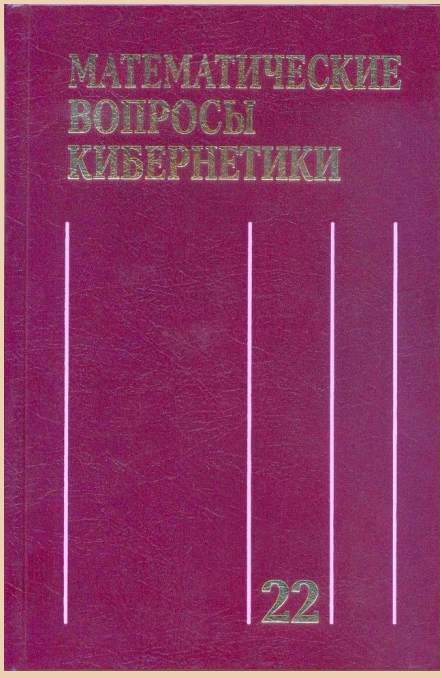

**С. В. Алешин,
Д. Н. Бабин,
А. А. Часовских**

Автоматы: полнота, выразимость, применение

Рекомендуемая форма библиографической ссылки: Алешин С. В., Бабин Д. Н., Часовских А. А. Автоматы: полнота, выразимость, применение // Математические вопросы кибернетики. Вып. 22. — М.: ФИЗМАТЛИТ, 2024. — С. 223–275. URL: https://library.keldysh.ru/mvk.asp?id=2024-223 DOI: 10.20948/mvk-2024-223

АВТОМАТЫ: ПОЛНОТА, ВЫРАЗИМОСТЬ, ПРИМЕНЕНИЕ

С. В. АЛЕШИН, Д. Н. БАБИН, А. А. ЧАСОВСКИХ

(МОСКВА)

Оглавление

§ 1. Введение

1.1. Автоматы с операциями суперпозиции. Понятие автомата относится к числу важнейших в математике. Оно возникло на стыке разных ее разделов, а также в технике, биологии и других областях. Содержательно автомат представляет собой устройство с входными и выходными каналами, обладающее памятью. На его входы последовательно поступает информация, которая перерабатывается им, и результат и выдается через выходные каналы. Эти устройства могут допускать соединение входных и выходных 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.

Отправной точкой возникновения теории автоматов является работа Э. Поста 1941 года [126]. В ней были получены фундаментальные результаты о строении решетки замкнутых классов булевых функций, которые были в дальнейшем методически переработаны в книге С. В. Яблонского,

DOI: 10.20948/mvk-2024-223

В. Б. Кудрявцева, Г. П. Гаврилова «Функции алгебры логики и классы Поста» [56]. Исследования самих автоматов и их алгебр начались в 30-е годы предыдущего столетия, но особенно активно шли начиная с 50-х годов.

Основополагающую роль здесь сыграли работы Тьюринга, авторов знаменитого сборника «Автоматы» Шеннона, Мура, Клини и др. [1]. Последующие работы по изучению алгебр автоматов велись под большим влиянием известных статей А. В. Кузнецова [59, 60] и С. В. Яблонского [114] 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 логик произвольной конечной значности. Затем усилиями многих исследователей [37, 70, 71, 81, 89] были открыты новые такие семейства, а заключительные построения провел Розенберг [127].

Одновременно с изучением функций без памяти (без учета времени) были сделаны попытки применения аппарата предполных классов в задаче полноты для автоматов с операцией суперпозиции. Сначала для автоматов, называемых функциями с задержками, В. Б. Кудрявцев эффективно решил задачу о полноте и ее естественных модификациях [49]. После этого им был рассмотрен общий случай и на этом пути получен фундаментальный результат негативного характера, который показал континуальность множества предполных классов автоматных функций [50]. В дальнейшем М. И. Кратко была показана алгоритмическая неразрешимость задачи выразимости относительно суперпозиции для автоматных функций [47].

В. Б. Кудрявцев [49] для функций с задержками относительно операции суперпозиции описал предполные классы, число которых оказалось счетным и нашел, тем не менее, алгоритм распознавания полноты конечных систем. С. В. Алешин [54] показал, что в этой функциональной системе существуют счетные базисы и в то же время есть полные системы, из которых базис выделить нельзя. Как в задаче Слупецкого для k-значных логик, в функциональной системе автоматов $\boldsymbol{P}$ с операцией суперпозиции является актуальным вопрос о добавке к базису, гарантирующей распознавание полноты конечных систем с этой добавкой. С. В. Алешин предложил в качестве такой добавки класс автоматов $\boldsymbol{P}_1$, в каждом состоянии которых

реализуется функция одного переменного (может быть, разная в разных состояниях). Оказалось, что этот класс имеет конечную глубину во множестве всех автоматов $\boldsymbol{P}$ и для конечных систем S существует алгоритм проверки на полноту системы $S \cup \boldsymbol{P}_1$, причем класс $\boldsymbol{P}_1$ вкладывается в континуум предполных классов [5]. Свойство иметь континуум предполных классов и одновременно счетный базис относительно операции суперпозиции выполнено для подклассов автоматов, в состояниях которых реализуются функции из некоторого собственного подкласса функций k-значной логики [5, 95].

С. С. Марченков [82] для автоматов с бесконечным числом состояний и операцией суперпозиции показал, что полные системы (естественно, бесконечные) имеют в совокупности еще и потенциально бесконечную арность (аналог 13 проблемы Гильберта для детерминированных функций). Д. Н. Бабин [11] для автоматов с конечным числом состояний и операцией суперпозиции показал, что существуют полные системы (естественно, бесконечные) арности два (аналог 13 проблемы Гильберта для конечно-автоматных функций). Более того, Д. Н. Бабину удалось показать, что система, состоящая из одноместных конечных автоматов и всех булевых функций, полна относительно суперпозиции.

Д. Н. Бабин в 1985 г. [10] в классе перестановочных автоматов показал неполноту относительно суперпозиции системы, состоящей из одноместных конечных автоматов и всех булевых функций. Позднее он доказал, что в функциональной системе автоматов с операцией суперпозиции есть замкнутые классы, не расширяющиеся до предполных [16].

Следует отметить результат А. А. Летуновского для выразимости с добавкой к выражающей системе булевых функций и автомата «задержки» [65]. Эта добавка позволяет проверить выразимость автоматов с безусловными переходами и групповых автоматов Медведева через произвольную конечную систему автоматов с добавкой из «штриха Шеффера» и «задержки». Таким образом, акцент в задаче выразимости переместился на анализ выражаемой части. Теперь основной вопрос в задаче выразимости автоматов с операцией суперпозиции: выразимость каких автоматов через базис с указанной добавкой алгоритмически разрешима.

Алгебра автоматов с операцией суперпозиции оказалась удобной для моделирования свойств бесконечных групп и решения проблем в этих группах. С. В. Алешину еще в 1972 году удалось построить естественный пример конечно-порожденной периодической группы (проблема Бернсайда), элементами которой являются конечные автоматы с одним входом и одним выходом, а операцией умножения в группе — операция суперпозиции автоматов. Эта технология позволила решать проблемы теории групп средствами теории автоматов [2]. Кроме того, он построил пример свободной группы, которая порождена двумя обратимыми автоматами с тремя состояниями [3]. Эта группа обратимых автоматов, как показал В. В. Макаров [76], может быть порождена своими элементами бесконечного порядка. Еще одной задачей в этой группе является построение автоматов конечного заданного порядка, лишь в одном состоянии которого реализуется функция отличная от тождественной. Последние продвижения в этой задаче рассмотрены в работе И. В. Виноградова [28] и В. В. Макарова [75].

Еще одной интересной нерешенной до конца задачей в этой группе автоматных перестановок является вопрос о порядке автомата с совпадаю-

щими входным и выходным алфавитами: конечно ли число автоматов, порожденных указанным автоматом или оно бесконечно. В 2017 году Пьер Жильбер доказал [120], что задача определения порядка автомата алгоритмически неразрешима. Он показал, что, начиная с размера входного алфавита, равного 22, задача определения порядка автомата с этим входвыходным алфавитом алгоритмически неразрешима. Позже этот результат был усилен Бартольди и Митрофановым [115]. Ранее С. В. Алешин показал [4], что в группе одноместных линейных автоматов над полем из двух элементов автомат имеет конечный порядок точно тогда, когда его переходы безусловны.

В 2020 году Н. В. Муравьев [85] нашел алгоритм определения порядка линейного (над любым конечным полем) автомата. Точная оценка конечного порядка линейного над полем автомата зависит лишь от характеристики поля и числа входов автомата. Таким образом, если число различных степеней заданного автомата оказывается больше этой точной оценки, то его порядок бесконечен. В работе Н. В. Муравьева [86] этот результат был распространен на случай поля рациональных чисел. Получилась точная оценка конечного порядка линейного над полем рациональных чисел автомата, зависящая лишь от числа входов автомата.

При синтезе автоматов с заданными свойствами важно знать, какие свойства оказываются инвариантными при построении сетей автоматов. Условие сохраняемости многообразия, которому принадлежит группа верхнего автомата суперпозиции, описывается конечным списком слов во входном алфавите и конечными системами уравнений. При таком подходе возможно построение сети автоматов, у которых рост порядка внутренней группы и числа состояний происходит с сохранением заданного многообразия группы. Как следствие возникает возможность моделирования конечных групп бернсайдовского типа с ограниченным в совокупности порядком степеней элементов [45]. Эти результаты получены в работе В. И. Малыгина [77]. Общее построение, связанное с вариацией операций над автоматами, осуществлено В. Б. Кудрявцевым в книге «Функциональные системы» [51].

1.2. Автоматы с операциями композиции. Из технических соображений для автоматов естественным образом возникла операция обратной связи в виде соединения выхода автомата с его собственным входом, исключающая мгновенную зависимость выхода от входа. Возникла вторая функциональная система автоматов с операциями суперпозиции и обратной связи, называемая композицией. В этой функциональной системе уже имеются конечные полные системы автоматов, например «штрих Шеффера» и «задержка». Более того, все полные системы в этом случае конечны. Для задачи полноты получился результат М. И. Кратко про алгоритмическую неразрешимость [47] и результат В. Б. Кудрявцева о континууме множества предполных классов [50]. Заметим, что критериальную систему образует счетное множество предполных классов (именно те, в которые вкладываются конечные множества автоматов). Но описать их другим способом не представляется возможным.

Нужны были новые методы исследования автоматных функций. Изменился характер задач в теории автоматов. Начался сбор положительных примеров и попытки различных вариаций этой задачи. Как отмечается в работе [52], возникли три основных подхода к задаче о полноте.

Первый подход связан с расширением понятия равенства автоматов и их множеств. Возникли следующие понятия полноты:

— A-полнота (В. А. Буевич, 1972 г. [19]). Для некоторого τ автоматные функции и считаются τ-равными, если они равны на словах длины τ. Автоматная функция A-выразима через множество автоматных функций S, если для каждого τ найдется τ-равная a-функция, выразимая через S. Оказалась, что проблема A-полноты алгоритмически неразрешима;
— Клини-полнота (Ю. Дассов, 1978 г. [118]). Автоматные функции считаются Клини-равными, если задаваемые ими регулярные множества совпадают. Проблема Клини-полноты также алгоритмически неразрешима;
— ε-полнота (А. С. Строгалов, 1986 г. [101]). Предполагается, что автоматные функции ε-равны, если они отличаются на множестве меры меньшей ε. Проблема ε-полноты также алгоритмически неразрешима.
— проблема полноты с учетом недостижимых состояний (И. В. Хазбун, 1992 г. [104]) также алгоритмически неразрешима.
— N-полнота (Д. Н. Бабин, 1994 г. [9]) — это выразимость относительно суперпозиции автоматов с не более чем N-состояниями. Здесь для каждого N удалось обнаружить двухместную универсальную функцию. Проблема N-полноты также алгоритмически неразрешима.

Второй подход связан с изучением полноты в подклассах автоматов.

А. А. Часовских в 1985 г. [106] в классе линейных автоматов над полем из двух элементов описал все предполные классы, число которых оказалось счетным и нашел, тем не менее, алгоритм распознавания полноты конечных систем. В дальнейшем этот результат был обобщен на классы линейных автоматов над конечными полями [110, 112].

Тальхайм [102] установил свойства решетки замкнутых классов одноместных стабильных автоматов. К. В. Коляда в 1984 г. [44] рассматривал классы функций, определенных на регулярных множествах (функции сопряженные к автоматным), и обнаружил для одних классов алгоритмическую неразрешимость, а для других алгоритмическую разрешимость проблемы полноты. Д. Н. Бабин [10] изучал полноту относительно суперпозиции и взятия подавтомата на словах фиксированной одинаковой длины.

Третий подход связан с ограничением на исследуемые системы автоматов. Еще в 1961 г. А. А. Летичевским [63] был получен алгоритм решения задачи о полноте для конечных систем автоматов, выдающих номер своего состояния (автоматов Медведева) при наличии всех булевых функций, а в 1986 г. В. А. Буевич [21] показал алгоритмическую разрешимость проблемы A-полноты для систем, содержащих все булевы функции. В 1992 г. Д. Н. Бабин [12] показал, что существует алгоритм распознавания полноты при наличии в рассматриваемой системе всех булевых функций. Очевидно, что для распознавания полноты существенна роль функций без памяти, присутствующих в базисе. Если присутствуют все функции без памяти, то алгоритм распознавания полноты и A-полноты существует. Если присутствует фактически лишь тождественная функция, то не существует алгоритма распознавания как полноты [47], так и A-полноты [19].

Верно ли, что по части базиса автоматов, не содержащей памяти, можно однозначно определить, разрешима ли проблема полноты для систем автоматов с этой частью и тем самым вскрыть природу алгоритмической неразрешимости по булевой части базиса? Д. Н. Бабин установил свойства всех классов диаграммы Поста [13]. В результате на диаграмме Поста получилась явная граница, отделяющая алгоритмически разрешимые случаи от неразрешимых. Эта же граница оказалась верной и для случая A-полноты. Оказалось, что для разрешимости полноты (A-полноты) необходимо и достаточно иметь в базисе либо функцию медиану, либо функцию тройную сумму. Похожие результаты позднее получил Д. Н. Жук [36] для дефинитных автоматов.

По определению предполагается, что вычисляющий автоматную функцию автомат «работает» бесконечно долго. Однако с точки зрения приложений совершенно очевидно, что каждое реальное кибернетическое устройство (в том числе, автомат) по истечении некоторого конечного промежутка времени прекращает свою «работу», т. е. либо становится ненужным, либо переводится в начальное состояние. В связи с этим естественно возникают задачи полноты и выразимости автоматных функций, работающих до момента τ. Эти задачи называются τ-полнота и τ-выразимость соответственно. В этом случае операция обратной связи автоматов выразима через суперпозицию. Множество автоматных функций на словах из множества $\{0, 1, \ldots, k-1\}$ длины τ становится замкнутым классом в $k\tau$-значной логике, и в следствие этого является конечно-порожденным.

В общем случае для любых $k \geqslant 2$, $\tau \geqslant 1$ задача о τ-полноте была решена В. А. Буевичем [19, 20]. Система автоматов называется аппроксимационно полной (A-полной), если она полна для всех $\tau \geqslant 1$. Проблема A-полноты, как показал В. А. Буевич, оказалась алгоритмически неразрешимой [22]. Для τ-полноты описание конечного числа предполных классов оказалось довольно сложным. В связи с этим возникла задача о полноте систем автоматных функций (S-функций), в каждом состоянии которых выходная функция принимает все k значений. Как показала М. А. Подколзина [93], описание S-предполных классов оказалось значительно проще, чем описание всех предполных классов для τ-полноты.

1.3. Применение автоматов. На практике сложность булевой функции приходится определять по ее таблице. Идеальной мерой сложности функции является число элементов в разложении функции по базису (сложность схемы из функциональных элементов, введенная и изученная С. В. Яблонским, О. Б. Лупановым и их учениками). Однако вычисление сложности булевой функции в упомянутой схеме приводит либо к трудноразрешимой задаче, либо к тотальному перебору всех схем ограниченной мощности. В этих условиях возрастает роль приближенных мер сложности, например числа коэффициентов полинома Жегалкина или автоматной сложности представления булевой функции.

Еще в работе 1966 г. [61] А. Д. Кузьмин ввел понятие автоматной сложности булевой функции как последовательно вычисляемой автоматом на наборе своих входных переменных. При таком способе задания сложностью функции будет число состояний вычисляющего автомата. В дальнейшем М. А. Кибкало нашла автоматную сложность функций из всех замкнутых классов Поста [42]. Для некоторых классов ей удалось получить точные значения функции Шеннона автоматной сложности булевых функций,

что само по себе редко встречается в теории сложности. Этот удивительный факт показывает, насколько хорошо автоматы моделируют вычисление булевых функций. Еще один новый эффект автоматной сложности, полученный М. А. Кибкало, — это возможность явного указания функций с максимальной автоматной сложностью.

А. Е. Андреевым, А. А. Часовских, А. А. Кудриным [7, 48] рассмотрена задача сложности вычисления автоматом значений формул и получено расслоение сложности автоматов на константную, логарифмическую и линейную по числу задержек в схемном представлении автомата в зависимости от длины формулы. Для почти всех базисов классов Поста эта сложность оказалась линейной.

Другой подход к реализации автоматами числовых функций заключается в том, что на вход автомата подается «случайная» последовательность из нулей и единиц, в которой единицы появляются с заданной частотой p. На выходе автомата возникает «случайная» последовательность из нулей и единиц, в которой единицы появляются с частотой $f(p)$, где функция f называется стохастической функцией автомата. Как показал А. В. Рябинин [100], стохастические функции автомата суть рациональные дроби с целыми коэффициентами.

В связи с широким применением искусственных нейронных сетей следует отметить, что их рекуррентные архитектуры являются автоматами, как правило, над полями характеристики 0. В работе [94] В. С. Половникова показано, что в некоторых базисах такие автоматы могут быть реализованы схемами, построенными с применением единственной операции обратной связи.

Известно, что не каждый конечный автомат моделируется линейным автоматом [119]. Однако если рассматривать линейные автоматы над полями характеристики 0 или трансцендентными расширениями конечных полей, то ситуация меняется [122]. В работе Д. В. Ронжина [97] рассматривались классы линейных автоматов над подкольцами рациональных чисел. В этом классе пропадает свойство конечных автоматов сохранять свойство периодичности последовательностей. Среди автономных автоматов здесь, например, содержится генератор последовательности Фибоначчи. Д. В. Ронжиным в [97] было найдено счетное множество A-предполных классов, что отличает рассматриваемый класс от классов линейных автоматов над конечными полями. Это позволило получить критерий A-полноты для множеств автоматов, реализующих сумматор в начальный момент времени, а также множеств автоматов, содержащих все одноместные автоматы.

Исследование операторов, позволяющих определять изменение состояний конечных автоматов во времени приводит к понятию переходной системы. С. Б. Родин в [96] получил критерий линейной реализуемости булевых операторов в случае отсутствия ограничений на длину кодировки и показал, что в этом случае для реализуемости рассматриваемых операторов достаточно полиномов Жегалкина степени не выше второй.

Распознавание через синтез вероятностного автомата заключается в настройке по обучающей выборке вероятностей переходов скрытых марковских моделей речевых образов, а затем распознавание их методом максимального правдоподобия. В 2007 году И. Л. Мазуренко предложил автоматную модель распознавания речи [74] и построил ряд демонстрационных

компьютерных систем распознавания речевых команд, в том числе ограниченного словаря в производственных шумах и с использованием датчиков различной природы (аудио, видео, тепло, движения губ, скорости воздушного потока и т. п.).

Обработка текстов на естественном языке включает поиск текстовой информации в больших и сверхбольших базах данных и знаний; автоматическая рубрикация текстов; построение интеллектуальных вопрос-ответных систем, способных отвечать на наиболее типичные вопросы пользователей; автоматический перевод текстов с одного языка на другой; генерацию текстов на заданную тему; аннотирование и реферирование текстов; распознавание речи; оптическое распознавание печатных и рукописных символов; создание человеко-машинных интерфейсов и так далее. Все эти области требуют специализированных лингвистических и математических моделей, позволяющих представлять синтаксис и семантику текста в удобном для автоматической обработке виде. Важным также является вопрос о проверке текста на естественность.

Одним из свойств естественного языка является постоянство частоты встречаемости в нем пар букв (и даже слов). Это свойство, названное «марковским», было открыто в 1913 г. А. А. Марковым при частотном анализе текста поэмы «Евгений Онегин» [80].

В 2008 году А. Б. Холоденко ввел определение регулярного языка с марковским свойством порядка n [105]. А именно для всех α и b должны существовать пределы частот встречаемости слова αb в слове ω из регулярного языка R при увеличении длины слова ω. Здесь α — слово длины n, а b — буква входного алфавита. Язык с марковским свойством порядка n является языком с марковским свойством порядка $n-1$. Существует язык с марковским свойством любого порядка, так сказать, абсолютно марковский язык. Свойство «марковости» порядка n и абсолютной «марковости» проверяемо по задающему язык автомату.

Конечный инициальный автомат порождает отображение

$$\mathfrak{F}: A^* \to B^*,$$

при этом B^* можно рассматривать как мультимножество, в котором допустимо вхождение нескольких копий одного и того элемента. В самом деле, некоторое слово β может быть выдано автоматом после подачи на начальное состояние нескольких слов $\alpha_1, \alpha_2, \ldots, \alpha_k$. В этом случае скажем что β имеет кратность k. Обозначим через B_k множество выходных слов кратности k. Д. В. Пархоменко [91, 92] доказал, что при любом k множество B_k регулярно.

Известная работа Э. Мура [123], приведшая к созданию теории экспериментов с автоматами, опиралась на явление отличимости состояний автомата, состоящее в том, что отличимые состояния по-разному реагируют на одно и то же входное слово. Для диагностики автоматов при возможности искажения входной последовательности понятие отличимости состояний было несколько расширено. Предполагалось, что подаваемая на автомат последовательность может исказиться не более чем в k позициях. Тогда для того, чтобы гарантированно отличить два состояния, мало потребовать отличимости их самой последовательностью. Необходима их отличимость всеми последовательностями, получаемыми из исходной искажением

не более чем в k позициях. Пары состояний, для которых существует такое слово, называются k-кратно отличимыми. Если никак не ограничивать класс автоматов, то сложность такого слова может быть экспоненциальной. В работе П. А. Пантелеева [90] получены некоторые оценки функции Шеннона для этого случая. Однако существует достаточно широкий класс так называемых кратно-приведенных автоматов, у которых все пары состояний отличимы для любого k, причем длина минимального отличающего слова ограничена полиномом второй степени относительно $|Q|$.

Для оптимизации скорости обработки информационных потоков важной задачей является прогнозирование входных данных. В работах [27, 31] А. Г. Вереникина и Э. Э. Гасанова показано, что множество бесконечных последовательностей букв входного алфавита (сверхслов) прогнозируемо некоторым конечным автоматом в точности тогда, когда оно состоит из периодических сверхслов с ограниченным периодом. В этих работах получены оценки на число состояний автомата, прогнозирующего заданное прогнозируемое множество сверхслов. Э. Э. Гасановым и А. А. Мастихиной в работах [33, 83] получены критерии частичной прогнозируемости автоматами общерегулярных сверхсобытий через свойства как этих сверхсобытий, так и представляющих их автоматов.

С задачей нахождения выхода из лабиринта люди сталкивались уже на ранних этапах развития цивилизации. Свидетельством этого может служить древнегреческий миф о том, как Тезей, убив Минотавра, сумел найти выход из лабиринта. Математической моделью лабиринта является граф, ребра которого соответствуют коридорам, а вершины — перекресткам лабиринта. Таким образом, в терминах графов задача о лабиринте заключается в построении метода, позволяющего найти маршрут в графе, который начинается в заданной вершине (вход) и наверняка приводит в другую заданную вершину (выход). В такой постановке задача о лабиринте близка к задачам обхода графов, т. е. к задачам, в которых требуется построить замкнутый маршрут, содержащий все вершины или все ребра графа. Действительно, следуя такому маршруту, мы обойдем все вершины графа, а значит, обязательно достигнем выхода.

Первым, кто начал изучать возможности автоматов по обходу лабиринтов, был К. Шеннон. В его работе 1951 года [128] рассматривалась задача поиска автоматом-мышью определенной цели в лабиринте. Л. Будах [117] доказал, что не существует конечного автомата, который обходил бы все плоские шахматные лабиринты. А. С. Подколзин [57] существенно упростил доказательство Будаха, а Г. Килибарда [43] привел другое доказательство, логически более простое, однако приводящее к более сложной ловушке.

Оказалось, что системы взаимодействующих автоматов, называемые также коллективами, уже могут решать задачу обхода лабиринтов. Автомат из такого коллектива в каждой вершине лабиринта получает информацию не только о возможных направлениях дальнейшего передвижения, но и о состояниях других автоматов, находящихся в той же вершине. При рассмотрении коллективов особо выделяют простейших членов коллектива — автоматы-камни. Камни — это автоматы без памяти, перемещение которых определяется другими автоматами коллектива. Коллектив, состоящий из n автоматов и t камней, называется коллективом типа (n, t).

М. Блюм и Д. Козен [116] доказали, что существуют коллектив типа $(1,2)$ и коллектив типа $(2,0)$, которые обходят произвольный конечный плоский мозаичный лабиринт и останавливаются после обхода.

В качестве другого усиления можно рассмотреть автоматы, оставляющие метки в вершинах лабиринта. А. З. Насыров [87] доказал, что существует автомат с одной краской, обходящий произвольный плоский прямоугольный лабиринт.

Представляет большой интерес автоматный аналог ситуации преследования хищниками своих жертв. В работе Н. Ю. Волкова [29], хищники и жертвы представляются в виде автоматов, которые, находясь в какой-либо клетке лабиринта, умеют обозревать некоторую ее окрестность и способны перемещаться в другую клетку лабиринта. Жертвы представляют собой независимую систему автоматов, а хищники — коллектив автоматов. Фиксируются скорости и обзоры хищников и жертв так, чтобы обзор хищников был не меньше обзора жертв, а скорость хищников — больше скорости жертв. Найдется лабиринт конечный квадрат, коллектив хищников и один автомат жертва с указанными свойствами такие, что жертва не будет поймана. Если же преследование происходит на бесконечной целочисленной плоскости, то существует конечный коллектив хищников, который ловит любую конечную независимую систему жертв.

Следует остановиться на вопросах сложности реализации конечных автоматов схемами. В работе [73] О. Б. Лупанова найдена асимптотика функции Шеннона $L(n)$ для булевых функций в произвольном конечном базисе, $L(n) \sim \rho\frac{2^n}{n}$, где ρ — константа, зависящая от базиса. Для автоматных базисов в общем случае задача поиска асимптотики функции Шеннона алгоритмически неразрешима [88].

Исследование плоских клеточных схем, реализующих булевы функции было начато С. С. Кравцовым [46], который определил, что порядок роста функции Шеннона сложности, определяемой через площадь схем, равен 2^n. Таким образом, по сравнению со схемами из функциональных элементов, как следует из представленного выше результата О. Б. Лупанова, порядок сложности функции Шеннона в этом классе, где «учитываются» проводники и изолирующие элементы, в n раз выше.

В работе [23] М. Н. Вайнцвайг ввел понятие мощности схемы из функциональных элементов как максимума по всем входным наборам элементов схемы, выдающих единицу. Г. В. Калачев исследовал переключательную мощность схемы, определяемую на парах входных наборов через количество элементов схемы, выходы которых отличаются на этой паре [39] и выяснил связь двух определений мощности. В работе [40] он показал, что при незначительных ограничениях на область определения булева оператора существует схема, имеющая оптимальный порядок мощности, площади и глубины. А. С. Воротников в работе [30] показал, что автомат с 2^n состояниями, не имеющий существенных входов, может быть реализован плоской схемой с площадью и средней по периоду выходной последовательности переключательной мощностью, равными по порядку 2^n и $\frac{2^{n/2}}{n}$ соответственно.

Понятие клеточного автомата было введено Джоном фон Нейманом для описания динамики биологических и технических систем [124, 125]. Клеточный автомат, называемый еще однородной структурой, состоит

из одинаковых автоматов, размещенных в клетках клеточной схемы, входы которых соединены с выходами соседних автоматов по некоторому шаблону. Клеточным автоматам посвящено много исследоваий. В работе [58] излагаются основные результаты по теории клеточных автоматов за 30 лет с момента возникновения этого понятия. Изучению структуры обратимых клеточных автоматов посвящена работа И. В. Кучеренко [62]. В ней полностью описана структура множества обратимых клеточных автоматов в классах бинарных клеточных автоматов с локальными функциями переходов из классов Поста.

Из многообразия задач, решаемых с использованием клеточных автоматов, отметим задачу однонаправленного движения точки на луче. Множество ячеек в этом случае представляет собой множество натуральных чисел. Каждая ячейка, кроме ячейки, соответствующей числу 1, имеет двух соседей. Определяемая структура называется экраном. Среди состояний ячеек выделяются черные состояния. Правильная конфигурация имеет ровно одну черную ячейку. На ячейку, соответствующую числу 1, потактово может подаваться управляющее сверхслово F из нулей и единиц, называемое законом движения, которое регулирует движение черной ячейки по лучу. В работе Е. Е. Титовой [103] доказано, что существует закон движения, который невозможно реализовать ни на каком экране, а также существование универсальных экранов для некоторых множеств законов движения.

Наличие только локальных связей между составляющими клеточного автомата приводит к значительным затратам времени при реализации ряда процессов. Поэтому естественным является рассмотрение моделей клеточных автоматов, составляющие которых могут передавать сигналы всем элементарным автоматам единовременно. В работе Э. Э. Гасанова [32] было дано определение клеточного автомата с локаторами, которое уточнено в дальнейшем Д. Э. Ибрагимовой [38]. В статье Д. И. Васильева [25] показано, что для задачи поиска ближайшего соседа на прямой использование клеточного автомата с локаторами, по сравнению с классической моделью, позволяет сократить сложность с линейной до логарифмической. Нижняя логарифмическая оценка для времени решения этой задачи одномерными клеточными автоматами с локаторами получена в работе Д. И. Васильева и Э. Э. Гасанова [26]. Рост производительности при переходе от классической модели клеточного автомата к клеточным автоматам с локаторами показан для задачи сложения векторов на прямой. В классическом случае время вычисления будет не меньше чем длина большего вектора, а в модели с локаторами эту задачу можно решить за время на константу большее, чем удвоенный логарифм длины меньшего вектора [38].

Как показано в работе Э. Э. Гасанова и А. А. Пропажина [34], использование клеточных автоматов с локаторами является эффективным для реализации баз данных типа «ключ-значение». Согласно результатам этой работы, существует клеточный автомат с локаторами и пользователем, который реализует базу данных типа «ключ-значение» и выполняет операции поиска, вставки и удаления за время, не превышающее суммарной длины ключа и значения.

Реализация клеточного автомата с локаторами чипом при ограничениях на локаторы и алфавит вещания предложена в работе Г. В. Калачева [41].

Последние результаты по теории автоматов в 2019 году вошли в книгу В. Б. Кудрявцева, С. В. Алешина, А. С. Подколзина «Введение в теорию автоматов (издание 2)» [55].

§ 2. Выразимость и полнота в классе конечных автоматов

2.1. Арность автоматных базисов. Будем рассматривать автоматные функции с операцией суперпозиции. Пусть $E_k = \{0, 1, \ldots, k-1\}$, функции вида $g\colon E_k^n \to E_k$ называются функциями k-значной логики, их множество обозначается через P_k. Пусть E_k^∞ — множество всех сверхслов вида $a(1)a(2)\ldots$, где $a(j) \in E_k$, $j = 1, 2, \ldots$. Через $\mathbb{N}$ обозначим множество натуральных чисел. Пусть

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

— автоматная функция (a-функция), т. е. она задается рекуррентно следующими соотношениями:

$$\begin{cases} q_1(1) = q0_1, \\ \ldots \\ q_s(1) = q0_s, \\ q_1(t+1) = \varphi_1(q_1(t), \ldots, q_s(t), a_1(t), \ldots, a_n(t)), \\ \ldots \\ q_s(t+1) = \varphi_s(q_1(t), \ldots, q_s(t), a_1(t), \ldots, a_n(t)), \\ b_1(t) = \psi_1(q_1(t), \ldots, q_s(t), a_1(t), \ldots, a_n(t)), \\ \ldots \\ b_m(t) = \psi_m(q_1(t), \ldots, q_s(t), a_1(t), \ldots, a_n(t)). \end{cases} \tag{1}$$

Вектор $q = (q_1, \ldots, q_s)$ задает состояние a-функции f, $q0$ — ее начальное состояние, буквы $a = (a_1, a_2, \ldots, a_n)$ и $b = (b_1, \ldots, b_m)$ называют входной и выходной буквами, а сверхслова $a(1)a(2)\ldots$ и $b(1)b(2)\ldots$ — входными и выходными сверхсловами соответственно. Вектор-функции φ и ψ называются функцией переходов и выходной функцией соответственно, а шестерка

$$(E_k^n, E_k^s, E_k^m, \varphi, \psi, q0)$$

— автоматом, порождающим функцию f. Далее в тексте мы иногда будем использовать для автомата обозначение $(A, Q, B, \varphi, \psi, q0)$, при этом предполагая, что $A \subseteq E_k^n$, $Q \subseteq E_k^s$, $B \subseteq E_k^m$.

Для определения автоматной функции мы будем также использовать следующие соотношения

$$\begin{cases} q(1) = q0, \\ q(t+1) = \varphi(q(t), a(t)), \\ b(t) = \psi(q(t), a(t)). \end{cases} \tag{2}$$

Обычным образом доопределим функции φ и ψ на слова:

$$\varphi(q, a(1)\dots a(t)) = \varphi(\varphi(\dots\varphi(q, a(1)), \dots, a(t-1)), a(t)), \tag{3}$$

$$\psi(q, a(1)\dots a(t)) = \psi(\varphi(q, a(1)\dots a(t-1)), a(t)) \tag{4}$$

и введем функцию

$$\overline{\psi}(q, a(1)\dots a(t)) = \overline{\psi}(q, a(1)\dots a(t-1))\psi(\varphi(q, a(1)\dots a(t-1)), a(t)).$$

Класс всех a-функций обозначим через $\boldsymbol{P}$. Заметим, что функция $\overline{\psi}(q0, a(1)\dots)$ — это и есть автоматная функция, задаваемая уравнениями (1), (2). Шестерка $(E_k^n, Q, E_k^m, \varphi, \psi, q0)$ неединственна для автоматной функции. Автоматы, имеющие одну и ту же автоматную функцию, называются эквивалентными.

Для автоматов обычным образом введем операции суперпозиции. Для суперпозиции будем использовать модификации операций из [78]:

$$(\eta f)(x_1, x_2, \dots, x_n) = f(x_2, x_3, \dots, x_n, x_1),$$
$$(\varepsilon f)(x_1, x_2, \dots, x_n) = f(x_2, x_1, x_3, \dots, x_n),$$
$$(\varpi f)(x_1, x_2, \dots, x_n) = f(x_1, x_1, \dots, x_{n-1}),$$
$$(\delta f)(x_1, x_2, \dots, x_n) = f(x_2, x_3, \dots, x_{n+1}),$$
$$(f * g)(x_1, x_2, \dots, x_{m+n-1}) = f(g(x_1, \dots, x_m), x_{m+1}, \dots, x_{m+n-1}).$$

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

Автоматная функция $d\colon E_k^* \to E_k^*$ с уравнениями

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

называется «задержкой». Будем обозначать через $\boldsymbol{K}$ множество всех автоматных функций без входа или константных (выдающих всегда одно и то же периодическое слово).

Конечных полных относительно суперпозиции систем автоматных функций не существует [113], поэтому важен вопрос о минимальном числе переменных полной системы конечных автоматов.

О п р е д е л е н и е 1. Пусть f и g — автоматные функции с одинаковым числом входов и одинаковым числом выходов. Будем говорить, что автоматная функция g копирует автоматную функцию f, если найдутся натуральные n, j, k $(n \leqslant j)$ такие, что для любого $l = 0, 1, 2, \dots$ и любой входной последовательности значение автоматной функции g в момент времени $j + kl$ совпадает со значением функции f в момент $n + kl$, т. е. $g(j + kl) = f(n + kl)$ для $l = 0, 1, 2\dots$.

П р и м е р 1. Пусть f — некоторая автоматная функция, выдающая свое состояние, это так называемая автоматная функция Медведева. Подставим на все ее выходы задержки d. Полученная функция $D(f)$ на одной

и той же последовательности выдает то же самое, что и исходная функция, но на один такт позже. Следовательно, $D(f)$ копирует f.

Заметим, что $\varphi(D(f(a)), D(a)) = f(a)$. В самом деле: $\widetilde{q} = D(f(a))$ — это прошлое состояние, $\widetilde{a} = D(a)$ — это прошлый входной сигнал. Согласно действию переходной функции $\varphi(\widetilde{q}, \widetilde{a}) = q$. Здесь q — это состояние автомата в настоящий момент.

Обобщая эту конструкцию, получаем лемму о выразимости копируемой функции через копирующую функцию, функции из P_k и константные функции через операции суперпозиции. Имеет место лемма [11].

Л е м м а 1. *Пусть $\mathcal{F}$ — автоматная функция Медведева и пусть некоторая автоматная функция g копирует ее, тогда $\mathcal{F} \in [\{g, d\} \cup K \cup P_k]$.*

Без ограничения общности рассмотрим систему автоматных функций для $k = 2$:

$$F = \{ f_i(x_1, \ldots, x_{m_i}), m_i = i \cdot 2^i, i = 1, 2, \ldots \} \cup P_2,$$

где f_i — автоматная функция с $m_i = i \cdot 2^i$ входами и i выходами, задаваемая системой уравнений:

$$\begin{cases} q_1(1) = 0, \ldots, q_i(1) = 0, \\ (q_1(t+1), \ldots, q_i(t+1)) = \varphi_i(q_1(t), \ldots, q_i(t), x_1(t), \ldots, x_{m_i}(t)), \\ f_i(t) = (q_1(t), \ldots, q_i(t)). \end{cases}$$

Занумеруем наборы из E_2^i лексикографическим образом: через $q^{(s)} \in E_2^i$ обозначим набор с номером s. Функция φ_i задается формулой

$$\varphi_i(q^{(s)}(t), x_1(t), \ldots, x_{m_i}(t)) = (x_{si+1}(t), x_{si+2}(t), \ldots, x_{si+i}(t)).$$

Согласно [54] система F полна относительно операции суперпозиции.

Заметим, что входная буква $x \in E_2^m$ задает подстановку $\varphi_x \colon E_2^i \mapsto E_2^i$, где $\varphi_x(q) = \varphi(q, x)$.

Функция φ такова, что любая подстановка множества E_2^i может быть задана некоторой, причем единственной, входной буквой из E_2^m. Таким образом, $\{\varphi_x | x \in E_2^m\}$ — это полная полугруппа подстановок множества E_2^i.

Входное слово $x(t+1), \ldots, x(t+m)$ длины m в алфавите E_2^m также задает подстановку

$$\varphi_{x(t+1),\ldots,x(t+m)}(q) = \varphi_{x(t+m)}(\varphi_{x(t+m-1)}(\ldots \varphi_{x(t+1)}(q) \ldots)).$$

Пусть отображение $\alpha \colon \left(E_2^m\right)^m \mapsto E_2^m$ каждому входному слову $x(1) \ldots x(m)$ длины m ставит в соответствие входную букву, задающую ту же подстановку, что и слово $x(1) \ldots x(m)$. Будем покомпонентно записывать $\alpha(y) = (\alpha_1(y), \alpha_2(y), \ldots, \alpha_m(y))$, через e обозначим букву, задающую тождественную подстановку ($\varphi_e(q) = q$, $q \in E_2^i$).

Определим вспомогательные автоматные функции u, v и w следующего вида. Функция u имеет m входов и m выходов и задается формулой:

$$u(t) = \begin{cases} e & \text{при } t \neq lm, \\ \alpha(x(lm - m + 1), \ldots, x(lm)) & \text{при } t = lm. \end{cases}$$

Функция v имеет m входов и 1 выход и на входной последовательности $a(t)=(a_1(t),\ldots,a_m(t))\in E_2^m$ выдает:

$$v(a)=\begin{cases}0 & \text{при } t<m,\\ a_{s+1}(ml) & \text{при } t=lm+s,\ 0\leqslant s<m.\end{cases}$$

Функция w имеет один вход и m выходов и на последовательности $b(t)\in E_k$ выдает

$$w(t)=\begin{cases}e & \text{при } t\neq lm,\ l=2,3,\ldots,\\ b(lm-m),b(lm-m+1),\ldots,b(lm-1) & \text{при } t=lm,\ l=2,3,\ldots.\end{cases}$$

Рассмотрим суперпозицию $g(x)=\mathcal{F}(w(v(u(x_1,\ldots,x_m))))$. Имеет место лемма [11].

Л е м м а 2. *A-функция g копирует a-функцию $\mathcal{F}$.*

A-функции u и v могут быть выражены через одноместные автоматные функции и функции из P_2. Имеют место

Л е м м а 3. *Автоматная функция u принадлежит $\left[K\cup P_2\cup\{d\}\right]$.*

Л е м м а 4. *Автоматная функция v принадлежит $\left[K\cup P_2\cup\{d\}\right]$.*

Поскольку задержка d является одноместной автоматной функцией, то справедлива

Л е м м а 5. *$f_i\in\left[P^1\cup P_2\right]$ при всех i.*

Здесь через P^1 обозначено множество одноместных a-функций. Поскольку $\{f_i\,|\,i=1,2,\ldots\}$ является базисом в P, то справедливы теоремы [11].

Т е о р е м а 1. *Объединение множества всех автоматных функций одной переменной и функций из P_k — полная система.*

Поскольку все функции из P_k выразимы через одну двуместную функцию Вебба, то справедлива

Т е о р е м а 2. *Множество всех автоматных функций от двух переменных — полная система.*

2.2. О выразимости некоторых автоматных функций. Сверхслово, получающееся на выходе константного автомата K_1, обозначим β_{K_1}. Периодическое сверхслово β можно представить в виде

$$\beta=\gamma\alpha^{\infty}.$$

Выберем из всех представлений такое, что γ и α имеют наименьшую длину. Для выбранного представления назовем γ наименьшим предпериодом сверхслова, а α — наименьшим периодом сверхслова.

Для множества сверхслов K' обозначим через $\Theta(K')$ множество длин минимальных периодов сверхслов K'.

Назовем автомат групповым, если все $\varphi_a(q)=\varphi(a,q)$, $a\in A$ являются биекциями на Q. Обозначим через $|\alpha|$ длину слова α.

Скажем, что множество натуральных чисел N_1 делит множество натуральных чисел N_2, $N_1\,|\,N_2$, если для любого числа $n_1\in N_1$ найдется $n_2\in N_2$, $n_1\,|\,n_2$.

Обозначим через $<M>$ замыкание относительно суперпозиции множества $[M \cup \{G_0, P_k\}]$. Назовем $<M>$ замыканием M относительно *расширенной суперпозиции*.

Рассмотрим множество $\Theta(<R> \cap K)$ для произвольного множества R. Заметим, что P_k можно заменить на одну функцию Вебба. Расширенная суперпозиция — это суперпозиция с конечной добавкой. Имеет место лемма [64].

Лемма 6. *Пусть* $K_1,\ K_2 \in \boldsymbol{K}$, *причем* $\Theta(K_2) \mid \Theta(K_1)$. *Тогда выполнено* $K_2 \in <K_1>$.

Из леммы следует, что, имея в замыкании хотя бы одну константу периода l, мы можем выразить любую константу периода делящего l.

Если множество периодов константных функций ограничено, то все они суть делители одного натурального числа. Имеет место

Замечание 1. Пусть $|\Theta(<R> \cap K)| < \infty$, тогда

$$\Theta(<R> \cap K) = \{l \in \boldsymbol{N} \colon l \mid \max \Theta(<R> \cap K)\}.$$

Конечное множество константных функций таково, что найдется периодическое сверхслово β такое, что $<K'> = <\{\beta\}>$.

Из известной леммы об удлинении периода периодических сверхслов автоматом [113] известно, что множество длин периодов констант, выразимых автоматом, имеет вид $2^{l_1} 3^{l_2} \dots p_i^{l_{i-1}}$, где p_i — простые числа, $p_i \leqslant |Q|$, а l_i — натуральные числа или ноль.

Для некоторого автомата M и произвольного слова $\alpha \in A^*$ обозначим через $s_\alpha = \varphi(q, \alpha)$ подстановку на множестве состояний, задаваемую этим словом, π_α — разбиение множества состояний Q на классы отличимости $Q_1, \dots, Q_s$ этим словом. Состояния q_i и q_j принадлежат одному классу отличимости, если $\overline{\psi}(q_i, \alpha) = \overline{\psi}(q_j, \alpha)$.

Обозначим $p_\alpha = (s_\alpha, \pi_\alpha)$. Пусть $P_l = \{p_\alpha, |\alpha| = l\}$.

Рассмотрим последовательность $n_1, n_2, \dots, n_k, \dots$ натуральных чисел, связанную с автоматом M, где n_{i+1} получается из n_i следующим рекуррентным способом.

Пусть $c_i = \{\alpha_i\}$ — множество сверхслов с длиной периода $l \mid n_i$. Рассмотрим множество $M(c_i)$ выходных сверхслов автомата A после подачи на него слов из c_i. Очевидно, что $M(c_i)$ — конечно. Тогда положим $n_{i+1} = \text{НОК}(\Theta(M(c_i)))$. Из замечания 1 следует, что n_i — максимальная длина периода констант, выразимых схемой глубины i.

По построению $n_i \mid n_{i+1}$. Пусть $m_i = \dfrac{n_{i+1}}{n_i}$, оказывается, что $m_1, m_2, \dots$ — периодическая последовательность. Имеет место лемма [64].

Лемма 7. *Последовательность* m_i *периодична*.

Теперь определим *цикловые индексы* автомата через алгоритм их вычисления.

- Вычисляем последовательность (n_i, P_i) до тех пор, пока не найдутся $j < i$ такие, что $P_{n_i} = P_{n_j}$.
- Назовем $b = n_j$ безусловным цикловым индексом автомата, $q = \dfrac{n_i}{n_j}$ — главным цикловым индексом автомата.

Имеют место следующие теоремы [64, 67].

Т е о р е м а 3. *Пусть R — конечное множество автоматных функций, тогда $\Theta(<R>\cap K)=\bigcup_{i=1}^{\infty}\{t\mid bq^i\}$, где b, q — цикловые индексы системы автоматов R.*

Из предыдущей теоремы следует

Т е о р е м а 4. *Пусть R — конечное множество автоматных функций и β — константная автоматная функция, тогда существует алгоритм, позволяющий проверить свойство $\beta\in<R>$.*

Т е о р е м а 5. *Сложность алгоритма, решающего задачу выразимости конечного множества константных автоматов через автомат с n состояниями составляет не более, чем $O(2^{n^n})$.*

С л е д с т в и е 1. *Пусть R — конечное множество автоматных функций, тогда существует алгоритм, позволяющий проверить свойство $|\Theta(<R>|\cap K)|<\infty$.*

Непосредственно из теоремы 3 следует также

Т е о р е м а 6 (необходимое условие выразимости). *Пусть R_1, R_2 — конечные множества автоматов и $R_2\in[R_1]$. b_1, q_1, b_2, q_2 — цикловые индексы R_1 и R_2 соответственно. Тогда*

$$\bigcup_{i=1}^{\infty}\{t\mid b_2q_2^i\}\subseteq\bigcup_{i=1}^{\infty}\{t\mid b_2q_2^i\}\quad и\quad \Theta(<R_2>\cap K)\subseteq\Theta(<R_1>\cap K).$$

Техника цикловых индексов позволяет усилить лемму 1, получается лемма [64].

Л е м м а 8. *Пусть f — a-функция Медведева и g копирует f, пусть также выполнено условие $|\Theta(<g>\cap K)|=\infty$, тогда $f\in<g>$.*

Автомат $H=(V,Q,W,\varphi,\psi,q0)$, называется *линейным*, если

$$\begin{cases}\varphi(x,q)=Aq+Bx,\\ \psi(x,q)=Cq+Dx,\\ q_0=(0,0,\ldots,0),\end{cases}$$

где A,B,C,D подходящие линейные операторы. Класс всех линейных автоматов обозначим через $\boldsymbol{L}$. Имеют место теоремы [66, 68].

Т е о р е м а 7. *Пусть M — произвольная конечная система автоматов, а L_1 — линейный автомат, тогда*

$$L_1\in<M>\Leftrightarrow\Theta(<L_1>\cap K)\in\Theta(<M>\cap K).$$

Т е о р е м а 8. *Задача выразимости линейных автоматов через произвольное конечное множество автоматов относительно расширенной суперпозиции алгоритмически разрешима.*

Т е о р е м а 9. *Пусть $M\in P$, $|M|<\infty$, G_1 — групповой автомат Медведева. Тогда задача $G_1\in<M>$ алгоритмически разрешима.*

Пусть $M\in P$, $|M|<\infty$, P^N — множество автоматов с не более, чем N состояниями.

Т е о р е м а 10. *Задача $<M>\supseteq P^N$ — алгоритмически разрешима.*

2.3. Класс автоматных функций не расширяющийся до предполного. Пусть $A' \subseteq A^*$ некоторое конечное подмножество входных слов одинаковой длины, автомат $\mathsf{A}' = (A', Q, B', \varphi, \overline{\psi}, q_0)$, где $\mathsf{B}' = \overline{\psi}(Q, A')$, называется *подавтоматом* автомата $\mathsf{A} = (A, Q, B, \varphi, \psi, q_0)$,

Автоматы $\mathsf{A}_1 = (A_1, Q_1, B_1, \varphi_1, \psi_1, {q_0}^1)$, $\mathsf{A}_2 = (A_2, Q_2, B_2, \varphi_2, \psi_2, {q_0}^2)$ называются изоморфными, если они получаются взаимнооднозначным переименованием входного, выходного алфавитов и множества состояний δ, λ, μ соответственно, $\mu({q_0}^1) = {q_0}^2$, т. е. следующие диаграммы коммутативны.

$$\begin{array}{ccc} \varphi_1 : Q_1 \times A_1 & \longrightarrow & Q_1 \\ \downarrow\mu \quad \downarrow\delta & & \downarrow\mu \\ \varphi_2 : Q_2 \times A_2 & \longrightarrow & Q_2 \end{array} \qquad \begin{array}{ccc} \psi_1 : Q_1 \times A_1 & \longrightarrow & Q_1 \\ \downarrow\mu \quad \downarrow\delta & & \downarrow\lambda \\ \varphi_2 : Q_2 \times A_2 & \longrightarrow & Q_2 \end{array}$$

Если при этом отображение μ не является взаимно-однозначным, то скажем, что автомат A_2 является гомоморфным образом автомата A_1.

Скажем, что автомат A_2 делит автомат A_1, $\mathsf{A}_2 \mid \mathsf{A}_1$, если A_2 является гомоморфным образом некоторого подавтомата A_1.

Будем говорить, что автоматная функция f_2 делит автоматную функцию f_1, если минимальный автомат функции f_2 делит минимальный автомат функции f_1.

Класс автоматных функций R называется предполным, если $R \subset \boldsymbol{P}$ и для любой автоматной функции $f \notin R$ выполнено $[\{f\} \bigcup R] = \boldsymbol{P}$.

Без ограничения общности рассмотрим случай, когда входной и выходной алфавиты всех автоматов — суть булевые векторы.

Автоматную функцию Медведева T_0 со следующими функциями переходов:

$$\begin{cases} \varphi(q_1, 00) = q_1, \varphi(q_2, 00) = q_2, \\ \varphi(q_1, 01) = q_1, \varphi(q_2, 01) = q_1, \\ \varphi(q_1, 10) = q_2, \varphi(q_2, 10) = q_2, \\ \varphi(q_1, 11) = q_2, \varphi(q_2, 11) = q_1 \end{cases}$$

назовем *триггером*.

Пусть $\varphi_a(q) = \varphi(q, a)$, $a \in A$, множество подстановок вида $\{\varphi_a, a \in A\}$ порождает полугруппу подстановок $S_{\mathsf{A}} = \{\varphi_\alpha, \alpha \in A^*\}$, называемую полугруппой автомата A.

Автомат называется групповым, если все φ_α, $\alpha \in A^*$ являются биекциями на Q. В этом случае полугруппа автомата является группой.

Если полугруппа S транзитивно действует на множестве Q, то автомат Медведева $\mathsf{A} = (S, Q, Q, \varphi, \psi_0, q_0)$, где $\varphi(q, s) = s(q)$, $q \in Q$, $s \in S$, $\psi_0(q, s) = q$, назовем *стандартным автоматом с полугруппой* S.

Пусть C — *простая некоммутативная группа*, стандартный автомат с группой C назовем *простым автоматом*.

Обозначим через $\boldsymbol{S}$ функциональную систему конечных полугрупп с операциями взятия подполугрупп, гомоморфных образов и расширения, а через $<\boldsymbol{S}'>$ — замыкание множества полугрупп $\boldsymbol{S}' \subseteq \boldsymbol{S}$ относительно указанных операций. Пусть $D_0 = \boldsymbol{P_2} \cup \{G_0, T_0\}$, $D_1 = \boldsymbol{K} \cup \boldsymbol{P_2} \cup \{G_0, T_0\}$.

Заметим что если $C_1 \subseteq C$ простая подгруппа простой группы C, то простой автомат с группой C_1 выразим суперпозициями с использованием булевых функций через простой автомат с группой C.

Более того, из леммы о копировании [11] следует

Лемма 9. *Пусть $\boldsymbol{C}$ — простой автомат. Для некоторого автомата $\boldsymbol{A}$ выполнено $\boldsymbol{C} \mid \boldsymbol{A}$ точно тогда, когда $\boldsymbol{C} \in [\boldsymbol{A} \cup \boldsymbol{D_1}]$.*

Из простоты группы C следует [16]

Лемма 10. *Пусть $\boldsymbol{M}$ — множество автоматов, простой автомат $\boldsymbol{C} \in [\boldsymbol{M} \bigcup \boldsymbol{D_1}]$, тогда найдется автомат $\boldsymbol{A} \in \boldsymbol{M}$ такой, что $\boldsymbol{C} \in [\mathrm{A} \bigcup \boldsymbol{D_1}]$*

Рассмотрим систему простых автоматов со знакопеременными группами, обозначим через $\boldsymbol{A_n}$ простой автомат с группой A_n. Обозначим через $\boldsymbol{Prime(M)}$ множество простых автоматов $\boldsymbol{A_n}$ в замыкании множества $\boldsymbol{M} \bigcup D_1$. Всякая группа является подгруппой подходящей знакопеременной, в том числе и знакопеременная меньшего порядка. Имеет место лемма [8].

Лемма 11. $[\{\boldsymbol{A_n} \mid n = 5, 6, \ldots\} \cup \boldsymbol{D_1}] = \boldsymbol{P}$.

Имеет место теорема [16].

Теорема 11. *Не существует предполного класса автоматных функций, содержащего замкнутый класс $[\boldsymbol{K} \cup \boldsymbol{P_2} \cup \{G_0, T_0\}]$.*

В самом деле. От противного, если существует предполный класс

$$\boldsymbol{M} \supseteq \boldsymbol{D_1} = [\boldsymbol{K} \cup \boldsymbol{P_2} \cup \{G_0, T_0\}],$$

то для $\boldsymbol{Prime(M)}$ имеются две возможности:

1. $|\{\boldsymbol{A_n} \mid n = 5, 6, \ldots\} \bigcap \boldsymbol{M}\}| = \infty$. Тогда для любого n выполнено $\boldsymbol{A_n} \in \boldsymbol{M}$, значит $[\boldsymbol{M}] = \boldsymbol{P}$ и $\boldsymbol{M}$ не предполный класс, а полная система.

2. $|\{\boldsymbol{A_n} \mid n = 5, 6, \ldots\} \bigcap \boldsymbol{M}\}| < \infty$, число простых автоматов $\boldsymbol{A_n}$ из $\boldsymbol{M}$ конечно и равно N. В этом случае добавление автомата $\boldsymbol{A_{N+1}}$ не приведет к полноте, так как в полной системе должны быть выразимы все простые автоматы. Однако $\boldsymbol{A_{N+2}}$ не делит ни один из автоматов системы $\{\boldsymbol{A_n} \mid n = 5, 6, \ldots, N+1\} \bigcup \boldsymbol{D_1}\}$.

Проанализируем замкнутые классы, вложимые в предполные. Заметим, что замкнутые классы содержащие $\boldsymbol{P_2} \cup \{T_0\}$, но не содержащие $\boldsymbol{K}$, вложимы в предполные. Имеют место [17]

Теорема 12. *Пусть замкнутые классы μ, X таковы, что*

$$[\boldsymbol{P_2} \cup \{T_0\}] \subseteq \mu \subset X, \quad \mu \not\supseteq \boldsymbol{K}, \quad \boldsymbol{K} \subset X,$$

тогда класс μ расширяется до предполного класса в X.

Следствие 2. *Всякий конечно-порожденный замкнутый класс μ в замкнутом классе автоматных функций $X \supseteq [\boldsymbol{K} \cup \boldsymbol{P_2} \cup \{T_0\}]$ расширяется до предполного.*

Следствие 3. *Всякий конечно-порожденный замкнутый класс μ в $\boldsymbol{P}$ расширяется до предполного.*

Получается итоговая

Теорема 13. *Замкнутый класс $\mu \supseteq [\boldsymbol{P_2} \cup \{T_0\}]$ расширяется до предполного точно тогда, когда $\mu \not\supseteq \boldsymbol{K}$.*

Все полученные результаты верны также для автоматных функций над $E_k = \{0, 1, \ldots, k-1\}$.

2.4. Классификация автоматных базисов Поста по разрешимости свойств полноты и A-полноты. В этой главе будут рассмотрены автоматы над множеством E_2 с двумя операциями: суперпозиции и обратной связи или так называемой композиции. Операция обратной связи (о. с.), примененная к i-й входной и j-й выходной переменным a-функции $f(x_1, \ldots, x_n) = (y_1, \ldots, y_m)$, задает a-функцию

$$g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = (y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_m),$$

вычисляемую алгоритмически следующим образом. Считаем, что о. с. применима к f в состоянии q, если ψ_j в уравнении (1) фиктивно зависит от a_i при $q(t) = q$, а вычисление $b_s(t)$ осуществляется по схеме

$$\begin{cases} q(1) = q_1, \\ q(t+1) = \varphi(q(t), a_1(t), \ldots, a_{i-1}(t), \psi_j(q(t), a_1(t), \ldots a_{i-1}(t), \\ \quad a_{i+1}(t), \ldots, a_n(t)), a_{i+1}(t), \ldots, a_n(t)), \\ b_s(t) = \psi_s(q(t), a_1(t), \ldots, a_{i-1}(t), \psi_j(q(t), a_1(t), \ldots, a_{i-1}(t), \\ \quad a_{i+1}(t), \ldots, a_n(t)), a_{i+1}(t), \ldots, a_n(t)), \\ s = 1, 2, \ldots, j-1, j+1, \ldots, m. \end{cases}$$

Считаем, что о. с. применима к f, если она применима в начальном состоянии q_1 и из ее применимости в состоянии $q(t)$ следует применимость в состоянии $q(t+1)$. Пусть $M \subseteq \boldsymbol{P}$, в этой главе обозначим через $[M]$ множество всех a-функций, получающихся из M с помощью операций суперпозиции и обратной связи. Множество M называется полным, если $[M] = \boldsymbol{P}$. Проблема полноты для $\boldsymbol{P}$ состоит в описании всех полных множеств M.

Пусть τ — натуральное число, $f(x_1, \ldots, x_n)$ — некоторая автоматная функция, $f^\tau \colon (E_2^\tau)^n \to (E_2^\tau)^m$ — ограничение этой функции на множество слов длины τ. Скажем, что a-функции $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_n)$ τ-равны, если $f^\tau = g^\tau$.

Обозначим через $[M]_\tau$ множество всех a-функций, τ-равных получающимся из M с помощью операций суперпозиции и обратной связи. Множество M называется τ-полным, если $[M]_\tau = \boldsymbol{P}$. Пусть τ — натуральное число, $f(x_1, \ldots, x_n)$ — некоторая автоматная функция, $f^\tau \colon (E_2^\tau)^n \to (E_2^\tau)^m$ — ограничение этой функции на множество слов длины τ. Скажем, что a-функции $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_n)$ τ-равны, если $f^\tau = g^\tau$.

Через $[M]_A$ обозначается множество $[M]_A = \bigcap_{\tau=1}^{\infty} [M]_\tau$. Проблема A-полноты для $\boldsymbol{P}$ состоит в описании всех A-полных множеств M. Очевидно, что полное множество M является A-полным.

Поскольку нас интересует работа схемы из автоматных функций лишь до некоторого момента времени, обратную связь в каждой конкретной схеме можно заменить на цепочку суперпозиций подходящей длины.

А. А. Летичевский [63] получил критерий полноты для автоматов, выдающих номер своего состояния (автоматы Медведева), относительно операции композиции. Кроме того, предполагалось, что в системе есть все функции без памяти. Таким образом, задача полноты относительно композиции была им ослаблена. Автомат рассматривался только как функция переходов, а выходную функцию автомата, которая задавала связь автоматов между собой, реализовывала подходящая функция без памяти.

В дальнейшем эти ограничения были преодолены в работах В. А. Буевича [21] в 1986 г. и Д. Н. Бабина [12] в 1992 г. Они показали разрешимость проблемы полноты для систем с добавкой из булевых функций.

Для выразимости констант требуется *несохранение* счетного числа предикатов $a(i) = a(j)$, $i, j = 2, 3, \ldots$ на *циклах* по состояниям автомата, т. е. для любых i, j найдутся слова α, β, γ, $|\alpha| = i$, $|\alpha\beta| = j$ и буква a такие, что $\psi(q, \alpha a) \neq \psi(q, \alpha\beta a)$, $\varphi(q, \alpha\beta\gamma) = q$ для некоторого состояния q.

Для A-полноты — несохранение этого же предиката на *путях* автомата. В этом случае достаточно лишь первого условия. Здесь i, j номера тактов работы автомата. Благодаря конечности автомата счетного перебора предикатов по всем i, j удалось избежать. Таким образом, выразимость констант — это умение автоматов отличать такты работы или последовательная память.

Параллельная память — это способность воспроизвести прошлый сигнал, эти свойством обладает автомат задержка. Для выразимости автомата задержки требуется *несохранение* предикатов на паре циклов: для любого i найдутся слова α, γ_1, γ_2, $|\alpha| = i$, $|\gamma_1| = |\gamma_2|$ и буквы a, b, c такие, что

$$\psi(q, \alpha a c) \neq \psi(q, \alpha b c), \qquad \varphi(q, \alpha a \gamma_1) = q, \qquad \varphi(q, \alpha b \gamma_2) = q.$$

Для A-выразимости автомата задержки требуется только первое условие.

Ввиду цикличности автомата условия 1) и 2) проверяемы. Дело в том, что счетное число проверяемых на сохранение предикатов образует конечное число классов с одинаковыми вход-выходными множествами пар букв (входная/выходная буква). Такая же конструкция, но с более сложными предикатами, проходит для использования в базисах вместо всех булевых функций, только булевы функций из некоторого замкнутого класса Поста.

Требуется рассмотреть сохранение предикатов на фрагментах диаграммы автомата: циклах, двойных циклах, тройных циклах. Оказывается, что несохранение отношений на циклах длины N является критериальным условием для выразимости счетчика по модулю N, отсутствие соотношений на двойных циклах — условием выразимости селекторных функций, отсутствие отношений на тройных циклах — условием выразимости булевой функции от двух переменных.

Для задачи A-полноты рассматривается сохранение отношений на путях, двойных путях, тройных путях. При этом несохранение отношений на путях длины τ является критериальным условием для τ-выразимости счетчика по модулю τ, отсутствие соотношений на двойных путях — условием A-выразимости селекторных функций, отсутствие отношений на тройных путях — условием выразимости булевой функции от двух переменных.

В разрешимом случае за время t такое, что $\log\log\log\log t \leqslant |Q|^2 2^{n+m}$, где $|Q|$ — число состояний автоматной функции, n — число входов, m — число выходов, удается установить наличие или отсутствие соответствующих отношений на циклах длины N при всех натуральных N.

Для выразимости «задержки» строится аппарат, который описывает процессы запоминания, хранения и выдачи информации автоматной функцией. Информационный цикл предполагает возможность сначала запоминания, затем произвольного времени хранения и, наконец, выдачи информа-

ции о том, какой сигнал поступил на вход. Информационный цикл обеспечивается работой схемы из автоматных функций, обменивающихся информацией. Выразимость задержки — это возможность построения схемы, обеспечивающей информационный цикл. Д. Н. Бабин показал [12], что этот факт может быть проверен за $O((2^{|Q|})!(2^{2n(2^{|Q|})!}))$.

Пусть π — множество всех классов Поста, Sol и Sol_A суть множества таких $\Phi \in \pi$, что для конечных $\nu \subset P$ проблема полноты $\Phi \bigcup \nu$ и, соответственно, A-полноты множества $\Phi \bigcup \nu$ разрешима, а $UnSol$ и $UnSol_A$ суть аналогичные множества с неразрешимой проблемой полноты. Назовем классы из Sol и Sol_A сильными классами Поста, а из $UnSol$ и $UnSol_A$, соответственно, — слабыми. В процессе доказательства теорем оказалось [14], что

$$Sol = Sol_A, \qquad UnSol = UnSol_A.$$

Заметим, что всякий надкласс сильного класса является сильным, а подкласс слабого — слабым. Двойственный к сильному, относительно замены 0 на 1, будет сильным, а к слабому — слабым классом Поста.

Для слабых классов Поста проверку сохранения предикатов выполнить не удается. Однако удается свести проблему полноты и A-полноты к проблеме конечности числа продукций Поста, которая алгоритмически неразрешима.

Тройка $\Theta = <D, \rho, w>$, где $D = \{d_1, \ldots, d_k\}$, D^* — множество слов в алфавите D, ρ: $D \to D^*$, $\rho(d_i) = R_i$, w — натуральное число, называется системой однородных продукций Поста. Если $l \geqslant w$, то скажем, что Θ применима к слову $\xi = d_{i_1} d_{i_2} \ldots d_{i_l}$ и слово $\Theta(\xi) = d_{i_{w+1}} d_{i_{w+2}} \ldots d_{i_l} R_{i_1}$ назовем результатом применения Θ к слову ξ. Последовательность $\xi_1, \xi_2, \ldots$ такую, что $\xi_1 = \xi$, а $\xi_{i+1} = \Theta(\xi_i)$, назовем последовательностью продукций слова ξ. Известно [79], что существует система однородных продукций Поста, для которой не существует алгоритма, по слову ξ решающего вопрос о конечности последовательности продукций слова ξ. Зафиксируем систему продукций Поста $<D, \rho, w>$ с неразрешимой проблемой конечности последовательности продукций. Сводимость полноты автоматов к проблеме конечности продукций Поста состоит в том, что автомат выполняет продукцию, задаваемую входным словом.

Очевидно, что если проблема полноты (A-полноты) алгоритмически неразрешима для систем вида $F_1 \bigcup \nu$, то она неразрешима для систем вида $F_2 \bigcup \nu$ и $F_1' \bigcup \nu$, где $F_2 \subseteq F_1$, а F_1' двойственный к F_1 замкнутый класс. Поэтому для построения классификации разрешимость проблемы полноты не надо проверять на всех классах Поста. Д. Н. Бабин проверил ее на классах L_4, D_2, F_3^4, S_6, O_9.

Имеет место [14]

Т е о р е м а 14. *Проблема полноты (A-полноты) системы $\Phi \cup \nu$, $\Phi \subseteq P_2$ разрешима точно тогда, когда функция $x \oplus y \oplus z \in \Phi$ либо функция $xy \cup xz \cup yz \in \Phi$.*

Пусть $h(x_1, x_2, x_3, x_4) = x_1x_2 \vee x_1x_3 \vee x_1x_4 \vee x_2x_3 \vee x_2x_4 \vee x_3x_4$, $F = [\{h, \overline{x} \vee y\}]$, и F' — двойственный к F.

Число классов $\Phi \in \pi$, содержащихся в F' или в F, — бесконечно, а не содержащихся ни в F' ни в F — конечно, поэтому имеет место

С л е д с т в и е 4. *Множества Sol и Sol_A конечны, множества $UnSol$ и $UnSol_A$ бесконечны.*

Для функций k-значной логики P_k решетка замкнутых классов не описана, но тем не менее, кое-что можно сказать о классификации автоматных базисов, содержащих конкретные замкнутые классы.

Множество функций $f\colon (E_k)^n \to E_k$, для которых выполнено одно из свойств: $n=1$ или f не принимает всех значений из E_k, называется классом Слупецкого. Известно, что класс Слупецкого замкнут относительно суперпозиции, т. е. результат применения суперпозиции к функциям из этого класса является функцией из этого же класса [113]. Будем обозначать класс Слупецкого через SLUP.

Для $l \in \{0, 1, \ldots, k-1\}$ функция $f \in P_k$ такая, что $f(l, l, \ldots, l) = l$, называется сохраняющей константу l, а множество всех таких функций — классом сохранения константы l, оно обозначается через U_l. Обозначим через U класс $\bigcap_{i=0}^{k-1} U_l$ сохранения всех констант. Известно, что классы U, U_l, $l=1, 2, \ldots, k-1$, замкнуты относительно суперпозиции, т. е. результаты применения суперпозиции к функциям из этих классов являются функциями из этих же классов [113].

Имеют место следующие утверждения [15].

Т е о р е м а 15. *Пусть* $\Phi \subseteq$ SLUP, *не существует алгоритма, по конечному множеству* $\nu \subseteq \boldsymbol{P}$ *решающего вопрос, верно ли, что* $[\Phi \cup \nu] = \boldsymbol{P}$.

Т е о р е м а 16. *Пусть* $\Phi \subseteq$ SLUP, *не существует алгоритма, по конечному множеству* $\nu \subseteq \boldsymbol{P}$ *решающего вопрос, верно ли, что* $[\Phi \cup \nu]_A = \boldsymbol{P}$.

Т е о р е м а 17. *Для любого* $\Phi \supseteq U$ *существует алгоритм, по конечному множеству* $\nu \subseteq \boldsymbol{P}$ *решающий, верно ли, что* $[\Phi \cup \nu] = \boldsymbol{P}$.

Т е о р е м а 18. *Для любого* $\Phi \supseteq U$ *существует алгоритм, по конечному множеству* $\nu \subseteq \boldsymbol{P}$ *решающий, верно ли, что* $[\Phi \cup \nu]_A = \boldsymbol{P}$.

Дефинитным называется автомат, для которого найдется натуральное t такое, что каждое входное слово длины t переводит автомат из любого состояния в одно и то же состояние, зависящее от этого входного слова.

Если выбирать множество автоматных функций ν из дефинитных автоматов, то задача полноты для системы $\Phi \cup \nu$ разрешима точно тогда, когда в классе Φ содержится функция $x \oplus y \oplus z$, либо функция $xy \cup xz \cup yz$, либо функции, порождающие класс F_2^3, либо функции, порождающие класс F_6^3 [36]. Заметим, что граница сильных классов в этом случае строго понижается (см. рис. 1). Оказывается, что понижение границы сильных классов (возможно, не строгое) будет происходить при переходе к системам $\nu \subseteq M \subseteq P$. То есть, свойство классов быть сильными сохраняется при сужении множества $M \supseteq \nu$.

§ 3. Линейные автоматы

Для простого числа p и натурального m через $GF(p^m)$, как принято, мы обозначаем конечное поле, состоящее из p^m элементов, а через $GF(p^m)^n$ обозначаем n-ю декартову степень этого поля:

$$GF(p^m)^n = \{\ (a_1, a_2 \ldots a_n)\ \mid\ a_i \in GF(p^m)\ \}\,.$$

Пусть $n, s \in \mathbb{N}$. Матрицу с n строками, s столбцами и элементами из $GF(p^m)$ будем называть (n, s)-матрицей над $GF(p^m)$.

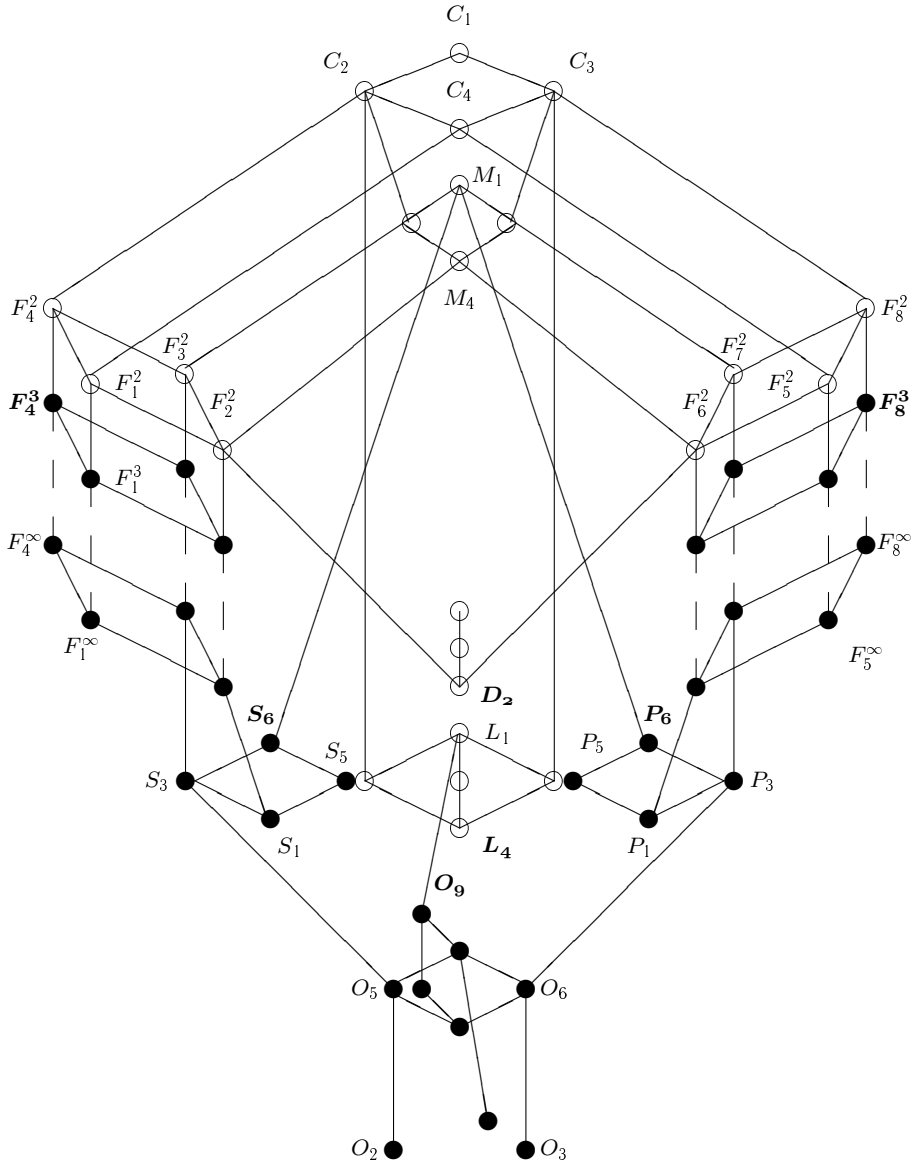

Рис. 1. Диаграмма классов Поста (сильные классы обозначены белыми кружками, слабые — черными)

Линейный инициальный автомат для некоторых натуральных чисел n и s задается шестеркой:

$$\left(GF(p^m)^n,\, GF(p^m)^s,\, GF(p^m),\, \varphi,\, \psi,\, q_0\right), \tag{5}$$

где $GF(p^m)^n$ — входной алфавит, $GF(p^m)^s$ — алфавит состояний, $GF(p^m)$ — выходной алфавит и

$$\varphi : GF(p^m)^n \times GF(p^m)^s \to GF(p^m)^s,$$
$$\psi : GF(p^m)^n \times GF(p^m)^s \to GF(p^m)$$

являются линейными по каждому аргументу, что означает существование (s,s)-матрицы A, (s,n)-матрицы B, а также векторов C и D, $C \in GF(p^m)^s$, $D \in GF(p^m)^n$ таких, что для любых x и q, $x \in GF(p^m)^n$, $s \in GF(p^m)^s$ выполнены равенства:

$$\varphi(q,x) = Aq^T + Bx^T, \quad \psi(q,x) = Cq^T + Dx^T,$$

q_0 — начальное состояние автомата, $q_0 \in GF(p^m)^s$.

О линейном автомате $\mathfrak{A}$, заданном шестеркой (5), будем говорить, что он имеет n входов и один выход. Функционирование линейного автомата $\mathfrak{A}$ во времени t, $t = 0, 1, 2, \ldots$, определяется системой канонических уравнений:

$$\begin{cases} q(0) = q_0, \\ q(t+1) = Aq^T(t) + Bx^T(t), \\ x(t) = Cq^T(t) + Dx^T(t). \end{cases}$$

Если на входы автомата $\mathfrak{A}$ в моменты t, $t = 0, 1, \ldots$ подавать наборы $x(t)$, $x(t) = \left(x_1(t), x_2(t), \ldots, x_n(t)\right)$, то на выходе автомата получаем последовательность $y(t)$, $t = 0, 1, \ldots$, элементов поля $GF(p^m)$. При этом на i-й вход автомата подается последовательность $x_i(t)$, $t = 0, 1, \ldots$. Сопоставим этим последовательностям степенные ряды: α_i, $\alpha_i = \sum_{t=0}^{\infty} x_i(t)\xi^t$, $i = \overline{1,n}$, а последовательности $y(t)$ — ряд β, $\beta = \sum_{t=0}^{\infty} y(t)\xi^t$.

В [35] показано, что для рассматриваемого автомата найдутся такие степенные ряды μ_i, $\mu_i = \sum_{t=0}^{\infty} a_i(t)\xi^t$, $i = \overline{0,n}$, такие, что последовательности $a_i(t)$, $t = 0, 1, \ldots$, их коэффициентов периодические (с предпериодом) и для любых входных последовательностей и соответствующей им выходной последовательности выполнено:

$$\beta = \sum_{i=1}^{n} \mu_i \alpha_i + \mu_0. \tag{6}$$

Множество всех степенных рядов от переменной ξ с коэффициентами из $GF(p^m)$ обозначим $R_{p^m}(\xi)$. Таким образом, автомат $\mathfrak{A}$ осуществляет отображение из $R_{p^m}(\xi)^n$ в $R_{p^m}(\xi)$ в соответствии с равенством (6). В дальнейшем коэффициент при ξ^t ряда α, $\alpha \in R_{p^m}(\xi)$, мы обозначаем $\alpha(t)$.

Степенной ряд, последовательность коэффициентов которого периодична (с предпериодом) можно представить отношением многочленов со знаменателем, не делящимся на ξ, причем такое сопоставление обратимо. Множество $GF(p^m)[\xi]$ состоит из многочленов от переменной ξ с коэффициентами из поля $GF(p^m)$. Положим

$$E'_{p^m}(\xi) = \left\{ \frac{u}{v} \;\middle|\; u, v \in GF(p^m)[\xi], v \not\vdots \xi \right\}.$$

Лемма 12 [35].

1. *Для любого линейного автомата с n входами в $E'_{p^m}(\xi)$ найдутся такие дроби μ_i, $i=\overline{0,n}$, что для любых входных последовательностей и соответствующей им выходной последовательности, представленных, соответственно, в виде рядов α_i, $i=\overline{1,n}$ и β, выполнено равенство (6).*
2. *Для любого n, $n\in\mathbb{Z}_+$, любых дробей μ_i, $\mu_i\in E'_{p^m}(\xi)$, $i=\overline{0,n}$, найдется линейный автомат, значения входов и выхода которого связаны равенством (6).*

Таким образом, линейный автомат $\mathfrak{A}$ для некоторого n задает отображение

$$\mathfrak{A}(x_1,x_2,\ldots,x_n)=\sum_{i=1}^{n}\mu_i x_i+\mu_0 \tag{7}$$

из $R_{p^m}(\xi)^n$ в $R_{p^m}(\xi)$. Коэффициенты μ_i, $i=\overline{1,n}$, называются передаточными функциями автомата $\mathfrak{A}$, а μ_0 — его свободным ходом.

Множество всех линейных автоматов над полем $GF(p^m)$ обозначим L_{p^m}.

Вход x_i линейного автомата, осуществляющего отображение (7), называется существенным, если $\mu_i\neq 0$, т. е. выход автомата зависит от этого входа. Два линейных автомата равны, если они осуществляют одинаковые входно-выходные отображения, в соответствии с равенством (7), на множествах существенных переменных.

Над линейными автоматами можно выполнять операции суперпозиции, включающие переименования переменных без отождествления, отождествление переменных, подстановку. Операции суперпозиции могут быть дополнены обратной связью. В этом случае получаем операции композиции. Перечисленные операции определены в [54].

Лемма 13 [35, 53]. *Пусть $\mathfrak{A}_1$ и $\mathfrak{A}_2$ — линейные автоматы,*

$$\mathfrak{A}_j: R_{p^m}^{n_j}\to R_{p^m},$$

$$\mathfrak{A}_j\left(x_{j,1},x_{j,2},\ldots,x_{j,n_j}\right)=\sum_{i=1}^{n_j}\mu_{j,i}x_{j,i}+\mu_{j,0},\quad j=\overline{1,2}.$$

1. *Переименовав входы $\mathfrak{A}_1$ с $x_{1,1},x_{1,2},\ldots,x_{1,n_1}$ на $x'_{1,1},x'_{1,2},\ldots,x'_{1,n_1}$, получим автомат $\mathfrak{A}_3$,*

$$\mathfrak{A}_3\left(x'_{1,1},x'_{1,2},\ldots,x'_{1,n_1}\right)=\sum_{i=1}^{n_1}\mu_{1,i}x'_{1,i}+\mu_{1,0}. \tag{8}$$

2. *Отождествив входы x_{1,n_1-1} и x_{1,n_1} автомата $\mathfrak{A}_1$, получим автомат $\mathfrak{A}_4$,*

$$\begin{aligned}\mathfrak{A}_4&\left(x_{1,1},x_{1,2},\ldots,x_{1,n_1-1}\right)=\\&=\sum_{i=1}^{n_1-2}\mu_{1,i}x_{1,i}+\left(\mu_{1,n_1-1}+\mu_{1,n_1}\right)x_{1,n_1-1}+\mu_{1,0}.\end{aligned} \tag{9}$$

3. *Подставив $\mathfrak{A}_2$ на вход x_{n_1} автомата $\mathfrak{A}_1$, получим автомат $\mathfrak{A}_5$,*

$$\begin{aligned}\mathfrak{A}_5&\left(x_{1,1},x_{1,2},\ldots,x_{1,n_1-1},x_{2,1},x_{2,2},\ldots,x_{2,n_2}\right)=\\&=\sum_{i=1}^{n_1-1}\mu_{1,i}x_{1,i}+\sum_{i=1}^{n_2}\mu_{1,n_1}\mu_{2,i}x_{2,i}+\mu_{1,0}+\mu_{1,n_1}\mu_{2,0}.\end{aligned} \tag{10}$$

4. *Операция обратной связи применима к входу x_{1,n_1} автомата $\mathfrak{A}_1$ в точности если $\mu_{1,n_1}(0)=0$. В этом случае, применив к x_{1,n_1} операцию обратной связи, получим автомат $\mathfrak{A}_6$,*

$$\mathfrak{A}_6\left(x_{1,1},x_{1,2},\ldots,x_{1,n_1-1}\right)=\sum_{i=1}^{n_1-1}\frac{\mu_{1,i}}{1-\mu_{1,n_i}}x_{1,i}+\frac{\mu_{1,0}}{1-\mu_{1,n_1}}. \qquad (11)$$

Замыкание множества M, $M\subseteq L_{p^m}$ по операциям суперпозиции обозначаем $S(M)$, а по операциям композиции — $K(M)$. Понятия замкнутого, предполного, полного множества по рассматриваемым операциям переносятся сюда с класса всех автоматов.

Пример полного в L_{p^m} по операциям композиции множества линейных автоматов:

$$M_K=\{x_1+x_2,\xi x,ax,1\mid a\in GF(p^m)\}.$$

Пусть p_i, $i=1,2,\ldots,$ — последовательность всех неприводимых приведенных многочленов из $GF(p^m)[\xi]$, где $p_1=\xi$ и $p_i\neq p_j$ при $i\neq j$. По операциям суперпозиции полным является, например, множество:

$$M_S=\left\{x_1+x_2,\xi x,ax,\frac{1}{p_i}x,1\;\middle|\;a\in GF(p^m),i\in\{2,3,\ldots\}\right\}.$$

В. А. Буевичем было введено понятие A-замыкания [19]. Для множества линейных автоматов M автомат $\mathfrak{A}$, заданный равенством (7), содержится в A-замыкании множества M, обозначаемом $A(M)$, в точности если для любого τ, $\tau\in\mathbb{Z}_+$, в $K(M)$ найдется автомат $\mathfrak{A}_\tau$,

$$\mathfrak{A}_\tau\left(x_1,x_2,\ldots,x_n\right)=\sum_{i=1}^{n}\mu_{\tau,i}x_i+\mu_{\tau,0}$$

такой, что для любого t, $t\in\{0,1,\ldots,\tau\}$, и для любого i, $i\in\{0,1,\ldots,n\}$, выполнено $\mu_i(t)=\mu_{\tau,i}(t)$. Автомат $\mathfrak{A}_\tau$ будем называть τ-эквивалентным автомату $\mathfrak{A}$.

Заметим, что для множества автоматов (не обязательно линейных) M выполнены включения:

$$S(M)\subseteq K(M)\subseteq A(M).$$

Для класса линейных автоматов задачу полноты оказалось удобнее решать, начиная с оператора A-замыкания, обладающего большими, по сравнению с S-замыканием и K-замыканием, выразительными возможностями.

Примером A-полного множества, не являющегося K-полным, является множество:

$$M_A=\{x_1+x_2,(\xi+\xi^p)\,x,ax,1\mid a\in GF(p^m)\}.$$

3.1. Полнота в классах линейных автоматов. Рассмотрим следующие подмножества множества L_{p^m}:

$$T_a=\left\{\mathfrak{A}\;\middle|\;\mathfrak{A}\in L_{p^m},(7)\Rightarrow\sum_{i=1}^{n}\mu_i(0)a+\mu_0(0)=a\right\},\quad\text{где } a\in GF(p^m),$$

$$V_p=\left\{\mathfrak{A}\;\middle|\;\mathfrak{A}\in L_{p^m},(7)\Rightarrow\sum_{i=1}^{n}\mu_i(0)-1=0\right\}.$$

Переменная x_i линейного автомата, заданного равенством (7), называется непосредственной, если $\mu_i(0)=1$.

$$V_1=\{\mathfrak{A}\mid \mathfrak{A}\in L_{p^m}, \text{в } \mathfrak{A} \text{ не более одной непосредственной переменной}\},$$
$$M_1=\{\mathfrak{A}\mid \mathfrak{A}\in L_{p^m}, (7)\Rightarrow \forall i, i\in\{1,2,\ldots,n\}, \mu_i(1)=0\}.$$

Если поле $GF(p^m)$ не является простым, т. е. если $m>1$, то оно содержит собственные подполя, не совпадающие с полем $GF(p^m)$. Любое подполе в $GF(p^m)$ является полем $GF(p^{m'})$ для некоторого делителя m' числа m [69]. Такое поле, не совпадающее с $GF(p^m)$ и являющееся максимальным по включению, назовем максимальным собственным подполем $GF(p^m)$. Пусть $GF(p^{m_s})$, $s=\overline{1,l}$ — все максимальные собственные подполя поля $GF(p^m)$.

Нам понадобятся еще следующие подмножества линейных автоматов:

$$P_s=\{\mathfrak{A}\mid \mathfrak{A}\in L_{p^m}, (7)\Rightarrow \forall i, i\in\{1,2,\ldots,n\}, \mu_i(0)\in GF(p^{m_s})\}\,,$$

где $s\in\{1,2,\ldots,l\}$.

Множество всех предполных классов в классе линейных автоматов L_{p^m} с операцией A-замыкания обозначим $J^A_{p^m}$.

Т е о р е м а 19 [112].

$$J^A_{p^m}=\begin{cases}\{T_a, V_p, V_1, M_1\mid a\in GF(p)\}\,, & \text{если } m=1,\\ \{T_a, V_p, V_1, M_1, P_s\mid a\in GF(p^m), s\in\{1,2,\ldots,l\}\}\,, & \text{если } m>1.\end{cases}$$

Для доказательства этой теоремы можно использовать следующий план.

Пусть $a\in GF(p)$. Используя автоматы, не содержащиеся в V_p и в V_1, можно получить автомат с передаточной функцией μ_a, $\mu_a(0)=a$. В случае $m>1$ для получения передаточных функций μ_a таких, что $\mu_a(0)=a$, $a\in GF(p^m)$, потребуются автоматы, не содержащиеся в классах P_s.

Действительно, если $m>1$, $M\subseteq GF(p^m)$ и для любого s, $s\in\{1,2,\ldots,l\}$, выполнено $M\not\subseteq GF(p^{m_s})$, тогда, что нетрудно видеть, из элементов множества M, используя только операцию умножения, можно получить все ненулевые элементы поля $GF(p^m)$.

Далее, из автоматов множества линейных автоматов M, не содержащегося в классах из $J^A_{p^m}$, можно получить автомат $f^{(1)}_+$ 1-эквивалентный сумматору $x_1+x_2+\ldots+x_{p+1}$ и две константы γ_0, γ_1 такие, что $\gamma_0(0)=0$, $\gamma_1(0)\neq 0$.

Для любого линейного автомата множество $M^{(1)}$:

$$M^{(1)}=A\left(\left\{\mu_a x+\mu'_a, f^{(1)}_+, \gamma_0, \gamma_1\right\}\right)$$

содержит автомат, который ему 1-эквивалентен. Из автоматов множества M остается получить автомат $g(x)$ 2-эквивалентный задержке ξx и показать A-полноту множества $M^{(1)}\cup\{g(x)\}$.

Из теоремы 19 несложными рассуждениями получаем следующее

С л е д с т в и е 5. *Проверка A-полноты конечных множеств линейных автоматов осуществляется на словах длины 2.*

Переход от задачи A-полноты к задаче K-полноты с учетом леммы 13 приводит к исследованию алгебры $E'_{p^m}(\xi)$ с оператором замыкания, включающим 3 операции: сложения, умножения и операцию «fb», индуцированную обратной связью для автоматов. Операция «fb» является частичной и применима к паре μ_1, μ_2, если $\mu_2(0)=0$. В этом случае $\mathrm{fb}\,(\mu_1, \mu_2)=\dfrac{\mu_1}{1-\mu_2}$.

Положим:

$$M_1^{(1)} = \left\{\mu \mid \mu \in E'_{p^m}(\xi),\ \mu(1)=0\right\},$$
$$P_s^{(1)} = \left\{\mu \mid \mu \in E'_{p^m}(\xi),\ \mu(0) \in GF\left(p^{m_s}\right)\right\},$$

где $GF\left(p^{m_s}\right)$, $s=\overline{1,l}$, — все максимальные собственные подполя в $GF\left(p^m\right)$.

Для каждого i, $i>1$, определим следующее множество дробей:

$$R_i^{(1)} = \left\{\mu \;\middle|\; \mu \in E'_{p^m}(\xi),\ \mu=\frac{u}{v},\ u \vdots p_i,\ v \not\vdots p_i\right\}, \quad i=2,3,4,\ldots.$$

Поле $GF(p^m)$ обладает ровно m автоморфизмами [69]. Множество этих автоморфизмов, образующих группу по операции композиции, обозначим $\mathrm{Aut}(GF(p^m))$. Известно, что для каждого ω, $\omega \in \mathrm{Aut}(GF(p^m))$, найдется j, $j \in \{0, 1, \ldots m-1\}$, что для любого a, $a \in GF(p^m)$, выполнено

$$\omega(a) = a^{p^j}.$$

Если $\mu \in E'_{p^m}(\xi)$, $\mu=\dfrac{u}{v}$ и $\deg u \leqslant \deg v$, то, представив дробь $\mu(1/\xi)$ в виде отношения многочленов $\mu'=\dfrac{u'}{v'}$, положим:

$$\Psi_0\,(\mu) = \left(\mu(0), \mu'(0)\right).$$

Если $\mu \in E'_{p^m}(\xi)$, $\mu=\dfrac{u}{v}$ и $v \not\vdots p_i$ для некоторого i, $i \in \{2, 3, \ldots\}$, то в $E'_{p^m}(\xi)$ найдется дробь μ', $\mu'=\dfrac{u'}{v}$ и в $E_{p^m}[\xi]$ найдется многочлен u', $\deg(u') < \deg(p_i)$, такие, что имеет место равенство

$$\mu = u' + p_i\mu'.$$

В этом случае положим:

$$\Psi_i\,(\mu) = \left(\mu(0), u'\right).$$

Нам понадобятся следующие подмножества в $E'_{p^m}(\xi)$:

$$M_{0,\omega}^{(1)} = \left\{\mu \;\middle|\; \mu \in E'_{p^m}(\xi),\ \mu=\frac{u}{v},\ \deg u \leqslant \deg v,\ \Psi_0\,(\mu) = (\mu(0),\ \omega(\mu(0)))\right\};$$
$$M_{i,\omega}^{(1)} = \left\{\mu \;\middle|\; \mu \in E'_{p^m}(\xi),\ \mu=\frac{u}{v},\ v \not\vdots p_i,\ \Psi_i\,(\mu) = (\mu(0), \omega(\mu(0)))\right\}.$$

Поле $GF(p)$ обладает единственным тождественным автоморфизмом id. Поэтому вместо обозначения $M_{i,\mathrm{id}}^{(1)}$ мы будем использовать обозначение $M_i^{(1)}$.

Через $J_{p^m}^{(1)}$ обозначим множество, состоящее из всех максимальных собственных подклассов в алгебре $E'_{p^m}(\xi)$.

Т е о р е м а 20 [112].

$$J_{p^m}^{(1)} = \begin{cases} \left\{M_i^{(1)}, R_i^{(1)} \mid i=0, 1, \ldots\right\}, & m=1, \\ \left\{M_1^{(1)}, M_{i,\omega}^{(1)}, R_i^{(1)}, P_s^{(1)} \mid i \in \{0, 2, 3, \ldots\},\right. & \\ \left.\omega \in \mathrm{Aut}(GF(p^m)),\ s \in \{1, 2, \ldots, l\}\right\}, & m>1. \end{cases}$$

Для доказательства этой теоремы сначала были расширены возможности оператора $K^{(1)}$-замыкания заменой операции fb на деление и показано, что множество дробей M из $E'_{p^m}(\xi)$, не содержащееся ни в одном из классов множества $J^{(1)}_{p^m}$ по операциям сложения, умножения и деления порождает все поле отношений многочленов из $GF(p^m)[\xi]$. Затем, при использовании того, что операция деления для представления любой дроби может быть применена не более одного раза, показано, как из элементов множества M получить $K^{(1)}$-полное множество, используя лишь оператор замыкания $K^{(1)}$.

Для линейного автомата $\mathfrak{A}$, заданного равенством (7), положим: $U(\mathfrak{A}) = \{\mu_i \mid i = \overline{1,n}\}$. Для определения множества всех предполных классов по операциям композиции в L_{p^m} нам понадобятся следующие множества:

$$M_{i,\omega} = \{\mathfrak{A} \mid U(\mathfrak{A}) \subset M^{(1)}_{i,\omega}\},$$

где $i \in \{0,2,3,\dots\}$, $\omega \in \mathrm{Aut}(GF(p^m))$. В случае простого поля вместо $M_{i,\mathrm{id}}$ мы используем обозначение M_i.

$$R^e_0 = \Big\{\mathfrak{A} \Big| (7) \Rightarrow \text{если } \mu_i = \frac{u}{v} \text{ и } x_i \text{ — единственная существенная переменная } \mathfrak{A}, \text{ то } \deg u \leqslant \deg v; \text{ в противном случае } \mu \in R^{(1)}_0 \Big\};$$

$$R^d_0 = \Big\{\mathfrak{A} \Big| (7) \Rightarrow \text{если } \mu_i = \frac{u}{v} \text{ и } x_i \text{ — единственная непосредственная переменная } \mathfrak{A}, \text{ то } \deg u \leqslant \deg v; \text{ в противном случае } \mu \in R^{(1)}_0 \Big\};$$

$$R^e_i = \Big\{\mathfrak{A} \Big| (7) \Rightarrow \text{если } \mu_i = \frac{u}{v} \text{ и } x_i \text{ — единственная существенная переменная } \mathfrak{A}, \text{ то } v \not\vdots p_i; \text{ в противном случае } \mu \in R^{(1)}_i \Big\};$$

$$R^d_i = \Big\{\mathfrak{A} \Big| (7) \Rightarrow \text{если } \mu_i = \frac{u}{v} \text{ и } x_i \text{ — единственная непосредственная переменная } \mathfrak{A}, \text{ то } v \not\vdots p_i; \text{ в противном случае } \mu \in R^{(1)}_i \Big\},$$

где $i = 2,3,\dots$.

В случае $m = 1$ положим:

$$J_p = J^A_p \cup \left\{M_i, R^e_i, R^d_i \mid i \in \{0,2,3,\dots\}\right\},$$

а в случае $m > 1$

$$J_{p^m} = J^A_{p^m} \cup \left\{M_{i,\omega}, R^e_i, R^d_i \mid i \in \{0,2,3,\dots\}, \omega \in \mathrm{Aut}(GF(p^m))\right\}.$$

Теорема 21 [112]. *Множество J_{p^m} является множеством предполных в L_{p^m} классов по операциям композиции.*

Индукцией по построению автоматов несложно показать, что каждое множество из J_{p^m} по операциям композиции является замкнутым классом, при этом ни один из классов множества J_{p^m} не содержится в другом. Следующим и основным этапом доказательства теоремы 21 является обоснование критериальности множества J_{p^m}, т. е. полнота любого M, $M \subseteq L_{p_m}$, такого, что $\forall\Theta$, $\Theta \in J_{p^m}$, выполнено: $M \not\subseteq \Theta$. Для этого потребовалось показать выразимость сумматора $x_1 + x_2 + \dots + x_{p+1}$ из такого множества M. После этого ясно, что выполнено включение

$$K^{(1)}(U(M)) \subseteq U(K(M))$$

и выразимость всех передаточных функций вытекает теперь из полноты $U(M)$ в $E'_{p^m}(\xi)$. Отсюда и из включения $x_1+x_2+\ldots+x_{p+1}\in K(M)$ следует, что для любой μ, $\mu\in E'_{p^m}$, выполнено

$$\mu x_1+\ldots+\mu x_p+x_{p+1}\in K(M).$$

Теперь, если получить из автоматов множества M нулевую константу, то несложно установить полноту M в L_{p^m}, выразив из элементов множества M все автоматы полного по операциям композиции множества M_K, которое было введено ранее.

Нулевую константу можно выразить, используя константы γ_0, γ_1, $\gamma_0(0)=0$, $\gamma_1(0)\neq 0$, получаемые так же, как и при доказательстве теоремы 19, и автоматы $\xi x_1+\ldots+x_px_p+x_{p+1}$, $ax_1+\ldots+ax_p+x_{p+1}$.

Теорема 21 позволяет получить алгоритм проверки K-полноты конечных множеств автоматов. Предполагаем, что на вход алгоритма подается конечное множество M линейных автоматов. Каждый автомат задан набором несократимых отношений многочленов из $E'_{p^m}(\xi)$: передаточными функциями и свободным ходом. В качестве входных параметров алгоритма будем использовать следующие:

- r — увеличенное на единицу количество линейных автоматов в множестве M, проверяемом на полноту;
- n — увеличенное на единицу максимальное количество входов линейных автоматов в M;
- d — максимальная степень дробей из множества $U(M)$,

  $$U(M)=\bigcup\nolimits_{\mathfrak{A}\in M}U(\mathfrak{A}),$$

  при этом, как известно, степенью несократимой дроби $\frac{u}{v}$ называется $\max(\deg u,\deg v)$;
- l — количество максимальных собственных подполей поля $GF(p^m)$, равное числу неприводимых делителей числа m [69].

Далее, наряду с построением алгоритма проверки множества M на полноту по операциям композиции, мы будем оценивать сверху количество операций в поле $GF(p^m)$, используемых для реализации этого алгоритма.

Для некоторого числа C_1, $C_1\in\mathbb{N}$, количество операций для проверки принадлежности множества M классам из $J^A_{p^m}$ не превышает C_1rnp^m.

В случае $M\subseteq\Theta$ для некоторого $\Theta\in J^A_{p^m}$ множество M не является полным по операциям композиции. В противном случае выполняем проверку включений $M\subseteq M_{0,\omega}$, $\omega\in\mathrm{Aut}(GF(p^m))$, следующим образом.

Проверка на включение в $M_{0,\omega}$.

1. Если $\exists\mu,\mu\in U(M)$, $\mu=\frac{u}{v}$, $\deg u>\deg v$, то $\forall\omega\in\mathrm{Aut}(GF(p^m))$ выполнено: $M\not\subseteq M_{0,\omega}$. Конец проверки.
2. Если $\exists\omega\in\mathrm{Aut}(GF(p^m))$, что $\forall\mu\in U(M)$ выполнено $\Psi_0(\mu)=\big(\mu(0),\omega(\mu(0))\big)$, то $M\subseteq M_{0,\omega}$. Конец проверки.
3. $M\not\subseteq M_{0,\omega}$. Конец проверки.

Найдется C_2, $C_2\in\mathbb{N}$ такое, что количество операций для этой проверки оценивается сверху через C_2rnm.

Для автоморфизма ω, $\omega \in \mathrm{Aut}(GF(p^m))$, через u_ω обозначим наибольший общий делитель числителей множества несократимых дробей:

$$\left\{ \frac{u}{v} \;\middle|\; \exists \mu \in U(M),\ \frac{u}{v} = \mu - \omega(\mu(0)) \right\},$$

если он не делится на ξ, или результат его деления на ξ в противном случае. Из $M \not\subseteq M_1$ следует, что u_ω не делится на ξ. Для некоторого C_3, $C_3 \in \mathbb{N}$, многочлен u_ω может быть вычислен с использованием не более чем $C_3 rnd^2$ операций.

В случае необходимости далее выполняется следующая проверка.

Проверка на включение в классы $M_{i,\omega}$, $i = 2, 3, \ldots$, $\omega \in \mathrm{Aut}(GF(p^m))$.

1. Если $\exists \omega \in \mathrm{Aut}(GF(p^m))$ такой, что $\deg(u_\omega) > 0$, то $\exists i$, $i > 1$, что $M \subseteq M_{i,\omega}$. Конец проверки.
2. $\forall i$, $i \in \{2, 3, \ldots\}$, и $\forall \omega$, $\omega \in \mathrm{Aut}(GF(p^m))$ выполнено: $M \not\subseteq M_{i,\omega}$. Конец проверки.

Общее количество операций для проверки на включение в классы $M_{i,\omega}$ составляет не более $C_3 rnd^2 m$.

Найдется C_6, $C_6 \in \mathbb{N}$ такое, что на проверку включений $M \subseteq R_0^e$, $M \subseteq R_0^d$ потребуется не более $C_6 rn$ операций.

Содержанием многочлена u назовем многочлен $\widehat{u}$, равный произведению неприводимых приведенных многочленов, отличных от ξ и делящих многочлен u.

Лемма 14. *Найдется C_4, $C_4 \in \mathbb{N}$ такое, что содержание многочлена $u(\xi)$ степени не большей d может быть найдено не более чем за $C_4 d^2$ операций.*

Доказательство. Для некоторых многочленов v_0 и v_1 из $GF(p^m)$ таких, что v_0 не делится на p-ю степень никакого неприводимого многочлена, выполнено: $u = v_0 v_1^p$. Многочлен v_1^p найдем, вычисляя последовательность формальных производных: $u_\xi^{(i)}$, $i = 1, 2, \ldots$, до того, как получим 0. Тогда предыдущая производная совпадает с v_1^p.

Содержание многочлена v_0 равно наибольшему общему делителю многочленов u и $\frac{u'_\xi}{v_1^p}$. Далее находим многочлен v_1, заменяя ξ^p на ξ в многочлене v_1^p. Далее рекурсивно продолжаем процедуру определением содержания многочлена v_1. Количество операций при выполнении этой процедуры для некоторой константы C можно ограничить числом

$$Cd^2 \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots\right) \leqslant 2Cd^2.$$

В итоге мы найдем многочлены u_i, $i = \overline{0, s-1}$, произведение которых равно содержанию многочлена $u(\xi)$. Нетрудно видеть, что количество операций, выполняемых при перемножении этих многочленов не превосходит $C_5 d^2$ для некоторой константы C_5.

Введем метасимвол ρ, принимающий два значения: e и d. Существенный вход линейного автомата будем называть e-входом, а непосредственный вход — d-входом. Через u_ρ обозначим наибольший общий делитель следую-

щего множества многочленов:

$$\left\{u \;\middle|\; \text{в } M \text{ найдется автомат, некоторому входу которого, не являющемуся единственным } \rho\text{-входом, соответствует коэффициент } \mu,\ \mu=\frac{u}{v},\ \text{и } (\mathrm{u,v})=1\right\}.$$

Пусть $\widehat{u}_\rho$ — содержание многочлена u_ρ. Из соотношения $M \not\subseteq V_1$ следует, что свободный член многочлена $\widehat{u}_\rho$ не ноль. Через $\widetilde{u}_\rho$ обозначим наибольший общий делитель следующего множества дробей:

$$\left\{\frac{\widehat{u}_\rho}{(\widehat{u}_\rho, v)} \;\middle|\; \text{в } M \text{ найдется автомат, некоторому входу которого, являющемуся единственным } \rho\text{-входом, соответствует коэффициент } \mu,\ \mu=\frac{u}{v},\ \text{и } (\mathrm{u,v})=1\right\}.$$

Если M не содержится во всех классах множества J_{p^m}, для которых проверка уже была выполнена, то выполняются следующие проверки.

Проверка на включение в классы R_i^ρ, $i=2,3,\dots$.

1. Если $\exists \rho \in \{e,d\}$ такое, что $\deg\left(\widetilde{u}_\rho\right)>0$, то $\exists i, i>1$, что $M \subseteq R_i^\rho$. Конец проверки
2. $\forall \rho,\ \rho \in \{e,d\}$, и $\forall i,\ i \in \{2,3,\dots\}$, выполнено: $M \not\subseteq R_i^\rho$. Конец проверки.

Количество операций, требуемое для последних проверок с учетом вычисления многочлена $\widetilde{u}_\rho$ не превосходит $C_7 rnd^2$ для некоторого числа C_7, $C_7 \in \mathbb{N}$. Это устанавливается с использованием леммы 14. Подводя итог оценкам на количество операций для определения полноты M, получаем:

Т е о р е м а 22. *Найдется константа C, $C \in \mathbb{N}$ такая, что для проверки полноты по операциям композиции множества, состоящего из r линейных автоматов над полем $GF(p^m)$, заданных наборами из не более чем n передаточных функций степени не выше d и свободными ходами, потребуется не более $C\left(rnp^m + rnd^2m\right)$ операций.*

В терминах предполных классов решена задача о полноте для класса L_2 с операциями суперпозиции [109]. Помимо определенных ранее, нам понадобятся следующие подмножества L_2:

$$\widetilde{M}_0 = \left\{\mathfrak{A} \;\middle|\; \forall \frac{u}{v} \in U(\mathfrak{A}),\ \deg u \leqslant \deg v\right\},$$
$$\widetilde{M}_i = \left\{\mathfrak{A} \;\middle|\; \forall \frac{u}{v} \in U(\mathfrak{A}), v \not\vdots p_i\right\}, \quad \text{где } i \in \{2,3,\dots\}.$$

Через J_2^S обозначим следующее множество:

$$\left\{T_0, T_1, V_1, V_2, M_1, \widetilde{M}_i \mid i \in \{0,2,3,\dots\}\right\}.$$

Т е о р е м а 23. *J_2^S — множество предполных по операциям суперпозиции классов в L_2.*

Следствие 6. *Любое подмножество класса L_2, не являющееся полным по операциям суперпозиции расширяется до предполного по этим операциям класса.*

Как и в случае операций композиции, основная сложность доказательства теоремы о предполных классах связана с обоснованием критериальности рассматриваемого множества классов. В случае операций суперпозиции из автоматов множества M, не содержащегося ни в одном из классов множества J_2^S, сначала строится сумматор с тремя входами $x_1+x_2+x_3$, затем для любого s, $s\in\mathbb{N}$, автомат g_s, $g_s=x_0+\sum_{i=1}^{s}\left(\xi^i x_i+\xi^i x_i'\right)$. Далее, что определяет основное ограничение возможностей операций суперпозиции от операций композиции, строится нулевая константа, используя которую вместе с ранее построенными автоматами, получаем сумматор x_1+x_2 и задержку ξx.

Для любого $u(\xi)$, $u(\xi)\in GF(2)[\xi]$, из x_1+x_2, ξx операциями суперпозиции строится автомат $u(\xi)x$. Для заданного i, $i\in\{2,3,\dots\}$, используя автоматы x_1+x_2, ξx и h_i, $h_i\in M\setminus\widetilde{M}_i$, можно получить автомат $\frac{1}{p_i}x$.

Для любого μ, $\mu\in E'(\xi)$, найдется конечное множество индексов I, $I\subseteq\{2,3,\dots\}$, найдутся целые неотрицательные числа j_i, $i\in I$, и найдутся многочлены u_i, $i\in I$, такие, что выполнено равенство:

$$\mu=\sum_{i\in I}u_i\left(\frac{1}{p_i}\right)^{j_i}.$$

Поэтому $\forall\mu\in E'(\xi)$ выполнено: $\mu x\in K(M)$.

Через $\mathfrak{A}_1$ обозначим один из автоматов множества $M\setminus T_0$. Автомат $\mathfrak{A}_1(0,\dots,0)$ реализует некоторую константу γ, $\gamma(0)=1$, $\gamma=\frac{u_1}{v_1}$. Тогда $\frac{v_1}{u_1}(\gamma)=1\in K(M)$. Таким образом, из автоматов множества M получено множество M_S, которое, как отмечалось ранее, является полным по операциям суперпозиции.

Из теоремы 23 следует, что в L_2, как и в классе всех конечных автоматов, по операциям суперпозиции отсутствуют конечные полные множества.

Согласно теоремам 19, 21 и 23, в L_2 найдены множества J_2^A, J_2^K и J_2^S предполных классов, соответственно, по операциям A-замыкания, операциям композиции и операциям суперпозиции. Заметим, что все A-предполные классы входят как в J_2^K, так и в J_2^S. Каждый класс $J_2^S\setminus J_2^A$ содержит ровно три класса из $J_2^K\setminus J_2^A$:

$$M_i\subset\widehat{M}_i,\quad R_i^e\subset\widehat{M}_i,\quad R_i^d\subset\widehat{M}_i,\quad i\in\{0,2,3,\dots\}.$$

Линейным над кольцом двоично-рациональных чисел $\mathbb{Q}_{\frac{m}{2^n}}$ называется автомат, алфавиты которого являются декартовыми степенями $\mathbb{Q}_{\frac{m}{2^n}}$, а его функции переходов и выхода линейны над этим кольцом. В работах Д. В. Ронжина [97–99] исследовалась задача A-полноты в классе $L\left(\mathbb{Q}_{\frac{m}{2^n}}\right)$ линейных автоматов над кольцом $\mathbb{Q}_{\frac{m}{2^n}}$.

Как и в случае линейных автоматов над конечными полями, линейный автомат из $L\left(\mathbb{Q}_{\frac{m}{2^n}}\right)$ от n переменных задает отображение (7). Только для коэффициентов μ_i, $i=0,1,\dots,n$, выполнены:

$$\mu_i\in E'_{\frac{m}{2^n}}(\xi),\qquad E'_{\frac{m}{2^n}}(\xi)=\left\{\frac{u}{v}\mid u,v\in\mathbb{Q}_{\frac{m}{2^n}},v(0)=1\right\},$$

а переменные принимают значения из множества степенных рядов с коэффициентами из $\mathbb{Q}_{\frac{m}{2^n}}$.

Будем говорить, что несократимая дробь $a/2^i$ кратна натуральному числу s, если числитель этой дроби делится на s. Про несократимую дробь $\frac{u}{v}$ из $E'_{\frac{m}{2^n}}(\xi)$ будем говорить, что она делится на многочлен $\widetilde{u}$, если $u \vdots \widetilde{u}$.

Д. В. Ронжиным найдены следующие A-предполные классы в $L\left(\mathbb{Q}_{\frac{m}{2^n}}\right)$:

$$T_p = \left\{\mathfrak{A} \;\middle|\; \forall \mu \in U(\mathfrak{A}), \mu(0) \vdots p\right\}, M_p = \left\{\mathfrak{A} \;\middle|\; (7) \Rightarrow \mu_0(0) \vdots p\right\},$$

где p — простое, $p \neq 2$,

$$T_{int} = \left\{\mathfrak{A} \;\middle|\; \forall \mu \in U(\mathfrak{A}),\ \mu(0) \in \mathbb{Z}_+\right\}, \qquad T_{\geqslant 0} = \left\{\mathfrak{A} \;\middle|\; \forall \mu \in U(\mathfrak{A}),\ \mu(0) \geqslant 0\right\},$$
$$D = \left\{\mathfrak{A} \;\middle|\; (7) \Rightarrow \exists u \in \mathbb{Q}_{\frac{m}{2^n}}[\xi],\ \deg u > 0,\ \mu_i \vdots u,\ i = 1, \ldots, n\right\},$$

для заданного конечного непустого множества нечетных простых чисел P:

$$V_P = \left\{\mathfrak{A} \;\middle|\; (7) \Rightarrow \text{либо } \exists p \in P,\ \mu_i(0) \vdots p, i = 1, 2, \ldots, n,\right.$$
$$\left.\text{либо все } \mu_i(0), \text{ кроме одного, делятся на } \prod_{p \in P} p\right\}.$$

Через $V^{(1)}$ обозначим множество всех одноместных автоматов из $L\left(\mathbb{Q}_{\frac{m}{2^n}}\right)$.

Теорема 24 [99]. *Если для любого непустого конечного множества P нечетных простых чисел выполнено: $L\left(\mathbb{Q}_{\frac{m}{2^n}}\right) \setminus V_P \neq \varnothing$, то $A\left(V^{(1)} \cup M\right) = L\left(\mathbb{Q}_{\frac{m}{2^n}}\right)$.*

Через $f_+^{(1)}(x_1, x_2)$ обозначим автомат из $L\left(\mathbb{Q}_{\frac{m}{2^n}}\right)$, реализующий сумматор в начальный момент времени.

Теорема 25 [97]. *Пусть $M \subseteq L\left(\mathbb{Q}_{\frac{m}{2^n}}\right)$ и для любого Θ такого, что $\Theta \in \{T_p, M_p, T_{int}, T_{\geqslant 0} \mid p - \text{простое}, p > 2\}$, выполнено $M \not\subseteq \Theta$, тогда $A\left(M \cup \left\{f_+^{(1)}(x_1, x_2)\right\}\right) = L\left(\mathbb{Q}_{\frac{m}{2^n}}\right)$.*

Таким образом, количество A-предполных классов в $L\left(\mathbb{Q}_{\frac{m}{2^n}}\right)$ не менее чем счетно, что отличает этот класс от классов линейных автоматов над конечными полями.

Используя теорему 24, несложно получить алгоритм проверки A-полноты множеств, состоящих из одноместных функций и конечных добавок к ним. Теорема 25 позволяет получить алгоритм проверки A-полноты конечных подмножеств автоматов из $L\left(\mathbb{Q}_{\frac{m}{2^n}}\right)$, содержащих сумматор.

3.2. Выразимость в классе линейных автоматов над полем $GF(2)$. В работе [107] описаны K-замкнутые классы с сумматором $x_1 + x_2$, содержащиеся в L_2, получен алгоритм, проверяющий выразимость в L_2 через конечные множества с двуместным сумматором, и критерий вхождения этого сумматора в замкнутый класс. В результате получен алгоритм, который по паре (M', M) конечных подмножеств из $L_{GF}(2)$ устанавливает, справедливо ли включение $\{x_1 + x_2\} \cup M' \subseteq K(M)$.

Через $L_{2,0}$ обозначим множество всех автоматов из L_2 с нулевым свободным ходом: $L_{2,0} = \{\mathfrak{A} \mid \mathfrak{A} \in L_2, (7) \Rightarrow \mu_0 = 0\}$. Множество всех одноместных линейных автоматов из L_2 обозначим $L_2^{(1)}$, а пересечение множеств $L_{2,0}$

и $L_2^{(1)}$ обозначим $L_{2,0}^{(1)}$. Множество, состоящее из всех константных автоматов, обозначим $L_{2,C}$.

Для множества M, $M \subseteq L_2$, как и ранее, через $U(M)$ обозначаем множество всех передаточных функций автоматов из M. Через $C(M)$ будем обозначать множество всех свободных ходов автоматов из M.

Замыкание по операциям сложения и умножения множества дробей M, $M \subseteq E_2'(\xi)$, мы обозначаем $S^{(1)}(M)$, а замыкание этого множества по операциям «+», «·» и «fb», как и прежде, обозначаем $K^{(1)}(M)$.

Каждой паре M, C, где $M \subseteq L_{2,0}^{(1)}$, $C \subseteq L_{2,C}$, сопоставим множество констант $S(M,C)$:

$$S(M,C) = \{\ \mu_1\gamma_1 + \mu_2\gamma_2 + \ldots + \mu_m\gamma_m \ \mid \\ m \in \mathbb{N},\ \ \gamma_i \in C,\ \ \mu_i \in K^{(1)}(M),\ \ i = 1,2,\ldots,m\ \}.$$

Л е м м а 15. *Пусть* $M \subseteq L_2$.

1. *Тогда выполнены включения:*

$$U(K(M)) \subseteq K^{(1)}(U(M)), \qquad C(K(M)) \subseteq S(U(M), C(M)).$$

2. *В случае*

$$x_1 + x_2 \in K(M) \tag{12}$$

линейный автомат $\mathfrak{A}$, *удовлетворяющий соотношению (7), содержится в* $K(M)$ *в точности тогда, когда для каждого* i, $i = 1,2,\ldots,n$, $\mu_i \in K^{(1)}(U(M))$ *и* $\mu_0 \in S(U(M), C(M))$.

Согласно лемме 15, для решения задачи выразимости через множества линейных автоматов, содержащих сумматор, следует изучить $K^{(1)}$-выразимость в классе $E_2'(\xi)$.

Пусть $M \subseteq L_2$ и имеет место (12). Тогда

$$1 \in U(M) \tag{13}$$

и

$$U(M) \not\subseteq R_i^{(1)}, \quad \forall i,\ i = 0,1,\ldots. \tag{14}$$

В поле $GF(2)(\xi)$ по теореме Люрота [24] для любого его подполя F, т. е. замкнутого по операциям сложения, умножения и деления подмножества $GF(2)(\xi)$, $F \neq GF(2)$, найдется дробь μ, $\mu \notin GF(2)$, такая, что F порождается элементами множества $\{1, \mu\}$. Не ограничивая общности, можно считать, что $\mu(0) = 0$.

Отсюда следует, что для любого $K^{(1)}$-замкнутого подкласса M, $M \subseteq E_2'(\xi)$, $M \not\subseteq GF(2)$, содержащего 1, найдется μ, $\mu \in \xi E_2'(\xi) \setminus \{0\}$, что выполнено: $M \subseteq K^{(1)}\left(\{1, \mu\}\right)$. Кроме этого, найдется μ_1, $\mu_1 \in S^{(1)}\left(\{1, \mu\}\right)$, для которого выполнено: $\mu\mu_1 \in S^{(1)}(M)$.

Нетрудно видеть, что μ не содержится в тех классах множества $\left\{M_i^{(1)} \mid i = 0,1,2,\ldots\right\}$, в которых не содержится множество M.

$E_2'(\xi)$ содержит следующие $K^{(1)}$-замкнутые подклассы:

$$M^{(1)}(\mu, u_0) = \Big\{ a_0 + \mu u_0(\mu)\frac{u(\mu)}{v(\mu)} \;\Big|\; a_0 \in GF(2),\ u(\xi) \in GF(2)[\xi],\ v(\xi) \in 1 + \xi GF(2)[\xi],\ (u_0(\xi), v(\xi)) = 1 \Big\},$$

$$P^{(1)}(\mu, u_0) = \Big\{ a_0 + \mu u_0(\mu)\frac{u(\mu)}{v(\mu)} \;\Big|\; a_0 \in GF(2),\ u(\xi) \in GF(2)[\xi],\ v(\xi) \in 1 + \xi GF(2)[\xi],\ (u_0(\xi), v(\xi)) = 1,\ \deg u(\xi) \leqslant \deg v(\xi) - 2(1 + \deg u_0(\xi)) \Big\}, \tag{15}$$

$$R^{(1)}(\mu, u_0) = \Big\{ u_0(\mu)\frac{u(\mu)}{v(\mu)} \;\Big|\; u(\xi) \in GF(2)[\xi],\ v(\xi) \in 1 + \xi GF(2)[\xi], (u_0(\xi), v(\xi)) = 1 \Big\},$$

$\mu \in \xi E_2'(\xi)$, $u_0 \in GF(2)[\xi] \setminus \{0\}$.

Для дроби $\mu \in \xi E_2'(\xi) \setminus 0$ через $E_2'(\mu)$ обозначим множество

$$\left\{ \frac{u(\mu)}{v(\mu)} \mid u, v \in GF(2)[\xi], v(0) = 1 \right\}.$$

Определим отображение $\Psi_\mu : E_2'(\mu) \to E_2'(\xi)$, положив

$$\Psi_\mu \left(\frac{u(\mu)}{v(\mu)} \right) = \frac{u(\xi)}{v(\xi)}.$$

Если $M \subseteq E_2'(\mu)$, то $\Psi_\mu(M) = \{\Psi(\mu') \mid \mu' \in M\}$.

Справедливы равенства:

$$\Psi_\mu \left(M^{(1)}(\mu, u_0) \right) = M^{(1)}(\xi, u_0),$$
$$\Psi_\mu \left(P^{(1)}(\mu, u_0) \right) = P^{(1)}(\xi, u_0),$$
$$\Psi_\mu \left(R^{(1)}(\mu, u_0) \right) = R^{(1)}(\xi, u_0).$$

В дальнейшем для обозначения классов $M^{(1)}(\xi, u_0)$, $P^{(1)}(\xi, u_0)$ и $R^{(1)}(\xi, u_0)$ будем использовать более короткие соответствующие обозначения: $M^{(1)}(u_0)$, $P^{(1)}(u_0)$ и $R^{(1)}(u_0)$.

Л е м м а 16. *Если для множества M, $M \subseteq E_2'(\mu)$, выполнено (13), то*

$$1 \in \Psi_\mu(M).$$

Если для множества M, $M \subseteq E_2'(\mu)$, выполнено (14), то для любого i, $i = 0, 1, \ldots$

$$\Psi_\mu(M) \not\subseteq R_i^{(1)}.$$

С принадлежностью классам $M_i^{(1)}$, $i \in \{0, 1, \ldots\}$, при переходе от M, $M \subseteq E_2'(\mu)$, к $\Psi_\mu(M)$ ситуация может измениться, но может не поменяться. В качестве первого примера рассмотрим множество M_0, $M_0 = K^{(1)}\left(\{1, \mu\}\right)$, $\mu = \frac{\xi}{1+\xi^2}$. Имеет место включение $M_0 \subseteq M_0^{(1)}$, но $\Psi_\mu(M_0) \not\subseteq M_0^{(1)}$.

Второй пример доставляет множество $K^1(M_1)$, $M_1 = \left\{1, \frac{\xi}{1+\xi^3}, \frac{\xi^2}{1+\xi^3}\right\}$. Замыкание множества M_1 по операциям поля дает $GF_2(\xi)$, а $\Psi_\xi\left(K^1(M_1)\right) = K^1(M_1)$, поэтому $\Psi_\xi\left(K^1(M_1)\right) = K^1(M_1) \subseteq M_0^{(1)}$.

Таким образом, не ограничивая общности рассуждений, исследование $K^{(1)}$-замкнутых классов M, $M \subseteq E_2'(\xi)$, содержащих 1, можно продолжить, предположив существование μ_1, $\mu_1 \in E_2'(\xi) \setminus \{0\}$, такого, что

$$\{\mu_1, \xi\mu_1\} \subset K^{(1)}(M). \tag{16}$$

Теорема 26 [107]. *Пусть для множества M, $M \subseteq E_2'(\xi)$, выполнены (13) и (16), где $\mu_1 \neq 0$. Тогда найдутся u_0, $u_0 \in GF(2)[\xi]$, и T, $T \in \mathbb{N}$, такие, что имеет место один из следующих случаев:*

$$M^{(1)}(u_0^T) \subseteq K^{(1)}(M) \subseteq M^{(1)}(u_0), \tag{17}$$

$$P^{(1)}(u_0^T) \subseteq K^{(1)}(M) \subseteq M_0^{(1)} \cap M^{(1)}(u_0). \tag{18}$$

В качестве многочлена u_0, фигурирующего в формулировке теоремы 26, можно взять произведение неприводимых многочленов p_i из $\{p_i \mid i = 2, 3, \dots\}$ таких, что $M \subseteq M_i^{(1)}$.

Заметим, что количество классов, удовлетворяющих как включениям (17), так и включениям (18), конечно.

Следствие 7. *Количество $K^{(1)}$-замкнутых классов в $E_2'(\xi)$, содержащих 1, счетно.*

Из доказательства теоремы 26 вытекает

Следствие 8. *Для множества M, $M \subseteq E_2'(\xi)$, соотношение (13) выполнено в точности тогда, когда выполнено (14).*

Далее остановимся на проверке выразимости линейного автомата $\mathfrak{A}$ через конечное множество M, $M \subset L_2$. Как следует из леммы 15, для этого нужно указать алгоритм, который по μ', $\mu' \in E_2'(\xi)$, проверяет справедливость соотношения

$$\mu \in K^{(1)}(U(M)), \tag{19}$$

и указать алгоритм, который по γ, $\gamma \in E_2'(\xi)$, определяет справедливость включения

$$\gamma \in S\left(U(M), C(M)\right). \tag{20}$$

Нам понадобится следующее вспомогательное утверждение, распространяющее формулу для деления с остатком с многочленов на дроби.

Лемма 17. *Пусть $\widetilde{u} \in GF_2[\xi]$, $\mu = \dfrac{u}{v} \in E_2'(\xi)$ и $\left(\widetilde{u}, v\right) = 1$.*

1. *Тогда найдется многочлен u_μ, $u_\mu \in GF_2[\xi]$, $\deg\left(u_\mu\right) < \deg\left(\widetilde{u}\right)$, что для некоторого u', $u' \in GF_2[\xi]$, выполнено:*

$$\mu = u_\mu + \widetilde{u}\frac{u'}{v}. \tag{21}$$

2. *Если $\deg u \leqslant \deg v$, то найдутся многочлены $u_{\mu,i}$, $i = 1, 2$, что для некоторых многочленов u', v' из $GF_2[\xi]$, $\deg u' \leqslant \deg v' - 2\deg\left(\widetilde{u}\right)$, выполнено:*

$$\mu = \frac{u_{\mu,1} + \widetilde{u}u_{\mu,2}}{1 + \widetilde{u}^2} + \frac{\widetilde{u}u'}{v'}. \tag{22}$$

Заметим, что первое утверждение леммы 17 в случае неприводимого многочлена $\widetilde{u}$ использовалось ранее при построении отображений Ψ_i.

Если выполнено (21), то многочлен u_μ будем называть остатком от деления μ на $\widetilde{u}$. Если выполнено (22), то дробь $\frac{u_{\mu,1}+\widetilde{u}u_{\mu,2}}{1+\widetilde{u}^2}$ будем называть дробным остатком от деления μ на $\widetilde{u}$.

Пусть $U(M)\not\subseteq GF(2)$. Сначала найдем μ, что поле, порождаемое множеством $U(M)$ совпадает с $GF(2)(\mu)$. Без оптимизации это можно выполнить следующим образом. Перебираем все дроби, степень которых не превосходит минимальной степени дробей из $U(M)$. Для каждой такой дроби проверяем, выразимы ли через нее все дроби из $U(M)$. Среди всех дробей, через каждое из которых выразимы все дроби из M, выбираем ту, которая имеет максимальную степень. Это будет искомая дробь.

Приведенный алгоритм корректен, потому что дробь не может быть выражена через другую дробь, если степень выражающей дроби больше степени выражаемой дроби.

Через $\widetilde{M}$ обозначим $\Psi_\mu(U(M))$. Далее в случае

$$\widetilde{M}\not\subseteq M_0^{(1)} \tag{23}$$

в соответствии с доказательством теоремы 26 находим многочлен u_0 и его степень T такие, что выполнены включения

$$M^{(1)}(u_0^T)\subseteq K^{(1)}(\widetilde{M})\subseteq M^{(1)}(u_0), \tag{24}$$

а в случае

$$\widetilde{M}\subseteq M_0^{(1)} \tag{25}$$

находим u_0 и T, для которых имеют место

$$P^{(1)}(u_0^T)\subseteq K^{(1)}(\widetilde{M})\subseteq M_0^{(1)}\cap M^{(1)}(u_0). \tag{26}$$

Теперь в случае (23) найдем множество R остатков от деления дробей из $\widetilde{M}$ на u_0^T. Через $\widetilde{R}$ обозначим замыкание R по операциям сложения и умножения по модулю u_0^T. Включение (19) выполнено в точности тогда, когда в $\widetilde{R}$ найдется остаток u такой, что $u+\mu\in M^{(1)}(u_0^T)$.

Дробные остатки можно естественным образом складывать. Произведением двух дробных остатков μ_1 и μ_2, получаемых при делении на один и тот же многочлен $\widetilde{u}$, будем называть дробный остаток произведения $\mu_1\mu_2$ от деления на $\widetilde{u}$. В случае (25) через $\widetilde{R}$ обозначим замыкание по операциям сложения и умножения множества дробных остатков от деления дробей из $U(M)$ на u_0^T. Включение (19) выполнено в точности тогда, когда в $\widetilde{R}$ найдется дробный остаток μ' такой, что $\mu'+\mu\in P^{(1)}(u_0^T)$.

Доказательство корректности приведенного алгоритма проверки соотношения (19) основано на конечности множества остатков и дробных остатков для заданных u_0 и T.

Теперь остановимся на проверке соотношения (20). Обозначим множество $\{\gamma_i\,|\,i=1,2,\ldots,m\}$ через $C(M)$. Не ограничивая общности, предположим, что γ_i, $i=1,2,\ldots,r$, линейно независимы над полем $GF(2)(\mu)$, где, как и прежде, $GF(2)(\mu)$ — поле, порождаемое множеством $U(M)$, а γ_i, $i=r+1,\ldots,m$, представимы линейными комбинациями констант γ_i, $i=1,2,\ldots,r$ над полем $GF(2)(\mu)$.

Нетрудно видеть, что для некоторых T' и T'' из $\mathbb{N}$, не меньших T, в случае (23) выполнено:

$$M^{(1)}(u_0^{T''},\mu)\gamma_j\subseteq\sum_{i=1}^{r}M^{(1)}(u_0^{T'},\mu)\gamma_i,\quad j=r+1,\ldots,m,$$

а в случае (25) выполнено:

$$P^{(1)}(u_0^{T''}, \mu)\gamma_j \subseteq \sum_{i=1}^{r} P^{(1)}(u_0^{T'}, \mu)\gamma_i, \quad j = r+1, \ldots, m.$$

В случае (23) через $\widehat{R}_i$ обозначим множество

$$\{u(\mu) \mid u(\mu) \text{ — остаток от деления } \mu'(\mu),\ \mu'(\mu) \in U(M) \text{ на } u_0^{T'}\}$$

для $i \in \{1, 2, \ldots, r\}$ и множество

$$\{u(\mu) \mid u(\mu) \text{ — остаток от деления } \mu'(\mu),\ \mu'(\mu) \in U(M) \text{ на } u_0^{T''}\}$$

для $i \in \{r+1, r+2, \ldots, m\}$.

В случае (25) через $\widehat{R}_i$ обозначим множество

$$\{u(\mu) \mid u(\mu) \text{ — дробный остаток от деления } \mu'(\mu),\ \mu'(\mu) \in U(M) \text{ на } u_0^{T'}\}$$

для $i \in \{1, 2, \ldots, r\}$ и множество

$$\{u(\mu) \mid u(\mu) \text{ — дробный остаток от деления } \mu'(\mu),\ \mu'(\mu) \in U(M) \text{ на } u_0^{T''}\}$$

для $i \in \{r+1, r+2, \ldots, m\}$.

В каждом из двух рассматриваемых случаев включение (20) означает наличие таких u_i, $u_i \in \widehat{R}_i$, $i = 1, 2, \ldots, m$, что в случае (23) выполнено:

$$\gamma + \sum_{i=1}^{m} u_i\gamma_i \in \sum_{i=1}^{r} M^{(1)}(u_0^{T'}, \mu)\gamma_i, \tag{27}$$

а в случае (25) выполнено:

$$\gamma + \sum_{i=1}^{m} u_i\gamma_i \in \sum_{i=1}^{r} P^{(1)}(u_0^{T'}, \mu)\gamma_i. \tag{28}$$

Учитывая конечность вариантов левой части полученных выражений и однозначность представления констант линейными комбинациями элементов множества $\{\gamma_i \mid i = 1, 2, \ldots, r\}$ над полем $GF(2)(\mu)$, заключаем возможность установить включение (20), используя конечный перебор.

Т е о р е м а 27. *Задача выразимости в L_2 по операциям композиции через его конечные подмножества, содержащие сумматор в замыкании, алгоритмически разрешима.*

Следующая задача текущего раздела — установить условия для выразимости двуместного сумматора из конечного множества линейных автоматов.

В предыдущем разделе было представлено множество J_2 K-предполных классов в L_2:

$$J_2 = \{\ T_0, T_1, V_1, V_2, M_i, R_j^e, R_j^d \mid i = 0, 1, \ldots, j = 0, 2, 3, \ldots\ \}.$$

Если $M \subseteq L_2$ и выполнено

$$x_1 + x_2 \in K(M), \tag{29}$$

то множество M не содержится ни в одном классе множества J_2, в котором не содержится x_1+x_2, т. е. $M \not\subseteq \Theta$, $\forall \Theta \in J_2'$,

$$J_2' = \left\{ \; T_1, V_1, V_2, R_j^e, R_j^d \mid j = 0, 2, 3, \ldots \; \right\}.$$

Обратное утверждение неверно. Примером множества линейных автоматов, не содержащимся ни в одном из классов Θ, $\Theta \in J_2'$, такого, что двуместный суммматор не содержится в его K-замыкании, является M_0, $M_0 = \{x_1 + x_2 + x_3, \xi x_1 + \xi x_1 + \xi\}$.

Действительно, индукцией по построению несложно показать, что любой автомат из $K(M_0)$ в первые два момента времени сохраняет слово 01, но двуместный сумматор этим свойством не обладает.

Проще с сумматором $x_1+x_2+x_3$.

Л е м м а 18. *Для множества M, $M \subseteq L_2$, включение $x_1+x_2+x_3 \in K(M)$ выполнено в точности тогда, когда $M \not\subseteq \Theta$ для любого Θ:*

$$\Theta \in \left\{ \; V_1, V_2, R_j^e, R_j^d \mid j = 0, 2, 3, \ldots \; \right\}$$

Следующая теорема доставляет несколько критериев для включения (29), если M — конечное множество.

Т е о р е м а 28. *Пусть $M \subseteq L_2$, $|M| < \infty$ и $M \not\subseteq \Theta$ для любого Θ, $\Theta \in J_2'$,*

$$C(M) = \{\gamma_1, \gamma_2, \ldots, \gamma_s\}, \qquad C(M \setminus V_2) = \{\gamma_1, \gamma_2, \ldots, \gamma_k\}.$$

Условия 1–4 эквивалентны.

1. *Найдутся μ_1, μ_2, …, μ_s из $K^{(1)}(U(M))$, такие что $\sum_{i=1}^{s} \mu_i \gamma_i = 0$ и число $|\{ i \mid \mu_i \in 1 + \xi E_2'(\xi),\ i = 1, 2, \ldots, k \}|$ нечетно.*
2. $$\left(K(M) \cap L_{2,0}\right) \setminus V_2 \neq \varnothing.$$
3. $$0 \in K(M).$$
4. $$x_1 + x_2 \in K(M).$$

Таким образом, сумматор с двумя входами выразим из M в точности тогда, когда для некоторых u_i, $u_i \in \widehat{R}_i$, при $\gamma = 0$ и ограничениях на коэффициенты при константах, накладываемых условием 1 теоремы 28, имеет место (27) в случае (23), или (28) в случае (25). Возможность такой проверки снова следует из конечности множеств остатков $\widehat{R}_i$ и единственности представления вектора в линейном пространстве над полем через систему линейно независимых векторов.

Множество M, $M \subseteq L_2$, называем вырожденным, если $U(M) \subseteq GF(2)$. Класс L_2 содержит континуум вырожденных K-замкнутых подклассов, содержащих сумматор. Действительно, пусть $I \subseteq \{2, 3, \ldots\}$. Положим

$$M_I = K\left\{ x_1 + x_2, \frac{1}{p_i} \mid i \in I \right\}.$$

Нетрудно видеть, что при $I_1 \neq I_2$ выполнено: $M_{I_1} \neq M_{I_2}$. Отсюда следует континуальность числа вырожденных K-замкнутых классов, содержащих сумматор.

Заметим также, что в L_2 существуют замкнутые по операциям композиции классы, не являющиеся вырожденными, содержащие сумматор и не являющиеся конечно-порожденными. Примером такого класса является M_0,

$$M_0 = K\left(\left\{x_1 + x_2,\ \left(\xi + \xi^2\right) x,\ \frac{1}{(1+\xi)^s} \;\middle|\; s = 1, 2, \ldots\right\}\right).$$

Действительно, для любого конечного подмножества $\widetilde{M}$ множества M_0 найдется такое r, $r \in \mathbb{N}$, что для любого автомата из $K\left(\widetilde{M}\right)$ знаменатель его свободного хода $\frac{u}{v}$, $(u, v) = 1$, не делится на $(1+\xi)^r$, но $\frac{1}{(1+\xi)^r} \in M_0$.

3.3. A-выразимость в классе линейных автоматов над полем $GF(2)$. Результаты, изложенные в этой части, получены в [108].

Ранее в классах линейных автоматов L_{p^m} был определен оператор A-замыкания и найдены A-предполные классы, множество которых для L_{p^m} обозначено $J^A_{p^m}$. В этом разделе мы рассмотрим задачу A-выразимости в классе L_2.

Сначала остановимся на обозначениях, которые понадобятся в дальнейшем. Пусть $\mu \in \xi E'_2(\xi) \setminus \{0\}$. Множество степенных рядов $\sum_{t=0}^{\infty} a_t \mu^t$ с коэффициентами из поля $GF(2)$ обозначим через $R_2(\mu)$ в соответствии с ранее введенным обозначением $R_2(\xi)$.

Замыкание множества M, $M \subseteq E'_2(\xi)$, по операциям сложения и умножения обозначаем $S^{(1)}(M)$. Оператор A-замыкания на множестве линейных автоматов индуцирует на $E'_2(\xi)$ оператор $A^{(1)}$-замыкания. Через $A^{(1)}(M)$ обозначаем множество дробей из $E'_2(\xi)$, состоящее из дробей, получаемых из M с использованием сложения, умножения, а также таких μ, $\mu \in E'(\xi)$, $\mu = \sum_{t=0}^{\infty} a_t \xi^t$, что для каждого τ, $\tau \in \mathbb{N}$, в $S^{(1)}(M)$ найдется μ_τ, $\mu_\tau = \sum_{t=0}^{\infty} a_{\tau,t} \xi^t$, такая, что для любого $t \in \{0, 1, \ldots, \tau - 1\}$ выполнено: $a_{\tau,t} = a_t$.

Согласно определению операторов замыкания $S^{(1)}$, $K^{(1)}$, $A^{(1)}$, для любого M, $M \subseteq E'_2(\xi)$, выполнено:

$$S^{(1)}(M) \subseteq K^{(1)}(M) \subseteq A^{(1)}(M).$$

Расширение выразительных возможностей при переходе от оператора $K^{(1)}$ к $A^{(1)}$ проиллюстрируем на примере $M_0 = \{\xi + \xi^2\}$.

Двучлен $\xi + \xi^2$, как нетрудно видеть, содержится в $M^{(1)}_{i_0}$ для индекса i_0 такого, что $p_{i_0} = \xi + 1$. Поэтому $K^{(1)}(M_0) \subseteq M^{(1)}_{i_0}$, но $\xi \not\subseteq M^{(1)}_{i_0}$. Поэтому $\xi \not\subseteq K^{(1)}(M_0)$. С другой стороны, имеет место равенство:

$$\xi = \sum_{t=0}^{\infty} \left(\xi + \xi^2\right)^{2^t}.$$

Поэтому $\xi \in A^{(1)}(M_0)$ и, следовательно, $K^{(1)}(M) \subsetneq A^{(1)}(M)$.

Приведенный пример демонстрирует возможность получения элементов множества $E'_2(\xi)$ из рядов $R_2(\mu)$, $\mu \in \xi E'_2(\xi) \setminus \{0\}$, не являющихся периодическими по μ.

Лемма 19. *Пусть*

$$M \subseteq E'_2(\xi),\ \ M \setminus GF(2) \neq \varnothing, \qquad (30)$$
$$A^{(1)}(M) = M.$$

Тогда найдутся μ_0, $\mu_0 \in \xi E_2'(\xi) \setminus \{0\}$, k', $k' \in \mathbb{Z}_+$, *и множество многочленов* M', $M' \subset E_2[\mu_0]$, *степень каждого из которых по* μ_0 *не более* k', *что выполнено равенство:*

$$A^{(1)}(M) = M' + \mu_0^{k'} \left(R_2(\mu_0) \cap E_2'(\xi)\right). \tag{31}$$

В рассмотренном нами примере: $A^{(1)}(M_0) = \xi E_2'(\xi)$.

Далее изучается структура множества $R_2(\mu_0) \cap E_2'(\xi)$ для $\mu_0 \in \xi E_2'(\xi) \setminus \{0\}$.

Лемма 20. *Для каждого* μ_0, $\mu_0 \in \xi E_2'(\xi) \setminus \{0\}$, *найдется* μ, $\mu \in \xi E_2'(\xi) \setminus \{0\}$, *такое, что*

$$R_2(\mu_0) \cap E_2'(\xi) = E_2'(\mu). \tag{32}$$

Леммы 19 и 20 позволяют получить структуру $A^{(1)}$-замкнутого класса, показав его совпадение с некоторым $K^{(1)}$-замкнутым классом.

Теорема 29. *Для любого* M, *удовлетворяющего соотношениям* (30), *найдется* μ, $\mu \in \xi E_2'(\xi)$, $\mu \neq 0$, *найдется целое неотрицательное число* k' *и найдется множество многочленов* M', $M' \subset E_2[\mu]$, *степень каждого из которых по* μ *меньше* k', *такие, что выполнено равенство:*

$$A^{(1)}(M) = M' + \mu^{k'} E_2'(\mu). \tag{33}$$

Следствие 9. *Любой* $A^{(1)}$*-замкнутый класс конечно-порожден. Число* $A^{(1)}$*-замкнутых классов счетно.*

Каждый $A^{(1)}$-замкнутый класс является $K^{(1)}$-замкнутым. Сравнивая структуру $A^{(1)}$-замкнутого класса, представленную равенством (33), с $K^{(1)}$-замкнутыми классами, определяемыми включениями (17) и (18), еще раз подтверждаем, что не каждый $K^{(1)}$-замкнутый класс является $A^{(1)}$-замкнутым.

Теорема 30. *Пусть* $\mu_0 \in \xi E_2'(\xi) \setminus \{0\}$. *Для дроби* μ, $\mu \in \xi E_2'(\xi) \setminus \{0\}$, *соотношение (32) выполнено в точности тогда, когда* μ *— дробь минимальной степени такая, что выполнены следующие 2 свойства:*

1. $\mu_0 \in E_2'(\mu)$.
2. *Если представить* μ_0 *в виде* $\frac{u(\mu)}{v(\mu)}$, *где* $u(\xi)$ *и* $v(\xi)$ *— элементы* $GF(2)[\xi]$, *то* $u(\xi) \in \xi + \xi^2 GF(2)[\xi]$.

Далее рассматривается способ определения дроби μ для $A^{(1)}$-замкнутого класса M, удовлетворяющего соотношению (33) и заданного своим конечным порождающим множеством $\widetilde{M}$, а затем числа k' и множества M', фигурирующих в этом равенстве.

Пусть имеет место (30). По теореме Люрота [24] в поле $GF(2)(\xi)$ найдется μ_0, $\mu_0 \notin GF(2)$, такой, что поле, порожденное множеством $\widetilde{M}$, совпадает с $GF(2)(\mu_0)$. Ввиду равенств

$$GF(2)(\mu_0) = GF(2)\left(\frac{1}{\mu_0}\right) = GF(2)\left(\mu_0 + 1\right),$$

не ограничивая общности рассуждений, предположим, что $\mu_0 \in E_2'(\xi)$. Конечность процедуры поиска дроби μ_0 следует из приведенных далее утверждений.

1. μ_0 — дробь наибольшей степени такая, что для любой μ', $\mu' \in \widetilde{M}$, найдется $\widetilde{\mu}$, $\widetilde{\mu} \in GF(2)(\xi)$, что выполнено $\mu' = \widetilde{\mu}(\mu_0)$.
2. Если $\mu' = \widetilde{\mu}(\mu_0)$ для некоторой $\widetilde{\mu}$, $\widetilde{\mu} \in GF(2)(\xi)$, то $\deg \widetilde{\mu} \cdot \deg \mu_0 = \deg \mu'$.
3. Количество дробей из $GF(2)(\xi)$ фиксированной степени конечно.

Определив дробь μ, удовлетворяющую равенству (33), мы находим такую дробь $\widehat{\mu}$, $\widehat{\mu} \in S^{(1)}(M)$, что $\mu\widehat{\mu} \in S^{(1)}(M)$. Поэтому несложно определить число k' такое, что для любого t, $t \geqslant k'$, найдется $\widetilde{\mu}_t$, $\widetilde{\mu}_t \in E_2'(\mu)$, что выполнено $\mu^t \widetilde{\mu}_t \in S^{(1)}(M)$. Отсюда получаем включение $\mu^{k'} E_2'(\mu) \subseteq M$ и находим конечное множество M' для разложения (33).

Т е о р е м а 31. *Существует алгоритм, проверяющий по данным μ' и M, $\mu' \in E_2'(\xi)$, $M \subset E_2'(\xi)$, $|M| < \infty$, справедливость включения:*

$$\mu' \in A^{(1)}(M). \tag{34}$$

Приведем пример проверки включения (34) для $\mu' = \dfrac{\xi^2 + \xi^3}{1 + \xi^2 + \xi^3}$ и

$$M = \{\mu_1, \mu_2\},$$

где

$$\mu_1 = \xi^2 + \xi^3 + \xi^8 + \xi^{12}$$

и

$$\mu_2 = \xi^4 + \xi^7 + \xi^8 + \xi^9 + \xi^{10} + \xi^{11} + \xi^{12} + \xi^{15} + \xi^{16} + \xi^{18}.$$

Для этого обозначим $\xi^2 + \xi^3 + \xi^4 + \xi^6$ через μ_0. Имеют место равенства

$$\mu_1 = \mu_0 + \mu_0^2, \qquad \mu_2 = \mu_0^2 + \mu_0^3.$$

Выполнено равенство

$$A^{(1)}(M) = A^{(1)}(\mu_0).$$

Положим: $\mu = \xi^2 + \xi^3$. Тогда $\mu_0 = \mu + \mu^2$ и соотношение (33) выполнено для $k' = 1$ и $M = \{0\}$.

Таким образом, вопрос о вхождении μ' в $A^{(1)}(M)$ для рассматриваемого примера сводится к проверке включения $\mu' \in \mu E_2'(\mu)$, которое справедливо ввиду $\mu' = \dfrac{\mu}{1 + \mu}$.

Далее будем рассматривать задачу об A-выразимости через подмножества L_2, не содержащиеся в V_1, т. е. содержащие линейный автомат с не менее чем двумя непосредственными входами, A-замыкание которых содержит множество $L_{2,C}$ всех констант. Такие подмножества L_2 названы S-системами.

Л е м м а 21. *Для множества M, $M \subseteq L_2$, соотношение*

$$M \setminus V_1 \neq \varnothing \tag{35}$$

выполнено тогда и только тогда, когда $x_1 + x_2 + x_3 \in A(M)$.

В соответствии с ранее введенным определением, S-система M, для которой выполнено $U(M) \subseteq E_2$, называется вырожденной. Как нетрудно видеть, замыкание любой вырожденной S-системы есть множество

$$\{\ x_1 + x_2 + \ldots + \gamma \ \mid \ n \in \mathbb{Z}_+, \gamma \in L_{2,C}\ \}.$$

Поэтому в дальнейшем будем предполагать, что

$$U(M) \setminus E_2 \neq \varnothing.$$

Из леммы 21 следует, что в случае (35) выполнено:

$$U(A(M)) = A^{(1)}(U(M)).$$

Т е о р е м а 32. *Пусть M является S-системой. Включение $f \in A(M)$ выполнено в точности тогда, когда $U(f) \subseteq A^{(1)}(U(M))$.*

Отсюда с учетом теоремы 31 получаем:

С л е д с т в и е 10. *Задача A-выразимости через конечные S-системы алгоритмически разрешима.*

Далее рассматривается вопрос об A-выразимости множества всех констант через заданное множество линейных автоматов.

Пусть $r \in \mathbb{N}$. Линейный автомат $\mathfrak{A}$ обладает r-свойством, если для любой передаточной функции μ, $\mu \in U(M)$, выполнено $\mu + \mu(0) \in \xi^r E_2'(\xi)$. Через S_r обозначим множество всех линейных автоматов, обладающих r-свойством.

Для множества линейных автоматов M такого, что выполнено $U(M) \not\subseteq E_2$, найдется r_0, $r_0 \in \mathbb{N}$, такое, что $M \subseteq S_{r_0}$, но $M \not\subseteq S_{r_0+1}$. Такое r_0 называется 1-глубиной множества M.

Пусть $\mu_0 \in L_{2,C}$. Для заданного r, $r \in \mathbb{N}$, представим μ_0 в виде:

$$\mu_0 = a_0 + a_1\xi + a_2\xi^2 + \ldots + a_{r-1}\xi^{r-1} + \xi^r \mu_0'.$$

Для линейного автомата $\mathfrak{A}$ со свободным ходом μ_0 положим:

$$V^{(r)}(\mathfrak{A}) = (b, a_0, a_1, \ldots, a_{r-1}),$$

где

$$b = \begin{cases} 1, & \text{если число непосредственных входов} \\ & \text{линейного автомата } \mathfrak{A} \text{ четно;} \\ 0, & \text{в противном случае.} \end{cases}$$

Для множества V векторов из $GF(2)^{r+1}$ через $V(M)$ обозначим замыкание этого множества по операции покомпонентного сложения.

Т е о р е м а 33. *Пусть $M \subseteq L_2$, $M \not\subseteq V_1$ и $U(M) \not\subseteq E_2$. Множество $A(M)$ содержит все константы (т. е. $L_{2,C} \subseteq A(M)$) в точности тогда, когда $S(V^{(r_0)}(M)) = E_2^{r_0+1}$, где через r_0 обозначена 1-глубина множества M.*

Ниже приведен пример конечной S-системы. Пусть

$$M = \{ x_1 + \xi^6 x_2 + (1+\xi^3)x_3 + 1 + \xi^2,\ \xi^4 x_1 + \xi + \xi^2,\ x_1 + 1 + \xi + \xi^2,\ 1 + \xi + \xi^2 \}.$$

Множество M имеет 1-глубину равную 3 и содержит существенный линейный автомат $x_1 + \xi^6 x_2 + (1+\xi^3)\, x_3 + 1 + \xi^2$.

Имеют место равенства:

$$V^{(3)}\left(x_1 + \xi^6 x_2 + \left(1+\xi^3\right) x^3 + 1 + \xi^2\right) = (1,1,0,1),$$
$$V^{(3)}\left(\xi^4 x_1 + \xi + \xi^2\right) = (1,0,1,1),$$
$$V^{(3)}\left(x_1 + 1 + \xi + \xi^2\right) = (0,1,1,1),$$
$$V^{(3)}\left(1 + \xi + \xi^2\right) = (1,1,1,1).$$

Нетрудно видеть, что множество векторов $\{(1,1,0,1),(1,0,1,1),(0,1,1,1),(1,1,1,1)\}$ порождает линейное пространство $GF(2^4)$ по операции сложения. Следовательно, по теореме 33, $L_{2,C} \subseteq A(M)$ и M является S-системой.

Из теоремы 33 вытекает следующий результат.

Т е о р е м а 34. *Задача проверки, является ли конечное множество линейных автоматов S-системой, алгоритмически разрешима.*

Алгоритмы, приведенные в доказательствах теоремы 34 и следствия 10, позволяют решать задачу A-выразимости через конечные множества линейных автоматов, не являющиеся вырожденными, в два этапа. Сначала проверяем, является ли множество автоматов S-системой. В случае положительного ответа проверяем выразимость через нее заданного автомата. В случае отрицательного ответа вопрос о выразимости остается открытым.

Т е о р е м а 35.

1. *Если*
$$M \subseteq L_2, \;\; x_1 + x_2 \in A(M), \;\; U(M) \setminus E_2 \neq \varnothing, \tag{36}$$
то $A(M)$ является A-конечно-порожденным.
2. *Множество, состоящее из всех A-замкнутых классов M, удовлетворяющих свойствам* (36), *счетно.*

В предыдущей части был приведен пример K-замкнутого класса M_0, содержащего сумматор $x_1 + x_2$, обладающего свойством $U(M) \not\subseteq GF(2)$, но не являющегося K-конечно-порожденным. Таким образом, найдено еще одно существенное отличие операторов A-замыкания и K-замыкания.

Заметим также, что вырожденные системы линейных автоматов, содержащие сумматор в A-замыкании, не всегда конечно-порождены. Так, A-замыкание никакого конечного подмножества множества M,
$$M = A\Big(\{x_1 + x_2, \xi^i \mid i = 0, 1, \dots\} \Big),$$
не совпадает с M.

3.4. Класс линейных 2-адических автоматов. Понятие p-адического числа было введено в работе [121]. Автоматные преобразователи целых p-адических чисел изучались в работе [72].

В этой части статьи будут использованы результаты работы [111].

Если бесконечной последовательности α, $\alpha = a(0), a(1), \dots, a(t) \in \{0,1\}$, сопоставить последовательность $\bar{\alpha}$ частичных сумм ряда $\sum_{t=0}^{\infty} \alpha(t) 2^t$, являющуюся целым 2-адическим числом [18], то конечный автомат с n входами и одним выходом осуществляет преобразование набора целых 2-адических чисел $\left(\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n\right)$ в целое 2-адическое число $\bar{\beta}$.

Множество всех целых 2-адических чисел будем обозначать $\mathbb{Z}_{(2)}$. Это множество является кольцом с операциями сложения и умножения, которое содержит подкольцо $\mathbb{Q} \cap \mathbb{Z}_{(2)}$,
$$\mathbb{Q} \cap \mathbb{Z}_{(2)} = \left\{ \frac{u}{v} \;\middle|\; u \in \mathbb{Z}, \; v \in \mathbb{N}, \; v \not\vdots 2 \right\}.$$
Конечный автомат $\mathfrak{A}$, $\mathfrak{A} : \mathbb{Z}_{(2)}^n \to \mathbb{Z}_{(2)}$ называется линейным 2-адическим [6], если найдутся r_i, $r_i \in \mathbb{Q} \cap \mathbb{Z}_{(2)}$, $i = 0, 1, \dots, n$, такие, что
$$\mathfrak{A}(x_1, x_2, \dots, x_n) = \sum_{i=1}^{n} r_i x_i + r_0. \tag{37}$$

Множество 2-адических линейных автоматов обозначим $L_{(2)}$. Будем рассматривать это множество автоматов вместе с операциями композиции. При этом базисом является, например, множество $B=\{x_1+x_2, 1\}$, состоящее из 2-адического сумматора и константы 1. Заметим, что задержка $\xi(x)$ с нулевым начальным состоянием получается после отождествления входов 2-адического сумматора x_1+x_2, и выполнено: $\xi(x)=2x$.

Отметим, что $L_2 \neq L_{(2)}$, ввиду $x_1+x_2 \notin L_2$ и $x_1 \oplus x_2 \notin L_{(2)}$, где операция суммирования по модулю 2 обозначена $\oplus$, чтобы отличить ее от операции 2-адического суммирования.

Пусть выполнено (37). Положим $U(\mathfrak{A})=\{\, r_i \mid i=1,2,\ldots,n \,\}$. Для множества M, $M \subseteq L_{(2)}$, положим $U(M)=\cup_{\mathfrak{A}\in M} U(\mathfrak{A})$.

Переменная x_i автомата $\mathfrak{A}(x_1, x_2, \ldots, x_n)$, удовлетворяющего равенству (37), называется существенной, если $r_i \neq 0$. Переменная x_i называется непосредственной, если число r_i, будучи представленным в несократимом виде, имеет нечетный числитель. Операция обратной связи применима к переменной x_i автомата $\mathfrak{A}(x_1, x_2, \ldots, x_n)$ в точности тогда, когда x_i не является непосредственной переменной.

Далее, рассматривая дроби u/v из $\mathbb{Q}$, считаем, что $(u, v)=1$. Положим:

$$H^1 = \{\; 1+2r \mid r \in \mathbb{Z}_{(2)} \;\}.$$

Рассмотрим следующие подмножества в L_2:

$$\widetilde{L}_e^1 = \{\; \mathfrak{A} \mid \mathfrak{A} \text{ имеет ровно одну существенную переменную} \;\};$$

$$\widetilde{L}_d^1 = \{\; \mathfrak{A} \mid \mathfrak{A} \text{ имеет ровно одну непосредственную переменную} \;\};$$

$$\widetilde{T}_a = \{\; \mathfrak{A} \mid \text{для любых } \bar{\alpha}_i, \bar{\alpha}_i \in a+2\mathbb{Z}_{(2)}, i=1,2,\ldots,n, \text{ выполнено: } \mathfrak{A}(\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n) \in a+2\mathbb{Z}_{(2)} \;\},\ a \in E_2;$$

$$\widetilde{V}_1 = \{\; \mathfrak{A} \mid \mathfrak{A} \text{ имеет не более одной непосредственной переменной} \;\};$$

$$\widetilde{V}_2 = \{\; \mathfrak{A} \mid \mathfrak{A} \text{ имеет нечетное число непосредственных переменных} \;\};$$

$$\widetilde{I} = \left\{\; \mathfrak{A} \;\middle|\; \text{если выполнено равенство (37), то } \sum_{i=1}^n |r_i| \leqslant 1 \;\right\}.$$

Пусть $p_1, p_2, \ldots$ $(p_1<p_2<\ldots)$ — последовательность всех простых чисел.

Тогда $p_1=2$. Положим для $i=2,3,\ldots$:

$$\widetilde{R}_i^e = \left\{\; \mathfrak{A} \;\middle|\; \mathfrak{A} \in L_{(2)} \setminus \widetilde{L}_e^1, \text{ для любого } \frac{u}{v} \text{ из } U(\mathfrak{A}) \text{ выполнено } (u, p_i)=p_i \;\right\} \cup$$
$$\cup \left\{\; \mathfrak{A} \;\middle|\; \mathfrak{A} \in \widetilde{L}_e^1, \text{ для } \frac{u}{v} \text{ из } U(\mathfrak{A}) \setminus \{0\} \text{ выполнено } (v, p_i)=1 \;\right\};$$

$$\widetilde{R}_i^d = \left\{\; \mathfrak{A} \;\middle|\; \mathfrak{A} \in L_{(2)} \setminus \widetilde{L}_d^1, \text{ для любого } \frac{u}{v} \text{ из } U(\mathfrak{A}) \text{ выполнено } (u, p_i)=p_i \;\right\} \cup$$
$$\cup \left\{\; \mathfrak{A} \;\middle|\; \mathfrak{A} \in \widetilde{L}_d^1, \text{ для любого } \frac{u}{v} \text{ из } U(\mathfrak{A}) \setminus H^1 \text{ выполнено } (u, p_i)=p_i, \text{ а для } \frac{u}{v} \text{ из } U(\mathfrak{A}) \cap H^1 \text{ имеет место } (v, p_i)=1 \;\right\}.$$

Через $\mathfrak{J}_2$ обозначим множество

$$\left\{\; \widetilde{T}_0, \widetilde{T}_1, \widetilde{V}_1, \widetilde{V}_2, \widetilde{I}, \widetilde{R}_i^e, R_i^d \;\middle|\; i=2,3,\ldots \;\right\}.$$

Лемма 22. *Для любого* Θ, $\Theta \in \mathfrak{J}_2$, *выполнено:*

$$K(\Theta) = \Theta. \tag{38}$$

Для любых различных Θ_1 *и* Θ_2 *из* $\mathfrak{J}_2$ *выполнено:*

$$\Theta_1 \not\subseteq \Theta_2. \tag{39}$$

Теорема 36. *Множество* $\mathfrak{J}_2$ *является приведенной критериальной системой в* $L_{(2)}$, *состоящей из предполных классов.*

Как и в случае линейных автоматов, через $C(\mathfrak{A})$ будем обозначать свободный ход r_0 автомата $\mathfrak{A}$, задаваемого равенством (37), а для множества M, $M \subseteq L_{(2)}$, $C(M) = \cup_{\mathfrak{A} \in M}\{C(\mathfrak{A})\}$.

Заметим, что 2-адический сумматор с двумя входами содержится лишь в одном предполном классе из $\mathfrak{J}_2$, в классе $\widetilde{T}_0$. Это существенно облегчает решение задачи выразимости через конечные подмножества 2-адических автоматов, содержащих 2-адический сумматор по сравнению с аналогичной задачей для класса линейных автоматов над полем $GF(2)$.

Действительно, пусть $M \subseteq L_{(2)}$, $x_1 + x_2 \in M$ и $\mathfrak{A} \in L_{(2)}$. Нетрудно видеть, что включение $\mathfrak{A} \in K(M)$ выполнено в точности тогда, когда в $C(M)$ найдется такое r, что $\dfrac{C(\mathfrak{A})}{r}$ является целым 2-адическим числом.

Более «слабым» вариантом сумматора для класса $L_{(2)}$ является автомат $x_1 + x_2 - x_3$, который содержится в трех предполных классах: $\widetilde{T}_0$, $\widetilde{T}_1$ и $\widetilde{V}_2$, и отождествляя все входы которого получаем проводник. Аналогом этого сумматора в классе L_2 является сумматор с тремя входами, из которого тоже получаем проводник после отождествления входов.

Относительно задачи проверки полноты получен следующий результат:

Теорема 37. *Задача проверки полноты конечных систем из* $L_{(2)}$ *алгоритмически разрешима.*

Здесь, как и в случае линейных автоматов, при проверке на полноту конечных множеств 2-адических автоматов с целью оптимизации можно использовать алгоритм Эвклида нахождения наибольшего общего делителя для заданного множества целых чисел, не прибегая к разложению чисел на простые множители.

СПИСОК ЛИТЕРАТУРЫ

1. Автоматы / Под ред. К. Э. Шеннона, Дж. Маккарти. — М.: Издательство иностранной литературы, 1956.
2. Алешин С. В. Конечные автоматы и проблема Бернсайда о периодических группах // Математические заметки. — 1972. — Т. 11, № 3. — С. 319–328.
3. Алешин С. В. Автоматное представление свободной группы // Дискретная математика. — 2011. — Т. 23, № 3. — С. 32–56.
4. Алешин С. В. Алгебраические системы автоматов. — М.: МАКС Пресс, 2016.
5. Алешин С. В. О континуальных структурах классов конечных автоматов // Интеллектуальные системы. Теория и приложения. — 2022. — Т. 26, № 3. — С. 75–87.
6. Алешин С. В., Пантелеев П. А. Конечные автоматы и числа // Дискретная математика. — 2015. — Т. 27, № 4. — С. 3–20.
7. Андреев А. Е., Часовских А. А. Сложность автоматов, вычисляющих значения формул // Вестник МГУ. Серия 1. Математика. Механика. — 1996. — № 4. — С. 22–24.

8. Арбиб М. Алгебраическая теория автоматов языков и полугрупп. — М.: Статистика, 1975.
9. Бабин Д. Н. О суперпозициях о.д.-функций ограниченного веса // Логико-алгебраические конструкции. — Калинин: КГУ, 1984. — С. 21–27.
10. Бабин Д. Н. Вербальные подавтоматы и задача полноты // Вестник МГУ. Серия 1. Математика. Механика. — 1985. — № 3. — С. 82–85.
11. Бабин Д. Н. О полноте двухместных о.д.-функций относительно суперпозиции // Дискретная математика. — 1989. — Т. 1, № 4. — С. 86–91.
12. Бабин Д. Н. Разрешимый случай задачи о полноте автоматных функций // Дискретная математика. — 1992. — Т. 4, № 4. — С. 41–55.
13. Бабин Д. Н. Конечность множества автоматных базисов Поста с разрешимой проблемой полноты // Дискретная математика. — 1998. — Т. 10, № 3. — С. 57–63.
14. Бабин Д. Н. О классификации автоматных базисов Поста по разрешимости свойств полноты и А-полноты // Доклады РАН. — 1999. — Т. 367, № 4. — С. 439–441.
15. Бабин Д. Н. О классификации базисов в P_k по разрешимости проблемы полноты для автоматов // Фундаментальная и прикладная математика. — 2010. — Т. 15, № 3. — С. 33–47.
16. Бабин Д. Н. Класс автоматов с суперпозициями, нерасширяющийся до предполного // Интеллектуальные системы. Теория и приложения. — 2016. — Т. 20, № 4. — С. 155–166.
17. Бабин Д. Н., Кудрявцев В. Б. О классах автоматов, вложимых в предполные // Вестник МГУ. Серия 1. Математика. Механика. — 2020. — № 2. — С. 55–58.
18. Боревич З. И., Шафаревич И. Р. Теория чисел. — 3-е изд. — М: Наука, 1985.
19. Буевич В. А. Об алгоритмической неразрешимости распознавания А-полноты для ограниченно-детерминированных функций // Математические заметки. — 1972. — Т. 11, № 6. — С. 687–697.
20. Буевич В. А. О τ-полноте в классе автоматных отображений // Доклады АН СССР. — 1980. — Т. 252, № 5. — С. 1037–1041.
21. Буевич В. А. Условия А-полноты для конечных автоматов. Ч. 1. — М.: Изд-во Московского университета, 1986.
22. Буевич В. А. Условия А-полноты для конечных автоматов. Ч. 2. — М.: Изд-во Московского университета, 1987.
23. Вайнцвайг М. Н. О мощности схем из функциональных элементов // Доклады АН СССР. — 1961. — Т. 139, № 2. — С. 320–323.
24. Ван Дер Варден Б. Л. Алгебра. — М: Наука, 1976.
25. Васильев Д. И. Поиск ближайшего соседа на прямой с помощью клеточного автомата с локаторами // Интеллектуальные системы. Теория и приложения. — 2020. — Т. 24, № 3. — С. 99–119.
26. Васильев Д. И., Гасанов Э. Э. Нижняя оценка сложности задачи поиска ближайшего соседа на прямой с помощью клеточного автомата с локаторами // Вестник МГУ. Серия 1. Математика. Механика. — 2023. — № 5. — С. 33–39.
27. Вереникин А. Г., Гасанов Э. Э. Об автоматной детерминизации множеств сверхслов // Дискретная математика. — 2006. — Т. 18, № 2. — С. 84–97.
28. Виноградов И. В. К вопросу о порядках элементов группы автоматных подстановок // Интеллектуальные системы. — 2013. — Т. 17, № 1–4. — С. 154–162.
29. Волков Н. Ю. Об автоматной модели преследования в базовых плоских областях // Интеллектуальные системы. — 2007. — Т. 11, № 1–4. — С. 361–402.
30. Воротников А. С. Верхние оценки переключательной мощности плоских схем, реализующих автономные автоматные функции // Интеллектуальные системы. Теория и приложения. — 2021. — Т. 25, № 4. — С. 96–99.
31. Гасанов Э. Э. Прогнозирование периодических сверхсобытий автоматами // Интеллектуальные системы. Теория и приложения. — 2015. — Т. 19, № 1. — С. 23–34.
32. Гасанов Э. Э. Клеточные автоматы с локаторами // Интеллектуальные системы. Теория и приложения. — 2020. — Т. 24, № 2. — С. 119–132.
33. Гасанов Э. Э., Мастихина А. А. Прогнозирование общерегулярных сверхсобытий // Интеллектуальные системы. Теория и приложения. — 2015. — Т. 19, № 3. — С. 127–154.
34. Гасанов Э. Э., Пропажин А. А. Реализация баз данных типа «ключ-значение» клеточными автоматами с локаторами // Интеллектуальные системы. Теория и приложения. — 2021. — Т. 25, № 4. — С. 108–112.
35. Гилл А. Линейные последовательностные машины. — М.: Наука, 1974.

36. Жук Д. Н. О классификации автоматных базисов Поста по разрешимости свойств A-полноты для дефинитных автоматов // Дискретная математика. — 2010. — Т. 22, № 2. — С. 80–95.
37. Захарова Е. Ю. Критерий полноты систем функций из P_k // Проблемы кибернетики. Вып. 18. — М.: Наука, 1967. — С. 5–10.
38. Ибрагимова Д. Э. Сложение векторов на прямой с помощью клеточного автомата с локаторами // Интеллектуальные системы. Теория и приложения. — 2022. — Т. 26, № 4. — С. 134–162.
39. Каланчев Г. В. Порядок мощности плоских схем, реализующих булевы функции // Дискретная математика. — 2014. — Т. 26, № 1. — С. 49–74.
40. Каланчев Г. В. Об одновременной минимизации площади, мощности и глубины плоских схем, реализующих частичные булевы операторы // Интеллектуальные системы. Теория и приложения. — 2016. — Т. 20, № 2. — С. 203–268.
41. Каланчев Г. В. Замечания к определению клеточного автомата с локаторами // Интеллектуальные системы. Теория и приложения. — 2020. — Т. 24, № 4. — С. 47–56.
42. Кибкало М. А. Об автоматной сложности некоторых классов булевых функций // Интеллектуальные системы. — 2010. — Т. 14, № 1–4. — С. 319–322.
43. Килибарда Г. Новое доказательство теоремы Будаха — Подколзина // Дискретная математика. — 1991. — Т. 3, № 3. — С. 135–146.
44. Коляда К. В. О полноте регулярных отображений // Проблемы кибернетики. Вып. 41. — М.: Наука, 1984. — С. 41–47.
45. Кострикин А. И. Вокруг Бернсайда. — М.: Наука, 1986.
46. Кравцов С. С. О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов // Проблемы кибернетики. Вып. 19. — М.: Наука, 1967. — С. 285–292.
47. Кратко М. И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов // Доклады АН СССР. — 1964. — Т. 155, № 1. — С. 35–37.
48. Кудрин А. А. Сложность автоматов, вычисляющих значения формул над базисом, состоящим из одной булевской функции (записанной в операторном виде) // Интеллектуальные системы. — 1999. — Т. 4, № 1/2. — С. 285–298.
49. Кудрявцев В. Б. Теорема полноты для одного класса автоматов без обратных связей // Проблемы кибернетики. Вып. 8. — М.: Физматгиз, 1962. — С. 91–115.
50. Кудрявцев В. Б. О мощностях множеств предполных классов некоторых функциональных систем, связанных с автоматами // Доклады АН СССР. — 1963. — Т. 151, № 3. — С. 493–496.
51. Кудрявцев В. Б. Функциональные системы. — М.: Изд-во Московского университета, 1982.
52. Кудрявцев В. Б. О функциональных системах автоматов // Дискретная математика. — 1995. — Т. 7, № 4. — С. 3–28.
53. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Элементы теории автоматов. — М.: Изд-во Московского унивеситета, 1978.
54. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.
55. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — 2-е изд. — М.: Изд-во Московского университета, 2019.
56. Кудрявцев В. Б., Гаврилов Г. П., Яблонский С. В. Функции алгебры логики и классы Поста. — М.: Наука, 1966.
57. Кудрявцев В. Б., Подколзин А. С., Ушчумлич Ш. Введение в теорию абстрактных автоматов. — М.: Изд-во Московского университета, 1985.
58. Кудрявцев В. Б., Подколзин А. С., Болотов А. А. Основы теории однородных структур. — М.: Наука, 1992.
59. Кузнецов А. В. О проблемах тождества и функциональной полноты для алгебраических систем // Труды третьего всесоюзного математического съезда. Т. 2. — М.: Изд-во АН СССР, 1956. — С. 145–146.
60. Кузнецов А. В. Структуры с замыканием и критерии функциональной полноты : Третий всесоюзный коллоквиум по общей алгебре // Успехи математических наук. — 1961. — Т. 16, № 2. — С. 201–202.
61. Кузьмин В. А. Реализация функций алгебры логики автоматами, нормальными алгорифмами и машинами Тьюринга // Проблемы кибернетики. Вып. 13. — М.: Наука, 1965. — С. 75–96.

62. Кучеренко И. В. О структуризации класса обратимых клеточных автоматов // Дискретная математика. — 2007. — Т. 19, № 3. — С. 102–121.
63. Летичевский А. А. Условия полноты для конечных автоматов // Вычислительная математика и математическая физика. — 1961. — Т. 1, № 4. — С. 702–710.
64. Летуновский А. А. О выразимости константных автоматов суперпозициями // Интеллектуальные системы. — 2009. — Т. 13, № 1–4. — С. 397–406.
65. Летуновский А. А. О задаче выразимости автоматов относительно суперпозиции для систем с фиксированной добавкой // Интеллектуальные системы. — 2011. — Т. 15, № 1–4. — С. 401–412.
66. Летуновский А. А. О выразимости суперпозициями групповых автоматов Медведева // Интеллектуальные системы. — 2013. — Т. 17, № 1–4. — С. 179–181.
67. Летуновский А. А. Задача выразимости автоматных функций относительно расширенной суперпозиции. — Дис. ... канд. физ.-мат. наук / Москва, МГУ им. М. В. Ломоносова. — 2014.
68. Летуновский А. А. Выразимость линейных автоматов относительно расширенной суперпозиции // Интеллектуальные системы. — 2015. — Т. 19, № 1. — С. 161–170.
69. Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1. — М.: Мир, 1988.
70. Ло Чжукай. Предполные классы, определяемые k-арными отношениями в k-значной логике // Acta Sci. Natur. Univ. Jilinensis. — 1964. — № 3. — С. 39–50.
71. Ло Чжукай, Лю Сюй Хуа. Предполные классы, определяемые бинарными отношениями в многозначной логике // Acta Sci. Natur. Univ. Jilinensis. — 1963. — № 4. — С. 27–33.
72. Лунц А. Г. p-адический аппарат теории конечных автоматов // Проблемы кибернетики. Вып. 14. — М.: Наука, 1965. — С. 17–30.
73. Лупанов О. Б. Об одном методе синтеза схем // Известия высших учебных заведений. Серия радиофизика. — 1958. — № 1. — С. 120–140.
74. Мазуренко И. Л. Эффективный способ введения метрики на множестве непрерывных СММ-автоматов // Интеллектуальные системы. — 2007. — Т. 11, № 1–4. — С. 593–608.
75. Макаров В. В. О группах автоматных перестановок // Фундаментальная и прикладная математика. — 1996. — Т. 2, № 1. — С. 171–186.
76. Макаров В. В. Группа автоматных перестановок AS_n порождается элементами бесконечного порядка // Дискретная математика. — 1997. — Т. 9, № 3. — С. 117–124.
77. Малыгин В. И. Суперпозиции автоматов и линейные пространства, связанные с ними // Дискретная математика. — 1990. — Т. 2, № 1. — С. 31–42.
78. Мальцев А. И. Итеративные алгебры Поста. — Новосибирск: Новосиб. гос. ун-т, 1976.
79. Мальцев А. И. Алгоритмы и рекурсивные функции. — М., Наука, 1986.
80. Марков А. А. Пример статистического исследования над текстом «Евгения Онегина», иллюстрирующий связь испытаний в цепь // Известия Императорской Академии наук, серия VI. — 1913. — Т. 10, № 3. — С. 153–162.
81. Мартынюк В. В. Исследование некоторых классов функций в многозначных логиках // Проблемы кибернетики. Вып. 3. — М.: Физматгиз, 1960. — С. 49–60.
82. Марченков С. С. Об одном методе анализа суперпозиций непрерывных функций // Проблемы кибернетики. Вып. 37. — М.: Наука, 1980. — С. 5–17.
83. Мастихина А. А. Критерий частичного предвосхищения общерегулярных сверхсобытий // Дискретная математика. — 2011. — Т. 23, № 4. — С. 103–114.
84. Муравьев Н. В. Разрешимость задачи определения порядка линейного автомата // Интеллектуальные системы. Теория и приложения. — 2020. — Т. 24, № 2. — С. 145–155.
85. Муравьев Н. В. Оценки порядков линейных автоматов // Вестник МГУ. Серия 1. Математика. Механика. — 2022. — № 6. — С. 8–14.
86. Насыров А. З. Об обходе лабиринтов автоматами, оставляющими нестираемые отметки // Дискретная математика. — 1997. — Т. 9, № 1. — С. 123–133.
87. Орлов В. А. О сложности реализации ограниченно-детерминированных операторов схемами в автоматных базисах // Проблемы кибернетики. Вып. 26. — М.: Наука, 1973. — С. 141–182.
88. Пан Юн-Цзе. Один разрешающий метод для отыскания всех предполных классов в многозначной логике, // Acta Sci. Natur. Univ. Jilinensis. — 1963. — № 3.
89. Пантелеев П. А. Об отличимости состояний автомата при искажениях на входе // Интеллектуальные системы. — 2007. — Т. 11, № 1–4. — С. 653–678.
90. Пархоменко Д. В. Вторая автоматная функция и с нею связанные классы регулярных языков // Интеллектуальные системы. — 2013. — Т. 17, № 1–4. — С. 186.

91. Пархоменко Д. В. Порожденные автоматами p-языки // Дискретная математика. — 2014. — Т. 26, № 1. — С. 96–102.
92. Подколзина М. А. О числе S-предполных классов в функциональной системе P_k^τ // Вестник МГУ. Серия 1. Математика. Механика. — 2009. — № 1. — С. 61–62.
93. Половников В. С. Об оптимизации структурной реализации нейронных сетей. — Дис. ... канд. физ.-мат. наук / Москва, МГУ им. М. В. Ломоносова. — 2007.
94. Родин А. А. О континуальности множества специальных предполных классов во множестве автоматных отображений // Интеллектуальные системы. — 2012. — Т. 16, № 1–4. — С. 329–334.
95. Родин С. Б. О свойствах кодирований состояний автомата // Интеллектуальные системы. Теория и приложения. — 2017. — Т. 21, № 1. — С. 97–111.
96. Ронжин Д. В. Об условиях A-полноты линейных автоматов над двоично-рациональными числами // Дискретная математика. — 2020. — Т. 32, № 2. — С. 44–60.
97. Ронжин Д. В. О конечной порожденности A-предполных классов в классе линейных автоматов над кольцом двоично-рациональных чисел // Интеллектуальные системы. Теория и приложения. — 2021. — Т. 25, № 3. — С. 191–202.
98. Ронжин Д. В. Распознавание A-полноты конечных систем линейных автоматов с добавками над кольцом двоично-рациональных чисел // Интеллектуальные системы. Теория и приложения. — 2021. — Т. 25, № 1. — С. 149–164.
99. Рябинин А. В. Стохастические функции конечных автоматов // Тезисы VI Всесоюзной конференции по математической кибернетике. — Саратов, 1983.
100. Строгалов А. С. Метрические свойства о.д.-функций // Межвузовский сборник трудов. № 56. — М.: МЭИ, 1985. — С. 80–84.
101. Тальхайм Б. О решетке замкнутых классов стабильных автоматов // Методы и системы диагностики. Вып. 1. — Саратов, 1979.
102. Титова Е. Е. Конструирование движущихся изображений клеточными автоматами // Интеллектуальные системы. — 2014. — Т. 18, № 1. — С. 153–180.
103. Хазбун И. В. Об условиях полноты и выразимости в точной алгебре автоматов // Логико-алгебраические конструкции. — Калинин: КГУ, 1984. — С. 35–41.
104. Холоденко А. Б. О построении статистических языковых моделей для систем распознавания русской речи // Интеллектуальные системы. — 2002. — Т. 6, № 1–4. — С. 381–394.
105. Часовских А. А. О полноте в классе линейных автоматов // Математические вопросы кибернетики. Вып. 3. — М.: Наука, 1991. — С. 140–166.
106. Часовских А. А. Замкнутые классы линейно-автоматных функций // Математические вопросы кибернетики. Вып. 13. — М.: ФИЗМАТЛИТ, 2004. — С. 113–136.
107. Часовских А. А. Об A-выразимости в классе линейно-автоматных функций // Математические вопросы кибернетики. Вып. 17. — М.: ФИЗМАТЛИТ, 2008. — С. 105–136.
108. Часовских А. А. Линейно-автоматные функции с операциями суперпозиции // Нейрокомпьютеры: разработка, применение. — 2013. — № 8. — С. 3–13.
109. Часовских А. А. Проблема полноты для класса линейно-автоматных функций // Дискретная математика. — 2015. — Т. 27, № 2. — С. 134–151.
110. Часовских А. А. О полноте в классе линейных 2-адических автоматов // Интеллектуальные системы. Теория и приложения. — 2016. — Т. 20, № 4. — С. 209–227.
111. Часовских А. А. Максимальные подклассы в классах линейных автоматов над конечными полями // Дискретная математика. — 2019. — Т. 31, № 4. — С. 88–101.
112. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.
113. Яблонский С. В. Функциональные построения в k-значной логике // Труды Математического института имени В. А. Стеклова. Т. 51. — М.: Изд-во АН СССР, 1958. — С. 5–142.
114. Bartholdi L., Mitrofanov I. The word and order problems for self-similar and automata groups. — eprint: 1710.10109. — URL: https://arxiv.org/abs/1710.10109.
115. Blum M., Kozen D. On the power of the compass (or, why mazes are easier to search than graphs) // 19th Annual Symposium on Foundations of Computer Science (sfcs 1978). — IEEE Computer Society. 1978. — P. 132–142. — DOI: 10.1109/SFCS.1978.30.
116. Budach L. Automata and labyrinths // Mathematische Nachrichten. — 1978. — V. 86. — P. 195–282. — DOI: 10.1002/mana.19780860120.
117. Dassow J. Ein modifizierter Vollstandigkeitsbegriff in einer Algebra von Automatenabbildungen. — Dissertation Doktor B / Rostock Universitet. — 1978.

118. Eichner L. Lineare Realisierbarkeit endlicher Automateen uber endlicher Korpern. — Dissertation / Freiburg. — 1971.
119. Gillibert P. An automaton group with undecidable order and Engel problems // Journal of Algebra. — 2018. — V. 497. — P. 363–392. — DOI: 10.1016/j.jalgebra.2017.11.049.
120. Hensel K. Zahlentheorie. — Berlin und Leipzig : G. J. Göschen'sche Verlagshandlung G.m.b.H., 1913.
121. Herman G. T. Every finite sequential machine is linearly realizable // Journal of Computer and System Sciences. — 1971. — V. 5. — P. 489–510. — DOI: 10.1016/S0022-0000(71)80012-0.
122. Moore E. F. Gedanken-experiments on sequential machines // Automata Studies / Ed. by C. E. Shannon, J. McCarthy. — Princeton : Princeton University Press, 1956. — P. 129–154. — DOI: 10.1515/9781400882618-006. — [Русский перевод: Мур Э. Умозрительные эксперименты с последовательностными машинами // Автоматы / Под ред. К. Э. Шеннона, Дж. Маккарти. — М.: Издательство иностранной литературы, 1956. — С. 179–210].
123. Neumann J. von. Collected works. Vol. 1–6. — New York : Pergamon, 1963.
124. Neumann J. von. Theory of Self-Reproducing Automata. — University of Illinois Press, 1966.
125. Post E. L. The two-valued iterative systems of mathematical logic. Vol. 5. — Princeton University Press, Princeton, NJ, 1941. — (Ann. Math. Stud.) — DOI: 10.1515/9781400882366.
126. Rosenberg I. La structure des fonctions de plusieurs variables sur un ensemble fini // Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences, Paris. — 1965. — T. 260. — P. 3817–3819.
127. Shannon C. E. Presentation of a maze-solving machine // Cybernetics. Trans. of the 8th Conf. — Josiah Macy, Jr. Found., 1951. — P. 173–180.

Поступило в редакцию 3 VI 2024