

THE AUTOMORPHISM GROUP OF A CODED SYSTEM

DORIS FIEBIG AND ULF-RAINER FIEBIG

ABSTRACT. We give a general construction of coded systems with an automorphism group isomorphic to $\mathbf{Z} \oplus G$ where G is any preassigned group which has a “continuous block presentation” (the isomorphism will map the shift to $(1, e_G)$). Several applications are given. In particular, we obtain automorphism groups of coded systems which are abelian, which are finitely generated and one which contains $\mathbf{Z}[1/2]$. We show that any group which occurs as a subgroup of the automorphism group of some subshift with periodic points dense already occurs for some synchronized system.

INTRODUCTION

For a finite set A consider $A^{\mathbf{Z}}$ endowed with the product topology of the discrete topology on A together with the (left) shift map. A *subshift* (S, σ) is a closed shift invariant subset S of $A^{\mathbf{Z}}$ together with the restricted shift map σ . In the following we shall suppress the map σ in our notation. The *automorphism group* $\text{aut}(S)$ of S is the group of shift commuting homeomorphisms of S . It is countable, since automorphisms are given by sliding block codes [H].

The automorphism groups of full shifts $S = A^{\mathbf{Z}}$ have been studied in the early 1960s by Hedlund and his coworkers [H]. Motivated by Williams’s shift equivalence problem [W], in the 1980s there was renewed interest in the groups $\text{aut}(S)$ where S is a shift of finite type (SFT); see [AM, DGS, LM] for basic definitions. They have been studied in various papers, for example [BK, BLR, BFK, KRW], where [BFK] treats the different one-sided case. These automorphism groups are very rich groups. By the so-called marker method it was shown that they are not finitely generated and have a large collection of subgroups, as for example the direct sums of every countable collection of finite groups and the free products of any finite number of copies of $\mathbf{Z}/2\mathbf{Z}$ ([BLR]).

It is a natural question how the structure of these automorphism groups may change if we enlarge the class of subshifts under consideration. Shifts of finite type are PPD subshifts, where PPD stands for “periodic points dense”. This implies that the automorphism groups of SFTs are residually finite ([BLR]). For general subshifts other countable groups can be realized as automorphism groups, for example \mathbf{Q} [BLR]. It is not clear what the obstructions in the general setting are.

We will consider two natural subclasses of PPD subshifts. For that we recall the notions (see [BH], [FF]) of synchronized systems and coded systems (any transitive SFT is synchronized and any synchronized system is coded) and indicate the dramatic change in the possible structures of automorphism groups when passing from

Received by the editors December 13, 1994 and, in revised form, July 17, 1995.

1991 *Mathematics Subject Classification.* Primary 58F03, 20B27; Secondary 20E26.

synchronized to general coded systems. For a point $s = (s_i)_{i \in \mathbf{Z}} \in S$, S an arbitrary subshift, let $s[n, m]$ denote the subblock s_n, \dots, s_m of s ($-\infty \leq n \leq m \leq \infty$). An S -block is a finite subblock of some point in S . An S -block w is *synchronizing* if for all pairs of S -blocks u, v the implication “if uw and wv are S -blocks then uwv is an S -block” holds. For a SFT there is an n such that all S -blocks of length n are synchronizing (which may be used as a definition of the SFT-property).

A *synchronized system* is a transitive subshift which has a synchronizing block. The existence of a synchronizing block suffices to carry over the marker construction of automorphisms as shown in [BLR], thus synchronized systems also have rich automorphism groups. We will show that given any subshift R with periodic points dense, there is a synchronized system S such that $\text{aut}(S)$ contains a copy of $\text{aut}(R)$.

A *coded system* T is a subshift which has a code X , i.e. X is a countable set of finite blocks and T is the closure of the points obtained by bi-infinite concatenations of blocks from X . We will see that there are coded systems with very small automorphism groups, in fact it may consist only of the powers of the shift map.

Starting with some general remarks, we give an outline of the organization and main results of this paper. We will study the set of groups which occur as automorphism groups (or as subgroups of automorphism groups) for coded systems. Coded systems have periodic points dense, thus the argument from Theorem 3.1 in [BLR] shows that the automorphism group of a coded system is residually finite [MKS] (which immediately excludes groups like \mathbf{Q} or $\mathbf{Z}(p^\infty) = \mathbf{Z}[1/p]/\mathbf{Z}$). Not every residually finite group is an automorphism group of a coded system, for example $\mathbf{Z}[1/2]$ cannot be realized (see Lemma 2.15). For subgroups no further restriction than residual finiteness is known to us (in the SFT case the subgroup also has to have solvable word problem [BLR, Proposition 2.8], a restriction that seems to vanish for coded systems).

We will show that for a variety of groups G there is a coded system T with $\text{aut}(T) \approx \langle \sigma \rangle \oplus G$, which means that there is an isomorphism from $\text{aut}(T)$ to the group $\mathbf{Z} \oplus G$, that maps the shift σ to $(1, e_G)$, where $e_G \in G$ is the identity element. In section 1 we describe a general technique to obtain such a coded system for any group G which has a “continuous block presentation” (see section 1 for definitions). This condition is of a very combinatorial nature, but is easily met by any finite group G , and is closed under taking countable sums of groups (Theorems 2.1 and 2.6). In section 2 we also show that a group G has a continuous block presentation iff G is isomorphic to a closed (w.r.t. periodic point topology) subgroup of $\text{aut}(R)$ for some subshift R with periodic points dense. This gives a second approach to constructing coded systems T with $\text{aut}(T) \approx \langle \sigma \rangle \oplus G$ for preassigned groups G : try to realize G as a closed subgroup of the automorphism group of some subshift with periodic points dense.

We get in particular the following results.

For any finite group G there is a coded system T with $\text{aut}(T) \approx \langle \sigma \rangle \oplus G$, in particular there is a coded system S with trivial automorphism group $\text{aut}(S) = \langle \sigma \rangle$ (Corollary 2.2). This contrasts with the fact that for SFTs the automorphism group is “large” (see above).

Any infinite, finitely generated abelian group is the automorphism group of some coded system. Thus the center of the automorphism group of a coded system need not to be the powers of the shift as in the SFT case [R].

There are two coded systems with distinct zeta functions (thus nonconjugate) which have isomorphic automorphism groups (Corollary 2.3) (see also Question 4.1 in [BLR]).

There are uncountably many nonisomorphic automorphism groups for coded systems.

There is a coded system T with $\text{aut}(T) \approx \langle \sigma \rangle \oplus \{a, b; a^2 = b^2 = e\}$.

There is a coded system T with $\text{aut}(T) \approx \langle \sigma \rangle \oplus \mathbf{Z}[1/2]$ (it is not known if $\mathbf{Z}[1/2]$ can be the subgroup of the automorphism group of an SFT [BLR, Problem 3.4]. The group $\mathbf{Z}[1/2]$ itself cannot be the automorphism group of a coded system (see Lemma 2.15)).

Let R be a shift with periodic points dense. Then there is a coded system T such that $\text{aut}(T) \approx \langle \sigma \rangle \oplus \text{aut}(R)$.

This shows in particular that passing from coded systems to shifts with periodic points dense does not increase the set of subgroups of the automorphism groups. But the set of possible automorphism groups does in fact change: there is a subshift R with periodic points dense and $\text{aut}(R) \approx \mathbf{Z}[1/2] \oplus C$ where C is some direct sum of finite cyclic groups (Theorem 2.14). Such a group cannot be the automorphism group of a coded system (Theorem 2.16). We do not know if there is such an example where R is also transitive.

It remains an open problem what the scope of our construction is: *which groups G admit a continuous block presentation?*

1. CODED SYSTEMS WITH PREASSIGNED AUTOMORPHISM GROUPS. GENERAL CONSTRUCTION

We consider inverse limits of finite groups, for which we define block presentations and the resulting subgroup of continuous elements. We show by construction that for any such subgroup of continuous elements, say G , there is a coded system with $\text{aut}(T) \approx \langle \sigma \rangle \oplus G$ (Theorem 1.4).

Let (G_n, π_n) be a sequence of finite groups G_n and onto group homomorphisms $\pi_n : G_{n+1} \rightarrow G_n$, $n \in \mathbf{N}$. Let $\lim_{\leftarrow} (G_n, \pi_n)$ denote the induced inverse limit system $\{(g_1, g_2, \dots) | g_n \in G_n, \pi_n(g_{n+1}) = g_n \text{ for all } n \in \mathbf{N}\}$, with coordinatewise group multiplication.

Definition 1.1. A *block presentation* \mathcal{B} of $\lim_{\leftarrow} (G_n, \pi_n)$ is a choice of a finite set A , a sequence $2 \leq k(1) < k(2) < \dots$ in \mathbf{N} , and injective maps $B_N : G_n \rightarrow A^{k(n)}$, $n \in \mathbf{N}$.

Any element $g = (g_1, g_2, \dots) \in \lim_{\leftarrow} (G_n, \pi_n)$ acts on $\lim_{\leftarrow} (G_n, \pi)$ by coordinatewise left-multiplication. Thus, for each n , the element g induces a permutation $B_n(h_n) \rightarrow B_n(g_n h_n)$ on the blocks in $B_n(G_n)$. We call the union of these permutations the \mathcal{B} -action of g .

Definition 1.2. Let ω be a new symbol not in A . The \mathcal{B} -action of g is a *sliding block code*, if for some $L \geq 0$ there is a map $\phi : (A \cup \{\omega\})^{2L+1} \rightarrow A$ such that for all $n \in \mathbf{N}$ and $h_n \in G_n$ we have $B_n(g_n h_n) = \Phi_n^{(\phi)}(B_n(h_n))$, where $\Phi_n^{(\phi)} : A^{k(n)} \rightarrow A^{k(n)}$ is the map given by $(\Phi_n^{(\phi)}(a_1, \dots, a_{k(n)}))_i := \phi(a_{-L+i}, \dots, a_{i+L})$, $1 \leq i \leq k(n)$, where on the right-hand side $a_m := \omega$ if $m < 1$ or $m > k(n)$.

Definition 1.3. An element $g \in \lim_{\leftarrow} (G_n, \pi_n)$ is called \mathcal{B} -continuous if the \mathcal{B} -actions of g and g^{-1} both are sliding block codes. This defines the subgroup

of \mathcal{B} -continuous elements in $\lim_{\leftarrow}(G_n, \pi_n)$. An abstract group G has a *continuous block presentation* if there is some block presentation \mathcal{B} of some inverse limit $\lim_{\leftarrow}(G_n, \pi_n)$ of finite groups such that G is isomorphic to $\{g \in \lim_{\leftarrow}(G_n, \pi_n) | g \text{ is } \mathcal{B}\text{-continuous}\}$.

If G has a continuous block presentation then G is a subgroup of $\lim_{\leftarrow}(G_n, \pi)$, thus residually finite. Every residually finite group G is a subgroup of an inverse limit of finite groups, but we do not know if it is always possible to obtain a continuous block presentation.

Theorem 1.4. *Let G be a group with a continuous block presentation. Then there is a coded system T with $\text{aut}(T) \approx \langle \sigma \rangle \oplus G$.*

The rest of this section is devoted to a proof of Theorem 1.4. First a general method of construction will lead us to a coded system T , then we show $\text{aut}(T) \approx \langle \sigma \rangle \oplus G$ by a series of lemmata and propositions.

We may assume that

$$G = \{g \in \lim_{\leftarrow}(G_n, \pi_n) | g \text{ is } \mathcal{B}\text{-continuous}\}$$

where $\lim_{\leftarrow}(G_n, \pi_n)$ is an inverse limit of finite groups, \mathcal{B} a block presentation of $\lim_{\leftarrow}(G_n, \pi_n)$ given by a sequence of injective maps $B_n : G_n \rightarrow A^{k(n)}$, $2 \leq k(1) < k(2) < \dots$, for some finite alphabet A . We may assume that the symbols 0, 1, 2 are not in A (replace A by a disjoint copy if necessary). If a is a symbol from some alphabet, then let a^n denote the block $aa \cdots a$ that consists of n repetitions of a . For a block $w = w_1 \cdots w_n$ let $|w|$ denote its length n , and for $1 \leq i \leq j \leq |w|$ let $w[i, j]$ denote the subblock $w_i w_{i+1} \cdots w_j$.

Definition of T . We will define a set X of blocks with symbols in $\{0, 1, 2\}$, then a function that assigns to each $w \in X$ a block $y(w)$ of the same length but with symbols in $\{0, 1, 2\} \cup A$. The code for T will then be

$$Y := \{0\} \cup \{0^{|w|+1}y(w)0^{|w|+1} | w \in X\}.$$

We start defining the set X . The set X will consist of all blocks $w \in \{0, 1, 2\}^m$, $m \in \mathbf{N}$, which are *stable*, *neutral*, and have a *proper skeleton*. Now we define these terms.

(i) *Stability:* Let $I = \bigcup_{k \in \mathbf{N}} \{n | 2^{2k} \leq n \leq 2^{2k+1}\}$ (any infinite subset $I \subset \mathbf{N}$ with $1 \notin I$, and I, I^c having unbounded gaps works). Let

$$J = \{(0, 0), (1, 1), (1, 2), (2, 1), (2, 2)\} \subset \{0, 1, 2\}^2.$$

A block $w \in \{0, 1, 2\}^m$, $m \in \mathbf{N}$, is *stable* if

- (1) the blocks 12 and 21 do not occur as subblocks of w ,
- (2) if $w' = 0^{m+1}w0^{m+1}$, then for any pair $i < j$ with $w'[i, j] = 0a^n0$, $a \in \{1, 2\}$, we have $a = 1$ if $(n, (w'_{i-n}, w'_{j+n})) \in (I \times J) \cup (I^c \times J^c)$, and $a = 2$ otherwise.

Remark. By (1) the block w' can be written as a finite concatenation of blocks from $\{0\} \cup \{01^n | n \in \mathbf{N}\} \cup \{02^n | n \in \mathbf{N}\}$. The definition of J is made such that $(w'_{i-n}, w'_{j+n}) \in J$ iff both are zero or both are not zero. Thus any stable block w can be recovered by the rule (2) from its length and 0-skeleton (the set of indices i with $w_i = 0$).

(ii) *Neutrality:* We define a map c from the finite blocks with symbols in $\{0, 1, 2\} \cup A$ into $\lim_{\leftarrow}(G_n, \pi_n)$. For that let $X_1 = \{0^{n+1}1^n0^{n+1} | n \in I\}$ and first fix a map $c : X_1 \rightarrow \lim_{\leftarrow}(G_n, \pi_n)$ such that $[g \in c(X_1) \Rightarrow g^{-1} \in c(X_1)]$ and $c(X_1)$ is dense

(i.e. for each $n \in \mathbf{N}$ and $h_n \in G_n$ it holds $c(w)_n = h_n$ for some $w \in X_1$). Now extend c to a map on blocks w with symbols in $\{0, 1, 2\} \cup A$ as follows. Let $c(w) = e$ if no subblock of w is in X_1 . Otherwise let $1 \leq i_1 < i_2 < \dots < i_n \leq |w|$ be the ordered set of indices i_j such that $w[i_j, |w|]$ begins with a block in X_1 . For each such i_j there is a unique k_j with $w[i_j, k_j] \in X_1$. Now let $c(w) = c(w[i_1, k_1])c(w[i_2, k_2]) \dots c(w[i_n, k_n])$ (the blocks $w[i_j, k_j]$ may have overlaps). A block $w \in \{0, 1, 2, \}^m$, $m \in \mathbf{N}$, is *neutral* if $c(w) = e$, the identity in $\lim_{\leftarrow} (G_n, \pi_n)$.

(iii) *Proper skeletons*: Let $X_2 = \{C(n) \mid n \in \mathbf{N}\}$, where $C(n) = 0020^{k(n)}2^{k(n)}0^{k(n)+1}$ if $k(n) \in I$ and $C(n) = 0000^{k(n)}2^{k(n)}0^{k(n)+1}$ if $k(n) \notin I$ (note that these blocks are stable). A block $w \in \{0, 1, 2\}^m$, $m \in \mathbf{N}$, has a *proper skeleton* if $w = C(n_1)u_1C(n_2)u_2 \dots C(n_{k-1})u_{k-1}C(n_k)$ with $k \geq 1$ and possibly empty blocks u_i such that $n_1 = n_k$, $n_1 \geq n_i$ for $1 \leq i \leq k$, and besides the indicated blocks $C(n_1), \dots, C(n_k)$ there are no further occurrences of X_2 -blocks in $0^{|w|+1}w0^{|w|+1}$.

This completes the definition of the block system X .

For example, any block w which has a proper skeleton where all the u_i are empty blocks is stable and neutral, thus belongs to X .

We define the function y on X . For $n \in \mathbf{N}$, $g_n \in G_n$, let $C(n, g_n)$ be the block obtained from $C(n)$ by replacing the subblock $2^{k(n)}$ with $B_n(g_n)$. Now let $w \in X$. Then w has a proper skeleton $w = C(n_1)u_1C(n_2)u_2 \dots C(n_{k-1})u_{k-1}C(n_k)$ as in (iii). Now define

$$y(w) = C(n_1, g_{n_1})u_1C(n_2, g_{n_2})u_2 \dots C(n_{k-1}, g_{n_{k-1}})u_{k-1}C(n_k, g_{n_k})$$

where the g_{n_i} are uniquely determined by

$$g_{n_i} = c(C(n_1)u_1C(n_2)u_2 \dots C(n_{i-1})u_{i-1}C(n_i))_{n_i} \in G_{n_i}, \quad 1 \leq i \leq k.$$

(Note that $g_{n_1} = e$ and also $g_{n_k} = e$ since w is neutral.)

This finishes the definition of the coded system T . A series of lemmata and propositions will lead us to $\text{aut}(T) \approx \langle \sigma \rangle \oplus G$.

We show that T -points can be approximated arbitrarily well by single blocks from Y , which implies a fundamental property of T -points.

Let f be the 1-block factor map on T which maps the symbols in A to 2 and leaves the symbols 0, 1, 2 fixed. Thus $f(y(w)) = w$ for all $w \in X$.

Lemma 1.5. (a) *Any finite concatenation of blocks in Y is a subblock of some Y -block.*

(b) *Any T -block $au0z0vb$ with $z \in (\{1, 2\} \cup A)^n$, $|a| = |b| = 1$, $|u| = |v| = n - 1$, satisfies the fundamental property, that is*

$$(*) \quad z = 1^n \text{ or } z = 2^n \text{ or } z \in A^n, \\ \text{and } z = 1^n \text{ iff } (n, (f(a), f(b))) \in (I \times J) \cup (I^c \times J^c).$$

(c) *Given a T -block $0^{|u|+3}u0^{|u|+3}$ with a block $u = u_1u_2 \dots u_n$ of length $n \in \mathbf{N}$, then the 0-skeleton of u (i.e. the set of i for which $u_i = 0$) determines for each $1 \leq i \leq n$ to which of the sets $\{0\}, \{1\}, \{2\}, A$ the value of u_i belongs.*

Proof. (a) Given a concatenation $y_1y_2 \dots y_j$ of blocks y_i from Y , choose n_0 so large that all $C(n)$ -blocks in $f(y_1y_2 \dots y_j)$ satisfy $n \leq n_0$. Then it is not hard to see that $0^{M+1}C(n_0, e)y_1y_2 \dots y_jC(n_0, e)0^{M+1} \in Y$ where $M = \text{length of } C(n_0, e)y_1y_2 \dots y_jC(n_0, e)$.

(b) By (a) the given block is contained in a single block $0^{|w|+1}y(w)0^{|w|+1}$ from Y . The definition of Y -blocks implies immediately that $z = 1^n$ or $z = 2^n$ or $z \in A^n$. By definition, w is a stable block, which implies the second statement.

(c) Consider $1 \leq i \leq n$ such that $u_i \neq 0$. There is a subblock $a'u'0z'0v'b'$ as in (b) of $0^{|u|+3}u0^{|u|+3}$ such that this i th coordinate belongs to the subblock z' . Thus, the fundamental property determines from the 0-skeleton of u if $u_i = 1$ or $u_i \in \{2\} \cup A$. Thus we know $f(u)$. Now assume $u_i \in \{2\} \cup A$, i.e. $f(u_i) = 2$. The block $0^{|u|+3}u0^{|u|+3}$ is contained in a concatenation of Y -blocks, thus by (a) in one Y -block, say $0^{|w|+1}y(w)0^{|w|+1}$ for some block $w \in X$. Thus, by definition of $y(w)$, $u_i \in A$ if and only if i is a coordinate contained in the $2^{k(n)}$ -block of some X_2 -block $C(n)$ in $f(0^{|w|+1}y(w)0^{|w|+1})$. But this is actually determined by $f(u)$, since such a $C(n)$ has to be a subblock of $0^{|u|+3}u0^{|u|+3}$. \square

Now the fundamental property implies that any automorphism of T can be combined with a unique power of the shift so that the resulting map leaves the $\{0, 1, 2\}$ -skeleton of every point in T fixed.

Proposition 1.6. *Let Φ be an automorphism of T . Let σ be the shift on T . Then there is an $i \in \mathbf{Z}$ such that $\Phi \circ \sigma^i$ is a skeleton automorphism, i.e. $\Phi \circ \sigma^i(t)_0 = t_0$ iff $t_0 \in \{0, 1, 2\}$ and $\Phi \circ \sigma^i(t)_0 \in A$ iff $t_0 \in A$, for all $t \in T$. Furthermore, an automorphism of T is a skeleton automorphism iff it fixes all periodic points $(0^{2^n}1^n)^\infty$, $n \in I$.*

Proof. The proof will be given in a series of claims. Let L be a coding length for Φ , i.e. $\Phi(t)_0$ is determined by $t[-L, L]$, for every $t \in T$.

Claim 1. $\Phi(0)^\infty = 0^\infty$.

Proof. Necessarily $\Phi(0^\infty) = c^\infty$ for some $c \in \{0, 1, 2\} \cup A$. Assume $c \neq 0$. There is a point $t \in T$ with $\Phi(t) = 0^\infty$. Then $t[-L, L]$ occurs in some block $y \in Y$ by Lemma 1.5(a). Since $0 \in Y$ we have that $t^N = 0^\infty y 0^N y 0^\infty$ is a point in T . Let $N > 2L$. Since y sees $t[-L, L]$, and L is a coding length for Φ , we have $\Phi(t^N) = c^\infty u 0 u' c^{N-2L} v' 0 v c^\infty \in T$, where u, v, u', v' are fixed blocks, each of length $\leq |y| + 2L$, and u' and v' do not see the symbol 0. Consider the numbers N with $|u' c^{N-2L} v'| > \max\{|u|, |v|\}$. Choose such an N with $|u' c^{N-2L} v'| \in I$; then the fundamental property of T implies $c = 1$. Choose such an N with $|u' c^{N-2L} v'| \notin I$, now the fundamental property of T implies $c \neq 1$, a contradiction. Thus $c = 0$. \square

Now let t^N be defined by $t^N(-\infty, 0] = 0^\infty$, $t^N[1, \infty) = 1^N 0^\infty$.

Claim 2. For $N \in I$ we have $t^N \in T$. Moreover, there is a unique $i \in \mathbf{Z}$ such that $\Phi \circ \sigma^i(t^N)[0, \infty)$ begins with $01^N 0$ for all $N \in I$ with $N > 4L$.

Proof. Fix $N \in I$. Take $w \in X_1$ such that $c(w) = c(0^{N+1}1^N 0^{N+1})^{-1}$. Then, for each $k \geq 1$,

$$0^{M+1}C(1, e)0^{N+k}1^N 0^{N+k}wC(1, e)0^{M+1} \in Y$$

for $M = |C(1, e)0^{N+1}1^N 0^{N+k}wC(1, e)|$, thus $t^N \in T$. We know $\Phi(1^\infty) = c^\infty$ for some $c \in \{1, 2\} \cup A$ ($c \neq 0$ by Claim 1). Since L is a coding length for Φ , for all $N > 4L$ with $N \in I$ we have $\Phi(t^N) = 0^\infty u 0 u' c^{N-2L} v' 0 v 0^\infty$, where u, v, u', v' are fixed blocks, each of length $\leq 2L$, and u', v' do not see the symbol 0. Moreover, the block $0u' c^{N-2L} v' 0$ starts at the same coordinate i for all N . It remains to show $u' c^{N-2L} v' = 1^N$ for all N . Since $n = N - |u' c^{N-2L} v'|$ is a fixed number and I

contains arbitrarily long intervals (the complement has unbounded gaps), there is an $N > 4L$ with $N \in I$ and $|u'c^{N-2L}v'| = N - n \in I$. For this N the fundamental property of T and $0^\infty u 0 u' c^{N-2L} v' 0 v 0^\infty \in T$ imply that $u'c^{N-2L}v' = 1^{N-n}$. Thus $u'c^{N-2L}v' = 1^{N-n}$ for all N . Finally $n = 0$, since otherwise we could choose $N > 4L$ with $N \in I$ and $|u'c^{N-2L}v'| = N - n \notin I$ (I is infinite with unbounded gaps); then $0^\infty u 0 u' c^{N-2L} v' 0 v 0^\infty \in T$ would violate the fundamental property. \square

Claim 3. Choose i as in Claim 2. Then $\Psi = \Phi \circ \sigma^i$ is a skeleton automorphism.

Proof. Let L be a coding length for Ψ . First let $t \in T$ with $t_0 = 0$. We show that $\Psi(t)_0 = 0$. There is a Y -block $w = w_{-r} \cdots w_0 \cdots w_s$ such that $w_{-L} \cdots w_0 \cdots w_L = t[-L, L]$. Choose an $N > 2L + |w| + 4$ with $N \in I$. For $u := w 0020^{N-s-3} 1^N 0^{2N}$ we have that $f(u)$ is stable, since $w_0 = t_0 = 0$, and neutral, since $c(u) = c(w) = e$. Thus $0^M C(p, e) u C(p, e) 0^M \in Y$ for p large enough and suitable M , which shows that u is a T -block. So let $t \in T$ be such that $t(-\infty, 0]$ ends with $w_{-r} \cdots w_0$ and $t[0, \infty)$ begins with $w_0 \cdots w_s 0020^{N-s-3} 1^N 0^{2N}$. Then $\Psi(t)[N, 2N+1] = 01^N 0$ by Claim 2, and $\Psi(t)_{3N+1} = 0$ by Claim 1. From the fundamental property it follows that $\Psi(t)_0 = 0$.

Now let $t \in T$ with $t_0 \neq 0$. As above it follows that for some Y -block w containing $t[-L, L]$ there are $N, K \in I$ with $N > 2L + |w| + 4$ and $4L \leq K < N - 2L$ such that $w 0020^{N-s-3} 1^N 0^{N-2L} 1^K 0^N$ is a T -block. Repeating the above argument shows $\Psi(t)_0 \neq 0$.

Thus $\Psi(t)_0 = 0$ iff $t_0 = 0$.

Again, let $t \in T$ with $t_0 \neq 0$. There is a Y -block $w = w_{-r} \cdots w_0 \cdots w_s$ such that $w_{-L} \cdots w_0 \cdots w_L = t[-L, L]$. Let $t' \in T$ with $t'[-r - |w| - 3, s + |w| + 3] = 0^{|w|+3} w 0^{|w|+3}$. By the above, t' and $\Psi(t')$ have the same 0-skeleton (i.e., $t'_n = 0$ iff $\Psi(t')_n = 0$ for all n). Thus the blocks $t'[-r - |w| - 3, s + |w| + 3]$ and $\Psi(t')[-r - |w| - 3, s + |w| + 3]$ are of the type as in Lemma 1.5(c), and have the same 0-skeleton; thus $\Psi(t')_0$ belongs to the same set of $\{1\}, \{2\}, A$ as t'_0 does. Since $t_0 = t'_0$ and $\Psi(t)_0 = \Psi(t')_0$, the same holds for t_0 and $\Psi(t)_0$.

The characterization of skeleton automorphisms follows immediately from Claim 3. \square

So far we have used the fundamental property of T . Now we shall use the following dependency structure between neighboring $C(n, g_n)$ -blocks.

Lemma 1.7. *Let $B_n(g_n)wB_n(h_n)$ be a T -block. Then $h_n = g_n \cdot c(w)_n$.*

Let $C(n+1, h_{n+1})C(n, h_n)$ be a T -block. Then $h_n = \pi_n(h_{n+1})$.

Proof. $B_n(g_n)wB_n(h_n)$ occurs as subblock of a block from Y . The lemma now follows from the definition of the code Y . The same applies to $C(n+1, h_{n+1})C(n, h_n)$. \square

Proposition 1.8. *Let Φ be a skeleton automorphism of T . If $t, t' \in T$ with $t[0, k(n) + 1] = t'[0, k(n) + 1] = 0B_n(g_n)0$ for some $g_n \in G_n$, then $\Phi(t)[1, k(n)] = \Phi(t')[1, k(n)] = B_n(h_n)$ for some $h_n \in G_n$.*

Proof. Let L be a coding length for Φ . There are blocks y, y' from Y such that $t[-L, k(n) + L]$ is a subblock of y and $t'[-L, k(n) + L]$ is a subblock of y' . Then for large enough N and suitable M , $u = 0^{M+1} C(N, e) y y' C(N, e) 0^{M+1} \in Y$. Write $y = aB_n(g_n)b$ and $y' = a'B_n(g_n)b'$. By Lemma 1.7, $g_n = g_n \cdot c(ba')_n$; thus $c(ba')_n = e$ in G_n . Since Φ is a skeleton automorphism, we will see some block $B_n(h_n)$

in $\Phi(0^\infty u 0^\infty)$ at the coordinates of $B_n(g_n)$ in y , and some block $B_n(h'_n)$ at the coordinates of $B'_n(g_n)$ in y' . Let w denote the block occurring in $\Phi(0^\infty u 0^\infty)$ at the same coordinates as the block ba' in $0^\infty u 0^\infty$. Then $c(w) = c(ba')$ since Φ is a skeleton automorphism. Again, by Lemma 1.7, $h'_n = h_n \cdot c(w)_n = h_n$. \square

Proposition 1.9. *Let Φ be a skeleton automorphism of T . Then Φ induces in an injective homomorphic way a \mathcal{B} -continuous element $g_\Phi \in \lim_{\leftarrow} (G_n, \pi_n)$.*

Proof. For $g_n \in G_n$ choose $w \in X_1$ with $c(w)_n = g_n$. Let $u \in X_1$ with $c(u) = c(w)^{-1}$. Then

$$0^{M+1}C(n, e)wC(n, g_n)uC(n, e)0^{M+1} \in Y$$

for

$$M = |C(n, e)wC(n, g_n)uC(n, e)|.$$

Thus $C(n, e)wC(n, g_n)$ is a T -block. Since Φ is a skeleton automorphism, by Proposition 1.8 Φ maps this block to $C(n, h_n)wC(n, h'_n)$ for some $h_n, h'_n \in G_n$. Thus $h'_n = h_n c(w)_n = h_n g_n$ by Lemma 1.7. Thus Φ acts on G_n as multiplication from the left by h_n . For each n we have that $C(n+1, e)C(n, e)$ is a T -block which is mapped by Φ to $C(n+1, h_{n+1})C(n, h_n)$. Thus $h_n = \pi_n(h_{n+1})$ by Lemma 1.7. Therefore $g_\Phi := (h_1, h_2, \dots) \in \lim_{\leftarrow} (G_n, \pi_n)$. The \mathcal{B} -action of g_Φ is a sliding block code with L = the coding length of Φ . Analogously, Φ^{-1} induces $g_{\Phi^{-1}} = (g_\Phi)^{-1} \in \lim_{\leftarrow} (G_n, \pi_n)$, whose \mathcal{B} -action is a sliding block code. Thus g_Φ is \mathcal{B} -continuous. Clearly the map $\Phi \rightarrow g_\Phi$ is an injective homomorphism. \square

Proposition 1.10. *The map $\Phi \rightarrow g_\Phi$ defines an isomorphism between the group of skeleton automorphisms of T and the subgroup of \mathcal{B} -continuous elements of $\lim_{\leftarrow} (G_n, \pi_n)$.*

Proof. It only remains to show that $\Phi \rightarrow g_\Phi$ is surjective. For that let $g = (g_1, g_2, \dots) \in \lim_{\leftarrow} (G_n, \pi_n)$ be \mathcal{B} -continuous. Let D be the set of points in T which see the symbol 0 infinitely often in the past and in the future. First define Φ_g on the set D as the map which leaves the symbols 0, 1, 2 fixed and maps each $B_n(h_n)$ to $B_n(g_n h_n)$. We show that $\Phi_g(D) \subset D$. By Lemma 1.5(a) it suffices to show that $\Phi_g(0^\infty y(w) 0^\infty) \in T$ for all $w \in X$. Since $y(w)$ is of the form $C(n_1, e)u_1 \cdots u_{k-1}C(n_k, e)$ with $n_1 = n_k$, we have $\Phi_g(0^\infty y(w) 0^\infty) = 0^\infty C(n_1, g_{n_1})u_1 \cdots C(n_{k-1}, g_{n_{k-1}})u_{k-1}C(n_1, g_{n_1})0^\infty$. Let $u \in X_1$ with $c(u)_{n_1} = g_{n_1}$ and $u' \in X_1$ with $c(u') = c(u)^{-1}$. Then for each $n \geq |w| + 1$ there is $M = M(n)$ such that $0^M C(n_1, e)u 0^n C(n_1, g_{n_1}) \cdots C(n_1, g_{n_1})0^n u' C(n_1, e)0^M \in Y$. Thus, $\Phi_g(0^\infty y(w) 0^\infty) \in T$. Define $\Phi_{g^{-1}}$ analogously. Since the \mathcal{B} -actions of g and g^{-1} are sliding block codes, Φ_g and $\Phi_{g^{-1}}$ are both uniformly continuous on D . Thus both maps can be uniquely extended to continuous shift-invariant mappings defined on T , which we call again Φ_g and $\Phi_{g^{-1}}$. By definition, $\Phi_g \Phi_{g^{-1}} = \text{id}$ on D , thus $\Phi_g \Phi_{g^{-1}} = \text{id}$ on T . The same applies to $\Phi_{g^{-1}} \Phi_g$, thus Φ_g is an automorphism of T . And obviously $\Phi_g \rightarrow g_{\Phi_g} = g$ under the map described in the proof of Proposition 1.9. \square

Now we can finish the proof of Theorem 1.4. Let H be the group of skeleton automorphisms of T . Define $j : \mathbf{Z} \oplus H \rightarrow \text{aut}(T)$ by $j((i, \phi)) = \sigma^i \phi$. Since σ commutes with any automorphism, j is a homomorphism. By Proposition 1.6 any automorphism of T has a presentation as $\sigma^i \phi$ with $i \in \mathbf{Z}, \phi \in H$; thus j is surjective. This presentation is unique; thus j is injective. So j^{-1} is an isomorphism

$\text{aut}(T) \rightarrow \mathbf{Z} \oplus H$ with $j^{-1}(\sigma) = (1, \text{id})$. This shows $\text{aut}(T) \approx \langle \sigma \rangle \oplus H$. By Proposition 1.10 $H \approx \{g \in \lim_{\leftarrow} (G_n, \pi_n) \mid g \text{ is } \mathcal{B}\text{-continuous}\}$. \square

2. CODED SYSTEMS WITH PREASSIGNED AUTOMORPHISM GROUPS. APPLICATIONS

For a variety of groups G we obtain coded systems T with $\text{aut}(T) \approx \langle \sigma \rangle \oplus G$. This will be an application of Theorem 1.4: in each case we show that G has a continuous block presentation. We show that this property is closed under taking direct sums. Moreover, a group G has a continuous block presentation iff G is isomorphic to a closed subgroup of $\text{aut}(R)$ for some subshift R with periodic points dense. We use this characterization to obtain a coded system T with $\text{aut}(T) \approx \langle \sigma \rangle \oplus \mathbf{Z}[1/2]$.

Recall that we write $\text{aut}(T) \approx \langle \sigma \rangle \oplus G$ if there is an isomorphism from $\text{aut}(T)$ to $\mathbf{Z} \oplus G$ which maps the shift σ to the element $(1, e)$, where e is the identity element in G .

Automorphism groups for nontrivial SFTs are not finitely generated [BLR, Theorem 7.8]. In contrast to that, the automorphism group of a coded system can be finitely generated. Theorem 2.1, Theorem 2.4 and Theorem 2.5 give particular examples for this.

Theorem 2.1. *Any finite group G has a continuous block presentation. In particular, there is a coded system T such that $\text{aut}(T) \approx \langle \sigma \rangle \oplus G$.*

Proof. Let $A = G$ and $(G_n, \pi_n) = (G, \text{id})$ for all n . Let $k(n) = n+1$ and let $B_n(g) = gg \cdots g$ be the block of $n+1$ repetitions of the symbol g . Then $G = \lim_{\leftarrow} (G_n, \pi_n)$ and the \mathcal{B} -action of any $g \in G$ is given by a sliding 1-block code (i.e. $L = 0$); thus all elements in $\lim_{\leftarrow} (G_n, \pi_n)$ are \mathcal{B} -continuous. Apply Theorem 1.4. \square

Corollary 2.2. *There is a coded system T with $\text{aut}(T) = \langle \sigma \rangle$.*

It is not known whether there are two SFT's S and T with isomorphic automorphism groups but such that neither S and T nor S and T^{-1} are conjugate [BLR, Question 4.1]. For coded systems this can be the case.

Corollary 2.3. *There are coded systems T and T' which have distinct zeta functions but isomorphic automorphism groups.*

Proof. Let T be given as in Theorem 2.1 with $G = \{e\}$, the trivial 1-element group. Observe that by construction the fixed points of T are $0^\infty, 1^\infty, 2^\infty, e^\infty$. To get T' we choose another continuous block presentation for $G = \{e\}$. As before let $(G_n, \pi_n) = (G, \text{id})$ and $k(n) = n+1$ for all n . But now choose $A = \{a, b\}$, and for even n let $B_n(e) = a^{n+1}$ (the block of $n+1$ repetitions of the symbol a), for odd n , $B_n(e) = b^{n+1}$. Then $G \approx$ the group of \mathcal{B} -continuous elements in $\lim_{\leftarrow} (G_n, \pi_n)$, since the only element of $\lim_{\leftarrow} (G_n, \pi_n)$, the identity, is of course \mathcal{B} -continuous. Now let T' be the system obtained from this continuous block presentation of G (Theorem 1.4). Observe that T' has five fixpoints: $0^\infty, 1^\infty, 2^\infty, a^\infty, b^\infty$. Thus T, T' have different zeta functions but $\text{aut}(T) \approx \mathbf{Z} \approx \text{aut}(T')$. \square

Theorem 2.4. *The group \mathbf{Z} has a continuous block presentation. In particular, there is a coded system T such that $\text{aut}(T) \approx \langle \sigma \rangle \oplus \mathbf{Z}$.*

Proof. This theorem follows also from Corollary 2.2 in combination with Theorem 2.12. But here we prefer to give a more direct construction. For each $n \geq 2$ let $G_n = \mathbf{Z}/2^n\mathbf{Z}$ and let $\pi_n : G_{n+1} \rightarrow G_n$ be the natural projection. With $H_n = 2^n\mathbf{Z}$

we have $G_n = \{iH_n | 0 \leq i < 2^n\}$. Let $A = \{(0,0), (0,1), (1,0)\}$, i.e. the symbols of our alphabet are 2-tuples. Let $k(n) = 2^{n-1}$ and for $0 \leq i < 2^n$ let $B_n(iH_n)$ be the block $(x_0, x_{2^n-1})(x_1, x_{2^n-2})(x_2, x_{2^n-3}) \cdots (x_{2^n-1-1}, x_{2^n-1}) \in A^{k(n)}$ with $x_i = 1$ and $x_j = 0$ for all $j \neq i$. We claim that the group of \mathcal{B} -continuous elements in $\lim_{\leftarrow}(G_n, \pi_n)$ is isomorphic to \mathbf{Z} and thus the system T exists by Theorem 1.4. To verify the claim we will show that $g = (i_2H_2, i_3H_3, \dots) \in \lim_{\leftarrow}(G_n, \pi_n)$ is \mathcal{B} -continuous iff there is an $m \in \mathbf{Z}$ such that $i_n = m \bmod 2^n$ for all n . If g is of this form, then $g_n = i_nH_n$ maps $B_n(iH_n)$ to $B_n((i+m) \bmod 2^n H_n)$ for all n , i.e. $x_i = 1$ becomes $x_{i+m \bmod 2^n} = 1$, a map which obviously can be described by a sliding block-code with code length $L = |m|$. And with g also g^{-1} is of the above form with $-m$, thus g is \mathcal{B} -continuous. On the other hand, if g is \mathcal{B} -continuous, then the \mathcal{B} -action of g is a sliding block code, say of coding length L . Let $n > 100L$ and consider the action of $g_n = i_nH_n$ on the block $B_n(2^{n-2}H_n)$ with the symbol $(1,0)$ in the middle. The image of this block has to be a block which sees at some offset m with $-L \leq m \leq L$ from the position of this symbol the symbol $(1,0)$ or $(0,1)$, where m is independent of n since we consider a sliding block code. Let k be the index such that $x_k = 1$ in the image-block; then $i_n = (k - 2^{n-2}) \bmod 2^n$. If the symbol in the image block would be $(0,1)$, then i_nH_n would map the block $B_n((2^{n-2} + 1)H_n)$ to $B_n((k-1)H_n)$ (since again $(0,1)$ in the image would occur at the same offset from the original $(1,0)$ -symbol) and $i_n = (k - 2 - 2^{n-2}) \bmod 2^n$ would contradict the above value of i_n . Thus the image symbol has to be $(1,0)$. Thus $i_n = m \bmod 2^n$ for all $n > 100L$, and thus, by the structure of the inverse limit, for all n . \square

Theorem 2.5. *There is a coded system T with $\text{aut}(T) \approx \langle \sigma \rangle \oplus G$, where $G = \{a, b; a^2 = b^2 = e\}$ is the free product of two copies of $\mathbf{Z}/2\mathbf{Z}$.*

Proof. The construction is quite similar to the last one. For each $n \geq 2$ let H_n be the subgroup of G generated by the element $(ab)^{2^{n-1}}$. Then H_n is normal; let $G_n = G/H_n$. The elements of G_n can be presented as $b^j(ab)^kH_n$, $0 \leq k \leq 2^{n-1} - 1$, $j \in \{0,1\}$. Let $A = \{(3,3), (3,0), (0,3), (3,1), (1,3)\}$. Let $k(n) = 2^{n-1}$ and let $B_n(b^j(ab)^k \cdot H_n)$ be the block $(x_0, x_{2^n-1})(x_1, x_{2^n-2})(x_2, x_{2^n-3}) \cdots (x_{2^n-1-1}, x_{2^n-1}) \in A^{k(n)}$ with $x_i = 3$ for all $i \neq 2k + j$ and $x_{2k+j} = j$.

We claim that the subgroup of \mathcal{B} -continuous elements in $\lim_{\leftarrow}(G_n, \pi_n)$ is isomorphic to G ; then we are done by Theorem 1.4. To prove this claim, we embed G into $\lim_{\leftarrow}(G_n, \pi_n)$ by a map that acts on the generators as $b \rightarrow g_b = (bH_2, bH_3, \dots)$ and $a \rightarrow g_a = (aH_2, aH_3, \dots)$. Let G' be the isomorphic image of G under this embedding. We show that g_b and g_a , and thus all elements of G' , are \mathcal{B} -continuous. Since bH_n maps $B_n(b^j(ab)^k \cdot H_n)$ to $B_n(b^{j+1 \bmod 2}(ab)^k \cdot H_n)$, its action on these blocks is a permutation which exchanges the blocks with $x_{2k} \neq 3$ and $x_{2k+1} \neq 3$ for all $0 \leq k \leq 2^{n-1} - 1$. Since $x_{2k} = 0$ if it is not 3, and $x_{2k+1} = 1$ if it is not 3, this permutation can be described for all n by a sliding block code of coding length $L = 1$. The same holds for the action of aH_n which exchanges the blocks with $x_{2k+1} \neq 3$ and $x_{2k+2 \bmod 2^n} \neq 3$ for all $0 \leq k \leq 2^{n-1} - 1$. Now let $g = (h_2H_2, h_3H_3, \dots)$ be a \mathcal{B} -continuous element of $\lim_{\leftarrow}(G_n, \pi_n)$. Say its \mathcal{B} -action has coding length L . As in the proof of Theorem 2.4, let $n > 100L$ and consider the action of h_nH_n on the block $B_n((ab)^k \cdot H_n)$ where $k = 2^{n-2}$, i.e. the block with the symbol $(0,3)$ in the middle. If the image block would see a symbol $(3,0)$ or $(3,1)$, this would contradict the fact that h_nH_n acts as left-multiplication (as in the proof of Theorem 2.4). Thus the image block sees a symbol $(0,3)$ or $(1,3)$ within an offset

of $-L \leq m \leq L$ from the position of $(0, 3)$ in $B_n((ab)^k \cdot H_n)$. Since we consider a block code, this offset and the image symbol are the same for all $n > 100L$. Thus there is a product $g' = g(1)g(2) \cdots g(j)$ with $j \leq L$ of generators $g(i)$ from $\{g_b, g_a\}$ such that, writing $g' = (g_2, g_3, \dots) \in \lim_{\leftarrow}(G_n, \pi_n)$, we have that $g_n = h_n H_n$ for all $n > 100L$. By the structure of an inverse limit this holds also for $n \leq 100L$; thus $g = g' = g(1) \cdots g(j) \in G'$. \square

It remains an open problem whether there is a coded system T with $\text{aut}(T) \approx \langle \sigma \rangle \oplus$ the free product of three copies of $\mathbf{Z}/2\mathbf{Z}$.

Our method of constructing automorphism groups is closed under taking direct sums.

Theorem 2.6. *For each $n \in \mathbf{N}$ let H_n be a countable group which has a continuous block presentation. Let $G = \bigoplus H_n$. Then G has a continuous block presentation. In particular, there is a coded system T such that $\text{aut}(T) \approx \langle \sigma \rangle \oplus G$.*

Proof. First observe that any block presentation with alphabet A of some inverse limit can be replaced by one with the alphabet $\{3, 4\}$ and the same continuous elements—simply replace any symbol of A by one of the blocks $3^i 4^{n-i}$, $1 \leq i \leq \text{card}(A)$, $n = \text{card}(A) + 1$.

Thus, for each $n \in \mathbf{N}$ there is an inverse limit $\varprojlim_k (H_{n,k}, \pi_{n,k})$ of finite groups $H_{n,k}$ and homomorphisms $\pi_{n,k} : H_{n,k+1} \rightarrow H_{n,k}$, and a block presentation \mathcal{B}_n with alphabet $\{3, 4\}$ and blocks $B_{n,k}(h)$, $h \in H_{n,k}$, such that the group of \mathcal{B}_n -continuous elements in $\varprojlim_k (H_{n,k}, \pi_{n,k})$ is isomorphic to H_n .

In the following let $p = 3$ and $q = 5$.

For each n we modify the block presentation \mathcal{B}_n in that in each $B_{n,k}(h)$ we replace a 3 by the block $5^i 35^i$ and a 4 by the block $5^i 45^i$, where $i = p^n$. We call the obtained block again $B_{n,k}(h)$ and the presentation \mathcal{B}_n . Observe that this “stretching” of the blocks did not change the group of continuous elements in $\varprojlim_k (H_{n,k}, \pi_{n,k})$.

Define $G_n = H_{1,n} \oplus H_{2,n} \oplus H_{3,n} \oplus \cdots \oplus H_{n,n}$. Let $\pi_n : G_{n+1} \rightarrow G_n$ be the map which drops the last coordinate and then applies the suitable $\pi_{n,k}$ ’s, i.e. $\pi_n(u_1, u_2, \dots, u_{n+1}) = (\pi_{1,n}(u_1), \pi_{2,n}(u_2), \dots, \pi_{n,n}(u_n))$.

We define a block presentation \mathcal{B} for $\lim_{\leftarrow}(G_n, \pi_n)$ with alphabet $\{*, 3, 4, 5\}$. Let $u(n) = *5 \cdots 535 \cdots 5 * 5 \cdots 545 \cdots 5$ where the strings of 5’s have length q^n . Let $B_n(g_n) = u(n) * B_{1,n}(h_1) * B_{2,n}(h_2) * \cdots * B_{n,n}(h_n) *$ for all n , $g_n = (h_1, \dots, h_n) \in G_n$.

It remains to show that the group of \mathcal{B} -continuous elements in $\lim_{\leftarrow}(G_n, \pi_n)$ is isomorphic to $\bigoplus H_n$.

For $h_n \in H_n$ let $\alpha(h_n)$ denote the element (g_1, g_2, \dots) in $\lim_{\leftarrow}(G_n, \pi_n)$ where the n th coordinate of each g_i with $i \geq n$ equals h_n and all the others are the identity element. Consider for $m \geq n$ a block $B_m(g'_m) = u(m) * B_{1,m}(h'_1) * B_{2,m}(h'_2) * \cdots * B_{m,m}(h'_m) *$, $g'_m = (h'_1, \dots, h'_m) \in G_m$. Then under the \mathcal{B} -action of $\alpha(h_n)$ this block gets mapped to a block where just $B_{n,m}(h'_n)$ is replaced by $B_{n,m}(h_n h'_n)$ and all other coordinates remain fixed. Since only $B_{n,m}(h'_n)$ contains blocks $a5^{2i}b$, with $i = p^n$ and $a, b \in \{3, 4\}$, it can be recognized by a sliding block code, and thus the block code describing the \mathcal{B}_n -action of h_n can be extended to a block code describing the \mathcal{B} -action of $\alpha(h_n)$. Observe that α extends to an embedding of $\bigoplus H_n$ into $\lim_{\leftarrow}(G_n, \pi_n)$. Thus $\alpha(\bigoplus H_n)$ is contained in the \mathcal{B} -continuous elements of $\lim_{\leftarrow}(G_n, \pi_n)$.

Now let $g = (g_1, g_2, \dots) \in \lim_{\leftarrow}(G_n, \pi_n)$ be \mathcal{B} -continuous. Let L be a coding length of the block code ϕ describing the \mathcal{B} -action of g . Consider n with $q^n > L$.

By g_n the block $B_n(e)$ gets mapped to $B_n(g_n)$. But $B_n(e)$ and $B_n(g_n)$ both begin with $u(n) = *5 \cdots 535 \cdots 5*5 \cdots 545 \cdots 5$. Thus the block code ϕ fixes all the blocks $5 \cdots 535 \cdots 5$ and $5 \cdots 545 \cdots 5$, where the strings of 5's exceed a certain length. This implies that ϕ fixes all the blocks $B_{n,k}(h)$, whenever n is large enough. It follows that there is an N such that for all $n \geq N$ $g_n = (h_1, h_2, \dots, h_N, e, e, \dots, e)$, i.e. $g = \alpha(h_1, h_2, \dots, h_N)$ and thus is an element of $\alpha(\bigoplus H_n)$. The last statement follows by Theorem 1.4. \square

Corollary 2.7. *For any infinite, finitely generated abelian group H there is a coded system T with $\text{aut}(T) \approx H$.*

Proof. Any such H can be written as $\mathbf{Z} \oplus G$ with G a direct sum of copies of \mathbf{Z} and finite cyclic groups. By Theorem 2.1, Theorem 2.4, and Theorem 2.6 there is a coded system T with $\text{aut}(T) \approx \langle \sigma \rangle \oplus G$. \square

Corollary 2.8. *If G is a subgroup of \mathbf{Q}/\mathbf{Z} then there is a coded system T with $\text{aut}(T) \approx \langle \sigma \rangle \oplus G$ iff G is residually finite (which holds if its p -torsion subgroup is finite for every prime).*

Proof. If $\text{aut}(T) \approx \langle \sigma \rangle \oplus G$ for a coded system T , then $G \approx \{e\} \oplus G$ has to be residually finite. On the other hand, each residually finite subgroup G in \mathbf{Q}/\mathbf{Z} is isomorphic to $\bigoplus H_p$ with each H_p a finite subgroup of $\mathbf{Z}(p^\infty)$, p prime (see the proof of Proposition 3.6 in [BLR]). Apply Theorem 2.1 and Theorem 2.6. \square

Since there are only countable many SFTs, there are only countable many automorphism groups of SFTs.

Corollary 2.9. *There are uncountably many nonisomorphic automorphism groups for coded systems.*

Proof. Let $J \subset \mathbf{N}$ be a set of primes. Then there is a coded system $T(J)$ with $\text{aut}(T(J)) \approx \langle \sigma \rangle \oplus G(J)$, where $G(J)$ is the direct sum of all cyclic groups of order p with $p \in J$, by Theorem 2.1 and Theorem 2.6. Distinct sets J yield nonisomorphic groups $G(J)$, and there are uncountably many such sets J . \square

A self-contained argument shows that shifts with periodic points dense and synchronized systems have the same automorphisms subgroups.

Theorem 2.10. *Let R be a subshift with periodic points dense. Then there is a synchronized system S such that $\text{aut}(S)$ contains a copy of $\text{aut}(R)$.*

Proof. We have $R \subset A^{\mathbf{Z}}$ for some finite alphabet A . For a periodic point $x \in R$ of least period, say k , define $B(x) = (x_1, x_k)(x_2, x_{k+1}) \cdots (x_k, x_1) \in (A \times A)^k$. Let $B_R = \{B(x) | x \text{ is a periodic point in } R\}$. Let $*$ be a symbol not in $A \times A$. Let S be the coded system given by the code $Y = \{*B(x) | x \text{ is a periodic point in } R\}$. Then $*$ is a synchronizing symbol for S . Any automorphism Φ of R induces a bijection $\pi_\Phi : B_R \rightarrow B_R$ by $B(x) \rightarrow B(\Phi(x))$. Since Φ is continuous and $|\pi_\Phi(B(x))| = |B(x)|$ and because of the special structure of the $B(x)$ -blocks, π_Φ extends to an automorphism of S which leaves the symbol $*$ fixed, also denoted π_Φ . Then $\alpha : \Phi \in \text{aut}(R) \rightarrow \pi_\Phi \in \text{aut}(S)$ is a group homomorphism, which is injective, since $\alpha(\Phi) = \text{id}$ implies that $\Phi = \text{id}$ on periodic points, which are dense in R , thus $\Phi = \text{id}$. \square

Definition 2.11. Let R be a subshift. For an automorphism $\Phi \in \text{aut}(R)$ let $\alpha_k(\Phi)$ denote the restriction of Φ to the periodic points with least period $\leq k$. A subgroup

$G \subset \text{aut}(R)$ is closed if whenever $\Phi_n \in G$, $n \in \mathbf{R}$, $\Phi_n \rightarrow \Phi \in \text{aut}(R)$ in periodic point topology (i.e. for each k there is an n_k such that $\alpha_k(\Phi_n) = \alpha_k(\Phi)$ for all $n \geq n_k$), then $\Phi \in G$.

Theorem 2.12. *An abstract group G has a continuous block presentation iff G is isomorphic to a closed subgroup of an automorphism group of some subshift R with periodic points dense.*

Thus an application of Theorem 1.4 yields immediately

Theorem 2.13. *Let R be a subshift with periodic points dense. Let $G \subset \text{aut}(R)$ be a closed subgroup. Then there is a coded system T such that $\text{aut}(T) \approx \langle \sigma \rangle \oplus G$. In particular, there is a coded system with $\text{aut}(T) \approx \langle \sigma \rangle \oplus \text{aut}(R)$.*

Proof of Theorem 2.12. A group with a continuous block presentation is isomorphic to a closed subgroup of the automorphism group of a coded system by Propositions 1.6 and 1.10.

Now assume that G is a closed subgroup. Let $P_n(R)$ denote the set of periodic points in R with period at most n . For any automorphism $g \in G$ let $\alpha_n(g)$ denote the restriction of g to the points in $P_n(R)$. Let $G_n = \{\alpha_n(g) | g \in G\}$ be the group of bijections on $P_n(R)$ obtained in this way. Since $P_{n+1}(R) \supset P_n(R)$, there are natural group homomorphisms $\pi_n : G_{n+1} \rightarrow G_n$. Periodic points are dense in R ; thus for any automorphism $g \neq \text{id}$ we have $\alpha_n(g) \neq \text{id}$ for some n . So $\alpha(g) := (\alpha_1(g), \alpha_2(g), \dots)$ defines an embedding of G into $\lim_{\leftarrow} (G_n, \pi_n)$. We will define a block presentation \mathcal{B} of $\lim_{\leftarrow} (G_n, \pi_n)$ such that $\alpha(G)$ is the group of \mathcal{B} -continuous elements of $\lim_{\leftarrow} (G_n, \pi_n)$.

We have $R \subset (A')^{\mathbf{Z}}$ for some infinite alphabet A' . The alphabet A for the block presentation \mathcal{B} will be $A := \{*\} \cup A' \cup A' \times A'$, where $*$ is a new symbol. For $x \in P_n(R)$ define $B'(x) = B(x)x[1, n!]B(x) \in A^{3n!}$ where $B(x) = (x_1, x_n)(x_2, x_{n-1}) \cdots (x_n, x_1) \in (A' \times A')^{n!}$. Fix an enumeration $B(n, 1), B(n, 2), \dots, B(n, s)$ of the blocks $B'(x)$, $x \in P_n(R)$. Any element $g_n \in G_n$ induces a permutation of these blocks, and thus of $\{1, 2, \dots, s\}$, say τ_{g_n} . We represent $g_n \in G_n$ by $B_n(g_n) := *B(n, \tau_{g_n}(1)) * B(n, \tau_{g_n}(2)) * \cdots * B(n, \tau_{g_n}(s)) *$.

Now let $g \in G$, and let L be a coding length for g . Then, by definition, the \mathcal{B} -action of $\alpha(g)$ is that, for all n , $\alpha_n(g)$ maps $B_n(h_n)$ to $B_n(\alpha_n(g)h_n)$. But this can be described by a sliding block code with the same coding length L since the symbol $*$, which remains fixed, separates the different $B(n, \tau_{g_n}(i))$ -blocks and because of the special structure of the $B'(x)$ -blocks at the left and right end of a $B(n, \tau_{g_n}(i))$ -block. The same holds for g^{-1} ; thus $\alpha(g)$ is \mathcal{B} -continuous.

Now let $h = (h_1, h_2, \dots) \in \lim_{\leftarrow} (G_n, \pi_n)$ be \mathcal{B} -continuous. Thus, for some $L \geq 0$ there is a map $\phi : (A \cap \{\omega\})^{2L+1} \rightarrow A$ such that for all $n \in \mathbf{Z}$, $g_n \in G_n$ we have $B_n(h_n g_n) = \Phi_n^{(\phi)}(B_n(g_n))$. Define a shift commuting map $\Psi : R \rightarrow A^{\mathbf{Z}}$ by $\Psi(t)_0 = \phi(t_{-L}, \dots, t_L)$. Let x be a periodic point. Choose n such that $n! \geq 2L + n$ and $x \in P_n(R)$. Then also $\Psi(x)$ is a periodic point in $A^{\mathbf{Z}}$ with period at most n . We show that $\Psi(x) \in R$. Now, $\Phi_n^{(\phi)}$ maps $B_n(e) = *B(n, 1) * B(n, 2) * \cdots * B(n, s) *$ to $B_n(h_n) = *B(n, \tau_{h_n}(1)) * B(n, \tau_{h_n}(2)) * \cdots * B(n, \tau_{h_n}(s)) *$. The block $x[1, n!]$ occurs as the middle part of $B(n, i)$, say. Let $y \in P_n(R)$ such that the middle part of $B(n, \tau_{h_n}(i))$ equals $y[1, n!]$. Thus $\Psi(x)[1 + L, n! - L] = y[1 + L, n! - L]$. The length of these blocks is larger than the periods of $\Psi(x)$ and y , thus $\Psi(x) = y$. This proves $\Psi : R \rightarrow R$, since periodic points are dense in R . The same arguments applied to h^{-1} lead to an endomorphism $\Psi_1 : R \rightarrow R$. Considering again the set of

periodic points shows that $\Psi\Psi_1 = \Psi_1\Psi = \text{id}$ on periodic points, which are dense; thus $\Psi \in \text{aut}(R)$. Observe that $\alpha(\Psi) = h$ by definition of Ψ . Thus it only remains to show that $\Psi \in G$. By definition of G_n , for each n there is a $g(n) \in G$ with $\alpha_n(g(n)) = h_n$. Thus $g(n)$ acts on the periodic points with period less than or equal to n in the same way as Ψ . Thus, $\Psi = \lim g(n)$ on periodic points. Since G is a closed subgroup, this implies $\Psi \in G$. \square

As an application, from Theorem 2.13 we get a coded system which has $\mathbf{Z}[1/2]$ as a subgroup of its automorphism group. In particular, this shows that an automorphism of a coded system of infinite order can have n th roots for infinitely many n . It is not known whether an SFT can have such an automorphism ([BLR, Problem 3.5]).

Theorem 2.14. (a) *There is a subshift R with periodic points dense with $\text{aut}(R) \approx \mathbf{Z}[1/2] \oplus C$, where C is the direct sum of the finite cyclic groups of orders $2^{(2^{n+2})} - 1$, $n \geq 1$, and $\mathbf{Z}[1/2]$ corresponds to a closed subgroup of $\text{aut}(R)$.*

(b) *There is a coded system T with $\text{aut}(T) \approx \langle \sigma \rangle \oplus \mathbf{Z}[1/2]$.*

(c) *There is a synchronized system S such that $\mathbf{Z}[1/2]$ is a subgroup of $\text{aut}(S)$.*

Remark. A straightforward modification of the following proof (which is left to the reader) shows that for any prime p there is a coded system T with $\text{aut}(T) \approx \langle \sigma \rangle \oplus \mathbf{Z}[1/p]$. For notational convenience we give the proof only for $p = 2$.

Proof. (a) implies (b) and (c) via Theorem 2.13 and Theorem 2.10, respectively. We shall prove (a). The following construction was inspired by [BLR, Example 3.9].

Let $A = \{0, a, b\}$. We start by defining a subshift $R \subset A^{\mathbf{Z}}$ as the closure of certain orbits $B(n)^{\infty}$ for certain blocks $B(n)$, $n \in \mathbf{N}$. For that we begin to define inductively a family of blocks $B(n, k)$, $1 \leq k \leq 2^n$, $n \geq 1$. Let $B(1, 1) = a$, $B(1, 2) = b$ and $L(1) = 1 = |B(1, 1)|$. Then for $n \geq 1$

$$\begin{aligned} B(n+1, 2i-1) &:= B(n, i)0^{L(n)}B(n, i), & 1 \leq i \leq 2^n, \\ B(n+1, 2i) &:= B(n, i)0^{L(n)}B(n, i+1), & 1 \leq i < 2^n, \\ B(n+1, 2^{n+1}) &:= B(n, 2^n)0^{L(n)-1}B(n, 1)0, \\ L(n+1) &:= |B(n+1, 1)|. \end{aligned}$$

Then by induction $L(n) = 3^{n-1} = |B(n, k)|$, $1 \leq k \leq 2^n$. Let

$$B(n) := B(n, 1)0^k B(n, 2)0^k \cdots B(n, 2^n - 1)0^k B(n, 2^n)0^{k-1},$$

where $k = k(n) \geq |B(n, 1)|$ is chosen (uniquely mod $2^{f(n)} - 1$) such that $|B(n)| = 2^{f(n)} - 1$, $f(n) = 2^{n+2}$, $n \geq 1$. Let R be the closure of the union of all orbits $B(n)^{\infty}$. Let σ be the shift on R . By induction on n it is easy to see that

- each $B(n, k)$ begins with a symbol $\neq 0$,
- each $B(n, 1)$ ends with the symbol “ a ”,
- for each $B(n, k)$ one of the last two symbols is $\neq 0$,
- the blocks $B(n, k)$, $1 \leq k \leq 2^n$, are pairwise distinct.

Thus, in particular no block $B(n, k)$ contains $0^{L(n)-1}$ as a subblock.

For $n \geq 1$ we define a map $\psi(n)$ on the union of all orbits $B(m)^{\infty}$, $m \in \mathbf{N}$, as follows:

If $x \in B(k)^{\infty}$ for some $1 \leq k < n$, then let $\psi(n)(x) = \sigma^K(x)$, where $0 \leq K < 2^{f(k)} - 1$ is chosen such that $K \cdot 2^n = 1 \pmod{2^{f(k)} - 1}$. On orbits $B(m)^{\infty}$ with

$m \geq n$, we define $\psi(n)$ by a block exchange rule: replace $B(n, i)$ by $B(n, i + 1)$ for $1 \leq i < 2^n$ and $0B(n, 2^n)$ by $B(n, 1)0$, and let no other action take place. This gives a well-defined map on $B(m)^\infty$ -orbits, since any two such blocks in $B(m)^\infty$ are on disjoint index sets by construction. Then we have that $\psi(n)(x)_i$ is determined by $x[-2|B(n)| + i, i + 2|B(n)|]$ for all points x of some $B(m)^\infty$ -orbit and all $i \in \mathbf{Z}$, and thus extends to a continuous map on R commuting with the shift.

We now show that $\psi(n)$ maps each $B(m)^\infty$ into itself. Then $\psi(n)$ extends to an endomorphism $R \rightarrow R$, which we call again $\psi(n)$.

Claim 1. For all $n \geq 0$, $m \geq 0$, and $x \in B(n + m)^\infty$

$$\psi(n)(x) = \sigma^{\alpha(n+m, n)}(x)$$

where $\alpha(k, n) = 2^{f(k)-n}$.

Proof. Induction on m .

For $m = 0$ and arbitrary $n \geq 0$, $x \in B(n)^\infty$ we have $\psi(n)(x) = \sigma^{\alpha(n, n)}(x)$ by inspection. Now assume the claim holds for all $m' \leq m + 1$, $n \geq 0$, $x \in B(n + m')^\infty$. Using the definition of the blocks $B(n + 1, k)$ and the definition of the map $\psi(n)$ shows that $\psi(n)$ maps the block $0B(n + 1, i)$ to $0B(n + 1, i + 2)$ for $1 \leq i < 2^{n+1} - 1$, the block $0B(n + 1, 2^{n+1} - 1)$ to $B(n + 1, 1)0$, and $0B(n + 1, 2^{n+1})$ to $B(n + 1, 2)0$. Thus $\psi(n)$ acts on the blocks $0B(n + 1, k)$ as $\psi(n + 1)^2$ does. Now let $x \in B(n + m + 1)^\infty$. Then $\psi(n)(x) = \psi(n + 1)^2(x) = \sigma^{2\alpha(n+1+m, n+1)}(x)$ by induction hypothesis, and by the definition of α this equals $\sigma^{\alpha(n+1+m, n)}(x)$.

Thus for all n we have that $\psi(n) : R \rightarrow R$ is onto and continuous. \square

Claim 2. $\psi(n + 1)^2 = \psi(n)$ for all n , and $\psi(1)^2 = \sigma$.

Proof. For $x \in B(n + 1 + k)^\infty$ for some $k \geq 0$ we have $\psi(n + 1)^2(x) = \psi(n)(x)$ from the last claim. If x lies in the orbit $B(k)^\infty$ for some $1 \leq k < n$ then $\psi(n + 1)(x) = \sigma^K(x)$, where $0 \leq K < 2^{f(k)} - 1$ satisfies $K \cdot 2^{n+1} = 1 \pmod{2^{f(k)} - 1}$, and $\psi(n)(x) = \sigma^L(x)$, where $0 \leq L < 2^{f(k)} - 1$ satisfies $L \cdot 2^n = 1 \pmod{2^{f(k)} - 1}$. Thus $\psi(n + 1)^2(x) = \sigma^{2K}(x) = \sigma^L(x) = \psi(n)(x)$. And for x in the orbit $B(n)^\infty$ we have that $\psi(n + 1)(x) = \sigma^K(x)$, where $0 \leq K < 2^{f(n)} - 1$ satisfies $K \cdot 2^{n+1} = 1 \pmod{2^{f(n)} - 1}$, i.e. $K = 2^{f(n)-n-1}$ and $\psi(n)(x) = \sigma^L(x)$, where $L = 2^{f(n)-n}$ just by the definition of the block $B(n)$. Thus, in this case $\psi(n + 1)^2 = \psi(n)$, too. Finally, $\psi(1)^2 = \sigma$ since $\psi(1)$ is the block exchange map $a \rightarrow b$, $0b \rightarrow a0$ and all the orbits $B(m)^\infty$ are built out of the blocks $B(1, 1) = a$ and $B(1, 2) = b$ against a background of zeros.

Thus $\psi(n)^{2^n} = \sigma$ for all n , which proves that each $\psi(n)$ is an automorphism of R . This proves that σ and the automorphisms $\psi(n)$, $n \geq 1$, generate a subgroup G of $\text{aut}(R)$ which is isomorphic to $\mathbf{Z}[1/2]$. Finally we have to show that the subgroup G is closed. \square

Claim 3. The periodic orbits of R are 0^∞ and the orbits $B(n)^\infty$, and no others.

Proof. Of course, $0^\infty \in R$. Let $x \in R$ be periodic with period M and $x_0 \neq 0$. Let $m = |B(1)| \cdot |B(2)| \cdots |B(M)|$. Since R is the closure of the periodic orbits $B(n)^\infty$, the block $x[0, mM]$ occurs as a subblock of some $B(n)^\infty$. Choose the least such n . Assume $n > M$. By the minimality of n , $x[0, mM]$ is not contained in a $B(n - 1, j)$ -block. Thus $x[0, mM]$ contains $0^{L(n-1)}$ or $0^{k(n)}$. But $k(n)$, $L(n - 1) \geq n - 1 \geq M$, contradicting the fact that x does not see 0^M . Thus $n \leq M$, and therefore m is a multiple of $|B(n)|$, which proves $x \in B(n)^\infty$. This proves the claim. \square

Claim 4. For any $\Phi \in \text{aut}(R)$ there is some $\psi \in G$ such that $\Phi = \psi$ on all but finitely many periodic orbits.

Proof. Let $\Phi \in \text{aut}(R)$ with coding length, say, L . Then $\Phi(0)^\infty = 0^\infty$, since R has only one fixed point. If x lies in the orbit $B(n)^\infty$ then so does $\Phi(x)^\infty$, since there is only one orbit with least period $|B(n)|$. Choose n so large that $k(n) - 2L > |B(n, 1)|$, where $k(n)$ is from the definition of the block $B(n)$. We have $\Phi(x) = \sigma^M(x)$ for all x in the orbit $B(n)^\infty$ for some M . We want to show that $M = j \cdot 2^{f(n)-n} + m$ for some $-L \leq m \leq L$ and $0 \leq j < 2^n$. For that consider $B(n) = B(n, 1)0^k B(n, 2)0^k \cdots B(n, 2^n - 1)0^k B(n, 2^n)0^{k-1}$. Since $\Phi(0)^\infty = 0^\infty$ and L is a coding length, Φ maps $0^k B(n)$ to a block of the form

$$0^{k-L} C(n, 1) 0^{k-2L} C(n, 2) 0^{k-2L} C(n, 3) \cdots C(n, 2^n) 0^{k-1-L}$$

where $|C(n, i)| = |B(n, i)| + 2L$. Since Φ acts on x as some power of the shift, and since $k - 2L > |B(n, 1)|$, we have that the block $C(n, 1)$ contains exactly one of the blocks $B(n, i)$. This determines the above form of M . Thus $\Phi = \psi(n)^j \circ \sigma^m$ on the orbit $B(n)^\infty$. But now consider $B(n+1)$. We have

$$B(n+1) = B(n+1, 1)0^k B(n+1, 2)0^k \cdots B(n+1, 2^n - 1)0^k B(n+1, 2^n)0^{k-1},$$

where

$$B(n+1, 1) = B(n, 1)0^p B(n, 1), \quad p = |B(n, 1)| \geq n.$$

Thus Φ maps $0^L B(n+1, 1)0^L$ to $\sigma^m(B(n, j)0^p B(n, j))$. From this it follows that $\Phi(x) = \sigma^{M'}(x)$ for all x in the orbit $B(n+1)^\infty$, where $M' = 2j \cdot 2^{f(n+1)-n-1} + m$. Thus $\Phi = \psi(n+1)^{2j} \circ \sigma^m = \psi(n)^j \circ \sigma^m$ on the orbit $B(n+1)^\infty$. Inductively it follows that $\Phi = \psi(n)^j \circ \sigma^m$ on all the orbits $B(n+k)^\infty$, with $k \geq 0$. \square

Claim 5. $\text{aut}(R) \approx \mathbf{Z}[1/2] \oplus C$, where C is the direct sum of the finite cyclic groups of orders $|B(n)| = 2^{(2^{n+2})} - 1$, $n \geq 1$.

Proof. This follows from Claim 3 and Claim 4 \square

Claim 6. $G \approx \mathbf{Z}[1/2]$ is a closed subgroup of $\text{aut}(R)$.

Proof. For $n \in \mathbf{N}$ and $f(n) = 2^{n+2}$ let $G_n = \mathbf{Z}/(2^{f(n)} - 1)$. Since $(2^{f(n+1)} - 1) = (2^{f(n)} - 1)(2^{f(n)} + 1)$, the orders of the groups divide each other and thus the maps $\pi_n : G_{n+1} \rightarrow G_n$ defined by $\pi_n(a) = a \bmod 2^{f(n)} - 1$ are onto group homomorphisms.

Let G be the group generated by σ and the $\psi(n)$, $n \geq 1$. For $m \geq n$ let $\alpha(m, n) = 2^{f(m)-n}$. Observe that

$$\begin{aligned} \pi_m(\alpha(m+1, n)) &= 2^{f(m+1)-n} \bmod 2^{f(m)} - 1 = 2^{f(m)+f(m)-n} \bmod 2^{f(m)} - 1 \\ &= 2^{f(m)} 2^{f(m)-n} \bmod 2^{f(m)} - 1 = \alpha(m, n) \bmod 2^{f(m)} - 1. \end{aligned}$$

For $m < n$ let $\alpha(m, n)$ be such that $\psi(n)(x) = \sigma^{\alpha(m, n)}(x)$ for all $x \in B(m)^\infty$. Thus, by definition, $\alpha(m, n) \cdot 2^n = 1 \bmod 2^{f(m)} - 1$. Thus $\alpha(m, n) = 2^{f(m)-n}$. Therefore $\pi_m(\alpha(m+1, n)) = \alpha(m, n) \bmod 2^{f(m)} - 1$ for all m, n . Define a map $\alpha : G \rightarrow \lim_{\leftarrow} (G_n, \pi_n)$ as follows. For $g \in G$ choose $n \geq 1$ and $k \geq 0$ such that $g = \psi(n)^k$. Let $\alpha_m(g) := k \cdot \alpha(m, n)$. Since $2 \cdot \alpha(m, n+1) = 2 \cdot 2^{f(m)-n-1} = 2^{f(m)-n} = \alpha(m, n)$, this is well-defined and thus a group homomorphism. Now let $g_k \in G$ and $\Phi \in \text{aut}(R)$ be such that g_k converges to Φ in periodic point topology.

By Claim 4 we may assume that Φ is the identity on all orbits $B(n)^\infty$, $n \geq N$, for some N . Choose k so large that Φ and g_k coincide on all orbits $B(n)^\infty$, $n \leq N$. In particular, g_k is the identity on $B(N)^\infty$. Thus $\alpha_N(g_k) = 0$, since α_N describes the shift of g_k on $B(N)^\infty$. Thus $\alpha_n(g_k) = 0$ for all $n \leq N$, and so $\Phi = g_k$ is the identity on all $B(n)^\infty$, $n \leq N$. So Φ is the identity on all orbits $B(n)^\infty$, $n \in \mathbf{N}$, which are dense in R ; thus Φ is the identity on R , and so $\Phi \in G$. This proves that G is a closed subgroup of $\text{aut}(R)$. \square

Claims 5 and 6 prove part (a) of the theorem. \square

The following lemma shows in particular that an automorphism of an SFT which has an infinite chain of p th roots cannot be topologically conjugate to a coded system (which generalizes a remark in [BLR, p. 79]).

Lemma 2.15. *Let S be a nonfinite subshift, $i \neq 0$, and p prime. Assume that there are $\phi(n) \in \text{aut}(S)$, $n \geq 0$, such that $\phi(0) = \sigma^i$ (where σ is the shift on S), and $\phi(n) = \phi(n+1)^p$ for all $n \geq 0$. Then S is not coded.*

Proof. Assume that S is coded. We want to use the following observation: if $g(n)$, $n \geq 0$, is a sequence of elements in some finite group G with $g(n) = g(n+1)^p$ for all $n \geq 0$, then the order of $g(0)$ is not divisible by p . (Fix $n, m > 0$ such that $g(n) = g(n+m)$. Then $g(m) = g(n+m)^{p^n} = g(n)^{p^n} = g(0)$; thus $g(0)^{p^m} = g(m)^{p^m} = g(0)$, and so $g(0)^{p^m-1} = \text{id}$.)

Thus all we have to show to derive a contradiction is that for some $k \in \mathbf{N}$ the set $P_{pki}(S)$ of S -points with least period pki is nonempty, since then the restrictions $g(n)$ of the automorphisms $\phi(n)$ to $P_{pki}(S)$ are elements of the symmetric group on $P_{pki}(S)$ and satisfy $g(n) = g(n+1)^p$ for all $n \geq 0$, but the order of $g(0) = (\sigma^i \text{ restricted to } P_{pki}(S))$ would be pk and thus divisible by p .

Let X be a code for S . If for any finite concatenation x of blocks from X the orbit x^∞ would be the same, then S would coincide with this orbit, thus would be finite. So there are concatenations of X -blocks, say x and y , such that x^∞, y^∞ are different orbits. Now replace x by $x^{|x|}$ and y by $y^{|x|}$ to obtain blocks of the same length. Then, for all $n > 3$, $(xy^n)^\infty$ is a periodic orbit with least period $(n+1)|x|$. Thus we may choose n such that $(n+1)/i$ is a multiple of p ; thus $(n+1)|x| = pki$ for some k . \square

Theorem 2.16. *There is a subshift R with periodic points dense such that $\text{aut}(R)$ is not isomorphic to the automorphism group of a coded system.*

Remark. It remains an open problem whether a transitive subshift with periodic points dense can have an automorphism group which is not that of a coded system.

Proof. By Theorem 2.14(a) there is a subshift R with periodic points dense and $\text{aut}(R) = \mathbf{Z}[1/2] \oplus C$, where C is the direct sum of the finite cyclic groups. Let T be a subshift such that $\text{aut}(T)$ is isomorphic to $\mathbf{Z}[1/2] \oplus C$. Let $g \in \mathbf{Z}[1/2] \oplus C$ be the image of the shift σ of T . Then there is an $i > 0$ such that $g^i = (h, e)$, where e is the identity element in C . There is a sequence of square roots $h(n) \in \mathbf{Z}[1/2]$ with $h(0) = h$ and $h(n) = h(n+1)^2$ for all $n \geq 0$. Thus the preimages $\phi(n) \in \text{aut}(T)$ of $(h(n), e)$, $n \in \mathbf{N}$, satisfy $\phi(0) = \sigma^i$ and $\phi(n) = \phi(n+1)^2$ for all $n \geq 0$. Then T is not coded by Lemma 2.15. \square

Theorem 2.4 in [BLR] shows that the free product of finitely many copies of $\mathbf{Z}/2\mathbf{Z}$ is a subgroup of the automorphism group of any SFT. This generalizes to

Theorem 2.17. *The automorphism group of any nonfinite synchronized system S contains a copy of the free product of all finite groups.*

Proof. Fix an enumeration of all finite groups, say H_1, H_2, \dots . Let e_n denote the identity element of H_n . Let G denote the free product of H_1, H_2, \dots . Let A be the disjoint union of the sets $H_n - \{e_n\}$. Elements in G are the identity e or can be uniquely presented in reduced form, i.e. by finite blocks $w_1 \cdots w_k$ with symbols in A such that $w_i \in H_n$ implies $w_{i+1} \notin H_n$.

Let m be a synchronizing block such that mm is an S -block. The set of all S -blocks of the form mwm , where w is a block, is a code for S . Now copy the argument from the proof of Lemma 2.15 to see that there are blocks $u = mam$ and $v = mbm$ such that the orbits u^∞ and v^∞ are distinct and of the same length $|u|$.

For each n fix an injective map

$$H_n - \{e_n\} \rightarrow \{v^2 u v^{n+3} u^{|H_n|-i+1} v u^{i+1} v^2 \mid 1 \leq i \leq |H_n| - 1\}.$$

We denote the image of $h \in H_n - \{e_n\}$ by $B(n, h)$. Let $B(n, e_n) = v^{L(n)/|v|}$. Let $L(n) = |B(n, h)|$, if $h \in H_n$. Observe that each $B(n, h)$ is an S -block and that distinct blocks $B(n, h)$, $B(m, g)$ can overlap at most $2|v|$.

For each $a \in H_n$ we define a map $\Psi(a)$ on S as follows: Let $\mathcal{C}_n = \{C \mid C \text{ is an } S\text{-block of length } L(n) \text{ and begins with } v^2 uv, C \neq B(n, h) \text{ for all } h \in H_n - \{e_n\}\}$. Then $\Psi(a)$ is the block exchange map which for each $C \in \mathcal{C}_n$, $h \in H_n$ replaces $B(n, e_n)B(n, h)C$ by $B(n, e_n)B(n, ah)C$ and lets no other action take place. $\Psi(a)$ is well defined, since the blocks in the definition of $\Psi(a)$ can overlap at most $L(n) - 2|v|$ and the replacements change only the middle part of length $\leq L(n)$. Since E and all blocks $B(n, h)$ begin and end with the synchronizing block v , $\Psi(a)$ is an endomorphism of S . Clearly $\Psi(a) \circ \Psi(a^{-1}) = \text{id} = \Psi(a^{-1}) \circ \Psi(a)$. Thus $\Psi(a) \in \text{aut}(S)$.

For $a, b \in H_n$ we have $\Psi(a) \circ \Psi(b) = \Psi(ab)$ by inspection. Now let G' be the subgroup of $\text{aut}(S)$ generated by $\Psi(a)$, $a \in A$. Let $w_1 \cdots w_k \in G$ be in reduced form. The map $\Psi : w_1 \cdots w_k \rightarrow \Psi(w_1) \circ \cdots \circ \Psi(w_k) \in G'$ defines a group homomorphism $G \rightarrow G'$, which is onto by definition of G' . Now let $w_1 \cdots w_k \neq e$ in G be given in reduced form and let n_i be such that $w_i \in H_{n_i} - \{e\}$. Then $\Psi(w_1) \circ \cdots \circ \Psi(w_k)(v^\infty uv^\infty) = v^\infty B(n_1, w_1) \cdots B(n_k, w_k) v^2 uv^\infty \neq v^\infty uv^\infty$. Thus $\Psi(w_1 \cdots w_k) \neq \text{id}$, i.e. Ψ is injective. Thus G is isomorphic to G' . \square

REFERENCES

- [AM] R. Adler and B. Marcus, *Topological entropy and equivalence of dynamical systems*, Mem. Amer. Math. Soc., no. **219** (1979). MR **83h**:28027
- [BFK] M. Boyle, J. Franks and B. Kitchens, *Automorphisms of one-sided subshifts of finite type*, Ergod. Theory Dynamical Systems **10** (1990), 421–449. MR **91h**:58037
- [BH] F. Blanchard and G. Hansel, *Systèmes codés*, Theoret. Comput. Sci. **44** (1986), 17–49. MR **88m**:68029
- [BK] M. Boyle and W. Krieger, *Periodic points and automorphisms of the shift*, Trans. Amer. Math. Soc. **302** (1987), 125–149. MR **88g**:54065
- [BLR] M. Boyle, D. Lind and D. Rudolph, *The automorphism group of a shift of finite type*, Trans. Amer. Math. Soc. **306** (1988), 71–114. MR **89m**:54051
- [DGS] M. Denker, C. Grillenberger and K. Sigmund, *Ergodic theory on compact spaces*, Lecture Notes in Math., vol. 527, Springer, New York, 1976. MR **56**:15879
- [FF] D. Fiebig and U. Fiebig, *Covers for coded systems*, Symbolic Dynamics and its Application, Contemporary Math., vol. 135, Amer. Math. Soc., Providence, RI, 1992, pp. 139–180. MR **93m**:54068

- [H] G. A. Hedlund, *Endomorphisms and automorphisms of the shift dynamical system*, Math. Systems Theory **3** (1969), 320–375. MR **41**:4510
- [KRW] K. H. Kim, F. W. Roush and J. B. Wagoner, *Automorphisms of the dimension group and gyration numbers*, J. Amer. Math. Soc. **5** (1992), 191–212. MR **93h**:54026
- [LM] D. Lind and B. Marcus, *An introduction to symbolic dynamics and coding*, Cambridge Univ. Press, (to appear).
- [MKS] W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory*, Dover, New York, 1976. MR **54**:10423
- [R] J. Ryan, *The shift and commutativity*. II, Math. Systems Theory **8** (1974), 249–250. MR **52**:4265
- [W] R. Williams, *Classification of subshifts of finite type*, Ann. of Math. **98** (1973), 120–153; Errata **99** (1974), 380–381. MR **48**:9769

INSTITUT FÜR ANGEWANDTE MATHEMATIK, UNIVERSITÄT HEIDELBERG, IM NEUENHEIMER FELD
294, 69120 HEIDELBERG, GERMANY

E-mail address: Fiebig@math.uni-heidelberg.de