УДК 512.55+519.17

В. В. Скобелев

Анализ задачи распознавания автомата над кольцом

(Представлено академиком НАН Украины А. А. Летичевским)

Разработан метод приближенного решения задачи идентификации семейств автоматов, представленных системами уравнений с параметрами над конечным ассоциативно-коммутативным кольцом с единицей. Предложенный метод основан на построении имитационной модели для исследуемого семейства автоматов. Выделены имитационные модели, моделирующие поведение автоматов исследуемого семейства автоматов с заданной точностью в "наихудшем случае" и "в среднем".

1. Актуальность задачи распознавания автоматных моделей обусловлена их многочисленными применениями при решении задач преобразования информации. Высокая сложность этой задачи стимулировала исследования приближенных методов ее решения, анализ которых содержится в [1]. Многочисленные попытки применения автоматно-алгебраических моделей при анализе современных шифров [2] выделяют в качестве новой актуальной задачи распознавание конечного автомата, представленного системой уравнений с параметрами над конечным ассоциативно-коммутативным кольцом $\mathcal{K} = (K, +, \cdot)$ с единицей. Анализ этой задачи дает возможность установить глубокие внутренние связи между современной алгеброй, теорией систем, теорией автоматов и криптологией.

2. Зафиксируем числа l, n_1, n_2, $n_3 \in \mathbb{N}$, множество $\mathbf{A} \subseteq K^l$ ($|\mathbf{A}| \geqslant 1$) и отображения $\mathbf{f}_1 \colon K^{n_1+n_2+l} \to K^{n_1}$ и $\mathbf{f}_2 \colon K^{n_1+n_2+l} \to K^{n_3}$. Система уравнений

$$\begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}), \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \end{cases} \qquad (t \in \mathbb{Z}_+) \tag{1}$$

определяет над кольцом $\mathcal{K}$ такое семейство конечных автоматов $\mathcal{M} = \{M_{\mathbf{a}}\}_{\mathbf{a}\in\mathbf{A}}$, что для каждого значения параметров $\mathbf{a} \in \mathbf{A}$ элементы $\mathbf{q}_t \in K^{n_1}$, $\mathbf{x}_t \in K^{n_2}$ и $\mathbf{y}_t \in K^{n_3}$ являются, соответственно, состоянием, входным символом и выходным символом автомата $M_{\mathbf{a}}$ в момент t.

Обозначим через $F_{\mathbf{a},\mathbf{q}_0}$ ($\mathbf{a} \in \mathbf{A}, \mathbf{q}_0 \in \mathbf{K}^{n_1}$) отображение множества входных слов $(K^{n_2})^+$ в множество выходных слов $(K^{n_3})^+$, реализуемое инициальным автоматом $(M_{\mathbf{a}}, \mathbf{q}_0)$. Ясно, что каждому автомату $M_{\mathbf{a}}$ ($\mathbf{a} \in \mathbf{A}$) может быть поставлено в соответствие семейство автоматных отображений $\mathcal{F}_{\mathbf{a}} = \{F_{\mathbf{a},\mathbf{q}_0}\}_{\mathbf{q}_0\in\mathbf{K}^{n_1}}$.

Расстоянием (по Хеммингу) между словами $v = u_1^{(1)} \dots u_m^{(1)}$ и $w = u_1^{(2)} \dots u_m^{(2)}$ в алфавите U, где $u_j^{(i)} \in U$ ($i = 1, 2$; $j = 1, \dots, m$), назовем количество $\varrho(v, w)$ таких позиций i ($1 \leqslant i \leqslant m$), что $u_i^{(1)} \neq u_i^{(2)}$.

Рассмотрим следующую задачу распознавания автомата над кольцом $\mathcal{K}$.

Дан автомат M, о котором известно только то, что $M \in \mathcal{M}$. Требуется на основе (возможно, кратного) эксперимента с автоматом M построить его следствие, т. е. автоматно-алгебраическую модель, которая с заданной точностью моделирует поведение автомата M на множестве входных слов $(K^{n_2})^+$.

Таким образом, предметом настоящего исследования является построение имитационной модели для семейства автоматов (1), т. е. алгоритма, основанного на использовании некоторого семейства автоматов над кольцом $\mathcal{K}$, более простого, чем семейство $\mathcal{M}$, осуществляющего моделирование поведения любого автомата $M_{\mathbf{a}} \in \mathcal{M}$ с заданной точностью.

3. Построим имитационную модель семейства автоматов $\mathcal{M}$ следующим образом.

Зафиксируем числа r, $l_1 \in \mathbb{N}$, непустое множество $\mathbf{B} \subseteq K^{l_1}$ ($|\mathbf{B}| \leqslant |\mathbf{A}|$) и три семейства отображений

$$\{\varphi_{\mathbf{b}}^{(1)} \colon K^{n_1} \times K^{n_2} \to K^{n_3}\}_{\mathbf{b}\in\mathbf{B}},$$

$$\left\{\varphi_{\mathbf{b}}^{(2)} \colon K^{n_1} \times \left(\bigcup_{j=1}^{r-1} K^{n_3}\right)^j \times K^{n_2} \to K^{n_3}\right\}_{\mathbf{b}\in\mathbf{B}},$$

$$\{\varphi_{\mathbf{b}}^{(3)} \colon K^{n_1} \times (K^{n_3})^r \times K^{n_2} \to K^{n_3}\}_{\mathbf{b}\in\mathbf{B}}.$$

Рассмотрим семейство таких отображений

$$\mathcal{G}_{\mathbf{B}} = \{G_{\mathbf{b}} \colon K^{n_1} \times (K^{n_2})^+ \to (K^{n_3})^+\}_{\mathbf{b}\in\mathbf{B}},$$

что $G_{\mathbf{b}}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_m) = \mathbf{y}_1 \dots \mathbf{y}_m$ ($\mathbf{b} \in \mathbf{B}, m \in \mathbb{N}$), где

$$\mathbf{y}_i = \begin{cases} \varphi_{\mathbf{b}}^{(1)}(\mathbf{q}_0, \mathbf{x}_1), & \text{если} \quad i = 1, \\ \varphi_{\mathbf{b}}^{(2)}(\mathbf{q}_0, \mathbf{y}_1 \dots \mathbf{y}_{i-1}, \mathbf{x}_i), & \text{если} \quad i = 2, \dots, r, \\ \varphi_{\mathbf{b}}^{(3)}(\mathbf{q}_0, \mathbf{y}_{i-r} \dots \mathbf{y}_{i-1}, \mathbf{x}_i), & \text{если} \quad r < i \leqslant m, \end{cases} \tag{2}$$

для любых $\mathbf{q}_0 \in K^{n_1}$ и $\mathbf{x}_1 \dots \mathbf{x}_m \in (K^{n_2})^+$.

Определим отображения $H_{\mathbf{b},\mathbf{q}_0} \colon (K^{n_2})^+ \to (K^{n_3})^+$ ($\mathbf{b} \in \mathbf{B}, \mathbf{q}_0 \in K^{n_1}$) следующим образом: $H_{\mathbf{b},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_m) = G_{\mathbf{b}}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_m)$ для любых $\mathbf{x}_1 \dots \mathbf{x}_m \in (K^{n_2})^+$ ($m \in \mathbb{N}$).

Из (2) вытекает, что $H_{\mathbf{b},\mathbf{q}_0}$ ($\mathbf{b} \in \mathbf{B}, \mathbf{q}_0 \in K^{n_1}$) — автоматные отображения, причем каждое семейство автоматных отображений $\mathcal{H}_{\mathbf{b}} = \{H_{\mathbf{b},\mathbf{q}_0}\}_{\mathbf{q}_0\in K^{n_1}}$ ($\mathbf{b} \in \mathbf{B}$) определяет конечный автомат над кольцом $\mathcal{K}$.

Зафиксировав сюръекцию $h \colon \mathbf{A} \to \mathbf{B}$, мы можем каждому автомату $M_{\mathbf{a}} \in \mathcal{M}$ поставить в соответствие автомат, определяемый семейством автоматных отображений $\mathcal{H}_{h(\mathbf{a})}$.

Таким образом, упорядоченная пара $(\mathcal{G}_{\mathbf{B}}, h)$ может быть выбрана в качестве имитационной модели семейства автоматов $\mathcal{M}$, если выполнены следующие три условия:

1) построение семейства отображений $\mathcal{G}_{\mathbf{B}}$ и сюръекции h осуществляется только на основе анализа системы уравнений (1) без дополнительных ограничений на значения параметра $\mathbf{a} \in \mathbf{A}$;

2) для каждого фиксированного значения параметра $\mathbf{a} \in \mathbf{A}$ сложность вычислений в соответствии с семейством отображений $\mathcal{F}_{\mathbf{a}}$ не меньше, чем сложность вычислений в соответствии с семейством отображений $\mathcal{H}_{h(\mathbf{a})}$;

3) для каждого фиксированного значения параметра $\mathbf{a} \in \mathbf{A}$ автомат, определяемый семейством автоматных отображений $\mathcal{H}_{h(\mathbf{a})}$, моделирует поведение автомата $M_{\mathbf{a}} \in \mathcal{M}$ с заданной точностью.

Ясно, что те или иные ограничения на структуру отображений $\varphi_{\mathbf{b}}^{(1)}$, $\varphi_{\mathbf{b}}^{(2)}$, $\varphi_{\mathbf{b}}^{(3)}$ ($\mathbf{b} \in \mathbf{B}$) накладывают соответствующие ограничения на каждое семейство автоматных отображений $\mathcal{H}_{\mathbf{b}}$ и, следовательно, на структуру автомата, определяемого этим семейством.

Естественно потребовать, чтобы для имитационной модели $(\mathcal{G}_{\mathbf{B}}, h)$ отображения $\varphi^{(1)}_{h(\mathbf{a})}$ и $\varphi^{(2)}_{h(\mathbf{a})}$ были выбраны так, чтобы истинными были равенства

$$H_{h(\mathbf{a}),\mathbf{q}_0}\big|_{\bigcup\limits_{i=1}^{r} K^{n_2}} = F_{\mathbf{a},\mathbf{q}_0}\big|_{\bigcup\limits_{i=1}^{r} K^{n_2}} \qquad (\mathbf{a} \in \mathbf{A}, \mathbf{q}_0 \in K^{n_1}). \tag{3}$$

Содержательный смысл равенств (3) состоит в следующем: имитационная модель $(\mathcal{G}_{\mathbf{B}}, h)$, подсоединенная к входу и выходу исследуемого автомата $M_{\mathbf{a}}$ $(\mathbf{a} \in \mathbf{A})$, пропускает первые r выходных символов, после чего блокирует выход автомата $M_{\mathbf{a}}$ и начинает моделировать его поведение на оставшейся части входного слова. Всюду в дальнейшем считаем, что это условие выполнено.

Среди ограничений на структуру отображений $\varphi^{(3)}_{\mathbf{b}}$ $(\mathbf{b} \in \mathbf{B})$ с прикладной точки зрения представляет интерес следующее ограничение: для каждого отображения $\varphi^{(3)}_{\mathbf{b}}$ $(\mathbf{b} \in \mathbf{B})$ переменная $\mathbf{q}_0$ является фиктивной. Это ограничение означает, что имитационная модель $(\mathcal{G}_{\mathbf{B}}, h)$ осуществляет моделирование поведения каждого автомата $M_{\mathbf{a}}$ $(\mathbf{a} \in \mathbf{A})$ посредством использования автоматов с конечной памятью.

4. Определим точность имитационной модели $(\mathcal{G}_{\mathbf{B}}, h)$, используя стандартный подход прикладной теории алгоритмов [3, 4].

Пусть $F_{\mathbf{a},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_m) = \mathbf{y}_1 \dots \mathbf{y}_m$ и $H_{h(\mathbf{a}),\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_m) = \widetilde{\mathbf{y}}_1 \dots \widetilde{\mathbf{y}}_m$, где $\mathbf{q}_0 \in K^{n_1}$, $\mathbf{a} \in \mathbf{A}$ и $\mathbf{x}_1 \dots \mathbf{x}_m \in (K^{n_2})^m$ $(m \in \mathbb{N})$.

Число

$$\alpha_{\mathbf{a},\mathbf{q}_0,m} = \sum_{\mathbf{x}_1 \dots \mathbf{x}_m \in (K^{n_2})^m} (m - \varrho(\mathbf{y}_1 \dots \mathbf{y}_m, \widetilde{\mathbf{y}}_1 \dots \widetilde{\mathbf{y}}_m)) \qquad (\mathbf{a} \in \mathbf{A},\ \mathbf{q}_0 \in K^{n_1},\ m \in \mathbb{N})$$

является средним количеством позиций в выходных словах, в которых отображения $F_{\mathbf{a},\mathbf{q}_0}$ и $H_{h(\mathbf{a}),\mathbf{q}_0}$ совпадают на множестве входных слов длины m. Отсюда вытекает, что число

$$\beta_{\mathbf{a},\mathbf{q}_0,m} = m^{-1}\alpha_{\mathbf{a},\mathbf{q}_0,m} \qquad (\mathbf{a} \in \mathbf{A},\ \mathbf{q}_0 \in K^{n_1},\ m \in \mathbb{N})$$

является средним количеством позиций в выходных словах, приходящимся на одну букву входного слова, в которых отображения $F_{\mathbf{a},\mathbf{q}_0}$ и $H_{h(\mathbf{a}),\mathbf{q}_0}$ совпадают на множестве входных слов длины m. Следовательно, число

$$\gamma_{\mathbf{a},\mathbf{q}_0,m} = \frac{|K^{n_2}| - 1}{|K^{n_2}|^{m+1} - |K^{n_2}|} \sum_{i=1}^{m} |K^{n_2}|^i \beta_{\mathbf{a},\mathbf{q}_0,m} \qquad (\mathbf{a} \in \mathbf{A},\ \mathbf{q}_0 \in K^{n_1},\ m \in \mathbb{N})$$

является средним количеством позиций в выходных словах, приходящимся на одну букву входного слова, в которых отображения $F_{\mathbf{a},\mathbf{q}_0}$ и $H_{h(\mathbf{a}),\mathbf{q}_0}$ совпадают на множестве всех входных слов длины, не превосходящей число m.

Числа

$$\underline{\gamma}_{\mathbf{a},\mathbf{q}_0} = \underline{\lim}\gamma_{\mathbf{a},\mathbf{q}_0,m} = \lim_{m\to\infty} \inf\{\gamma_{\mathbf{a},\mathbf{q}_0,i} \mid i \in \mathbb{N}_m\} \qquad (\mathbf{a} \in \mathbf{A}, \mathbf{q}_0 \in K^{n_1})$$

и

$$\overline{\gamma}_{\mathbf{a},\mathbf{q}_0} = \overline{\lim}\gamma_{\mathbf{a},\mathbf{q}_0,m} = \lim_{m\to\infty} \sup\{\gamma_{\mathbf{a},\mathbf{q}_0,i} \mid i \in \mathbb{N}_m\} \qquad (\mathbf{a} \in \mathbf{A}, \mathbf{q}_0 \in K^{n_1})$$

определяют, соответственно, нижнюю и верхнюю границу для среднего количества позиций в выходных словах, приходящегося на одну букву входного слова, в которых отображения $F_{\mathbf{a},\mathbf{q}_0}$ и $H_{h(\mathbf{a}),\mathbf{q}_0}$ совпадают на своей области определения $(K^{n_2})^+$.

Следовательно, для каждого $\mathbf{a} \in \mathbf{A}$:

1) числа $\underline{\eta}_{\mathbf{a}} = \min\limits_{\mathbf{q}_0 \in K^{n_1}} \underline{\gamma}_{\mathbf{a},\mathbf{q}_0}$ и $\overline{\eta}_{\mathbf{a}} = \max\limits_{\mathbf{q}_0 \in K^{n_1}} \overline{\gamma}_{\mathbf{a},\mathbf{q}_0}$ определяют, соответственно, нижнюю и верхнюю границу для среднего количества позиций в выходных словах, приходящегося на одну букву входного слова, в которых отображения, принадлежащие семейству отображений $\mathcal{F}_{\mathbf{a}}$, реализуемых автоматом $M_{\mathbf{a}} \in \mathcal{M}$, совпадают с соответствующими отображениями, принадлежащими семейству отображений $\mathcal{H}_{h(\mathbf{a})}$;

2) если $\underline{\gamma}_{\mathbf{a},\mathbf{q}_0} = \overline{\gamma}_{\mathbf{a},\mathbf{q}_0} = \gamma_{\mathbf{a},\mathbf{q}_0}$ для всех $\mathbf{q}_0 \in K^{n_1}$, то:

а) число $\eta_{\mathbf{a}} = \min\limits_{\mathbf{q}_0 \in K^{n_1}} \gamma_{\mathbf{a},\mathbf{q}_0}$ определяет в наихудшем случае среднее количество позиций в выходных словах, приходящееся на одну букву входного слова, в которых отображения, принадлежащие семейству отображений $\mathcal{F}_{\mathbf{a}}$, реализуемых автоматом $M_{\mathbf{a}} \in \mathcal{M}$, совпадают с соответствующими отображениями, принадлежащими семейству отображений $\mathcal{H}_{h(\mathbf{a})}$;

б) число $\zeta_{\mathbf{a}} = |K^{n_1}|^{-1} \sum\limits_{\mathbf{q}_0 \in K^{n_1}} \gamma_{\mathbf{a},\mathbf{q}_0}$ определяет в среднем количество позиций в выходных словах, приходящееся на одну букву входного слова, в которых отображения, принадлежащие семейству отображений $\mathcal{F}_{\mathbf{a}}$, реализуемых автоматом $M_{\mathbf{a}} \in \mathcal{M}$, совпадают с соответствующими отображениями, принадлежащими семейству отображений $\mathcal{H}_{h(\mathbf{a})}$.

Таким образом,

1) числа $\underline{\eta} = \min\limits_{\mathbf{a} \in \mathbf{A}} \underline{\eta}_{\mathbf{a}}$ и $\overline{\eta} = \max\limits_{\mathbf{a} \in \mathbf{A}} \underline{\eta}_{\mathbf{a}}$ определяют, соответственно, нижнюю и верхнюю границу для среднего количества позиций в выходных словах, приходящегося на одну букву входного слова, в которых автоматные отображения, реализуемые семейством автоматов $\mathcal{M}$, совпадают с автоматными отображениями, реализуемыми имитационной моделью $(\mathcal{G}_{\mathbf{B}}, h)$;

2) если $\underline{\gamma}_{\mathbf{a},\mathbf{q}_0} = \overline{\gamma}_{\mathbf{a},\mathbf{q}_0} = \gamma_{\mathbf{a},\mathbf{q}_0}$ для всех $\mathbf{q}_0 \in K^{n_1}$ и $\mathbf{a} \in \mathbf{A}$, то

а) число $\nu_1 = \min\limits_{\mathbf{a} \in \mathbf{A}} \eta_{\mathbf{a}}$ определяет в наихудшем случае среднее количество позиций в выходных словах, приходящееся на одну букву входного слова, в которых автоматные отображения, реализуемые семейством автоматов $\mathcal{M}$, совпадают с автоматными отображениями, реализуемыми имитационной моделью $(\mathcal{G}_{\mathbf{B}}, h)$;

б) число $\nu_2 = |\mathbf{A}|^{-1} \sum\limits_{\mathbf{a} \in \mathbf{A}} \eta_{\mathbf{a}}$ определяет среднее для наихудших случаев от средних количеств позиций в выходных словах, приходящихся на одну букву входного слова, в которых автоматные отображения, реализуемые семейством автоматов $\mathcal{M}$, совпадают с автоматными отображениями, реализуемыми имитационной моделью $(\mathcal{G}_{\mathbf{B}}, h)$;

в) число $\nu_3 = \min\limits_{\mathbf{a} \in \mathbf{A}} \zeta_{\mathbf{a}}$ определяет наихудший случай для средних от средних количеств позиций в выходных словах, приходящееся на одну букву входного слова, в которых автоматные отображения, реализуемые семейством автоматов $\mathcal{M}$, совпадают с автоматными отображениями, реализуемыми имитационной моделью $(\mathcal{G}_{\mathbf{B}}, h)$;

г) число $\nu_4 = |\mathbf{A}|^{-1} \sum\limits_{\mathbf{a} \in \mathbf{A}} \zeta_{\mathbf{a}}$ определяет среднее от средних количеств позиций в выходных словах, приходящееся на одну букву входного слова, в которых автоматные отображения, реализуемые семейством автоматов $\mathcal{M}$, совпадают с автоматными отображениями, реализуемыми имитационной моделью $(\mathcal{G}_{\mathbf{B}}, h)$.

Рассмотренные случаи охватывают все представляющие интерес комбинации понятий "в наихудшем случае" и "в среднем" и дают возможность охарактеризовать имитационную модель $(\mathcal{G}_{\mathbf{B}}, h)$ как $[\underline{\eta}, \overline{\eta}]$-точную или, в случае, когда $\underline{\gamma}_{\mathbf{a},\mathbf{q}_0} = \overline{\gamma}_{\mathbf{a},\mathbf{q}_0}$ для всех $\mathbf{q}_0 \in K^{n_1}$ и $\mathbf{a} \in \mathbf{A}$, как ν-точную, где ν — любое из чисел ν_1, ν_2, ν_3 или ν_4. Естественно определить имитационную модель $(\mathcal{G}_{\mathbf{B}}, h)$ как асимптотически точную, если $\nu = 1$.

5. Проиллюстрируем построение имитационной модели $(\mathcal{G}_{\mathbf{B}}, h)$ на примере семейства автоматов $\mathcal{M}$ с лагом 2, определенного над кольцом $\mathcal{K}$ системой уравнений

$$\begin{cases} q_{t+2} = a_1 + a_2 q_{t+1}^2 + a_3 q_t + a_4 x_{t+1}, \\ y_{t+1} = a_5 q_{t+2}, \end{cases} \qquad (t \in \mathbb{Z}_+), \tag{4}$$

где множество параметров имеет вид

$$\mathbf{A} = \{(a_1, a_2, a_3, a_4, a_5) \mid a_1, a_2, a_3 \in K \setminus \{0\}; a_4, a_5 \in K^{inv}\}.$$

При каждом фиксированном $\mathbf{a} \in \mathbf{A}$ для автомата $M_{\mathbf{a}} \in \mathcal{M}$ вектор $\mathbf{q}_t = (q_{t+1}, q_t)$ — состояние в момент t, а x_{t+1} и y_{t+1} — соответственно, входной и выходной символы в момент $t+1$. Таким образом, для рассматриваемого примера $l = 5$, $n_1 = 2$, а $n_2 = n_3 = 1$.

Отметим, что уравнение

$$q_{t+2} = a_1 + a_2 q_{t+1}^2 + a_3 q_t + a_4$$

определяет над кольцом $\mathcal{K}$ аналоги ряда модельных хаотических динамических систем [5], в том числе отображения Эно.

Подставив значение q_{t+2}, определенное 1-м уравнением системы (4), во 2-е уравнение этой системы, получим

$$y_{t+1} = a_1 a_5 + a_2 a_5 q_{t+1}^2 + a_3 a_5 q_t + a_4 a_5 x_{t+1}. \tag{5}$$

Подставив $t = 0, 1, \ldots$ в (5), учитывая 2-е уравнение системы (4) и то обстоятельство, что $a_4 \in K^{inv}$, получим, что для каждого автомата $M_{\mathbf{a}} \in \mathcal{M}$ система уравнений (4) эквивалентна системе уравнений

$$\begin{cases} y_1 = a_1 a_5 + a_2 a_5 q_1^2 + a_3 a_5 q_0 + a_4 a_5 x_1, \\ y_2 = a_1 a_5 + a_2 a_5^{-1} y_1^2 + a_3 a_5 q_1 + a_4 a_5 x_2, \qquad (t \geqslant 2), \\ y_{t+1} = a_1 a_5 + a_2 a_5^{-1} y_{t+1}^2 + a_3 y_t + a_4 a_5 x_{t+1}, \end{cases} \tag{6}$$

Из (6) вытекает, что для семейства автоматов $\mathcal{M}$, представленного над кольцом $\mathcal{K}$ системой уравнений (4), система уравнений

$$\begin{cases} y_1 = b_1 + b_2 q_1^2 + b_3 q_0 + b_4 x_1, \\ y_2 = b_1 + b_5 y_1^2 + b_3 q_1 + b_4 x_2, \qquad (t \geqslant 2), \\ y_{t+1} = b_1 + b_5 y_{t+1}^2 + b_6 y_t + b_4 x_{t+1}, \end{cases} \tag{7}$$

где

$$b_1 = a_1 a_5, \qquad b_2 = a_2 a_5, \qquad b_3 = a_3 a_5, \qquad b_4 = a_4 a_5, \qquad b_5 = a_2 a_5^{-1}, \qquad b_6 = a_3, \tag{8}$$

определяет для каждого $\nu \in \{\nu_1, \nu_2, \nu_3, \nu_4\}$ асимптотически точную имитационную модель $(\mathcal{G}_{\mathbf{B}}, h)$ ($\mathbf{B} \subset K^6$). Таким образом, $l_1 = 6$, $r = 2$, а отображение $h\colon \mathbf{A} \to \mathbf{B}$, определенное равенствами (8), является биекцией (т. е. условие $|\mathbf{B}| \leqslant |\mathbf{A}|$ выполнено).

Для каждого $\mathbf{a} \in \mathbf{A}$ значение $h(\mathbf{a}) = (b_1, \ldots, b_6)$ вычисляется следующим образом. Осуществляется поиск входного слова $x_1 \ldots x_m \in K^m$ ($m \geqslant 6$) заранее неизвестной длины, которое дает возможность сформировать в результате эксперимента с автоматом $M_{\mathbf{a}} \in \mathcal{M}$ систему линейных уравнений

$$\begin{cases} b_1 + b_2 q_1^2 + b_3 q_0 + b_4 x_1 = y_1, \\ b_1 + b_5 y_1^2 + b_3 q_1 + b_4 x_2 = y_2, \\ b_1 + b_5 y_2^2 + b_6 y_1 + b_4 x_3 = y_3, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_1 + b_5 y_{m-1}^2 + b_6 y_{m-2} + b_4 x_m = y_m \end{cases}$$

относительно неизвестных $b_1, \ldots, b_6$, ранг матрицы которой равен 6. Решив эту систему, найдем значения $b_1, \ldots, b_6$.

Так как $a_4 \in K^{inv}$, то из (4) вытекает, что $\mathcal{M}$ — семейство обратимых автоматов, причем для каждого автомата $M_{\mathbf{a}} \in \mathcal{M}$ обратный автомат $M_{\mathbf{a}}^{-1}$ имеет следующий вид:

$$\begin{cases} q_{t+2} = a_5^{-1} y_{t+1}, \\ x_{t+1} = -a_1 a_4^{-1} - a_2 a_4^{-1} q_{t+1}^2 - a_3 a_4^{-1} q_t + a_4^{-1} a_5^{-1} y_{t+1} \end{cases} \qquad (t \in \mathbb{Z}_+).$$

Из (7) вытекает, что для семейства автоматов $\mathcal{M}^{-1} = \{M^{-1}\}_{\mathbf{a} \in \mathbf{A}}$ асимптотически точная для каждого $\nu \in \{\nu_1, \nu_2, \nu_3, \nu_4\}$ имитационная модель $(\mathcal{G}_{\mathbf{B}}^{-1}, h)$ ($\mathbf{B} \subset K^6$) имеет вид

$$\begin{cases} x_1 = -b_4^{-1} b_1 - b_4^{-1} b_2 q_1^2 - b_4^{-1} b_3 q_0 + b_4^{-1} y_1, \\ x_2 = -b_4^{-1} b_1 - b_4^{-1} b_5 y_1^2 - b_4^{-1} b_3 q_1 + b_4^{-1} y_2, \\ x_{t+1} = b_4^{-1} b_1 - b_4^{-1} b_5 y_{t+1}^2 - b_4^{-1} b_6 y_t + b_4^{-1} y_{t+1} \end{cases} \qquad (t \geqslant 2). \tag{9}$$

Отметим, что если упорядоченная пара $(M_{\mathbf{a}}, M_{\mathbf{a}}^{-1})$ ($M_{\mathbf{a}} \in \mathcal{M}$) используется в качестве математической модели симметричного поточного шифра (в этом случае параметры $a_1, \ldots, a_5$ играют роль долговременного секретного ключа, а начальное состояние $\mathbf{q}_0$ — роль секретного сеансового ключа), то имитационные модели $(\mathcal{G}_{\mathbf{B}}, h)$ и $(\mathcal{G}_{\mathbf{B}}^{-1}, h)$ предоставляют криптоаналитику большие возможности для вмешательства как в процесс шифрования информации, так и в процесс расшифрования.

6. Таким образом, разработан подход к приближенному решению задачи идентификации семейств автоматов, представленных системами уравнений с параметрами над кольцом $\mathcal{K}$. Выделение над кольцом $\mathcal{K}$ нетривиальных классов семейств автоматов, для которых построение любой достаточно точной имитационной модели — трудная задача, а также нетривиальных классов семейств автоматов, для которых построение некоторой достаточно точной имитационной модели — легкая задача, представляет собой одно из направлений исследований. Другое направление исследований связано с выделением над кольцом $\mathcal{K}$ нетривиальных классов семейств автоматов, для которых существуют такие $[\underline{\eta}, \overline{\eta}]$-точные имитационные модели, для которых $|\overline{\eta} - \underline{\eta}| < \varepsilon$, где ε — заданное положительное число.

1. *Бабаш А. В.* Приближенные модели конечных автоматов // Обозрение прикл. и промышл. математики. – 2005. – **12**, вып. 2. – С. 108–117.
2. *Харин Ю. С., Берник В. И., Матвеев Г. В. и др.* Математические и компьютерные основы криптологии. – Минск: Новое знание, 2003. – 382 с.
3. *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. – Москва: Мир, 1979. – 536 с.
4. *Рейнгольд Э., Нивергельт Ю., Део Н.* Комбинаторные алгоритмы: теория и практика. – Москва: Мир, 1980. – 476 с.
5. *Кузнецов С. П.* Динамический хаос. – Москва: Физматлит, 2001. – 296 с.

Институт прикладной математики и механики НАН Украины, Донецк

Поступило в редакцию 22.12.2011

В. В. Скобелєв

Аналіз задачі розпізнавання автомата над кільцем

Розроблено метод наближеного розв'язання задачі ідентифікації сімей автоматів, наведених системами рівнянь з параметрами над скінченним асоціативно-комутативним кільцем з одиницею. Запропонований метод базується на побудові імітаційної моделі для досліджуваної сім'ї автоматів. Виділено імітаційні моделі, які моделюють поведінку сім'ї автоматів з заданою точністю у "найгіршому випадку" та "у середньому".

V. V. Skobelev

Analysis of the problem of recognition of an automaton over some ring

A method of approximate solution of the problem of identification for families of automata presented by systems of equations with parameters over a finite associative-commutative ring with unity is proposed. The method is based on the construction of a simulation model for the family of automata under study. The models simulating the behavior of such family with given exactness "in the worst case" and "on the average" are separated.