Natural Computing manuscript No.
(will be inserted by the editor)

Glider Automorphisms and a Finitary Ryan's Theorem for Transitive Subshifts of Finite Type

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

Received: date / Accepted: date

Abstract For any mixing SFT X 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 prove a finitary Ryan's theorem: the automorphism group $\mathrm{Aut}(X)$ contains a two-element subset S whose centralizer consists only of shift maps. We also give an example which shows that a stronger finitary variant of Ryan's theorem does not hold even for the binary full shift.

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 w is a finite word over A, we may say that an element $x \in X$ is w-finite if it begins and ends with infinite repetitions of w. In this paper we consider the problem of constructing reversible shift-commuting continuous maps (automorphisms) on X which decompose all w-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 replaces 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 0-finite $x \in X$. It can be seen that the sequence x eventually diffuses into two different "fleets",

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

J. Kopra
Department of Mathematics and Statistics, FI-20014, University of Turku, Finland
E-mail: jtjkop@utu.fi

the one consisting of 1s going to the left and the one consisting of 11s going to the right. It can be proved, along similar lines as in the proofs of Lemma 6 and Lemma 7, that this diffusion happens eventually no matter which finite initial point $x \in X$ is chosen. In Section 4 we construct, on all nontrivial mixing SFTs, a function that we call a diffusive glider automorphism and that has the same diffusion property as the binary automorphism g above.

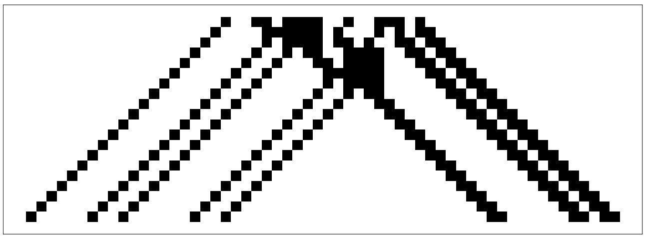

Fig. 1 The diffusion of $x \in X$ under the map $g : X \to X$. White and black squares correspond to digits 0 and 1 respectively.

The existence of such a diffusive 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 all the information concerning the original point x because g is invertible. Such maps have been successfully applied to other problems. We give some examples. The paper [6] contains a construction of a finitely generated group G of automorphisms of $A^{\mathbb{Z}}$ (when $|A| = 4$) whose elements can implement any permutation on any finite collection of 0-finite non-constant configurations that belong to different shift orbits. An essential part of the construction is that one of the generators of G is a diffusive glider automorphism on $A^{\mathbb{Z}}$. Another example is the construction of a physically universal cellular automaton g on $A^{\mathbb{Z}}$ (when $|A| = 16$) in [7]. Also here it is essential that g is a diffusive glider automorphism (but g also implements certain additional collision rules for gliders).

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 [2,5] 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 $C(S)$ are generated by σ. Denote the minimal cardinality of such a finite set S by $k(X)$. In [6] 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. Finding good isomorphism invariants of $\mathrm{Aut}(X)$ is of great interest, and it is an open problem whether for example $\mathrm{Aut}(\{0,1\}^{\mathbb{Z}}) \cong \mathrm{Aut}(\{0,1,2\}^{\mathbb{Z}})$ (Problem 22.1 in [1]). We show that $k(X) = 2$ for all nontrivial mixing SFTs, the proof of which uses our diffusive glider automorphism construction and Lemma 1 (Main lemma). It is then a simple corollary that $k(X) = 2$ for every transitive SFT X that does not consist of the orbit of a single periodic point. The diffusive glider automorphism construction and the proof of $k(X) = 2$ was done for mixing SFTs containing a fixed point in the paper [3] published in the proceedings of AUTOMATA 2018.

Lemma 1 is a criterion saying essentially that if S is a collection of automorphisms that acts together with the diffusive glider automorphism g in a special way, then $C(S \cup \{g\})$ is not very complicated. We have formulated a reasonably general version of the lemma to allow its application in other contexts. To further showcase our Main lemma, we consider an alternative finitary variant of Ryan's theorem. In Section 7.3 of [6] the question was raised whether for a mixing SFT X and for every $G \subseteq \mathrm{Aut}(X)$ such that $C(G) = \langle\sigma\rangle$ there is a finite subset $S \subseteq G$ such that also $C(S) = \langle\sigma\rangle$. In the same section it was noted that to construct a counterexample it would be sufficient to find a locally finite group $G \subseteq \mathrm{Aut}(X)$ whose centralizer is generated by σ. We use a different strategy based on Lemma 1 to construct a counterexample in the case when X is the binary full shift.

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 $x[i, j] = x[i]x[i+1]\cdots x[j]$, $x[i, \infty] = x[i]x[i+1]\cdots$ and $x[-\infty, i] = \cdots x[i-1]x[i]$. Occasionally we signify the symbol at position zero in a configuration x by a dot as follows:

$$x = \cdots x[-2]x[-1].x[0]x[1]x[2]\cdots .$$

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 $w = w[1]w[2]\cdots w[n]$ (also the empty sequence, which is denoted by λ) where $w[i] \in A$ is a *word* over A. The concatenation of a word or a left-infinite sequence u with a word or a right-infinite sequence v is denoted by uv. A word u is a *prefix* of a word or a right-infinite sequence x if there is a word or a right-infinite sequence v such that $x = uv$. Similarly, u is a *suffix* of a word or a left-infinite sequence x if there is a word or a left-infinite sequence v such that $x = vu$. 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

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

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.

$|w| = n \iff w \in A^n$. Given $x \in A^{\mathbb{Z}}$ and $w \in A^+$ we define the sets of left (resp. right) occurrences of w in x by

$$\begin{aligned} &\mathrm{occ}_\ell(x,w) = \{i \in \mathbb{Z} \mid x[i, i+|w|-1] = w\} \\ \text{(resp.)} \quad &\mathrm{occ}_\mathrm{r}(x,w) = \{i \in \mathbb{Z} \mid x[i-|w|+1, i] = w\}. \end{aligned}$$

Note that both of these sets contain the same information up to a shift in the sense that $\mathrm{occ}_\mathrm{r}(x,w) = \mathrm{occ}_\ell(x,w) + |w| - 1$. Typically we refer to the left occurrences and we say that $w \in A^n$ *occurs* in $x \in A^{\mathbb{Z}}$ at position i if $i \in \mathrm{occ}_\ell(x,w)$. 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 $A^{\mathbb{Z}}$. For any $S \subseteq A^{\mathbb{Z}}$ the collection of words appearing as factors of elements of S is the *language* of S, denoted by $L(S)$. Any closed set $X \subseteq A^{\mathbb{Z}}$ such that $\sigma(X) = X$ is called a *subshift*. The restriction of σ to X may be denoted by σ_X, but typically the subscript X is omitted. The *orbit* of a point $x \in X$ is $\mathcal{O}(x) = \{\sigma^i(x) \mid i \in \mathbb{Z}\}$.

For any word $w \in A^+$ we denote by ${}^\infty w$ and w^∞ the left- and right-infinite sequences obtained by infinite repetitions of the word w. We denote by $w^{\mathbb{Z}} \in A^{\mathbb{Z}}$ the configuration defined by $w^{\mathbb{Z}}[in, (i+1)n-1] = w$ (where $n = |w|$) for every $i \in \mathbb{Z}$. We say that $x \in A^{\mathbb{Z}}$ is *w-finite* if $x[-\infty, i] = {}^\infty w$ and $x[j, \infty] = w^\infty$ for some $i, j \in \mathbb{Z}$.

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

Definition 1 A (directed) *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* or *arrows*. 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 $e \in E$ is an outgoing edge of $\iota(e)$ and an incoming edge of $\tau(e)$. For a state $s \in V$, E_s denotes the set of outgoing edges of s and E^s denotes the set of incoming edges of s.

Although the notation for the set E^s of incoming edges of s is similar to the notation for the set E^n of words of length n over E, in practice the distinction should be clear from the context.

A sequence of edges $e[1] \cdots e[n]$ in a graph $\mathcal{G} = (V, E)$ is a *path* (of length n) if $\tau(e[i]) = \iota(e[i+1])$ for $1 \leq i < n$, it is a *cycle* if in addition $\tau(e[n]) = \iota(e[1])$ and it is a *simple cycle* if in addition $\iota(e[i])$ for $1 \leq i \leq n$ are all distinct. We say that the path starts at $\iota(e[1])$ and ends at $\tau(e[n])$. A graph $\mathcal{G}$ is *irreducible* if for every $v_1, v_2 \in V$ there is a path starting at v_1 and ending at v_2 and it 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

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

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

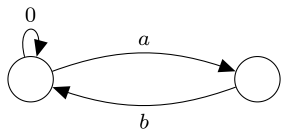

Fig. 2 The golden mean shift.

Definition 2 A subshift $X \subseteq A^{\mathbb{Z}}$ is a *subshift of finite type* (SFT) if it is conjugate to some edge subshift. It is a *transitive SFT* if it is conjugate to the edge subshift of an irreducible graph $\mathcal{G} = (V, E)$. It is a *mixing SFT* if $\mathcal{G}$ is primitive and it is a nontrivial mixing SFT if $\mathcal{G}$ contains at least two edges. We will mostly consider an SFT X as being equal to an edge subshift instead of just being conjugate (in which case $E \subseteq A$).

Example 1 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

$$\cdots 000abab0ab00ab000 \cdots$$

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

Definition 3 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 $\mathrm{Aut}(X)$. (In the case $X = A^{\mathbb{Z}}$ automorphisms are also known as reversible cellular automata.)

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 $S \subseteq \mathrm{Aut}(X)$ is denoted by $\langle S \rangle$. The following definition is from [6]:

Definition 4 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.

It is proven in [5] and as Theorem 7.7 in [2] that $k(X) \neq \perp$ whenever X is a mixing SFT. The following observation is from Section 7.6 of [6].

Theorem 1 *Let X be a subshift. The case $k(X) = 0$ occurs if and only if $\mathrm{Aut}(X) = \langle \sigma \rangle$. The case $k(X) = 1$ cannot occur.*

Proof. The statement $k(X) = 0$ is equivalent to $\langle \sigma \rangle = C(\emptyset) = \mathrm{Aut}(X)$.

The statement $k(X) = 1$ means that $C(\{f\}) = \langle \sigma \rangle$ for some $f \in \mathrm{Aut}(X)$. Because f commutes with itself, it follows that $f = \sigma^i$ for some $i \in \mathbb{Z}$. But all $g \in \mathrm{Aut}(X)$ commute with σ^i and so $\mathrm{Aut}(X) = C(\{f\}) = \langle \sigma \rangle$ and $k(X) = 0$, a contradiction. $\square$

For conjugate subshifts X and Y it necessarily holds that $k(X) = k(Y)$.

3 Main Lemma

In this section we prove as our main lemma a useful criterion which can be used to significantly restrict the kinds of automorphisms that can occur in $C(G)$ when $G \subseteq \mathrm{Aut}(X)$ is chosen carefully. We state a reasonably general version of the lemma to make it applicable in many different contexts. A special case occurs as part of the proof of Theorem 14 in [3].

Definition 5 Given a subshift $X \subseteq A^{\mathbb{Z}}$, an *abstract glider automorphism group* is any tuple $(G, \mathbf{0}, \mathcal{I}, \mathrm{spd}, \varsigma, \mathrm{GF})$ (or just G when the rest of the tuple is clear from the context) where $G \subseteq \mathrm{Aut}(X)$ is a subgroup, $\mathcal{I}$ is an index set, $\mathbf{0} \in A^+$ and

- $\mathrm{spd} : \mathcal{I} \to \mathbb{Z}$ is called a *speed map* and $\varsigma : \mathcal{I} \to G$ (image at $i \in \mathcal{I}$ is denoted by ς_i) is called a *local shift map*
- GF is a map from $\mathcal{I}$ to subsets of X whose image at $i \in \mathcal{I}$ is

$$\mathrm{GF}_i = \{x \in X \mid x \text{ is } \mathbf{0}\text{-finite and } \varsigma_i(x) = \sigma^{\mathrm{spd}(i)}(x)\} \supsetneq \mathcal{O}(0^{\mathbb{Z}})$$

  and is called a *glider fleet set*. Elements of GF_i are called glider fleets.

This tuple is an *abstract diffusive glider automorphism group* if in addition

- for every $\mathbf{0}$-finite $x \in X$ and every $N \in \mathbb{N}$ there is a $g \in G$ such that for every $i \in \mathbb{Z}$, $g(x)[i, i+N] \in L(\mathrm{GF}_j)$ for some $j \in \mathcal{I}$.

If G is generated by a single automorphism $g \in \mathrm{Aut}(X)$, we say that g is an *abstract (diffusive) glider automorphism.*

The idea of an abstract diffusive glider automorphism group is the following. For any $\mathbf{0}$-finite $x \in X$ there is a $g \in G$ that can be used to “diffuse” x into a point $g(x)$ such that elements of $\mathcal{O}(g(x))$ locally look like elements of some GF_i, and in practice $\overline{\mathrm{GF}_i}$ will be in some sense simpler subshifts than X. The local shift maps ς_i are used to dynamically distinguish the points in $\mathrm{GF}_i \setminus \mathcal{O}(\mathbf{0}^{\mathbb{Z}})$. In the proof of our main lemma we will also require that the points of GF_i consist of gliders in a more concrete sense. We encode this in the following definition.

Definition 6 Given a subshift $X \subseteq A^{\mathbb{Z}}$, a *(diffusive) glider automorphism group* is any tuple $(G, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ (or just G when the rest of the tuple is clear from the context) where $(G, \mathbf{0}, \mathcal{I}, \mathrm{spd}, \varsigma, \mathrm{GF})$ is an abstract (diffusive) glider automorphism group and

- $\boxed{\leftrightarrow} : \mathcal{I} \to A^+$ is a map whose image at $i \in \mathcal{I}$ is denoted by $\boxed{\leftrightarrow}_i$ and is called a *glider*
- for every $i \in \mathcal{I}$ there is some $n \in \mathbb{N}$ such that $\mathrm{GF}_i = {}^{\infty}\mathbf{0}(\boxed{\leftrightarrow}_i \mathbf{0}^n \mathbf{0}^*)^* \mathbf{0}^{\infty}$; note that these configurations are $\mathbf{0}$-finite
- for every $i \in \mathcal{I}$ and $x \in \mathrm{GF}_i$ it holds that $|i - j| \geq |\boxed{\leftrightarrow}_i|$ whenever $i, j \in \mathrm{occ}_{\ell}(x, \boxed{\leftrightarrow}_i)$ are distinct, i.e. the occurrences of $\boxed{\leftrightarrow}_i$ do not overlap in any point of GF_i.

If G is generated by a single automorphism $g \in \mathrm{Aut}(X)$, we say that g is a *(diffusive) glider automorphism.*

Example 2 Let $B = \{0,1\}$, $A = B \times B$ and $X = A^{\mathbb{Z}}$, i.e. X is the four-letter full shift. Any point $x \in X$ can be naturally identified with a point $(x_1, x_2) \in B^{\mathbb{Z}} \times B^{\mathbb{Z}}$ such that $x[i] = (x_1[i], x_2[i])$ for all $i \in \mathbb{Z}$. We define $g \in \mathrm{Aut}(X)$ by $g(x) = (\sigma(x_1), x_2)$. This map is a diffusive glider automorphism with an associated diffusive glider automorphism group $(G, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ where $G = \langle g \rangle$, $\mathbf{0} = (0,0) \in A$, $\mathcal{I} = \{0,1\}$, $\boxed{\leftrightarrow}_0 = (0,1) \in A$, $\boxed{\leftrightarrow}_1 = (1,0) \in A$, $\mathrm{spd}(i) = i$, $\varsigma_i = g$ (for $i \in \mathcal{I}$) and GF_0 (resp. GF_1) consists of those $\mathbf{0}$-finite points $x = (x_1, x_2) \in B^{\mathbb{Z}} \times B^{\mathbb{Z}}$ such that x_1 (resp. x_2) contains no occurrences of the digit 1.

For X and $\mathbf{0}$ as above we let $\mathrm{Aut}(X, \mathbf{0}) = \{f \in \mathrm{Aut}(X) \mid f(\mathcal{O}(\mathbf{0}^{\mathbb{Z}})) = \mathcal{O}(\mathbf{0}^{\mathbb{Z}})\}$. For $x, y \in A^{\mathbb{Z}}$ and $i \in \mathbb{Z}$ we denote by $x \otimes_i y \in A^{\mathbb{Z}}$ the "gluing" of x and y at i, i.e. $(x \otimes_i y)[-\infty, i-1] = x[-\infty, i-1]$ and $(x \otimes_i y)[i, \infty] = y[i, \infty]$. Typically we perform gluings at the origin and we denote $x \otimes y = x \otimes_0 y$.

In the next lemma we need the notion of a bipartite non-directed graph. By this we mean a pair $\mathcal{B} = (V, E)$ where V is the set of vertices with a nontrivial partition $V = V_1 \cup V_2$ and $E \subseteq V_1 \times V_2$ is the set of edges, i.e. an edge cannot connect two vertices belonging in the same element of the partition. V and E are not necessarily finite. We say that $\mathcal{B}$ is connected if the equivalence relation on V generated by E is equal to $V \times V$, which is equivalent to saying that it is possible to traverse between any two vertices by a finite path in which edges can be crossed in both directions.

Lemma 1 (Main lemma) *Let $X \subseteq A^{\mathbb{Z}}$ be a subshift with a diffusive glider automorphism group $(G, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ such that $\mathbf{0}$-finite configurations are dense in X. Let $\mathcal{I}_1 \cup \mathcal{I}_2 = \mathcal{I}$ be a nontrivial partition and let $\mathcal{B} = (\mathcal{I}, E)$ be a bipartite non-directed graph with an edge from $i \in \mathcal{I}_1$ to $j \in \mathcal{I}_2$ if and only if there are $d, e \in \mathbb{N}_+$, a strictly increasing sequence $(N_m)_{m \in \mathbb{N}} \in \mathbb{N}^{\mathbb{N}}$ and $(g_m)_{m \in \mathbb{N}} \in G^{\mathbb{N}}$ such that for any $x\boxed{\leftrightarrow}_i\mathbf{0}^{\infty} \in \mathrm{GF}_i$, ${}^{\infty}\mathbf{0}\boxed{\leftrightarrow}_j y \in \mathrm{GF}_j$ we have*

- $x\boxed{\leftrightarrow}_i.\mathbf{0}^{N_m}\boxed{\leftrightarrow}_j y \in X$
- $g_m(x\boxed{\leftrightarrow}_i.\mathbf{0}^{N}\boxed{\leftrightarrow}_j y) = x\boxed{\leftrightarrow}_i\mathbf{0}^d.\mathbf{0}^N\mathbf{0}^e\boxed{\leftrightarrow}_j y$ *for every* $N > N_m$
- $g_m(x\boxed{\leftrightarrow}_i.\mathbf{0}^{N_m}\boxed{\leftrightarrow}_j y) = x\mathbf{0}^d\boxed{\leftrightarrow}_i.\mathbf{0}^{N_m}\boxed{\leftrightarrow}_j\mathbf{0}^e y.$

If $\mathcal{B}$ is connected then $C(G) \cap \mathrm{Aut}(X, \mathbf{0}) = \langle \sigma \rangle$.

Before the proof we continue our previous example and show how this lemma can be applied to it.

Example 3 We use the notation of the previous example. Furthermore, we denote $\boxed{\leftarrow} = \boxed{\leftrightarrow}_1$ and $\boxed{} = \boxed{\leftrightarrow}_0$ to reflect the fact that occurrences $\boxed{\leftarrow}$ move to the left and occurrences of $\boxed{}$ remain stationary under the action of the map g. Note that $(G, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ remains a diffusive glider automorphism group even when G is replaced by a larger group $G' \supseteq G$. We let $G' = \langle g, f \rangle$ where $f = f_2 \circ f_1$ for automorphisms $f_1, f_2 : X \to X$ such that

– f_1 replaces every occurrence of $(0,1)(0,0)(0,0)(1,0) = \boxed{\ }\mathbf{00}\boxed{\leftarrow}$ by $(0,1)(0,0)(1,0)(0,0) = \boxed{\ }\mathbf{0}\boxed{\leftarrow}\mathbf{0}$ and vice versa
– f_2 replaces every occurrence of $(0,1)(0,0)(1,0) = \boxed{\ }\mathbf{0}\boxed{\leftarrow}$ by $(0,0)(0,1)(1,0) = \mathbf{0}\boxed{\ }\boxed{\leftarrow}$ and vice versa.

The map f has two important properties. First, it replaces any occurrence of $\boxed{\ }\mathbf{00}\boxed{\leftarrow}$ by $\mathbf{0}\boxed{\ }\boxed{\leftarrow}\mathbf{0}$. Second, if $x \in X$ is a configuration containing only gliders $\boxed{\ }$ and $\boxed{\leftarrow}$ and every occurrence of $\boxed{\ }$ is sufficiently far from every occurrence of $\boxed{\leftarrow}$, then $f(x) = x$.

We use the lemma to show that $C(G') \cap \mathrm{Aut}(X, \mathbf{0}) = \langle\sigma\rangle$. The bipartite graph $\mathcal{B}$ in the statement of the lemma has in this case the set of vertices $\{0,1\}$ with the partition $\mathcal{I}_1 = \{0\}$ and $\mathcal{I}_2 = \{1\}$, so it suffices to show that there is an edge between 0 and 1.

Still using the same notation as in the statement of the lemma, let $d = e = 1$, $(N_m)_{m\in\mathbb{N}}$ with $N_m = 2+m$ and $(g_m)_{m\in\mathbb{N}}$ with $g_m = \sigma \circ g^{-(m+2)} \circ f \circ g^m$. Let $x\boxed{\ }\mathbf{0}^\infty \in \mathrm{GF}_0 = {}^\infty\mathbf{0}\{\mathbf{0}, \boxed{\ }\}^*\mathbf{0}^\infty$, ${}^\infty\mathbf{0}\boxed{\leftarrow}y \in \mathrm{GF}_1 = {}^\infty\mathbf{0}\{\mathbf{0}, \boxed{\leftarrow}\}^*\mathbf{0}^\infty$ be arbitrary. Fix some $m \in \mathbb{N}$. Since X is a full shift, it is clear that $x\boxed{\ }.\mathbf{0}^{N_m}\boxed{\leftarrow}y \in X$ and it is easy to verify that

– $g_m(x\boxed{\ }.\mathbf{0}^N\boxed{\leftarrow}y) = x\boxed{\ }\mathbf{0}.\mathbf{0}^N\mathbf{0}\boxed{\leftarrow}y$ for $N > N_m$
– $g_m(x\boxed{\ }.\mathbf{0}^{N_m}\boxed{\leftarrow}y) = x\mathbf{0}\boxed{\ }.\mathbf{0}^{N_m}\boxed{\leftarrow}\mathbf{0}y$.

It follows that there is an edge between 0 and 1, so $C(G') \cap \mathrm{Aut}(X, \mathbf{0}) = \langle\sigma\rangle$. In other words, if $h \in \mathrm{Aut}(X)$ has $0^\mathbb{Z}$ as a fixed point and if it commutes with both f and g, then $h = \sigma^i$ for some $i \in \mathbb{Z}$.

In our example the construction of a nontrivial diffusive glider automorphism g was simple because of the existence of a decomposition $A^\mathbb{Z} = B^\mathbb{Z} \times B^\mathbb{Z}$. On more general subshifts we cannot rely on such decompositions. In the example we also augmented G by an automorphism f and got a group G' satisfying the assuptions of Lemma 1. The construction of such a map f will be essentially the same in all our later applications of the lemma. To gain a better understanding of Main Lemma, it may be helpful to consider how the following proof would go in the case of the previous example.

Proof of Lemma 1. Assume that $f \in C(G) \cap \mathrm{Aut}(X, \mathbf{0})$ is a radius-r automorphism whose inverse is also a radius-r automorphism. Since we aim to prove that $f \in \langle\sigma\rangle$, we lose no generality by transforming f throughout the proof by taking inverses and composing it with some shift. We start by noting that without loss of generality (by composing f with a suitable power of σ if necessary) $\mathbf{0}^\mathbb{Z}$ is a fixed point of f.

We have that $f(\mathrm{GF}_i) \subseteq \mathrm{GF}_i$ for $i \in \mathcal{I}$. To see this, assume to the contrary that $x \in \mathrm{GF}_i$ but $f(x) \notin \mathrm{GF}_i$. Then $f(\varsigma_i(x)) = f(\sigma^{\mathrm{spd}(i)}(x)) = \sigma^{\mathrm{spd}(i)}(f(x)) \neq \varsigma_i(f(x))$, contradicting the assumption $f \in C(G)$.

For all $i \in \mathcal{I}_1$, $j \in \mathcal{I}_2$ and all $x_1 \in \mathrm{GF}_i$ and $x_2 \in \mathrm{GF}_j$ not in $\mathcal{O}(\mathbf{0}^\mathbb{Z})$ we define the right and left offsets

$$\mathrm{off}_\mathrm{r}(x_1) = \max\{\mathrm{occ}_\mathrm{r}(f(x_1), \boxed{\leftrightarrow}_i)\} - \max\{\mathrm{occ}_\mathrm{r}(x_1, \boxed{\leftrightarrow}_i)\},$$

$$\mathrm{off}_\ell(x_2) = \min\{\mathrm{occ}_\ell(f(x_2), \boxed{\leftrightarrow}_j)\} - \min\{\mathrm{occ}_\ell(x_2, \boxed{\leftrightarrow}_j)\}.$$

We claim that $\mathrm{off}_\ell(x_2) - \mathrm{off}_\mathrm{r}(x_1) = 0$. To see this, assume to the contrary that this does not hold. Since $\mathcal{B}$ is connected, there is a path from i to j, along which there is an edge from $i' \in \mathcal{I}_1$ to $j' \in \mathcal{I}_2$ and some $x_1' \in \mathrm{GF}_{i'}$, $x_2' \in \mathrm{GF}_{j'}$ not in $\mathcal{O}(\mathbf{0}^\mathbb{Z})$ such that $\mathrm{off}_\ell(x_2') - \mathrm{off}_\mathrm{r}(x_1') \neq 0$. Then we can assume without loss of generality that $\mathrm{off}_\mathrm{r}(x_1') = 0$ (by replacing f with $f \circ \sigma^{\mathrm{off}_\mathrm{r}(x_1')}$ if necessary), that $\mathrm{off}_\ell(x_2') > 0$ (by replacing f with f^{-1}, x_1' with $f(x_1')$ and x_2' with $f(x_2')$ if necessary) and that $\min\{\mathrm{occ}_\ell(x_2', \boxed{\leftrightarrow}_j)\} = N_m$, $\max\{\mathrm{occ}_\mathrm{r}(x_1', \boxed{\leftrightarrow}_i)\} = -1$ with $m \in \mathbb{N}$ such that $N_m \geq 2r+1$ (by shifting x_1' and x_2' suitably). Then consider $x = x_1' \otimes x_2'$ and note that $f(x) = f(x_1') \otimes f(x_2')$ by the choice of N_m. By our assumption on offsets and the map g_m it follows that

$$\begin{aligned} f^{-1}(g_m(f(x))) &= f^{-1}(\sigma^{|\mathbf{0}|d}(f(x_1')) \otimes \sigma^{-|\mathbf{0}|e}(f(x_2'))) \\ &= \sigma^{|\mathbf{0}|d}(x_1') \otimes \sigma^{-|\mathbf{0}|e}(x_2') \neq g_m(x) \end{aligned}$$

and thus $g_m \circ f \neq f \circ g_m$, contradicting the assumption $f \in C(G)$. In the following we may therefore assume that $\mathrm{off}_\ell(x_2) = \mathrm{off}_\mathrm{r}(x_1) = 0$ for all $i \in \mathcal{I}_1$, $j \in \mathcal{I}_2$ and all $x_1 \in \mathrm{GF}_i$ and $x_2 \in \mathrm{GF}_j$ not in $\mathcal{O}(\mathbf{0}^\mathbb{Z})$.

If $x \in \mathrm{GF}_i$ is a configuration containing exactly one occurrence of $\boxed{\leftrightarrow}_i$, then $f(x) = x$. To see this, assume to the contrary (without loss of generality), that $f(x)$ contains at least two occurrences of $\boxed{\leftrightarrow}_i$, that $i \in \mathcal{I}_1$ (the case $i \in \mathcal{I}_2$ being similar), that $y \in \mathrm{GF}_j$ is a configuration containing a single $\boxed{\leftrightarrow}_j$ for j such that there is an edge from i to j in $\mathcal{B}$ and that $\min\{\mathrm{occ}_\ell(y, \boxed{\leftrightarrow}_j)\} = N_m$, $\max\{\mathrm{occ}_\mathrm{r}(x, \boxed{\leftrightarrow}_i)\} = -1$ with $m \in \mathbb{N}$ such that $N_m \geq 2r+1$ (by shifting x and y suitably). Then consider $z = x \otimes y$ and note that $g_m(z) = z$ but $g_m(f(z)) \neq f(z)$ because g_m at least shifts the leftmost glider in $f(z)$. Thus $f(g_m(z)) = f(z) \neq g_m(f(z))$, contradicting the assumption $f \in C(G)$.

Now let us prove that if $x \in \mathrm{GF}_i$, then $f(x) = x$. To see this, assume to the contrary that $f(x) \neq x$, that $i \in \mathcal{I}_1$ (the case $i \in \mathcal{I}_2$ being similar), that x contains a minimal number of occurrences of $\boxed{\leftrightarrow}_i$ (at least two by the previous paragraph) and that the distance from the rightmost $\boxed{\leftrightarrow}_i$ to the second-to-rightmost $\boxed{\leftrightarrow}_i$ in x is maximal. Let $y \in \mathrm{GF}_j$ be a configuration containing a single $\boxed{\leftrightarrow}_j$ for j such that there is an edge from i to j in $\mathcal{B}$ and assume that $\min\{\mathrm{occ}_\ell(y, \boxed{\leftrightarrow}_j)\} = N_m$, $\max\{\mathrm{occ}_\mathrm{r}(x, \boxed{\leftrightarrow}_i)\} = -1$ with $m \in \mathbb{N}$ such that $N_m \geq 2r+1$ (by shifting x and y suitably). Then $x[-\infty,-1], f(x)[-\infty,-1]$ are of the form $z_1\boxed{\leftrightarrow}_i, z_2\boxed{\leftrightarrow}_i \in {}^\infty\mathbf{0}L(\mathrm{GF}_i)$ with $z_1 \neq z_2$. Consider $z = x \otimes y$ and note that

$$\begin{aligned} g_m(z)[-\infty,-1] &= z_1\mathbf{0}^d\boxed{\leftrightarrow}_i \\ f(g_m(z))[-\infty,-1] &= g_m(f(x))[-\infty,-1] = z_2\mathbf{0}^d\boxed{\leftrightarrow}_i. \end{aligned}$$

It follows that

$$f(z_1\mathbf{0}^d\boxed{\leftrightarrow}_i.\mathbf{0}^\infty) = z_2\mathbf{0}^d\boxed{\leftrightarrow}_i.\mathbf{0}^\infty \neq z_1\mathbf{0}^d\boxed{\leftrightarrow}_i.\mathbf{0}^\infty,$$

contradicting the maximal distance between the two rightmost occurrences of $\boxed{\leftrightarrow}_i$ in x.

If x is a $\mathbf{0}$-finite configuration, then $f(x) = x$. Namely, let $N \geq 2r + 1$, and because G is a diffusive glider automorphism group of X, there exists $g \in G$ such that for every $i \in \mathbb{Z}$, $g(x)[i, i + N] \in L(\mathrm{GF}_j)$ for some $j \in \mathcal{I}$. Because F acts like the identity on all GF_j, it follows that $f(g(x)) = g(x)$. By using the assumption $f \in C(G)$ it follows that

$$f(x) = f(g^{-1}(g(x))) = g^{-1}(f(g(x))) = g^{-1}(g(x)) = x.$$

Finally, because f is a continuous map that agrees with the identity map on the dense set of $\mathbf{0}$-finite configurations, it follows that f is the identity map and in particular $f \in \langle \sigma \rangle$. □

4 Diffusive Glider Automorphisms for Mixing SFTs

In this section we construct for an arbitrary nontrivial mixing SFT X (with a distinguished periodic point $\mathbf{0}^{\mathbb{Z}}$) an automorphism g which breaks every $\mathbf{0}$-finite point of X into a collection of gliders traveling in opposite directions. More precisely, we will construct a diffusive glider automorphism $g : X' \to X'$ for a subshift X' which is conjugate to X (via some conjugacy $\phi : X \to X'$) but has a graph presentation that makes our constructions simpler. Then the map $\phi^{-1} \circ g \circ \phi$ is an abstract diffusive glider automorphism on X.

To begin, consider a nontrivial mixing SFT X defined by a graph $\mathcal{G} = (V, E)$ and let $\mathbf{0} = 0_1 \cdots 0_p \in E^p$ be some fixed simple cycle in $\mathcal{G}$. We will want, among other things, that occurrences of the letters 0_i can only occur within occurrences of the word $\mathbf{0}$ in points of X. We start with some auxiliary definitions.

Definition 7 Given a graph $\mathcal{G} = (V, E)$, we say that a path $w \in E^+$ has a unique successor in $\mathcal{G}$ (resp. a unique predecessor) if wa (resp. aw) is a path for a unique $a \in E$. Then we say that a is the unique successor (resp. the unique predecessor) of w.

Definition 8 Let $\mathcal{G} = (V, E)$ be a graph and let $w = w[1] \cdots w[n]$ be a path. If $w[i]$ have unique successors for $1 \leq i < n$, we say that w is future deterministic in $\mathcal{G}$ and if $w[j]$ have unique predecessors for $1 < j \leq n$, we say that w is past deterministic in $\mathcal{G}$. If w is both future and past deterministic in $\mathcal{G}$, we say that w is deterministic in $\mathcal{G}$.

We emphasize that if w is a deterministic path, we do not require that $w[1]$ has a unique predecessor or that $w[n]$ has a unique successor.

Lemma 2 *Let X_1 be a nontrivial mixing SFT defined by the graph $\mathcal{G} = (V, E)$ and let $\mathbf{0} = 0_1 \cdots 0_p \in E^p$ be a simple cycle in $\mathcal{G}$. Then X_1 is conjugate to a subshift X_2 defined by a graph $\mathcal{H} = (V', E')$ such that $\mathbf{0}$ is a past deterministic simple cycle in $\mathcal{H}$.*

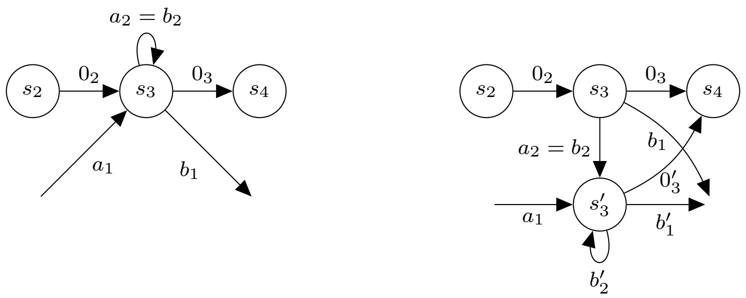

Fig. 3 In-splitting at state s_3.

Proof. The proof is by induction. We assume that $0_1 \cdots 0_{i-1}$ is past deterministic for some $1 < i \leq p$ in $\mathcal{G}$ and we will construct a conjugate subshift Y defined by $\mathcal{H} = (V', E')$ such that $0_1 \cdots 0_i$ is past deterministic in $\mathcal{H}$. The induction can be started because 0_1 is vacuously past deterministic in $\mathcal{G}$, and the claim will follow by repeating the argument for increasing i.

Denote $s_j = \iota(0_j)$ for $1 \leq j \leq p$. Let us assume that $0_1 \cdots 0_i$ is not past deterministic in $\mathcal{G}$, because otherwise we could choose $\mathcal{H} = \mathcal{G}$. Then $E^{s_i} = \{0_{i-1}, a_1, \ldots, a_k\}$ for some $k \geq 1$ and $a_1, \ldots, a_k \in E$. We denote by $b_1, \ldots, b_\ell$ the outgoing edges of s_i different from 0_i (some may be equal to an edge a_j) and construct an in-split graph $\mathcal{H} = (V', E')$ where $V' = V \cup \{s'_i\}$, $E' = E \cup \{0'_1, b'_1, \ldots, b'_\ell\}$ with the starting and ending nodes of $e \in E$ the same as in $\mathcal{G}$ with the exception of $\tau(a_j) = s'_i$. Let $\iota(0'_i) = s'_i$, $\tau(0'_i) = s_{i+1}$ and for all b_j let $\iota(b'_j) = s'_i$. For b_j equal to some $a_{j'}$ let $\tau(b'_j) = s'_i$ and for b_j distinct from any $a_{j'}$, $\tau(b'_j) = \tau(b_j)$ (see Figure 3). The edge subshift of $\mathcal{H}$ is conjugate to X_1 (see Section 2.4 of [4]), $\mathcal{H}$ contains the cycle $0_1 \cdots 0_p$ with $\iota(0_i) = s_i$, and all the states $s_2, \ldots, s_i$ have only one incoming edge so $0_1 \cdots 0_i$ is past deterministic. □

Lemma 3 *Let X_2 be a nontrivial mixing SFT defined by the graph $\mathcal{G} = (V, E)$ and let $\mathbf{0} = 0_1 \cdots 0_p \in E^p$ be a past deterministic simple cycle in $\mathcal{G}$. Then X_2 is conjugate to a subshift X_3 defined by a graph $\mathcal{H} = (V', E')$ such that $\mathbf{0}$ is a deterministic simple cycle in $\mathcal{H}$.*

Proof. The proof is by induction. We assume that $0_i \cdots 0_p$ is future deterministic for some $1 < i \leq p$ in $\mathcal{G}$ and we will construct a conjugate subshift X_3 defined by $\mathcal{H} = (V', E')$ such that $0_{i-1} \cdots 0_p$ is future deterministic and $\mathbf{0}$ is still past deterministic in $\mathcal{H}$.

Denote $s_j = \iota(0_j)$ for $1 \leq j \leq p$ and assume that $0_{i-1} \cdots 0_p$ is not future deterministic in $\mathcal{G}$. Then $E_{s_i} = \{0_i, a_1, \ldots, a_k\}$ for some $k \geq 1$ and $a_1, \ldots, a_k \in E$ and it would be possible to construct an out-split graph $\mathcal{H} = (V', E')$ where $V' = V \cup \{s'_i\}$, $E' = E \cup \{0'_{i-1}\}$ with the starting and ending nodes of $e \in E$ the same as in $\mathcal{G}$ with the exception of $\iota(a_j) = s'_i$ and $\iota(0'_{i-1}) = s_{i-1}$, $\tau(0'_{i-1}) = s'_i$ (see Figure 4). The edge subshift of $\mathcal{H}$ is conjugate to X_2 (see again Section

Fig. 4 Out-splitting at state s_3.

2.4 of [4]), $\mathcal{G}$ contains the cycle $0_1 \cdots 0_p$ with $\iota(0_i) = s_i$, and all the states $s_i, \dots, s_p$ have only one outgoing edge. $\square$

Lemma 4 *Let X_3 be a nontrivial mixing SFT defined by the graph $\overline{\mathcal{G}} = (\overline{V}, \overline{E})$ and let $\mathbf{0} = 0_1 \cdots 0_p \in E^p$ be a deterministic simple cycle in $\overline{\mathcal{G}}$. Then X_3 is conjugate to a subshift X defined by a graph $\mathcal{G} = (V, E)$ such that $\mathbf{0}$ is a deterministic simple cycle in $\mathcal{G}$ and the graph*

$$\mathcal{G}' = (V', E') = (V \setminus \{s_i \mid 1 < i \le p\}, E \setminus \{0_i \mid 1 \le i \le p\})$$

gained by removing the cycle $\mathbf{0}$ from $\mathcal{G}$ is primitive (here we denote $s_i = \iota(0_i)$). Furthermore, $\mathcal{G}'$ contains a cycle $\mathbf{1} = a_1 \cdots a_q \in E'^q$ with p and q coprime such that $\iota(a_1) = \tau(a_q) = s_1$ and $\iota(a_i) \neq s_1$ for $1 < i \le q$.

Proof. We denote $s_i = \iota(0_i)$ in $\overline{\mathcal{G}}$. Let $E^{s_1} = \{0_p, d_1, d_2, \dots, d_k\}$, $E_{s_1} = \{0_1, e_1, \dots, e_\ell\}$ and construct the graph

$$\mathcal{G} = (V, E) = (\overline{V} \cup \{s'_1, \dots, s'_p\}, \overline{E} \cup \{0'_1, \dots, 0'_p, d'_1, \dots, d'_k\})$$

with $\iota(0'_1) = s_1$, $\tau(0'_1) = s'_2$, $\iota(0'_i) = s'_i$, $\tau(0'_i) = s'_{i+1}$, $\iota(0'_p) = s'_p$, $\tau(0'_p) = s'_1$, $\tau(d_j) = s'_1 = \iota(e_m)$, $\iota(d'_j) = \iota(d_j)$ and $\tau(d'_j) = s_1$ for $1 < i < p$, $1 \le j \le k$, $1 \le m \le \ell$ with the other initial and terminal vertices remaining the same as in $\overline{\mathcal{G}}$ (see Figure 5). If X is the edge subshift of $\mathcal{G}$, then it is easy to see that the map $\Phi : X \to X_3$ defined by

$$\Phi(x)[i] = \begin{cases} 0_i \text{ when } x[i] = 0'_i, \\ d_i \text{ when } x[i] = d'_i, \\ x[i] \text{ otherwise.} \end{cases}$$

is a conjugacy. Since X is mixing, there is a large enough prime number $p' > p$ such that $\overline{\mathcal{G}}$ contains a path of length p' from s_1 to s_1. If all cycles $\mathbf{0}$ are removed from this path, we get a path $wc_{p'-np} = c_1 \cdots c_{p'-np} \in \overline{E}^{p'-np}$ from s_1 to s_1, where n is the number of removed $\mathbf{0}$-cycles. In particular, the length of $wc_{p'-np}$ is coprime with p. Then $\mathbf{1} = 0'_1 \cdots 0'_p wc'_{p'-np}$ is a path in $\mathcal{G}$ which visits s_1 only at the beginning and ending and $|\mathbf{1}|$ is coprime with p. Moreover, the graph $\mathcal{G}'$ is primitive, because it contains cycles $wc_{p'-np}$ and $\mathbf{1}$ of coprime length. $\square$

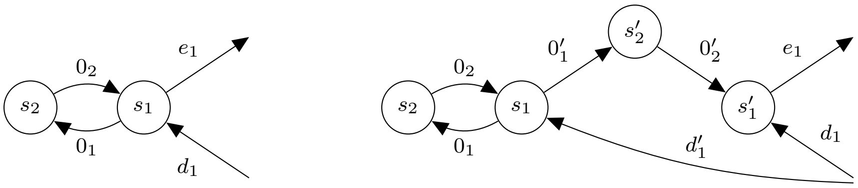

Fig. 5 Creating a graph with suitable cycles $\mathbf{0}$ and $\mathbf{1}$ (in this case $p = 2$).

Now let X be a nontrivial mixing SFT. By applying the three previous lemmas consecutively, we may assume up to conjugacy that X is defined by a graph $\mathcal{G} = (V, E)$ such that $\mathcal{G}'$, $\mathbf{0}$, $\mathbf{1}$, etc. are as in the conclusion of the previous lemma. In the rest of this section we will construct a diffusive glider automorphism $g : X \to X$ with the associated diffusive glider automorphism group $(\langle g \rangle, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$. Let $\mathcal{I} = \{\ell, \mathrm{r}\}$, $\mathrm{spd}(\ell) = pq$ and $\mathrm{spd}(\mathrm{r}) = -pq$, which reflect the fact that we will have left- and rightbound gliders. The gliders will be

$$\boxed{\leftrightarrow}_\ell = \boxed{\leftarrow} = \mathbf{0}^q\mathbf{1} \qquad \boxed{\leftrightarrow}_\mathrm{r} = \boxed{\rightarrow} = \mathbf{1}^{p+1};$$

note that these are of equal length $(p + 1)q$. We define the glider fleet sets

$$\mathrm{GF}_\ell = {}^\infty\mathbf{0}(\boxed{\leftarrow}\mathbf{0}\mathbf{0}^*)^*\mathbf{0}^\infty \qquad \mathrm{GF}_\mathrm{r} = {}^\infty\mathbf{0}(\mathbf{0}^*\mathbf{0}\boxed{\rightarrow})^*\mathbf{0}^\infty$$

and languages

$$L_\ell = (\boxed{\leftarrow}\mathbf{0}\mathbf{0}^*)^* \subseteq L(\mathrm{GF}_\ell) \qquad L_\mathrm{r} = (\mathbf{0}^*\mathbf{0}\boxed{\rightarrow})^* \subseteq L(\mathrm{GF}_\mathrm{r}).$$

Since $\mathcal{G}'$ is primitive, it has a mixing constant $n \geq |\mathbf{1}|^{p+2}$, i.e. a number such that for every $n' \geq n$ and $s, s' \in V'$ there is a path of length n' in $\mathcal{G}'$ from s to s'. Denote $N = 2n$ and for each $a \in E' \cup \{0_1\}$ let $W'_a = \{w_{a,1}, \ldots, w_{a,k_a}\} \subseteq E'^N$ be the set of *all* those words over E' of length N such that $w_{a,i}$ does not have prefix $\mathbf{1}^{p+2}$ and $0_p w_{a,i} a \in L(X)$ for $1 \leq i \leq k_a$, let $w_a \in E'^N$ be some single word with prefix $\mathbf{1}^{p+2}$ such that $0_p w_a a \in L(X)$ (such a word w_a exists by the choice of the mixing constant n), and denote $W_a = W'_a \cup \{w_a\}$. For each $j \in \{1, \ldots, p\}$ let $u'_j = \mathbf{1}^{p+1+j}$ and let $U'_j = \{u'_{j,1}, \ldots, u'_{j,n_j}\} \subseteq E'^+$ be *all* the cycles from s_1 to s_1 (which may visit s_1 several times) of length at most $N-1$ such that $|u'_{j,i}| \equiv |u'_j| \pmod p$ and $u'_{j,i}$ does not have prefix $\mathbf{1}^{p+2}$, with the additional restriction that $\mathbf{1}, \mathbf{1}^{p+1} \notin U'_p$. Finally, these words are padded to constant length; let $u_j = \mathbf{0}^{c_j} u'_j$ and $u_{j,i} = \mathbf{0}^{c_{j,i}} u'_{j,i}$, where $c_j, c_{j,i} \geq 100N$ are chosen in such a way that all u_j, $u_{j,i}$ are of the same length for any fixed j. The words in W_a and U'_j have been chosen so as to allow the following structural definition.

Definition 9 Let $x \notin \mathrm{GF}_\ell$ be a $\mathbf{0}$-finite element of X not in $\mathcal{O}(\mathbf{0}^\mathbb{Z})$. Then there is a maximal $i \in \mathbb{Z}$ such that

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

and there is a unique word $w \in \{\mathbf{10}\} \cup \{\mathbf{1}^{p+1}\mathbf{0}\} \cup \{\mathbf{1}^{p+2}\} \cup (\bigcup_{j=1}^{p} U'_j\mathbf{0}) \cup (\bigcup_{a \in E' \cup \{0_1\}} W'_a a)$ such that w is a prefix of $x[i,\infty]$. If $w = \mathbf{1}^{p+1}\mathbf{0}$ or $w \in U'_j\mathbf{0}$, let $k = i + |w| - 1$ and otherwise let $k = i + |\mathbf{10}| - 1$. We say that x is of *left bound type* (w,k) and that it has left bound k (note that $k > i$).

We outline a deterministic method to narrow down the word w of the previous definition in a way that clarifies its existence and uniqueness. First, by the maximality of i it follows that $x[i] \in E'$. If $x[i, i+N-1] \in E'^N$, then $w \in W'_{x[i+N]} x[i+N]$ directly by the definition of the sets W'_a *unless* $x[i,\infty]$ has prefix $\mathbf{1}^{p+2}$, in which case $w = \mathbf{1}^{p+2}$ is the only option. Otherwise $x[i, i+N-1] \notin E'^N$ and there is a minimal $m < N$ such that $x[i, i+m-1] \in E'^m$ and $x[i+m, i+m+p-1] = \mathbf{0}$. Then $x[i, i+m-1]$ is a cycle of length $m < N$ from s_1 to s_1 and $w \in U'_j\mathbf{0}$ for some $j \in \{1,\ldots,p\}$ *unless* we have specifically excluded $x[i, i+m-1]$ from all the sets U'_j. But this happens precisely if $x[i, i+m-1] \in \{\mathbf{1}, \mathbf{1}^{p+1}\}$ or $x[i, i+m-1]$ has prefix $\mathbf{1}^{p+2}$. In these cases $w \in \{\mathbf{10}, \mathbf{1}^{p+1}\mathbf{0}, \mathbf{1}^{p+2}\}$.

The point of this definition is that if x is of left bound type (w,k), then the diffusive glider automorphism g defined later will eventually create a new leftbound glider at position k and break it off from the rest of the configuration. (A possible exception to this is if $w = \mathbf{1}^{p+1}\mathbf{0} = \boxed{\rightarrow}\mathbf{0}$, in which case it might happen that the rightbound glider just travels to the right.)

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

- g_1 replaces every occurrence of $\mathbf{0}(\mathbf{0}^q\mathbf{1})\mathbf{0}$ by $\mathbf{0}(\mathbf{1}^{p+1})\mathbf{0}$ and vice versa.
- g_2 replaces every occurrence of $\mathbf{0}(\mathbf{1}^{p+1})\mathbf{0}$ by $\mathbf{0}(\mathbf{1}\mathbf{0}^q)\mathbf{0}$ and vice versa.
- g_3 replaces every occurrence of $\mathbf{0}^{q+1}(\mathbf{1}^{p+2})$ by $\mathbf{0}^{q+1}(\mathbf{1}\mathbf{0}^q\mathbf{1})$ and vice versa.
- g_4 replaces every occurrence of $\mathbf{0}w_a a$, $\mathbf{0}w_{a,i}a$ and $\mathbf{0}w_{a,k_a}a$ by $\mathbf{0}w_{a,1}a$, $\mathbf{0}w_{a,i+1}a$ and $\mathbf{0}w_a a$ respectively (for $a \in E' \cup \{0_1\}$ and $1 \leq i < k_a$) and every occurrence of $\mathbf{0}u_j\mathbf{0}$, $\mathbf{0}u_{j,i}\mathbf{0}$ and $\mathbf{0}u_{j,n_j}\mathbf{0}$ by $\mathbf{0}u_{j,1}\mathbf{0}$, $\mathbf{0}u_{j,i+1}\mathbf{0}$ and $\mathbf{0}u_j\mathbf{0}$ respectively (for $j \in \{1,\ldots,p\}$ and $1 \leq i < n_j$).

It is easy to see that these maps are well-defined automorphisms of X. The automorphism $g : X \to X$ is defined as the composition $g_4 \circ g_3 \circ g_2 \circ g_1$. We commence arguing that g is a diffusive glider automorphism with respect to $(\langle g \rangle, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$, where we choose $\varsigma_\ell = \varsigma_\mathrm{r} = g$.

Lemma 5 *If $x \in \mathrm{GF}_\ell$ (resp. $x \in \mathrm{GF}_r$), then $g(x) = \sigma^{pq}(x)$ (resp. $g(x) = \sigma^{-pq}(x)$).*

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

$$
\begin{aligned}
&x[i-p, i+(pq+q)+p-1] = \mathbf{0}\boxed{\leftarrow}\mathbf{0} = \mathbf{0}(\mathbf{0}^q\mathbf{1})\mathbf{0} \\
&g_1(x)[i-p, i+(pq+q)+p-1] = \mathbf{0}(\mathbf{1}^{p+1})\mathbf{0} \\
&g_2(g_1(x))[i-p-pq, i+q+p-1] = \mathbf{0}^q\mathbf{0}(\mathbf{10}) = \mathbf{0}\boxed{\leftarrow}\mathbf{0} \\
&g(x) = g_4(g_3(g_2(g_1(x)))) = g_2(g_1(x))),
\end{aligned}
$$

so every glider has been shifted by distance pq to the left and $g(x) = \sigma^{pq}(x)$. $\square$

We first give a heuristic argument showing that g could be a diffusive glider automorphism. It is easier to convince oneself that with the choices $g' = g_2 \circ g_1$, $G = \langle g', g_3, g_4 \rangle$ and $\varsigma'_\ell = \varsigma'_{\mathrm{r}} = g'$ the tuple $(G, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma', \mathrm{GF})$ is a diffusive glider automorphism group. Namely, the previous lemma would hold even if g were replaced by g', and it also seems reasonable that GF_ℓ, GF_{r} are glider fleet sets with respect to ς'_ℓ, ς'_{r} in the sense of Definitions 5 and 6, so g' is a glider automorphism. It remains to show diffusiveness. If $x \in X$ is $\mathbf{0}$-finite, then $x_1 = {g'}^i(x)$ for large $i \in \mathbb{N}$ contains gliders very far from the origin going to opposing directions and possibly there is an occurrence of a word $\mathbf{0}^M w$ (with large $M \in \mathbb{N}$) that does not look like a glider near the origin. Then for some j, the occurrence of this word is replaced in $x_2 = g_4^j(x_1)$ by $\mathbf{0}^{M'} \mathbf{1}^{p+2}$, and then g_3 separates an occurrence of a glider from this pattern; $x_3 = g_3(x_2)$ contains $\boxed{\leftarrow}$ near the origin which can be shifted away by sufficiently many applications of g'. By repeating this argument we find an element $\overline{g} \in G$ such that $\overline{g}(x)$ contains only leftbound gliders far to the left and rightbound gliders far to the right, so in particular the last item in Definition 5 is satisfied.

The reason why $g = g_4 \circ g_3 \circ g'$ could also have the diffusion property is that the words in points $x \in X$ on which g', g_3 and g_4 can act nontrivially are for the most part distinct, e.g. g_3 can change occurrences of the word $\mathbf{0}^{q+1}(\mathbf{1}^{p+2})$ but in the definition of g_4 this occurs as a subword only in $\mathbf{0}^{q+1} w_a a$ and $\mathbf{0} u_j \mathbf{0}$. Therefore, whenever one component in the map g does something conductive to the diffusion of x, it is unlikely that this effect is immediately reversed by some other component. We proceed with the actual proof that g is a diffusive glider automorphism.

Lemma 6 *If $x \in X$ has left bound k, then there exists $t \in \mathbb{N}_+$ such that the left bound of $g^t(x)$ is strictly greater than k. Moreover, the left bound of $g^{t'}(x)$ is at least k for all $t' \in \mathbb{N}$.*

Proof. Let $x \in X$ be of left bound type (w, k) with $w \in \{\mathbf{10}\} \cup \{\mathbf{1}^{p+1}\mathbf{0}\} \cup \{\mathbf{1}^{p+2}\} \cup (\bigcup_{j=1}^{p} U'_j \mathbf{0}) \cup (\bigcup_{a \in E' \cup \{0_1\}} W'_a a)$. The gliders to the left of the occurrence of w near k move to the left at constant speed pq under action of g without being affected by the remaining part of the configuration. We show by case analysis that the left bound of $g^t(x)$ increases for sufficiently large t. The cases from 1 to 5 correspond to different left bound types and Case 3.1 can be reached as a subcase from Case 1 and Case 3. From each case it is possible to proceed only to a case with a higher numbering, which prevents the possibility of circular arguments. The fact that the left bound never decreases can be extracted from the case analysis.

Case 1. Assume that $w = \mathbf{1}^{p+1}\mathbf{0}$. Then $g_1(x)[k - (q + 2p) + 1, k] = \mathbf{010}$ and we proceed to Case 3.1.

Case 2. Assume that $w = u'_{j,i}\mathbf{0}$ for $1 \leq j \leq p$, $1 \leq i \leq n_j$. There is a minimal $t \in \mathbb{N}$ such that $g_3(g_2(g_1(g^t(x))))[k - (2p + |u_j|) + 1, k] = \mathbf{0} u_{j,i} \mathbf{0}$. Denote

$y = g^{t+n_j-i+1}(x)$ so in particular $y[k-(2p+|u_j|)+1,k] = \mathbf{0}u_j\mathbf{0}$. Then $g(y)[-\infty,k] = g_3(g_2(g_1(y)))[-\infty,k]$ has suffix $\mathbf{0}^{q+1}\mathbf{1}\mathbf{0}^q\mathbf{1}^j\mathbf{0}$ and $g(y)$ is of left bound type $(\mathbf{1}^j\mathbf{0},k)$. If $j=1$, we proceed as in Case 3. If $j>1$, then $|\mathbf{1}^j| \equiv |\mathbf{1}^{p+j}| = |u'_{j-1}| \pmod p$ and $\mathbf{1}^j = u'_{j-1,i'} \in U'_{j-1}$ for some i'. Thus $g(y)$ is of left bound type $(u'_{j-1,i'},k)$ and we may repeat the argument in this paragraph with a smaller value of j.

Case 3. Assume that $w = \mathbf{10}$. Then $x[k-(q+2)p-q+1,k] \neq \mathbf{0}(\mathbf{0}^q\mathbf{1})\mathbf{0} = \mathbf{0}\boxed{\leftarrow}\mathbf{0}$ because otherwise the left bound of x would already be greater than k. Therefore $g_1(x)[k-(q+2p)+1,k] = \mathbf{010}$ and we proceed to Case 3.1.

Case 3.1. Assume that $g_1(x)[k-(q+2p)+1,k] = \mathbf{010}$. If $g_1(x)[k-(q+2p)+1,k+qp] = \mathbf{0}(\mathbf{10}^q)\mathbf{0}$, then $g(x)[k-(q+2p)+1,k+qp] = g_2(g_1(x))[k-(q+2p)+1,k+qp] = \mathbf{01}^{p+1}\mathbf{0}$ so $g(x)$ is of left bound type $(\mathbf{1}^{p+1}\mathbf{0},k+qp)$ and we are done. Let us therefore assume that $g_1(x)[k-(q+2p)+1,k+qp] \neq \mathbf{0}(\mathbf{10}^q)\mathbf{0}$, in which case $g_2(g_1(x))[k-(q+2p)+1,k] = \mathbf{010}$. Denote $y = g_3(g_2(g_1(x)))$.

If $y[k-(q+2p)+1,k] = \mathbf{010}$, then $g(x)[-\infty,k] = g_4(y)[-\infty,k] \in {}^{\infty}\mathbf{0}L_\ell$ and $g(x)$ has left bound strictly greater than k. Otherwise $y[k-(q+2p)+1,k+(-p+(p+1)q)] = \mathbf{01}^{p+2}$. If $y[-\infty,k+(p+j)q]$ has suffix $\mathbf{0}u_j\mathbf{0}$ for some $j \in \{1,\dots,p\}$, then $g(x)[-\infty,k+(p+j)q]$ has suffix $\mathbf{0}u_{j,1}\mathbf{0}$, $g(x)$ is of left bound type $(u'_{j,1}\mathbf{0},k+(p+j)q)$ and we are done. On the other hand, if $y[-\infty,k+(p+j)q]$ does not have suffix $\mathbf{0}u_j\mathbf{0}$ for any j, then $g(x)$ is of left bound type (w',k) for some $w' \in W'_a a \cup \{\mathbf{1}^{p+2}\}$ ($a \in E' \cup \{0_1\}$) and we proceed as in Case 4 or Case 5.

Case 4. Assume that $w = w_{a,i}a$ for $a \in E' \cup \{0_1\}$ and $1 \leq i \leq k_a$. Then $g^{k_a-i+1}(x)[k-|\mathbf{10}|+1,\infty]$ has prefix $\mathbf{1}^{p+2}$ and we proceed as in Case 5.

Case 5. Assume that $w = \mathbf{1}^{p+2}$. Then $g_2(g_1(x))[k-(q+2)p-q+1,k-p+(p+1)q] = \mathbf{0}^{q+1}(\mathbf{1}^{p+2})$, $g_3(g_2(g_1))[k-(q+2)p-q+1,k-p+(p+1)q] = \mathbf{0}^{q+1}(\mathbf{10}^q\mathbf{1}) = \mathbf{0}\boxed{\leftarrow}\mathbf{0}^q\mathbf{1}$ and the left bound of $g(x)$ is strictly greater than $k+(q-1)p$.

□

Definition 10 Let $x \notin \mathrm{GF_r}$ be a $\mathbf{0}$-finite element of X not in $\mathcal{O}(\mathbf{0}^{\mathbb{Z}})$. Then there is a minimal $k \in \mathbb{Z}$ such that

$$x[k+1,\infty] \in L_{\mathrm{r}}\mathbf{0}^{\infty}$$

and we say that x has right bound k.

Lemma 7 *If $x \in X$ has right bound k, then there exists $t \in \mathbb{N}_+$ such that the right bound of $g^t(x)$ is strictly less than k. Moreover, the right bound of $g^{t'}(x)$ for $0 \leq t' \leq t$ is at most $k+C$ for some C that does not depend on x, k or t.*

Proof. We prove that the right bound of $g^t(x)$ eventually decreases by case analysis and that we can choose $C = pq$. The constant C does not play any role in the first case but it can be extracted from the second case and its subcases.

Case 1. Assume that the right bound of $g^t(x)$ is at most k for every $t \in \mathbb{N}_+$. By the previous lemma the left bound of $g^t(x)$ tends to ∞ as t tends to ∞, which means that for some $t \in \mathbb{N}_+$ $g^t(x)$ contains only $\boxed{\leftarrow}$-gliders to the left of $k + 3pq$ and only $\boxed{\rightarrow}$-gliders to the right of k. This can happen only if $g^t(x)[k+1, k+3pq-1]$ does not contain any glider of either type. Then the right bound of $g^{t+1}(x)$ is at most $k - pq$ and we are done.

Case 2. Assume that the right bound of $g^t(x)$ is strictly greater than k for some $t \in \mathbb{N}_+$ and fix the minimal such t. This can happen only if $g_1(g^{t-1}(x))[k-(p+q)+1, k+(q+1)p] = \mathbf{0}\mathbf{1}\mathbf{0}^q\mathbf{0}$ and then $g_2(g_1(g^{t-1}(x)))[k-(p+q)+1, k+(q+1)p] = \mathbf{0}\mathbf{1}^{p+1}\mathbf{0}$. We proceed to Case 2.1 or Case 2.2.

Case 2.1. Assume that $g_2(g_1(g^{t-1}(x)))[-\infty, k+(q+1)p]$ does not have suffix $\mathbf{0}^{q+1}\mathbf{1}\mathbf{0}^q\mathbf{1}^{p+1}\mathbf{0}$. Then $g_3(g_2(g_1(g^{t-1}(x))))[-\infty, k+(q+1)p]$ and $g^t(x)[-\infty, k+(q+1)p]$ have suffix $\mathbf{0}\mathbf{1}^{p+1}\mathbf{0} = \mathbf{0}\boxed{\rightarrow}\mathbf{0}$. This contradicts the choice of t, because the right bound of $g^t(x)$ is at most $k-(p+q)$.

Case 2.2. Assume that $g_2(g_1(g^{t-1}(x)))[-\infty, k+(q+1)p]$ has suffix $\mathbf{0}^{q+1}\mathbf{1}\mathbf{0}^q\mathbf{1}^{p+1}\mathbf{0}$. Then $g_3(g_2(g_1(g^{t-1}(x))))[-\infty, k+qp]$ and $g^t(x)[-\infty, k+qp]$ have suffix $\mathbf{0}^{q+1}(\mathbf{1}^{2p+2})$ and the configuration $g^t(x)$ has right bound $k+pq$. By the previous lemma the left bound of $g^s(x)$ tends to ∞ as s tends to ∞, so we may fix a minimal $s > t$ such that $g^s(x)[k+qp-q, k+qp] \notin E'^{q+1}$. We proceed to Case 2.2.1 or Case 2.2.2.

Case 2.2.1. Assume that $g^{t'}(x)[k-(p+q)+1, k+qp] = \mathbf{0}\mathbf{1}^{p+1} = \mathbf{0}\boxed{\rightarrow}$ for some $t < t' < s$ and fix the minimal such t'. Then the right bound of $g^{t'}(x)$ is at most $k-(p+q) < k$ and we are done.

Case 2.2.2. Assume that $g^{t'}(x)[k-(p+q)+1, k+qp] \neq \mathbf{0}\mathbf{1}^{p+1}$ for all $t < t' < s$, so in particular $g^{s-1}(x)[k-(p+q)+1, k+qp] \neq \mathbf{0}\mathbf{1}^{p+1}$ and from $g^{s-1}(x)[k+qp-q, k+qp] \in E'^{q+1}$ it follows that $g^{s-1}(x)[k-(p+q)+1, k+qp] \neq \mathbf{0}^{q+1}\mathbf{1}$. Therefore $g_1(g^{s-1}(x))[k+qp-q, k+qp] \in E'^{q+1}$, $g_1(g^{s-1}(x))[k-(p+1)+1, k+qp] \neq \mathbf{0}\mathbf{1}^{p+1}$ and thus $g_2(g_1(x))[k+qp-q, k+qp] \in E'^{q+1}$. By the choice of s, the map g_3 must act now so that $g_3(g_2(g_1(g^{s-1}(x))))[-\infty, k+qp]$ and $g^s(x)[-\infty, k+qp]$ have suffix $\mathbf{0}^{q+1}\mathbf{1}\mathbf{0}^q\mathbf{1}$. Then $g_1(g^s(x))[-\infty, k+qp+(q+1)p]$ has suffix $\mathbf{0}\mathbf{1}^{p+1}\mathbf{0}^q\mathbf{1}\mathbf{0}^{q+1}$ and $g^{s+1}(x)[-\infty, k+qp+(q+1)p]$ has suffix $\mathbf{0}^q\mathbf{0}^q\mathbf{1}^{p+1}\mathbf{0} = \mathbf{0}^{2q}\boxed{\rightarrow}\mathbf{0}$. Therefore the right bound of $g^{s+1}(x)$ is at most $k-(p+1)q < k$ and we are done.

□

Lemma 8 *If $x \in X$ is a $\mathbf{0}$-finite configuration, then for every $M \in \mathbb{N}$ there exist $t, N_\ell, N_r, M' \in \mathbb{N}$, $N_\ell, N_r \geq M$ such that $g^t(x)[-N_\ell, N_r] = \mathbf{0}^{M'}$, $g^t(x)[-\infty, -(N_\ell+1)] \in {}^\infty\mathbf{0}L_\ell$ and $g^t(x)[N_r+1, \infty] \in L_r\mathbf{0}^\infty$.*

Proof. By inductively applying the previous two lemmas we see that if $t \in \mathbb{N}_+$ tends to ∞, then the left bound (resp. the right bound) of $g^t(x)$ tends to ∞ (resp. to $-\infty$). □

Theorem 2 *The map g is a diffusive glider automorphism associated to the tuple $(\langle g \rangle, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ constructed in this section.*

Proof. By Lemma 5 we know that for $i \in \mathcal{I}$,

$$\mathrm{GF}_i \subseteq \{x \in X \mid x \text{ is } \mathbf{0}\text{-finite and } g(x) = \sigma^{\mathrm{spd}(i)}(x)\} \doteqdot S_i.$$

We prove the other inclusion when $i = \ell$, the case $i = \mathrm{r}$ being similar. Assume therefore that $x \notin \mathrm{GF}_\ell$ is $\mathbf{0}$-finite and apply the previous lemma for sufficiently large M. By Lemma 5 the set GF_i is invariant under the map g, so $g^t(x) \notin \mathrm{GF}_\ell$ and $g^t(x)$ contains an occurrence of $\boxed{\rightarrow}$ which is shifted to the right by the map g. Therefore $g(g^t(x)) \neq \sigma^{pq}(g^t(x)) = \sigma^{\mathrm{spd}(\ell)}(g^t(x))$ and $g^t(x) \notin S_\ell$. Since S_ℓ is invariant under the map g, it follows that $x \notin S_\ell$.

The other conditions necessary for showing that g is a glider automorphism are easy to check. Then the fact that g is a diffusive glider automorphism follows from the previous lemma. □

5 Finitary Ryan's Theorem for Transitive SFTs

In this section we prove our finitary version of Ryan's theorem. This is done by applying Lemma 1. As in Example 3, we need a suitable automorphism f to augment the diffusive glider automorphism group of Theorem 2.

As earlier, let X be a mixing SFT from the conclusion of Lemma 4 and consider the notation of the previous section. First we define maps $f_1, f_2 : X \to X$ as follows. In any $x \in X$,

- f_1 replaces every occurrence of $\mathbf{0}\boxed{\rightarrow}\mathbf{000}\boxed{\leftarrow}\mathbf{0}$ by $\mathbf{0}\boxed{\rightarrow}\mathbf{00}\boxed{\leftarrow}\mathbf{00}$ and vice versa
- f_2 replaces every occurrence of $\mathbf{0}\boxed{\rightarrow}\mathbf{00}\boxed{\leftarrow}\mathbf{0}$ by $\mathbf{00}\boxed{\rightarrow}\mathbf{0}\boxed{\leftarrow}\mathbf{0}$ and vice versa.

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 $f_2 \circ f_1$. Similarly to Example 3, f has the following properties. First, it replaces any occurrence of $\mathbf{0}\boxed{\rightarrow}\mathbf{000}\boxed{\leftarrow}\mathbf{0}$ by $\mathbf{00}\boxed{\rightarrow}\mathbf{0}\boxed{\leftarrow}\mathbf{00}$. Second, if $x \in X$ is a configuration containing only gliders $\boxed{\leftarrow}$ and $\boxed{\rightarrow}$ and every occurrence of $\boxed{\leftarrow}$ is sufficiently far from every occurrence of $\boxed{\rightarrow}$, then $f(x) = x$.

Proposition 1 *Let $X \subseteq A^{\mathbb{Z}}$ and $g, f : X \to X$ be as above. Then $C(\langle g, f\rangle) = \langle \sigma \rangle$.*

Proof. Consider the diffusive glider automorphism group $(\langle g \rangle, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ from Theorem 2. If we define $G = \langle g, f\rangle$, then it directly follows that $(G, \mathbf{0}, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ is also a diffusive glider automorphism group of X. We want to use Lemma 1 to show that $C(G) \cap \mathrm{Aut}(X, \mathbf{0}) = \langle \sigma \rangle$. The bipartite graph $\mathcal{B}$ in the statement of the lemma has in this case the set of vertices $\mathcal{I} = \{\mathrm{r}, \ell\}$ with the partition $\mathcal{I}_1 = \{\mathrm{r}\}$ and $\mathcal{I}_2 = \{\ell\}$, so it suffices to show that there is an edge between r and ℓ.

Recall that we denote $p = |\mathbf{0}|$, $q = |\mathbf{1}|$. Using the same notation as in the statement of Lemma 1, let $d = e = 1$, $(N_m)_{m\in\mathbb{N}}$ with $N_m = 2mq + 3$ and $(g'_m)_{m\in\mathbb{N}}$ with $g'_m = g^{-(m+1)} \circ f \circ g^m$. Let $x\boxed{\rightarrow} \in {}^\infty\mathbf{0}L_r$, $\boxed{\leftarrow}y \in L_\ell\mathbf{0}^\infty$ be arbitrary. Fix some $m \in \mathbb{N}$. Since X is an edge shift, it is clear that $x\boxed{\rightarrow}.\mathbf{0}^{N_m}\boxed{\leftarrow}y \in X$ and it is easy to verify that

- $g'_m(x\boxed{\rightarrow}.\mathbf{0}^N\boxed{\leftarrow}y) = x\boxed{\rightarrow}\mathbf{0}.\mathbf{0}^N\mathbf{0}\boxed{\leftarrow}y$ for $N > N_m$
- $g'_m(x\boxed{\rightarrow}.\mathbf{0}^{N_m}\boxed{\leftarrow}y) = x\mathbf{0}\boxed{\rightarrow}.\mathbf{0}^{N_m}\boxed{\leftarrow}\mathbf{0}y$.

It follows that there is an edge between r and ℓ, so $C(G) \cap \mathrm{Aut}(X, \mathbf{0}) = \langle\sigma\rangle$.

Now let $h \in C(G)$ be arbitrary. Let us show that $h \in \mathrm{Aut}(X, \mathbf{0})$. Namely, assume to the contrary that $h(\mathbf{0}^{\mathbb{Z}}) = w^{\mathbb{Z}} \notin \mathcal{O}(\mathbf{0}^{\mathbb{Z}})$ for some $w = w_1 \cdots w_p$ ($w_i \in A$). The maps g_k in the definition of g have been defined so that $g_k(x)[i] = x[i]$ whenever x contains occurrences of $\mathbf{0}$ only at positions strictly greater than i, so in particular $g(w^{\mathbb{Z}}) = w^{\mathbb{Z}}$. Consider $x = {}^\infty\mathbf{0}.\boxed{\leftarrow}\mathbf{0}^\infty \in \mathrm{GF}_\ell$ with the glider $\boxed{\leftarrow}$ at the origin. Note that $h(x)[(i-1)p, ip-1] \neq w$ for some $i \in \mathbb{Z}$ (otherwise $h(x) = w^{\mathbb{Z}} = h(\mathbf{0}^{\mathbb{Z}})$, contradicting the injectivity of h) and $h(x)[-\infty, ip-(jq)p-1] = \cdots www$ for some $j \in \mathbb{N}_+$. By the earlier observation on the maps g_k it follows that $g^t(h(x))[-\infty, ip-(jq)p-1] = \cdots www$ for every $t \in \mathbb{Z}$ but $h(g^j(x))[ip-(j+1)qp, ip-(jq)p-1] = h(\sigma^{(pq)j}(x))[ip-(j+1)qp, ip-(jq)p-1] = h(x)[ip-qp, ip-1] \neq w^q$, contradicting the commutativity of h and g. Thus $h \in \mathrm{Aut}(X, \mathbf{0})$.

We have shown that $h \in C(G) \cap \mathrm{Aut}(X, \mathbf{0}) = \langle\sigma\rangle$, so we are done. □

Theorem 3 $k(X) = 2$ *for every nontrivial mixing SFT* X.

Proof. Every nontrivial mixing SFT is conjugate to a subshift X of the form given in the conclusion of Lemma 4, so $k(X) \leq 2$ follows from the previous proposition. Clearly $\mathrm{Aut}(X) \neq \langle\sigma\rangle$, so by Theorem 1 it is not possible that $k(X) < 2$ and therefore $k(X) = 2$. □

Corollary 1 (Finitary Ryan's theorem) $k(X) = 2$ *for every transitive SFT* X *which is not the orbit of a single point.*

Proof. Let X be a transitive SFT given as the edge subshift of a graph $\mathcal{G} = (V, E)$ containing more than a single cycle. By Section 4.5 in [4] there is a partition $E = \bigcup_{i=1}^n E_n$ with the following properties. First, the ending states of E_i can be starting states only for edges of E_{i+1} (where $i+1$ is considered modulo n) and this induces a partition $X = \bigcup_{i=1}^n X_i$ such that $X_i = \{x \in X \mid x[0] \in E_i\}$ and $\sigma(X_i) = X_{i+1}$. Second, the edge shift X' of the graph $\mathcal{G}' = (V', E')$ is a nontrivial mixing SFT where $V' \subseteq V$ contains the starting states of edges in E_1 and E' contains all paths $w = w_1 \cdots w_n$ of length n in $\mathcal{G}$ with $w_1 \in E_1$ and we let $\iota(w) = \iota(w_1)$, $\tau(w) = \tau(w_n)$. There is a natural homeomorphism $\phi : X' \to X_1$ such that $\phi \circ \sigma = \sigma^n \circ \phi$. By the previous theorem there are $f'_1, f'_2 \in \mathrm{Aut}(X')$ which commute with only $\langle\sigma_{X'}\rangle$ and there are unique $f_1, f_2 \in \mathrm{Aut}(X)$ such that $f_{i\restriction X_1} = \phi \circ f'_i \circ \phi^{-1}$. By Theorem 1 it remains to show that $C(\{f_1, f_2\}) = \langle\sigma\rangle$. Assume therefore that h commutes with f_1 and f_2 and without loss of generality (by composing h with some power of σ_X if necessary) that $h(X_1) = X_1$. There is $h' \in \mathrm{Aut}(X')$ commuting with f'_i such that $\phi \circ h' = h \circ \phi$. It follows that $h' = \sigma^k_{X'}$ and $h = \sigma^{nk}_X$. □

6 A Nontrue Finitary Version of Ryan's Theorem

Finitary Ryan's theorem can be interpreted as a compactness result saying that, for nontrivial mixing SFT X, the group $\mathrm{Aut}(X)$ has a finite subset S such that $C(S) = \langle\sigma\rangle$. One may wonder whether this compactness phenomenon is more general: if $G \subseteq \mathrm{Aut}(X)$ is an arbitrary infinite set such that $C(G) = \langle\sigma\rangle$, does there exist a finite $F \subseteq G$ such that $C(F) = \langle\sigma\rangle$? We will show by an example that this is not true for general G even if X is the binary full shift.

In this section let $X = \{0,1\}^{\mathbb{Z}}$. For every $n \in \mathbb{N}_+$ we define two automorphisms $g_{n,1}, g_{n,2} : X \to X$ as follows. In any $x \in X$,

- $g_{n,1}$ replaces every occurrence of $001^{2n-1}0$ by $011^{2n-1}0$ and vice versa.
- $g_{n,2}$ replaces every occurrence of $01^{2n-1}10$ by $01^{2n-1}00$ and vice versa.

It is easy to see that these maps are well-defined automorphisms of X. The maps $g_n : X \to X$ are defined as the compositions $g_{n,2} \circ g_{n,1}$. We will define a tuple $(G', 0, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$, which will turn out to be a diffusive glider automorphism group for the binary full shift X. Let $G' = \langle\{g_n \mid i \in \mathbb{N}_+\}\rangle$ and let $\mathcal{I} = \{(n,\mathrm{r}) \mid n \in \mathbb{N}_+\} \cup \{(n,\ell) \mid n \in \mathbb{N}_+\}$ be the index set. We define gliders $\boxed{\leftrightarrow}_{n,\ell} = \boxed{\leftarrow}_n = 01^{2n-1}$ and $\boxed{\leftrightarrow}_{n,\mathrm{r}} = \boxed{\rightarrow}_n = 1^{2n}$ and glider fleet sets

$$\mathrm{GF}_{n,\ell} = {}^{\infty}0(\boxed{\leftarrow}_n 00^*)^* 0^{\infty} \qquad \mathrm{GF}_{n,\mathrm{r}} = {}^{\infty}0(0^*0\boxed{\rightarrow}_n)^* 0^{\infty}.$$

We define languages

$$L_{n,\ell} = (\boxed{\leftarrow}_n 00^*)^* \qquad L_{n,\mathrm{r}} = (0^*0\boxed{\rightarrow}_n)^*.$$

For $n \in \mathbb{N}_+$ we let $\mathrm{spd}(n,\ell) = 1$, $\mathrm{spd}(n,\mathrm{r}) = -1$ and $\varsigma_{(n,\mathrm{r})} = \varsigma_{(n,\ell)} = g_n$.

Lemma 9 *The tuple $(G', 0, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ defined above is a glider automorphism group of X, i.e. for $n \in \mathbb{N}_+$*

- *$\mathrm{GF}_{n,\ell}$ is the set of 0-finite configurations x for which $g_n(x) = \sigma(x)$*
- *$\mathrm{GF}_{n,r}$ is the set of 0-finite configurations x for which $g_n(x) = \sigma^{-1}(x)$.*

Proof. We prove the first claim, the proof of the second claim being similar. Assume first that $x \in \mathrm{GF}_{n,\ell}$ and assume that $i \in \mathbb{Z}$ is some position in x where $\boxed{\leftarrow}_n$ occurs. Then

$$\begin{aligned}
&x[i-1, i+2n] = 0\boxed{\leftarrow}_n 0 = 0(01^{2n-1})0 \\
&g_{n,1}(x)[i-1, i+2n] = 0(1^{2n})0 \\
&g_n(x)[i-2, i+2n-1] = g_{n,2}(g_{n,1}(x))[i-2, i+2n-1] \\
&= 00(1^{2n-1}0) = 0\boxed{\leftarrow}_n 0,
\end{aligned}$$

so every glider has been shifted by distance 1 to the left and $g_n(x) = \sigma(x)$.

Assume next that $x \in X$ is 0-finite and $g_n(x) = \sigma(x)$. First of all, x cannot contain an occurrence of the pattern $01^{n'}0$ at any position $i \in \mathbb{Z}$ for any $n' \notin \{2n-1, 2n\}$, because otherwise $x[i, i+n'+1] = g_n(x)[i, i+n'+1] = 01^{n'}0$. Second, if x contains an occurrence of the pattern $01^{2n}0$ at a position $i \in \mathbb{Z}$, then $g_{n,1}(x)[i, i+2n+1] = 001^{2n-1}0$ and $g_n(x)[i+1] = 0$, which contradicts $g_n(x)[i+1] = \sigma(x)[i+1] = 1$. Therefore, every occurrence of 1 in x is part of a segment of exactly $2n-1$ consecutive ones. If it were that $x \notin \mathrm{GF}_{n,\ell}$, then x would contain an occurrence of the pattern $101^{2n-1}0$ at some position i. Then $g_{n,1}(x)[i, i+2n+1] = 101^{2n-1}0$ and $g_n(x)[i+1] = 0$, which contradicts $g_n(x)[i+1] = \sigma(x)[i+1] = 1$. $\square$

Lemma 10 *The tuple* $(G', 0, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ *defined above is a diffusive glider automorphism group of* X*.*

Proof. By the previous lemma G' is a glider automorphism group. For the diffusion property it is sufficient to prove for all 0-finite $x \in X$ and $N \in \mathbb{N}$ the existence of a $g \in G'$ such that $g(x) \in {}^{\infty}0((\cup_{i \in S} L_i)0^N)^* 0^{\infty}$. To do this we define for every 0-finite $x \in X$ the quantity

$$N_x = \sum_{i=1}^{\infty} |\operatorname{occ}_{\ell}(x, 01^n 0)|,$$

i.e. the total number of consecutive runs of ones in x. We remark that $N_x = N_{g(x)}$ for $g \in G'$, because this clearly holds for $g \in \{g_{n,1}, g_{n,2} \mid n \in \mathbb{N}_+\}$ and these generate a group containing G'. We prove the diffusion property by induction on N_x. As the base case we choose $x \in \mathrm{GF}_s$ ($s \in \mathcal{I}$), for which the claim is trivial. Assume therefore that $x \notin \mathrm{GF}_s$ for all $s \in \mathcal{I}$ and fix $N \in \mathbb{N}$. If the leftmost occurrence of 1 in x is at position $i \in \mathbb{Z}$, then $x[i-1, \infty]$ has the prefix $01^{2n-1}0$ or $01^{2n}0$ for some $n \in \mathbb{N}_+$. We assume without loss of generality that the prefix is of the form $01^{2n-1}0$ (otherwise in the following we replace the map g_n by its inverse g_n^{-1}).

Note that by definition g_n treats words of the form $01^{2n-1}0$ and $01^{2n}0$ in all 0-finite $y \in X$ as gliders which rebound from words of the form $01^{2n'-1}0$ and $01^{2n'}0$ ($n' \neq n$) that remain stationary under the action of g_n. For every $t \in \mathbb{N}$ there is a maximal $i_t \in \mathbb{Z}$ such that $g_n^t(x)[-\infty, i_t] \in {}^{\infty}0(\boxed{\leftarrow}_n 00^*)^*$, so fix $t' \in \mathbb{N}$ such that $g_n^{t'}(x)[-\infty, i_{t'}]$ contains a maximal number of occurrences of $\boxed{\leftarrow}_n$. It is easy to see that also every $t \geq t'$ has this property. Similarly, for every $t \in \mathbb{N}$ there is a minimal $j_t \in \mathbb{Z}$ such that $g_n^t(x)[j_t, \infty] \in (0^*0\boxed{\rightarrow}_n)^* 0^{\infty}$, so fix $t \geq t'$ such that $g_n^t[j_t, \infty] \in (0^*0\boxed{\rightarrow}_n)^* 0^{\infty}$ contains a maximal number of occurrences of $\boxed{\rightarrow}_n$. If $j_t \leq i_t$, this indicates that $g_n^t(x)$ is of the form $g_n^t(x) \in {}^{\infty}0(0^*0\boxed{\leftarrow}_n)^*(0^*0\boxed{\rightarrow}_n)^* 0^{\infty}$ and therefore $g_n^T(x) \in {}^{\infty}0(0^*0\boxed{\leftarrow}_n)^* 0^N (0^*0\boxed{\rightarrow}_n)^* 0^{\infty}$ for sufficiently large $T \in \mathbb{N}$, proving our claim. Let us therefore assume in the following that $i_t < j_t$.

Let $y = g_n^t(x)$ and $y = y_1 \otimes_{i_t+1} y_2 \otimes_{j_t} y_3$, where y_1 (resp. y_2 or y_3) agrees with y on the interval $(-\infty, i_t]$ (resp. on the interval (i_t, j_t) or $[j_t, \infty)$) and contains zeroes at all other positions. By the choice of t, i_t, and j_t it follows that

$$g_n^T(y) = \sigma^T(y_1) \otimes_{i_t+1} g_n^T(y_2) \otimes_{j_t} \sigma^{-T}(y_3)$$

and $\mathrm{supp}(g_n^T(y_2)) \subseteq (i_t, j_t)$ for every $T \in \mathbb{N}$, where we denote $\mathrm{supp}(x) = \{i \in \mathbb{Z} \mid x[i] \neq 0\}$ for $x \in X$. Since $N_x = N_{g_n^T(x)} < N_{g_n^T(y_2)}$, it follows from the induction assumption that for every $T \in \mathbb{N}$ there is $g_T \in \mathrm{Aut}(X)$ such that

$$g_T(g_n^T(y_2)) \in {}^{\infty}0((\cup_{i \in S} L_i)0^N)^* 0^{\infty}.$$

Furthermore all g_T can be chosen so that they are all radius-r automorphisms for some uniform $r \in \mathbb{N}_+$, since there are only finitely many different configurations $g_n^T(y_2)$. Fix therefore $T = 2r + N$. Note also that $g(\mathrm{GF}_{n,\mathrm{r}} \cup \mathrm{GF}_{n,\ell}) =$

$\mathrm{GF}_{n,\mathrm{r}} \cup \mathrm{GF}_{n,\ell}$ for $g \in G'$, because this clearly holds for $g \in \{g_{n',1}, g_{n',2} \mid n' \in \mathbb{N}_+\}$. We see that

$$\begin{aligned} g_T(g_n^T(y)) &= g_T(\sigma^T(y_1)) \otimes_{i_t+1-r} g_T(g_n^T(y_2)) \otimes_{j_t+r} g_T(\sigma^{-T}(y_3)) \\ &\in {}^{\infty}0(L_{n,\ell} \cup L_{n,\mathrm{r}})0^N((\cup_{i\in S} L_i)0^N)^* 0^N (L_{n,\mathrm{r}} \cup L_{n,\ell})0^{\infty}; \end{aligned}$$

which proves our induction step. □

We construct the group G generated by G' and all automorphisms $f_{n,m} = f_{n,m,2} \circ f_{n,m,1}$ for $n, m \in \mathbb{N}_+$ defined as follows. In any $x \in X$,

- $f_{n,m,1}$ replaces every occurrence of $0\boxed{\rightarrow}_n 000\boxed{\leftarrow}_m 0$ by $0\boxed{\rightarrow}_n 00\boxed{\leftarrow}_m 00$ and vice versa
- $f_{n,m,2}$ replaces every occurrence of $0\boxed{\rightarrow}_n 00\boxed{\leftarrow}_m 0$ by $00\boxed{\rightarrow}_n 0\boxed{\leftarrow}_m 0$ and vice versa.

It is easy to see that these maps are well-defined automorphisms of X. Similarly to Example 3, the map $f_{n,m}$ has two important properties. First, it replaces any occurrence of $0\boxed{\rightarrow}_n 000\boxed{\leftarrow}_m 0$ by $00\boxed{\rightarrow}_n 0\boxed{\leftarrow}_m 00$. Second, if $x \in X$ is a configuration containing only gliders $\boxed{\leftarrow}_m$ and $\boxed{\rightarrow}_n$ and every occurrence of $\boxed{\leftarrow}_m$ is sufficiently far from every occurrence of $\boxed{\rightarrow}_n$, then $f_{n,m}(x) = x$.

The following two propositions conclude our current example.

Proposition 2 $C(G) = \langle \sigma \rangle$

Proof. Since $G' \subseteq G$, it follows from the previous lemma that $(G, 0, \mathcal{I}, \boxed{\leftrightarrow}, \mathrm{spd}, \varsigma, \mathrm{GF})$ is also a diffusive glider automorphism group of X. We want to use Lemma 1 to show that $C(G) \cap \mathrm{Aut}(X, 0) = \langle \sigma \rangle$. The bipartite graph $\mathcal{B}$ in the statement of the lemma has in this case the set of vertices $\mathcal{I}$ with the partition $\mathcal{I}_1 = \{(n, \mathrm{r}) \mid n \in \mathbb{N}\}$ and $\mathcal{I}_2 = \{(n, \ell) \mid n \in \mathbb{N}\}$, so it suffices to show that there is an edge between (n, r) and (k, ℓ) for any fixed $n, k \in \mathbb{N}_+$.

Using the same notation as in the statement of Lemma 1, let $d = e = 1$ and $(N_m)_{m\in\mathbb{N}}$ with $N_m = 2m+3$. Let $g_{n,k} = g_n$ if $n = k$, $g_{n,k} = g_n \circ g_k$ if $n \neq k$ and let $(g'_m)_{m\in\mathbb{N}}$ with $g'_m = g_{n,k}^{-(m+1)} \circ f_{n,k} \circ g_{n,k}^m$. Let $x\boxed{\rightarrow}_n \in {}^{\infty}0L_{n,\mathrm{r}}$ and $\boxed{\leftarrow}_k y \in L_{k,\ell}0^{\infty}$ be arbitrary. Fix some $m \in \mathbb{N}$. It is clear that $x\boxed{\rightarrow}_n.0^{N_m}\boxed{\leftarrow}_k y \in X$ and it is easy to verify that

- $g'_m(x\boxed{\rightarrow}_n.0^N\boxed{\leftarrow}_k y) = x\boxed{\rightarrow}_n 0.0^N 0\boxed{\leftarrow}_k y$ for $N > N_m$
- $g'_m(x\boxed{\rightarrow}_n.0^{N_m}\boxed{\leftarrow}_k y) = x0\boxed{\rightarrow}_n.0^{N_m}\boxed{\leftarrow}_k 0y$.

It follows that there is an edge between (n, r) and (k, r), so $C(G) \cap \mathrm{Aut}(X, 0) = \langle \sigma \rangle$.

Now let $h \in C(G)$ be arbitrary. Let us show that $h \in \mathrm{Aut}(X, 0)$. Namely, if it were that $h(0^{\mathbb{Z}}) = 1^{\mathbb{Z}}$, consider $x = {}^{\infty}0.\boxed{\leftarrow}_1 0^{\infty}$ with the glider $\boxed{\leftarrow}_1 = 01$ at the origin and note that $h(x)[i] = 0$ for some $i \in \mathbb{Z}$ and $h(x)[-\infty, j] = {}^{\infty}1$ for some $j \in \mathbb{N}_+$. Then $g_1^t(h(x))[-\infty, j] = {}^{\infty}1$ for every $t \in \mathbb{Z}$ but $h(g_1^{i-j}(x))[j] = h(\sigma^{i-j}(x))[j] = h(x)[i] = 0 \neq 1$, contradicting the commutativity of h and g_1. Thus $h \in \mathrm{Aut}(X, 0)$.

We have shown that $h \in C(G) \cap \mathrm{Aut}(X, 0) = \langle \sigma \rangle$, so we are done. □

Proposition 3 *If $F \subset G$ is finite, then $C(F) \supsetneq \langle\sigma\rangle$.*

Proof. Fix some finite $F \subseteq G$. It is a simple observation that for every $f \in F$ there is n_f such that f does not change occurrences of the words $u_n = 01^{n+1}00^n01^{n+1}0$ and $v_n = 01^{n+1}01^n01^{n+1}0$ in any configurations for $n \geq n_f$. Let $n = \max_{f \in F}\{n_f\}$ and let $h \in \mathrm{Aut}(X)$ be the automorphism that replaces every occurrence of u_n by v_n (and vice versa) in any configuration $x \in X$. Now it is evident that $h \in C(F)$ even though $h \notin \langle\sigma\rangle$. □

7 Conclusions

We have constructed diffusive glider automorphisms g for nontrivial mixing SFTs X (with some fixed periodic point $\mathbf{0}^{\mathbb{Z}}$) that decompose all $\mathbf{0}$-finite configurations into two fleets of gliders traveling into opposing directions. This construction was somewhat complicated and finding a simpler construction (and/or a simpler proof) would be desirable. One might also want to construct diffusive glider automorphisms on general mixing SFTs with several different types of gliders that travel at different speeds and that would satisfy some carefully specified collision rules (this is simpler on full shifts when the cardinality of the alphabet is not a prime, see e.g. [7] for the case of the full shift $A^{\mathbb{Z}}$ with $|A| = 16$).

We have applied these glider maps to prove for any nontrivial mixing SFT X that $k(X) = 2$. As a simple corollary we have also shown that $k(X) = 2$ for any transitive SFT X that consists of more than a single orbit. It would be interesting to find more sensitive isomorphism invariants of $\mathrm{Aut}(X)$. As one possible invariant related to $k(X)$ we suggest

$$k_2(X) = \min\{|S| \mid S \subseteq \mathrm{Aut}(X) \text{ contains only involutions and } C(S) = \langle\sigma\rangle\}.$$

It is previously known by Theorem 7.17 of [6] that $k_2(A^{\mathbb{Z}}) \in \mathbb{N}$ when $|A| = 4$. Some upper bounds for this quantity for general transitive SFTs can be given by noting that the automorphisms in Proposition 1 can be represented as compositions of involutions. However, it might be difficult to recognize an optimal upper bound when it has been found. For example, we do not know the answer to the following.

Problem 1 Does there exist a mixing SFT X such that $k_2(X) = 2$? Do all mixing SFTs have this property?

We have also given an example of a finitary variant of Ryan's theorem which is not true, i.e. there exists $G \subseteq \mathrm{Aut}(\{0,1\}^{\mathbb{Z}})$ such that $C(G) = \langle\sigma\rangle$ but $C(F) \supsetneq \langle\sigma\rangle$ for every finite $F \subseteq G$.

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

References

1. M. Boyle: *Open problems in symbolic dynamics.* Geometric and probabilistic structures in dynamics, Contemp. Math. 469, 69–118, Amer. Math. Soc., Providence, RI (2008).
2. M. Boyle, D. Lind, D. Rudolph: *The automorphism group of a shift of finite type.* Transactions of the American Mathematical Society 306(1), 71–114 (1988)
3. J. Kopra: *Glider Automorphisms on Some Shifts of Finite Type and a Finitary Ryan's Theorem.* In: Cellular Automata and Discrete Complex Systems. Lecture Notes in Computer Science vol 10875, 88–99 (2018)
4. D. Lind, B. Marcus: *An introduction to symbolic dynamics and coding.* Cambridge University Press, Cambridge (1995)
5. J. Patrick Ryan: *The shift and commutativity.* Mathematical systems theory 6 (1-2), 82–85 (1972)
6. V. Salo: *Transitive action on finite points of a full shift and a finitary Ryan's theorem.* arXiv:1610.05487v2 (2017)
7. 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)