

*AUTOMORPHISMS OF SUBSHIFTS DEFINED BY
B-FREE SETS OF INTEGERS*

BY

MIECZYSLAW K. MENTZEN (Toruń)

Abstract. We prove that for the subshifts defined by the sets of \mathcal{B} -free numbers, where $\sum_{b \in \mathcal{B}} 1/b < \infty$ and the elements of \mathcal{B} are pairwise coprime, the set of homeomorphisms commuting with the shift T is trivial, i.e. $\text{Aut}(T) = \{T^n : n \in \mathbb{Z}\}$.

Introduction. In [7], Sarnak proposed to study dynamical properties of the subshifts determined by the Möbius function $(^1) \mu : \mathbb{Z} \rightarrow \{-1, 0, 1\}$ and its square μ^2 . The function μ^2 is the characteristic function of the set \mathcal{F}_S of square-free numbers:

$$\mathcal{F}_S = \{n \in \mathbb{Z} : \text{no square of prime number divides } n\}.$$

By setting $\eta_S = \mathbb{1}_{\mathcal{F}_S} \in \{0, 1\}^{\mathbb{Z}}$ and $\mathcal{O}(\eta_S) = \{T^n(\eta_S) : n \in \mathbb{Z}\}$, the orbit of η_S under the shift $T : \{0, 1\}^{\mathbb{Z}} \rightarrow \{0, 1\}^{\mathbb{Z}}$, $T(x)[n] = x[n+1]$, we obtain the square-free subshift (X_S, T) , where $X_S = \overline{\mathcal{O}(\eta_S)}$. Sarnak proved that it has positive topological entropy (equal to $\frac{6}{\pi^2} \log 2$).

The square-free subshift (X_S, T) is a particular case of \mathcal{B} -free subshifts which are defined in the following way (e.g. [2], [3], [5]).

Let $b_1 < b_2 < \dots$ be a sequence of positive integers satisfying the following conditions:

- S-1. $b_1 > 1$,
- S-2. b_i, b_j are coprime for $i \neq j$,
- S-3. $\sum_{i \geq 1} 1/b_i < \infty$.

Denote $\mathcal{B} = \{b_1, b_2, b_3, \dots\}$ and let

$$\mathcal{F} = \mathbb{Z} \setminus \bigcup_{i \geq 1} b_i \mathbb{Z} = \{n \in \mathbb{Z} : \text{no } b_i \text{ divides } n\}$$

be the set of \mathcal{B} -free numbers.

2010 *Mathematics Subject Classification*: Primary 37B05; Secondary 37B10.

Key words and phrases: \mathcal{B} -free numbers, automorphisms of discrete flow, Möbius function.

Received 17 March 2016; revised 29 May 2016.

Published online 9 December 2016.

⁽¹⁾ Recall $\mu(\pm 1) = 1$, $\mu(\pm n) = (-1)^k$ if n is the product of k different primes, and $\mu(n) = 0$ in other cases.

Define $\eta \in \{0, 1\}^{\mathbb{Z}}$ by the formula

$$\eta[n] = 0 \Leftrightarrow \exists_i b_i \mid n,$$

i.e. $\eta = \mathbf{1}_{\mathcal{F}}$. As before, let $X = \overline{\mathcal{O}(\eta)}$ be the orbit closure of η in $\{0, 1\}^{\mathbb{Z}}$ and denote $\mathcal{X} = (X, T)$. Note that if \mathcal{B} is the set of squares of all prime numbers, then we obtain the square-free subshift.

The subshift \mathcal{X} defined above has positive topological entropy equal to $\prod_{j \geq 1} (1 - 1/b_j) \log 2$ (see [2]). It is proved in [5] that X is *hereditary*, i.e. if $x \in X$ and $y \preceq x$ then $y \in X$, where $y \preceq x$ iff $y[n] \leq x[n]$ for all n . The flow \mathcal{X} is also *proximal* ([3], see [7] for the square-free case), that is, for any $x, y \in X$ there is a sequence $(k_j)_{j \geq 1}$ of integers such that both $(T^{n_j}(x))_{j \geq 1}$ and $(T^{n_j}(y))_{j \geq 1}$ converge to the same limit ([4]). The proximality property forces \mathcal{X} to contain a unique minimal subset, which must be a fixed point; in our case this fixed point is $\bar{0} = \dots 0000 \dots$, the zero-sequence ([3]).

Recall that the *centralizer* $C(\mathcal{X}) = C(T)$ of \mathcal{X} is the semigroup of all continuous $\varphi : X \rightarrow X$ that commute with T , i.e. $T\varphi = \varphi T$. The group of all homeomorphisms from $C(T)$ will be denoted by $\text{Aut}(\mathcal{X})$; elements of this group will be called *automorphisms*. Notice that for no non-trivial proximal system do we have $C(T) = \text{Aut}(T)$. Indeed, the map $\varphi(x) = x_0$ (where $Tx_0 = x_0$) defines a non-invertible element of $C(T)$ (in other words the systems under consideration are never topologically coalescent, [1]).

The main aim of this note is to prove that for \mathcal{B} -free subshifts, when \mathcal{B} satisfies S-1, S-2, S-3, we have

$$\text{Aut}(T) = \{T^n : n \in \mathbb{Z}\}.$$

Let us introduce the following notation. All finite sequences of 0's and 1's, i.e. elements of $\{0, 1\}^k$ for some $k \geq 1$, will be called *blocks*. For a block $U \in \{0, 1\}^k$ denote $J(U) = \{1 \leq i \leq k : U[i] = 1\}$, the *support* of U . Similarly, for $x \in \{0, 1\}^{\mathbb{Z}}$ set $J(x) = \{i \in \mathbb{Z} : x[i] = 1\}$, the *support* of x . For any set A the cardinality of A will be denoted by $\text{card}(A)$.

Following [2], [7], we will say that a block $U \in \{0, 1\}^k$ is *admissible* if $\text{card}(J(U) \bmod b_j) < b_j$ for all b_j . Analogously, a sequence $x \in \{0, 1\}^{\mathbb{Z}}$ is *admissible* if $\text{card}(J(x) \bmod b_j) < b_j$ for all b_j . It is clear that a sequence $x \in \{0, 1\}^{\mathbb{Z}}$ is admissible if and only if each block $x[k, l]$, $k < l \in \mathbb{Z}$, is admissible.

Let us collect some facts that will be used in this note.

FACT 1 (e.g. [3, Cor. 4.27]). $J(\eta) \bmod b_i = \{1, \dots, b_i - 1\}$ for each $i \geq 1$.

FACT 2 (heredity property, [5], [3, Thm. D]). *If $y \in X$ and $x \preceq y$ then $x \in X$.*

FACT 3 ([2, Cor. 4.2]). *Let $x \in \{0, 1\}^{\mathbb{Z}}$. Then $x \in X$ if and only if x is admissible.*

COROLLARY 1. $U \in \{0, 1\}^k$ is admissible if and only if there exists $n \in \mathbb{Z}$ such that $U = \eta[n, n + k - 1]$.

1. Automorphisms of \mathcal{X} . Let $S : X \rightarrow X$ be a homeomorphism commuting with T , i.e. $T \circ S = S \circ T$. In other words, $S \in \text{Aut}(\mathcal{X})$. By the Curtis–Lyndon–Hedlund Theorem [6, Theorem 6.2.9], S is defined by a finite code, i.e. there exists a number $a \geq 0$ and a function $\varrho : \{0, 1\}^{2a+1} \rightarrow \{0, 1\}$ such that $S(x)[n] = \varrho(x[-a + n, a + n])$ for all $x \in X$ and $n \in \mathbb{Z}$. Denote $|\varrho| = 2a + 1$ (the length of the code ϱ). Denote also $0^{-\infty} = \dots 000$, $0^p = \underbrace{0 \dots 0}_p$, $0^\infty = 000 \dots$, $\bar{0} = \dots 000 \dots$.

Observe that S and ϱ have the following properties:

LEMMA 1.

- (a) $S(\eta)$ has a dense orbit in X ,
- (b) $S(\bar{0}) = \bar{0}$,
- (c) $\varrho(0^{|\varrho|}) = 0$.

Proof. Statement (a) is a consequence of the fact that η has dense orbit in X and S is a homeomorphism.

(b) Clearly $T(\bar{0}) = \bar{0}$ and $\bar{0}$ is the only fixed point of T on X . Since $S(\bar{0}) = S(T(\bar{0})) = T(S(\bar{0}))$, the result follows.

Statement (c) is a straightforward consequence of (b). ■

LEMMA 2. In the collection of all blocks of length $|\varrho|$ which contain $|\varrho| - 1$ digits 0 and one digit 1, exactly one goes to 1 under ϱ .

Proof. Let $U_s = 0^s 10^{2a-s}$, $s = 0, 1, \dots, 2a$. Let $x \in \{0, 1\}^{\mathbb{Z}}$ be given by $x[1] = 1$, $x[n] = 0$ for $n \neq 1$. By Fact 3, $x \in X$. Then $S(x) \neq \bar{0}$ because S is a homeomorphism and $S(\bar{0}) = \bar{0}$. Thus $\varrho(U_i) = 1$ for at least one block U_i .

Suppose that, contrary to our claim, $\varrho(U_s) = \varrho(U_{s+r}) = 1$ for some $r > 0$. Let $t = \min\{i > 1 : r \not\equiv 0 \pmod{b_i}\}$ and $\lambda_{t-1} = b_1 \dots b_{t-1}$. Set $m = b_t - 2$. Choose $p > 2a + 1$ in such a way that

$$(1) \quad 2a + p + 1 \equiv 0 \pmod{\lambda_{t-1}}, \quad 2a + p + 1 \equiv 1 \pmod{b_t}$$

(this is possible because λ_{t-1} and b_t are relatively prime). Let

$$x = 0^{-\infty} V_1 0^p V_2 0^p V_3 \dots 0^p V_{m+1} 0^\infty,$$

where $V_i = U_{s+r}$, $i = 1, \dots, m + 1$, and $x[0] = V_1[a + 1]$. Then $x[k] = 1$ if and only if

$$k \in (s + r - a) + \{0, 2a + 1 + p, 2(2a + 1 + p), \dots, m(2a + 1 + p)\} = J(x).$$

It follows from (1) that $J(x) \pmod{\lambda_{t-1}} = \{s + r - a\} \pmod{\lambda_{t-1}}$. As $J(x)$ consists of $m + 1 = b_t - 1$ elements, we have $x \in X$ (Fact 3).

Now, we will find the positions of 1's in $y = S(x)$. The sequence y is of the form

$$0^{-\infty} \overline{2a+1} 1 \overline{r-1} 1 \overline{2a+p-r} 1 \overline{r-1} 1 \overline{2a+p-r} 1 \dots \overline{2a+p-r} 1 \overline{r-1} 1 \overline{2a+1} 0^{\infty},$$

where \overline{i} denotes a block of zeros of length i . The first digit 1 written above is at position 0 in y , i.e. $1 = y[0]$. Thus

$$J(y) \supset \{k(2a+1+p), k(2a+1+p)+r; k=0, 1, \dots, m\} =: \bar{J}(y).$$

Observe that

$$\begin{aligned} \bar{J}(y) \bmod b_t &= \{0, r, 1, 1+r, 2, 2+r, \dots, m, m+r\} \bmod b_t \\ &= \{0, 1, \dots, m, r, r+1, \dots, r+m\} \bmod b_t = \{0, 1, \dots, b_t-1\}, \end{aligned}$$

as $m = b_t - 2$ and $r \not\equiv 0 \pmod{b_t}$. This implies that $y \notin X$, so at most one of the blocks U_i may be transformed by ϱ into 1. ■

Let $-a \leq n \leq a$ be such that $\varrho(0^{a+n}10^{a-n}) = 1$. Consider the automorphism $T^{-n}S$. It has the property described in Lemma 2 and is defined by a code of length $2a'+1$, where $a' = \max\{a-n, a+n\}$. Therefore without loss of generality, we may assume that $n = 0$ and keep the notation S , ϱ , a . Then $|\varrho| = 2a+1$ and $\varrho(0^a10^a) = 1$.

LEMMA 3. *If $V \in \{0, 1\}^{2a+1}$ is admissible and $V[a+1] = 0$, then $\varrho(V) = 0$.*

Proof. Suppose that $\varrho(V) = 1$. Let s be the number of ones in V . Fix t such that $2a+1 < b_t$ and $b_{t+1} > b_t + s$. Let $m = b_t - 1$. Set $U = 0^a10^a$; then $\varrho(U) = 1$.

Define $x \in \{0, 1\}^{\mathbb{Z}}$ in the following way:

$$x = 0^{-\infty} V 0^{p_1} U_1 0^{p_2} U_2 0^{p_3} \dots 0^{p_m} U_m 0^{\infty},$$

where $U_1 = \dots = U_m = U$ and $x[-a, a] = V$. What are the numbers p_1, \dots, p_m ?

Let the digits 1 of the block V occur in x at positions c_1, \dots, c_s and let $J = \{v_1, \dots, v_s\} = \{c_1, \dots, c_s\} \bmod b_t$. Then $0 \notin J$. Let

$$\{v_0 = 0, v_{s+1}, \dots, v_m\} = \{0, 1, \dots, m\} \setminus \{v_1, \dots, v_s\}.$$

Next, denote by d_1, \dots, d_m the centers of the blocks U_1, \dots, U_m , i.e. $x[d_i - a, d_i + a] = U_i$, $i = 1, \dots, m$. We choose the numbers p_1, \dots, p_s determining d_1, \dots, d_s so that

$$(2) \quad d_i \equiv c_i \pmod{\lambda_t}, \quad i = 1, \dots, s.$$

As λ_{t-1} and b_t are relatively prime, we may find p_{s+1}, \dots, p_m determining d_{s+1}, \dots, d_m in such a way that

$$(3) \quad d_i \equiv c_1 \pmod{\lambda_{t-1}}, \quad i = s+1, \dots, m,$$

$$(4) \quad d_i \equiv v_i \pmod{b_t}, \quad i = s+1, \dots, m.$$

Observe that the digits 1 occur in x at positions

$$\{c_i : i = 1, \dots, s\} \cup \{d_i : i = 1, \dots, m\},$$

which gives $m + s$ positions. Therefore $\text{card}(J(x) \bmod b_j) < b_j$ for $j > t$ (since $b_{t+1} > b_t + s$).

Now, take $j < t$. It follows from (2) that

$$\{c_1, \dots, c_s\} \bmod b_j = \{d_1, \dots, d_s\} \bmod b_j.$$

From (3) we obtain

$$\{d_{s+1}, \dots, d_m\} \bmod b_j = \{c_1\} \bmod b_j.$$

Therefore

$$J(x) \bmod b_j = \{c_1, \dots, c_s\} \bmod b_j,$$

hence

$$\text{card}(J(x) \bmod b_j) = \text{card}(J(V) \bmod b_j) < b_j,$$

because V is admissible.

Let us examine the set $J(x)$ modulo λ_t . It follows from (2) that

$$\begin{aligned} J(x) \bmod \lambda_t &= (\{c_1, \dots, c_s\} \cup \{d_1, \dots, d_s, d_{s+1}, \dots, d_m\}) \bmod \lambda_t \\ &= \{d_1, \dots, d_s, d_{s+1}, \dots, d_m\} \bmod \lambda_t. \end{aligned}$$

Therefore the set $J(x) \bmod b_t$ has at most $m = b_t - 1$ elements.

We have proved that $\text{card}(J(x) \bmod b_j) < b_j$ for all j . By virtue of Fact 3, we have $x \in X$.

Let us consider $S(x)$. Since $\varrho(V) = \varrho(U) = 1$, the digits 1 are in $S(x)$ exactly at positions d_i , $i = 1, \dots, m$, and moreover at position 0. Thus

$$J(S(x)) \supset \{0, d_1, \dots, d_m\}.$$

We deduce from (4) that

$$J(S(x)) \bmod b_t \supset \{0, d_1, \dots, d_m\} \bmod b_t = \{0, 1, \dots, b_t - 1\},$$

so $S(x) \notin X$, a contradiction. ■

LEMMA 4. *If a block $U \in \{0, 1\}^{2a+1}$ is admissible and $U[a+1] = 1$ then $\varrho(U) = 1$.*

Proof. Suppose this is not true. Take an admissible block U of length $2a + 1$ such that $U[a + 1] = 1$ and $\varrho(U) = 0$. Let $\gamma = S^{-1}(\eta)$. Then γ has a dense orbit. Therefore there exists k such that $\gamma[k - a, k + a] = U$. By Lemma 3, if $\eta[i] = 1$, then also $\gamma[i] = 1$, $i \in \mathbb{Z}$. Thus $J(\eta) \subset J(\gamma)$.

On the other hand, $\gamma[k] = U[a + 1] = 1$ and $\eta[k] = 0$. By the definition of η , there exists j such that b_j divides k , so $0 \in J(\gamma) \bmod b_j$. Since $J(\eta) \bmod b_j = \{1, \dots, b_j - 1\}$ (see Fact 1) and $\gamma \in X$, we have $J(\gamma) \bmod b_j = \{1, \dots, b_j - 1\}$; that contradicts the fact $0 \in J(\gamma) \bmod b_j$. ■

Now, we are ready to prove the following proposition.

PROPOSITION 1. $\text{Aut}(\mathcal{X}) = \{T^n : n \in \mathbb{Z}\}$.

Proof. Take any $S \in \text{Aut}(\mathcal{X})$. Let ϱ be the code defining S and $|\varrho| = 2a + 1$. By Lemma 2, $\varrho(0^n 10^{2a-n}) = 1$. Now, applying Lemmas 3 and 4 to $T^{-n}S$ we may assume that $T^{-n}S$ is defined by a code of length 1: $\varrho(0) = 0$, $\varrho(1) = 1$, i.e. $T^{-n}S = \text{Id}$. Therefore $S = T^n$. ■

2. Final remarks. In the proof of Lemma 2—the “at least one” part—we used the assumption that S is one-to-one. This assumption is essential, as the (continuous) map $\varphi_0 : X \rightarrow X$ given by $\varphi_0(x) = \bar{0}$ commutes with T and is defined by a code ϱ_0 of length 1, $\varrho_0(0) = \varrho_0(1) = 0$. In particular ϱ_0 does not satisfy the assertion of Lemma 4. This phenomenon and the heredity property of \mathcal{X} suggest natural questions: Does each code with the property that the blocks with 0 in the center are transformed into 0 define a continuous map $\varphi : X \rightarrow X$ commuting with T ? Is each map, continuous and commuting with T , of the form $T^n\varphi$, where φ satisfies the property defined in the previous question?

We are able to answer only the first question, and the answer is positive. Before formulating the results let us isolate some properties of a code ϱ .

- (Z) If $U \in \{0, 1\}^{2a+1}$ is admissible and $U[a + 1] = 0$, then $\varrho(U) = 0$.
- (J) If $U \in \{0, 1\}^{2a+1}$ is admissible and $U[a + 1] = 1$, then $\varrho(U) = 1$.

Observe that the code ϱ satisfying both (Z) and (J) is actually of the form $\varrho(0) = 0$, $\varrho(1) = 1$, and it defines the identity map: $\varphi_\varrho = \text{Id}$.

LEMMA 5. *Assume that a code $\varrho : \{0, 1\}^{2a+1} \rightarrow \{0, 1\}$ satisfies condition (Z). Then the map $\varphi = \varphi_\varrho : X \rightarrow \{0, 1\}^{\mathbb{Z}}$ given by*

$$\varphi(x)[n] = \varrho(x[n - a, n + a])$$

is an element of the centralizer $C(T)$ of T .

Proof. It is enough to prove that $\varphi(X) \subset X$. Indeed, if $x \in X$, then $J(\varphi(x)) \subset J(x)$ (by (Z)), and the result follows (see Fact 3). ■

Next we prove that the map φ_ϱ defined by a code ϱ satisfying condition (Z) is one-to-one or onto if and only if $\varphi_\varrho = \text{Id}$.

LEMMA 6. *Assume that a code $\varrho : \{0, 1\}^{2a+1} \rightarrow \{0, 1\}$ satisfies condition (Z). The following conditions are equivalent:*

- (i) φ_ϱ is one-to-one,
- (ii) φ_ϱ is onto,
- (iii) ϱ fulfills condition (J).

Proof. Clearly (iii) implies both (i) and (ii), as $\varphi_\varrho = \text{Id}$.

Suppose that φ_ϱ is one-to-one and (J) does not hold. Take an admissible block $U \in \{0, 1\}^{2a+1}$ that satisfies $U[a + 1] = 1$ and $\varphi(U) = 0$. We may

assume that U has the smallest number of digits 1 among all such blocks. Let $x = 0^{-\infty}U0^\infty$ and $y = \varphi(x)$. By condition (Z) we have $y = 0^{-\infty}W0V0^\infty$, where W and V are blocks of length a and $\text{card}(J(W0V)) < \text{card}(J(U))$. This forces $\varphi(y) = y = \varphi(x)$ because U has the smallest number of digits 1 among all blocks transformed via ϱ into 1. Therefore φ is not one-to-one, a contradiction.

Assume now that φ is onto. Then there exists $\gamma \in X$ such that $\varphi(\gamma) = \eta$. By condition (Z), if $\eta[n] = 1$, then also $\gamma[n] = 1$. If there were $k \in \mathbb{Z}$ such that $\gamma[k] = 1$ and $\eta[k] = 0$, then, by definition of η , $k \equiv b_j \pmod{b_j}$ for some b_j , which would force $J(\gamma) \bmod b_i = \{0, 1, \dots, b_j - 1\}$, a contradiction. Thus $\gamma = \eta$. All admissible blocks occur in the sequence η , and the result follows. ■

In Lemmas 5 and 6 we considered codes transforming into 0 blocks with digit 0 in the center (condition (Z)). An analogous assumption was given in condition (J): blocks with digit 1 in the center are transformed via ϱ into 1. Nevertheless without loss of generality we may reformulate conditions (Z) and (J).

Let $\varrho : \{0, 1\}^{2a+1} \rightarrow \{0, 1\}$ be a code. Let $\varphi = \varphi_\varrho : X \rightarrow \{0, 1\}^{\mathbb{Z}}$ be given by $\varphi(x)[n] = \varrho(x[n - a, n + a])$. Suppose $s \in [-a, a]$. Consider the following conditions:

- (Z_s) If $U \in \{0, 1\}^{2a+1}$ is admissible and $U[a + 1 + s] = 0$, then $\varrho(U) = 0$.
- (J_s) If $U \in \{0, 1\}^{2a+1}$ is admissible and $U[a + 1 + s] = 1$, then $\varrho(U) = 1$.

By the same arguments as in the proofs of Lemmas 5 and 6 we may show the following proposition.

PROPOSITION 2. *Assume that a code $\varrho : \{0, 1\}^{2a+1} \rightarrow \{0, 1\}$ satisfies condition (Z_s). Then:*

- (i) $\varphi = \varphi_\varrho$ is an element of the centralizer $C(T)$ of T .
- (ii) If ϱ additionally satisfies (J_s), then $\varphi = T^s$.
- (iii) If ϱ does not satisfy (J_s), then φ is neither one-to-one nor onto, and $\varrho(x) \preccurlyeq T^s(x)$ for each $x \in X$.

Acknowledgements. The author would like to thank Mariusz Lemańczyk for motivation, priceless tips and general support that became a cause of this article.

REFERENCES

- [1] J. Auslander, *Minimal Flows and their Extensions*, North-Holland Math. Stud. 153, North-Holland, Amsterdam, 1988.
- [2] E. H. El Abdalaoui, M. Lemańczyk and T. de la Rue, *A dynamical point of view on the set of B-free integers*, Int. Math. Res. Notices 2015, no. 16, 7258–7286.

- [3] A. Bartnicka, S. Kasjan, J. Kułaga-Przymus and M. Lemańczyk, *\mathcal{B} -free sets and dynamics*, arXiv:1509.08010 (2015).
- [4] S. Glasner, *Proximal Flows*, Lecture Notes in Math. 517, Springer, 1976.
- [5] J. Kułaga-Przymus, M. Lemańczyk and B. Weiss, *On invariant measures for \mathcal{B} -free systems*, Proc. London Math. Soc. (3) 110 (2015), 1435–1474.
- [6] D. Lind and B. Marcus, *An Introduction to Symbolic Dynamics and Coding*, Cambridge Univ. Press, 1995.
- [7] P. Sarnak, *Three lectures on the Möbius function randomness and dynamics*, publications.ias.edu/sarnak/.

Mieczysław K. Mentzen
Faculty of Mathematics and Computer Science
Nicolaus Copernicus University
Chopina 12/18
87-100 Toruń, Poland
E-mail: jkm@mat.umk.pl