УДК 519.7+681.3

©2010. **В.Г. Скобелев**

АНАЛИЗ АВТОМАТА СПРОТТА НАД КОНЕЧНЫМ КОЛЬЦОМ

Над конечным ассоциативно-коммутативным кольцом с единицей исследуется автомат, построенный на основе 1-й хаотической динамической системы Спротта. Для исследуемой модели охарактеризованы классы эквивалентных состояний, решена задача параметрической идентификации. Получены соотношения,характеризующие вариацию поведения исследуемого автомата при вариации его начального состояния.

Ключевые слова: *конечные кольца, конечные автоматы, эквивалентные состояния, параметрическая идентификация.*

1. Введение. Защита информации является одной из актуальных проблем современных информационных технологий. Для решения этой проблемы предназначено шифрование информации. При построении почти всех кандидатов на современный стандарт поточного шифрования используются вычисления в кольцах вычетов. Это обстоятельство является обоснованием актуальности систематического исследования автоматов над конечными кольцами.

Автономные автоматы над конечными ассоциативно-коммутативными кольцами с единицей систематически исследованы в [1], а линейные и нелинейные автоматы общего вида – в [2].

В последнее время осуществлялись многочисленные попытки применения хаотических динамических систем [3] при решении задач преобразования информации. Непосредственное использование таких систем обнажило целый комплекс проблем, связанных с устойчивостью поведения и точностью вычислений. Для нивелирования последней проблемы достаточно перейти к вычислениям в конечной алгебраической системе. В качестве такой алгебраической системы естественно выбрать конечное кольцо, так как наличие делителей нуля автоматически приводит к поиску в процессе решения уравнений. Таким образом, построение аналогов над конечным кольцом для модельных хаотических динамических систем является мощным источником автоматов над конечным кольцом. Один из таких автоматов, а именно, автомат, построенный на основе 1-й хаотической динамической системы Спротта и исследуется в настоящей работе.

2. Автомат Спротта. Первая хаотическая динамическая система Спротта имеет следующий вид [3]:

$$\begin{cases} \dot{x} = y \\ \dot{y} = -x + yz \\ \dot{z} = 1 - y^2 \end{cases} .$$

Внесем информационную переменную в 1-е уравнение и перейдем к действиям в конечном ассоциативно-коммутативном кольце с единицей $\mathcal{K} = (K, +, \cdot)$. После

переобозначения переменных получим автомат

$$M_S : \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} + hq_t^{(2)} - hax_{t+1} \\ q_{t+1}^{(2)} = q_t^{(2)} - hq_t^{(1)} + hq_t^{(2)}q_t^{(3)} \\ q_{t+1}^{(3)} = h + q_t^{(3)} - h(q_t^{(2)})^2 \\ y_{t+1} = q_{t+1}^{(1)} \end{cases} \quad (t \in \mathbf{Z}_+), \tag{1}$$

где a, h – обратимые элементы кольца $\mathcal{K}$.

Автомат M_S допускает обращение. Обратный автомат имеет следующий вид:

$$M_S^{-1} : \begin{cases} q_{t+1}^{(1)} = x_{t+1} \\ q_{t+1}^{(2)} = q_t^{(2)} - hq_t^{(1)} + hq_t^{(2)}q_t^{(3)} \\ q_{t+1}^{(3)} = h + q_t^{(3)} - h(q_t^{(2)})^2 \\ y_{t+1} = (ha)^{-1}(q_t^{(1)} + hq_t^{(2)} - x_{t+1}) \end{cases} \quad (t \in \mathbf{Z}_+).$$

Пара инициальных автоматов $((M_S, \mathbf{q}_0), (M_S^{-1}, \mathbf{q}_0))$ $(\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T)$ определяет поточный шифр. А так как в процессе «шифрование-расшифрование» автоматы M_S и M_S^{-1} движутся в пространстве состояний по одной и той же траектории в одном и том же направлении, то достаточно исследовать только свойства автомата M_S.

3. Классы эквивалентных состояний автомата Спротта. Установим критерий эквивалентности состояний автомата Спротта M_S.

Теорема 1. *Состояния* $\boldsymbol{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ *и* $\widetilde{\boldsymbol{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$ *автомата* M_S *эквивалентны тогда и только тогда, когда*

$$\begin{cases} \widetilde{q}_0^{(1)} - q_0^{(1)} + h(\widetilde{q}_0^{(2)} - q_0^{(2)}) = 0 \\ \widetilde{q}_0^{(2)} - q_0^{(2)} - h(\widetilde{q}_0^{(1)} - q_0^{(1)}) + h(\widetilde{q}_0^{(2)}\widetilde{q}_0^{(3)} - q_0^{(2)}q_0^{(3)}) = 0 \\ \widetilde{q}_t^{(2)}\widetilde{q}_t^{(3)} - q_t^{(2)}q_t^{(3)} = 0 \ \ (t = 1, \ldots, |K^3| - 3) \end{cases} \tag{2}$$

для всех $x_1 \ldots x_t \in K^t$.

Доказательство. Состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$ автомата M_S эквивалентны тогда и только тогда, когда

$$y_t = \widetilde{y}_t \Leftrightarrow \widetilde{q}_t^{(1)} - q_t^{(1)} = 0 \tag{3}$$

для всех $x_1 \ldots x_t \in K^t$ $(t = 1, \ldots, |K|^3 - 1)$.

Представим систему уравнений (3) в виде

$$\widetilde{q}_1^{(1)} - q_1^{(1)} = 0, \tag{4}$$

$$\widetilde{q}_t^{(1)} - q_t^{(1)} = 0 \ \ (t = 2, \ldots, |K|^3 - 1). \tag{5}$$

Из 1-го уравнения системы (1) вытекает, что (4) и (5) эквивалентны уравнениям

$$\widetilde{q}_0^{(1)} - q_0^{(1)} + h(\widetilde{q}_0^{(2)} - q_0^{(2)}) = 0, \tag{6}$$

$$\widetilde{q}_t^{(1)} - q_t^{(1)} + h(\widetilde{q}_t^{(2)} - q_t^{(2)}) = 0 \tag{7}$$

для всех $x_1 \ldots x_t \in K^t$ $(t = 1, \ldots, |K|^3 - 2)$. А так как $h \in K$ – обратимый элемент кольца $\mathcal{K}$, то уравнения (7) эквивалентны уравнениям

$$\widetilde{q}_t^{(2)} - q_t^{(2)} = 0 \tag{8}$$

для всех $x_1 \ldots x_t \in K^t$ $(t = 1, \ldots, |K|^3 - 2)$.

Из 2-го уравнения системы (1) находим, что

$$\widetilde{q}_t^{(2)} - q_t^{(2)} = (\widetilde{q}_{t-1}^{(2)} - q_{t-1}^{(2)}) - h(\widetilde{q}_{t-1}^{(1)} - q_{t-1}^{(1)}) + h(\widetilde{q}_{t-1}^{(2)}\widetilde{q}_{t-1}^{(3)} - q_{t-1}^{(2)}q_{t-1}^{(3)}) \tag{9}$$

для всех $x_1 \ldots x_t \in K^t$ $(t = 1, \ldots, |K|^3 - 2)$.

Из (8) в (9) вытекает, что

$$(\widetilde{q}_0^{(2)} - q_0^{(2)}) - h(\widetilde{q}_0^{(1)} - q_0^{(1)}) + h(\widetilde{q}_0^{(2)}\widetilde{q}_0^{(3)} - q_0^{(2)}q_0^{(3)}) = 0, \tag{10}$$

$$\widetilde{q}_t^{(2)}\widetilde{q}_t^{(3)} - q_t^{(2)}q_t^{(3)} = 0 \tag{11}$$

для всех $x_1 \ldots x_t \in K^t$ $(t = 1, \ldots, |K|^3 - 3)$.

Уравнения (6), (10) и (11) и составляют систему уравнений (2). □

Следствие 1. *Состояния* $\boldsymbol{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ *и* $\widetilde{\boldsymbol{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$ *автомата* M_S *являются близнецами тогда и только тогда, когда*

$$\begin{cases} \widetilde{q}_0^{(1)} = q_0^{(1)} - h\Delta \\ \widetilde{q}_0^{(2)} = q_0^{(2)} + \Delta \\ \widetilde{q}_0^{(3)} = q_0^{(3)} + 2hq_0^{(2)}\Delta + h\Delta^2, \end{cases} \tag{12}$$

где Δ *– решение уравнения*

$$\Delta^3 + 3q_0^{(2)}\Delta^2 + (2(q_0^{(2)})^2 + h^{-1}q_0^{(3)} + 1 + h^{-2})\Delta = 0. \tag{13}$$

Доказательство. Состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$ автомата M_S являются близнецами тогда и только тогда, когда

$$\widetilde{q}_1^{(i)} - q_1^{(i)} = 0 \ \ (i = 1, 2, 3). \tag{14}$$

При $i = 1$ получим уравнение (6), а при $i = 2$ – уравнение (10). Кроме того, из 3-го уравнения системы (1) вытекает, что

$$\widetilde{q}_1^{(3)} - q_1^{(3)} = 0 \Leftrightarrow \widetilde{q}_0^{(3)} - q_0^{(3)} - h((\widetilde{q}_0^{(2)})^2 - (q_0^{(2)})^2) = 0.$$

Следовательно, уравнения (14) имеют следующий вид:

$$\begin{cases} \widetilde{q}_0^{(1)} - q_0^{(1)} + h(\widetilde{q}_0^{(2)} - q_0^{(2)}) = 0 \\ \widetilde{q}_0^{(2)} - q_0^{(2)} - h(\widetilde{q}_0^{(1)} - q_0^{(1)}) + h(\widetilde{q}_0^{(2)}\widetilde{q}_0^{(3)} - q_0^{(2)}q_0^{(3)}) = 0 \\ \widetilde{q}_0^{(3)} - q_0^{(3)} - h((\widetilde{q}_0^{(2)})^2 - (q_0^{(2)})^2) = 0 \end{cases} . \tag{15}$$

Положив

$$\begin{cases} \widetilde{q}_0^{(1)} = q_0^{(1)} + \Delta_1 \\ \widetilde{q}_0^{(2)} = q_0^{(2)} + \Delta \\ \widetilde{q}_0^{(3)} = q_0^{(3)} + \Delta_3 \end{cases} \tag{16}$$

и подставив (16) в (15), получим

$$\begin{cases} \Delta_1 + h\Delta = 0 \\ \Delta - h\Delta_1 + h(q_0^{(3)}\Delta + q_0^{(2)}\Delta_3 + \Delta\Delta_3) = 0 \\ \Delta_3 - h\Delta(2q_0^{(2)} + \Delta) = 0 \end{cases} . \tag{17}$$

Из 1-го и 3-го уравнений системы (17) находим

$$\begin{cases} \Delta_1 = -h\Delta \\ \Delta_3 = h\Delta(2q_0^{(2)} + \Delta) \end{cases} . \tag{18}$$

Подставив (18) во 2-е уравнение системы (17), получим, что Δ – решение уравнения

$$h^2\Delta^3 + 3h^2q_0^{(2)}\Delta^2 + (2h^2(q_0^{(2)})^2 + hq_0^{(3)} + h^2 + 1)\Delta = 0. \tag{19}$$

А так как $h \in K$ – обратимый элемент кольца $\mathcal{K}$, то уравнение (19) эквивалентно уравнению (13). □

4. Параметрическая идентификация автомата Спротта. Вначале предположим, что экспериментатор полностью управляет входным каналом автомата M_S, а также может устанавливать автомат M_S в любое требуемое начальное состояние сколько угодно раз. Такие предположения соответствуют одной из наиболее сильных атак на соответствующий поточный шифр.

Положив $\mathbf{q}_0 = (0,1,0)^T$ и $x_1 = 0$, получим $h = y_1$.

Положив $\mathbf{q}_0 = (0,0,0)^T$ и $x_1 = 1$, получим $a = -h^{-1}y_1$.

Таким образом, при сделанных предположениях задача параметрической идентификации автомата M_S тривиальна.

Теперь предположим, что экспериментатор не располагает возможностью устанавливать автомат M_S в требуемое состояние, но может проводить с автоматом M_S, по крайней мере, двухкратный классический эксперимент.

Подав на автомат M_S входной символ $x_1 = 0$, получим уравнение

$$y_1 = q_0^{(1)} + hq_0^{(2)}, \tag{20}$$

а подав входной символ $x_1 = 1$ – уравнение

$$\widetilde{y}_1 = q_0^{(1)} + hq_0^{(2)} - ha. \tag{21}$$

Вычитая (21) из (20), получим

$$ha = y_1 - \widetilde{y}_1. \tag{22}$$

Если экспериментатору известны компоненты $q_0^{(1)}$ и $q_0^{(2)}$ начального состояния автомата M_S, то из уравнения (20) находится параметр h, а из уравнения (22) – параметр a, т.е. в этом случае задача параметрической идентификации автомата M_S также тривиальна.

Ситуация изменяется, если экспериментатору не известны компоненты $q_0^{(1)}$ и $q_0^{(2)}$ начального состояния автомата M_S, так как решение нелинейного уравнение (22) эквивалентно поиску всех разложений элемента $y_1 - \widetilde{y}_1 \in K$ на два сомножителя, являющиеся обратимыми элементами кольца $\mathcal{K}$ с последующим различением всех возможных кандидатов на автомат M_S методами классической теории экспериментов с автоматами [4], а любая попытка увеличения высоты эксперимента автоматически приводит к нелинейной системе уравнений для поиска значения h.

Таким образом, поиск секретного ключа $(q_0^{(1)}, q_0^{(2)}, q_0^{(3)}, a, h)$ для поточного шифра $((M_S, \mathbf{q}_0), (M_S^{-1}, \mathbf{q}_0))$ является сложной задачей, если экспериментатор не располагает возможностью устанавливать автомат M_S в требуемое состояние.

5. Вариация поведения автомата Спротта. Пусть, что для автомата M_S осуществляется переход от начального состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ к начальному состоянию $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$. Подставив $\widetilde{\mathbf{q}}_0$ в систему уравнений (1), получим

$$M_S : \begin{cases} \widetilde{q}_{t+1}^{(1)} = \widetilde{q}_t^{(1)} + h\widetilde{q}_t^{(2)} - hax_{t+1} \\ \widetilde{q}_{t+1}^{(2)} = \widetilde{q}_t^{(2)} - h\widetilde{q}_t^{(1)} + h\widetilde{q}_t^{(2)}\widetilde{q}_t^{(3)} \\ \widetilde{q}_{t+1}^{(3)} = h + \widetilde{q}_t^{(3)} - h(\widetilde{q}_t^{(2)})^2 \\ \widetilde{y}_{t+1} = \widetilde{q}_{t+1}^{(1)} \end{cases} \qquad (t \in \mathbf{Z}_+). \tag{23}$$

Вычитая из (23) соответствующие уравнения системы (1), получим

$$\begin{cases} \Delta q_{t+1}^{(1)} = \Delta q_t^{(1)} + h\Delta q_t^{(2)} \\ \Delta q_{t+1}^{(2)} = (1 + hq_t^{(3)})\Delta q_t^{(2)} + h(q_t^{(2)} + \Delta q_t^{(2)})\Delta q_t^{(3)} - h\Delta q_t^{(1)} \\ \Delta q_{t+1}^{(3)} = \Delta q_t^{(3)} - h(2 + \Delta q_t^{(2)})\Delta q_t^{(2)} \\ \Delta y_{t+1} = \Delta q_{t+1}^{(1)} \end{cases} \qquad (t \in \mathbf{Z}_+), \tag{24}$$

где $\Delta q_t^{(i)} = \widetilde{q}_t^{(i)} - q_t^{(i)}$ $(i = 1, 2, 3)$ и $\Delta y_{t+1} = \widetilde{y}_{t+1} - y_{t+1}$ для всех $t \in \mathbf{Z}_+$.

Таким образом, вариация поведения автомата Спротта M_S при переходе от начального состояния $\mathbf{q}_0$ к начальному состоянию $\widetilde{\mathbf{q}}_0$ характеризуется системой уравнений (24).

6. Заключение. В работе исследован автомат Спротта M_S над конечным ассоциативно-коммутативным кольцом с единицей, являющийся аналогом соответствующей модельной хаотической динамической системы.

Исследование классов эквивалентных состояний автомата M_S показало, что эти классы имеют достаточно сложную структуру. Поэтому, любые попытки минимизации автомата Спротта M_S приведут к существенному усложнению модели. На это обстоятельство также указывает сложность соотношений, описывающих вариацию поведения автомата M_S при изменении его начального состояния.

Дальнейшее исследование автомата M_S может быть связано с решением задачи идентификации его начального состояния. Другое направление связано с исследованием сложности анализа автомата M_S в зависимости от значений его параметров. Третье направление связано с исследованием автоматов, построенных для остальных систем Спротта.

1. *Кузьмин А.С., Куракин В.Л., Нечаев А.А.* Свойства линейных и полилинейных рекуррент над кольцами Галуа (I) // Труды по дискретной математике. Т.2. / Под общей редакцией В.Я. Козлова. – М.: ТВП, 1998. – С. 191-222.
2. *Скобелев В.В., Скобелев В.Г.* Анализ шифрсистем. – Донецк: ИПММ НАНУ, 2009. – 479 с.
3. *Кузнецов С.П.* Динамический хаос. – М: Физматлит, 2001. – 296 с.
4. *Гилл А.* Введение в теорию конечных автоматов. – М: Наука, 1966. – 272 с.

V.G. Skobelev

Analysis of Sprott's automaton over some finite ring.

It is analyzed the automaton over a finite associative-commutative ring with the unit designed on the base of the first chaotic dynamical Sprott's system. For investigated model it is characterized classes of equivalent states and solved the problem of parametric identification. Formula characterizing variation of behavior of the investigated automaton under condition of variation of its initial state are established.

Keywords: *finite rings, finite automata, equivalent states, parametric identification.*

В.Г. Скобелєв

Аналіз автомата Спротта над скінченним кільцем.

Над скінченним асоціативно-комутативним кільцем з одиницею досліджено автомат, який отримано на основі 1-ї хаотичної динамічної системи Спротта. Для досліджуваної моделі охарактеризовано класи еквівалентних станів, розв'язано задачу параметричної ідентифікації. Отримано співвідношення, які характеризують варіацію поведінки досліджуваного автомата при варіації його початкового стану.

Ключові слова: *скінченні кільця, скінченні автомати, еквівалентні стани, параметрична ідентифікація.*

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

Получено 27.10.10