**УДК 512.552+519.713**

# О некоторых свойствах нелинейных автоматов над конечным кольцом

В.Г. Скобелев[1]

*Abstract* – **Properties of automata over a finite associative-commutative ring are investigated. Complexity of parametric identification and of reconstruction of initial state is characterized.**

*Key words* – **Finite rings, automata, parametric identification.**

## I. Введение

Исследование автоматов, представленных уравнениями над конечным ассоциативно-коммутативным кольцом $(K,+,\cdot)$ с единицей, актуально как с позиции теории автоматов, так и с позиции их возможных применений при решении задач криптографии. В настоящей работе дан обзор результатов, представленных в [1-3].

## II. Автоматы общего вида

Обозначим через $A_1$ множество всех автоматов Мили $M_1$, а через $A_2$ множество всех автоматов Мура $M_2$, определенных, соответственно, уравнениями

$$M_1:\begin{cases}\vec{q}_{t+1}=\vec{f}_1(\vec{q}_t)+\vec{f}_3(\vec{x}_{t+1})\\ \vec{y}_{t+1}=\vec{f}_2(\vec{q}_t)+\vec{f}_4(\vec{x}_{t+1})\end{cases}, \qquad (1)$$

$$M_2:\begin{cases}\vec{q}_{t+1}=\vec{f}_1(\vec{q}_t)+\vec{f}_3(\vec{x}_{t+1})\\ \vec{y}_{t+1}=\vec{f}_2(\vec{q}_{t+1})\end{cases}, \qquad (2)$$

где $\vec{f}_i: K^n \to K^n$ $(i=1,\dots,4)$, а $\vec{q}_t, \vec{x}_t, \vec{y}_t \in K^n$ – соответственно, состояние автомата, входной и выходной символ в момент $t$. Из (1) и (2) вытекает, что:

1) $M \in A_1 \cup A_2$ – сильно-связный автомат, диаметр автоматного графа которого равен 1, тогда и только тогда, когда $\vec{f}_3: K^n \to K^n$ – биекция;

2) $M \in A_1 \cup A_2$ – перестановочный автомат только тогда, когда $\vec{f}_3: K^n \to K^n$ – биекция;

3) если $\vec{f}_2: K^n \to K^n$ – биекция, то $M \in A_1$ – приведенный автомат, любые два состояния которого различимы любым входным символом;

4) если $\vec{f}_1: K^n \to K^n$ и $\vec{f}_2: K^n \to K^n$ – биекции, то $M \in A_2$ – приведенный автомат, любые два состояния которого различимы любым входным символом;

5) состояния $\vec{q}^{(1)}, \vec{q}^{(2)} \in K^n$ $(\vec{q}^{(1)} \neq \vec{q}^{(2)})$ автомата $M \in A_1 \cup A_2$ являются близнецами тогда и только тогда, когда они принадлежат одному и тому же классу разбиения $K^n/\varepsilon$, где $\varepsilon = \ker\vec{f}_1 \cap \ker\vec{f}_2$, если $M \in A_1$ и $\varepsilon = \ker\vec{f}_1$, если $M \in A_2$.

6) для любых отображений $\vec{f}_i: K^n \to K^n$ $(i=1,2,3)$ множество $A_1^{inv}$ обратимых автоматов $M \in A_1$ определяется равенством

$$A_1^{inv} = \{M_1 \in A_1 \mid \vec{f}_4: K^n \to K^n - \text{биекция}\}.$$

7) для любого отображения $\vec{f}_1: K^n \to K^n$ множество $A_2^{inv}$ обратимых автоматов $M \in A_2$ определяется равенством истинно равенство

$$A_2^{inv} = \{M_2 \in A_2 \mid \vec{f}_i: K^n \to K^n \ (i=2,3) - \text{биекции}\}.$$

Далее рассмотрим такие подмножества $A_{j+2} \subseteq A_j$ $(j=1,2)$, автоматов $M_i$ $(i=3,4)$, что

$$M_3:\begin{cases}\vec{q}_{t+1}=A\vec{q}_t\vec{q}_t^{\,T}\vec{b}+C\vec{q}_t+\vec{d}+E\vec{x}_{t+1}\\ \vec{y}_{t+1}=G\vec{q}_t+F\vec{x}_{t+1}\end{cases}, \qquad (3)$$

$$M_4:\begin{cases}\vec{q}_{t+1}=A\vec{q}_t\vec{q}_t^{\,T}\vec{b}+C\vec{q}_t+\vec{d}+E\vec{x}_{t+1}\\ \vec{y}_{t+1}=G\vec{q}_{t+1}\end{cases}, \qquad (4)$$

где $\vec{q}_t=(q_t^{(1)},\dots,q_t^{(n)})^T$ – состояние, $\vec{x}_t=(x_t^{(1)},\dots,x_t^{(n)})^T$ – входной символ, $\vec{y}_t=(y_t^{(1)},\dots,y_t^{(n)})^T$ – выходной символ в момент $t$, $A, C, E, G, F$ – фиксированные $n\times n$-матрицы, а $\vec{b}=(b^{(1)},\dots,b^{(n)})^T$ и $\vec{d}=(d^{(1)},\dots,d^{(n)})^T$ – фиксированные векторы.

## III. Сложность параметрической идентификации

Из (3) вытекает, что:

1) идентификация каждой из матриц F и G осуществляется в результате $n$-кратного эксперимента высоты 1;

2) при известных F и G вектор $\vec{d}$ вычисляется единственным образом в результате простого эксперимента длины 2 тогда и только тогда, когда G – обратимая матрица;

3) при известных F, G и $\vec{d}$ матрица E вычисляется единственным образом в результате $n$-кратного эксперимента высоты 2 тогда и только тогда, когда G – обратимая матрица;

4) при известных F, G, E и $\vec{d}$ вычисление матриц A, C и вектора $\vec{b}$ сводится к поиску входных слов заранее

[1] Институт прикладной математики и механики НАН Украины, ул. Розы Люксембург, 74, Донецк, 83114, Украина
E-mail: skbv@iamm.ac.donetsk.ua

неизвестной длины и соответствующих начальных состояний с целью формирования и решения системы уравнений

$$G(A\vec{q}_t\vec{q}_t^{\,T}\vec{b}+C\vec{q}_t)=\vec{y}_{t+2}-F\vec{x}_{t+2}-G\vec{d}-GE\vec{x}_{t+1}. \quad (5)$$

Из (4) вытекает, что:

1) идентификация вектора $G\vec{d}$ осуществляется в результате простого эксперимента длины 1

2) при известном $G\vec{d}$ идентификация матрицы $GE$ осуществляется в результате $n$-кратного эксперимента высоты 1;

3) при известных $G\vec{d}$ и $GE$ вычисление матриц $GA$, $GC$ и вектора $\vec{b}$ сводится к поиску входных слов заранее неизвестной длины и соответствующих начальных состояний с целью формирования и решения системы уравнений

$$(GA)\vec{q}_t\vec{q}_t^{\,T}\vec{b}+(GC)\vec{q}_t=\vec{y}_{t+1}-G\vec{d}-(GE)\vec{x}_{t+1}. \quad (6)$$

## III. Сложность восстановления вектора начального состояния

Из (3) вытекает, что:

1) если $G$ – обратимая матрица, то вектор начального состояния автомата $M_3\in A_3$ однозначно определяется в результате любого простого эксперимента длины 1;

2) если $G$ – необратимая матрица, то восстановление вектора начального состояния автомата $M_3\in A_3$ сводится к поиску входных слов заранее неизвестной длины с целью формирования и решения системы уравнений

$$\begin{cases} G\vec{q}_0=\vec{y}_1-F\vec{x}_1\\ G\vec{q}_1=\vec{y}_2-F\vec{x}_2\\ \ldots\ldots\ldots\ldots\\ G\vec{q}_{i-1}=\vec{y}_i-F\vec{x}_i \end{cases}.$$

Из (4) вытекает, что восстановление вектора начального состояния автомата $M_4\in A_4$ сводится к поиску входных слов заранее неизвестной длины с целью формирования и решения системы уравнений

$$\begin{cases} G(A\vec{q}_0\vec{q}_0^{\,T}\vec{b}+C\vec{q}_0)=\vec{y}_1-G(E\vec{x}_1+\vec{d})\\ G(A\vec{q}_1\vec{q}_1^{\,T}\vec{b}+C\vec{q}_1)=\vec{y}_2-G(E\vec{x}_2+\vec{d})\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ G(A\vec{q}_{i-1}\vec{q}_{i-1}^{\,T}\vec{b}+C\vec{q}_{i-1})=\vec{y}_i-G(E\vec{x}_i+\vec{d}) \end{cases}.$$

## III. Выводы

Полученные результаты показывают, что анализ подмножеств множеств автоматов $A_i$ $(i=1,2)$, определяемых конкретными типами отображений $\vec{f}_j$ $(j=1,\ldots,4)$ (полиномы, экспоненты и т.д.) – возможное направление исследований.

Задача параметрической идентификации автомата $M_i\in A_i$ $(i=3,4)$ имеет высокую сложность. Переход к обратимым автоматам ничуть не упрощает решение задачи параметрической идентификации для исследуемых моделей. Поэтому при использовании автомата (3) или (4) в качестве математической модели симметричного поточного шифра (параметры играют роль долговременного секретного ключа) особое внимание следует уделить обеспечению секретности параметров $A$, $C$ и $\vec{b}$.

Выделение и исследование подмножеств множеств автоматов $A_i$ $(i=3,4)$, определяемых ограничениями на структуру матриц $A$, $C$ и вектора $\vec{b}$, для которых решение задачи параметрической идентификации существенно проще, чем в общем случае – другое направление исследований.

Задача восстановления вектора начального состояния автомата $M_4\in A_4$ всегда имеет высокую сложность, а задача восстановления вектора начального состояния автомата $M_3\in A_3$ имеет высокую сложность, если $G$ – необратимая матрица. При использовании обратимого автомата $M_i\in A_i$ $(i=3,4)$ в качестве поточного шифра вектор начального состояния играет роль секретного сеансового ключа. Поэтому при использовании обратимого автомата Мили в качестве поточного шифра должно быть обеспечено условие: $G$ – необратимая матрица.

Третье направление исследований состоит в выделении и исследовании подмножеств множеств автоматов $A_i$ $(i=3,4)$, определяемых ограничениями на структуру параметров, для которых решение задачи восстановления вектора начального состояния проще, чем в общем случае.

## Литература


[1] В.Г. Скобелев, "Анализ задачи параметрической идентификации нелинейных автоматов над конечным кольцом," *Проблемы управления и информатики*, 2010, № 5, с.37-41.

[2] В.Г. Скобелев, "Восстановление вектора начального состояния нелинейных автоматов над конечным кольцом," *Проблемы управления и информатики*, 2010, № 6, с.31-34.

[3] В.Г. Скобелев, "О некоторых множествах автоматов над конечным кольцом," *Кибернетика и системный анализ*, 2011, № 2, с. 27-30.