ equals the number of elements on the interval $[0, (pq)^{n+1})$ which are divisible by q^n but not divisible by $(pq)^{n+1-i}$. Divisibility by both q^n and $(pq)^{n+1-i}$ is equivalent to divisibility by $q^n p^{n+1-i}$ because p and q are coprime and because $i \neq 0$ by the assumption

$(pq)^{n+1-i} < q^n$. Therefore

$$|d_n(i)| = (pq)^{n+1}/q^n - (pq)^{n+1}/(q^n p^{n+1-i}) = (pq)p^n - qp^i$$

.

We may compute

$$
\begin{aligned}
(pq)^{n+1} I_{n,\mu}^- &= \sum_{i=0}^{\kappa-1} i|P_n(i)| + \sum_{i=\kappa}^{n} i|P_n(i)| \\
&= n|p_n(n)| + \sum_{i=\kappa}^{n-1} i(|p_n(i)| - |p_n(i+1)|) \\
&= \kappa|p_n(\kappa)| + \sum_{i=\kappa+1}^{n} |p_n(i)|,
\end{aligned}
$$

in which

$$
\begin{aligned}
\kappa|p_n(\kappa)| &= \kappa(pq)^{n+1-\kappa}|d_n(\kappa)| \\
&= \kappa(pq)^{n+1-\kappa}(pq)^{\kappa} = \kappa(pq)^{n+1}
\end{aligned}
$$

and

$$
\begin{aligned}
\sum_{i=\kappa+1}^{n} |p_n(i)| &= \sum_{i=\kappa+1}^{n} (pq)^{n+1-i}|d_n(i)| \\
&= \sum_{i=\kappa+1}^{n} (pq)^{n+1-i}((pq)p^n - qp^i) \\
&= (pq)p^n \underbrace{\sum_{i=\kappa+1}^{n} (pq)^{n+1-i}}_{} \\
&\leq \sum_{i=\kappa+1}^{\infty}(pq)^{n+1-i} - q(pq)^{n+1} \underbrace{\sum_{i=\kappa+1}^{n} q^{-i}}_{\geq 0} \\
&\leq (pq)p^n (pq)^{n-\kappa} \underbrace{\sum_{i=0}^{\infty}(pq)^{-i}}_{\leq 2} \\
&\leq 2(pq)p^n(pq)^{n-(n-n\log_{pq} q+1)+1} \\
&= 2(pq)p^n(pq)^{\log_{pq} q^n} = 2(pq)^{n+1}.
\end{aligned}
$$

Finally, the left average Lyapunov exponent is

$$
\begin{aligned}
I_{\mu}^- &= \lim_{n\to\infty} \frac{I_{n,\mu}^-}{n} \\
&= \lim_{n\to\infty} \frac{\kappa|p_n(\kappa)|}{(pq)^{n+1}n} + \lim_{n\to\infty} \frac{\sum_{i=\kappa+1}^{n}|p_n(i)|}{(pq)^{n+1}n} = \lim_{n\to\infty} \frac{\kappa}{n} \\
&= 1 - \log_{pq} q = \log_{pq} p.
\end{aligned}
$$

$\square$

Remark 3 Multiplication automata can also be defined more generally. Denote by $\Pi_{\alpha,n} : \Sigma_n^{\mathbb{Z}} \to \Sigma_n^{\mathbb{Z}}$ the CA that performs multiplication by $\alpha \in \mathbb{R}_{>0}$ in base $n \in \mathbb{N}$, $n > 1$ (if exists). A characterization of all admissible pairs α, n can be extracted from the paper (Blanchard et al. 1996),

which considers multiplication automata on one-sided configuration spaces $\Sigma_n^{\mathbb{N}}$. We believe that $I_{\mu}^-(\Pi_{\alpha,n}) = \log_n \alpha$ for all $\alpha \geq 1$ and all natural numbers $n > 1$ such that $\Pi_{\alpha,n}$ is defined (when μ is the uniform measure on $\Sigma_n^{\mathbb{Z}}$). Replacing the application of Lemma 4 by an application of Lemma 5.7 from Kari and Kopra (2017) probably yields the result for $\Pi_{p/q,pq}$ when $p > q > 1$ are coprime. A unified approach to cover the general case would be desirable.

6 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. Note that the result does not restrict the size of the alphabet A of the CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ whose Lyapunov exponents are to be determined. Standard encoding methods might be sufficient to solve the following problem.

Problem 1 Is there a fixed full shift $A^{\mathbb{Z}}$ such that the Lyapunov exponents of a given reversible CA $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ cannot be computed to arbitrary precision? Can we choose here $|A| = 2$?

In our constructions we controlled only the right exponent $\lambda^+(F)$ and let the left exponent $\lambda^-(F)$ vary freely. Controlling both Lyapunov exponents would be necessary to answer the following.

Problem 2 Is it decidable whether the equality $\lambda^+(F) = \lambda^-(F) = 0$ holds for a given reversible cellular automaton $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$?

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

By an application of Fekete's lemma the limit that defines $\lambda^+(F)$ is actually the infimum of a sequence whose elements are easily computable when $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a CA on a full shift. This yields the natural obstruction that $\lambda^+(F)$ has to be an upper semicomputable number. We are not aware of a cellular automaton on a full shift that has an irrational Lyapunov exponent (see Question 5.7 in (Cyr et al. 2019)), 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 $F : X \to X$ on general subshifts X, and furthermore for every real $t \geq 0$ there is a subshift X_t and a reversible CA $F_t : X_t \to X_t$ such that $\lambda^+(F_t) = \lambda^-(F_t) = t$ (Hochman 2011).

In the previous section we computed that the average Lyapunov exponent I_μ^- of the multiplication automaton $\Pi_{p,pq}$ is equal to $\log_{pq} p$ when $p, q > 1$ are coprime integers. This in particular shows that average Lyapunov exponents can be irrational numbers. We do not know whether such examples can be found in earlier literature.

References

Blanchard F, Host B, Maass A (1996) Représentation par automate de fonctions continues de tore. J de théorie des nombres de Bordeaux 8(1):205–214

Cyr V, Franks J, Kra B (2019) The spacetime of a shift endomorphism. Trans Am Math Soc 371(1):461–488

D'amico M, Manzini G, Margara L (2003) On computing the entropy of cellular automata. Theor Comput Sci 290(3):1629–1646

Guillon P, Salo V (2017) Distortion in one-head machines and cellular automata. In: International Workshop on Cellular Automata and Discrete Complex Systems, pp. 120–138. Springer

Guillon P, Zinoviadis C (2012) Densities and entropies in cellular automata. In: Conference on Computability in Europe, pp. 253–263. Springer

Hedlund GA (1969) Endomorphisms and automorphisms of the shift dynamical system. Math Syst Theory 3(4):320–375

Hochman M (2011) Non-expansive directions for $\mathbb{Z}^2$ actions. Ergodic Theory Dyn Syst 31(1):91–112

Hurd LP, Kari J, Culik K (1992) The topological entropy of cellular automata is uncomputable. Ergodic Theory Dyn Syst 12(2):255–265

Kari J (1992) The nilpotency problem of one-dimensional cellular automata. SIAM J Comput 21(3):571–586

Kari J (2012) Universal pattern generation by cellular automata. Theor Comput Sci 429:180–184

Kari J, Kopra J (2017) Cellular automata and powers of p/q. RAIRO-Theor Inform Appl 51(4):191–204

Kim KH, Roush FW (1990) On the automorphism groups of subshifts. Pure Math Appl 1(4):203–230

Kopra J (2019) Cellular automata with complicated dynamics. Ph.D. thesis, University of Turku

Kopra J (2019) The Lyapunov exponents of reversible cellular automata are uncomputable. In: International Conference on Unconventional Computation and Natural Computation, pp. 178–190. Springer

Lind D, Marcus B (1995) An introduction to symbolic dynamics and coding. Cambridge University Press, Cambridge

Lukkarila V (2010) On undecidable dynamical properties of reversible one-dimensional cellular automata. Ph.D. thesis, University of Turku

Pivato M (2009) Ergodic theory of cellular automata. In Meyers RA (ed) Encyclopedia of complexity and systems science. pp 2980–3015. https://doi.org/10.1007/978-0-387-30440-3_178

Shereshevsky MA (1992) Lyapunov exponents for one-dimensional cellular automata. J Nonlinear Sci 2(1):1–8

Tisseur P (2000) Cellular automata and Lyapunov exponents. Nonlinearity 13(5):1547