УДК 518.6+681.3

©2008. **В.В. Скобелев**

ХАРАКТЕРИСТИКИ ЛИНЕЙНЫХ ОДНОМЕРНЫХ АВТОМАТОВ С ЛАГОМ l НАД КОНЕЧНЫМ КОЛЬЦОМ

Для линейных одномерных автоматов с лагом l над кольцом $\mathcal{Z}_{p^k}$ охарактеризован подкласс, состоящий из БПИ-автоматов. Исследована структура классов сильно связных и перестановочных линейных одномерных автоматов с лагом l над кольцом $\mathcal{Z}_{p^k}$.

Введение. Естественным обобщением регистров сдвига с линейной обратной связью [1], построенных над полем $\mathbf{GF}(p^k)$ (где p – простое число, а $k \in \mathbf{N}$), являются линейные управляемые последовательности над кольцом

$$\mathcal{Z}_{p^k} = (\mathbf{Z}_{p^k}, \oplus, \circ),$$

где

$$a \oplus b = a + b \ (mod\ p^k),$$

$$a \circ b = ab \ (mod\ p^k).$$

В [2] с позиции как современной теории кодирования, так и с позиции современной криптографии, исследованы свойства таких последовательностей, в случае, когда управление – тождественный нуль.

Однако с указанных выше позиций, а также с позиции теории автоматов [3–5], значительно больший интерес представляет исследование поведения такой пары взаимодействующих линейных управляемых последовательностей, что одна из них определяет изменение состояния, а вторая – выходной символ. Таким образом, мы естественно приходим к одномерным линейным автоматам с лагом l над конечным кольцом. Отметим следующие три обстоятельства.

Во-первых, по-видимому, первая попытка систематического исследования таких автоматов именно с позиции математической теории систем [6, 7] предпринята в [8, 9].

Во-вторых, фрагменты схем, построенных на основе указанных пар последовательностей являются типичными, практически, для всех кандидатов, представленных в реализуемых в настоящее время европейском и японском проектах, соответственно, NESSIE и CRYPTREC, разработки схем поточного шифрования.

В третьих, такие автоматы являются нетривиальным обобщением специального случая n-мерных линейных автоматов над конечным кольцом, исследованных в [10].

Отличие настоящей работы от [8, 9] состоит в том, что мы исследуем именно те свойства, которые естественно формулируются в классических терминах теории автоматов.

Структура работы – следующая. В п.1 введены необходимые понятия и определения. В п.2 охарактеризованы некоторые подклассы исследуемых моделей. Заключение содержит ряд выводов.

1. Основные понятия и определения. Объектом исследования являются инициальные автоматы Мили и Мура, определяемые, соответственно, уравнениями

$$(M_1, \mathbf{q}_0) : \begin{cases} q_{n+l} = \bigoplus\limits_{i=1}^{l} a_i \circ q_{n+l-i} \oplus b \circ x_{n+1} \\ y_{n+1} = \bigoplus\limits_{i=1}^{l} c_i \circ q_{n+l-i} \oplus d \circ x_{n+1} \end{cases} \tag{1}$$

и

$$(M_2, \mathbf{q}_0) : \begin{cases} q_{n+l} = \bigoplus\limits_{i=1}^{l} a_i \circ q_{n+l-i} \oplus b \circ x_{n+1} \\ y_{n+1} = \bigoplus\limits_{i=1}^{l} c_i \circ q_{n+l+1-i} \end{cases}, \tag{2}$$

где $a_i, b_i, c, d \in \mathbf{Z}_{p^k}$ $(i = 1, \ldots, l)$ – параметры, x и y – соответственно, входная и выходная переменная, а $\mathbf{q}_0 = (q_0, q_1, \ldots, q_{l-1}) \in \mathbf{Z}_{p^k}^l$ – начальное состояние автомата M_j $(j = 1, 2)$.

Обозначим через $\mathcal{A}_{l,j}$ $(j = 1, 2)$ – множество всех автоматов M_j. Из (1) и (2) вытекает, что для всех $l \in \mathbf{N}$

$$|\mathcal{A}_{l,j}| = p^{k\cdot(2\cdot l+3-j)} \ \ (j = 1, 2). \tag{3}$$

При решении задач разработки методов защиты информации особый интерес представляет случай, когда M_j $(j = 1, 2)$ – БПИ-автомат [11], т.е. когда ограниченно-детерминированная функция $f : \mathbf{Z}_{p^k}^+ \to \mathbf{Z}_{p^k}^+$, реализуемая инициальным автоматом $(M_j, \mathbf{q}_0)$ $(j = 1, 2)$, является биекцией при любом начальном состоянии $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^l$. В связи с этим обозначим через $\mathcal{A}_{l,j}^{inv}$ $(j = 1, 2)$ множество всех обратимых автоматов $M_j \in \mathcal{A}_{l,j}$.

Из (1) и (2) вытекает

Утверждение 1. Для всех $l \in \mathbf{N}$:

1) $M_1 \in \mathcal{A}_{l,1}^{inv}$ тогда и только тогда, когда d – обратимый элемент кольца $\mathcal{Z}_{p^k}$.

2) $M_2 \in \mathcal{A}_{l,2}^{inv}$ тогда и только тогда, когда c_1 и b – обратимые элементы кольца $\mathcal{Z}_{p^k}$.

Из утверждения 1 вытекает, что обратные автоматы имеют следующий вид:

$$(M_1^{-1}, \mathbf{q}_0) : \begin{cases} q_{n+1} = \bigoplus\limits_{i=1}^{l} \alpha_i \circ q_{n+l-i} \oplus \beta \circ x_{n+1} \\ y_{n+1} = \bigoplus\limits_{i=1}^{l} \gamma_i \circ q_{n+l-i} \oplus \delta \circ x_{n+1} \end{cases},$$

где $\beta = b \circ d^{-1}$, $\delta = d^{-1}$ и $\alpha_i = a_i \ominus b \circ d^{-1} \circ c_i$, $\gamma_i = \ominus d^{-1} \circ c_i$ для всех $i = 1, \ldots, l$,

$$(M_2^{-1}, \mathbf{q}_0) : \begin{cases} q_{n+l} = \bigoplus\limits_{i=2}^{l} \alpha_i \circ q_{n+l+1-i} \oplus \beta \circ x_{n+1} \\ y_{n+1} = \bigoplus\limits_{i=1}^{l} \gamma_i \circ q_{n+l+1-i} \oplus \delta \circ x_{n+1} \end{cases},$$

где $\beta = c_1^{-1}$, $\delta = b^{-1} \circ c_1^{-1}$, $\alpha_i = c_1^{-1} \circ c_i$ $(i = 2, \ldots, l)$ и

$$\gamma_i = \begin{cases} \ominus b^{-1} \circ (c_1^{-1} \circ c_{i+1} \oplus a_i), & i = 1, \ldots, l-1 \\ \ominus b^{-1} \circ a_l, & i = l \end{cases}.$$

Из (3) и утверждения 1 вытекает, что для всех $l \in \mathbf{N}$

$$|\mathcal{A}_{l,j}^{inv}| = p^{-j} \cdot (p-1)^j \cdot |\mathcal{A}_{l,j}| \ \ (j = 1, 2). \tag{4}$$

Из (4) вытекает, что истинно

Следствие 1. *Для всех $l \in \boldsymbol{N}$*

$$\frac{|\mathcal{A}_{l,j}^{inv}|}{|\mathcal{A}_{l,j}|} = p^{-j} \cdot (p-1)^j \ \ (j = 1, 2).$$

Итак, показано, что в множестве $\mathcal{A}_{l,j}$ $(j = 1, 2)$ доля обратимых автоматов не зависит от значения числа k.

2. Основные результаты. Охарактеризуем некоторые подмножества множеств $\mathcal{A}_{l,j}$ $(j = 1, 2)$ и $\mathcal{A}_{l,j}^{inv}$ $(j = 1, 2)$, естественно определяемые в терминах теории автоматов.

Теорема 1. *Для всех $l \in \mathbf{N}$ автомат $M_i \in \mathcal{A}_{l,j}$ $(j = 1, 2)$ – сильно связный тогда и только тогда, когда b – обратимый элемент кольца $\mathcal{Z}_{p^k}$.*

Доказательство.

1. Необходимость. Пусть автомат $M_i \in \mathcal{A}_{l,j}$ $(j = 1, 2)$ – сильно связный. Тогда для любых двух его состояний $\mathbf{q} = (q_0, q_1, \ldots, q_{l-1}) \in \mathbf{Z}_{p^k}^l$ и $\mathbf{q}' = (q_0', q_1', \ldots, q_{l-1}') \in \mathbf{Z}_{p^k}^l$ существует входное слово $x_1 x_2 \ldots x_n \in \mathbf{Z}_{p^k}^n$, переводящее состояние $\mathbf{q}$ в состояние $\mathbf{q}'$.

Предположим противное, т. е. что b – необратимый элемент кольца $\mathcal{Z}_{p^k}$. Тогда

$$b \equiv 0 \ (mod\ p).$$

Рассмотрим любое такое состояние $\mathbf{q}_0 = (q_0, q_1, \ldots, q_{l-1})$ автомата M_j $(j = 1, 2)$, что

$$q_i \equiv 0 \ (mod\ p)$$

для всех $i = 0, 1, \ldots, l-1$.

Из 1-го уравнения, определяющего автомат M_j, вытекает, что

$$q_l \equiv 0 \ (mod\ p)$$

для любого входного символа $x \in \mathbf{Z}_{p^k}$. Таким образом, состояние $\mathbf{q}_0$ под действием любого входного символа $x \in \mathbf{Z}_{p^k}$ переходит в такое состояние $\mathbf{q}_1 = (q_1, \ldots, q_{l-1}, q_l) \in \mathbf{Z}^l_{p^k}$, что $q_i \equiv 0 \ (mod\ p)$ для всех $i = 1, \ldots, l$.

Отсюда вытекает (что доказывается индукцией по длине входного слова), что для любого входного слова $x_1 x_2 \ldots x_n \in \mathbf{Z}^n_{p^k}$ состояние $\mathbf{q}_0$ переходит в такое состояние $\mathbf{q}_n = (q_n, q_{n+1}, \ldots, q_{n+l-1}) \in \mathbf{Z}^l_{p^k}$, что $q_i \equiv 0 \ (mod\ p)$ для всех $i = n, n+1, \ldots, n+l-1$.

Это означает, что из состояния $\mathbf{q}_0$ недостижимо ни одно состояние $\mathbf{q}' = (q'_0, \ldots, q'_{l-1}) \in \mathbf{Z}^l_{p^k}$, удовлетворяющее следующему условию: существует такое $j \in \{0, 1, \ldots, l-1\}$, что $q'_j \equiv m \ (mod\ p)$, где $m \in \{1, 2, ..., l-1\}$. Отсюда вытекает, что автомат M_j не является сильно связным.

Полученное противоречие показывает, что предположение – ложное, т. е. если $M_j \in \mathcal{A}_{l,j}$ $(j = 1, 2)$ – сильно связный автомат, то b – обратимый элемент кольца $\mathcal{Z}_{p^k}$, что и требовалось показать.

2. Достаточность. Пусть b – обратимый элемент кольца $\mathcal{Z}_{p^k}$. Покажем, что из любого состояния $\mathbf{q}_0 = (q_0, q_1, ..., q_{l-1}) \in \mathbf{Z}^l_{p^k}$ автомата M_j $(j = 1, 2)$ достижимо любое его состояние $\mathbf{q}'_0 = (q'_0, q'_1, ..., q'_{l-1}) \in \mathbf{Z}^l_{p^k}$.

Выберем такое входное слово $x_1 ... x_l \in \mathbf{Z}^l_{p^k}$, что

$$b \circ x_{i+1} = q'_i \ominus \bigoplus_{m=1}^{i} a_m \circ q'_{i-m} \ominus \bigoplus_{m=i}^{l-1} a_m \circ q_m \ \ (i = 0, 1, ..., l-1). \tag{5}$$

Так как b – обратимый элемент кольца $\mathcal{Z}_{p^k}$, то система (5) имеет единственное решение

$$x_{i+1} = b^{-1} \circ (q'_i \ominus \bigoplus_{m=1}^{i} a_m \circ q'_{i-m} \ominus \bigoplus_{m=i}^{l-1} a_m \circ q_m) \ \ (i = 0, 1, ..., l-1). \tag{6}$$

Из 1-го уравнения, определяющего автомат M_j $(j = 1, 2)$ вытекает, что входное слово $x_1 ... x_l \in \mathbf{Z}^l_{p^k}$, где x_{i+1} $(i = 0, 1, ..., l-1)$ определяется равенством (6), порождает следующую последовательность переходов состояний автомата M_j $(j = 1, 2)$

$$\mathbf{q}_0 \to \mathbf{q}_1 \to ... \to \mathbf{q}_{l-1} \to \mathbf{q}_l = \mathbf{q}'_0, \tag{7}$$

где

$$\mathbf{q}_i = (q_i, ..., q_{l-1}, q'_0, q'_1, ..., q'_{i-1}) \ \ (i = 1, ..., l). \tag{8}$$

Из (8) вытекает, что если b – обратимый элемент кольца $\mathcal{Z}_{p^k}$, то из любого состояния $\mathbf{q}_0 \in \mathbf{Z}^l_{p^k}$ автомата M_j $(j = 1, 2)$ достижимо любое его состояние $\mathbf{q}'_0 \in \mathbf{Z}^l_{p^k}$. Это означает, что M_j $(j = 1, 2)$ – сильно связный автомат, что и требовалось показать.

Теорема доказана.

Обозначим через $\mathcal{A}^{sc}_{l,j}$ $(j = 1, 2)$ множество всех сильно связных автоматов $M_j \in \mathcal{A}_{l,j}$.

Из теоремы 1 вытекает, что для всех $l \in \mathbf{N}$

$$|\mathcal{A}_{l,j}^{sc}| = p^{-1} \cdot (p-1) \cdot |\mathcal{A}_{l,j}| \ \ (j = 1, 2).$$

Следующее утверждение характеризует степень достижимости [5] автомата $M_j \in \mathcal{A}_{l,j}^{sc}$ $(j = 1, 2)$.

Утверждение 2. Для всех $l \in \mathbf{N}$ диаметр графа переходов любого автомата $M_j \in \mathcal{A}_{l,j}^{sc}$ $(j = 1, 2)$ равен l.

Доказательство. Выберем такие состояния $\mathbf{q}_0 = (q_0, q_1, ..., q_{l-1}) \in \mathbf{Z}_{p^k}^l$ и $\mathbf{q}_0' = (q_0', q_1', ..., q_{l-1}') \in \mathbf{Z}_{p^k}^l$, что

$$q_i' \neq q_i$$

для всех $i = 0, 1, ..., l-1$.

Из (5)–(8) вытекает, что $x_1, ..., x_l \in \mathbf{Z}_{p^k}^l$ – кратчайшее входное слово, переводящее состояние $\mathbf{q}_0$ в состояние $\mathbf{q}_0'$. Следовательно, диаметр графа переходов автомата M_j равен l.

Утверждение доказано.

Положим

$$\mathcal{A}_{l,j}^{sc-inv} = \mathcal{A}_{l,j}^{sc} \bigcap \mathcal{A}_{l,j}^{inv} \ \ (j = 1, 2).$$

Из утверждения 1 и теоремы 1 вытекает, что для всех $l \in \mathbf{N}$

$$\mathcal{A}_{l,2}^{inv} \subset \mathcal{A}_{l,2}^{sc-inv}$$

и

$$|\mathcal{A}_{l,j}^{sc-inv}| = p^{-2} \cdot (p-1)^2 \cdot |\mathcal{A}_{l,i}| = (1 - p^{-1})^2 \cdot |\mathcal{A}_{l,j}| \ \ (j = 1, 2).$$

Теорема 2. *Для всех $l \in \mathbf{N}$ автомат $M_j \in \mathcal{A}_{l,j}$ $(j = 1, 2)$ – перестановочный тогда и только тогда, когда a_l – обратимый элемент кольца $\mathcal{Z}_{p^k}$.*

Доказательство. Автомат $M_j \in \mathcal{A}_{l,j}$ $(j = 1, 2)$ не является перестановочным тогда и только тогда, когда существуют два такие его состояния $\mathbf{q}_0 = (q_0, q_1, ..., q_{l-1}) \in \mathbf{Z}_{p^k}^l$ и $\mathbf{q}_0' = (q_0', q_1'...., q_{l-1}') \in \mathbf{Z}_{p^k}^l$ и такой входной символ $x \in \mathbf{Z}_{p^k}$, что

$$\mathbf{q}_1 = \mathbf{q}_1', \tag{9}$$

где $\mathbf{q}_1 = (q_1, ..., q_{l-1}, q_l)$ и $\mathbf{q}_1' = (q_1', ..., q_{l-1}', q_l')$, а q_l и q_l' вычисляются из 1-го уравнения, определяющего автомат M_j.

Из (9) вытекает, что

$$q_i = q_i' \ \ (i = 1, ..., l). \tag{10}$$

Так как

$$\mathbf{q}_0 \neq \mathbf{q}_0',$$

то равенство (9) эквивалентно тому, что

$$\mathbf{q}_0 = (q_0, q_1, ..., q_{l-1}),$$

$$\mathbf{q}'_0 = (q'_0, q_1, ..., q_{l-1}),$$

где

$$q_0 \neq q'_0$$

и

$$q_l = q'_l.$$

Из 1-го уравнения, определяющего автомат M_j $(j = 1, 2)$ вытекает, что равенство $q_l = q'_l$ эквивалентно тому, что $q'_0 \ominus q_0$ — ненулевое решение уравнения

$$a_l \circ u = 0. \tag{11}$$

Уравнение (11) имеет ненулевое решение тогда и только тогда, когда $a_l \equiv 0 \pmod{\text{p}}$, т. е. когда a_l – необратимый элемент кольца $\mathcal{Z}_{p^k}$.

Итак, показано, что автомат $M_j \in \mathcal{A}_{l,j}$ $(j = 1, 2)$ не является перестановочным автоматом тогда и только тогда, когда элемент $a_l \in \mathbf{Z}_{p^k}$ не является обратимым элементом кольца $\mathcal{Z}_{p^k}$.

Теорема доказана.

Обозначим через $\mathcal{A}^p_{l,j}$ $(j = 1, 2)$ множество всех перестановочных автоматов $M_j \in \mathcal{A}_{l,i}$. Из (3) и теоремы 2 вытекает, что для всех $l \in \mathbf{N}$

$$|\mathcal{A}^p_{l,j}| = (1 - p^{-1}) \cdot |\mathcal{A}_{l,j}| \ \ (j = 1, 2).$$

Положим

$$\mathcal{A}^{p-inv}_{l,j} = \mathcal{A}^{inv}_{l,j} \bigcap \mathcal{A}^p_{l,j} \ \ (j = 1, 2).$$

Из утверждения 1, теоремы 2 и (3) вытекает, что для всех $l \in \mathbf{N}$

$$|\mathcal{A}^{p-inv}_{l,j}| = (1 - p^{-1})^{j+1} \cdot |\mathcal{A}_{l,j}| \ \ (j = 1, 2).$$

Заключение. В настоящей работе установлен ряд характеристик для линейных одномерных автоматов Мили и Мура с лагом l над кольцом $\mathcal{Z}_{p^k}$. Исследована структура подклассов, состоящих из сильно связных автоматов, из перестановочных автоматов, а также подсчитано число автоматов в этих классах. Охарактеризована структура подкласса БПИ-автоматов, которые представляют особый интерес при решении задач защиты информации.

Характеристика структуры классов эквивалентных состояний для автоматов, принадлежащих множествам $\mathcal{A}_{l,j}$, $\mathcal{A}^{inv}_{l,j}$ $(j = 1, 2)$, а также поиск критерия эквивалентности автоматов, принадлежащих этим множествам, представляет собой одно из направлений дальнейших исследований.

Другое направление исследований состоит в анализе сложности параметрической идентификации и сложности идентификации начального состояния для автоматов, принадлежащих множествам $\mathcal{A}_{l,j}$, $\mathcal{A}^{inv}_{l,j}$ $(j = 1, 2)$.

1. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576с.
2. *Кузьмин А.С., Куракин В.Л., Нечаев А.А.* Свойства линейных и полилинейных рекуррент над кольцами Галуа (I) / В кн.: Труды по дискретной математике. Т.2. – М.: ТВП, 1998. – С.191-222.
3. *Глушков В.М.* Синтез цифровых автоматов. – М: Физматгиз, 1962. – 476с.
4. *Кудрявцев В.Б. и др.* Введение в теорию конечных автоматов. – М: Наука, 1985. – 320с.
5. *Трахтенброт Б.А., Барздинь Я.М.* Конечные автоматы: поведение и синтез. – М: Наука, 1970. – 400с.
6. *Калман Р., Фалб П., Арбиб М.* Очерки по математической теории систем. – М: Мир, 1971. – 400с.
7. *Месарович М., Такахара Я.* Общая теория систем: математические основы. – М: Мир, 1978. – 311с.
8. *Фараджев Р.Г.* Линейные последовательностные машины. – М: Советское радио, 1975. – 248с.
9. *Гилл А.* Линейные последовательностные машины. – М: Наука, 1974. – 287с.
10. *Скобелев В.В.* Исследование структуры множества линейных БПИ-автоматов над кольцом $\mathbb{Z}_{p^k}$ // Доповіді НАН України. – 2007. – №10. – С.44-49.
11. *Курмит А.А.* Автоматы без потери информации конечного порядка. – Рига: Зинатне, 1972. – 266с.

Ин-т прикл. математики и механики НАН Украины, Донецк
vv_skobelev@iamm.ac.donetsk.ua

Получено 20.03.08