Компьютерная математика

УДК 519.713:512.55

В.В. СКОБЕЛЕВ

СЛОЖНОСТЬ ИДЕНТИФИКАЦИИ НЕЛИНЕЙНЫХ ОДНОМЕРНЫХ АВТОМАТОВ С ЛАГОМ 2 НАД КОНЕЧНЫМ КОЛЬЦОМ

Получено решение задачи анализа сложности идентификации (параметрической и начального состояния) для простейших нелинейных одномерных обратимых автоматов с лагом 2 над произвольным конечным коммутативно-ассоциативным кольцом с единицей.

Введение. Интерес к исследованию автоматов над конечными кольцами обусловлен следующими причинами. Во-первых, это устойчивая тенденция перехода криптографии от чисто комбинаторных моделей к математическим моделям, построенным на основе конечных алгебраических систем [1–3]. Во-вторых, многочисленные попытки применения хаотических динамических систем [4] к решению задач преобразования информации столкнулись с проблемой обеспечения корректной обратимости процессов при нелинейных преобразованиях в поле R (или в поле Q). Естественный способ избежать этой проблемы – это переход к вычислениям в конечной алгебраической системе. В-третьих, логическое развитие алгебраической теории автоматов, сформировало ее новый раздел – автоматы, представленные уравнениями над конечным кольцом, для которого математические основы криптологии – прикладная предметная область это [5–9].

В силу последнего обстоятельства актуальным является исследование обратимых автоматов над произвольным конечным коммутативно-ассоциативным кольцом с единицей [10] $(K,+,\cdot)$ (для краткости, будем говорить «кольцо K»). Любой такой автомат может рассматриваться как математическая модель симметричного поточного шифра, для которого параметры – это секретный

ключ средней длительности, а начальное состояние – секретный сеансовый ключ [9].

Поэтому особую значимость приобретает анализ сложности решения задач идентификации [11] такого автомата (параметрической и начального состояния). Такая сложность является теоретической аргументацией обоснования вычислительной стойкости соответствующего шифра.

Существенное отличие задач идентификации автомата над конечным кольцом от задач идентификации классических динамических систем [12] состоит в следующем. При идентификации автоматов над конечным кольцом не возникает проблемы, связанной с точностью идентификации из-за различного рода приближений (приближения, как таковые, отсутствуют вообще). Однако конечное кольцо является настолько «жесткой» структурой, что любая ошибка приводит к непредсказуемым последствиям.

В работах [7–9] рассмотрены, в основном, n-мерные автоматы с лагом 1 над кольцом Z_{p^k} (p простое число). Однако, не исследованы простейшие обратимые нелинейные одномерные автоматы с лагом 2, которые представляют интерес из-за высокой скорости преобразования информации. Этот пробел частично восполнен в [13].

Настоящая работа посвящена анализу сложности решения задач идентификации (параметрической и начального состояния) простейших обратимых нелинейных одномерных автоматов с лагом 2 над произвольным кольцом K.

Исследуемая модель. Система уравнений над кольцом K

$$\begin{cases} q_{t+2} = a + b \cdot q_{t+1}^2 + c \cdot q_t + d \cdot x_{t+1} \\ y_{t+1} = e \cdot q_{t+2} \end{cases} \quad (t \in Z_+), \qquad (1)$$

где $a,b,c,d,e \in K$ определяет класс автоматов Мура, для которых x_{t+1} и y_{t+1} – соответственно, входной и выходной символ в момент $t+1$, а $\vec{q}_t = (q_{t+1}, q_t)$ – состояние в момент t. Если зафиксировать параметры $a,b,c,d,e \in K$, то система уравнений (1) определяет конкретный автомат M, принадлежащий этому классу. При фиксации начального состояния $\vec{q}_0 = (q_1, q_0)$ инициальный автомат $(M, \vec{q}_0)$ осуществляет отображение входной полугруппы K^+ в себя.

Отметим, что уравнение $q_{t+2} = a + b \cdot q_{t+1}^2 + c \cdot q_t$ – аналог над кольцом K ряда модельных хаотических отображений, в том числе, отображения Эно [4].

Пусть S – множество всех таких автоматов M, определенных системой уравнений (1), что $a,c \in K$, $b \in K \setminus \{0\}$, а $d,e \in K_{inv}$, где K_{inv} – множество всех обратимых элементов кольца K. Тогда S – множество обратимых автоматов, причем автомат M^{-1}, обратный автомату $M \in S$, имеет вид

$$\begin{cases} q_{t+2} = e^{-1} \cdot x_{t+1} \\ y_{t+1} = d^{-1} \cdot (e^{-1} \cdot x_{t+1} - a - b \cdot q_{t+1}^2 - c \cdot q_t) \end{cases} \quad (t \in Z_+). \qquad (2)$$

С точки зрения алгебры инициальный автомат $(M,\vec{q}_0)$ $(M\in S,\vec{q}_0\in K^2)$ на каждом такте своего функционирования осуществляет сюръективное отображение множества K на себя, представляющее собой линейное преобразование $u=e\cdot v$ линейной комбинации $v=\alpha+\beta$ квадратичной формы $\alpha=b\cdot q_{t+1}^2+c\cdot q_t$ текущего состояния автомата M и аффинного преобразования $\beta=a+d\cdot x_{t+1}$ множества K.

Упорядоченная пара $((M,\vec{q}_0),(M^{-1},\vec{q}_0))$ $(M\in S,\vec{q}_0\in K^2)$ определяет симметричный поточный шифр: набор параметров $(a,b,c,d,e)\in$ $\in K\times(K\setminus\{0\})\times K\times K_{inv}^2$ – секретный ключ средней длительности, а $\vec{q}_0\in K^2$ – секретный сеансовый ключ. Отметим, что в процессе «шифрование-расшифрование» оба автомата M и M^{-1} движутся в пространстве состояний по одной и той же траектории в одном и том же направлении.

Для шифра $((M,\vec{q}_0),(M^{-1},\vec{q}_0))$ $(M\in S,\vec{q}_0\in K^2)$ число секретных ключей средней длительности равно $|K|^2\cdot|_{inv}|^2\cdot(|K|-1)$, а число секретных сеансовых ключей – $|K|^2$. Если число $|K|$ достаточно велико (например, $K=Z_{p^k}$, где p – простое число, для записи которого необходимо 100 бит), то вероятность угадывания секретного ключа чрезвычайно мала. Поэтому актуальны задачи анализа сложности идентификации (параметрической и начального состояния) автомата $M\in S$. С позиции криптографии эти задачи имеют различную значимость. Действительно, из (1) вытекает, что

$$y_{t+1}=e\cdot(a+b\cdot q_{t+1}^2+c\cdot q_t+d\cdot x_{t+1})\quad(t\in Z_+). \tag{3}$$

Подставив $t=0,1,\ldots,l$ $(l>2)$ в (3), с учетом 2-го уравнения системы (1), получаем

$$\begin{cases} y_1=e\cdot a+b\cdot e\cdot q_1^2+c\cdot e\cdot q_0+e\cdot d\cdot x_1\\ y_2=e\cdot a+b\cdot e^{-1}\cdot y_1^2+c\cdot e\cdot q_1+e\cdot d\cdot x_2\\ y_i=e\cdot a+b\cdot e^{-1}\cdot y_{i-1}^2+c\cdot y_{i-2}+e\cdot d\cdot x_i\quad(i=3,\ldots,l)\end{cases}. \tag{4}$$

Из последних $l-2$ уравнений системы (4) вытекает, что при известном наборе параметров $(a,b,c,d,e)\in K\times(K\setminus\{0\})\times K\times K_{inv}^2$ криптоаналитик, не располагая информацией о начальном состоянии автомата $M\in S$, может идентифицировать суффикс $x_3\ldots x_l$ входного слова, так как

$$x_i=(e\cdot d)^{-1}\cdot(e\cdot a+b\cdot e^{-1}\cdot y_{i-1}^2+c\cdot y_{i-2}-y_i)\quad(i=3,\ldots,l).$$

Поэтому, с позиции криптографии задача идентификации начального состояния автомата $M \in S$ актуальна, если префикс длины 2 входного слова содержит уникальную информацию, без которой суффикс $x_3 \dots x_l$ практически не дает возможность восстановить исходный текст.

Такая неравнозначность задач идентификации обусловлена исключительно тем, что функция выходов автомата $M \in S$ осуществляет линейное преобразование одной из компонент состояния. Эта неравнозначность исчезает при изменении модели, состоящем в переходе к автомату Мили с нелинейной функцией выходов (достаточно положить $y_{t+1} = e \cdot q_{t+2} \cdot q_{t+1} + d \cdot x_{t+1}$). Таким образом, множество автоматов S характеризует нижнюю границу сложности, с которой придется столкнуться криптоаналитику при решении задач идентификации нелинейных одномерных автоматов с лагом 2 над конечным кольцом.

Рассмотрим эти задачи в предположении (соответствующем одной из наиболее сильных атак криптоаналитика), что экспериментатор наблюдает вход и выход исследуемого автомата, управляет его входом, а также может осуществлять кратный эксперимент любой кратности.

Идентификация начального состояния. Охарактеризуем сложность идентификации начального состояния автомата $M \in S$ при условии, что экспериментатору известны параметры $(a,b,c,d,e) \in K \times (K \setminus \{0\}) \times K \times K_{inv}^2$.

Теорема 1. Для любого автомата $M \in S$:

1) если $c \in K_{inv}$, то идентификация начального состояния осуществляется посредством любого простого эксперимента длины 2;

2) если $c \notin K_{inv}$, то идентификация начального состояния с точностью до класса эквивалентных состояний осуществляется посредством кратного эксперимента кратности $|K|^2$ и высоты 2.

Доказательство. Пусть $c \in K_{inv}$. Из первых двух уравнений системы (4) получим, что для любого входного слова $x_1 x_2 \in K^2$:

$$\begin{cases} q_1 = c^{-1} \cdot (e^{-1} \cdot y_2 - a - b \cdot e^{-2} \cdot y_1^2 - d \cdot x_2) \\ q_0 = c^{-1} \cdot (e^{-1} \cdot y_1 - a - b \cdot q_1^2 - d \cdot x_1) \end{cases}.$$

Пусть $c \notin K_{inv}$. Рассмотрим первые два уравнения системы (4)

$$\begin{cases} y_1 = e \cdot a + b \cdot e \cdot q_1^2 + c \cdot e \cdot q_0 + e \cdot d \cdot x_1 \\ y_2 = e \cdot a + b \cdot e^{-1} \cdot y_1^2 + c \cdot e \cdot q_1 + e \cdot d \cdot x_2 \end{cases}. \qquad (5)$$

Пусть $U_{x_1x_2}$ – множество решений (q_1, q_0) системы (5) для фиксированного входного слова $x_1x_2 \in K^2$. Из последних $l-2$ уравнений системы (4) вытекает, что суффикс $y_3 \dots y_l$ выходного слова полностью определяется значением его префикса y_1y_2. Отсюда следует, что $\bigcap\limits_{x_1x_2 \in K^2} U_{x_1x_2}$ – класс состояний, эквивалентных начальному состоянию автомата $M \in S$.

Теорема доказана.

Из теоремы 1 вытекает, что задача идентификации начального состояния автомата $M \in S$ тривиальна, если $c \in K_{inv}$. Ситуация меняется, когда $c \notin K_{inv}$. В этом случае поиск решений (q_1, q_0) системы (5) – нетривиальная задача (даже если $K = Z_{p^k}$, то множества $U_{x_1x_2}$ имеют сложную структуру, представляются громоздкими формулами, а множество $\bigcap\limits_{x_1x_2 \in K^2} U_{x_1x_2}$ вообще трудно подлежит анализу [13]). Эта нетривиальность обусловлена внутренней сложностью исследуемой модели, и характеризуется необходимостью анализа принадлежности коэффициентов системы уравнений (5) различным классам ассоциированных элементов кольца K.

Параметрическая идентификация. Будем говорить, что для задачи параметрической идентификации автомата $M \in S$ алгоритм A вычисляет:

1) точное решение, если выходом алгоритма A является набор параметров $(a,b,c,d,e) \in K \times (K \setminus \{0\}) \times K \times K_{inv}^2$ исследуемого автомата M;

2) решение с точностью до имитационной модели, если выходом алгоритма A является набор значений комбинаций параметров исследуемого автомата M, на основе которых может быть построен алгоритм, моделирующий внешнее поведение автомата M (возможно, с учетом тех или иных ограничений).

Теорема 2. Никакой простой эксперимент с автоматом $M \in S$ не дает возможность вычислить точное решение для задачи его параметрической идентификации. Однако может существовать простой эксперимент с автоматом $M \in S$, который дает возможность для задачи его параметрической идентификации вычислить решение с точностью до имитационной модели, причем только параметр $c \in K$ будет вычислен точно.

Доказательство. Возможны следующие два случая.

Случай 1. Начальное состояние $\vec{q}_0 = (q_1, q_0)$ известно экспериментатору.

Пусть $\vec{q}_0 = (0,0)$. Тогда система уравнений (4) примет вид

$$\begin{cases} u_1 & + x_1 \cdot u_4 = y_1 \\ u_1 + y_1^2 \cdot u_2 & + x_2 \cdot u_4 = y_2 \\ u_1 + y_{i-1}^2 \cdot u_2 & + y_{i-2} \cdot u_3 + x_i \cdot u_4 = y_i \quad (i = 3, \dots, l) \end{cases}, \qquad (6)$$

где

$$(u_1,u_2,u_3,u_4)=(e\cdot a,b\cdot e^{-1},c,e\cdot d)\,. \qquad (7)$$

Матрица системы уравнений (6) имеет вид

$$A=\begin{pmatrix}1 & 0 & 0 & x_1\\ 1 & y_1^2 & 0 & x_2\\ 1 & y_2^2 & y_1 & x_3\\ \vdots & \vdots & \vdots & \vdots\\ 1 & y_{l-1}^2 & y_{l-2} & x_l\end{pmatrix}.$$

Если существует такое входное слово $x_1\ldots x_l\in K^l$ заранее неизвестной длины $l\ge 4$, что матрица A содержит обратимую матрицу 4-го порядка, то может быть вычислено единственное решение (u_1,u_2,u_3,u_4) системы уравнений (6).

Из равенства (7) вытекает, что тем самым будут вычислены величины $e\cdot a$, $b\cdot e^{-1}$, c и $e\cdot d$, т. е. только параметр c будет вычислен точно. При этом из (6) вытекает, что имитационная модель автомата $M\in S$ имеет вид

$$\begin{cases} y_1=u_1+x_1\cdot u_4\\ y_2=u_1+y_1^2\cdot u_2+x_2\cdot u_4\\ y_i=u_1+y_{i-1}^2\cdot u_2+y_{i-2}\cdot u_3+x_i\cdot u_4 \quad (i\ge 3)\end{cases},$$

где значения u_j $(j=1,\ldots,4)$ определены равенством (7).

Пусть $\vec{q}_0\ne(0,0)$. Тогда система уравнений (4) примет вид

$$\begin{cases} v_1+q_1^2\cdot v_2+q_0\cdot v_4+x_1\cdot v_6=y_1\\ v_1+y_1^2\cdot v_3+q_1\cdot v_4+x_2\cdot v_6=y_2\\ v_1+y_{i-1}^2\cdot v_3+y_{i-2}\cdot v_5+x_i\cdot v_6=y_i \quad (i=3,\ldots,l)\end{cases}, \qquad (8)$$

где

$$(v_1,v_2,v_3,v_4,v_5,v_6)=(e\cdot a,b\cdot e,b\cdot e^{-1},c\cdot e,c,e\cdot d)\,. \qquad (9)$$

Матрица системы уравнений (8) имеет вид

$$B=\begin{pmatrix} 1 & q_1^2 & 0 & q_0 & 0 & x_1 \\ 1 & 0 & y_1^2 & q_1 & 0 & x_2 \\ 1 & 0 & y_2^2 & 0 & y_1 & x_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & y_{l-1}^2 & 0 & y_{l-2} & x_l \end{pmatrix}.$$

Если существует такое входное слово $x_1 \ldots x_l \in K^l$ заранее неизвестной длины $l \geq 6$, что матрица B содержит обратимую матрицу 6-го порядка, то может быть вычислено единственное решение $(v_1, v_2, \ldots, v_6)$ системы уравнений (8).

Из равенства (9) вытекает, что тем самым будут вычислены величины $e \cdot a$, $b \cdot e$, $b \cdot e^{-1}$, $c \cdot e$, c и $e \cdot d$, т. е. только параметр c будет вычислен точно. При этом из (8) вытекает, что имитационная модель автомата $M \in S$ имеет вид

$$\begin{cases} y_1 = v_1 + q_1^2 \cdot v_2 + q_0 \cdot v_4 + x_1 \cdot v_6 \\ y_2 = v_1 + y_1^2 \cdot v_3 + q_1 \cdot v_4 + x_2 \cdot v_6 \\ y_i = v_1 + y_{i-1}^2 \cdot v_3 + y_{i-2} \cdot v_5 + x_i \cdot v_6 \quad (i \geq 3) \end{cases},$$

где значения v_j $(j = 1, \ldots, 6)$ определены равенством (9).

Случай 2. Начальное состояние $\vec{q}_0 = (q_1, q_0)$ не известно экспериментатору.

Учитывая, что ситуации различаются при $\vec{q}_0 = (0,0)$ и $\vec{q}_0 \neq (0,0)$, отбросим в системе (8) первые 2 уравнения. Получим систему уравнений

$$w_1 + y_{i-1}^2 \cdot w_2 + y_{i-2} \cdot w_3 + x_i \cdot w_4 = y_i \quad (i = 3, \ldots, l), \tag{10}$$

где

$$(w_1, w_2, w_3, w_4) = (e \cdot a, b \cdot e^{-1}, c, e \cdot d). \tag{11}$$

Матрица системы уравнений (10) имеет вид

$$C=\begin{pmatrix} 1 & y_2^2 & y_1 & x_3 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & y_{l-1}^2 & y_{l-2} & x_l \end{pmatrix}.$$

Если существует такое входное слово $x_1 \ldots x_l \in K^l$ заранее неизвестной длины $l \geq 6$, что матрица C содержит обратимую матрицу 4-го порядка, то может быть вычислено единственное решение (w_1, w_2, w_3, w_4) системы уравнений (10).

Из равенства (11) вытекает, что тем самым будут вычислены величины $e \cdot a$, $b \cdot e^{-1}$, c и $e \cdot d$, т. е. только параметр c будет вычислен точно. При этом из (10) вытекает, что имитационная модель, моделирующая поведение автомата $M \in S$ на суффиксах входных слов, полученных отбрасыванием префикса длины 2, имеет вид

$$y_i = w_1 + y_{i-1}^2 \cdot w_2 + y_{i-2} \cdot w_3 + x_i \cdot w_4 \ (i = 3,\ldots,l),$$

где значения w_j $(j = 1,\ldots,4)$ определены равенством (11).

Теорема доказана.

Следствие. Никакой кратный эксперимент с автоматом $M \in S$ не дает возможность вычислить точное решение для задачи его параметрической идентификации. Однако может существовать кратный эксперимент с автоматом $M \in S$, который дает возможность для задачи его параметрической идентификации вычислить решение с точностью до имитационной модели, причем только параметр $c \in K$ будет вычислен точно.

Доказательство. В процессе кратного эксперимента с автоматом $M \in S$ будет построено несколько систем уравнений (6), (8) или (10) (число этих систем уравнений равно кратности эксперимента). Однако решение этих систем определяет точно такие же комбинации параметров, как и в случае простого эксперимента с автоматом $M \in S$.

Следствие доказано.

Полученные результаты показывают, что при решении задачи параметрической идентификации автомата $M \in S$ экспериментатор вынужден осуществлять поиск входного слова длины не меньшей, чем $|K|^4$. Отсюда вытекает, что сложность решения этой задачи достаточно высокая (достаточно положить $K = Z_{p^k}$, где p – простое число, для записи которого необходимо 100 бит). Однако, возможность построения в результате эксперимента с автоматом $M \in S$ достаточно простых имитационных моделей (выше было отмечено, что это обусловлено именно тем, что функция выходов автомата M осуществляет линейное преобразование одной из компонент состояния) является достаточно серьезной аргументацией против выбора класса S в качестве кандидата на симметричный поточный шифр.

Заключение. В работе показано, что даже для простейших обратимых нелинейных одномерных автоматов с лагом 2 над произвольным кольцом K решение задач идентификации (параметрической и начального состояния (в случае, когда $c \notin K_{inv}$)) имеет достаточно высокую сложность. Для задачи идентификации начального состояния эта сложность обусловлена необходимостью решения (в случае, когда $c \notin K_{inv}$) систем нелинейных уравнений над конечным кольцом, а для задачи параметрической идентификации – поиском в достаточно объемном множестве входного слова, обладающего заданными условиями (выражаемыми в терминах ранга матрицы).

Показано, что в результате эксперимента с автоматом $M \in S$ возможно построение достаточно простых имитационных моделей. Поэтому актуальной является задача выделения, описания и характеристики классов обратимых автоматов, отличающихся от класса S только функциями выходов, для которых любая имитационная модель, построенная в результате эксперимента с автоматом существенно сложнее, чем система уравнений, определяющая автомат. Решение этой задачи – основное направление дальнейших исследований.

В.В. Скобелєв

СКЛАДНІСТЬ ІДЕНТИФІКАЦІЇ НЕЛІНІЙНИХ ОДНОВИМІРНИХ АВТОМАТІВ З ЛАГОМ 2 НАД СКІНЧЕННИМ КІЛЬЦЕМ

Отримано вирішення задачі аналізу складності ідентифікації (параметричної та початкового стану) для найпростіших нелінійних одновимірних автоматів з лагом 2, що допускають обернення, над будь-яким скінченним комутативно-асоціативним кільцем з одиницею.

V.V. Skobelev

COMPLEXITY OF IDENTIFICATION OF NON-LINEAR ONE-DIMENSIONAL AUTOMATA WITH DELAY 2 OVER arbitrary FINITE RING

A solution to a problem of analysis of complexity of identification (parametric one as well as of initial state) for simplest non-linear one-dimensional reversible automata with delay 2 over arbitrary finite commutative-associative ring with a unit is obtained.

1. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. – М.: Гелиос АРВ, 2002. – 480 с.
2. *Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В.* Математические и компьютерные основы криптологии. − Минск: Новое знание, 2003. − 382 с.
3. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. − М.: ТРИУМФ, 2003. − 816 с.
4. *Кузнецов С.П.* Динамический хаос. – М.: Физматлит, 2001. – 296 с.
5. *Кузьмин А.С., Куракин В.Л., Нечаев А.А.* Псевдослучайные и полилинейные последовательности. – Труды по дискретной математике. Т.1. – М.: Научное изд-во «ТВП», 1997. – С. 139–202.
6. *Кузьмин А.С., Куракин В.Л., Нечаев А.А.* Свойства линейных и полилинейных рекуррент над кольцами Галуа (I). – Труды по дискретной математике. Т. 2. – М.: Научное изд-во «ТВП», 1998. – С. 191–222.
7. *Скобелев В.Г.* Нелинейные автоматы над конечным кольцом // Кибернетика и системный анализ. – 2006. – № 6. – С. 29–42.
8. *Скобелев В.В.* Анализ структуры класса линейных автоматов над кольцом Z_{p^k} // Кибернетика и системный анализ. – 2008. – № 3 – С. 60–74.
9. *Скобелев В.В., Скобелев В.Г.* Анализ шифрсистем. – Донецк: ИПММ НАН Украины, 2009. – 479 с.
10. *Курош А.Г.* Лекции по общей алгебре. – М.: Наука, 1973. – 400 с.
11. *Калман Р., Фалб П., Арбиб М.* Очерки по математической теории систем. – М.: Мир, 1971. – 400 с.
12. *Льюнг Л.* Идентификация систем. Теория для пользователя. − М.: Наука, 1991. − 432 с.
13. *Скобелев В.В., Скобелев В.Г.* Анализ нелинейных автоматов с лагом 2 над конечным кольцом // Прикладная дискретная математика. – 2010. – № 1 (7). – С. 68–85.

Получено 19.05.2010

Об авторе:

Скобелев Владимир Владимирович,
кандидат физико-математических наук, младший научный сотрудник
отдела теории управляющих систем Института прикладной математики и механики
НАН Украины.
e-mail: skobelev_vv@iamm.ac.donetsk.ua