Glider Automorphisms on Some Shifts of Finite Type and a Finitary Ryan's Theorem *

Johan Kopra (ORCiD: 0000-0002-6401-6795)

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

Abstract. For any mixing SFT X containing a fixed point we construct a reversible shift-commuting continuous map (automorphism) which breaks any given finite point of the subshift into a finite collection of gliders traveling into opposing directions. As an application we show that the automorphism group $\mathrm{Aut}(X)$ contains a two-element subset S whose centralizer consists only of shift maps.

Keywords: Mixing SFTs, Automorphisms, Cellular automata

1 Introduction

Let $X \subseteq A^{\mathbb{Z}}$ be a one-dimensional subshift over a symbol set A. If X contains some constant sequence $0^{\mathbb{Z}}$ ($0 \in A$), we may say that an element $x \in X$ is finite if it differs from $0^{\mathbb{Z}}$ only at finitely many coordinates. In this paper we consider the problem of constructing reversible shift-commuting continuous maps (automorphisms) on X which decompose all finite configurations into collections of gliders traveling into opposing directions. As a concrete example, consider the binary full shift $X = \{0,1\}^{\mathbb{Z}}$ and the map $g = g_3 \circ g_2 \circ g_1 : X \to X$ defined as follows. In any $x \in X$, g_1 replaces every occurrence of 0010 by 0110 and vice versa, g_2 replaces every occurrence of 0100 by 0110 and vice versa, and g_3 replace every occurrence of 00101 by 00111 and vice versa. In Figure 1 we have plotted the sequences $x, g(x), g^2(x), \ldots$ on consecutive rows for some $x \in X$. It can be seen that the sequence x eventually diffuses into two different "fleets", the one consisting of 1s going to the left and the one consisting of 11s going to the right. It can be proved that this diffusion happens eventually no matter which finite initial point $x \in X$ is chosen.[1] In Section 3 we construct on all mixing SFTs (that contain the point $0^{\mathbb{Z}}$) a glider automorphism with the same diffusion property as the binary automorphism g above.

The existence of a glider automorphism g on a subshift X is interesting, because g can be used to convert an arbitrary finite $x \in X$ into another sequence $g^t(x)$ (for some $t \in \mathbb{N}_+$) with a simpler structure, which nevertheless contains

* The work was partially supported by the Academy of Finland grant 296018 and by the Vilho, Yrjö and Kalle Väisälä Foundation

[1] This can be proved along similar lines as in the proof of Lemma 10 and Lemma 11.

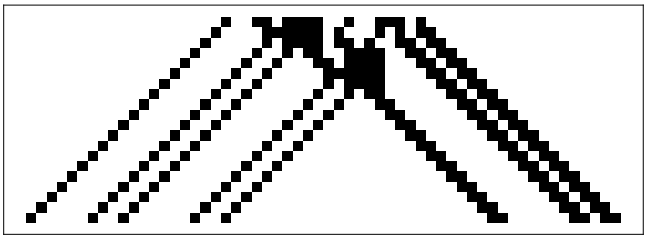

Fig. 1. The diffusion of $x \in X$ under the map $g : X \to X$. White and black squares correspond to digits 0 and 1 respectively.

all the information concerning the original point x because g is invertible. Such maps have been successfully applied to other problems e.g. in [3, 4].

We also consider a finitary version of Ryan's theorem. Let X be a mixing SFT and denote the set of its automorphisms by $\mathrm{Aut}(X)$, which we may consider as an abstract group. According to Ryan's theorem [2] the center of the group $\mathrm{Aut}(X)$ is generated by the shift map σ. There may also be subsets $S \subseteq \mathrm{Aut}(X)$ whose centralizers are generated by σ. Denote the minimal cardinality of such a finite set S by $k(X)$. In [3] it was proved that $k(X) \leq 10$ when X is the full shift over the four-letter alphabet. In the same paper it is noted that $k(X)$ is an isomorphism invariant of $\mathrm{Aut}(X)$ and therefore computing it could theoretically separate $\mathrm{Aut}(X)$ and $\mathrm{Aut}(Y)$ for some mixing SFTs X and Y. We use our glider automorphism construction to prove that $k(X) = 2$ for all mixing SFTs that contain the point $0^{\mathbb{Z}}$.

2 Preliminaries

A finite set A containing at least two elements (*letters*) is called an *alphabet* and the set $A^{\mathbb{Z}}$ of bi-infinite sequences (*configurations*) over A is called a *full shift*. Formally any $x \in A^{\mathbb{Z}}$ is a function $\mathbb{Z} \to A$ and the value of x at $i \in \mathbb{Z}$ is denoted by $x[i]$. It contains finite and one-directionally infinite subsequences denoted by $x[i, j] = x[i]x[i+1] \dots x[j]$, $x[i, \infty] = x[i]x[i+1] \dots$ and $x[-\infty, i] = \dots x[i-1]x[i]$. A *factor* of $x \in A^{\mathbb{Z}}$ is any finite sequence $x[i, j]$ where $i, j \in \mathbb{Z}$, and we interpret the sequence to be empty if $j < i$. Any finite sequence $w = w[1]w[2] \dots w[n]$ (also the empty sequence, which is denoted by λ) where $w[i] \in A$ is a *word* over A. The set of all words over A is denoted by A^*, and the set of non-empty words is $A^+ = A^* \setminus \{\lambda\}$. More generally, for any $L \subseteq A^*$, let

$$L^* = \{w_1 \dots w_n \mid n \geq 0, w_i \in L\} \subseteq A^*,$$

i.e. L^* is the set of all finite concatenations of elements of 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. $|w| = n \iff w \in A^n$. We say that the word $w \in A^n$ *occurs* in $x \in A^{\mathbb{Z}}$ at position i if $w = x[i] \dots x[i + n - 1]$. We define the shift map $\sigma_A : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ by $\sigma_A(x)[i] = x[i + 1]$ for $x \in A^{\mathbb{Z}}$, $i \in \mathbb{Z}$. The subscript A in σ_A is typically

omitted. The set $A^{\mathbb{Z}}$ is endowed with the product topology (with respect to the discrete topology on A), under which σ is a homeomorphism on $A^{\mathbb{Z}}$. Any closed set $X \subseteq A^{\mathbb{Z}}$ such that $\sigma(X) = X$ is called a *subshift*, and the collection of words appearing as factors of elements of X is the *language* of X, denoted by $L(X)$. The restriction of σ to X may be denoted by σ_X, but typically the subscript X is omitted.

If $X \subseteq A^{\mathbb{Z}}$ is a subshift and $z \in X$ is such that $\sigma(z) = z$ (i.e. z is a fixed point), then there exists $a \in A$ such that $z[i] = a$ for all $i \in \mathbb{Z}$. For such subshifts we always fix one such point and denote $a = 0$, $z = 0^{\mathbb{Z}}$. Then for $x \in X$ we define its support $\operatorname{supp}(x) = \{i \in \mathbb{Z} \mid x[i] \neq 0\}$ and say that x is finite if $\operatorname{supp}(x)$ is finite. Finite points $x, y \in X$ with disjoint supports can be glued together; if $\operatorname{supp}(x) \cap \operatorname{supp}(y) = \emptyset$ we define $x \otimes y \in A^{\mathbb{Z}}$ by $(x \otimes y)[i] = x[i]$ when $i \in \operatorname{supp}(x)$ and $(x \otimes y)[i] = y[i]$ otherwise.

Definition 1. A *graph* is a pair $\mathcal{G} = (V, E)$ where V is a finite set of *vertices* (or *nodes* or *states*) and E is a finite set of *edges*. Each edge $e \in E$ starts at an initial state denoted by $\iota(e) \in V$ and ends at a terminal state denoted by $\tau(e) \in V$. We say that $e \in A$ is an outgoing edge of $\iota(e)$ and an incoming edge of $\tau(e)$.

A sequence of edges $e[1] \dots e[n]$ in a graph $\mathcal{G} = (V, E)$ is a *path* (of length n) if $\tau(e[i]) = \iota(e[i+1])$ for $1 \leq i < n$ and it is a *cycle* if in addition $\tau(e[n]) = \iota(e[1])$. We say that the path starts at $e[1]$ and ends at $e[n]$. A graph $\mathcal{G}$ is *primitive* if there is $n \in \mathbb{N}_+$ such that for every $v_1, v_2 \in V$ there is a path of length n starting at v_1 and ending at v_2. For any graph $\mathcal{G} = (V, E)$ we call the set

$$\{x \in E^{\mathbb{Z}} \mid \tau(x[i]) = \iota(x[i+1])\}$$

(i.e. the set of bi-infinite paths on $\mathcal{G}$) the *edge subshift* of $\mathcal{G}$.

Definition 2. A subshift $X \subseteq A^{\mathbb{Z}}$ is a *mixing subshift of finite type* (mixing SFT) if it is the edge subshift of a primitive graph $\mathcal{G} = (V, E)$ containing at least two edges (in particular $E \subseteq A$).

Example 3. Let $A = \{0, a, b\}$. The graph in Figure 2 defines a mixing SFT X also known as the *golden mean shift*. A typical point of X looks like

$$\dots 000abab0ab00ab000 \dots$$

i.e. the letter b cannot occur immediately after 0 or b and every occurrence of a is followed by b.

Definition 4. An *automorphism* of a subshift $X \subseteq A^{\mathbb{Z}}$ is a continuous bijection $f : X \to X$ such that $\sigma \circ f = f \circ \sigma$. We say that f is a radius-r automorphism if $f(x)[0] = f(y)[0]$ for all $x, y \in X$ such that $x[-r, r] = y[-r, r]$ (such r always exists by continuity of f). The set of all automorphisms of X is a group denoted by $\operatorname{Aut}(X)$. (In the case $X = A^{\mathbb{Z}}$ automorphisms are also known as reversible cellular automata.)

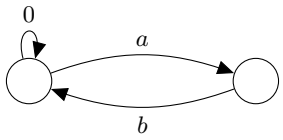

Fig. 2. The golden mean shift.

The *centralizer* of a set $S \subseteq \mathrm{Aut}(X)$ is

$$C(S) = \{f \in \mathrm{Aut}(X) \mid f \circ g = g \circ f \text{ for every } g \in S\}$$

and the subgroup generated by $f \in \mathrm{Aut}(X)$ is denoted by $\langle f \rangle$. The following definition is from [3]:

Definition 5. For a subshift X, let $k(X) \in \mathbb{N} \cup \{\infty, \perp\}$ be the minimal cardinality of a set $S \subseteq \mathrm{Aut}(X)$ such that $C(S) = \langle \sigma \rangle$ if such a set S exists, and $k(X) = \perp$ otherwise.

The main result of [2] is that $k(X) \neq \perp$ whenever X is a mixing SFT.

We say that subshifts $X \subseteq A^{\mathbb{Z}}$ and $Y \subseteq B^{\mathbb{Z}}$ are *conjugate* if there is a continuous bijection $\psi : X \to Y$ such that $\psi \circ \sigma_X = \sigma_Y \circ \psi$. For conjugate subshifts X and Y it necessarily holds that $k(X) = k(Y)$.

3 Glider Automorphisms

In this section we define as a technical tool a subclass of mixing SFTs, and for any subshift X from this class we construct an automorphism which breaks every finite point of X into a collection of gliders traveling in opposite directions.

Note that if X is a mixing SFT with a fixed point $0^{\mathbb{Z}}$, then necessarily in its graph $\mathcal{G} = (V, E)$ it holds that $\tau(0) = \iota(0)$. For such a graph we denote $\mathcal{G}' = (V, E')$ and $E' = E \setminus \{0\}$, i.e. we get $\mathcal{G}'$ from $\mathcal{G}$ by removing the 0-edge.

Definition 6. A mixing SFT X with a fixed point $0^{\mathbb{Z}}$ and defined by the graph $\mathcal{G} = (V, E)$ is called a 0-*mixing SFT* if the graph $\mathcal{G}'$ is also primitive and contains at least two edges.

The golden mean shift given by the graph in Figure 2 is an example of a mixing SFT which strictly speaking isn't 0-mixing. Nevertheless, in the following lemma we show that the definition of a 0-mixing SFT is only technical and that it is not an actual restriction.

Lemma 7. Any mixing SFT with a fixed point is conjugate to a 0-mixing SFT.

Proof. Let X be a mixing SFT with a fixed point $0^{\mathbb{Z}}$ defined by the graph $\mathcal{G} = (V, E)$ and let $s = \iota(0) = \tau(0)$. Let $0, a_1, \ldots, a_t$ be all the outgoing edges of s, let $0, b_1, \ldots, b_u$ be all the incoming edges of s and construct a new graph

$$\mathcal{H} = (V \cup \{s'\}, E \cup \{0', b'_1, \ldots, b'_u\})$$

with the starting and ending nodes of $e \in E$ the same as in $\mathcal{G}$ with the exception that $\iota(a_i) = s'$ for $1 \le i \le t$, and additionally $\iota(0') = s$, $\tau(0') = s'$, $\iota(b'_j) = \iota(b_j)$ and $\tau(b'_j) = s'$ for $1 \le j \le u$.[2] Let Y be the edge subshift of $\mathcal{H}$; it is conjugate with X via the continuous shift-commuting map $\psi : X \to Y$ defined for $x \in X$, $i \in \mathbb{Z}$ as

$$\psi(x)[i] = \begin{cases} 0' \text{ when } x[i] = 0 \text{ and } x[i+1] \in \{a_1, \ldots, a_t\}, \\ b'_j \text{ when } x[i] = b_j \text{ for some } 1 \le j \le u \text{ and } x[i+1] \in \{a_1, \ldots, a_t\}, \\ x[i] \text{ otherwise.} \end{cases}$$

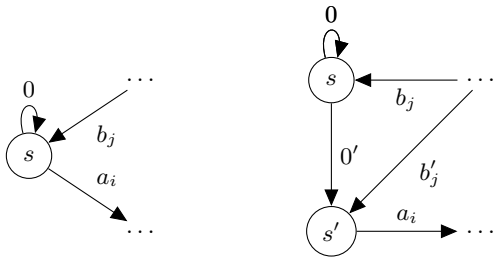

Fig. 3. Splitting the state s.

Construct the graphs $\mathcal{G}'$, $\mathcal{H}'$ and let $c[1] \ldots c[n] b_j$ be a cycle in $\mathcal{G}'$ visiting s only at the beginning and ending. Then $c[1] \ldots c[n] b_j 0'$ and $c[1] \ldots c[n] b'_j$ are distinct cycles in $\mathcal{H}'$ of coprime length, so $\mathcal{H}'$ has to be primitive and Y is a 0-mixing SFT. □

In the rest of the section we assume that X is a 0-mixing SFT defined by the graph $\mathcal{G} = (V, E)$. This means that the edge subshift of $\mathcal{G}'$ is also a mixing SFT. Denote $s = \iota(0) = \tau(0)$. Let v_1 be a cycle in $\mathcal{G}'$ visiting s only at the beginning and ending, denote $p = |v_1|$ and let $v_0 = 0^p$. The words

$$g_\ell = v_0 v_1, \qquad g_r = v_1 v_1$$

will be left- and rightbound gliders of the automorphism g defined later. The languages of left- and rightbound gliders are

$$L_\ell = (g_\ell 00^*)^*, \qquad L_r = (0^* 0 g_r)^*.$$

We denote by ${}^\infty 0$ and 0^∞ left- and right-infinite sequences of zeroes and define the glider fleet sets

$$\mathrm{GF}_\ell = {}^\infty 0 (g_\ell 00^*)^* 0^\infty \qquad \mathrm{GF}_r = {}^\infty 0 (0^* 0 g_r)^* 0^\infty \qquad \mathrm{GF} = \mathrm{GF}_\ell \cup \mathrm{GF}_r$$

[2] In other words we have performed an *elementary state splitting* of $\mathcal{G}$ at state s. State splitting is a well-known method to produce conjugate subshifts, see e.g. Chapter 2.4 of [1].

(note that these consist of finite configurations).

Denote $u' = v_1v_1v_1$ and let $n \in \mathbb{N}_+$ be a mixing constant of $\mathcal{G}'$ (i.e. a number such that for every $n' \geq n$ and $s_1, s_2 \in V$ there is a path of length n' in $\mathcal{G}'$ from s_1 to s_2) chosen such that $n \geq |u'| = 3p$. For every $a \in E$ we may choose some path $w_a \in E'^{2n}$ in $\mathcal{G}'$ such that w_a begins with u' and $0w_a a \in L(X)$. For every $a \in E$ let $W'_a = \{w_{a,1}, \ldots, w_{a,k_a}\} \subseteq E'^{2n}$ be the paths of length $2n$ in $\mathcal{G}'$ such that $w_{a,i}$ does not have a prefix u' and $0w_{a,i}a \in L(X)$ for $1 \leq i \leq k_a$, and let $W_a = W'_a \cup \{w_a\}$. Let $U' = \{u'_1, \ldots, u'_k\} \subseteq (E')^+$ be the cycles from s to s (which may visit s several times) of length at most $2n - 1 \geq 5p$ which are different from v_1 and v_1v_1 and do not have u' as a prefix. Finally, these words are padded to constant length; $u = 0^{2n-1-|u'|}u'$ and $u_i = 0^{2n-1-|u'_i|}u'_i$. The words in W_a and U' are chosen so as to allow the following structural definition.

Definition 8. Assume that $x \notin \mathrm{GF}_\ell$ is a non-zero finite element of X. Then there is a maximal $i \in \mathbb{Z}$ such that

$$x[-\infty, i-1] \in {}^\infty 0 L_\ell,$$

and there is a unique word $w \in \{v_10\} \cup \{v_1v_10\} \cup \{u'\} \cup (U'0) \cup (\bigcup_{a \in E} W'_a a)$ such that w is a prefix of $x[i, \infty]$. If $w = v_1v_10$ or $w \in U'0$, let $j = i + |w| - 1$ and otherwise let $j = i + |v_1|$. We say that x is of *left bound type* (w, j) and that it has left bound j (note that $j > i$).

Similarly, if $x \notin \mathrm{GF}_r$ is a non-zero finite element of X, then there is a minimal $j \in \mathbb{Z}$ such that

$$x[j+1, \infty] \in L_r 0^\infty$$

and we say that x has right bound j.

The point of this definition is that if x is of left bound type (w, j), then the glider automorphism g defined later will create a new leftbound glider at position j and break it off from the rest of the configuration.

We define four maps $g_1, g_2, g_3, g_4 : X \to X$ as follows. In any $x \in X$,

- g_1 replaces every occurrence of $0(v_0v_1)0$ by $0(v_1v_1)0$ and vice versa
- g_2 replaces every occurrence of $0(v_1v_0)0$ by $0(v_1v_1)0$ and vice versa
- g_3 replaces every occurrence of $0v_0(v_1v_0v_1)$ by $0v_0(v_1v_1v_1)$ and vice versa
- g_4 replaces every occurrence of $0w_a a$, $0w_{a,i}a$ and $0w_{a,k_a}a$ by $0w_{a,1}a$, $0w_{a,i+1}a$ and $0w_a a$ respectively (for $a \in E$ and $1 \leq i < k_a$) and every occurrence of $0u0$, $0u_i0$ and $0u_k0$ by $0u_10$, $0u_{i+1}0$ and $0u0$ respectively (for $1 \leq i < k$).

It is easy to see that these maps are well defined automorphisms of X. The *glider automorphism* $g : X \to X$ is defined as the composition $g_4 \circ g_3 \circ g_2 \circ g_1$. The name is partially justified by the following lemma.

Lemma 9. If $x \in \mathrm{GF}_\ell$ (resp. $x \in \mathrm{GF}_r$), then $g(x) = \sigma^p(x)$ (resp. $g(x) = \sigma^{-p}(x)$).

Proof. Assume that $x \in \mathrm{GF}_\ell$ (the proof for $x \in \mathrm{GF}_r$ is similar) and assume that $i \in \mathbb{Z}$ is some position in x where g_ℓ occurs. Then

$$\begin{aligned}
&x[i-1, i+2p] = 0g_\ell 0 = 0(v_0v_1)0\\
&g_1(x)[i-1, i+2p] = 0(v_1v_1)0\\
&g_2(g_1(x))[i-p-1, i+p] = 0v_0(v_10) = 0g_\ell 0\\
&g(x) = g_4(g_3(g_2(g_1(x)))) = g_2(g_1(x))),
\end{aligned}$$

so every glider has shifted by distance p to the left and $g(x) = \sigma^p(x)$. □

In fact, the previous lemma would hold even if g were replaced by $g_2 \circ g_1$. The role of the part $g_4 \circ g_3$ is, for a given finite point $x \in X$, to "erode" non-zero non-glider parts of x from the left and to turn the eroded parts into new gliders. This is the content of the following lemmas.

Lemma 10. Assume that $x \in X$ has left bound j. Then there exists $t \in \mathbb{N}_+$ such that the left bound of $g^t(x)$ is strictly greater than j.

Proof. Let $x \in X$ be of left bound type (w, j) with $w \in \{v_10\} \cup \{v_1v_10\} \cup \{u'\} \cup (U'0) \cup (\bigcup_{a\in E} W'_a a)$. The gliders to the left of the occurrence of w near j move to the left at constant speed p under action of g without being affected by the remaining part of the configuration.

Case 1. Assume that $w = v_1v_10$. Then $g_1(x)[j-(p+1), j] = 0v_10$. If $g_1(x)[j-(p+1), j+p] = 0v_1v_00$, then $g(x)[j-(p+1), j+p] = g_2(g_1(x))[j-(p+1), j+p] = 0v_1v_10$, $g(x)$ is of left bound type $(v_1v_10, j+p)$ and we are done. Otherwise $g_2(g_1(x))[j-(p+1), j] = 0v_10$. Denote $y = g_3(g_2(g_1(x)))$. If $y[j-(p+1), j] = 0v_10$, then $g(x) = g_4(y)$ is of left bound type (v_10, j) and we proceed as in Case 3. Otherwise $y[j-(p+1), j+(2p-1)] = 0u'$. If $y[(j+2p)-2n, j+2p] = 0u0$, then $g(x)[(j+2p)-2n, j+2p] = 0u_10$, $g(x)$ is of left bound type $(u'_10, j+2p)$ and we are done. On the other hand, if $y[(j+2p)-2n, j+2p] \neq 0u0$, then $g(x)$ is of left bound type (w', j) for some $w' \in W'_a a \cup \{u'\}$ $(a \in E)$ and we proceed as in Case 4 or Case 5.

Case 2. Assume that $w = u'_i0$ for $1 \leq i \leq k$. There is a minimal $t \in \mathbb{N}$ such that $g_3(g_2(g_1(g^t(x))))[j-2n, j] = 0u_i0$. Because $g^{t+k-i+1}(x)[j-2n, j] = 0u0$, it follows that $y = g^{t+k-i+1}(x)$ is of left bound type $(u', j-2p)$. Then $g(y)[j-5p, j] = g_3(g_2(g_1(y)))[j-5p, j] = v_0(v_0v_1)v_0v_10$ is of left bound type (v_10, j) and we proceed as in Case 3.

Case 3. Assume that $w = v_10$. Then $x[j-(2p+1), j] \neq 0v_0v_10 = 0g_\ell 0$ because otherwise the left bound of x would already be greater than j, so $g_1(x)[j-(p+1), j] = 0v_10$. If moreover $g_1(x)[j-(p+1), j+p] = 0v_1v_00$, then $g(x)[j-(p+1), j+p] = g_2(g_1(x))[j-(p+1), j+p] = 0(v_1v_1)0$ so $g(x)$ is of left bound type $(v_1v_10, j+p)$ and we are done. Let us therefore assume that $g_1(x)[j-(p+1), j+p] \neq 0v_1v_00$, in which case $g_2(g_1(x))[j-(2p+1), j] = 0v_0v_10$.

If $g_2(g_1(x))[j-(2p+1), j+2p-1] \neq 0v_0v_1v_0v_1$, then $g(x)[j-(2p+1), j] = g_3(g_2(g_1(x)))[j-(2p+1), j] = 0v_0v_10$. The left bound of $g(x)$ is now

greater than j and we are done. Otherwise $g_3(g_2(g_1(x)))[j-(2p+1), j+2p-1] = 0v_0u'$. If $g_3(g_2(g_1(x)))[(j+2p)-2n, j+2p] = 0u0$, then $g(x)[(j+2p)-2n, j+2p] = 0u_10$ and the left bound of $g(x)$ equals $j+2p$. Finally, if $g_3(g_2(g_1(x)))[(j+2p)-2n, j+2p] \neq 0u0$, then $g(x)$ is of left bound type (w', j) for some $w' \in W'_a a \cup \{u'\}$ $(a \in E)$ and we proceed as in Case 4 or Case 5.

Case 4. Assume that $w = w_{a,i}a$ for $a \in E$ and $1 \leq i \leq k_a$. Then $g^{k_a-i+1}(x)[j-p, j+(2p-1)] = u'$ and we proceed as in Case 5.

Case 5. Assume that $w = u'$. Then $g_2(g_1(x))[j-(2p+1), j+(2p-1)] = 0v_0u'$, $g_3(g_2(g_1))[j-(2p+1), j+(2p-1)] = 0v_0v_1v_0v_1$ and the left bound of $g(x)$ is at least $j+2p$.

□

Lemma 11. Assume that $x \in X$ has right bound j. Then there exists $t \in \mathbb{N}_+$ such that the right bound of $g^t(x)$ is strictly less than j.

Proof. Let us assume to the contrary that the right bound of $g^t(x)$ is at least j for every $t \in \mathbb{N}_+$.

Assume first that the right bound of $g^t(x)$ is equal to j for every $t \in \mathbb{N}_+$. By the previous lemma there is $t \in \mathbb{N}_+$ such that the left bound of $g^t(x)$ is at least $j+3n$, which means that $g^t(x)$ contains only g_ℓ-gliders to the left of $j+n$ and only g_r-gliders to the right of j. This can happen only if $g^t(x)[j+1, n-1] = 0^{n-1}$. Then the right bound of $g^{t+1}(x)$ is at least $j-p$, a contradiction.

Assume then that the right bound of $g^t(x)$ is strictly greater that j for some $t \in \mathbb{N}_+$ and fix the minimal such t. This can happen only if $g_1(g^{t-1}(x))[j-p, j+p+1] = 0v_1v_00$, in which case $g^t(x)[j-p, j+p+1] = 0v_1v_10 = 0g_r0$. But then the right bound of $g^t(x)$ is less than $j-p$, a contradiction. □

Together these two lemmas yield the following theorem.

Theorem 12. If $x \in X$ is a finite configuration, then for every $N \in \mathbb{N}$ there exists $t \in \mathbb{N}$ such that $g^t(x)[-N, N] = 0^{2N+1}$, $g^t(x)[\infty, -(N+1)] \in {}^\infty 0 L_\ell$ and $g^t(x)[N+1, \infty] \in L_r 0^\infty$.

4 Finitary Ryan's Theorem

In this section we prove a finitary version of Ryan's theorem. The idea is that only very specific automorphisms commute with the glider map $g : X \to X$ defined in the previous section, so it will be relatively easy to choose another automorphism f on X such that only powers of the shift map commute with both g and f. We make a simple choice of such f.

First we define maps $f_1, f_2 : X \to X$ for a 0-mixing SFT X as follows. In any $x \in X$,

- f_1 replaces every occurrence of $0(v_1v_1)v_0v_0v_0(v_1)0$ by $0(v_1v_1)v_0v_0(v_1)v_00$ and vice versa

– f_2 replaces every occurrence of $0(v_1v_1)v_0v_0(v_1)0$ by $0v_0(v_1v_1)v_0(v_1)0$ and vice versa,

where v_0 and v_1 are as in the previous section. It is easy to see that these maps are well defined automorphisms of X. The automorphism $f : X \to X$ is then defined as the composition $f_2 \circ f_1$. The map f has two important properties. First, it replaces any occurrence of $0(v_1v_1)v_0v_0v_0(v_1)0$ by $0v_0(v_1v_1)v_0(v_1)v_00$. Second, if $x \in X$ is a configuration containing only gliders g_ℓ and g_r and every occurrence of g_ℓ is sufficiently far from every occurrence of g_r, then $f(x) = x$.

To prove our main result we need the following lemma.

Lemma 13 ([3], Lemma 7.5)**.** If X is a mixing SFT containing a fixed point $0^{\mathbb{Z}}$ and $h : X \to X$ is an automorphism which is not a power of σ, then there exists a finite configuration $x \neq 0^{\mathbb{Z}}$ such that $h(x) \notin \mathcal{O}(x) \doteqdot \{\sigma^i(x) \mid i \in \mathbb{Z}\}$.

Theorem 14. Let $X \subseteq A^{\mathbb{Z}}$ be a 0-mixing SFT and $g, f : X \to X$ as above. The only automorphisms of X which commute with both g and f are powers of σ.

Proof. Assume to the contrary that $h : X \to X$ is a radius-r automorphism whose inverse is also a radius-r automorphism and which commutes with g and f but is not a power of σ. Let us first show that $h(0^{\mathbb{Z}}) = 0^{\mathbb{Z}}$. Namely, if it were that $h(0^{\mathbb{Z}}) = a^{\mathbb{Z}}$, for some $a \in A \setminus \{0\}$, consider $x = \ldots 000 g_\ell 000 \ldots$ with the glider g_ℓ at the origin and note that $h(x)[i] \neq a$ for some $-r \leq i \leq (2p-1)+r$ (recall: $g_\ell = v_0v_1$, $|v_0| = |v_1| = p$) and $h(x)[-\infty, i-jp] = \ldots aaa$ for some $j \in \mathbb{N}_+$. Then $g^t(h(x))[-\infty, i-jp] = \ldots aaa$ for every $t \in \mathbb{Z}$ but $h(g^j(x))[i-jp] = h(\sigma^{jp}(x))[i-jp] = h(x)[i] \neq a$, contradicting the commutativity of h and g. Thus h maps finite configurations to finite configurations.

We have $h(\mathrm{GF}_\ell) \subseteq \mathrm{GF}_\ell$. To see this, assume to the contrary that there exists $x \in \mathrm{GF}_\ell$ such that $h(x) \notin \mathrm{GF}_\ell$. Recall that g is reversible and $g(\mathrm{GF}_\ell) = \mathrm{GF}_\ell$, so $g^t(h(x)) \notin \mathrm{GF}_\ell$ for all $t \in \mathbb{N}$. Combining this with Theorem 12 it follows that $g^t(h(x))$ contains an occurrence of $0v_1v_10$ to the right of coordinate r for all sufficiently large t and therefore $h^{-1}(g^t(h(x)))[i]$ is non-zero for some $i \geq 0$ which depends on t. This contradicts the fact that $h^{-1}(g^t(h(x)))[i] = g^t(x)[i] = 0$ for all $i \geq 0$ given that t is sufficiently big. Similarly $h(\mathrm{GF}_r) \subseteq \mathrm{GF}_r$.

For any finite $x \neq 0^{\mathbb{Z}}$ define its left and right offsets

$$\begin{aligned}\mathrm{off}_\ell(x) &= \min\{\mathrm{supp}(h(x))\} - \min\{\mathrm{supp}(x)\},\\ \mathrm{off}_r(x) &= \max\{\mathrm{supp}(h(x))\} - \max\{\mathrm{supp}(x)\}.\end{aligned}$$

For all nonzero $x_\ell \in \mathrm{GF}_\ell$ and $x_r \in \mathrm{GF}_r$ we have $\mathrm{off}_\ell(x_\ell) - \mathrm{off}_r(x_r) = 0$. If this did not hold, we could assume without loss of generality that $\mathrm{off}_\ell(x_\ell) - \mathrm{off}_r(x_r) > 0$ (by replacing h with h^{-1} if necessary) and that $\min\{\mathrm{supp}(x_\ell)\} = (r+2)p$, $\max\{\mathrm{supp}(x_r)\} = -(r+1)p - 1$ (by shifting x_ℓ and x_r suitably). Then consider $x = x_r \otimes x_\ell$ and note that from $\min\{\mathrm{supp}(x_\ell)\} = (r+2)p > r$, $\max\{\mathrm{supp}(x_r)\} = -(r+1)p - 1 < -r$ it follows that $h(x) = h(x_r) \otimes h(x_\ell)$. Then $g^r(x)[-3p-1, 3p] = 0(v_1v_1)v_0v_0v_0(v_1)0$ and $g^r(h(x))$ contains no occurrence of the words mentioned in the definition of f_1 and f_2 by the assumption $\mathrm{off}_\ell(x_\ell) - \mathrm{off}_r(x_r) > 0$, so

$f(g^r(x)) \neq g^r(x)$ and $f(g^r(h(x))) = g^r(h(x))$. Now

$$\begin{aligned} x \neq g^{-r}(f(g^r(x))) =& h^{-1}(g^{-r}(f(g^r(h(x))))) \\ =& h^{-1}(g^{-r}(g^r(h(x)))) = x, \end{aligned}$$

a contradiction. It also follows that there is a fixed $s \in \mathbb{Z}$ such that $\mathrm{off}_\ell(x_\ell) = \mathrm{off}_r(x_r) = s$ for all nonzero $x_\ell \in \mathrm{GF}_\ell$, $x_r \in \mathrm{GF}_r$.

If $x_\ell \in \mathrm{GF}_\ell$ and $x_r \in \mathrm{GF}_r$ are configurations containing exactly one occurrence of g_ℓ and g_r respectively, then $h(x_\ell) = \sigma^{-s}(x_\ell)$ and $h(x_r) = \sigma^{-s}(x_\ell)$. To see this, assume to the contrary (without loss of generality) that $\min\{\mathrm{supp}(x_\ell)\} = (r+2)p$ (i.e. the occurrence of g_ℓ in x is at $(r+1)p$), $\max\{\mathrm{supp}(x_r)\} = -(r+1)p-1$ and $h(x_\ell)[(r+1)p+s, (r+3)p-1+s] = h(x_\ell)[(r+1)p+s+k, (r+3)p-1+s+k] = g_\ell$ for some $k > 2p$ (i.e. $h(x_\ell)$ contains at least two occurrences of g_ℓ, the case in which $h(x_r)$ contains at least two occurrences of g_r being similar). Then consider $x = x_r \otimes x_\ell$ and note that

$$\begin{aligned} &g^r(x)[-3p-1, 3p] = 0(v_1v_1)v_0v_0v_0(v_1)0 \\ &f(g^r(x))[-3p-1, 3p] = 0v_0(v_1v_1)v_0(v_1)v_00 \\ &g^{-1}(f(g^r(x)))[-3p-1, 3p] = 0(v_1v_1)v_0v_0v_0(v_1)0 \\ &g^{-(r+1)}(f(g^r(x))) = x, \end{aligned}$$

therefore also $h(x) = g^{-(r+1)}(f(g^r(h(x)))) \div y$. On the other hand,

$$\begin{aligned} & f(g^r(h(x)))[p+s+k, 3p-1+s+k] \\ =& g^r(h(x))[p+s+k, 3p-1+s+k] = g_\ell \\ & g^{-(r+1)}(f(g^r(h(x))))[(r+2)p+s+k, (r+4)p-1+s+k] = g_\ell, \end{aligned}$$

so in particular $y[(r+2)p+s+k, (r+3)p-1+s+k] = v_0$. Because we assumed that

$$\begin{aligned} & h(x)[(r+2)p+s+k, (r+3)p-1+s+k] \\ =& h(x_\ell)[(r+2)p+s+k, (r+3)p-1+s+k] = v_1, \end{aligned}$$

it follows that $h(x) \neq y$, a contradiction.

By Lemma 13 there exists a finite configuration $x \neq 0^{\mathbb{Z}}$ such that $h(x) \notin \mathcal{O}(x)$ and $h(x)$ is finite. Use Theorem 12 to get $t \in \mathbb{N}$ such that $g^t(x)[-r, r] = 0^{2r+1}$ and $g^t(x) = y_\ell \otimes y_r$ where $y_\ell \in \mathrm{GF}_\ell$ has $\max\{\mathrm{supp}(y_\ell)\} < -r$ and $y_r \in \mathrm{GF}_r$ has $\min\{\mathrm{supp}(y_r)\} > r$ (it is possible that either y_ℓ or y_r is equal to $0^{\mathbb{Z}}$). Then also $h(g^t(x)) = h(y_\ell) \otimes h(y_r) \notin \mathcal{O}(g^t(x))$, and combining this with $\mathrm{off}_\ell(y_\ell) = \mathrm{off}_r(y_r)$ it follows that $h(y_\ell) \notin \mathcal{O}(y_\ell)$ or $h(y_r) \notin \mathcal{O}(y_r)$. Without loss of generality assume that $h(y_\ell) \notin \mathcal{O}(y_\ell)$ (the case $h(y_r) \notin \mathcal{O}(y_r)$ is similar), that y_ℓ contains a minimal number of occurrences of g_ℓ (at least two by the previous paragraph) and that the distance from the leftmost g_ℓ to the second-to-leftmost g_ℓ in y_ℓ is maximal (at most $2r+2p$ since otherwise by dropping the leftmost g_ℓ we would get a new

configuration y'_ℓ such that $h(y'_\ell) \notin \mathcal{O}(y'_\ell)$, contradicting the minimal number of occurrences of g_ℓ in y_ℓ). Let $x_r \in \mathrm{GF}_r$ contain exactly one occurrence of g_r and assume that $\min\{\mathrm{supp}(y_\ell)\} = (r+2)p$, $\max\{\mathrm{supp}(x_r)\} = -(r+1)p - 1$. Decompose $y_\ell = x_\ell \otimes x'_\ell$ so that x_ℓ contains only the leftmost g_ℓ from y_ℓ and x'_ℓ contains all the other occurrences of g_ℓ from y_ℓ. In a similar way as in the previous paragraph we see that

$$g^{-(r+1)}(f(g^r))(x_r \otimes y_\ell) = x_r \otimes (x_\ell \otimes (\sigma^{-p}(x'_\ell))).$$

Denote $h' = (g^{-(r+1)} \circ f \circ g^r)^{-1}$. By the maximality of distance from the leftmost g_ℓ to the second-to-leftmost g_ℓ in y_ℓ we know that

$$h(x_\ell \otimes (\sigma^{-p}(x'_\ell))) \in \mathcal{O}(x_\ell \otimes (\sigma^{-p}(x'_\ell))),$$

and this is possible only if

$$\begin{aligned}
&h(x_\ell \otimes (\sigma^{-p}(x'_\ell))) = \sigma^{-s}(x_\ell \otimes (\sigma^{-p}(x'_\ell))),\\
&h(x_r \otimes x_\ell \otimes (\sigma^{-p}(x'_\ell))) = \sigma^{-s}(x_r \otimes x_\ell \otimes (\sigma^{-p}(x'_\ell))),\\
&h(h'(x_r \otimes x_\ell \otimes (\sigma^{-p}(x'_\ell)))) = \sigma^{-s}(h'(x_r \otimes x_\ell \otimes (\sigma^{-p}(x'_\ell)))),\\
&h(x_r \otimes y_\ell) = \sigma^{-s}(x_r \otimes y_\ell),
\end{aligned}$$

so in particular $h(y_\ell) \in \mathcal{O}(y_\ell)$, a contradiction. □

Corollary 15 (Finitary Ryan's theorem)**.** $k(X) = 2$ for every mixing SFT X with a fixed point.

Proof. The fact that $k(X) \geq 2$ follows from the previous theorem and Lemma 7. To see that $k(X) = 2$, assume to the contrary that $k(X) < 2$. From $k(X) = 0$ it would follow that $\mathrm{Aut}(X)$ contains only powers of the shift, which is evidently false. Assume then that $k(X) = 1$ and that h is a single automorphism which commutes with $h' \in \mathrm{Aut}(X)$ only if h' is a power of the shift. Because h commutes with itself, it follows that $h = \sigma^i$ for some $i \in \mathbb{Z}$. But all $h' \in \mathrm{Aut}(X)$ commute with σ^i and so $\mathrm{Aut}(X)$ contains again only powers of the shift, a contradiction. □

5 Conclusions

We have constructed glider automorphisms g for mixing SFTs X which have a fixed point, and we have applied these glider maps to prove for such X that $k(X) = 2$. It seems that our construction of g should generalize to arbitrary mixing SFTs X which do not necessarily have any fixed points. In this case instead of a fixed point $0^{\mathbb{Z}}$ we need to fix some periodic configuration $p \in X$ (i.e. $\sigma^k(p) = p$ for some $k \in \mathbb{N}_+$) and we consider points $x \in X$ which are finite (in some sense) *with respect to* p instead of $0^{\mathbb{Z}}$. In light of this it is probable that $k(X) = 2$ for all mixing SFTs X.

Acknowledgments. The author thanks Ville Salo for helpful discussions concerning these topics.

References

1. D. Lind, B. Marcus: *An introduction to symbolic dynamics and coding.* Cambridge University Press, Cambridge (1995)
2. J. Patrick Ryan: *The shift and commutativity.* Mathematical systems theory 6 (1-2), 82–85 (1972)
3. V. Salo: *Transitive action on finite points of a full shift and a finitary Ryan's theorem.* arXiv:1610.05487v2 (2017)
4. V. Salo, I. Törmä: *A One-Dimensional Physically Universal Cellular Automaton.* In: Kari J., Manea F., Petre I. (eds) Unveiling Dynamics and Complexity. CiE 2017. Lecture Notes in Computer Science, vol 10307. Springer, Cham (2017)