Полугруппы и группы автоматов

Алёшин С. В. (Москва, МГУ им. М. В. Ломоносова)

Связь теории автоматов с теорией полугрупп и групп проявилась сразу после первых работ, посвящённых автоматам. Не случайно один из первых сборников (под редакцией М. А. Арбиба) [6] получил название «Алгебраическая теория автоматов, языков и полугрупп».

Автомат можно рассматривать как носитель «внутренней» полугруппы подстановок на множестве состояний. В то же время автомат — это отображение множества входных слов (последовательностей) в множество выходных слов. Последовательное соединение автоматов даёт суперпозицию таких отображений, что приводит к возникновению различных полугрупп автоматных отображений. В разных задачах теории автоматов и алгебры свойства внутренних полугрупп автоматов и свойства полугрупп автоматных отображений стали предметом изучения и сильным инструментом для решения этих задач.

Мы рассматриваем здесь только конечные автоматы (Мили). Автомат — это пятёрка (A, Q, B, φ, ψ), где A, B, Q — конечные множества, называемые, соответственно, входным, выходным алфавитом и алфавитом состояний, а $\varphi\colon A \times Q \to Q$ — функция переходов, $\psi\colon A \times Q \to B$ — функция выходов.

Из определения сразу следует возможность смотреть на автомат как на многоосновную алгебру с бинарными операциями φ, ψ, которые связывают своим действием три конечные множества A, Q, B. Однако, более важным оказалось рассмотрение, наряду с этой алгеброй, отображения множества слов во входном алфавите A^* (входной полугруппы) во множество слов в выходном алфавите B^*, которое реализуется автоматом.

Такой подход утвердился после работ [2], [3], [6], и взгляд на автомат одновременно как на алгебру и как на функцию оказался плодотворным при рассмотрении самых разных объектов, связанных с автоматами.

A^* является свободной полугруппой с множеством образующих A. С автоматом (A, Q, B, φ, ψ) с начальным состоянием $q_0 \in Q$ свяжем отображение $F_{q_0}(x)$ так, что $F_{q_0}(x) = \overline{\psi}(q_0, x)$, $x \in A^*$. Здесь дей-

ствие функции выходов ψ и функции переходов φ распространено на множество A^* по правилу

$$\overline{\psi}(q_0, \alpha a) = \overline{\psi}(q_0, \alpha)\, \psi\left(\overline{\varphi}(q_0, \alpha), a\right), \;\; \overline{\varphi}(q_0, \alpha a) = \varphi\left(\varphi(q_0, \alpha), a\right).$$

Определим отношение эквивалентности $\equiv$ на множестве слов A^*

$$\alpha_1 \equiv \alpha_2 \quad \Leftrightarrow \quad \forall\, \alpha,\, \beta \quad \psi(\alpha\, \alpha_1\, \beta) = \psi(\alpha\, \alpha_2\, \beta).$$

Это отношение является конгруенцией на A^* и определяет конечную полугруппу S_ψ как образ A^* при естественном гомоморфизме. Полученную полугруппу называют полугруппой автоматного отображения F_{q_0}.

Ясно, что строение полугруппы S_ψ зависит от выбора функции выходов и, если менять ψ, сохраняя остальные параметры автомата, полугруппа также, вообще говоря, будет меняться.

Можно определить еще одну полугруппу, рассматривая только «переходную систему» автомата $\mathcal{A}$, то есть тройку (A, Q, φ). Для каждого слова $\alpha \in A^*$ определим отображение

$$\mathcal{J}_\alpha \colon Q \to Q, \quad \varphi_\alpha(q) = \varphi(q, \alpha).$$

Таким образом на A^* определено отношение эквивалентности, которое является конгруентностью. Каждая буква входного алфавита $a \in A$ задает отображение $\varphi_\alpha \colon Q \to Q$ и может рассматриваться как образующая в конечной полугруппе $P_\mathcal{A}$ отображений на Q, которую будем называть внутренней полугруппой автомата $\mathcal{A}$. Если все состояния автомата достижимы из начального и попарно отличимы, то абстрактная полугруппа, изоморфная внутренней полугруппе $P_\mathcal{A}$, является гомоморфным образом полугруппы отображения S_ψ.

Одной из первых задач теории автоматов стала задача декомпозиции, то есть построение автомата из компонент, которые в каком-то смысле были бы проще исходного автомата [6]. Обычно различают компоненты двух видов — автоматы без памяти, операторы, у каждого такого автомата только одно состояние, и автоматы, с числом отличимых состояний больше единицы. Внутренняя полугруппа оператора тривиальна — это единичная группа. Полугруппа отображения оператора более сложная — из определения видно,что ею

будет полугруппа нулей, множество элементов полугруппы совпадает с множеством букв входного алфавита. Удобно рассматривать не только абстрактные алфавиты, но и их представления в виде декартовых произведений. В этом случае буквы алфавита представляются набором, например, из 0 и 1, что позволяет использовать операторы и автоматы с многими входами и выходами.

Связывая с автоматами соответствующие полугруппы, можно воспользоваться традиционной техникой разложения полугрупп (групп) и строить на этой основе теорию декомпозиции автоматов.

В традиционной схеме декомпозиции используют так называемые стандартные групповые автоматы — для заданной группы G рассматривают автомат $(G, G, G, \varphi_G, \psi_G)$, у которого входной, выходной алфавиты и множество состояний совпадают с множеством элементов группы. Функция переходов и выходов — это «умножение» в группе, начальное состояние — «единица» группы: $\varphi_G(g, g') = \psi_G(g, g') = g \cdot g'$. Для разложения группового автомата используют автомат нормального делителя, автомат факторгруппы и соединяют их в параллельно-последовательной схеме с помощью операторов.

Подобные приемы декомпозиции автоматов, которые прямо заимствованы из соответствующих конструкций для групп и полугрупп, наряду с силой, демонстрируют и определенные слабые стороны, поскольку не учитывают ряд важных требований, предъявляемых к реальным автоматам.

В частности, всякая реализация автомата приводит к некоторому кодированию алфавитов состояний входов и выходов. Разные кодирования определяют разные сложности, при этом важное значение имеет число входных и выходных каналов, число каналов связи между компонентами, соотношение сложности компонент и связей между ними и т. д.

Одна и та же абстрактная группа может быть представлена с помощью автоматов различной сложности. Так например, группа S_n может быть представлена автоматом с $n!$ состояниями и входным алфавитом той же мощности, а может быть представлена автоматом с n состояниями и одним бинарным входом.

В приведённом выше примере декомпозиции были использованы явно избыточные средства. Однако можно заметить, что некоторая

информация оказывается необходимой и присутствует в любой декомпозиции.

В алгебраической теории разложений (расширений) групп и полугрупп роль неразложимых элементов играют простые группы. Как было показано в [6] в декомпозициях автоматов простые группы сохраняют особую роль «неисчезающих» элементов, если не используется операция обратной связи.

Абстрактная полугруппа H называется делителем автомата $\mathcal{A}$, если H является гомоморфным образом внутренней полугруппы $P_{\mathcal{A}}$. Оказывается, если H — простая группа, являющаяся делителем $\mathcal{A}$, то в любой декомпозиции $\mathcal{A}$ без обратных связей найдётся компонента $\mathcal{A}'$ такая, что H является делителем $\mathcal{A}'$.

Этот факт был установлен благодаря обнаруженной в [6] связи между суперпозициями автоматов и операцией сплетения полугрупп. Операция сплетения полугрупп подстановок имеет отчетливо выраженный «автоматный» характер, и элемент сплетения можно описать как подстановку, реализуемую некоторой «двухтактной машиной».

Пусть H — полугруппа подстановок на множестве M и G — полугруппа подстановок на множестве N. Через F обозначим множество отображений из M в полугруппу N. Сплетением полугрупп подстановок H и G (обозначается $H \int G$) называется полугруппа W подстановок на множестве $M \times N$ такая, что каждая подстановка из W определяется некоторой парой

$$w = (h, f), \quad h \in H,\ f \in F,$$

и действие W на $M \times N$ задается соотношением: для $(m, n) \in M \times N$

$$(h, f)[(m, n)] = (m', n'), \quad m' = h[m],\ n' = f(m)[n].$$

Здесь запись $p[k]$ обозначает результат действия элемента p полугруппы подстановок на элемент k.

Для произвольной пары $w \in W$, $w = (p, f)$ рассмотрим «машину» $L(w)$, на вход которой в начальный момент времени поступает некоторая буква $m \in M$, а во второй такт — буква $n \in N$. В первый момент $L(w)$ вычисляет значение $p[m]$ и под действием m переходит в такое состояние, в котором во второй момент вычисляется $f(m)[n]$.

Нетрудно видеть, что действие машины $L(w)$ на множестве $M \times N$ совпадает с действием элемента сплетения w из W.

Соединяя выход машины $L(w_1)$ с входом машины $L(w_2)$, получим машину $L(w)$ такую, что w есть произведение w_1 и w_2 в полугруппе $H \int G$.

С другой стороны, как было замечено в [6], если автомат получен в результате суперпозиции автоматов $\mathcal{A}$ и $\mathcal{L}$, то его полугруппа является подполугруппой сплетения полугрупп $P_{\mathcal{A}}$ и $P_{\mathcal{L}}$. В то же время важным является следующее свойство простых делителей, если D — простая группа и D делит сплетение $H \int G$, то D делит H или делит G. Из этих двух утверждений, очевидно, следует отмеченное выше свойство делителей автоматов.

Свойства полугрупп автоматов переносятся на композиции, и это дает возможность совместно рассматривать «внутренние» алгебры автоматов и алгебры, в которых автоматы являются элементами.

Если зафиксировать алфавит A и рассматривать множество (инициальных) автоматов вида $(A, Q, A, \varphi, \psi, q_0)$, у которых A является и входным и выходным алфавитом, то на этом множестве естественно определяется ассоциативная операция умножения — последовательное соединение автоматов. Полученная полугруппа AP_n автоматных отображений изучалась в [10] и обладает рядом интересных свойств. В AP_n любая порождающая система бесконечна и приводима, то есть содержит собственную подсистему, порождающую AP_n. Среди отображений, реализуемых автоматами из AP_n можно выделить взаимнооднозначные, которые образуют подгруппу полугруппы AP_n. Эту группу называют группой автоматных подстановок AS_n (мощность A). В группе можно найти большой набор подгрупп с интересными свойствами.

Уже первые работы [7] показали, что группа AS_n обладает уникальными свойствами и богатыми возможностями для представления как конечных, так и бесконечных групп. С помощью автоматных подстановок можно моделировать различные групповые конструкции. Работа [8] показала, что сплетения групп вкладываются в AS_n, а это, в свою очередь, открывало возможности для моделирования. Начиная с работ [11], [15] внимание многих исследователей было привле-

чено к двум «полярным» классам автоматных групп — класс периодических и класс свободных групп.

Оказалось, в AS_n содержатся конечнопорождённые бесконечные периодические подгруппы, что даёт серию примеров, решающих известную проблему Бернсайда. В многочисленных последующих работах [13], [14], [23] группы, описанные в [11] подробно исследовались, результат [11] передоказывался (подробный разбор этого проведён в [12]).

Интересно, что на возможную связь автоматов с проблемой Бернсайда указывал еще В. М. Глушков в работе [2]. Правда, В. М. Глушков связывал надежды с внутренней полугруппой автомата или с изучением конгруэнтностей на свободной (входной) полугруппе с нерегулярными (в смысле Клини) классами эквивалентности, а решение нашлось в алгебре, элементами которой являются автоматы.

Как уже сказано, первый пример группы автоматных подстановок, который решает «общую проблему Бернсайда» [12], был построен автором в 1972 году [11]. В дальнейшем появилось несколько работ, где использовались близкие конструкции. Авторы этих работ не скрывали (что естественно с точки зрения научной этики) связи своих работ с первой работой, показавшей возможность «автоматного» решения проблемы Бернсайда. Исключение составили работы Р. И. Григорчука, который странным образом продолжает удивлять научный мир легендой о своём приоритете в этом вопросе. Последнее его «упражнение» на эту тему — абзац в статье [26]. Хотя это коллективная работа (содержание которой не связано с Бернсайдовской проблематикой), можно уверенно говорить, что данный абзац вставлен туда Р. И. Григорчуком, которого остальные авторы, по-видимому, сочли авторитетом. Приведём этот текст полностью в оригинале и переводе.

«The methods used in [Ale 72] are typical for the theory of finite automata (in fact the provided proof was incorrect; the first correct proof appears in [Mer 83] as a combination of the results from [Gri 80] and [Mer 83], as well as in the third edition of the book [KM 82] and [KAP 85]).»

«Использованные в [Ale 72] методы типичны для теории конечных автоматов (в действительности, доказательство было неверным; первое верное доказательство представлено в [Mer 83] как комбина-

ция результатов из [Gri 80] и [Mer 83], а также в третьем издании книги [KM 82] и в [KAP 85]).»

Здесь [Ale 72], [Mer 83], [Gri 80], [KM 82], [KAP 85] — это, соответственно, статья С. В. Алёшина [11], статья Ю. И. Мерзлякова [27], статья Р. И. Григорчука [14], книга М. И. Каргаполова и Ю. И. Мерзлякова [12] и книга В. Б. Кудрявцева, С. В. Алёшина, А. С. Подколзина [5].

Как видно, нашему «герою» хочется быть если не автором, то хотя бы соавтором «первого верного доказательства», при этом взяв в соавторы выдающегося русского математика.

Ю. И. Мерзляков, один из авторов книги «Основы теории групп», которая долгие годы была и остаётся настольной книгой всех, кто интересуется теорией групп, увы, уже не может по достоинству ответить на попытки Р. И. Григорчука использовать авторитет его имени, и мы покажем, как на самом деле складывалась история публикаций Р. И. Григорчука.

В 1980 году, ещё до опубликования статьи Р. И. Григорчука в журнале «Функциональный анализ», его научный руководитель профессор А. Стёпин обратился ко мне с предложением послушать рассказ его аспиранта о новой работе по Бернсайдовской теме. В аудитории 16-го этажа Главного здания МГУ мы вместе с А. Стёпиным прослушали доклад Р. И. Григорчука. К тому времени язык представления автоматных отображений как отображений отрезков был достаточно известен в научном фольклоре, о чём сразу Р. И. Григорчуку было сказано, и ему был дан совет явно указать в предполагаемой публикации диаграммы соответствующих автоматов — порождающих группу. Это, по нашему мнению, существенно прояснило бы суть дела и упростило восприятие материала читателем. Совет этот Р. И. Григорчуком не был воспринят, и как выяснилось позднее, не случайно.

В 1982 году вышло третье издание книги М. И. Каргаполова и Ю. И. Мерзлякова, в которой появился раздел, написанный Ю. И. Мерзляковым, с подробным анализом связи примеров С. В. Алёшина и Р. И. Григорчука. Ю. И. Мерзляков приводит полное доказательство С. В. Алёшина, при этом форма изложения, система обозначений им выбиралась исходя из методических соображений —

так что, разумеется, текст книги не является копией оригинального текста статьи [11].

Приводя диаграммы автомата Алёшина и «автомата Григорчука», Ю. И. Мерзляков не без сарказма замечает, что переход от первого ко второму напоминает «выламывание адамова ребра», и увидев эти автоматы, «вы можете почувствовать операцию выламывания ребра почти физически».

В то же время, вторичность конструкции Р. И. Григорчука не может снизить интереса к ней, его доказательство короче и, на наш взгляд, математически изящнее, Р. И. Григорчуку удалось использовать тот факт, что теперь автоматы-образующие являются подавтоматами одного автомата. Это, в свою очередь, приводит к идее рассмотреть интересный класс групп, каждая из которых порождается подавтоматами соответствующего автомата.

Что же касается его претензий на первенство, то, возвращаясь к цитируемому выше тексту из [26], заметим, что Р. И. Григорчук выстроил последовательность «верных» решений так, что доказательство из книги [5] оказывается последним в этом ряду. Однако текст доказательства в этой книги — это копия текста из книги тех же авторов «Элементы теории автоматов», вышедшей в издательстве МГУ в 1978 году, когда Р. И. Григорчук ещё учился на мехмате, а книга имела достаточно широкое хождение на мехмате [4].

Другой вариант проблемы Бернсайда — «ослабленная проблема: конечно ли число конечных групп данного периода с заданным числом образующих элементов» — также нашла отражение в работах по теории конечных автоматов. Прежде всего, это работы В. И. Малыгина, в которых периодические группы выступают как внутренние группы автоматов [18]. Идея В. И. Малыгина заключалась в том, что при последовательном соединении автоматов, у которых внутренние полугруппы являются группами, внутренняя группа суперпозиции вкладывается в сплетение «соединяемых» групп. Если строить цепочку из автоматов так, чтобы в получаемых группах выполнялось тождество $x^n = 1$, то можно получать оценки размеров таких групп.

При рассмотрении последовательных соединений абелевых автоматов, то есть автоматов с коммутативными внутренними группами, возникали линейные пространства, элементами пространств [18] вы-

ступали наборы выходных функций автоматов, и изучение размерностей дало возможность получить оценки порядка бернсайдовских конечных групп.

Группа автоматных подстановок содержит большое количество подгрупп с разными свойствами. Задача полной классификации таких подгрупп далека от завершения. В работе [22] приводятся примеры бесконечных автоматных групп, дающие решение ряда известных проблем теории групп. В ней содержится полное доказательство теоремы Алёшина, а также показано, что группа Алёшина из [4] имеет подэкспоненциальную функцию роста (как известно, пример группы промежуточного роста был указан Р. И. Григорчуком в 1984 г. [15]). В статье [22] также строится пример автомата с тремя состояниями, который порождает группу без кручения, содержащую свободную полугруппу.

В основательной большой работе [26] были описаны группы, каждая из которых порождается подавтоматами какого-нибудь автомата с не более чем тремя состояниями. Даже при таком малом числе состояний порождающих автоматов оказалось 122 неизоморфных группы. Интересно, что среди них только автомат из [21] порождает свободную группу. Заметим, что требование, чтобы все образующие группы были подавтоматами одного автомата, является сильным ограничением, и группы, порождённые автоматами с тремя состояниями, описаны не все. Это показывает пример свободной группы, порождённой двумя автоматами с тремя состояниями, которые не являются подавтоматами одного автомата с тремя состояниями [20].

Ряд работ, начиная с работы [21], посвящены свободным группам автоматов. Полное доказательство того, что группа из [21] является свободной, получено в 2006 году в работе [28]. Интересно, что автоматы-образующие этой группы являются «дважды групповыми», то есть внутренние полугруппы у них и у обратных к ним автоматам являются группами.

Такие автоматы составляют малую долю всех автоматов, а множество всех таких автоматов образуют подгруппу группы автоматных подстановок. Эта подгруппа не только содержит свободную группу, но и, как оказалось, периодическая часть этой подгруппы содержит элементы всех порядков (конечно, вида 2^n) [29].

Проблема порядков элементов группы автоматных подстановок в общем случае не решена. В группе A_{S_2} каждый элемент может быть представлен как произведение автоматов, у которых только в одном состоянии реализуется нетривиальная подстановка на входном алфавите $\{0, 1\}$. В этой порождающей системе содержатся элементы второго и бесконечного порядков, в [30] построен пример автомата четвертого порядка. Наиболее интересным является вопрос о существовании алгоритма определения порядка автомата по его диаграмме.

Для некоторых подгрупп группы автоматных подстановок удается получить структурные теоремы. Например, группа линейных автоматов разрешима, она получается расширением бесконечной абелевой группы, каждый элемент в которой имеет порядок 2, с помощью бесконечной абелевой группы без кручения [4].

Группы автоматных отображений финитно аппроксимируемы. В частности, автоматной является группа кос [25]. А. В. Рожков в большом цикле работ изучал класс групп, который является естественным обобщением автоматных групп [23], [24], и показал, что в этом классе существенно расширяются возможности для моделирования различных групповых свойств.

Автоматное отображение входной свободной полугруппы в свободную полугруппу выходных слов при подходящем кодировании алфавитов превращается в детерминированную функцию многих переменных. Алгебры автоматных функций с различными наборами операций изучались, как правило, с позиций проблемы выразимости, когда для двух множеств функций M, N и заданного набора операций Ω требовалось определить, верно ли, что все элементы M порождаются из элементов N с помощью операций из Ω.

Связь с задачей декомпозиции здесь очевидна, так как каждый элемент M «раскладывается» на элементы из N. Поэтому алгебраические конструкции активно использовались и для решения задач выразимости, хотя свойства соответствующих алгебраических объектов не всегда обозначались в явном виде. Для примера, в [9] была построена бесконечная полная относительно суперпозиции система функций S. Эта система оказалась наследственно приводимой, то есть любая ее полная подсистема вновь была приводима. В то же время с помощью системы S удалось построить неприводимую полную

систему (базис), что показало большое отличие алгебры автоматов от известных алгебр функций.

Можно заметить, что элементы системы S таковы, что их внутренние полугруппы — это полные полугруппы подстановок на соответствующем множестве состояний. При этом представление полугруппы (диаграмма переходов) выбрано таким образом, что для любой подстановки из полугруппы найдётся буква входного алфавита, которая индуцирует эту подстановку.

Это свойство внутренних полугрупп элементов S оказалось весьма удобным для конструкции, с помощью которой Д. Н. Бабиным был получен результат о полноте относительно суперпозиции функций двух переменных [16].

Важность результата [16] состоит ещё и в том, что при использовании традиционных приёмов построения расширений групп, как правило, не обращали внимания на конкретные представления используемых групп и полугрупп. В то же время, в задаче выразимости автоматных функций важно не просто смоделировать умножение в данной абстрактной полугруппе, а сделать это с учётом ограничений на кодирование алфавитов. И результаты [6] о полноте специальных систем функций не проясняли ситуацию, поскольку рассматривались автоматы с неограниченным в совокупности числом входов. После работы [16] стало ясно, что можно существенно сузить класс представлений групп, используемых для построения полных систем.

В самом деле, в [19] было показано, что при наличии булевских операторов и константных автоматов простой делитель G выделяется из любого группового автомата, внутренняя группа которого делится на G. Так что не важно, какое представление группы имеется в нашем распоряжении. Отсюда, в частности, следует и результат [16] о полноте, поскольку любая конечная простая группа является делителем группы S_n при подходящем n, а группа S_n может быть порождена двумя элементами и, следовательно, представлена автоматом с одним бинарным входом.

Список литературы

[1] Автоматы / Сборник статей под ред. К. Э. Шеннона, Дж. Маккарти. — М.: Изд-во иностранной литературы, 1956.

[2] Глушков В. М. Абстрактная теория автоматов // Успехи матем. наук. — 1961. Т. 16. № 6 (101). — С. 3–62.

[3] Кудрявцев В. Б. Лекции по теории конечных автоматов. — М.: МГУ, 1976.

[4] Кудрявцев В. Б., Алёшин С. В., Подколзин А. С. Элементы теории автоматов. — М.: МГУ, 1978.

[5] Кудрявцев В. Б., Алёшин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

[6] Алгебраическая теория автоматов, языков и полугрупп / Под ред. М. А. Арбиба. — М.: Статистика, 1975.

[7] Чакань Б., Гечег Ф. О группе автоматных подстановок // Кибернетика. — 1965. № 5. — С. 14–17.

[8] Заровный В. П. Автоматные подстановки и сплетения групп // ДАН СССР. — 1965. Т. 160. № 3. — С. 128–144.

[9] Алёшин С. В. О суперпозициях автоматных отображений // Кибернетика. — 1975. № 1. — С. 29–34.

[10] Алёшин С. В. Об отсутствии базисов в некоторых классах инициальных автоматов // Проблемы кибернетики. — 1970. Вып. 22. — С. 33–58.

[11] Алёшин С. В. Конечные автоматы и проблема Бернсайда о периодических группах // Матем. заметки. — 1972. Вып. 3. — С. 56–78.

[12] Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. — М.: Наука, 1982.

[13] Сущанский В. И. Периодические p-группы подстановок и неограниченная проблема Бернсайда // ДАН СССР. — 1979. Т. 247. № 3. — С. 557–561.

[14] Григорчук Р. И. К проблеме Бернсайда о периодических группах // Функц. анализ и его прил. — 1980. Т. 14. Вып. 1. — С. 53–54.

[15] Григорчук Р. И. Степени роста конечно-порожденных групп и теория инвариантных средних // Изв. АН СССР. Сер. матем. — 1984. Т. 48. № 5. — С. 939–985.

[16] Бабин Д. Н. О полноте двухместных о. д.-функций относительно суперпозиции // Дискрет. матем. — 1989. Т. 1. Вып. 4. — С. 86–91.

[17] Часовских А. А. Об алгоритмической разрешимости проблемы полноты для линейных автоматов // Вестн. Моск. ун-та. Сер. 1, Математика, механика. — 1985. Вып. 2. — С. 47–61.

[18] Малыгин В. И. О некоторых пространствах, связанных с композициями автоматов // Вестн. Моск. ун-та. Сер. 1, Математика, механика. — 1988. Вып. 4. — С. 88–90.

[19] Алёшин С. В. Об одном следствии теоремы Крона — Роудза // Дискрет. матем. — 1999. Т. 11. Вып. 4. — С. 31–37.

[20] Алёшин С. В. Автоматное представление свободной группы // Дискрет. матем. — 2011. Т. 23. Вып. 3. — С. 32–56.

[21] Алёшин С. В. Свободная группа конечных автоматов // Вестн. Моск. ун-та. Сер. 1, Математика, механика. — 1983. Вып. 4. — С. 12–14.

[22] Zuk A. Groupes engenders par les automates // Astérisque. — 2008. V. 317. — P. 141–174.

[23] Рожков А. В. К теории групп алёшинского типа // Матем. заметки. — 1986. Т. 40. № 5. — С. 122–131.

[24] Рожков А. В. Условия конечности в группах автоморфизмов деревьев // Алгебра и логика. — 1998. Т. 37. № 5. — С. 568–605.

[25] Lavrenyuk Y., Mazorchuk V., Oliynyk A. On braid groups acting on rooted trees // Uppsala University Report. — 2005. V. 7.

[26] Bondarenko I., Grigorchuk R., Kravchenko R. On classification of groups generated by 3-state automata over a 2-letter alphabet // Algebra and Discrete Math. — 2008. № 1. — P. 1–163.

[27] Мерзляков Ю. И. О бесконечных конечнопорождённых периодических группах // ДАН СССР. — 1983. Т. 208. № 4.

[28] Vorobets M., Vorobets Y. On a free group of transformation defined by an automaton // Geom. Dedicata. — 2007. V. 134. — P. 237–249.

[29] Бокк Н. Г. О порядке элемента в группе автоматных подстановок // Интеллектуальные системы. — 2012. Т. 16. Вып. 1–4. — С. 275–290.

[30] Макаров В. В. О группах автоматных подстановок // Фундамент. и прикл. матем. — 1996. Т. 2. Вып. 1. — С. 171–186.

О суперпозициях автоматов

Бабин Д. Н. (Москва, МГУ им. М. В. Ломоносова)

d.n.babin@mail.ru

Понятие автомата относится к числу важнейших в математике. Содержательно автомат представляет собой устройство с входными и выходными каналами. На его входы последовательно поступает информация, которая перерабатывается им с учетом строения этой последовательности и выдается через выходные каналы. Эти устройства могут допускать соединение их каналов между собой. Отображение входных последовательностей в выходные называют автоматной функцией, а возможность получения новых таких отображений за счет соединения автоматов приводит к алгебре автоматных функций.

Первый толчок к возникновению теории автоматов дала работа Поста Э. 1921 года [1]. В ней были получены фундаментальные результаты о строении решетки замкнутых классов булевых функций, которые были в дальнейшем методически переработаны и упрощены в книге Яблонского С. В., Кудрявцева В. Б., Гаврилова Г. П. «Функции алгебры логики и классы Поста» [2].

Сами автоматы и их алгебры начали исследоваться в тридцатые годы текущего столетия, но особенно активно в период с 50-х годов. Основополагающую роль здесь сыграли работы Тьюринга, авторов знаменитого сборника «Автоматы» [3] Шеннона, Мура, Клини и других. Последующие работы по изучению алгебр автоматов велись под большим влиянием известных статей А. В. Кузнецова [4, 5] и С. В. Яблонского [6] по теории функций k-значной логики.

Эти функции могут рассматриваться как автоматы без памяти, к которым применяются операции суперпозиции. Возникшие для таких функций постановки задач о выразимости, полноте, базисах, решетке замкнутых классов и другие, а также развитый аппарат сохранения предикатов как ключевой для решения этих задач, оказались весьма действенными и для алгебр автоматных функций. При этом под выразимостью понимается возможность получения функций одного

множества через функции другого с помощью заданных операций, а под полнотой — выразимость всех функций через заданные.

Основу результатов для функций k-значной логики составляет подход А. В. Кузнецова, опирающийся на понятие предполного класса. Для конечно-порожденных систем таких функций семейство предполных классов образует критериальную систему; другими словами, произвольное множество является полным точно тогда, когда не является подмножеством ни одного предполного класса. Множество этих предполных классов оказалось конечным и из их характеризации вытекает алгоритмическая разрешимость задачи о полноте.

На этом пути С. В. Яблонским путем явного описания всех предполных классов была решена задача о полноте для функций трехзначной логики, а вместе с А. В. Кузнецовым найдены отдельные семейства предполных классов для логики произвольной конечной значности. Затем усилиями многих исследователей [7–11] последовательно были открыты новые такие семейства, а заключительные построения провел Розенберг [12].

Одновременно с изучением функций без памяти (без учета времени), были сделаны попытки применения аппарата предполных классов в задаче полноты для автоматов. Сначала для автоматов без обратных связей, называемых функциями с задержками, В. Б. Кудрявцев эффективно решил задачу о полноте и ее естественных модификациях [13]. После этого им было проведено рассмотрение общего случая и на этом пути был получен фундаментальный результат негативного характера, который показал континуальность множества предполных классов автоматных функций [14]. В дальнейшем, Кратко М. И. была показана алгоритмическая неразрешимость задачи выразимости автоматных функций [15].

Особенностью операций с автоматами является то, что число состояний растет с ростом схемы, состояния дублируют друг друга или не достижимы вовсе из начального состояния. Но даже если учитывать недостижимые состояния проблема полноты [16] также остается алгоритмически неразрешимой.

Известно [17], что всякая полная относительно суперпозиции система автоматов бесконечна. С. В. Алешин [18] установил в каких

случаях, в зависимости от мощностей алфавитов входного, выходного и состояний, существуют базисы для автоматов.

Автор [19] показал, что существуют полные системы (естественно, бесконечные) арности два (аналог 13 проблемы Гильберта для о.д.-функций). Более того автору удалось показать, что система, состоящая из одноместных конечных автоматов и всех булевых функций, полна относительно суперпозиции.

Как уже отмечалось, задача выразимости для конечных автоматов в общем случае алгоритмически неразрешима. Представляет интерес накопить примеры, когда эта задача имеет положительное решение.

Рассматривая автоматную функцию, трудно учесть разницу между о.д.-функцией и д.-функцией, поэтому решение задачи выразимости для конечных автоматов относительно суперпозиции путем анализа сохраняемых автоматом предикатов неизбежно наталкивается на большие сложности. Представляет интерес рассматривать системы автоматов, не сохраняющие никаких конечных предикатов, например, когда в выражающей системе есть автоматы «штрих Шеффера и задержка». В этом случае задача выразимости решается в терминах внутренней структуры рассматриваемых автоматов, а не в терминах сохраняемых предикатов.

В частности на этом пути удалось решить задачу выразимости константных автоматных функций. Летуновский А. А. [20] показал, что если конечные системы автоматов S содержат «штрих Шеффера и задержку», то существует алгоритм, проверяющий выразимость константной автоматной функции через систему S.

Определим простой автомат по аналогии со свойством простых чисел. Автомат C назовем простым, если из того, что C выразим через автоматы A и B следует, что C выразим через автомат A, или C выразим через автомат B. Если рассматривать функциональную систему с операцией суперпозиции (а также композиции), то простых автоматов в таком понимании вообще нет. Операцию суперпозиции при наличии конечной добавки назовем расширенной суперпозицией, в этом случае техника разложения на простые автоматы позволяет решать некоторые задачи выразимости. В частности в этой функциональной системе можно описать все простые автоматы.

Ослабленной задачей полноты относительно суперпозиции назовем задачу выразимости всех автоматов с фиксированным числом состояний N. Оказывается, что для всех натуральных N все автоматы с не более чем N состояниями выразимы через один автомат с N состояниями и двумя входами [23].

Список литературы

[1] Post E. Two-valued iterative systems of mathematical logic. — Princeton, 1941.

[2] Кудрявцев В. Б., Гаврилов Г. П., Яблонский С. В. Функции алгебры логики и классы Поста. — М.: Наука, 1966.

[3] Автоматы / Сб. статей под ред. Маккарти и Шеннона. — М.: ИЛ, 1956.

[4] Кузнецов А. В. О проблемах тождества и функциональной полноты для алгебраических систем // Труды третьего всесоюзного математического съезда. — М.: Изд. АН СССР, 1956. Т. 2. — С. 145–146.

[5] Кузнецов А. В. Структуры с замыканием и критерии функциональной полноты // Успехи математических наук. — 1961. Т. 16. № 2. — С. 201–202.

[6] Яблонский С. В. Функциональные построения в k-значной логике // Труды Матем. ин-та им. В. А. Стеклова. — М.: АН СССР, 1958. Т. 51. — С. 5–142.

[7] Ло Чжу-Кай. Предполные классы, определяемые k-арными отношениями в k-значной логике // Acta Sci. Natur. Univ. Jilinensis. — 1964. N 3.

[8] Ло Чжу-Кай, Лю Сюй Хуа. Предполные классы, определяемые бинарными отношениями в многозначной логике // Acta Sci. Natur. Univ. Jilinensis. — 1963. N 4.

[9] Захарова Е. Ю. Критерий полноты системы функций из P_k // Проблемы кибернетики. — 1967. № 18. — С. 5–10.

[10] Мартынюк В. В. Исследование некоторых классов функций в многозначных логиках // Проблемы кибернетики. — 1960. № 3. — С. 49–60.

[11] Пан Юн-Цзе. Один разрешающий метод для отыскания всех предполных классов в многозначной логике // Acta Sci. Natur. Univ. Jilinensis. — 1963. N 3.

[12] Rosenberg J. La structure des fonctions de plusiers variables sur un ensemble fini // Comptes Rendus Acad. Sci. Paris. — 1965. N 260. — P. 3817–3819.

[13] Кудрявцев В. Б. Теорема полноты для одного класса автоматов без обратных связей // Проблемы кибернетики. — 1962. № 8. — С. 91–115.

[14] Кудрявцев В. Б. О мощностях множеств предполных классов некоторых функциональных систем, связанных с автоматами // ДАН СССР. — 1963. Т. 151. № 3. — С. 493–496.

[15] Кратко М. И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов // ДАН СССР. — 1964. Т. 155. № 1. — С. 35–37.

[16] Хазбун И. В. Об условиях полноты и выразимости в точной алгебре автоматов // Логико-алгебраические конструкции. — Тверь, 1984. — С. 35–41.

[17] Loomis Jr. H. H. Completeness of sets of delayed-logic devices // IEEE Trans. Electron. Comput. — EC-14 (1965). — P. 157–172.

[18] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

[19] Бабин Д. Н. О полноте двухместных о.д.-функций относительно суперпозиции // Дискретная математика. — 1989. Т. 1. Вып. 4. — С. 86–91.

[20] Летуновский А. А. О выразимости константных автоматов // Интеллектуальные системы. — 2005. Т. 9. Вып. 1–4. — С. 457–469.

[21] Арбиб М. Алгебраическая теория автоматов языков и полугрупп. — М.: Статистика, 1975.

[22] Алешин С. В. Об одном следствии теоремы Крона — Роудза // Дискретная математика. — 1999. Т. 11. Вып. 4. — С. 101–109.

[23] Бабин Д. Н. О суперпозициях о.д.-функций ограниченного веса // Логико-алгебраические конструкции. — Тверь, 1984. — С. 21–27.

Простые автоматы в задаче полноты относительно суперпозиции

Бабин Д. Н. (Москва, МГУ им. М. В. Ломоносова)

d.n.babin@mail.ru

Автоматная функция является отображением, ее задающий минимальный автомат имеет полугруппу переходов. Суперпозиция автоматов, индуцирует операцию расширения над полугруппами автоматов. Этот подход рассмотрен во многих работах [1,2,3]. Определим простой автомат по аналогии со свойством простых чисел. Автомат C — простой, если из того, что C выразим через автоматы A и B следует, что C выразим через автомат A, или C выразим через автомат B. Понятие простого автомата становится интересным, если при суперпозиции разрешается использовать служебные автоматы из класса K — «штрих Шеффера», «задержку», а также все автоматы с безусловными переходами. В этом случае верна лемма о копировании [4], которая позволяет получать из автоматов с некоторой полугруппой автоматы с большими входными алфавитами и той же полугруппой. Простыми автоматами в этом случае будут автоматы, полугруппы которых — суть простые группы. В отличие от простых чисел, простые автоматы могут быть друг через друга выразимы. Простые знакопеременные группы A_n как раз таковы, что все автоматы с не более чем n состояниями выразимы через автомат с группой A_n. Класс K не расширяется до предполного. В самом деле: если в некотором классе R, до которого расширяется класс K, есть все автоматы с группами A_n, то в R есть все автоматы. Если нет автоматов с группой A_n для $n > N$, то ввиду их простоты добавкой одного автомата их не получить. Если вместо класса K использовать K_1 — «штрих Шеффера» и «задержку», то список простых автоматов расширяется. Простыми будут не только автоматы с простыми циклическими группами и безусловные автоматы с простыми циклическими группами [5].

Список литературы

[1] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

[2] Арбиб М. Алгебраическая теория автоматов языков и полугрупп. — М.: Статистика, 1975.

[3] Алешин С. В. Об одном следствии теоремы Крона — Роудза // Дискретная математика. — 1999. Т. 11. Вып. 4. — С. 101–109.

[4] Бабин Д. Н. О полноте двухместных автоматных функций относительно суперпозиции // Дискретная матетматика. — 1989. Т. 1. Вып. 4. — С. 423–431.

[5] Летуновский А. А. О выразимости константных автоматов // Интеллектуальные системы. — 2005. Т. 9. Вып. 1–4. — С. 457–469.

Автоматная модель взаимодействия организационных систем

Богомолов С. А. (Саратов)

alexbogomolov@yandex.ru

В сообщении рассматривается автоматная модель выбора варианта поведения в процессе управления организационной системы при конкурентном взаимодействии в зависимости от сложившихся обстоятельств. Организационные автономные управляемые системы рассматриваются в качестве динамических моделей. Рынок оборонной промышленности и продукции стратегического назначения представляет собой систему различного рода заказов.

В настоящее время процессы взаимодействия в основном приводят к проблемным (конкурентным) взаимодействиям, вызванными как сокращениями госзаказа, так и определенной самостоятельности при выборе направления развития. В этой связи возникает проблема выбора рациональной стратегии поведения, которая позволит предприятиям сохранить свой потенциал и конкурентоспособность, адаптироваться к динамике внешней среды и рынка, функционировать и развиваться согласно своему назначению и миссии.

Приведем процедуру исследования ситуаций и вывода рекомендаций по поведению организационной системы в ситуациях, когда требуется принять решение по вопросам конкурентного взаимодействия. Основой взаимодействия являются различные виды (активных или пассивных) областей, воздействие которых проявляется через воздействие как на элементы так и на структуру систем.

Динамические организационные системы обладают следующими свойствами: R_j $(j = 1, 2, \ldots)$, — возможность развиваться (повышать свой потенциал и конкурентоспособность); I_j $(j = 1, 2, \ldots)$ — возможность осуществлять информационное взаимодействие с внешней средой, в частности адекватно реагировать на негативные воздействия конкурентов; F_j $(j = 1, 2, \ldots)$ — возможность оказывать воздействие на внешнюю среду. Под областью понимается область взаимодействий систем, а именно совокупность ситуаций, в которых осуществляется хотя бы один из указанных типов взаимодействий. Простран-

ство определяется как множество ситуаций, возникающих в процессе рыночных отношений между организационными системами. Элементы пространства представляют ситуации, связывающие рынок заказов, возможных исполнителей с их потенциалами, взаимодействиями между собой и отношениями конкуренции, партнерства, нейтралитета и другими. Таким образом, пространство — это множество ситуаций, образованных следующими элементами: организационные системы, рынок заказов и инновационных предложений, различные виды взаимодействий посредством областей. Не ограничивая общности, полагаем, что на рынке заказов имеется только две организационные системы W, V. Предполагается, что системы обладают следующими возможностями: наблюдать поведение каждой из систем, относительно интересующих заказов и инноваций, осуществлять поиск информации относительно потенциала другой, развиваться, не учитывая динамику развития другой, оказывать прямое воздействие на другую систему путем участия в конкурсе или вынося на рынок свои инновации, тем самым повышая свою конкурентоспособность. Обозначим C_V — цель, выбираемая системой V. Задача управления состоит в выборе в каждой ситуации пространства s векторов $r_V(s)$, $i_V(s)$, $f_V(s)$, принадлежащих соответствующим полям, так, чтобы достичь заданной цели и удовлетворить заданному критерию. Целью может быть: достижение определенной ситуации пространства, осуществление информационного взаимодействия с внешней средой (мониторинг или маркетинговые исследования), конкурентное взаимодействие с другой системой, участвуя в конкурсе заказов. При этом необходимо удовлетворить одному из критериев K_V: минимизация затрат, сохранение экономического потенциала, репутации и положения. Соответственно, цель системы W обозначается как C_W, а критерий K_W. Эти цели стоят перед системами, пока не существует взаимодействие между ними (каждая из систем не имела информации о присутствии другой). Как только средствами информационного взаимодействия одна из систем обнаруживает присутствие на рынке заказов другую, которая может помешать в достижении поставленной цели, то система может менять целевую установку и в соответствии с вновь возникшей ситуацией переходит в новый режим функционирования, призванный обеспечить достижение новой цели. Другая

система, в свою очередь, получив информацию о наличие конкурента поступает аналогичным образом. Переход систем в новые состояния приводит к изменениям ситуации системы в целом. В наиболее общем виде, в понятии «ситуация» содержится описание возможных действий систем, то есть предоставляется выбор одного из вариантов поведения. Рассмотрим процедуру принятия решения, и уточним, как и в каких случаях происходит выбор одного из рекомендуемых вариантов поведения. В качестве моделей описания динамического поведения системы предлагается рассматривать конечные детерминированные автоматы, функционирование которых задается функциями переходов и выходов, определяющих для каждого входного сигнала и внутреннего состояния состояние в следующий тактовый момент и выходную реакцию автомата [1]. Пусть автомат $A = \{X, Y, S, \delta, \lambda\}$ [1], где $x \in X$ — входное слово (воздействие среды); $y \in Y$ — выходное слово (реакция на воздействие среды); $s \in S$ — состояние автомата. Состояние автомата $s \in S_A$ определяется следующим образом. Пусть определены дискретные множества $I = \{I_1, I_2, \ldots, I_k\}$ — система имеет информацию о внешней среде (в частности о конкуренте) в различной степени. $P = \{P_1, P_2, \ldots, P_n\}$ — варианты направления развития системы (до обнаружения конкурента, после обнаружения, противостояние с конкурентом — участие в конкурсе, уход от конкурентной борьбы — поиск других рынков, компромиссное решение, диверсификация). $F = \{F_1, F_2, \ldots, F_r\}$ — система оказывает активное воздействие с разной степенью и в различной форме с целью ослабления позиций конкурента. Содержательно, множество I — различная степень неполноты информации о внешней среде, наличие конкурентов $I = \{I_1, I_2, I_3, I_4\}$, где I_1 — система имеет максимально полную информацию об окружающей среде (достаточной для принятия решения относительно выбора или изменения стратегии поведения во внешней среде) для выбора варианта поведения; I_2 — система обладает неполной информацией (недостаточной) для принятия решения относительно поведения во внешней среде; I_3 — система не имеет вообще информации об окружающей среде, необходимой для принятия решения относительно выбора варианта поведения, но в состоянии провести необходимые информационные воздействия с целью увеличения объема информации о конкуренте; I_4 — система не имеет во-

обще информации об окружающей среде и нет возможности ее приобрести. Пусть также определено такое множество (меры противостояния или компромиссного разрешения ситуаций, сотрудничество, переговоры) $F = \{F_1, F_2\}$: F_1 — оказывает воздействие на конкурирующий объект и участвует в конкурсе заказов; F_2 — объект не оказывает воздействие на объекты внешней среды, игнорирует предлагаемые заказы и не выходит на рынок со своими инновациями. Определим множество $P = \{P_1P_2, P_3, P_4\}$: P_1 — состояние динамического покоя системы (без учета влияния внешней среды); P_2 — направление развития системы под действием управления, выработанного до обнаружения конкурента W во внешней среде; P_3 — направление развития системы (противостояние конкуренту), успеть принять меры когда конкурент уже обнаружен (возможных функциональных воздействий со стороны конкурентов); P_4 — направление развития, позволяющее осуществить мероприятия или действия (маневр), с целью избежать прямого конфликта в состоянии, допускающем воздействие со стороны конкурента (меры, принимаемые или направленные на минимальное взаимодействие с конкурентами). Границы областей определяется совокупностью предикатов (условий). Таким образом, каждое состояние s_i описывается тройкой:

$$s_j = \{I_i, F_n, P_e\} n = 1, 2; e = 1, 2, 3, 4; I = l, 2, 3.$$

Входными сообщениями (символами) полагаем следующие сообщения о внешней среде: x_1 — W имеет преимущества в конкуре перед V; x_2 — V имеет преимущества в конкурсе перед W; x_3 — V определяет наличие конкурента; x_4 — W оказывает воздействие на V, с целью не допустить к конкурсу систему V и т. п. Затем формируется таблица переходов автомата, который в данном случае представляется автоматом-акцептором, имеющим два финальных состояния s_C — система достигает намеченной цели; s_O — система прекращает деятельность, не достигнув цели. Для примера рассмотрим следующую ситуацию. Ситуация. Взаимодействие в условиях, когда V обладает полной информацией о возможностях конкурента и его положении относительно системы V. Перед V встает выбор: избежать прямого столкновения при участии в конкурсе, потеряв при этом заказ или выйти на конкурс со своим инновационным предложением и попы-

таться выиграть конкурс. Таких ситуаций при конкурентном взаимодействии достаточно большое множество и, при соответствующей перенумерации состояний автомата, для каждой из них может быть построен автомат, представляющий всевозможные пути развития ситуации.

Список литературы

[1] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

К вопросу о порядках элементов группы автоматных подстановок

Виноградов И. В.
(Москва, МГУ им. М. В. Ломоносова)
vanum@yandex.ru

В работе рассмотрен автомат 8-го порядка в группе автоматных подстановок AS_2 [1], реализующий отрицание в одном состоянии и тождественную функцию в остальных. Пример автомата 4-го порядка, обладающего теми же свойствами, был дан в работе [2]. Изучение автоматов с одним отрицанием представляет особенный интерес, поскольку любой автомат из группы AS_2 разлагается в суперпозицию автоматов такого вида.

Пусть дан алфавит A, состоящий из k символов. Пусть $\alpha_1, \ldots, \alpha_m$ — различные слова в алфавите A длины n и $m = k^n$. Тогда обобщённой диаграммой переходов в алфавите A относительно слов $\alpha_1, \ldots, \alpha_m$ будем называть ориентированный граф, в котором из одних вершин выходят рёбра с метками (α_i, α_j), а из других — рёбра с метками (α_i, α_i). Первые вершины назовём вершинами первого типа, а последние — вершинами второго типа. Потребуем, чтобы для каждой вершины первого типа для любого $1 \leqslant i \leqslant k$ существовало ребро с меткой (α_i, α_j), а для каждой вершины второго типа для любого $1 \leqslant i \leqslant k^n$ существовало ребро с меткой (α_i, α_i).

Заметим, что в каждой вершине первого типа реализуется отображение из A в A в соответствии с метками рёбер. В вершинах второго типа реализуется тождественное отображение из A^n в A^n. Это отображение можно реализовать, заменив каждую вершину второго типа древовидным подграфом с $k^n - 1$ вершиной первого типа с метками вида (α_i, α_i).

Пусть дана обобщённая диаграмма переходов D в алфавите A относительно слов $\alpha_1, \ldots, \alpha_m$ с t вершинами первого типа и l вершинами второго типа, где $|A| = k$ и $m = k^n$. Тогда диаграммой переходов, соответствующей обобщённой диаграмме переходов D, назовём граф с $p + l(k^n - 1)$ вершинами, представляющий из себя граф диаграммы D, в котором каждая вершина второго типа заменена на древовидный

подграф из $k^n - 1$ вершины, реализующий тождественное отображение из A^n в A^n. Причём входящие в вершину второго типа рёбра заменены рёбрами, входящими в корневую вершину заменившего её подграфа, а исходящие — рёбрами, исходящими из соответствующих концевых вершин данного подграфа.

Автоматом, соответствующим обобщённой диаграмме D, назовём автомат, диаграмма которого соответствует обобщённой диаграмме D.

Легко видеть, что с точностью до изоморфизма обобщённой диаграмме соответствует единственный автомат. Имея обобщённую диаграмму, можно в соответствующем автомате естественным образом рассматривать некоторые состояния как одно, реализующее тождественную функцию из A^n в A^n. Эту идею поясняет следующее определение.

Пусть даны обобщённая диаграмма D и соответствующий ей автомат V. Тогда обобщёнными состояниями первого типа автомата V будем называть состояния соответствующие вершинам первого типа на диаграмме D, а обобщёнными состояниями второго типа будем называть подмножества множества состояний, соответствующие вершинам второго типа.

Все данные выше определения применимы и к инициальным автоматам, в частности к элементам группы AS_2. Интересующий нас автомат представлен обобщённой диаграммой на рис. 1. В качестве входного алфавита принято множество $\{0, 1\}$, а в качестве слов, относительно которых рассматривается обобщённая диаграмма, взяты слова 11, 10, 01 и 00. Они обозначаются соответственно α, β, γ, μ. Начальным обобщённым состоянием здесь является q_1 — единственное состояние, реализующее отрицание.

Комментарий к рисунку 1. По определению каждому ребру в обобщённой диаграмме должна быть приписана пара символов, но в нашем случае для каждого ребра, исходящего не из первой вершины второй элемент соответствующей пары равен первому, а для двух рёбер, исходящих из первой вершины, вторые элементы пар обратны первым (так как q_1 — обобщённое состояние первого типа, реализующее отрицание). Поэтому на рисунке каждому ребру приписан только первый элемент из соответствующей ему пары.

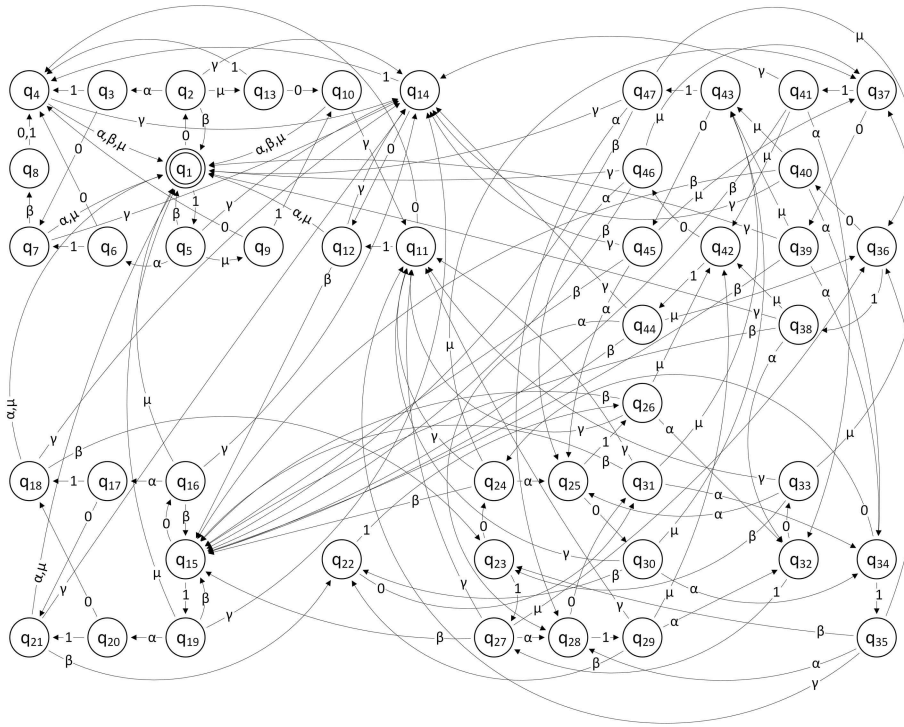

Рис. 1.

В автомате соответствующем представленной диаграмме (назовём его V_8) присутствует следующее свойство. Для любого n слово вида $a_1\alpha_1 a_2\alpha_2 a_3 \dots \alpha_{n-1} a_n \alpha_n$ преобразуется в слово вида $b_1\alpha_1 b_2\alpha_2 b_3 \dots \alpha_{n-1} b_n \alpha_n$, где $a_i, b_i \in \{0,1\}$, $\alpha_i \in \{\alpha, \beta, \gamma, \mu\}$. Это свойство сохраняется при суперпозиции. Следовательно, у суперпозиции n автоматов V_8 существует обобщённая диаграмма относительно слов $\alpha, \beta, \gamma, \mu$. Это позволяет задавать обобщённые состояния суперпозиции n автоматов V_8 наборами из n обобщённых состояний автомата V_8. Обозначим через V_8^8 суперпозицию восьми автоматов V_8.

В автомате V_8^8 обобщённые состояния $(q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8})$ и $(q'_{i1}, q'_{i2}, q'_{i3}, q'_{i4}, q'_{i5}, q'_{i6}, q'_{i7}, q'_{i8})$ назовём циклически эквивалентными, если наборы $(q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8})$ и $(q'_{i1}, q'_{i2}, q'_{i3}, q'_{i4}, q'_{i5}, q'_{i6}, q'_{i7}, q'_{i8})$ получаются друг из друга циклическими сдвигами.

Замечание. Два обобщённых состояния автомата V_8^8 могут быть циклически эквивалентны только тогда, когда они принадлежат к одному типу.

Очевидно, что циклически эквивалентные состояния образуют классы эквивалентности.

Утверждение 1. *Если в автомате V_8^8 обобщённые состояния второго типа $(q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8})$ и $(q'_{i1}, q'_{i2}, q'_{i3}, q'_{i4}, q'_{i5}, q'_{i6}, q'_{i7}, q'_{i8})$ циклически эквивалентны, то под действием слова $\delta \in \{\alpha, \beta, \gamma, \mu\}$ они перейдут в циклически эквивалентные состояния первого типа.*

Доказательство. Обобщённое состояние второго типа q_i автомата V_8 под действием слова δ перейдёт в некоторое обобщённое состояние первого типа, обозначим его $q_i(\delta)$. При этом в силу отмеченного выше свойства на выходе снова получится слово δ. Из этого следует, что обобщённые состояния второго типа $(q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8})$ и $(q'_{i1}, q'_{i2}, q'_{i3}, q'_{i4}, q'_{i5}, q'_{i6}, q'_{i7}, q'_{i8})$ перейдут под действием слова δ в обобщённые состояние первого типа $(q_{i1}(\delta), q_{i2}(\delta), q_{i3}(\delta), q_{i4}(\delta), q_{i5}(\delta), q_{i6}(\delta), q_{i7}(\delta), q_{i8}(\delta))$ и $(q'_{i1}(\delta), q'_{i2}(\delta), q'_{i3}(\delta), q'_{i4}(\delta), q'_{i5}(\delta), q'_{i6}(\delta), q'_{i7}(\delta), q'_{i8}(\delta))$ соответственно. Но если первые два состояния были циклически эквивалентными, то такими же, очевидно, будут и последние.

Утверждение 2. *Пусть в автомате V_8^8 циклически эквивалентны два обобщённых состояния первого типа $(q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8})$ и $(q'_{i1}, q'_{i2}, q'_{i3}, q'_{i4}, q'_{i5}, q'_{i6}, q'_{i7}, q'_{i8})$. Причём в наборе $\{q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8}\}$ чётное число состояний отрицания. Тогда для обобщённого состояния второго типа, полученного из $(q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8})$ под действием $a \in \{0, 1\}$ существует циклически эквивалентное ему обобщённое состояние второго типа, получаемое из $(q'_{i1}, q'_{i2}, q'_{i3}, q'_{i4}, q'_{i5}, q'_{i6}, q'_{i7}, q'_{i8})$ под действием некоторого $b \in \{0, 1\}$, для любого a из $\{0, 1\}$.*

Замечание. Из симметричности отношения циклической эквивалентности следует, что в формулировке утверждения, можно поменять местами состояния $(q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8})$ и $(q'_{i1}, q'_{i2}, q'_{i3}, q'_{i4}, q'_{i5}, q'_{i6}, q'_{i7}, q'_{i8})$. Это означает, что не только для каждого состояния, в которое может перейти $(q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8})$ под действием буквы из алфавита $\{0, 1\}$ существует циклически экви-

валентное ему состояние, получаемое из состояния $(q'_{i1}, q'_{i2}, q'_{i3}, q'_{i4}, q'_{i5}, q'_{i6}, q'_{i7}, q'_{i8})$, но и для каждого состояния, в которое может перейти $(q'_{i1}, q'_{i2}, q'_{i3}, q'_{i4}, q'_{i5}, q'_{i6}, q'_{i7}, q'_{i8})$ под действием буквы из алфавита $\{0, 1\}$ также существует циклически эквивалентное ему состояние, достижимое из $(q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8})$ под действием одной буквы.

Доказательство утверждения 2. Будем доказывать, что это утверждение выполняется, если состояние $(q'_{i1}, q'_{i2}, q'_{i3}, q'_{i4}, q'_{i5}, q'_{i6}, q'_{i7}, q'_{i8})$ получено из состояния $(q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8})$ циклическим сдвигом вправо на одну позицию, иными словами состояние $(q'_{i1}, q'_{i2}, q'_{i3}, q'_{i4}, q'_{i5}, q'_{i6}, q'_{i7}, q'_{i8})$ есть $(q_{i8}, q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7})$. Применяя такой циклический сдвиг несколько раз, можно получить любой другой, поэтому достаточно доказать утверждение для него. Рассмотрим два случая: состояние q_{i8} является тождественным состоянием, и состояние q_{i8} является состоянием отрицания. В первом случае под действием буквы $a \in \{0, 1\}$ состояние $(q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8})$ перейдёт в некоторое состояние $(q_{j1}, q_{j2}, q_{j3}, q_{j4}, q_{j5}, q_{j6}, q_{j7}, q_{j8})$, а состояние $(q_{i8}, q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7})$ — в состояние $(q_{k8}, q_{j1}, q_{j2}, q_{j3}, q_{j4}, q_{j5}, q_{j6}, q_{j7})$, потому что q_{i8} является тождественным состоянием. Но число состояний отрицания в наборе $\{q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8}\}$ было чётным, значит, при подаче входного символа a на суперпозицию восьми автоматов V_8 (образующую автомат V_8^8), находящуюся в состоянии $\{q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8}\}$, последний автомат V_8 получит на вход именно символ a. Тогда под действием этого символа состояние q_{i8} переходит в q_{j8}. Но $(q_{i8}, q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7})$ под действием a переходит в $(q_{k8}, q_{j1}, q_{j2}, q_{j3}, q_{j4}, q_{j5}, q_{j6}, q_{j7})$. Следовательно, $q_{j8} = q_{k8}$. Состояния $(q_{j1}, q_{j2}, q_{j3}, q_{j4}, q_{j5}, q_{j6}, q_{j7}, q_{j8})$ и $(q_{j8}, q_{j1}, q_{j2}, q_{j3}, q_{j4}, q_{j5}, q_{j6}, q_{j7})$ циклически эквивалентны, поэтому для первого случая утверждение доказано.

Пусть q_{i8} — состояние отрицания. Пусть $(q_{j1}, q_{j2}, q_{j3}, q_{j4}, q_{j5}, q_{j6}, q_{j7}, q_{j8})$ получено из $(q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8})$ под действием символа $a \in \{0, 1\}$. Тогда под действием символа $\bar{a}$ ($\bar{a}$ — отрицание a) состояние $(q_{i8}, q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7})$ перейдёт в состояние $(q_{k8}, q_{j1}, q_{j2}, q_{j3}, q_{j4}, q_{j5}, q_{j6}, q_{j7})$, так как q_{i8} является состоянием отрицания. Тогда рассматривая снова суперпозицию восьми автоматов V_8, находящуюся в состоянии $(q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8})$, и по-

давая на вход символ a, мы получаем, что из чётности числа состояний отрицания в наборе $\{q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7}, q_{i8}\}$ следует, что последний из автоматов V_8 получает на вход $\bar{a}$. Следовательно, под действием $\bar{a}$ q_{i1} переходит в q_{j8}. С другой стороны, под действием $\bar{a}$ состояние $(q_{i8}, q_{i1}, q_{i2}, q_{i3}, q_{i4}, q_{i5}, q_{i6}, q_{i7})$ переходит в состояние $(q_{k8}, q_{j1}, q_{j2}, q_{j3}, q_{j4}, q_{j5}, q_{j6}, q_{j7})$. Следовательно, и в этом случае $q_{j8} = q_{k8}$. Утверждение доказано.

Для автомата V_8^8 будем называть класс циклически эквивалентных обобщённых состояний достижимым, если хотя бы один из его элементов достигается из состояния $(q_1q_1q_1q_1q_1q_1q_1q_1)$.

Теорема. *Автомат V_8 является автоматом восьмого порядка.*

Доказательство. На слове $1\mu1\gamma1\beta1\alpha1\beta1$ достигается восьмой порядок. Это можно проверить явно.

Для суперпозиции восьми автоматов будем рассматривать слова вида $a_1\alpha_1a_2\alpha_2a_3\ldots\alpha_{n-1}a_n\alpha_n$, где $a_i \in \{0,1\}$, $\alpha_i \in \{\alpha,\beta,\gamma,\mu\}$. Если окажется, что на каждом таком слове автомат V_8^8 осуществляет тождественное преобразование, то это будет означать, что V_8 является автоматом восьмого порядка, поскольку каждое слово в алфавите $\{0,1\}$ является началом некоторого слова такого вида. Остаётся доказать, что каждое достижимое из $(q_1, q_1, q_1, q_1, q_1, q_1, q_1, q_1)$ обобщённое состояние автомата V_8^8 содержит в своём наборе из восьми обобщённых состояний автомата V_8 чётное число состояний q_1. Но обобщённые состояния второго типа вообще не содержат состояний отрицания в соответствующих им наборах. Из двух последних утверждений следует, что можно рассматривать не достижимые обобщённые состояния, а достижимые классы циклической эквивалентности обобщённых состояний. И если ни один из таких классов не переходит в недопустимый класс (класс, имеющий нечётное число состояний отрицания), то не существует допустимого обобщённого состояния, которое может под действием некоторого символа перейти в недопустимое. Тогда автомат V_8^8 является автоматом порядка не большего восьми. Но для того, чтобы рассмотреть все классы циклической эквивалентности, достаточно рассмотреть по одному обобщённому состоянию из каждого класса. Следующие таблицы являются таблицами переходов для обобщённых состояний автомата V_8^8, сокращёнными так, что

для каждого класса циклической эквивалентности в них дано лишь одно состояние из этого класса. Здесь представлено две таблицы, поскольку разным типам обобщённых состояний соответствуют разные входные символы (в таблицах для краткости опущены символы q и круглые скобки заменены на фигурные) Заметим, что автомат V_8 устроен таким образом, что для любой суперпозиции таких автоматов (в частности для V_8^8) верно, что любое обобщённое состояние при получении любого входного символа, соответствующего его типу, переходит в обобщённое состояние другого типа. С учётом приведённых таблиц теорема доказана.

1	0
{1,1,1,1,1,1,1,1}	{5,2,5,2,5,2,5,2}	{2,5,2,5,2,5,2,5}
{14,14,14,14,14,14,14,14}	{4,4,4,4,4,4,4,4}	{12,12,12,12,12,12,12,12}
{13,9,13,9,13,9,13,9}	{4,10,4,10,4,10,4,10}	{10,4,10,4,10,4,10,4}
{6,3,6,3,6,3,6,3}	{7,4,7,4,7,4,7,4}	{4,7,4,7,4,7,4,7}
{14,11,14,11,14,11,14,11}	{4,12,4,12,4,12,4,12}	{12,4,12,4,12,4,12,4}
{3,20,6,17,3,20,6,17}	{4,21,7,18,4,21,7,18}	{7,18,4,21,7,18,4,21}
{11,11,11,11,11,11,11,11}	{12,12,12,12,12,12,12,12}	{4,4,4,4,4,4,4,4}
{20,20,20,20,20,20,20,20}	{21,21,21,21,21,21,21,21}	{18,18,18,18,18,18,18,18}
{17,17,17,17,17,17,17,17}	{18,18,18,18,18,18,18,18}	{21,21,21,21,21,21,21,21}
{8,1,8,1,8,1,8,1}	{4,5,4,2,4,5,4,2}	{4,2,4,5,4,2,4,5}
{13,1,9,1,13,1,9,1}	{4,5,4,2,4,5,4,2}	{10,2,10,5,10,2,10,5}
{3,1,6,1,3,1,6,1}	{4,5,4,2,4,5,4,2}	{7,2,7,5,7,2,7,5}
{14,1,11,1,14,1,11,1}	{4,5,4,2,4,5,4,2}	{12,2,12,5,12,2,12,5}
{9,43,1,37,13,42,1,36}	{10,47,5,39,10,46,2,38}	{4,45,2,41,4,44,5,40}
{8,23,1,22,8,23,1,22}	{4,27,5,31,4,24,2,26}	{4,24,2,26,4,27,5,31}
{3,32,1,28,6,34,1,25}	{4,27,5,31,4,24,2,26}	{7,33,2,29,7,35,5,30}
{1,15,1,15,1,15,1,15}	{5,16,2,19,5,16,2,19}	{2,19,5,16,2,19,5,16}
{15,15,15,15,15,15,15,15}	{19,19,19,19,19,19,19,19}	{16,16,16,16,16,16,16,16}
{36,36,36,36,36,36,36,36}	{38,38,38,38,38,38,38,38}	{40,40,40,40,40,40,40,40}
{37,37,37,37,37,37,37,37}	{41,41,41,41,41,41,41,41}	{39,39,39,39,39,39,39,39}
{22,22,22,22,22,22,22,22}	{26,26,26,26,26,26,26,26}	{31,31,31,31,31,31,31,31}
{25,25,25,25,25,25,25,25}	{26,26,26,26,26,26,26,26}	{30,30,30,30,30,30,30,30}
{28,28,28,28,28,28,28,28}	{29,29,29,29,29,29,29,29}	{31,31,31,31,31,31,31,31}
{43,43,43,43,43,43,43,43}	{47,47,47,47,47,47,47,47}	{45,45,45,45,45,45,45,45}
{42,42,42,42,42,42,42,42}	{44,44,44,44,44,44,44,44}	{46,46,46,46,46,46,46,46}
{23,23,23,23,23,23,23,23}	{27,27,27,27,27,27,27,27}	{24,24,24,24,24,24,24,24}
{32,32,32,32,32,32,32,32}	{27,27,27,27,27,27,27,27}	{33,33,33,33,33,33,33,33}
{34,34,34,34,34,34,34,34}	{35,35,35,35,35,35,35,35}	{24,24,24,24,24,24,24,24}

Таблица 1.

Рассмотрим теперь, имея все необходимые определения, идею, лежащую в основе конструкции этого автомата. Если мы обратим внимание на первые восемь обобщённых состояний, причём для обобщённых состояний второго типа ограничимся переходами по состояниям α и β, то увидим, что перед нами предстаёт автомат четвёртого порядка. В этом случае α и β можно рассматривать как слова

	α	β	γ	μ
{4,4,4,4,4,4,4,4}	{1,1,1,1,1,1,1,1}	{1,1,1,1,1,1,1,1}	{14,14,14,14,14,14,14,14}	{1,1,1,1,1,1,1,1}
{4,10,4,10,4,10,4,10}	{1,1,1,1,1,1,1,1}	{1,1,1,1,1,1,1,1}	{14,11,14,11,14,11,14,11}	{1,1,1,1,1,1,1,1}
{7,18,4,21,7,18,4,21}	{1,1,1,1,1,1,1,1}	{8,23,1,22,8,23,1,22}	{14,14,14,14,14,14,14,14}	{1,1,1,1,1,1,1,1}
{7,4,7,4,7,4,7,4}	{1,1,1,1,1,1,1,1}	{8,1,8,1,8,1,8,1}	{14,14,14,14,14,14,14,14}	{1,1,1,1,1,1,1,1}
{4,12,4,12,4,12,4,12}	{1,1,1,1,1,1,1,1}	{1,15,1,15,1,15,1,15}	{14,14,14,14,14,14,14,14}	{1,1,1,1,1,1,1,1}
{12,12,12,12,12,12,12,12}	{1,1,1,1,1,1,1,1}	{15,15,15,15,15,15,15,15}	{14,14,14,14,14,14,14,14}	{1,1,1,1,1,1,1,1}
{18,18,18,18,18,18,18,18}	{1,1,1,1,1,1,1,1}	{23,23,23,23,23,23,23,23}	{14,14,14,14,14,14,14,14}	{1,1,1,1,1,1,1,1}
{21,21,21,21,21,21,21,21}	{1,1,1,1,1,1,1,1}	{22,22,22,22,22,22,22,22}	{14,14,14,14,14,14,14,14}	{1,1,1,1,1,1,1,1}
{2,29,7,35,5,30,7,33}	{3,32,1,28,6,34,1,25}	{1,22,8,23,1,22,8,23}	{14,11,14,11,14,11,14,11}	{13,42,1,36,9,43,1,37}
{2,41,4,44,5,40,4,45}	{3,32,1,28,6,34,1,25}	{1,15,1,15,1,15,1,15}	{14,14,14,14,14,14,14,14}	{13,42,1,36,9,43,1,37}
{2,26,4,27,5,31,4,24}	{3,32,1,28,6,34,1,25}	{1,15,1,15,1,15,1,15}	{14,11,14,11,14,11,14,11}	{13,42,1,36,9,43,1,37}
{2,38,10,47,5,39,10,46}	{3,32,1,28,6,34,1,25}	{1,15,1,15,1,15,1,15}	{14,1,11,1,14,1,11,1}	{13,42,1,36,9,43,1,37}
{2,5,2,5,2,5,2,5}	{3,6,3,6,3,6,3,6}	{1,1,1,1,1,1,1,1}	{14,14,14,14,14,14,14,14}	{13,9,13,9,13,9,13,9}
{2,19,5,16,2,19,5,16}	{3,20,6,17,3,20,6,17}	{1,15,1,15,1,15,1,15}	{14,14,14,14,14,14,14,14}	{13,1,9,1,13,1,9,1}
{19,19,19,19,19,19,19,19}	{20,20,20,20,20,20,20,20}	{15,15,15,15,15,15,15,15}	{14,14,14,14,14,14,14,14}	{1,1,1,1,1,1,1,1}
{16,16,16,16,16,16,16,16}	{17,17,17,17,17,17,17,17}	{15,15,15,15,15,15,15,15}	{14,14,14,14,14,14,14,14}	{1,1,1,1,1,1,1,1}
{2,4,5,4,2,4,5,4}	{3,1,6,1,3,1,6,1}	{1,1,1,1,1,1,1,1}	{14,14,14,14,14,14,14,14}	{13,1,9,1,13,1,9,1}
{2,10,5,10,2,10,5,10}	{3,1,6,1,3,1,6,1}	{1,1,1,1,1,1,1,1}	{14,11,14,11,14,11,14,11}	{13,1,9,1,13,1,9,1}
{2,7,5,7,2,7,5,7}	{3,1,6,1,3,1,6,1}	{1,8,1,8,1,8,1,8}	{14,14,14,14,14,14,14,14}	{13,1,9,1,13,1,9,1}
{2,12,5,12,2,12,5,12}	{3,1,6,1,3,1,6,1}	{1,15,1,15,1,15,1,15}	{14,14,14,14,14,14,14,14}	{13,1,9,1,13,1,9,1}
{38,38,38,38,38,38,38,38}	{32,32,32,32,32,32,32,32}	{15,15,15,15,15,15,15,15}	{1,1,1,1,1,1,1,1}	{42,42,42,42,42,42,42,42}
{41,41,41,41,41,41,41,41}	{32,32,32,32,32,32,32,32}	{15,15,15,15,15,15,15,15}	{14,14,14,14,14,14,14,14}	{42,42,42,42,42,42,42,42}
{26,26,26,26,26,26,26,26}	{32,32,32,32,32,32,32,32}	{15,15,15,15,15,15,15,15}	{11,11,11,11,11,11,11,11}	{42,42,42,42,42,42,42,42}
{29,29,29,29,29,29,29,29}	{32,32,32,32,32,32,32,32}	{22,22,22,22,22,22,22,22}	{11,11,11,11,11,11,11,11}	{42,42,42,42,42,42,42,42}
{39,39,39,39,39,39,39,39}	{34,34,34,34,34,34,34,34}	{15,15,15,15,15,15,15,15}	{1,1,1,1,1,1,1,1}	{43,43,43,43,43,43,43,43}
{40,40,40,40,40,40,40,40}	{34,34,34,34,34,34,34,34}	{15,15,15,15,15,15,15,15}	{14,14,14,14,14,14,14,14}	{43,43,43,43,43,43,43,43}
{31,31,31,31,31,31,31,31}	{34,34,34,34,34,34,34,34}	{15,15,15,15,15,15,15,15}	{11,11,11,11,11,11,11,11}	{43,43,43,43,43,43,43,43}
{30,30,30,30,30,30,30,30}	{34,34,34,34,34,34,34,34}	{22,22,22,22,22,22,22,22}	{11,11,11,11,11,11,11,11}	{43,43,43,43,43,43,43,43}
{46,46,46,46,46,46,46,46}	{25,25,25,25,25,25,25,25}	{15,15,15,15,15,15,15,15}	{1,1,1,1,1,1,1,1}	{37,37,37,37,37,37,37,37}
{45,45,45,45,45,45,45,45}	{25,25,25,25,25,25,25,25}	{15,15,15,15,15,15,15,15}	{14,14,14,14,14,14,14,14}	{37,37,37,37,37,37,37,37}
{24,24,24,24,24,24,24,24}	{25,25,25,25,25,25,25,25}	{15,15,15,15,15,15,15,15}	{11,11,11,11,11,11,11,11}	{37,37,37,37,37,37,37,37}
{33,33,33,33,33,33,33,33}	{25,25,25,25,25,25,25,25}	{23,23,23,23,23,23,23,23}	{11,11,11,11,11,11,11,11}	{37,37,37,37,37,37,37,37}
{47,47,47,47,47,47,47,47}	{28,28,28,28,28,28,28,28}	{15,15,15,15,15,15,15,15}	{1,1,1,1,1,1,1,1}	{36,36,36,36,36,36,36,36}
{44,44,44,44,44,44,44,44}	{28,28,28,28,28,28,28,28}	{15,15,15,15,15,15,15,15}	{14,14,14,14,14,14,14,14}	{36,36,36,36,36,36,36,36}
{27,27,27,27,27,27,27,27}	{28,28,28,28,28,28,28,28}	{15,15,15,15,15,15,15,15}	{11,11,11,11,11,11,11,11}	{36,36,36,36,36,36,36,36}
{35,35,35,35,35,35,35,35}	{28,28,28,28,28,28,28,28}	{23,23,23,23,23,23,23,23}	{11,11,11,11,11,11,11,11}	{36,36,36,36,36,36,36,36}

Таблица 2.

единичной длины. Но мы ввели новые слова γ и μ, и «достроили» автомат четвёртого порядка до автомата восьмого порядка. Чтобы избежать очевидной некорректности, длины слов α и β необходимо увеличить, что, конечно, приводит к увеличению числа тождественных состояний в известной нам области диаграммы выстраиваемого автомата. Поэтому проще работать с обобщёнными диаграммами, где этого увеличения не происходит. Имея автомат четвёртого порядка и два «неиспользуемых» слова (γ и μ), мы вводим новые состояния с 9-го по 15-е и рёбра, позволяющие пройти по словам вида $a\mu b\gamma c\beta$ $(a, b, c \in \{0, 1\})$, как показано в диаграмме. Заметим, что после применения к автомату V_8^8 любого слова такого вида мы достигнем либо состояния $(q_1q_{15}, q_1q_{15}, q_1q_{15}, q_1q_{15})$, либо состояния $(q_{15}, q_1q_{15}, q_1q_{15}, q_1q_{15}, q_1)$. Рассмотрим первый случай (исходя из доказанных выше утверждений, мы вправе работать лишь с одним представителем класса циклической эквивалентности), автомат находится в состоянии $(q_1q_{15}, q_1q_{15}, q_1q_{15}, q_1q_{15})$, поскольку для состояния 15 автомата V_8 ещё не определены переходы по словам

$a_1\alpha_1 a_2\alpha_2 a_3 \ldots \alpha_{n-1} a_n \alpha_n$, где $a_i \in \{0,1\}$, $\alpha_i \in \{\alpha, \beta\}$, можно потребовать, чтобы никакое слово такого вида не переводило бы автомат V_8 из состояния 15 в какое-либо из первых четырнадцати состояний. Уже построенной части автомата и выполнения этого требования достаточно, чтобы утверждать, что автомат V_8 имеет не менее чем восьмой порядок (действительно, по слову $1\alpha1\beta$ из состояния $(q_1q_{15}, q_1q_{15}, q_1q_{15}, q_1q_{15})$ достигается состояние $(q_8, *, q_1, *, q_8, *, q_1, *)$, где каждая $*$ не равна q_1). Далее требуется достроить автомат V_8 так, чтобы его порядок не превышал восьми (не используя при этом состояния, реализующие отрицание). В решении этой задачи следует опираться на понятие циклической эквивалентности и рассматривать только одно состояние из класса циклически эквивалентных (как это было сделано для состояний $(q_1q_{15}, q_1q_{15}, q_1q_{15}, q_1q_{15})$ и $(q_{15}, q_1q_{15}, q_1q_{15}, q_1q_{15}q_1)$). Одним из примеров её решения является построенный автомат V_8

Аналогичным образом из автомата V_8 строится автомат V_{16} и можно показать, что несколько обобщая эти идеи, из автомата V_{2^n} порядка 2^n, имеющего одно отрицание, можно построить автомат $V_{2^{n+1}}$ порядка 2^{n+1}, также имеющий одно отрицание.

Автор выражает благодарность Станиславу Владимировичу Алёшину, под чьим руководством было выполнено решение рассмотренной задачи.

Список литературы

[1] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

[2] Макаров В. В. О группах автоматных перестановок // Фундаментальная и прикладная математика. — 1996. Т. 2. Вып. 1. — С. 171–186.

Методы интерполяции частично заданных законов функционирования автоматов

Епифанов А. С. (Саратов)

EpifanovAS@list.ru

Введение

В основополагающих работах, содержащих развитие теории автоматов (см., например, [1–4]), не рассматривается задача доопределения автоматов на основе единого подхода. Существуют задачи, при решении которых используемые методы предполагают полностью заданные законы функционирования автоматов, а в исходных данных эти законы представлены частично. Фундаментальные математические результаты по доопределению частично заданных графиков представлены классическими методами интерполяции Ньютона, Лагранжа, Гаусса, Бесселя, Стирлинга и др. Неприменимость этих методов для частично заданных автоматов связана с символьной формой задания автоматов таблицами, матрицами, графами, системами логических уравнений и т. п. Задание числовыми структурами законов функционирования автоматов на основе представления автоматных отображений числовыми графиками, предложенное и разработанное В. А. Твердохлебовым (см., например, [6]), позволяет использовать классические методы интерполяции в теории автоматов. В статье [5] изложены общие положения о возможности доопределения частично заданных геометрическими образами законов функционирования автоматов методами интерполяции.

В данной работе разработаны методы интерполяции для частично заданных законов функционирования автоматов, представленных геометрическими образами и использующие: базовые точки, вторые координаты которых получены сечениями геометрических образов прямыми линиями, параллельными оси абсцисс; базовые точки интерполяции, выделенные первыми элементами некоторых вершин геометрических образов. Получены оценки для сравнения по точности интерполяции методами Ньютона, Лагранжа и др. для частично заданных законов функционирования автоматов, последовательно-

сти вторых координат вершин геометрических образов которых определены числовыми последовательностями из массива The On-Line Encyclopedia of Integer Sequences (OEIS [8]). Получены оценки для автоматов с частично заданными геометрическими образами, представляющими класс (4,2,2)-автоматов и его подклассы и класс линейных (8,2,2)-автоматов.

Геометрические образы законов функционирования автоматов

Конечные детерминированные автоматы как математические модели сформировались для описания связей множеств сигналов и состояний с небольшим числом элементов. Это отражено в способах задания автоматов, основанных на явном указании функций переходов и выходов (таблицы, конечные графы, матрицы, логические уравнения с переменными, заданными на конечных множествах). Функционирование автоматов базируется на рекурсии, которая позволяет представлять как угодно большой, но только начальный, фрагмент процесса функционирования. В работе [6] В. А. Твердохлебовым разработан новый способ задания законов функционирования дискретных детерминированных динамических систем, основанный на числовых структурах. Предложенный подход позволяет задавать законы функционирования геометрическими фигурами, которые в свою очередь могут быть заданы аналитически.

Преобразование символьной формы автоматной модели в числовую структуру (геометрический образ законов функционирования автомата) включает линейное упорядочивание автоматного отображения $\rho_s = \bigcup\limits_{p \in X^*} \{(p, \lambda(s,p))\}$ для инициального автомата $A_s = (S, X, Y, \delta, \lambda, s)$, где S, X и Y — соответственно множества состояний, входных и выходных сигналов, а $\delta : S \times X \to S$ — функция переходов, $\lambda : S \times X \to Y$ — функция выходов и $s \in S$ — начальное состояние. Автоматное отображение ρ_s взаимнооднозначно преобразуется в автоматное отображение вида $\rho'_s = \bigcup\limits_{p \in X^*} \{(p, \lambda'(s,p))\}$, где $\lambda'(s,p)$ — последний знак последовательности $\lambda(s,p)$. Для преобразования множества пар ρ_s и ρ'_s в графики на множестве всех слов в алфавите X

вводится линейный порядок ω_1 (см. [6]). Упорядоченные множества пар (ρ_s, ω_1) и (ρ'_s, ω_1) дополняются линейными порядками ω_0 на Y^* и ω_2 на Y. В результате получаем графики $(\rho_s, \omega_1, \omega_0)$ и $(\rho'_s, \omega_1, \omega_2)$. Построенные графики размещены в системе координат с осью абсцисс (X^*, ω_1) и осями ординат соответственно (Y^*, ω_0) и (Y, ω_2). Замена элементов множеств X^* и Y в графике $\gamma_s = (\rho'_s, \omega_1, \omega_2)$ их номерами по порядкам ω_1 и ω_2 позволяет преобразовать символьный график γ_s в числовой график в системе координат с осью абсцисс N^+ и осью ординат $\{1, 2, \ldots, l\}$, где $|Y| = l$.

Из геометрического образа γ_s автомата A_s выделяется последовательность вторых координат точек геометрического образа, которая взаимнооднозначно соответствует полному геометрическому образу(при выбранном порядке ω_1 на X^*). В результате произвольная последовательность элементов из конечного множества может рассматриваться как последовательность вторых координат точек геометрического образа автомата и, следовательно, как задание законов функционирования автомата.

Методы интерполяции частично заданных законов функционирования автоматов

Выбор и применение метода интерполяции по смыслу соответствуют принятию и реализации гипотезы о том, что метод интерполяции, применяемый к числовому графику, представляющему частично заданный геометрический образ автомата, достаточно точно восстанавливает точки геометрического образа, то есть достаточно точно доопределяет частично заданные законы функционирования автомата. Следовательно, обоснованность результатов, полученных с использованием выбранного метода интерполяции, сведена к обоснованию правильности гипотезы.

Исследованные инициальные автоматы вида $A_s = (S, X, Y, \delta, \lambda, s)$, представлены классами автоматов: классами (n, m, l)-автоматов, где $n = |S|$, $m = |X|$, $l = |Y|$, и классами $(n, m, l)_d$ начальных отрезков геометрических образов длины d, определяющих автоматы из класса (n, m, l)-автоматов. В данной работе проведен сравнительный анализ точности интерполяции методами Ньютона и Лагранжа, а также

модифицированными методами Ньютона и Лагранжа. Модификация методов интерполяции состоит в том, что базовыми точками интерполяции являются точки геометрических образов автономных подавтоматов вида $A_1 = (S, \{0\}, Y, \delta, \lambda, s)$ и $A_2 = (S, \{1\}, Y, \delta, \lambda, s)$ (в случае $|X| = 2$).

Результаты анализа эффективности применения методов интерполяции Ньютона и Лагранжа по отношению к частично заданным геометрическими образами автономных подавтоматов автоматам классов (4,2,2)-автоматов и линейных (8,2,2)-автоматов при различных значениях длины начального отрезка геометрического образа систематизированы в форме лемм. Показано, что при небольших длинах частично заданных геометрических образах законов функционирования автоматов из класса (4,2,2)-автоматов, следует использовать метод интерполяции Ньютона, а при длинах геометрических образов от 126 до 254 интерполяция методами Ньютона и Лагранжа выравнивается по точности.

Также в работе предлагается следующий критерий выбора базовых точек интерполяции: базовыми точками интерполяции для доопределения графика, представляющего частично заданные законы функционирования автомата, предлагается использовать точки, расположенные на прямых, параллельных оси абсцисс. Такие точки удобно определять экспериментально с помощью простых устройств, выделяющих только один заданный сигнал — 0 или 1. На основе такого выбора базовых точек и использования классических методов интерполяции Ньютона и Лагранжа проведен анализ эффективности доопределения частичных автоматов, законы функционирования которых заданы последовательностями вторых координат точек геометрических образов длины до 1 млн. знаков. Полученные результаты систематизированы и представлены в виде лемм.

Список литературы

[1] Глушков В. М. Синтез цифровых автоматов. — М.: Физматгиз, 1962.

[2] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

[3] Брауер В. Введение в теорию конечных автоматов. — М.: Радио и связь, 1987.

[4] Гилл А. Введение в теорию конечных автоматов. — М.: Наука, 1966.

[5] Твердохлебов В. А. Методы интерполяции в техническом диагностировании // Проблемы управления. — 2007. № 2. — С. 28–34.

[6] Твердохлебов В. А. Геометрические образы законов функционирования автоматов. — Саратов: Научная книга, 2008.

[7] Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения / Под. ред. В. С. Харченко. Харьков: Изд-во Национальный аэрокосмический университет им. Н. Е. Жуковского («ХАИ»), 2011.

[8] www.oeis.org (дата обращения 20.07.2011).

Сложность полиномов Жегалкина и автоматная сложность булевых функций

Кибкало М. А. (Москва, МГУ им. М. В. Ломоносова)

mkibkalo@gmail.com

Определение сложности представления языков различными структурами — одна из традиционных задач теории автоматов. В случае представимости конечными автоматами под сложностью языка понимается число состояний в представляющем его приведенном автомате. В работе рассматривается сложность представления булевых функций конечными автоматами и устанавливаются точные значения и асимптотические оценки функции Шеннона для замкнутых классов булевых функций, входящих в решетку Поста.

Ключевые слова: булевы функции, конечные автоматы, сложность, классы Поста.

В произвольном конечном алфавите A определим класс конечных языков, содержащих слова равной длины: $\mathcal{L}_n(A) = \{L \subseteq A^n\}$. Каждой $f \in P_2^n$ можно взаимно однозначно сопоставить конечный язык $L(f) \in \mathcal{L}_n(E)$, где $E = \{0,1\}$ по следующему правилу: слово $\tilde{\alpha} = \alpha_1 \dots \alpha_n \in L(f) \Leftrightarrow f(\tilde{\alpha}) = f(\alpha_1, \dots, \alpha_n) = 1, \alpha_i \in E, i \in 1, \dots, n$.

Введем согласно [1] понятия инициального конечного автомата (ИКА) и представимости конечного языка в ИКА. Будем говорить, что ИКА $V_q = (E, Q, E, \varphi, \psi, q)$ представляет $f \in P_2^n$, если он представляет $L(f) \in \mathcal{L}_n(E)$.

Сложностью $S(V_q)$ ИКА V_q назовем число состояний в нем. Автоматной сложностью булевой функции $f \in P_2^n$ назовем наименьшую сложность ИКА, представляющего $L(f) \in \mathcal{L}_n(E)$:
$S(f,n) = \min_{V_q \sim L(f)} S(V_q)$. Пусть $\mathcal{K} \subseteq P_2$ — класс булевых функций, $\mathcal{K}(n) = \mathcal{K} \cap P_2^n$. Сложностью $\mathcal{K}(n)$ (функцией Шеннона класса $\mathcal{K}$) назовем $S(\mathcal{K}, n) = \max_{f \in \mathcal{K}(n)} S(f,n)$. Поскольку множество $\mathcal{K}(n)$ определяет совокупность языков из класса $\mathcal{L}_n(E)$, будем называть $S(\mathcal{K}, n)$ функцией Шеннона соответствующего класса конечных языков.

Будем пользоваться нотацией классов Поста, введенной в [2]. Асимптотическое поведение функции Шеннона автоматной сложности классов Поста C_i, $i = 1-4$, D_1, D_3, $F_i^\mu(n)$, $i = 1,4,5,8$, $\mu > 1$,

$\mu \in \mathbb{N}$, A_i, $i = 1-4$, $F_i^{\infty}(n)$, $i = 1-8$, $F_i^{\mu}(n)$, $i = 2,3,6,7$, $\mu > 2$, $\mu \in \mathbb{N}$ описано в [3],[4].

Положим $A(n) \asymp B(n)$, если $\exists c_1, c_2, 0 < c_1 \leqslant c_2$ такие, что $c_1 \cdot B(n) \lesssim A(n) \lesssim c_2 \cdot B(n)$.

Для получения оценок функции Шеннона для классов Поста D_2 и $F_i^2, i = 2,3,6,7$ использовались результаты, изложенные в [3]–[6].

Теорема 1. *Пусть $\mathcal{K}$ — один из классов D_2, $F_i^2, i = 2,3,6,7$. Тогда:*

$$S(\mathcal{K}, n) \asymp \frac{2^n}{n \cdot \sqrt{\log n}}.$$

При этом константы c_1, c_2 из определения отношения $\asymp$ равны

$$c_1 = \sqrt{2/\pi},\ c_2 = 2\sqrt{2/\pi}.$$

Отметим, что сложность реализации булевых функций конечными автоматами не коррелирует со сложностью реализации булевых функций полиномами Жегалкина. Сложность полинома Жегалкина булевой функции f определяется как число его ненулевых коэффициентов и обозначается $S^{\oplus}(f)$. В данной работе показано, что сложность полиномов Жегалкина для булевых функций, представляемых сложными автоматами, может кардинально отличаться.

Теорема 2. *Существует последовательность $n_p \to \infty$ при $p \to \infty$, такая что для функций $f'_{n_p}, f''_{n_p} \in P_2^{n_p}$ выполнено:*
$S(f'_{n_p}) = S(f''_{n_p}) \sim \frac{2^{n_p+1}}{n_p}$, *но* $S^{\oplus}(f'_{n_p}) \sim n_p$ *и* $S^{\oplus}(f''_{n_p}) \sim 2^{n_p}$.

Автор выражает благодарность академику Кудрявцеву В. Б. и проф. Бабину Д. Н. за ценные замечания и внимание к работе.

Список литературы

[1] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

[2] Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. — М.: Наука, 1966.

[3] Кузьмин А. Д. Реализация функций алгебры логики автоматами, нормальными алгорифмами и машинами Тьюринга // Проблемы кибернетики. — М.: Наука, 1955. Вып. 13. — С. 75–96. (РЖМат. 1966. 1В223).

[4] Кибкало М. А. Об автоматной сложности некоторых классов булевых функций // Интеллектуальные системы. — 2010. Т. 14. Вып. 1–4. — С. 319–322.

[5] Коршунов А. Д. О числе монотонных функций // Проблемы кибернетики. — 1981. Вып. 38. — С. 5–109.

[6] Сапоженко А. А. О числе антицепей в многослойных ранжированных множествах // Дискретная математика. — 1989. Т. 1. Вып. 2. — С. 110–128.

Внутреннее и внешнее наблюдение коллектива автоматов с одним состоянием

Курганский А. Н. (Донецк, ИПММ НАН Украины)

topologia@mail.ru

В работе рассматриваются коллективы автоматов с одним состоянием, взаимодействующие между собой в однородной вычислительной среде, заданной в виде ориентированного графа. Такие коллективы, а в работе они, чтобы подчеркнуть физические аналогии, названы телами, представляют собой распределенные вычислительные структуры и рассматриваются как цельные автоматоподобные системы. Можно провести аналогию между телами и клеточными автоматами, но вопросы, рассматриваемые в настоящей работе, и их решение делает разницу ними принципиальной. Прежде всего речь идет о том, как мы вводим понятие состояния тела.

В классических примерах автоматов, взаимодействующих со средой, автомат занимает одну вершину среды и в каждый момент времени переходит в одну из соседних вершин среды, при этом скорость изменения состояния автомата равна одному состоянию в единицу времени. Примерами здесь могут служить автоматы в лабиринте, машины Тьюринга, счётчиковые автоматы и др. Особенностью коллективов автоматов является распределенность по среде, которая влечет сложности при определении понятия состояния коллектива. В данной работе развивается подход [2], основывающийся на следующих рассуждениях. Во-первых, по определению элементарной частью коллектива является автомат с одним состоянием, поэтому состояние всего коллектива естественно определять его геометрией, то есть как инвариант некоторой группы преобразований среды. Во-вторых, всякое вычисление некоторым объектом невозможно без изменений в этом объекте, поэтому вычисление коллективом должно быть связано с изменениями его геометрии. Идея всей работы основывается на следующем примере шахматной доски и нескольких пешек.

Пусть пешки могут делать движение на одну клетку в любом из множества фиксированных на доске направлений в один такт времени. Составим из пешек на доске фигуру, например, букву «О» и

посмотрим на пешки как один цельный объект. Определим его скорость перемещения по шахматной доске как среднюю скорость пешек. Пусть объект движется с максимальной скоростью «одна клетка в единицу времени» в одном направлении. Может ли объект при этом каким-либо образом перестроиться из буквы «О», например, в букву «Т»? Нет, в этом примере при максимальной скорости в объекте невозможны вычисления. И, наоборот, в объекте возможны максимальные относительно шахматной доски по скорости вычисления, если он имеет близкую к 0 скорость. Эта идея, почерпнутая в [1], применяется к телам для определения связи между скоростью изменения состояния тела (вычислительное свойство) и скоростью перемещения (динамическое свойство). При этом сравниваются две точки зрения, названные внешним и внутренним наблюдением.

Внешнее наблюдение есть такое определение состояния тела, при котором тело рассматривается относительно среды, вернее, относительно системы отсчета, связанной со средой. В этом случае можно, например, говорить об абсолютных скоростях перемещения.

Внутреннее наблюдение характеризуется тем, что состояние тела определяется относительно самого тела, вернее, относительно системы отсчета связанной с телом. Состояние, определяемое таким образом, называется внутренним. Внутреннее состояние, как следует из определения, не зависит от скорости и деформации среды.

Тело как вычислительная модель определяется с точки зрения внутреннего наблюдения. Но для ее исследования естественно внешнее наблюдение. Например, при внешнем наблюдении естественен вопрос: может ли тело определить свою абсолютную скорость? Для внутреннего наблюдения он не имеет смысла. Еще пример: при внешнем наблюдении рассматриваемые среды являются дискретными и имеют некоторый порядок симметрии вращения. Будет ли среда дискретной и иметь тот же порядок симметрии вращения при внутреннем наблюдении? В целом работа имеет целью именно сравнение внешнего и внутреннего наблюдения.

Назовем $D = \{1, 2, \ldots, m\}$ множеством актуальных пространственных направлений. (n, m)-Среда — ориентированный граф. Дугам графа приписывается направление из D. Если различные дуги входят в одну и ту же вершину, то говорим, что они пересекаются.

Граф вложен в n-мерное аффинное метрическое пространство E так, что дуги среды являются отрезками прямых, имеют длину $\frac{1}{n+1}$ и дуги одного направления лежат на параллельных прямых. Зафиксируем систему отсчета в E. Пространство E назовем абсолютным, а координаты в нем абсолютными пространственными координатами. Пару (x, t), где $x \in E$, t — время, называем пространственно-временной координатой в абсолютной системе отсчета O или, просто, *событием*. Пусть D является множеством векторов $\{\overrightarrow{1}, \overrightarrow{2}, \ldots, \overrightarrow{m}\}$ в E. Обозначим $e_i = (\overrightarrow{i}, 1)$, $1 \leqslant i \leqslant m$. Назовем $\{e_i\}_{1 \leqslant i \leqslant m}$ множеством *актуальных пространственно-временных* направлений, которые образуют абсолютную *актуальную систему отсчета* Q.

Элементарным телом или, короче, 1-телом назовем автомат Мили с одним состоянием. Для удобства говорим, что изоморфные 1-тела имеют одинаковые цвета, неизоморфные — разные. Предполагаем, что используются r различных цветов, пронумерованных целыми от 1 до r. В каждый момент времени $t \in Z$ 1-тело b находится на какой-либо одной дуге $b(t)$ среды. Входным сигналом тела b, находящегося на дуге e, входящей в вершину v, является упорядоченный набор чисел $(p_{ij})_{1 \leqslant i \leqslant |D|, 1 \leqslant j \leqslant r}$, где p_{ij} — число 1-тел цвета j, находящихся на дуге направления i, входящей в вершину v. Выходом тела b является направление из D. Если выходом тела b, находящегося в момент t на дуге, входящей в вершину v, является направление i, то в момент $t+1$ оно находится на дуге направления i, исходящей из v. Если направления дуг $b(t)$ и $b(t+1)$ совпадают, то говорим, что *внешнее состояние* тела b не изменилось и оно движется прямолинейно. Иначе говорим, что внешнее состояние b изменилось. 1-тело движется прямолинейно, если все пересекающие $b(t)$ дуги пусты.

Обозначим через $\tau_b(t)$ меру изменений внешнего состояния b, состоявшихся к моменту времени t. По определению, если с t_1 до t_2 b двигалось прямолинейно, то $\tau_b(t_1) = \tau_b(t_2)$. Обозначим $w_b(t) = \tau_b(t+1) - \tau_b(t)$.

Представим дискретную динамику b на графе непрерывной динамикой в пространстве E. Координату b в момент t обозначим через $x_b(t)$. Пусть $b(t) = (v_0, v_1)$, $t \in Z$, и координаты вершин v_0 и v_1 равны x_0 и x_1 соответственно, тогда $x_b(t + \lambda) = x_0 + \lambda(x_1 - x_0)$, $0 \leqslant \lambda < 1$.

Определение. Тело — конечное множество 1-тел.

Тело состоящее из k 1-тел называем также k-телом. Если 1-тело принадлежит телу, то называем его элементарной частью этого тела.

Пусть $B = \{b_1, \ldots, b_k\}$ — k-тело. Координатой тела B в момент времени t называется $x_B(t) = (x_1(t) + \cdots + x_k(t))/k$. Введем меру $\tau = \tau_B(t)$ изменения внешнего состояния тела B, которую также назовем $\tau_B(t)$ собственным временем B. Величину $w_B(t) = \tau_B(t+1) - \tau_B(t)$ назовем скоростью собственного времени тела B, а величину $v_B(t) = x_B(t+1) - x_B(t)$ абсолютной скоростью перемещения B.

Определение. Для любого тела B $w_B(t) = 0 \Leftrightarrow \forall_{b \in B} w_b(t) = 0$.

То есть, два тела находятся в среде в одном и том же внешнем состоянии, если одно из них может быть получено из другого прямолинейным сдвигом каждой его элементарной части на равное число шагов в направлении, соответствующем внешнему состоянию.

Следствие. *Если* $|v_B(t)| = 1$, *то* $w_B(t) = 0$.

Следствие. *Два тела, движущиеся с различной скоростью, находятся в различных внешних состояниях.*

Система отсчета O_B тела B есть такой способ приписывания пространственно-временных координат событиям, при котором, по определению, $x_{BB}(\tau_B) \equiv 0$, $v_{BB}(\tau_B) \equiv 0$ и $w_{BB}(\tau_B) \equiv 1$, где $x_{AB}(\tau_B)$, $v_{AB}(\tau_B)$, $w_{AB}(\tau_B)$ и $\tau_{AB}(\tau_B)$ обозначают координату, скорость перемещения, скорость собственного времени и собственное время тела A в момент времени τ_B в системе отсчета O_B соответственно.

Определение. Тела A и B находятся в одном внутреннем состоянии в моменты собственного времени τ_A и τ_B соответственно, если $\{(b, x_{bA}(\tau_A)) | b \in A\} = \{(\varphi(b), x_{bB}(\tau_B)) | b \in B\}$ для некоторой биекции $\varphi : A \to B$ такой, что $b \in A$ и $\varphi(b) \in B$ изоморфны.

Состояние тела как вычислительной модели есть его внутреннее состояние. Тело B инерциальное в O_A, если v_{BA} и w_{BA} константы. Система отсчета O_A инерциальная, если A инерциальное в O.

Определение. Среда корректная, если любые инерциальные системы отсчета в ней можно связать аффинным преобразованием.

Теорема 1. $\{e_i\}_{1 \leqslant i \leqslant m}$ — *собственные вектора аффинных преобразований, связывающих инерциальные системы отсчета.*

Следствие. *Верно:* $v_{AB} = -v_{BA}$, $w_{AB} \cdot w_{BA} = 1 - v_{AB}^2 = 1 - v_{BA}^2$.

Следствие. *Если* $m \neq n + 1$, *то* (n, m)*-среда не корректная.*

Теорема 2. *Степень симметрии вращения среды может не совпадать при внутреннем и внешнем наблюдении.*

Абсолютная скорость и актуальные пространственные направления не имеют смысла при внутреннем наблюдении.

Список литературы

[1] Пуанкаре А. О науке. — М.: Наука, 1983.

[2] Kurganskyy O. A state of a dynamic computational structure distributed in an environment: a model and its corollaries // Труды ИПММ НАНУ. — 2010. Вып. 21. — С. 150–160.

О минимизации монофункциональных классов бинарных клеточных автоматов с неразрешимым свойством обратимости

Кучеренко И. В. (Москва, МГУ им. М. В. Ломоносова)

kucherenko@intsys.msu.ru

Клеточные автоматы (КА) являются дискретной математической моделью процессов, для которых существенна не только временная, но и пространственная протяженность [1]. Важное семейство клеточных автоматов образуют обратимые КА, то есть такие, в которых «предыстория» возникновения конфигурации определяется однозначно. Класс обратимых КА представляет как теоретический, так и прикладной интерес — в связи с задачами защиты информации, синтеза квантовых вычислителей, проектирования вычислительных систем с пониженным энергопотреблением и других.

В работе пойдет речь о задаче алгоритмического распознавания свойства обратимости в классах двумерных бинарных КА (у которых ячейка имеет два состояния). Автором установлено, что свойство обратимости не распознаваемо в классе всех двумерных бинарных клеточных автоматов [2]. С другой стороны, в классе двумерных бинарных клеточных автоматов, в которых содержатся только КА с линейными локальными функциями переходов, свойство обратимости разрешимо [3]. В связи с этим возникает задача классификации «естественных» классов КА на те, в которых свойство обратимости разрешимо, и те, для которых это не так.

В работе рассматриваются классы бинарных двумерных КА, имеющих фиксированную локальную функцию переходов (в таком классе варьируются исключительно вектора в локальном шаблоне соседства); такие классы будем называть монофункциональными. Автором построен монофункциональный класс двухмерных бинарных клеточных автоматов, в котором задача распознавания свойства обратимости является алгоритмически не разрешимой. Получена оценка для числа существенных переменных локальной функции переходов в данном классе.

Приведем необходимые для понимания полученного результата определения. Формально клеточный автомат σ представляет из себя четверку вида (Z^k, E_n, V, φ), где Z^k — совокупность всех k-мерных векторов с целочисленными координатами, E_n — конечное множество из n элементов, природа которых не существенна. Для простоты их можно считать числами из множества $\{0, 1, \ldots, n-1\}$. $V = \{v_1, v_2, \ldots, v_m\}$ — упорядоченный набор различных ненулевых векторов из Z^k. $\varphi : (E_n)^{m+1} \mapsto E_n$, $\varphi(0, 0, \ldots, 0) = 0$. Элементы множества Z^k называются ячейками, E_n — состояниями ячеек, 0 — состояние покоя. При помощи шаблона соседства V каждой ячейке α ставится в соответствие набор векторов $V(\alpha) = \{\alpha, \alpha + v_1, \alpha + v_2, \ldots, \alpha + v_m\}$, который называется ее окрестностью. Функция φ называется локальной функцией переходов клеточного автомата.

Функции $g : Z^k \mapsto E_n$ называются состояниями КА. Основная функция переходов Φ задается как отображение множества всех состояний клеточного автомата σ в себя, причем если $g = \Phi(g')$, то $g(\alpha) = \varphi(g'(\alpha), g'(\alpha + v_1), g'(\alpha + v_2), \ldots, g'(\alpha + v_m)), \forall\alpha$. Функционирование КА определяется как последовательность его состояний $g_0, g_1, g_2, \ldots$, получающаяся в результате применения основной функции переходов к некоторому его состоянию g_0, то есть $g_t = \Phi(g_{t-1}) = \Phi^t(g_0)$, t — натуральное число. Состояние клеточного автомата, в котором только конечное число ячеек находится в ненулевом состоянии, называется конфигурацией.

Клеточный автомат, основная функция переходов которого инъективна на множестве всех конфигураций, называется обратимым. По теореме Мура-Майхилла [1] множество обратимых клеточных автоматов совпадает с множеством КА, основная функция переходов которых является сюръективной.

Пусть φ — булева функция, зависящая от $m + 1$ переменных и сохраняющая ноль. Множество двумерных клеточных автоматов с локальной функцией переходов φ обозначим через $CA(2, 2, m, \varphi)$. Будем задавать индивидуальные клеточные автоматы из множества $CA(2, 2, m, \varphi)$ набором из m двумерных ненулевых целочисленных векторов V (их шаблоном соседства). Задача алгоритмического распознавания свойства обратимости заключается в построении машины Тьюринга (МТ), которая на наборе $V = ((x_1, y_1), (x_2, y_2), \ldots,$

(x_m, y_m)), записанному на ее ленте в виде последовательности из $2 \cdot m$ натуральных чисел $x_1, y_1, x_2, y_2, \ldots, x_m, y_m$ в унитарной записи (отдельные числа разделяются одиночной буквой «0»; в начальном состоянии на всей «свободной» части ленты записана буква «0», головка находится над самой левой буквой «1» конфигурации), останавливалась, при этом в ячейке ленты, находящейся под головкой в момент остановки, должно находиться буква «1», если клеточный автомат $\sigma = (Z^2, E_2, V, \varphi)$ обратим, или «0», если σ не обратим.

Основной результат работы получается сведением проблемы обратимости КА к проблеме остановки МТ в специальной формулировке. Применяемая конструкция позволяет дополнительно получить оценку на число переменных функции φ, но это требует определения параметров исходной проблемы. Обозначим через q число состояний головки машины Тьюринга $\varkappa$, обладающей следующими свойствами.

1) МТ $\varkappa$ имеет одну ленту с двумя состояниями.
2) Рассматриваются только вычисления $\varkappa$, в которых в начальный момент времени головка стоит над самой левой буквой слова.
3) Проблема остановки $\varkappa$ на словах, представляющих из себя наборы из одних единиц, не разрешима.

Теорема 1. *Существует булева функция $\varphi(x_0, x_1, \ldots, x_m)$, такая, что в классе $CA(2, 2, m, \varphi)$ свойство обратимости алгоритмически не разрешимо, при этом*

$$m \leqslant 7 \cdot (5 + 2 \cdot] \log_2(26 \cdot (q + 5))[) - 1.$$

Автор выражает благодарность научному руководителю академику В. Б. Кудрявцеву за постановку задачи и внимание к работе.

Список литературы

[1] Кудрявцев В. Б., Подколзин А. С., Болотов А. А. Основы теории однородных структур. — М.: Наука, 1990.

[2] Кучеренко И. В. О разрешимости обратимости клеточных автоматов // Интеллектуальные системы. — 2004. Т. 8. Вып. 1–4. — С. 465–482.

[3] Кучеренко И. В. О структуризации класса обратимых бинарных клеточных автоматов // Интеллектуальные системы. — 2005. Т. 9. Вып. 1–4. — С. 445–456.

О выразимости суперпозициями групповых автоматов Медведева

Летуновский А. А. (Москва)

alekseyletunovskiy@gmail.com

Рассматривается задача выразимости конечного автомата A суперпозициями систем вида $\Phi \cup \nu$, где Φ состоит из всех булевых функций и «задержки», ν — произвольная конечная система автоматов. Ранее автор показал, что для автомата A с безусловными переходами существует алгоритм проверки $A \in [\Phi \cup \nu]$. В настоящей работе показано, что задача выразимости через системы $\Phi \cup \nu$ групповых автоматов Медведева алгоритмически разрешима.

Задача выразимости автоматов относительно суперпозиции наталкивается на существенные трудности [2]. В общем случае она является алгоритмически неразрешимой, а разрешимые случаи сводятся к теоретико-групповым конструкциям [3, 4]. Относительно суперпозиции не существует конечных полных систем, а как показал Бабин Д. Н. [5], арность полных систем может быть выбрана равной 2. Задача полноты относительно композиции разрешима, когда в базисе всегда есть булевы функции [6, 7]. В нашем случае предполагается наличие в выражающей системе автоматов штрих Шеффера и «задержка». Ранее автором было показано существование алгоритма выразимости константных автоматов [8], а в настоящей работе в список автоматов, для которых есть алгоритм выразимости через системы с добавкой из штриха Шеффера и «задержки», включены групповые автоматы Медведева.

Пусть $E_2 = \{0, 1\}$, функции вида $g : E_2^n \to E_2$ называются булевыми функциями, их множество обозначается через P_2. Пусть E_2^∞ — множество всех сверхслов вида $a(1)a(2)\ldots$, где $a(j) \in E_2$, $j = 1, 2, \ldots$. Пусть

$$f : (E_2^\infty)^n \to (E_2^\infty)^m$$

— автоматная функция (a-функция), то есть она задается рекуррентно соотношениями, согласно каноническим уравнениям [1].

Шестерка

$$(E_2^n, E_2^s, E_2^m, \varphi, \psi, q_0),$$

где вектор $q = (q_1, \ldots, q_s) \in E_2^s$ — состояние a-функции f, q_0 — ее начальное состояние, буквы $a = (a_1, a_2, \ldots, a_n) \in E_2^n$ и $b = (b_1, \ldots, b_m) \in E_2^m$ — входная и выходная буквы, а сверхслова $a(1)a(2)\ldots$ и $b(1)b(2)\ldots$ — входные и выходные сверхслова соответственно, вектор-функции $\varphi : E_2^n \times E_2^s \to E_2^s$ и $\psi : E_2^n \times E_2^s \to E_2^m$ — функции переходов и выходов соответственно, называется автоматом, задающим автоматную функцию.

Класс всех a-функций обозначим через P. Автомат M называется *автоматом Медведева,* если $s = m, \psi(a, q) = q$.

В этом классе обычным образом введем операции суперпозиции [1].

Пусть $M \subseteq P$, обозначим через $[M]$ множество a-функций, получающихся из M с помощью операций суперпозиции.

Автоматную функцию G_0, задаваемую уравнениями

$$\begin{cases} q(1) = 0, \\ q(t+1) = a(t), \\ b(t) = q(t), \end{cases}$$

назовём автоматной функцией «задержки».

Если для каждого $a \in A$ $\varphi_a(q) : E_2^s \to E_2^s$, где $\varphi(q, a) = \varphi_a(q)$ является биекцией, то автомат называется групповым.

Мы будем рассматривать задачу выразимости групповых автоматов Медведева через системы вида $\Phi \cup \nu$, где Φ состоит их всех булевых функций и «задержки», ν — произвольная конечная система автоматов.

Теорема. *Пусть A — произвольный групповой автомат Медведева, тогда задача $A \in [\Phi \cup \nu]$ является алгоритмически разрешимой.*

Список литературы

[1] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

[2] Кратко М. И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов // ДАН СССР. — 1964. Т. 155. № 1. — С. 35–37.

[3] Арбиб М. Алгебраическая теория автоматов языков и полугрупп. — М.: Статистика, 1975.

[4] Алешин С. В. Об одном следствии теоремы Крона — Роудза // Дискретная математика. — 1999. Т. 11. Вып. 4. — С. 101–109.

[5] Бабин Д. Н. О полноте двухместных автоматных функций относительно суперпозиции // Дискретная матетматика. — 1989. Т. 1. Вып. 4. — С. 423–431.

[6] Буевич В. А. Условия A-полноты для автоматов. — М.: МГУ, 1986.

[7] Бабин Д. Н. О классификации автоматных базисов Поста по разрешимости свойств полноты и A-полноты // ДАН. — 1999. Т. 367. № 4. — С. 439–441.

[8] Летуновский А. А. О выразимости константных автоматов // Интеллектуальные системы. — 2005. Т. 9. Вып. 1–4. — С. 457–469.

Частичное угадывание сверхсобытий, образованных детерминированными контекстно-свободными языками

Мастихина А. А. (Москва, МГУ им. М. В. Ломоносова)

anmast@yandex.ru

Рассматривается задача частичного угадывания любой последовательности из нулей и единиц из заданного множества детерминированными, но, возможно, бесконечными автоматами. Детерминированность автомата означает, что после подачи на его вход t первых символов сверхслова он однозначно выдает некоторый выходной символ. Ранее критерии частичной угадываемости были получены для общерегулярных сверхсобытий [3] и для сверхсобытий вида L^∞, где L порождается простой $LL(1)$-грамматикой [4].

Выходное сверхслово некоторого автомата $\mathfrak{A}$ при подаче на его вход сверхслова $\alpha \in \{0,1\}^\infty$ будем обозначать через $y_\alpha^{\mathfrak{A}}$.

Автомат $\mathfrak{A}$ *угадывает сверхслово* $\alpha \in \{0,1\}^\infty$ *со степенью* $\sigma \in [0,1]$, если

$$c^{\mathfrak{A}}(\alpha) = \underline{\lim}_{t\to\infty} \frac{1}{t} \sum_{i=1}^{t} (1 - |y_\alpha^{\mathfrak{A}}(i) - \alpha(i+1)|) = \sigma.$$

Автомат $\mathfrak{A}$ *частично угадывает* множество сверхслов A, если для любого $\alpha \in A$ найдется такое $\sigma > 0$, что выполнено $c^{\mathfrak{A}}(\alpha) > \sigma > 0$. Множество A *частично угадываемо*, если найдется частично угадывающий его автомат $\mathfrak{A}$.

Степень угадывания множества A

$$c^{\mathfrak{A}}(A) = \inf_{\alpha\in A} c^{\mathfrak{A}}(\alpha).$$

Определим *автомат с магазинной памятью* как семерку $(Q, \Sigma, \Gamma, Z, \Phi, q_0, F)$, где Q — множество состояний, выделенное начальное состояние $q_0 \in Q$ и некоторое множество $F \subseteq Q$ заключительных состояний, Σ — входной алфавит, Γ — магазинный алфавит, Φ — множество команд, каждая команда — отображение $(Q \times (\Sigma \cup \lambda) \times \Gamma \to Q \times \Gamma^*)$, где λ — пустое слово, Z — символ для обозначения пустого магазина. Тактом работы будем считать выполнение возможных команд после поступления одного входного символа.

Выполнение команды, содержащей в левой части λ, не будем считать отдельным тактом.

Конфигурацией будем называть пару $(q, \xi), q \in Q, \xi \in \Gamma^*$: текущее состояние и содержимое магазина.

МП-автомат *допускает язык* L, если только после подачи слов $\alpha \in L$ на начальную конфигурацию (q_0, S) автомат приходит в конфигурацию $(q, Z), q \in F$.

Автомат называется *детерминированным*, если для каждой конфигурации (q, ξ) имеется либо не более одной команды вида $(q, a, \xi]_1 \to r, \beta), q, r \in Q, \xi, \beta \in \Gamma^*$ для каждого $a \in \Sigma$ и ни одной команды вида $(q, \lambda, \xi]_1 \to r', \beta'), r' \in Q, \beta' \in \Gamma^*$, либо ни одной команды вида $(q, a, \xi]_1 \to r, \beta)$ и не более одной вида $(q, \lambda, \xi]_1 \to r', \beta')$.

Класс языков, допускаемых детерминированными автоматами с магазинной памятью — класс детерминированных контекстно-свободных языков.

Так как класс детерминированных контекстно-свободных языков не замкнут относительно конкатенации, будем рассматривать такие языки, что их итерация есть детерминированный контекстно-свободный язык.

Далее будем рассматривать Z как элемент Γ, а (q_0, Z) возьмем в качестве начальной конфигурации, то есть автомат работает с пустым магазином.

Строится допускающий детерминированный автомат с магазинной памятью для итерации языка L. На него подается его сверхитерация. Можно заметить, что при подаче любого сверхслова из множества L^∞ автомат оказывается в какой-нибудь конфигурации $(q, Z), q \in F$ бесконечное число раз. Это может быть верно и для других сверхслов, но предполагается, что сверхслова не из L^∞ просто не поступают на вход.

Теорема. *Пусть язык L^* допускается детерминированным автоматом с магазинной памятью $\mathfrak{A} = (Q, \{0, 1\}, \Gamma, Z, \Phi, q_0, F)$. Множество L^∞ является частично угадываемым тогда и только тогда, когда для некоторой пары $(q, A), q \in Q, A \in \Gamma$ существует только одна команда вида $(q, a, A \to r, \beta), a \in \{0, 1\}, r \in Q, \beta \in \Gamma^*$.*

Необходимость обосновывается тем, что в противном случае в любой конфигурации $\mathfrak{A}$ есть два варианта следующей входной буквы, поэтому для любого детерминированного автомата возможно построение сверхслова из L^∞ с любым количеством неугаданных подряд символов. Для такого сверхслова можно выбрать подпоследовательность, на которой доля угаданных символов стремится к нулю. Поэтому степень угадывания соответствующего множества будет равна нулю.

Если же есть конфигурации, в которых возможна только одна команда (не с λ в левой части), то следующая буква известна. Для остальных конфигураций выбирается та буква, которая отдаляет допускающий автомат от конфигурации с одной альтернативой. С этой целью для состояния и магазинного символа вычисляется кратчайшее слово, приводящий автомат в конфигурацию с одной альтернативой без укорачивания магазина, если такой существует, либо кратчайший путь, укорачивающий магазин.

Для частичного угадывания используется автомат с магазинной памятью с выходом.

Пример. Рассмотрим детерминированный автомат с магазинной памятью $\mathfrak{A} = (Q, \{0,1\}, \Gamma, Z, \Phi, q_0, F)$, где $Q = \{q_0, q_1, q_2\}$, $\Gamma = \{A, Z\}$, $F = q_0$, а множество команд Φ таково:

$$
\begin{array}{l}
(q_0, 1, Z \to q_1, \lambda),\\
(q_1, 1, Z \to q_1, A)\\
(q_1, 0, A \to q_1, AA),\\
(q_1, 1, A \to q_2, A),\\
(q_2, \lambda, Z \to q_0, \lambda),\\
(q_2, 0, A \to q_2, \lambda),\\
(q_2, 1, A \to q_1, A).
\end{array}
$$

Данный автомат допускает итерацию языка
$L = \{110^{n_1}10^{n_2}1\ldots10^{n_{2k}} | \Sigma_{i=1}^{k} n_{2i} = \Sigma_{i=1}^{k} n_{2i-1} + 1\}$.

Добавим автомату выходную функцию, сопоставив парам (q, B), $q \in Q$, $B \in \Gamma$, для которых есть команды, начинающиеся на q, a, B, $a \in \{0,1\}$, значение $f(q, B) \in \{0,1\}$. Полученное устройство $\mathfrak{A}'$ будет частично угадывать L^∞.

В конфигурациях (q_1, Z) и (q_0, Z) есть только по одной команде для входной буквы 1, поэтому выходная функция будет $f(q_1, Z) = 1$, $f(q_0, Z) = 1$, и в этих конфигурациях автомат будет угадывать.

Введем функцию $\mu : Q \times \Gamma \to \{0, 1, 2, \ldots\}$, равную наименьшей длине входного слова, переводящего автомат из конфигурации $(q, A\xi)$ в (r, ξ) для некоторого $r \in Q$, то есть укорачивающего магазин.

$\mu(q_2, A) = 1$, причем укорачивание происходит при выполнении команды $(q_2, 0, A \to q_2, \lambda)$, поэтому зададим $f(q_2, A) = 1$.

$\mu(q_1, A) = 2$, так как после команды $(q_1, 1, A \to q_2, A)$ автомат попадает в конфигурацию $(q_2, A\xi)$, слово, укорачивающее магазин — 10, поэтому $f(q_1, A) = 0$.

Степень угадывания $c^{\mathfrak{A}'}(L^\infty) = \frac{1}{2}$, и $\frac{1}{2}$ достигается на сверхслове $(1110)^\infty$.

Автор выражает благодарность профессору Э. Э. Гасанову за постановку задачи и помощь в работе.

Список литературы

[1] Вереникин А. Г., Гасанов Э. Э. Об автоматной детерминизации множеств сверхслов // Дискретная математика. — 2006. Т. 18. № 2. — С. 84–97.

[2] Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции: Пер. с англ. — М.: Мир, 1978.

[3] Мастихина А. А. Критерий частичного предвосхищения общерегулярных свехсобытий // Дискретная математика. — 2011.

[4] Мастихина А. А. Частичное угадывание некоторых контекстно-свободных языков // Материалы XVIII Международной конференции студентов, аспирантов и молодых учёных «Ломоносов».

Вторая автоматная функция и с нею связанные классы регулярных языков

Пархоменко Д. В. (Москва, МГУ им. М. В. Ломоносова)

dcdenis@rambler.ru

В докладе будут рассмотрены множества слов конечного алфавита, возникающие на выходе детерминированных автоматов и изучены их свойства. Будут введены ранее не исследовавшиеся классы регулярных языков. Введено новое понятие второй автоматной функции.

Пусть задан КДА $V = (A, Q, B, \varphi, \psi, q_0)$, $|A| = |B|$, *и его автоматная функция* $f_V \colon A^* \to B^*$. *Тогда функция* $\kappa \colon B^* \to \mathbb{N} \cup \{0\}$, $\kappa(\beta) = |\{\alpha \in B^* \mid f_V(\alpha) = \beta\}|$ *называется второй автоматной функцией автомата* V.

Пусть для любого натурального $p : L_p(V) = \{\beta \in B^* | \kappa_V(\beta) \in p\}$. В частности, при $p = 1, L_p(V)$ суть автоматно перечислимое множество слов. Очевидно, для любого автомата $V : L_p(V) \subseteq L_{p-1}(V)$, для всех $p \geqslant 2$. Справедлива:

Теорема 1. *Для любого конечного инициального автомата* V *и для всякого* $p \geqslant 1$, $L_p(V)$ *— регулярный язык.*

Утверждение. *Пусть дан автомат* V. *Если для некоторого* $i \in \aleph$, *слово* $\beta \in L_p(V)$, *то найдется буква* b *выходного алфавита автомата* V *такая, что* $\beta b \in L_p(V)$.

Следствие. *Для любого натурального* p *и автомата* $V, L_p(V)$ *либо бесконечное множество, либо пустое.*

Пусть $\mathcal{L}_p = \{L_p(V)|V\}$. Имеет место

Теорема 2. *Для любых натуральных* $i < j$ *выполнено:* $\mathcal{L}_i \nsubseteq \mathcal{L}_j$.

Автор выражает глубокую благодарность своему профессору, д.ф.-м.н. Бабину Дмитрию Николаевичу за постановку задачи и ценные советы в процессы работы.

Список литературы

[1] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Элементы теории автоматов. — М.: Изд-во МГУ, 1978.

Геометрические модели и методы распознавания автоматов

Твердохлебов В. А. (Саратов)

TverdokhlebovVA@list.ru

В работах 1995–1996 гг. [1–2] предложен, а в дальнейшем [3–5] разработан новый способ задания инициального дискретного детерминированного автомата $A = (S, X, Y, \delta, \lambda, s_0)$, где S, X и Y — множества состояний, входных и выходных сигналов, $\delta : S \times X \to S$ и $\lambda : S \times X \to Y$ — функции переходов и выходов, а s_0 — начальное состояние. Построены и проанализированы примеры эффективности предлагаемого способа задания автоматов, которые убедили не только автора (см. [6]), но и других специалистов в полезности нового способа задания автоматов. В связи с этим приводятся модели и методы, в которых представлен новый способ. Автомату A соответствуют эквивалентные автоматные отображения $\rho_s = \bigcup\limits_{p \in X^*} \{(p, \lambda(s, p))\}$ и $\rho'_s = \bigcup\limits_{p \in X^*} \{(p'x, \lambda(\delta(s, p'), x))\}$. Предлагаемому способу задания автоматов соответствуют три вида структур — символьный график и два числовых графика с целочисленными и вещественными координатами точек. Символьный график автоматного отображения представляется в системе координат с осью абсцисс (X^*, ω_1) и осью ординат (Y, ω_2), где ω_1 и ω_2 — линейные порядки на множествах X^* и Y. В графике с положительными целочисленными координатами точек каждая точка (p, y), где $p \in X^*$ и $y \in Y$, преобразована в точку $(r_1(p), r_2(y))$, где $r_1(p)$ и $r_2(y)$ — номера p и y по линейным порядкам ω_1 и ω_2. В связи с тем, что задание автоматного отображения числовыми графиками позволяет использовать в теории автоматов мощные идеализации непрерывной математики (актуальную бесконечность, бесконечно малую величину, непрерывность, предельный переход, суммирование бесконечных рядов и др.), разработан способ задания автомата, основывающийся на отображении вида $\varphi_X : X^* \to R^+$ и $\varphi_Y : Y \to \{\alpha_1, \alpha_2, \ldots, \alpha_l\}$, где α_i — полуинтервалы, составляющие единый полуинтервал на оси ординат, являющейся частью оси ординат первого квадранта прямоугольной декартовой системы ко-

ординат на плоскости. В этом случае положение на оси абсцисс элемента $p \in X^*$ определяется точно, а элементу $y \in Y$ соответствует полуинтервал. При новом способе задания инициального автомата моделью автоматного отображения является множество точек, представляющее автоматное отображение в целом и варианты сечений этого множества, выделяющие подмножества, соответствующие конкретным вариантам функционирования автомата. Числовая форма автоматного отображения позволяет располагать точки графика на геометрических кривых линиях, заданных аналитически. Это, в свою очередь, позволяет рассматривать свойства автоматного отображения как свойства геометрических кривых и использовать вычисления с применением уравнений и неравенств, связанных с геометрическими кривыми. Для линейных порядков ω_1 и ω_2, соответствующих лексикографическому упорядочиванию, имеет место теорема.

Теорема 1. *Пусть $p \in X^*$ и $p = x_{i_1}x_{i_2}\dots x_{i_k}$, где $k \in N^+$. Тогда номер $r(p)$ слова p по порядку ω_1 определяется равенством:*

$$r(p) = \sum_{j=1}^{k} r(x_{i_j}) \cdot |X|^{j-1} - 1.$$

Следующие теоремы устанавливают связи между произвольными геометрическими кривыми и результатами их интерпретации в представлении графиков автоматных отображений.

Теорема 2. *Пусть $A = (S, X, Y, \delta, \lambda, s_0)$ — инициальный дискретный детерминированный автомат с конечным или счетно-бесконечным множеством состояний S, ω_1 — линейный порядок на X^* и $(\alpha_0, \alpha_l]$ — полуинтервал на оси ординат, где $l = |Y|$. Тогда для любых*

– взаимно-однозначного отображения «в» $\varphi : N^+ \to R$, где для любых $n, n' \in N^+$ из $n < n'$ следует $\varphi(n) < \varphi(n')$;

– разбиения полуинтервала $(\alpha_0, \alpha_l]$ на l полуинтервалов $(\alpha_0,\ \alpha_1]$, $(\alpha_1,\ \alpha_2]$, $\dots$, $(\alpha_{l-1}, \alpha_l]$ и взаимно-однозначного отображения

$\nu :\ Y\ \to\ (\alpha_{i-1}, \alpha_i], 1 \leqslant i \leqslant l$,

пара чисел (j, β), где $j \in Pr_2\varphi$ и $\beta \in (\alpha_0, \alpha_l]$, однозначно определяет пару (p, y_i), для которой j — номер $p \in X^*$ по порядку ω_1 и $\beta \in (\alpha_{i-1}, \alpha_i]$.

Теорема 3. *Любые:*

– геометрическая кривая $y = f(x)$;

– *последовательность h точек $(x_{i_1}, f(x_{i_1})), (x_{i_2}, f(x_{i_2})), \ldots, (x_{i_j}, f(x_{i_j})), \ldots$, где $x_{i_1} < x_{i_2} < \ldots x_{i_j} < \ldots$;*

– *число $m \in N^+$ и разбиение последовательности h на подпоследовательности из m элементов каждая;*

– *полуинтервал $\Delta = (\alpha, \beta]$ на оси ординат, где $\min\limits_{x \in \Delta} f(x) < \alpha < \beta \leqslant \max\limits_{x \in \Delta} f(x)$;*

– *разбиение полуинтервала Δ на конечное множество полуинтервалов вида $(\alpha, \alpha_1]$, $(\alpha_1, \alpha_2]$, $\ldots$, $(\alpha_{l-1}, \beta]$, где $l \in N^+$,*

однозначно определяют геометрический образ законов функционирования дискретного детерминированного автомата с конечным или счетно-бесконечным множеством состояний, с m входными и l выходными сигналами.

Методы распознавания инициальных автоматов, заданных числовыми графиками автоматных отображений, ориентированы на автоматы с большим, в общем случае счетно-бесконечным, числом состояний и построены на следующих процедурах.

Все варианты поведения инициального автомата представлены числовым графиком, точки которого предполагаются расположенными на геометрической кривой $y = f(x)$. Конкретное расположение точек на этой кривой определяется в соответствии с фактической информацией, как правило, частичной и дополняемой с использованием гипотез о свойствах процесса функционирования автомата.

Существует простой метод преобразования геометрического задания автоматного отображения в функции переходов и выходов и, если позволяют мощности множеств состояний, входных и выходных сигналов, в табличное задание автоматов.

Методу минимизации автомата по табличному заданию автомата соответствует простой и эффективный метод минимизации по геометрическому образу автомата. Можно утверждать, что известные методы анализа свойств автоматов имеют аналогичные методы действий с геометрическими образами автоматов. Основной метод распознавания автомата в классе автоматов, заданных числовыми графиками автоматных отображений, содержит следующие этапы (условие исключительности класса автоматов предполагается).

1 Этап. Для уравнений кривых $y_i = f_i(x)$, $i \in I$, на которых расположены точки автоматных отображений, строятся:

– неравенства $f_i(x) \neq f_j(x)$, $i, j \in I$ и $i \neq j$;
– равенства $f_i(x) = f_j(x)$, $i, j \in I$ и $i \neq j$.

2 Этап. По равенствам определяются интервалы оси абсцисс, содержащие точки, определяющие входные последовательности, на которых автоматы не распознаются по наблюдаемому поведению.

3 Этап. По неравенствам определяются интервалы оси абсцисс, содержащие точки, определяющие входные последовательности, на которых автоматы распознаются по наблюдаемому поведению.

4 Этап. Анализируются результаты второго и третьего этапов и строится общая картина областей оси абсцисс (множеств входных последовательностей), в которых находятся входные последовательности — решения задачи распознавания автомата в рассматриваемом классе автоматов.

Список литературы

[1] Твердохлебов В. А. Техническое диагностирование в геометрической интерпретации задач, моделей и методов // Материалы междунар. конф. Автоматизация проектирования дискретных систем / Белорус. гос. ун-т, Ин-т техн. кибернетики АНБ. — Минск: Изд-во Белорус. гос. ун-та, 1995. Т. 1: Тезисы докладов. — С. 97.

[2] Твердохлебов В. А. Распознавание автоматов на основе геометрической интерпретации // Проблемы теоретической кибернетики: тез. докл. XI Междунар. конф., 10–14 июня 1996 г. — М.: Изд-во. РГГУ, 1996. — С. 85–93.

[3] Твердохлебов В. А. Геометрические образы конечных детерминированных автоматов // Изв. Сарат. ун-та. Нов. сер. Сер. Математика, Механика, Информатика. — 2005. Т. 5. Вып. 1. — С. 141–153.

[4] Твердохлебов В. А. Методы интерполяции в техническом диагностировании // Проблемы управления. — 2007. № 2. — С. 28–34.

[5] Твердохлебов В. А. Геометрические образы законов функционирования автоматов. — Саратов: Научная книга, 2008.

[6] Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения / Под. ред. В. С. Харченко. Харьков: Изд-во Национальный аэрокосмический университет им. Н. Е. Жуковского («ХАИ»), 2011.

Сложность конструирования изображений клеточными автоматами

Титова Е. Е. (Москва, МГУ им. М. В. Ломоносова)

titovaee@yandex.ru

В работе рассматривается задача конструирования изображений клеточным автоматом на прямоугольном экране. В каждую клетку прямоугольного экрана $n \times m$ помещено по одному экземпляру одного и того же автомата $\mathcal{A}$ (элементарного), к его входам присоединены выходы автоматов, стоящих в соседних клетках, выход автомата — его текущее состояние. Доопределим нулями крайние входы автоматов n-й строки и m-го столбца. Неопределенные входы автоматов первой строки и первого столбца будем называть свободными входами, а всю эту конструкцию — (n, m)-*экраном* $S =< \mathcal{A}, n, m >$. Также имеется внешний автомат $\mathcal{A}_e$ с $(n+m)$ выходами, который генерирует входные последовательности для свободных входов элементарных автоматов. Пара $G =< \mathcal{A}_e, S >$, состоящая из экрана и внешнего автомата называется *генератором*. Если каждый элементарный автомат экрана находится состоянии 0 или 1, то такую конфигурацию состояний экрана будем называть *черно-белой конфигурацией*. Черно-белую конфигурацию назовем *изображением*, если ее можно удерживать сколь угодно долго, подавая на свободные входы автоматов нулевые значения. *Кодом* K изображения назовем матрицу $n \times m$, состоящую из нулей и единиц. Скажем, что изображение $\Im_K$ *соответствует данному коду* K, если положение нулей и единиц в изображении и в коде совпадают. Обозначим $\Im(n, m)$ — множество всех изображений размера $n \times m$. Экран $S =< \mathcal{A}, n, m >$ — *универсальный*, если для любого кода K существует внешний автомат $\mathcal{A}_e^K$, такой что генератор $G =< \mathcal{A}_e^K, S >$ формирует изображение $\Im_K$, соответствующее коду K. $\mathcal{U}(n, m)$ — множество всех универсальных (n, m)-экранов. Через $\mathcal{G}(S, \Im)$ обозначим множество генераторов $< \mathcal{A}_e, S >$, формирующих изображение $\Im$. Если $S =< \mathcal{A}, n, m >$ — экран, то $Q(S)$ — число состояний элементарного автомата $\mathcal{A}$, $Q(n, m) = \min_{S \in \mathcal{U}(n,m)} Q(S)$.

Пусть $G =< \mathcal{A}_e, S >$ — некоторый генератор. Автомат A_e получает на вход некоторую последовательность, содержащую информацию

о коде изображения, которое должен построить генератор. Эту последовательность будем генерировать по коду K с помощью следующих устройств: перестановка π, разреживатель с коэффициентом $d \leqslant 1$, разреживатель с коэффициентом $d \geqslant 1$, задержка G_a^k.

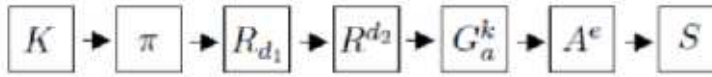

Рис. 1. Схема построения входных последовательностей для свободных входов экрана.

Перестановкой π будем называть отображение матрицы K (кода изображения) в некоторый вектор, элементами которого для разных алгоритмов могут быть нули и единицы, либо пары координат некоторых элементов кода изображения (например тех, которые равны 1), либо какая-то другая информация, взятая из K.

Пусть имеется некоторое множество V. *Разреживателем* R_d с коэффициентом $d, d = 1/s, s \in \mathbf{N}$, будем называть отображение из множества конечномерных векторов над V в множество конечномерных векторов над $V^{1/d}$, такое что если $v = (v_1, \ldots, v_{k \cdot s}) \in V^k$, то $R_d(v) = ((v_1, \ldots, v_s), \ldots, (v_{(k-1)s+1}, \ldots, v_{ks}))$, то есть элементами нового вектора являются векторы, состоящие из s элементов вектора v. *Разреживателем* R^d с коэффициентом $d, d \in \mathbf{N}$ будем называть отображение из множества конечномерных векторов над V в множество конечномерных векторов над $V \cup \{0\}$ (возможно $0 \in V$), такое что если $v = (v_1, \ldots, v_k) \in V^k$, то

$$R^d(v) = (v_1, 0, \ldots, 0, v_2, 0 \ldots, 0, \ldots, v_{k-1}, 0, \ldots, 0, v_k),$$

где между всеми элементами вектора v вставлено по $(d-1)$-му новому элементу, каждый из которых для вектора $R^d(v)$ равен 0.

Задержкой $G_a^k, k \in \mathbf{N} \cup \{0\}$ для конечной последовательности элементов из множества V (возможно $a \in V$), будем называть устройство, которое, получая на вход эту последовательность, в первые k тактов выдает элемент a, а затем по порядку все полученные на вход элементы.

Итак, на вход перестановки π поступает код K некоторого изображения. π формирует из него некоторый информационный вектор, который поступает на вход разреживателя R_{d_1}. R_{d_1} объединяет элементы входного вектора в группы по d_1 элементов и подает на вход разреживателю R^{d_2}, который между этими информационными элементами вектора вставляет нулевые элементы. Полученный вектор поступает на вход задержки G_a^k, которая в начало вектора добавляет k элементов a. Полученная таким образом последовательность поступает на вход внешнего автомата A_e, который генерирует последовательности для свободных входов экрана. Описанная схема изображена на рисунке 1.

Алгоритмом построения изображений на заданном универсальном экране будем называть множество последовательностей входных элементов для свободных входов экрана, при подаче которых на экране формируются наперед заданные соответствующие им изображения. Скажем, что генератор $G =< \mathcal{A}_e, S >$ соответствует алгоритму $\mathcal{A}$ построения изображений на универсальном экране S, если для любого K автомат $\mathcal{A}_e$ (получая на вход построенную по коду K с помощью описанной выше схемы последовательность) генерирует последовательность, соответствующую изображению $\Im_K$ в алгоритме $\mathcal{A}$. Пусть $\mathcal{A}$ — алгоритм построения изображений на универсальном экране $S(n, m)$. Множество всех генераторов, соответствующих алгоритму $\mathcal{A}$ обозначим $\mathcal{G}(\mathcal{A})$. Если $G =< \mathcal{A}_e, S(n, m) >\in \mathcal{G}(\mathcal{A})$, то обозначим $Q_e(G)$ — число состояний внешнего автомата $\mathcal{A}_e$, $Q(G) = Q(S) \cdot Q_e(G)$ — сложность генератора G. Сложностью алгоритма $\mathcal{A}$ назовем $Q(\mathcal{A}) = \min_{G\in\mathcal{G}(\mathcal{A})} Q(G)$.

В [3] и [4] приведены алгоритмы построения изображений на универсальных экранах с $Q(S) = 3$ (*Алгоритм 3*), $Q(S) = 4$ (*Алгоритм 4*), $Q(S) = 5$ (*Алгоритм 5*), $Q(S) = 2n + 2$ (*Алгоритм* A_{min}), также приведен *Алгоритм 7* построения изображения на экране с одним свободным входом. Будем обозначать эти алгоритмы $\mathcal{A}3$, $\mathcal{A}4$, $\mathcal{A}5$, $\mathcal{A}_{min}$ и $\mathcal{A}7$ соответственно.

Приведем здесь *Алгоритм 3*. Без ограничения общности будем считать, что $m \geqslant n$. Опишем элементарный автомат. Множество состояний — $E_q = \{0, 1, 2\}$. Функцию переходов состояний зададим следующим образом: $\varphi(q, 2, r, u, d) = 2$ для любых $q, r, u, d \in \{0, 1\}$;

$\varphi(2,l,r,2,d)=2$ для любых $l,r,d\in\{0,2\}$; $\varphi(2,l,r,u,d)=u$ для любых $u\in\{0,1\}$, $d\in\{0,1,2\}$, $l,r\{0,2\}$; $\varphi(q,l,r,2,2)=2$ для любых $l,q,r\in\{0,1\}$ $d\in\{0,1\}$; $\varphi(q,l,r,u,d)=q$ в остальных случаях.

Опишем выходы внешнего автомата, соответствующие изображению с кодом K. Первый выходной вектор (длины n) в первый такт будет равен $(2,2,\ldots,2)_n$, во второй и все последующие такты первый выходной вектор будет нулевым, то есть $(0,0,\ldots,0)_n$. Вектор $(b_1,\ldots,b_m)$, подаваемый на верхнюю границу экрана будем строить по следующим правилам: в первый такт это нулевой вектор, то есть $(0,0,\ldots,0)_m$; далее при $2\leqslant i\leqslant m+1$ в i-й такт в первых $(i-1)$ битах стоят 2, в остальных битах вектора стоят нули, то есть $(2,\ldots,2,0,\ldots,0)_m$; при $m+2\leqslant i\leqslant m+2n$: если $i=(m+2)+2s$, $0\leqslant s\leqslant n-1$, то в i-й такт выходной вектор равен $(m-s)$-й строке кода K; если $i=(m+2)+2s+1$, $0\leqslant s\leqslant n-1$, то в i-й такт в каждом бите выходного вектора стоит 2, то есть он равен $(2,2,\ldots,2)_m$; при $i\geqslant m+2n+1$ выходной вектор нулевой, то есть $(0,0,\ldots,0)_m$.

При подаче выходов описанного внешнего автомата на свободные входы экрана состояние 2 распространяется по горизонтали слева направо, пока не заполнит весь экран. Далее на верхнюю границу с задержкой в один такт подаются друг за другом строки кода изображения начиная с нижней и заканчивая верхней строкой. Такая строка кода продвигается по экрану вниз до тех пор, пока и сверху и снизу от нее находятся строки из двоек. Если соседняя снизу строка состоит из нулей и единиц, то строка кода останавливается и дальше не двигается. Таким образом на экране снизу вверх по строкам восстанавливается изображение, соответствующее заданному коду. Оно появляется на экране в следующий такт после подачи на свободные входы экрана последнего ненулевого вектора.

Имеют место следующие оценки сложности алгоритмов построения изображений на универсальных экранах.

Теорема 1. *Если* $<\mathcal{A}_e,S(n,m)>\in\mathcal{G}(\mathcal{A}3)$, $n,m\in\boldsymbol{N},n\leqslant m$, *то* $Q_e(G)\leqslant m+2, Q(\mathcal{A}3)\leqslant 3m+6$.

Если $<\mathcal{A}_e,S(n,m)>=G\in\mathcal{G}(\mathcal{A}4)$, $n,m\in\boldsymbol{N},n\leqslant m$, *то* $Q_e(G)\leqslant 2n, Q(\mathcal{A}4)\leqslant 8n$.

Если $<\mathcal{A}_e,S(n,m)>=G\in\mathcal{G}(\mathcal{A}5)$, $n,m\in\boldsymbol{N},n\leqslant m$, *то* $Q_e(G)\leqslant 3, Q(\mathcal{A}5)\leqslant 15$.

Если $< \mathcal{A}_e, S(n,m) >= G \in \mathcal{G}(\mathcal{A}_{min})$, $n, m \in \boldsymbol{N}, n \leqslant m$, *то*
$Q_e(G) \leqslant n, Q(\mathcal{A}_{min}) \leqslant 2n^2 + 2n$.
Если $< \mathcal{A}_e, S(n,m) >= G \in \mathcal{G}(\mathcal{A}7)$, $n, m \in \boldsymbol{N}, n \leqslant m$, *то*
$Q_e(G) \leqslant 6, Q(\mathcal{A}7) \leqslant 48$.

Автор выражает глубокую признательность научному руководителю д.ф.-м.н., профессору Э. Э. Гасанову за постановку задачи и научное руководство.

Список литературы

[1] Кудрявцев В. Б., Подколзин А. С., Болотов А. А. Основы теории однородных структур. — М.: Наука, 1990.

[2] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

[3] Титова Е. Е. Конструирование изображений клеточными автоматами // Интеллектуальные системы. — 2008. Т. 12. Вып. 1–4. — С. 105–121.

[4] Титова Е. Е. Линейное по времени конструирование изображений клеточными автоматами // Интеллектуальные системы. — 2012. Т. 16. Вып. 1–4. — С. 215–234.

Дискретные динамические системы, определяемые геометрическими образами автоматов

Тяпаев Л. Б., Василенко Д. В.
(Саратов, Саратовский государственный университет)
TiapaevLB@info.sgu.ru

Объектом исследования является динамическая система, определяемая геометрическими образами автоматов. Фазовое пространство системы определяется ортогональными и аффинными преобразованиями геометрических образов. Изучаются произведения динамических систем заданного типа и их характеристики.

Динамической системой называется тройка объектов $D = (S, f, G)$, где S — пространство состояний, $|S| < \infty$, $f : S \longrightarrow S$ — функция эволюции, G — граф фазового пространства динамической системы.

В дальнейшем будем использовать термин *точка динамической системы* в качестве синонима для термина состояние динамической системы.

Аттракторами динамической системы $D = (S, f, G)$ называют циклы графа G. *Точкой ветвления* динамической системы D называется вершина графа G, в которую входит более чем одна ветвь. *Стволом* дерева называется ветвь, содержащая точки ветвления.

Произведением динамических систем $D_1 = (S, f, G)$ и $D_2 = (T, g, G')$ будем называть динамическую систему $D_1 \circ D_2 = (S \times T, f \times g,\ G \circ G')$, где $S \times T$ — декартово произведение множеств S и T; $f \times g : S \times T \longrightarrow S \times T$ — прямое произведение отображений $f : S \longrightarrow S$ и $g : T \longrightarrow T$, $f \times g : (s, t) \mapsto (f(s), g(t))$; $G \circ G'$ — граф определяемый следующим образом:

1. $V(G \circ G') = VG \times VG'$;

2. Вершины (u, u') и (v, v') графа $G \circ G'$ смежны тогда и только тогда, когда одновременно вершины u и v смежны в графе G, и вершины u' и v' смежны в графе G'.

Будем рассматривать динамические системы, определяемые геометрическими образами автоматов [3]. Пространство состояний динамической системы — конечное множество геометрических образов

конечных автоматов. Геометрические образы автоматов суть множества точек плоскости с рациональными координатами, прообразами которых являются множества входных слов автомата и его реакций [1, 2]. Фазовое пространство динамической системы формируется посредством ортогональных и аффинных преобразований пространства состояний [3].

Дадим необходимые определения.

Конечный автомат это пятёрка $A = (S, X, Y, \delta, \lambda)$, где

$S = \{s_0, s_1, \ldots, s_{N-1}\}$ — множество состояний автомата,

$X = \{x_1, x_2, \ldots, x_L\}$ — множество входных символов (входной алфавит), $Y = \{y_1, y_2, \ldots, y_M\}$ — множество выходных символов (выходной алфавит), $\delta : S \times X \to S$ — функция переходов автомата, $\lambda : S \times X \to Y$ — функция выходов автомата. Расширим функции δ и λ на словах из множеств X^* и Y^* соответственно, и в дальнейшем будем использовать те же обозначения для этих функций. Здесь X^* и Y^* — множества слов конечной длины над алфавитами X и Y соответственно.

Пусть s_0 — начальное состояние автомата A. *Инициальным автоматом* называется пара $(A,\ s_0)$. Автомат A называется *автономным*, если $|X| = 1$.

Поведение автомата A определяется множеством

$$\Lambda = \{(p, q)\,|p \in X^* \exists s \in S\ \&q = \lambda\,(s, p)\}\,.$$

Множество $\Lambda_A(s_0) = \{(p, q)\,|p \in X^*, q \in Y^* \quad \lambda\,(s_0, p) = q\}$ определяет поведение автомата A из состояния s_0.

Геометрическое пространство Γ для автомата (A, s_0) определяется следующим образом [1]:

1) Сопоставим элементам множества X натуральные числа от 1 до L, то есть осуществим взаимно однозначное отображение $f : X \longrightarrow \{1, 2, \ldots, L\}$.

2) Определим координатную ось абсцисс $\tilde{X}$ для пространства Γ как отрезок числовой оси $[0, L + 1]$.

3) Каждому слову $p = x_{i_1} x_{i_2} \ldots x_{i_k}$ сопоставим вектор $\omega = (f\,(x_{i_1})\,, f\,(x_{i_2})\,, \ldots, f\,(x_{i_k}))$, то есть осуществим взаимно однозначное соответствие $g : X^* \longrightarrow V_N$, где V_N — пространство

конечномерных векторов, элементами которых являются натуральные числа.

4) Каждому такому вектору $\omega = (\omega_1,\ \omega_2, \ldots,\ \omega_k)$ взаимно однозначно сопоставим точку $\tilde{x} \in \mathbb{Q}$ на оси абсцисс:

$$\tilde{x} = \frac{\omega_1}{(L+1)^0} + \frac{\omega_2}{(L+1)^1} + \frac{\omega_3}{(L+1)^2} + \cdots + \frac{\omega_k}{(L+1)^{k-1}}.$$

Аналогично определяется нумерация элементов множества Y, ось ординат $\tilde{Y}$ пространства Γ и отображение $h : Y^* \longrightarrow V_N$.

Каждой паре $(p, q) \in \Lambda_A(s_0)$ в пространстве Γ сопоставляется точка с координатами $(\tilde{x}, \tilde{y})$, где $\tilde{x} = \sum_{i=1}^{|p|} \frac{c_i}{(L+1)^{i-1}}$, $\big(c_1, c_2, \ldots, c_{|p|}\big) = g(p)$, $\tilde{y} = \sum_{i=1}^{|q|} \frac{b_i}{(M+1)^{i-1}}$, $\big(b_1, b_2, \ldots, b_{|q|}\big) = h(q)$.

Под *геометрическим образом* $\Omega_{\mathrm{A}}(\mathrm{s}_0)$ автомата (A, s_0) понимается множество таких пар $(\tilde{x}, \tilde{y})$. *Кривой f, задающей поведение автомата* (A, s), называется любая непрерывная кривая, такая, что любая точка $(\tilde{x}, \tilde{y}) \in \Omega_A(s)$ принадлежит кривой f. Кривая f называется *функциональной кривой*, если f есть график некоторой непрерывной функции. Понятие функции, определяющей функциональную кривую, отождествляется с самой кривой. Будем обозначать класс $K(N, L, M)$ автоматов, у которых $|S| = N$, $|X| = L$, и $|Y| = M$. Класс автономных автоматов обозначим $K(N, M)$. Аналитическое задание геометрического образа автономного автомата характеризует следующая теорема.

Теорема 1 [2]. *Пусть $A \in K(N, M)$. Тогда поведение автомата (A, s) в пространстве Γ можно определить функциональной кривой f, которая может быть задана следующим уравнением:*

$$f(\tilde{x}) = \sum_{j=1}^{M} \left(j \cdot \sum_{i=1}^{l_j} (M+1)^{\Delta_i^{(j)} - \log_2 \frac{1}{2-\tilde{x}}} \right),$$

где $0 \leqslant l_j \leqslant N$, $\Delta_i^{(j)} = (N-1) - r_i^{(j)}$, $r_i^{(j)} \in \{0, 1, \ldots, N-1\}$.

Две кривые называются *аффинно-эквивалентными*, если они могут быть получены одна из другой с помощью аффинного преобразования. Совокупность всех кривых, аффинно-эквивалентных какой-

нибудь определенной кривой f, называется *аффинным классом* кривой f.

Зафиксируем некоторый класс автономных автоматов $K(N,M)$ и рассмотрим множество Ω всех различных геометрических образов из данного класса. Будем рассматривать аффинные преобразования, которые преобразуют некоторый образ $\Omega_i \in \Omega$ в другой образ $\Omega_j \in \Omega$. При рассмотрении преобразований геометрических образов из одного класса $K\,(N,M)$ имеет смысл рассматривать только следующее преобразование: параллельный перенос вдоль оси ординат и растяжение и сжатие относительно оси абсцисс. Данное преобразование имеет вид: $\tilde{x}' = \tilde{x}, \tilde{y}' = a\tilde{y} + b, \quad a, b \in \mathbb{Q}$. Тогда образ $\Omega_i \in \Omega$ переводится в образ $\Omega_j \in \Omega$ описанным преобразованием с коэффициентами (a,b), если $(\forall(\tilde{x},\tilde{y}) \in \Omega_i\ )\,((\tilde{x}, a\tilde{y}+b) \in \Omega_j)$. Будем говорить, что образы Ω_i, Ω_j *совместимы* выбранным видом аффинного преобразования. Бинарное отношение $\rho \subseteq \Omega^2$, образованное парами совместимых образов

$$\rho = \{(\Omega_i, \Omega_j) \in \Omega | \exists a, b \in \mathbb{Q}\,(\forall\,(\tilde{x},\tilde{y}) \in \Omega_i)\,((\tilde{x}, a\tilde{y}+b) \in \Omega_j)\}$$

является отношением эквивалентности на множестве Ω и задает разбиение этого множества на классы эквивалентности. Определен вид коэффициентов (a,b) афинных преобразований геометрических образов Ω и установлено, что множества коэффициентов афинных преобразований для классов $K(N,M)$, $K(2,M)$ и $K(N,L,M)$ совпадают [4].

Рассмотрим максимальный класс эквивалентности K отношения совместимости $\rho \subseteq \Omega^2$ геометрических образов автоматов из класса $K(N,M)$. Выберем произвольным образом периодическую последовательность $u(v)$ элементов данного класса, где u и v — конечные последовательности различных элементов. Каждая такая последовательность $u(v)$ порождает последовательность F преобразований геометрических образов автоматов из класса K. Построим динамическую систему D, состояниями S которой будут элементы последовательности $u(v)$, а эволюция состояний будет определяться последовательностью F преобразований.

Рассмотрим свойства операции произведения динамических систем. Граф динамической системы состоит из циклов-аттракторов и притягиваемых деревьев.

Обозначим через $O_m + P_n$ динамическую систему, граф которой представляет собой цикл-аттрактор длины m и притягиваемую цепь длины n, а через $P^m_{n,q}$ притягиваемое дерево, содержащее m цепей длины n, где q — номер первой точки ветвления ствола данного дерева. Нумерация вершин ствола предполагается от листа к корню.

Расстоянием между корнями притягиваемых деревьев будем называть минимальную длину пути между ними.

Теорема 2. *Пусть динамическая система D имеет структуру $O_m + P_n$. Тогда каждая из компонент связности графа системы $D \circ D$ представляет собой структуру вида $P^m_{n,q_1} + O^i_m + P^m_{n,q_2}$, где q_1 и q_2 — номера первых точек ветвления для первого и второго дерева соответственно, i — расстояние между корнями деревьев, и обладает следующими характеристиками:*

1. Количество компонент связности равно m. Длина цикла в каждой компоненте связности равна m. В каждой из компонент связности присутствует два притягиваемых дерева, каждое из которых имеет ствол. В каждой компоненте связности удалённость всех листов деревьев от аттрактора равна n.

2. Точками ветвления являются вершины графа, которые определяются точкой вхождения притягиваемой цепи в аттрактор системы D и точкой, находящейся вне аттрактора системы D, и располагаются на стволах с периодичностью, равной m. Первые точки ветвления для каждой компоненты связности вычисляются по формулам: $q_1 = n - m + i$, $q_2 = n - i$, где q_1 и q_2 — номера элементов ствола, являющихся первым точками ветвления для первого и второго дерева. Если $q_i < 0$, то искомая точка ветвления не существует.

3. В одной компоненте связности расстояние между корнями притягиваемых деревьев равно 0 и в одной компоненте связности расстояние между корнями притягиваемых деревьев равно $m/2$ (для чётных m). Во всех остальных компонентах связности расстояние между корнями меняется от 1 до $m/2 - 1$ для чётных m и до $(m-1)/2$ для нечётных m с шагом 1, причём каждая из таких

компонент будет встречаться в полученной динамической системе дважды.

4. Если расположить ствол деревьев перпендикулярно входящим в них цепям, они образуют прямоугольные равнобедренные треугольники. При таком способе отображения компоненты связности с расстоянием между корнями деревьев, равным 0 и $m/2$ (для чётных m) обладают свойством симметрии относительно вертикали.

Список литературы

[1] Тяпаев Л. Б. Геометрическая модель поведения автоматов и их неотличимость // Математика, Механика, Математическая кибернетика. Сб. науч. тр. — Саратов: Изд-во Сарат. ун-та, 1999. — С. 139–143.

[2] Тяпаев Л. Б. Решение некоторых задач для конечных автоматов на основе анализа их поведения // Изв. Сарат. ун-та. Сер. Математика. Механика. Информатика. — 2006. Т. 6. Вып. 1/2. — С. 121–133.

[3] Тяпаев Л. Б. Геометрические образы автоматов и динамические системы // Дискретная математика и ее приложения. Материалы X Межд. семинара / Под ред. О. М. Касим-Заде. — М.: Изд-во МГУ, 2010. — С. 510–513.

[4] Матов Д. О. Аффинные преобразования геометрических образов конечных автоматов // Проблемы теоретической кибернетики: Материалы XVI Межд. конф. / Под ред. Ю. И. Журавлева. — Нижний Новгород: Изд-во Нижегородского госуниверситета, 2011. — С. 303–306.

О полноте в классе конечных автоматов, вычисляющих некоторые аффинные функции

Часовских А. А. (Москва, МГУ им. М. В. Ломоносова)

chasovskikh@mail.ru

Все необходимые определения можно найти в работах [1, 2]. Известно, что в классе $P_{\text{о.д.}}$ всех ограниченно-детерминированных функций, рассматриваемых вместе с операциями композиции, проблема проверки полноты конечных множеств алгоритмически неразрешима. Все-же в $P_{\text{о.д.}}$ содержатся нетривиальные подклассы, для которых указанная проблема алгоритмически разрешима. К ним относится, например, подкласс линейно-автоматных функций. Здесь приведен пример другого содержательного подкласса $P_{\text{о.д.}}$ с разрешимой задачей о полноте.

Бесконечной последовательности нулей и единиц α, $\alpha = \alpha(0), \alpha(1), \ldots, \alpha(t), \ldots$, $\alpha(t) \in E_2$, $t = 0, 1, \ldots$ сопоставим формальный ряд

$$\bar{\alpha} = \sum_{t=0}^{\infty} \alpha(t) 2^t.$$

Положим

$$R = \{\, \bar{\alpha} \mid \alpha \in E_2^{\infty} \,\},$$

$PR = \{\bar{\alpha} \mid \alpha \in E_2^{\infty},\ \alpha$ — периодическое (с предпериодом) сверхслово$\}$.

На множестве R введем операции сложения и умножения,при этом $\bar{\alpha}_1$ и $\bar{\alpha}_2$ суммируются или перемножаются как числа в двоичной записи с младшими разрядами $\alpha_1(0)$ и $\alpha_2(0)$.

Множество PR совпадает с кольцом рациональных чисел, которые, будучи представленными в несократимом виде, имеют нечетный знаменатель.

Нетрудно видеть, что любой автомат с входным алфавитом E_2^n и выходным алфавитом E_2 задает отображение из PR^n в PR. Например, для задержки $\xi_1(x)$ с начальным состоянием 1 имеем: $\xi(\bar{\alpha}) = 1 + 2\bar{\alpha}$ для любого $\bar{\alpha} \in R$.

Конечный автомат с входным алфавитом E_2^2, задаваемый следующей системой канонических уравнений

$$\begin{cases} q(0) = 0, \\ q(t+1) = x_1(t) \wedge x_2(t) \vee q(t) \wedge x_1(t) \vee q(t) \wedge x_2(t), \\ y(t) = x_1(t) \oplus x_2(t) \oplus q(t) \end{cases}$$

осуществляет отображение $F_+^{(2)}$ из R^2 в R по следующему правилу:

$$F_+^{(2)}(\bar{\alpha}_1, \bar{\alpha}_2) = \bar{\alpha}_1 + \bar{\alpha}_2.$$

Через L обозначим замыкание множества $\left\{\xi_1(x), F_+^{(2)}(x_1, x_2)\right\}$ по операциям композиции.

Для любого n, $n \in \{0, 1, \dots\}$, и для любой $F(x_1, x_2, \dots, x_n)$ найдутся r_i, $r_i \in PR$, $i = 0, 1, \dots, n$, такие, что для любых $\bar{\alpha}_i$, $\bar{\alpha}_i \in R$, $i = 1, 2, \dots, n$, выполнено:

$$F(\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n) = \sum_{i=1}^{n} r_i \bar{\alpha}_i + r_0. \tag{1}$$

Пусть выполнено (1). Положим

$$U(F) = \{\, r_i \mid i = 1, 2, \dots, n \,\}.$$

Для множества M, $M \subseteq L$, положим:

$$U(M) = \cup_{F \in M} U(F).$$

Переменная x_i функции $F(x_1, x_2, \dots, x_n)$, удовлетворяющей равенству (1), называется существенной, если $r_i \neq 0$. Переменная x_i называется непосредственной, если r_i, будучи представленным в несократимом виде, имеет нечетный знаменатель.

Операция обратной связи применима к переменной x_i функции $F(x_1, x_2, \dots, x_n)$ в точности тогда, когда x_i не является непосредственной переменной.

Далее, рассматривая дроби p/q из PR, считаем, что $(p, q) = 1$. Положим:

$$H^1 = \{\, 1 + 2 \cdot p/q \mid p/q \in PR \,\}.$$

Рассмотрим следующие подмножества в L.

$$L_c^1 = \{\, F \mid F \text{ имеет ровно одну существенную переменную} \,\},$$

$$L_n^1 = \{\, F \mid F \text{ имеет ровно одну непосредственную переменную} \,\},$$

$$T_a = \{\, F \mid \text{для любых } \alpha_i,\ \alpha_i \in E_2^\infty,\ \alpha_i(0) = a,\ i = 1, 2, \ldots, n, \text{ выполнено } F(\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n)(0) = a \,\},\ a = 0, 1,$$

$$V_1 = \{\, F \mid F \text{ имеет не более одной существенной переменной} \,\},$$

$$V_n = \{\, F \mid F \text{ имеет нечетное число непосредственных переменных} \,\},$$

$$J = \left\{ F \mid \sum_{r \in U(F)} |r| \leqslant 1 \right\},$$

Пусть $p_1, p_2, \ldots$ — последовательность всех простых чисел, причем $p_1 < p_2 < \ldots$. Тогда $p_1 = 2$. Положим:

$$R_c(p_i) = \{\, F \mid F \in L \setminus L_c^1, \text{ для любого } p/q \text{ из } U(F) \text{ выполнено: } (p, p_i) = p_i \,\} \cup \{F \mid F \in L_c^1, \text{ для любого } p/q \text{ из } U(F) \setminus \{0\} \text{ выполнено: } (q, p_i) = 1\},\ i = 2, 3, \ldots,$$

$$R_n(p_i) = \{\, F \mid F \in L \setminus L_n^1, \text{ для любого } p/q \text{ из } U(F) \text{ выполнено: } (p, p_i) = p_i \,\} \cup \{F \mid F \in L_n^1, \text{ для любого } p/q \text{ из } U(F) \setminus H^1 \text{ выполнено: } (p, p_i) = p_i, \text{ а для любого } p/q \text{ из } U(F) \cap H^1 \text{ имеет место } (q, p_i) = 1 \,\},\ i = 2, 3, \ldots.$$

Через A обозначим следующее множество:

$$\{\, T_0, T_1, V_1, V_n, J, R_c(p_i), R_n(p_i) \mid i = 2, 3, \ldots \,\}.$$

Имеют место:

Теорема 1. *Множество A является приведенной критериальной системой, состоящей из предполных в L классов.*

Теорема 2. *Задачи проверки а-полноты и полноты конечных систем из L алгоритмически разрешимы.*

Автор выражает благодарность академику В. Б. Кудрявцеву за постоянную поддержку в работе.

Список литературы

[1] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Элементы теории автоматов. — М.: мзд-во МГУ, 1978.

[2] Часовских А. А. О полноте в классе линейных автоматов // Математические вопросы кибернетики. — М.: Наука, 1991. Вып. 3. — С. 140–166.

О характеризации состояний автоматной модели лёгких в чистой среде

Чернова Ю. Г. (Москва, МГУ им. М. В. Ломоносова)

yulyaha@list.ru

В предлагаемой работе продолжается изучение функционирования легких человека, начатое в работах [2], [3] и [4]. В качестве главной функции легких рассматривается свойство их самоочищения как от внутреннего секрета, так и от поступающего извне вещества в легкие. В работе [2] установлено, что процесс самоочищения легких может быть промоделирован с помощью автоматов. Здесь мы изучаем свойства таких автоматов.

Легкие образуют древовидную структуру бронхов, в которых имеются реснички, играющие роль эскалаторного механизма вывода как внутреннего секрета, так и привнесенного извне вещества во внешнюю среду. Бронхи имеют разные пропускные способности и разную эффективность ресничек. Чем выше от самых мелких бронхов, тем мощнее механизм передачи вещества изнутри вовне.

Предполагается, что в момент t распределено некоторое количества вещества по ресничкам легких. Тогда в момент $t+1$ по определенным правилам происходит перемещение вещества в легких с помощью ресничек по направлению к трахее. Этот процесс продолжается до полного освобождения легких от этого вещества.

Возникает задача построения модели легочного механизма самоочищения как в условиях чистой среды, так и в условиях возможного запыления легких из среды в процессе дыхания, а также задача изучения свойств этой модели.

Ранее автором была построена такая модель процесса самоочищения запыленных легких в предположении чистой среды [3], в которой оно функционирует. Как отмечено выше, автором было показано, что такая модель является автоматной, и потому разные свойства процесса самоочищения могут быть исследованы с помощью изучения соответствующих автоматов.

Основной характеристикой автоматов, как известно [1], является его диаграмма Мура, построение и изучение свойств которой для

модели легких означало бы установление свойств процесса их самоочищения.

В предлагаемой работе проводится изучение этой диаграммы Мура. В качестве характерных состояний диаграммы выбраны те состояния, которые имеют наибольшее число предшественников. Такие состояния называются состояниями конденсации. Содержательно, это те состояния, для которых предыстория наиболее неопределена.

Основными результатами предлагаемой работы являются критериальное описание таких состояний конденсации, нахождение количества этих состояний, а также получение оценок для количества их предшественников.

Представим легкие полным дихотомическим ориентированным к корню деревом, которое будем называть *I-деревом* и обозначать D^{-1}, со следующими параметрами.

Пусть $\mathbb{N}$ — множество натуральных чисел и l, $l \in \mathbb{N}$, считаем глубиной этого I-дерева. Полагаем, что ребро I-дерева D^{-1}, инцидентное корню, имеет глубину 1.

Каждое ребро из D^{-1} разделено на n, $n \in \mathbb{N}$, равных частей, называемых *ресничками*, и занумерованных числами i, $i = 1, 2, \ldots, n$, возрастающими в направлении, обратном ориентации ребра.

Припишем каждому ребру глубины j, $j = 1, 2, \ldots, l$, два числа $2^{l-j}b$ и $2^{l-j}r$, где $b, r \in \mathbb{N}$ и $r \leqslant b$, называемых *максимальной нагрузкой* и *мерой переброса* ресничек ребер глубины j соответственно.

Такое I-дерево D^{-1} с описанными выше параметрами b, r, n и l обозначим $D^{-1}(b, r, n, l)$.

Свяжем с ним некоторый процесс, который назовем *процессом дыхания*. Он обусловлен рядом допущений.

Считаем, что в $D^{-1}(b, r, n, l)$ заданы распределения значений нагрузок по всем ресничкам, учитывая, что нагрузка может быть нулевой. Пусть V' — суммарная нагрузка по всем ресничкам, а V — максимально возможная суммарная нагрузка по всем ресничкам. V назовем *объемом I-дерева (легких)*, а V' — *исходным объемом загруженности I-дерева*.

I-дерево $D^{-1}(b, r, n, l)$ с исходным объемом загруженности V' обозначим $D^{-1}(b, r, n, l; V')$.

Каждая ресничка осуществляет прием вещества извне и переброс своей нагрузки на следующую ресничку с меньшим номером внутри ребра.

Прием ресничкой вещества, имеющего массу d, $d \in \mathbb{N}_0$ и $d \leqslant V - V'$, из внешней среды внутри ребра осуществляется по следующему правилу (для этого правила ориентация считается обратной к заданной).

$А_1$) Если ресничка имеет максимальную нагрузку, то прием вещества не осуществляется.

$Б_1$) При немаксимальной нагрузке d_1 первой такой реснички она осуществляет прием вещества максимально возможной массы d_2, такой, что $d_1 + d_2 \leqslant \min(b, d)$, где b — максимальная нагрузка этой реснички.

$В_1$) Следующая за ресничкой из $Б_1$) принимает массу d_3, как и в $Б_1$), с заменой там d на $d - d_2$.

$Г_1$) Оставшаяся масса вещества опускается до следующей реснички с большим номером в ребре, для которой не выполняется условие $А_1$). Она осуществляет прием вещества по правилу $В_1$) или $Б_1$).

$Д_1$) Если ресничка в рассматриваемом ребре является последней, не удовлетворяющей условию $А_1$), то оставшаяся масса вещества делится пополам (если число нечетное, то одна из частей на единицу больше другой); и каждая из частей вещества воспринимается соответствующими ребрами, как описано выше.

$Е_1$) Процесс, описываемый позициями $А_1$)–$Д_1$), начинается с ребра, которое инцидентно корню.

Переброс ресничкой вещества осуществляется на следующую ресничку с меньшим номером внутри ребра по такому правилу.

$А_2$) Если следующая ресничка имеет не нулевую нагрузку, то переброс с реснички не осуществляется.

$Б_2$) Если нагрузка реснички не превосходит r, где r — ее мера переброса, и не выполнено условие $А_2$), то перебрасывается на следующую вся нагрузка реснички и считается, что ее нагрузка становится равной нулю.

$В_2$) Если на ресничке нагрузка m и $m > r$, то она перебрасывает на следующую ресничку нагрузку r и оставляет у себя нагрузку $m - r$.

Если ресничка в ребре последняя, то переброс нагрузки осуществляется по правилам А$_2$), Б$_2$), В$_2$).

Г$_2$) Если ребро инцидентно корню, то переброс с наименьшей по номеру реснички осуществляется в среду по правилам Б$_2$) и В$_2$) в предположении, что среда играет роль реснички с нулевой нагрузкой.

Д$_2$) Если ребро не инцидентно корню, то есть его вершина инцидентна следующему ребру, то нагрузка с наименьшей по номеру реснички этого ребра передается наибольшей по номеру ресничке другого ребра по правилам А$_2$), Б$_2$), В$_2$).

Считаем, что процесс дыхания осуществляется в дискретные моменты времени $t = 1, 2, 3, \ldots$

В первый момент I-дерево $D^{-1}(b, r, n, l; V')$ имеет заданное распределение нагрузок по его ресничкам.

Ко второму моменту осуществляется прием вещества массой $d(1)$ по правилам А$_1$)–Е$_1$), и затем осуществляется переброс нагрузок с реснички на ресничку во всем I-дереве или выброс в среду в соответствии с правилами А$_2$), Б$_2$), В$_2$), Г$_2$), Д$_2$). А если в легкие подается масса d, не превосходящая объема легких, то та ее часть, которая не осела на ресничках, выбрасывается в среду.

Другими словами, за один момент (шаг) происходит «вдох» и «выдох».

Если в каждый момент $t = 1, 2, 3, \ldots$ все реснички I-дерева $D^{-1}(b, r, n, l; V')$ осуществляют прием вещества нулевой массы, то такой процесс называется *процессом самоочищения* этого I-дерева. Процесс самоочищения заканчивается в такой момент t, в котором нагрузки всех ресничек I-дерева $D^{-1}(b, r, n, l; V')$ впервые стали равными нулю.

Под распределением нагрузки V' I-дерева $D^{-1}(b, r, n, l; V')$ будем понимать любое из возможных распределений нагрузок всех его ресничек таких, что суммарный объем их нагрузок равен V'. Ясно, что $V' \leqslant V$, где V — объем I-дерева $D^{-1}(b, r, n, l; V')$ и $V = 2^{l-1}bnl$. Такие распределения будем называть *конфигурациями* нагрузки V' по ресничкам I-дерева $D^{-1}(b, r, n, l)$.

Занумеруем все реснички I-дерева $D^{-1}(b, r, n, l)$ таким образом, что ресничка с номером ijk является k-ой ресничкой j-го ребра глубины i, где $1 \leqslant i \leqslant l$, $1 \leqslant j \leqslant 2^{i-1}$, $1 \leqslant k \leqslant n$, а нумерация

ребер одной глубины идет слева направо. Тогда в каждый момент t конфигурацию нагрузки $V'(t)$ в I-дереве $D^{-1}(b,r,n,l)$ можно задать набором

$$q(t) = (q_{111}(t), q_{112}(t), \ldots, q_{ijk}(t), \ldots, q_{l2^{l-1}n}(t)),$$

в котором каждая координата $q_{ijk}(t)$ равна нагрузке реснички с номером ijk в момент t, причем $0 \leqslant q_{ijk}(t) \leqslant 2^{l-i}b$ и $\sum_{111}^{l2^{l-1}n} q_{ijk}(t) = V'(t)$.

Пусть в процессе самоочищения конфигурации нагрузки $V'(t)$ в каждый момент t изменяются по правилам $A_2) - -Д_2)$. Тогда процесс самоочищения можно представить некоторым инициальным конечным автоматом без выхода с одним финальным состоянием, что было сделано автором ранее в статье [2]. Там построен такой автомат и представлена схематическая диаграмма Мура этого автомата. Состояниями построенного автомата являются конфигурации нагрузки $V'(t)$ в I-дереве $D^{-1}(b,r,n,l)$. Такие конфигурации нагрузок I-дерева $D^{-1}(b,r,n,l)$ будем называть далее состояниями этого I-дерева.

Обозначим множество состояний I-дерева $D^{-1}(b,r,n,l)$ при всевозможных его нагрузках $V'(t)$ через $Q(b,n,l)$.

Введем понятие состояния конденсации для I-дерева $D^{-1}(b,r,n,l)$. Именно, q из $Q(b,n,l)$ считаем *состоянием конденсации* для I-дерева $D^{-1}(b,r,n,l)$, если в него за один шаг переходит наибольшее число состояний из $Q(b,n,l)$, то есть состояние q имеет наибольшее число предшественников (прообразов).

Нашими задачами будут выяснение того, какие состояния q из $Q(b,n,l)$ являются состояниями конденсации для I-дерева $D^{-1}(b,r,n,l)$, нахождение их количества, а также нахождение числа прообразов состояний конденсации.

Для решения этих задач выделим некоторые свойства состояний, которые назовем *c_i-свойствами* при $i = 1,2,3,4,5$.

Отметим, что c_1-свойство будет определено только при $b \geqslant 2r$, c_2- и c_3-свойства — только при $r < b < 2r$, а c_4- и c_5-свойства — только при $b = r$.

Будем говорить, что состояние q из $Q(b,n,l)$ обладает:

– *c_1-свойством*, если при данном q выполнено: $q_{ij1} = 0$, $q_{ijn} = 2^{l-(i+1)}r$, $q_{ijk} = 2^{l-i}r$, где $1 \leqslant i < l$, $1 \leqslant j \leqslant 2^{i-1}$, $2 \leqslant k \leqslant n-1$;

при $i = l$ выполнено $q_{lj1} = 0$, $q_{ljk} = r$, где $1 \leqslant j \leqslant 2^{l-1}$, $2 \leqslant k \leqslant n-2$, и либо $q_{lj(n-1)} = r$ и $0 \leqslant q_{ljn} \leqslant b - r$, либо $1 \leqslant q_{lj(n-1)} \leqslant r - 1$ и $q_{ljn} = 0$;

– c_2-*свойством*, если n четное и при данном q выполнено: $q_{ijn} = 2^{l-(i+1)}r$, $q_{ij1} = 0$, $q_{ij(2k)} = 2^{l-i}r$ и $1 \leqslant q_{ij(2k+1)} \leqslant 2^{l-i}(b-r)$, где $1 \leqslant i < l$, $1 \leqslant j \leqslant 2^{i-1}$, $1 \leqslant k \leqslant \frac{n-2}{2}$; при $i = l$ выполнено $q_{lj1} = 0$, $q_{ljn} = 0$, $1 \leqslant q_{lj(2k+1)} \leqslant b-r$ и $q_{lj(2k)} = r$, где $1 \leqslant j \leqslant 2^{l-1}$, $1 \leqslant k \leqslant \frac{n-2}{2}$;

– c_3-*свойством*, если n нечетное и при данном q выполнено: при i четном $q_{ijn} = 2^{l-(i+1)}r$, $1 \leqslant q_{ij(2k)} \leqslant 2^{l-i}(b-r)$ и $q_{ij(2k-1)} = 2^{l-i}r$ и при i нечетном $q_{ij1} = 0$, $1 \leqslant q_{ij(2k+1)} \leqslant 2^{l-i}b$ и $q_{ij(2k)} = 2^{l-i}r$, $1 \leqslant i < l$, $1 \leqslant j \leqslant 2^{i-1}$, $1 \leqslant k \leqslant \frac{n-1}{2}$; при $i = l$, когда l четно, выполнено $q_{ljn} = 0$, $1 \leqslant q_{lj(2k)} \leqslant b - r$ и $q_{lj(2k-1)} = r$, где $1 \leqslant j \leqslant 2^{l-1}$, $1 \leqslant k \leqslant \frac{n-1}{2}$; при $i = l$, когда l нечетно, выполнено $q_{lj1} = 0$, $q_{lj2} = r$, $0 \leqslant q_{ljn} \leqslant b - r$, $1 \leqslant q_{lj(2k-1)} \leqslant b - r$ и $q_{lj(2k)} = r$, где $1 \leqslant j \leqslant 2^{l-1}$, $1 < k \leqslant \frac{n-1}{2}$;

– c_4-*свойством*, если n четное и при данном q выполнено: $q_{ij(n-1)} = 0$, $q_{ijn} = 2^{l-(i+1)}b$, $1 \leqslant q_{ij(2k)} \leqslant 2^{l-i}b$ и $q_{ij(2k-1)} = 0$, где $1 \leqslant i < l$, $1 \leqslant j \leqslant 2^{i-1}$, $1 \leqslant k \leqslant \frac{n-2}{2}$; при $i = l$ выполнено $q_{lj(n-1)} = 0$, $q_{ljn} = 0$, $1 \leqslant q_{lj(2k)} \leqslant b$ и $q_{lj(2k-1)} = 0$, где $1 \leqslant j \leqslant 2^{l-1}$, $1 \leqslant k \leqslant \frac{n-2}{2}$;

– c_5-*свойством*, если n нечетное и при данном q выполнено: при i четном $q_{ijn} = 2^{l-(i+1)}b$, $1 \leqslant q_{ij(2k-1)} \leqslant 2^{l-i}b$ и $q_{ij(2k)} = 0$ и при i нечетном $q_{ijn} = 0$, $1 \leqslant q_{ij(2k)} \leqslant 2^{l-i}b$ и $q_{ij(2k-1)} = 0$, где $1 \leqslant i < l$, если l четно и $1 \leqslant i \leqslant l$, если l нечетно, $1 \leqslant j \leqslant 2^{i-1}$, $1 \leqslant k \leqslant \frac{n-1}{2}$; при $i = l$, когда l четно, выполнено $q_{ljn} = 0$, $1 \leqslant q_{lj(2k-1)} \leqslant b$ и $q_{lj(2k)} = 0$, где $1 \leqslant j \leqslant 2^{l-1}$, $1 \leqslant k \leqslant \frac{n-1}{2}$.

Пусть $C = \{c_1, c_2, c_3, c_4, c_5\}$. Класс всех состояний q из $Q(b, n, l)$ с c_i-свойством при $c_i \in C$ обозначим через K_{c_i}, мощность множества K_{c_i} — через $|K_{c_i}|$, а число прообразов каждого состояния q из K_{c_i} обозначим через $S_{K_{c_i}}$.

Справедливо следующее утверждение.

Теорема 1. *Множество состояний конденсации I-дерева* $D^{-1}(b, r, n, l)$ *совпадает с:*

а) K_{c_1}, *если* $b \geqslant 2r$;

б) K_{c_2} *при четном* n *и с* K_{c_3} *при нечетном* n, *если* $r < b < 2r$;

в) K_{c_4} *при четном* n *и с* K_{c_5} *при нечетном* n, *если* $b = r$.

Следующее утверждение дает решение задачи нахождения количества всех состояний конденсации I-дерева $D^{-1}(b,r,n,l)$.

Теорема 2. *Справедливы следующие равенства:*

1) $|K_{c_1}| = b^{2^{l-1}}$,

2) $|K_{c_2}| = ((b-r)^{2^l-1} \cdot 2^{2^l-l-1})^{\frac{n}{2}-1}$,

3) $|K_{c_3}| = \begin{cases} ((b-r)^{2^l-1} \cdot 2^{2^l-l-1})^{\frac{n-1}{2}}, & \text{если } l \text{ четно}, \\ (b-r)^{2^{l-1}(n-2)-\frac{n-1}{2}} \cdot (b-r+1)^{2^{l-1}} \cdot 2^{\frac{n-1}{2}(2^l-l-1)}, & \text{иначе}, \end{cases}$

4) $|K_{c_4}| = (b^{2^l-1} \cdot 2^{2^l-l-1})^{\frac{n}{2}-1}$,

5) $|K_{c_5}| = (b^{2^l-1} \cdot 2^{2^l-l-1})^{\frac{n-1}{2}}$.

Следствие. *Имеет место:*

1) $|K_{c_2}| \asymp 2^{(2^l \cdot c_2 - l) \cdot (\frac{n}{2}-1)}$, *где* $c_2 = 1 + \log_2(b-r)$,

2) $|K_{c_3}| \asymp \begin{cases} 2^{(2^l \cdot c_2 - l) \cdot \frac{n-1}{2}}, & \text{если } l \text{ четно}, \\ 2^{2^{l-1} \cdot c_3 - \frac{n-1}{2} \cdot l}, & \text{если } l \text{ нечетно}, \end{cases}$
где $c_3 = n - 1 + (n-2)\log_2(b-r) + \log_2(b-r+1)$,

3) $|K_{c_4}| \asymp 2^{(2^l \cdot c_4 - l) \cdot (\frac{n}{2}-1)}$, *где* $c_4 = 1 + \log_2 b$,

4) $|K_{c_5}| \asymp 2^{(2^l \cdot c_4 - l) \cdot \frac{n-1}{2}}$

при $l \to \infty$.

Теперь рассмотрим задачу нахождения числа прообразов $S_{K_{c_i}}$ состояния конденсации q из K_{c_i} для всех $c_i \in C$.

Пусть $d'_1 = \log_2 \left(2 \cdot r \cdot \left(\frac{(1+\sqrt{5})^{n-3} - (1-\sqrt{5})^{n-3}}{2^{n-3}\sqrt{5}} \right)^2 \right)$,

$d''_1 = \log_2 \left(6\sqrt{3} \cdot r \cdot \left(\frac{(1+\sqrt{5})^{n} - (1-\sqrt{5})^{n}}{2^{n}\sqrt{5}} \right)^2 \right)$, $d'_2 = n - 3 + \log_2 r$,

$d''_2 = n + 1 + \log_2(3\sqrt{3} \cdot r)$, $d'_3 = \frac{3n+2}{9} + \frac{1}{3} \cdot \log_2 r$,

$d''_3 = \frac{9n+17}{9} + \frac{1}{3} \cdot \log_2(3 \cdot r)$, $p'_3 = \frac{9n-23}{9} + \frac{2}{3} \cdot \log_2 r$,

$p''_3 = \frac{9n+2}{9} + \frac{2}{3} \cdot \log_2(3 \cdot r)$, $d'_4 = \log_2 \left(2 \cdot r \cdot \left(\frac{(1+\sqrt{5})^{\frac{n}{2}} - (1-\sqrt{5})^{\frac{n}{2}}}{2^{\frac{n}{2}}\sqrt{5}} \right)^2 \right)$,

$d''_4 = \log_2 \left(6\sqrt{3} \cdot r \cdot \left(\frac{(1+\sqrt{5})^{\frac{n}{2}+1} - (1-\sqrt{5})^{\frac{n}{2}+1}}{2^{\frac{n}{2}+1}\sqrt{5}} \right)^2 \right)$,

$d'_5 = \frac{5}{9} + \frac{1}{3} \cdot \log_2 r + \frac{2}{3} \cdot \log_2 \left(\frac{(1+\sqrt{5})^{\frac{n-3}{2}} - (1-\sqrt{5})^{\frac{n-3}{2}}}{2^{\frac{n-3}{2}}\sqrt{5}} \right)$,

$$d''_5 = \tfrac{14}{9} + \tfrac{1}{3}\cdot\log_2(27\cdot r) + 2\cdot\log_2\left(\frac{(1+\sqrt{5})^{\frac{n+1}{2}} - (1-\sqrt{5})^{\frac{n+1}{2}}}{2^{\frac{n+1}{2}}\sqrt{5}}\right),$$

$$p'_5 = \tfrac{2}{9} + \tfrac{1}{3}\cdot\log_2 r + \log_2\left(\frac{(1+\sqrt{5})^{\frac{n-3}{2}} - (1-\sqrt{5})^{\frac{n-3}{2}}}{2^{\frac{n-3}{2}}\sqrt{5}}\right),$$

$$p''_5 = \tfrac{2}{9} + \tfrac{1}{3}\cdot\log_2(27\cdot r) + \log_2\left(\frac{(1+\sqrt{5})^{\frac{n+1}{2}} - (1-\sqrt{5})^{\frac{n+1}{2}}}{2^{\frac{n+1}{2}}\sqrt{5}}\right).$$

Теорема 3. *Имеет место:*

1) $2^{2^{l-1}\cdot d'_1} \preccurlyeq S_{K_{c_1}} \preccurlyeq 2^{2^{l-1}\cdot d''_1}$,

2) $2^{2^{l-1}\cdot d'_2} \preccurlyeq S_{K_{c_2}} \preccurlyeq 2^{2^{l-1}\cdot d''_2}$,

3) $2^{2^{l-1}\cdot min(d'_3,p'_3)+\frac{1}{3}\cdot l} \preccurlyeq S_{K_{c_3}} \preccurlyeq 2^{2^{l-1}\cdot max(d''_3,p''_3)+\frac{1}{3}\cdot l}$,

4) $2^{2^{l-1}\cdot d'_4} \preccurlyeq S_{K_{c_4}} \preccurlyeq 2^{2^{l-1}\cdot d''_4}$,

5) $2^{2^{l-1}\cdot min(d'_5,p'_5)+\frac{1}{3}\cdot l} \preccurlyeq S_{K_{c_5}} \preccurlyeq 2^{2^{l-1}\cdot max(d''_5,p''_5)+\frac{1}{3}\cdot l}$

при $l \to \infty$.

Следствие. *Имеет место* $log_2 S_{K_{c_i}} \asymp 2^l$ *при* $l \to \infty$ *для всех* $i = 1, 2, 3, 4, 5$.

Автор выражает глубокую благодарность академикам Кудрявцеву Валерию Борисовичу и Чучалину Александру Григорьевичу за постановку задачи и научное руководство.

Список литературы

[1] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

[2] Гераськина Ю. Г. Об одной автоматной модели в биологии // Дискретная математика. — 2007. Т. 19. Вып. 3. — С. 122–139.

[3] Гераськина Ю. Г. Модель процесса дыхания живых организмов // Интеллектуальные системы. — 2004. Т. 8. Вып. 1–4. — С. 429–456.

[4] Гераськина Ю. Г. Модель самоочищения легочных структур // Интеллектуальные системы. — 2002–2003. Т. 7. Вып. 1–4. — С. 41–54.

[5] Прудников А. П., Брычков Ю. А., Маричев О. И. Интегралы и ряды. — М.: Наука, 1981.

On some types of automata over finite ring

Skobelev V. G. (Donetsk, IAMM of NAS of Ukraine)

skbv@iamm.ac.donetsk.ua

Applications of the ring theory in the process of design of modern ciphers has grounded actuality of investigation of automata presented via systems of equations over finite ring [1, 2]. Some basic characteristics of general models of Mealy and Moore automata over arbitrary finite associative-commutative ring $\mathcal{K} = (K, +, \cdot)$ with the unit are presented in the given paper.

We denote by $\mathcal{A}_{n,1}$ the set of all Mealy automata

$$\mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t) + \mathbf{f}_3(\mathbf{x}_{t+1}),$$
$$\mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_t) + \mathbf{f}_4(\mathbf{x}_{t+1})$$

and by $\mathcal{A}_{n,2}$ the set of all Moore automata

$$\mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t) + \mathbf{f}_3(\mathbf{x}_{t+1}),$$
$$\mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_{t+1}),$$

where $\mathbf{f}_i : K^n \to K^n$ $(i = 1, \ldots, 4)$ ($\mathbf{f}_2$ is a non-linear mapping) and $\mathbf{q}_t, \mathbf{x}_t, \mathbf{y}_t \in K^n$ are correspondingly internal state, input and output at instant $t \in \mathbf{Z}_+$.

Let $\mathcal{A}_{n,i}^{inv}$ $(i = 1, 2)$ be the set of all automata $M_i \in \mathcal{A}_{n,i}$ such that for every initial state $\mathbf{q}_0 \in K^n$ the mapping $\mathbf{F}_{(M,\mathbf{q}_0)} : (K^n)^+ \to (K^n)^+$, realized by initialized automaton $(M, \mathbf{q}_0)$ is bijection. It is evident that

$$\mathcal{A}_{n,1}^{inv} = \{M_1 \in \mathcal{A}_{n,1} | \mathbf{f}_4 : K^n \to K^n \ \textit{is bijection}\},$$
$$\mathcal{A}_{n,2}^{inv} = \{M_2 \in \mathcal{A}_{n,2} | \mathbf{f}_2 : K^n \to K^n \ \textit{and} \ \mathbf{f}_3 : K^n \to K^n \ \textit{are bijections}\}.$$

It is worth to note that the inverse M_i^{-1} $(i = 1, 2)$ of an automaton $M \in \mathcal{A}_{n,i}^{inv}$ is Mealy automaton.

Automata $M_i \in \mathcal{A}_{n,i}^{inv}$ $(i = 1, 2)$ determine the class of stream ciphers for which initial state is secret short-term key, while parameters are long-term key. For any stream cipher $((M, \mathbf{q}_0), (M^{-1}, \mathbf{q}_0))$ $(M \in \mathcal{A}_{n,1}^{inv} \cup \mathcal{A}_{n,2}^{inv})$ in the process 'coding-decoding' automata M_i and M_i^{-1} move in the space of states during the same trajectory in the same direction.

Some non-trivial subsets of the sets $\mathcal{A}_{n,i}$ $(i = 1, 2)$ can be characterized in the following way:

1) an automaton $M \in \mathcal{A}_{n,1} \cup \mathcal{A}_{n,2}$ is a strongly connected one if and only if $\mathbf{f}_3 : K^n \to K^n$ is bijection;

2) if $\mathbf{f}_3 : K^n \to K^n$ is bijection then an automaton $M \in \mathcal{A}_{n,1}$ is a reduced one and any of its two states can be distinguished by any input symbol;

3) if $\mathbf{f}_1 : K^n \to K^n$ and $\mathbf{f}_2 : K^n \to K^n$ are bijections then an automaton $M \in \mathcal{A}_{n,2}$ is a reduced one and any of its two states can be distinguished by any input symbol;

4) states $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ of an automaton $M \in \mathcal{A}_{n,1} \cup \mathcal{A}_{n,2}$ are twins if and only if they are elements of the same class of the partition K^n/ε where $\varepsilon = \ker \mathbf{f}_1 \cap \ker \mathbf{f}_2$ for $M \in \mathcal{A}_{n,1}$ and $\varepsilon = \ker \mathbf{f}_1$ for $M \in \mathcal{A}_{n,2}$.

Let the subset $\widetilde{\mathcal{A}}_{n,1}$ of the set $\mathcal{A}_{n,1}$ consists of all automata

$$\mathbf{q}_{t+1} = A\mathbf{q}_t\mathbf{q}_t^T\mathbf{b} + C\mathbf{q}_t + \mathbf{d} + E\mathbf{x}_{t+1},$$
$$\mathbf{y}_{t+1} = G\mathbf{q}_t + F\mathbf{x}_{t+1}$$

and the subset $\widetilde{\mathcal{A}}_{n,2}$ of the set $\mathcal{A}_{n,2}$ consists of all automata

$$\mathbf{q}_{t+1} = A\mathbf{q}_t\mathbf{q}_t^T\mathbf{b} + C\mathbf{q}_t + \mathbf{d} + E\mathbf{x}_{t+1},$$
$$\mathbf{y}_{t+1} = G\mathbf{q}_{t+1}$$

where $\mathbf{b} = (b^{(1)}, \ldots, b^{(n)})^T \in K^n$, $\mathbf{d} = (d^{(1)}, \ldots, d^{(n)})^T \in K^n$ and A, C, E, G, F are $n \times n$-matrices.

Complexity of identification of initial state $\mathbf{q}_0 \in K^n$ of an automaton $M \in \widetilde{\mathcal{A}}_{n,1} \cup \widetilde{\mathcal{A}}_{n,2}$ can be characterized in the following way.

It is supposed that the experimenter can apply any experiment of any multiplicity. The problem of identification of initial state of an automaton $M \in \widetilde{\mathcal{A}}_{n,1}$ is trivial, if G is an invertible matrix. In all other cases this problem is a hard one. Its high complexity is justified by the following reasons. Firstly, searching in the set of input sequences is a hard problem. Secondly, design the set of solutions for non-linear systems of equations is a hard problem. Thirdly, checking the property 'to be subset of the set of equivalent states' is also a hard problem.

It is worth to note that additional condition $M \in \widetilde{\mathcal{A}}_{n,1}^{inv} \cup \widetilde{\mathcal{A}}_{n,2}^{inv}$ does not simplify the problem of identification of initial state. Thus, selection initial state of an automaton $M \in \widetilde{\mathcal{A}}_{n,1}^{inv} \cup \widetilde{\mathcal{A}}_{n,2}^{inv}$ in the role of short-term key for corresponding stream cipher is grounded.

For an automaton $M \in \widetilde{\mathcal{A}}_{n,1} \cup \widetilde{\mathcal{A}}_{n,2}$ complexity of parametric identification can be characterized in the following way.

Parametric identification for an automaton $M_2 \in \widetilde{\mathcal{A}}_{n,2}$ is a hard problem, since it is always is reduced to design the set of solutions for non-linear systems of equations.

Let $M_1 \in \widetilde{\mathcal{A}}_{n,1}$. It is easy to identify matrices G and F. Also it is easy to identify vector $\mathbf{d}$ and matrix E if and only if G is an invertible matrix. But it is a hard problem to identify matrices A, C and vector $\mathbf{b}$ since it is always is reduced to design the set of solutions for non-linear systems of equations.

It is worth to note that additional condition $M \in \widetilde{\mathcal{A}}^{inv}_{n,1} \cup \widetilde{\mathcal{A}}^{inv}_{n,2}$ does not simplify the problem of parametric identification. Thus, selection parameters of an automaton $M \in \widetilde{\mathcal{A}}^{inv}_{n,1} \cup \widetilde{\mathcal{A}}^{inv}_{n,2}$ in the role of long-term key for corresponding stream cipher is grounded.

The set $S^{(i)}_{fxd}(M, \mathbf{q}_0)$ ($M \in \widetilde{\mathcal{A}}_{n,1} \cup \widetilde{\mathcal{A}}_{n,2}, \mathbf{q}_0 \in K^n$) of fixed points of the length i for the mapping $\mathbf{F}_{(M,\mathbf{q}_0)}$ can be characterized in the following way (I is the unit matrix):

1) $S^{(1)}_{fxd}(M_1, \mathbf{q}_0) \neq \varnothing$ ($M_1 \in \widetilde{\mathcal{A}}_{n,1}$) if and only if the set of solutions of equation $(I - F)\mathbf{x} = G\mathbf{q}_0$ is not empty (thus, if the matrix $I - F$ is an invertible one then $|S^{(i)}_{fxd}(M_1, \mathbf{q}_0)| = 1$ ($i \in \mathbf{N}, \mathbf{q}_0 \in K^n$));

2) if $F = I$ then $S^{(1)}_{fxd}(M_1, \mathbf{q}_0) = K^n$ ($M_1 \in \widetilde{\mathcal{A}}_{n,1}$) for any initial state $\mathbf{q}_0 \in K^n$ such that $G\mathbf{q}_0 = \mathbf{0}$;

3) $S^{(1)}_{fxd}(M_2, \mathbf{q}_0) \neq \varnothing$ ($M_2 \in \widetilde{\mathcal{A}}_{n,2}$) if and only if the set of solutions of equation $(G^{-1} - E)\mathbf{x} = A\mathbf{q}_0\mathbf{q}_0^T B + C\mathbf{q}_0 + \mathbf{d}$ is not empty (thus, if the matrix $G^{-1} - E$ is an invertible one then $|S^{(i)}_{fxd}(M_2, \mathbf{q}_0)| = 1$ ($i \in \mathbf{N}, \mathbf{q}_0 \in K^n$));

4) if $E = G^{-1}$ then $S^{(1)}_{fxd}(M_2, \mathbf{q}_0) = K^n$ ($M_2 \in \widetilde{\mathcal{A}}_{n,2}$) for any initial state $\mathbf{q}_0 \in K^n$ such that $A\mathbf{q}_0\mathbf{q}_0^T B + C\mathbf{q}_0 + \mathbf{d} = \mathbf{0}$.

References

[1] Skobelev V. V. Skobelev V. G. Analysis of ciphersystems. 2009 Donetsk: IAMM of NAS of Ukraine.

[2] Skobelev V. V., Glazunov N. M., Skobelev V. G. Manifolds over rings. Theory and applications. 2011. Donetsk: IAMM of NAS of Ukraine.