COLLOQUIUM MATHEMATICUM

VOL. 105 2006 NO. 2

CYCLES OF DISTANCE-DECREASING MAPPINGS IN THE RING OF n-ADIC INTEGERS

BY

V. I. SUSHCHANSKI (Gliwice), E. MOĆKO (Gliwice)
and V. V. NEKRASHEVYCH (College Station, TX)

Abstract. We give a description of possible sets of cycle lengths for distance-decreasing maps and isometries of the ring of n-adic integers.

1. Introduction. Recall that a subset $\{x_0, \ldots, x_{n-1}\}$ of a set X is called a *cycle* of the mapping $f : X \to X$ if $x_i^f = x_{i+1}$ for $0 \le i \le n-2$ and $x_{n-1}^f = x_0$. The number n is called the *length* of the cycle and the elements x_i are said to be *cyclic of order* n for f. We denote by $\mathrm{Cycl}(f)$ the set of lengths of all cycles of the mapping f. Let Σ be some class of mappings of the set X. The main problems concerning the cyclic structure of the mappings from Σ are the following:

(i) What positive integers are lengths of cycles of mappings from the class Σ?
(ii) For which sets A of positive integers does there exist a mapping $f \in \Sigma$ such that $A = \mathrm{Cycl}(f)$?

The class Σ can be defined using different conditions (topological, metrical, algebraic, etc.). Many authors studied the class of polynomial mappings over different rings. The main results in this direction are collected in the remarkable monograph of W. Narkiewicz [6]. T. Pezda [8] has studied the orders of cyclic elements for polynomial mappings over discrete valuation rings of zero characteristic and finite residual fields. He has given a complete answer to question (i) for the ring $\mathbb{Z}_p$ of p-adic integers. Namely, he showed that if $p \ne 2, 3$ then an integer n is the length of a polynomial cycle if and only if $n = ab$, where $1 \le a \le p$ and $b \mid p-1$; in the cases $p = 2, 3$ additionally cycles of length p^2 occur.

Every polynomial mapping $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is a distance-decreasing mapping (in the sense of [1, p. 152]) of the metric space $\mathbb{Z}_p$ with the natural metric

2000 *Mathematics Subject Classification*: 13B35, 37E15, 54H20.

Key words and phrases: cycle of a mapping, length of a cycle, distance-decreasing mapping, n-adic integers.

$$\varrho(u,v) = v_p(u-v),$$

where v_p is the p-adic valuation (see [7, p. 328]). In other words, if $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is a polynomial, then for any $x, y \in \mathbb{Z}_p$ we have

$$\varrho(x^f, y^f) \leq \varrho(x,y).$$

Let $\mathbb{Z}_n$ be the ring of n-adic integers for $n > 1$, i.e., the completion of the ring $\mathbb{Z}$ with respect to the metric

$$\varrho(u,v) = n^{-k(u-v)},$$

where $k(x)$ is the maximal positive integer such that $n^{k(x)} \mid x$.

The class $H(\mathbb{Z}_n)$ of all distance-decreasing mappings over $\mathbb{Z}_n$ is larger than the class of polynomial mappings and contains the class $\mathrm{Is}(\mathbb{Z}_n)$ of all isometries of the metric space $\mathbb{Z}_n$. We will give complete answers to questions (i) and (ii) for the class $H(\mathbb{Z}_n)$.

We denote by E_n the set of all positive integers with all prime factors not greater than n.

The aim of this work is to prove the following statements.

Theorem 1. *For both semigroups $\Sigma = \mathrm{Is}(\mathbb{Z}_n)$ and $\Sigma = H(\mathbb{Z}_n)$, a number l is the length of some f-cycle, where $f \in \Sigma$, if and only if $l \in E_n$.*

Theorem 2. *For any subset $A \subset E_n$ there exists a mapping $f \in \mathrm{Is}(\mathbb{Z}_n) \subset H(\mathbb{Z}_n)$ such that* $\mathrm{Cycl}(f) = A$.

The results of this paper were announced in [5].

2. Preliminaries. The *wreath product* of a finite or infinite sequence $(P_1, M_1), (P_2, M_2), \ldots$ of transformation semigroups (see [3, p. 75], [4, p. 276]) is defined as the semigroup of all transformations t of the set $M = \prod_i M_i$, whose action on any element $\overline{x} = (x_1, x_2, \ldots) \in M$ satisfies the following conditions:

(i) for every i the ith coordinate y_i of the sequence $\overline{y} = (\overline{x})^t$ depends only on the first coordinates $x_1, \ldots, x_i$ of $\overline{x}$ (and on t);

(ii) for any fixed sequence $x_1^0, x_2^0, \ldots, x_{i-1}^0$, the transformation $x_i \mapsto y_i$ of the set M_i, defined by t, belongs to the semigroup P_i.

We denote the wreath product of a finite or infinite sequence (P_1, M_1), $(P_2, M_2), \ldots$ of semigroups by $\wr_{i=1}^{n} P_i$, where n is a positive integer or the symbol ∞ respectively.

It follows from the definition that every transformation from $\wr_{i=1}^{\infty} P_i$ is uniquely determined by an infinite tuple of the form

$$u = [t_1, t_2(x_1), t_3(x_1, x_2), \ldots], \tag{1}$$

where $t_1 \in P_1$ and $t_i(x_1, \ldots, x_{i-1}) \in P_i^{M_1 \times \cdots \times M_{i-1}}$ for $i = 2, 3, \ldots$. For finitely iterated wreath products such tuples are finite.

The wreath product of the sequence (P, M), (P, M), $\dots$ is called the (*finite or infinite*) *wreath power of the semigroup* (P, M).

Following the pioneering work of L. Kaluzhnin [2] we call a tuple (1) a (finite or infinite) *tableau*. Tableau (1) acts on an element $\overline{m} = (m_1, m_2, \dots)$ of the set M by the rule

$$\overline{m}^u = (m_1^{t_1}, m_2^{t_2(m_1)}, m_3^{t_3(m_1,m_2)}, \dots). \tag{2}$$

If all (P_i, M_i) are permutation groups, then the semigroup $\wr_{i=1}^{\infty} P_i$ is also a permutation group. If for all i the semigroup P_i is a symmetric transformation semigroup of the set M_i then condition (ii) from the definition of the wreath product holds automatically. Hence, the wreath product of an infinite sequence of symmetric semigroups (resp. symmetric groups) of sets $M_1, M_2, \dots$ is the semigroup of all transformations (resp. the group of all permutations) of the set $M = \prod_{i=1}^{\infty} M_i$, satisfying only condition (i) of the definition of the wreath product. It is possible to characterize the iterated wreath products $\wr_{i=1}^{\infty} S(M_i)$ as the isometry groups of some Baire metric spaces [9].

The *canonical form* of an n-adic number a is an infinite sequence $x_1 x_2 \dots$, where $x_i \in \{0, 1, \dots, n-1\}$, such that $a = x_1 + x_2 n + x_3 n^2 + \cdots$.

Let $X = \{0, 1, \dots, n-1\}$, where $n \geq 2$. We consider the space X^ω of all infinite sequences (words) $x_1 x_2 \dots$ over the alphabet X. We identify every sequence $w = x_1 x_2 \dots \in X^\omega$ with the n-adic number having the canonical expansion w, i.e., with the number $\Phi(w) = x_1 + x_2 n + x_3 n^2 + \cdots \in \mathbb{Z}_n$.

We also consider the set X^* of finite words over the alphabet X, including the empty word $\emptyset$.

If $u = x_1 \dots x_k \in X^*$ is a finite word and $v = x_{k+1} x_{k+2} \dots \in X^\omega$ is an infinite word, then we denote by uv the concatenation $x_1 \dots x_k x_{k+1} x_{k+2} \dots$.

In what follows, we will talk mostly about words over the alphabet X, rather than n-adic numbers.

Let us define two relations $\approx_k$ and $\sim_k$ on $\mathbb{Z}_n$ by the following conditions:

(i) $x \approx_k y \Leftrightarrow x - y \in n^k \mathbb{Z}_n$;
(ii) $x \sim_k y \Leftrightarrow x - y \in n^k \mathbb{Z}_n \setminus n^{k+1} \mathbb{Z}_n$.

The respective relations on the space X^ω are defined by the conditions

(i) $w_1 \approx_k w_2$ if and only if the initial strings of length k of w_1 and w_2 are equal;
(ii) $w_1 \sim_k w_2$ if and only if the longest common initial string of w_1 and w_2 has length k.

It is easy to see that the relations $\approx_k$ are equivalence relations on $\mathbb{Z}_n$ and X^ω. For any two different $w_1, w_2 \in X^\omega$ there exists exactly one integer $k = \kappa(w_1, w_2) \geq 0$ such that $w_1 \sim_k w_2$.

If $w_1, w_2 \in X^\omega$, then $\kappa(w_1, w_2)$ is the length of the longest common initial string of w_1 and w_2, and $\varrho(w_1, w_2) = n^{-\kappa(w_1,w_2)}$ is a metric on X^ω such that the identification map $\Phi : X^\omega \to \mathbb{Z}_n$ is an isometry.

LEMMA 1. *A mapping $f : X^\omega \to X^\omega$ is distance-decreasing (respectively an isometry) if and only if it preserves all the relations $\approx_k$ (respectively $\sim_k$), that is, for any infinite words w_1, w_2 and $k \in \mathbb{N}$ the relation $w_1 \approx_k w_2$ (respectively $w_1 \sim_k w_2$) implies $w_1^f \approx_k w_2^f$ (respectively $w_1^f \sim_k w_2^f$).*

Proof. Let $f : X^\omega \to X^\omega$ be distance-decreasing and let $w_1 = x_1x_2\ldots$ and $w_2 = y_1y_2\ldots$ be any two infinite words. If $w_1 \approx_k w_2$ then $x_i = y_i$ for $i = 1, \ldots, k$ and $\varrho(w_1, w_2) \le n^{-k}$. Hence $\varrho(w_1^f, w_2^f) \le n^{-k}$ and w_1^f, w_2^f have a common initial string of length k, so $w_1^f \approx_k w_2^f$.

Conversely, if f preserves $\approx_k$ then for every $w_1, w_2 \in X^\omega$ such that $\varrho(w_1, w_2) = n^{-k}$ we have $w_1 \approx_k w_2$ and hence $w_1^f \approx_k w_2^f$, so $\varrho(w_1^f, w_2^f) \le n^{-k}$ and f is distance-decreasing.

For isometries the proof is analogous. ■

LEMMA 2.

(i) *The semigroup $H(X^\omega)$ of all distance-decreasing transformations of the metric space X^ω is isomorphic to the infinitely iterated wreath power of the symmetric semigroup of degree n:*

$$H(X^\omega) \simeq \mathop{\wr}_{i=1}^{\infty} T_n^{(i)}.$$

(ii) *The group $\mathrm{Is}(X^\omega)$ of all isometries of the metric space X^ω is isomorphic to the infinitely iterated wreath power of the symmetric group S_n of degree n:*

$$\mathrm{Is}(X^\omega) \simeq \mathop{\wr}_{i=1}^{\infty} S_n^{(i)}.$$

This follows from Lemma 1 and the definition of the wreath product of symmetric semigroups or symmetric groups.

We will denote by X^k the metric space of all words of length k with the metric defined by

$$\varrho_k(v_1, v_2) = \begin{cases} n^{-\kappa(v_1,v_2)} & \text{if } v_1 \ne v_2, \\ 0 & \text{otherwise,} \end{cases}$$

where $\kappa(v_1, v_2)$ is, as usual, the length of the longest common initial string of the words v_1 and v_2.

Let $H(X^k)$ (respectively $\mathrm{Is}(X^k)$) be the semigroup of all distance-decreasing mappings of X^k (respectively the group of all isometries of X^k). We have

$$H(X^k) \simeq \mathop{\wr}_{i=1}^{k} T_k^{(i)}, \qquad \mathrm{Is}(X^k) \simeq \mathop{\wr}_{i=1}^{k} S_n^{(i)}.$$

LEMMA 3. *Let $f \in H(X^\omega)$ and let $C \subseteq X^\omega$ be a closed subset of X^ω which is the union of some cycles of f. Then there exists $\widetilde{f} \in \mathrm{Is}(X^\omega)$ such that the union of all cycles of $\widetilde{f}$ is equal to C and $f|_C = \widetilde{f}|_C$.*

Proof. The set C is obviously f-invariant, i.e., $C^f = C$. Moreover, the restriction of f to C is invertible. If $a_1, a_2 \in C$ and each a_i belongs to an f-cycle of length n_i, then $\varrho(a_1^{f^{k+1}}, a_2^{f^{k+1}}) \le \varrho(a_1^{f^k}, a_2^{f^k})$ for every k. But $a_i^{f^{n_1 n_2}} = a_i$, thus we always have equality and the action of f on C is isometric.

For every $a \in X^\omega \setminus C$ define $[a]$ to be the longest initial string of a common with some element of C. Since C is closed, the string $[a]$ is finite for every $a \in X^\omega \setminus C$. Let $l(a)$ be its length and denote by $\overline{a}$ the word obtained from a by deleting $[a]$.

The transformation $\alpha : a \mapsto \Phi^{-1}(\Phi(a)+1)$ obviously belongs to $\mathrm{Is}(X^\omega)$ and it has no cycles, since this is true for the conjugate transformation $a \mapsto a+1$ of $\mathbb{Z}_n$. Let now $\beta : X^\omega \to X^\omega$ act by the rule $(xw)^\beta = x(w^\alpha)$, i.e., β does not change the first letter and acts on the rest of the word as α. Then β also has no cycles.

Define now $\widetilde{f} : X^\omega \to X^\omega$ by the rule

$$a^{\widetilde{f}} = \begin{cases} a^f & \text{if } a \in C, \\ [a]^f \overline{a}^\beta & \text{if } a \notin C. \end{cases}$$

It is easy to prove, using Lemma 1, that $\widetilde{f}$ is an isometry. It follows easily from the definition of β that $\widetilde{f}$ has no cycles outside C. ∎

LEMMA 4. *A number l is the length of a cycle of some $f \in H(X^\omega)$ if and only if it is the length of a cycle of some $\widetilde{f} \in \mathrm{Is}(X^\omega)$.*

Proof. In Lemma 3, take C equal to a cycle of f. ∎

LEMMA 5. *If $u \in \mathrm{Is}(X^k)$, then $\mathrm{Cycl}(u) \subseteq E_n$.*

Proof. Since $\mathrm{Is}(X^k) \simeq \wr_{i=1}^k S_n^{(i)}$, by definition of the wreath product of permutation groups we have

$$|\mathrm{Is}(X^k)| = n!(n!)^n \cdots (n!)^{n^{k-1}},$$

so $|\mathrm{Is}(X^k)| \in E_n$. Since the order of every permutation from $\mathrm{Is}(X^k)$ is a factor of $|\mathrm{Is}(X^k)|$ and cycle lengths for permutations are factors of their orders, the cycle lengths for the isometry u are factors of $|\mathrm{Is}(X^k)|$, proving the statement. ∎

A subset $A \subset k\mathbb{N}$ containing k is called a *D-subset with basis k*.

Lemma 6. *For any $A \subset E_n$ there exist D-subsets $A_1, \dots, A_l$ with bases $k_1, \dots, k_l$ such that*

$$A = \bigcup_{i=1}^{l} A_i \quad \textit{and} \quad k_i \nmid k_j \quad \textit{for } i \neq j.$$

Proof. Let $p_1 < \cdots < p_s$ be all primes from E_n. We say that two elements a and b are *comparable* if $a \,|\, b$ or $b \,|\, a$. It is sufficient to prove that each infinite subset $A \subset E_n = E_{p_s}$ contains an infinite set of pairwise comparable elements. Then the statement of the lemma follows, since one can take $\{k_1, \dots, k_l\}$ to be the set of all minimal elements of A (with respect to the order included by division). The set of all minimal elements is finite, since otherwise it would be an infinite set without comparable elements.

We use induction on s. The case $s = 1$ is trivial.

Let $s > 1$. Define

$$\bar{A} = \{p_1^{k_1} \cdots p_{s-1}^{k_{s-1}} \mid p_1^{k_1} \cdots p_{s-1}^{k_{s-1}} p_s^{k_s} \in A \text{ for some } k_s\} \subset E_{p_{s-1}}.$$

If $\bar{A}$ is finite then there exists $p_1^{k_1^{(0)}} \cdots p_{s-1}^{k_{s-1}^{(0)}} \in \bar{A}$ such that the set

$$C = \{l = p_1^{k_1^{(0)}} \cdots p_{s-1}^{k_{s-1}^{(0)}} p_s^{k_s} \mid l \in A,\, k_s \geq 0\}$$

is infinite. Since all pairs of elements of C are comparable, A contains an infinite set of pairwise comparable elements.

If $\bar{A}$ is infinite then, by the inductive assumption, it contains an infinite subset $C \subset E_{p_{s-1}}$ of pairwise comparable elements $c_i = p_1^{k_1^{(i)}} \cdots p_{s-1}^{k_{s-1}^{(i)}}$, $i = 1, 2, \dots,$ such that $p_1^{k_1^{(i)}} \cdots p_{s-1}^{k_{s-1}^{(i)}} \mid p_1^{k_1^{(i+1)}} \cdots p_{s-1}^{k_{s-1}^{(i+1)}}$. The numbers ap_s^l and bp_s^r with $a, b \in C$ and $a < b$ are not comparable if $r > l$. Since for any l there exist only finitely many r such that $r < l$, and C is infinite, the set A contains an infinite subset of pairwise comparable elements. ∎

In the proof of Theorem 1, we will use the following construction for tableaux of finite lengths. Let

$$u = [a_1, a_2(x_1), \dots, a_m(x_1 \dots x_{m-1})],$$
$$v = [b_1, b_2(x_1), \dots, b_k(x_1 \dots x_{k-1})]$$

be tableaux from $H(X^m)$ and $H(X^k)$ respectively, and let $\alpha \in X^m$. We denote by $u \triangle_\alpha v$ the tableau

$$u \triangle_\alpha v = [c_1, c_2(x_1), \dots, c_{m+k}(x_1, \dots, x_{m+k-1})],$$

from $H(X^{m+k})$ constructed in the following way:

(1) $c_i(x_1, \dots, x_{i-1}) = a_i(x_1, \dots, x_{i-1})$ for $i = 1, \dots, m$;
(2) $c_{m+1}(\alpha) = b_1$,

(3) $c_{m+i}(\alpha, x_{m+1}, \ldots, x_{m+i-1}) = b_i(x_{m+1}, \ldots, x_{m+i-1})$ for $i = 2, \ldots, k$;
(4) $c_{m+i}(y, x_{m+1}, \ldots, x_{m+i-1}) = \varepsilon$ for $y \neq \alpha$ and $i = 1, \ldots, k$,

where ε is the trivial permutation on X.

In other words, $u \bigtriangleup_\alpha v$ acts on the words of length $m + k$ by the rule

$$(x_1 \ldots x_m x_{m+1} \ldots x_{m+k})^{u \bigtriangleup_\alpha v} = \begin{cases} (x_1 \ldots x_m)^u x_{m+1} \ldots x_{m+k} & \text{if } x_1 \ldots x_m \neq \alpha, \\ (x_1 \ldots x_m)^u (x_{m+1} \ldots x_{m+k})^v & \text{if } x_1 \ldots x_k = \alpha. \end{cases}$$

Lemma 7. *Let $u \in \mathrm{Is}(X^m)$, $v \in \mathrm{Is}(X^k)$, $l_1 \in \mathrm{Cycl}(u)$, $l_2 \in \mathrm{Cycl}(v)$, and let $\alpha \in X^m$ be an element of a cycle of length l_1 for u. Then $u \bigtriangleup_\alpha v \in \mathrm{Is}(X^{m+k})$ and $l_1 \cdot l_2 \in \mathrm{Cycl}(u \bigtriangleup_\alpha v)$.*

Proof. The fact that $u \bigtriangleup_\alpha v \in \mathrm{Is}(X^{m+k})$ is straightforward (by Lemma 1).

It is also easy to see that if $\alpha \in X^m$ is an element of a u-cycle of length l_1 and $\beta \in X^k$ is an element of a v-cycle of length l_2, then $\alpha\beta$ is an element of a $u \bigtriangleup_\alpha v$-cycle of length $l_1 \cdot l_2$. This follows directly from the definition of $u \bigtriangleup_\alpha v$. ∎

Lemma 8. *Let $u \in H(X^m)$ and $v \in H(X^k)$ have only one cycle each, of respective lengths l_1 and l_2. Let α be an element of the cycle of u. Then $u \bigtriangleup_\alpha v$ has only one cycle, of length $l_1 \cdot l_2$.*

This also follows directly from the definitions.

3. Proof of Theorem 1. Firstly we prove that the lengths of all cycles for distance-decreasing transformations of X^ω belong to E_n.

In view of Lemma 4, we can assume that l is the length of some f-cycle $(a_1, \ldots, a_l)$, where $f = [h_1, h_2(x_1), h_3(x_1, x_2), \ldots]$ belongs to $\mathrm{Is}(X^\omega)$ and $a_i \in X^\omega$ $(1 \leq i \leq l)$. Let k be a positive integer such that the initial strings $a_1^{(k)}, \ldots, a_n^{(k)}$ of the words $a_1, \ldots, a_l$ are pairwise different. The words $a_1^{(k)}, \ldots, a_l^{(k)}$ form a cycle of length l for the permutation

$$f^{(k)} = [h_1, h_2(x_1), \ldots, h_l(x_1, \ldots, x_{k-1})].$$

Since $f^{(k)} \in \mathrm{Is}(X^k)$, Lemma 5 implies that $l \in E_n$.

Now we prove that for every $l \in E_n$ there exists $f \in \mathrm{Is}(X^\omega)$ such that $l \in \mathrm{Cycl}(f)$. Let $l = p_1 \cdots p_s$ be a prime factorization of l. Since $l \in E_n$, we have $p_i \leq n$ for all $i = 1, \ldots, s$. For each p_i we can construct a tableau $u_i = [g_i] \in H(X^1)$ having a cycle of length p_i, where $g_i = (0, 1, \ldots, p_i - 1)$. Using the construction preceding Lemma 7, suppose that $u = (\ldots(u_1 \bigtriangleup_{a_1} u_2) \bigtriangleup_{a_2} \ldots) \bigtriangleup_{a_{s-1}} u_s$, where a_i is an element of the cycle of length $p_1 \ldots p_i$ for the tableau $u = u_1 \bigtriangleup_{a_1} u_2 \bigtriangleup_{a_2} \ldots \bigtriangleup_{a_{i-1}} u_i$, $i = 1, \ldots, s-1$. Then $p_1 \cdots p_s \in \mathrm{Cycl}(u)$ by Lemma 7.

4. Proof of Theorem 2

STEP 1. *For every* $l \in E_n$ *there exists* $u \in H(X^s)$ *for some* $s \in \mathbb{N}$ *such that* $\mathrm{Cycl}(u) = \{l\}$, *and there exists* $\widehat{u} \in H(X^\omega)$ *such that* $\mathrm{Cycl}(\widehat{u}) = \{l\}$ *and the union of the cycles of* $\widehat{u}$ *is closed.*

Let $l = p_1 \cdots p_s$ be a prime factorization with $p_i \le n$, $i = 1, \ldots, s$. For each p_i we define the transformation

$$g_i = \begin{pmatrix} 0 & \cdots & p_i - 2 & p_i - 1 & p_i & \cdots & p-1 \\ 1 & \cdots & p_i - 1 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

in the semigroup T_n having only the cycle $(0, 1, \ldots, p_i - 1)$ of length p_i (all other elements go to 0). We define $u_i = [g_i] \in H(X^1)$, which has only one cycle of length p_i, $i = 1, \ldots, s$. Put $u = u_1 \triangle_{a_1} u_2 \triangle_{a_2} \ldots \triangle_{a_{s-1}} u_s$, where a_i is an element of the unique cycle of length $p_1 \cdots p_i$ for $u = u_1 \triangle_{a_1} u_2 \triangle_{a_2} \ldots \triangle_{a_{i-1}} u_i$, $i = 1, \ldots, s-1$. By Lemma 8, u has only one cycle, of length $p_1 \cdots p_s$.

Put $\widehat{u} = [u, \varepsilon, \varepsilon, \ldots] \in H(X^\omega)$. Then $\widehat{u}$ has only cycles of length l. Their union C is a closed subset of X^ω of the form

$$C = \{aw \mid a \text{ is an element of a cycle of } u, \text{ and } w \in X^\omega\}.$$

STEP 2. *For any D-subset A, there exists* $u \in H(\mathbb{Z}_n)$ *such that* $\mathrm{Cycl}(u) = A$ *and the union C of all its cycles is closed.*

Let A be a finite or infinite D-subset with basis m, and let $m = m_0, m_1, m_2, \ldots$ be an infinite sequence such that $A = \{m_0, m_1, \ldots\}$ (if A is finite, then the sequence m_i must have repetitions). Let $m_j/m = k_j$, $j \ge 1$. According to Step 1, we can construct $u_0 \in H(X^{s_0})$ having a unique cycle whose length is m. For each $j \ge 1$ by Step 1 we can also construct $u_j \in H(X^{s_j})$ having a unique cycle whose length is k_j. Without loss of generality, we may assume that the word $0^{s_j} = 00\ldots0 \in X^{s_j}$ belongs to the unique cycle of u_j, $j = 0, 1, \ldots$.

We now define $u \in H(X^\omega)$ by

$$(x_1 x_2 \ldots)^u = \begin{cases} (x_1 x_2 \ldots x_{s_0})^{u_0} \underbrace{00\ldots0}_{j \text{ times}} 1 (x_{s_0+j+2} x_{s_0+j+3} \ldots x_{s_0+j+s_j+1})^{u_j} \\ \qquad \cdot x_{s_0+s_j+j+2} x_{s_0+s_j+j+3} \cdots \\ \qquad \text{if } x_1 x_2 \ldots x_{s_0+j+1} = 00\ldots01,\ j = 0, 1, 2, \ldots \\ (x_1 x_2 \ldots x_{s_0})^{u_0} x_{s_0+1} x_{s_0+2} \ldots \text{ in all other cases.} \end{cases}$$

It follows as in the proof of Lemmas 7 and 8 that $\mathrm{Cycl}(u) = A$.

STEP 3. *For any* $A \subset E_n$, *there exists* $u \in H(\mathbb{Z}_n)$ *such that* $\mathrm{Cycl}(u) = A$ *and the union of its cycles is closed.*

By Lemma 6 there exist D-subsets $A_1, \ldots, A_r$ with bases $m_1, \ldots, m_r$ such that $A = \bigcup_{j=1}^r A_j$ and $m_i \nmid m_j$ for $i \ne j$. For each j by Step 2 we construct $u_j \in H(X^\omega)$ such that $\mathrm{Cycl}(u_j) = A_j$, and then define u by $(x_1x_2\ldots)^u$

$$= \begin{cases} \underbrace{00\ldots0}_{j-1 \text{ times}} 1(x_{j+1}x_{j+2}\ldots)^{u_j} & \text{if } x_1\ldots x_j = \underbrace{00\ldots0}_{j-1 \text{ times}} 1 \\ & \qquad \text{for some } j = 1,\ldots,r, \\ \underbrace{00\ldots0}_{j-1 \text{ times}} 1x_{j+1}x_{j+2}\ldots & \text{if } x_1\ldots x_{j-1} = 00\ldots0 \text{ and } x_j \neq 0,1 \\ & \qquad \text{for some } j = 1,\ldots,r; \\ \underbrace{00\ldots0}_{r-1 \text{ times}} 1x_{r+1}x_{r+2}\ldots & \text{if } x_1\ldots x_r = 00\ldots0. \end{cases}$$

It is easy to see that the cycles of u are of the form $\underbrace{00\ldots0}_{j-1 \text{ times}} 1C_j$, where C_j is a cycle of u_j.

Acknowledgments. The authors are grateful to the referee for his help in improving the paper.

REFERENCES

[1] K. S. Brown, *Buildings*, Springer, Berlin, 1988.

[2] L. A. Kaluzhnin, *On some generalization of Sylow p-subgroups of symmetric groups*, Acta Math. Hungar. 2 (1951), 198–221 (in Russian).

[3] L. A. Kaluzhnin, P. M. Beleckij and V. Z. Feinberg, *Kranzprodukte*, Teubner, Leipzig, 1987.

[4] J. P. P. Meldrum, *Wreath Products of Groups and Semigroups*, Pitman Monogr. Surveys Pure Appl. Math. 74, Longman, Harlow, 1995.

[5] E. Moćko, V. Nekrashevych and V. Sushchansky, *Dynamics of triangular transformations of the sequences over finite alphabets*, Mat. Zametki 73 (2003), 436–439 (in Russian).

[6] W. Narkiewicz, *Polynomial Mappings*, Lecture Notes in Math. 1800, Springer, Berlin, 1995.

[7] —, *Theory of Numbers*, PWN, Warszawa, 1977 (in Polish).

[8] T. Pezda, *Polynomial cycles in certain local domains*, Acta Arith. 66 (1994), 11–22.

[9] V. I. Sushchansky, *Isometry groups of Baire p-spaces*, Dopovidi AN URSR 1984, no. 8, 28–30 (in Ukrainian).

Institute of Mathematics
Silesian University of Technology
44-100 Gliwice, Poland
E-mail: Wital.Suszczanski@polsl.pl
ewilgl@zeus.polsl.gliwice.pl

Department of Mathematics
Texas A&M University
3368 TAMU
College Station, TX 77843-3368, U.S.A.
E-mail: nekrash@math.tamu.edu

Received 30 June 2004;
revised 14 October 2005 (4477)