2008 Прикладная теория автоматов № 1(1)

DOI 10.17223/20710410/1/20

УДК 518.6+681.3

ХАРАКТЕРИСТИКА НЕПОДВИЖНЫХ ТОЧЕК ЛИНЕЙНЫХ АВТОМАТОВ НАД КОНЕЧНЫМ КОЛЬЦОМ

В.В. Скобелев

Институт прикладной математики и механики НАН Украины, г. Донецк

E-mail: vv_skobelev@iamm.ac.donetsk.ua

Исследуется структура множества неподвижных точек словарной функции, реализуемой инициальными линейными автоматами Мили и Мура над кольцом $\mathbf{Z}_{p^k}$. Охарактеризованы входные символы, являющиеся неподвижными точками для текущего состояния исследуемых автоматов.

Ключевые слова: *поточные шифры*, *линейные автоматы*, *конечные кольца*, *неподвижные точки.*

Нетривиальным обобщением линейных автоматов над конечным полем [1] являются линейные автоматы над кольцом $\mathbf{Z}_{p^k} = (\mathbf{Z}_{p^k}, \oplus, \circ)$ (p – простое число, $a \oplus b = a+b \pmod{p^k}$ и $a \circ b = a \cdot b \pmod{p^k}$). Сложность исследования таких автоматов обусловлена тем, что при переходе от поля к кольцу осуществляется переход от линейного пространства к модулю линейных форм [2]. В [3, 4] исследован ряд характеристик таких моделей с позиции теории автоматов и теории систем, а в [5] – применение этих моделей в качестве поточных шифров, при условии, что они являются БПИ-автоматами [6]. С этой позиции актуальным является исследование неподвижных точек словарных функций [7, 8], реализуемых инициальными линейными автоматами над кольцом $\mathbf{Z}_{p^k}$. Действительно, неподвижной точкой словарной функции $f: X^+ \to X^+$ называется любая такая последовательность $u \in X^+$, что истинно равенство $f(u) = u$. Поэтому именно неподвижная точка представляет собой «открытый текст», который не изменяется в процессе шифрования. Исследование структуры множества неподвижных точек линейных автоматов над кольцом $\mathbf{Z}_{p^k}$ и является основной целью настоящей работы.

Структура работы следующая: в п. 1 введены основные понятия; в п. 2 охарактеризовано множество неподвижных точек словарной функции, реализуемой инициальными линейными автоматами Мили и Мура над кольцом $\mathbf{Z}_{p^k}$; в п. 3 охарактеризованы входные символы, являющиеся неподвижными точками для текущего состояния исследуемых автоматов. Заключение содержит ряд выводов.

1. Основные понятия

Объектом исследования являются линейные автоматы Мили и Мура над кольцом $\mathbf{Z}_{p^k}$ соответственно

$$M_1: \begin{cases} \boldsymbol{q}_{t+1} = A \circ \boldsymbol{q}_t \oplus B \circ \boldsymbol{x}_{t+1}, \\ \boldsymbol{y}_{t+1} = C \circ \boldsymbol{q}_t \oplus D \circ \boldsymbol{x}_{t+1}, \end{cases} \quad (t \in \mathbf{Z}_+) \tag{1}$$

и

$$M_2: \begin{cases} \boldsymbol{q}_{t+1} = A \circ \boldsymbol{q}_t \oplus B \circ \boldsymbol{x}_{t+1}, \\ \boldsymbol{y}_{t+1} = C \circ \boldsymbol{q}_{t+1}, \end{cases} \quad (t \in \mathbf{Z}_+), \tag{2}$$

где n – фиксированное число; A, B, C, D – $(n \times n)$-матрицы над кольцом $\mathbf{Z}_{p^k}$, а $\boldsymbol{q}_t$, $\boldsymbol{x}_t$, $\boldsymbol{y}_t \in \mathbf{Z}_{p^k}^n$ – вектор-столбцы, соответствующие соответственно состоянию автомата, входному символу и выходному символу в момент t. Обозначим через A_1 и A_2 множества всех автоматов соответственно M_1 и M_2. При фиксации начального состояния $\boldsymbol{q}_0 \in \mathbf{Z}_{p^k}^n$ автомата $M \in \mathsf{A}_1 \cup \mathsf{A}_2$ получим инициальный автомат $(M, \boldsymbol{q}_0)$.

Обозначим через $S_{fxd}(M, \boldsymbol{q}_0)$ $(M \in \mathsf{A}_1 \cup \mathsf{A}_2, \boldsymbol{q}_0 \in \mathbf{Z}_{p^k}^n)$ множество всех неподвижных точек словарной функции $f_{(M,\boldsymbol{q}_0)} : (\mathbf{Z}_{p^k}^n)^+ \to (\mathbf{Z}_{p^k}^n)^+$, реализуемой инициальным автоматом $(M, \boldsymbol{q}_0)$. Положим

$$S_{fxd}^{(t+1)}(M, \boldsymbol{q}_0) = S_{fxd}(M, \boldsymbol{q}_0) \cap (\mathbf{Z}_{p^k}^n)^{t+1} \quad (t \in \mathbf{Z}_+).$$

Для любого инициального автомата $(M, \boldsymbol{q}_0)$ истинно равенство

$$S_{fxd}(M, \boldsymbol{q}_0) = \bigcup_{t=0}^{\infty} S_{fxd}^{(t+1)}(M, \boldsymbol{q}_0). \tag{3}$$

При этом если $t_1 \neq t_2$, то

$$S_{fxd}^{(t_1+1)}(M, \boldsymbol{q}_0) \cap S_{fxd}^{(t_2+1)}(M, \boldsymbol{q}_0) = \varnothing.$$

Поэтому для исследования структуры множества $S_{fxd}(M, \boldsymbol{q}_0)$ ($M \in \mathsf{A}_1 \cup \mathsf{A}_2$, $\boldsymbol{q}_0 \in \mathbf{Z}_{p^k}^n$) достаточно охарактеризовать общий элемент последовательности $S_{fxd}^{(t+1)}(M, \boldsymbol{q}_0)$ ($t \in \mathbf{Z}_+$).

Отметим, что из включения $S_{fxd}^{(t+2)}(M, \boldsymbol{q}_0) \subseteq S_{fxd}^{(t+1)}(M, \boldsymbol{q}_0) \cdot \mathbf{Z}_{p^k}^n$ ($t \in \mathbf{Z}_+$) вытекает

Утверждение 1. Для любого автомата $M \in \mathsf{A}_1 \cup \mathsf{A}_2$ при любом начальном состоянии $\boldsymbol{q}_0 \in \mathbf{Z}_{p^k}^n$, если существует такое значение $t_0 \in \mathbf{Z}_+$, что $S_{fxd}^{(t_0+1)}(M, \boldsymbol{q}_0) = \varnothing$, то $S_{fxd}^{(t+1)}(M, \boldsymbol{q}_0) = \varnothing$ для всех $t > t_0$.

Из утверждения 1 и равенства (3), в свою очередь, вытекает

Утверждение 2. Множество $S_{fxd}(M, \boldsymbol{q}_0)$ ($M \in \mathsf{A}_1 \cup \mathsf{A}_2$, $\boldsymbol{q}_0 \in \mathbf{Z}_{p^k}^n$) – конечное тогда и только тогда, когда существует такое значение $t_0 \in \mathbf{Z}_+$, что $S_{fxd}^{(t_0+1)}(M, \boldsymbol{q}_0) = \varnothing$.

2. Характеристика множества $S_{fxd}(M, \boldsymbol{q}_0)$ ($M \in \mathsf{A}_1 \cup \mathsf{A}_2$, $\boldsymbol{q}_0 \in \mathbf{Z}_{p^k}^n$)

Выразим $\boldsymbol{y}_{t+1}$ ($t \in \mathbf{N}$) из систем (1) и (2) через начальное состояние $\boldsymbol{q}_0 \in \mathbf{Z}_{p^k}^n$ автомата $M \in \mathsf{A}_1 \cup \mathsf{A}_2$ и элементы входной последовательности $\boldsymbol{x}_1 \ldots \boldsymbol{x}_{t+1} \in (\mathbf{Z}_{p^k}^n)^{t+1}$. Получим

$$\boldsymbol{y}_{t+1} = C \circ (A^t \circ \boldsymbol{q}_0 \oplus (\bigoplus_{j=1}^{t-1} A^{t-j} \circ B \circ \boldsymbol{x}_j) \oplus B \circ \boldsymbol{x}_t) \oplus D \circ \boldsymbol{x}_{t+1} \ (t \in \mathbf{N}), \tag{4}$$

если $M \in \mathsf{A}_1$ и

$$\boldsymbol{y}_{t+1} = C \circ (A^{t+1} \circ \boldsymbol{q}_0 \oplus (\bigoplus_{j=0}^{t-1} A^{t-j} \circ B \circ \boldsymbol{x}_{j+1}) \oplus B \circ \boldsymbol{x}_{t+1}) \ (t \in \mathbf{N}), \tag{5}$$

если $M \in \mathsf{A}_2$.

Из (1), (2), (4) и (5) вытекает

Теорема. Для любого автомата $M \in \mathsf{A}_1 \cup \mathsf{A}_2$ при любом начальном состоянии $\boldsymbol{q}_0 \in \mathbf{Z}_{p^k}^n$ для всех $t \in \mathbf{Z}_+$ множество $S_{fxd}^{(t+1)}(M, \boldsymbol{q}_0)$ состоит из всех таких слов $\boldsymbol{x}_1 \ldots \boldsymbol{x}_{t+1} \in (\mathbf{Z}_{p^k}^n)^{t+1}$, что:

а) если $M \in \mathsf{A}_1$, то $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{t+1})$ – множество решений системы уравнений

$$\begin{cases} (I \ominus D) \circ \boldsymbol{x}_1 = C \circ \boldsymbol{q}_0, \\ (I \ominus D) \circ \boldsymbol{x}_{i+1} = C \circ (A^i \circ \boldsymbol{q}_0 \oplus (\bigoplus_{j=1}^{i-1} A^{i-j} \circ B \circ \boldsymbol{x}_j) \oplus B \circ \boldsymbol{x}_i) \quad (i = 1, \ldots, t), \end{cases} \tag{6}$$

б) если $M \in \mathsf{A}_2$, то $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{t+1})$ – множество решений системы уравнений

$$\begin{cases} (I \ominus C \circ B) \circ \boldsymbol{x}_1 = C \circ A \circ \boldsymbol{q}_0, \\ (I \ominus C \circ B) \circ \boldsymbol{x}_{i+1} = C \circ A \circ (A^i \circ \boldsymbol{q}_0 \oplus \bigoplus_{j=1}^{i-1} A^{i-j} \circ B \circ \boldsymbol{x}_j \oplus B \circ \boldsymbol{x}_i) \quad (i = 1, \ldots, t). \end{cases} \tag{7}$$

Отметим, что каждое уравнение систем (6) и (7) имеет вид

$$A \circ \boldsymbol{x} = \boldsymbol{b}. \tag{8}$$

Известно (см., напр., [9]), что для уравнения (8) возможна одна из следующих трех ситуаций:

1) уравнение (8) не имеет решений;

2) уравнение (8) имеет единственное решение;

3) число решений уравнения (8) равно p^r, где $r \in \{1, \ldots, kn\}$.

Именно эти утверждения и характеризуют число решений систем уравнений (6) и (7).

Рассмотрим ряд следствий из теоремы.

Следствие 1. Для любого автомата $M \in \mathsf{A}_1$, если матрица $I \ominus D$ – обратимая, то при любом начальном состоянии $\boldsymbol{q}_0 \in \mathbf{Z}_{p^k}^n$ множество $S_{fxd}(M, \boldsymbol{q}_0)$ – бесконечное, причем множество $S_{fxd}^{(t+1)}(M, \boldsymbol{q}_0)$ – одноэлементное для каждого $t \in \mathbf{Z}_+$ и имеет вид $S_{fxd}^{(t+1)}(M, \boldsymbol{q}_0) = \{\boldsymbol{x}_1 \ldots \boldsymbol{x}_{t+1}\}$, где

$$\begin{cases} \boldsymbol{x}_1 = (I \ominus D)^{-1} \circ C \circ \boldsymbol{q}_0, \\ \boldsymbol{x}_{i+1} = (I \ominus D)^{-1} \circ C \circ (A^i \circ \boldsymbol{q}_0 \oplus (\overset{i-1}{\underset{j=1}{\oplus}} A^{i-j} \circ B \circ \boldsymbol{x}_j) \oplus B \circ \boldsymbol{x}_i) \quad (i = 1, ..., t). \end{cases}$$

Следствие 2. Для любого автомата $M \in \mathsf{A}_2$, если матрица $I \ominus C \circ B$ – обратимая, то при любом начальном состоянии $\boldsymbol{q}_0 \in \mathbf{Z}_{p^k}^n$ множество $S_{fxd}(M, \boldsymbol{q}_0)$ – бесконечное, причем множество $S_{fxd}^{(t+1)}(M, \boldsymbol{q}_0)$ – одноэлементное для каждого $t \in \mathbf{Z}_+$ и имеет вид $S_{fxd}^{(t+1)}(M, \boldsymbol{q}_0) = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{t+1}\}$, где

$$\begin{cases} \boldsymbol{x}_1 = (I \ominus C \circ B)^{-1} \circ C \circ A \circ \boldsymbol{q}_0, \\ \boldsymbol{x}_{i+1} = (I \ominus C \circ B)^{-1} \circ C \circ A \circ (A^i \circ \boldsymbol{q}_0 \oplus \overset{i-1}{\underset{j=1}{\oplus}} A^{i-j} \circ B \circ \boldsymbol{x}_j \oplus B \circ \boldsymbol{x}_i) \quad (i = 1, \ldots, t). \end{cases}$$

Из 1-го уравнения систем (6) и (7) вытекает, что для любого автомата $M \in \mathsf{A}_1 \cup \mathsf{A}_2$ при любом начальном состоянии $\boldsymbol{q}_0 \in \mathbf{Z}_{p^k}^n$ существует следующий локальный критерий проверки пустоты множества $S_{fxd}(M, \boldsymbol{q}_0)$.

Следствие 3. Для любого автомата $M \in \mathsf{A}_1 \cup \mathsf{A}_2$ множество $S_{fxd}(M, \boldsymbol{q}_0)$ – непустое для таких и только таких состояний $\boldsymbol{q}_0 \in \mathbf{Z}_{p^k}^n$, для которых имеет решения уравнение

$$(I \ominus D) \circ \boldsymbol{x} = C \circ \boldsymbol{q}_0 \ (\boldsymbol{x} \in \mathbf{Z}_{p^k}^n), \tag{9}$$

если $M \in \mathsf{A}_1$, и уравнение

$$(I \ominus C \circ B) \circ \boldsymbol{x} = C \circ A \circ \boldsymbol{q}_0 \ (\boldsymbol{x} \in \mathbf{Z}_{p^k}^n), \tag{10}$$

если $M \in \mathsf{A}_2$.

Если $\boldsymbol{q}_0 = \mathbf{0}$, то и (9) и (10) имеют решение $\boldsymbol{x}_1 = \mathbf{0}$. Отсюда вытекает

Следствие 4. Для любого автомата $M \in \mathsf{A}_1 \cup \mathsf{A}_2$

$$S_{fxd}(M, \mathbf{0}) \neq \varnothing.$$

3. Характеристика множества $S_{fxd}^{(1)}(M, q)$ ($M \in \mathsf{A}_1 \cup \mathsf{A}_2$, $q \in \mathbf{Z}_{p^k}^n$)

Особенность следствия 3 состоит в том, что оно представляет собой «локальный критерий», т.е. характеристику структуры всего множества $S_{fxd}(M, \boldsymbol{q}_0)$, являющегося подмножеством свободной полугруппы $(\mathbf{Z}_{p^k}^n)^+$, в терминах образующего элемента $\boldsymbol{x} \in \mathbf{Z}_{p^k}^n$ полугруппы, выраженных через структуру множества $S_{fxd}^{(1)}(M, \boldsymbol{q}_0)$. Отсюда вытекает целесообразность исследования структуры множества $S_{fxd}(M, \boldsymbol{q})$ для $M \in \mathsf{A}_1 \cup \mathsf{A}_2$ при любом текущем состоянии $\boldsymbol{q} \in \mathbf{Z}_{p^k}^n$. Рассмотрим некоторые такие характеристики.

Из следствия 3 вытекает

Следствие 5. Для любого автомата $M \in \mathsf{A}_1 \cup \mathsf{A}_2$ проверка пустоты множества $S_{fxd}(M, \boldsymbol{q})$ при любом текущем состоянии $\boldsymbol{q} \in \mathbf{Z}_{p^k}^n$ сводится к проверке пустоты множества решений уравнения

$$(I \ominus D) \circ \boldsymbol{x} = C \circ \boldsymbol{q} \ (\boldsymbol{x} \in \mathbf{Z}_{p^k}^n), \tag{11}$$

если $M \in \mathsf{A}_1$, и уравнения

$$(I \ominus C \circ B) \circ \boldsymbol{x} = C \circ A \circ \boldsymbol{q} \ (\boldsymbol{x} \in \mathbf{Z}_{p^k}^n), \tag{12}$$

если $M \in \mathsf{A}_2$.

Из равенств (11) и (12) вытекает

Следствие 6. Для любого автомата $M \in \mathsf{A}_1 \cup \mathsf{A}_2$ и для любых состояний $\boldsymbol{q}', \boldsymbol{q}'' \in \mathbf{Z}_{p^k}^n$, если $\boldsymbol{x}' \in S_{fxd}^{(1)}(M, \boldsymbol{q}')$ и $\boldsymbol{x}''' \in S_{fxd}^{(1)}(M, \boldsymbol{q}'')$, то $\boldsymbol{x}' \ominus \boldsymbol{x}''' \in S_{fxd}^{(1)}(M, \boldsymbol{q}' \ominus \boldsymbol{q}'')$.

Множество $S_{fxd}(M, \mathbf{0})$ ($M \in \mathsf{A}_1 \cup \mathsf{A}_2$) следующим образом характеризует множество $S_{fxd}(M, \boldsymbol{q})$ для любого текущего состояния $\boldsymbol{q} \in \mathbf{Z}_{p^k}^n$.

Следствие 7. Для любого автомата $M \in \mathsf{A}_1 \cup \mathsf{A}_2$ при каждом текущем состоянии $\boldsymbol{q} \in \mathbf{Z}_{p^k}^n$ для любого входного символа $\boldsymbol{x}' \in S_{fxd}^{(1)}(M, \boldsymbol{q})$ истинно равенство

$$S^{(1)}_{fxd}\ (M, \boldsymbol{q}) = \{\, \boldsymbol{x}' \oplus\ \boldsymbol{x}'' \mid \boldsymbol{x}'' \in\ S^{(1)}_{fxd}\ (M, \mathbf{0})\}. \tag{13}$$

Из следствия 7 вытекает, что для любого автомата $M \in \mathsf{A}_1 \cup \mathsf{A}_2$ в явном виде достаточно построить только множество $S^{(1)}_{fxd}\ (M, \mathbf{0})$. Для любого текущего состояния $\boldsymbol{q} \in \mathbf{Z}^n_{p^k}$ множество $S^{(1)}_{fxd}\ (M, \boldsymbol{q})$ всегда может быть вычислено в соответствии с равенством (13).

Рассмотрим теперь автомат $M \in \mathsf{A}_1 \cup \mathsf{A}_2$ специального вида.

Из (11) и (12) вытекает

Следствие 8. Пусть матрицы, определяющие автомат $M \in \mathsf{A}_1 \cup \mathsf{A}_2$, выбраны так, что:

а) $D = I$, если $M \in \mathsf{A}_1$;

б) $C \circ B = I$, если $M \in \mathsf{A}_2$.

Тогда

$$S^{(1)}_{fxd}\ (M, \boldsymbol{q}) = \mathbf{Z}^n_{p^k}$$

для любого такого текущего состояния $\boldsymbol{q} \in \mathbf{Z}^n_{p^k}$, что имеет решение уравнение

$$C \circ \boldsymbol{q} = \mathbf{0},$$

если $M \in \mathsf{A}_1$, и уравнение

$$C \circ A \circ \boldsymbol{q} = \mathbf{0},$$

если $M \in \mathsf{A}_2$.

Пусть матрицы, определяющие автомат $M \in \mathsf{A}_1 \cup \mathsf{A}_2$, выбраны так, что:

а) $I \ominus D = \alpha \circ C$, если $M \in \mathsf{A}_1$;

б) $I \ominus C \circ B = \alpha \circ C \circ A$, если $M \in \mathsf{A}_2$,

α – фиксированный элемент кольца $\mathbf{Z}_{p^k}$. Тогда уравнения (11) и (12) принимают соответственно вид

$$C \circ (\alpha \circ \boldsymbol{x}) = C \circ \boldsymbol{q}\ (\boldsymbol{x} \in \mathbf{Z}^n_{p^k}) \tag{14}$$

и

$$C \circ A\ (\alpha \circ \boldsymbol{x}) = C \circ A \circ \boldsymbol{q}\ (\boldsymbol{x} \in \mathbf{Z}^n_{p^k}). \tag{15}$$

Из (14) (15) вытекает

Следствие 9. Пусть существует такой элемент α кольца $\mathbf{Z}_{p^k}$, что для автомата $M \in \mathsf{A}_1 \cup \mathsf{A}_2$ имеет место равенство $I \ominus D = \alpha \circ C$, если $M \in \mathsf{A}_1$, и равенство $I\ \ominus C \circ B = \alpha \circ C \circ A$, если $M \in \mathsf{A}_2$. Тогда

$$S^{(1)}_{fxd}\ (M, \boldsymbol{q}) \neq \varnothing$$

для любого такого текущего состояния $\boldsymbol{q} \in \mathbf{Z}^n_{p^k}$, для которого имеет решение уравнение

$$\alpha \circ \boldsymbol{x} = \boldsymbol{q}\ (\boldsymbol{x} \in\ \mathbf{Z}^n_{p^k}). \tag{16}$$

Заключение

В работе исследована структура множества $S_{fxd}\ (M, \boldsymbol{q}_0)$ неподвижных точек словарной функции, реализуемой инициальными линейными автоматами $(M, \boldsymbol{q}_0)$ Мили и Мура над кольцом $\mathbf{Z}_{p^k}$. Установлен критерий, когда множество $S_{fxd}\ (M, \boldsymbol{q}_0)$ – непустое, а также найдены условия, при которых $S_{fxd}\ (M, \boldsymbol{q}_0)$ – бесконечное множество. Охарактеризованы входные символы, являющиеся неподвижными точками для текущего состояния исследуемых автоматов. Показано, что в явном виде достаточно хранить только множество входных символов, являющихся неподвижными точками для состояния $\boldsymbol{q} = \mathbf{0}$ исследуемого автомата, а множество входных символов, являющихся неподвижными точками для любого текущего состояния $\boldsymbol{q}$, достаточно легко может быть вычислено по этому множеству. Таким образом, в процессе подачи на исследуемый автомат входного слова $\boldsymbol{x}_1 \ldots \boldsymbol{x}_{t+1} \in (\mathbf{Z}^n_{p^k})^{t+1}$ $(t \in \mathbf{Z}_+)$ определение тех элементов выходного слова $\boldsymbol{y}_1 \ldots \boldsymbol{y}_{t+1} \in (\mathbf{Z}^n_{p^k})^{t+1}$, которые совпадают с соответствующими входными символами, может быть сведено к локальным действиям. Действительно, если $\boldsymbol{q} \in \mathbf{Z}^n_{p^k}$ – текущее состояние $\boldsymbol{q} \in \mathbf{Z}^n_{p^k}$ автомата M, $\boldsymbol{x} \in \mathbf{Z}^n_{p^k}$ – текущий входной символ, то проверка равенства входного символа $\boldsymbol{x}$ соответствующему выходному символу сводится к проверке равенства (11) для автомата Мили и равенства (12) для автомата Мура.

Полученные в работе результаты имеют следующее естественное обобщение. Зафиксируем обратимый элемент $\gamma \in \mathbf{Z}_{p^k}^n$ кольца $\mathbf{Z}_{p^k}$. Назовем γ-неподвижной точкой словарной функции $f_{(M,\boldsymbol{q}_0)}: (\mathbf{Z}_{p^k}^n)^+ \to (\mathbf{Z}_{p^k}^n)^+$ любое такое входное слово $\boldsymbol{x}_1 \ldots \boldsymbol{x}_{t+1} \in (\mathbf{Z}_{p^k}^n)^{t+1}$ $(t \in \mathbf{Z}_+)$, что

$$f_{(M,\boldsymbol{q}_0)}(\boldsymbol{x}_1 \ldots \boldsymbol{x}_{t+1}) = (\gamma \circ \boldsymbol{x}_1) \ldots (\gamma \circ \boldsymbol{x}_{t+1}).$$

Если под множеством $S_{fxd}(M, \boldsymbol{q})$ понимать множество всех γ-неподвижных точек словарной функции $f_{(M,\boldsymbol{q}_0)}$, то все полученные в работе результаты остаются истинными, если матрицу I заменить матрицей $\gamma \circ I$.

ЛИТЕРАТУРА

1. *Гилл А*. Линейные последовательностные машины. М.: Наука, 1974. 288 с.
2. *Ван дер Варден Б.Л.* Алгебра. М.: Наука, 1979. 624 с.
3. *Скобелев В.В.* Анализ линейных автоматов над кольцом $\mathbf{Z}_{p^k}$ // Труды института прикладной математики и механики НАН Украины. 2007. Т. 14. С. 162 – 173.
4. *Скобелев В.В.* Задача идентификации линейных автоматов над кольцом $\mathbf{Z}_{p^k}$ // Труды VII Междунар. конф. «Идентификация систем и задачи управления (SICPRO'08)» (Москва, 28 – 31 января 2008 г.). М.: ИПУ РАН, 2008. С. 1154 – 1185.
5. *Скобелев В.В.* Шифры на основе линейных БПИ-автоматов над кольцом $\mathbf{Z}_{p^k}$ // Вестник ТГУ. Приложение. 2007. № 23. С. 118 – 122.
6. *Курмит А.А.* Автоматы без потери информации конечного порядка. Рига: Зинатне, 1972. 266 с.
7. *Кудрявцев В.Б. и др*. Введение в теорию конечных автоматов. М.: Наука, 1985. 320 с.
8. *Трахтенброт Б.А.*, *Барздинь Я.М.* Конечные автоматы (поведение и синтез). М.: Наука, 1970. 400 с.
9. *Скобелев В.В.* Об обратимых матрицах над кольцом $\mathbf{Z}_{p^k}$ // Труды института прикладной математики и механики НАН Украины. 2006. Вып. 13. С. 185 – 192.