УДК 512.7+519.7+681.3

©2012. **В. Г. Скобелев**

АНАЛИЗ АВТОМАТНО-АЛГЕБРАИЧЕСКИХ МОДЕЛЕЙ

Рассмотрены методы анализа автоматно-алгебраических моделей над конечным ассоциативно-коммутативным кольцом с единицей с позиции их возможного применения при решении задач защиты информации. Охарактеризована сложность решения задач идентификации (параметрической и начального состояния) и анализа множества неподвижных точек.

Ключевые слова: *кольца, автоматы, управляемые операции, идентификация, неподвижные точки.*

1. Введение. Основы теории конечных автоматов (в дальнейшем, для краткости, автоматов) были заложены в середине XX века. Ее предназначение – анализ вычислений, осуществляемых на компьютерах в реальное время на конечной памяти. При этом, автомат рассматривался либо как преобразователь информации (модели Мили и Мура, а также их варианты, связанные с представлением функционирования автомата во времени), либо как распознаватель языка (настроенные автоматы и источники). В 1961 году фундаментальные работы [1, 2] В.М. Глушкова заложили основу для формирования алгебраической теории автоматов – нового направления теории автоматов. Именно это направление, связанное с анализом структуры входной полугруппы автомата, дало возможность выделить ряд фундаментальных положений теории автоматов, в том числе была создана теория Крона-Роудза декомпозиции автоматов, нашедшая нетривиальное применение в общей теории систем [3]. Результаты алгебраической теории автоматов достаточно полно представлены в [4, 5].

В 90-х годах XX века во всем мире начинают достаточно интенсивно исследоваться математические основы криптологии. Эти исследования привели к переосмыслению проблематики теории булевых функций [6], а также теории автоматов, в том числе алгебраической теории автоматов. Для последней существенными оказались следующие три обстоятельства. Во-первых, в кандидатах на стандарты современных шифров применяются вычисления в конечных полях и кольцах вычетов. Во-вторых, при использовании хаотических динамических систем при построении математических моделей шифров для того, чтобы нивелировать ошибки округления, естественно перейти к вычислениям в конечных алгебраических системах. В-третьих, успешное применение эллиптических кривых над конечными полями при решении задач защиты информации (прежде всего, в формировании электронной подписи) привело к формированию эллиптической криптографии – одного из перспективных направлений современной криптографии [7-11]. Указанные обстоятельства обосновывают актуальность исследования преобразований конечных алгебраических систем, осуществляемых автоматно-алгебраическими моделями, заданными системами уравнений над этими алгебраических системами. В качестве базовой алгебраической си-

стемы естественно выбрать конечное кольцо. Такой выбор обусловлен следующими двумя обстоятельствами. Во-первых, поле является специальным случаем кольца, так что все полученные для кольца результаты в случае поля могут быть только усилены. Во-вторых, наличие в кольце делителей нуля заведомо вносит необходимость осуществить связанный с ними полный перебор вариантов при решении систем уравнений над кольцом, что существенно усложняет анализ автоматно-алгебраических моделей, заданных системами уравнений. Таким образом, исследование автоматно-алгебраических моделей, заданных системами уравнений над конечными кольцами, формирует новый раздел алгебраической теории автоматов, имеющий потенциальные приложения в процессе решения задач защиты информации.

Рассмотрим методы исследования таких автоматно-алгебраических моделей.

2. Автоматы над кольцом. Известно, что простейшими являются автономные автоматы (т.е. имеющие однобуквенный входной алфавит). Такие автоматы часто используются в роли математических моделей генераторов псевдослучайных последовательностей. В этом случае автономные автоматы представляются, как правило, линейными рекуррентными последовательностями (методы математического анализа нелинейных рекуррентных последовательностей, за исключением статистических методов, практически отсутствуют), а реализуются на основе регистров сдвига с линейными обратными связями. Свойства линейных рекуррентных последовательностей над конечными полями были достаточно глубоко исследованы в 3-й четверти XX века (см., напр., [12, 13]). При этом, в [14] была решена задача идентификации начального состояния линейного автономного автомата над конечным полем. Исследование линейных рекуррентных последовательностей над конечными кольцами началось (во многом, в связи с разработкой методов решения задач криптографии) только в последнее десятилетие XX века. Основные результаты в этом направлении представлены в [15, 16].

Аналогичная ситуация сложилась и с не автономными автоматами (т.е. имеющими многобуквенный входной алфавит) над конечными полями. Основы теории таких линейных автоматов разработаны в 3-й четверти XX века [17-19]. В [20] предпринята одна из первых попыток исследования нелинейных автоматов над конечными полями, где нелинейность состоит в том, что функции переходов и выходов автомата – билинейные формы компонент векторов состояния и входного символа. Значительное внимание было уделено экспериментам, предназначенным для идентификации начального или финального состояния автомата. Так как такие автоматы не являются обратимыми, то они могут иметь весьма ограниченные применения при решении задач защиты информации. В [21, 22] исследованы автоматы над конечным кольцом $\mathcal{K} = (K, +, \cdot)$ с учетом возможности использования обратимых автоматов в качестве математических моделей поточных шифров. В качестве общих моделей были выбраны множества $\mathcal{A}_{n,1}$ автоматов Мили и $\mathcal{A}_{n,2}$ автоматов Мура, заданных, соответственно, системами уравнений

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

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

где $\mathbf{f}_i : K^n \to K^n$ $(i = 1, \ldots, 4)$, а $\mathbf{q}_t, \mathbf{x}_t, \mathbf{y}_t \in K^n$ есть, соответственно, состояние, входной и выходной символ в момент t. Полученные для этих моделей результаты были проработаны в деталях для:

1) подмножеств $\widetilde{\mathcal{A}}_{n,1} \subset \mathcal{A}_{n,1}$ и $\widetilde{\mathcal{A}}_{n,2} \subset \mathcal{A}_{n,2}$ автоматов, заданных, соответственно, системами уравнений

$$\begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t\mathbf{q}_t^T\mathbf{b} + C\mathbf{q}_t + \mathbf{d} + E\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = G\mathbf{q}_t + F\mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+),$$

$$\begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t\mathbf{q}_t^T\mathbf{b} + C\mathbf{q}_t + \mathbf{d} + E\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = G\mathbf{q}_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+),$$

где A, C, E, G, F – фиксированные $n \times n$-матрицы над кольцом $\mathcal{K}$, а $\mathbf{b}, \mathbf{d} \in K^n$ – фиксированные векторы;

2) подмножеств $\widetilde{\mathcal{A}}_{n,3} \subset \mathcal{A}_{n,1}$ и $\widetilde{\mathcal{A}}_{n,4} \subset \mathcal{A}_{n,2}$ обратимых автоматов, предназначенных для эффективного представления над кольцом $\mathcal{K}$ аналогов хаотических динамических систем, и заданных, соответственно, системами уравнений

$$\begin{cases} q_{t+1}^{(i)} = \mathbf{q}_t^T A_i \mathbf{q}_t + \mathbf{c}_i\mathbf{q}_t + d_i + \alpha_i e_i x_{t+1}^{(i)} \quad (i \in \mathbb{N}_n) \\ y_{t+1}^{(i)} = g_i q_t^{(i)} + f_i x_{t+1}^{(i)} \quad (i \in \mathbb{N}_r) \end{cases} \quad (t \in \mathbb{Z}_+),$$

$$\begin{cases} q_{t+1}^{(i)} = \mathbf{q}_t^T A_i \mathbf{q}_t + \mathbf{c}_i\mathbf{q}_t + d_i + \alpha_i e_i x_{t+1}^{(i)} \quad (i \in \mathbb{N}_n) \\ y_{t+1}^{(i)} = g_i q_t^{(i)} \quad (i \in \mathbb{N}_r) \end{cases} \quad (t \in \mathbb{Z}_+),$$

где $r \le n$, $\alpha_i = 1$, если $i \in \mathbb{N}_r$ и $\alpha_i = 0$, если $i \in \mathbb{N}_n \backslash \mathbb{N}_r$, A_i $(i \in \mathbb{N}_n)$ – фиксированные $n \times n$-матрицы над кольцом $\mathcal{K}$, $\mathbf{c}_i \in K^n$ $(i \in \mathbb{N}_n)$ – фиксированные векторы, а d_i, e_i $(i \in \mathbb{N}_n)$ и g_i, f_i $(i \in \mathbb{N}_r)$ – фиксированные элементы кольца $\mathcal{K}$, причем обратимыми элементами являются f_i $(i \in \mathbb{N}_r)$, а также e_i, g_i $(i \in \mathbb{N}_r)$ для автомата $M \in \widetilde{\mathcal{A}}_{n,4}$;

3) подмножеств $\widetilde{\mathcal{A}}_{n,5} \subset \widetilde{\mathcal{A}}_{n,1}$ и $\widetilde{\mathcal{A}}_{n,6} \subset \widetilde{\mathcal{A}}_{n,2}$ линейных автоматов, заданных, соответственно, системами уравнений

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

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

где A, B, C, D – фиксированные $n \times n$-матрицы над кольцом $\mathcal{K}$.

Для любого обратимого автомата M, перечисленного выше вида, пара инициальных автоматов $((M, \mathbf{q}_0), (M^{-1}, \mathbf{q}_0))$ может рассматриваться как математическая

модель поточного шифра, для которого параметры, определяющие автомат, являются секретным ключом средней длительности, а начальное состояние $\mathbf{q}_0$ – секретным сеансовым ключом. Поэтому сложность решения задач идентификации (параметрической и начального состояния), а также анализа неподвижных точек автоматных отображений, является теоретическим обоснованием вычислительной стойкости соответствующих шифров. Под действием любого входного слова инициальные автоматы $(M, \mathbf{q}_0)$ и $(M^{-1}, \mathbf{q}_0)$ движутся в пространстве состояний по одной и той же траектории в одном и том же направлении. Это обстоятельство дает возможность осуществлять дополнительный контроль ряда ошибок, возникающих именно в процессе передачи информации. Отметим, что классы эквивалентных состояний автомата $M \in \widetilde{\mathcal{A}}_{n,i} \cup \widetilde{\mathcal{A}}_{n,i+1}$ $(i = 1, 5)$ имеют достаточно сложную структуру. Отсюда вытекает, что минимизация автомата однозначно приводит к существенному усложнению системы уравнений, определяющей автомат.

Анализ задачи параметрической идентификации автомата $M \in \widetilde{\mathcal{A}}_{n,i} \cup \widetilde{\mathcal{A}}_{n,i+1}$ $(i = 1, 3, 5)$ дал возможность выделить параметры, идентификация которых осуществляется достаточно легко, а также параметры, идентификация которых сводится к поиску множеств решений систем нелинейных уравнений над кольцом $\mathcal{K}$, формируемых в процессе кратных экспериментов с исследуемым автоматом. Показано, что переход к обратимым автоматам не упрощает решение задачи параметрической идентификации. Таким образом, для шифра, определяемого обратимым автоматом, выделено множество параметров, которые целесообразно выбирать в качестве секретного ключа средней длительности, а также выделены параметры, обеспечению секретности которых нужно уделить особое внимание.

Аналогичным образом, анализ задачи идентификации начального состояния автомата $M \in \widetilde{\mathcal{A}}_{n,i} \cup \widetilde{\mathcal{A}}_{n,i+1}$ $(i = 1, 3, 5)$ дал возможность выделить множества параметров, для которых решение может быть получено достаточно легко, а также множества параметров, для которых решение сводится к поиску множеств решений систем уравнений над кольцом $\mathcal{K}$, формируемых в процессе кратных экспериментов с исследуемым автоматом. Показано, что переход к обратимым автоматам не упрощает решение задачи идентификации начального состояния.

Анализ множества неподвижных точек отображения входной полугруппы в выходную полугруппу, реализуемого инициальным автоматом $M \in \widetilde{\mathcal{A}}_{n,i} \cup \widetilde{\mathcal{A}}_{n,i+1}$ $(i = 1, 3, 5)$, дал возможность установить условия, при которых это множество пусто, а также условия, когда это множество бесконечное. Это, в свою очередь, дает возможность выделить множества обратимых автоматов, которые целесообразно использовать при построении соответствующих поточных шифров.

Следует также отметить, что система уравнений, предназначенная для анализа вариации поведения автомата $M \in \widetilde{\mathcal{A}}_{n,i} \cup \widetilde{\mathcal{A}}_{n,i+1}$ $(i = 1, 3, 5)$ при вариации его параметров и/или начального состояния значительно сложнее системы уравнений, определяющей исследуемый автомат. Это обстоятельство делает весьма призрачной возможность разработки для шифров, определяемых обратимыми автоматами, методов криптоанализа, аналогичных дифференциальному и интегральному криптоанализу для DES-подобных алгоритмов блочного шифрования.

3. Общая модель автоматного преобразователя информации. Анализ представленных выше результатов, а также анализ управляемых перестановочных и подстановочных операций [6, 21, 23] показывает, что исследование достаточно широкого класса задач криптографии укладывается в рамки следующей концептуальной модели $\mathcal{M} = (F, \mathcal{A}_{\mathbf{a}})$ дискретного преобразователя информации, рассмотренной в [24].

Пусть S_1 и S_2 – такие конечные множества,что $|S_1| \leq |S_2|$. Зафиксируем конечное семейство инъекций $F = \{f_i\}_{i \in \mathbf{N}_k}$ множества S_1 в множество S_2, а также алгоритм $\mathcal{A}_{\mathbf{a}}$, генерирующий псевдослучайную последовательность элементов множества $\mathbf{N}_k$, где $\mathbf{a}$ – вектор параметров, предназначенных для инициализации алгоритма $\mathcal{A}$. Преобразование последовательности $s_1, \ldots, s_l$ элементов множества S_1 состоит в ее замене последовательностью $f_{i_1}(s_1), \ldots, f_{i_l}(s_l)$, где $i_1, \ldots, i_l$ – последовательность, генерируемая алгоритмом $\mathcal{A}$ при его инициализации $\mathbf{a}$.

Так как модель $\mathcal{M} = (F, \mathcal{A}_{\mathbf{a}})$ предназначена для быстрого преобразования информации, то естественно потребовать, чтобы семейство инъекций $F = \{f_i\}_{i \in \mathbf{N}_k}$ удовлетворяло следующим трем требованиям: 1) семейство F представлено в неявном виде; 2) построение каждой инъекции $f_i \in F$ – легкая задача; 3) каждая инъекция $f_i \in F$ – легко вычислимое отображение.

Отметим следующие результаты, полученные в рамках рассмотренной модели $\mathcal{M} = (F, \mathcal{A}_{\mathbf{a}})$. В [25] на основе регулярного графа со специальной структурой построено и исследовано семейство попарно различных перестановок F, имеющее субэкспоненциальную мощность. В [26] построены и исследованы семейства перестановок F, получаемых в результате всевозможных вычеркиваний элементов фиксированной суперпозиции перестановок, предназначенные для преобразования информационного вектора. Выделены семейства перестановок субэкспоненциальной мощности, а также семейства перестановок, для которых почти все точки не являются неподвижными точками. В [27] построен и исследован класс семейств легко вычислимых разложимых (по компонентам) подстановок F над конечным кольцом, предназначенных для преобразования информационного вектора (этому классу, в частности, принадлежат некоторые семейства подстановок, которые могут быть использованы для построения поточных шифров, управляемых фракталом). Показано, что поиск подсемейства, обладающего фиксированной неподвижной точкой, сводится к решению системы многостепенных диофантовых уравнений с последующей проверкой разрешимости задач поиска дискретного логарифма. Также выделены параметры, определяющие семейство подстановок, идентификация которых сводится к решению задач поиска дискретного логарифма.

4. Заключение. В работе кратко рассмотрены методы анализа автоматно-алгебраических моделей над конечным ассоциативно-коммутативным кольцом с единицей с позиции их возможного применения при решении задач защиты информации. Высокая сложность решения задачи параметрической идентификации автомата $M \in \widetilde{\mathcal{A}}_{n,i} \cup \widetilde{\mathcal{A}}_{n,i+1}$ $(i = 1, 3, 5)$ показывает целесообразность разработки методов построения алгоритмов, моделирующих поведение исследуемого автомата с заданной точностью. Первые попытки решения этой задачи предприняты в [22, 28-31].

Алгоритмический анализ указанной задачи представляет возможное направление исследований. Другое направление связано с исследованием автоматов, на которые наложены ограничения в терминах структуры кольца. Отметим, что в [32] исследованы множества автоматов, на функции переходов и выходов которых наложены ограничения в терминах идеалов, а в [33] рассмотрены автоматы, определенные на эллиптических кривых над конечным полем.

1. *Глушков В.М.* Абстрактная теория автоматов // Успехи мат. наук. – 1961. – № 5. – С. 3-62.
2. *Глушков В.М.* Абстрактные автоматы и разбиение свободных полугрупп // Докл. АН СССР. – 1961. – № 4. – С. 765-768.
3. *Месарович М., Такахара Я.* Общая теория систем: математические основы. – М.: Мир, 1978. – 311 с.
4. *Eilenberg S.* Automata, languages,and macines. Vol. A. – NY.: Academic Press, 1974. – 451 p.
5. *Eilenberg S.* Automata, languages,and macines. Vol. B. – NY.: Academic Press, 1976. – 387 p.
6. *Логачев О.А., Сальников А.А., Ященко В.В.* Булевы функции в теории кодирования и криптологии. – М.: МЦНМО, 2004. – 470 с.
7. *Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А.* Алгоритмические основы эллиптической криптографии. – М.: МЭИ, 2000. – 100 с.
8. *Коблиц Н.* Курс теории чисел и криптография.–М.: ТВП, 2001. – 262 с.
9. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – 328 с.
10. *Бессалов А.В., Телиженко А.Б.* Криптосистемы на эллиптических кривых. – Киев: Политехника, 2004. – 223 с.
11. *Маховенко Е.Б.* Теоретико-числовые методы в криптографии.–М.: Гелиос АРВ, 2006.–320 с.
12. *Элспас Б.* Теория автономных линейных последовательных сетей // Кибернетический сборник. Вып. 7. – М.: Мир, 1963. – С. 90-128.
13. *Zierler N., Mills W.* Products of linear recurring sequences // Journal of Algebra, 1973. – № 1. – P. 147-157.
14. *Агибалов Г.П.* Распознавание операторов, реализуемых в линейных автономных автоматах // Известия АН СССР. Техническая кибернетика. – 1970. – № 3. – С. 99-108.
15. *Кузьмин А.С., Куракин В.Л., Нечаев А.А.* Псевдослучайные и полилинейные последовательности // Труды по дискретной математике. – Т.1. – М.: ТВП, 1997. – С. 139-202.
16. *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.: ТВП, 1998. – С. 191-222.
17. *Медведев И.Л., Фараджев Р.Г., Чуйко А.С.* Применение модулярных линейных уравнений для описания линейных последовательностных машин // АиТ. – 1971. – № 8. – С. 73-81.
18. *Гилл А.* Линейные последовательностные машины. – М.: Наука, 1974. – 298 с.
19. *Фараджев Р.Г.* Линейные последовательностные машины. – М.: Сов. Радио, 1975. – 248 с.
20. *Сперанский Д.В.* Эксперименты с линейными и билинейными конечными автоматами. – Саратов: СГУ, 2004. – 144 с.
21. *Скобелев В.В., Скобелев В.Г.* Анализ шифрсистем. – Донецк: ИПММ НАНУ, 2009. – 479 с.
22. *Скобелев В.В., Глазунов Н.М., Скобелев В.Г.* Многообразия над кольцами. Теория и приложения. – Донецк: ИПММ НАНУ, 2011. – 323 с.
23. *Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В.* Криптография. Скоростные шифры. – СПб.: БХВ-Петербург, 2002. – 496 с.
24. *Скобелев В.Г.* Про один клас автоматно-алгебраїчних моделей дискретних перетворювачів інформації // Вісник Київського університету. Серія фізико-математичні науки. – 2011. – Вип. 2. – С. 151-154.
25. *Скобелев В.Г.* Оцінка кількості гамільтонових циклів у регулярних графах спеціального типу // Вісник Київського університету. Серія фізико-математичні науки. – 2010. – Вип. 2. – С. 169-171.
26. *Скобелев В.Г.* Об одном семействе суперпозиций подстановок // Компьютерная математика. – 2011. – № 1. – С. 116-121.

27. *Скобелев В.Г., Зайцева Э.Е.* Анализ класса легко вычислимых перестановок // Кибернетика и системный анализ. – 2008. – № 5. – С. 12-24.
28. *Скобелев В.В., Скобелев В.Г.* Анализ нелинейных автоматов с лагом 2 над конечным кольцом // Прикладная дискретная математика. – 2010. – № 1. – С. 68-85.
29. *Скобелев В.В., Скобелев В.Г.* О сложности анализа автоматов над конечным кольцом // Кибернетика и системный анализ. – 2010. – № 4. – С. 17-30.
30. *Скобелев В.В.* Сложность идентификации нелинейных одномерных автоматов с лагом 2 над конечным кольцом // Компьютерная математика. – 2011. – Вып. 2. – С. 81-89.
31. *Скобелев В.В.* О построении имитационной модели нелинейного обратимого автомата над конечным кольцом // Матеріали XVIII Міжнародної конференції з автоматичного управління «AUTOMATICS-2011» (м. Львів, 28-30 вересня 2011р.). – Львів: Видавництво Львівської політехніки. – 2011. – С. 289-290.
32. *Скобелєв В.В.* Про множини автоматів над скінченним кільцем, які визначено у термінах ідеалів // Вісник Київського університету. Серія фізико-математичні науки. – 2011. – Вип. 3. – С. 212-218.
33. *Skobelev V.V.* On automata over elliptic curves // Proceedings of the VI International Conference on Computer Science and Information Technologies (м. Львів, 16-19 листопада 2011р.). – Львів: Видавництво «Вежа і Ко». – 2011. – С. 29.

V. G. Skobelev

Analysis of automata-algebraic models.

Methods of analysis of automata-algebraic models over finite associative-commutative ring are presented considering their possible applications for solving information-protection problems. Complexity of solving of problems of identification (parametric and initial state) and of fixed-points analysis is characterized.

Keywords: *rings, automata, controlled operations, identification, fixed points.*

В. Г. Скобелєв

Аналіз автоматно-алгебраїчних моделей.

Розглянуто методи аналізу автоматно-алгебраїчних моделей над скінченним асоціативно-комутативним кільцем. Охарактеризовано складність розв'язання задач ідентифікації (параметричної і початкового стану) і аналізу множин нерухомих точок.

Ключові слова: *кільця, автомати, керовані операції, ідентифікація, нерухомі точки.*

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

Получено 31.05.12