УДК 512.7+519.7+681.3

АВТОМАТЫ НА АЛГЕБРАИЧЕСКИХ СТРУКТУРАХ

В. В. Скобелев

Кандидат физико-математических наук, старший научный сотрудник отдела теории управляющих систем, Институт прикладной математики и механики НАН Украины, Донецк, vv_skobelev@iamm.ac.donetsk.ua

В работе представлен обзор результатов, полученных при исследовании автоматов над конечными алгебраическими структурами. Объектами исследования являются автоматы над конечным кольцом, автоматы, определенные в терминах идеалов, автоматы на многообразиях и семейства хеш-функций, определяемые автоматами без выхода. Для исследуемых автоматов охарактеризованы вычислительная стойкость, сложность построения имитационной модели и гомоморфизмы.

Ключевые слова: кольца, автоматы, идентификация, вычислительная стойкость.

ВВЕДЕНИЕ

Автоматы, заданные системой уравнений над конечной алгебраической структурой, определяют новый раздел алгебраической теории автоматов. Потенциальная область его приложений — разработка моделей и методов преобразования и защиты информации в современных информационных технологиях. При этом обратимые автоматы являются математическими моделями поточных шифров (обладающих тем свойством, что прямой и обратный автомат движутся в пространстве состояний по одной и той же траектории в одном и том же направлении), а автоматы без выхода определяют семейства хэш-функций (являющиеся вычислительно стойкими, если структура графа переходов удовлетворяет определенным условиям). Следует отметить, что исследование указанных выше автоматов открывает большие возможности для взаимопроникновения моделей и методов теории автоматов, теории алгоритмов, теории алгебраических систем, комбинаторного анализа и теории систем.

Основная цель настоящей работы — представить результаты исследование автоматов, заданных системой уравнений над конечной алгебраической структурой. В п. 1 кратко охарактеризованы автоматы над конечным кольцом и автоматы, определенные в терминах идеалов кольца. В п. 2 представлено решение задачи построения имитационной модели для параметрического семейства автоматов над конечным кольцом. В п. 3 охарактеризованы гомоморфизмы автоматов, определенных на двух типах многообразий над конечным кольцом: многообразиях с алгеброй и параметризованных многообразиях. В п. 4 выделен класс вычислительно стойких семейств хеш-функций, определяемых автоматами без выхода над конечным кольцом. Заключение содержит ряд выводов.

1. АВТОМАТЫ НАД КОНЕЧНЫМ КОЛЬЦОМ

Исследования задач анализа и синтеза линейных автоматов над конечным полем представлены в [1, 2], а задач идентификации соответствующих автоматных отображений — в [3, 4]. По видимому, [5] является одной из первых монографий, посвященных систематическому исследованию экспериментов с линейными и билинейными автоматами над конечным полем. Естественным нетривиальным обобщением поля является кольцо [6]. Возможность наличия делителей нуля, некоммутативности умножения и отсутствия единицы открывают широкие перспективы для применения теории колец при решении задач защиты информации в современных информационных системах (отметим, что все кандидаты на стандарты современных поточных шифров используют вычисления в кольцах вычетов).

В [7] исследованы семейства линейных автоматов Мили:

$$\begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t + B\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C\mathbf{q}_t + D\mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+) \tag{1}$$

и Мура

$$\begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t + B\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C\mathbf{q}_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+), \tag{2}$$

над кольцом вычетов (эти результаты обобщены в [8] для произвольного конечного ассоциативно-коммутативного кольца $\mathscr{K} = (K, +, \cdot)$ с единицей), где $\mathbf{q}_t, \mathbf{x}_t, \mathbf{y}_t \in K^n$ есть соответственно состояние, входной и выходной символ в момент $t \in \mathbb{Z}_+$, а квадратные $n \times n$-матрицы A, B, C, D являются параметрами, определяющими конкретный автомат, принадлежащий данному семейству. Показано, что:

1) автомат (1) (соответственно автомат (2)) — обратимый, тогда и только тогда, когда D — обратимая матрица (соответственно B и C — обратимые матрицы);

2) при известных параметрах решение задачи идентификации начального состояния автоматов (1) и (2) сводится к решению системы линейных уравнений, формируемой в процессе эксперимента с автоматом;

3) при решении задачи параметрической идентификации автоматов (1) и (2) идентификация матриц A и B сводится к решению системы нелинейных уравнений, формируемой в процессе эксперимента с автоматом.

Для любого кольца, не являющегося кольцом с сокращением (т. е. ненулевые элементы кольца не образуют гауссовой полугруппы относительно умножения), при решении системы линейных уравнений возникает необходимость поиска по множеству допустимых кандидатов. Ситуация является значительно более сложной при решении нелинейных уравнений над кольцом (известно, что даже над полем $GF(2^k)$ решение уравнения 2-й степени от многих переменных является NP-полной задачей).

Таким образом, приведенные выше результаты показывают, что, во-первых, переход к обратимым автоматам не упрощает решения задач идентификации даже для линейных автоматов над кольцом, а, во-вторых, что при использовании автомата над кольцом в качестве преобразователя информации начальное состояние целесообразно выбирать в качестве секретного сеансового ключа, а параметры — в качестве секретного ключа средней длительности.

В [9, 10] исследована сложность задач параметрической идентификации и идентификации начального состояния автомата

$$\begin{cases} q_{t+2} = a + bq_{t+1}^2 + cq_t + dx_{t+1} \\ y_{t+1} = eq_{t+2} \end{cases} \quad (t \in \mathbb{Z}_+) \tag{3}$$

над конечным ассоциативно-коммутативным кольцом с единицей (отметим, что первое уравнение системы (3) является аналогом над кольцом ряда модельных хаотических отображений, в том числе отображения Эно [11]).

На основе полученных результатов в [8, 12] разработан подход к решению уравнений над ассоциативно-коммутативным кольцом с единицей, основанный на классах ассоциированных элементов кольца (т. е. элементов, которые могут быть получены друг из друга умножением на обратимый элемент кольца). Суть этого подхода состоит в следующем. Для переменных выделяются допустимые комбинации классов ассоциированных элементов. Для каждой такой комбинации переменная заменяется переменным элементом класса, т. е. произведением фиксированного элемента класса на переменный обратимый элемент (таким образом, задача сводится к поиску обратимых элементов кольца). Далее осуществляется поиск допустимых комбинаций обратимых элементов для данной комбинации классов ассоциированных элементов.

В [13] рассмотренный выше подход обобщен для произвольных ассоциативных некоммутативных колец с левой или правой единицей.

В [14] исследованы автоматы Мили:

$$\begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t) + \mathbf{f}_3(\mathbf{x}_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_t) + \mathbf{f}_4(\mathbf{x}_{t+1}) \end{cases} \quad (t \in \mathbb{Z}_+) \tag{4}$$

и Мура

$$\begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t) + \mathbf{f}_3(\mathbf{x}_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_{t+1}) \end{cases} \quad (t \in \mathbb{Z}_+), \tag{5}$$

над конечным ассоциативно-коммутативным кольцом $\mathscr{K} = (K, +, \cdot)$, где $\mathbf{f}_i : K^n \to K^n$ $(i = 1, \ldots, 4)$ — такие отображения, что $Val\, \mathbf{f}_1 = \mathbf{I}_1$ и $Val\, \mathbf{f}_2 = \mathbf{I}_2$ для фиксированных наборов идеалов

$\mathbf{I}_r = (I_1^{(r)}, \ldots, I_n^{(r)})$ $(r = 1, 2)$ кольца $\mathscr{K}$. Определим на входной полугруппе $(K^n)^+$ отношение эквивалентности $\sim_{n,12}$ равенством $\sim_{n,12} = \sim_{n,1} \cap \sim_{n,2}$, где для любых входных слов $\mathbf{u}' = \mathbf{x}'_1 \ldots \mathbf{x}'_k \in (K^n)^+$ и $\mathbf{u}'' = \mathbf{x}''_1 \ldots \mathbf{x}''_k \in (K^n)^+$

$$\mathbf{u}' \sim_{n,r} \mathbf{u}'' \Leftrightarrow (\forall 1 \le j \le k)(\mathbf{f}_{2+r}(\mathbf{x}'_j) \equiv \mathbf{f}_{2+r}(\mathbf{x}''_j) \pmod{\mathbf{I}_r}) \ \ (r = 1, 2),$$

а отношение эквивалентности $\sim'_{n,12}$ — формулой

$$\mathbf{u}' \sim'_{n,12} \mathbf{u}'' \Leftrightarrow \mathbf{u}' \sim_{n,1} \mathbf{u}'' \ \& \ (\forall \mathbf{q}'_0, \mathbf{q}''_0 \in K^n)(\forall 1 \le j \le k)(\mathbf{q}'_j \equiv \mathbf{q}''_j \ (\ker \ \mathbf{f}_2)).$$

В [14] доказаны следующие теоремы.

Теорема 1. *Для автомата* (4) *при любых наборах идеалов* $\boldsymbol{I}_r = (I_1^{(r)}, \ldots, I_n^{(r)})$ $(r = 1, 2)$ *для любых входных слов* $\boldsymbol{u}' = \boldsymbol{x}'_1 \ldots \boldsymbol{x}'_k \in (K^n)^+$ *и* $\boldsymbol{u}'' = \boldsymbol{x}''_1 \ldots \boldsymbol{x}''_k \in (K^n)^+$ *истинна формула*

$$\mathbf{u}' \sim_{n,12} \mathbf{u}'' \Leftrightarrow (\forall \mathbf{q}'_0, \mathbf{q}''_0 \in K^n)(\forall 1 \le j \le k)(\mathbf{q}'_j \equiv \mathbf{q}''_j (\mathrm{mod}\ \mathbf{I}_1) \& \mathbf{y}'_j \equiv \mathbf{y}''_j (\mathrm{mod}\ \mathbf{I}_2)).$$

Теорема 2. *Для автомата* (5) *при любых наборах идеалов* $\boldsymbol{I}_r = (I_1^{(r)}, \ldots, I_n^{(r)})$ $(r = 1, 2)$ *для любых входных слов* $\boldsymbol{u}' = \boldsymbol{x}'_1 \ldots \boldsymbol{x}'_k \in (K^n)^+$ *и* $\boldsymbol{u}'' = \boldsymbol{x}''_1 \ldots \boldsymbol{x}''_k \in (K^n)^+$ *истинна формула*

$$\mathbf{u}' \sim'_{n,12} \mathbf{u}'' \Leftrightarrow (\forall \mathbf{q}'_0, \mathbf{q}''_0 \in K^n)(\forall 1 \le j \le k)(\mathbf{q}'_j \equiv \mathbf{q}''_j (\mathrm{mod}\ \mathbf{I}_1) \& \mathbf{y}'_j \equiv \mathbf{y}''_j (\mathrm{mod}\ \mathbf{I}_2)).$$

Отметим, что, по своей сути, эти теоремы определяют гомоморфные образы автоматов вида (4) и (5) при гомоморфизме колец.

2. ИМИТАЦИОННАЯ МОДЕЛЬ СЕМЕЙСТВА АВТОМАТОВ НАД КОНЕЧНЫМ КОЛЬЦОМ

Анализ задачи параметрической идентификации автомата над конечным кольцом $\mathscr{K} = (K, +, \cdot)$ показывает, что параметры не всегда могут быть идентифицированы однозначно (такая ситуация, в частности, имеет место для автомата (3)). Поэтому естественно возникает задача построения алгоритма, моделирующего с определенной точностью любой автомат, принадлежащий заданному семейству. Эта задача была решена в [15, 16]. Суть предложенного решения состоит в следующем.

Рассмотрим такое семейство автоматов $\mathscr{M} = \{M_{\mathbf{a}}\}_{\mathbf{a} \in \mathbf{A}}$ $(\mathbf{A} \subseteq K^l)$, что

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

где $\mathbf{f}_1 : K^{n_1+n_2+l} \to K^{n_1}$ и $\mathbf{f}_2 : K^{n_1+n_2+l} \to K^{n_3}$ — фиксированные отображения.

Зафиксируем множество параметров $\mathbf{B} \subseteq K^{l_1}$ $(|\mathbf{B}| < |\mathbf{A}|)$ и три семейства отображений $\{\varphi_{\mathbf{b}}^{(1)} : K^{n_1} \times K^{n_2} \to K^{n_3}\}_{\mathbf{b} \in \mathbf{B}}$, $\{\varphi_{\mathbf{b}}^{(2)} : K^{n_1} \times \bigcup_{j=1}^{r-1} (K^{n_3})^j \times K^{n_2} \to K^{n_3}\}_{\mathbf{b} \in \mathbf{B}}$ и $\{\varphi_{\mathbf{b}}^{(3)} : K^{n_1} \times (K^{n_3})^r \times K^{n_2} \to K^{n_3}\}_{\mathbf{b} \in \mathbf{B}}$. Рассмотрим семейство таких отображений $\mathscr{G}_{\mathbf{B}} = \{G_{\mathbf{b}} : K^{n_1} \times (K^{n_2})^+ \to (K^{n_3})^+\}_{\mathbf{b} \in \mathbf{B}}$, что $G_{\mathbf{b}}(\mathbf{q}_0, \mathbf{x}_1 \ldots \mathbf{x}_m) = \mathbf{y}_1 \ldots \mathbf{y}_m$ $(\mathbf{b} \in \mathbf{B}, m \in \mathbb{N})$, где

$$\mathbf{y}_i = \begin{cases} \varphi_{\mathbf{b}}^{(1)}(\mathbf{q}_0, \mathbf{x}_1), \ \text{если } i = 1, \\ \varphi_{\mathbf{b}}^{(2)}(\mathbf{q}_0, \mathbf{y}_1 \ldots \mathbf{y}_{i-1}, \mathbf{x}_i), \ \text{если } i = 2, \ldots, r, \\ \varphi_{\mathbf{b}}^{(3)}(\mathbf{q}_0, \mathbf{y}_{i-r} \ldots \mathbf{y}_{i-1}, \mathbf{x}_i), \ \text{если } r < i \le m. \end{cases} \tag{6}$$

Определим отображения $H_{\mathbf{b},\mathbf{q}_0} : (K^{n_2})^+ \to (K^{n_3})^+$ $(\mathbf{b} \in \mathbf{B}, \mathbf{q}_0 \in K^{n_1})$ равенством $H_{\mathbf{b},\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_m) = G_{\mathbf{b}}(\mathbf{q}_0, \mathbf{x}_1 \ldots \mathbf{x}_m)$ $(m \in \mathbb{N})$. Из (6) 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 $\mathscr{H}_{\mathbf{b}} = \{H_{\mathbf{b},\mathbf{q}_0}\}_{\mathbf{q}_0 \in K^{n_1}}$ $(\mathbf{b} \in \mathbf{B})$ определяет конечный автомат над кольцом $\mathscr{K}$. Зафиксировав сюръекцию $h : \mathbf{A} \to \mathbf{B}$, сопоставим с каждым автоматом $M_{\mathbf{a}} \in \mathscr{M}$ автомат, определяемый семейством автоматных отображений $\mathscr{H}_{h(\mathbf{a})}$, т. е. упорядоченная пара $(\mathscr{G}_{\mathbf{B}}, h)$ является имитационной моделью семейства автоматов $\mathscr{M}$. Естественно потребовать, чтобы выполнялись равенства $H_{h(\mathbf{a}),\mathbf{q}_0}\big|_{\bigcup_{i=1}^{r} (K^{n_2})^i} = F_{\mathbf{a},\mathbf{q}_0}\big|_{\bigcup_{i=1}^{r} (K^{n_2})^i}$ $(\mathbf{a} \in \mathbf{A}, \mathbf{q}_0 \in K^{n_1})$, где $F_{\mathbf{a},\mathbf{q}_0} : (K^{n_2})^+ \to (K^{n_3})^+$ — отображение, реализуемое инициальным автоматом $(M_{\mathbf{a}}, \mathbf{q}_0)$. Содержательный смысл этих равенств

состоит в том, что имитационная модель $(\mathscr{G}_{\mathbf{B}}, h)$, 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 моделирует его поведение на оставшейся части входного слова. Всюду в дальнейшем считаем, что это условие выполнено. Отметим, что если переменная $\mathbf{q}_0$ фиктивна для каждого отображения $\varphi_{\mathbf{b}}^{(3)}$ $(\mathbf{b} \in \mathbf{B})$, то $(\mathscr{G}_{\mathbf{B}}, h)$ моделирует поведения каждого автомата $M_{\mathbf{a}}$ $(\mathbf{a} \in \mathbf{A})$ посредством автоматов с конечной памятью.

Определим точность имитационной модели $(\mathscr{G}_{\mathbf{B}}, h)$ на основе стандартной техники теории алгоритмов.

Пусть $F_{\mathbf{a},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_m) = \mathbf{y}_1 \dots \mathbf{y}_m$ и $H_{h(\mathbf{a}),\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_m) = \widetilde{\mathbf{y}}_1 \dots \widetilde{\mathbf{y}}_m$.

Число $\alpha_{\mathbf{a},\mathbf{q}_0,m} = |K^{n_2}|^{-m} \sum\limits_{\mathbf{x}_1 \dots \mathbf{x}_m \in (K^{n_2})^m} (m - \varrho(\mathbf{y}_1 \dots \mathbf{y}_m, \widetilde{\mathbf{y}}_1 \dots \widetilde{\mathbf{y}}_m))$ (где ϱ — расстояние по Хеммингу) 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 $\beta_{\mathbf{a},\mathbf{q}_0,m} = m^{-1}\alpha_{\mathbf{a},\mathbf{q}_0,m}$ — среднее количество позиций в выходных словах, приходящихся 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 $\gamma_{\mathbf{a},\mathbf{q}_0,m} = \dfrac{|K^{n_2}| - 1}{|K^{n_2}|^{m+1} - |K^{n_2}|} \sum\limits_{i=1}^{m} |K^{n_2}|^i \beta_{\mathbf{a},\mathbf{q}_0,m}$ — среднее количество позиций в выходных словах, приходящихся 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 m.

Числа $\underline{\gamma}_{\mathbf{a},\mathbf{q}_0} = \lim\limits_{m\to\infty} \inf\{\gamma_{\mathbf{a},\mathbf{q}_0,i} | i \in \mathbb{N}_m\}$ и $\overline{\gamma}_{\mathbf{a},\mathbf{q}_0} = \lim\limits_{m\to\infty} \sup\{\gamma_{\mathbf{a},\mathbf{q}_0,i} | i \in \mathbb{N}_m\}$ определяют соответственно нижнюю и верхнюю границу 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:

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 среднего количества позиций в выходных словах, приходящегося на одну букву входного слова, в которых элементы семейства $\mathscr{F}_{\mathbf{a}} = \{F_{\mathbf{a},\mathbf{q}_0}\}_{\mathbf{q}_0 \in K^{n_1}}$ совпадают с соответствующими элементами семейства $\mathscr{H}_{h(\mathbf{a})}$;

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 элементы семейства $\mathscr{F}_{\mathbf{a}}$ совпадают с соответствующими элементами семейства $\mathscr{H}_{h(\mathbf{a})}$;

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 элементы семейства $\mathscr{F}_{\mathbf{a}}$ совпадают с соответствующими элементами семейства $\mathscr{H}_{h(\mathbf{a})}$.

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 $\mathscr{M}$, совпадают с автоматными отображениями, реализуемыми имитационной моделью $(\mathscr{G}_{\mathbf{B}}, h)$;

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 $\mathscr{M}$, совпадают с автоматными отображениями, реализуемыми имитационной моделью $(\mathscr{G}_{\mathbf{B}}, h)$;

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 $\mathscr{M}$, совпадают с автоматными отображениями, реализуемыми имитационной моделью $(\mathscr{G}_{\mathbf{B}}, h)$;

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, приходящихся на одну букву входного слова, в которых автоматные отображения,

реализуемые семейством автоматов $\mathscr{M}$, совпадают с автоматными отображениями, реализуемыми имитационной моделью $(\mathscr{G}_{\mathbf{B}}, h)$;

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 $\mathscr{M}$, совпадают с автоматными отображениями, реализуемыми имитационной моделью $(\mathscr{G}_{\mathbf{B}}, h)$.

Рассмотренные случаи охватывают все представляющие интерес комбинации понятий «в наихудшем случае» и «в среднем», и дают возможность охарактеризовать имитационную модель $(\mathscr{G}_{\mathbf{B}}, h)$ как асимптотически $[\underline{\eta}, \overline{\eta}]$-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 $\mathbf{a} \in \mathbf{A}$, то как асимптотически ν-точную, где ν — любое из чисел ν_1, ν_2, ν_3 или ν_4. В последнем случае естественно определить имитационную модель $(\mathscr{G}_{\mathbf{B}}, h)$ как асимптотически точную, если $\nu = 1$.

В [15, 16] показано, что для семейства автоматов (3) существует асимптотически точная имитационная модель, моделирующая каждый автомат этого семейства автоматом с конечной памятью.

3. АВТОМАТЫ НА МНОГООБРАЗИИ НАД КОНЕЧНЫМ КОЛЬЦОМ

Применение эллиптических кривых над конечными полями при решении задач преобразования информации, в частности криптографии, обосновывают актуальность исследования автоматов, определенных на многообразиях (т. е. на множествах решений систем алгебраических уравнений) над конечным кольцом $\mathscr{K} = (K, +, \cdot)$. Такое исследование дает возможность установить внутренние связи между современной алгебраической геометрией, теорией систем, теорией автоматов и криптологией. Рассмотрим некоторые результаты, полученные в этом направлении в [17–21].

С позиции алгебраической теории автоматов и ее приложений наибольший интерес представляют следующие два класса многообразий над кольцом $\mathscr{K}$:

1) класс $\mathscr{V}_1(\mathscr{K})$, состоящий из всех таких многообразий $\mathbf{V} \subseteq K^n$, что определена алгебра $(\mathbf{V}, \mathscr{F}_1 \cup \mathscr{F}_2)$, где $\mathscr{F}_1 = \{\alpha_0, \alpha_1, \ldots, \alpha_{k_1}\}$ и $\mathscr{F}_2 = \{\beta_1, \ldots, \beta_{k_2}\}$ — множество соответственно унарных и бинарных операций;

2) класс $\mathscr{V}_2(\mathscr{K})$, состоящий из всех многообразий $\mathbf{V} \subseteq K^n$, представленных полиномиальной параметризацией $\mathbf{v} = \mathbf{h}(\overrightarrow{\tau})$ $(\overrightarrow{\tau} \in K^m)$.

Отметим, что эллиптическая кривая γ над областью целостности $\mathscr{K}$ — многообразие, принадлежащее классу $\mathscr{V}_1(\mathscr{K})$. Действительно, в поле дробей $\widetilde{\mathscr{K}}$ множество $\widetilde{\mathscr{K}}(\gamma)$ точек кривой γ (включая бесконечно удаленную точку O) образует абелеву группа $(\widetilde{\mathscr{K}}(\gamma), +_\gamma)$ (точка O — нейтральный элемент). Положив $\mathscr{F}_1 = \{\alpha_0, \alpha_1, \ldots, \alpha_{k_1}\}$ $(1 \le k_1 < |\widetilde{\mathscr{K}}(\gamma)|)$, где $\alpha_0(P) = O$ $(P \in \widetilde{\mathscr{K}}(\gamma))$ и $\alpha_i(P) = \underbrace{P +_\gamma \ldots +_\gamma P}_{i \text{ раз}}$ $(P \in \widetilde{\mathscr{K}}(\gamma))$ для всех $i = 1, \ldots, k_1$ и $\mathscr{F}_2 = \{+_\gamma\}$, мы определяем алгебру $(\widetilde{\mathscr{K}}(\gamma), \mathscr{F}_1 \cup \mathscr{F}_2)$.

Для многообразия $\mathbf{V} \in \mathscr{V}_1(\mathscr{K})$ алгебра $(\mathbf{V}, \mathscr{F}_1 \cup \mathscr{F}_2)$ дает возможность определить множество $\mathscr{A}^{(1)}(\mathbf{V})$ автоматов Мили:

$$\begin{cases} \mathbf{q}_{t+1} = \beta_{j_1}(\alpha_{i_1}(\mathbf{q}_t), \alpha_{x_{t+1}}(\mathbf{v}_1)) \\ \mathbf{y}_{t+1} = \beta_{j_2}(\alpha_{i_2}(\mathbf{q}_t), \alpha_{x_{t+1}}(\mathbf{v}_2)) \end{cases} \qquad (t \in \mathbb{Z}_+)$$

и множество $\mathscr{A}^{(2)}(\mathbf{V})$ автоматов Мура:

$$\begin{cases} \mathbf{q}_{t+1} = \beta_{j_1}(\alpha_{i_1}(\mathbf{q}_t), \alpha_{x_{t+1}}(\mathbf{v}_1)) \\ \mathbf{y}_{t+1} = \beta_{j_2}(\alpha_{i_2}(\mathbf{q}_{t+1}), \mathbf{v}_2) \end{cases} \qquad (t \in \mathbb{Z}_+),$$

где $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}$ — фиксированные точки, $i_1, i_2 \in \mathbb{Z}_{k_1+1}$ и $j_1, j_2 \in \mathbb{N}_{k_2}$ — фиксированные числа, $\mathbf{q}_0 \in \mathbf{V}$, а $x_{t+1} \in \mathbb{Z}_{k_1+1}$ $(t \in \mathbb{Z}_+)$. Таким образом, x_t, $\mathbf{q}_t$ и $\mathbf{y}_t$ являются соответственно входным символом, состоянием и выходным символом автомата $M \in \mathscr{A}^{(1)}(\mathbf{V}) \cup \mathscr{A}^{(2)}(\mathbf{V})$ в момент t.

Пусть $\mathbf{V}, \mathbf{U} \in \mathscr{V}_1(\mathscr{K})$. Будем говорить, что:

1) многообразие $\mathbf{U}$ — гомоморфный образ многообразия $\mathbf{V}$, если алгебра $(\mathbf{U}, \mathscr{F}_1^{(2)} \cup \mathscr{F}_2^{(2)})$ — гомоморфный образ алгебры $(\mathbf{V}, \mathscr{F}_1^{(1)} \cup \mathscr{F}_2^{(1)})$;

2) многообразия $\mathbf{U}$ и $\mathbf{V}$ изоморфны, если алгебры $(\mathbf{U}, \mathscr{F}_1^{(2)} \cup \mathscr{F}_2^{(2)})$ и $(\mathbf{V}, \mathscr{F}_1^{(1)} \cup \mathscr{F}_2^{(1)})$ изоморфны.

В [17] доказана следующая теорема.

Теорема 3. *Пусть* $\mathbf{U}, \mathbf{V} \in \mathscr{V}_1(\mathscr{K})$. *Если многообразие* $\mathbf{U}$ *— гомоморфный образ многообразия* $\mathbf{V}$, *то существуют такие отображения* $\Psi_j : \mathscr{A}^{(j)}(\mathbf{V}) \to \mathscr{A}^{(j)}(\mathbf{U})$ $(j = 1, 2)$, *что автомат* $\Psi_j(M_j)$ *— гомоморфный образ автомата* $M_j \in \mathscr{A}^{(j)}(\mathbf{V})$.

Следствие 1. *Пусть* $\mathbf{U}, \mathbf{V} \in \mathscr{V}_1(\mathscr{K})$. *Если многообразия* $\mathbf{U}$ и $\mathbf{V}$ *изоморфны, то существуют такие отображения* $\Psi_j : \mathscr{A}^{(j)}(\mathbf{V}) \to \mathscr{A}^{(j)}(\mathbf{U})$ $(j = 1, 2)$, *что автоматы* $M_j \in \mathscr{A}^{(j)}(\mathbf{V})$ *и* $\Psi_j(M_j)$ *изомофны*.

Пусть $\mathbf{V} \in \mathscr{V}_2(\mathscr{K})$, а $\mathbf{v} = \mathbf{h}(\overrightarrow{\tau})$ $(\overrightarrow{\tau} \in K^m)$ — полиномиальная параметризация многообразия $\mathbf{V}$. Фиксированное семейство отображений $\Theta = \{\theta_i : K^m \to K^m\}_{i \in \mathbf{Z}_k}$ дает возможность определить множество $\mathscr{A}^{(1)}(\mathbf{V}, \Theta)$ автоматов Мили:

$$\begin{cases} \mathbf{q}_{t+1} = \mathbf{h}(P_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{r}_{x_{t+1}}(\mathbf{q}_t) \end{cases} \qquad (t \in \mathbf{Z}_+)$$

и множество $\mathscr{A}^{(2)}(\mathbf{V}, \Theta)$ Мура:

$$\begin{cases} \mathbf{q}_{t+1} = \mathbf{h}(P_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{r}(\mathbf{q}_{t+1}) \end{cases} \qquad (t \in \mathbf{Z}_+),$$

где $P_0 \in K^m$ — фиксированная точка, $\mathbf{q}_0 = \mathbf{h}(P_0)$, $\mathbf{r}_i : K^n \to K^l$ $(i \in \mathbb{Z}_k)$ и $\mathbf{r} : K^n \to K^l$ — фиксированные отображения, а $x_{t+1} \in \mathbb{Z}_k$ $(t \in \mathbb{Z}$. Таким образом, x_t, $\mathbf{q}_t$ и $\mathbf{y}_t$ — соответственно входной символ, состояние и выходной символ автомата $M \in \mathscr{A}^{(1)}(\mathbf{V}, \Theta) \cup \mathscr{A}^{(2)}(\mathbf{V}, \Theta)$ в момент t.

Пусть для многообразия $\mathbf{V} \in \mathscr{V}_2(\mathscr{K})$ определена полиномиальная параметризация $\mathbf{v} = \mathbf{h}_1(\overrightarrow{\tau}_1)$ $(\overrightarrow{\tau}_1 \in K^{m_1})$ и зафиксировано семейство $\Theta_1 = \{\theta_i^{(1)}\}_{i \in \mathbf{Z}_k}$ отображений $\theta_i^{(1)} : K^{m_1} \to K^{m_1}$, а для многообразия $\mathbf{U} \in \mathscr{V}_2(\mathscr{K})$ — полиномиальная параметризация $\mathbf{v} = \mathbf{h}_2(\overrightarrow{\tau}_2)$ $(\overrightarrow{\tau}_2 \in K^{m_2})$ и зафиксировано семейство $\Theta_2 = \{\theta_i^{(2)}\}_{i \in \mathbf{Z}_k}$ отображений $\theta_i^{(2)} : K^{m_2} \to K^{m_2}$. Будем говорить, что:

1) пара $(\mathbf{U}, \Theta_2)$ — гомоморфный образ пары $(\mathbf{V}, \Theta_1)$, если существует такая пара сюръекций $\Phi = (\varphi_1, \varphi_2)$ $(\varphi_1 : \mathbf{V} \to \mathbf{U}, \varphi_2 : K^{m_1} \to K^{m_2})$, что равенства $\varphi_2(\theta_i^{(1)}(\overrightarrow{\tau}_1)) = \theta_i^{(2)}(\varphi_2(\overrightarrow{\tau}_1))$ и $\varphi_1(\mathbf{h}_1(\overrightarrow{\tau}_1)) = \mathbf{h}_2(\varphi_2(\overrightarrow{\tau}_1))$ истинны для всех $\overrightarrow{\tau}_1 \in K^{m_1}$ и $i \in \mathbf{Z}_k$;

2) пары $(\mathbf{U}, \Theta_2)$ и $(\mathbf{V}, \Theta_1)$ изоморфны, если указанные выше отображения φ_1 и φ_2 — биекции.

В [17] доказана следующая теорема.

Теорема 4. *Пусть* $\mathbf{U}, \mathbf{V} \in \mathscr{V}_2(\mathscr{K})$. *Если пара* $(\mathbf{U}, \Theta_2)$ *— гомоморфный образ пары* $(\mathbf{V}, \Theta_1)$, *то существуют такие отображения* $\Psi_j : \mathscr{A}^{(j)}(\mathbf{V}, \Theta_1) \to \mathscr{A}^{(j)}(\mathbf{U}, \Theta_2)$ $(j = 1, 2)$, *что автомат* $\Psi_j(M_j)$ *— гомоморфный образ автомата* $M_j \in \mathscr{A}^{(j)}(\mathbf{V}, \Theta_1)$.

Следствие 2. *Пусть* $\mathbf{U}, \mathbf{V} \in \mathscr{V}_2(\mathscr{K})$. *Если пары* $(\mathbf{U}, \Theta_2)$ и $(\mathbf{V}, \Theta_1)$ *изоморфны, то существуют такие отображения* $\Psi_j : \mathscr{A}^{(j)}(\mathbf{V}, \Theta_1) \to \mathscr{A}^{(j)}(\mathbf{U}, \Theta_2)$ $(j = 1, 2)$, *что автоматы* $M_j \in \mathscr{A}^{(j)}(\mathbf{V}, \Theta_1)$ и $\Psi_j(M_j)$ *изоморфны*.

В [17, 21] в явном виде построены отображения Ψ_j $(j = 1, 2)$, о которых идет речь в теоремах 3 и 4. В [18] исследована структура автоматов на многообразии с алгеброй, а в [19, 20] — структура автоматов на полиномиально параметризованном многообразии. В [22] исследованы автоматы, определенные на эллиптической кривой над конечной областью целостности. В частности, решена задача построения имитационной модели для этих автоматов.

4. СЕМЕЙСТВА ХЕШ-ФУНКЦИЙ, ОПРЕДЕЛЯЕМЫХ АВТОМАТАМИ НАД КОНЕЧНЫМ КОЛЬЦОМ

Известно, что хеш-функция $H : X^+ \to Y$, применяемая при решении задач защиты информации, должна удовлетворять следующим трем условиям:

1) H легко вычислимая функция;

2) для любого $y \in Y$ сложность поиска такого $u \in X^+$, что $H(u) = y$ является экспонентой;

3) сложность случайного поиска двух таких $u, u' \in X^+$ одной и той же длины, что $H(u) = H(u')$ является экспонентой.

Ясно, что любая хеш-функция — это отображение входной полугруппы во множество состояний, реализуемое инициальным автоматом без выхода. Поэтому актуально исследование семейств хеш-

функций, определенных автоматами без выхода над над конечным кольцом $\mathscr{K} = (K, +, \cdot)$. Рассмотрим некоторые результаты, полученные в этом направлении в [23].

Пусть $\mathscr{F}_{k,m}$ $(k \leq m)$ — множество таких отображений $\mathbf{f} : K^k \times K^m \to K^k$, что

$$|\{\mathbf{x} \in K^m | \mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{q}''\}| = |K|^{m-k}$$

и

$$\{\mathbf{x} \in K^m | \mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{q}''\} \cap \{\mathbf{x} \in K^m | \mathbf{f}(\mathbf{q}', \mathbf{x}) = \mathbf{q}''\} = \emptyset$$

для всех $\mathbf{q}, \mathbf{q}', \mathbf{q}'' \in K^k$ $(\mathbf{q} \neq \mathbf{q}')$. Отображение $\mathbf{f} \in \mathscr{F}_{k,m}$ определяет сильно связный автомат без выхода $M_{\mathbf{f}}$ с множеством состояний K^k и входным алфавитом K^m.

Обозначим через $H_{\mathbf{f},\mathbf{q}_0}$ отображение входной полугруппы $(K^m)^+$ во множество состояний K^k, реализуемое инициальным автоматом $(M_{\mathbf{f}}, \mathbf{q}_0)$. Таким образом, автомат $M_{\mathbf{f}}$ определяет семейство хэш-функций $\{H_{\mathbf{f},\mathbf{q}_0}\}_{\mathbf{q}_0 \in K^k}$. В [23] доказаны следующие теоремы, характеризующие свойства структуры этого семейства хэш-функций.

Теорема 5. *Для любого отображения* $\mathbf{f} \in \mathscr{F}_{k,m}$ *если* $\mathbf{q}_0 \neq \mathbf{q}_0'$ $(\mathbf{q}_0, \mathbf{q}_0' \in K^k)$, *то* $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) \neq H_{\mathbf{f},\mathbf{q}_0'}(\mathbf{u})$ *для любого входного слова* $\mathbf{u} \in (K^m)^+$.

Следствие 3. *Для любого отображения* $\mathbf{f} \in \mathscr{F}_{k,m}$ *если* $\mathbf{q}_0 \neq \mathbf{q}_0'$ $(\mathbf{q}_0, \mathbf{q}_0' \in K^k)$, *то* $H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}) \cap H^{-1}_{\mathbf{f},\mathbf{q}_0'}(\mathbf{q}) = \emptyset$ *для любого состояния* $\mathbf{q} \in K^k$ *автомата* $M_{\mathbf{f}}$.

Теорема 6. *Для любых* $\mathbf{f} \in \mathscr{F}_{k,m}$ *и* $\mathbf{q}_0 \in K^k$ *равенство* $|H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_t) \cap (K^m)^t| = |K|^{tm-k}$ $(\mathbf{q}_t) \in K^k)$ *истинно при всех* $t \in \mathbb{N}$.

Обозначим через $p^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q})$ вероятность того, что случайно выбранное из множества $(K^m)^t$ входное слово $\mathbf{u}$ является решением уравнения $H(\mathbf{u}) = \mathbf{q}$, а через $p^{(2)}_{\mathbf{f},\mathbf{q}_0,t}$ — вероятность того, что для двух случайно выбранных из множества $(K^m)^t$ различных входных слов $\mathbf{u}$ и $\mathbf{u}'$ истинно равенство $H(\mathbf{u}) = H(\mathbf{u}')$. В [23] вычислительная стойкость семейства хэш-функций $\{H_{\mathbf{f},\mathbf{q}_0}\}_{\mathbf{q}_0 \in K^k}$ охарактеризована следующим образом.

Теорема 7. *Для любых* $\mathbf{f} \in \mathscr{F}_{k,m}$ *и* $\mathbf{q}_0, \mathbf{q} \in K^k$ *равенство* $p^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q}) = |K|^{-k}$ *истинно при всех* $t \in \mathbb{N}$.

Теорема 8. *Для любых* $\mathbf{f} \in \mathscr{F}_{k,m}$ *и* $\mathbf{q}_0 \in K^k$ *равенство* $p^{(2)}_{\mathbf{f},\mathbf{q}_0,t} = |K|^{-k}\left(1 - \dfrac{|K|^k - 1}{|K|^{mt} - 1}\right)$ *истинно при всех* $t \in \mathbb{N}$.

Таким образом, число $|K|^{-k}$ характеризует вычислительную стойкость семейства хэш-функций $\{H_{\mathbf{f},\mathbf{q}_0}\}_{\mathbf{q}_0 \in K^k}$. Отсюда вытекает целесообразность использования таких семейств хэш-функций при решении задач защиты информации. При этом начальное состояние $\mathbf{q}_0$ целесообразно использовать в качестве секретного сеансового ключа, а значения параметров, входящих в формулу $\mathbf{f}(\mathbf{q}_t, \mathbf{x}_{t+1})$, — в качестве секретного ключа средней длительности.

ЗАКЛЮЧЕНИЕ

В работе кратко охарактеризованы результаты, полученные при исследовании автоматов над конечными алгебраическими структурами.

Анализ автоматов, определенных в терминах идеалов кольца, показывает целесообразность исследования их свойств в зависимости от тех или иных соотношений между идеалами, входящими в наборы идеалов $\mathbf{I}_r = (I_1^r, \ldots, I_n^r)$ $(r = 1, 2)$. Это определяет одно из направлений дальнейших исследований.

Анализ задачи построения имитационной модели для семейства автоматов показывает целесообразность выделения нетривиальных классов семейств автоматов, для которых любая асимптотически ν-точная имитационная модель при всех значениях числа ν, достаточно близких к единице, существенно сложнее, чем система уравнений с параметрами, определяющая автомат, а также исследование классов обратимых автоматов, для которых при обращении имитационной модели существенно теряется ее точность. Это определяет второе направление дальнейших исследований.

Анализ автоматов, определенных на многообразиях, показывает целесообразность исследования свойств таких автоматов при дополнительных ограничениях на многообразие, определенную на нем

алгебру, либо на заданное семейство отображений $\Theta = \{\theta_i : K^m \to K^m\}_{i \in \mathbf{Z}_k}$. Это определяет третье направление дальнейших исследований.

Анализ семейств хэш-функций, определяемых автоматами без выхода над конечным кольцом показывает целесообразность исследования семейств хэш-функций, определяемых автоматами на многообразиях, в частности, семейств хэш-функций, определяемых автоматами на эллиптических кривых над конечными областями целостности. Это определяет четвертое направление дальнейших исследований.

Библиографический список

1. *Гилл А.* Линейные последовательностные машины. М. : Наука, 1974. 298 с.
2. *Фараджев Р. Г.* Линейные последовательностные машины. М. : Сов. радио, 1975. 248 с.
3. *Агибалов Г. П.* Распознавание операторов, реализуемых в линейных автономных автоматах // Изв. АН СССР. Техн. кибернетика. 1970. № 3. С. 99–108.
4. *Агибалов Г. П., Юфит Я. Г.* О простых экспериментах для линейных инициальных автоматов // Автоматика и вычислительная техника. 1972. № 2. С. 17–19.
5. *Сперанский Д. В.* Эксперименты с линейными и билинейными конечными автоматами. Саратов : Изд-во Сарат. ун-та, 2004. 144 с.
6. *Курош А. Г.* Лекции по общей алгебре. М. : Наука, 1973. 400 с.
7. *Скобелев В. В., Скобелев В. Г.* Анализ шифрсистем / ИПММ НАНУ. Донецк, 2009. 479 с.
8. *Скобелев В. В., Глазунов Н. М., Скобелев В. Г.* Многообразия над кольцами. Теория и приложение / ИПММ НАНУ. Донецк, 2011. 323 с.
9. *Скобелев В. В., Скобелев В. Г.* Анализ нелинейных автоматов с лагом 2 над конечным кольцом // Прикладная дискретная математика. 2010. № 1. С. 68–85.
10. *Скобелев В. В.* Сложность идентификации нелинейных одномерных автоматов с лагом 2 над конечным кольцом // Компьютерная мат. 2011. Вып. 2. С. 81–89.
11. *Кузнецов С. П.* Динамический хаос. М. : Физматлит, 2001. 296 с.
12. *Скобелев В. В., Скобелев В. Г.* О сложности анализа автоматов над конечным кольцом // Кибернетика и системный анализ. 2010. № 4. С. 17–30.
13. *Skobelev V. V.* On systems of polynomial equations over finite rings // Наукові записки НаУ-КМА. Сер. Комп'ютерні науки. 2012. Т. 138. С. 15–19.
14. *Скобелєв В. В.* Про множини автоматів над скінченним кільцем, які визначено у термінах ідеалів // Вісник Київського університету. Сер. : фіз.-мат. науки. 2011. № 3. С. 212–218.
15. *Скобелев В. В.* Моделирование автоматов над кольцом автоматами с конечной памятью // Проблемы управления и информатики. 2012. № 3. С. 114–122.
16. *Скобелев В. В.* Анализ задачи распознавания автомата над кольцом // Доповіді НАНУ. 2012. № 9. С. 29–35.
17. *Скобелев В. В.* Об автоматах на многообразиях над кольцом // Труды ИПММ НАНУ. 2012. Т. 24. С. 190–201.
18. *Скобелєв В. В.* Автомати на многовидах з алгеброю // Вісник Київського університету. Сер. : фіз.-мат. науки. 2012. № 2. С. 234–238.
19. *Skobelev V. V.* Analysis of automata determined over parametric varieties over an associative ring // Вісник Київського університету. Сер.: фіз.-мат. науки. 2012. № 3. С. 239–244.
20. *Скобелев В. В.* Об автоматах на полиномиально-параметризованном многообразии над конечным кольцом // Труды ИПММ НАНУ. 2012. Т. 25. С. 185–195.
21. *Скобелев В. В.* О гомоморфизмах автоматов на многообразиях над кольцом // Доповіді НАНУ. 2013. № 1. С. 42–46.
22. *Скобелєв В. В.* Аналіз автоматів, які визначено на еліптичних кривих // Вісник Київського університету. Сер. : фіз.-мат. науки. 2012. № 1. С. 223–230.
23. *Скобелев В. В.* Анализ семейств хэш-функций, определяемых автоматами над конечным кольцом // Кибернетика и системный анализ. 2013. № 2. С. 46–55.

Automata on Algebraic Structures

V. V. Skobelev

Institute of Applied Mathematics and Mechanics, National Academy of Sciences of Ukraine, Ukraine, 83114, Donetsk, R. Luxemburg st., 74, vv_skobelev@iamm.ac.donetsk.ua

A survey of results obtained in investigations of automata determined over finite algebraic structures. The objects of research are automata over some finite ring, automata determined in terms of ideals, automata over varieties, and families of hash-functions determined by automata without output function. Computational security, complexity of simulation and homomorphisms of investigated automata are characterized.

Key words: rings, automata, identification, computational security.

References

1. Gill A. *Lineinye posledovatel'nostnye mashiny* [Linear sequential machines]. Moscow, Nauka, 1974. 298 p. (in Russian).
2. Faradgev R. G. *Lineinye posledovatel'nostnye mashiny* [Linear sequential machines]. Moscow, Sovetskoje Radio, 1975, 248 p. (in Russian).
3. Agibalov G. P. Recognition of operators realized by linear autonomous automata. *Izv. AN USSR. Tech. Cybernetika*, 1970, no. 3, pp. 99–108 (in Russian).
4. Agibalov G. P., Jufit Ya.G. O prostykh eksperimentakh dlia lineinykh initsial'nykh avtomatov [On simple experiments for linear initial automata]. *Avtomatica i vychisliteljnaja technika*, 1972, no. 2, pp. 17–19 (in Russian).
5. Speranskij D. V. *Eksperimenty s lineinymi i bilineinymi konechnymi avtomatami* [Experiments with linear and bi-linear finite automata]. Saratov, Saratov. Univ. Press, 2004. 144 p. (in Russian).
6. Kurosh A.G. *Lektsii po obshchei algebre* [Lectures in general algebra]. Moscow, Nauka, 1973, 400 p. (in Russian).
7. Skobelev V. V., Skobelev V. G. Analiz shifrsistem [Analysis of ciphersystems]. Donetsk, IAMM NASU, 2009, 479 p. (in Russian).
8. Skobelev V. V., Glazunov N. M., Skobelev V. G. *Mnogoobraziia nad kol'tsami. Teoriia i prilozhenie* [Varieties over rings. Theory and applications]. Donetsk, IAMM NASU, 2011, 323 p. (in Russian).
9. Skobelev V. V., Skobelev V. G. Analysis of nonlinear automata with lag 2 over finite ring. *Prikladnaja discretnaja matematika*, 2010, no. 1, pp. 68–85 (in Russian).
10. Skobelev V. V. Complexity of identification of nonlinear 1-dimensional automata with lag 2 over finite ring. *Computernaja mathematika*, 2011, vol. 2, pp. 81–89 (in Russian).
11. Kuznetsov S. P. *Dinamicheskii khaos* [Dynamical chaos]. Moscow, Fizmatlit, 2001. 296 p. (in Russian).
12. Skobelev V. V., Skobelev V. G. On the complexity of analysis of automata over a finite ring. *Cybernet. Systems Anal.*, 2010, vol. 46, no. 4, pp. 533–545.
13. Skobelev V. V. On systems of polynomial equations over finite rings. *Naukovi zapysky NaU-KMA. Ser. Computerny nauky*, 2012, vol. 138, pp. 15–19.
14. Skobelev V. V. On subsets of automata over finite ring determined via terms of ideals. *Visn., Ser. Fiz.-Mat. Nauky, Kyïv. Univ. Im. Tarasa Shevchenka*, 2011, no. 3, pp. 212–218 (in Ukrainian).
15. Skobelev V. V. Simulation of automata over a finite ring by the automata with finite memory. *J. of Automation and Information Sci.* 2012, vol. 44, no. 5, pp. 57–66.
16. Skobelev V. V. Analysis of the problem of recognition of automaton over some ring. *Dopov. Nats. Akad. Nauk Ukr., Mat., Pryr., Tekh. Nauky*, 2012, no. 9, pp. 29–35 (in Russian).
17. Skobelev V. V. On automata determined over varieties over some ring. *Tr. Inst. Prikl. Mat. Mekh.*, 2012, vol. 24, pp. 190–201 (in Russian).
18. Skobelev V. V. Automata over vatieties with some algebra. *Visn., Ser. Fiz.-Mat. Nauky, Kyïv. Univ. Im. Tarasa Shevchenka*, 2012, no 2, pp. 234–238 (in Ukrainian).
19. Skobelev V. V. Analysis of automata determined over parametric varieties over an associative ring. *Visn., Ser. Fiz.-Mat. Nauky, Kyïv. Univ. Im. Tarasa Shevchenka*, 2012, no. 3, pp. 239–244.
20. Skobelev V. V. On automata determined over polynomially parametric varieties over some finite ring. *Tr. Inst. Prikl. Mat. Mekh.* 2012, vol. 25, pp. 185–195 (in Russian).
21. Skobelev V. V. On homomorphisms of automata over varieties over some ring. *Dopov. Nats. Akad. Nauk Ukr., Mat., Pryr., Tekh. Nauky*, 2013, no. 1, pp. 42–46 (in Russian).
22. Skobelev V. V. Analysis of automata determined over elliptic curves. *Visn., Ser. Fiz.-Mat. Nauky, Kyïv. Univ. Im. Tarasa Shevchenka*, 2012, no. 1, pp. 223–230 (in Ukrainian).
23. Skobelev V. V. Analysis of families of hash functions defined by automata over a finite ring. *Cybernet. Systems Anal.*, 2013, vol. 49, no. 2, pp. 209–216.

УДК 62-50

ДИАГНОСТИЧЕСКИЕ ЭКСПЕРИМЕНТЫ С НЕЧЕТКИМИ АВТОМАТАМИ

Д. В. Сперанский

Доктор технических наук, профессор кафедры высшей и прикладной математики, Московский государственный университет путей сообщения (МИИТ), Speranskiy.DV@gmail.com

Для нечетких автоматов введено понятие обобщенной диагностической последовательности. Предложен метод ее построения. Метод базируется на использовании конструкции диагностического дерева. Установлено, что задача синтеза обобщенной диагностической последовательности является многокритериальной задачей оптимизации.

Ключевые слова: нечеткий автомат, диагностический эксперимент.