МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА

На правах рукописи

Часовских Анатолий Александрович

Полнота и выразимость в классах линейных автоматов

01.01.09 – Дискретная математика и математическая кибернетика

ДИССЕРТАЦИЯ
на соискание ученой степени
доктора физико-математических наук

Научный консультант
доктор физико-математических наук,
профессор
Кудрявцев Валерий Борисович

Москва – 2021

Оглавление

Введение

Актуальность темы. Интерес к автоматам, как преобразователям накапливающим и обобщающим поступающую в дискретные моменты времени информацию благодаря возможности менять свое внутреннее состояние, возник с середины прошлого столетия. Начало теории автоматов было положено работами Дж. фон-Неймана [54], С. К. Клини [36], М. Л. Минского [51], Э. Ф. Мура [53].

Возможность моделирования автоматами процессов обработки информации живыми организмами и бурное развитие вычислительной техники обусловили интенсивные исследования в области теории автоматов и их обобщений. Работа [53] Э. Ф. Мура об отличимости состояний конечного автомата и работа [36] С. К. Клини о представимых конечными автоматами событиях задали начальное направление развития теории. Решения задачи об автоматах в лабиринтах, полученные Л. Будахом [89] и А. С. Подколзиным [18], положили начало многочисленным исследованиям поведения конечных автоматов в сложных средах.

Одним из важных направлений исследований стала структурная теория автоматов, развиваемая в работах научной школы кибернетики, основателями которой являются А. А. Ляпунов, В. М. Глушков, С. В. Яблонский, О. Б. Лупанов, Р. Г. Бухараев, В. Б. Кудрявцев. В рамках структурной теории решаются задачи, связанные с выразимостью через заданные множества конечных автоматов при использовании некоторого "естественного" набора операций. В качестве операций, как правило, при этом выбираются операции суперпозиции, перенесенные из классов функций, не обладающих памятью, или операции композиции, включающие помимо суперпозиций операцию обратной связи.

Важнейшие обобщения понятия конечного автомата связаны с моделированием функционирования биологических систем. К ним относятся однородные структуры, называемые еще клеточными автоматами, начало исследованиям которых было положено Дж. фон-Нейманом [102] и Э. Ф. Муром [95]. Предложенная модель исследовалась в работах Е. А. Гото [91], Д. Майхилла [96], А. С. Подколзина [59]–[61], А. А. Болотова [15], И. В. Кучеренко [43] и других авторов.

Ввиду существенных современных результатов, достигнутых в областях, связанных с моделированием восприятия и поведения биологических существ, в последние годы возникла потребность к теоретическим исследованиям в классах искусственных нейронных сетей, рекуррентный вариант которых также является обобщением конечных автоматов. В 1982 году Д. Хопфилд предложил использовать рекуррентные нейронные сети для сжатия данных и моделирования ассоциативной памяти [93]. В дальнейшем были предложены архитектуры рекуррентных нейронных сетей, позволившие получить практически значимые решения для задач автоматического распознавания речи, перевода, распознавания сцен в видеоряде и других. К таким архитектурам следует отнести сеть с долговременной и кратковременной памятью (англ. Long short term memory, LSTM)[92], управляемый рекуррентный блок (англ. Gated recurrent units, GRU) [90].

Известно, что для класса конечных автоматов с операциями суперпозиции отсутствуют конечные полные системы. Ситуация меняется при переходе к операциям композиции. Несмотря на конечнопорожденность этого класса конечных автоматов, исследование полноты его конечных подмножеств затруднено, с одной стороны, по причине континуальности количества максимальных собственных подклассов, называемых предполными классами [40], с другой стороны, отсутствием алгоритма для определения полноты конечных подмножеств [38]. Сложность класса конечных автоматов показана в работе С. В. Алешина [4] о вложенности в этот класс группы Бернсайда.

Возникшие трудности преодолевались несколькими путями, среди которых следует выделить следующие три: изменение понятия замыкания, возможность использования некоторого “естественного” множества автоматов, изучение “содержательных” подклассов в классе автоматов. Так в работах В. А. Буевича рассматривались отображения, осуществляемые конечными автоматами на словах длины τ. Им найдены все τ-предполные классы, что позволило получить алгоритм проверки τ-полноты конечных множеств конечных автоматов. В. А. Буевичем было введено понятие аппроксимационной полноты [17] множества конечных автоматов, означающее τ-полноту этого множества для любого натурального τ. Оказалось, что количество аппроксимационно предполных классов счетно, но задача проверки аппроксимационной полноты конечных множеств конечных автоматов осталась алгоритмически неразрешимой.

А. А. Летичевским был получен критерий полноты множеств автоматов Медведева (автоматов без выходов) при использовании специальной операции замыкания[45].

Д. Н. Бабиным для каждого замкнутого класса решетки Поста [65] определено, является ли алгоритмически разрешимой проблема проверки полноты конечных множеств конечных автоматов, если к этим множествам добавлять данный замкнутый класс [8], [9]. В дальнейшем Д. Н. Бабиным для автоматов с k-значными входами и выходами были найдены достаточные условия на добавки предполных классов из P_k, которые обеспечивают алгоритмическую разрешимость или сохраняют неразрешимость проверки полноты конечных множеств [10].

Неразрешимость задачи полноты в классе дефинитных автоматов, являющемся одним из содержательных автоматных подклассов, показана Д. Н. Жуком [32]. Оказалось, что этот класс содержит континуум предполных классов [33].

Исследованию свойств конечных автоматов посвящено значительное количество работ, имеющих важное теоретическое и прикладное значение. Отметим здесь работы в области защиты информации [24], [55], построения датчиков псевдослучайных последовательностей [50], распознавания образов [49], [13], разработки компьютерных систем обучения [6], прогнозирования [25], вычислительной техники [30], технической диагностики [14], исследования различных свойств автоматов и их обобщений [3], [7], [21], [22], [31], [35], [37], [52], [56–58], [62], [64]. Следует выделить теорию вероятностных автоматов [98], [19], [1]. Широкий спектр свойств конечных автоматов используется в образовательном процессе [23], [27], [42], [2].

Степень разработанности темы исследования. Инициальный конечный автомат $\mathfrak{A}$ может быть задан шестеркой $(A, Q, B, \phi, \psi, \mathbf{q}_0)$ [42], где A, Q и B – конечные множества, называемые входным алфавитом, алфавитом состояний и выходным алфавитом, соответственно, $\phi : A \times Q \to Q$, $\psi : A \times Q \to B$ – функции переходов и выходов, соответственно, $\mathbf{q}_0$ – некоторый элемент множества Q, называемый начальным состоянием. Обрабатывая последовательность α, $\alpha = \mathbf{a}(0), \mathbf{a}(1), \ldots, \mathbf{a}(t), \ldots$, состоящую из элементов входного алфавита, автомат $\mathfrak{A}$ последовательно переходит в состояния $\mathbf{q}(1), \mathbf{q}(2), \ldots, \mathbf{q}(t+1), \ldots$ и вычисляет выходные значения $\mathbf{b}(0), \mathbf{b}(1), \ldots, \mathbf{b}(t), \ldots$, где

$$\mathbf{q}(0) = \mathbf{q}_0,$$

$$\mathbf{q}(t+1) = \phi\left(\mathbf{q}(t), \mathbf{a}(t)\right),$$

$$\mathbf{b}(t) = \psi\left(\mathbf{q}(t), \mathbf{a}(t)\right)$$

для любого значения t, пробегающего множество целых неотрицательных чисел и называемого параметром времени.

Таким образом, автомат $\mathfrak{A}$ сопоставляет каждой бесконечной последовательности (сверхслову) α элементов входного алфавита сверхслово β,

$$\beta = \mathbf{b}(0), \mathbf{b}(1), \ldots, \mathbf{b}(t), \ldots,$$

из элементов выходного алфавита и задает ограниченно-детерминированную функцию [42]

$$f_{\mathfrak{A}} : A^{\infty} \to B^{\infty},$$

где через A^∞ и B^∞ обозначены множества сверхслов в алфавитах A и B, соответственно. Мы не отличаем автоматы $\mathfrak{A}$ и $\mathfrak{A}'$, задающие равные ограниченно-детерминированные функции и в дальнейшем под конечным автоматом понимаем ограниченно-детерминированную функцию, которую он задает.

Пусть k – натуральное число, являющееся натуральной степенью некоторого простого числа p. Через E_k мы обозначаем конечное поле (поле Галуа) из k элементов. Конечный автомат $\mathfrak{A}$, задаваемый шестеркой $(A, Q, B, \phi, \psi, \mathbf{q}_0)$, называется линейным автоматом (ЛА) над полем E_k, если найдутся такие натуральные числа n, s, что $A = E_k^n$, $Q = E_k^s$ и $B = E_k$, а ϕ и ψ – линейные операторы k-значной логики. Таким образом, мы используем определение ЛА из работы [29], которое включает исследование оптимизации схемной реализации ЛА. Значительное число работ посвящено исследованиям свойств ЛА [100] и [63].

Линейные автоматы, отличающиеся лишь множествами фиктивных переменных, а на множествах существенных переменных задающие одну и ту же ограниченно-детерминированную функцию, мы называем равными. Предполагаем, что вместе с каким-либо линейным автоматом мы получаем все автоматы, равные ему.

Множество всех ЛА над полем E_k обозначим $\mathfrak{L}_k$. Ранее для множества $\mathfrak{L}_2$, рассматриваемого вместе с операциями композиции (переименования переменных, отождествления переменных, подстановки и обратной связи), были найдены все предполные классы. Оказалось, что таких классов счетное число, но задача проверки конечных подмножеств из $\mathfrak{L}_2$ на полноту алгоритмически разрешима [67], [68].

Цели и задачи диссертации:

Цели диссертации:

1. Найти все максимальные замкнутые по операциям композиции собственные подклассы в классах линейных автоматов над конечными полями.

2. Решить проблему существования алгоритма, проверяющего полноту конечных подмножеств этих классов и, при положительном решении, построить этот алгоритм.

3. Исследовать выразительные свойства операторов замыкания в классе линейных автоматов над полем из двух элементов через подмножества этих автоматов с естественными допущениями.

4. Разработать и исследовать алгебраические структуры, соответствующие классам линейных автоматов над конечными полями и связанных с ними классами.

Для достижения поставленных целей были сформулированы задачи, перечисленные далее.

1. Для классов $\mathfrak{L}_k$, рассматриваемых вместе с операцией аппроксимационного замыкания, найти все предполные классы. Построить алгоритм проверки аппроксимационной полноты конечных множеств ЛА.

2. Найти все максимальные собственные подалгебры в алгебре одноместных ЛА, сохраняющих нулевое сверхслово, с операциями, индуцированными операциями композиции в классе $\mathfrak{L}_k$.

3. Для конечных полей E_k найти все предполные классы в классах $\mathfrak{L}_k$ ЛА, рассматриваемых вместе с операциями композиции. Получить приведенную критериальную систему замкнутых классов.

4. Получить алгоритм проверки полноты конечных подмножеств из $\mathfrak{L}_k$ при использовании операций композиции.

5. Изучить структуру замкнутых по операциям композиции подклассов $\mathfrak{L}_2$, содержащих сумматор. Получить алгоритм проверки выразимости через конечные подмножества из $\mathfrak{L}_2$ при использовании сумматора и операций

композиции. В рассматриваемом классе найти критерий выразимости сумматора.

6. При "естественных" ограничениях на подмножества из $\mathfrak{L}_2$ получить критерии аппроксимационной выразимости через эти подмножества.

7. Найти все предполные по операциям суперпозиции классы в $\mathfrak{L}_2$. Сравнить композиционный, суперпозиционный и аппроксимационный операторы замыкания на множестве $\mathfrak{L}_2$.

8. Используя технику, разработанную для ЛА, решить задачу полноты для линейных 2-адических автоматов, рассматриваемых вместе с операциями композиции, то есть найти в указанном классе все предполные подклассы, получить алгоритм проверки полноты конечных подмножеств.

Объект и предмет исследования. Объектом исследования является класс $\mathfrak{L}_k$ линейных автоматов над конечным полем из k элементов. Наиболее полно выразительные свойства линейных автоматов изучены для случая $k = 2$. Рассатривается также класс линейных 2-адических автоматов.

Предметом исследования являются собственные подклассы в $\mathfrak{L}_k$, замкнутые по операциям композиции, суперпозиции или оператора аппроксимационного замыкания, прежде всего, являющиеся максимальными по включению. В классе линейных 2-адических автоматов изучаются максимальные замкнутые по операциям композиции собственные подклассы.

Научная новизна диссертации. В работе решена проблема полноты для классов ЛА над конечными полями. Часть результатов обобщают полученное ранее решение проблемы полноты для ЛА над полем из двух элементов, рассматриваемых вместе с операциями композиции. При этом, в основном, сохранился подход к решению, использованному для указанного частного случая. Сначала были найдены все аппроксимационно предполные классы и получен алгоритм проверки аппроксимационной полноты конечных подмножеств. Затем, рассмотрена алгебра одноместных ЛА, сохраняющих нулевое сверхслово, вместе с операциями, индуцированными многоместным случаем. В этом классе найдена приведенная критериальная система, состоящая из всех максимальных собственных подалгебр. Эта система в общем случае конечного поля, не являющегося простым, содержит двухпараметрическую серию максимальных подалгебр, в отличии от рассмотренного ранее двузначного случая, для которого в соответствующую систему входят только однопараметрические серии.

Для построения множества всех предполных по операциям композиции классов в $\mathfrak{L}_k$, помимо обобщения ранее построенных для случая поля E_2 классов, понадобилось найти принципиально новые классы, возникающие в случае полей Галуа, не являющихся простыми. Разработанная автором техника, опирается на некоторые результаты о подкольцах трансцендентных расширений конечных полей, например, на теорему Люрота о структуре подполей трансцендентного расширения конечного поля, содержащих это конечное поле, но включает и более общие алгебраические построения. Для построения предполных классов в $\mathfrak{L}_k$ и нахождения инвариантов, сохраняемых при операциях композиции, потребовалось использовать известные теоремы о структуре полей Галуа и их множеств автоморфизмов.

Основным результатом работы следует считать нахождение множества всех предполных по операциям композиции классов для $\mathfrak{L}_k$, включающего пять серий, три из которых счетны, а два – конечны, и три отдельных класса. В работе получен алгоритм проверки полноты конечных систем по этим операциям, имеющий полиномиальную временную сложность, в оценку которой входит пять параметров.

Для случая $k = 2$ решена задача выразимости через подмножества с сумматором при использовании операций композиции (K-выразимости). Найдена структура замкнутых по операциям композиции классов, содержащих сумматор. Получен алгоритм проверки K-выразимости сумматора через конечные множества ЛА, а, в случае положительного решения, K-выразимости через это множество произвольного линейного автомата.

Известно [42], что для решения задачи аппроксимационной выразимости (A-выразимости) не требуется операция обратной связи. С использованием этого результата в настоящей работе решено несколько задач об A-выразимости. Сначала, в качестве вспомогательного результата, решена задача A-выразимости в алгебре одноместных ЛА, сохраняющих нулевое сверхслово, что позволило получить теорему об A-выразимости через множества ЛА, содержащих существенный автомат, а также все константы в своем аппроксимационном замыкании (A-замыкании). Также получен критерий A-выразимости констант через заданное множество ЛА, содержащее существенный автомат, позволяющий проверять это свойство для конечных множеств ЛА. Кроме перечисленного, в работе получены некоторые достаточные условия, позволяющие проверять A-выразимость ЛА через заданное конечное подмножество $\mathfrak{L}_k$. Показана конечнопорожденность невырожденных A-замкнутых множеств ЛА, содержащих сумматор, и, как следствие, их счетность.

Разработанная для ЛА техника позволила найти все предполные классы для $\mathfrak{L}_2$, рассматриваемого вместе с операциями суперпозиции, а также распространить использованный в работе подход на множество линейных 2-адических автоматов, рассматриваемое вместе с операциями композиции. Для этого класса также найдены все максимальные собственные подалгебры и получен алгоритм проверки полноты конечных подмножеств.

Теоретическая значимость работы. Работа имеет теоретический характер. Ее результаты могут быть использованы для продолжения исследований проблемы полноты как в подклассах ЛА, так и в классах автоматов, не являющихся линейными, но обладающих некоторыми аналогичными свойствами. Выполненные в работе исследования проблем полноты и выразимости для классов ЛА могут определить содержание специальных курсов, семинаров и вычислительных практикумов.

Исследования, выполненные для трансцендентных расширений конечных полей могут быть использованы в алгебре при изучении подколец и, в частности, подполей этих расширений. Подкольца при этом должны обладать свойством замкнутости по операции “близкой” к операции деления, которая рассматривается в настоящей работе.

Практическая значимость работы. Практическая значимость работы определяется возможностью использования ее результатов для вычислений в полях Галуа, в системах кодирования, обнаруживающих и исправляющих ошибки, датчиках псевдослучайных чисел и других важных прикладных областях.

Результаты работы могут быть использованы для решения задач в области рекуррентных нейронных сетей, используемых, например, для моделирования ассоциативной памяти, при решении задач распознавания речи, машинного перевода и других задач, связанных с исследованиями в области искусственного интеллекта.

Методология и методы исследования.

В работе используются методы дискретной математики, математической кибернетики, алгебры и математического анализа. В частности, использованы результаты по теории автоматов и теории функциональных систем, теории алгоритмов, теории полей Галуа и их расширений, теории колец.

Если для заданного конечнопорожденного класса дискретных функций существует алгоритм проверки полноты конечных подмножеств, то этот алгоритм может быть получен путем нахождения всех предполных подклассов этого класса. Соответствующий подход был использован, например, в случае классов конечнозначных логик [97], [99], для других классов, а также в настоящей работе.

Автором были исследованы вспомогательные алгебры с операциями, имеющими меньшие ограничения, чем операции композиции в рассматриваемых классах ЛА. Далее решение осуществлялось путем переноса свойств вспомогательных подалгебр на классы $\mathfrak{L}_k$ с изменениями, позволяющими преодолеть возникающие при этом ограничения. Следовательно, для решения проблемы полноты в классах ЛА над конечными полями автором была неоднократно использована редукция к связанным с ними алгебраическим структурам, что и составило основное содержание метода, использованного в настоящей работе.

Положения, выносимые на защиту:

1. В соответствии с существующими подходами к изучению функциональных систем, наиболее важной их характеристикой является структура предполных классов. Так, для классов конечнозначных логик множества предполных классов конечны, а в классе всех конечных автоматов множество предполных классов континуально. В настоящей работе для всех классов ЛА над конечными полями, рассматриваемых вместе с операциями композиции, являющимися содержательными подклассами соответствующих классов конечных автоматов, найдены все предполные классы, множества которых счетны.

2. Несмотря на бесконечность множества предполных классов, составляющих приведенную критериальную систему в классе ЛА, для конечных подмножеств таких автоматов получен алгоритм проверки полноты. Этот алгоритм имеет полиномиальную временную сложность от нескольких параметров.

3. Основу используемой техники составляют методы, изложенные в книге [29]. В настоящей работе разработана техника, позволяющая при определенных условиях сводить исследования операций над многоместными ЛА к операциям в алгебре одноместных ЛА. При этом используется разложение изучаемых автоматов в сумму одноместных. Элементы этой алгебры одноместных ЛА, сохраняют нулевое сверхслово и составляют подкольцо трансцендентного расширения поля Галуа, которое обозначено через $E'_k(\xi)$. В этой алгебре, рассматриваемой вместе с операциями сложения и умножения, а также некоторой частичной операцией “ослабленного деления”, найдены все максимальные подалгебры. В случае простого поля

максимальные собственные подалгебры естественным образом группируются в две однопараметрические серии, а, в противном случае, при наличии одного не параметризованного класса, в две однопараметрические серии и одну двухпараметрическую.

Алгебра $E'_k(\xi)$ используется как при решении проблемы K-полноты в $\mathfrak{L}_k$, так и при исследовании вопросов K- и A-выразимости в $\mathfrak{L}_2$.

4. В классе $\mathfrak{L}_2$ решена проблема K-выразимости через конечные множества, содержащие сумматор, а также задача выразимости сумматора через такие множества. Для этого в алгебре $E'_2(\xi)$ выделено счетное семейство $R_i^{(1)}$, $i = 0, 1, 2, \dots$, замкнутых классов, каждый из которых не содержит единицу. Каждому K-замкнутому множеству ЛА, содержащему сумматор, соответствует (в некотором смысле) единственное замкнутое подмножество в $E'_2(\xi)$, которое не содержится ни в одном из классов семейства $R_i^{(1)}$ или, что равносильно, не содержит единицу. Найдена структура всех таких замкнутых подмножеств множества $E'_2(\xi)$, которая зависит от наличия в замкнутом подмножестве дроби с положительной степенью. Это позволило определить структуру конечнопорожденных невырожденных K-замкнутых классов, содержащих сумматор от трех переменных.

5. В структуре замкнутых классов алгебры $E'_2(\xi)$ найдена подструктура замкнутых по операциям одноместного аппроксимационного замыкания, $A^{(1)}$-замыкания, классов, которая является счетной, а каждый ее элемент конечнопорожден. Получен алгоритм проверки включения $\mu \in A^{(1)}(M)$ для любого конечного подмножества M алгебры $E'_2(\xi)$ и любого ее элемента μ.

6. Получен алгоритм проверки A-выразимости через конечные подмножества ЛА из $\mathfrak{L}_2$, содержащие существенный автомат (автомат, имеющий две или более непосредственных переменных, то есть переменных, от зна-

чения которых в некоторый момент времени значение выхода зависит в тот же момент времени), а также все константы в A-замыкании. Показано, что любое невырожденное множество ЛА M содержит конечное подмножество M' такое, что A-выразимость всех констант через M равносильна их A-выразимости через M'. Найден алгоритм проверки A-выразимости всех констант через конечные множества ЛА.

7. Получены некоторые достаточные условия для возможности проверки A-выразимости в $\mathfrak{L}_2$ через конечные множества ЛА. При некоторых "естественных" ограничениях на множества ЛА получено необходимое и достаточное условие совпадения операторов K-замыкания и A-замыкания.

8. Для множества $\mathfrak{L}_2$ ЛА вместе с операциями суперпозиции найдены все предполные классы, количество которых оказалось счетным. Найденное множество предполных классов составляет приведенную критериальную систему по операциям суперпозиции.

9. Проблема полноты решена для класса линейных 2-адических автоматов, рассматриваемых вместе с операциями композиции. В этом классе также построена счетная критериальная система, состоящая из всех предполных классов. Здесь, как и в случае ЛА, используется возможность декомпозиции автоматов и перехода к исследованию класса одноместных автоматов.

Степень достоверности результатов. Все результаты диссертации математически строго доказаны.

Апробация результатов. Основные результаты диссертации докладывались на следующих конференциях и научных семинарах:

- XIII Международном научном семинаре «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (Москва, 2019 г.)

- научной конференции "Ломоносовские чтения" (Москва, 2018 г., 2016 г., 2014 г., 2013 г., 2012 г., 2011 г., 2010 г.)

- XI международной конференции "Интеллектуальные системы и компьютерные науки"(Москва, 2016 г.)

- XII Международном научном семинаре «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (Москва, 2016 г.)

- XI Международном научном семинаре «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (Москва, 2012 г.)

- международной конференции «Современные проблемы математики, механики и их приложений», посвященной 70-летию ректора МГУ академика В. А. Садовничего (Москва, 2009 г.)

Результаты диссертации неоднократно докладывались на специальных семинарах механико-математического факультета МГУ:

- “Теория автоматов” под руководством заведующего кафедрой МаТИС профессора В. Б. Кудрявцева (2012 – 2019 гг.)

- “Математические вопросы кибернетики” под руководством профессора О. М. Касим-Заде (2019 г.)

- “Дискретная математика и математическая кибернетика” под руководством профессора С. А. Ложкина и профессора В. Б. Алексеева (2019 г.)

- “Вопросы сложности алгоритмов поиска” под руководством профессора Э. Э. Гасанова и научных сотрудников В. В. Осокина, Ю. С. Шуткина, Г. В. Калачева (2017 г.)

- “Дискретный анализ” под руководством профессора С. В. Алешина, профессора В. А. Буевича и старшего научного сотрудника М. В. Носова (2016 г.)

Публикации. Материалы диссертации опубликованы в 22 работах автора, из них 15 статей в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 01.01.09 – Дискретная математика и математическая кибернетика [66, 67, 74–84, 86, 87], кроме того, 1 статья опубликована в издании из Перечня ведущих рецензируемых научных журналов и изданий, выпускаемых в Российской Федерации, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора наук, индексируемом РИНЦ [73].

Личный вклад автора. Результаты, представленные теоремами в диссертационной работе и автореферате, помимо имеющих ссылки на работы других авторов, положения, выносимые на защиту, получены автором самостоятельно. Подготовка к публикации полученных результатов проводилась без соавторов.

Структура и объем диссертации. Диссертация состоит из введения, 5 глав, состоящих в совокупности из 18 параграфов, заключения, списка сокращений и условных обозначаний и списка литературы. Общий объем диссертации 268 страниц, из них 268 страницы текста, рисунков нет. Список литературы включает 102 наименования на 9 страницах.

Краткое содержание работы. В параграфе 1 главы 1 введены необходимые понятия и обозначения. Кольцо формальных степенных рядов переменной ξ с коэффициентами из E_k и операциями сложения и умножения мы обозначаем $R_k(\xi)$. Подкольцо этого кольца, состоящее из периодических (с предпериодом) рядов обозначаем $E'_k(\xi)$. Это подкольцо изоморфно кольцу отношений многочленов из $E_k[\xi]$, знаменатели которых не делятся на ξ. Поэтому мы не отличаем указанные подкольца. Линейный автомат от n переменных реализует функцию из $R_k^n(\xi)$ в $R_k(\xi)$ и отождествляется нами с этой функцией.

В этом параграфе введено три набора операций замыкания: операции суперпозиции, композиции и аппроксимационного замыкания, а также приведены две теоремы, которые содержатся в работе [29] и определяют понимание ЛА, как преобразователей рядов. Эти теоремы доказаны с использованием техники работы с рядами.

Теорема 1.1.1. [29] *Для каждого* f, $f \in \mathfrak{L}_k$, *от переменных* $x_1, x_2, \ldots, x_n$ *найдутся элементы* μ_i, $i = 0, 1, 2, \ldots, n$, *кольца* $E'_k(\xi)$, *что выполнено равенство:*

$$f\left(x_1, x_2, \ldots, x_n\right) = \sum_{i=1}^{n} \mu_i x_i + \mu_0. \tag{1}$$

Теорема 1.1.2. [29] *Для любых элементов* μ_i *кольца* $E'_k(\xi)$, $i = 0, 1, 2, \ldots, n$ *найдется ЛА* f, *для которого выполнено разложение*

$$f\left(x_1, x_2, \ldots, x_n\right) = \sum_{i=1}^{n} \mu_i x_i + \mu_0.$$

В §2 главы 1 найдены все A-предполные классы, что составляет результат теоремы 1.2.1. Как и в случае поля E_2, состоящего из двух элементов, в общем случае проверка A-полноты осуществляется на словах длины 2. Для случая поля, не являющегося простым, мы получили серию A-предполных классов, каждый из которых соответствует определенному максимальному собственному подполю конечного поля E_k.

Через T_a обозначим множество всех ЛА, сохраняющих в начальный момент времени элемент a поля E_k. Множество V_1 состоит из ЛА, имеющих не более одной непосредственной переменной. ЛА $f\left(x_1, x_2, \ldots, x_n\right)$, для которого имеет место разложение (1), содержится в множестве V_p, $V_p \subset \mathfrak{L}_k$, в точности тогда, когда $\sum_{i=1}^{n} \mu_i(0) = 1$, $n = 1, 2, \ldots$. Множество M_1 состоит из ЛА f, выход которого в состоянии $\mathbf{q}(1)$ не зависит от входов в начальный момент времени.

Положим в случае простого k:

$$J_k^A = \left\{\; T_a,\;\; V_1,\;\; V_p,\;\; M_1 \;\mid\; a \in E_k \;\right\}.$$

В случае k, не являющимся простым, через P_s обозначим множество всех ЛА f, свободные члены коэффициентов при переменных в разложении (1) которого содержатся в некотором максимальном по включению подполе E_{k_s} поля E_k, не совпадающему с E_k. Пусть E_{k_1}, E_{k_2}, ..., E_{k_l} — все максимальные по включению подполя в E_k, не совпадающие с E_k. Положим в рассматриваемом случае:

$$J_k^A = \{\ T_a,\ \ V_1,\ \ V_p,\ \ M_1,\ \ P_s\ \mid\ a \in E_k,\ \ s \in \{1, 2, \ldots, l\}\}\,.$$

Теорема 1.2.1. *Множество J_k^A является приведенной A-критериальной системой в $\mathfrak{L}_k$.*

Для построения множества предполных классов в $\mathfrak{L}_k$ в §3 главы 1 найдено множество максимальных собственных подклассов в $E'_k(\xi)$, замкнутых относительно операций сложения, умножения и операции fb, определенной на парах μ_1, μ_2, в точности если $\mu_2(0) = 0$. При этом $\mathrm{fb}\,(\mu_1, \mu_2) = \frac{\mu_1}{1-\mu_2}$. Замыкание множества M по перечисленным операциям мы обозначаем $K^{(1)}(M)$.

Через $R_0^{(1)}$ обозначим множество дробей из $E'_k(\xi)$, степень числителя которых меньше степени знаменателя.

Перенумеруем все приведенные неприводимые многочлены кольца $E_k[\xi]$ [20]: $p_1, p_2, \ldots$, так, что $p_1 = \xi$. Множество всех дробей из $E'_k(\xi)$, несократимый вид которых имеет числитель, делящийся на p_i, обозначим $R_i^{(1)}$.

Множество всех дробей μ из $E'_k(\xi)$, для которых выполнено включение $\mu(0) \in E_{k_s}$ обозначим $P_s^{(1)}$.

Множество $M_1^{(1)}$ состоит из всех μ, $\mu \in E'_k(\xi)$, для которых имеет место включение: $\mu - \mu(0) \in \xi^2 E'_k(\xi)$.

Через Ω_k обозначим множество всех автоморфизмов поля E_k. Пусть $\mu \in E'_k(\xi)$. Дробь $\mu'(\xi)$, $\mu'(\xi) = \mu(1/\xi)$, содержится в $E'_k(\xi)$ в точности тогда, когда степень числителя дроби $\mu(\xi)$ не превосходит степени ее знаменателя. Для заданного автоморфизма ω, $\omega \in \Omega_k$, дробь μ включаем в множество $M_{0,\omega}$, если $\mu'(\xi) \in E'_k(\xi)$ и $\mu'(0) = \omega(\mu(0))$.

Если знаменатель дроби μ, $\mu \in E'_k(\xi)$, не делится на многочлен p_i, $i \in$

$\{2, 3, \dots\}$, то в кольце $E'_k(\xi)$ для μ имеет место формула для деления с остатком:

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

где $\mu' \in E'_k(\xi)$, $u' \in E_k[\xi]$ и $\deg u' < \deg p_i$. Для заданного автоморфизма ω, $\omega \in \Omega_k$, множество $M^{(1)}_{i,\omega}$ состоит из таких μ, что $u' = \omega(\mu(0))$.

Положим в случае поля E_k, не являющегося простым:

$$\begin{aligned} J^{(1)}_k \;=\; \Big\{ \; & M^{(1)}_{i,\omega}, M^{(1)}_1, R^{(1)}_i, P^{(1)}_s \;| \\ & \omega \in \Omega_k, i = 0, 2, 3, \dots, s = 1, 2, \dots, l, \;\; \Big\}. \end{aligned}$$

В случае простого k имеем лишь один его тождественный автоморфизм id. В этом случае, обозначая множество $M^{(1)}_{i,\mathrm{id}}$ через $M^{(1)}_i$, имеем:

$$J^{(1)}_k = \left\{ M^{(1)}_i, R^{(1)}_i | i = 0, 1, \dots \right\}.$$

Расширение поля [20] F множеством M обозначаем $F(M)$. Если M состоит из единственного элемента μ, то вместо $F(\{\mu\})$ мы можем использовать обозначение $F(\mu)$.

Теорема 1.3.1. *Если для заданного множества M, $M \subseteq E'_k(\xi)$, и любого Θ, $\Theta \in J^{(1)}_k$, выполнено: $M \not\subseteq \Theta$, то*

$$E_p(M) = E_k(\xi).$$

Теорема 1.3.2. *Множество $J^{(1)}_k$ является приведенной $K^{(1)}$-критериальной системой $K^{(1)}$-замкнутых классов. Кроме этого, множество $J^{(1)}_k$ состоит из $K^{(1)}$- предполных классов и все $K^{(1)}$-предполные классы содержатся в $J^{(1)}_k$.*

В главе 2 найдены все предполные классы в $\mathfrak{L}_k$, в терминах предполных классов сформулирован алгоритм проверки полноты конечных множеств.

В §1 этой главы доказаны теоремы 2.1.1 и 2.1.2, позволяющие использовать результаты главы 1 для исследования K-полноты множеств ЛА.

Через J'_k обозначим следующее множество:

$$\{\ V_1,\ V_p,\ T_a\ \mid\ a \in E_k\ \}.$$

Если для линейного автомата f имеет место разложение (1), то множество,

$$\{\ \mu_i\ \mid\ i = 1, 2, \ldots, n\ \},$$

состоящее из коэффициентов при переменных этого разложения, обозначим $U(f)$. Для множества M, $M \subseteq \mathfrak{L}_k$, положим: $U(M) = \cup_{f \in M} U(f)$.

Теорема 2.1.1. *Для множества M, $M \subseteq \mathfrak{L}_k$, равенство*

$$K(M) = \mathfrak{L}_k$$

выполнено в точности тогда, когда имеют место следующие два свойства:

$$\forall \Theta,\ \ \Theta \in J'_k,\ \ \textit{выполнено: } M \not\subseteq \Theta,$$

$$U(K(M)) = E'_k(\xi).$$

Через $\tilde{M}_0^{(1)}$ обозначим множество, состоящее из всех дробей кольца $E'_k(\xi)$, степень числителя которых не превосходит степени знаменателя, а для $j \in \{2, 3, \ldots\}$ через $\tilde{M}_j^{(1)}$ обозначим множество всех дробей из $E'_k(\xi)$, знаменатель которых не делится на p_j.

Теорема 2.1.2. *Множество M, $M \subseteq \mathfrak{L}_k$, является K-полным в $\mathfrak{L}_k$ тогда и только тогда, когда имеет место:*

$$\forall \Theta,\ \ \Theta \in J'_k,\ \ \textit{выполнено: } M \not\subseteq \Theta,$$

а также:

$$\forall \Theta, \Theta \in J_k^{(1)}, \quad U(M) \not\subseteq \Theta,$$

и

$$\forall j, j = 0, 2, 3, \ldots, \quad U(K(M)) \not\subseteq \tilde{M}_j^{(1)}.$$

В §2 главы 2 найдены все предполные классы в $\mathfrak{L}_k$. В случае k, не являющегося простым, для каждого $\Theta^{(1)}$ из множества

$$\left\{ \ M^{(1)}_{i,\omega}, M^{(1)}_1, P^{(1)}_s \ \mid \ \omega \in \Omega_k, i = 0, 2, 3, \dots, s = 1, 2, \dots, l \ \right\}$$

положим:

$$\Theta = \left\{ \ f \ \mid \ f \in \mathfrak{L}_k, \ \ U(f) \subset \Theta^{(1)} \ \right\}.$$

Тем самым определено множество классов J''_k:

$$J''_k = \{ \ M_{i,\omega}, M_1, P_s \ \mid \ \omega \in \Omega_k, i = 0, 2, 3, \dots, s = 1, 2, \dots, l \ \}.$$

В случае простого k для каждого i, $i \in \{0, 1, \dots\}$, определим множество M_i

$$M_i = \left\{ \ f \ \mid \ f \in \mathfrak{L}_k, \ \ U(f) \subset M^{(1)}_i \ \right\},$$

и множество J''_k,

$$J''_k = \{ \ M_i \ \mid \ i = 0, 2, 3, \dots \ \}.$$

Далее положим:

$$\begin{aligned} R^e_j \ = \ \Bigg\{ \ & f \ \mid \ f \in \mathfrak{L}_k, \ \ f\left(x_1, x_2, \dots, x_n\right) = \sum_{i=1}^{n} \mu_i x_i + \mu_0, \\ & \forall i, i = 1, 2, \dots, n, \ \ \text{если} \ \ x_i \ \text{— единственная существенная} \\ & \text{переменная ЛА} \ \ f, \ \ \text{то} \ \ \mu_i \in \tilde{M}^{(1)}_j, \\ & \ \ \text{в противном случае:} \ \ \mu_i \in R^{(1)}_j \ \Bigg\}, \end{aligned}$$

$$\begin{aligned} R^d_j \ = \ \Bigg\{ \ & f \ \mid \ f \in \mathfrak{L}_k, \ \ f\left(x_1, x_2, \dots, x_n\right) = \sum_{i=1}^{n} \mu_i x_i + \mu_0, \\ & \forall i, i = 1, 2, \dots, n, \ \ \text{если} \ \ x_i \ \text{— единственная непосредственная} \\ & \text{переменная ЛА} \ \ f, \ \ \text{то} \ \ \mu_i \in \tilde{M}^{(1)}_j, \\ & \ \ \text{в противном случае:} \ \ \mu_i \in R^{(1)}_j \ \Bigg\}, \end{aligned}$$

$j = 0, 2, 3, \ldots,$

$$J_k''' = \left\{ \; R_j^e, R_j^d \;\mid\; j = 0, 2, 3, \ldots \; \right\},$$

$$J_k = J_k' \cup J_k'' \cup J_k'''.$$

Теорема 2.2.1. *Множество K-замкнутых классов J_k является K-критериальной системой в $\mathfrak{L}_k$, то есть для любого подмножества M множества $\mathfrak{L}_k$ его K-полнота в $\mathfrak{L}_k$ равносильна невключению в каждый K-замкнутый класс множества J_k.*

Теорема 2.2.2. *Множество J_k является приведенной K-критериальной системой.*

Теорема 2.2.3. *Множество J_k состоит из K-предполных классов в $\mathfrak{L}_k$ и содержит все K-предполные классы.*

В §3 главы 2 мы приводим алгоритм проверки K-полноты конечных множеств ЛА и оцениваем его сложность.

Пусть множество M ЛА содержит r элементов, количество переменных каждого из которых не превосходит r, а наибольшая степень дроби из $U(M)$ не больше d. Через m обозначим $\log_p k$.

Теорема 2.3.1. *Полученный алгоритм проверки полноты конечных подмножеств ЛА корректен и может быть реализован с временной сложностью*

$$O\left(rnk\right) + O\left(rnd^2 m\right)$$

для поля E_k, не являющегося простым. В случае простого поля E_k этот алгоритм может быть реализован с временной сложностью

$$O\left(rnk\right) + O\left(rnd^2\right).$$

В главах 3 — 5 рассматривается класс ЛА над полем E_2. Вместо обозначения $\mathfrak{L}_2$ мы используем $\mathfrak{L}$, а вместо $E_k'(\xi)$ — используем $\mathfrak{L}_0^{(1)}$, подчеркивая автоматное «происхождение» этого множества.

В главе 3 решены некоторые задачи выразимости в $\mathfrak{L}_0^{(1)}$, связанные с наличием сумматора или его получением.

В §1 этой главы введены необходимые понятия и обозначения.

Положим:

$$M^{(1)}(\mu, u_0) = \Big\{ a_0 + \mu u_0(\mu) \frac{u(\mu)}{v(\mu)} | \\ a_0 \in E_2, u(\xi) \in E_2[\xi], v(\xi) \in 1 + \xi E_2[\xi], (u_0(\xi), v(\xi)) = 1 \Big\},$$

$$P^{(1)}(\mu, u_0) = \Big\{ a_0 + \mu u_0(\mu) \frac{u(\mu)}{v(\mu)} | a_0 \in E_2, u(\xi) \in E_2[\xi], \\ v(\xi) \in 1 + \xi E_2[\xi], (u_0(\xi), v(\xi)) = 1, \\ \deg u(\xi) \leq \deg v(\xi) - 2(1 + \deg u_0(\xi)) \Big\},$$

$$R^{(1)}(\mu, u_0) = \Big\{ u_0(\mu) \frac{u(\mu)}{v(\mu)} | \\ u(\xi) \in E_2[\xi], v(\xi) \in 1 + \xi E_2[\xi], (u_0(\xi), v(\xi)) = 1 \Big\},$$

где $\mu \in \xi \mathfrak{L}_0^{(1)}$, $u_0 \in E_2[\xi] \setminus \{0\}$.

Множество $R^{(1)}(\xi, p_i)$, как ранее, так и в дальнейшем, мы обозначаем $R_i^{(1)}$, $i = 1, 2, \ldots$.

В §2 главы 3 получена структура $K^{(1)}$-замкнутых классов в $\mathfrak{L}_0^{(1)}$, содержащих сумматор (теорема 3.2.1), а также найден критерий вхождения элемента 1 в замкнутый класс из $\mathfrak{L}_0^{(1)}$ (теорема 3.2.2).

Теорема 3.2.1. *1. Пусть*

$$M \subseteq \mathfrak{L}_0^{(1)}, \quad K^{(1)}(M) = M, \quad M \setminus E_2 \neq \emptyset, \\ M \not\subseteq R_i^{(1)}, \quad i = 0, 1, 2, \ldots.$$

Тогда найдутся μ, u_0, T, $\mu \in \xi \mathfrak{L}_0^{(1)}$, $u_0 \in 1 + \xi E_2[\xi]$, $T \in \mathbb{N}$, *что выполнено одно из двух следующих соотношений:*

Случай 1.

$$M^{(1)}(\mu, (\xi u_0)^T) \subseteq M \subseteq M^{(1)}(\mu, u_0) \tag{2}$$

Случай 2.

$$P^{(1)}(\mu, (\xi u_0)^T) \subseteq M \subseteq M_0^{(1)}(\mu) \cap M^{(1)}(\mu, u_0) \tag{3}$$

2. Число $K^{(1)}$-замкнутых в $\mathfrak{L}_0^{(1)}$ классов M, удовлетворяющих включениям (2) или включениям (3) конечно.

Теорема 3.2.2. *Соотношение*

$$1 \in K^{(1)}(M)$$

выполнено тогда и только тогда, когда для каждого i, $\quad i = 0, 1, 2, \dots,$

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

В §3 главы 3 получен алгоритм проверки выразимости через конечное множество ЛА, содержащее сумматор в замыкании.

Множество ЛА, реализующих константы, мы обозначаем $\mathfrak{L}_c$. Если $M \subseteq \mathfrak{L}_0^{(1)}$ и $C \subseteq \mathfrak{L}_c$, то множество

$$\left\{ \sum_{\substack{\gamma \in C', \\ \mu \in K^{(1)}(M)}} \mu\gamma \quad | \quad C' \subset C, \ \ |C'| < \infty \right\}$$

обозначаем $S(M, C)$.

Теорема 3.3.1. *Существует алгоритм, который для любых μ', γ', M, C,*

$$\mu' \in \mathfrak{L}_0^{(1)}, \quad \gamma' \in \mathfrak{L}_c, \quad M \subset \mathfrak{L}_0^{(1)}, \quad C \subset \mathfrak{L}_c,$$

$$|M| < \infty, \quad |C| < \infty, \quad 1 \in K^{(1)}(M),$$

определяет справедливость соотношений

$$\mu' \in K^{(1)}(M),$$

$$\gamma' \in S(M, C).$$

Теорема 3.3.2. *Проблема выразимости в $\mathfrak{L}$ через конечные системы, содержащие сумматор в замыкании, алгоритмически разрешима.*

Алгоритм проверки выразимости сумматора через конечные множества ЛА содержится в §4 главы 3. Если для линейного автомата выполнено разложение (1), то через $C(f)$ обозначим константную часть $\{\mu_0\}$ этого разложения, а для $M \subseteq \mathfrak{L}$ положим: $C(M) = \cup_{f \in M} C(f)$.

Из множества J_2, которое определялось в главе 2, удалим классы, в которых содержится сумматор $x_1 + x_2$, получим множество J',

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

Множество, состоящее из всех ЛА f, для которых $C(f) = 0$, обозначим $\mathfrak{L}_0$.

Теорема 3.4.1. *Пусть $M \not\subseteq \Theta$ для любого Θ,$\Theta \in J' \setminus \{T_1\}$, $|M| < \infty$,*

$$C(M) = \{\gamma_1, \gamma_2, \ldots, \gamma_s\},$$

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

Условия 1-4 эквивалентны.

1. *Найдутся β_1, β_2, $\ldots$, β_s из $K^{(1)}(U(M))$,*

$$\sum_{i=1}^{s} \beta_i \gamma_i = 0^\infty$$

и

$$\left| \left\{ \ i \ \mid \ \beta_i \in 1 + \xi \mathfrak{L}_0^{(1)}, \ \ i = 1, 2, \ldots, k \ \right\} \right|$$

нечетно.

2.

$$(K(M) \cap \mathfrak{L}_0) \setminus V_2 \neq \emptyset.$$

3.

$$0 \in K(M).$$

4.

$$x_1 + x_2 \in K(M).$$

Теорема 3.4.2. *Существует алгоритм, проверяющий для любой пары конечных множеств M, M_1, $\quad M \subset \mathfrak{L}, \quad M_1 \subset \mathfrak{L}, \quad$ справедливо ли включение:*

$$M_1 \cup \{x_1 + x_2\} \subseteq K(M).$$

В теореме 3.4.3 получена структура константных частей конечнопорожденных K-замкнутых классов, содержащих трехместный сумматор в замыкании в каждом из двух случаев, выделенных в теореме 3.2.1.

В четвертой главе при некоторых естественных ограничениях решены задачи A-выразимости в $\mathfrak{L}$.

В §1 главы 4 рассматривается задача $A^{(1)}$-выразимости в классе $\mathfrak{L}_0^{(1)}$. Для $\mu \in \xi\mathfrak{L}_0^{(1)} \setminus \{0\}$ через $E_2[\mu]$ будем обозначать кольцо многочленов с коэффициентами из E_2, в которых μ является переменной. Класс одноместных ЛА, которые могут быть построены из сумматора и автомата μ с использованием операций композиции, мы обозначаем $\mathfrak{L}_0^{(1)}(\mu)$.

Теорема 4.1.1. *Для любого M,*

$$M \subseteq \mathfrak{L}_0^{(1)}, \;\; M \setminus E_2 \neq \emptyset,$$

найдется μ, $\mu \in \xi\mathfrak{L}_0^{(1)}$, $\mu \neq 0$, найдется целое неотрицательное число k' и найдется множество многочленов M', $M' \subset E_2[\mu]$, степень каждого из которых меньше k', такие, что выполнено равенство

$$A^{(1)}(M) = M' + \mu^{k'}\mathfrak{L}_0^{(1)}(\mu). \tag{4}$$

Линейные автоматы из $\mathfrak{L}_0^{(1)}$, которые могут быть заданы суммой ряда степеней некоторого μ, $\mu \in \xi\mathfrak{L}_0^{(1)}$, с коэффициентами из E_2, составляют множество $R_2(\mu_0) \cap \mathfrak{L}_0^{(1)}$.

Теорема 4.1.2. *Пусть $\mu_0 \in \xi\mathfrak{L}_1^0 \setminus \{0\}$. Для ЛА $\mu \in \xi\mathfrak{L}_1^0 \setminus \{0\}$ соотношение*

$$R_2(\mu_0) \cap \mathfrak{L}_0^{(1)} = \mathfrak{L}_0^{(1)}(\mu)$$

выполнено в точности тогда, когда μ – дробь минимальной степени такая, что имеют место следующие два свойства.

1.
$$\mu_0 \in \mathfrak{L}_1^0(\mu),$$

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

Теорема 4.1.3. *Существует алгоритм, проверяющий по данным μ' и M, $\mu' \in \mathfrak{L}_1^0$, $M \subset \mathfrak{L}_1^0$, $|M| < \infty$, справедливость соотношения*

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

Теорема 4.1.4. *Любое $A^{(1)}$-замкнутое множество M, $M \subseteq \mathfrak{L}_1^0$, является конечнопорожденным. Число $A^{(1)}$-замкнутых множеств в $\mathfrak{L}_1^0$ счетно.*

Подмножество $\mathfrak{L}$ называется S-системой, если $M \setminus V_1 \neq \emptyset$ и $\mathfrak{L}_c \subset A(M)$. В параграфе 2 главы 4 рассматриваются вопросы A-выразимости через S-системы.

Теорема 4.2.1. *Пусть M является S-системой. Тогда включение $f \in A(M)$ выполнено в точности тогда, когда*

$$U(f) \subseteq A^{(1)}(U(M)).$$

Теорема 4.2.2. *Задача A-выразимости через конечные S-системы алгоритмически разрешима.*

Автомат из множества $\mathfrak{L} \setminus V_1$ называется существенным. В §3 главы 4 получен критерий выразимости констант для множества ЛА, содержащего существенный автомат. Этот критерий позволяет для конечного множества ЛА определять, является ли оно S-системой.

Пусть $M \subset \mathfrak{L}$, $U(M) \nsubseteq E_2$. Тогда существует наибольшее натуральное число r_0 такое, что для любого μ, $\mu \in U(M)$, выполнено:

$$\mu + \mu(0) \in \xi^{r_0}\mathfrak{L}_0^{(1)}.$$

Число r_0 мы называем 1-глубиной множества M. Если для линейного автомата f имеет место разложение (1) и $\mu_0 = \sum_{t=0}^{\infty} a_0(t)\xi^t$, то через $V^{(r_0)}(f)$ мы обозначаем вектор $(b, a_0, a_1, \ldots, a_{r_0-1})$, где $b = 0$, если f имеет нечетное число непосредственных переменных, и $b = 1$, в противном случае. Для множества M ЛА полагаем:

$$V^{(r_0)}(M) = \bigcup_{f \in M} \left\{ V^{(r_0)}(f) \right\}.$$

Замыкание множества $\hat{V}$ векторов из $E_2^{r_0+1}$ по операции сложения обозначим $S(\hat{V})$.

Теорема 4.3.1. *Пусть $M \subseteq \mathfrak{L}$, M содержит существенный ЛА и $U(M) \nsubseteq E_2$. Множество $A(M)$ содержит все константы (т.е. $\mathfrak{L}_c \subseteq A(M)$) в точности тогда, когда $S(V^{(r_0)}(M)) = E_2^{r_0+1}$, где через r_0 обозначена 1-глубина множества M.*

Теорема 4.3.2. *Задача проверки, является ли конечное множество ЛА S-системой, алгоритмически разрешима.*

В §4 главы 4 получены некоторые достаточные условия, обеспечивающие возможность проверки A-выразимости через заданное конечное множество ЛА.

Множество ЛА называется S_0-системой, если оно содержит существенный ЛА, а в его K-замыкание входит нулевая константа. Множество M ЛА называется вырожденным, если $U(M) \subseteq E_2$.

Замыкание по операции сложения множества C констант из $\mathfrak{L}_c$ мы обозначаем $\Sigma(C)$.

Теорема 4.4.1. *Пусть M - конечная вырожденная S_0-система и*

$$f(x_1, x_2, \dots, x_n) \in \mathfrak{L}.$$

Включение $f(x_1, x_2, \dots, x_n) \in A(M)$ выполнено в точности тогда, когда

1. *$U(f) \subseteq E_2$ и*

2. *$C(f) \subseteq \Sigma(C(M))$.*

Пусть $f \in \mathfrak{L}$. Отбрасывая первую компоненту вектора $V^{(T_0)}(f)$, получим $\tilde{V}^{(T_0)}(f)$. Для $M \subseteq \mathfrak{L}$ положим

$$\tilde{V}^{(T_0)}(M) = \bigcup_{f \in M} \left\{ \tilde{V}^{(T_0)}(f) \right\}.$$

Теорема 4.4.2. *Пусть конечное множество M таково, что для некоторого T_0 выполнено:*

$$\xi^{T_0} \cdot \mathfrak{L}_c \subseteq A(M).$$

Тогда включение $f \in A(M)$ равносильно выполнению следующих двух свойств.

1. *$U(f) \subseteq A^{(1)}(U(M))$,*

2. *$\tilde{V}^{(T_0)}(f) \in \tilde{V}^{(T_0)}(A(M))$.*

Теорема 4.4.3. *Для конечной невырожденной S_0-системы M и ЛА f проверка включения*

$$\tilde{V}^{(T_0)}(f) \in \tilde{V}^{(T_0)}(A(M))$$

алгоритмически разрешима.

Элемент μ, $\mu \in \xi\mathfrak{L} \setminus \{0\}$, удовлетворяющий равенству (4) для некоторого множества M, $M \subseteq \mathfrak{L}_0^{(1)}$, называется A-основанием множества M.

Теорема 4.4.4. *Пусть M - конечная невырожденная S_0-система, μ_0 является A-основанием $U(M)$, $\mu_0 = \xi^2 + \xi^3\mu'$, для некоторого μ', $\mu' \in \mathfrak{L}_0^{(1)}$. Тогда задача A-выразимости через множество M алгоритмически разрешима.*

В §5 главы 4 показано существенное различие операторов замыкания K и A.

Теорема 4.5.1. *Пусть* $\mu \in \xi\mathfrak{L}_0^{(1)} \setminus \{0\}$*. Равенство* $K(M) = A(M)$ *имеет место для любого* M *со свойствами*

$$M \subseteq \mathfrak{L},\ \ x_1 + x_2 \in K(M),\ \ U(M) \setminus E_2 \neq \emptyset,$$

и с основанием μ *в точности тогда, когда* $\mu \notin M_i^{(1)}$, $i = 0, 2, 3, \ldots$

В заключительном, шестом параграфе главы 4 показана конечнопорожденность невырожденных A-замкнутых классов, содержащих сумматор.

Теорема 4.6.1.

1. *Если для множества* M *имеют место свойства*

$$M \subseteq \mathfrak{L},\ \ x_1 + x_2 \in A(M),\ \ U(M) \setminus E_2 \neq \emptyset \tag{5}$$

   то $A(M)$ *является* A*-конечнопорожденным.*

2. *Множество, состоящее из всех* A*-замкнутых классов* M*, удовлетворяющих свойствам (5), счетно.*

Глава 5 содержит два параграфа, решаемая в каждом из которых задача, использует технику, разработанную в предыдущих главах.

В §1 этой главы множество ЛА $\mathfrak{L}$ рассматривается вместе с операциями суперпозиции, включающими переименование переменных, их отождествление и подстановку. Имея ввиду эти операции, мы используем понятия S-замыкания, S-полного множества, S-замкнутого класса, S-предполного класса и S-критериальной системы. В $\mathfrak{L}$ найдены все S-предполные классы, выполнено сравнение оператора S-замыкания с рассмотренными в предыдущих главах операторами A- и K-замыкания.

Пусть

$$\tilde{M}_i = \left\{\ f\ \mid\ U(f) \subset \tilde{M}_i^{(1)}\ \right\},$$

$i = 0, 2, 3, \dots$, и

$$J_2^S = \left\{ \; T_0, T_1, V_1, V_2, M_1, \tilde{M}_i \;\mid\; i = 0, 2, 3, \dots \; \right\}.$$

Теорема 5.1.1. *Множество J_2^S является приведенной S-критериальной системой в $\mathfrak{L}$, состоящей из S-предполных классов.*

Теорема 5.1.2. *Каждый A-предполный класс в $\mathfrak{L}$ является S-предполным и K-предполным. В $\mathfrak{L}$ каждый K-предполный класс содержится в некотором S-предполном классе и любой S-предполный класс из $J_2^S \setminus J_2^A$ содержит ровно три K-предполных класса из $J_2 \setminus J_2^A$.*

Теорема 5.1.3. *Пусть $\rho \in \{A, K\}$. Множество, состоящее из всех ρ-замкнутых классов, содержащих сумматор и константные ЛА, счетно. Множество, состоящее из всех S-замкнутых классов, содержащих сумматор и константные ЛА, континуально.*

Теорема 5.1.4. *В классе $\mathfrak{L}$ любое подмножество, не являющееся S-полным, расширяется до S-предполного класса.*

В §2 главы 5 найдены все K-предполные классы в классе L_2 линейных 2-адических автоматов, вычисляющих линейные функции от переменных, принимающих значения из кольца $\mathbb{Z}_{(2)}$ целых 2-адических чисел, с рациональными коэффициентами, знаменатели которых нечетны.

Множество всех коэффициентов при переменных в разложении

$$f\left(x_1, x_2, \dots, x_n\right) = \sum_{i=1}^{n} r_i x_i + r_0 \tag{6}$$

для линейного 2-адического автомата f обозначим $\tilde{U}(f)$. Рациональные числа мы будем задавать несократимыми дробями.

Переменная автомата из L_2 является непосредственной, если числитель соответствующего ей коэффициента – нечетное число. Через $\tilde{V}_1$ обозначим множество автоматов из L_2, имеющих не более одной непосредственной переменной, а через $\tilde{V}_2$ — имеющих нечетное число непосредственных переменных.

Множество всех автоматов из L_2, сохраняющих в начальный момент времени элемент a множества E_2, обозначим $\tilde{T}_a$. Множество всех автоматов из L_2, для коэффициентов разложения (6) которого выполнено неравенство $\sum_{i=1}^{n} |r_i| \leq 1$, обозначим $\tilde{I}$.

Все простые числа упорядочим по возрастанию: $\tilde{p}_1, \tilde{p}_2, \ldots$. Поэтому $\tilde{p}_1 = 2$. Множество $\tilde{R}_i^e$ состоит из всех автоматов с не более чем одной существенной переменной из L_2, знаменатель коэффициента при существенной переменной которого не делятся на $\tilde{p}_i$, а также всех элементов L_2, числители коэффициентов при переменных которых делятся на $\tilde{p}_i$.

Множество $\tilde{R}_i^d$ состоит из всех автоматов, знаменатель коэффициента которой при единственной непосредственной переменной не делятся на $\tilde{p}_i$, а числители остальных коэффициентов при переменных делятся на $\tilde{p}_i$.

$$J_2^L = \left\{ \ \tilde{T}_0, \tilde{T}_1, \tilde{V}_1, \tilde{V}_2, \tilde{I}, \tilde{R}_i^e, \tilde{R}_i^d \ \mid \ i = 2, 3, \ldots \ \right\}$$

Теорема 5.2.1. *Для любого Θ, $\Theta \in J_2^L$, выполнено*

$$K(\Theta) = \Theta.$$

Для любых различных Θ_1 и Θ_2 из J_2^L выполнено

$$\Theta_1 \not\subseteq \Theta_2.$$

Автомат f из L_2 называется однородным, если для его разложения (6) выполнено: $r_0 = 0$. Множество всех однородных автоматов из L_2 обозначим L_2^0. Положим:

$$J_2^{L^0} = \left\{ \ \Theta \cap L_2^0 \ \mid \ \Theta \in \ J_2^L \setminus \left\{ \tilde{T}_0, \tilde{T}_1 \right\} \ \right\},$$

Теорема 5.2.2. *Множество $J_2^{L^0}$ является K-критериальной системой в L_2^0.*

Теорема 5.2.3. *Множество J_2^L является приведенной K-критериальной системой в L_2, состоящей из K-предполных классов.*

Теорема 5.2.4. *Задача проверки K-полноты конечных систем из L_2 алгоритмически разрешима.*

Глава 1

Постановка задач, вспомогательные классы

1.1. Линейный автомат, операции композиции

Пусть k — натуральное число, большее 1. Через $R_k(\xi)$ обозначим множество формальных степенных рядов переменной ξ с коэффициентами из E_k,

$$E_k = \{ \ 0, \ 1, \dots, k-1 \ \} .$$

Конечный инициальный автомат с n входами и одним выходом [42], входным алфавитом E_k^n и выходным алфавитом E_k, определяет отображение из $R_k(\xi)^n$ в $R_k(\xi)$ в следующем смысле. Каждую бесконечную последовательность α, $\alpha = \mathbf{a}(0), \mathbf{a}(1), \dots$, векторов $\mathbf{a}(t)$, $\mathbf{a}(t) = (a_1(t), a_2(t), \dots, a_n(t))$, из E_k^n этот автомат преобразует в бесконечную последовательность β, $\beta = b(0), b(1), \dots$, из элементов множества E_k. Ряд $\sum_{t=0}^{\infty} a_i(t)\xi^t$ обозначим через $\alpha_i(\xi)$, $i = 1, 2, \dots, n$, а через $\beta(\xi)$ обозначим ряд $\sum_{t=0}^{\infty} b(t)\xi^t$. Тогда и получаем отображение из $R_k(\xi)^n$ в $R_k(\xi)$, которое определяет рассматриваемый автомат. При этом будем говорить, что рассматривается конечный автомат над множеством E_k.

Нам потребуются множества E_k, которые образуют поле по операциям сложения и умножения. Это возможно, как известно [47], когда число k является степенью простого числа, то есть найдется простое число p и найдется натуральное число m такие, что $k = p^m$.

Рассматривая сумматор в поле E_k с двумя входами, мы получаем отображение $x_1 + x_2$ из $R_k(\xi)^2$ в $R_k(\xi)$, где переменные x_i принимают значения из $R_k(\xi)$, а суммируются элементы рядов с одинаковыми степенями. Автомат $a \cdot x$, умножающий каждый коэффициент ряда на некоторый элемент a поля E_k, называем усилителем [29]. Задержка $\xi_a(x)$ с начальным состоянием a, $a \in E_k$, осуществляет отображение $\xi x + a$.

Сумматор, усилители и задержки являются линейными автоматами (ЛА)

[29]. Над ЛА будем выполнять операции композиции [42]: переименования переменных, отождествления переменных, подстановки и обратной связи. Пусть имеются два ЛА $f_1(x_1, x_2, \ldots, x_{n_1})$ и
$f_2(x_{n_1+1}, x_{n_1+2}, \ldots, x_{n_1+n_2})$, $f_i : R_k(\xi)^{n_i} \to R_k(\xi)$, $i = 1, 2$.

1. Операция переименования переменных. Пусть переменные x'_1, x'_2, $\ldots$, x'_{n_1} различны. Подставляя их соответственно вместо переменных x_1, x_2, $\ldots$, x_{n_1} ЛА f_1, получим ЛА $f_3\left(x'_1, x'_2, \ldots, x'_{n_1}\right)$.

2. Операция отождествления переменных. Из $f_1(x_1, x_2, \ldots, x_{n_1})$ отождествлением переменных x_{n_1-1} и x_{n_1} получим ЛА $f_4(x_1, x_2, \ldots, x_{n_1-1})$.

3. Операция подстановки. Подстановкой ЛА $f_1(x_1, x_2, \ldots, x_{n_1})$ вместо переменной $x_{n_1+n_2}$ ЛА $f_2(x_{n_1+1}, x_{n_1+2}, \ldots, x_{n_1+n_2})$ получим ЛА
$f_5(x_1, x_2, \ldots, x_{n_1+n_2-1})$.

4. Операция обратной связи. Если к переменной x_{n_1} ЛА f_1 применима операция обратной связи, то, выполнив эту операцию, получим ЛА $f_6(x_1, x_2, \ldots, x_{n_1-1})$.

Операции 1-3, в соответствии с [42], называем в дальнейшем операциями суперпозиции.

Замыкая множество B, $B = \{\ x_1 + x_2, a \cdot x, \xi_a(x)\ \mid\ a \in E_k\ \}$, по операциям композиции, получаем класс ЛА над полем E_k [29], который обозначим $\mathfrak{L}_k$.

На множестве $R_k(\xi)$ мы уже ввели операцию сложения, умножали также ряды на переменную ξ и на элементы поля. Операция умножения определяется естественным образом для любой пары рядов из $R_k(\xi)$. Определим операцию деления на ряд, у которого свободный член не равен нулю. Пусть $\alpha_i \in R_k(\xi)$, $i = 1, 2$ и $\alpha_2(0) \neq 0$. Результатом деления α_1 на α_2 назовем такой ряд α, что $\alpha \cdot \alpha_2 = \alpha_1$. Нетрудно видеть, что ряд α существует и единственен.

Таким образом, кольцо $R_k(\xi)$ содержит подкольцо $E'_k(\xi)$,

$$E'_k(\xi) = \left\{\ \frac{u}{v}\ \mid\ u, v \in E_k[\xi],\ \ v(0) \neq 0\ \right\},$$

где через $E_k[\xi]$ обозначено множество многочленов переменной ξ с коэффициентами из E_k.

Лемма 1.1.1. *Пусть для ЛА f_1 и f_2 выполнены равенства:*

$$f_1\left(x_1, x_2, \ldots, x_{n_1}\right) = \sum_{i=1}^{n_1} \mu_i x_i + \mu_{0,1}, \tag{1.1}$$

$$f_2\left(x_{n_1+1}, x_{n_1+2}, \ldots, x_{n_1+n_2}\right) = \sum_{i=1}^{n_2} \mu_{n_1+i} x_{n_1+i} + \mu_{0,2}, \tag{1.2}$$

где $\mu_i \in E_k'(\xi)$, $i = 1, 2, \ldots, n_1+n_2$, и $\mu_{0,i} \in E_k'(\xi)$, $i = 1, 2$, а ЛА f_j, $j = 3, 4, 5, 6$, построены из f_1 и f_2 так, как при определении операций композиции. Тогда имеют место равенства:

$$f_3\left(x_1', x_2', \ldots, x_{n_1}'\right) = \sum_{i=1}^{n_1} \mu_i x_i' + \mu_{0,1}, \tag{1.3}$$

$$f_4\left(x_1, x_2, \ldots, x_{n_1-1}\right) = \sum_{i=1}^{n_1-2} \mu_i x_i + \left(\mu_{n_1-1} + \mu_{n_1}\right) x_{n_1-1} + \mu_{0,1}, \tag{1.4}$$

$$f_5\left(x_1, x_2, \ldots, x_{n_1+n_2-1}\right) = \sum_{i=1}^{n_1} \mu_i \mu_{n_1+n_2} x_i + \sum_{i=n_1+1}^{n_1+n_2-1} \mu_i x_i + \mu_{0,1}\mu_{n_1+n_2} + \mu_{0,2}, \tag{1.5}$$

$$f_6\left(x_1, x_2, \ldots, x_{n_1-1}\right) = \sum_{i=1}^{n_1-1} \frac{\mu_i}{1-\mu_{n_1}} x_i + \frac{\mu_{0,1}}{1-\mu_{n_1}} \tag{1.6}$$

Доказательство. Равенства (1.3), (1.4), (1.5) непосредственно вытекают из (1.1), (1.2) и определения соответствующих операций. Докажем равенство (1.6).

Нетрудно видеть, что операция обратной связи применима к переменной x_{n_1} ЛА f_1 в точности тогда, когда $\mu_{n_1}(0) = 0$. Пусть последнее равенство выполнено. Имеет место:

$$f_1\left(x_1, x_2, \ldots, x_{n_1}\right) = \left(\sum_{i=1}^{n_1-1} \mu_i x_i + \mu_{0,1}\right) + \mu_{n_1} x_{n_1},$$

поэтому ЛА $f_1\left(x_1, x_2, \ldots, x_{n_1}\right)$ является результатом подстановки ЛА $\sum_{i=1}^{n_1-1} \mu_i x_i + \mu_{0,1}$ вместо переменной x ЛА g, $g\left(x, x_{n_1}\right) = x + \mu_{n_1} x_{n_1}$. Применив операцию обратной связи к переменной x_{n_1} ЛА g, получим ЛА $h(x)$, для которой справедливо равенство:

$$f_6\left(x_1, x_2, \ldots, x_{n_1-1}\right) = h\left(\sum_{i=1}^{n_1-1} \mu_i x_i + \mu_{0,1}\right). \tag{1.7}$$

Докажем, что ЛА $h'(x)$, $h'(x) = x - \mu_{n_1} x$ удовлетворяет равенству:

$$h(h'(x)) = x. \tag{1.8}$$

Обрабатывая последовательно коэффициенты ряда $\sum_{t=0}^{\infty} a(t)\xi^t$, автомат h' переходит последовательно в состояния $\mathbf{q}_0$, $\mathbf{q}_1$, $\ldots$, а на выходе этого автомата получаем последовательность $b(0)$, $b(1)$, $\ldots$. В момент времени $t = 0$ автоматы h и h', входящие в $h(h'(x))$, имеют одно и то же состояние $\mathbf{q}_0$. В этот момент вход автомата h' и выход автомата h имеют одно и то же значение $a(0)$, поэтому h' и h переходят в одно и то же состояние $\mathbf{q}_1$. На выходе автомата $h(h'(x))$ при $t = 0$ будет значение $a(0)$. Проводя индукцию по значению параметра t, убеждаемся, что для каждого его значения состояния автоматов h и h', входящих в $h(h'(x))$, будут совпадать, на вход h' подается значение $a(t)$, которое получается и на выходе $h(h'(x))$. Таким образом, равенство (1.8) справедливо.

Следовательно, для любого значения x выполнены равенства:
$h\left(\left(1 - \mu_{n_1}\right) x\right) = x$ и $\frac{1}{1-\mu_{n_1}}\left(1 - \mu_{n_1}\right) x = x$. Ввиду равенства
$\left(1 - \mu_{n_1}\right) R_k = R_k$, получаем:

$$h(x) = \frac{1}{1 - \mu_{n_1}} x.$$

Из равенства (1.7), применяя доказанное ранее, получаем (1.6).

Лемма доказана.

Из леммы 1.1.1 непосредственно вытекает следующая теорема.

Теорема 1.1.1. [29] *Для каждого f, $f \in \mathfrak{L}_k$, от переменных x_1, x_2, $\ldots$, x_n найдутся элементы μ_i, $i = 0, 1, 2, \ldots, n$, кольца $E'_k(\xi)$, что выполнено равенство:*

$$f\left(x_1, x_2, \ldots, x_n\right) = \sum_{i=1}^{n} \mu_i x_i + \mu_0. \tag{1.9}$$

Выполнено также утверждение обратное к доказанному.

Теорема 1.1.2. [29] *Для любых элементов μ_i кольца $E'_k(\xi)$, $i = 0, 1, 2, \dots, n$ найдется ЛА f, для которого выполнено разложение (1.9).*

Доказательство. Пусть заданы μ_i, $\mu_i \in E'_k(\xi)$, $i = 0, 1, 2, \dots, n$. Исходя из обратимости ненулевых элементов поля, каждую дробь μ_i можно представить в виде: $\mu_i = \frac{u_i}{1-v_i}$, где $v_i(0) = 0$, $i = 0, 1, 2, \dots, n$. Нетрудно видеть, что ЛА $u_i x$ и $v_i x$ можно построить при помощи операций суперпозиции из сумматоров, усилителей и задержек с нулевым начальным состоянием.

Далее, для каждого i, $i = 0, 1, \dots, n$, подставляя вместо переменной x_i сумматора $x_i + x$ ЛА $u_i x_i$, а вместо переменной x этого сумматора ЛА $v_i x$, и, применяя операцию обратной связи к переменной x полученных ЛА, имеем ЛА $g_i(x_i)$, $g_i(x_i) = \mu_i x_i$. С использованием сумматора и этих ЛА получим следующий ЛА:

$$h\left(x, x_1, x_2, \dots, x_{n_1}\right) = \mu_0 x + \sum_{i=1}^{n} \mu_i x_i.$$

Автомат $g(x)$,

$$g(x) = \xi_1(\underbrace{x + x + \cdots + x}_{p \text{ раз } x})$$

реализует константу 1. Поэтому ЛА f, $f = h\left(g(x), x_1, x_2, \dots, x_n\right)$, удовлетворяет равенству (1.9) и содержится в $\mathfrak{L}_k$.

Теорема доказана.

На множестве $\mathfrak{L}_k$ ЛА будем рассматривать три оператора замыкания, которые определены в работе [42]:

1. Оператор замыкания по операциям суперпозиции, S-замыкание. В этом случае для множества M, $M \subseteq \mathfrak{L}_k$, через $S(M)$ будем обозначать множество всех ЛА, которые можно получить из элементов множества M применением (многократным) операций суперпозиции.

2. Оператор аппроксимационного замыкания, A-замыкание. Понятие A-замыкания было введено в работе [17]. Для того, чтобы ввести это понятие, на входы линейного автомата будем подавать последовательности α, $\alpha = \mathbf{a}(0), \mathbf{a}(1), \ldots, \mathbf{a}(\tau - 1)$, длины τ. На выходе автомата при этом будем получать последовательности β, $\beta = b(0), b(1), \ldots, b(\tau - 1)$, то есть будем рассматривать автомат, как преобразователь слов длины τ. Для множества M, $M \subseteq \mathfrak{L}_k$, через $A(M)$ будем обозначать множество всех ЛА f, таких, что для любого натурального τ, $\tau \in \mathbb{N}$, в $S(M)$ найдется ЛА, определяющий с f на словах длины τ одно и то же отображение.

3. Оператор замыкания по операциям композиции, K-замыкание. Этот оператор уже встречался при определении класса $\mathfrak{L}_k$. Его получаем путем добавления к суперпозициям операции обратной связи. При этом для множества M, $M \subseteq \mathfrak{L}_k$, через $K(M)$ будем обозначать множество всех ЛА, получаемых из элементов множества M применением (многократным) операций композиции.

Пусть метасимвол ρ принимает значения S, K или A. В соответствии с [42], множество M, $M \subseteq \mathfrak{L}_k$, называется ρ-полным, если $\rho(M) = \mathfrak{L}_k$, M называется ρ-замкнутым классом, если $\rho(M) = M$. ρ-замкнутый класс M называется ρ-предполным, если $M \neq \mathfrak{L}_k$, но для любого f, $f \in \mathfrak{L}_k \setminus M$, выполнено:

$$\rho\left(M \cup \{f\}\right) = \mathfrak{L}_k.$$

Основной целью настоящей работы является рассмотрение классов ЛА вместе с оператором K-замыкания, но будут получены также некоторые результаты и для двух других операторов (A и S-замыканий). Мы найдем сначала все A-предполные, а затем и все K-предполные классы в $\mathfrak{L}_k$ как для простых k, так и для k, не являющихся простыми.

Множество ρ-замкнутых классов J называем ρ-критериальной системой в $\mathfrak{L}_k$, если для произвольного подмножества M ЛА из $\mathfrak{L}_k$ ρ-полнота множества

M равносильна его не включению в каждый ρ-замкнутый класс системы J. ρ-критериальная система называется приведенной, если, удаляя любой элемент из этой системы, получаем систему, которая не является ρ-критериальной. В дальнейшем для $\rho \in \{A, K\}$ мы найдем в $\mathfrak{L}_k$ приведенную ρ-критериальную систему, которая, что несложно показать, является множеством ρ-предполных классов. В случае $k = 2$ будут найдены все S-предполные классы, множество которых является приведенной S-критериальной системой в $\mathfrak{L}_2$.

1.2. Аппроксимационная полнота

Пусть для ЛА $f(x_1, x_2, \ldots, x_n)$ имеет место равенство (1.9). Переменная x_i этого ЛА называется существенной, если $\mu_i \neq 0$. Мы считаем ЛА равными, если они задают одинаковые отображения на множестве значений существенных переменных. Переменная x_i ЛА $f(x_1, x_2, \ldots, x_n)$ называется непосредственной, если $\mu_i(0) \neq 0$.

Через $U(f)$ обозначим множество

$$\{\ \mu_i \mid i = 1, 2, \ldots, n\ \},$$

а через $C(f)$ обозначим множество с одним элементом:

$$C(f) = \{\ \mu_0\ \}.$$

Для множества M ЛА полагаем:

$$U(M) = \bigcup_{f \in M} U(f),$$

$$C(M) = \bigcup_{f \in M} C(f).$$

В дальнейшем нам понадобятся следующие подмножества ЛА.

$$T_a = \Big\{\ f(x_1, x_2, \ldots, x_n) \mid n \in \mathbb{N},\ f \in \mathfrak{L}_k, \text{ из равенства (1.9) следует } \sum_{i=1}^{n} \mu_i(0) \cdot a + \mu_0(0) = a\ \Big\},$$

где $a \in E_k$.

$$V_1 \;=\; \{\; f\,(x_1,x_2,\ldots,x_n) \;\mid n \in \mathbb{N},\;\; f \in \mathfrak{L}_k, \\ f \text{ имеет не более одной непосредственной переменной } \}\,.$$

$$V_p \;=\; \{\; f\,(x_1,x_2,\ldots,x_n) \;\mid n \in \mathbb{N},\;\; f \in \mathfrak{L}_k, \;\text{ и из} \\ \text{равенства (1.9) следует} \sum_{i=1}^{n} \mu_i(0) = 1 \Bigg\}\,.$$

$$M_1 \;=\; \{\; f\,(x_1,x_2,\ldots,x_n) \;\mid n \in \mathbb{N},\;\; f \in \mathfrak{L}_k, \\ \text{из равенства (1.9) следует } \; \mu_i(\xi) - \mu_i(0) \in \xi^2 \cdot E'_k(\xi),\;\; i = 1,2,\ldots,n \;\}\,.$$

Далее будем определять подмножества $\mathfrak{L}_k$ для случая, когда поле E_k не является простым. В противном случае, предлагаемые построения смысла не имеют.

Разложим число m в произведение различных простых чисел q_s, $s = 1,2\ldots,l$:

$$m = q_1^{r_1} \cdot q_2^{r_2} \ldots q_l^{r_l}. \tag{1.10}$$

Для каждого s, $s = 1,2\ldots,l$, в поле E_k содержится подполе E_{k_s} из $k_s = p^{\frac{m}{q_s}}$ элементов [47]. Это поле является максимальным собственным подполем в E_k, то есть для каждого s, $s = 1,2\ldots,l$, в поле E_k не существует собственного подполя, для которого E_{k_s} было бы собственным подполем. Положим:

$$P_s = \{\; f \;\mid\; f \in \mathfrak{L}_k,\;\; \forall \mu,\;\; \mu \in U(M),\;\text{ выполнено: } \mu(0) \in E_{k_s} \;\}\,.$$

Положим в случае простого k:

$$J_k^A = \{\; T_a,\;\; V_1,\;\; V_p,\;\; M_1 \;\mid\; a \in E_k,\;\; \}\,,$$

и

$$J_k^A = \{\ T_a,\ \ V_1,\ \ V_p,\ \ M_1,\ \ P_s\ \mid\ a \in E_k,\ \ s \in \{1, 2, \ldots, l\}\}$$

в случае k, не являющегося простым.

Лемма 1.2.1. *Каждый элемент множества J_k^A является K-замкнутым классом в $\mathfrak{L}_k$, не совпадающим с $\mathfrak{L}_k$.*

Доказательство. Классы T_a, V_1, V_p, а, в случае, когда k не является простым, еще и P_s, определяются отображениями, осуществляемыми ЛА на элементах поля E_k. Поэтому обоснование K-замкнутости этих классов можно получить, рассмотрев соответствующие функции k-значной логики. Эти классы были рассмотрены в работах [101] и [94].

Докажем K-замкнутость класса M_1. Рассмотрим ЛА f_i, $i = 1, 2, \ldots, 6$, определенные в параграфе 1 первой главы. Пусть $f_i \in M_1$, $i = 1, 2$. Тогда, по определению класса M_1, $\forall \mu \in U(\{\ f_1,\ \ f_2\ \})$ выполнено: $\mu - \mu(0) \in \xi^2 E_k'(\xi)$. Заметим, что, если

$$\mu_i - \mu_i(0) \in \xi^2 E_k'(\xi), \quad i = 1, 2,$$

то

$$\mu_1 + \mu_2 - (\mu_1(0) + \mu_2(0)) \in \xi^2 E_k'(\xi),$$

$$\mu_1 \cdot \mu_2 - \mu_1(0) \cdot \mu_2(0) \in \xi^2 E_k'(\xi).$$

Кроме того, если $\mu_2(0) = 0$, то

$$\frac{\mu_1}{1 - \mu_2} - \frac{\mu_1(0)}{1 - \mu_2(0)} \in \xi^2 E_k'(\xi).$$

Отсюда и из леммы 1.1.1 следует, что для ЛА f_i, $i = 3, 4, 5, 6$, получаемых из f_1 и f_2 применением одной из операций композиции, и

$$\forall \mu \in U(M), \quad M = \{\ f_i\ \mid\ i = 3, 4, 5, 6\ \},$$

выполнено: $\mu - \mu(0) \in E_k'(\xi)$. Поэтому $M \subset M_1$. Таким образом, каждый класс из J_k^A является K-замкнутым.

Неравенство $\Theta \neq \mathfrak{L}_k$ для любого $\Theta \in J_k^A$ следует из определений классов множества J_k^A и теоремы 1.1.2.

Лемма доказана.

Заметим, что $\forall \Theta \in J_k^A$ в соответствующем случае для k, $\forall f \in A(\Theta)$ ЛА f должен быть 2-эквивалентен некоторому ЛА из $K(\Theta)$, то есть должен содержаться в Θ. Отсюда получаем следующее утверждение.

Следствие 1. *Каждый класс системы J_k^A в соответствующем случае для k является A-замкнутым классом.*

ЛА без существенных переменных будем называть константным.

Лемма 1.2.2. *Если множество ЛА M не содержится в классах V_1 и V_p, то замыкание $K(M)$ содержит некоторый константный ЛА.*

Доказательство. Рассмотрим множество M, $M \subseteq J_k^A$, не содержащееся ни в одном из классов V_1 и V_p. Найдется $g_1 \in M \setminus V_1$, $g_1 = g_1(x_1, x_2, \ldots, x_n)$. Не ограничивая общность рассуждений, считаем, что x_1 и x_2 – непосредственные переменные ЛА g_1. Тогда для некоторых μ_i, $i = 0, 1, 2, 3$, и μ'_j, $j = 1, 2$, выполнены равенства:

$$g_1(x_1, x_2, x \ldots, x) = \mu_1 x_1 + \mu_2 x_2 + \mu_3 x + \mu_0,$$

$$g_1(x_1, x, x \ldots, x) = \mu_1 x_1 + \mu'_1 x + \mu_0,$$

$$g_1(x, x_2, x \ldots, x) = \mu_2 x_2 + \mu'_2 x + \mu_0.$$

ЛА $g_1(x_1, x_2, x \ldots, x)$, $g_1(x_1, x, x \ldots, x)$ и $g_1(x, x_2, x \ldots, x)$ обозначим, соответственно, $g_2(x_1, x_2, x)$, $g_3(x_1, x)$ и $g_4(x, x_2)$.

Каждый ненулевой элемент конечного поля имеет конечный порядок. Поэтому найдутся такие натуральные числа T_i, $i = 1, 2$, что $\mu_i^{T_i}(0) = 1$. Используя операцию подстановки, из ЛА g_2, g_3 и g_4 получим ЛА $g_5(x_1, x_2, x)$ такой, что для некоторых μ'_3 и μ'_0 из $E'_k(\xi)$ выполнено:

$$g_5(x_1, x_2, x) = \mu_1^{T_1} x_1 + \mu_2^{T_2} x_2 + \mu'_3 x + \mu'_0.$$

Для ЛА g_6,

$$g_6\left(x_1,\ldots,x_{p+1}\right)=g_5\left(x_1,g_5\left(x_2,\ldots g_5\left(x_p,x_{p+1},x\right),x\right),x\right),$$

найдутся такие элементы $\tilde{\mu}_i$, $i=0,1,\ldots,p+2$, множества $E'_k(\xi)$, что $\tilde{\mu}_0(0)=0$, $\tilde{\mu}_i(0)=1$, $i=1,2\ldots,p+1$, $\tilde{\mu}_{p+2}(0)=0$ и

$$g_6=\sum_{i=1}^{p+1}\tilde{\mu}_i x_i+\tilde{\mu}_{p+2}x+\tilde{\mu}_0.$$

Из соотношения $M\not\subset V_p$ следует, что в M найдется ЛА h такой, что для $h_1(x)$, $h_1(x)=h(x,x,\ldots,x)$, найдутся такие $\hat{\mu}$ и $\hat{\mu}_0$, для которых имеем: $\hat{\mu}(0)\neq 1$,

$$h_1(x)=\hat{\mu}x+\hat{\mu}_0.$$

Обозначим через a элемент $\hat{\mu}(0)$ поля E_k. Найдется натуральное число T, для которого выполнено: $b=a^T\in E_p\setminus\{1\}$. В случае простого k, к примеру, можно взять $T=1$. Тогда r, $r=\frac{1}{1-b}$, также является числом из E_p, для которого выполнено:

$$rb+(p+1)-r=0.$$

Поэтому, подставляя вместо переменных x_1, x_2, $\ldots$, x_r ЛА g_6 ЛА $h_1^T(x)$, а вместо остальных переменных – переменную x, получим ЛА $h_3(x)$, выход которой в начальный момент времени не зависит существенно от переменной x. Применяя к переменной x ЛА $h_3(x)$ операцию обратной связи, получим константный ЛА.

Лемма доказана.

Используя рассуждения из [42], несложно показать, что $\forall M,\ M\subseteq\mathfrak{L}_k$, выполнено:

$$K(M)\subseteq A(M). \tag{1.11}$$

Отсюда получаем следующее утверждение.

Следствие 2. *Если $M\subseteq\mathfrak{L}_k\setminus(V_1\cup V_p)$, то в $A(M)$ содержится некоторый константный ЛА.*

Пусть $\tau \in \mathbb{N}$ и даны два ЛА f_1 и f_2, зависящие от одних и тех же переменных, например, от x_1, x_2, …, x_n,

$$f_i\left(x_1, \dots, x_n\right) = \mu_{i,1}x_1 + \dots + \mu_{i,n}x_n + \mu_{i,0}, \quad i = 1, 2$$

Эти ЛА являются τ-эквивалентными, если для любых многочленов $u_j(\xi)$, $u_j(\xi) \in E_k[\xi]$, $j = 1, 2, \dots, n$ степени которых не превосходят $\tau - 1$, совпадают соответствующие коэффициенты рядов $\sum_{j=1}^{n} \mu_{1,j}u_j + \mu_{1,0}$ и $\sum_{j=1}^{n} \mu_{2,j}u_j + \mu_{2,0}$ при ξ^0, ξ^1, …, $\xi^{\tau-1}$.

Например, ЛА $\left(1 + \xi^2\mu_1\right)x_1 + \left(1 + \xi^2\mu_2\right)x_2 + \xi^2\mu_3$ и $\xi\left(1 + \xi^2\mu_4\right)x + 1 + \xi^3\mu_5$, где $\mu_i \in E'_k(\xi)$, $i = 1, 2, \dots, 5$, соответственно, 2-эквивалентен сумматору от двух переменных и 3-эквивалентен задержке с начальным состоянием 1.

Лемма 1.2.3. *Пусть множество ЛА M не содержится ни в одном классе множества $J_k^A \setminus \{M_1\}$. Тогда $A(M)$ содержит сумматор от $p+1$ переменной:*

$$x_1 + x_2 + \dots + x_{p+1} \in A(M). \tag{1.12}$$

Кроме того, $\forall f$, $f \in \mathfrak{L}_k$, в $K(M)$ содержится ЛА 1-эквивалентный f.

Доказательство. Пусть $M \subseteq \mathfrak{L}_k$, $M \setminus \Theta \neq \emptyset$ для любого $\Theta \in J_k^A \setminus \{M_1\}$. Тогда согласно следствию 2 замыкание $A(M)$ содержит некоторую константу γ.

Сначала докажем включение (1.12). Как в доказательстве леммы 1.2.2, рассмотрим ЛА $g_1\left(x_1, x_2, \dots, x_n\right)$, которая содержится в M и переменные x_1, x_2 которой являются непосредственными. В $E'_k(\xi)$ найдутся такие μ и γ'_0, что для ЛА $g_2\left(x_1, x_2\right)$, $g_2\left(x_1, x_2\right) = g_1\left(g_1\left(\gamma, x_1, \gamma \dots, \gamma\right), g_1\left(x_2, \gamma, \dots, \gamma\right), \gamma \dots, \gamma\right)$ имеет место равенство:

$$g_2\left(x_1, x_2\right) = \mu x_1 + \mu x_2 + \gamma'_0,$$

и при этом $\mu(0) \neq 0$.

Через $h(x)$ обозначим ЛА $g_2(x,\gamma)$. Найдется натуральное число T такое, что $\mu(0)^T = 1$. Тогда для ЛА $h_1(x_1,x_2)$, $h_1(x_1,x_2) = g_2\left(h^{T-1}(x_1), h^{T-1}(x_2)\right)$ и некоторых μ' и γ', выполнены:

$$h_1(x_1,x_2) = \mu' x_1 + \mu' x_2 + \gamma',$$

$\mu'(0) = 1$.

Пусть r таково, что $r \geq \tau$ и для некоторого r', $r' \in \mathbb{N}$, $r = p^{r'}$. Через $h_2(x)$ обозначим ЛА $h_1(x,\gamma)$ и положим:

$$h_3(x_1,x_2) = h_1\left(h_2^{r-1}(x_1), h_2^{r-1}(x_2)\right).$$

Нетрудно видеть, что ЛА

$$h_3\left(h_3\left(h_3\left(x_1,x_2\right),x_3\right),\ldots,x_{p+1}\right)$$

τ – эквивалентен сумматору $x_1 + x_2 + \cdots + x_{p+1}$. Поэтому включение (1.12) доказано.

В M найдется ЛА g, не сохраняющая $\gamma(0)$ в начальный момент времени $t = 0$. Поэтому для константного ЛА γ_1, $\gamma_1 = g(\gamma,\ldots,\gamma)$, имеем: $\gamma_1(0) \neq \gamma(0)$.

Далее, множество

$$\{\ \mu(0)\ \mid\ \mu \in U(M)\ \}$$

порождает E_k по операциям сложения и умножения. Это следует из $M \not\subseteq V_1$ в случае простого поля E_k и из $M \not\subseteq P_s$, $\forall s, s \in \{1,2,\ldots,l\}$, в противном случае. Отсюда, из леммы 1.2.2 и включения (1.12) следует, что с использованием операций суперпозиции для некоторого элемента b поля E_k такого, что

$$\tilde{r} = \frac{\gamma_1(0)}{b\left(\gamma(0) - \gamma_1(0)\right)} \in E_p,$$

и некоторых дробей $\tilde{\mu}$ и $\tilde{\gamma}$ из элементов множества M можно получить ЛА

$$\tilde{g}(x) = \tilde{\mu} x + \tilde{\gamma},$$

и при этом $\tilde{\mu}(0) = b$.

Подставим $\tilde{g}\,(\gamma)$ вместо переменных x_1, x_2, $\ldots$, $x_{p-\tilde{r}}$ сумматора $x_1 + x_2 + \cdots + x_{p+1}$, вместо переменных $x_{p-\tilde{r}+1}$, $x_{p-\tilde{r}+1}$, $\ldots$, x_p этого сумматора подставим $\tilde{g}\,(\gamma_1)$, а вместо переменной x_{p+1} подставим константный ЛА γ_1. Получим константный ЛА γ_0 такой, что $\gamma_0(0) = 0$.

Для любого элемента a поля E_k, как указывалось выше, в $K(M)$ содержится некоторый ЛА $\mu_a x + \gamma_a$ такой, что $\mu_a(0) = a$. Тогда ЛА $\mu_a(x)$,

$$\mu_a(x) = (\mu_a x + \gamma_a) + \underbrace{(\mu_a\gamma_0 + \gamma_a) + \cdots + (\mu_a\gamma_0 + \gamma_a)}_{p-1 \text{ раз } \mu_a} + \gamma_0$$

1-эквивалентен усилителю ax и содержится в $K(M)$.

Рассмотрим ЛА f, $f\,(x_1, \ldots, x_n)$, который в начальный момент реализует функцию $a_1x_1 + a_2x_2 + \cdots + a_nx_n + a_0$ для некоторых a_i, $a_i \in E_k$. Из сумматора $x_1 + x_2 + \cdots + x_{p+1}$, используя операции суперпозиции, построим сумматор от n' переменных, где $n' \geq n + 1$.

И, наконец, получаем ЛА

$$\mu_{a_1}x_1 + \mu_{a_2}x_2 + \cdots + \mu_{a_n}x_n + \mu_b\tilde{\gamma} + \underbrace{\gamma_0 + \cdots + \gamma_0}_{n'-n-1 \text{ раз } \gamma_0},$$

где $\tilde{\gamma}$ константа из $K(M)$такая, что $\tilde{\gamma}(0) \neq 0$. Такая существует, так как ранее показано, что $K(M)$ содержит не менее двух констант, отличающихся значениями в начальный момент времени; $b = \frac{a_0}{\tilde{\gamma}(0)}$.

Таким образом, $\forall f$, $f \in \mathfrak{L}_k$, в $A(M)$ содержится ЛА 1-эквивалентный f. Отсюда и из определения A-замыкания следует последнее утверждение леммы 1.2.3.

Лемма доказана.

Замечание 1. *Функция $f\,(x_1, x_2, \ldots, x_n)$ из E_k^n в E_k называется линейной над полем E_k, если найдутся такие элементы a_0, a_1, $\ldots$, a_n поля E_k, что*

$$f\,(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} a_i x_i + a_0,$$

где операции сложения и умножения определяются полем E_k. Нетрудно видеть, что в начальный момент времени ЛА из $\mathfrak{L}_k$ реализуют линейные функции над полем E_k. В работах [101] и [94] для класса линейных функций над полем E_k построены замкнутые по операциям суперпозиции классы, не содержащиеся в множестве одноместных функций. Доказанная нами лемма 1.2.3 позволяет выделить все максимальные подклассы в классе линейных функций над полем E_k из замкнутых классов, полученных в работах [101] и [94].

Теорема 1.2.1. *Множество J_k^A является приведенной A-критериальной системой в $\mathfrak{L}_k$.*

Доказательство. Если множество M, $M \subseteq \mathfrak{L}_k$, содержится в каком-то из классов Θ системы J_k^A, то по лемме 1.2.1 выполнено: $A(M) \subseteq \Theta \neq \mathfrak{L}_k$, то есть M не является A-полным.

В обратную сторону. Пусть $M \not\subseteq \Theta$, $\forall\Theta, \Theta \in J_k^A$.

По лемме 1.2.2 в $K(M)$ содержится некоторый константный ЛА γ, а из соотношения $M \not\subseteq M_1$ следует, что $\exists g$, $g \in M$, $\exists\mu_1 \in U(g)$, $\mu_1 - \mu_1(0) = \xi\frac{u}{v}$, $u(0) \neq 0$.

Из ЛА g и константного ЛА γ с использованием операции подстановки получим ЛА $g_1(x) = \mu_1 x + \gamma_1$. По лемме 1.2.3 в $A(M)$ содержится сумматор $x_1 + x_2 + \cdots + x_{p+1}$. Для ЛА $g_2(x) = g_1^k(x)$ имеем: $g_2(x) = \mu_2 x + \gamma_2$, $\mu_2 = \mu_1(0) + \xi^p\mu_2'$, для некоторых γ_2 и μ_2' из $E_k'(\xi)$.

Из леммы 1.2.3 и следствия 2, вытекает, что для каждого a, $a \in E_k$, в $A(M)$ содержится константный ЛА γ_a, $\gamma_a(0) = a$. Тогда для некоторых константных ЛА γ_4, γ_0, $\gamma_0(0) = 0$, имеют место соотношения:

$$g_3(x) = g_1(x) + g_2(x) + \gamma_3 + \gamma_0 + \cdots + \gamma_0 = \xi\mu_3 x + \gamma_3', \ \ \mu_3(0) \neq 0, \ \ \gamma_3'(0) = 0.$$

По лемме 1.2.3 $\forall h'(x)$, $h' \in \mathfrak{L}_k$, в $A(M)$ содержится ЛА $h_1'(x)$, 1-эквивалентный этому ЛА. Пусть для некоторого натурального числа τ $\forall h'(x)$, $h' \in \mathfrak{L}_k$, $\exists h_\tau'(x)$,

$h'_\tau(x) \in A(M)$, и ЛА $h'_\tau(x)$ τ-эквивалентен $h'(x)$. В частности, для любой последовательности $\alpha = a_0, a_1, \ldots, a_{\tau-1}$ элементов поля E_k в $A(M)$ есть константный ЛА γ_α, для которого $\gamma_\alpha(t) = a_t$, $t = 0, 1, \ldots, \tau - 1$.

Рассмотрим ЛА $h(x)$ от одной переменной x. Согласно предположению, в $A(M)$ содержится ЛА $h_\tau(x)$, τ-эквивалентный h. Построим ЛА τ+1-эквивалентный h. Для некоторых константных ЛА $\tilde{\gamma}$ и $\tilde{\gamma}_0$, $\tilde{\gamma}_0(t) = 0$, $t = 0, 1, \ldots, \tau - 1$, существующих в $A(M)$ по предположению, для ЛА $g_4(x)$,

$$g_4(x_1, x_2) = h_\tau(x_1) + g_3^\tau(x_2) + \tilde{\gamma} + \underbrace{\tilde{\gamma}_0 + \cdots + \tilde{\gamma}_0}_{p-1 \text{ раз } \tilde{\gamma}_0},$$

выполнены соотношения:

$$g_4(x_1, x_2) = h_\tau(x_1) + \xi^\tau \mu_4(x_2) + \xi^\tau \gamma_4, \quad \mu_4(0) \neq 0$$

Как нетрудно видеть, для некоторых a и b из E_k ЛА $g_4(x, ax+b)$ и ЛА $h(x)$ являются τ+1-эквивалентными. Обозначим через $h_{a,b}(x)$ ЛА из $A(M)$, 1-эквивалентный $ax + b$, который существует по лемме 1.2.3. Тогда ЛА $h(x)$ и $g_4(x, h_{a,b}(x))$ являются $\tau + 1$-эквивалентными.

Таким образом, для любого μ, $\mu \in E'(\xi)$, в $A(M)$ содержится ЛА μx. Например, в $A(M)$ содержится константный ЛА, генерирующий 0 в каждый момент времени. Используя этот ЛА и сумматор $x_1 + x_2 + \cdots + x_{p+1}$ можно получить сумматор от любого заданного числа переменных. Поэтому ЛА с разложением (1.9) получаем, используя сумматор $x_1 + x_2 + \cdots + x_{n+1}$, одноместные ЛА $\mu_i x_i$, $i = 1, 2, \ldots, n$, а также константный ЛА μ_0.

Отсюда и из теоремы 1.1.1 следует утверждение теоремы 1.2.1.

Теорема доказана.

1.3. Класс одноместных ЛА, сохраняющих нулевую последовательность

Здесь мы будем рассматривать кольцо $E'_k(\xi)$ вместе с тремя операциями: сложения, умножения и двуместной операцией, которая определена на паре μ_1, μ_2 элементов из $E'_k(\xi)$, если $\mu_2(0) = 0$. Результат применения этой операции обозначаем $\mathrm{fb}\,(\mu_1, \mu_2)$, который через операцию деления выражается так:

$$\mathrm{fb}\,(\mu_1, \mu_2) = \frac{\mu_1}{1 - \mu_2}.$$

Замыкание множества M, $M \subseteq E'_k(\xi)$, по этим операциям обозначим $K^{(1)}(M)$. Понятия замкнутого класса, полного множества, предполного класса, критериальной системы, приведенной критериальной системы естественно переносятся на множество $E'_k(\xi)$, рассматриваемое вместе с оператором замыкания $K^{(1)}$. Множество M называется $K^{(1)}$-замкнутым классом, если $K^{(1)}(M) = M$, а при $K^{(1)}(M) = E'_k(\xi)$ множество M называется $K^{(1)}$-полным. Целью настоящего параграфа является нахождение максимальных собственных $K^{(1)}$-замкнутых подклассов в $E'_k(\xi)$, то есть $K^{(1)}$-замкнутых классов в $E'_k(\xi)$, не совпадающих с $E'_k(\xi)$ и не содержащихся в других $K^{(1)}$-замкнутых классах, отличных от $E'_k(\xi)$. Такие $K^{(1)}$-замкнутые классы будем называть $K^{(1)}$-предполными, или, в рамках настоящего параграфа, предполными. Множество $K^{(1)}$-замкнутых классов $\tilde{J}^{(1)}$ называется $K^{(1)}$-критериальной системой, если для любого M, $M \subseteq E'_k(\xi)$, $K^{(1)}$-полнота множества M равносильна невключению M ни в один из классов множества $\tilde{J}^{(1)}$. Если, удаляя любой элемент из некоторой $K^{(1)}$-критериальной системы $\tilde{J}^{(1)}$, получаем множество, не являющееся $K^{(1)}$-критериальной системой, то $\tilde{J}^{(1)}$ называется приведенной $K^{(1)}$-критериальной системой. Естественность исследования задачи полноты для этой функциональной системы [41] вытекает из следующего утверждения, доказательство которого следует из леммы 1.1.1.

Лемма 1.3.1. $\forall M, M \subseteq \mathfrak{L}_k$, *выполнено:* $U(K(M)) \subseteq K^{(1)}(U(M))$.

В дальнейшем нам понадобятся следующие подмножества $E'_k(\xi)$.

$$M_0^{(1)} = \left\{ \ \mu \ \mid \ \mu \in E'_k(\xi), \ \ \mu - \mu(0) = \frac{u}{v}, \ \ \deg u < \deg v \ \right\},$$

$$\tilde{M}_0^{(1)} = \left\{ \ \mu \ \mid \ \mu \in E'_k(\xi), \ \ \mu = \frac{u}{v}, \ \ \deg u \le \deg v \right\}.$$

Упорядочим все неприводимые приведенные многочлены из кольца $E_k[\xi]$:

$$p_1, \ \ p_2, \ \ , \dots p_i, \ \ \dots$$

так, что $p_1 = \xi$. Положим далее,

$$M_i^{(1)} = \left\{ \ \mu \ \mid \ \mu \in E'_k(\xi), \ \ \mu - \mu(0) = \frac{u}{v}, \ \ (u, v) = 1, \ \ u \in \xi p_i \cdot E_k[\xi] \ \right\},$$

$i = 1, 2, \dots$.

$$\tilde{M}_i^{(1)} = \left\{ \ \mu \ \mid \ \mu \in E'_k(\xi), \ \ \mu = \frac{u}{v}, \ \ p_i \ \text{ не делит } \ v \ \right\},$$

$i = 2, 3, \dots$.

$$R_0^{(1)} = \left\{ \ \mu \ \mid \ \mu \in E'_k(\xi), \ \ \mu = \frac{u}{v}, \ \ \deg u < \deg v \right\},$$

$$R_i^{(1)} = \left\{ \ \mu \ \mid \ \mu \in E'_k(\xi), \ \ \mu = \frac{u}{v}, \ \ (u, v) = 1, \ \ p_i \ \text{ делит } \ u \ \right\},$$

$i = 1, 2, 3, \dots,$

Если k не является простым, то нам понадобятся такие множества:

$$P_s^{(1)} = \{ \ \mu \ \mid \ \mu \in E'_k(\xi), \ \ \mu(0) \in E_{k_s} \ \},$$

$s = 1, 2, \dots, l$.

Для дроби $\mu \in E'_k(\xi)$, $\mu = \frac{u}{v}$, такой, что выполнено $\deg u \leq \deg v$, найдется число r, $r \in \mathbb{N}$, и найдутся a, a', b, b', u', v', $a, a' \in E_k$, $b, b' \in E_k \setminus \{0\}$, $u', v' \in E_k[\xi]$, $\deg u' < r-1$, $\deg v' < r-1$, такие, что имеет место равенство:

$$\mu = \frac{a + \xi u' + a'\xi^r}{b + \xi v' + b'\xi^r}.$$

Тогда положим:

$$\Psi_0(\mu) = \left(\frac{a}{b}, \frac{a'}{b'}\right). \tag{1.13}$$

Нетрудно видеть, что первая компонента пары из правой части равенства (1.13) совпадает с $\mu(0)$ для соответствующей дроби μ.

Если $M \subseteq \tilde{M}_0^{(1)}$, то

$$\Psi_0(M) = \{\ \Psi_0(\mu)\ \mid\ \mu \in M\ \}.$$

Лемма 1.3.2. *Пусть $i \in \{2, 3, \dots\}$. Для дроби μ такой, что $\mu \in \tilde{M}_i^{(1)}$, найдется многочлен $u' \in E_k[\xi]$ и найдется дробь $\mu' \in E'_k(\xi)$, что*

$$\deg u' < \deg p_i$$

и

$$\mu = u' + p_i \mu'. \tag{1.14}$$

Доказательство. Рассмотрим дробь μ из $\tilde{M}_i^{(1)}$, $\mu = \frac{u}{v}$, где $u, v \in E_k[\xi]$, $(u, v) = 1$. Используя расширенный алгоритм Эвклида, в $E_k[\xi]$ можно найти такие многочлены u_i, $i = 1, 2$, что выполнено равенство:

$$u_1 v + u_2 p_i = 1.$$

Умножая левую и правую часть этого равенства на μ, получаем:

$$\mu = u_1 u + p_i u_2 \mu.$$

Далее, используя формулу для деления с остатком многочлена $u_1 u$ на p_i,

$$u_1 u = u' + p_i u'', \quad \deg(u') < \deg(p_i),$$

получаем нужное разложение:

$$\mu = u' + p_i\left(u'' + u_2\mu\right).$$

Лемма 1.3.2 доказана.

Пусть $i \in \{2, 3, \dots\}$. Введем отображение Ψ_i из множества $\tilde{M}_i^{(1)}$ в $E_k \times E_k[\xi]$, следующим образом. Для дроби μ, $\mu \in \tilde{M}_i^{(1)}$, по лемме 1.3.2 имеет место разложение (1.14). Положим:

$$\Psi_i(\mu) = (\mu(0), u'). \tag{1.15}$$

Если $M \subseteq \tilde{M}_i^{(1)}$, то

$$\Psi_i(M) = \{\ \Psi_i(\mu)\ \mid\ \mu \in M\ \}.$$

Для каждого автоморфизма ω поля E_k определим следующие множества:

$$M_{i,\omega}^{(1)} = \left\{\ \mu\ \mid\ \mu \in \tilde{M}_i^{(1)},\ \ \Psi_i(\mu) = (\mu(0), \omega(\mu(0)))\ \right\},$$

$i = 0, 2, 3, \dots$.

Для тождественного автоморфизма $\omega = \mathrm{id}$ справедливы равенства:

$$M_{i,\mathrm{id}}^{(1)} = M_i^{(1)},\ \ i = 0, 2, 3, \dots$$

Заметим, что простое поле обладает единственным тождественным автоморфизмом. В этом случае для каждого i, $i \in \{0, 2, 3, \dots\}$, вместо $M_{i,\mathrm{id}}^{(1)}$ будем использовать обозначение $M_i^{(1)}$. Известно, что конечное поле E_k, где $k = p^m$, обладает m автоморфизмами [47]. Множество всех автоморфизмов поля E_k обозначим Ω_k.

Положим в случае простого k:

$$J_k^{(1)} = \left\{M_i^{(1)}, R_i^{(1)} | i = 0, 1, \dots\right\}.$$

В противном случае:

$$J_k^{(1)} = \Big\{ M_{i,\omega}^{(1)}, M_1^{(1)}, R_j^{(1)}, P_s^{(1)} \mid \omega \in \Omega_k, i = 0, 2, 3, \dots,$$
$$j = 0, 2, 3, \dots, s = 1, 2, \dots, l, \Big\}.$$

Заметим, что в случае простого поля справедливо включение $R_1^{(1)} \in J_k^{(1)}$, которое не выполнено для случая k, не являющегося простым.

Имеет место следующее утверждение.

Лемма 1.3.3. *Каждый элемент множества $J_k^{(1)}$ является $K^{(1)}$-замкнутым классом в $E'_k(\xi)$, не совпадающим с $E'_k(\xi)$.*

Доказательство. Пусть $\omega \in \Omega_k$ и $\mu_j \in M_{i,\omega}^{(1)}$, $i \in \{0, 2, 3, \dots\}$, $j = 1, 2$. Тогда по определению множества $M_{i,\omega}^{(1)}$ для некоторого a_j, $a_j \in E_k$, имеем:

$$\Psi_i(\mu_j) = (a_j, \omega(a_j)), \;\; j = 1, 2.$$

Отсюда, используя свойства автоморфизма и операций над дробями, получаем:

$$\Psi_i(\mu_1 + \mu_2) = (a_1 + a_2, \omega(a_1 + a_2)) \in M_{i,\omega}^{(1)},$$

$$\Psi_i(\mu_1\mu_2) = (a_1a_2, \omega(a_1a_2)) \in M_{i,\omega}^{(1)}$$

и, если $\mu_2(0) = 0$, то

$$\Psi_i\left(\frac{1}{1-\mu_2}\right) = (1, 1) \in M_{i,\omega}^{(1)}. \tag{1.16}$$

Действительно, при $i = 0$ для некоторых многочленов u' и v' из $E_k[\xi]$ выполнены соотношения:

$$\mu_2 = \frac{\xi u'}{v'},$$
$$\deg(\xi u') < \deg(v').$$

Отсюда получаем равенство

$$\frac{1}{1-\mu_2} = \frac{v'}{v' - \xi u'},$$

из которого следует (1.16).

Если $i \in \{2, 3, \dots\}$, то для некоторого μ' из $\tilde{M}_i^{(1)}$ имеем:

$$\mu_2 = \xi p_i \mu',$$

поэтому

$$\frac{1}{1-\mu_2} = 1 + \frac{\xi p_i \mu'}{1 - \xi p_i \mu'},$$

откуда следует (1.16).

Таким образом, $\mathrm{fb}\,(\mu_1, \mu_2) \in M_{i,\omega}^{(1)}$ как произведение двух элементов множества $M_{i,\omega}^{(1)}$. $K^{(1)}$-замкнутость множества $M_{i,\omega}^{(1)}$ доказана.

Пусть $\mu_j \in M_1^{(1)}$, $j = 1, 2$. Тогда $\mu_j - \mu_j(0) = \xi^2 \frac{u_j}{v_j}$, где $u_j, v_j \in E_k[\xi]$, $(v_j, \xi) = 1$, $j = 1, 2$.

Тогда имеем:

$$\mu_1 + \mu_2 - (\mu_1(0) + \mu_2(0)) = \xi^2 \left(\frac{u_1}{v_1} + \frac{u_2}{v_2} \right) \in M_1^{(1)},$$

$$\begin{aligned} \mu_1\mu_2 - \mu_1(0)\mu_2(0) &= \mu_1 (\mu_2 - \mu_2(0)) + \mu_2(0) (\mu_1 - \mu_1(0)) = \\ &\xi^2 \left(\mu_1 \frac{u_2}{v_2} + \mu_2(0) \frac{u_1}{v_1} \right) \in M_1^{(1)}, \end{aligned}$$

Если к паре μ_1, μ_2 применима операция fb, то $\mu_2(0) = 0$, $\mathrm{fb}(\mu_1, \mu_2) = \mu_1 \frac{1}{1-\mu_2}$ и

$$\frac{1}{1-\mu_2} - \frac{1}{1-\mu_2(0)} = \frac{\xi^2 u_2}{v_2 - \xi^2 u_2} \in M_1^{(1)}.$$

Поэтому $\mathrm{fb}(\mu_1, \mu_2) \in M_1^{(1)}$ ввиду того, что $\mathrm{fb}(\mu_1, \mu_2)$ является произведением двух элементов множества $M_1^{(1)}$, а, как было доказано, операция умножения не выводит из $M_1^{(1)}$.

$K^{(1)}$-замкнутость множества $M_1^{(1)}$ доказана.

Как нетрудно видеть, операции сложения и умножения сохраняют множества $R_i^{(1)}$, $i \in \{0, 1, 2, \dots\}$.

Пусть выполнено: $\mu_j \in R_i^{(1)}$, $\mu_j(\xi) = \frac{u_j}{v_j}$, $j = 1, 2$ и $\mu_2(0) = 0$.

В случае $i = 0$ имеем: $\deg u_2 < \deg v_2$, $u_2(0) = 0$, поэтому $\frac{1}{1-\mu_2} = \frac{v_2}{v_2-u_2}$, $\deg v_2 = \deg (v_2 - u_2)$,

$$\mathrm{fb}\,(\mu_1, \mu_2) = \frac{u_1 v_2}{v_1\,(v_2 - u_2)} \tag{1.17}$$

и $\deg (u_1 v_2) < \deg v_1\,(v_2 - u_2)$. Поэтому $\mathrm{fb}\,(\mu_1, \mu_2) \in R_0^{(1)}$ и $K^{(1)}(R_0^{(1)}) = R_0^{(1)}$.

В случае $i \in \{1, 2, \dots\}$ помимо равенства (1.17) имеем: u_j делится на p_i, а v_j не делится на p_i, $j = 1, 2$. Поэтому $\mathrm{fb}\,(\mu_1, \mu_2) \in R_i^{(1)}$. Таким образом, $R_i^{(1)}$ является $K^{(1)}$-замкнутым для любого i, $i \in \{0, 1, \dots\}$.

$K^{(1)}$-замкнутость множеств $P_s^{(1)}$ по операциям сложения и умножения следует из замкнутости поля E_{k_s} по этим операциям и правил сложения и умножения формальных степенных рядов. Пусть $\mu_j \in P_s^{(1)}$, для некоторого s, $s \in \{1, 2, \dots, l\}$, $j = 1, 2$, и к паре (μ_1, μ_2) применима операция fb. Тогда $\mu_2(0) = 0$ и $\mathrm{fb}\,(\mu_1, \mu_2)\,(0) = \mu_1(0) \in E_{k_i}$. Поэтому операция fb сохраняет множество $P_s^{(1)}$ и $K^{(1)}\left(P_s^{(1)}\right) = P_s^{(1)}$.

Лемма доказана.

Пусть $E_{k'}$ – подполе поля E_k и M – некоторое множество элементов поля $E_k(\xi)$ через $E_{k'}(M)$ будем обозначать подполе поля $E_k(\xi)$, порожденное множеством M по операциям сложения, умножения и деления над полем $E_{k'}$. Если множество M состоит из одной дроби, $M = \{\mu\}$, то вместо $E_{k'}(M)$ мы можем использовать более простое обозначение: $E_{k'}(\mu)$.

Таким образом, мы имеем алгебраический оператор замыкания [42] в поле $E_k(\xi)$, которое является конечнопорожденным. Собственное подполе поля $E_k(\xi)$, не содержащееся ни в каком другом собственном его подполе, будем называть максимальным подполем поля $E_k(\xi)$. Как известно, ввиду конечной порожденности поля $E_k(\xi)$, множество всех максимальных собственных подполей этого поля является критериальной системой. Отсюда следует, что любое подмножество поля $E_k(\xi)$, не порождающее это поле по рассматриваемым операциям, содержится в некотором максимальном подполе.

Нам понадобится следующее достаточное условие полноты в поле $E_k(\xi)$.

Теорема 1.3.1. *Если для заданного множества M, $M \subseteq E'_k(\xi)$, и любого Θ, $\Theta \in J_k^{(1)}$, выполнено: $M \not\subseteq \Theta$, то*

$$E_p(M) = E_k(\xi). \tag{1.18}$$

Для доказательства этой теоремы нам понадобятся некоторые вспомогательные утверждения, которые приводятся далее.

Степенью дроби μ, $\mu = \frac{u}{v}$, из $E_k(\xi)$ будем называть, как принято, число $\deg(\mu)$, равное максимуму из степеней ее числителя и знаменателя, если дробь является несократимой.

Лемма 1.3.4. *Пусть Θ — максимальное подполе в $E_k(\xi)$. Тогда либо для некоторого μ, $\mu \in \xi E'_k(\xi)$, $\mu \neq 0$, выполнено:*

$$\Theta = E_k(\mu), \tag{1.19}$$

либо для некоторого максимального подполя E_{k_s} поля E_k и μ, $\mu \in E'_k(\xi)$, $\deg \mu = 1$, выполнено:

$$\Theta = E_{k_s}(\mu). \tag{1.20}$$

Доказательство. Рассмотрим максимальное подполе Θ в $E_k(\xi)$. Заметим, что

$$\Theta \not\subseteq E_k,$$

так как в противном случае, поле Θ строго содержалось бы в собственном подполе $E_k(\xi^2)$ поля $E_k(\xi)$ и не являлось бы максимальным подполем этого поля.

Если выполняется включение

$$E_k \subset \Theta, \tag{1.21}$$

то по теореме Люрота из [20] поле Θ является простым расширением поля E_k. Поэтому найдется $\mu' \in E_k(\xi) \setminus E_k$, что справедливо равенство (1.19).

Учитывая, что

$$E_k(\mu') = E_k\left(\frac{1}{\mu'}\right), \tag{1.22}$$

не ограничивая общности рассуждений, полагаем:

$$\mu' \in E'_k(\xi).$$

Имеет место равенство:

$$E_k(\mu') = E_k(\mu' - \mu'(0)),$$

поэтому для $\mu = \mu' - \mu'(0)$ выполнены соотношения $\mu \in \xi E'_k(\xi)$, $\mu \neq 0$, а также равенство (1.19).

Теперь рассмотрим случай

$$E_k \not\subset \Theta. \tag{1.23}$$

Простое поле E_p содержится в Θ. Положим:

$$k_0 = \max\{\ k' \mid E_{k'} \subseteq \Theta\ \}, \tag{1.24}$$

Известно [47], что найдется элемент a поля E_k и найдется натуральное число m_0 такие, что $E_p(a) = E_k$ и $k_0 = p^{m_0}$, кроме того, m делится на m_0. Через m_1 обозначим число $m : m_0$.

Из соотношения (1.23) следует, что

$$a \notin \Theta.$$

Поэтому

$$E_p(\Theta \cup \{a\}) = E_k(\xi).$$

Согласно [34], $E_k(\xi)$ является линейным пространством над Θ, порожденным элементами множества A, $A = \{a^0, a, a^2, ..., a^{m_1-1}\}$. Найдем максимальное m_2 такое, что множество M, $M = \{a^0, a, a^2, ..., a^{m_2-1}\}$, является линейно независимым над Θ. Тогда $E_k(\xi)$ является линейным пространством над Θ с базисом M. Отсюда следует равенство:

$$\xi = \sum_{i=0}^{m_2-1} \mu_i \cdot a^i, \tag{1.25}$$

$$\mu_i \in \Theta,\ \ i = 0, 1, \ldots, m_2 - 1.$$

Таким образом, в Θ найдутся μ_i, $i = 0, 1, \ldots, m_2 - 1$, что многочлен

$$z - \sum_{i=0}^{m_2-1} \mu_i \cdot a^i$$

имеет корень $z = \xi$.

Пусть $\mu_i = \frac{u_i}{v_i}$ – несократимые дроби,

$$u_i \in E_k[\xi],\ \ v_i \in E_k[\xi],\ \ i = 0, 1, ..., m_2 - 1.$$

Среди коэффициентов μ_i, $i = 0, 1, \ldots, m_2-1$ найдется такой μ_{i_0}, что $\deg \mu_{i_0} > 0$, иначе ξ, согласно равенству (1.25), содержалось бы в E_k.

Многочлен $\mu_{i_0} \cdot v_{i_0}(z) - u_{i_0}(z)$ переменной z имеет корень $z = \xi$. Нетрудно видеть, что он делится на многочлен $z - \sum_{i=0}^{m_2-1} \mu_i \cdot a^i$, так как в противном случае элементы поля a^0, a^1,..., a^{m_2-1}, были бы линейно зависимы над полем Θ.

Через $\tilde{v}$ обозначим наименьшее общее кратное многочленов v_0, v_1, $\ldots$, v_{m_2-1}.

Многочлен $f(\xi)$, $f(\xi) = u_{i_0}(\xi) \cdot v_{i_0}(z) - u_{i_0}(z) \cdot v_{i_0}(\xi)$ переменной ξ делится на многочлен $g(\xi)$, $g = \tilde{v} \cdot \left(z - \sum_{i=0}^{m_2-1} \mu_i \cdot a^i\right)$ этой же переменной [20]. Поэтому $\deg_\xi(f(\xi)) \geq \deg_\xi(g(\xi))$. С другой стороны, $\deg_\xi(f(\xi)) \leq \deg_\xi(g(\xi))$. Отсюда, $\deg_\xi(f(\xi)) = \deg_\xi(g(\xi))$. Следовательно, для некоторого многочлена $h(z)$, $h(z) \in E_k[z]$, получаем:

$$f(\xi) = h(z) \cdot g(\xi).$$

Разделив многочлен $\mu_{i_0} \cdot v(z) - u(z)$ переменной z на $h(z)$, получим многочлен первой степени от z с коэффициентами из $E_k(\mu_{i_0})$. Отсюда следует, что найдутся такие дроби μ_i', $\mu_i' \in E_{k_0}(\mu_{i_0})$, $i = 0, 1, \ldots, m_1 - 1$, что

$$\xi = \sum_{i=0}^{m_1-1} \mu_i' \cdot a^i. \tag{1.26}$$

По одному из утверждений о конечных алгебраических расширениях, содержащихся в [44], поле $E_k(\mu_{i_0})$ является линейным пространством, которое порождается множеством $\{a^0, a^1, \ldots, a^{m_1-1}\}$ над полем $E_{k_0}(\mu_{i_0})$, а поле $E_k(\xi)$ является линейным пространством над полем $E_k(\mu_{i_0})$, порождаемым множеством $\{\xi^0, \xi^1, \ldots, \xi^{\deg\mu_{i_0}-1}\}$. Следовательно [34], поле $E_k(\xi)$ является линейным пространством над полем $E_{k_0}(\mu_{i_0})$ с порождающим множеством

$$\left\{\ a^i\xi^j \ \mid \ i = 0, 1, \ldots, m_1 - 1,\ \ j = 0, 1, \ldots, \deg\mu_{i_0} - 1 \ \right\}.$$

Поэтому, учитывая равенство (1.26), получаем:

$$E_k\left(\mu_{i_0}\right) = E_k(\xi).$$

С другой стороны, согласно [20], поле $E_k(\xi)$ является алгебраическим расширением поля $E_k\left(\mu_{i_0}\right)$ степени μ_{i_0}. Поэтому

$$\deg\mu_{i_0} = 1.$$

Согласно нашему предположению множество $\left\{a^0, a^1, \ldots, a^{m_1-1}\right\}$ является базисом поля E_k, рассматриваемого как линейное пространство над полем E_{k_0}.

Предположим, что E_{k_0} не является максимальным подполем в E_k.

Если A — линейно независимо над Θ, то размерность $[E_k(\xi) : \Theta]$ линейного пространства $E_k(\xi)$ над Θ не меньше m_1. При этом, для максимального подполя E_{k_s} поля E_k, содержащего E_{k_0}, имеем:

$$\Theta \subset E_{k_s}(\Theta) \neq E_k(\Theta),\ \ \Theta \neq E_{k_s}(\Theta),$$

то есть Θ, вопреки предположению, не является максимальным подполем в $E_k(\xi)$.

Таким образом, A — линейно зависимо над Θ. Поэтому найдутся такие μ_i, $\mu_i \in \Theta$, $i = 0, 1, \ldots, m_1 - 1$, не все равные нулю, такие, что многочлен

$$g(z) = \sum_{i=0}^{m_1-1} \mu_i z^i$$

имеет корень a. Кроме того, ввиду линейной зависимости множества $A \cup \{a^{m_1}\}$ над E_{k_0} найдутся такие, не все равные нулю, μ'_i, $\mu'_i \in E_{k_0}$, $i = 0, 1, \ldots, m_1$, что справедливо равенство:

$$f(a) = \sum_{i=0}^{m_1} \mu_i' a^i = 0.$$

Приведенный наибольший общий делитель многочленов $f(z)$ и $g(z)$ обозначим $\tilde{g}(z)$. Имеют место неравенства:

$$0 \leq \deg \tilde{g}(z) < m_1.$$

Так как многочлен $\tilde{g}(z)$ делит $f(z)$, а многочлен $f(z)$ степени m_1 имеет m_1 корней, a^{p^0}, $a^{p^{m_0}}$, $a^{p^{2m_0}}$, $\ldots$, $a^{p^{(m_1-1)m_0}}$, то все коэффициенты $g(z)$ лежат в поле E_k, а, кроме того, они содержатся в Θ. Все эти коэффициенты не могут содержаться в E_{k_0}, так как A линейно независимо над E_{k_0}.

Поэтому, $\Theta \cap E_k \neq E_{k_0}$. Полученное противоречие означает, что E_{k_0} — максимальное подполе в E_k. Тогда имеет место включение:

$$\frac{m}{m_1} \in \{q_1, q_2, \ldots, q_l\}, \tag{1.27}$$

где q_1, q_2, $\ldots$, q_l, как ранее указывалось, все простые делители числа m. Кроме того,

$$E_{k_0}(\mu_{i_0}) \subseteq \Theta.$$

Пусть $E_{k_0}(\mu_{i_0})$ — собственное подполе поля Θ, тогда, согласно [44], число:

$$[E_k(\xi) : E_{k_0}(\mu_{i_0})] = [E_k(\xi) : \Theta] \cdot [\Theta : E_{k_0}(\mu_{i_0})]$$

не является простым.

С другой стороны,

$$[E_k(\xi) : E_{k_0}(\mu_{i_0})] = \frac{m}{m_1}.$$

Получили противоречие с включением (1.27).

Лемма 1.3.4 доказана.

Доказательство теоремы 1.3.1. Рассмотрим множество M, $M \subseteq E_k'(\xi)$, такое, что для любого Θ, $\Theta \in J_k^{(1)}$, выполнено: $M \not\subseteq \Theta$.

Предположим, что (1.18) не выполнено. В конечнопорожденной алгебре любое множество, не являющееся полным, содержится в некоторой собственной максимальной подалгебре [42]. Поэтому множество M содержится в некотором собственном максимальном подполе Θ поля $E_k(\xi)$. При этом $\Theta \cap E'_k(\xi)$ не содержится ни в одном из классов множества $J_k^{(1)}$.

Пусть имеет место равенство (1.19) для ненулевой дроби μ, $\mu \in \xi \cdot E'_k(\xi)$.

Отсюда следует, что $\Theta \cap E'_k(\xi)$ совпадает с $K^{(1)}\left(\{\mu, E_k\}\right)$.

Действительно, если $\mu' \in K^{(1)}\left(\{\mu, E_k\}\right)$, то $\mu' \in E_k(\mu)$ и $\mu' \in E'_k(\xi)$, то есть, согласно (1.19), имеем:

$$K^{(1)}\left(\{\mu, E_k\}\right) \subseteq \Theta \cap E'_k(\xi). \tag{1.28}$$

С другой стороны, если $\mu' \in \Theta \cap E'_k(\xi)$, то для некоторых взаимно простых многочленов $u'(\xi)$ и $v'(\xi)$ из $E_k[\xi]$ справедливо равенство:

$$\mu' = \frac{u'(\mu)}{v'(\mu)}.$$

При этом $v'(0) \neq 0$, так как в противном случае дробь μ' не содержалась бы в $E'_k(\xi)$. Из результата, приведенного в [29] следует, что для некоторого натурального числа T и некоторого многочлена u'' из $E_k[\xi]$ выполнено:

$$\frac{u'(\xi)}{v'(\xi)} = \mathrm{fb}\left(u''(\xi), \xi^T\right).$$

Поэтому

$$\mu' = \mathrm{fb}\left(u''(\mu), \mu^T\right) \in K^{(1)}\left(\{\mu, E_k\}\right)$$

и

$$\Theta \cap E'_k(\xi) \subseteq K^{(1)}\left(\{\mu, E_k\}\right).$$

Таким образом, с учетом (1.28), доказано равенство:

$$K^{(1)}\left(\{\mu, E_k\}\right) = \Theta \cap E'_k(\xi).$$

Предположим, что $\deg \mu > 1$. Тогда $\mu = \xi \frac{u}{v}$, $u, v \in E_k[\xi]$, $(u, v) = 1$. Если $\deg u \geq 1$, то для некоторого i, $i \in \{1, 2, \dots\}$, получаем включение

$$\Theta \cap E'_k(\xi) \subseteq M_{i,\mathrm{id}}^{(1)},$$

что противоречит предположению. Если $u \in E_k \setminus \{0\}$ и $\deg v = r > 1$, то для некоторых a_1, b_0, b_r из $E_k \setminus \{0\}$ и некоторого $\tilde{v}$, $\tilde{v} \in E_k[\xi]$, $\deg \tilde{v} < r - 1$, имеем:

$$\mu = \xi \frac{a_1}{b_0 + \xi \tilde{v} + b_r \xi^r}.$$

Поэтому

$$\Psi_0(\mu) = (0, 0) \ \text{и} \ \Theta \cap E'_k(\xi) \subseteq M^{(1)}_{0,\mathrm{id}}.$$

Снова получаем противоречие.

Таким образом, $\deg(\mu) = 1$, и, как следует из [44],

$$\Theta = E_k(\mu) = E_k(\xi),$$

что противоречит предположению о том, что Θ — собственное подполе в $E_k(\xi)$.

Для простого k включение $E_k \subseteq \Theta$ справедливо для любого подполя Θ поля $E_k(\xi)$. Следовательно, утверждение теоремы 1.3.1 для этого случая доказано.

Поэтому дальнейшее доказательство теоремы 1.3.1 относится к случаю, когда k не является простым.

Пусть

$$E_k \not\subset \Theta.$$

Тогда по лемме 1.3.4 для некоторой ненулевой дроби μ, $\mu \in E'_k(\xi)$, степени 1 выполнено равенство (1.20).

Тогда умножением числителя и знаменателя дроби μ на один и тот же элемент поля E_k можно добиться того, что для некоторых элементов a, b и c поля E_k имеет место равенство:

$$\mu = \frac{a + b\xi}{1 + c\xi},$$

причем хотя бы один из двух элементов b, c не равен нулю.

Для элемента d поля E_k, не равного нулю и не являющегося корнем знаменателя дроби μ, имеем:

$$\Psi_{i_d}(\mu) = \left(a, \frac{a + bd}{1 + cd}\right),$$

где через i_d обозначен индекс неприводимого многочлена $\xi - d$ в упомянутой ранее последовательности неприводимых приведенных многочленов $p_1, p_2, \ldots$.

Сначала заметим, что

$$ca - b \neq 0. \tag{1.29}$$

Действительно, если это не так, то при $c = 0$ мы получали бы $b = 0$ и, поэтому, $\deg \mu < 1$, что не верно. Если же $c \neq 0$, то $a = b/c$ и дробь μ сократима, и здесь $\deg \mu < 1$.

Как известно [44], поле E_k обладает $(E_k : E_{k_s})$ автоморфизмами сохраняющими поле E_{k_s}. Рассмотрим один из таких автоморфизмов ω, не являющийся тождественным.

Если $c\omega(a) - b \neq 0$, то положим: $d = \frac{a-\omega(a)}{c\omega(a)-b}$. Тогда получаем равенство:

$$\Psi_{i_d}(\mu) = \left(a, \frac{\omega(a)(ca-b)}{ca-b}\right) = (a, \omega(a))$$

и, таким образом,

$$E_{k_s} \cup \{\mu\} \subset M^{(1)}_{i_d,\omega}.$$

Если $c\omega(a) - b = 0$, то $c \neq 0$, иначе выполнялось бы $b = 0$, что противоречило бы равенству $\deg \mu = 1$. Тогда $\frac{b}{c} = \omega(a)$ и

$$E_{k_s} \cup \{\mu\} \subset M^{(1)}_{0,\omega}.$$

Таким образом, в рассматриваемом случае для некоторого i, $i \in \{0, 2, 3, \ldots\}$ и некоторого минимального автоморфизма ω, не являющегося тождественным, выполнено:

$$E_{k_s} \cup \{\mu\} \subset M^{(1)}_{i,\omega}. \tag{1.30}$$

Так как $K^{(1)}(M) \subseteq E_{k_s}(\mu)$, то для всякого $\tilde{\mu}$, $\tilde{\mu} \in K^{(1)}(M)$, найдется целое неотрицательное число n и в E_{k_s} найдутся такие элементы a_i и b_i, $i = 0, 1, \ldots, n$, что выполнено равенство:

$$\tilde{\mu} = \frac{\sum_{i=0}^{n} a_i (\mu)^i}{\sum_{i=0}^{n} b_i (\mu)^i},$$

и при этом дробь $\mu' = \frac{u(\xi)}{v(\xi)}$, где $u(\xi) = \sum_{i=0}^{n} a_i \xi^i$ и $v(\xi) = \sum_{i=0}^{n} b_i \xi^i$, является несократимой.

Заметим, что если $v(\mu(0)) = 0$, то из $\mu'(\mu(\xi)) \in E'_k(\xi)$ следует $u(\mu(0)) = 0$. Поэтому

$$\deg_\xi(\mu'(\mu(\xi))) < \deg_\mu(\mu'(\mu)),$$

что не верно, так как

$$\deg_\xi(\mu'(\mu(\xi))) = (E_k(\xi) : E_k(\mu))(E_k(\mu) : E_k(\mu'(\mu))),$$

$$(E_k(\xi) : E_k(\mu)) = 1,$$

и

$$(E_k(\mu) : E_k(\mu'(\mu))) = \deg_\mu(\mu'(\mu)).$$

Так как $v(\mu(\xi))$ можно получить из элементов множества $E_{k_s} \cup \{\mu\}$ с использованием операций сложения и умножения, то из (1.30) следует включение

$$v(\mu(\xi)) \in M_{i,\omega}^{(1)},$$

и, кроме того, для некоторого a, $a \in E_k \setminus \{0\}$, имеем:

$$\Psi_i(v(\mu(\xi))) = (a, \omega(a)).$$

Для $u(\mu(\xi))$ найдется b, $b \in E_k$, такое, что

$$\Psi_i(u(\mu(\xi))) = (b, \omega(b)).$$

Поэтому $\Psi(\tilde{\mu})$ определена и равна $\left(\frac{b}{a}, \frac{\omega(b)}{\omega(a)}\right)$, следовательно,

$$\Psi(\tilde{\mu}) = \left(\frac{b}{a}, \omega\left(\frac{b}{a}\right)\right) \in M_{i,\omega}^{(1)}.$$

Таким образом,

$$K^{(1)}(M) \subseteq M_{i,\omega}^{(1)},$$

что противоречит предположению.

Получили противоречие с предположением о том, что M не порождает поле $E_k(\xi)$.

Теорема 1.3.1 доказана.

Теперь сформулируем основной результат настоящего параграфа.

Теорема 1.3.2. *Множество $J_k^{(1)}$ является приведенной $K^{(1)}$-критериальной системой $K^{(1)}$-замкнутых классов. Кроме этого, множество $J_k^{(1)}$ состоит из $K^{(1)}$- предполных классов и все $K^{(1)}$-предполные классы содержатся в $J_k^{(1)}$.*

Для доказательства этой теоремы нам понадобятся вспомогательные утверждения.

Замыкание множества M, $M \subseteq E_k'(\xi)$, по операциям сложения и умножения, как и в работе [77], будем обозначать $S^{(1)}(M)$.

Используя рассуждения из [75], несложно доказать следующую лемму.

Лемма 1.3.5. *Для любого M, $M \subseteq E_k'(\xi)$, и для любого μ, $\mu \in K^{(1)}(M)$, найдутся μ_i, $\mu_i \in S^{(1)}(M)$, $i = 1, 2$, такие, что $\mu = \mathrm{fb}(\mu_1, \mu_2)$.*

Лемма 1.3.6. *Пусть $M \subseteq \tilde{M}_0^{(1)}$. Соотношение*

$$K^{(1)}(M) \not\subseteq \tilde{M}_0^{(1)} \tag{1.31}$$

выполнено в точности тогда, когда найдется b, $b \in E_k \setminus \{0\}$, такое, что

$$(0, b) \in \Psi_0(S^{(1)}(M)). \tag{1.32}$$

Доказательство. Если $M \subseteq \tilde{M}_0^{(1)}$, то $S^{(1)}(M) \subseteq \tilde{M}_0^{(1)}$. Поэтому из (1.31) и леммы 1.3.5 вытекает, что найдутся μ_j, $\mu_j \in S^{(1)}(M)$, $j = 1, 2$, такие, что $\mathrm{fb}\,(\mu_1, \mu_2) \notin \tilde{M}_0^{(1)}$. Тогда для некоторого b, $b \in E_k \setminus \{0\}$, выполнено: $\Psi_0\,(\mu_2) = (0, b)$, откуда вытекает (1.32).

Обратно, пусть выполнено (1.32) и μ, $\mu \in S^{(1)}(M)$, таково, что для некоторого b, $b \in E_k \setminus \{0\}$, имеем: $\Psi_0(\mu) = (0, b)$. Тогда для дроби μ', $\mu' = \frac{u'}{v'}$, $\mu' = \mathrm{fb}\left(\mu, \mu^{k-1}\right)$, имеем: $\deg u' > \deg v'$. Поэтому (1.31) выполнено.

Лемма доказана.

На множестве E_k^2 пар чисел поля E_k будем рассматривать операции сложения и умножения, которые определяются покомпонентно:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)\,,$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)\,.$$

Замыкание множества M, $M \subseteq E_k^2$, по операциям сложения и умножения обозначим $S(M)$.

Нетрудно видеть, что $\Psi_0(S^{(1)}(M)) = S(\Psi_0(M))$. При этом множество пар $S(\Psi_0(M))$ элементов из E_k конечно, и существование b, $b \in E_k \setminus \{0\}$, для которого выполнено соотношения (1.32), в случае конечного множества M может быть выполнена.

Пусть $i \in \{2, 3, \dots\}$. Для множества дробей M' такого, что $M' \subseteq \tilde{M}_i^{(1)}$, рассмотрим конечное множество пар $\Psi_i(M')$:

$$\Psi_i(M') = \{\ \Psi_i(\mu)\ \mid\ \mu \in M'\ \}$$

Имеет место следующая лемма.

Лемма 1.3.7. *Пусть для некоторого i, $i \in \{2, 3, \dots\}$, имеет место включение $M \subseteq \tilde{M}_i^{(1)}$. Соотношение*

$$K^{(1)}(M) \not\subseteq \tilde{M}_i^{(1)} \tag{1.33}$$

выполнено в точности тогда, когда в $\Psi_i(S^{(1)}(M))$ найдется пара $(0, v')$ такая, что $v' \neq 0$.

Доказательство. Пусть $M \subseteq \tilde{M}_i^{(1)}$ для некоторого i, $i \in \{2, 3, \dots\}$, и выполнено (1.33). Тогда по лемме 1.3.5 найдутся μ_j, $\mu_j \in S^{(1)}(M)$, такие, что

$$\mathrm{fb}\,(\mu_1, \mu_2) \notin \tilde{M}_i^{(1)}.$$

При этом, в $E_k[\xi]$ найдется многочлен v', что выполнено равенство:

$$\Psi_i\left(\mu_2\right) = \left(0, v'\right).$$

Если, к тому же, $v' = 0$, то знаменатель дроби $\mathrm{fb}\left(\mu_1, \mu_2\right)$ не делится на p_i, что противоречит предположению.

В обратную сторону. Пусть $M \subseteq \tilde{M}_i^{(1)}$ и найдется дробь μ, $\mu \in S^{(1)}(M)$, такая, что $\Psi_i(\mu) = (0, v')$ и $v' \neq 0$. Тогда для некоторого натурального числа T числитель дроби $1 - \mu^T$, представленной в несократимом виде, делится на p_i.

Действительно, пусть $\mu = \frac{u}{v}$ – несократимая дробь. Согласно предположениям, многочлены u и v не делятся на p_i. Поэтому найдутся такие натуральные числа T_1 и T_2, что остатки от деления u^{T_1} и v^{T_2} на многочлен p_i равны 1. Поэтому многочлен $v^{T_1 \cdot T_2} - u^{T_1 \cdot T_2}$ делится на p_i. Положим $T = T_1 \cdot T_2$. Тогда числитель несократимой дроби $1 - \mu^T$ делится на p_i.

Поэтому $\mathrm{fb}\left(\mu, \mu^T\right) \notin \tilde{M}_i^{(1)}$.

Лемма доказана.

Лемма 1.3.8. *Пусть $M \subseteq E_k'(\xi)$ и для любого Θ, $\Theta \in J_k^{(1)}$, выполнено:*

$$M \not\subseteq \Theta. \tag{1.34}$$

Тогда для любого j, $j = 0, 2, 3\ldots$, справедливо:

$$K^{(1)}(M) \not\subseteq \tilde{M}_j^{(1)}. \tag{1.35}$$

Доказательство. Рассмотрим подмножество M множества $E_k'(\xi)$ такое, что

$$\forall\Theta,\ \ \Theta \in J_k^{(1)},$$

справедливо (1.34).

Для заданного j, $j \in \{0, 2, 3, \ldots\}$, если

$$M \not\subseteq \tilde{M}_j^{(1)},$$

то выполнено (1.35). Поэтому рассмотрим случай, когда

$$M \subseteq \tilde{M}_j^{(1)}.$$

По леммам 1.3.6 и 1.3.7 из этой работы: для каждого j, $j = 0, 2, 3\ldots$, соотношение (1.35) следует из существования μ_j, $\mu_j \in S^{(1)}(M)$, такого, что

$$\mu_j \notin R_j^{(1)}$$

и

$$\mu_j(0) = 0.$$

Поэтому предположим, что множество M не содержит дроби с такими свойствами.

Найдется μ_0',

$$\mu_0' \in M \setminus R_j^{(1)}.$$

Для некоторых a' и b' имеем:

$$\Psi_j(\mu_0') = (a', b'),$$

$b' \neq 0$.

Согласно предположению, $a' \neq 0$.

В случае k, не являющегося простым, из соотношений

$$M \not\subseteq P_s^{(1)}, \ \ s = 1, 2, \ldots, l,$$

следует, что для некоторого примитивного элемента a поля E_k в $S^{(1)}(M)$ найдется элемент μ такой, что для некоторого b, $b \in E_k$ при $j = 0$ и $b \in E_k[\xi]$ при $j \in \{2, 3, \ldots\}$, справедливо:

$$\Psi_j(\mu) = (a, b).$$

В случае простого k соответствующее включение получаем из соотношения

$$M \not\subseteq R_1^{(1)}.$$

Если $b = 0$, то через r обозначим такое натуральное число, что $a^r = a'$. Тогда дробь

$$\mu_0' - \mu^r$$

— искомая. Если же $b \neq 0$ и b не сопряжено с a, рассмотрим ненулевой многочлен $g(z)$ над E_p степени m такой, что $g(a) = 0$. Тогда $g(b) \neq 0$ и дробь $g(\mu)$ — искомая. В противном случае, через ω обозначим автоморфизм поля E_k, переводящий элемент a в элемент b. Из соотношения

$$M \nsubseteq M_{j,\omega}^{(1)}$$

и ограничений, наложенных на множество M следует, что в M найдется такое μ'', что для некоторого натурального i выполнено равенство

$$\Psi_j\left(\mu''\right) = \left(a^i, c\right)$$

и

$$c \neq b^i.$$

Тогда дробь $\mu^i - \mu''$ является искомой.

Лемма 1.3.8 доказана.

Замечание 2. *Известно, что примитивный элемент a поля $E_k(\xi)$ имеет m сопряженных элементов: a^{p^0}, a^{p^1}, a^{p^2}, $\ldots$, $a^{p^{m-1}}$. Все они являются элементами поля E_k. Поэтому при доказательстве леммы 1.3.8 для случая $j \in \{2, 3, \ldots\}$ в качестве μ'' можно взять такую дробь из M, что вторая компонента пары $\Psi_j\left(\mu''\right)$ является многочленом ненулевой степени, если, конечно, такая дробь найдется в M.*

Лемма 1.3.9. *Пусть $M \subseteq E_k'(\xi)$, $E_p(M) = E_k(\xi)$. Тогда для некоторого μ, $\mu \in E_k'(\xi) \setminus \{0\}$, и любого a, $a \in E_k$, имеет место:*

$$\{\ a \cdot \mu,\ \ a \cdot \xi\mu\ \} \subset S^{(1)}(M). \tag{1.36}$$

Доказательство. Через b обозначим некоторый примитивный элемент поля E_k. Пусть $M \subseteq E'_k(\xi)$, $E_p(M) = E_k(\xi)$. Тогда в $E'_k(\xi) \setminus \{0\}$ найдутся μ_1 и μ_2, что

$$\{\ \mu_1,\ \ b \cdot \mu_1,\ \ \mu_2,\ \ \xi \cdot \mu_2\ \} \subset S^{(1)}(M).$$

В случае простого k для любого a, $a \in E_k$, дроби $a \cdot \mu_2$ и $a \cdot \xi \cdot \mu_2$ получаем, сложив a раз дробь μ_2 и дробь $\xi \cdot \mu_2$, соответственно. В противном случае, положим $\mu = \mu_1^{m-1}\mu_2$. Тогда для любого i, $i = 0, 1, \ldots, m-1$, справедливы включения:

$$b^i \cdot \mu \in S^{(1)}(M)$$

и

$$b^i \cdot \xi \cdot \mu \in S^{(1)}(M).$$

Поэтому, для любого a, $a \in E_k \setminus \{0\}$, дроби $a \cdot \mu$ и $a \cdot \xi \cdot \mu$ содержатся в $S^{(1)}(M)$. Константу 0 получаем из любого элемента множества M, используя операцию сложения.

Лемма доказана.

Для некоторого целого неотрицательного числа τ множество M, $M \subseteq E'_k(\xi)$, назовем τ-предельным, если

$$\xi^\tau E'_k(\xi) \subseteq K^{(1)}(M). \tag{1.37}$$

Множество M назовем предельным, если найдется τ, для которого оно является τ-предельным.

Лемма 1.3.10. *Пусть $M \subseteq E'_k(\xi)$. Множество M является предельным в точности тогда, когда имеет место условие (1.18), а также для любого i, $i = 0, 2, 3, \ldots,$ из $M \subseteq \tilde{M}_i^{(1)}$ следует (1.33).*

Доказательство. Пусть множество M является предельным. Тогда для некоторого натурального τ выполнено включение (1.37). Поэтому множество M',

$$M' = \{\ \xi^\tau,\ \ a \cdot \xi^\tau,\ \ \xi^{\tau+1}\ \mid\ a \in E_k\ \},$$

содержится в $K^{(1)}(M)$.

Нетрудно видеть, что множество M'',

$$M'' = \{\ a,\ \ \xi\ \mid\ a \in E_k\ \},$$

содержится в $E_p\,(M')$. Далее из

$$E_k(\xi) = E_p\,(M'') \subseteq E_p(M) \subseteq E_k(\xi).$$

получаем равенство (1.18).

Для любого целого числа i, $i \in \{0, 2, 3, \ldots\}$, имеем:

$$\xi^\tau E'_k(\xi) \not\subseteq \tilde{M}_i^{(1)},$$

откуда с учетом (1.37) получаем (1.33).

В обратную сторону. Пусть для множества M, $M \subseteq E'_k(\xi)$, выполнены (1.18), (1.33), $i = 0, 2, 3, \ldots$.

Тогда из леммы 1.3.9 и соотношения (1.31) для некоторого $\tilde{\mu}$, $\tilde{\mu} = \frac{\tilde{u}}{\tilde{v}}$, $\deg\,(\tilde{u}) \geq \deg\,(\tilde{v})$, и любого a, $a \in E_k$, имеем:

$$\{\ a\tilde{\mu},\ \ a\xi\tilde{\mu}\ \} \subset K^{(1)}(M). \tag{1.38}$$

Поэтому, как и при доказательстве леммы 8 работы [75], где рассмотрен случай простого k, покажем, что существует натуральное число s_1 такое, что для любых целых неотрицательных чисел i и j таких, что $i \geq s_1$, $j \geq s_1$, и любого a, $a \in E_k$, имеет место:

$$a\xi^i\tilde{\mu}^j \in K^{(1)}(M). \tag{1.39}$$

Справедливость соотношения (1.39) для любого целого неотрицательного числа i, любого натурального числа j, удовлетворяющих неравенству $i \leq j$ и любого a, $a \in E_k$, вытекает из включения (1.38), которое выполнено для любого элемента a поля E_k, и возможности использования операции умножения.

Для некоторых целых неотрицательных чисел n_1 и n_2, связанных неравенством $n_1 \geq n_2$, в поле E_k найдутся такие элементы $a_0, a_1, \ldots, a_{n_1}$, $b_0, b_1, \ldots, b_{n_2}$, что $a_{n_1} \neq 0$, $b_0 \neq 0$ и

$$\tilde{\mu} = \frac{a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{n_1}\xi^{n_1}}{b_0 + b_1\xi + b_2\xi^2 + \cdots + b_{n_2}\xi^{n_2}}.$$

Из последнего равенства вытекает следующее тождество:

$$\begin{gathered} a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{n_1}\xi^{n_1} - \\ -b_0\tilde{\mu} - b_1\xi\tilde{\mu} - b_2\xi^2\tilde{\mu} - \cdots - b_{n_2}\xi^{n_2}\tilde{\mu} = 0, \end{gathered}$$

откуда для любых целых неотрицательных чисел i, T и любого элемента a поля E_k имеет место равенство:

$$\begin{aligned} a\xi^{n_1+i}\tilde{\mu}^T \;=\; & a\left(a_{n_1}\right)^{-1} b_0\xi^i\tilde{\mu}^{T+1} + a\left(a_{n_1}\right)^{-1} b_1\xi^{i+1}\tilde{\mu}^{T+1} + \\ & a\left(a_{n_1}\right)^{-1} b_2\xi^{i+2}\tilde{\mu}^{T+1} + \cdots + a\left(a_{n_1}\right)^{-1} b_{n_2}\xi^{i+n_2}\tilde{\mu}^{T+1} \\ & -a\left(a_{n_1}\right)^{-1} a_0\xi^i\tilde{\mu}^T - a\left(a_{n_1}\right)^{-1} a_1\xi^{i+1}\tilde{\mu}^T - \\ & a\left(a_{n_1}\right)^{-1} a_2\xi^{i+2}\tilde{\mu}^T - \cdots - a\left(a_{n_1}\right)^{-1} a_{n_1-1}\xi^{i+n_1-1}\tilde{\mu}^T \end{aligned} \tag{1.40}$$

Выберем натуральное число T, такое, что $T \geq n_1$. Индукцией по i, $i = 0, 1, 2, \ldots$, используя равенство (1.40), а также соотношение (1.39), справедливое для пар i, j таких, что $i \leq j$, нетрудно показать, что для любого a, $a \in E_k$, и любого целого неотрицательного числа i имеет место включение:

$$a\xi^{n_1+i}\tilde{\mu}^T \in K^{(1)}(M). \tag{1.41}$$

Используя включение $\tilde{\mu} \in K^{(1)}(M)$, заключаем, что соотношение (1.39) имеет место для любых i и j, не меньших $s_1 = \max\left(n_1, T\right)$ и любого a, $a \in E_k$.

Отсюда и из условий (1.33) с использованием рассуждений из доказательства той же леммы работы [75] заключаем, что M - предельное множество.

Действительно, для некоторого целого неотрицательного числа s_2 и некоторых многочленов $\hat{u}$ и $\hat{v}$ из $E_k[\xi]$ таких, что $\hat{u}(0) \neq 0$ и $\hat{v}(0) \neq 0$, имеет место равенство:

$$\tilde{\mu}^{s_1} = \xi^{s_2}\frac{\hat{u}}{\hat{v}}.$$

Отсюда и из соотношения (1.39), выполненного для $j = s_1$, и любых i, a, таких, что $i \in \mathbb{Z}_+$, $i \geq s_1$, $a \in E_k$, получаем включения:

$$a\xi^{s_1+s_2+i}\hat{v}\tilde{\mu}^{s_1} = a\xi^{s_1+s_2+i}\hat{u} \in K^{(1)}(M), \;\; i = 0, 1, \dots, \;\; a \in E_k. \tag{1.42}$$

Разложим многочлен $\hat{u}$ в произведение неприводимых приведенных многочленов:

$$\hat{u} = b \cdot p_{i_1}^{j_1} \cdot p_{i_2}^{j_2} \cdot \dots \cdot p_{i_{s'}}^{j_{s'}}, \tag{1.43}$$

где $1 < i_1 < i_2 < \dots < i_{s'}$, и $j_r \in \mathbb{N}$, $r = 1, 2, \dots, s'$.

По лемме 1.3.8 для каждого r, $r = 1, 2, \dots, s'$, в $K^{(1)}(M)$ найдется дробь μ_r, не содержащаяся в $\tilde{M}_{i_r}^{(1)}$. Поэтому числитель дроби μ_r', $\mu_r' = \hat{u} \cdot \mu_r^{j_r}$ не делится на p_{i_r}.

Отсюда и из включения (1.42), справедливого для любого целого неотрицательного i и любого элемента a поля E_k, с использованием операции умножения получаем включение

$$a\xi^{s_1+s_2+i}\mu_r' \in K^{(1)}(M), \tag{1.44}$$

справедливое для любых a и i, $a \in E_k$, $i \in \mathbb{Z}_+$.

Наибольший общий делитель числителей дробей из множества

$$\{\;\hat{u},\;\; \mu_r' \;\mid\; r = 1, 2, \dots\; s'\;\}$$

равен 1. Поэтому для некоторых многочленов w_i, $w_i \in E_k[\xi]$, $i = 0, 1, \dots, s'$, справедливо равенство:

$$w_0\hat{u} + w_1\mu_1' + w_2\mu_2' + \dots + w_{s'}\mu_{s'}' = 1.$$

Отсюда и из (1.42), (1.44) следует, что для любых a и i, $a \in E_k$, $i \in \mathbb{Z}_+$ имеет место включение:

$$a\xi^{s_1+s_2+i} \in K^{(1)}(M)$$

Обозначим число s_1+s_2 через T_0. Для любого j, $j \geq T_0$, и любого a, $a \in E_k$, выполнено:

$$a\xi^{j} \in K^{(1)}(M). \tag{1.45}$$

Как указано в [29], для любого многочлена v из $E_k[\xi]$ такого, что $v(0) \neq 0$, найдется такое натуральное число $T(v)$, что многочлен $1 - \xi^{T(v)}$ делится на v. Действительно, существуют два различных целых неотрицательных числа T_1 и T_2 таких, что остатки от деления одночленов ξ^{T_1} и ξ^{T_2} на v совпадают. Пусть $T_1 > T_2$. Тогда многочлен $\xi^{T_1} - \xi^{T_2} = \xi^{T_2}\left(\xi^{T_1 - T_2} - 1\right)$ делится на v, откуда $1 - \xi^{T_1 - T_2}$ делится на v. Следовательно, для любой дроби μ, $\mu \in E'_k(\xi)$, найдутся такие T и u, что $T \in \mathbb{N}$, $u \in E_k[\xi]$ и

$$\mu = \frac{u}{1 - \xi^T}.$$

Так как для любого натурального числа i многочлен $1 - \xi^{iT}$ делится на многочлен $1 - \xi^T$, то выберем натуральное число i_0 такое, что $T \cdot i_0 \geq T_0$. В $E_k[\xi]$ найдется многочлен u_0 такой, что

$$\mu = \frac{u_0}{1 - \xi^{T \cdot i_0}}.$$

Тогда для любого натурального j, $j \geq T_0$, с использованием (1.45) имеем:

$$\xi^j \mu = \mathrm{fb}\left(\xi^j u_0, \xi^{T \cdot i_0}\right) \in K^{(1)}(M),$$

то есть M является предельным множеством.

Лемма доказана.

Лемма 1.3.11. *Множество $J_k^{(1)}$ является $K^{(1)}$-критериальной системой.*

Доказательство. Рассмотрим множество M, $M \subseteq E'_k(\xi)$, не содержащееся ни в одном из замкнутых классов системы $J_k^{(1)}$.

В случае поля E_k, не являющимся простым, рассмотрим разложение (1.10) числа m. Через μ_s обозначим элемент множества M, не содержащийся в $P_s^{(1)}$, $s = 1, 2, \ldots, l$. Поле E_k порождается элементами $\mu_s(0)$ по операциям сложения и умножения. В случае простого поля, в M найдется дробь $\tilde{\mu}_1$, $\tilde{\mu}_1 \in M \setminus R_1^{(1)}$.

Из приведенных рассуждений следует, что для любого a, $a \in E_k$, в $K^{(1)}(M)$ содержится элемент μ_a, удовлетворяющая равенству $\mu_a(0) = a$.

Далее, ввиду соотношения $M \not\subseteq M_1^{(1)}$, в M содержится дробь μ_1' такая, что для некоторых b_0', b_1', μ'', таких, что $b_0' \in E_k$, $b_1' \in E_k \setminus \{0\}$, $\mu'' \in E_k'(\xi)$, выполнено:

$$\mu' = b_0' + b_1'\xi\left(1 + \xi\mu''\right).$$

Используя дробь μ', а также дроби μ_a, $a \in E_k$, индукцией по s, $s \geq 1$, покажем, что для любого многочлена u, $u \in E_k[\xi]$, $\deg u < s$, найдутся такие дроби μ_u и μ_u' из $E_k'(\xi)$, что

$$\mu_u = u + \xi^s\mu_u' \in K^{(1)}(M). \tag{1.46}$$

Действительно, в случае $s = 1$ многочлены u являются константами, а дроби μ_a, удовлетворяющие соотношениям (1.46), найдены выше.

Пусть теперь $s' > 1$ и для любого натурального s, $s < s'$, утверждение доказано. Для некоторой дроби $\tilde{\mu}$ из $E_k'(\xi)$ имеет место равенство:

$$\mu' + \mu_{b_0'}^k = b_1'\xi\left(1 + \xi\tilde{\mu}\right).$$

Поэтому для любого a, $a \in E_k$, в $K^{(1)}(M)$ содержится дробь $\hat{\mu}_a$,

$$\hat{\mu}_a = \mu_a\left(\mu_{(b_1')^{-1}}\left(\mu' + \mu_{b_0'}^k\right)\right)^{s'-1},$$

для которой найдется $\tilde{\mu}_a$, $\tilde{\mu}_a \in E_k'(\xi)$, такая, что имеет место равенство:

$$\hat{\mu}_a = a\xi^{s'-1}\left(1 + \xi\tilde{\mu}_a\right).$$

Используя дроби $\hat{\mu}_a$, предположение индукции и операцию сложения, для любого многочлена u степени меньшей $s = s'$ можно получить μ_u, удовлетворяющее соотношению (1.46).

Из этого и леммы 1.3.10 следует, что $E_k[\xi] \subset K^{(1)}(M)$, откуда вытекает равенство

$$K^{(1)}(M) = E_k'(\xi)$$

.

Лемма доказана.

Для доказательства теоремы 1.3.2. нам осталось показать, что

$$\forall \Theta \left(\Theta \in J_k^{(1)} \right) \forall \Theta' \left(\Theta' \in J_k^{(1)} \right)$$

из $\Theta \neq \Theta'$ следует $\Theta \nsubseteq \Theta'$.

Лемма 1.3.12. *Для любых различных классов Θ и Θ' из множества $J_k^{(1)}$ выполнено:*

$$\Theta \not\subset \Theta'. \tag{1.47}$$

Доказательство. Для каждого Θ, $\Theta \in J_k^{(1)}$, укажем такое множество $\hat{\Theta}$, что

$$\hat{\Theta} \subset \Theta, \tag{1.48}$$

но для любого Θ', $\Theta' \in J_k \setminus \{\Theta\}$, выполнено:

$$\hat{\Theta} \nsubseteq \Theta'. \tag{1.49}$$

Сначала рассмотрим случай простого поля. Введем следующие множества:

$$\hat{M}_0^{(1)} = \left\{ \; 1, \;\; \frac{\xi}{1+\xi^2} \; \right\},$$

$$\hat{M}_i^{(1)} = \{ \; 1, \;\; \xi p_i \; \},$$

$i = 1, 2, \ldots,$

$$\hat{R}_0^{(1)} = \left\{ \; \frac{1}{1+\xi} \; \right\},$$

$$\hat{R}_1^{(1)} = \{ \; \xi \; \},$$

$$\hat{R}_i^{(1)} = \{ \; p_i, \;\; \xi p_i \; \},$$

$i = 2, 3, \ldots.$

В рассматриваемом случае среди классов множества $J_k^{(1)}$ только в классе $R_1^{(1)}$ содержится элемент ξ, только в классе $R_0^{(1)}$ содержится элемент $\frac{1}{1+\xi}$. Поэтому утверждение леммы справедливо для этих классов.

Только классы $M_i^{(1)}$, $i = 0, 1, \ldots$, содержат элемент 1. Но каждый класс этой серии содержит элемент, не содержащийся ни в каком другом ее классе. Для $i = 0$ таким элементом является $\frac{\xi}{1+\xi^2}$, а для другого i – элемент ξp_i.

Осталось рассмотреть только классы $R_i^{(1)}$, $i = 2, 3, \ldots$. Заметим, что для фиксированного i такой класс содержит элемент ξp_i, который также содержится только в классах: $M_i^{(1)}$ и $R_1^{(1)}$. Но, каждый из этих двух классов не содержит элемент p_i. Таким образом, утверждение леммы выполнено и для рассматриваемых классов. Случай простого поля рассмотрен.

Теперь рассмотрим случай поля, не являющегося простым.

Пусть b — примитивный элемент поля E_k, а b_s – элемент поля E_{k_s}, являющийся примитивным элементом этого поля. Через id обозначим тождественный автоморфизм поля E_k.

Положим:

$$\hat{P}_s^{(1)} = \{\ \xi,\ \ b_s\ \},$$

для $s = 1, 2, \ldots, l$.

$$\hat{M}_{0,\mathrm{id}}^{(1)} = \left\{\ b,\ \ \frac{\xi}{1+\xi^2}\ \right\},$$

$$\hat{M}_{0,\omega}^{(1)} = \left\{\ \ \frac{b+\omega(b)\xi}{1+\xi},\ \ \frac{\xi}{1+\xi^2}\ \right\},$$

для $\omega \in \Omega_k \setminus \{\mathrm{id}\}$.

$$\hat{M}_1^{(1)} = \{\ b,\ \ \xi^2\ \}.$$

$$\hat{M}_{j,\mathrm{id}}^{(1)} = \{\ b,\ \ \xi p_j\ \},$$

для $j = 2, 3, \ldots$,

$$\hat{M}_{j,\omega}^{(1)} = \left\{\ \omega(b) + \frac{b-\omega(b)}{p_j(0)} p_j,\ \ \xi p_j\ \right\},$$

для $j = 2, 3, \ldots, \quad \omega \in \Omega_k \setminus \{\mathrm{id}\}$.

$$\hat{R}_0^{(1)} = \left\{\ \frac{b}{1+\xi},\ \ \frac{\xi}{1+\xi^2}\ \right\},$$

$$\hat{R}_j^{(1)} = \left\{\ b\frac{p_j}{p_j(0)},\ \ \xi p_j\ \right\},$$

для $j = 2, 3, \ldots$.

Из соотношения $\xi \notin \Theta$, справедливого для каждого Θ,

$$\Theta \in J_k^{(1)} \setminus \left\{ \ P_s^{(1)} \ \mid \ s = 1, 2, \ldots, l \ \right\},$$

а также невключения элемента b_s поля E_k ни в какой из замкнутых классов $P_{s'}^{(1)}$ при $s \neq s'$ получаем, что

$$\hat{P}_s^{(1)} \not\subseteq \Theta, \ \ \forall \Theta \in J_k^{(1)} \setminus \{P_s^{(1)}\},$$

но, при этом,

$$\hat{P}_s^{(1)} \subset P_s^{(1)}.$$

Следовательно $P_s^{(1)}$ не содержится ни в каком другом классе множества $J_k^{(1)}$.

Продолжая проверку, устанавливаем, что

$$\hat{M}_{0,\mathrm{id}}^{(1)} \subset M_{0,\mathrm{id}}^{(1)},$$

а также,

$$b \notin \Theta, \ \ \forall \Theta \in \left\{ \ P_s^{(1)}, M_{0,\omega}^{(1)}, R_j^{(1)} \ | s \in \{1, 2, \ldots, l\}, \omega \in \Omega_k \setminus \{\mathrm{id}\}, j \in \{0, 2, 3 \ldots\} \right\}, \tag{1.50}$$

$$\frac{\xi}{1+\xi^2} \notin \bigcup_{j=2,3,\ldots,\omega \in \Omega_k} M_{j,\omega}^{(1)} \cup \bigcup_{j=2,3,\ldots} R_j^{(1)} \cup M_1^{(1)}. \tag{1.51}$$

Таким образом, класс $M_{0,\mathrm{id}}^{(1)}$ не содержится ни в одном другом классе множества $J_k^{(1)}$.

Учитывая соотношение (1.51), а также

$$\frac{b+\omega(b)\xi}{1+\xi} \notin \Theta, \ \ \forall \Theta \in \left\{ \ P_s^{(1)}, \ \ M_{0,\omega'}^{(1)}, \ \ R_0^{(1)} \ \mid \ s = 1, 2, \ldots, l, \omega' \in \Omega_k \setminus \{\omega \ \ \} \right\}$$

и

$$\hat{M}_{0,\omega}^{(1)} \subset M_{0,\omega}^{(1)},$$

заключаем, что $M_{0,\omega}^{(1)}$ не содержится ни в одном другом классе из $J_k^{(1)}$.

Далее,

$$\xi^2 \notin \left\{ \ M^{(1)}_{j,\omega}, R^{(1)}_j \ \mid \ \omega \in \Omega_k, j \in \{0, 2, 3, \dots\} \ \right\}.$$

Учитывая это, а также (1.50) и $\hat{M}^{(1)}_1 \subset M^{(1)}_1$, получаем требуемое утверждение для класса $M^{(1)}_1$.

Для каждого j, $j \in \{2, 3, \dots\}$ дробь ξp_j содержится только в классах $P^{(1)}_s$, $s = 1, 2, \dots, l$, $M^{(1)}_{j,\omega}$, $\omega \in \Omega_k$, $R^{(1)}_j$, среди которых только класс $M^{(1)}_{j,\mathrm{id}}$ содержит b – примитивный элемент поля E_k. Отсюда получаем утверждение леммы для классов $M^{(1)}_{j,\mathrm{id}}$. Среди перечисленных классов только класс $M^{(1)}_{j,\omega}$ содержит элемент $\omega(b) + \frac{b-\omega(b)}{p_j(0)} p_j$ и только класс $R^{(1)}_j$ содержит элемент $b \frac{p_j}{p_j(0)}$. Поэтому утверждение леммы доказано для классов $M^{(1)}_{j,\omega}$ и $R^{(1)}_j$.

Из соотношения (1.51), а также из

$$\frac{b}{1+\xi} \notin \bigcup_{s=1,2,\dots,l} P^{(1)}_s \cup \bigcup_{\omega \in \Omega_k} M^{(1)}_{0,\omega}$$

и

$$\hat{R}^{(1)}_0 \subset R^{(1)}_0$$

следует, что класс $R^{(1)}_0$ не содержится ни в каком другом классе множества $J^{(1)}_k$.

Лемма доказана.

Таким образом, теорема 1.3.2 доказана.

Глава 2

Проблема полноты для линейных автоматов

2.1. Редукция

В настоящем параграфе мы получим критерий K-полноты множеств ЛА, который позволит в дальнейшем построить приведенную K-критериальную систему, состоящую из K-предполных классов и включающую все K-предполные классы.

Через J'_k обозначим следующее множество K-замкнутых классов, которые определены в параграфе 2 главы 1.

$$J'_k = \{\ V_1,\ \ V_p,\ \ T_a\ \mid\ a \in E_k\ \}\,,$$

Теорема 2.1.1. *Для множества M, $M \subseteq \mathfrak{L}_k$, равенство*

$$K(M) = \mathfrak{L}_k \tag{2.1}$$

выполнено в точности тогда, когда имеют место следующие два свойства.

$$\forall\Theta,\ \ \Theta \in J'_k,\ \ \textit{выполнено: } M \not\subseteq \Theta, \tag{2.2}$$

$$U(K(M)) = E'_k(\xi). \tag{2.3}$$

Для доказательства полноты множества M, удовлетворяющего свойствам (2.2) и (2.3) нам понадобится вспомогательное утверждение.

Лемма 2.1.1. *Если для некоторого M, $M \subseteq \mathfrak{L}_k$, выполнены свойства (2.2) и (2.3), то:*

$$x_1 + x_2 + \cdots + x_{p+1} \in K(M); \tag{2.4}$$

для любого μ, $\mu \in E'_k(\xi)$, *в* $K(M)$ *содержится ЛА*

$$x_1 + \mu \cdot x_2 + \mu \cdot x_3 + \cdots + \mu \cdot x_{p+1}; \tag{2.5}$$

в $K(M)$ *содержатся константные ЛА* ν_0 *и* ν'_0 *такие, что*

$$\nu_0(0) = 0, \quad \nu'_0(0) \neq 0. \tag{2.6}$$

Доказательство. Рассмотрим множество M, $M \subseteq \mathfrak{L}_k$, обладающее свойствами (2.2) и (2.3).

Тогда найдется ЛА $f\,(x_1, x_2, \ldots, x_n)$, $f \in M \setminus V_1$. Для некоторых μ_i, $\mu_i \in E'_k(\xi)$, $i = 0, 1, \ldots, n$, имеет место равенство (1.9). Не ограничивая общности рассуждений, будем предполагать, что $\mu_i(0) \neq 0$, $i = 1, 2$. Найдутся ЛА g_i, $g_i \in K(M)$, $i = 1, 2$, такие, что $\mu_i^{-1} \in U(g_i)$. Из ЛА g_i, используя операции переименования и отождествления переменных, получим ЛА $g'_i(x_i, x_3)$,

$$g'_i(x_i, x_3) = \mu_i^{-1} \cdot x_i + g''_i(x_3), \ \ i = 1, 2.$$

Тогда, обозначив ЛА

$$f\,(g'_1(x_1, x_3), g'_2(x_2, x_3), x_3, \ldots, x_3)$$

через $h\,(x_1, x_2, x_3)$, для некоторых μ'_i, $i = 0, 1$, имеем:

$$h\,(x_1, x_2, x_3) = x_1 + x_2 + \mu'_1 \cdot x_3 + \mu'_0.$$

Имеет место равенство

$$h\,(x_1, h\,(x_2, \ldots h\,(x_p, x_{p+1}, x)\,, \ldots x)\,, x) = x_1 + x_2 + \cdots + x_{p+1}.$$

Поэтому включение (2.4) доказано.

Далее, для каждого μ, $\mu \in E'_k(\xi)$, в $K(M)$ содержится ЛА $f_\mu(x, x_1)$ такой, что для некоторых μ_1 и μ_0 из $E'_k(\xi)$ выполнено:

$$f_\mu(x, x_1) = \mu \cdot x + \mu_1 \cdot x_1 + \mu_0.$$

Имеет место равенство:

$$x_1 + f_\mu(x_2, x) + f_\mu(x_3, x) + \cdots + f_\mu(x_{p+1}, x) = x_1 + \mu \cdot x_2 + \mu \cdot x_3 + \cdots + \mu \cdot x_{p+1},$$

откуда вытекает утверждение (2.5).

Из леммы 1.2.2 следует, что в $K(M)$ содержится некоторый константный ЛА ν. а в случае поля, не являющегося простым, из равенства (2.3) для каждого s, $s \in \{1, 2, \ldots, l\}$, вытекает соотношение:

$$M \not\subseteq P_s.$$

Отсюда и из леммы 1.2.3 получаем, что в $K(M)$ найдется ЛА $\hat{h}$, который 1-эквивалентен константному ЛА 0. Действительно, ЛА ν_0, $\nu_0 = \hat{h}\,(\nu, \nu, \ldots, \nu)$ является константным и реализует 0 в начальный момент. Далее, найдется ЛА h', $h' \in M \setminus T_0$. Подстановкой константного ЛА ν_0 вместо всех переменных ЛА h' получим константный ЛА ν_0', реализующий в начальный момент элемент множества $E_k \setminus \{0\}$.

Свойство (2.6), а, вместе с ним лемма, доказаны.

Доказательство теоремы. Пусть выполнено (2.1). Тогда свойство (2.2) следует из леммы 1.2.1, а справедливость (2.3) вытекает из теоремы 1.1.2.

Пусть для множества M, $M \subseteq \mathfrak{L}_k$, выполнены свойства (2.2) и (2.3). Согласно лемме 2.1.1 в $K(M)$ содержатся константы ν_0 и ν_0' такие, что $\nu_0(0) = 0$, $\nu_0'(0) \neq 0$. Тогда для некоторых многочленов $u(\xi)$, $u'(\xi)$, $v(\xi)$, $v'(\xi)$ из $E_k[\xi]$ имеют место равенства:

$$\nu_0 = \frac{\xi \cdot u(\xi)}{1 + \xi \cdot v(\xi)}, \quad \nu_0' = \frac{-1 + \xi \cdot u'(\xi)}{v'(\xi)}.$$

Справедливо тождество:

$$(1 - \xi \cdot u'(\xi))\,(1 + \xi \cdot v(\xi))\,\nu_0 + \xi \cdot u(\xi) v'(\xi) \nu_0' = 0.$$

Через $u_1(\xi)$ и $u_2(\xi)$ обозначим многочлены $\xi\,(v(\xi) - u'(\xi) - \xi v(\xi) u'(\xi))$ и $\xi u(\xi) v'(\xi)$, соответственно. Имеем тождество:

$$\nu_0 + u_1(\xi)\nu_0 + u_2(\xi)\nu_0' = 0,$$

причем $u_i(\xi) \in \{\xi\} \cdot E_k[\xi]$, $i = 1, 2$.

Из леммы 2.1.1 следует:

$$x_1 + u_i \cdot x_2 + u_i \cdot x_3 + \cdots + u_i \cdot x_{p+1} \in K(M), \quad i = 1, 2.$$

Используя эти ЛА, операции подстановки, переименования и отождествления переменных, получаем ЛА

$$f(x_1, x_2, x_3) = x_1 + u_1 \cdot x_1 + u_2 \cdot x_2 - (u_1 + u_2)\, x_3.$$

Применяя операцию обратной связи к единственной переменной ЛА $f(\nu_0, \nu_0', x)$, получим константу 0.

Далее используем (2.4). Подставляя константу 0 вместо переменных x_3, x_4, $\ldots$, x_{p+1} сумматора $x_1 + x_2 + \cdots + x_{p+1}$, получим сумматор $x_1 + x_2$.

Для любого μ, $\mu \in E_k'(\xi)$, выполнено (2.5). Поэтому,

$$\mu \cdot x = 0 + \mu \cdot x + \mu \cdot 0 + \cdots + \mu \cdot 0 \in K(M).$$

Отсюда,

$$\xi \cdot x \in K(M)$$

и для любого a, $a \in E_k$,

$$a \cdot x \in K(M).$$

Далее,

$$(\nu_0')^{-1} \cdot x \in K(M),$$

поэтому,

$$1 = (\nu_0')^{-1} (\nu_0') \in K(M),$$

$$\xi_a(x) = \xi x + a \cdot 1 \in K(M).$$

Отсюда и из определения класса $\mathfrak{L}_k$, приведенного в параграфе 1 главы 1, следует равенство (2.1).

Теорема 2.1.1 доказана.

Нашей дальнейшей целью является доказательство следующего критерия K-полноты в $\mathfrak{L}_k$.

Теорема 2.1.2. *Множество M, $M \subseteq \mathfrak{L}_k$, является K-полным в $\mathfrak{L}_k$ тогда и только тогда, когда имеет место (2.2), а также:*

$$\forall \Theta, \Theta \in J_k^{(1)}, \quad U(M) \not\subseteq \Theta, \tag{2.7}$$

и

$$\forall j, j = 0, 2, 3, \dots, \quad U(K(M)) \not\subseteq \tilde{M}_j^{(1)}. \tag{2.8}$$

Для доказательства теоремы нам понадобится следующее утверждение.

Лемма 2.1.2. *Если для множества M, $M \subseteq \mathfrak{L}_k$, выполнены: (2.2), (2.7) и (2.8), то*

$$x_1 + x_2 + \dots + x_{p+1} \in K(M). \tag{2.9}$$

Доказательство леммы.

Пусть для M, $M \subseteq \mathfrak{L}_k$, выполнены (2.2), (2.7) и (2.8). Докажем, что выполнено (2.9).

Из ЛА $f(x_1, x_2, \dots, x_n)$, $f \in M \setminus V_1$, используя операции суперпозиции, можно получить ЛА $g(x_1, x_2, x)$,

$$g(x_1, x_2, x) = \mu_1 \cdot x_1 + \mu_1 \cdot x_2 + \mu' \cdot x + \mu_0,$$

где $\mu_1(0) = 1$. Также при $\mu_1 \in \tilde{M}_0^{(1)} \setminus R_0^{(1)}$ можно добиться, чтобы выполнялось равенство $\Psi_0(\mu_1) = (1, 1)$.

Если $\mu_1 = 1$, то

$$x_1 + x_2 + \dots + x_{p+1} = g(x_1, g(x_2, \dots g(x_p, x_{p+1}, x) \dots, x), x),$$

поэтому включение (2.9) выполнено.

В противном случае, одноместный ЛА μ_1 содержится лишь в конечном множестве классов системы

$$\{\ R_i^{(1)} \mid i = 0, 2, 3, \dots \ \}.$$

Положим

$$\Omega' = \{\ j\ \mid\ \mu_1 \in R_j^{(1)}\ \}.$$

Согласно предположению, найдутся конечные множества $M'_{i'}$, $i' = 1, 2$, такие, что

$$M'_1 \subseteq U(M), \quad \forall \Theta, \Theta \in J_k^{(1)},\ \ M'_1 \not\subseteq \Theta;$$

$$M'_2 \subset K(U(M)), \quad \forall j, j \in \Omega',\ \ M'_2 \not\subseteq \tilde{M}_j^{(1)}.$$

Положим:

$$M' = M'_1 \cup M'_2.$$

Через r обозначим число $1 + |M'|$. Выберем некоторое натуральное число τ, такое, что $p^{\tau-1} \geq 2r$.

Для каждого μ', $\mu' \in M'$, найдется натуральное число $T(\mu')$, такое, что множество

$$M'' = \{\mu_1^{p^\tau}\} \cup \{\ (\mu')^{T(\mu')}\, \mu_1^{p^\tau}\ \mid\ \mu' \in M'\}$$

не содержится ни в одном из классов $J_k^{(1)}$.

Из свойств множества M'' и теоремы 1.3.2 следует, что $1 \in K^{(1)}(M'')$. Поэтому из леммы 1.3.5 вытекает, что для некоторых μ_i^*, $\mu_i^* \in S(M'')$, $i = 1, 2$, имеет место равенство:

$$1 = \frac{\mu_1^*}{1 - \mu_2^*},$$

откуда

$$1 = \mu_1^* + \mu_2^*,$$

то есть

$$1 \in S^{(1)}(M''). \tag{2.10}$$

Пусть

$$M'' = \{\ \mu'_j\ \mid\ j = 1, 2, \ldots, r\ \}.$$

Нетрудно видеть, что ЛА h,

$$h = \sum_{i=1}^{r} \mu'_i \sum_{j=1}^{p} x_{i,j} + \sum_{i=1}^{r} \mu'_i \sum_{j=1}^{p} x'_{i,j} + \mu'' x + \mu''_0,$$

для некоторых μ'', μ_0'' из $E_k'(\xi)$, содержится в $K(M)$.

Если выполнено (2.10), то одноместный ЛА, осуществляющий тождественное отображение, получаем как многочлен над E_p от r переменных μ_1', μ_2', ..., μ_r' степени не меньшей 1 с нулевым свободным членом.

Покажем, что для любого многочлена u от переменных μ_1', μ_2', ..., μ_r' степени не меньшей 1 с нулевым свободным членом в $E_k'(\xi)$ найдутся μ_u и γ_u такие, что выполнено:

$$ux_1 + ux_2 + \mu_u x + \gamma_u \in S\left(\{h\}\right). \tag{2.11}$$

Если $\deg_{M''} u = 1$, то найдутся числа d_1, d_2, $\ldots$, d_r из E_p такие, что

$$u = \sum_{i=1}^{r} d_i \mu_i'.$$

Положим:

$$\begin{aligned} h'\left(x_1, x_2, x\right) \;&=\; h\Bigg(\underbrace{x_1, \ldots x_1}_{d_1}, \underbrace{x, \ldots, x}_{p-d_1}, \ldots, \underbrace{x_1, \ldots x_1}_{d_r}, \underbrace{x, \ldots, x}_{p-d_r}, \\ &\qquad \underbrace{x_2, \ldots x_2}_{d_1}, \underbrace{x, \ldots, x}_{p-d_1}, \ldots, \underbrace{x_2, \ldots x_2}_{d_r}, \underbrace{x, \ldots, x}_{p-d_r}, x\Bigg). \end{aligned}$$

Тогда для некоторых μ_u и γ_u выполнено (2.11).

Предположим, что для некоторого натурального числа s и любого u,

$$u \in S^{(1)}\left(M''\right), \;\; \deg_{M''} u \le s,$$

найдется такое μ_u, что выполнено (2.11). Пусть теперь u, $u \in S^{(1)}\left(M''\right)$, таково, что $\deg_{M''}(u) = s + 1$.

Тогда найдутся числа d_j, $d_j \in E_p$, $j = 1, 2, \ldots, r$, и многочлены u_j от μ_1', μ_2', ..., μ_r' с нулевым свободным членом, $j = 1, 2, \ldots, r$, такие, что

$$u_j \in S^{(1)}\left(M''\right), \quad \deg_{M''} u_j \le s, \;\; j = 1, 2, \ldots, r,$$

и

$$u = \sum_{j=1}^{r} d_j \mu_j' + \sum_{j=1}^{r} \mu_j' u_j.$$

Из предположения индукции следует, что в $S(M)$ содержатся ЛА $h'_j(x, x')$,

$$h'_j(x, x') = u_j x + \mu_{u_j} x' + \gamma_{u_j}.$$

Пусть

$$\tilde{h}(x_1, x_2, x) = h\Bigg(\underbrace{x_1, \ldots x_1}_{d_1}, h'_1(x_1, x), \underbrace{x, \ldots, x}_{p-d_1-1}, \ldots,$$

$$\underbrace{x_1, \ldots x_1}_{d_r}, h'_r(x_1, x), \underbrace{x, \ldots, x}_{p-d_r-1}, \underbrace{x_2, \ldots x_2}_{d_1}, h'_1(x_2, x), \underbrace{x, \ldots, x}_{p-d_1-1}, \ldots,$$

$$\underbrace{x_2, \ldots x_2}_{d_r}, h'_r(x_2, x), \underbrace{x, \ldots, x}_{p-d_r-1}, x\Bigg).$$

Тогда, как нетрудно видеть, для некоторых μ_u и γ_u из $E'_k(\xi)$ выполнено:

$$\tilde{h}(x_1, x_2, x) = ux_1 + ux_2 + \mu_u x + \gamma_u.$$

Таким образом, включение (2.11) доказано для любого u из $S^{(1)}(M'')$, в частности, для u, который тождественен проводнику.

Из ЛА $x_1 + x_2 + \mu_u x + \gamma_u$, используя операции суперпозиции, как уже показано в доказательстве этой леммы, можно получить сумматор

$$x_1 + x_2 + \cdots + x_{p+1}.$$

Лемма доказана.

Доказательство теоремы 2.1.2.

Предположим, что множество M, $M \subseteq \mathfrak{L}_k$, является K-полным в $\mathfrak{L}_k$. Соотношения (2.2) получаем из леммы 1.2.1, соотношение (2.7) следуют из леммы 1.3.1 и теоремы 1.3.2, а соотношение (2.8) вытекает из K-полноты множества M.

В обратную сторону. Пусть для множества M, $M \subseteq \mathfrak{L}_k$, выполнены: (2.2), (2.7) и (2.8). Тогда по лемме 2.1.2 имеет место (2.9).

Если имеем μ_i, $\mu_i \in U(K(M))$, $i = 1, 2$, то для некоторых μ_i' и γ_i из $E_k'(\xi)$ для ЛА $g_i\,(x_i, x)$,

$$g_i\,(x_i, x) = \mu_i x_1 + \mu_i' x + \gamma_i$$

выполнены включения: $g_i \in K(M)$.

Поэтому для ЛА $h\,(x_1, x_2, x)$,

$$h\,(x_1, x_2, x) = g_1\,(x_1, x) + g_2\,(x_2, x) + \underbrace{x + \cdots + x}_{p-1 \text{ раз } x} \in K(M),$$

в $E_k'(\xi)$ найдутся такие $\tilde{\mu}$ и $\tilde{\gamma}$, что

$$h\,(x_1, x_2, x) = \mu_1 x_1 + \mu_2 x_2 + \tilde{\mu} x + \tilde{\gamma} \in K(M).$$

Тогда

$$\mu_1 + \mu_2 \in U\,(h\,(x_1, x_1, x))\,,$$

$$\mu_1 \mu_2 \in U\,(h\,(h\,(x, x_1, x)\,, x, x))\,,$$

а, если к паре μ_1, μ_2 может быть применена операция fb, то к переменной x_2 ЛА $h\,(x_1, x_2, x)$ может быть применена операция обратной связи, в результате которой получим ЛА $h'\,(x_1, x)$, для которого

$$\mathrm{fb}\,(\mu_1, \mu_2) \in U\,(h'\,(x_1, x))\,.$$

Из этого получаем включение:

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

откуда и из леммы 1.3.1 вытекает равенство

$$K^{(1)}\,(U(M)) = U(K(M)).$$

Отсюда, из соотношения (2.2) и теоремы 2.1.1 следует равенство (2.1). Теорема 2.1.2 доказана.

2.2. Приведенная K-критериальная система

В этом параграфе мы найдем множество всех K-предполных классов в классе ЛА над конечным полем, являющееся приведенной критериальной системой в классе $\mathfrak{L}_k$.

Мы будем рассматривать общий случай, когда $k = p^m$ и E_k является полем по операциям сложения и умножения. При этом, если понадобится, нам придется выделять случай простого поля.

Далее введем некоторые подмножества $\mathfrak{L}_k$, для построения которых понадобятся определения из главы 1. Положим:

$$M_{0,\omega} = \left\{\ f \ \mid\ f \in \mathfrak{L}_k,\ U(f) \subseteq M^{(1)}_{0,\omega}\ \right\}. \tag{2.12}$$

$$M_{j,\omega} \ = \ \left\{\ f \ \mid\ f \in \mathfrak{L}_k,\ U(f) \subseteq M^{(1)}_{j,\omega}\ \right\}.$$

$j = 2, 3, \ldots.$

$$M_1 \ = \ \left\{\ f \ \mid\ f \in \mathfrak{L}_k,\ U(f) \subseteq M^{(1)}_{1}\ \right\}.$$

Таким образом,

$$\begin{aligned} M_1 \ = \ \{\ f \ \mid\ f \in \mathfrak{L}_k,\ \forall \mu \in U(M) \ \text{выполнено:} \\ \mu(\xi) - \mu(0) \in \xi^2 \cdot E'_k(\xi)\ \}. \end{aligned}$$

$$\begin{aligned} R^e_j \ = \ \Bigg\{\ f \ \mid\ f \in \mathfrak{L}_k,\ f\,(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0, \\ \forall i, i = 1, 2, \ldots, n, \ \text{если} \ x_i \ \text{— единственная существенная} \\ \text{переменная ЛА} \ f, \ \text{то} \ \mu_i \in \tilde{M}^{(1)}_j, \\ \text{в противном случае:} \ \mu_i \in R^{(1)}_j\ \Bigg\}, \end{aligned}$$

$$R_j^d \;=\; \Bigg\{\; f \;\mid\; f \in \mathfrak{L}_k,\;\; f\left(x_1, x_2, \ldots, x_n\right) = \sum_{i=1}^{n} \mu_i x_i + \mu_0,$$
$$\forall i, i = 1, 2, \ldots, n, \;\text{ если }\; x_i \text{ — единственная непосредственная}$$
$$\text{переменная ЛА }\; f, \;\text{ то }\; \mu_i \in \tilde{M}_j^{(1)},$$
$$\text{в противном случае: }\; \mu_i \in R_j^{(1)} \;\Bigg\},$$

$j = 0, 2, 3, \ldots$.

Нам понадобится множество J_k,

$$J_k = \{\; V_1,\;\; V_p,\;\; P_s,\;\; T_a,\;\; M_1,\;\; M_{i,\omega},\;\; R_i^e,\;\; R_i^d,\;\; \mid$$
$$s \in \{1, 2, \ldots, l\},\;\; a \in E_k,\;\; \omega \in \Omega_k,\;\; i \in \{0, 2, 3, \ldots\}\;\; \}.$$

Заметим, что в случае простого поля, удалив из J_k не существующие элементы, получим:

$$J_k = \{\; V_1,\;\; V_p,\;\; T_a,\;\; M_j,\;\; R_i^e,\;\; R_i^d\;\; \mid$$
$$a \in E_k,\;\; j \in \{0, 1, \ldots\},\;\; i \in \{0, 2, 3, \ldots\}\;\; \}.$$

При этом класс $M_{j,\mathrm{id}}$ мы обозначаем M_j.

Для начала докажем следующее утверждение.

Лемма 2.2.1. *Множество J_k состоит из замкнутых в $\mathfrak{L}_k$ классов, не совпадающих с $\mathfrak{L}_k$.*

Доказательство. K-замкнутость классов V_1, V_p, T_a, M_1, P_s обоснована леммой 1.2.1. K-замкнутость классов $M_{j,\omega}$, $j = 0, 2, 3, \ldots$, следует из $K^{(1)}$-замкнутости классов $M_{j,\omega}^{(1)}$, если обратиться к лемме 1.3.1, и определению этих классов.

Осталось показать замкнутость R_i^e, R_i^d для $i = 0, 2, 3, \ldots$. Существенную переменную ЛА будем называть e-переменной, а непосредственную переменную – d-переменной, в соответствии со знаками, используемыми для обозначения соответствующих классов. Введем метаобозначение λ для символа из множества $\{e, d\}$. Это позволит привести доказательство замкнутости классов сразу из обоих серий R_i^e, R_i^d.

Пусть ЛА f_j, $j = 1, 2, \ldots, 6$, определены равенствами (1.1), (1.2), (1.3), (1.4), (1.5), (1.6). Предположим, что $f_j \in R_i^\lambda$, $j = 1, 2$. Требуется доказать, что $f_j \in R_i^\lambda$ для $j = 3, 4, 5, 6$.

Набор коэффициентов при переменных x_i', $i = 1, 2, \ldots, n_1$, ЛА f_3 совпадает с соответствующим набором для f_1. Так как принадлежность классу R_i^λ зависит только от набора (неупорядоченного, учитывающего кратность) этих коэффициентов, то $f_3 \in R_i^\lambda$.

Для ЛА f_4 имеем следующий набор коэффициентов:

$$\mathfrak{M}(f_4) = \left\langle \mu_1, \mu_2, \ldots, \mu_{n_1-1} + \mu_{n_1} \right\rangle .$$

Если среди переменных в ЛА f_1 нет единственной λ-переменной, то выполнено:

$$\forall i', \;\; i' = 1, 2, \ldots, n_1, \;\; \mu_{i'} \in R_i^{(1)}.$$

Поэтому

$$\mu_{n_1-1} + \mu_{n_1} \in R_i^{(1)},$$

и все коэффициенты ЛА f_4 содержатся в $R_i^{(1)}$. Поэтому

$$f_4 \in R_i^\lambda.$$

Если ЛА f_1 имеет единственную λ-переменную, то и единственную λ-переменную имеет f_4, коэффициент для которой содержится в $\tilde{M}_i^{(1)}$, а все остальные коэффициенты содержатся в $R_i^{(1)}$. Поэтому $f_4 \in R_i^\lambda$ и в этом случае.

ЛА f_5 имеет набор коэффициентов:

$$\mathfrak{M}(f_5) = \left\langle \mu_1\mu_{n_1+n_2}, \mu_2\mu_{n_1+n_2}, \ldots, \mu_{n_1}\mu_{n_1+n_2}, \mu_{n_1+1}, \mu_{n_1+2}, \ldots, \mu_{n_1+n_2-1} \right\rangle .$$

Если ЛА f_2 не имеет единственной λ-переменной или имеет единственную λ-переменную $x_{n_1+n_2}$, а ЛА f_1 не имеет единственной λ-переменной, то все коэффициенты ЛА f_5 содержатся в $R_i^{(1)}$, поэтому

$$f_5 \in R_i^\lambda. \tag{2.13}$$

Пусть ЛА f_2 имеет единственную λ-переменную. Если она совпадает с $x_{n_1+n_2}$, то осталось рассмотреть случай, когда f_1 тоже содержит единственную λ-переменную. При этом, как нетрудно видеть, ЛА f_5 тоже содержит единственную λ-переменную, коэффициент при которой входит в множество $\tilde{M}_i^{(1)}$, а остальные коэффициенты из множества $R_i^{(1)}$. Поэтому (2.13) имеет место.

В оставшемся случае, если ЛА f_2 имеет единственную λ-переменную, не совпадающую с $x_{n_1+n_2}$, то эта переменная остается единственной λ-переменной и в f_5, коэффициент при которой входит в $\tilde{M}_i^{(1)}$, остальные коэффициенты содержатся в $R_i^{(1)}$. То есть и в этом случае выполнено (2.13).

Далее,

$$\mathfrak{M}(f_6) = \left\langle \frac{\mu_1}{1-\mu_{n_1}}, \frac{\mu_2}{1-\mu_{n_1}}, \ldots, \frac{\mu_{n_1-1}}{1-\mu_{n_1}}, \right\rangle,$$

где $\mu_{n_1}(0) = 0$. Если f_1 не имела единственной λ-переменной, то

$$\forall i',\ \ i' = 1, 2, \ldots, n_1 - 1,\ \ \frac{\mu_{i'}}{1-\mu_{n_1}} \in R_i^{(1)},$$

следовательно,

$$f_6 \in R_i^{\lambda}. \tag{2.14}$$

В противном случае, если x_{n_1} – единственная e-переменная ЛА f_1, то f_6 не имеет e-переменных, поэтому при $\lambda = e$ включение (2.14) имеет место. При $\lambda = d$, когда f_1 имеет единственную d-переменную x_{l_0}, то она не совпадает с x_{n_1} и остается единственной d-переменной для ЛА f_6. При этом

$$\mu_{n_1} \in R_i^{(1)},$$

$$\frac{\mu_{l_0}}{1-\mu_{n_1}} \in \tilde{M}_i^{(1)},$$

а при

$$i' \neq l_0$$

выполнено:

$$\frac{\mu_{i'}}{1-\mu_{n_1}} \in R_i^{(1)}.$$

Следовательно, и в этом случае имеет место включение (2.14) и операции композиции не выводят из множества R_i^λ.

Таким образом, доказана замкнутость всех классов из J_k. Для завершения доказательства леммы для каждого класса из рассматриваемого множества приведем пример ЛА, не содержащегося в этом классе:

$$x_1 + x_2 \notin V_1 \cup V_p \cup \left(\bigcup_i R_i^e\right) \cup \left(\bigcup_i R_i^d\right),$$

$$1 \notin T_0,$$

$$\xi x \notin \left(\bigcup_{a, a\neq 0} T_a\right) \cup \left(\bigcup_{j,\omega} M_{j,\omega}\right) \cup M_1,$$

пусть b — примитивный элемент поля E_k, тогда

$$bx \notin \left(\bigcup_s P_s\right).$$

Лемма 2.2.1 доказана.

Теорема 2.2.1. *Множество K-замкнутых классов J_k является K-критериальной системой [42] в $\mathfrak{L}_k$, то есть для любого подмножества M множества $\mathfrak{L}_k$ его K-полнота в $\mathfrak{L}_k$ равносильна невключению в каждый замкнутый класс множества J_k.*

Доказательство. Рассмотрим подмножество M множества $\mathfrak{L}_k$ такое, что $\forall\Theta, \Theta \in J_k$, справедливо

$$M \nsubseteq \Theta. \tag{2.15}$$

Тогда имеет место (2.2). Справедливость утверждения (2.7) следует из (2.15) и определения классов $M_{i,\omega}$, $\omega \in \Omega_k$, $i = 0, 2, 3 \ldots$, M_1, R_j^e, R_j^d, $j = 0, 2, 3, \ldots$, V_1, P_s, $s = 1, 2, \ldots, l$.

Докажем справедливость утверждения (2.8). Требуется доказать, что из включения

$$U(M) \subseteq \tilde{M}_i^{(1)}. \tag{2.16}$$

вытекает

$$U(K(M)) \not\subseteq \tilde{M}_i^{(1)}. \qquad (2.17)$$

Для этого нам понадобится понятие i-сумматора. ЛА $g(x_1, x_2)$,

$$g(x_1, x_2) = \mu_1 x_1 + \mu_2 x_2 + \mu_0,$$

называется i-сумматором , $i \in \{0, 2, 3, \dots\}$, если

$$\Psi_i\left(\mu_j\right) = (1, 1), \;\; j = 1, 2.$$

Пусть $K(M)$ содержит i-сумматор $h\left(x_1, x_2\right)$,

$$h = \mu_1 x_1 + \mu_2 x_2 + \nu,$$

и пусть ЛА f_j, $f_j \in \mathfrak{L}_k$, таковы, что

$$f_j\left(x_{j,1}, x_{j,2}, \dots, x_{j,n_j}\right) = \sum_{r=1}^{n_j} \mu_{j,r} x_{j,r} + \mu_{j,0},$$

$j = 1, 2.$

Выберем произвольно r_j, $r_j \in \{1, 2, \dots, n_j\}$, $j = 1, 2$. Тогда, как нетрудно видеть,

$$\begin{aligned}\Psi_i(\mu_{1,r_1} \cdot \mu_{2,r_2}) \;\; &\in \;\; \Psi_i\left(U\left(f_1\left(x_{1,1}, x_{1,2}, \dots, x_{1,r_1-1},\right.\right.\right. \\ &\left.\left.\left. f_2\left(x_{2,1}, x_{2,2}, \dots, x_{2,n_2}\right), x_{1,r_1+1}, \dots, x_{1,n_1}\right)\right)\right),\end{aligned}$$

$$\begin{aligned}\Psi_i(\mu_{1,r_1} + \mu_{2,r_2}) \;\; &\in \;\; \Psi_i\left(U\left(h\left(f_1(x_{1,1}, x_{1,2}, \dots, x_{1,r_1}, \dots, x_{1,n_1}),\right.\right.\right. \\ &\left.\left.\left. f_2(x_{2,1}, x_{2,2}, \dots, x_{2,r_2}, \dots, x_{2,n_2})\right)\right)\right),\end{aligned}$$

Так как выполнено (2.7), то множество $U(M)$ является $K^{(1)}$-полным. Отсюда и из лемм 1.3.6, 1.3.7 следует, что в $U(S(M))$ содержится такое $\tilde{\mu}$, что

$$\tilde{\mu}(0) = 0 \;\text{ и }\; \tilde{\mu} \in \tilde{M}_i^{(1)} \setminus R_i^{(1)}.$$

Следовательно, найдется константный ЛА $\tilde{\nu}$ такой, что ЛА $\tilde{g}$,

$$\tilde{g}(x) = \tilde{\mu}x + \tilde{\nu},$$

содержится в $K(M)$. Тогда для любых натуральных чисел τ и T к переменной x_2 ЛА

$$h\left(x_1, \tilde{g}^{Tp^\tau}(x_2)\right)$$

применима операция обратной связи, и найдутся такие T и τ, что в результате применения этой операции получаем ЛА $\tilde{h}(x_1)$,

$$\tilde{h}(x_1) = \tilde{\mu}' x_1 + \tilde{\nu}',$$

такой, что

$$\tilde{\mu}' \not\subseteq \tilde{M}_i^{(1)},$$

то есть (2.17) справедливо.

По лемме 1.2.2 в $K(M)$ содержится константный ЛА ν_0.

Нетрудно видеть, что если ЛА f,

$$f(x_1, x_2, x) = \mu_1' x_1 + \mu_2' x_2 + \mu_3' x + \nu' \in S(M),$$

таков, что x_1 и x_2 — непосредственные переменные и $\mu_j' \notin R_i^{(1)}$, $j = 1, 2$, а ν' – константный ЛА, то множество $S(\{f, \nu_0\})$, а, следовательно, и $K(M)$, содержат i-сумматор, то есть имеет место (2.17). Это вытекает из существования таких натуральных чисел $\hat{T}_j$, что

$$\Psi_i\left(\left(\mu_j'\right)^{\hat{T}_j}\right) = (1, 1),$$

$j = 1, 2$.

Рассмотрим ЛА $g\left(x_1, x_2, \ldots, x_{n'}\right) \in M \setminus R_i^e$,

$$g\left(x_1, x_2, \ldots, x_{n'}\right) = \sum_{j=1}^{n'} \mu_j' x_j + \mu'. \tag{2.18}$$

Из (2.16) и определения класса R_i^e следует, что правая часть разложения (2.18) содержит не менее двух ненулевых коэффициентов, причем хотя бы один из них не содержится в $R_i^{(1)}$. Без ограничения общности, предположим, что $\mu_1' \notin R_i^{(1)}$ и $\mu_2' \neq 0$.

Тогда для ЛА g',

$$g'(x_1, x_2) = g(x_1, x_2, \nu_0, \nu_0 \ldots, \nu_0),$$

найдется ν_0', $\nu_0' \in E_k'(\xi)$, такое, что

$$g'(x_1, x_2) = \mu_1' x_1 + \mu_2' x_2 + \nu_0'.$$

Случай 1. Если $\mu_1'(0) = 0$, то найдутся натуральные числа T и τ такие, что

$$\frac{\mu_2'}{1 - (\mu_1')^{T \cdot p^\tau}} \notin \tilde{M}_i^{(1)},$$

то есть выполнено (2.17).

Случай 2. $\mu_1'(0) \neq 0$. Рассмотрим следующие случаи.

Случай 2.1. $\mu_2' \notin R_i^{(1)}$. Тогда при $\mu_2'(0) = 0$, как и в случае 1, получим справедливость соотношения (2.17), а при $\mu_2'(0) \neq 0$, учитывая отмеченное выше, заключаем, что $K(M)$ содержит i-сумматор.

Случай 2.2. Пусть $\mu_2' \in R_i^{(1)}$. Рассматриваем:

Случай 2.2.1. $\mu_2'(0) \neq 0$. Тогда, используя операции суперпозиции, из ЛА $g'(x_1, x_2)$ и константы ν_0 получим ЛА $g''(x_1, x_2)$,

$$g'' = g'(\underbrace{g'(\ldots g'(g'}_{k-2 \text{ раз } g'}(x_1, \nu_0), \nu_0) \ldots,), \underbrace{g'(\nu_0, g'(\nu_0, \ldots g'}_{k-2 \text{ раз } g'}(\nu_0, x_2) \ldots))),$$

$$g''(x_1, x_2) = \mu_1'' x_1 + \mu_2'' x_2 + \mu_0'',$$

где $\mu_j'' = (\mu_i')^{k-1}$, $j = 1, 2$.

Имеем:

$$\mu_j''(0) = 1, \;\; j = 1, 2, \quad \mu_1'' \notin R_i^{(1)}, \;\; \mu_2'' \in R_i^{(1)}.$$

В $K(M)$ содержится ЛА $\tilde{g}(x_1, x_2)$,

$$\tilde{g} = \underbrace{g''(x_1, g''(x_1, \ldots, g''}_{p \text{ раз } g''}(x_1, x_2) \ldots)),$$

Имеем

$$\tilde{g}\,(x_1, x_2) = \tilde{\mu}_1 x_1 + \tilde{\mu}_2 x_2 + \tilde{\mu}_0,$$

причем

$$\tilde{\mu}_1 = \sum_{j=0}^{p-1} \mu_1'' \left(\mu_2''\right)^j,$$

$$\tilde{\mu}_2 = \left(\mu_2''\right)^p,$$

для которых

$$\tilde{\mu}_1(0) = 0,\ \ \tilde{\mu}_1 \notin R_i^{(1)},\ \ \tilde{\mu}_2 \neq 0.$$

Как показано в случае 1, используя ЛА $\tilde{g}$ и операции композиции, можно получить ЛА $\hat{g}$ такой, что

$$U(\hat{g}) \notin \tilde{M}_i^{(1)},$$

то есть (2.17) справедливо.

Осталось рассмотреть

Случай 2.2.2. $\mu_2'(0) = 0$. Тогда x_1 — единственная непосредственная переменная ЛА

$$g' = g'\,(x_1, x_2)\,.$$

По условию найдется ЛА f, $f \in M \setminus R_i^d$. Для f имеем разложение (1.9). ЛА f имеет переменную, которая не является единственной непосредственной и коэффициент при которой в разложении (1.9) не содержится в $R_i^{(1)}$. Не ограничивая общность рассуждений, полагаем, что x_1 не является единственной непосредственной переменной ЛА f и $\mu_1 \notin R_i^{(1)}$.

Если $\mu_1(0) = 0$, то из ЛА

$$g'\left(f\left(x_1, \nu_0, \nu_0, \ldots, \nu_0\right), x_2\right),$$

как и в случае 1, с использованием операций композиции можно получить ЛА $\tilde{f}$ такой, что $U(\tilde{f}) \notin \tilde{M}_i^{(1)}$, то есть выполнено (2.17).

Если $\mu_1(0) \neq 0$, то, не ограничивая общности рассуждений, среди переменных $x_2, x_3, \ldots x_n$ ЛА f есть непосредственная переменная. Предположим, что x_2

является этой непосредственной переменной. Тогда для ЛА $f(x_1, x_2, \nu, \nu, \dots, \nu)$ можно применить либо рассуждения случая 2.1, если $\mu_2 \notin R_i^{(1)}$, либо рассуждения случая 2.2.1, если $\mu_2 \in R_i^{(1)}$.

Таким образом, по теореме 2.1.2 множество M является K-полным.

В обратную сторону. Если

$$M \subseteq \mathfrak{L}_k \quad \text{и} \quad K(M) = \mathfrak{L}_k,$$

то по лемме 2.2.1множество M не может содержаться ни в одном из классов множества J_k, являющихся собственными замкнутыми подклассами в $\mathfrak{L}_k$.

Теорема доказана.

Теорема 2.2.2. *Множество J_k является приведенной K-критериальной системой.*

Доказательство. Требуется показать, что для любых различных элементов Θ и Θ' множества J_k справедливо:

$$\Theta \not\subseteq \Theta'. \tag{2.19}$$

Сначала рассмотрим случай поля E_k, не являющегося простым.

Множество J_k разобьем на три подмножества:

$$J'_k = \{\ V_1,\ V_p,\ T_a \mid a \in E_k\ \},$$

$$J''_k = \{\ P_s,\ M_1,\ M_{i,\omega} \mid s \in \{1, 2, \dots, l\}, i \in \{0, 2, 3, \dots\}, \omega \in \Omega_k\ \},$$

$$J'''_k = \{\ R_i^e,\ R_i^d \mid i \in \{0, 2, 3, \dots\}\ \}.$$

Для каждого Θ, $\Theta \in J'_k$, укажем такое множество $\hat{\Theta}$, что

$$\hat{\Theta} \subset \Theta, \tag{2.20}$$

но для любого Θ', $\Theta' \in J_k \setminus \{\Theta\}$ выполнено:

$$\hat{\Theta} \not\subseteq \Theta' : \tag{2.21}$$

$$\hat{V}_1 = \{\ \xi x_1 + \xi x_2 + 1,\ \ bx\ \},$$

$$\hat{V}_p = \{\ \xi x_1 + x_2 + 1,\ \ bx_1 + bx_2 + \dots + bx_p + x_{p+1}\ \},$$

$$\hat{T}_a = \{\ (p-1)bx_1 + bx_2 + a,\ \ \xi x_1 + \xi x_2 + a\ \},$$

$a \in E_k$, где через b обозначен некоторый примитивный элемент поля E_k.

Свойства (2.20) и (2.21) для элементов множества J_k' устанавливаются с использованием простой проверки.

Далее заметим, что каждый класс из множества J_k'' содержит сумматор $x_1 + x_2$ и все константы, но никакой класс из множества $J_k' \cup J_k'''$ этим свойством не обладает. Поэтому ни один класс из множества J_k'' не является подмножеством никакого класса из $J_k' \cup J_k'''$. Теперь, воспользовавшись определением классов из множества J_k'', а также леммой 1.3.12, заключаем, что для любых различных Θ и Θ' из J_k'' выполнено:

$$\Theta \not\subseteq \Theta'.$$

Наконец, каждому классу Θ из множества J_k''' сопоставим подмножество элементов $\hat{\Theta}$ этого класса, не содержащееся ни в одном другом классе из J_k, следующим образом:

$$\hat{R}_0^e = \left\{\ \frac{\xi}{1+\xi}x,\ \ \frac{b}{1+\xi}x_1 + \frac{b}{1+\xi}x_2,\ \ 1\ \right\},$$

$$\hat{R}_i^e = \left\{\ \xi x,\ \ b\frac{p_i}{p_i(0)}x_1 + p_i x_2,\ \ 1\ \right\},$$

$i = 2, 3 \dots,$

$$\hat{R}_0^d = \left\{\ \frac{\xi}{1+\xi^2}x_1 + bx_2,\ \ \frac{b}{1+\xi}x_1 + \frac{b}{1+\xi}x_2,\ \ 1\ \right\},$$

$$\hat{R}_i^d = \{\ bx_1 + \xi p_i x_2,\ \ p_i x_1 + p_i x_2,\ \ 1\ \},$$

$i = 2, 3 \dots.$

Проверка позволяет установить справедливость свойств, требуемых от множества $\hat{\Theta}$, если $\Theta \in J_k'''$.

Теперь рассмотрим случай простого поля. Положим:

$$\hat{V}_1 = \{\ \xi x_1 + \xi x_2,\ \ 1\ \},$$

$$\hat{V}_p = \{\ \xi x_1 + x_2 + 1,\ \ x_1 + x_2 + \cdots + x_{p+1}\ \},$$

$$\hat{T}_a = \{\ \xi x_1 + a,\ \ x_1 + x_2 + \cdots + x_{p+1}\ \},$$

$a = 0, 1, \ldots, k-1,$

$$\hat{M}_0 = \left\{\ x_1 + x_2 + 1,\ \ \frac{\xi}{1+\xi^2}x\ \right\},$$

$$\hat{M}_j = \{\ x_1 + x_2 + 1,\ \ \xi p_j x\ \},$$

$j = 1, 2, \ldots,$

$$\hat{R}^e_0 = \left\{\ \frac{\xi}{1+\xi}x,\ \ \frac{1}{1+\xi}x_1 + \frac{1}{1+\xi}x_2 + 1\ \right\},$$

$$\hat{R}^e_i = \{\ \xi x,\ \ p_i x_1 + p_i x_2 + 1\ \},$$

$i = 2, 3, \ldots,$

$$\hat{R}^d_0 = \left\{\ \frac{\xi}{1+\xi^2}x_1 + x_2 + 1,\ \ \frac{1}{1+\xi}x_1 + \frac{1}{1+\xi}x_2\ \right\},$$

$$\hat{R}^d_i = \left\{\ x_1 + \xi p_i x_2 + 1,\ \ \frac{p_i}{p_i(0)}x_1 + \frac{p_i}{p_i(0)}x_2\ \right\},$$

$i = 2, 3, \ldots.$

Проверкой убеждаемся, что и в случае простого поля

$$\forall \Theta, \Theta' \in J_k,\ \ \Theta \neq \Theta'$$

выполнены соотношения:

$$\hat{\Theta} \subset \Theta,$$

$$\hat{\Theta} \not\subseteq \Theta'.$$

Теорема 2.2.2 доказана.

Из доказанной критериальности и приведенности множества J_k, используя известные рассуждения [42], получаем следующий результат.

Теорема 2.2.3. *Множество J_k состоит из K-предполных классов в $\mathfrak{L}_k$ и содержит все K-предполные классы.*

2.3. Об алгоритме проверки полноты

Решение задачи нахождения всех предполных классов в $\mathfrak{L}_k$ позволяет построить полиномиальный алгоритм проверки полноты конечных множеств ЛА над полем E_k. Мы будем рассматривать случай поля, не являющегося простым, и давать комментарии для случая простого поля при необходимости.

Многочлен u из $E_k[\xi]$ будем называть некратным, если для любого v, $v \in E_k[\xi] \setminus E_k$, многочлен u не делится на v^2. Некратный многочлен v, $v \in E_k[\xi]$, будем называть сокращением многочлена u, $u \in E_k[\xi]$, если множества неприводимых приведенных делителей этих многочленов совпадают. Нам понадобится следующая лемма.

Лемма 2.3.1. *Существует алгоритм, который за время $O(d^2)$ находит сокращение многочлена степени d, $d \in \mathbb{N}$.*

Доказательство. На вход алгоритм получает многочлен u_0 из $E_k[\xi]$ степени d. Этот многочлен имеет вид:

$$u_0 = v_0 \cdot v_1^p \cdot v_2^{p^2} \cdot \dots \cdot v_{s-1}^{p^{s-1}},$$

где для каждого i, $i = 0, 1, \dots, s-1$, кратность каждого неприводимого делителя многочлена v_i меньше p.

Степень многочлена v_i обозначим d_i, $i = 0, 1, \dots, s-1$. Имеет место равенство:

$$d = \sum_{i=0}^{s-1} d_i p^i. \tag{2.22}$$

Сначала выделим сокращение сомножителя v_0 и многочлен u_1,

$$u_1 = v_1 \cdot v_2^p \cdot v_3^{p^2} \cdot \dots \cdot v_{s-1}^{p^{s-2}}.$$

Имеем:

$$u_0 = v_0 \cdot u_1^p.$$

Производную [20] по ξ многочлена $\tilde{u}$, $\tilde{u} \in E_k[\xi]$, мы обозначаем $\frac{d\tilde{u}}{d\xi}$. Нетрудно видеть, что имеет место равенство:

$$\frac{du_0}{d\xi} = \frac{dv_0}{d\xi} \cdot u_1^p.$$

Наибольший общий делитель многочленов u_0 и $\frac{du_0}{d\xi}$ обозначим w_0. Многочлен $\frac{u_0}{w_0}$ является сокращением для v_0.

Будем вычислять производные многочлена u_0: $\frac{du_0}{d\xi}, \frac{d^2u_0}{d\xi^2}, \frac{d^3u_0}{d\xi^3}, \ldots$ до тех пор, пока получим константу 0. Ясно, что с точностью до ненулевого сомножителя из E_k производная, полученная на предыдущем шаге, совпадает с u_1^p. Не ограничивая общности рассуждений, будем предполагать, что многочлен u_1^p найден. Подставляя ξ вместо ξ^p в u_1^p, получим u_1.

Для реализации рассмотренных действий потребуется не более C_1d^2 операций над элементами поля E_k.

Используя рассмотренные действия, можно получить сокращения для всех многочленов v_i, $i = 0, 1, \ldots, s-1$. Произведение этих сокращений является сокращением для многочлена u_0.

Для построения многочленов v_i, $i = 0, 1, \ldots, s-1$, используется не более

$$C_1d^2\left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots \frac{1}{p^{s-1}}\right) \leq C_2d^2$$

операций в поле E_k.

Оценивая сверху количество таких операций при перемножении сокращений с учетом 2.22, получаем:

$$C_3\sum_{i=0}^{s-2}\left(d_{i+1}\sum_{j=0}^{i}d_j\right) \leq C_3\left(\sum_{j=0}^{s}d_j\right)^2 \leq C_3d^2.$$

Поэтому лемма доказана.

Пусть имеется множество M, $M \subset \mathfrak{L}_k$, $|M| < \infty$, причем каждый ЛА f из M задан набором несократимых дробей $\hat{U}(f)$, являющихся коэффициентами при переменных ЛА f, и константной частью $C(f)$. По наборам $\hat{U}(f)$ строится множество $U(M)$ всех коэффициентов при переменных множества M.

Шаг 1. Проверяем включения:

$$M \subset V_1,$$

$$M \subset V_p,$$

$$M \subset M_1,$$

$$M \subset P_s, \quad s = 1, 2, \dots l, \text{ (в случае простого поля этой проверки нет),}$$

$$M \subset T_a, \quad a \in E_k.$$

Если хотя-бы одно из этих включений выполнено, то множество M не является K-полным в $\mathfrak{L}_k$, алгоритм заканчивает работу.

Шаг 2. Проверяем, верно ли включение:

$$U(M) \subset \tilde{M}_0^{(1)}.$$

Если нет, то переходим к шагу 4.

Шаг 3. Находим множество

$$\Psi_0(U(M)) = \{\ \Psi_0(\mu)\ |\ \mu \in U(M)\ \}.$$

Пусть a — какой-либо примитивный элемент поля E_k. Каждый сопряженный к a элемент b поля E_k порождает автоморфизм ω поля E_k такой, что

$$\omega(a) = b.$$

При этом сопряженные к a элементы ищутся как корни минимального многочлена, корнем которого является a. Такими корнями являются: $a^{p^0} = a$, a^{p^1}, a^{p^2}, $\dots$, $a^{p^{m-1}}$. Следовательно, количество рассматриваемых автоморфизмов ограничено числом m [20]. Для каждого автоморфизма ω проверяем включение

$$\Psi_0(U(M)) \subset M_{0,\omega}.$$

Если хотя бы одно из включений выполнено, то M не является полным в $\mathfrak{L}_k$, алгоритм заканчивает работу.

В случае простого поля следует только проверить включение

$$M \subset M_0.$$

Если оно выполняется, то множество M не является K-полным, алгоритм заканчивает работу. Если нет, то работает дальше.

Шаг 4. Для каждого автоморфизма ω поля E_k находим наибольший общий делитель D_ω числителей дробей из множества U'_ω,

$$U'_\omega = \{ \ \mu - \omega\left(\mu(0)\right) \ \mid \ \mu \in U(M) \ \}.$$

Если

$$\deg(D_{\mathrm{id}}) > 1 \tag{2.23}$$

или найдется ω, $\omega \in \Omega \setminus \{\mathrm{id}\}$, такое, что

$$\deg(D_\omega) > 0, \tag{2.24}$$

то для некоторого i, $i \in \{2, 3, \dots\}$, множество M содержится в предполном классе $M_{i,\mathrm{id}}$ или $M_{i,\omega}$, соответственно, и не является полным в $\mathfrak{L}_k$. Алгоритм заканчивает работу.

Шаг 5. Проверяем включения:

$$M \subset R_0^e,$$

$$M \subset R_0^d.$$

Если хотя бы одно из этих включений выполнено, то множество M не является K-полным. Алгоритм заканчивает работу. В противном случае осуществляется переход к шагу 6.

Шаг 6. Находим наибольший общий делитель D_e числителей дробей из множества U^e,

$$U^e = \{ \ \mu \ \mid \ \text{в } M \text{ имеется ЛА, а в нем переменная с}$$

$$\text{коэффициентом } \mu, \text{ не являющейся единственной существенной} \}.$$

Находим наибольший общий делитель D_d числителей дробей из множества U^d,

$$U^d = \{\ \mu\ |\ \ \text{в}\ M\ \text{имеется ЛА, а в нем переменная с}$$

$$\text{коэффициентом}\ \mu,\ \text{не являющейся единственной непосредственной}\}\,.$$

Далее вычисляем сокращения D'_e и D'_d для многочленов D_e и D_d, соответственно.

Нам понадобятся следующие множества дробей:

$$K_e = U(f) \setminus U^e,$$

$$K_d = U(f) \setminus U^d.$$

Через D''_ρ обозначим наибольший общий делитель D'_ρ и произведения всех знаменателей дробей из K_ρ. Многочлены D''_ρ, $\rho \in \{e, d\}$, являются некратными. В случае, когда

$$\deg D''_\rho < \deg D'_\rho \tag{2.25}$$

хотя бы для одного ρ, множество M не является K-полным, и алгоритм заканчивает работу с отрицательным результатом. В противном случае,

$$K(M) = \mathfrak{L}_k,$$

и алгоритм заканчивает работу с положительным результатом.

В качестве параметров для оценки времени работы этого алгоритма выберем следующие:

r — количество ЛА в множестве M, проверяемом на K-полноту;

n — максимальное количество переменных в ЛА множества M;

d — максимальная степень дробей из множества $U(M)$, при этом, как принято, $\deg \frac{u}{v} = \max(\deg u, \deg v)$ для несократимой дроби $\frac{u}{v}$

k — как и ранее, количество элементов конечного поля;

m – количество автоморфизмов поля E_k; в случае простого поля, $m = 1$;

l — количество максимальных подполей в поле E_k, если k не является простым.

В случае простого поля этот параметр опускается, а в случае k, не являющимся простым, в приведенных ниже результатах этого параграфа оценивается сверху числом k.

Несложный анализ приводит к следующей теореме.

Теорема 2.3.1. *Полученный алгоритм проверки полноты конечных подмножеств ЛА корректен и может быть реализован с временной сложностью*

$$O(rnk) + O\left(rnd^2m\right)$$

для поля E_k, не являющегося простым. В случае простого поля E_k этот алгоритм может быть реализован с временной сложностью

$$O(rnk) + O\left(rnd^2\right).$$

Доказательство. Предложенный алгоритм проверяет справедливость включения конечного множества линейных автоматов M в каждый из классов Θ системы J_k. Проверка корректности может иметь смысл только для классов Θ,

$$\Theta \in \{\ M_{i,\omega}, R_i^e, R_i^e \ \mid\ i \in \{2, 3, \dots\}, \omega \in \Omega\ \},$$

невключение в которые проверяется на шагах 4 и 6 алгоритма.

На шаге 4 проверяются включения M в классы $M_{i,\omega}$.

Если выполнено (2.23), то ввиду соотношения $M \not\subseteq M_1$, проверенного на шаге 1, найдется неприводимый приведенный многочлен p_i, $i \in \{2, 3, \dots\}$, на который делится числитель каждой дроби из множества $\{\ \mu - \mu(0)\ \mid\ \mu \in U(M)\ \}$, то есть $M \subset M_{i,\mathrm{id}}$, согласно определению этого класса.

Если выполнено (2.24), то для некоторого i, $i \in \{2, 3, \dots\}$, и каждого μ, $\mu \in U(M)$ имеет место равенство

$$\Psi_i(\mu) = (\mu(0), \omega(\mu(0))),$$

поэтому $M \subset M_{i,\omega}$.

Таким образом, справедливость хотя бы одного из соотношений (2.23) или (2.24) влечет включение

$$M \subset M_{i,\omega} \tag{2.26}$$

для некоторой пары i, ω.

Пусть включение (2.26) не выполнено для каждой пары i, ω. Тогда, как нетрудно видеть, для любого ω, $\omega \in \Omega$, не может иметь место как (2.23), так и (2.24).

Таким образом, на шаге 4 алгоритма проверка включения в классы $M_{i,\omega}$ выполняется корректно.

Покажем корректность проверки включений

$$M \subseteq R_i^\rho, \tag{2.27}$$

$\rho \in \{e, d\}$, $i \in \{2, 3, \dots\}$, на шаге 6 алгоритма.

Нетрудно видеть, что неравенство (2.25) выполнено в точности тогда, когда найдется i, $i \in \{2, 3, \dots\}$, что p_i делит числитель каждой дроби из U^ρ и не делит знаменатель никакой дроби из K_ρ. Отсюда следует, что $M \subset R_i^\rho$.

В обратную сторону, если для данного ρ последнее включение не выполнено для любого i, $i \in \{2, 3, \dots\}$, то, согласно определению классов R_i^ρ, если некоторый неприводимый многочлен p_i делит числитель каждой дроби из U^ρ, то есть делит D_ρ, то знаменатель некоторой дроби из K_ρ делится на p_i. Поэтому D'_ρ делит произведение всех многочленов из K_ρ и $\deg D''_\rho = \deg D'_\rho$, то есть неравенство (2.25) не имеет места.

Корректность проверки соотношений $M \subset R_i^\rho$ на шаге 6 показана.

Выберем некоторый элемент b поля E_k, являющийся примитивным для этого поля. Для упрощения реализации алгоритма и оптимизации времени его работы проиндексируем элементы поля E_k: элемент 0 индексируем числом 0, каждый ненулевой элемент a индексируем степенью i такой, что $1 \leq i \leq k-1$ и $b^i = a$. Для элементов поля E_k, используя индексы, составим таблицы сложения, умножения, возведения в степень до степени $k-1$, таблицу принадлежности максимальным подполям P_s, $s = 1, 2, \ldots, l$. Для каждого автоморфизма поля E_k составим таблицу, сопоставляющую каждому элементу поля сопряженный ему элемент. После этого считаем, что соответствующие операции над элементами поля (сложение, умножение, возведение в степень, взятие любого сопряжения), а также выяснение принадлежности элемента поля E_k данному максимальному подполю выполняется за единицу времени.

Нетрудно видеть, что шаги 1-3 и 5 алгоритма могут быть реализованы с временной сложностью $O(rnk)$, шаг 4 — с временной сложностью $O\left(rnd^2m\right)$, а шаг 6, в согласно с леммой 2.3.1, имеет временную сложность $O\left(rnd^2\right)$. Таким образом, для случая поля, не являющегося простым, теорема доказана.

Результат теоремы для простого поля получаем, если учесть, что в этом случае $m = 1$.

Теорема 2.3.1 доказана.

Заметим, что рассмотренный алгоритм проверки K-полноты не использует процедуры разложения многочленов в произведение неприводимых многочленов, что может показаться необходимым в соответствии с определениями классов $M_{i,\omega}$ и R_i^ρ.

Следует также заметить, что для линейного автомата f, задаваемого равенством

$$f = \sum_{i=1}^{n} \mu_i x_i,$$

для которого

$$d = \max\{\ \deg \mu_i \mid i = 1, 2, \ldots, n\ \},$$

произведение nd ограничивает сверху число задержек, которое может быть использовано для реализации f схемой [29]. Следовательно, по количеству состояний автомата оценка сложности предложенного алгоритма проверки K-полноты все-же является экспоненциальной.

Глава 3

Замкнутые классы, содержащие сумматор

Известно, что проблема K-полноты для класса $\mathfrak{P}_2$ конечных автоматов над множеством E_2 алгоритмически неразрешима [42], о чем уже упоминалось в этой работе. В главах 1 и 2 для класса ЛА $\mathfrak{L}_{p^m}$, построен алгоритм, проверяющий K-полноту конечных систем. Алгоритм получен путем описания K-предполных классов.

Результаты, полученные в первой и второй главах, обуславливают переход к изучению K-замкнутых классов ЛА. В настоящей главе описаны K-замкнутые классы с сумматором $x_1 + x_2$ в классе ЛА над полем из двух элементов.

Пусть $M \subseteq \mathfrak{L}_2$ и $f \in \mathfrak{L}_2$. В соответствии с [42], будем говорить, что ЛА f K-выразим через M, если f может быть получен из элементов множества M с использованием операций композиции (суперпозиции и обратной связи). Множество M', $M' \subseteq \mathfrak{L}_2$, называется K-выразимым через M, если каждый ЛА из M' K-выразим через M.

Для $\mathfrak{P}_2$ известен критерий полноты систем, содержащих полную в классе функций алгебры логики подсистему [8]. Мы построили алгоритм, проверяющий выразимость в $\mathfrak{L}_2$ через конечные системы с двуместным сумматором и критерий вхождения этого сумматора в замкнутый класс. Следовательно, получен алгоритм, который по паре (M', M) конечных множеств из $\mathfrak{L}_2$ устанавливает справедливо ли включение

$$\{x_1 + x_2\} \cup M' \subseteq K\left(M\right).$$

Таким образом, в настоящей главе для класса $\mathfrak{L}_2$ линейных автоматов получено описание K-замкнутых классов, содержащих сумматор $x_1 + x_2$ и решена задача K-выразимости конечных систем с сумматором.

3.1. Необходимые понятия и обозначения

Результаты этой главы получены в работах [67], [69]. Мы рассматриваем ЛА как функции, переменные которых принимают значения из $R_2(\xi)$. Значения этих функций также являются элементами $R_2(\xi)$. ЛА рассматриваются с точностью до отношения равенства указанных функций. В этой главе и далее множество ЛА над полем E_2 мы будем обозначать $\mathfrak{L}$, вместо $\mathfrak{L}_2$.

На множестве $\mathfrak{L}$, как и ранее, помимо оператора K-замыкания, нам будет полезен оператор S-замыкания по операциям суперпозиции.

Для каждого ЛА f из $\mathfrak{L}$ выполнено разложение (1.9), коэффициенты μ_i которого являются элементами множества $E_2'(\xi)$, $i = 0, 1, \ldots, n$.

Положим

$$\mathfrak{L}_0 = \{\ f \ \mid \ f \in \mathfrak{L},\ \text{ в разложении (1.9) имеет место: } \mu_0 = 0.\ \},$$

Множество всех одноместных ЛА из $\mathfrak{L}$ обозначим $\mathfrak{L}^{(1)}$.

$$\mathfrak{L}^{(1)} = \{\ f \ \mid \ f \in \mathfrak{L},\ \ f : R_2(\xi) \to R_2(\xi)\ \},$$

а пересечение множеств $\mathfrak{L}_0$ и $\mathfrak{L}^{(1)}$ обозначим $\mathfrak{L}_0^{(1)}$.

Множество, состоящее из всех константных ЛА, обозначим $\mathfrak{L}_c$.

Нетрудно видеть, что каждый элемент как множества $\mathfrak{L}_0^{(1)}$, так и множества $\mathfrak{L}_c$ определяется некоторым элементом из $E_2'(\xi)$. Поэтому, чтобы избежать путаницы, мы ввели для этих множеств обозначения, отличные от $E_2'(\xi)$.

На множестве $\mathfrak{L}_0^{(1)}$, как и в главе 1, рассматривается оператор $K^{(1)}$-замыкания, включающий операции сложения, умножения и операцию fb. Оператор замыкания на этом множестве, включающий только сложение и умножение, как и прежде, обозначаем $S^{(1)}$.

Пусть ЛА f задана равенством (1.9) и $M \subseteq \mathfrak{L}$. В главе 1 были также введены следующие обозначения:

$$U(f) = \{\ \mu_i \ \mid \ i = 1, 2, \ldots, n\ \},$$

$$C(f) = \{\ \mu_0\ \},$$

$$U(M) = \bigcup_{f \in M} U(f).$$

Положим:

$$C(M) = \bigcup_{f \in M} C(f).$$

Каждой паре M, C, где $M \subseteq \mathfrak{L}_0^{(1)}$, $C \subseteq \mathfrak{L}_c$, соответствует множество

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

которое обозначим $S(M, C)$.

Лемма 3.1.1. *Пусть $M \subseteq \mathfrak{L}$.*

1. *Тогда выполнены включения:*

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

$$C(K(M)) \subseteq S(U(M), C(M)).$$

2. *В случае*

$$x_1 + x_2 \in K(M) \tag{3.1}$$

ЛА f, удовлетворяющий соотношению (1.9), содержится в $K(M)$ в точности тогда, когда для каждого i, $i = 1, 2, \dots, n$,

$$\mu_i \in K^{(1)}(U(M))$$

и

$$\mu_0 \in S(U(M), C(M)).$$

Доказательство. Утверждение 1 леммы нетрудно доказать, используя индукцию по построению элементов из $K(M)$ и равенства (1.1) -(1.6).

Докажем утверждение 2. Пусть выполнено (3.1), тогда

$$0 = x + x \in K(M).$$

Для ЛА f из M рассмотрим его разложение (1.9). Имеем:

$$\mu_0 = f(0, 0, \dots 0),$$

$$\mu_i x = \mu_0 + f(\underbrace{0, 0, \dots 0}_{i-1 \text{ раз } 0}, x, 0, 0, \dots 0).$$

Заметим, что из $\mu x \in K(M)$ и $\mu' x \in K(M)$ при условии (3.1) вытекают включения:

$$(\mu + \mu')x \in K(M)$$

$$(\mu \cdot \mu')x \in K(M),$$

а в случае $\mu'(0) = 0$ еще и включение $\mathrm{fb}\,(\mu, \mu')\, x \in K(M)$.

Таким образом, $\forall \mu$, $\mu \in K^{(1)}(U(M))$, справедливо включение: $\mu(x) \in K(M)$, то есть

$$K^{(1)}(U(M)) \subseteq U(K(M)). \tag{3.2}$$

Пусть теперь $\gamma \in S(U(M), C(M))$. Тогда для некоторого m, $m \in \mathbb{N}$, некоторых μ_i и γ_i, $\mu_i \in K^{(1)}(U(M))$, $\gamma_i \in C(M)$, $i = 1, 2, \dots, m$, справедливо равенство:

$$\gamma = \mu_1 \gamma_1 + \mu_2 \gamma_2 + \dots + \mu_m \gamma_m.$$

при этом, как показано выше, $\mu_i x_i \in K(M)$ и $\gamma_i \in K(M)$, $i = 1, 2, \dots, m$. Отсюда и из включения (3.1) следует $\gamma \in K(M)$. Таким образом,

$$S(U(M), C(M)) \subseteq C(K(M)). \tag{3.3}$$

Для произвольных μ_i, $\mu_i \in K^{(1)}(U(M))$, $i = 1, 2, \dots n$ и произвольного μ_0 из $S(U(M), C(M))$ с учетом включений (3.1), (3.2) и (3.3) получаем:

$$\sum_{i=1}^{n} \mu_i x_i + \mu_0 \in K(M).$$

Отсюда и из первого утверждения леммы вытекает ее второе утверждение.

Лемма доказана.

Из утверждения 2 леммы следует, что, если $x_1 + x_2 \in K(M)$, то

$$U(K(M)) = K^{(1)}(U(M))$$

$$C(K(M)) = S(U(M), C(M)).$$

Нетрудно видеть, что из (3.1) и части 1 леммы 3.1.1 следует

$$1 \in K^{(1)}(U(M)). \tag{3.4}$$

Поэтому в дальнейшем изучается множество $\mathfrak{L}_0^{(1)}$ и замыкания $K^{(1)}(M)$, $S(M, C)$, $|C| < \infty$, с некоторыми ограничениями на систему M, вытекающими из (3.4).

Рассмотрим следующие замкнутые в $\mathfrak{L}_0^{(1)}$ по операциям $"+"$, $"\cdot"$, $"\mathrm{fb}"$ классы.

$$\begin{gathered} M^{(1)}(\mu, u_0) = \left\{ a_0 + \mu u_0(\mu) \frac{u(\mu)}{v(\mu)} \;\middle|\; \right. \\ \left. a_0 \in E_2, u(\xi) \in E_2[\xi], v(\xi) \in 1 + \xi E_2[\xi], (u_0(\xi), v(\xi)) = 1 \right\}, \end{gathered}$$

$$\begin{gathered} P^{(1)}(\mu, u_0) = \left\{ a_0 + \mu u_0(\mu) \frac{u(\mu)}{v(\mu)} \;\middle|\; a_0 \in E_2, u(\xi) \in E_2[\xi], \right. \\ v(\xi) \in 1 + \xi E_2[\xi], (u_0(\xi), v(\xi)) = 1, \\ \left. \deg u(\xi) \leq \deg v(\xi) - 2(1 + \deg u_0(\xi)) \right\}, \end{gathered} \tag{3.5}$$

$$\begin{gathered} R^{(1)}(\mu, u_0) = \left\{ u_0(\mu) \frac{u(\mu)}{v(\mu)} \;\middle|\; \right. \\ \left. u(\xi) \in E_2[\xi], v(\xi) \in 1 + \xi E_2[\xi], (u_0(\xi), v(\xi)) = 1 \right\}, \end{gathered}$$

$\mu \in \xi \mathfrak{L}_0^{(1)}$, $u_0 \in E_2[\xi] \setminus \{0\}$.

Введем следующие обозначения

$$\mathfrak{L}_0^{(1)}(\mu) = M^{(1)}(\mu, 1),$$

$$M^{(1)}(u_0) = M^{(1)}(\xi, u_0),$$

$$R^{(1)}(u_0) = R^{(1)}(\xi, u_0).$$

Нетрудно видеть, что

$$\mathfrak{L}_0^{(1)}(\xi) = M^{(1)}(1) = R^{(1)}(1) = \mathfrak{L}_0^{(1)}.$$

Пусть $p_1, p_2, \dots$ - последовательность всех неприводимых многочленов из $E_2[\xi]$, $p_1 = \xi$ и $p_i \neq p_j$, если $i \neq j$. Положим

$$M_i^{(1)}(\mu) = M^{(1)}(\mu, p_i),$$

$$R_i^{(1)}(\mu) = R^{(1)}(\mu, p_i),$$

$i = 1, 2, \dots$

$$M_0^{(1)}(\mu) = \left\{ a_0 + \frac{\mu u(\mu)}{v(\mu)} \mid a_0 \in E_2, \right.$$
$$\left. u(\xi) \in E_2[\xi], v(\xi) \in 1 + \xi E_2[\xi], \deg \xi u(\xi) < \deg v(\xi) \right\},$$

$$R_0^{(1)}(\mu) = \left\{ \frac{u(\mu)}{v(\mu)} \mid \right.$$
$$\left. u(\xi) \in E_2[\xi], v(\xi) \in 1 + \xi E_2[\xi], \deg u(\xi) < \deg v(\xi) \right\},$$

$\mu \in \xi \mathfrak{L}_0^{(1)}$.

В дальнейшем $M_i^{(1)}(\xi)$ и $R_i^{(1)}(\xi)$ обозначаем соответственно $M_i^{(1)}$ и $R_i^{(1)}$, $i = 0, 1, 2, \dots$. Заметим, что эти обозначения для соответствующих классов были введены в параграфе 3 главы 1.

Как показано в теореме 1.3.2, множество $J_2^{(1)}$,

$$J_2^{(1)} = \left\{ \ R_i^{(1)}, \ \ M_i^{(1)} \ \mid \ i = 0, 1, 2, \dots \ \right\}$$

является приведенной K-критериальной системой в $\mathfrak{L}_0^{(1)}$, то есть для любого M, $M \subseteq \mathfrak{L}_0^{(1)}$, равенство

$$K^{(1)}(M) = \mathfrak{L}_0^{(1)}$$

выполнено в точности тогда, когда

$$M \not\subseteq \Theta$$

для любого Θ, $\Theta \in J_2^{(1)}$.

3.2. Замкнутые классы одноместных линейных автоматов, сохраняющих нулевую последовательность

K-замкнутые в $\mathfrak{L}_0^{(1)}$ классы, не содержащиеся в тех же предполных классах, в которых не содержится проводник, имеют структуру, описанную в следующей теореме.

Теорема 3.2.1. *1. Пусть*

$$\begin{aligned} &M \subseteq \mathfrak{L}_0^{(1)}, \quad K^{(1)}(M) = M, \quad M \setminus E_2 \neq \emptyset, \\ &M \not\subseteq R_i^{(1)}, \quad i = 0, 1, 2, \dots . \end{aligned} \tag{3.6}$$

Тогда найдутся μ, u_0, T, $\mu \in \xi\mathfrak{L}_0^{(1)}$, $u_0 \in 1 + \xi E_2[\xi]$, $T \in \mathbb{N}$, что выполнено одно из двух следующих соотношений

$$M^{(1)}(\mu, (\xi u_0)^T) \subseteq M \subseteq M^{(1)}(\mu, u_0) \tag{3.7}$$

$$P^{(1)}(\mu, (\xi u_0)^T) \subseteq M \subseteq M_0^{(1)}(\mu) \cap M^{(1)}(\mu, u_0) \tag{3.8}$$

2. Число $K^{(1)}$-замкнутых в $\mathfrak{L}_0^{(1)}$ классов M, удовлетворяющих включениям (3.7) или включениям (3.8) конечно.

Прежде, чем приступить к доказательству теоремы, проведем некоторые рассуждения.

Если $\mu' \in \mathfrak{L}_0^{(1)}(\mu)$, то найдутся $a_i, b_j, \quad i = 0, 1, \ldots, n', j = 1, 2, \ldots, n''$, такие, что

$$\mu' = \frac{a_0 + a_1\mu + a_2\mu^2 + \cdots + a_{n'}\mu^{n'}}{1 + b_1\mu + b_2\mu^2 + \cdots + b_{n''}\mu^{n''}}$$

Рассмотрим отображение Ψ_μ из $\mathfrak{L}_0^{(1)}(\mu)$ в $\mathfrak{L}_0^{(1)}$, положив

$$\Psi_\mu(1) = 1,$$

$$\Psi_\mu(\mu) = \xi,$$

$$\Psi_\mu(\mu' + \mu'') = \Psi_\mu(\mu') + \Psi_\mu(\mu''),$$

$$\Psi_\mu(\mu'\mu'') = \Psi_\mu(\mu')\Psi_\mu(\mu''),$$

$$\Psi_\mu(\frac{\mu'}{1 + \mu\mu''}) = \frac{\Psi_\mu(\mu')}{1 + \xi\Psi_\mu(\mu'')}$$

для любых μ', μ'' из $\mathfrak{L}_0^{(1)}(\mu)$.

Для множества M, $M \subseteq \mathfrak{L}_0^{(1)}(\mu)$, через $\Psi_\mu(M)$ обозначим $\{\ \Psi_\mu(\mu')\ \mid\ \mu' \in M\ \}$.

Лемма 3.2.1. *Пусть выполнены (3.6). Тогда найдутся* μ, μ_0, $\mu \in \xi\mathfrak{L}_0^{(1)} \setminus \{0\}$, $\mu_0 \in \mathfrak{L}_0^{(1)} \setminus \{0\}$, *что*

$$\{\mu\mu_0, \mu_0\} \subset S^{(1)}(M), \tag{3.9}$$

$$M \subseteq \mathfrak{L}_0^{(1)}(\mu), \tag{3.10}$$

$$K^{(1)}(\Psi_\mu(M)) = \Psi_\mu(M), \quad \Psi_\mu(M) \setminus E_2 \neq \emptyset, \tag{3.11}$$

$$\Psi_\mu(M) \not\subseteq R_i^{(1)}, \tag{3.12}$$

$i = 0, 1, 2, \ldots.$

Доказательство. Рассмотрим множество M, удовлетворяющее соотношениям (3.6). Поле $E_2(M)$, порожденное множеством M над полем E_2 по операциям сложения, умножения и деления, является простым трансцендентным расширением поля E_2 [20]. Поэтому найдется μ, $\mu \in E_2(\xi) \setminus E_2$, такой, что $E_2(M) = E_2(\mu)$. Не ограничивая общности рассуждений, будем предполагать, что $\mu \in \xi\mathfrak{L}$.

Поэтому найдется μ_0, $\mu_0 \in \xi\mathfrak{L}_0^{(1)} \setminus \{0\}$, такое, что выполнены включения (3.9) и (3.10). Соотношение (3.11) нетрудно получить исходя из (3.6).

Докажем (3.12) при $i = 0$.

Пусть $\mu = \frac{u}{v}$, многочлены u и v взаимно просты и

$$\mu' = \frac{a_0 + a_1\mu + \cdots + a_n\mu^n}{1 + b_1\mu + \cdots + b_{s-1}\mu^{s-1} + \mu^s}, \quad n < s.$$

Тогда

$$\mu' = \frac{\left(a_0v^n + a_1uv^{n-1} + \cdots + a_nu^n\right)v^{s-n}}{v^s + b_1uv^{s-1} + \cdots + b_{s-1}u^{s-1}v + u^s}$$

Поэтому в случае $\mu' \in R_0^{(1)}(\mu)$ и $\deg v \geq 1$, справедливо $\mu' \in R^{(1)}(v)$. Если же $\mu' \in R_0^{(1)}(\mu)$ и $v = 1$, то $\deg u \geq 1$ и $\mu' \in R_0^{(1)}$. Отсюда следует: $\Psi_\mu(M) \not\subseteq R_0^{(1)}$.

Нетрудно видеть, что (3.12) справедливо при $i = 1$.

Докажем (3.12) при $i \in \mathbb{N} \setminus \{0, 1\}$.

Рассмотрим неприводимые многочлены u', u'' из $E_2[\xi]$,

$$u' = 1 + a_1\xi + a_2\xi^2 + \cdots + a_{n'-1}\xi^{n'-1} + \xi^{n'},$$

$$u'' = 1 + b_1\xi + b_2\xi^2 + \cdots + b_{n''-1}\xi^{n''-1} + \xi^{n''}.$$

Тогда $v^{n'}u'\left(\frac{u}{v}\right) \in E_2[\xi]$ и $v^{n''}u''\left(\frac{u}{v}\right) \in E_2[\xi]$.

Если

$$\left\{v^{n'}u'\left(\frac{u}{v}\right), v^{n''}u''\left(\frac{u}{v}\right)\right\} \subseteq pE_2[\xi] \tag{3.13}$$

для некоторого неприводимого p из $E_2[\xi]$, то

$$u' = u''. \tag{3.14}$$

Действительно, пусть (3.14) не имеет места. Тогда найдутся многочлены u_1' и u_1'' из $E_2[\xi]$, $\deg u_1'(\xi) = n_1'$, $\deg u_1''(\xi) = n_1''$, что

$$u_1'(\xi)u'(\xi) + u_1''(\xi)u''(\xi) = 1,$$

поэтому

$$n' + n_1' = n'' + n_1'',$$

$$v^{n_1'}u_1'\left(\frac{u}{v}\right) \cdot v^{n'}u'\left(\frac{u}{v}\right) + v^{n_1''}u_1''\left(\frac{u}{v}\right) \cdot v^{n''}u''\left(\frac{u}{v}\right) = v^{n'+n_1'}$$

и

$$v \in pE_2[\xi].$$

Отсюда и из (3.13) получаем $u \in pE_2[\xi]$, противоречие с $(u, v) = 1$.

Равенство (3.14) доказано.

Далее, пусть $\Psi_\mu(M) \subseteq R^{(1)}(u'')$, $\deg u'' = n''$ и $v^{n''}u''(\mu) \neq 1$. Для любого μ', $\mu' \in M$, найдутся u_1 и u_2 - многочлены из $E_2[\xi]$ и найдутся целые неотрицательные числа k_1 и k_2 такие, что $\mu' = v^{n''}u''(\mu)\frac{v^{k_1}u_1(\mu)}{v^{k_2}u_2(\mu)}$ и $v^{k_i}u_i(\mu) \in E_2[\xi], \quad i = 1, 2$. Из приведенных выше рассуждений с учетом взаимной простоты многочленов v и $v^{n''}u''(\mu)$ следует

$$M \subseteq R^{(1)}\left(v^{n''}u''(\mu)\right)$$

Для завершения доказательства соотношения (3.12) при $i > 1$ осталось рассмотреть случай

$$\Psi_\mu(M) \subseteq R^{(1)}(u''), \quad v^{n''}u''(\mu) = 1 \tag{3.15}$$

Пусть $u''(\mu)\frac{u_1(\mu)}{v_1(\mu)} \in M$, $u_1(\xi) \in E_2[\xi]$ и $v_1(\xi) \in 1 + \xi E_2[\xi]$. Степени многочленов $u_1(\xi)$и $v_1(\xi)$ обозначим соответственно через t и s. Не ограничивая общности рассуждений, будем в дальнейшем считать, что $(v_1(\xi), u''(\xi)) = 1$ и $s > n''$. (Этих соотношений можно добиться, сначала представив дробь $\frac{u_1(\mu)}{v_1(\mu)}$ в несократимом виде, а потом умножив числитель и знаменатель полученной дроби на многочлен из $E_2[\mu]$ взаимно простой с $\mu u''(\mu)$.)

Имеет место тождество

$$u''(\mu)\frac{u_1(\mu)}{v_1(\mu)} = \left(v^{n''}u''(\mu)\right) \cdot \frac{(v^t u_1(\mu))\, v^s}{(v^s v_1(\mu))\, v^{n''+t}}.$$

Из (3.15) вытекает $\deg u(\xi) = \deg v(\xi)$. Нетрудно видеть, что в $E_2[\xi]$ найдутся $u_2(\xi)$, $u_3(\xi)$, удовлетворяющие равенству

$$v^s v_1(\mu) = v^s u''(\mu)u_2(\mu) + v^s \mu^{s-n''+1} u_3(\mu) \tag{3.16}$$

и неравенствам $u_3(\xi) \neq 0$, $\deg u_2(\xi) \leq s - n''$. Обозначим $\deg u(\xi)$ через k.

Имеют место следующие соотношения:

$$\begin{aligned} &\deg\,(v^s u''(\mu)u_2(\mu)) = \\ &\quad \deg\left((v^{n''}u''(\mu))(v^{\deg u_2(\xi)}u_2(\mu))v^{s-n''-\deg u_2(\xi)}\right) \leq k(s-n'') \end{aligned}$$

Нетрудно видеть, что выражения

$$v^s(\xi)v_1(\mu(\xi)), \quad v^s(\xi)u''(\mu(\xi))u_2(\mu(\xi))$$

являются многочленами из $E_2[\xi]$. Поэтому из (3.16) следует, что

$$v^s(\xi)\mu^{s-n''+1}(\xi)u_3(\mu(\xi)) \in E_2[\xi].$$

Так как $v^s(\xi)\mu^{s-n''+1}(\xi)u_3(\mu(\xi)) = u^{s-n''+1}(\xi)(v^{n''-1}(\xi)u_3(\mu(\xi)))$ и знаменатель дроби $v^{n''-1}(\xi)u_3(\mu(\xi))$ взаимно прост с $u(\xi)$, то $v^{n''-1}(\xi)u_3(\mu(\xi)) \in E_2[\xi]$. Поэтому

$$\deg\left(v^s(\xi)\mu^{s-n''+1}(\xi)u_3(\mu(\xi))\right) \geq (s-n''+1)k.$$

Таким образом,

$$\deg\,(v^s(\xi)v_1(\mu(\xi))) \geq (s-n''+1)k \tag{3.17}$$

Положим

$$u'(\xi) = \left(v^{n''}u''(\mu)\right)\left(v^t u_1(\mu)\right) v^s,$$

$$v'(\xi) = (v^s v_1(\mu))\, v^{n''+t},$$
$$\mu'(\xi) = \frac{u'}{v'}.$$

Для степеней числителя и знаменателя дроби $\mu'(\xi)$ из (3.17) следуют неравенства $\deg u'(\xi) \leq k \cdot s + k \cdot t$ и $\deg v'(\xi) \geq k(s+1) + kt$. Поэтому $\mu'(\xi) \in R_0^{(1)}$.

Ввиду равенства $\mu' = u''(\mu)\frac{u_1(\mu)}{v_1(\mu)}$ в случае (3.15) справедливо $M \subseteq R_0^{(1)}$.

Тем самым получено доказательство (3.12) при $i > 1$. Соотношение (3.12) доказано для любого i, $i \in \{0, 1, \dots\}$.

Лемма 3.2.1 доказана.

Доказательство теоремы 3.2.1 проведем при условии, что найдется $\mu_0, \mu_0 \in \mathfrak{L}_0^{(1)} \setminus \{0\}$, такой, что выполнено:

$$\{\mu_0, \xi\mu_0\} \subset S^{(1)}(M) \tag{3.18}$$

По лемме 3.2.1 это условие не ограничивает общность рассуждений.

Утверждение 1 теоремы 3.2.1 будет доказано, если в предположениях (3.6), (3.18) показать, что для некоторого $T, T \in \mathbb{N}$,

$$M^{(1)}\left((\xi u_0)^T\right) \subseteq M \subseteq M^{(1)}(u_0) \tag{3.19}$$

или

$$P^{(1)}\left((\xi u_0)^T\right) \subseteq M \subseteq M_0^{(1)} \cap M^{(1)}(u_0) \tag{3.20}$$

Через $\Omega(T', \mu')$, где $T' \in \mathbb{N}$, $\mu' \in 1 + \xi\mathfrak{L}_0^{(1)}$, обозначим следующее множество:

$$\left\{\ \xi^j \mu' \ \mid\ j \in \mathbb{N}, j \geq T'\ \right\}.$$

Через $\Omega_1(\lambda', \mu')$, где $\lambda' \in \mathbb{N}$, $\mu' \in 1 + \xi\mathfrak{L}_0^{(1)}$, $\mu' = \frac{u'}{v'}$, $\deg u' < \deg v' - 2$, обозначим множество

$$\left\{\ \xi^j \mu'\left(\xi^{2^{\lambda'}}\right)\ \mid\ j \in \mathbb{N}, 2^{\lambda'} \leq j \leq (\deg v'(\xi) - \deg u'(\xi) - 1)\, 2^{\lambda'}\ \right\}.$$

Лемма 3.2.2. *Пусть имеют место (3.6), (3.18). В случае*

$$M \not\subseteq M_0^{(1)} \tag{3.21}$$

для некоторых μ_1, T_0 *выполнено:*

$$\Omega\left(T_0, \mu_1^{T_0}\right) \subseteq K^{(1)}(M). \tag{3.22}$$

В случае

$$M \subseteq M_0^{(1)} \tag{3.23}$$

для некоторых μ_1 *и* λ_1 *выполнено:*

$$\Omega_1\left(\lambda_1, \mu_1\right) \subseteq K^{(1)}(M). \tag{3.24}$$

Доказательство (3.22) в случае (3.21) нетрудно получить, воспользовавшись обоснованием леммы 9 в [68].

Пусть выполнено (3.23).

Для некоторых n_1, μ_1, $n_1 \in \mathbb{N}$, $\mu_1 \in 1 + \xi\mathfrak{L}_0^{(1)}$, имеет место включение:

$$\left\{\xi^{n_1}\mu_1, \xi^{n_1+1}\mu_1\right\} \subset M.$$

Найдутся n_2 и n_3 из $\mathbb{N}$, что

$$\mu_1 = \frac{a_{1,0} + a_{1,1}\xi + \cdots + a_{1,n_2-1}\xi^{n_2-1} + \xi^{n_2}}{1 + a_{2,1}\xi + \cdots + a_{2,n_3-1}\xi^{n_3-1} + \xi^{n_3}},$$

где $a_{ij} \in E_2$. Если $n_2 > 0$, то в последнем равенстве $a_{10} = 1$.

Из (3.23) вытекают неравенства

$$n_3 > n_2 + n_1 + 1,$$

$$\mu_1 \neq 1.$$

Положим

$$A_0 = \{\ (j_1, j_2)\ \mid n_1 j_1 \leq j_2 \leq (n_1+1)j_1, j_1 \in \mathbb{N} \setminus \{0\}\ \}.$$

Для любого i, $i \in \mathbb{N} \setminus \{0\}$, найдутся и притом единственным образом числа n' и n'', удовлетворяющие соотношениям

$$n' \in \mathbb{N} \setminus \{0\},$$

$$n'' \in \{1, 2, \ldots, n_3 - n_2 - n_1 - 1\},$$

$$i = (n_3 - n_2 - n_1 - 1)(n' - 1) + n''.$$

Если выполнены последние три соотношения, то положим

$$A'_i = \{\ (j_1, j_2)\ \mid\ j_2 = (n_1 + 1)j_1 + i, j_1 \geq n' + n_3 - 2\ \},$$

$$A''_i = \{\ (j_1, j_2)\ \mid\ j_2 = n_1 j_1 - i, j_2 \geq (n_3 - 1)n_1\ \},$$

$i = 1, 2, \ldots$.

Множество $\bigcup_{i=1}^{r} (A'_i \cup A''_i) \cup A_0$ обозначим через A_r, $r = 1, 2, \ldots$. Положим

$$A = \bigcup_{r=1}^{\infty} A_r.$$

Покажем, что для любой пары (j_1, j_2) из A справедливо

$$\xi^{j_2} \mu_1^{j_1} \in K^{(1)}(M). \tag{3.25}$$

Соотношение (3.25) выполнено, очевидно, если $(j_1, j_2) \in A_0$. Пусть (3.25) имеет место для любой (j_1, j_2), $(j_1, j_2) \in A_{r-1}$, $r \geq 1$. Из соотношения $(j_1, j_2) \in A'_r$ следует

$$\begin{aligned} \{(j_1, j_2 - n_3), (j_1, j_2 - n_3 + 1), \ldots (j_1, j_2 - 1), (j_1 - 1, j_2 - n_3), \\ (j_1 - 1, j_2 - n_3 + 1), \ldots (j_1 - 1, j_2 - n_3 + n_2)\} \subseteq A_{r-1}, \end{aligned} \tag{3.26}$$

а из $(j_1, j_2) \in A''_r$ следует

$$\begin{aligned} \{(j_1, j_2 + 1), \ldots, (j_1, j_2 + n_3 - 1), (j_1, j_2 + n_3), \\ (j_1 - 1, j_2), (j_1 - 1, j_2 + 1), \ldots (j_1 - 1, j_2 + n_2 - 1), \\ (j_1 - 1, j_2 + n_2)\} \subseteq A_{r-1}, \end{aligned} \tag{3.27}$$

Воспользуемся тождеством

$$\begin{aligned} \mu_1 + a_{2,1}\xi\mu_1 + \cdots + a_{2,n_3-1}\xi^{n_3-1}\mu_1 + \xi^{n_3}\mu_1 \\ + a_{1,0} + a_{1,1}\xi + \cdots + a_{1,n_2-1}\xi^{n_2-1} + \xi^{n_2} = 0. \end{aligned}$$

При $j_1 \geq 1$ получим

$$\xi^{j_2}\mu_1^{j_1} = a_{2,1}\xi^{j_2+1}\mu_1^{j_1} + \dots + a_{2,n_3-1}\xi^{j_2+n_3-1}\mu_1^{j_1} +$$
$$+\xi^{j_2+n_3}\mu_1^{j_1} + a_{1,0}\xi^{j_2}\mu_1^{j_1-1} + a_{1,1}\xi^{j_2+1}\mu_1^{j_1-1} + \dots +$$
$$+a_{1,n_2-1}\xi^{j_2+n_2-1}\mu_1^{j_1-1} + \xi^{j_2+n_2}\mu_1^{j_1-1}, \tag{3.28}$$

При $j_2 \geq n_3$ и $j_1 \geq 1$ получим

$$\xi^{j_2}\mu_1^{j_1} = \xi^{j_2-n_3}\mu_1^{j_1} + a_{2,1}\xi^{j_2-n_3+1}\mu_1^{j_1} + \dots +$$
$$+a_{2,n_3-1}\xi^{j_2-1}\mu_1^{j_1} + a_{10}\xi^{j_2-n_3}\mu_1^{j_1-1} + \dots +$$
$$+a_{1,n_2-1}\xi^{j_2-n_3+n_2-1}\mu_1^{j_1-1} + \xi^{j_2-n_3+n_2}\mu_1^{j_1-1}. \tag{3.29}$$

Используя свойства (3.26), (3.27) множеств A'_r, A''_r и тождества (3.28), (3.29), получим (3.25) при $(j_1, j_2) \in A_r$.

Таким образом, (3.25) доказано для любой (j_1, j_2) из A.

Нетрудно видеть, что

$$\{\ (j_1, j_2)\ \mid\ (n_3-1)n_1 \leq j_2 \leq (n_3-n_2)j_1 +$$
$$+(n_3-1)(n_2+n_1+1-n_3),$$
$$j_1 \in \mathbb{N}\setminus\{0\}, j_2 \in \mathbb{N}\setminus\{0\}\ \} \subseteq A \tag{3.30}$$

Отсюда следует (3.24) для λ_1,

$$2^{\lambda_1} \geq \max\left((n_3-1)n_1, (n_3-1)(n_3-n_2-n_1-1)\right).$$

Лемма 3.2.2 доказана.

С использованием известных рассуждений (см. обоснование леммы 9 в [68]) доказывается

Лемма 3.2.3. *Если имеют место (3.6) и, кроме того,*

$$M \not\subseteq M_j^{(1)}, j = j_1, j_2, \dots, j_{n'}, 1 < j_1 < j_2 < \dots < j_{n'},$$

то найдется μ',

$$\mu' \in K^{(1)}(M), \quad \mu' = \frac{u'}{v'}, \quad (u', v') = 1, \tag{3.31}$$

$$v' \in p_{j_1} p_{j_2} \dots p_{j_{n'}} E_2[\xi]. \tag{3.32}$$

Продолжая доказательство теоремы 1, положим

$$I_0 = \left\{ \ i \ \mid \ i \in \mathbb{N} \setminus \{0, 1\}, M \subseteq M_i^{(1)} \ \right\}$$

$$I_2 = \left\{ \ j \ \mid \ j \in \mathbb{N} \setminus (\{0, 1\} \cup I_0), \mu_1 \in R_j^{(1)} \ \right\},$$

где μ_1 - дробь из $L_0^{(1)}$, $\mu_1 = \frac{u_1}{v_1}$, удовлетворяющая в случае (3.21) соотношению (3.22) или в случае (3.23) соотношению (3.24).

Найдутся многочлены u_M, u_2 из $E_2[\xi]$ такие, что

$$u_1 = u_M u_2$$

и для любых i, j, $i \in I_0$, $j \in I_2$,

$$(u_M, p_j) = 1, \qquad (u_2, p_i) = 1.$$

Пусть имеет место (3.21). Из леммы 3.2.2 для некоторого $T_0, T_0 \in N$, вытекает

$$\Omega\left(T_0, (u_M u_2)^{T_0}\right) \subseteq M \tag{3.33}$$

По лемме 3.2.2 в M найдется дробь $\frac{u_3}{v_3 u_2}$, $(u_3, u_2) = 1$. Отсюда и из (3.33)

$$\Omega\left(T_0, (u_M u_3)^{T_0}\right) \subseteq M. \tag{3.34}$$

Используя (3.33) и (3.34) и равенство

$$u_4 u_2^{T_0} + u_5 u_3^{T_0} = 1,$$

справедливое для некоторых многочленов u_4, u_5 из $E_2[\xi]$, получим

$$\Omega\left(T_0, u_M^{T_0}\right) \subseteq M.$$

В дальнейшем используется следующая лемма.

Лемма 3.2.4. *Для взаимно простых многочленов* u' *и* $\xi u_M(\xi)$, $u'(\xi) \in E_2[\xi]$, $u_M(\xi) \in E_2[\xi]$ *найдется* u'', $u'' \in E_2[\xi]$,

$$(u''(\xi), \xi u_M(\xi)) = 1, \tag{3.35}$$

такой, что

$$u'u'' \in E_2[\xi u_M(\xi)] \tag{3.36}$$

Доказательство. Для любого i, $i \in \mathbb{N}$, в $E_2[\xi]$ найдутся $u_i^{(1)}(\xi)$, $u_i^{(2)}(\xi)$, удовлетворяющие соотношениям

$$(\xi u_M(\xi))^i = u'(\xi)u_i^{(1)}(\xi) + u_i^{(2)}(\xi), \quad \deg u_i^{(2)} < \deg u'(\xi).$$

Ввиду конечности множества многочленов со степенями меньше $\deg u'(\xi)$, в $\mathbb{N}$ найдутся i_0, i_1 такие, что $i_0 < i_1$ и $u_{i_0}^{(2)} = u_{i_1}^{(2)}$. При этом

$$(\xi u_M(\xi))^{i_0} \left(1 + (\xi u_M(\xi))^{i_1 - i_0}\right) = u'(\xi) \left(u_{i_0}^{(1)} + u_{i_1}^{(1)}\right) \tag{3.37}$$

Обозначим $\frac{u_{i_0}^{(1)}(\xi)+u_{i_1}^{(1)}(\xi)}{(\xi u_M(\xi))^{i_0}}$ через u''. Из условий леммы и равенства (3.37) вытекает $u''(\xi) \in E_2[\xi]$, а также соотношения (3.35) и (3.36).

Лемма 3.2.4 доказана.

Пусть $\mu' = \frac{u'}{v'}$, $(v', u_M) = 1$. Тогда из доказательства леммы 3.2.4 найдутся T' и u'', $T' \in \mathbb{N}$, $T' \geq T_0$, $u'' \in E_2[\xi]$, что выполнено равенство:

$$\mu' = \frac{u''}{1 + (\xi u_M)^{T'}}.$$

Отсюда следует

$$(\xi u_M)^{T_0} \mu' \in M,$$

так как

$$\left\{(\xi u_M)^{T_0} u'', \quad (\xi u_M)^{T'}\right\} \subset S^{(1)}\left(\Omega\left(T_0, u_M^{T_0}\right)\right).$$

Положим

$$u_0 \;=\; \begin{cases} \Pi_{(i \in I_0)} p_i, & \text{если} \quad I_0 \neq \emptyset \\ \quad 1 & \text{если} \quad I_0 = \emptyset. \end{cases}$$

Для некоторого T, $T \in \mathbb{N} \setminus \{0\}$

$$(\xi u_0)^T \in (\xi u_M)^{T_0} E_2[\xi].$$

Поэтому

$$(\xi u_0)^T \mu' \in M,$$

если $\mu' = \frac{u'}{v'}$, $(v', u_0) = 1$.

Найдется μ_e, $\mu_e \in M \cap \left(1 + \xi \mathfrak{L}_0^{(1)}\right)$.

Заметим, что

$$\mu_e^{2^T} = 1 + (\xi u_0)^T \mu^*$$

для некоторого μ^*, $\mu^* = \frac{u^*}{v^*}$, $(v^*, u_0) = 1$. Отсюда

$$1 \in M.$$

Таким образом,

$$M^{(1)}\left((\xi u_0)^T\right) \subseteq M.$$

Очевидно

$$M \subseteq M^{(1)}(u_0).$$

Поэтому имеет место (3.19).

Утверждение 1 теоремы 3.2.1 в случае (3.21) доказано. Докажем утверждение 1 теоремы в случае (3.23).

Имеют место следующие свойства M.

Свойство 1. Если

$$\Omega_1(\lambda', \mu') \subseteq M,$$

то для любого λ'', $\lambda'' \in \mathbb{N}$, $\lambda'' \geq \lambda'$,

$$\Omega_1(\lambda'', \mu') \subseteq M.$$

Свойство 2. Если

$$\Omega_1\left(\lambda', \frac{u'}{v'}\right) \subseteq M, \tag{3.38}$$

$$\Omega_1\left(\lambda', \frac{u''}{v'}\right) \subseteq M, \tag{3.39}$$

$$\deg u' = n', \quad \deg u'' = n'', \quad n' \geq n'', \tag{3.40}$$

$$u' + \xi^{n'-n''}u'' = \xi^{n'_1}u'_1, \quad u'_1 \in 1 + \xi E_2[\xi], \tag{3.41}$$

то для некоторого λ'', $\lambda'' \in \mathbb{N}$,

$$\Omega_1\left(\lambda'', \frac{u'_1}{v'}\right) \subseteq M \tag{3.42}$$

Свойство 3. Если

$$\Omega_1\left(\lambda', \frac{u'}{v'}\right) \subseteq M,$$

$$\Omega_1\left(\lambda'', \frac{u''}{v'}\right) \subseteq M,$$

то для некоторого λ'_1 из N

$$\Omega_1\left(\lambda'_1, \frac{(u', u'')}{v'}\right) \subseteq M.$$

Свойство 1 следует из (3.30). Докажем свойство 2. Пусть имеют место (3.38)–(3.41). Тогда

$$\frac{\xi^{2^{\lambda'}(n'_1+1)}u'_1\left(\xi^{2^{\lambda'}}\right)}{v'\left(\xi^{2^{\lambda'}}\right)} \in M$$

и

$$\frac{\xi^{2^{\lambda'}(n'_1+1)+1}u'_1\left(\xi^{2^{\lambda'}}\right)}{v'\left(\xi^{2^{\lambda'}}\right)} \in M.$$

Используя последние два соотношения и лемму 3.2.2, получим (3.42). Свойство 2 доказано.

Свойство 3 доказывается с использованием свойств 1, 2 и алгоритма Эвклида.

Докажем, что найдутся $d_0(\xi)$, λ_2, $d_0(\xi) \in E_2[\xi]$, $\deg d_0(\xi) \geq u$, $\lambda_2 \in \mathbb{N}$,

$$\Omega_1\left(\lambda_2, \frac{u_M(\xi)}{d_0(\xi u_M(\xi))}\right) \subseteq M. \tag{3.43}$$

Используя леммы 3.2.2 и 3.2.4, для некоторых $d_0(\xi)$, $u_6(\xi)$, λ_3, $d_0(\xi) \in 1 + E_2[\xi]$, $\deg d_0(\xi) \geq 4$, $u_6(\xi) \in 1 + \xi E_2[\xi]$, $\lambda_3 \in \mathbb{N}$, получаем

$$\Omega_1\left(\lambda_3, \frac{u_M(\xi)u_6(\xi)}{d_0(\xi u_M(\xi))}\right) \subseteq M, \tag{3.44}$$

где $(u_6(\xi), \xi u_M(\xi)) = 1$.

По лемме 3.2.3 в M содержится некоторая дробь $\frac{\xi^s u_7(\xi)}{u_6(\xi)v_0(\xi)}$, $u_7(\xi) \in 1 + \xi E_2[\xi]$, $v_0(\xi) \in 1 + \xi E_2[\xi]$, $(u_7(\xi), u_6(\xi)) = 1$.

Тогда из (3.43) и доказательства леммы 3.2.2

$$\Omega_1\left(\lambda_4, \frac{u_M(\xi)u_7(\xi)}{d_0(\xi u_M(\xi))v_0(\xi)}\right) \subseteq M. \tag{3.45}$$

Используя свойство 3 множества M, равенство $(u_6(\xi)v_0(\xi), u_7(\xi)) = 1$ и соотношения (3.44), (3.45), получим

$$\Omega_1\left(\lambda_2, \frac{u_M}{d_0(\xi u_M(\xi))v_0(\xi)}\right) \subseteq M. \tag{3.46}$$

Из (3.46) следует (3.43).

Обозначим $\deg d_0(\xi)$ через n, $\deg u_M(\xi)$ через m, $\xi^{2^{\lambda_2}}$ через η.

Покажем, что для любых r, i, j,

$$r \in \mathbb{N} \setminus \{0\}, \quad 0 \leq i \leq 2^{\lambda_2}(m+1), \quad 1 \leq j \leq nr - 2, \tag{3.47}$$

имеет место

$$\frac{(\eta u_M(\eta))^j \xi^i}{d_0^r(\eta u_M(\eta))} \in M \tag{3.48}$$

Доказательство проведем индукцией по r. При $r = 1$ справедливость (3.48) для любых i, j, удовлетворяющих (3.47), вытекает из (3.43).

Пусть (3.48) выполнено при $r = r'$, $r' \geq 1$, для всех указанных в (3.47) i, j.

Нетрудно видеть, что (3.48) выполнено при

$$r = r' + 1, \quad 0 \leq i \leq 2^{\lambda_2}(m+1), \quad 2 \leq j \leq (r'+1)n - 3.$$

Имеет место

$$d_0 = 1 + a_1\xi + a_2\xi^2 + \cdots + a_{n-1}\xi^{n-1} + \xi^n,$$

$a_i \in E_2$, $i = 1, 2, \ldots, n-1$.

Обозначим $\eta u_M(\eta)$ через Υ. Тогда

$$\frac{\Upsilon\xi^i}{d_0^{r'+1}(\Upsilon)} = \frac{\Upsilon d_0(\Upsilon)\xi^i}{d_0^{r'+1}(\Upsilon)} + a_1\frac{\Upsilon^2\xi^i}{d_0^{r'+1}(\Upsilon)} + \\ a_2\frac{\Upsilon^3\xi^i}{d_0^{r'+1}(\Upsilon)} + \cdots + a_{n-1}\frac{\Upsilon^n\xi^i}{d_0^{r'+1}(\Upsilon)} + \frac{\Upsilon^{n+1}\xi^i}{d_0^{r'+1}(\Upsilon)}, \tag{3.49}$$

$$\frac{\Upsilon^{(r'+1)n-2}\xi^i}{d_0^{r'+1}(\Upsilon)} = \frac{\Upsilon^{r'n-2}d_0(\Upsilon)\xi^i}{d_0^{r'+1}(\Upsilon)} + \frac{\Upsilon^{r'n-2}\xi^i}{d_0^{r'+1}(\Upsilon)} + \\ a_1\frac{\Upsilon^{r'n-1}\xi^i}{d_0^{r'+1}(\Upsilon)} + a_2\frac{\Upsilon^{r'n}\xi^i}{d_0^{r'+1}(\Upsilon)} + \cdots + a_{n-2}\frac{\Upsilon^{(r'+1)n-3}\xi^i}{d_0^{r'+1}(\Upsilon)}. \tag{3.50}$$

Так как $\deg d_0(\xi) \geq 4$, то каждое слагаемое в правых частях равенств (3.49), (3.50) содержится в M. Поэтому (3.48) выполнено для всех i, j, удовлетворяющих (3.47) при $r = r' + 1$.

Таким образом, (3.48) при ограничениях (3.47) доказано.

Из (3.48) для любых r, $u'(\xi)$, $r \in \mathbb{N} \setminus \{0\}$, $u'(\xi) \in E_2[\xi]$, $\deg u' \leq nr2^{\lambda_2}(m+1) - 2^{\lambda_2+1}(m+1)$, вытекает

$$\frac{\Upsilon u'(\xi)}{d_0^r(\Upsilon)} \in M \tag{3.51}$$

Пусть $u'(\xi) \in E_2[\xi]$, $v'(\xi) \in E_2[\xi]$, $(v'(\xi), \xi u_M(\xi)) = 1$, $\deg u'(\xi) \leq \deg v' - 2^{\lambda_2+1}(m+1)$,

$$\mu' = \frac{\Upsilon u'(\xi)}{v'(\xi)}.$$

Докажем, что

$$\mu' \in M \tag{3.52}$$

Предположим

$$v'(\xi) \in 1 + \Upsilon E_2[\Upsilon],$$

$$\deg v'(\xi) = nr_0(m+1)2^{\lambda_2}.$$

Ввиду леммы 3.2.3 эти предположения не ограничивают общности рассуждений.

Из (3.51) для μ_1', μ_2',

$$\mu_1' = \frac{v'(\xi) + d_0^{r_0}(\Upsilon)}{d_0^{r_0}(\Upsilon)},$$

$$\mu_2' = \frac{\Upsilon u'(\xi)}{d_0^{r_0}(\Upsilon)},$$

получим

$$\mu_1' \in M, \qquad \mu_2' \in M.$$

Отсюда и из равенства

$$\mu' = \frac{\mu_2'}{1 + \mu_1'}$$

следует (4.19).

Через T обозначим натуральное число, $T \geq 1$, удовлетворяющее соотношению

$$(\xi u_0(\xi))^T \subseteq \Upsilon E_2[\xi].$$

Для любого μ', $\mu' \in \mathfrak{L}_0^{(1)}$, $\mu' = \frac{u'}{v'}$, такого, что $(v', u_0) = 1$ и $\deg u'(\xi) \leq \deg v' - 2T\,(\deg u_0(\xi) + 1)$, выполнено:

$$(\xi u_0(\xi))^T \mu' \in M.$$

Найдется μ_e, $\mu_e \in M \cap \left(1 + \xi \mathfrak{L}_0^{(1)}\right)$. Тогда

$$\mu_e^{2^{T(\deg u_0 + 1)}} = 1 + \frac{(\xi u_0)^T u^*(\xi)}{v^*(\xi)},$$

где $(v^*(\xi), u_0(\xi)) = 1$, $\deg u^*(\xi) \leq \deg v^*(\xi) - 2T(\deg u_0(\xi) + 1)$, то есть $1 \in M$.

Таким образом,

$$P^{(1)}\left((\xi u_0)^T\right) \subseteq M.$$

Очевидно,

$$M \subseteq M_0^{(1)} \cap M^{(1)}(u_0).$$

Поэтому имеет место (3.20).

Утверждение 1 теоремы 3.2.1 доказано. Докажем утверждение 2.

Пусть $u_0 \in 1 + \xi E_2[\xi]$, положим

$$M_*^{(1)}(u_0^T) = \{ \ \xi u \ | \ u \in E_2[\xi], \deg \xi u < T(\deg u_0 + 1) \ \} ,$$

$$P_*^{(1)}\left(u_0^T\right) = \left\{ \ \frac{\xi u_1 + (\xi u_0)^T \xi u_2}{1 + (\xi u_0)^{2T}} \ | \ u_i \in E_2[\xi], \right. \\ \left. \deg \xi u_i < T(\deg u_0 + 1), i = 1, 2 \ \right\} .$$

Для доказательства второй части теоремы 3.2.1 используется

Лемма 3.2.5. *1. В случае $\mu' \in M^{(1)}(u_0)$ для любого T, $T \in \mathbb{N} \setminus \{0\}$, найдутся и притом единственным образом μ'_1, μ'_2, $\mu'_1 \in M_*^{(1)}(u_0^T)$, $\mu'_2 \in M^{(1)}((\xi u_0)^T)$, что*

$$\mu' = \mu'_1 + \mu'_2. \tag{3.53}$$

2. В случае $\mu' \in M_0^{(1)} \cap M^{(1)}(u_0)$ для любого T, $T \in \mathbb{N} \setminus \{0\}$, найдутся и притом единственным образом μ'_1, μ'_2, $\mu'_1 \in P_*^{(1)}(u_0^T)$, $\mu'_2 \in P^{(1)}((\xi u_0)^T)$, что выполнено (3.53).

Доказательство леммы.

Пусть $\mu' = \frac{u'}{v'}$,

$$\mu' \in M^{(1)}(u_0). \tag{3.54}$$

Не ограничивая общности, предположим, что

$$v' \in 1 + (\xi u_0)^T E_2[\xi u_0].$$

Найдутся u'_1, u'_2, $\deg u'_1 < T(\deg u_0 + 1)$, удовлетворяющие равенству

$$u' = u'_1 v'(\xi) + (\xi u_0)^T u'_2.$$

Отсюда

$$\mu' = u'_1 + \frac{(\xi u_0)^T u'_2}{v'},$$

то есть имеет место разложение (3.53).

Если помимо (3.54) выполнено еще

$$\mu' \in M_0^{(1)}, \tag{3.55}$$

то для некоторых $a, \quad u_1', \quad u_2', \quad u_3', \quad a \in E_2, \quad u_i' \in E_2[\xi], \quad i = 1, 2, 3, \quad \deg \xi u_j' < T(\deg u_0 + 1), \quad j = 1, 2, \quad \deg u_3' \le \deg v' - 2T(\deg u_0 + 1)$,

$$\frac{u'}{v'} = a + \frac{\xi u_1' + (\xi u_0)^T u_3' + (\xi u_0)^{\deg v' - T} \xi u_2'}{v'}.$$

Тогда

$$\mu' + \frac{\xi u_1' + (\xi u_0)^T \xi u_2'}{1 + (\xi u_0)^{2T}} \in P^{(1)}((\xi u_0)^T) \tag{3.56}$$

и разложение (3.53) имеет место при

$$\mu_1' = \frac{\xi u_1' + (\xi u_0)^T \xi u_2'}{1 + (\xi u_0)^{2T}}$$

и

$$\mu_2' = \mu' + \mu_1'.$$

Докажем единственность разложения (3.53).

Пусть в случае (3.54) наряду с (3.53) имеет место

$$\mu' = \mu_1'' + \mu_2'', \tag{3.57}$$

где $\mu_1'' \in M_*^{(1)}(u_0^T), \quad \mu_2'' \in M^{(1)}((\xi u_0)^T)$. Тогда

$$\mu_1' + \mu_1'' = \mu_2' + \mu_2''. \tag{3.58}$$

Ввиду

$$M_*^{(1)}(u_0^T) \cap M^{(1)}((\xi u_0)^T) = \{0\}, \tag{3.59}$$

из (3.58) получим $\mu_1' = \mu_1'', \quad \mu_2' = \mu_2''$. Единственность разложения (3.53) в случае (3.54) доказана.

Пусть имеют место (3.54) и (3.55) и наряду с (3.56) выполнено

$$\mu' + \frac{\xi u_1'' + (\xi u_0)^T \xi u_2''}{1 + (\xi u_0)^{2T}} \in P^{(1)}((\xi u_0)^T), \tag{3.60}$$

$$\deg \xi u_i'' < T(\deg u_0 + 1), \quad i = 1, 2.$$

Из (3.56) и (3.60) получим

$$\frac{\xi(u_1' + u_1'') + (\xi u_0)^T \xi(u_2' + u_2'')}{1 + (\xi u_0)^{2T}} \in P^{(1)}((\xi u_0)^T),$$

откуда $u_1' = u_1''$ и $u_2' = u_2''$.

Из приведенных рассуждений следует единственность разложения (3.53), когда выполнены (3.54) и (3.55).

Лемма 3.2.5 доказана.

Из леммы 3.2.5, первой части теоремы 3.2.1, конечности множеств $M_*^{(1)}(u_0^T)$ и $P_*^{(1)}(u_0^T)$ и изоморфизма множеств $\mathfrak{L}_0^{(1)}$ и $\mathfrak{L}_0^{(1)}(\mu)$ вытекает второе утверждение.

Теорема 3.2.1 доказана.

Теорема 3.2.2. *Соотношение*

$$1 \in K^{(1)}(M) \tag{3.61}$$

выполнено тогда и только тогда, когда для каждого i, $\quad i = 0, 1, 2, \ldots,$

$$M \not\subseteq R_i^{(1)}. \tag{3.62}$$

Доказательство. Если (3.61) имеет место, то (3.62) выполнено ввиду $1 \notin R_i^{(1)}, \quad i = 0, 1, 2, \ldots$. Необходимость утверждения теоремы доказана.

Его достаточность установлена при доказательстве теоремы 3.2.1.

Теорема 3.2.2 доказана.

3.3. Об алгоритме проверки выразимости через конечные множества с сумматором

Теорема 3.3.1. *Существует алгоритм, который для любых μ', γ', M, C,*

$$\mu' \in \mathfrak{L}_0^{(1)}, \quad \gamma' \in \mathfrak{L}_c, \quad M \subset \mathfrak{L}_0^{(1)}, \quad C \subset \mathfrak{L}_c, \tag{3.63}$$

$$|M| < \infty, \quad |C| < \infty, \quad 1 \in K^{(1)}(M), \tag{3.64}$$

определяет справедливость соотношений

$$\mu' \in K^{(1)}(M), \tag{3.65}$$

$$\gamma' \in S(M, C). \tag{3.66}$$

Доказательство. Пусть имеют место (3.63), (3.64). Положим

$$M^* = \left\{ \ \mu' \ \mid \ \mu' \in M \cap \xi \mathfrak{L}_0^{(1)} \ \right\} \cup \\ \cup \left\{ \ \mu' + 1 \ \mid \ \mu' \in M \setminus \xi \mathfrak{L}_0^{(1)} \ \right\} \cup \{1\}.$$

Выполнено

$$K^{(1)}(M) = K^{(1)}(M^*).$$

Поэтому в дальнейшем, не ограничивая общности, рассмотрим случай

$$M = \{1\} \cup M', \quad M' \subseteq \xi \mathfrak{L}_0^{(1)} \setminus \{0\}.$$

Доказательство теоремы 3.3.1 нетривиально при условии $M' \neq \emptyset$, что равносильно соотношению

$$K^{(1)}(M) \setminus E_2 \neq \emptyset. \tag{3.67}$$

Пусть (3.67) имеет место. Как уже отмечалось при доказательстве леммы 3.2.1, для некоторой дроби μ, $\mu \in \xi \mathfrak{L}_0^{(1)}$, выполнено:

$$E_2(M) = E_2(\mu), \tag{3.68}$$

где через $E_2(M)$ и $E_2(\mu)$ обозначены замыкания по операциям сложения, умножения и деления множеств $E_2 \cup M$ и $E_2 \cup \{\mu\}$ соответственно.

Из [20] вытекает

Лемма 3.3.1. *Пусть* $\{\mu'', \mu_1''\} \subset \xi\mathfrak{L}_0^{(1)}$ *и*

$$E_2(\mu'') \subseteq E_2(\mu_1'').$$

Тогда $\mu'' = \mu_a(\mu_1'')$ *для некоторого* $\mu_a(\xi)$ *из* $\mathfrak{L}_0^{(1)}$ *и* $\deg \mu_a(\xi) \cdot \deg \mu_1'' = \deg \mu''(\xi)$.

Имеет место также

Лемма 3.3.2. *Дробь* μ*, удовлетворяющая равенству (3.68), содержится в множестве*

$$M_a = \Big\{ \ \mu^* \ \mid \ \mu^* \in \mathfrak{L}_0^{(1)}, \quad E_2(\mu'') \subseteq E_2(\mu^*) \\ \text{для любого } \mu'' \text{ из } M \ \Big\}.$$

и имеет максимальную возможную степень.

Докажем лемму 3.3.2. Из (3.68) следует $\mu \in M_a$. Если бы в M_a нашлась дробь μ^*, $\deg \mu^* > \deg \mu$, то

$$E_2(\mu) \subseteq E_2(\mu^*) \subseteq E_2(\xi),$$

что противоречит лемме 3.3.1.

Таким образом, лемма 3.3.2 доказана.

Заметим, что для любого M, $|M| < \infty$, множество M_a конечно и может быть найдено ввиду леммы 3.3.1.

Далее, найдется μ_0, $\mu_0 \in S^{(1)}(M)$, что $\mu\mu_0 \in S^{(1)}(M)$ и $M \subseteq \mathfrak{L}_0^{(1)}(\mu)$.

Для каждого μ', $\mu' \in M$, строится $\mu''(\xi)$, $\mu''(\xi) \in \mathfrak{L}_0^{(1)}$, удовлетворяющая соотношению

$$\mu''(\mu) = \mu'.$$

Конечность этой процедуры следует из леммы 3.3.1.

Далее доказательство ведется параллельно для двух случаев.

Случай 1. $M \not\subseteq M_0^{(1)}(\mu)$.

Случай 2. $M \subseteq M_0^{(1)}(\mu)$.

Используя доказательство теоремы 3.2.1, для M можно найти $u_0(\xi)$ и T такие, что в случае 1 имеет место (3.7), а в случае 2 выполнено (3.8)

Положим в случае 1

$$M^* = \{\ u'(\mu)\ \mid\ \deg u'(\xi) < T(1+\deg u_0(\xi))\ \},$$

$$M'' = \Big\{(\ \mu u_0(\mu))^T \frac{u'(\mu)}{v'(\mu)}\ \mid \\ \frac{u'(\xi)}{v'(\xi)} \in \mathfrak{L}_0^{(1)},\ \ (v'(\xi), \xi u_0(\xi)) = 1\ \Big\},$$

а в случае 2

$$M^* = \Big\{\ \frac{u^{(1)}(\mu) + (\mu u_0(\mu))^T \mu u^{(2)}(\mu)}{1+(\mu u_0(\mu))^{2T}}\ \mid \\ u^{(i)}(\xi) \in E_2[\xi],\ \ \deg u^{(i)}(\xi) < T(\deg u_0(\xi)+1),\ \ i=1,2\ \Big\},$$

$$M'' = \Big\{\ \frac{(\mu u_0(\mu))^T\, u'(\mu)}{v'(\mu)}\ \mid\ \frac{u'(\xi)}{v'(\xi)} \in \mathfrak{L}_0^{(1)}, \\ (v'(\xi), \xi u_0(\xi)) = 1,\quad \deg u'(\xi) \le \deg v'(\xi) - 2T\,(1+\deg u_0(\xi))\ \Big\}.$$

Имеет место

$$K^{(1)}(M) = M' + M'',$$

где

$$M' \subseteq M^*.$$

Множество M' находится следующим образом. Пусть

$$M'_n = \{\ u'\ \mid\ \mu' = u' + \mu'',\ \ u' \in M^*,\ \ \mu'' \in M'',$$

μ' может быть получен из элементов множества M.

с использованиемне более чем n операций ‘ + ‘, ‘ $\cdot$ ‘, ‘ fb ‘} ,

$n = 1, 2, \ldots$.

Тогда для некоторого n_0, $n_0 \in N$, выполнено

$$M'_{n_0} = M'_{n_0+1}.$$

Нетрудно видеть, что

$$M' = M'_{n_0}.$$

Таким образом, указан алгоритм, определяющий справедливость соотношения (3.65).

Множество $S(M, C)$ - линейное пространство над кольцом $K^{(1)}(M)$ с порождающим множеством C, $C = \{\gamma_1, \gamma_2, \dots \gamma_m\}$.

Рассмотрим линейное пространство $S'(\mu, C)$ над полем $E_2(\mu)$ с порождающим множеством C. Пусть γ_1, γ_2,$\dots \gamma_r$, $r \leq m$, базис этого пространства. Согласно [20], конечный базис в $S'(\mu, C)$ существует и может быть выделен из C известными методами.

Для любого i, $r < i \leq m$, определяются $\eta_i(\mu)$, $\eta_{1,i}(\mu)$, $\eta_{2,i}(\mu)$,$\dots \eta_{r,i}(\mu)$, удовлетворяющие равенству

$$\eta_i(\mu)\gamma_i = \eta_{1,i}(\mu)\gamma_1 + \dots + \eta_{r,i}(\mu)\gamma_r$$

и такие, что

$$\eta_i(\mu) = \xi u_0(\xi)\frac{\tilde{u}_i}{\tilde{v}_i},$$

$$\eta_{j,i}(\mu) = \xi u_0(\xi)\frac{\tilde{u}_{j,i}}{\tilde{v}_{j,i}},$$

$$(\tilde{v}_i, \xi u_0(\xi)) = 1, \ \ (\tilde{v}_{j,i}, \xi u_0(\xi)) = 1,$$

$j = 1, 2, \dots, r, \ \ i = r + 1, r + 2, \dots, m.$

Положим

$$\chi(\xi) = \begin{cases} (\xi u_0(\xi))^T, & r = m, \\ \eta_{r+1}(\xi) \cdot \eta_{r+2}(\xi) \cdot \dots \cdot \eta_m(\xi), & \text{если} \quad r \neq m. \end{cases}$$

Тогда для некоторых $u_1(\xi)$, $u_2(\xi)$, $v_1(\xi)$,

$$\chi(\xi) = \frac{u_1(\xi)u_2(\xi)}{v_1(\xi)},$$

$$\left(u_1(\xi), (\xi u_0(\xi))^T\right) = (\xi u_0(\xi))^T,$$

$$(u_2(\xi)v_1(\xi), \xi u_0(\xi)) = 1.$$

Пусть $s = \deg u_1(\xi)$. Положим в случае 1

$$N = \{u'(\mu) \quad | \quad \deg u' < s\},$$

$$N'' = \left\{u_1(\mu)\frac{u'(\mu)}{v'(\mu)} \quad | \quad \frac{u'(\xi)}{v'(\xi)} \in \mathfrak{L}_0^{(1)}, \quad (v'(\xi), \xi u_0(\xi)) = 1\right\},$$

а в случае 2:

$$N = \left\{\frac{u^{(1)}(\mu) + u_1(\mu)u^{(2)}(\mu)}{1 + u_1^2(\mu)} \quad | \right.$$
$$\left. u^{(i)}(\xi) \in E_2[\xi], \quad \deg u^{(i)}(\xi) < s, \quad i = 1, 2\right\},$$

$$N'' = \left\{u_1(\mu)\frac{u'(\mu)}{v'(\mu)} \quad | \right.$$
$$\left. \frac{u'(\xi)}{v'(\xi)} \in \mathfrak{L}_0^{(1)}, \quad (v'(\xi), \xi u_0(\xi)) = 1, \deg u'(\xi) \leq \deg v'(\xi) - 2s\right\}$$

Для некоторого N', $N' \in N$,

$$K^{(1)}(M) = N' + N''.$$

Множество N' определяется методом, использованным для получения M'.

Включение (3.66) имеет место в точности тогда, когда

$$\{\zeta_1\gamma_1 + \cdots + \zeta_m\gamma_m + \gamma \quad | \quad \zeta_i \in N', \quad i = 1, 2, \ldots, m\} \bigcap$$
$$\{\zeta_1\gamma_1 + \cdots + \zeta_m\gamma_m \quad | \quad \zeta_i \in N'', \quad i = 1, 2, \ldots, m\} \neq \emptyset,$$

что, в свою очередь, равносильно соотношению

$$\{\zeta_1\gamma_1 + \cdots + \zeta_m\gamma_m + \gamma \quad | \quad \zeta_i \in N', \quad i = 1, 2, \ldots, m\} \bigcap$$
$$\{\zeta_1\gamma_1 + \cdots + \zeta_r\gamma_r \quad | \quad \zeta_i \in N'', \quad i = 1, 2, \ldots, r\} \neq \emptyset. \tag{3.69}$$

Соотношение (3.69) может быть установлено с использованием известных алгоритмов.

Таким образом, теорема 3.3.1 доказана.

Теорема 3.3.2. *Проблема выразимости в $\mathfrak{L}$ через конечные системы, содержащие сумматор в замыкании, алгоритмически разрешима.*

Эта теорема вытекает из леммы 3.1.1 и теоремы 3.3.1.

3.4. Выразимость сумматора через конечные множества

Далее будет получен алгоритм для проверки свойства

$$x_1 + x_2 \in K(M) \tag{3.70}$$

любой конечной системы ЛА M.

В главе 2 для $\mathfrak{L}$ построена приведенная критериальная система J_2,

$$\begin{gathered} J_2 = \{\ T_0,\ \ T_1,\ \ V_1,\ \ V_2,\ \ M_i,\ \ R_j^e,\ \ R_j^d\ \mid \\ i = 0, 1, \ldots,\ \ j = 0, 2, 3, \ldots\ \}. \end{gathered} \tag{3.71}$$

Положим

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

Из (3.70) для любого Θ,

$$\Theta \in J',$$

следует

$$M \not\subseteq \Theta.$$

Обратное, вообще говоря, неверно. Приведем соответствующий пример. Пусть

$$M_0 = \{\ x_1 + x_2 + x_3,\ \ \xi x_1 + \xi x_2 + \xi\ \ \}.$$

Тогда $M \not\subseteq \Theta$ для любого Θ, $\Theta \in J'$, но любой f, $f \in K(M_0)$, либо имеет нечетное число непосредственных переменных и коэффициент при ξ ряда $f(0,0,\ldots,0)$ равен 0, либо имеет четное число непосредственных переменных и этот коэффициент равен 1. Доказательство последнего утверждения нетрудно провести индукцией по построению ЛА из $K(M_0)$.

Положим

$$J^* = J' \setminus \{T_1\}.$$

Справедлива следующая

Лемма 3.4.1. *Если* $M \not\subseteq \Theta$ *для любого* Θ, $\Theta \in J^*$, *то*

$$x_1 + x_2 + x_3 \in K(M). \tag{3.72}$$

Доказательство. Пусть $M \not\subseteq \Theta$ для любого Θ, $\Theta \in J^*$. Тогда, как нетрудно видеть, для некоторых μ_i', $\mu_i' \in \mathfrak{L}_0^{(1)}$, $i = 1, 2$, $\mu_0' \in \mathfrak{L}_c$, и некоторого ЛА $f\left(x_1, x_2, x\right)$ имеем:

$$f\left(x_1, x_2, x\right) = \mu_1' x_1 + \mu_1' x_2 + \mu_2' x + \mu_0' \in K(M),$$

$$\mu_1' \in 1 + \xi \mathfrak{L}_0^{(1)}. \tag{3.73}$$

Если $\mu_1' = 1$, то из ЛА $f\left(x_1, x_2, x\right)$, то получаем

$$x_1 + x_2 + x_3 = f\left(x_1, f\left(x_2, x_3, x\right), x\right),$$

и (3.72) имеет место.

В противном случае, из включения (3.73) следует $\mu_1' \notin R_1^{(1)}$. Если для некоторого i, $i \in \{0, 2, 3, \ldots\}$, выполнено $M \subset M_i$, то $\mu_1' + 1 \in R_i^{(1)}$, а, следовательно, $\mu_1' \notin R_i^{(1)}$.

Отсюда получаем, что для любого i, $i \in \{0, 2, 3, \ldots\}$, из $\mu_1 \in R_i^{(1)}$ следует

$$M \not\subseteq M_i.$$

При этом из условия леммы имеем:

$$M \not\subseteq R_i^e, \;\; M \not\subseteq R_i^d.$$

Поэтому и по лемме 10 из [?] в $\mathfrak{L}_0^{(1)} \setminus \{0\}$ найдется μ_i'' такое, что

$$\mu_i'' \notin \tilde{M}_i^{(1)}$$

и

$$\mu_i'' \in U(K(M)).$$

Используя ЛА из множества

$$\left\{\; f\left(x_1, x_2, x\right), \;\; f_i \;\mid\; M \subseteq M_i, f_i \in K(M), U\left(f_i\right) \not\subset \tilde{M}_i^{(1)} \;\right\}$$

и операции суперпозиции, для некоторых $\mu_0, \mu_1, \ldots, \mu_n$ и l, $\mu_i \in \mathfrak{L}_0^{(1)}$, $i = 1, 2, \ldots, n$, $\mu_0 \in \mathfrak{L}_{\mathrm{C}}$, $l \in \mathbb{N} \cup \{0\}$,

$$\{\; \mu_i \;\mid\; i = 1, 2, \ldots, n \;\} \not\subset R_j^{(1)},$$

$j = 0, 1, 2, \ldots,$ выполнено:

$$\begin{gathered}\mu_1^{2^l} x_1 + \mu_1^{2^l} x_2 + \mu_2^{2^l} x_3 + \mu_2^{2^l} x_4 + \ldots \\ + \mu_n^{2^l} x_{2n-1} + \mu_n^{2^l} x_{2n} + \mu_0 \in K(M)\end{gathered}$$

Далее, по теореме 3.2.2 имеем

$$1 \in K^{(1)}\left(\{\mu_1, \mu_2, \ldots, \mu_n\}\right).$$

Отсюда, как нетрудно видеть,

$$1 \in K^{(1)}\left(\left\{\mu_1^{2^l}, \mu_2^{2^l}, \ldots, \mu_n^{2^l}\right\}\right).$$

Используя последнее включение, нетрудно показать, что для некоторых $\tilde{\mu}$ и $\tilde{\gamma}$, $\tilde{\mu} \in \mathfrak{L}_0^{(1)}$, $\tilde{\gamma} \in \mathfrak{L}_c$, выполнено:

$$x_1 + x_2 + \tilde{\mu} x + \tilde{\gamma} \in K(M)$$

Отсюда, как уже отмечалось ранее, получим (3.72).

Лемма доказана.

Используя лемму 3.4.1, получим критерий для свойства (3.70).

Теорема 3.4.1. *Пусть* $M \not\subseteq \Theta$ *для любого* $\Theta, \Theta \in J^*$, $|M| < \infty$,

$$C(M) = \{\gamma_1, \gamma_2, \ldots, \gamma_s\},$$

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

Условия 1-4 эквивалентны.

1. *Найдутся* $\beta_1, \beta_2, \ldots, \beta_s$ *из* $K^{(1)}(U(M))$,

$$\sum_{i=1}^{s} \beta_i \gamma_i = 0$$

и

$$\left| \left\{ \ i \ \mid \ \beta_i \in 1 + \xi \mathfrak{L}_0^{(1)}, \ \ i = 1, 2, \ldots, k \ \right\} \right|$$

нечетно.

2.

$$(K(M) \cap \mathfrak{L}_0) \setminus V_2 \neq \emptyset.$$

3.

$$0 \in K(M).$$

4.

$$x_1 + x_2 \in K(M).$$

Доказательство. Пусть $M \not\subseteq \Theta$ для любого Θ, $\Theta \in J^*$, $|M| < \infty$. По лемме 3.4.1 выполнено:

$$x_1 + x_2 + x_3 \in K(M).$$

Пусть выполнено условие 1 теоремы. Можно считать, что $\beta_i \in S(U(M))$.

Для каждого μ из $U(M)$ имеем:

$$\mu x_1 + \mu x_2 + x_3 \in K(M).$$

Имеет место

$$\sum_{i=1}^{s} \sum_{j=1}^{r_i} \Pi_{ij} \gamma_i = 0,$$

где Π_{ij} получается с использованием лишь операции подстановки из элементов множества $U(M)$ и

$$\left| \left\{ \ (i,j) \ \mid \ i = 1, 2, \ldots, k, \ \ j = 1, 2, \ldots, r_i, \ \ \Pi_{ij} \in 1 + \xi \mathfrak{L}_0^{(1)} \ \right\} \right|$$

нечетно. Положим

$$k^* = \sum_{i=1}^{s} r_i.$$

Из $x_1 + x_2 + x_3$ с использованием операции подстановки построим $x_1 + x_2 + \cdots + x_m$ с $m \geq k^*$. Для некоторого m', $m' \geq m$ в $\mathfrak{L}_0^{(1)}$ найдутся μ_{k+1}, μ_{k+2},..., $\mu_{m'}$ такие, что выполнено:

$$\begin{aligned} &\Pi_{11} x_{11} + \Pi_{12} x_{12} + \cdots + \Pi_{1r_1} x_{1r_1} + \Pi_{21} x_{21} + \Pi_{22} x_{22} + \ldots \\ &+ \Pi_{2r_2} x_{2r_2} + \cdots + \Pi_{s1} x_{s1} + \Pi_{s2} x_{s2} + \cdots + \Pi_{sr_s} x_{sr_s} + \mu_{k+1} x_{k+1} + \\ &\mu_{k+2} x_{k+2} + \cdots + \mu_{m'} x_{m'} \in K \left(\{ \ x_1 + x_2 + \cdots + x_m, \right. \\ &\left. \mu x_1 + \mu x_2 + x_3 \ \mid \ \mu \in U(M) \ \} \right) \cap V_2. \end{aligned}$$

Через g_i, $g_i = g_i(x_{i1}, \ldots, x_{ip_i})$, $i = 1, 2, \ldots, s$, обозначим ЛА из множества M, что $\gamma_i = C(g_i)$ и, если $1 \leq i \leq k$, то $g_i \notin V_2$.

Тогда

$$\begin{aligned} &\Pi_{11} g_1 + \Pi_{12} g_1 + \ldots \Pi_{1r_1} g_1 + \Pi_{21} g_2 + \Pi_{22} g_2 + \ldots \\ &+ \Pi_{2r_2} g_2 + \cdots + \Pi_{s1} g_s + \Pi_{s2} g_s + \cdots + \Pi_{sr_s} g_s + \mu_{k+1} x_{k+1} + \\ &\mu_{k+2} x_{k+2} + \cdots + \mu_{m'} x_{m'} \in (K(M) \cap \mathfrak{L}_0) \setminus V_2. \end{aligned}$$

Пусть выполнено условие 2 теоремы. Отождествляя переменные ЛА $f(x_1, x_2, \ldots, x_n)$ из $(K(M) \cap \mathfrak{L}_0) \setminus V_2$, получим ЛА $f'(x)$, $f'(x) \in \xi\mathfrak{L}_0^{(1)}$. Тогда

$$\mathrm{fb}\,(f') = 0.$$

Условие 3 теоремы доказано.

Если выполнено условие 3 теоремы, то из равенства

$$x_1 + x_2 = x_1 + x_2 + 0$$

вытекает условие 4.

Пусть имеет место условие 4 теоремы. Индукцией по построению ЛА из $K(M)$ нетрудно показать, что справедлива

Лемма 3.4.2. *В условиях теоремы 3.4.1 пусть* $f \in K(M)$, $C(f) = \{\gamma\}$,

$$\gamma = \sum_{i=1}^{s} \beta_i' \gamma_i,$$

$$\mathbb{N}' = \left\{ \ i \ \mid \ \beta_i' \in 1 + \xi\mathfrak{L}_0^{(1)}, \ \ i = 1, 2, \ldots, k \ \right\}.$$

Тогда либо $f \in V_2$ *и* $|\mathbb{N}'|$ *четно, либо* $f \notin V_2$ *и* $|\mathbb{N}'|$ *нечетно.*

Так как $x_1 + x_2 \notin V_2$, то из приведенной леммы следует условие 1 теоремы.

Теорема доказана.

Теорема 3.4.2. *Существует алгоритм, проверяющий для любой пары конечных множеств* M, M_1, $M \subset \mathfrak{L}$, $M_1 \subset \mathfrak{L}$, *справедливо ли*

$$M_1 \cup \{x_1 + x_2\} \subseteq K(M).$$

Доказательство. По теореме 3.3.2 достаточно доказать алгоритмическую разрешимость проверки соотношения (3.70) для любого конечного M, $M \subset \mathfrak{L}$.

Пусть $C(M) = \{\gamma_1, \gamma_2, \ldots, \gamma_m\}$, $\gamma_1, \gamma_2, \ldots, \gamma_r$ - базис $S'(\mu, C(M))$ в смысле доказательства теоремы 3.3.1 и N', M'' – множества, построенные в этом доказательстве.

Линейной комбинации l, $\quad l = \zeta_1\gamma_1 + \cdots + \zeta_m\gamma_m$, $\quad \zeta_i \in N'$, $\quad i = 1, 2, \ldots, m$, сопоставим число $v(l)$,

$$v(l) = \left| \left\{ \; i \mid \zeta_i \in 1 + \xi\mathfrak{L}_0^{(1)}, \;\; \gamma_i \in C\left(M \setminus V_2\right) \; \right\} \right|.$$

По условию 1 теоремы 3.4.1 включение (3.70) выполнено в точности тогда, когда

$$\{ \; l \mid l = \zeta_1\gamma_1 + \cdots + \zeta_m\gamma_m, \quad \zeta_i \in N', \;\; i = 1, 2, \ldots, m,$$
$$v(l) \;\; \text{нечетно} \; \} \cap$$
$$\{ \; \zeta_1\gamma_1 + \cdots + \zeta_r\gamma_r, \mid \zeta_i \in M'', \;\; i = 1, 2, \ldots, r \; \} \neq \emptyset.$$

Отсюда вытекает конечность процедуры проверки соотношения (3.70).

Теорема 3.4.2 доказана.

Далее подробнее исследуется строение K-замкнутых классов, содержащих сумматор от трех переменных. Основной результат будет получен для конечно-порожденных классов.

Рассмотрим множество W, состоящее из ЛА. соотношение $x_1 + x_2 \in K(W)$. Пусть

$$W \not\subseteq \Theta \quad \text{для любого} \quad \Theta, \quad \Theta \in J^*. \tag{3.74}$$

По лемме 3.4.1 справедливо:

$$x_1 + x_2 + x_3 \in K(W). \tag{3.75}$$

Сначала рассмотрим случай

$$U(W) \subseteq E_2. \tag{3.76}$$

Введем операцию $" + "$ над векторами из E_2^n. Пусть $v_i \in E_2^n$,

$$v_i = (v_{i1}, v_{i2}, \ldots, v_{in}),$$

$i = 1, 2$. Положим

$$v_1 + v_2 = (v_{11} + v_{21}, v_{12} + v_{22}, v_{13} + v_{23}, \ldots, v_{1n} + v_{2n}).$$

Таким образом, введена рассматривается операция покомпонентной суммы (по модулю 2) двух векторов.

Множество E_2^n вместе с введенной операцией обозначим $V^{(n)}$. Замыкание множества V, $V \subseteq V^{(n)}$, по операции покомпонентного сложения обозначим $S(V)$.

Не ограничивая общности рассуждений, будем считать, что τ_0 и τ - длины предпериода и периода, соответственно, каждой последовательности коэффициентов рядов из $C(W)$. Пусть $f \in W$, $C(f) = \{\gamma\}$,

$$\gamma = \sum_{t=0}^{\infty} \gamma(t)\xi^t.$$

Через $V^{(\tau_0+\tau)}(f)$ обозначим вектор $(i, \gamma(0), \gamma(1), \ldots, \gamma(\tau_0+\tau-1))$, где

$$i = \begin{cases} 0, & \text{если} \quad W \in V_2 \\ 1, & \text{если} \quad W \notin V_2. \end{cases}$$

Далее положим

$$V^{(\tau_0+\tau)}(W) = \{\ V^{(\tau_0+\tau)}(f)\ \mid\ f \in W\ \}.$$

Имеет место

Лемма 3.4.3. *В случае (3.74) и (3.76) соотношение*

$$x_1 + x_2 \in K(W) \tag{3.77}$$

выполнено в точности тогда, когда

$$10^{\tau_0+\tau} \in S(V^{(\tau_0+\tau)}(W)). \tag{3.78}$$

(Через 10^k обозначается вектор размерности k, первая компонента которого равна 1, а все остальные компоненты равны 0.)

Доказательство. Нетрудно видеть, что в случае (3.76) операция обратной связи неприменима ни к одной существенной переменной любой ЛА из W, а операции отождествления и переименования переменных ЛА f не изменяют вектор $V^{(\tau_0+\tau)}(f)$. Осталось рассмотреть операцию подстановки. Пусть ЛА $f^{\surd}(x_1, x_2, \ldots, x_{n+n'-1})$ получен подстановкой $f(x_1, x_2, \ldots, x_n)$ вместо переменной $x_{n+n'}$ ЛА $f'(x_{n+1}, x_{n+2}, \ldots, x_{n+n'})$ и $U(\{f, f'\}) \subseteq E_2$. Тогда если $x_{n+n'}$ - несущественная переменная ЛА f', то $V^{(\tau_0+\tau)}(f^{\surd}) = V^{(\tau_0+\tau)}(f')$. Если $x_{n+n'}$ - существенная переменная ЛА f', то $V^{(\tau_0+\tau)}(f^{\surd}) = V^{(\tau_0+\tau)}(f') + V^{(\tau_0+\tau)}(f')$. Отсюда вытекает, что

$$V^{(\tau_0+\tau)}(K(W)) = S(V^{(\tau_0+\tau)}(W)). \tag{3.79}$$

Нетрудно видеть, что $V^{(\tau_0+\tau)}(x_1+x_2) = 10^{\tau_0+\tau}$. Поэтому из (3.77) и (3.79) следует (3.78). Необходимость утверждения леммы доказана.

Докажем достаточность. Пусть выполнено (3.78). Тогда с учетом (3.79) в $K(W)$ найдется ЛА f такой, что $V^{(\tau_0+\tau)}(f) = 10^{\tau_0+\tau}$. Для любого ЛА f' из $K(W)$ множество $C(f')$ состоит из периодической последовательности с предпериодом τ_0 и периодом τ. Поэтому $C(f) = \{0\}$. Так как ЛА f имеет четное число непосредственных входов, остальные входы несущественные и выполнено (3.76), то, отождествляя все переменные ЛА f, получим ЛА, реализующий константу 0. Отсюда, из (3.75) и теоремы 3.4.2 получаем (3.77).

Лемма 3.4.3 доказана.

Далее укажем способ, позволяющий по V, $\;V \subseteq V^{(n)}$, проверять включение

$$10^n \in S(V). \tag{3.80}$$

Итак, пусть $V \subseteq V^{(n)}$. Через V_1 обозначим множество всех векторов из V, первая компонента которых равна 1. Далее положим

$$V_0 = \{\ v_1 + v_2 \mid v_i \in V_1,\ \ i = 1, 2\ \} \cup$$
$$\{\ v \mid v \in V,\ \text{ первая компонента } v \text{ равна } 0\ \}$$

Если $V_i' \subseteq E_2^n$, $\quad i = 1, 2$, $\quad$ то положим

$$V_1' + V_2' = \{\ v_1 + v_2 \mid v_1 \in V_1',\ \ v_2 \in V_2'\ \}.$$

Несложный способ проверки включения (3.80) можно получить, учитывая, что имеет место

Лемма 3.4.4. *1.*

$$S(V) = (V_1 + S(V_0)) \cup S(V_0). \tag{3.81}$$

2. Множество $S(V_0)$ является векторным пространством над полем E_2, которое порождается множеством V_0.

Доказательство. Сначала докажем равенство (3.81). Пусть $v \in S(V)$. Тогда для некоторых $v_1, v_2, \dots, v_k$, $v_i \in V$, $i = 1, 2, \dots, k$, выполнено $v = v_1 + v_2 + \dots + v_k$. Не ограничивая общность рассуждений, можно считать, что $v_i \in V_1$ при $i = 1, 2, \dots, s$ и $v_i \notin V_1$ при $i = s+1, s+2, \dots k$.

Если s четно, то для каждого i, $i = 1, 2, \dots \frac{s}{2}$ положим $u_i = v_{2i-1} \uplus v_{2i}$. Тогда $v = u_1 + u_2 + \dots + u_{\frac{s}{2}} + v_{s+1} + v_{s+2} + \dots + v_k$, то есть $v \in S(V_0)$.

Если s нечетно, то для каждого i, $i = 1, 2, \dots \frac{s-1}{2}$ положим $u_i = v_{2i} + v_{2i+1}$. Тогда $v = v_1 + u_1 + u_2 + \dots + u_{\frac{s-1}{2}} + v_{s+1} + v_{s+2} + \dots + v_k$, то есть $v \in V_1 + S(V_0)$.

Таким образом, $v \in (V_1 + S(V_0)) \cup S(V_0)$ и первая часть леммы доказана.

Докажем вторую часть леммы. Заметим, что множество $S(V_0)$ является линейным подпространством векторного пространства E_2^{n+1} над полем E_2.

Вторая часть леммы 3.4.4, а, следовательно, вся лемма доказаны.

Далее рассмотрим случай

$$U(W) \not\subseteq E_2. \tag{3.82}$$

В соответствии с теоремой 3.2.1 рассмотрим два случая.

Случай 1. Для некоторых μ, u_0, T, $\mu \in \xi\mathfrak{L}_0^{(1)}$, $u_0 \in 1 + \xi E_2[\xi]$, $T \in \mathbb{N}$, выполнено

$$M^{(1)}(\mu, (\xi u_0)^T) \subseteq K^{(1)}(M) \subseteq M^{(1)}(\mu, u_0) \tag{3.83}$$

Случай 2. Для некоторых μ, u_0, T, $\mu \in \xi\mathfrak{L}_0^{(1)}$, $u_0 \in 1 + \xi E_2[\xi]$, $T \in \mathbb{N}$, выполнено

$$P^{(1)}(\mu, (\xi u_0)^T) \subseteq K^{(1)}(M) \subseteq M_0^{(1)}(\mu, u_0) \cap M^{(1)}(\mu, u_0). \tag{3.84}$$

Имеет место

Лемма 3.4.5. *Пусть* $W' \subseteq \mathfrak{L}$, $W' \nsubseteq \Theta$. *Тогда для любого* Θ, $\Theta \in J^*$, *найдутся* W'' *и* γ, $W'' \subseteq V_2$, $\gamma \in \mathfrak{L}_c$, *что*

$$K(W') = K\left(W'' \cup \{\gamma\}\right). \tag{3.85}$$

Доказательство. Через $f(x_1, \ldots, x_n)$ обозначим какой-нибудь элемент множества $W' \setminus V_2$. (По условию леммы $W' \setminus V_2 \neq \emptyset$.)

Положим: $W^* = \emptyset$, если $W' \setminus (V_2 \cup \{f\}) = \emptyset$. В противном случае положим

$$W^* = \{f(x_1, \ldots, x_n) + f'(x'_1, \ldots, x'_{n'}) + x'' \quad | \\ f' \in W' \setminus (V_2 \cup \{f\})\}.$$

Из лемме 3.4.1 следует $x_1 + x_2 + x_3 \in K(W')$, поэтому $W^* \subseteq K(W')$. Кроме того, для любого $f'(x'_1, \ldots, x'_{n'})$ выполнено

$$f'(x'_1, \ldots, x'_{n'}) = \\ f(x_1, \ldots, x_n) + f'(x'_1, \ldots, x'_{n'}) + f(x_1, \ldots, x_n).$$

Отсюда вытекает включение

$$W' \setminus V_2 \subseteq K(W^* \cup \{f\}).$$

Таким образом,

$$K(W') = K(\{f\} \cup W^* \cup (W' \cap V_2)).$$

Множество $W^* \cup (W' \cap V_2)$ обозначим через W^{**}. Нетрудно видеть, что $W^{**} \subseteq V_2$ и $K(W') = K(W^{**} \cup \{f\})$.

Обозначим через γ константу, получаемую применением операции обратной связи к переменной x ЛА $f(x \ldots x)$. Имеет место соотношение

$$f(x_1, \ldots x_n) = f(x_1, \ldots x_n) + f(\gamma, \ldots \gamma) + \gamma.$$

Отсюда получаем

$$K(W') = K(\{\gamma\} \cup \{f(x_1, \dots x_n) + f(x'_1, \dots x'_n) + x''\} \cup W^{**}).$$

Так как $f(x_1, \dots x_n) + f(x'_1, \dots x'_n) + x'' \in V_2$, то лемма 3.4.5 доказана.

Рассмотрим векторное пространство $S'(\mu, C)$ над полем $E_2(\mu)$ с порождающим множеством C. Положим

$$B(\mu, C) = \{\ b \ \mid \ b \text{ базис в } S'(\mu, C) \text{ над } E_2(\mu)\ \}.$$

Имеет место следующая лемма.

Лемма 3.4.6. *Пусть выполнены соотношения (3.75), (3.82). Для любого γ', $\gamma' \in S'(\mu, C(W))$, любого T, $T \in \mathbb{N}$, и любого b, $b \in B(\mu, C(W))$, имеют место следующие утверждения.*

1. *Найдется такое целое число n, найдутся многочлены $u_\gamma(\xi)$ и дроби $\mu^*_\gamma(\xi)$, такие, что имеют место соотношения:*

$$(u_\gamma(\xi), \xi u_0(\xi)) = 1, \ \deg u_\gamma(\xi) < (T+n)(1 + \deg u_0(\xi)), \ \ \gamma \in b,$$

$$\mu^*_\gamma(\mu) \in M^{(1)}(\mu, (\xi u_0)^T) \setminus (1 + \mu \mathfrak{L}_0^{(1)}(\mu)), \ \ \gamma \in b,$$

$$\gamma' = \sum_{\gamma \in b} \left(\frac{u_\gamma(\mu)}{(\mu u_0(\mu))^n} + \mu^*_\gamma(\mu) \right) \gamma. \tag{3.86}$$

При этом для каждого γ, $\gamma \in b$, ЛА $u_\gamma(\mu)$ и $\mu^*_\gamma(\mu)$ определяются единственным образом.

2. *Найдется такое целое число n, найдутся многочлены $u_\gamma(\xi)$, $u'_\gamma(\xi)$ и дроби $\mu^*_\gamma(\xi)$, такие, что имеют место соотношения:*

$$(u_\gamma(\xi), \xi u_0(\xi)) = 1, \ \deg u'_\gamma(\xi) < 2T(1 + \deg u_0(\xi)), \ \ \gamma \in b,$$

$$\mu^*_\gamma \in P^{(1)}(\mu, (\xi u_0(\xi))^T) \setminus (1 + \mu \mathfrak{L}_0^{(1)}(\mu)), \ \ \gamma \in b,$$

$$\gamma' = \sum_{\gamma \in b} \left(\frac{u_\gamma(\mu)}{(\mu u_0(\mu))^n} + \frac{u'_\gamma(\mu)}{1 + (\mu u_0(\mu))^{2T}} + \mu^*_\gamma(\mu) \right) \gamma. \tag{3.87}$$

При этом для каждого γ, $\gamma \in b$, ЛА $u_\gamma(\mu)$, $u'_\gamma(\mu)$ и $\mu^*_\gamma(\mu)$ определяются единственным образом.

Доказательство. Пусть $\gamma' \in S'(\mu, C(W))$. Тогда найдутся дроби $\mu_\gamma(\xi)$, $\gamma \in b$, такие, что

$$\gamma' = \sum_{\gamma \in b} \mu_\gamma(\mu)\gamma. \tag{3.88}$$

Найдется натуральное n' такое, что для любого γ, $\gamma \in b$, найдутся многочлены $u_{1\gamma}$ и $v_{1\gamma}$, удовлетворяющие соотношениям

$$\mu_\gamma(\xi) = \frac{u_{1\gamma}(\xi)}{(\xi u_0(\xi))^{n'} v_{1\gamma}(\xi)}, \tag{3.89}$$

$$(v_{1\gamma}(\xi), \xi u_0(\xi)) = 1.$$

Сначала получим разложение (3.86). Найдутся многочлены $u_{2\gamma}(\xi)$ и $u_{3\gamma}(\xi)$,

$$u_{2\gamma}(\xi) \cdot v_{1\gamma}(\xi) + u_{3\gamma}(\xi)(\xi u_0(\xi))^{n'+T} = u_{1\gamma}(\xi), \tag{3.90}$$

$$\deg u_{2\gamma}(\xi) < (n' + T)(1 + \deg u_0(\xi)).$$

Из (3.89) и (3.90) получаем

$$\mu_\gamma(\xi) = \frac{u_{2\gamma}(\xi)}{(\xi u_0(\xi))^{n'}} + \frac{u_{3\gamma}(\xi)}{v_{1\gamma}(\xi)}(\xi u_0(\xi))^T.$$

Отсюда и из (3.88) получаем (3.86).

Теперь докажем возможность разложения (3.87). Найдется натуральное число n' и найдутся многочлены $u_{2\gamma}(\xi)$, $u_{3\gamma}(\xi)$, что

$$\mu_\gamma(\xi) = \frac{u_{2\gamma}(\xi)}{(\xi u_0(\xi))^{n'}} + \frac{u_{3\gamma}(\xi)}{v_\gamma(\xi)}, \tag{3.91}$$

$\deg u_{3\gamma}(\xi) < \deg v_\gamma(\xi)$.

Далее, несколько модифицировав доказательство леммы 3.2.5, можно показать, что найдутся и притом единственным образом многочлены $u_{5\gamma}(\xi)$, $u_{6\gamma}(\xi)$, $v_{2\gamma}(\xi)$, такие, что выполнены следующие соотношения:

$$\deg u_{5\gamma}(\xi) < 2T(1+\deg u_0(\xi)),$$

$$\deg u_{6\gamma}(\xi) < T(1+\deg u_0(\xi))(\deg v_{2\gamma}(\xi)-1),$$

$$\frac{u_{3\gamma}(\xi)}{v_\gamma(\xi)} = \frac{u_{5\gamma}(\xi)}{1+(\xi u_0(\xi))^{2T}} + \frac{u_{6\gamma}(\xi)\,(\xi u_0(\xi))^T}{1+(\xi u_0(\xi))^T\, v_{2\gamma}\left((\xi u_0(\xi))^T\right)}. \tag{3.92}$$

Отсюда и из (3.91) вытекает (3.87).

Теперь обоснуем единственность разложения (3.86). Если наряду с (3.86) для некоторых n', $n'\in\mathbb{Z}$, некоторых $u'_\gamma(\xi)$ из $E_2[\xi]$, таких, что

$$\deg u'_\gamma(\xi) < (T+n')(1+\deg u_0(\xi))$$

и некоторого $\mu^{**}_\gamma(\xi)$,

$$\mu^{**}_\gamma(\xi)\in M^{(1)}(\mu,(\xi u_0(\xi))^T)\setminus(1+\mu\mathfrak{L}^{(1)}_0(\mu)),$$

справедливо

$$\gamma' = \sum_{\gamma\in b}\left(\frac{u'_\gamma(\mu)}{(\mu u_0(\mu))^{n'}} + \mu^{**}_\gamma(\mu)\right)\gamma.$$

то ввиду линейной независимости системы b в $S'(\mu, C(W))$,

$$\frac{u_\gamma(\mu)}{(\mu u_0(\mu))^n} + \mu^*_\gamma(\mu) = \frac{u'_\gamma(\mu)}{(\mu u_0(\mu))^{n'}} + \mu^{**}_\gamma(\mu), \tag{3.93}$$

для любого γ, $\gamma\in b$.

Из условия леммы и этого равенства вытекает равенство $n=n'$. Поэтому имеем:

$$u_\gamma(\mu) + u'_\gamma(\mu) = (\mu u_0)^n\left(\mu^*_\gamma(\mu)+\mu^{**}_\gamma(\mu)\right) \tag{3.94}$$

Так как $\deg\left(u_\gamma(\xi)+u'_\gamma(\xi)\right) < \deg\left((\xi u_0(\xi))^n\right)$ и $\xi u_0(\xi)$ взаимно прост со знаменателем дроби $\mu^*_\gamma(\xi)+\mu^{**}_\gamma(\xi)$, то то из (3.94) получаем:

$$u_\gamma(\xi)+u'_\gamma(\xi)\ \text{ и }\ \mu^*_\gamma(\xi)+\mu^{**}_\gamma(\xi).$$

Таким образом, единственность разложения (3.86) доказана.

Единственность разложения (3.87) вытекает из линейной независимости векторов системы b и единственности разложений (3.91) и (3.92).

Лемма доказана.

Если для W, $W \subseteq \mathfrak{L}$, выполнены (3.75) и (3.82), то для некоторого μ, $\mu \in \left(\xi\mathfrak{L}_0^{(1)}\right) \setminus \{0\}$, имеет место $E_2(\mu) = E_2(U(W))$. Пусть $\gamma' \in S'(\mu, C(W))$, $b \in B(\mu, C(W))$. Тогда имеют место равенства (3.86) и (3.87). Положим

$$\omega_{\mu,u_0,b,T}(\gamma') = \begin{cases} \sum_{\gamma\in b} \frac{u_\gamma(\mu)}{(\mu u_0(\mu))^n}\gamma, & \text{если } U(W) \not\subseteq M_0(\mu) \text{ (случай 1)}, \\ \sum_{\gamma\in b} \left(\frac{u_\gamma(\mu)}{(\mu u_0(\mu))^n} + \frac{u'_\gamma(\mu)}{1+(\mu u_0(\mu))^{2T}}\right)\gamma, & \text{если } U(W) \subseteq M_0(\mu) \text{ (случай 2)}. \end{cases}$$

Пусть $C \subset S'(\mu, C(W))$ и $b \in B(\mu, C(W))$. Положим

$$\omega_{\mu,u_0,b,T}(C) = \{\ \omega_{\mu,b,T}(\gamma') \mid \gamma' \in C\ \}.$$

Пусть теперь заданы μ, b, T, n, u_0, где $\mu \in \xi\mathfrak{L}_0^{(1)} \setminus \{0\}$, b – линейно независимое над полем $E_2(\mu)$ множество векторов, $T \in \mathbb{N}$, $n \in \mathbb{Z}$, $u_0 \in 1 + \xi E_2[\xi]$.

Определим множество $\varpi_{\mu,u_0,b,T,n}$, положив в случае 1:

$$\varpi_{\mu,u_0,b,T,n} = \left\{ \sum_{\gamma\in b} \frac{u_\gamma(\mu)}{(\mu u_0(\mu))^n}\gamma \mid \deg u_\gamma(\xi) < (T+n)(1+\deg u_0(\xi)) \right\}, \quad (3.95)$$

а в случае 2 имеем еще один параметр T', $T' \in \mathbb{N}$:

$$\varpi_{\mu,u_0,b,T,n,T'} = \left\{ \sum_{\gamma\in b} \left(\frac{u_\gamma(\mu)}{(\mu u_0(\mu))^n} + \frac{u'_\gamma(\mu)}{1+(\mu u_0(\mu))^{2T}}\right)\gamma \mid \right.$$
$$\left. \deg u'_\gamma(\xi) < 2T(1+\deg u_0(\xi)),\ \deg(u_\gamma(\xi)) < T' \right\}.$$

Теорема 3.4.3. *Пусть для конечного множества W, $W \subset \mathfrak{L}$, выполнены соотношения (3.75), (3.82). Тогда в случае 1 для некоторых μ, u_0, b, T, n, $\mu \in \xi\mathfrak{L}_0^{(1)} \setminus \{0\}$, $u_0 \in 1 + \xi E_2[\xi]$, $b \subseteq C(W)$, $T \in \mathbb{N}$, $n \in \mathbb{N}$, имеет место включение:*

$$\omega_{\mu,u_0,b,T}(C(K(W))) \subseteq \varpi_{\mu,u_0,b,T,n}, \quad (3.96)$$

а в случае 2 для некоторых μ, u_0, b, T, n, T', $\mu \in \xi\mathfrak{L}_0^{(1)} \setminus \{0\}$, $u_0 \in 1 + \xi E_2[\xi]$, $b \subseteq C(W)$, $T \in \mathbb{N}$, $n \in \mathbb{N}$, $T' \in \mathbb{N}$, *имеет место включение:*

$$\omega_{\mu,u_0,b,T}\left(C(K(W))\right) \subseteq \varpi_{\mu,u_0,b,T,n,T'}. \tag{3.97}$$

Доказательство. Рассмотрим конечное множество W, $W \subset \mathfrak{L}$, для которого выполнены соотношения (3.75), (3.82). Пусть имеет место случай 1. Тогда для любого i, $i = 0, 1, \ldots$, выполнено:

$$W \not\subseteq R_i^{(1)},$$

и по теореме 3.2.1 найдутся такие μ, u_0, T, $\mu \in \xi\mathfrak{L}_0^{(1)}$, $u_0 \in 1 + \xi E_2[\xi]$, $T \in \mathbb{N}$, что выполнено соотношение (3.7). Заметим, что для любых μ_1, $\mu_1 \in U(K(W))$ и любых γ_i, $i = 1, 2$, из

$$\omega_{\mu,u_0,b,T}\left(\gamma_i\right) \in \varpi_{\mu,u_0,b,T,n}$$

следуют включения:

$$\omega_{\mu,u_0,b,T}\left(\mu_1\gamma_i\right) \in \varpi_{\mu,u_0,b,T,n},$$

$$\omega_{\mu,u_0,b,T}\left(\gamma_1 + \gamma_2\right) \in \varpi_{\mu,u_0,b,T,n},$$

Поэтому, определив b и n, $b \in B\left(\mu, C\left(W\right)\right)$, $n \in \mathbb{N}$, такие, что

$$\omega_{\mu,u_0,b,T}\left(C\left(W\right)\right) \subseteq \varpi_{\mu,u_0,b,T,n},$$

получаем соотношение (3.96).

Включение (3.97) доказывается аналогичными рассуждениями.

Теорема 3.4.3 доказана.

Теоремы 3.2.1 и 3.4.3 полностью определяют структуру конечнопорожденных K-замкнутых классов, содержащих сумматор от трех переменных, за исключением простого случая, когда для K-замкнутого класса W не выполнено: (3.82).

Глава 4

Аппроксимационная выразимость в классе линейных автоматов через множества, содержащие существенный автомат

В параграфе 2 главы 1 рассматривался оператор аппроксимационного замыкания. Для $\mathfrak{L}_k$ была найдена приведенная A-критериальная система. В настоящей главе рассматриваются задачи A-выразимости для ЛА над полем E_2.

4.1. Аппроксимационная выразимость в классе одноместных линейных автоматов, сохраняющих нулевую последовательность

Рассмотрим множество $\mathfrak{L}_0^{(1)}$ одноместных ЛА, сохраняющих нулевую последовательность. Как указано в [68], множество $\mathfrak{L}_0^{(1)}$ строится из проводника $\mathrm{id}(x)$, и задержки $\xi(x)$ с нулевым начальным состоянием с использованием следующих трех операций.

1. Сложения "+". Если $\mu_i(x) \in \mathfrak{L}_0^{(1)}, i = 1, 2$, то суммой $\mu_1(x)$ и $\mu_2(x)$ называется ЛА $\mu_1(x) + \mu_2(x)$.

2. Умножения "$\cdot$". Если $\mu_i(x) \in \mathfrak{L}_0^{(1)}, i = 1, 2$, то произведением $\mu_1(x)$ на $\mu_2(x)$ называется ЛА $\mu_1 \cdot \mu_2$, получаемый подстановкой μ_1 вместо переменной μ_2.

3. Операции "fb". Если $\mu_1(x) \in \mathfrak{L}_0^{(1)}$ и $\mu_2(x) \in \xi\mathfrak{L}_0^{(1)}$, то, применяя операцию обратной связи к переменной x_2 ЛА $\mu_1(x_1) + \mu_2(x_2)$, получим новый ЛА, который будем обозначать $\mathrm{fb}_{x_2}(\mu_1(x_1) + \mu_2(x_2))$.

Как и в главе 1, замыкание множества M, $M \subseteq \mathfrak{L}_0^{(1)}$, по операциям сложения и умножения обозначим $S^{(1)}(M)$, а замыкание этого множества по операциям сложения, умножения и операции "fb"обозначим $K^{(1)}(M)$.

Как показано в главе 1, [68], для любого ЛА $f(x)$ из множества $\mathfrak{L}_0^{(1)}$, найдутся натуральные числа n и k и найдутся числа $a_0, a_1, \dots a_n, b_1, b_2, \dots b_k$ из множества $E_2 = \{0, 1\}$ такие, что

$$f(x) = \frac{\sum_{i=0}^{n} a_i \xi^i}{1 + \sum_{i=1}^{k} b_i \xi^i} x.$$

На множестве $\mathfrak{L}_0^{(1)}$ рассмотрим оператор $A^{(1)}$-замыкания [17]. Пусть τ – натуральное число. Два ЛА называются τ-эквивалентными, если отображения, задаваемые ими на словах длины не большей τ, совпадают. ЛА f $A^{(1)}$-выразима через элементы множества M, если для любого натурального числа τ в $S^{(1)}(M)$ найдется ЛА, τ-эквивалентный f. Множество всех ЛА $A^{(1)}$-выразимых через элементы множества M называется $A^{(1)}$-замыканием множества M и обозначается $A^{(1)}(M)$.

Используя известную технику [42], можно показать, что ЛА f содержится в $A^{(1)}(M)$ в точности тогда, когда для любого натурального числа τ в $K^{(1)}(M)$ содержится ЛА τ-эквивалентный f. Таким образом, добавление операции "fb"к операциям сложения и умножения не изменяет $A^{(1)}$-замыкания множества M.

В настоящем параграфе получен алгоритм проверки $A^{(1)}$-выразимости в $\mathfrak{L}_0^{(1)}$ заданного ЛА через заданную конечную систему ЛА.

Если на множествах M_i, $i = 1, 2$, $M_i \subseteq \mathfrak{L}_0^{(1)}$, введены операции сложения и умножения, то можно рассмотреть новые множества $M_1 + M_2$, $M_1 \cdot M_2$, определяемые следующим образом

$$M_1 + M_2 = \{\ \mu_1 + \mu_2 \ |\ \mu_i \in M_i,\ \ i = 1, 2\ \},$$

$$M_1 \cdot M_2 = \{\ \mu_1 \cdot \mu_2 \ |\ \mu_i \in M_i,\ \ i = 1, 2\ \}.$$

Мы ранее уже использовали обозначение $\xi\mathfrak{L}$, понимая под ним произведение $\{\xi\} \cdot \mathfrak{L}_0^{(1)}$ множества $\{\xi\}$, состоящего из единственной задержки с нулевым начальным состоянием, и множества $\mathfrak{L}_0^{(1)}$. Еще использовалось выражение $1 + \xi E_2[\xi]$ для обозначения множества $\{1\} + \{\xi\} \cdot E_2[\xi]$.

Пусть $\mu_0 \in \xi \cdot \mathfrak{L}_0^{(1)} \setminus \{0\}$. Множество всех ЛА, построенных из проводника и элемента μ_0 с использованием операций сложения, умножения и обратной связи обозначим $\mathfrak{L}_0^{(1)}(\mu_0)$.

Множество формальных степенных рядов (вообще говоря, непериодических) переменной μ_0, $\mu_0 \in \{\xi\} \cdot \mathfrak{L}_0^{(1)} \setminus \{0\}$, над полем E_2 обозначим $R_2(\mu_0)$. Таким образом, если $\rho \in R_2(\mu_0)$, то для некоторых чисел $a_i, \quad a_i \in E_2, \quad i = 0, 1, \ldots,$ выполнено:

$$\rho = \sum_{i=0}^{\infty} a_i \mu_0^i.$$

Как показано в [68], дробь μ_0 можно представить степенным рядом переменной ξ: $\mu_0 = \sum_{i=0}^{\infty} b_i \xi^i$, $b_i \in E_2$. При этом последовательность коэффициентов $b_i, \quad i = 0, 1, \ldots,$ является периодической (с предпериодом) и $b_0 = 0$. Таким образом, каждый элемент из $R_2(\mu_0)$ является рядом, члены которого – степени некоторого ряда. Нетрудно видеть также, что для каждого натурального i i-я степень ряда μ_0 также является рядом из $R_2(\xi)$, первые i коэффициентов которого равны нулю. Поэтому любой ряд ρ из $R_2(\mu_0)$,

$$\rho = \sum_{i=0}^{\infty} a_i \mu_0^i,$$

можно просуммировать, т.е. сопоставить ему ряд

$$\sum_{i=0}^{\infty} b_i \xi^i$$

из $R_2(\xi)$ следующим образом. Пусть

$$\mu_0^i = \sum_{j=0}^{\infty} b_{ij} \xi^j$$

Зафиксируем целое неотрицательное n и положим

$$b_n = a_0 b_{0n} \oplus a_1 b_{1n} \oplus \cdots \oplus a_n b_{nn}.$$

Искомая сумма есть ряд
$$\sum_{i=0}^{\infty} b_i \xi^i.$$

Пусть $\rho_0 \in R_2(\mu_0)$ и $\rho_1 \in R_2(\mu_1)$. Ряды ρ_0 и ρ_1 будем называть τ-эквивалентными, если их первые τ коэффициентов совпадают. Нетрудно видеть, что введенное понятие τ-эквивалентности рядов является расширением понятия τ-эквивалентности ЛА с $\mathfrak{L}_0^{(1)}$ на $R_2(\xi)$.

Пусть $\rho_0 \in R_2(\mu_0)$ и $\rho_1 \in R_2(\mu_1)$. Ряды ρ_0 и ρ_1 будем называть равными, если равны их суммы. Равенство рядов ρ_0 и ρ_1 обозначается как обычно,
$$\rho_0 = \rho_1.$$
Понятие равенства рядов является расширением понятия равенства ЛА с $\mathfrak{L}_0^{(1)}$ на $R_2(\xi)$.

Таким образом, любой элемент из $R_2(\mu_0)$ равен некоторому элементу из $R_2(\xi)$. Например, рассмотрим ЛА $\mu = \frac{\xi}{1+\xi^2}$. Имеет место равенство $\mu = \frac{\xi}{1+\xi} + \left(\frac{\xi}{1+\xi}\right)^2$. Поэтому ЛА μ является элементом множества $R_2(\frac{\xi}{1+\xi})$, а последовательность коэффициентов соответствующего ряда – $0, 1, 1, 0, 0, 0, \ldots$. С другой стороны, имеет место равенство
$$\mu = \xi + \xi^3 + \xi^5 + \xi^7 + \ldots,$$
т. е. этот ЛА является элементом $R_2(\xi)$, а коэффициенты соответствующего ряда – $0, 1, 0, 1, 0, 1, \ldots$.

Два множества M_1 и M_2, $\quad M_i \subseteq R_2(\mu_i), \quad i = 1, 2$, равны $(M_1 = M_2)$ в точности тогда, когда для каждого элемента из M_1 найдется равный ему в M_2 и наоборот. Следующий пример устанавливает равенство
$$R_2(\xi) = R_2(\xi + \xi^2).$$
Действительно, включение $R_2(\xi + \xi^2) \subseteq R_2(\xi)$ уже фактически упоминалось выше, а справедливость включения
$$R_2(\xi) \subseteq R_2(\xi + \xi^2)$$

можно продемонстрировать следующим образом. Рассмотрим некоторый ряд $\mu = \sum_{i=0}^{\infty} a_i \xi^i, \quad a_i \in E_2$. Индукцией по i будем строить последовательность b_i, $i = 0, 1, 2, \ldots$ коэффициентов ряда ρ, $\rho = \sum_{i=0}^{\infty} b_i \left(\xi + \xi^2\right)^i$, равного μ. При $i = 0$ полагаем $b_0 = a_0$. Пусть коэффициенты $b_0, b_1, \ldots, b_k$ уже найдены. Представим $\sum_{i=0}^{k} b_i \left(\xi + \xi^2\right)^i$ рядом из $R_2(\xi)$. Пусть коэффициент при x^{k+1} последнего ряда равен c. Положим $b_{k+1} = c \oplus a_{k+1}$. Таким образом, указан способ вычисления коэффициентов $\{b_i\}$. Следуя этому построению, получим, например,

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

где в последовательности коэффициентов единицы находятся на местах с номерами, равными степеням двойки. Заметим, что полученная последовательность коэффициентов b_0, b_1, $\ldots$ не является периодической.

Пусть k – натуральное число и $u(\xi) \in 1 + \xi E_2[\xi]$. Через $P_1^0(\xi, k, u)$ обозначим множество

$$\left\{ \ \xi^k u(\xi) \frac{u'(\xi)}{v(\xi)} \ \mid \ u'(\xi), v(\xi) \in E_2[\xi], \ \ (\xi u(\xi), v(\xi)) = 1 \ \right\}.$$

Далее, пусть k – натуральное число, $u(\xi)$ – многочлен из $1 + \xi E_2[\xi]$. Через $Q_1^0(\xi, k, u)$ обозначим множество

$$\left\{ \ \xi^k \frac{u(\xi) u'(\xi)}{v(\xi)} \ \mid \ u'(\xi), v(\xi) \in E_2[\xi], \right.$$
$$\left. \deg v(\xi) - \deg u(\xi) - \deg u'(\xi) \geq 2k, \ \ (\xi u(\xi), v(\xi)) = 1 \ \right\}.$$

Исходя из теоремы 3.2.1 главы 3 нетрудно получить следующую лемму, использующую новые, более удобные для рассматриваемой задачи, обозначения.

Лемма 4.1.1. *Если $M \subseteq \mathfrak{L}_0^{(1)}$, $M \setminus E_2 \neq \emptyset$, то найдутся ЛА μ_0, $\mu_0 \in \xi \mathfrak{L}_0^1$, некоторое целое неотрицательное число k', многочлен u_0, $u_0 \in E_2[\mu_0]$, степени s и конечное множество ЛА M', что либо выполнено равенство*

$$K^{(1)}(M) = M' + P_1^0(\mu_0, k', u_0), \tag{4.1}$$

либо равенство

$$K^{(1)}(M) = M' + Q_1^0(\mu_0, k', u_0), \tag{4.2}$$

Лемма 4.1.1 доставляет описание структуры замкнутых по оператору $K^{(1)}$ классов в $\mathfrak{L}_1^0$. Соответствующий результат для оператора $A^{(1)}$ выглядит следующим образом.

Лемма 4.1.2. *Пусть*

$$M \subseteq \mathfrak{L}_0^{(1)}, \;\; M \setminus E_2 \neq \emptyset \tag{4.3}$$

и выполнено (4.1) либо (4.2). Тогда найдется целое неотрицательное число k' и найдется множество многочленов M', $M' \subseteq E_2[\mu_0]$, степень каждого из которых не более k', что выполнено равенство

$$A^{(1)}(M) = M' + \mu_0^{k'}\left(R_2(\mu_0) \cap \mathfrak{L}_1^0\right), \tag{4.4}$$

где множество $R_2(\mu_0) \cap \mathfrak{L}_1^0$ состоит из тех и только тех ЛА из $\mathfrak{L}_1^0$, которые разлагаются в ряд из множества $R_2(\mu_0)$.

Доказательство. Рассмотрим множество ЛА M со свойствами (4.3). Докажем сначала, что для ЛА μ, $\mu \in A^{(1)}(M)$, найдется ряд r, $r \in R_2(\mu_0)$, равный μ.

Найдутся натуральное число m и ЛА μ_1 из $1 + \xi\mathfrak{L}_1^0$ такие, что выполнено равенство

$$\mu_0 = \xi^m \mu_1.$$

Как в случае (4.1), так и в случае (4.2), имеем включение

$$K^{(1)}(M) \subseteq \mathfrak{L}(\mu_0).$$

Поэтому для каждого натурального числа t в $K^{(1)}(M)$ найдется ЛА $\mu^{(t)}(\xi)$ такой, что $\mu^{(t)}(\mu_0) \in K^{(1)}(M)$ и, кроме того, ЛА $\mu^{(t)}(\mu_0)$ и μ являются mt-эквивалентными.

Представим ЛА $\mu^{(t)}(\mu_0)$ рядом:

$$\mu^{(t)}(\mu_0) = \sum_{i=0}^{\infty} a_{ti}{\mu_0}^i,$$

$t = 1, 2, \dots$. Пусть t_1 и t_2 – два натуральных числа. Для определенности будем считать, что $t_1 < t_2$. Покажем, что первые t_1 слагаемых в рядах $\mu^{(t_1)}(\mu_0)$ и $\mu^{(t_2)}(\mu_0)$ совпадают. Предположим противное. Тогда ряд $\mu^{(t_1)}(\mu_0) + \mu^{(t_2)}(\mu_0)$ содержит слагаемое степени меньше t_1. Пусть t_0 – минимальная такая степень. Это означает, что для некоторого $\mu'(\xi)$, $\mu'(\xi) \in 1 + \xi\mathfrak{L}_1^0$ выполнено:

$$\mu^{(t_1)}(\mu_0) + \mu^{(t_2)}(\mu_0) = {\mu_0}^{t_0}\mu'(\mu_0) = \xi^{t_0 m}{\mu_1}^{t_0}\mu'(\mu_0).$$

Т.к. ${\mu_1}^{t_0}\mu'(\mu_0) \in 1 + \xi\mathfrak{L}_1^0$, то ЛА $\mu^{(t_1)}(\mu_0) + \mu^{(t_2)}(\mu_0)$ представляется рядом r из $R_2(\xi)$ среди первых mt_1 коэффициентов которого не все равны нулю. Но из mt_1-эквивалентности ЛА μ ЛА $\mu^{(t_1)}$ и $\mu^{(t_2)}$ следует соотношение $\mu^{(t_1)} + \mu^{(t_2)} \in \xi^{mt_1}\mathfrak{L}_1^0$. Полученное противоречие доказывает равенство первых t_1 коэффициентов рядов $\mu^{(t_1)}(\mu_0)$ и $\mu^{(t_2)}(\mu_0)$.

Далее определим ряд $r'(\mu_0) = \sum_{i=0}^{\infty} a_i\mu_0^i$, взяв в качестве a_i коэффициент при μ_0^i в ряде $\mu^{(i+1)}(\mu_0)$. Тогда для каждого натурального числа t первые t коэффициентов рядов $\mu^{(t)}(\mu_0)$ и $r'(\mu_0)$ совпадают, а поэтому эти ряды mt-эквивалентны. Таким образом, сумма ряда $r'(\mu_0)$ совпадает с μ. Следовательно, доказано, что

$$A^{(1)}(M) \subseteq R_2(\mu_0) \cap \mathfrak{L}_0^{(1)}.$$

Рассмотрим следующее множество ЛА:

$$A = \left\{{\mu_0}^{k'}\right\} \cdot \left(R_2(\mu_0) \cap \mathfrak{L}_1^0\right),$$

где k' – число, фигурирующее в лемме 1.

Таким образом, множество A состоит из всех ЛА, которые могут быть представлены рядом из $R_2(\mu_0)$, первые k коэффициентов которого равны нулю.

Заметим, что для любого μ, $\mu \in R_2(\mu_0) \cap \mathfrak{L}_0^{(1)}$ в $E_2[\mu_0]$ и A найдутся соответственно $u(\mu_0)$ и μ', удовлетворяющие соотношениям

$$\mu = u(\mu_0) + \mu', \ \deg u(\xi) < k', \ \mu' \in A.$$

Положим

$$M' = \Big\{ \ u(\mu_0) \ \mid \ u(\mu_0) \in E_2[\mu_0], \ \deg u(\xi) < k' \\ \text{и найдется ЛА } \ \mu \in A^{(1)}(M), \ \text{ что } \ u(\mu_0) + \mu \in A \ \Big\}.$$

Таким образом, имеет место включение

$$A^{(1)}(M) \subseteq M' + A. \tag{4.5}$$

Докажем далее, что, если выполнено (4.1) или (4.2), то имеет место

$$M' + \left\{\mu_0^{k'}\right\} \cdot \mathfrak{L}_1^0(\mu_0) \subseteq A^{(1)}(M), \tag{4.6}$$

в частности,

$$M' \subseteq A^{(1)}(M). \tag{4.7}$$

Действительно, рассмотрим ЛА μ, $\mu \in M' + \left\{\mu_0^{k'}\right\} \cdot \mathfrak{L}_1^0(\mu_0)$. Тогда найдется многочлен $u(\mu_0)$ степени меньшей k' и найдется ряд $r(\mu_0)$, $r(\mu_0) = \sum_{i=0}^{\infty} a_i\mu_0^i$, такие, что

$$\mu = u(\mu_0) + \mu_0^{k'} r(\mu_0).$$

ЛА

$$u(\mu_0) + \mu_0^{k'} u_0^{2^\tau}(\mu_0) \sum_{i=0}^{2^\tau-1} a_i\mu_0^i \ \text{ и } \ u(\mu_0) + \mu_0^{k'} \frac{u_0^{2^\tau}(\mu_0) \sum_{i=0}^{2^\tau-1} a_i\mu_0^i}{1 + (\mu_0 u_0(\mu_0))^{2^{\tau+k}}}$$

при любом натуральном τ содержатся, соответственно, в $M' + P_1^0(\mu_0, k', u_0)$ и $M' + Q_1^0(\mu_0, k', u_0)$ и являются τ-эквивалентными ЛА μ. Таким образом, включение (4.6) доказано.

Используя соотношение (4.6), нетрудно показать, что все элементы множества A содержатся в $A^{(1)}(M)$. Из включений $A \subseteq A^{(1)}(M)$, (4.7) и (4.5) вытекает доказываемое равенство (4.4).

Лемма 4.1.2 доказана.

Далее будет получен критерий представимости ЛА рядом из $R_2(\mu_0)$. Точнее, будет найден алгоритм, проверяющий, найдется ли в $R_2(\mu_0)$ ряд, сумма которого равна заданному ЛА.

Рассмотрим два ЛА μ_1 и μ_2 из $\xi\mathfrak{L}_1^0$. Тогда формально определены поля отношений многочленов $E_2(\mu_i)$, $i = 1, 2$. Поле $E_2(\mu_i)$ содержит подкольцо $\mathfrak{L}_1^0(\mu_i)$. Обозначим через $E_2(\mu_1, \mu_2)$ поле, получаемое расширением поля E_2 элементами μ_1 и μ_2 (см. [20]). По теореме Люрота [20] в $E_2(\xi)$ найдется дробь μ такая, что

$$E_2(\mu_1, \mu_2) = E_2(\mu). \tag{4.8}$$

Нетрудно показать (и это уже было показано в [68]), что μ, удовлетворяющее равенству (4.8), может быть выбрано из $\xi\mathfrak{L}_1^0$. Сначала получим следующий результат.

Лемма 4.1.3. *Пусть для каждого μ_i, $\mu_i \in \mathfrak{L}_1^0$, $i = 1, 2$, выполнено включение*

$$\mu_i \in R_2(\mu_0). \tag{4.9}$$

Тогда для μ, $\mu \in \{\xi\}\mathfrak{L}_1^0$, удовлетворяющего равенству (4.8), имеет место

$$\mu \in R_2(\mu_0). \tag{4.10}$$

Доказательство. Пусть выполнены соотношения (4.9), $i = 1, 2$, (4.8) и $\mu \in \xi\mathfrak{L}_1^0$. Тогда для некоторых рядов $r_i(\mu_0)$, $r_i(\mu_0) \in R_2(\mu_0)$, $i = 1, 2$, и некоторых многочленов двух переменных $u_i(x, y)$, $u_i(x, y) \in E_2[x, y]$, $i = 1, 2$ справедливы равенства:

$$\mu_i = r_i(\mu_0), \quad i = 1, 2, \tag{4.11}$$

$$\mu = \frac{u_1(\mu_1, \mu_2)}{u_2(\mu_1, \mu_2)}. \tag{4.12}$$

Последнее равенство нужно воспринимать как формальное соотношение, выполняющееся в поле $E_2(\xi)$.

Ввиду равенства (4.12) и равенств (4.11) в $1 + \mu_0 R_2(\mu_0)$ найдутся ряды $r_i'(\mu_0)$, $i = 1, 2$, и найдется целое число k' такие, что

$$\mu = \mu_0^{k'} \frac{r_1'(\mu_0)}{r_2'(\mu_0)}.$$

Дробь $\frac{r_1'(\mu_0)}{r_2'(\mu_0)}$ соответствует некоторому ряду r' из $\{1\} + \{\mu_0\} R_2(\mu_0)$. Отсюда следует, что k' – положительное число, а также включение (4.10).

Лемма 4.1.3 доказана.

Множество $R_2(\mu_0) \cap \mathfrak{L}_1^0$ состоит из всех одноместных ЛА, сохраняющих нулевую последовательность, каждый из которых равен сумме какого-нибудь ряда из $R_2(\mu_0)$. Таким образом,

$$R_2(\mu_0) \cap \mathfrak{L}_1^0 = \{ \ \mu \ | \ \mu \in \mathfrak{L}_1^0, \ \text{найдется} \ r(\mu_0) \in R_2(\mu_0), \ \text{что} \ \mu = r(\mu_0) \ \}.$$

Последняя лемма позволяет описать структуру $R_2(\mu_0) \cap \mathfrak{L}_1^0$.

Лемма 4.1.4. *Для каждого μ_0, $\mu_0 \in \xi \mathfrak{L}_1^0 \setminus \{0\}$ найдется μ, $\mu \in \xi \mathfrak{L}_1^0 \setminus \{0\}$, такое, что*

$$R_2(\mu_0) \cap \mathfrak{L}_1^0 = \mathfrak{L}_1^0(\mu). \tag{4.13}$$

Доказательство. Как было сказано в главе 1, степенью несократимой дроби μ', $\mu' \in \mathfrak{L}_1^0$ называется максимум из степеней числителя и знаменателя, степень дроби μ' обозначается $\deg \mu'$.

Заметим сначала, что множество $\big(R_2(\mu_0) \cap \mathfrak{L}_1^0\big) \setminus \{0\}$ содержит элемент из $\big(\xi \mathfrak{L}_1^0\big) \setminus \{0\}$. Пусть μ_1 – такой элемент, имеющий наименьшую степень.

Нетрудно видеть, что $\mathfrak{L}_1^0(\mu_1) \subseteq R_2(\mu_0) \cap \mathfrak{L}_1^0$. Пусть $R_2(\mu_0) \cap \mathfrak{L}_1^0 \neq \mathfrak{L}_1^0(\mu_1)$. Тогда найдется μ_2, $\mu_2 \in \big(R_2(\mu_0) \cap \mathfrak{L}_1^0\big) \setminus \mathfrak{L}_1^0(\mu_1)$, что $\mu_2 \in \big(\xi \mathfrak{L}_1^0\big) \setminus \{0\}$.

Тогда по лемме 3 ЛА μ, $\mu \in \xi \mathfrak{L}_1^0$, удовлетворяющий соотношению (4.8), содержится в $R_2(\mu_0)$, т.е. $\mathfrak{L}_1^0(\mu) \subseteq R_2(\mu_0) \cap \mathfrak{L}_1^0$. Поле $E_2(\xi)$ является алгебраическим расширением поля $E_2(\mu_1)$ степени $\deg \mu_1$ (см. теорему на стр. 258 [20]). Т.к. μ_2 не содержится в поле $E_2(\mu_1)$, то поле $E_2(\xi)$ – алгебраическое расширение поля $E_2(\mu_1, \mu_2)$ степени меньшей, чем $\deg \mu_1$. Отсюда и последней из упоминавшихся выше теорем, вытекает неравенство $\deg \mu < \deg \mu_1$. Получили противоречие с предположением о минимальности степени μ_1, поэтому доказано равенство

$$R_2(\mu_0) \cap \mathfrak{L}_1^0 = \mathfrak{L}_1^0(\mu_1),$$

а, вместе с ним, и лемма 4.1.4.

Теперь можно уточнить структуру $A^{(1)}$-замкнутых классов.

Теорема 4.1.1. *Для любого* M*,*

$$M \subseteq \mathfrak{L}_0^{(1)}, \;\; M \setminus E_2 \neq \emptyset, \tag{4.14}$$

найдется μ*,* $\mu \in \xi\mathfrak{L}_0^{(1)}$*,* $\mu \neq 0$*, найдется целое неотрицательное число* k' *и найдется множество многочленов* M'*,* $M' \subset E_2[\mu]$*, степень каждого из которых меньше* k'*, такие, что выполнено равенство*

$$A^{(1)}(M) = M' + \mu^{k'}\mathfrak{L}_0^{(1)}(\mu). \tag{4.15}$$

Доказательство. Пусть для некоторого множества M выполнены соотношения (4.14). Тогда по леммам 4.1.2 и 4.1.4 в множестве $\xi\mathfrak{L}_0^{(1)}$ найдутся ненулевые элементы μ_0 и μ, а также найдется целое неотрицательное число k' такие, что для некоторого конечного множества многочленов M', $\;M' \subset E_2[\mu_0]$ степени меньшей k' выполнено равенство

$$A^{(1)}(M) = M' + \mu_0^{k'}\mathfrak{L}_0^{(1)}(\mu), \tag{4.16}$$

причем $\mu_0 \in \mathfrak{L}_0^{(1)}(\mu)$.

Тогда, для некоторого натурального числа s и некоторого $\mu_1(\xi)$, $\;\mu_1(\xi) \in \{1\} + \{\xi\}\mathfrak{L}_0^{(1)}$, выполнено $\mu_0 = \mu^s\mu_1(\mu)$. Поэтому $\mu_0^{k'}\mathfrak{L}_0^{(1)}(\mu) = \mu^{k's}\mathfrak{L}_0^{(1)}(\mu)$ и из равенства (4.16) получаем

$$A^{(1)}(M) = M' + \mu^{k's}\mathfrak{L}_0^{(1)}(\mu), \tag{4.17}$$

Далее, найдется множество M'' многочленов из $E_2[\mu]$, степень каждого из которых меньше $k's$, такое, что

$$M' \subset M'' + \mu^{ks}\mathfrak{L}_0^{(1)}(\mu).$$

Отсюда и из (4.17) получаем

$$M = M'' + \mu^{k's}\mathfrak{L}_0^{(1)}(\mu).$$

Теорема доказана.

Далее будет получено необходимое и достаточное условие того, что ЛА μ удовлетворяет соотношению (4.13).

Теорема 4.1.2. *Пусть $\mu_0 \in \left(\xi\mathfrak{L}_1^0\right) \setminus \{0\}$. Для ЛА $\mu \in \left(\xi\mathfrak{L}_1^0\right) \setminus \{0\}$ соотношение (4.13) выполнено в точности тогда, когда μ – дробь минимальной степени такая, что выполнены следующие два свойства.*

1. $$\mu_0 \in \mathfrak{L}_1^0(\mu),$$

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

Доказательство. Предположим сначала, что для ЛА μ и μ_0 выполнено равенство (4.13). Так как

$$\mu_0 \in R_2(\mu_0) \cap \mathfrak{L}_1^0,$$

то справедливо первое из указанных в формулировке теоремы свойств. Поэтому найдутся многочлены $u(\xi)$ и $v(\xi)$ из $E_2[\xi]$ такие, что дробь $\frac{u(\xi)}{v(\xi)}$ несократима и

$$\mu_0 = \frac{u(\mu)}{v(\mu)}.$$

Так как

$$\mu_0 \in \xi\mathfrak{L}_1^0$$

и

$$\mu \in \xi \mathfrak{L}_1^0$$

, то

$$u(\mu) \in \{\mu\} E_2[\mu].$$

Если коэффициент при ξ в многочлене $u(\xi)$ равен нулю, то для некоторых чисел a_i, $a_i \in E_2$, $i = 2, 3, \ldots$ ЛА μ_0 равен сумме ряда

$$\sum_{i=2}^{\infty} a_i \mu^i.$$

Отсюда следует: если сумма некоторого ряда $r(\mu_0)$,

$$r(\mu_0) \in R_2(\mu_0), \;\; r(0) = 0,$$

равна μ',

$$\mu' \in \mathfrak{L}_1^0,$$

то μ' является также суммой некоторого ряда $r(\mu)$ из $R_2(\mu)$, причем

$$r(\mu) = \sum_{i=2}^{\infty} b_i \mu^i$$

для некоторых чисел b_i из E_2. В частности,

$$\mu = \sum_{i=2}^{\infty} c_i \mu^i, \;\; c_i \in E_2, \;\; i = 2, 3, \ldots,$$

что противоречим единственности представления ЛА суммой ряда из $R_2(\mu)$. Таким образом,

$$u \in \{\xi\} + \{\xi^2\} E_2[\xi].$$

Если дробь μ',

$$\mu' \in \left(\xi \mathfrak{L}_0^{(1)} \right) \setminus \{0\}$$

такова, что

$$\mu_0 = \frac{u'(\mu')}{v'(\mu')}$$

и

$$u'(\xi) \in \{\xi\} + \{\xi^2\}\mathfrak{L}_0^{(1)},$$

то

$$\mathfrak{L}_0^{(1)}(\mu') \subseteq R_2(\mu_0) \cap \mathfrak{L}_0^{(1)} = \mathfrak{L}_0^{(1)}(\mu),$$

откуда

$$E_2(\mu') \subseteq E_2(\mu)$$

и

$$\deg \mu'(\xi) \geq \deg \mu(\xi).$$

([20]). Таким образом, μ имеет минимальную степень среди всех дробей из

$$\left(\xi\mathfrak{L}_0^{(1)}\right) \setminus \{0\},$$

со свойствами 1, 2. Необходимость доказана.

Теперь докажем достаточность. Пусть для некоторых ЛА μ и μ_0 из множества $\left(\xi\mathfrak{L}_1^0\right) \setminus \{0\}$ выполнены указанные в теореме свойства. Тогда найдутся числа a_i, $a_i \in E_2$, $i = 2, 3, \ldots$ такие, что

$$\mu_0 = \mu + \mu^2 \sum_{i=2}^{\infty} a_i \mu^{i-2}.$$

Тогда найдутся числа b_i, $i = 1, 2, \ldots$ такие, что

$$\mu = \sum_{i=1}^{\infty} b_i (\mu_0)^i.$$

Поэтому

$$\mathfrak{L}_1^0(\mu) \subseteq R_2(\mu_0) \cap \mathfrak{L}_0^{(1)}.$$

С другой стороны, по лемме 4.1.4 для некоторого μ' из множества $\left(\xi\mathfrak{L}_0^{(1)}\right) \setminus \{0\}$ имеет место равенство

$$R_2(\mu_0) \cap \mathfrak{L}_0^{(1)} = \mathfrak{L}_0^{(1)}(\mu'),$$

т.е.

$$\mathfrak{L}_0^{(1)}(\mu) \subseteq \mathfrak{L}_0^{(1)}(\mu'). \tag{4.18}$$

При этом μ' обладает свойствами 1, 2 из условия леммы, а, следовательно, по выбору μ, $\deg\mu \le \deg\mu'$. Отсюда и из 4.18 получаем равенство

$$\mathfrak{L}_0^{(1)}(\mu) = \mathfrak{L}_0^{(1)}(\mu').$$

Теорема доказана.

Доказанная теорема совместно с леммой 4.1.2 позволяют получить конечную процедуру проверки $A^{(1)}$-выразимости через конечные множества ЛА из $\mathfrak{L}_0^{(1)}$.

Теорема 4.1.3. *Существует алгоритм, проверяющий по данным μ' и M, $\mu' \in \mathfrak{L}_1^0$, $M \subset \mathfrak{L}_1^0$, $|M| < \infty$, справедливость соотношения*

$$\mu' \in A^{(1)}(M). \tag{4.19}$$

Доказательство. Если $M \subseteq E_2$, то алгоритм проверки соотношения (4.19) тривиален. В противном случае, найдутся натуральное k и найдется ненулевой ЛА μ_0 из $\xi\mathfrak{L}_0^{(1)}$ такие, что для некоторого множества многочленов M', $M' \subseteq E_2[\mu_0]$, степень каждого из которых не более k, справедливо равенство (4.4). Сначала найдем число k и ЛА μ_0. Это делается построением разложения (4.1), либо (4.2), в зависимости от встретившегося случая (см. главу 3).

Далее проверим включение

$$\mu' \in R_2(\mu_0) \cap \mathfrak{L}_1^0. \tag{4.20}$$

Следуя лемме 4.1.2, справедливость этого включения является необходимым условием $A^{(1)}$-выразимости ЛА μ' через множество M. Для этого перечислим все ненулевые ЛА μ_i, $i = 1, 2, \ldots, s$, из $\xi\mathfrak{L}_1^0$, степени которых не превосходят $\deg\mu_0$, таким образом, что $\deg\mu_i \le \deg\mu_{i+1}$, $i = 1, 2, \ldots, s-1$. Далее, найдем минимальное i_0, $i_0 \in \{1, 2, \ldots, s\}$, такое, что

$$\mu_0 \in \mathfrak{L}_1^0(\mu_{i_0}) \tag{4.21}$$

и, если представить μ_0 в виде несократимой дроби $\frac{u(\mu_{i_0})}{v(\mu_{i_0})}$, где $u(\xi)$ и $v(\xi)$ – элементы $E_2[\xi]$, то $u(\xi) \in \{\xi\} + \{\xi^2\}E_2[\xi]$. Для этого используем следующее соображение: Из включения (4.21) следует существование такой дроби $\tilde{\mu}$, $\tilde{\mu} \in \mathfrak{L}$, что

$$\tilde{\mu}(\mu_{i_0}) = \mu_0, \;\; \deg\left(\tilde{\mu}(\xi)\right) \leq \deg\left(\mu_0(\xi)\right).$$

Как уже говорилось выше, такое число i_0 найдется. Используя опять же приведенное соображение, проверяем включение $\mu' \in \mathfrak{L}_1^0(\mu_{i_0})$. Если это включение не выполнено, то по теореме 4.1.1 и лемме 4.1.2 включение (4.20) не имеет места.

В противном случае, $\mu' \in R_2(\mu_0)$. Тогда для целого неотрицательного числа k_1, $k_1 = k\frac{\deg \mu_0}{\deg \mu_{i_0}}$ выполнены включения

$$\{\mu_{i_0}^{k_1}\}\mathfrak{L}_0^{(1)}(\mu_{i_0}) \subseteq A^{(1)}(M) \subseteq \mathfrak{L}_0^{(1)}(\mu_{i_0}).$$

Для сокращения дальнейших построений нам понадобится одно вспомогательное понятие. Пусть $\mu \in \mathfrak{L}_1^0(\mu_{i_0})$. Тогда найдется многочлен $u_0(\xi)$ степени меньшей k_1, что $\mu + u_0(\mu_0) \in \left\{\mu_{i_0}^{k_1}\right\}\mathfrak{L}_1^0(\mu_{i_0})$. Многочлен $u_0(\xi)$ называется проекцией дроби μ на множество многочленов степени меньшей k_1. Таким образом,

$$A^{(1)}(M) = M' + \left\{\mu_{i_0}^{k_1}\right\}\mathfrak{L}_1^0(\mu_{i_0}),$$

где M' представляет собой множество проекций всех дробей из $A^1(M)$ на множество многочленов степени меньшей k_1. Множество M' содержится в множестве многочленов степени меньшей k_1, а поэтому может быть построено за конечное число шагов из элементов множества M. Теперь остается только спроектировать μ' на множество многочленов степени меньшей k_1 и проверить, принадлежит ли проекция p множеству M'. Соотношение $\mu' \in A^{(1)}(M)$ имеет место в точности тогда, когда $p \in M'$.

Теорема 4.1.3 доказана.

Приведем пример, поясняющий результаты этого параграфа.

Рассмотрим ЛА μ_i, $\quad i = 1, 2$,

$$\mu_1 = \xi^2 + \xi^3 + \xi^6 + \xi^7 + \xi^9 + \xi^{14} + \xi^{16} + \xi^{18},$$

$$\mu_2 = \xi^4 + \xi^7 + \xi^8 + \xi^9 + \xi^{16} + \xi^{18} + \xi^{19} + \xi^{24} + \xi^{26} + \xi^{27}$$

и проверим, содержится ли ЛА μ', $\mu' = \frac{1}{1+\xi^2+\xi^3}$ в множестве $A^{(1)}(\{\mu_1, \mu_2\})$.

Для этого обозначим ЛА $\xi^2+\xi^3+\xi^4+\xi^7+\xi^8+\xi^9$ через μ_0. Путем подстановки упомянутого многочлена от ξ вместо ЛА μ_0 нетрудно проверить справедливость равенств

$$\mu_1 = \mu_0 + \mu_0^2,$$

$$\mu_2 = \mu_0^2 + \mu_0^3.$$

Отсюда и из формального равенства $\mu_0 = \frac{\mu_2}{\mu_1}$, выполненного в поле $E_2(\xi)$, заключаем, что

$$E_2(\mu_1, \mu_2) = E_2(\mu_0).$$

Поэтому и по лемме 4.1.2 найдется целое неотрицательное число k такое, что выполнены включения

$$\{\mu_0^k\}\left(R_2(\mu_0) \cap \mathfrak{L}_1^0\right) \subseteq A^1(\{\mu_1, \mu_2\}) \subseteq R_2(\mu_0) \cap \mathfrak{L}_1^0. \tag{4.22}$$

Следуя разобранному выше примеру, можно получить соотношение

$$\mu_0 \in A^{(1)}(\{\mu_1, \mu_2\}).$$

Отсюда и из (4.22) получаем

$$A^{(1)}(\{\mu_1, \mu_2\}) = A^1(\{\mu_0\}).$$

Далее через μ обозначим ЛА $\xi^2 + \xi^3$. Нетрудно проверить равенство

$$\mu_0 = \mu + \mu^2 + \mu^3,$$

и, используя теорему 2, заключить:

$$A^1(\{\mu_0\}) = \mathfrak{L}_1^0(\mu).$$

Таким образом, вопрос о вхождении ЛА μ' в множество $A^1(\{\mu_1, \mu_2\})$, равносилен справедливости включения

$$\mu' \in \mathfrak{L}_1^0(\mu),$$

которое следует из равенства [68], т.к.

$$\mu' = \frac{1}{1+\mu}.$$

Результатом приведенных рассуждений стало доказательство включения

$$\mu' \in A^{(1)}\left(\{\mu_1, \mu_2\}\right).$$

Дале заметим, что для любого μ, $\mu \in \xi\mathfrak{L}_0^{(1)}$, справедливо $\mathfrak{L}_0^{(1)}(\mu) \subseteq A^{(1)}\left(\{\mu\}\right)$. ЛА μ, $\mu \in \{\xi\}\mathfrak{L}_0^{(1)}$, будем называть A-минимальным, если

$$\mathfrak{L}_0^{(1)}(\mu) = A^{(1)}\left(\{\mu\}\right).$$

По теореме 4.1.1 для любого M, $M \subseteq \mathfrak{L}_1^0$, найдется A-минимальный ЛА μ_0, найдется целое неотрицательное число k и найдется множество M' многочленов, степень каждого из которых не превосходит k такие, что

$$A^{(1)}\left(M\right) = M' + \{\mu_0^k\}\mathfrak{L}_1^0(\mu_0), \tag{4.23}$$

ЛА μ_0, удовлетворяющий этому равенству, будем называть A-основанием множества M. Минимальное число k, для которого найдется M',

$$M' \subset \left\{ \sum_{i=0}^{k-1} a_i\xi^i \mid a_i \in E_2, \;\; i = 0, 1, \ldots, k-1 \right\},$$

удовлетворяющее равенству (4.23), называется глубиной множества M по A-основанию μ_0, а само множество M' называется k-приближением для M.

Заметим, что A-основание множества ЛА M вообще говоря не единственно. Так для множества $\mathfrak{L}_0^1$ A-основанием является как задержка ξ, так и ЛА μ', $\mu' = \frac{\xi}{1+\xi}$. Действительно, нетрудно убедиться, что

$$\xi x_1 = \mathrm{fb}_{x_2}\left(\mu' x_1 + \mu' x_2\right).$$

Поэтому $\mathfrak{L}_1^0 = \mathfrak{L}_1^0(\mu')$ и $A^{(1)}(\{\xi\}) = \mathfrak{L}_1^0 = \mathfrak{L}_1^0(\mu') = A^{(1)}(\mu')$. Последнее соотношение доказывает, что ЛА ξ и μ' являются A-основаниями множества $\mathfrak{L}_1^0$ всех одноместных ЛА, сохраняющих нулевую последовательность.

Множество всех A-оснований множества M обозначается $B(M)$. Если $\mu_0 \in B(M)$, то глубину множества M по A-основанию μ_0 обозначим $G(M, \mu_0)$, а $G(M, \mu_0)$-приближение для M обозначим $P(M, \mu_0)$, т.к. оно однозначно определяется по паре M и μ_0.

Нетрудно видеть, что множество $\{\mu_0^k\}\mathfrak{L}_1^0(\mu_0)$ $A^{(1)}$-порождается системой

$$\left\{\ \mu_0^k,\ \ \mu_0^{k+1}, \ldots, \mu_0^{2k-1}\ \right\},$$

т.е. имеет место равенство

$$A^{(1)}\left\{\mu_0^k, \mu_0^{k+1}, \ldots, \mu_0^{2k-1}\right\} = \{\mu_0^k\}\mathfrak{L}_1^0(\mu_0).$$

Отсюда и из равенства (4.23) вытекает следующая теорема.

Теорема 4.1.4. *Любое $A^{(1)}$-замкнутое множество M, $M \subseteq \mathfrak{L}_1^0$ является конечнопорожденным. Поэтому число $A^{(1)}$-замкнутых множеств в $\mathfrak{L}_1^0$ счетно.*

4.2. Аппроксимационная выразимость через множества линейных автоматов с существенным автоматом, замыкания которых содержат все константы

В настоящем параграфе мы рассмотрим проблему A-выразимости (аппроксимационной выразимости) в классе $\mathfrak{L}$ всех ЛА через множества, на которые накладываются некоторые ограничения.

Как и в главе 1, ЛА, все переменные которой фиктивны, назовем константным, а множество, состоящее из всех константных ЛА, обозначаем $\mathfrak{L}_c$, как и в главе 3.

Сумматор от n переменных, как и прежде, обозначаем через $x_1 + x_2 + \cdots + x_n$.

В главе 1 показано, что для любого ЛА $f(x_1, x_2, \ldots, x_n)$ найдутся одноместные ЛА $\mu_i(x)$, $\mu_i \in \mathfrak{L}_1^0$ и найдется константа $\mu_0, \mu_0 \in \mathfrak{L}_c$ такие, что

$$f(x_1, x_2, \ldots, x_n) = \mu_1 x_1 + \mu_2 x_2 + \cdots + \mu_n x_n + \mu_0. \tag{4.24}$$

В главе 3 было введено множество $\mathfrak{L}^0$ всех ЛА, сохраняющих 0. Нетрудно видеть, что множество $\mathfrak{L}^0$ является K-замкнутым, а также A-замкнутым классом в $\mathfrak{L}$, т.е.

$$\mathfrak{L}^0 = K(\mathfrak{L}^0),$$

$$\mathfrak{L}^0 = A(\mathfrak{L}^0).$$

K-базисом, а также A-базисом в $\mathfrak{L}$ является, например, множество

$$\{\ \xi x + 1,\ \ x_1 + x_2\ \},$$

состоящее из задержки с начальным состоянием 1 и сумматора с двумя входами. K-базис и A-базис в $\mathfrak{L}^0$ составляет, например, задержка ξ с начальным состоянием 0 и тот же сумматор. Таким образом,

$$\mathfrak{L} = K\left(\{\xi x + 1, x_1 + x_2\}\right) = A\left(\{\xi x + 1, x_1 + x_2\}\right),$$

$$\mathfrak{L}^0 = K\left(\{\xi x, x_1 + x_2\}\right) = A\left(\{\xi x, x_1 + x_2\}\right).$$

Напомним, что переменная x_i ЛА $f(x_1, x_2, \ldots, x_n)$, удовлетворяющего соотношению (4.24), называется непосредственной, если $\mu_i \in 1+\xi\mathfrak{L}_1^0$. ЛА $f(x_1, x_2, \ldots, x_n)$ называется существенным, если среди его переменных есть не менее двух непосредственных. В главе 1 был рассмотрен K-замкнутый и A-замкнутый класс V_1, состоящий из всех ЛА, не являющихся существенными. Там же показано, что V_1 – A-предполный класс в $\mathfrak{L}$.

В настоящем параграфе мы будем рассматривать задачу об A-выразимости через подмножества $\mathfrak{L}$, не содержащиеся в V_1, (т.е. через множества ЛА, содержащие существенный автомат), и A-замыкания которых содержат $\mathfrak{L}_c$.

Множество M, $M \subseteq \mathfrak{L}$, называется S-системой, если

$$M \setminus V_1 \neq \emptyset \text{ и } \mathfrak{L}_c \subset A(M).$$

Лемма 4.2.1. *Для множества M, $M \subseteq \mathfrak{L}$, соотношение*

$$M \setminus V_1 \neq \emptyset. \tag{4.25}$$

выполнено тогда и только тогда, когда

$$x_1 + x_2 + x_3 \in A(M). \tag{4.26}$$

Доказательство. Пусть выполнено включение (4.26). Т.к. $x_1 + x_2 + x_3 \notin V_1$, то, ввиду A-замкнутости V_1, справедливо (4.25). Достаточность условия (4.26) для (4.25) доказана. Далее докажем его необходимость.

Пусть имеет место (4.25). Тогда найдется $f(x_1, x_2, \dots, x_n)$, $f(x_1, x_2, \dots, x_n) \in M \setminus V_1$. Не ограничивая общность рассуждений, будем считать, что переменные x_1 и x_2 ЛА f являются непосредственными. Пусть (4.24) – разложение f в сумму одноместных ЛА. Обозначим ЛА $f(x_1, x, x, \dots, x)$ и $f(x, x_2, x, x, \dots, x)$ через $f_1(x_1, x)$ и $f_2(x_2, x)$ соответственно. Тогда для ЛА $g_i(x_i, x)$,

$$g_i(x_i, x) = \underbrace{f_i(f_i(\dots f_i(}_{2^k-1 \text{ символов } f_i} x_i, x), \dots, x), x), \;\; i = 1, 2,$$

найдутся ЛА $\eta_i(x)$, $\eta_i(x) \in \mathfrak{L}_1^0(x)$, $i = 1, 2$, и найдутся константные автоматы $\mu^{(i)}$, $i = 1, 2$, что

$$g_i(x_i, x) = \mu_i^{2^k-1} x_i + \eta_i x + \mu^{(i)}, \;\; i = 1, 2.$$

Тогда для некоторого $g(x)$, $g(x) \in \mathfrak{L}_1^0(x)$, и некоторого γ, $\gamma \in \mathfrak{L}_c$, ЛА $h(x_1, x_2, x)$,

$$h(x_1, x_2, x) = f\left(g_1(x_1, x), g_2(x_2, x), x, x, \dots\right),$$

совпадает с

$$\mu_1^{2^k}(x_1) + \mu_2^{2^k}(x_2) + g(x) + \gamma.$$

Как нетрудно видеть,

$$\mu_i^{2^k}(x) \in \{1\} + \left\{\xi^{2^k}\right\} \mathfrak{L}_1^0.$$

Поэтому ЛА $h(x_1, x_2, x)$ и $x_1 + x_2 + G(x) + \gamma$ являются 2^k-эквивалентными. Отсюда вытекает, что 2^k-эквивалентны ЛА $h(x_1, h(x_2, x_3, x_3), x_3)$ и $x_1 + x_2 + x_3$. Таким образом, соотношение (4.26), а вместе с ним и лемма 4.2.1 доказаны.

Рассматривая множество M, $M \subseteq \mathfrak{L}$, в дальнейшем $U(M)$ будем называть U-основаним M, а $C(M)$ – его C-основанием.

Множество всех ЛА из $\mathfrak{L}$, имеющих нечетное число непосредственных входов, как и раньше, обозначаем V_2. Заметим, что любая S-система не содержится в V_2, т.к. V_2 является A-замкнутым классом, а никакая константа в нем не содержится.

Поэтому, если S-система M такова, что $U(M) \subseteq E_2$ (такие S-системы будем называть вырожденными), то, как нетрудно видеть, выполнено:

$$A(M) = \{\ \gamma,\ \ x_1 + x_2 + \cdots + x_n + \gamma\ \mid\ n = 1, 2, \ldots,\ \ \gamma \in \mathfrak{L}_c\ \}\,.$$

Поэтому в дальнейшем будем предполагать, что

$$U(M) \setminus E_2 \neq \emptyset, \tag{4.27}$$

т.е. будем рассматривать невырожденные S-системы.

Теперь исследуем, какими могут быть U-основания и C-основания A-замкнутых невырожденных S-систем.

Имеет место следующая лемма.

Лемма 4.2.2. *Если множество M, $M \subseteq \mathfrak{L}$, не содержится в V_1, то*

$$U(A(M)) = A^{(1)}(U(M)). \tag{4.28}$$

Доказательство. Пусть $M \subseteq \mathfrak{L}$ и $M \not\subseteq V_1$. Сначала докажем включение

$$U(A(M)) \subseteq A^{(1)}(U(M)). \tag{4.29}$$

Пусть $f \in A(M)$. Тогда для каждого натурального числа τ, $\tau \in \mathbb{N}$, из ЛА множества M с использованием операций суперпозиции можно построить ЛА f_τ, который τ-эквивалентен ЛА f. Отсюда, для любого μ, $\mu \in U(f)$, и любого натурального τ найдется ЛА μ_τ, $\mu_\tau \in U(f_\tau)$, τ-эквивалентен μ, причем $\mu_\tau \in S^{(1)}(U(M))$. Поэтому $\mu \in A^{(1)}(U(M))$ и включение (4.29) доказано.

Теперь докажем, что

$$A^{(1)}(U(M)) \subseteq U(A(M)). \tag{4.30}$$

Пусть $\mu \in A^1(U(M))$. Тогда для любого натурального τ в $S^{(1)}(U(M))$ найдется ЛА μ_τ, который является τ-эквивалентной μ. Через $S(M)$, как и ранее, мы обозначаем множество всех ЛА, получаемых с использованием операций суперпозиции из элементов множества M. Нетрудно видеть, что, если μ' и μ'' содержатся в $U(S(M))$, то $\mu'\mu''$ содержится в $U(S(M))$. Кроме того, учитывая лемму 4.2.1, если $\mu' \in U\left(f'\left(x_1, x_2, \ldots, x_n\right)\right)$ и $\mu'' \in U(f''\left(x_{n+1}, x_{n+2}, \ldots, x_{n+k}\right))$, то, не ограничивая общности рассуждений, можно считать, что найдутся ЛА $g'\left(x_2, x_3 \ldots, x_n\right)$ и $g''\left(x_{n+2}, x_{n+3}, \ldots, x_{n+k}\right)$ такие, что

$$f'\left(x_1, x_2, \ldots, x_n\right) = \mu'(x_1) + g'\left(x_2, x_2, \ldots, x_n\right),$$

$$f''\left(x_{n+1}, x_{n+2}, \ldots, x_{n+k}\right) = \mu''(x_{n+1}) + g'\left(x_{n+2}, x_{n+3}, \ldots, x_{n+k}\right).$$

Тогда для некоторого ν, $\nu \in \mathfrak{L}_1$, имеет место равенство

$$f'\left(x', x, x, \ldots, x\right) + f''\left(x', x, x, \ldots, x\right) + x = \left(\mu' + \mu''\right) x' + \nu(x),$$

т.е. $\mu' + \mu'' \in U(S^{(1)}(M))$. Следовательно,

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

Теперь вернемся к рассмотренным выше ЛА μ_τ. Выше доказано, что для любого натурального τ выполнено $\mu_\tau \in U(S(M))$. Поэтому для каждого натурального τ найдется ЛА $f_\tau\left(x_{1,\tau}, x_{2,\tau}, \ldots, x_{n_\tau,\tau}\right)$ такой, что для некоторого $g_\tau\left(x_{2,\tau}, x_{3,\tau}, \ldots, x_{n_\tau,\tau}\right)$ выполнено равенство:

$$f_\tau\left(x_{1,\tau}, x_{2,\tau}, \ldots, x_{n_\tau,\tau}\right) = \mu_\tau\left(x_{1,\tau}\right) + g_\tau\left(x_{2,\tau}, x_{3,\tau}, \ldots, x_{n_\tau,\tau}\right).$$

Теперь рассмотрим ЛА $g_\tau\left(x_1, x_2, x\right)$,

$$g_\tau\left(x_1, x_2, x\right) = f_\tau\left(x_1, x, x, \ldots x\right) + f_\tau\left(x_2, x, x, \ldots x\right) + x.$$

Нетрудно видеть, что

$$g_\tau(x_1, x_2, x) = \mu_\tau(x_1) + \mu_\tau(x_2) + x.$$

Поэтому

$$\mu(x_1) + \mu(x_2) + x \in A(M),$$

Откуда, $\mu \in U(A(M))$. Включение (4.30), а вместе с ним и лемма доказаны.

Лемма 4.2.3. *Пусть M является S-системой. Тогда имеет место включение*

$$A^1(U(M)) \subseteq A(M). \tag{4.31}$$

Доказательство. Пусть $\mu \in A^{(1)}(U(M))$. Тогда по лемме 4.2.2 выполнено: $\mu \in U(A(M))$, т.е. найдется натуральное число n и найдется ЛА $g(x_1, \ldots, x_n)$ такой, что $\mu \in U(g)$. По условию леммы, $0 \in A(M)$ и $x_1 + x_2 + x_3 \in A(M)$. Обозначим константу $g(0, \ldots, 0)$ через γ. Имеем

$$\gamma \in A(M),$$

и для некоторого i, $i \in \{1, 2, \ldots n\}$, выполнено:

$$g\left(_{i-1}\underbrace{0, \ldots, 0}_{\text{символов}}\ _0, x, 0, \ldots, 0\right) = \mu x + \gamma \in A(M).$$

Отсюда,

$$(\mu x + \gamma) + \gamma + 0 = \mu x \in A(M).$$

Поэтому доказано включение (4.31).

Лемма доказана.

Теорема 4.2.1. *Пусть M является S-системой. Тогда включение $f \in A(M)$ выполнено в точности тогда, когда*

$$U(f) \subseteq A^{(1)}(U(M)). \tag{4.32}$$

Доказательство. Необходимость утверждения теоремы вытекает из леммы 4.2.2. Докажем достаточность. Пусть M является S-системой, $f \in \mathfrak{L}$, и выполнено (4.32).

По определению S-системы, $0 \in A(M)$, а по лемме 4.2.1, $x_1 + x_2 + x_3 \in A(M)$.

Используя ЛА $x_1 + x_2 + x_3$, 0 и операцию подстановки, можно получить сумматор с $n+1$ входом $x_1+x_2+\cdots+x_{n+1}$. Из определения S-системы следует $\mu_0 \in A(M)$, а с учетом леммы 4.2.3, $\mu_i x_i \in A(M)$, $i = 1, 2, \ldots, n$. Поэтому,

$$\mu_1 x_1 + \mu_2 x_2 + \cdots + \mu_n x_n + \mu_0 \in A(M),$$

т.е. $f \in A(M)$. Достаточность утверждения теоремы, а с ним и сама теорема, доказаны.

Из теоремы 4.2.1 вытекает следующая теорема.

Теорема 4.2.2. *Задача A-выразимости через конечные S-системы алгоритмически разрешима.*

4.3. Аппроксимационная выразимость всех констант через множества линейных автоматов, содержащие существенный автомат

В настоящем параграфе получен алгоритм проверяющий, является ли данное конечное множество M, $M \subset \mathfrak{L}$, S-системой. Учитывая теорему 4.1.2 из предыдущего параграфа, A-выразимость через заданное конечное множество ЛА может быть проверена в два этапа. На первом этапе проверяем, является ли исследуемое множество S-системой, и, в случае положительного решения, определяем A-выразимость данного ЛА через эту систему. К сожалению, если после первого этапа на вопрос, является ли M S-системой, будет получен отрицательный ответ, то вопрос об A-выразимости через такую систему может остаться открытым.

Пусть $r \in \mathbb{N}$, $f(x_1, x_2, \dots, x_n) \in \mathfrak{L}$ и для $f(x_1, x_2, \dots, x_n)$ имеет место разложение (4.24). ЛА $f(x_1, x_2, \dots, x_n)$ обладает r-свойством в точности если для любого i, $i = 1, 2, \dots, n$, выполнено соотношение $\mu_i(\xi) + \mu_i(0) \in \{\xi^r\} \cdot \mathfrak{L}_0^{(1)}$. Таким образом, ЛА $f(x_1, x_2, \dots, x_n)$ обладает r-свойством тогда и только тогда, когда найдутся натуральные числа $i_1, i_2, \dots, i_k$, $1 \le i_1 < i_2 < \dots < i_k \le n$, и найдется константа γ, $\gamma \in \mathfrak{L}_c$, такие, что $f(x_1, x_2, \dots, x_n)$ и $x_{i_1} + x_{i_2} + \dots + x_{i_n}$ являются r-эквивалентными.

Множество всех ЛА, обладающих r-свойством, обозначим S_r. Нетрудно видеть, что для любого множества ЛА M, $U(M) \setminus E_2 \neq \emptyset$, найдется натуральное число r_0 такое, что $M \subseteq S_{r_0}$, но $M \not\subseteq S_{r_0+1}$. Такое число r_0 называется 1-глубиной множества M.

Пусть $r \in \mathbb{N}$. В главе 3 было определено отображение $V^{(r)}$. Распространим это отображение на S_r. Пусть для ЛА f, $f \in S_r$ имеет место разложение (4.24). Для некоторых чисел a_t, $a_t \in E_2$, $t = 0, 1, \dots, r-1$, и некоторой константы μ_0', $\mu_0' \in \mathfrak{L}_c$, справедливо равенство

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

Положим

$$V^{(r)}(f) = (b, a_0, a_1, \dots, a_{r-1}),$$

где, как и ранее,

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

Если $M \subseteq S_r$, то, как принято, через $V^{(r)}(M)$ обозначается множество $\{\ V^{(r)}(f) \mid f \in M\ \}$. Множество векторов E_2^{r+1} будем рассматривать вместе с операцией "$+$"покомпонентного сложения по модулю 2. Если $M \subseteq E_2^{r+1}$, то замыкание множества M по операции сложения обозначим $S(M)$.

Лемма 4.3.1. *Пусть $M \subseteq S_r$ и M содержит существенный автомат. Тогда*

$$V^{(r)}(A(M)) = S(V^{(r)}(M)).$$

Доказательство. Сначала докажем включение

$$S(V^{(r)}(M)) \subseteq V^{(r)}(A(M)). \tag{4.33}$$

Ввиду справедливости соотношения

$$V^{(r)}(M) \subseteq V^{(r)}(A(M)),$$

достаточно показать, что из

$$\bar{a} \in V^{(r)}(A(M)) \quad \text{и} \quad \bar{b} \in V^{(r)}(A(M)) \tag{4.34}$$

вытекает

$$\bar{a} + \bar{b} \in V^{(r)}(A(M)). \tag{4.35}$$

Действительно, пусть включения (4.34) имеют место. Тогда в $A(M)$ найдутся ЛА f и g, $f = f(x_1, x_2, \ldots, x_n)$, $g = g(x_{n+1}, x_{n+2}, \ldots, x_{n+k})$ такие, что $\bar{a} = V^{(r)}(f)$ и $\bar{b} = V^{(r)}(g)$. По лемме 4.2.1 из предыдущего параграфа имеем $x_1 + x_2 + x_3 \in A(M)$. Поэтому ЛА $h(x, x_1, x_2, \ldots, x_{n+k})$,

$$h(x, x_1, x_2, \ldots, x_{n+k}) = x + f(x_1, x_2, \ldots, x_n) + g(x_{n+1}, x_{n+2}, \ldots, x_{n+k})),$$

содержится в $A(M)$.

Нетрудно видеть, что $V^{(r)}(h) = \bar{a} + \bar{b}$. Поэтому включение (4.35), а, вместе с ним, включение (4.33) доказано.

Теперь докажем соотношение

$$V^{(r)}(A(M)) \subseteq S(V^{(r)}(M)). \tag{4.36}$$

Если $M \subseteq \mathfrak{L}$, то, как и прежде, через $S(M)$ мы обозначаем замыкание множества M по операциям суперпозиции. Из определения A-замыкания следует, что

$$S(M) \subseteq A(M). \tag{4.37}$$

С другой стороны, для любого ЛА f, $f \in A(M)$, найдется ЛА f_r, $f_r \in S(M)$, такой, что f и f_r являются r-эквивалентными. Поэтому $f_r \in S_r$ и $V^{(r)}(f) = V^{(r)}(f_r)$. Отсюда и из (4.37) получаем $V^{(r)}(S(M)) = V^{(r)}(A(M))$. Таким образом, соотношение (4.36) будет доказано, если установить справедливость соотношения

$$V^{(r)}(S(M)) \subseteq S(V^{(r)}(M)). \tag{4.38}$$

Пусть $f(x_1, x_2, \ldots, x_n) \in S(M)$ и $g(x_{n+1}, x_{n+2}, \ldots, x_{n+k}) \in S(M)$.

Если ЛА h получен из f с использованием операции переименования переменных или отождествления переменных, то $V^{(r)}(h) = V^{(r)}(f)$. Если h получена подстановкой f вместо непосредственной переменной ЛА g, то $V^{(r)}(h) = V^{(r)}(f) + V^{(r)}(g)$. Если h получен подстановкой f вместо переменной ЛА g, не являющейся непосредственной, то $V^{(r)}(h) = V^{(r)}(g)$. Следовательно, если $V^{(r)}(f) \in S(V^{(r)}(M))$ и $V^{(r)}(g) \in S(V^{(r)}(M))$, то $V^{(r)}(h) \in S(V^{(r)}(M))$. Включение (4.38) получаем теперь ввиду $V^{(r)}(M) \subseteq S(V^{(r)}(M))$.

Лемма доказана.

Следующая теорема сводит вопрос об A-выразимости всех констант через некоторое множество ЛА (с ограничениями) к проверке полноты некоторой системы векторов в конечномерном векторном пространстве.

Теорема 4.3.1. *Пусть $M \subseteq \mathfrak{L}$, M содержит существенный ЛА и $U(M) \nsubseteq E_2$. Множество $A(M)$ содержит все константы (т.е. $\mathfrak{L}_c \subseteq A(M)$) в точности тогда, когда $S(V^{(r_0)}(M)) = E_2^{r_0+1}$, где через r_0 обозначена 1-глубина множества M.*

Доказательство. Необходимость. Пусть $M \subseteq \mathfrak{L}$, M содержит существенный ЛА, $U(M) \nsubseteq E_2$, $\mathfrak{L}_c \subseteq A(M)$ и M имеет 1-глубину r_0.

Учитывая лемму, требуется доказать равенство

$$V^{(r_0)}(A(M)) = E_2^{r_0+1}. \tag{4.39}$$

Для любых чисел a_0, a_1, $\ldots$, a_{r_0-1}, $a_t \in E_2$, $t = 0, 1, \ldots, r_0 - 1$, найдутся константы γ и γ', $\gamma \in \mathfrak{L}_c$, $\gamma' \in \mathfrak{L}_c$, такие, что

$$\gamma = a_0 + a_1\xi + \cdots + a_{r_0-1}\xi^{r_0-1} + \xi^{r_0}\gamma'.$$

Справедливы соотношения:

$$\gamma \in A(M),$$

$$V^{(r_0)}(\gamma) = (1, a_0, a_1, \ldots, a_{r_0-1}).$$

По лемме 4.2.1 выполнено (4.26). Тогда получаем:

$$x + 0 + \gamma \in A(M),$$

$$V^{(r_0)}(x + 0 + \gamma) = (0, a_0, a_1, \ldots, a_{r_0-1}).$$

Отсюда,

$$(1, a_0, a_1, \ldots, a_{r_0-1}) \in V^{(r_0)}(A(M)),$$

$$(0, a_0, a_1, \ldots, a_{r_0-1}) \in \ V^{(r_0)}(A(M)).$$

Равенство (4.39) и необходимость теоремы доказаны.

Достаточность. Пусть $M \subseteq \mathfrak{L}$, M содержит существенный ЛА, $U(M) \not\subseteq E_2$, M имеет 1-глубину r_0 и

$$S(V^{(r_0)}(M)) = E_2^{r_0+1}. \tag{4.40}$$

Из равенства (4.40) и леммы 4.36 следует, что $M \not\subseteq V_2$. Пусть $g \in M \setminus V_2$. Отождествляя все переменные ЛА g и применяя операцию обратной связи к единственной переменной ЛА $g(x, \ldots, x)$, получаем некоторую константу. Эту константу обозначим γ'.

Далее выберем в $\mathfrak{L}_c$ произвольную константу γ, $\gamma = \sum_{t=0}^{\infty} b_t\xi^t$, и покажем, что $\gamma \in A(M)$.

Заметим, прежде всего, что для любых чисел a_0, a_1, $\ldots$, a_{r_0-1}, $a_t \in E_2$, $t = 0, 1, \ldots, r_0 - 1$ из (4.40) вытекает существование в $A(M)$ ЛА $g_{0,a_0,a_1,\ldots,a_{r_0-1}}(x)$

и $g_{1,a_0,a_1,\ldots,a_{r_0-1}}(x)$, r_0-эквивалентных соответственно $x+\gamma''$ и γ'', где через γ'' обозначена константа $\sum_{t=0}^{\infty} a_t\xi^t$.

Из определения 1-глубины следует, что найдется ЛА f, $f \in M$, такой, что для некоторого μ', $\mu' \in 1+\xi\cdot\mathfrak{L}_0^{(1)}$, и некоторого b, $b \in E_2$, справедливо: $b+\xi^{r_0}\cdot\mu' \in U(f)$. Не ограничивая общность рассуждений, предположим, что $f = f(x_1, x_2, \ldots, x_n)$, для f выполнено разложение (4.24) и $\mu_1 = b+\xi^{r_0}\cdot\mu'$. Через $f'(x)$ обозначим ЛА $f(x, \gamma', \gamma', \ldots, \gamma')$.

Для некоторой константы γ_1, $\gamma_1 \in \mathfrak{L}_c$, $\gamma_1 = \sum_{t=0}^{\infty} c_t\xi^t$ имеем $f'(x) = (b+\xi^{r_0}\cdot\mu')\cdot x+\gamma_1$.

Построим далее последовательность одноместных ЛА $f_1(x), f_2(x), \ldots$ такую, что $f_j(x)$ и γ являются $j\cdot r_0$-эквивалентными.

По лемме 4.2.1 из предыдущего параграфа выполнено: $x_1+x_2+x_3 \in A(M)$. Положим

$$h_{a_0a_1\ldots a_{r_0-1}}(x) \quad = \quad \begin{cases} f'(x)+x+g_{1a_0a_1\ldots a_{r_0-1}}(\gamma'), & \text{если } b=1, \\ f'(x)+\gamma'+g_{0a_0a_1\ldots a_{r_0-1}}(\gamma'), & \text{если } b=0. \end{cases}$$

Нетрудно видеть, что для некоторой константы γ_2, $\gamma_2 \in \mathfrak{L}_c$, выполнено

$$h_{c_0+b_0,c_1+b_1,\ldots,c_{r_0-1}+b_{r_0-1}}(x) = \xi^{r_0}\cdot\mu'(x)+\sum_{t=0}^{r_0-1} b_t\xi^t+\xi^{r_0}\gamma_2. \tag{4.41}$$

Положим

$$f_1(x) = h_{c_0+b_0,c_1+b_1,\ldots,c_{r_0-1}+b_{r_0-1}}(x).$$

ЛА $f_1(x)$ r_0-эквивалентна константе γ.

Пусть уже построен ЛА

$$f_j(x) = \xi^{r_0\cdot j}\mu^{(j)}\cdot x+\sum_{t=0}^{r_0j-1} b_t\xi^t+\xi^{r_0j}\gamma_{j+1},$$

причем $\mu^{(j)}(x) \in 1+\xi\cdot\mathfrak{L}_0^{(1)}$, $\gamma_{j+1} = \sum_{t=0}^{\infty} c_{j+1,t}\xi^t\ldots$.

Найдется последовательность $d_0, d_1, \ldots, d_{r_0-1}$, $d_t \in E_2$,

$t=0,1,\dots,r_0-1$, такая, что для некоторого $\tilde{\mu}^{(j)}$, $\tilde{\mu}^{(j)}\in\mathfrak{L}_1^0$, выполнено:

$$\mu^{(j)}\cdot\left(d_0+d_1\xi+\dots+d_{r_0-1}\xi^{r_0-1}\right)=$$
$$c_{j+1,0}+c_{r_0\cdot j}+\left(c_{j+1,1}+c_{r_0\cdot j+1}\right)\xi+\dots$$
$$+\left(c_{j+1,r_0-1}+c_{r_0\cdot(j+1)-1}\right)\xi^{r_0-1}+\xi^{r_0}\cdot\tilde{\mu}^{(j)}.$$

Положим

$$f_{j+1}(x)=f_j\left(h_{d_0,d_1\dots d_{r_0-1}}(x)\right).$$

Тогда для некоторых $\mu^{(j+1)}\cdot x$ и γ_{j+2},

$$\mu^{(j+1)}\in 1+\xi\cdot\mathfrak{L}_0^{(1)},\ \ \gamma_{j+2}\in\mathfrak{L}_c,$$

выполнено:

$$f_{j+1}(x)=\xi^{r_0(j+1)}\cdot\mu^{(j+1)}\cdot x+\sum_{t=0}^{(j+1)r_0-1}c_t\xi^t+\xi^{(j+1)r_0}\gamma_{j+2}.$$

Построенная последовательность ЛА $\{f_j(x)\}$ обладает требуемым свойством: $f_j(x)$ и γ являются $j\cdot r_0$- эквивалентными, следовательно, $\gamma\in A(M)$.

Достаточность утверждения теоремы и сама теорема доказаны.

Ниже приведен пример конечной S-системы.

Пусть

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

Множество M содержит существенный ЛА $x_1+\xi^6x_2+\left(1+\xi^3\right)x_3+1+\xi^2$ и его 1-глубина равна 3. Имеют место следующие равенства.

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

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

$$V^{(3)}\left(x_1+1+\xi+\xi^2\right)=(0,1,1,1),$$

$$V^{(3)}\left(1+\xi+\xi^2\right)=(1,1,1,1).$$

Нетрудно видеть, что множество векторов
$\{(1,1,0,1),(1,0,1,1),(0,1,1,1),(1,1,1,1)\}$ порождает линейное пространство E_2^4 по операции сложения. Следовательно, по теореме 4.3.1, $\mathfrak{L}_c \subseteq A(M)$ и M является S-системой,

Из теоремы 4.3.1 вытекает следующий результат.

Теорема 4.3.2. *Задача проверки, является ли конечное множество ЛА S-системой, алгоритмически разрешима.*

4.4. Достаточные условия аппроксимационной выразимости

В настоящем параграфе приведены некоторые "естественные"условия на множество ЛА, обеспечивающие возможность проверки A-выразимости заданных ЛА через его элементы.

Будем рассматривать множества ЛА, содержащие существенный ЛА и A-замыкания которых содержат константу 0. Такие множества ЛА будем называть S_0-системами.

Лемма 4.4.1. *Множество M, $M \subseteq \mathfrak{L}$, является S_0-системой в точности тогда, когда $x_1 + x_2 \in A(M)$.*

Доказательство. Пусть M, $M \subseteq \mathfrak{L}$, является S_0-системой. Тогда по лемме 4.2.1, $x_1+x_2+x_3 \in A(M)$. По определению S_0-системы, $0 \in A(M)$. Поэтому, $x_1+x_2 = x_1 + x_2 + 0 \in A(M)$ и достаточность утверждения леммы доказана.

Необходимость. Пусть $x_1 + x_2 \in A(M)$. Тогда $M \not\subseteq V_1$ и M содержит существенный ЛА. Кроме того, $0 = x + x \in A(M)$. Следовательно, множество M является S_0-системой.

Лемма доказана.

Сначала рассмотрим вопрос об A-выразимости через конечные вырожденные S_0-системы, т.е. S_0-системы M, для которых выполнены соотношения:

1. $|M| < \infty$;

2. $U(M) \subseteq E_2$.

Для множества C', $C' \subseteq \mathfrak{L}_c$, через $\Sigma(C')$ обозначим замыкание множества C' по операции сложения.

Теорема 4.4.1. *Пусть M - конечная вырожденная S_0-система и*

$$f(x_1, x_2, \ldots, x_n) \in \mathfrak{L}.$$

Включение $f(x_1, x_2, \ldots, x_n) \in A(M)$ выполнено в точности тогда, когда

1. $U(f) \subseteq E_2$ и

2. $C(f) \subseteq \Sigma(C(M))$.

Доказательство.

Необходимость. Рассмотрим конечную вырожденную S_0-систему M и пусть $f(x_1, x_2, \ldots, x_n) \in A(M)$. Для $f(x_1, x_2, \ldots, x_n)$ имеет место разложение (4.24). Если $U(f) \not\subseteq E_2$, то найдется i_0, $i_0 \in \{1, 2, \ldots, n\}$, такое, что $\mu_{i_0} \notin E_2$ и для некоторого натурального числа k_0 и некоторого μ', $\mu' \in 1 + \{\xi\}\mathfrak{L}_0^{(1)}$, выполнено

$$\mu_{i_0}(\xi) + \mu_{i_0}(0) = \xi^{k_0}\mu'.$$

Если f A-выразимо через M, то в $S(M)$ найдется ЛА $f_{k_0+1}(x_1, x_2, \ldots, x_n)$, который $k_0 + 1$-эквивалентен ЛА f. Нетрудно видеть, что $U\left(f_{k_0+1}\right) \not\subseteq E_2$, что невозможно. Свойство 1 доказано.

Докажем теперь, что выполнено свойство 2. Не ограничивая общность рассуждений, будем считать, что все константы из множества $C(M)$ и константа из $C(f)$ имеют общую длину предпериода T_0 и общую длину периода T. Тогда любая константа из $\Sigma(M)$ имеет тоже длину предпериода T_0 и длину периода T. Из включения $f \in A(M)$ следует, что в $S(M)$ найдется ЛА g, T_0+T-эквивалентный

f. Поэтому первые T_0+T элементов последовательностей из $C(f)$ и $C(g)$ совпадают. Отсюда следует, что $C(f) = C(g)$, т.е. $C(f) \subseteq C(S(M))$. Нетрудно видеть также, что $C(S(M)) = \Sigma(C(M))$. Необходимость утверждения теоремы доказана.

Достаточность. Пусть, как и раньше, M – конечная вырожденная S_0-система и для некоторого ЛА $f(x_1, x_2, \dots, x_n)$ выполнены свойства 1 и 2.

Из свойства 2 следует, что для некоторых γ_i, $\gamma_i \in C(M)$, $j = 1, 2, \dots s$, справедливо: $C(f) = \{\gamma_1 + \gamma_2 + \dots + \gamma_s\}$. Используя операцию подстановки и константу 0, из ЛА множества M получим константы $\gamma_1, \gamma_2, \dots, \gamma_s$. Из леммы 4.4.1 следует: $x_1 + x_2 \in A(M)$. Из $x_1 + x_2$ операциями суперпозиции получим $x_1 + x_2 + \dots + x_s$. Подставляя вместо каждой переменной x_j этого сумматора константу γ_j, получим константу из $C(f)$. Далее, на $n+1$-й вход сумматора $x_1 + x_2 + \dots + x_{n+1}$ подставим константу из $C(f)$. Используя полученный ЛА, константу 0 и операцию подстановки, получим $f(x_1, x_2, \dots, x_n)$.

Достаточность утверждения теоремы установлена.

Теорема 4.4.1 доказана.

Далее будем рассматривать конечные невырожденные S_0-системы.

Пусть M - такая система, A-основанием множества $U(M)$ является μ_0, $\mu_0 \in \xi \cdot \mathfrak{L}_0^{(1)}$, $\mu_0 \neq 0$. Тогда для некоторого натурального числа r и ЛА μ', $\mu' \in 1 + \xi \cdot \mathfrak{L}_0^{(1)}$, выполнено: $\mu_0 = \xi^r \cdot \mu'$. Если для любого j, $j = 0, 1, \dots, r-1$, найдется целое неотрицательное число q_j такое, что для некоторой константы γ_j, $\gamma_j \in 1 + \xi\mathfrak{L}_c$, имеет место $\xi^{j+r\cdot q_j} \cdot \gamma_j \in A(M)$, то множество M называется PS-системой. Имеет место следующая лемма.

Лемма 4.4.2. *Пусть M является PS-системой. Тогда существует целое неотрицательное число T_0 такое, что для любой константы $\gamma, \gamma \in \mathfrak{L}_c$, справедливо: $\xi^{T_0} \cdot \gamma \in A(M)$.*

Доказательство. По определению PS-системы для любого j, $j = 0$, $1, \dots,$

$r-1$, найдутся q_j и γ_j, $q_j \in \mathbb{Z}_+$, $\gamma_j \in 1+\xi\cdot\mathfrak{L}_c$, что

$$\xi^{j+r\cdot q_j}\cdot\gamma_j \in A(M).$$

Через q обозначим

$$\max\{\ q_j\ \mid\ j=0,1,\ldots,r-1\ \}.$$

Тогда для некоторого T_1, $T_1 \in \mathbb{Z}_+$, и для любого j, $j=0,1,\ldots,r-1$, константы γ_j', $\gamma_j'=\mu_0^{T_1+(q-q_j)}\xi^{j+r\cdot q_j}\cdot\gamma_j$, содержатся в $A(M)$.

Поэтому для некоторых констант γ_j'', $\gamma_j'' \in 1+\xi\cdot\mathfrak{L}_c$, выполнено:

$$\gamma_j'=\xi^{j+r\cdot(q+T_1)}\cdot\gamma_j'',\quad j=0,1,\ldots,r-1.$$

Обозначим произведение $r\cdot(q+T_1)$ через T_0. Для любого целого неотрицательного числа T, $T\geq T_0$, найдутся s и s', $s\in\mathbb{Z}_+$, $s'\in\{0,1,\ldots,r-1\}$, такие, что $T=T_0+r\cdot s+s'$. Отсюда, для некоторой константы $\tilde{\gamma}_T$, $\tilde{\gamma}_T\in 1+\xi\cdot\mathfrak{L}_c$, выполнено $\xi^T\cdot\tilde{\gamma}_T\in A(M)$. Это вытекает из включения

$$\mu_0^s\cdot\gamma_{s'}'\in A(M).$$

Пусть γ - некоторая константа, $\gamma=a_0+a_1\xi+a_2\xi^2+\ldots$, и $\tau\in N$. Тогда для некоторых чисел a_0', a_1',..., $a_{\tau-1}'$ из E_2 константа $a_0'\xi^{T_0}\tilde{\gamma}_{T_0}+a_1'\xi^{T_0+1}\tilde{\gamma}_{T_0+1}+a_2'\xi^{T_0+2}\tilde{\gamma}_{T_0+2}+\cdots+a_{\tau-1}'\xi^{T_0+\tau-1}\tilde{\gamma}_{T_0+\tau-1}$ является $T_0+\tau$-эквивалентной константе $\xi^{T_0}\gamma$ и содержится в $S(M)$ ввиду $x_1+x_2\in A(M)$. По определению A-замыкания, отсюда следует включение $\xi^{T_0}\gamma\in A(M)$.

Лемма 4.4.2 доказана.

В параграфе 3 настоящей главы введено отображение $V^{(r)}$, $V^{(r)}:S_r\to E_2^{r+1}$. Здесь нам понадобится отображение $\tilde{V}^{(T_0)}$, $\tilde{V}^{(T_0)}:\mathfrak{L}\to E_2^{T_0}$, определяемое следующим образом. Пусть $f\in\mathfrak{L}$ и для f выполнено разложение (4.24). Тогда для μ_0 найдутся числа $a_0,a_1,\ldots,a_{T_0-1}$, $a_t\in E_2$, $t=0,1,\ldots,T_0-1$, для которых справедливо равенство

$$\mu_0=a_0+a_1\xi+a_2\xi^2+\cdots+a_{T_0-1}\xi^{T_0-1}+\xi^{T_0}\cdot\mu_0',$$

где μ_0' - некоторая константа из $\mathfrak{L}_c$. Положим

$$\tilde{V}^{(T_0)}(f) = (a_0, a_1, \ldots, a_{T_0-1}) .$$

Как обычно, для M', $M' \subseteq \mathfrak{L}$, через $\tilde{V}^{(T_0)}(M)$ обозначим

$$\left\{ \ \tilde{V}^{(T_0)}(f) \ \mid \ f \in M' \ \right\}.$$

Теорема 4.4.2. *Пусть множество M является PS-системой и T_0 таково, что*

$$\{\xi^{T_0}\} \cdot \mathfrak{L}_c \subseteq A(M). \tag{4.42}$$

Тогда включение $f \in A(M)$ равносильно выполнению следующих двух свойств.

1. $U(f) \subseteq A^{(1)}(U(M))$,
2. $\tilde{V}^{(T_0)}(f) \in \tilde{V}^{(T_0)}(A(M))$.

Доказательство.

Необходимость. Если $f \in A(M)$, то свойство 1 вытекает из леммы 4.2.2, а свойство 2 следует непосредственно из включения $f \in A(M)$. Необходимость утверждения теоремы доказана.

Достаточность. Рассмотрим PS-систему M и ЛА f, для которых выполнены свойства 1 и 2. Т.к. $x_1 + x_2 \in A(M)$, то, следуя доказательству леммы 4.2.3, получаем включение

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

Отсюда, если f, $f = f(x_1, x_2, \ldots, x_n)$, разложить в сумму одноместных ЛА согласно равенству (4.24), то

$$\mu_i \cdot x_i \in A(M). \tag{4.43}$$

Далее, для некоторой константы γ, $\gamma \in \mathfrak{L}_c$, и некоторых чисел a_0, a_1, $\ldots$, a_{T_0-1} выполнено:

$$\mu_0 = a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{T_0-1}\xi^{T_0-1} + \xi^{T_0} \cdot \gamma.$$

Поэтому $\tilde{V}^{(T_0)}(f) = (a_0, a_1, \ldots, a_{T_0-1})$. Но, по свойству 2 в $A(M)$ содержится ЛА g такой, что $\tilde{V}^{(T_0)}(g) = \tilde{V}^{(T_0)}(f)$. Поэтому

$$C(g) = \{\ a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{T_0-1}\xi^{T_0-1} + \xi^{T_0}\gamma'\ \}$$

для некоторой константы γ', $\gamma' \in \mathfrak{L}_c$. Подставляя константу 0 вместо всех переменных ЛА g, получим

$$\gamma'' = a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{T_0-1}\xi^{T_0-1} + \xi^{T_0}\gamma' \in A(M).$$

Но, $\mu_0 + \gamma'' = \xi^{T_0}(\gamma + \gamma') \in A(M)$ по условию (4.42).

Поэтому $\mu_0 = \gamma'' + (\mu_0 + \gamma'') \in A(M)$. Отсюда, из (4.43), а также учитывая $x_1 + x_2 \in A(M)$, получаем включение

$$\mu_1(x_1) + \mu_2(x_2) + \cdots + \mu_n(x_n) + \mu_0 \in A(M)$$

или $f \in A(M)$.

Необходимость утверждения теоремы и сама теорема доказаны.

Теорема 4.4.3. *Для конечной невырожденной S_0-системы M и ЛА f проверка включения*

$$\tilde{V}^{(T_0)}(f) \in \tilde{V}^{(T_0)}(A(M)) \tag{4.44}$$

алгоритмически разрешима.

Доказательство. Из $S(M) \subseteq A(M)$ получаем

$$\tilde{V}^{(T_0)}(S(M)) \subseteq \tilde{V}^{(T_0)}(A(M)).$$

С другой стороны, для любого ЛА f, $\in A(M)$, найдется T_0-эквивалентный ему ЛА g, $g \in S(M)$. Поэтому

$$\tilde{V}^{(T_0)}(S(M)) = \tilde{V}^{(T_0)}(A(M)).$$

Таким образом, проверка включения (4.44) сводится к прверке включения

$$\tilde{V}^{(T_0)}(f) \in \tilde{V}^{(T_0)}(S(M)).$$

Учитывая равенство

$$\tilde{V}^{(T_0)}(S(M)) = \tilde{V}^{(T_0)}(C(S(M))),$$

рассмотрим множество констант $C(S(M))$. Нетрудно видеть, что

$$\tilde{V}^{(T_0)}(C(S(M))) = \tilde{V}^{(T_0)}\left(\sum_{\gamma\in C(M)} S^{(1)}(U(M))\cdot\gamma\right).$$

Пусть $U(M)$ имеет A-основание μ_0, $\mu_0 = \xi^r\cdot\mu'$, $\mu' \in 1+\xi\mathfrak{L}_c$. Положим

$$\begin{gathered} M_{T_0} = \Big\{\ u\left(\mu_0\right)\ \mid u\left(\mu_0\right) \in E_2[\mu_0],\ \deg u(\xi) < \tfrac{T_0}{r}, \\ \text{и найдется ЛА}\ \ \mu,\ \ \mu \in S^{(1)}(U(M)),\ \ \text{такой, что} \\ u(\mu_0) + \mu \in \mu_0^{]\frac{T_0}{r}[}\cdot\mathfrak{L}_0^{(1)}\left(\mu_0\right)\Big\} \end{gathered}$$

Утверждение теоремы вытекает из конечности множества M_{T_0} и равенства

$$\tilde{V}^{(T_0)}(C(S(M))) = \tilde{V}^{(T_0)}\left(\sum_{\gamma\in C(M)} M_{T_0}\cdot\gamma\right).$$

Теорема доказана.

Теорема 4.4.4. *Пусть M - конечная невырожденная S_0-система, μ_0 является A-основанием $U(M)$, $\mu_0 = \xi^2+\xi^3\mu'$, для некоторого μ', $\mu'\in\mathfrak{L}_0^{(1)}$. Тогда задача A-выразимости через множество M алгоритмически разрешима.*

Доказательство, Т. к. $0\in A(M)$, то сначала рассмотрим случай $C(M) = \{0\}$. Тогда $M\subseteq\mathfrak{L}^0$ и для любой f, $f\in A(M)$, справедливо $f\in\mathfrak{L}^0$. Поэтому найдется натуральное число n и найдутся ЛА $\mu_i(x)$, $\mu_i(x)\in\mathfrak{L}_0^{(1)}$, $\quad i=1,2,\ldots,n$, такие, что выполнено

$$f = \mu_1\left(x_1\right) + \mu_2\left(x_2\right) + \cdots + \mu_n\left(x_n\right),$$

и проверка включения $f\in A(M)$ сводится к проверке соотношений

$$\mu_i \in A^{(1)}(U(M))$$

для каждого i, $i = 1, 2, \ldots, n$.

Далее рассмотрим случай $C(M) \setminus \{0\} \neq \emptyset$.

Тогда найдется константа γ, $\gamma \in C(M)$, $\gamma \neq 0$. Существуют T_γ и γ', $T_\gamma \in \mathbb{Z}_+$, $\gamma' \in 1 + \xi \mathfrak{L}_c$, удовлетворяющие равенству $\gamma = \xi^{T_\gamma} \cdot \gamma'$. Не ограничивая общность рассуждений, будем считать, что для любой константы β, $\beta \in C(M) \setminus \{0\}$, $\beta = \xi^{T_\beta} \cdot \beta'$, $\beta' \in 1 + \xi \cdot \mathfrak{L}_c$, $T_\beta \in \mathbb{Z}_+$, $T_\beta \geq T_\gamma$.

Нетрудно видеть, что для любой константы β, $\beta \in C(M) \setminus \{0, \gamma\}$ справедливо одно из следующих двух свойств.

1. $\beta \in A^{(1)}(\mu_0) \cdot \gamma$.

2. Найдутся числа $a_0, a_1, \ldots, a_s$, $a_j \in E_2$, $j = 0, 1, \ldots, s$, найдется натуральное число T', имеющее отличную от T_γ четность, и найдется константа $\tilde{\gamma}$, $\tilde{\gamma} \in 1 + \xi \cdot \mathfrak{L}_c$, удовлетворяющие равенству

$$\beta = a_0\gamma + a_1\mu_0\gamma + a_2\mu_0^2\gamma + \cdots + a_s\mu_0^s\gamma + \xi^{T'} \cdot \tilde{\gamma}.$$

Включение

$$\beta \in A^{(1)}(\{\mu_0\}) \cdot \gamma \tag{4.45}$$

можно проверить. Действительно, оно означает существование ряда $r(\mu_0)$ такого, что $\beta = r(\mu_0) \cdot \gamma$. Отсюда, $r(\mu_0) = \frac{\beta}{\gamma}$. Но $\frac{\beta}{\gamma}$ равно некоторой дроби из $\mathfrak{L}_0^{(1)}$. Поэтому, учитывая выбор μ_0, имеем, что $r(\mu_0)$ - периодический (с предпериодом) ряд. Таким образом, проверка включения (4.45) сводится к проверке включения $\frac{\beta}{\gamma} \in \mathfrak{L}_0^{(1)}(\mu_0)$, что алгоритмически разрешимо.

Далее, если хотя бы для одной константы β из $C(M) \setminus \{0, \gamma\}$ выполнено свойство 2, то множество M является PS-системой и по теореме 4.4.2 проверка A-выразимости через M алгоритмически разрешима.

В противном случае, сначала проверим включение

$$C(f) \subseteq A^{(1)}(\{\mu_0\}) \cdot \gamma.$$

Если проверяемое включение не имеет места, то $f \notin A(M)$. Пусть это включение имеет место. Находим $\mu\,(\mu_0)$, $\mu\,(\mu_0) \in \mathfrak{L}_0^{(1)}\,(\mu_0)$, такую, что $C(f) = \{\mu\,(\mu_0)\,\gamma\}$.

Как следует из результатов параграфа 2 этой главы, найдется натуральное T такое, что для любого $\mu'\,(\mu_0)$, $\mu'\,(\mu_0) \in \mathfrak{L}_0^{(1)}\,(\mu_0)$, выполнено:

$$\mu_0^T \mu'\,(\mu_0) \in A^{(1)}(M).$$

Тогда найдется многочлен $g(\xi)$, $g(\xi) \in E_2[\xi]$, $\deg g(\xi) < T$, и найдется μ'', $\mu'' \in \mathfrak{L}_0^{(1)}$, удовлетворяющие равенству

$$\mu\,(\mu_0) = g\,(\mu_0) + \mu_0^T \mu''\,(\mu_0)\,.$$

Кроме того, для каждого γ', $\gamma' \in C(M)$, найдутся многочлен $g_{\gamma'}(\xi)$ и ЛА $\tilde{\mu}_{\gamma'}$ из $\mathfrak{L}_0^{(1)}$ такие, что $\deg g_{\gamma'}(\xi) < T$,

$$\gamma' = \left(g_{\gamma'}(\mu_0) + \mu_0^T \tilde{\mu}_{\gamma'}(\mu_0)\right)\gamma.$$

Соотношение $C(f) \subseteq C(A(M))$ выполнено в точности тогда, когда для констант γ', $\gamma' \in C(M)$, в $A^{(1)}(U(M))$ найдутся ЛА $h_{\gamma'}\,(\mu_0)$ такие, что

$$\sum_{\gamma \in C(M)} h_{\gamma'}\,(\mu_0) \cdot g_{\gamma'}\,(\mu_0) + g\,(\mu_0) \in \mu_0^T \mathfrak{L}_0^{(1)}\,(\mu_0)\,,$$

что можно проверить.

Теорема доказана.

4.5. Об основаниях систем с сумматором, для которых выразимость и аппроксимационная выразимость равносильны

В настоящем параграфе рассматриваются множества ЛА, содержащие сумматор в замыкании. Безусловно, выразимость какого-либо ЛА через заданное множество ЛА означает его A-выразимость через эту же систему ЛА. Понятие A-выразимости возникло с целью увеличения выразительных возможностей конечных автоматов. С другой стороны, для некоторых множеств конечных автоматов переход от выразимости к A-выразимости не приводит к расширению их выразительных возможностей.

Рассмотрим множество M, $M \subseteq \mathfrak{L}$, удовлетворяющее соотношениям: $x_1 + x_2 \in K(M)$, $U(M) \setminus E_2 \neq \emptyset$. Как следует из теоремы 3.2.1 из главы 3, найдутся такие μ, u_0, T, $\mu \in \xi\mathfrak{L}_0^{(1)} \setminus \{0\}$, $u_0 \in 1 + \{\xi\}E_2[\xi]$, $T \in N$, что выполнено одно из двух следующих соотношений:

$$M^{(1)}\left(\mu, (\xi u_0)^T\right) \subseteq K^{(1)}(U(M)) \subseteq M^{(1)}\left(\mu, u_0\right), \tag{4.46}$$

$$P^{(1)}\left(\mu, (\xi u_0)^T\right) \subseteq K^{(1)}(U(M)) \subseteq M_0^{(1)}(\mu) \cap M^{(1)}\left(\mu, u_0\right), \tag{4.47}$$

ЛА μ будем называть основанием множества M.

В настоящем параграфе приведен критерий, позволяющий определить основания, что для любого множества ЛА с таким основанием его замыкание и A-замыкание совпадают.

Таким образом, необходимо распознать те μ, $\mu \in \xi\mathfrak{L}_0^{(1)} \setminus \{0\}$, для которых справедливо равенство $K(M) = A(M)$ лишь только $M \subseteq \mathfrak{L}$, $|M| < \infty$, $x_1 + x_2 \in K(M)$ и M имеет основание μ.

Лемма 4.5.1. *Пусть $\mu \in \xi\mathfrak{L}_0^{(1)} \setminus \{0\}$ и для любого множества ЛА M,*

$$M \subseteq \mathfrak{L}, \;\; x_1 + x_2 \in K(M), \;\; U(M) \setminus E_2 \neq \emptyset, \tag{4.48}$$

с основанием μ выполнено:

$$K(M) = A(M). \tag{4.49}$$

Тогда найдется натуральное число k и найдется многочлен $v(\xi)$, $v(\xi) \in 1 + \xi E_2[\xi]$, $\deg v(\xi) \leq k$, такие, что $\frac{\xi^k}{v(\xi)}$ является основанием множества M.

Доказательство. Пусть $\mu \in \xi\mathfrak{L}_0^{(1)} \setminus \{0\}$ и для любого M со свойствами (4.48) и основанием μ выполнено равенство (4.49).

При этом для основания μ найдутся натуральное число k и ЛА μ', $\mu' \in 1 + \xi\mathfrak{L}_0^{(1)}$, такие, что $\mu = \xi^k \cdot \mu'$.

Через C' обозначим множество констант $\left\{1, \xi, \xi^2 \dots, \xi^{k-1}\right\}$. Если множество M обладает свойствами (4.48), имеет основание μ и $C' = C(M)$, то по теореме 1 из параграфа 3 множество M является S-системой, т.е.

$$\mathfrak{L}_c \subseteq A(M). \tag{4.50}$$

С другой стороны, при $\deg \mu > k$ справедливо

$$\mathfrak{L}_c \not\subseteq K(M). \tag{4.51}$$

Действительно,

$$C(K(M)) \subseteq \sum_{\gamma \in C(M)} \mathfrak{L}_0^{(1)}(\mu) \cdot \gamma = \sum_{i=0}^{k-1} \mathfrak{L}_0^{(1)}(\mu)\xi^i.$$

При этом множество $\left\{1, \xi, \xi^2, \dots, \xi^{\deg \mu - 1}\right\}$ линейно независимо над полем $E_2(\mu)$ [20]. Поэтому ξ^k нельзя представить в виде $\sum_{i=0}^{k-1} \mathfrak{L}_0^{(1)}(\mu)\xi^i$. Соотношение (4.51) доказано.

Из соотношений (4.50) и (4.51) получаем противоречие с (4.49).

Таким образом, $\deg \mu = k$. Поэтому найдется многочлен $v(\xi)$, $v(\xi) \in 1 + \xi \cdot E_2[\xi]$, $\deg v(\xi) \le k$, удовлетворяющий равенству $\mu' = \frac{1}{v(\xi)}$.

Лемма доказана.

Лемма 4.5.2. *Если выполнены соотношения (4.48) и для некоторых k и $v(\xi)$, $k \in \mathbb{N}$, $v(\xi) \in 1 + \xi E_2[\xi]$, $\deg v(\xi) \le k$, дробь μ, $\mu = \frac{\xi^k}{v(\xi)}$ является основанием M, то найдется натуральное число T, для которого*

$$\mu^T \cdot \mathfrak{L}_0^{(1)}(\mu) \subseteq U(K(M)) \subseteq \mathfrak{L}_0^{(1)}(\mu). \tag{4.52}$$

Доказательство. Основанием множества M, удовлетворяющим соотношениям (4.48), является ЛА μ из $\mathfrak{L}_0^{(1)}$, не содержащийся в $M_i^{(1)}$ для любого i, $\quad i = 0, 2, 3, \ldots$.

Из доказательства теоремы 3.2.1 и соотношения $\mu \notin M_0^{(1)}$ следует, что для некоторого T, $T \in \mathbb{N}$, имеет место соотношение (4.46).

А из соотношений $\mu \notin M_i^{(1)}$, $i = 2, 3, \ldots$, получим равенство $u_0 = 1$. Поэтому

$$M^{(1)}\left(\mu, \xi^T\right) \subseteq K^{(1)}(U(M)) \subseteq M^{(1)}(\mu, 1),$$

что в точности и означает соотношение (4.52).

Лемма 4.5.2 доказана.

Лемма 4.5.3. *Пусть выполнены соотношения (4.48) и для некоторых k и $v(\xi)$ справедливы:*

$$k \in \mathbb{N}, \;\; v(\xi) \in 1 + \xi E_2[\xi], \;\; \deg v(\xi) \leq k, \;\; \mu = \frac{\xi^k}{v(\xi)}. \tag{4.53}$$

Если при этом μ является основанием M, то μ является также A-основанием множества M.

Доказательство. Пусть для μ найдутся k и $v(\xi)$, удовлетворяющие соотношениям (4.53), и μ - основание для M, удовлетворяющей условиям (4.48). И пусть μ_0 - A-основание для M. Тогда по теореме 4.1.2 из параграфа 1 этой главы имеем: $\deg \mu_0 \leq k$ и, если $\mu_0 = \xi^s \cdot \mu_0'$ для некоторых s и μ_0', $s \in \mathbb{N}$, $\mu_0' \in 1 + \xi \cdot \mathfrak{L}_0^{(1)}$, то $s = k$ (из свойства 2 теоремы 4.1.2). Отсюда, $\deg \mu_0 = k$. Поэтому μ - ЛА минимальной степени, для которого выполнены свойства 1 и 2 теоремы 4.1.2. Следовательно, μ также является A-основанием множества M.

Лемма 4.5.3 доказана.

Лемма 4.5.4. *Пусть для множества M выполнены соотношения (4.48) и μ является A-основанием для M. Тогда*

1. *Найдется s, $s \in \mathbb{N}$, и найдутся γ_i, $\gamma_i \in C(M)$, $i = 1, 2, \ldots, s$, такие, что для любой γ, $\gamma \in C(A(M))$, найдутся r_i, $r_i \in R_2(\mu)$, $i = 1, 2, \ldots, s$, и выполнено:*

$$\gamma = \sum_{i=1}^{s} r_i \gamma_i.$$

2. *Найдутся s', T, $s' \in \mathbb{N}$, $T \in \mathbb{N}$, найдутся γ'_i, $\gamma'_i \in C(M)$, $i = 1, 2, \ldots, k'$, γ'_1, γ'_2, $\ldots$, $\gamma'_{s'}$ – линейно независимы над $R_2(\mu)$ и найдется C', $C' \subseteq C(S(M))$, $|C'| < \infty$, такие, что*

$$C(A(M)) = C' + \left(\sum_{i=1}^{s'} \mu^T R_2(\mu) \gamma'_i \right) \cap \mathfrak{L}_c.$$

Доказательство. Пусть $\mu = \xi^k \mu'$, $\mu' \in 1 + \xi \mathfrak{L}_0^{(1)}$.

Рассмотрим множество пар целых неотрицательных чисел Π,

$$\begin{gathered}\Pi = \{ \ (j, T_j) \ \mid \ j \in \{0, 1, \ldots, k-1\}, \ T_j \in \mathbb{Z}_+, \ \text{найдутся} \ l_j, \\ l_j \in \mathbb{N}, \ \text{найдутся} \ \beta_{1,j}, \beta_{2,j}, \ldots, \beta_{l_j,j}, \\ \beta_{i,j} \in C(M), \ \text{найдутся} \ u_{1,j}, u_{2,j}, \ldots, u_{l_j,j}, \\ u_{i,j} \in E_2[\mu], \\ \beta_{1,j} u_{1,j} + \beta_{2,j} u_{2,j} + \ldots \beta_{l_j,j} u_{l_j,j} \in \xi^{j + T_j \cdot k} \left(1 + \xi \mathfrak{L}_c\right) \right\}.\end{gathered}$$

Обозначим через Π_1 проекцию множества Π на первую компоненту:

$$\Pi_1 = \{ \ j \ \mid \ \text{найдется} \ T, \ (j, T) \in \Pi \ \}.$$

Каждому j, $j \in \Pi_1$, сопоставим число $T(j)$ такое, что

$$T(j) = \min\{ \ T \ \mid \ (j, T) \in \Pi \ \},$$

а также наборы $\bar{\beta}(j)$, $\bar{u}(j)$,

$$\bar{\beta}(j) = \left(\beta_{1,j}, \beta_{2,j}, \ldots, \beta_{l_j,j}\right), \ \ \bar{u}(j) = \left(u_{1,j}, u_{2,j}, \ldots, u_{l_j,j}\right),$$

такие, что

$$\left(\bar{u}(j), \bar{\beta}(j)\right) \in \xi^{j + T(j) \cdot k} \left(1 + \xi \mathfrak{L}_c\right),$$

где через $\left(\bar{u}(j), \bar{\beta}(j)\right)$ обозначено скалярное произведение векторов $\bar{u}(j)$ и $\bar{\beta}(j)$.

Нетрудно видеть, что для любой γ, $\gamma \in C(A(M))$, найдутся r_j, $j \in \Pi_1$, $r_j \in R_2(\mu)$, что

$$\sum_{j\in\Pi_1} r_j \left(\bar{u}(j), \bar{\beta}(j)\right) = \gamma. \tag{4.54}$$

Действительно, предположим противное. Тогда для некоторого j_0, $j_0 \in \{0, 1, \dots, k-1\} \setminus \Pi_1$, некоторого T', $T' \in \mathbb{Z}_+$, и некоторых u'_j, $u'_j \in E_2[\mu]$, $j \in \Pi_1$, выполнено:

$$\gamma + \sum_{j\in\Pi_1} u'_j \left(\bar{u}(j), \bar{\beta}(j)\right) \in \xi^{j_0+T'\cdot k} \cdot \left(1 + \xi E_2[\xi]\right).$$

Из включения $\mu^{\bar{T}} \mathfrak{L}_0^{(1)}(\mu) \subseteq U(A(M))$ для $\bar{\gamma}$,

$$\bar{\gamma} = \left(\mu^{\bar{T}}\right)^2 \gamma + \sum_{j\in\Pi_1} \left(\mu^{\bar{T}} \cdot u'_j\right) \left(\left(\mu^{\bar{T}} \cdot \bar{u}(j)\right), \bar{\beta}(j)\right),$$

следует

$$\bar{\gamma} \in \xi^{j_0+\left(T'+2\bar{T}\right)k} \cdot \left(1 + \xi E_2[\xi]\right)$$

и

$$\bar{\gamma} \in C(A(M)).$$

Отсюда, $j_0 \in \Pi_1$. Полученное противоречие означает справедливость утверждения (4.54), из которого непосредственно вытекает равенство $\gamma = \sum_{i=1}^{s} r_i \gamma_i$ для некоторых γ_i и r_i, $\gamma_i \in C(M)$, $r_i(\mu) \in R_2(\mu)$, $i = 1, 2, \dots, s$. При этом $\{\ \gamma_i \mid i = 1, 2, \dots, s\ \}$ не зависит от γ.

Пункт 1 леммы 4.5.4 доказан.

Докажем пункт 2. Утверждение 1 леммы означает, что

$$C(A(M)) \subseteq \sum_{i=1}^{s} R_2(\mu)\gamma_i.$$

Пусть Γ', $\Gamma' = \{\gamma'_1, \gamma'_2, \dots, \gamma'_{s'}\}$ – максимальное линейно независимое над $R_2(\mu)$ множество, содержащееся в множестве Γ, $\Gamma = \{\gamma_1, \gamma_2, \dots, \gamma_s\}$. Тогда для любого $\gamma, \gamma \in \Gamma \setminus \Gamma'$ найдутся ряды $r_\gamma, r_1, r_2, \dots, r_{s'}$ из $R_2(\mu)$ и $r_\gamma \neq 0$, для которых

$$r_\gamma \gamma + r_1 \gamma'_1 + \gamma'_2 + \dots + r_{s'} \gamma_{s'} = 0.$$

Поэтому найдется натуральное число T' такое, что для любого γ, $\gamma \in \Gamma \backslash \Gamma'$, выполнено:

$$\mu^{T'}\gamma \in \sum_{i=1}^{s'} R_2(\mu)\gamma_i'.$$

Найдется такое T'', $T'' \in \mathbb{N}$, что любая константа из $\sum_{i=1}^{s} R_2(\mu)\mu^{T''}\gamma_i'$ содержится в $C(A(M))$. Положим $T = T' + T''$.Тогда для любой $\gamma, \gamma \in \Gamma \setminus \Gamma'$, имеем: $\mu^T\gamma \in C(A(M))$.

Через $E_2^{(T)}[\xi]$ обозначим множество всех многочленов над E_2 от переменной ξ, имеющих степень меньше T,

$$E_2^{(T)}[\xi] = \{\ a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{T-1}\xi^{T-1}\ \mid\ a_i \in E_2,$$

$$i = 0, 1, \ldots, T-1\ \}.$$

Тогда $R_2(\mu) = E_2^{(T)}[\mu] + \mu^T R_2(\mu)$ и

$$\begin{gathered}
\textstyle\sum_{i=1}^{s} R_2(\mu)\gamma_i = \sum_{\gamma\in\Gamma'} R_2(\mu)\gamma + \sum_{\gamma\in\Gamma\backslash\Gamma'} R_2(\mu)\gamma = \\
\textstyle= \sum_{\gamma\in\Gamma'} R_2(\mu)\gamma + \sum_{\gamma\in\Gamma\backslash\Gamma'} E_2^{(T)}[\mu]\gamma + \\
\textstyle\sum_{\gamma\in\Gamma\backslash\Gamma'} R_2(\mu)\left(\mu^T\gamma\right) = \\
\textstyle= \sum_{\gamma\in\Gamma'} R_2(\mu)\gamma + \sum_{\gamma\in\Gamma\backslash\Gamma'} E_2^{(T)}[\mu]\gamma = \\
\textstyle= \sum_{\gamma\in\Gamma} E_2^{(T)}[\mu]\gamma + \sum_{\gamma\in\Gamma'} \mu^T R_2(\mu)\gamma.
\end{gathered}$$

Таким образом,

$$\begin{gathered}
\left(\textstyle\sum_{\gamma\in\Gamma'} \mu^T R_2(\mu)\gamma\right) \cap \mathfrak{L}_c \subseteq C(A(M)) \subseteq \\
\left(\textstyle\sum_{\gamma\in\Gamma} E_2^{(T)}[\mu]\gamma + \sum_{\gamma\in\Gamma'} \mu^T R_2(\mu)\gamma\right) \cap \mathfrak{L}_c = \\
\textstyle\sum_{\gamma\in\Gamma} E_2^{(T)}[\mu]\gamma + \left(\sum_{\gamma\in\Gamma'} \mu^T R_2(\mu)\gamma\right) \cap \mathfrak{L}_c,
\end{gathered}$$

откуда получаем утверждение 2 леммы 4.5.4.

Лемма доказана.

Лемма 4.5.5. *Пусть μ, $\mu = \frac{\xi^k}{u(\xi)}$, $u(\xi) \in 1 + \{\xi\}E_2[\xi]$, $\deg u(\xi) \le k$, является A-основанием некоторого множества M, для которого выполнены соотношения (4.48). Тогда*

$$U(K(M)) = U(A(M)) \tag{4.55}$$

и

$$C(K(M)) = C(A(M)). \tag{4.56}$$

Доказательство. Сначала докажем равенство (4.55).

По лемме 4.5.2 для некоторого T, $T \in \mathbb{N}$, имеет место (4.52). По теореме 4.1.1 для некоторого T_1, $T_1 \in \mathbb{N}$, выполнено

$$\mu^{T_1}\mathfrak{L}_0^{(1)}(\mu) \subseteq U(A(M)) \subseteq \mathfrak{L}_0^{(1)}(\mu).$$

Положим $\bar{T} = max\,(T, T_1)$. Имеем,

$$\mu^{\bar{T}}\mathfrak{L}_0^{(1)}(\mu) \subseteq U(K(M)) \subseteq \mathfrak{L}_0^{(1)}(\mu),$$

$$\mu^{\bar{T}}\mathfrak{L}_0^{(1)}(\mu) \subseteq U(A(M)) \subseteq \mathfrak{L}_0^{(1)}(\mu).$$

Обозначим через M_1 множество

$$\Big\{\ u(\mu)\ \mid\ \deg u(\xi) < \bar{T},\ \text{ найдется }\ \tilde{\mu}(\xi),\ \ \tilde{\mu}(\mu) \in U(K(M)),$$
$$\text{найдется }\ \tilde{\tilde{\mu}},\ \ \tilde{\tilde{\mu}} \in \mathfrak{L}_0^{(1)},\ \ \tilde{\mu}(\mu) = u(\mu) + \mu^{\bar{T}} \cdot \tilde{\tilde{\mu}}(\mu)\Big\},$$

а через M_2 множество

$$\Big\{\ u(\mu)\ \mid\ \deg u(\xi) < \bar{T},\ \text{ найдется }\ \tilde{\mu}(\xi),\ \ \tilde{\mu}(\xi) \in U(A(M)),$$
$$\text{найдется }\ \tilde{\tilde{\mu}},\ \ \tilde{\tilde{\mu}} \in \mathfrak{L}_0^{(1)},\ \ \tilde{\mu}(\mu) = u(\mu) + \mu^{\bar{T}} \cdot \tilde{\tilde{\mu}}(\mu)\Big\}.$$

Нетрудно видеть, что

$$U(K(M)) = M_1 + \mu^{\bar{T}}\mathfrak{L}_0^{(1)}(\mu),$$

$$U(A(M)) = M_2 + \mu^{\bar{T}}\mathfrak{L}_0^{(1)}(\mu)$$

и $M_1 = M_2$.

Отсюда получаем равенство (4.55).

Теперь докажем равенство (4.56).

Ввиду справедливости включения $K(M) \subseteq A(M)$, получаем $C(K(M)) \subseteq C(A(M))$. Таким образом, требуется доказать соотношение $C(A(M)) \subseteq C(K(M))$.

Пусть Γ', $\Gamma' = \{\gamma'_1, \gamma'_2, \ldots, \gamma'_{k'}\}$, множество констант линейно независимое над $R_2(\mu)$. Тогда

$$\left(\sum_{i=1}^{k'} R_2(\mu)\gamma'_i\right) \cap \mathfrak{L}_c = \sum_{i=1}^{k'} \mathfrak{L}_0^{(1)}(\mu)\gamma'_i.$$

Докажем последнее утверждение. Включение

$$\sum_{i=1}^{k'} \mathfrak{L}_0^{(1)}(\mu)\gamma'_i \subseteq \sum_{i=1}^{k'} R_2(\mu)\gamma'_i,$$

очевидно, выполнено. Поэтому для доказательства рассматриваемого утверждения требуется показать справедливость соотношения

$$\left(\sum_{i=1}^{k'} R_2(\mu)\gamma'_i\right) \cap \mathfrak{L}_c \subseteq \sum_{i=1}^{k'} \mathfrak{L}_0^{(1)}(\mu)\gamma'_i. \tag{4.57}$$

Рассмотрим сначала случай, когда из того, что множество $\{\gamma, \gamma'_i | i = 1, 2, \ldots, k'\}$ линейно зависимо над $R_2(\mu)$ следует, что множество $\{\gamma, \gamma'_i | i = 1, 2, \ldots, k'\}$ линейно зависимо над $\mathfrak{L}_0^{(1)}(\mu)$. В этом случае пусть $\gamma \in \sum_{i=1}^{k'} R_2(\mu)\gamma'_i$. Тогда найдутся ряды $r_1(\mu)$, $r_2(\mu)$, $\ldots$, $r_{k'}(\mu)$ из $R_2(\mu)$, что

$$\gamma = \sum_{i=1}^{k'} r_i(\mu)\gamma'_i,$$

т.е. множество $\{\gamma, \gamma'_1, \gamma'_1, \ldots, \gamma'_{k'}\}$ линейно зависимо над $R_2(\mu)$.

Тогда по предположению найдутся $\mu_0(\mu)$, $\mu_1(\mu)$, $\ldots$, $\mu_{k'}(\mu)$, - ЛА из $\mathfrak{L}_0^{(1)}$, не все равные 0, что

$$\mu_0(\mu)\gamma + \sum_{i=1}^{k'} \mu_i(\mu)\gamma'_i = 0.$$

Т.к. множество $\{\gamma_i | i = 1, 2, \ldots, k'\}$ линейно независимо над $\mathfrak{L}_0^{(1)}(\mu)$, то $\mu_0(\mu) \neq 0$. Поэтому

$$\gamma = \sum_{i=1}^{k'} \frac{\mu_i(\mu)}{\mu_0(\mu)}\gamma'_i.$$

Получили еще одно разложение константы γ через константы γ'_i над полем

$$\cup_{j=0}^{\infty} \left\{\mu^{-j}\right\} \cdot R_2(\mu).$$

Ввиду однозначности такого разложения, заключаем:

$$r_i(\mu) = \frac{\mu_i(\mu)}{\mu_0(\mu)}.$$

Это означает, что $r_i(\mu) \in \mathfrak{L}_0^{(1)}(\mu)$ и включение (4.57) в рассматриваемом случае доказано.

Пусть теперь найдется константа γ такая, что множество Γ,

$$\Gamma = \{ \ \gamma, \ \ \gamma_i' \ | \ i = 1, 2, \ldots, k' \ \},$$

линейно зависимо над множеством $R_2(\mu)$, но не является линейно зависимым над $\mathfrak{L}_0^{(1)}(\mu)$. Тогда Γ не является линейно зависимым над полем $E_2(\mu)$. Т.к. $\deg \mu = k$, то множество Γ можно дополнить до линейного базиса в $E_2(\xi)$, добавив $k - (k' + 1)$ констант $\gamma'_{k'+1}, \gamma'_{k'+2}, \ldots, \gamma'_{k-1}$. Тогда константы множества

$$\{ \ \gamma_i' \ | \ i = 1, 2, \ldots, k - 1 \ \}$$

образуют базис в $\cup_{i=0}^{\infty} \left\{\xi^{-j}\right\} R_2(\xi)$ над полем $\cup_{i=0}^{\infty} \left\{\mu^{-j}\right\} R_2(\mu)$. Но базисом в $\cup_{i=0}^{\infty} \left\{\xi^{-j}\right\} R_2(\xi)$ над полем $\cup_{i=0}^{\infty} \left\{\mu^{-j}\right\} R_2(\mu)$ является множество

$$\left\{1, \xi, \xi^2, \ldots, \xi^{k-1}\right\},$$

состоящее из k констант. Полученное противоречие означает, что рассматриваемый случай невозможен.

Отсюда и из леммы 4.5.4 получаем для некоторого конечного множества констант Γ и максимального линейно независимого подмножества в нем Γ':

$$\begin{gathered} \textstyle\sum_{\gamma\in\Gamma'} \mu^T \mathfrak{L}_0^{(1)}(\mu)\gamma \subseteq C(A(M)) \subseteq \\ \textstyle\sum_{\gamma\in\Gamma} E_2^{(T)}[\mu]\gamma + \sum_{\gamma\in\Gamma'} \mu^T \mathfrak{L}_0^{(1)}(\mu)\gamma, \end{gathered}$$

т.е. для любого T', $T' \geq T$, найдется $R_{T'}$, $R_{T'} \subseteq \sum_{\gamma\in\Gamma} E_2^{(T)}[\mu]\gamma$ и

$$C(A(M)) = R_{T'} + \sum_{\gamma\in\Gamma'} \mu^{T'} \mathfrak{L}_0^{(1)}(\mu)\gamma.$$

Но, для некоторого T'' справедливо:

$$\sum_{\gamma\in\Gamma'} \mu^{T''}\mathfrak{L}_0^{(1)}(\mu)\gamma \subseteq C(K(M)),$$

поэтому найдется $\tilde{T}$, $\tilde{T}\in\mathbb{N}$, и найдутся $R_{\tilde{T}}$, $R'_{\tilde{T}}$,

$$R_{\tilde{T}} \subseteq \sum_{\gamma\in\Gamma} E_2^{\tilde{T}}[\mu]\gamma,\;\; R'_{\tilde{T}} \subseteq \sum_{\gamma\in\Gamma} E_2^{\tilde{T}}[\mu]\gamma,$$

для которых

$$C(A(M)) = R_{\tilde{T}} + \sum_{\gamma\in\Gamma'} \mu^{\tilde{T}}\mathfrak{L}_0^{(1)}(\mu)\gamma \quad \text{и}$$

$$C(K(M)) = R'_{\tilde{T}} + \sum_{\gamma\in\Gamma'} \mu^{\tilde{T}}\mathfrak{L}_0^{(1)}(\mu)\gamma.$$

Далее, равенство $R_{\tilde{T}} = R'_{\tilde{T}}$ следует из (4.55). Поэтому соотношение (4.56) справедливо.

Лемма доказана.

Теорема 4.5.1. *Пусть $\mu\in\xi\mathfrak{L}_0^{(1)}\setminus\{0\}$. Равенство $K(M)=A(M)$ имеет место для любого M со свойствами (4.48) и с основанием μ в точности тогда, когда $\mu\notin M_i^{(1)}$, $i=0,2,3,\ldots$*

Доказательство. Пусть $\mu\in\xi\mathfrak{L}_0^{(1)}\setminus\{0\}$, и, кроме того, для любого M со свойствами (4.48) и основанием μ выполнено соотношение (4.49). Тогда по лемме 4.5.1 для некоторого k, $k\in\mathbb{N}$, и для некоторого $v(\xi)$, $v(\xi)\in 1+\xi E_2[\xi]$, $\deg v(\xi)\le k$, справедливо: $\mu=\frac{\xi^k}{v(\xi)}$. Нетрудно видеть, что $\mu\notin M_i^{(1)}$ для каждого i, $i=0,2,3,\ldots$. Необходимость утверждения теоремы доказана.

Достаточность. Пусть для μ, $\mu\in\xi\mathfrak{L}_0^{(1)}\setminus\{0\}$ выполнены соотношения $\mu\notin M_i^{(1)}$, $i=0,2,3,\ldots$. Отсюда следует, что для некоторого k, $k\in\mathbb{N}$, и некоторого $v(\xi)$, $\deg v(\xi)\le k$ выполнено равенство: $\mu=\frac{\xi^k}{v(\xi)}$. Пусть при этом μ является основанием множества M, обладающего свойствами (4.48). По лемме 4.5.3 дробь μ также является A-основанием M. Тогда по лемме 4.5.5 выполнены равенства (4.55) и (4.56), а это, с учетом $x_1+x_2\in K(M)$, означает равенство $K(M)=A(M)$.

Теорема доказана.

Следствие 3. *Если для некоторого M со свойствами (4.48) и для любого i, $i = 0, 2, 3, \ldots$, имеет место $U(M) \nsubseteq M_i^{(1)}$, то справедливо равенство (4.49).*

Доказательство. Пусть для множества M ЛА выполнены свойства (4.48) и

$$U(M) \nsubseteq M_i^{(1)} \text{ при } i, \;\; i = 0, 2, 3, \ldots. \tag{4.58}$$

Тогда для основания μ множества M имеем:

$$\mu \notin M_i^{(1)}, \;\; i = 0, 2, 3, \ldots$$

По теореме 4.5.1 для множества M получаем (4.49).

Следствие доказано.

Заметим, что проверка счетного числа свойств (4.58), согласно определению классов $M_i^{(1)}$, может быть осуществлена алгоритмически.

4.6. Структура аппроксимационно замкнутых множеств линейных автоматов, содержащих сумматор в аппроксимационном замыкании

Обратим внимание на то, что лемму 4.5.4 из предыдущего параграфа можно обобщить следующим образом.

Лемма 4.6.1. *Пусть для множества M имеют место следующие соотношения.*

$$\begin{gathered} M \subseteq \mathfrak{L}, \;\; x_1 + x_2 \in A(M), \;\; U(M) \setminus E_2 \neq \emptyset \\ \text{и } \mu \text{ является } A\text{-основанием для } M. \end{gathered} \tag{4.59}$$

Тогда найдутся s', T, $s' \in \mathbb{N}$, $T \in \mathbb{N}$, найдутся γ_i', $\gamma_i' \in C(M)$, $i = 1, 2, \ldots, k'$, $\gamma_1', \gamma_2', \ldots, \gamma_{s'}'$ – линейно независимы над $R_2(\mu)$ и найдется C', $C' \subseteq C(S(M))$,

$|C'| < \infty$, *такие, что*

$$C(A(M)) = C' + \left(\sum_{i=1}^{s'} \mu^T R_2(\mu)\gamma_i' \right) \cap \mathfrak{L}_c.$$

Доказательство приведенной леммы без труда можно получить из доказательства упомянутой выше леммы 4.5.4 предыдущего параграфа.

Заметим также, что найдется натуральное число T_0 такое, что для любых констант γ_i', $\gamma_i' \in A(M)$, выполнено:

$$\left(\sum_{i=1}^{s'} \mu^{T_0} R_2(\mu)\gamma_i' \right) \cap \mathfrak{L}_c \subseteq C(A(M)).$$

Отсюда и из приведенной леммы получаем для некоторого конечного множества констант C'', $C'' \subseteq C(S(M))$ следующее равенство.

$$C(A(M)) = C'' + \left(\sum_{i=1}^{s'} \mu^{T+T_0} R_2(\mu)\gamma_i' \right) \cap \mathfrak{L}_c.$$

Нетрудно видеть, что множество $U(A(M))$ является $A^{(1)}$-замкнутым. Поэтому по теореме 4.1.4 из параграфа 4.1 множество $U(A(M))$ $A^{(1)}$-порождено некоторым своим конечным подмножеством M', которое содержится в $U(M)$, потому что ввиду свойств (4.59), выполнено:

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

Поэтому конечное множество $M' \cup \{x_1 + x_2\}$ A-порождает $U(A(M))$.

Множество

$$\left(\sum_{i=1}^{s'} \mu^{T+T_0} R_2(\mu)\gamma_i' \right) \cap \mathfrak{L}_c$$

A-порождается множеством $U(M) \cup \Gamma' \cup \{x_1 + x_2\}$, где через Γ' обозначено множество

$$\{\ \gamma_i' \mid i = 1, 2, \ldots, s'\ \}.$$

Поэтому множество $C(A(M))$ A-порождается множеством

$$\{x_1 + x_2\} \cup M' \cup \Gamma' \cup C''.$$

Учитывая равенство

$$A(M) = A\left(\{x_1 + x_2\} \cup U(M) \cup C(M)\right) =$$

$$A\left(\{x_1 + x_2\} \cup M' \cup \Gamma' \cup C''\right),$$

получаем A-конечнопорожденность множества $A(M)$.

Таким образом, доказана первая часть следующей теоремы.

Теорема 4.6.1. *1. Если для множества M имеют место свойства (4.59), то $A(M)$ является A-конечнопорожденным.*

2. Множество, состоящее из всех A-замкнутых классов M, удовлетворяющих свойствам (4.59), счетно.

Доказательство части 2 теоремы вытекает из первого ее утверждения и существования счетного числа попарно различных A-замкнутых классов $\tilde{M}_i$, со свойствами

$$\tilde{M}_i \subseteq \mathfrak{L},\ \ x_1 + x_2 \in A(M_i),\ \ U(\tilde{M}_i) \setminus E_2 \neq \emptyset,\ \ i = 1, 2, \ldots.$$

Для этого положим

$$\tilde{M}_i = A\left(\left\{\ x_1 + x_2,\ \ \xi^i x\ \right\}\right).$$

и необходимый пример получен.

Теорема доказана.

Вырожденные системы ЛА, содержащие сумматор в A-замыкании, не всегда конечнопорождены. Так, A-замыкание никакого конечного подмножества множества

$$M,\ \ M = A\left(\left\{x_1 + x_2, \xi^i | i = 0, 1, \ldots\right\}\right),$$

где, как и ранее, через ξ^i обозначена константа

$$\underbrace{0, \ldots, 0}_{i \text{ нулей}}, 1, 0, 0, \ldots,$$

не совпадает с M.

Глава 5

О полноте в некоторых содержательных классах

В настоящее время продолжается изучение широкого спектра свойств класса конечных автоматов, как, например, в работах [25], [28], [26]. Также не ослабевает внимание исследователей к вопросам выразимости в этом классе, ставшими уже классическими. При этом допускаются различные варианты операций. Задачам выразимости автоматов через операции суперпозиции посвящены работы [46], [11], [12].

Изучение выразительных свойств в классе P всех конечных автоматов по операциям композиции [42] затруднено в связи алгоритмической неразрешимостью проблемы полноты [38] и аппроксимационной полноты [17], а также континуальностью числа максимальных подклассов [40]. Поэтому интерес представляют содержательные подклассы P, для которых проблема полноты конечных подмножеств алгоритмически разрешима. К ним относится, например, подкласс $\mathfrak{L}$ линейных автоматов [77], [78], рассмотренный в предыдущих главах.

В первом параграфе настоящей главы решена задача о полноте в классе линейных автоматов с операциями суперпозиции. Найдены все предполные классы в нем. Выполнено сравнение операторов K-замыкания и S-замыкания. Во втором параграфе рассмотрен класс линейных 2-адических автоматов с операциями композиции. Получен алгоритм проверки полноты конечных подмножеств таких автоматов. Найдены все предполные классы, число которых оказалось счетным.

5.1. Линейные автоматы с операциями суперпозиции

5.1.1. Предполные классы по операциям суперпозиции

Все необходимые определения были даны в предыдущих главах. В настоящей главе, как и в главах 3, 4, мы рассматриваем линейные автоматы над полем E_2, составляющие класс $\mathfrak{L}_2$. Каждый линейный автомат f из $\mathfrak{L}_2$ с входными переменными $x_1, x_2, \ldots, x_n$ задает отображение из $R_2(\xi)^n$ в $R_2(\xi)$, где через $R_2(\xi)$ мы обозначаем множество всех формальных степенных рядов переменной ξ с коэффициентами из поля E_2,

$$R_2(\xi) = \left\{ \sum_{t=0}^{\infty} a(t)\xi^t \mid a(t) \in E_2, \ t = 0, 1, \ldots \right\}.$$

Для каждого линейного автомата $f(x_1, x_2, \ldots, x_n)$ имеет место разложение (1.9), в котором μ_i являются элементами множества $E_2'(\xi)$,

$$E_2'(\xi) = \Bigg\{ \alpha \mid \alpha \in R_2(\xi), \ \sum_{t=0}^{\infty} a(t)\xi^t, \ \text{последовательность коэффициентов}$$

$$a(0), a(1), \ldots \ \text{является периодической (с предпериодом)} \ \Bigg\}$$

Ранее, в главах 1 и 2, была, в частности, решена задача K-полноты в классе линейных автоматов $\mathfrak{L}_2$ с операциями композиции K [68]. В этом классе были найдены все K-предполные классы, число которых оказалось счетным. В настоящем параграфе рассматривается задача полноты для класса $\mathfrak{L}_2$ линейных автоматов с операциями суперпозиции S. Найдены все S-предполные классы, число которых, как и в случае K-замыкания, оказалось счетным. Множество, состоящее из всех S-предполных классов является приведенной S-критериальной системой.

Как и ранее, замыкание множества M, $M \subseteq \mathfrak{L}$, по операциям суперпозиции будем обозначать $S(M)$. Множество M, $M \subseteq \mathfrak{L}$, называется S-замкнутым, если $S(M) = M$. Множество M, $M \subseteq \mathfrak{L}$, называется S-полным, если $S(M) = \mathfrak{L}$. Множество M, $M \subset \mathfrak{L}$, называется S-предполным, если M не является S-полным, но для любой f, $f \in \mathfrak{L} \setminus M$, множество $M \cup \{f\}$ является S-полным. Множество S-замкнутых классов Ω называется S-критериальной системой в точности тогда, когда для любого множества M, $M \subseteq \mathfrak{L}$, равенство $S(M) = \mathfrak{L}$ равносильно невключению множества M ни в один из классов θ, $\theta \in \Omega$. S-критериальная система Ω называется приведенной, если из нее нельзя удалить ни одного класса так, чтобы оставшееся множество составляло критериальную систему.

Для ЛА $f\,(x_1, x_2, \ldots, x_n)$, задаваемого равенством (1.9), переменная x_i называется *непосредственной*, если μ_i, будучи представленной в несократимом виде, имеет числитель со свободным членом 1.

Как и в случае задачи о K-полноте, здесь нам понадобятся классы T_0, T_1, V_1, V_2 и M_1, введенные в параграфе 1 главы 1. В параграфе 3 главы 1 были введены классы одноместных линейных автоматов $\tilde{M}_i^{(1)}$, которые мы используем для определения следующих множеств:

$$\tilde{M}_0 = \left\{\; f \;\mid\; U(f) \subset \tilde{M}_0^{(1)} \;\right\},$$
$$\tilde{M}_i = \left\{\; f \;\mid\; U(f) \subset \tilde{M}_i^{(1)} \;\right\},$$

$i = 2, 3, \ldots$.

Через J_2^S обозначим следующее множество:

$$\left\{\; T_0, T_1, V_1, V_2, M_1, \tilde{M}_i \;\mid\; i = 0, 2, 3, \ldots \;\right\}.$$

Через $\mathfrak{L}_0^{(1)}$, как и прежде, мы обозначаем множество всех одноместных линейных автоматов, сохраняющих нулевую последовательность. Таким образом, для любой $f(x)$, $f(x) \in \mathfrak{L}_0^{(1)}$, найдется дробь μ, $\mu \in E_2'(\xi)$, такая, что для любого ряда α, $\alpha \in R_2$, выполнено: $f(\alpha) = \mu \cdot \alpha$.

Лемма 5.1.1. *Пусть $M \subseteq \mathfrak{L}$ и для любого θ, $\theta \in J_2^S$, выполнено: $M \not\subseteq \theta$. Тогда $x_1 + x_2 + x_3 \in S(M)$.*

Доказательство. В параграфе 3 главы 1 введены классы $R_i^{(1)}$, $i = 0, 1, \ldots$, $M_i^{(1)}$, $i = 0, 1, \ldots$, одноместных линейных автоматов. Согласно теореме 1.3.2

множество $J_2^{(1)}$,

$$J_2^{(1)} = \left\{ \ M_i^{(1)}, \ \ R_i^{(1)} \ \mid \ i = 0, 1, \dots \ \right\}$$

является приведенной $K^{(1)}$-критериальной системой в $\mathfrak{L}_0^{(1)}$.

Пусть $M \subseteq \mathfrak{L}$ и для любого θ, $\theta \in J_2^S$, выполнено: $M \not\subseteq \theta$.

Заметим, что тогда $U(M)$ не содержится и ни в одном множестве из $J_2^{(1)}$. Поэтому для некоторых μ_1 и μ_2 из $S^{(1)}(U(M))$ выполнено:

$$1 = \mathrm{fb}\left(\mu_1, \mu_2\right).$$

(Через $S^{(1)}$ мы, как и прежде, обозначаем замыкание множества M по операциям сложения и умножения.) Поэтому $1 = \mu_1 + \mu_2$ и из элементов множества $U(M)$ с использованием операций сложения и умножения выразима единица, то есть

$$1 \in S^{(1)}(U(M)). \tag{5.1}$$

Найдется $f\left(x_1, x_2, \dots, x_n\right) \in M \setminus V_1$. Не ограничивая общности рассуждений, будем считать переменные x_1 и x_2 ЛА $f\left(x_1, x_2, \dots, x_n\right)$ непосредственными. Положим

$$g\left(x_1, x_2, x_3\right) = f\left(x_1, x_2, x_3, x_3 \dots, x_3\right),$$

$$h_1\left(x_1, x_2, x_3\right) = g\left(g\left(x_3, x_1, x_3\right), g\left(x_2, x_3, x_3\right), x_3\right).$$

Тогда для некоторых μ, μ_1 и μ_0 из $E_2'(\xi)$ имеем:

$$h_1\left(x_1, x_2, x_3\right) = \mu \cdot x_1 + \mu \cdot x_2 + \mu_1 x_3 + \mu_0,$$

и при этом $\mu \in 1 + \xi E_2'(\xi)$.

Если $\mu = 1$, то $h_1\left(x_1, h_1\left(x_2, x_3, x\right), x\right) = x_1 + x_2 + x_3 \in S(M)$, что и требуется доказать. Поэтому в дальнейшем предполагаем, что $\mu \neq 1$.

Используя операции суперпозиции, для каждого натурального k и некоторых μ', μ_0', μ', $\mu_0' \in E_2'(\xi)$, из ЛА $h_1\left(x_1, x_2, x_3\right)$ можно получить ЛА

$$h_k\left(x_1, x_2, \dots, x_{2^k}, x\right) = \mu^k \cdot x_1 + \mu^k \cdot x_2 + \dots + \mu^k \cdot x_{2^k} + \mu' \cdot x + \mu_0'.$$

Заметим, что множество

$$J_{\mu}^{(1)} = \left\{ \ \theta \ \mid \ \theta \in J_2^{(1)}, \ \ \mu \in \theta \ \right\}$$

конечно.

Далее, положим

$$I = \left\{ \ j \ \mid \ j \in \mathbb{Z}_+, \ \ \mu \in M_j^{(1)} \cup R_j^{(1)} \ \right\}.$$

Пусть $m = |I|$, $I = \{j_1, j_2, \ldots, j_m\}$ и натуральное число k_0 таково, что $2^{k_0} \geq 2m + 2$. Для каждого i, $i \in \{1, 2, \ldots, m\}$, найдется μ_i^*, $\mu_i^* \in U(M)$, и найдется целое неотрицательное число r_i такое, что

$$(\mu_i^*)^{r_i} \cdot \mu^{k_0} \not\subseteq M_{j_i}^{(1)} \cup R_{j_i}^{(1)}.$$

Из ЛА h_{k_0} и ЛА множества M, используя операции суперпозиции, можно получить ЛА $h\left(x_1, x_2, \ldots, x_{m+1}, y_1, y_2, \ldots, y_{m+1}, x\right)$,

$$h\left(x_1, x_2, \ldots, x_{m+1}, y_1, y_2, \ldots, y_{m+1}, x\right) = \mu^{k_0} \cdot x_1 + \sum_{i=1}^{m} (\mu_i^*)^{r_i} \cdot \mu^{k_0} \cdot x_{i+1} +$$

$$\mu^{k_0} \cdot y_1 + \sum_{i=1}^{m} (\mu_i^*)^{r_i} \cdot \mu^{k_0} \cdot y_{i+1} + \mu'' \cdot x + \mu_0''.$$

Имеем:

$$h\left(x_1, x_2, \ldots, x_{m+1}, y_1, y_2, \ldots, y_{m+1}, x\right) =$$
$$\sum_{i=1}^{m+1} \tilde{\mu}_i \cdot x_i + \sum_{i=1}^{m+1} \tilde{\mu}_i \cdot y_i + \mu'' \cdot x + \mu_0''.$$

Положим

$$M' = \left\{ \ \tilde{\mu}_i \ \mid \ i = 1, 2, \ldots, m+1 \ \right\}.$$

Для любого θ, $\theta \in J_2^{(1)}$, справедливо:

$$M' \not\subseteq \theta.$$

Поэтому, в соответствии с (5.1), найдутся такие Π_i, $i = 1, 2, \ldots, l$, полученные из элементов множества M' с использованием лишь операции подстановки, что

$$1 = \sum_{i=1}^{l} \Pi_i. \tag{5.2}$$

Из ЛА h с использованием операций суперпозиции можно получить ЛА h',

$$h'\left(x_{1,1}, x_{1,2}, \ldots, x_{1,l}, x_{2,1}, x_{2,2}, \ldots, x_{2,l}, \ldots, x_{m+1,1}, x_{m+1,2}, \ldots, x_{m+1,l},\right.$$

$$\left.y_{1,1}, y_{1,2}, \ldots, y_{1,l}, y_{2,1}, y_{2,2}, \ldots, y_{2,l}, \ldots, y_{m+1,1}, y_{m+1,2}, \ldots, y_{m+1,l}, x\right) =$$
$$\sum_{i=1}^{m+1}\sum_{j=1}^{l} \tilde{\mu}_i{}^{2^l} \cdot x_{i,j} + \sum_{i=1}^{m+1}\sum_{j=1}^{l} \tilde{\mu}_i{}^{2^l} \cdot y_{i,j} + \tilde{\mu} \cdot x + \tilde{\mu}_0.$$

Из ЛА h', используя операции суперпозиции, получаем ЛА

$$\hat{h}\left(x_1, x_2, \ldots, x_l, y_1, y_2, \ldots, y_l, x\right) =$$

$$\Pi_1^{2^l} \cdot x_1 + \Pi_2^{2^l} \cdot x_2 + \ldots \Pi_l^{2^l} \cdot x_l + \Pi_1^{2^l} \cdot y_1 + \Pi_2^{2^l} \cdot y_2 + \ldots \Pi_l^{2^l} \cdot y_l + \hat{\mu} \cdot x + \hat{\mu}_0.$$

Из (5.2) следует:

$$1 = \sum_{i=1}^{l} \Pi_i^{2^l}.$$

Поэтому для ЛА $\check{h}$,

$$\check{h}\left(x_1, x_2, x\right) = \hat{h}\left(\underbrace{x_1, x_1, \ldots, x_1}_{l \text{ раз } x_1}, x_2, x_2, \ldots, x_2, x\right),$$

имеем:

$$\check{h}\left(x_1, x_2, x\right) = x_1 + x_2 + \hat{\mu} \cdot x + \hat{\mu}_0.$$

Отсюда,

$$\check{h}\left(x_1, \check{h}\left(x_2, x_3, x\right), x\right) = x_1 + x_2 + x_3 \in S(M).$$

Лемма 5.1.1 доказана.

Лемма 5.1.2. *Пусть $M \subseteq \mathfrak{L}$ и для любого θ, $\theta \in J_2^S$, выполнено: $M \not\subseteq \theta$. Тогда для любого натурального k выполнено:*

$$x_0 + \xi x_1 + \xi^2 x_2 + \ldots + \xi^k x_k + \xi y_1 + \xi^2 y_2 + \ldots + \xi^k y_k \in S(M).$$

Доказательство. Пусть $M \subseteq \mathfrak{L}$ и для любого θ, $\theta \in J_2^S$, выполнено: $M \not\subseteq \theta$. Тогда, что упоминалось выше, для любого θ, $\theta \in J_2^{(1)}$, справедливо: $U(M) \not\subseteq \theta$. Поэтому, как показано в [68], найдется дробь μ_0, $\mu_0 \in 1 + \xi E_2'(\xi)$, и найдется целое неотрицательное число k такие, что $\xi^k \mu_0$ и $\xi^{k+1}\mu_0$ можно получить из элементов множества $U(M)$ с использованием операций сложения и умножения.

Пусть $\mu_0 = u_0/v_0$.

В случае $\deg u_0 < \deg v_0$ через μ' и μ'' обозначим соответственно дроби из $U(M) \setminus M_0$ и $U(M) \setminus \xi E_2'(\xi)$, которые существуют ввиду соотношений $M \not\subset \tilde{M}$ и $M \not\subseteq V_1$.

В множестве $\{\mu', \mu'', \mu' + \mu''\}$ найдется дробь μ^* такая, что $\mu^* \notin M_0 \cup \xi E_2'(\xi)$. Положим

$$\mu_1 = \begin{cases} \mu_0, & \text{если} \quad \deg u_0 \geq \deg v_0, \\ \mu_0 \cdot (\mu^*)^{\deg v_0 - \deg u_0}, & \text{если} \quad \deg u_0 < \deg v_0. \end{cases}$$

Для μ_1, $\mu_1 = u_1/v_1$, имеем: $\deg u_1 \geq \deg v_1$ и $\mu_1 \in 1 + \xi E_2'(\xi)$.

Дроби $\xi^k \mu_1$, $\xi^{k+1}\mu_1$ могут быть получены из элементов множества $U(M)$ с использованием операций сложения и умножения.

Из [68] тогда следует, что найдутся такие $\mu_2 = u_2/v_2$ и T, $\mu_2 \in 1 + \xi E_2'(\xi)$, $T \in \mathbb{Z}_+$, что для любого целого неотрицательного числа l, $l \geq T$ выполнено:

$$\xi^l \mu_2 \in S^{(1)}(U(M)).$$

Отсюда, для любого целого неотрицательного числа l, $l \geq T$ выполнено:

$$\xi^l u_2 \in S^{(1)}(U(M)). \tag{5.3}$$

В дальнейшем, не ограничивая общности рассуждений, будем предполагать, что $T \geq 2$. Из $M \not\subseteq M_1$ вытекает существование таких a и μ_3, что $a \in E_2$, $\mu_3 \in E_2'(\xi)$, $\mu_3 = u_3/v_3$ и

$$a + \xi + \xi^2 \mu_3 \in U(M).$$

Далее, нетрудно видеть, что для некоторого $\mu_3' = u_3'/v_3'$ справедливо:

$$\xi + \xi^T \mu_3' \in S^{(1)}\left(\{\mu_3\}\right) \tag{5.4}$$

Представим многочлены u_2 и v_3' произведением неприводимых многочленов:

$$u_2 = p_{i_1}^{j_1} \cdot p_{i_2}^{j_2} \cdot \dots \cdot p_{i_k}^{j_k},$$

$$v_3' = p_{i_1'}^{j_1'} \cdot p_{i_2'}^{j_2'} \cdot \dots \cdot p_{i_r'}^{j_r'},$$

Через μ_k^* обозначим дробь, которая содержится в $U(M) \setminus \tilde{M}_{i_k}^{(1)}$. Тогда знаменатель дроби $\tilde{\mu}_k = \tilde{u}_k / \tilde{v}_k$,

$$\tilde{\mu}_k = \left(\mu_k^*\right)^{j_k},$$

делится на $p_{i_k}^{j_k}$.

Нетрудно видеть, что из справедливости для каждого целого неотрицательного числа l, $l \geq T$, соотношения (5.3), а также соотношения

$$\xi^l \tilde{\mu}_k u_2 \in S^{(1)}(U(M))$$

следует, что для каждого целого неотрицательного числа l, $l \geq T$, выполнено соотношение

$$\xi^l p_{i_1}^{j_1} \cdot p_{i_2}^{j_2} \cdot \dots \cdot p_{i_{k-1}}^{j_{k-1}} \in S^{(1)}(U(M)).$$

Поэтому, используя индукцию, можно показать, что для каждого неотрицательного числа l, $l \geq T$, справедливо:

$$\xi^l \in S^{(1)}(U(M)).$$

Рассуждая аналогично, нетрудно доказать, что для любого s, $s \in \{1, 2, \dots, r\}$, и каждого целого неотрицательного числа l, $l \geq T$, выполнено:

$$\frac{\xi^l}{p_{i_s'}^{j_s'}} \in S^{(1)}(U(M)),$$

откуда следует, что для любого целого неотрицательного числа l, $l \geq T$, имеет место:

$$\frac{\xi^l}{v_3'} \in S^{(1)}(U(M)).$$

Поэтому

$$\xi^T \mu_3' \in S^{(1)}(U(M)),$$

а с учетом (5.4), получаем:

$$\xi \in S^{(1)}(U(M)).$$

Полученное включение означает, что для некоторых дробей Π_i, $i = 1, 2, \ldots, r$, каждая из которых получена из элементов множества $U(M)$ с использованием лишь операции умножения, выполнено:

$$\xi = \sum_{i=1}^{r} \Pi_i.$$

Поэтому найдутся μ_i' и Π_i', $\mu_i' \in U(M)$, Π_i' либо равно 1, либо может быть получено из элементов множества $U(M)$ с использованием только операции умножения, $i = 1, 2, \ldots, r$, такие, что

$$\xi = \sum_{i=1}^{r} \mu_i' \Pi_i'.$$

По лемме 5.1.1 имеем: $x_1 + x_2 + x_3 \in S(M)$. Поэтому в $E_2'(\xi)$ найдутся $\hat{\mu}$ и $\hat{\mu}_0$ такие, что линейный автомат

$$\hat{f}\left(x_1, x_2, \ldots, x_r, x\right) = \sum_{i=1}^{r} \mu_i' x_i + \hat{\mu} x + \hat{\mu}_0$$

содержится в $S(M)$.

Тогда для некоторых $\hat{\hat{\mu}}$, $\hat{\hat{\mu}}_0$ из $E_2'(\xi)$ и некоторого $\tilde{f}(x_1)$ из $\mathfrak{L}$ выполнено:

$$\hat{f}\left(\Pi_1'(x), \Pi_2'(x), \ldots, \Pi_r'(x), x_1\right) + \tilde{f}\left(x_1\right) = \xi x + \hat{\hat{\mu}} x_1 + \hat{\hat{\mu}}_0 \in S(M).$$

Далее, используя этот ЛА и сумматор от трех переменных, получаем:

$$x_0 + (\xi x_1 + \hat{\mu} x_1 + \hat{\mu}_0) + (\xi y_1 + \hat{\mu} x_1 + \hat{\mu}_0) = x_0 + \xi x_1 + \xi y_1 \in S(M). \tag{5.5}$$

Наконец, индукцией по k покажем, что для ЛА

$$g_k\left(x_0, x_1, y_1, x_2, y_2, \ldots, x_k, y_k\right) =$$

$$x_0 + \xi x_1 + \xi^2 x_2 + \ldots + \xi^k x_k + \xi y_1 + \xi^2 y_2 + \ldots + \xi^k y_k$$

выполнено:

$$g_k \in S(M), \tag{5.6}$$

$k = 1, 2, \ldots$.

При $k = 1$ включение (5.6) совпадает с (5.5). Пусть это включение выполнено при $k = r$. Тогда

$$g_{r+1}\left(x_0, x_1, y_1, x_2, y_2, \ldots, x_r, y_r, x_{r+1}, y_{r+1}\right) =$$

$$g_r\left(x_0, x_1, y_1, x_2, y_2, \ldots, x_r, y_r + \xi x_{r+1} + \xi y_{r+1}\right) \in S(M).$$

Следовательно, включение (5.6) справедливо для любого k, $k = 1, 2, \ldots$, что и требовалось.

Лемма 5.1.2 доказана.

Лемма 5.1.3. *Пусть $M \subseteq \mathfrak{L}$ и для любого θ, $\theta \in J_2^S$, выполнено: $M \not\subseteq \theta$. Тогда найдется $\hat{\mu}_0 \in E_2'(\xi)$ такая, что $\xi \cdot \hat{\mu}_0 x \in S(M)$.*

Доказательство. Рассмотрим множество M, $M \subseteq \mathfrak{L}$, такое, что для любого θ, $\theta \in J_2^S$, выполнено: $M \not\subseteq \theta$.

Найдется f, $f \in M \setminus V_2$. Тогда для ЛА $g(x)$,

$$g(x) = f\left(x, x, \ldots, x\right),$$

найдутся дроби $\tilde{\mu}$ и $\tilde{\mu}_0$ такие, что

$$g(x) = \tilde{\mu}x + \tilde{\mu}_0$$

и $\tilde{\mu}(0) = 0$, то есть единственная входная переменная $\tilde{\mu}$ не является непосредственной.

Пусть $\tilde{\mu}_0(0) = a$, $a \in E_2$.

В M содержится ЛА f', не сохраняющий число a в первый момент времени. Тогда выход ЛА $h(x) = f'(g(x), g(x), \ldots, g(x))$ в начальный момент не зависит от значения входа в начальный момент времени и равен $\bar{a}$.

Для определенности будем считать, что $a = 0$. В $E_2'(\xi)$ найдутся μ_i, μ_i', $i = 0, 1$, такие, что $g(x) = \mu_0 x + \mu_0'$ и $h(x) = \mu_1 x + \mu_1'$, при этом

$$\mu_i(0) = 0, \;\; \mu_i'(0) = i, \;\; i = 0, 1.$$

Для некоторых многочленов u_i и v_i имеют место равенства: $\mu_i' = u_i/v_i$, $i = 0, 1$, причем $u_i(0) = i$, $i = 0, 1$.

Далее воспользуемся тождеством:

$$u_1 v_0 \mu_0' + u_0 v_1 \mu_1' = 0.$$

Найдутся числа s, a_i, b_i, $s \in \mathbb{N}$, $a_i \in E_2$, $b_i \in E_2$, $i = 1, \ldots, s$, такие, что выполнены тождества:

$$u_1 v_0 = 1 + \sum_{i=1}^{s} a_i \xi^i \;\text{ и}$$

$$u_0 v_1 = \sum_{i=1}^{s} b_i \xi^i.$$

По лемме 5.1.2 в $K(M)$ содержится ЛА

$$g_s\left(x_0, x_1, y_1, x_2, y_2, \ldots, x_s, y_s\right) =$$

$$x_0 + \xi x_1 + \xi^2 x_2 + ... + \xi^s x_s + \xi y_1 + \xi^2 y_2 + ... + \xi^s y_s.$$

Из ЛА $g_s\left(x_0, x_1, y_1, x_2, y_2, \ldots, x_s, y_s\right)$, $g(x)$ и $h(x)$ построим одноместный ЛА следующим образом. Вместо переменной x_i ЛА $g_s\left(x_0, x_1, y_1, x_2, y_2, \ldots, x_s, y_s\right)$ подставим $g(x)$ для $i = 0$ и для таких i, что $a_i = 1$. Вместо переменной y_i этого же ЛА подставим $h(x)$ для таких i, что $b_i = 1$. Все переменные, вместо которых не подставлен ни $g(x)$, ни $h(x)$, переименуем в x. Для полученного ЛА $\hat{g}\left(x\right)$ найдется $\hat{\mu}_0 \in E_2'(x)$ такая, что

$$\hat{g}\left(x\right) = \xi \cdot \hat{\mu}_0 x \in S(M).$$

Лемма 5.1.3 доказана.

Лемма 5.1.4. *Пусть $M \subseteq \mathfrak{L}$ и для любого θ, $\theta \in J_2^S$ выполнено: $M \not\subseteq \theta$. Тогда*

$$\{\ x_1 + x_2,\ \ \xi \cdot x\ \} \subset S(M). \tag{5.7}$$

Доказательство. По лемм 5.1.3 найдется $\hat{\mu}_0 \in E_2'(\xi)$ такая, что

$$\xi \cdot \hat{\mu}_0 x \in S(M). \tag{5.8}$$

Если $\hat{\mu}_0 = 0$, то $S(M)$ содержит константу 0. Тогда, учитывая лемму 5.1.1, получаем:

$$x_1 + x_2 + 0 = x_1 + x_2 \in S(M),$$

а по лемме 5.1.2,

$$0 + \xi x + \xi 0 = \xi x \in S(M),$$

что требуется доказать.

Поэтому далее предполагаем, что $\hat{\mu}_0 \neq 0$.

По лемме 5.1.2 в $K(M)$ содержится ЛА

$$g_{k+1}\left(x_0, x_1, y_1, x_2, y_2, \ldots, x_{k+1}, y_{k+1}\right) =$$

$$x_0 + \xi x_1 + \xi^2 x_2 + ... + \xi^{k+1} x_{k+1} + \xi y_1 + \xi^2 y_2 + ... + \xi^{k+1} y_{k+1}.$$

Пусть u^* – какой-то многочлен из $E_2[\xi]$, $u^* = \sum_{i=0}^{k} a_i \xi^k$. Для каждого i, $i = 0, 1, \ldots, k$, в случае, если $a_i = 1$, вместо переменной x_{i+1} ЛА

$$g_{k+1}\left(x_0, x_1, y_1, x_2, y_2, \ldots, x_{k+1}, y_{k+1}\right)$$

подставим $\xi \hat{\mu}_0 x_{i+1}$. Далее переименуем переменные x_1, y_1, x_2, y_2, $\ldots$, x_{k+1}, y_{k+1} полученного ЛА в переменную x. Получим ЛА от двух переменных:

$$x_0 + \xi u^* \left(1 + \xi \hat{\mu}_0\right) x.$$

Таким образом, для любого многочлена u^* имеем:

$$x_0 + \xi u^* \left(1 + \xi \hat{\mu}_0\right) x \in S(M).$$

Если $\hat{\mu}_0 = u_0/v_0$, $v_0 = 1 + \xi v_0'$, то из предыдущего утверждения следует, что для любого многочлена u^* выполнено:

$$x_0 + \xi u^* \left(1 + \xi \left(u_0 + v_0'\right)\right) x \in S(M). \tag{5.9}$$

Разложим многочлен $1+\xi\left(u_0 + v_0'\right)$ в произведение неприводимых многочленов:

$$1 + \xi\left(u_0 + v_0'\right) = p_1^{i_1} \cdot p_2^{i_2} \cdot \ldots p_k^{i_k},$$

где для каждого j, $j \in \{1, 2, \ldots, k\}$, выполнено: $p_j \neq \xi$.

Для каждого j, $j \in \{1, 2, \ldots, k\}$, справедливо: $M \not\subseteq \tilde{M}_i$. Поэтому в M найдется ЛА f_j такой, что для некоторой несократимой дроби $\check{\mu}_j = \check{u}_j/\check{v}_j$, $\check{\mu}_j \in U(f_j)$, многочлен p_j делит $\check{v}_j$.

Используя операции суперпозиции, из ЛА $x_1 + x_2 + x_3$ и ЛА f_j для любого натурального n можно получить ЛА $x_1 + (\check{\mu}_j)^n x_2 + (\check{\mu}_j)^n x_3$.

Отсюда и из (5.8) следует, что для любого n, $n \in \mathbb{N}$, справедливо:

$$\left(1 + \left(1 + \xi\hat{\mu}_0\right)(\check{\mu}_j)^n\right) x \in K(M).$$

Найдется такое натуральное число n_0, что при $n = n_0$ числитель дроби $\tilde{\mu}_{j,n}$,

$$\tilde{\mu}_{j,n} = \left(1 + \xi\left(u_0 + v_0'\right)\right)\left(1 + \left(1 + \xi\hat{\mu}_0\right)(\check{\mu}_j)^n\right)$$

не делится на p_j.

Числитель дроби $\tilde{\mu}_{j,n_0}$ обозначим через $\tilde{u}_j$. Из (5.9) следует, что для любого многочлена u_j^* справедливо соотношение:

$$x_0 + \xi u_j^* \tilde{u}_j x_1 \in S(M).$$

Отсюда и из (5.9) для любых многочленов u^*, u_1^*, u_2^*, …, u_k^*, выполнено:

$$x + \xi u^* \left(1 + \xi\left(u_0 + v_0'\right)\right) x_0 + \sum_{j=1}^{k} \xi u_j^* \tilde{u}_j x_j \in S(M).$$

Поэтому для любого u^*, $u^* \in E_2[\xi]$, справедливо:

$$x + \xi u^* x_1 \in S(M). \tag{5.10}$$

Далее, знаменатель дроби $\hat{\mu}_0$, $\hat{\mu}_0 = u_0/v_0$, представим в виде произведений различных неприводимых многочленов:

$$v_0 = q_1^{r_1} q_2^{r_2} \ldots q_s^{r_s}.$$

Согласно изложенному выше, для каждого j, $j \in \{1, 2, \ldots, s\}$, в $U(M)$ найдется дробь $\hat{\mu}_j$, знаменатель которой делится на q_j. Поэтому знаменатель дроби $1 + (1 + \xi\hat{\mu}_0)\,\hat{\mu}_j^{r_j}$ делится на $q_j^{r_j}$.

Из предыдущих рассуждений следует, что

$$x_1 + \hat{\mu}_j^{r_j} x_2 + \xi\hat{\mu}_0\hat{\mu}_j^{r} x_2 \in S(M). \tag{5.11}$$

Дробь $1 + (1 + \xi\hat{\mu}_0)\,\hat{\mu}_j^{r_j}$ обозначим через μ'_j. Из (5.10) и (5.11) вытекает, что для любого многочлена u_j^* выполнено:

$$x + \xi\mu'_j u_j^* x_j \in S(M). \tag{5.12}$$

Пусть $\mu'_j = u'_j/v'_j$. Из (5.12) и делимости многочлена v'_j на $q_j^{r_j}$ для любого многочлена u_j^* следует включение:

$$x + \xi u_j^* \frac{u'_j}{q_j^{r_j}} x_j \in S(M).$$

Поэтому для любых многочленов u^*, u_j^*, $j = 1, 2, \ldots, s$ выполнено:

$$x + \xi \cdot \left(u^* + \sum_{j=1}^{s} u_j^* \frac{u'_j}{q_j^{r_j}} \right) x_1 \in S(M).$$

Найдутся такие многочлены u'', u''_j, $j = 1, 2, \ldots, s$, что выполнено равенство:

$$u'' + \sum_{j=1}^{s} u''_j \frac{u'_j}{q_j^{r_j}} = u_0/v_0.$$

Следовательно,

$$x + \xi\hat{\mu}_0 x_1 \in S(M).$$

Отсюда и из (5.8) получаем: $0 \in S(M)$. Поэтому, согласно рассуждениям, приведенным в начале доказательства леммы 5.1.4, заключаем, что (5.7) справедливо.

Лемма 5.1.4 доказана.

Имеет место:

Теорема 5.1.1. *Множество J_2^S является приведенной S-критериальной системой в $\mathfrak{L}$, состоящей из S-предполных классов.*

Доказательство. Нетрудно видеть, что каждый элемент множества J_2^S является S-замкнутым классом в $\mathfrak{L}$, не совпадающим с $\mathfrak{L}$.

Докажем сначала, что J_2^S – S-критериальная система. Пусть $M \subseteq \mathfrak{L}$ и для любого θ, $\theta \in J_2^S$, выполнено: $M \not\subseteq \theta$. Тогда по лемме 5.1.4 выполнено (5.7).

Понятно, что для любого многочлена u, $u \in E_2[\xi]$, из ЛА $x_1 + x_2$ и ξx с использованием операций суперпозиции может быть получен ЛА $u \cdot x$.

Пусть $u/v \in E_2'(\xi)$. Представим многочлен v в виде произведения неприводимых многочленов:

$$v = q_1^{i_1} q_2^{i_2} \dots q_s^{i_s}.$$

Для каждого j, $j \in \{1, 2, \dots, s\}$, в M содержится ЛА f_j такой, что для некоторого μ_j, $\mu_j \in U(f)$, $\mu_j = u_j/v_j$, многочлен v_j делится на q_j. Имеют место включения:

$$\mu_j x \in S\left(\{f_j, x_1 + x_2\}\right),$$

$j = 1, 2, \dots, s$. Поэтому

$$\left(\mu_j\right)^{i_j} x \in S(M),$$

$j = 1, 2, \dots, s$, причем знаменатель дроби $\left(\mu_j\right)^{i_j} = u_j^*/v_j^*$ делится на $q_j^{i_j}$. Тогда для любого j, $j \in \{1, 2, \dots, s\}$, найдется многочлен u_j' такой, что выполнено: $\left(\mu_j\right)^{i_j} u_j' = u_j^*/q_j^{i_j}$. Следовательно,

$$u_j^*/q_j^{i_j} x \in S(M),$$

$j = 1, 2, \dots, s$.

Далее, для некоторых многочленов $\tilde{u}_j$ имеет место равенство:

$$\sum_{j=1}^{s} \tilde{u}_j \frac{u_j}{q_j^{i_j}} = \frac{u}{v}.$$

Поэтому

$$\frac{u}{v}x \in S(M).$$

Пусть теперь $f(x_1, x_2, \ldots, x_n)$ – какой-нибудь ЛА из $\mathfrak{L}$. Тогда для некоторых μ_i, $i = 0, 1, \ldots, n$, выполнено разложение (1.9). Из только что доказанного вытекают включения:

$$\mu_i x_i \in S(M), \tag{5.13}$$

$i = 1, 2, \ldots, n$.

Из доказательства леммы 5.1.3 следует, что в $S(M)$ содержится ЛА $h(x)$ такой, что для любого α, $\alpha \in R_2$, выполнено: $h(\alpha)(0) = 1$. Следовательно, для некоторых многочленов u и v в $S(M)$ содержится константный ЛА $h(x+x) = \hat{u}/\hat{v}$, причем $\hat{u}/\hat{v} \in 1 + \xi E_2'(\xi)$. Но, что ранне доказано,

$$\frac{\hat{v}}{\hat{u}}\mu_0 x \in S(M).$$

Отсюда получаем:

$$\mu_0 = \frac{\hat{v}}{\hat{u}}\mu_0\frac{\hat{u}}{\hat{v}} \in S(M).$$

Учитывая это, а также (5.13) и включение $x_1 + x_2 \in S(M)$, получаем:

$$f(x_1, x_2, \ldots, x_n) \in S(M),$$

т.е. J_2^S является S-критериальной системой.

Теперь каждому S-замкнутому классу θ из множества J_2^S сопоставим множество $\hat{\theta}$ ЛА следующим образом.

$$\hat{T}_0 = \left\{\ x_1 + x_2,\ \ \xi \cdot x,\ \ \frac{1}{p_i}x\ \mid\ i = 2, 3, \ldots\ \right\},$$

$$\hat{T}_1 = \left\{\ x_1 + x_2 + 1,\ \ \xi \cdot x + 1,\ \ \frac{1}{p_i}x\ \mid\ i = 2, 3, \ldots\ \right\},$$

$$\hat{V}_1 = \left\{\ 1,\ \ 0,\ \ \xi \cdot x,\ \ \frac{1}{p_i}x\ \mid\ i = 2, 3, \ldots\ \right\},$$

$$\hat{V}_2 = \left\{\ x + 1,\ \ x_1 + x_2 + x_3,\ \ \xi \cdot x_1 + x_2,\ \ \frac{1}{p_i}x\ \mid\ i = 2, 3, \ldots\ \right\},$$

$$\hat{\hat{M}}_0 = \left\{ \; x+1, \;\; x_1+x_2, \;\; \frac{1}{1+\xi}x, \;\; \frac{1}{p_i}x \;\mid\; i=2,3,\ldots \; \right\},$$

$$\hat{M}_1 = \left\{ \; x+1, \;\; x_1+x_2, \;\; \xi^2 \cdot x, \;\; \frac{1}{p_i^2}x \;\mid\; i=2,3,\ldots \; \right\},$$

$$\hat{\hat{M}}_j = \left\{ \; x+1, \;\; x_1+x_2, \;\; \xi \cdot x, \;\; \frac{1}{p_i}x \;\mid \right.$$
$$\left. i=2,3,\ldots j-1, j+1, j+2, \ldots \; \right\},$$

$j = 2, 3, \ldots .$

Несложной проверкой можно убедиться, что для любых различных замкнутых классов θ и θ' из J_2^S имеют место соотношения:

$$\hat{\theta} \subseteq \theta,$$

$$\hat{\theta} \not\subseteq \theta'.$$

Из этого следует, что удаление из J_2^S какого-либо замкнутого класса приводит к множеству, не являющемуся S-критериальной системой, следовательно, J_2^S – приведенная S-критериальная система. Следуя известным рассуждениям [42], заключаем, что каждый элемент множества J_2^S является S-предполным классом.

Теорема доказана.

Следствие 4. *Множество J_2^S содержит все S-предполные классы и состоит только из S-предполных классов.*

5.1.2. Сравнение операторов замыкания в классе линейных автоматов

Известно [42], что в классе P всех конечных автоматов любое подмножество, не являющееся полным по операциям композиции, расширяется до K-предполного класса. В работе [11] в P найден класс, который не расширяется до предполного по операциям суперпозиции. Тем самым, найдено новое существенное отличие двух операторов замыкания в классе конечных автоматов. В настоящем параграфе проводится сравнение этих операторов замыкания, а также оператора аппроксимационного замыкания, в классе линейных автоматов.

В параграфе 1 настоящей главы найдено множество J_2^S всех S-предполные классы в классе $\mathfrak{L}$ линейных автоматов. Несложным следствием из этого является отсутствие конечных S-полных множеств в $\mathfrak{L}$. Нетрудно также привести примеры бесконечных счетных S-базисов и бесконечных S-полных множеств, из которых нельзя выделить S-базис.

В главе 1 показано, что конечное множество J_2^A состоит из всех A-предполных классов в $\mathfrak{L}$. В главе 2, в частности, найдено счетное множество J_2 всех K-предполных классов в $\mathfrak{L}$, но при этом, конечно, в $\mathfrak{L}$ имеются конечные K-полные системы.

Справедлива следующая теорема.

Теорема 5.1.2. *Каждый A-предполный класс в $\mathfrak{L}$ является S-предполным и K-предполным. В $\mathfrak{L}$ каждый K-предполный класс содержится в некотором S-предполном классе и любой S-предполный класс из $J_2^S \setminus J_2^A$ содержит ровно 3 K-предполных класса из $J_2 \setminus J_2^A$.*

Из определений классов ЛА, составляющих множества J_2^A, J_2^S и J_2, следуют включения

$$M_0 \cup R_0^e \cup R_0^d \subset \tilde{M}_0,$$

$$M_i \cup R_i^e \cup R_i^d \subset \tilde{M}_i, \;\; i = 2, 3, \ldots,$$

используя которые, получаем доказательство теоремы 5.1.2.

Теорема 5.1.3. *Пусть $\rho \in \{A, K\}$. Множество, состоящее из всех ρ-замкнутых классов, содержащих сумматор и константные ЛА, счетно. Множество, состоящее из всех S-замкнутых классов, содержащих сумматор и константные ЛА, континуально.*

Доказательство. Пусть

$$\mathbb{M}_A = \{ \; M \; \mid \; M \subseteq \mathfrak{L}, \;\; A(M) = M, \;\; x_1 + x_2 \in M, \;\; \mathfrak{L}_c \subset M \; \} \, .$$

Таким образом, $\mathbb{M}_A$ – множество, состоящее из всех A-замкнутых классов в $\mathfrak{L}$, содержащих сумматор $x_1 + x_2$ и все константные автоматы. По теореме 4.6.1 множество $\mathbb{M}_A$ содержит не более чем счетное число невырожденных A-замкнутых классов. Как нетрудно видеть, в $\mathbb{M}_A$ имеется только один вырожденный A-замкнутый класс. Поэтому множество $\mathbb{M}_A$ не более чем счетно. Через $\hat{M}_i$ обозначим A-замкнутый класс

$$A \left(\{ \; \xi^i, \;\; x_1 + x_2 \; \} \cup \mathfrak{L}_c \right) .$$

Нетрудно видеть, что для любого i, $i = 1, 2, \ldots$, выполнено:

$$\hat{M}_i \in \mathbb{M}_A.$$

Кроме того, для любых различных натуральных чисел i и i' имеет место:

$$\hat{M}_i \neq \hat{M}_{i'}.$$

Таким образом, множество $\mathbb{M}_A$ счетно.

Пусть

$$\mathbb{M}_K = \{ \; M \; \mid \; M \subseteq \mathfrak{L}, \;\; K(M) = M, \;\; x_1 + x_2 \in M, \;\; \mathfrak{L}_c \subset M \; \} \, .$$

Из леммы 3.1.1 следует, что для любых M и M' из $\mathbb{M}_K$ равенство $M = M'$ равносильно равенству $K^{(1)}(U(M)) = K^{(1)}(U(M'))$.

А из теоремы 3.2.1 следует, что $K^{(1)}$-замкнутых классов в $\mathfrak{L}_0^{(1)}$ не более чем счетно. Счетность множества $\mathbb{M}_K$ вытекает из счетности множества

$$\{ \; K \left(\{ \; \xi^i, \;\; x_1 + x_2 \; \} \cup \mathfrak{L}_c \right) \; \mid \; i = 1, 2, \ldots \; \} \, ,$$

являющегося подмножеством $\mathbb{M}_K$.

Докажем теперь, что множество

$$\mathbb{M}_S = \{\ M \mid M \subseteq \mathfrak{L},\ \ S(M) = M,\ \ x_1 + x_2 \in M,\ \ \mathfrak{L}_c \subset M\ \}$$

имеет мощность континуума. Для этого через I обозначим некоторое подмножество множества натуральных чисел, положим:

$$M'_I = S\left(\left\{\ \frac{1}{p_i}x,\ \ x_1 + x_2 \mid i \in I\ \right\} \cup \mathfrak{L}_c\right).$$

Нетрудно видеть, что для любого I, $I \subseteq \mathbb{N}$, имеет место включение

$$M'_I \in \mathbb{M}_S$$

, и для различных подмножеств I и I' множества натуральных чисел выполнено:

$$M'_I \neq M'_{I'}.$$

Тем самым, доказана континуальная мощность множества $\mathbb{M}_S$, а, вместе с этим, и теорема 5.1.3.

Непосредственно из теоремы 5.1.1 следует

Теорема 5.1.4. *В классе $\mathfrak{L}$ любое подмножество, не являющееся S-полным, расширяется до S-предполного класса.*

5.2. Класс линейных 2-адических автоматов

5.2.1. Решаемая задача

В этом параграфе мы будем рассматривать класс L_2 линейных 2-адических автоматов [5], вычисляющих линейные функции от переменных, принимающих значения из кольца $\mathbb{Z}_2$ целых 2-адических чисел, коэффициенты которых принимают значения из подкольца $\mathbb{Z}_{(2)}$ кольца рациональных чисел,

$$\mathbb{Z}_{(2)} = \mathbb{Z}_2 \cap \mathbb{Q}.$$

Формулировка полученного в этой главе результата была анонсирована в [74], а полностью он опубликован в [80].

Понятие p-адического числа введено в работе [88]. Подробное исследование кольца $\mathbb{Z}_p$ целых p-адических чисел содержится в книге [16].

Для заданного натурального числа u_0 определим следующее подмножество в $\mathbb{Z}_{(2)}$:

$$u_0\mathbb{Z}_{(2)} = \left\{\ u/v \ \mid\ u/v \in \mathbb{Z}_{(2)}, (u_0, u) = u_0, (u_0, v) = 1\ \right\},$$

Если u_0 не делится на 2, то через $\frac{\mathbb{Z}_{(2)}}{u_0}$ будем обозначать следующее множество чисел:

$$\left\{\ u/v \ \mid\ u/v \in \mathbb{Z}_{(2)}, (u_0, u) = 1, (u_0, v) = u_0\ \right\},$$

Инициальный конечный автомат [42], задаваемый шестеркой

$$\left(E_2^n, E_2^s, E_2, \phi, \psi, q_0\right),$$

сопоставляет каждому набору бесконечных входных последовательностей

$$\alpha_i,\ \ \alpha_i = \alpha_i(0), \alpha_i(1), \ldots,\ \ \alpha_i(t) \in E_2,\ \ t = 0, 1, \ldots,\ \ i = 1, \ldots, n,\ \ E_2 = \{0, 1\},$$

некоторую бесконечную выходную последовательность β, $\beta = \beta(0), \beta(1), \ldots$, $\beta(t) \in E_2$, $t = 0, 1, \ldots$. Если бесконечной последовательности нулей и единиц α, $\alpha = \alpha(0), \alpha(1), \ldots$, сопоставлять последовательность $\bar{\alpha}$ частичных сумм ряда $\sum_{t=0}^{\infty} \alpha_i(t)2^t$, являющуюся 2-адическим числом, то рассматриваемый конечный автомат осуществляет преобразование набора 2-адических чисел $(\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n)$ в 2-адическое число $\bar{\beta}$. Автоматные преобразователи целых p-адических чисел изучались в работе [48].

Конечный инициальный автомат из P с входным алфавитом E_2^n и выходным алфавитом E_2 называется линейным 2-адическим автоматом (ЛАА), если для определяемого им отображения $f\left(x_1, x_2, \ldots, x_n\right)$ в $\mathbb{Z}_{(2)}$ найдутся такие числа r_0, r_1, ..., r_n, что для любых $\bar{\alpha}_1$, $\bar{\alpha}_2$, ..., $\bar{\alpha}_n$ из $\mathbb{Z}_2$ выполнено:

$$f\left(\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n\right) = \sum_{i=1}^{n} r_i\bar{\alpha}_i + r_0.$$

В этом случае для ЛАА $f\left(x_1, x_2, \ldots, x_n\right)$ имеет место разложение:

$$f\left(x_1, x_2, \ldots, x_n\right) = \sum_{i=1}^{n} r_i x_i + r_0. \tag{5.14}$$

Множество всех ЛАА обозначим L_2.

В L_2 содержится, например, рассматриваемая в этой работе ранее, задержка $\xi_a(x)$ с начальным состоянием a, $a \in E_2$, [42], а также последовательный двоичный сумматор $f_+^{(2)}\left(x_1, x_2\right)$, задаваемый линейным 2-адическим автоматом с системой канонических уравнений:

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

Нетрудно видеть, что справедливы равенства:

$$\xi_a(x) = a + 2x,$$

$$f_+^{(2)}\left(x_1, x_2\right) = x_1 + x_2,$$

где операции сложения и умножения выполняются в кольце $\mathbb{Z}_2$ целых 2-адических чисел.

Класса L_2 мы рассматриваем в этом параграфе вместе с операциями композиции [42]. Вместо терминов K-замыкание и K-полнота мы будем использовать термины замыкание и полнота. В этом параграфе найдено множество J_2^L всех максимальных подклассов. Множество J_2^L оказалось счетным, но, несмотря на это, как и в случае класса $\mathfrak{L}$ ЛА, в классе L_2 найден алгоритм проверки полноты конечных подмножеств. Этот алгоритм по заданному конечному множеству автоматов из L_2 находит конечное подмножество классов из J_2^L, невключение в каждый из которых равносильно полноте рассматриваемого множества.

5.2.2. Операции композиции

Пусть для ЛАА $f\left(x_1, x_2, \ldots, x_n\right)$ и $f'\left(x_{n+1}, x_{n+2}, \ldots, x_{n+n'}\right)$, некоторых чисел r_i, $i = 0, 1, \ldots, n+n'$, r_0' из $\mathbb{Z}_{(2)}$ выполнены равенства (5.14) и (5.15), соответственно,

$$f'\left(x_{n+1}, x_{n+2}, \ldots, x_{n+n'}\right) = \sum_{i=n+1}^{n+n'} r_i x_i + r'_0. \qquad (5.15)$$

Через f_1, f_2, f_3 обозначим ЛАА, получаемые, соответственно, отождествлением переменных x_{n-1} и x_n ЛАА f, переименованием переменных ЛАА f с x_1, x_2, ..., x_n на x'_1, x'_2, ..., x'_n, подстановкой ЛАА f вместо переменной $x_{n+n'}$ ЛАА f'. Если к переменной x_n ЛАА f применима обратная связь, то через f_4 обозначим результат ее применения к этой переменной.

Лемма 5.2.1. *Имеют место следующие равенства.*

$$f_1\left(x_1, x_2, \ldots, x_{n-1}\right) = \sum_{i=1}^{n-2} r_i x_i + \left(r_{n-1} + r_n\right) x_{n-1} + r_0, \qquad (5.16)$$

$$f_2\left(x'_1, x'_2, \ldots, x'_n\right) = \sum_{i=1}^{n} r_i x'_i + r_0, \qquad (5.17)$$

$$f_3\left(x_1, x_2, \ldots, x_{n+n'-1}\right) = \sum_{i=n+1}^{n+n'-1} r_i x_i + \sum_{i=1}^{n} r_i r_{n+n'} x_i + r'_0 + r_{n+n'} r_0, \qquad (5.18)$$

$$f_4\left(x_1, x_2, \ldots, x_{n-1}\right) = \sum_{i=1}^{n-1} r_i \left(1 - r_n\right)^{-1} x_i + r_0 \left(1 - r_n\right)^{-1}. \qquad (5.19)$$

Доказательство.

Доказательство равенств (5.16) – (5.18) может быть получено с использованием рассуждений, приведенных в [68] для класса $\mathfrak{L}$ ЛА.

Докажем равенство (5.19). Пусть выполнено равенство (5.14) и к переменной x_n ЛАА f применима операция обратной связи. Тогда $r_n \in 2\mathbb{Z}_{(2)}$. Применив операцию обратной связи к переменной x_n, получим ЛАА $f_4\left(x_1, x_2, \ldots, x_{n-1}\right)$.

Через $f_-(x)$ обозначим ЛАА из L_2, получаемый применением операции обратной связи к переменной x' ЛАА $x + 2 \cdot x'$. Построив диаграмму переходов конечного автомата $x + f_-(x)$, убеждаемся в справедливости равенства:

$$f_-(x) = -x.$$

Из последнего равенства и равенств (5.14), (5.18) для ЛАА $g_n(x_n)$,

$$g_n(x_n) = f(0, 0, \ldots, 0, x_n) + f_-(f(0, 0, \ldots, 0))$$

вытекает:

$$g_n(x_n) = r_n x_n.$$

Используя это соотношение, а также (5.14) и (5.18), получим:

$$f(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_{n-1}, 0) + g_n(x_n) \tag{5.20}$$

Через $h_n(x)$ обозначим ЛАА, полученный применением обратной связи к переменной x_n ЛАА $x + g_n(x_n)$. Ввиду (5.20), справедливо:

$$f_4(x_1, x_2, \ldots, x_{n-1}) = h_n(f(x_1, x_2, \ldots, x_{n-1}, 0)).$$

Отсюда, из свойства (5.18), а также равенства (5.14) следует, что для доказательства (5.19) осталось установить справедливость соотношения:

$$h_n(x) = (1 - r_n)^{-1} x. \tag{5.21}$$

ЛАА $h'_{n,\tau}$,

$$h'_{n,\tau}(x) = \underbrace{x + g_n(x + g_n(x + \ldots g_n(x + g_n}_{\tau-1 \quad \text{символов} \ g}(x)))),$$

τ-эквивалентен [17] ЛАА $h_n(x)$, $\tau = 1, 2, \ldots$. Отсюда следует

$$h_n(x) = \sum_{t=0}^{\infty} r_n^t x,$$

где $r_n^0 = 1$.

Поэтому из равенства $(1 - r_n) \sum_{t=0}^{\infty} r_n^t = 1$ вытекает (5.21).

Равенство (5.19), а, вместе с ним, и лемма 5.2.1 доказаны.

Замыкание множества M, $M \subseteq L_2$, по операциям композиции (отождествления и переименования переменных, подстановки, обратной связи) мы, как и ранее, обозначаем $K(M)$ [42]. Множество ЛАА M называется замкнутым, если

$K(M) = M$, а замкнутое множество M является максимальным (или предполным) классом, если $M \neq L_2$, но для любого ЛАА f, $f \in L_2 \setminus M$, выполнено: $K(M \cup \{f\}) = L_2$.

Лемма 5.2.2. *Справедливо равенство:*

$$K\left(\left\{\ f_{+}^{(2)},\ \ \xi_1\ \right\}\right) = L_2. \tag{5.22}$$

Доказательство. Заметим, что $\xi_0(x) = f_{+}^{(2)}(x,x)$. Применяя операцию обратной связи к переменной x ЛАА $\xi_0(x)$, получим константу 0. Для любого натурального числа n из сумматора и константы 0 с использованием операций подстановки и переименования переменных можно получить ЛАА $x_1+x_2+\cdots+x_n$, отождествляя все переменные которого, получим nx_1. Как замечено в предыдущей лемме, ЛАА $(-x)$ получается путем применения операции обратной связи к переменной x' ЛАА $x + \xi_0\,(x')$. Таким образом, для любого целого числа m выполнено:

$$mx \in K\left(\left\{\ f_{+}^{(2)},\ \ \xi_1\ \right\}\right).$$

Пусть $r \in \mathbb{Z}_{(2)}$, $r = u/v$. По лемме 5.2.1 ЛАА rx получается применением операции обратной связи к переменной x' ЛАА $ux + (1-v)x'$.

Подставляя константу 0 вместо переменной x задержки $\xi_1(x)$, получим константу 1. Константу r_0, $r_0 \in \mathbb{Z}_{(2)}$, получим, подставив константу 1 вместо единственной переменной ЛАА r_0x.

Используя ЛАА r_ix_i, $i = 1,2,\ldots,n$, константу r_0, сумматор $x_1 + x_2 + \cdots + x_{n+1}$ и операции подстановки, получим ЛАА $f\,(x_1,x_2,\ldots,x_n)$, для которой выполнено равенство (5.14).

Лемма 5.2.2 доказана.

Соотношение между классом $\mathfrak{L}$ ЛА и классом L_2 ЛАА устанавливает следующее

Замечание 3. *Имеют место соотношения:*

$$L_2 \not\subseteq \mathfrak{L}, \tag{5.23}$$

$$\mathfrak{L} \not\subseteq L_2, \tag{5.24}$$

Действительно, соотношение (5.23) вытекает из

$$x_1 + x_2 \notin \mathfrak{L}, \tag{5.25}$$

а соотношение (5.24) – из

$$x_1 \oplus x_2 \notin L_2, \tag{5.26}$$

где операция сложения в поле E_2 обозначена через "$\oplus$", чтобы отличать ее от операции сложения в $\mathbb{Z}_2$.

И, далее, если для некоторого ЛАА $f\,(x_1, x_2)$ из L_2 выполнены равенства $f\,(0,0) = 0$, $f\,(x_1, 0) = x_1$ и $f\,(0, x_2) = x_2$, то из соотношения $f\,(x_1, x_2) = r_1x_1 + r_2x_2 + r_0$ следует, что $f\,(x_1, x_2) = x_1 + x_2$.

Если те же 3 равенства выполнены для некоторого ЛАА $f\,(x_1, x_2)$ из $\mathfrak{L}$, то из соотношения

$$f\,(x_1, x_2) = r_1x_1 \oplus r_2x_2 \oplus r_0$$

следует, что

$$f\,(x_1, x_2) = x_1 \oplus x_2.$$

Свойства (5.25) и (5.26) справедливы ввиду неравенства

$$x_1 + x_2 \neq x_1 \oplus x_2.$$

5.2.3. Некоторые замкнутые классы

Пусть выполнено (5.14). Положим:

$$\tilde{U}(f) = \{\ r_i \ \mid\ i = 1, 2, \ldots, n\ \}.$$

Для множества M, $M \subseteq L_2$, положим:

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

Переменная x_i ЛАА $f(x_1, x_2, \ldots, x_n)$, удовлетворяющей равенству (5.14), 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 ЛАА $f(x_1, x_2, \ldots, x_n)$ в точности тогда, когда x_i не является непосредственной переменной.

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

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

Рассмотрим следующие подмножества в L_2.

$$\tilde{L}^e = \{\ f \ \mid \ f \ \text{ имеет ровно одну существенную переменную }\ \},$$

$$\tilde{L}^d = \{\ f \ \mid \ f \ \text{ имеет ровно одну непосредственную переменную }\ \},$$

$$\tilde{T}_a = \{\ f \ \mid \ \text{для любых } \ \bar{\alpha}_i, \bar{\alpha}_i \in a + 2\mathbb{Z}_2, i = 1, 2, \ldots, n \\ \text{выполнено} f(\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n) \in a + 2\mathbb{Z}_2\ \},$$

$a \in E_2$,

$$\tilde{V}_1 = \{\ f \ \mid \ f \ \text{ имеет не более одной непосредственной переменной }\ \},$$

$$\tilde{V}_2 = \{\ f \ \mid \ f \ \text{ имеет нечетное число непосредственных переменных }\ \},$$

$$\tilde{I} = \left\{\ f \ \mid \ \text{если выполнено равенство } \ (5.14), \text{то} \sum_{i=1}^{n} |r_i| \leq 1\ \right\},$$

Пусть $\tilde{p}_1$, $\tilde{p}_2$, $\ldots$ – последовательность всех простых чисел, причем $\tilde{p}_1 < \tilde{p}_2 < \ldots$. Тогда $\tilde{p}_1 = 2$. Положим:

$$\tilde{R}_i^e = \left\{\ f \ \mid \ f \in L_2 \setminus \tilde{L}^e, \ \text{ для любого } \ u/v \\ \text{из } \ \tilde{U}(f) \ \text{ выполнено: } \ (u, \tilde{p}_i) = \tilde{p}_i\ \right\} \cup \\ \left\{\ f \ \mid \ f \in \tilde{L}^e, \ \text{ для } \ u/v \ \text{ из } \ \tilde{U}(f) \setminus \{0\} \ \text{ выполнено: } \ (v, \tilde{p}_i) = 1\ \right\}$$

$i = 2, 3, \dots,$

$$\tilde{R}_i^d = \Big\{\ f \ \mid\ f \in L_2 \setminus \tilde{L}^d,\ \text{ для любого } \ u/v \\ \text{из } \ \tilde{U}(f) \ \text{ выполнено: } \ (u, \tilde{p}_i) = \tilde{p}_i \ \Big\} \cup \\ \Big\{\ f \ \mid\ f \in \tilde{L}^d,\ \text{ для любого } \ u/v \ \text{ из } \ \tilde{U}(f) \setminus H^1 \ \text{ выполнено: } \ (u, \tilde{p}_i) = \tilde{p}_i \\ \text{а для } \ u/v \ \text{ из } \ \tilde{U}(f) \cap H^1 \ \text{ имеет место: } \ (v, \tilde{p}_i) = 1 \ \Big\},$$

$i = 2, 3, \dots,$

Через J_2^L обозначим следующее множество:

$$\Big\{\ \tilde{T}_0, \tilde{T}_1, \tilde{V}_1, \tilde{V}_2, \tilde{I}, \tilde{R}_i^e, \tilde{R}_i^d \ \mid\ i = 2, 3, \dots \ \Big\}.$$

Теорема 5.2.1. *Для любого Θ, $\Theta \in J_2^L$, выполнено:*

$$K(\Theta) = \Theta. \tag{5.27}$$

Для любых различных Θ_1 и Θ_2 из J_2^L выполнено:

$$\Theta_1 \not\subseteq \Theta_2. \tag{5.28}$$

Доказательство. Замкнутость множества Θ, $\Theta \in J_2^L \setminus \{\tilde{I}\}$, проводится индукцией по построению элементов из $K(\Theta)$ с использованием рассуждений, имеющихся в [68].

Докажем равенство (5.27) в случае $\Theta = \tilde{I}$.

Рассмотрим ЛАА $f\,(x_1, x_2, \dots, x_n)$ и $f'\,(x_{n+1}, x_{n+2}, \dots, x_{n+n'})$ из $\tilde{I}$. Пусть имеют место равенства (5.14) и (5.15), и пусть f_1, f_2, f_3, f_4 построены из f и f' также, как в условии леммы 5.2.1. Тогда справедливы равенства (5.16) – (5.18). А, в случае применимости к переменной x_n ЛАА $f\,(x_1, x_2, \dots, x_n)$ операции обратной связи, выполнено также равенство (5.19).

Имеют место соотношения:

$$\sum_{i=1}^{n} |r_i| \le 1,$$

$$\sum_{i=n+1}^{n+n'} |r_i| \leq 1.$$

Отсюда вытекают неравенства:

$$\sum_{i=1}^{n-2} |r_i| + |r_{n-1} + r_n| \leq 1,$$

$$\sum_{i=n+1}^{n+n'-1} |r_i| + \sum_{i=1}^{n} |r_i r_{n+n'}| \leq 1,$$

$$\sum_{i=1}^{n-1} |r_i \left(1 - r_n\right)^{-1}| \leq \frac{\sum_{i=1}^{n-1} |r_i|}{(1 - |r_n|)} \leq 1,$$

из которых следует включение:

$$\{ \ f_i \ \mid \ i = 1, 2, 3, 4 \ \} \subseteq \tilde{I}.$$

Поэтому равенство (5.27) в случае $\Theta = \tilde{I}$ доказано.

Теперь покажем справедливость (5.28) для любых различных Θ_1 и Θ_2 из J_2^L. Для этого каждому классу $\tilde{\Theta}$ из J_2^L сопоставим множество $\hat{\Theta}$ ЛАА из L_2 следующим образом.

$$\hat{T}_0 = \{x_1 + x_2\},$$

$$\hat{T}_1 = \{x_1 + x_2 + 2x_3 + 1\},$$

$$\hat{V}_1 = \{x_1 + 2x_2 + 2x_3 + 1, 0\},$$

$$\hat{V}_2 = \{x_1 + x_2 + x_3 + 1\},$$

$$\hat{I} = \{x + 1, x_1/3 + x_2/3\},$$

$$\hat{R}_i^e = \{\tilde{p}_i x_1 + \tilde{p}_i x_2, 2x + 1\},$$

$$\hat{R}_i^d = \{\tilde{p}_i x_1 + \tilde{p}_i x_2, x_1 + 2\tilde{p}_i x_2 + 1\}.$$

Нетрудно видеть, что для любых $\tilde{\Theta}_1$ и $\tilde{\Theta}_2$ из J_2^L выполнено: $\hat{\Theta}_1 \subseteq \tilde{\Theta}_2$, если $\tilde{\Theta}_1 = \tilde{\Theta}_2$ и $\hat{\Theta}_1 \not\subseteq \tilde{\Theta}_2$, в противном случае. Отсюда вытекает второе утверждение теоремы.

Теорема 5.2.1 доказана.

5.2.4. Однородные 2-адические автоматы

ЛАА $f(x_1, x_2, \ldots, x_n)$, заданный равенством (5.14), называется однородным, если $r_0 = 0$. Множество всех однородных ЛАА обозначим L_2^0. Имеют место включения:

$$x_1 + x_2 + \cdots + x_n \in L_2^0, \quad n \in \mathbb{N};$$

$$rx \in L_2^0, \quad r \in \mathbb{Z}_{(2)};$$

$$\sum_{i=1}^{n} r_i x_i \in L_2^0, \quad r_i \in \mathbb{Z}_{(2)}, \quad i = 1, 2, ..., n, \quad n \in \mathbb{N};$$

Распространим определения критериальной системы и приведенной критериальной системы на любой замкнутый класс конечных автоматов. Множество J^* замкнутых подклассов замкнутого класса R называется критериальной системой [42] в R, если для любого множества M, $M \subseteq R$, равенство $K(M) = R$ имеет место в точности тогда, когда M не содержится в каждом классе системы J^*. Критериальная система в R, не содержащая собственных критериальных подсистем, называется приведенной.

Положим:

$$J_2^{L^0} = \left\{ \ \Theta^0 \ | \ \Theta^0 = \Theta \cap L_2^0, \ \Theta \in J_2^L \setminus \left\{ \tilde{T}_0, \tilde{T}_1 \right\} \ \right\}.$$

Теорема 5.2.2. *Множество $J_2^{L^0}$ является критериальной системой в L_2^0.*

Доказательство. Пусть $M \subseteq L_2^0$ и для любого Θ^0 из $J_2^{L^0}$ выполнно: $M \not\subseteq \Theta^0$. Докажем, что

$$K(M) = L_2^0. \tag{5.29}$$

В M содержится ЛАА f_o с четным числом непосредственных переменных. Отождествим все переменные этого ЛАА, а к единственной оставшейся переменной применим операцию обратной связи. Получим константу 0.

Выбрав какие-либо две непосредственные переменные некоторого ЛАА f_1 из $M \setminus \tilde{V}_1$, переименуем их в x_1 и x_2, а вместо остальных переменных подставим константу 0. Тогда для некоторых чисел s_i', $s_i' \in H^1$, $i = 1, 2$, получим ЛАА $f'(x_1, x_2) = s_1' x_1 + s_2' x_2$. Для ЛАА $f''(x_1, x_2)$,

$$f''(x_1, x_2) = f'(f'(0, x_1), f'(x_2, 0)),$$

имеем:

$$f''(x_1, x_2) = s'' x_1 + s'' x_2,$$

где $s'' = s_1' s_2'$. Далее положим $f(x_1, x_2) = f''(f''(x_1, 0), f''(x_2, 0))$. Тогда для некоторого s, $s \in H^1$, $s > 0$, имеем:

$$f(x_1, x_2) = s x_1 + s x_2 \in K(M).$$

Докажем, что в $K(M)$ есть ЛАА $r_1' x$, где $r_1' > 1$. Найдется ЛАА f_I', $f_I' \in M \setminus \tilde{I}$. Если все числа в $\tilde{U}(f_I')$ имеют один знак, то, отождествив все переменные ЛАА f_I' и переименовав единственную переменную полученной одноместного ЛАА в x, получим ЛАА $f_I''(x)$. Нетрудно видеть, что ЛАА $f_I''(f_I''(x))$ – искомый.

В противном случае, используя операции отождествления и переименования переменных, из f_I' можно получить ЛАА

$$f_I(x_1, x_2), \ \ f_I(x_1, x_2) = r_1 x_1 + r_2 x_2, \ \text{ где } \ r_1 > 0, \ \ r_2 < 0, \ \ r_1 - r_2 > 1.$$

Если $r_1 \geq 1$ или $r_2 \leq -1$, то ЛАА $f_I(x, f_I(0, x))$ – искомый.

Пусть

$$r_1 < 1, \quad r_2 > -1. \tag{5.30}$$

Рассмотрим последовательность ЛАА f_n', $n = 1, 2, \ldots$, где

$$f_n'(x) = f_I(x, \underbrace{f_I(f_I(\ldots f_I(f_I}_{n \text{ символов } f}(x, x), x) \ldots), x)).$$

Справедливо равенство

$$f_n'(x) = \left(r_1 + r_2^2 \sum_{i=0}^{n-1} r_1^i + r_2 r_1^n \right) x.$$

Кроме того, несложно показать, что для любого целого неотрицательного n выполнено:

$$r_1 + r_2^2 \sum_{i=0}^{n-1} r_1^i - r_2 r_1^n \geq r_1 - r_2.$$

Поэтому для некоторого n_0 имеет место:

$$r_1 + r_2^2 \sum_{i=0}^{n_0-1} r_1^i + r_2 r_1^{n_0} > 1.$$

Таким образом, ЛАА $r_1'x$ с некоторым $r_1' > 1$ содержится в $K(M)$ и в случае (5.30).

Для некоторых натуральных чисел u_s и v_s имеем: $s = u_s/v_s$, $(u_s, v_s) = 1$.

Положим

$$P = \left\{ \ \tilde{p}_i \ \mid \ s \in \tilde{p}_i \mathbb{Z}_{(2)} \ \right\},$$

$$m = |P|.$$

Пусть $P = \{ \ \tilde{p}_{i_1}, \tilde{p}_{i_2}, \ldots \tilde{p}_{i_m} \ \}$. Для каждого j, $j = 1, 2, \ldots, m$, найдутся ЛАА $f_{e,j}$, $f_{d,j}$, $f_{e,j} \in M \setminus \tilde{R}_{i_j}^e$, $f_{d,j} \in M \setminus \tilde{R}_{i_j}^d$. Докажем, что в $K(M)$ содержатся ЛАА

$$r_j'x, \quad j = 1, 2, \ldots, m, \tag{5.31}$$

такие, что

$$r_j' \in \frac{\mathbb{Z}_{(2)}}{\tilde{p}_{i_j}}. \tag{5.32}$$

Для заданного j, $j \in \{1, 2, \ldots, m\}$, возможны 2 случая.

Случай 1. В $\{f_{e,j}, f_{d,j}\}$ найдется ЛАА f_j'',

$$f_j'' \notin \tilde{R}_{i_j}^e \cup \tilde{R}_{i_j}^d.$$

Случай 2. Имеют место соотношения:

$$f_{e,j} \in \tilde{R}_{i_j}^d \setminus \tilde{R}_{i_j}^e,$$

$$f_{d,j} \in \tilde{R}_{i_j}^e \setminus \tilde{R}_{i_j}^d.$$

Рассмотрим случай 1. Если

$$\tilde{U}\left(f_j''\right) \cap \frac{\mathbb{Z}_{(2)}}{\tilde{p}_{i_j}} \neq \emptyset, \tag{5.33}$$

то ЛАА $r_j'x$, такой, что r_j' удовлетворяет (5.32), можно получить, используя операции подстановки и переименования переменных из ЛАА f_j'' и 0.

Пусть (5.33) не имеет места. Можно выбрать 2 переменные ЛАА f_j'' так, что переименовав их в x_1 и x_2 и подставив вместо остальных переменных константу 0, получим ЛАА $\tilde{r}_1'x_1 + \tilde{r}_2'x_2$ такой, что

$$\tilde{r}_1'x_1 + \tilde{r}_2'x_2 \notin \tilde{R}_{i_j}^e \cup \tilde{R}_{i_j}^d$$

и $\tilde{r}_1' \notin \tilde{p}_{i_j}\mathbb{Z}_{(2)}$. Множество

$$\left\{\tilde{r}_1'x_1 + \tilde{r}_2'x_2, \tilde{r}_1'x_2 + \tilde{r}_2'x_1, \tilde{r}_1'x_1 + \tilde{r}_2'\left(sx_1 + sx_2\right)\right\}$$

содержит ЛАА $r_1''x_1 + r_2''x_2$ со свойствами:

$$r_1'' \in 2\mathbb{Z}_{(2)}, \quad r_1'' \notin \tilde{p}_{i_j}\mathbb{Z}_{(2)}, \quad r_2'' \neq 0. \tag{5.34}$$

Отсюда следует, что найдется n_j, $n_j \in \mathbb{N}$, что

$$\frac{r_2''}{1 - \left(r_1''\right)^{n_j}} \in \frac{\mathbb{Z}_{(2)}}{\tilde{p}_{i_j}} \setminus \{0\}.$$

ЛАА $\left(r_1''\right)^{n_j} x_1 + r_2''x$ содержится в $K(M)$ и к переменной x_1 этого ЛАА вследствие (5.34) применима обратная связь. Применяя обратную связь к этой переменной, получаем ЛАА $r_j'x$, удовлетворяющий (5.32). Случай 1 разобран.

В случае 2 ЛАА $f_{e,j}$ имеет не менее двух существенных переменных и ровно одну непосредственную. Поэтому, из нее подстановкой константы 0 и переименованием переменных можно получить ЛАА $r_1^*x_1 + r_2^*x_2$, где

$$r_1^* \in H^1, \quad r_1^* \notin \tilde{p}_{i_j}\mathbb{Z}_{(2)}, \quad r_2^* \neq 0.$$

ЛАА $f_{d,j}$ имеет единственную существенную переменную,

$$f_{d,j}(x) = r^*x, \quad r^* \in 2\mathbb{Z}_{(2)}, \quad r^* \notin \tilde{p}_{i_j}\mathbb{Z}_{(2)}.$$

ЛАА $r_1''x_1 + r_2''x_2$,

$$r_1''x_1 + r_2''x_2 = r_1^* r^* x_1 + r_2^* x_2$$

содержится в $K(M)$ и обладает свойствами (5.34). Потому существование в $K(M)$ ЛАА $r_j'x$ со свойством (5.32) доказывается с использованием рассуждений, приведенных для случая 1.

Существование последовательности (5.31) со свойством (5.32) доказано.

Для каждого j, $j = 1, 2, \ldots, m$, найдется τ_j, $\tau_j \in \mathbb{N}$, удовлетворяющее соотношениям:

$$\left(r_j'\right)^{\tau_j} s^n \notin \tilde{p}_{i_j}\mathbb{Z}_{(2)}, \quad \left(r_j'\right)^{\tau_j} s^n > 0,$$

найдется τ_0, $\tau_0 \in \mathbb{N}$, удовлетворяющее неравенству:

$$2\left(r_1'\right)^{\tau_0} s^2 > 1.$$

Положим

$$s_0 = s^n, \quad s_j = \left(r_j'\right)^{\tau_j} s^n, \ \ j = 1, 2, \ldots, m,$$

$$s_{m+1} = s^{n+1} / \left(1 - 2\left(r_1'\right)^{\tau_0} s^2\right).$$

Найдется τ', $\tau' \in \mathbb{N}$, такое, что числитель положительного числа

$$\left(r_1'\right)^{\tau'} s$$

больше его знаменателя. Положим:

$$\tilde{s} = \left(r_1'\right)^{\tau'} s.$$

Представим число $\tilde{s}$ несократимой дробью: $\tilde{s} = \frac{\tilde{u}}{\tilde{v}}$.

Положим $n = \tilde{u}(m+2) + 2$, откуда $n > 4$. Тогда

$$4(m+2)\tilde{u} = 4(n-2) < 4 \cdot 2^{n-2} = 2^n.$$

Поэтому из ЛАА f и 0, используя операции суперпозиции, можно получить ЛАА $\tilde{f}\left(x_1, x_2, \ldots, x_{4(m+2)\tilde{u}}\right)$,

$$\tilde{f}\left(x_1, x_2, \ldots, x_{4(m+2)\tilde{u}}\right) = s^n x_1 + s^n x_2 + \cdots + s^n x_{4(m+2)\tilde{u}}.$$

Через $h\left(x_1, x_2, \ldots, x_{4(m+2)\tilde{u}}\right)$ обозначим ЛАА

$$\tilde{f}\left(x_1, x_2, \ldots, x_{4\tilde{u}}, \left(r'_1\right)^{\tau_1} x_{4\tilde{u}+1}, \left(r'_1\right)^{\tau_1} x_{4\tilde{u}+2}, \ldots, \left(r'_1\right)^{\tau_1} x_{8\tilde{u}}\right.$$
$$\left(r'_2\right)^{\tau_2} x_{8\tilde{u}+1}, \left(r'_2\right)^{\tau_2} x_{8\tilde{u}+2}, \ldots, \left(r'_2\right)^{\tau_2} x_{12\tilde{u}}, \ldots$$
$$\left(r'_m\right)^{\tau_m} x_{4m\tilde{u}+1}, \left(r'_m\right)^{\tau_m} x_{4m\tilde{u}+2}, \ldots, \left(r'_m\right)^{\tau_m} x_{4(m+1)\tilde{u}},$$
$$\tfrac{s}{1-2\left(r'_1\right)^{\tau_0} s^2} x_{4(m+1)\tilde{u}+1}, \tfrac{s}{1-2\left(r'_1\right)^{\tau_0} s^2} x_{4(m+1)\tilde{u}+2}, \ldots,$$
$$\left.\tfrac{s}{1-2\left(r'_1\right)^{\tau_0} s^2} x_{4(m+2)\tilde{u}}\right).$$

Справедливо равенство

$$h\left(x_1, x_2, \ldots, x_{4(m+2)\tilde{u}}\right) = \textstyle\sum_{j=0}^{m+1} \sum_{i=1}^{4\tilde{u}} s_j x_{4j\tilde{u}+i}.$$

Так как наибольший общий делитель числителей положительных чисел $s_0, s_1, \ldots, s_m$ равен 1, а число s_{m+1} отрицательное, то найдутся целые неотрицательные числа n_i, $i = 0, 1, 2, \ldots, m+1$, удовлетворяющие равенству:

$$1 = \sum_{i=0}^{m+1} n_i s_i. \tag{5.35}$$

Каждое из чисел n_i представим в следующем виде:

$$n_i = \sum_{j=0}^{l_i} n_{i,j} \tilde{s}^j, \tag{5.36}$$

где $n_{i,j} \in \mathbb{Z}$, $0 \leq n_{i,j} < \tilde{u}$, $j = 0, 1, \ldots, l_i$, $i = 0, 1, \ldots, m+1$.

Используя операции подстановки и переименования переменных, из ЛАА

$$h\left(x_1, x_2, \ldots, x_{4(m+2)\tilde{u}}\right), \;\; \tilde{s}x_1 + \tilde{s}x_2, \;\; 0$$

получим ЛАА h',

$$h' = \sum_{i=0}^{m+1} \sum_{j=0}^{l_i} \sum_{j'=1}^{2\tilde{u}} \tilde{s}^j s_i x_{2\tilde{u}(l_0+l_1+\ldots+l_{i-1}+i+j)+j'}.$$

Из ЛАА h', отождествляя нужным образом переменные, подставляя константу 0 и переименовывая переменные, получим ЛАА h'',

$$h'' = \sum_{i=0}^{m+1}\sum_{j=0}^{l_i} n_{i,j}\tilde{s}^j s_i x_{l_0+l_1+\ldots+l_{i-1}+i+j+1}+ \sum_{i=0}^{m+1}\sum_{j=0}^{l_i} n_{i,j}\tilde{s}^j s_i x'_{l_0+l_1+\ldots+l_{i-1}+i+j+1}.$$

Из равенств (5.35) и (5.36) следует, что, используя ЛАА h'' и операции отождествления и переименования переменных, можно получить сумматор $x_1 + x_2$. Используя рассуждения из доказательства леммы 5.2.2, несложно показать, что $K(\{x_1 + x_2\}) = L_2^0$.

Теорема 5.2.2 доказана.

5.2.5. Основные результаты и их доказательства

Имеет место:

Теорема 5.2.3. *Множество J_2^L является приведенной критериальной системой в L_2, состоящей из предполных классов.*

Доказательство. Пусть $M \subseteq L_2$ и для любого Θ, $\Theta \in J_2^L$, выполнено: $M \not\subseteq \Theta$. Из теоремы 5.2.3 следует, что найдется r', $r' \in \mathbb{Z}_{(2)}$, для которого имеет место включение:

$$x_1 + x_2 + r' \in K(M). \tag{5.37}$$

Применив к переменной x ЛАА $(x + x + r') + x_3 + r'$ обратную связь, получим ЛАА $-x_3 - 2r'$. Из равенства

$$(x_1 + x_2 + r') + (-x_3 - 2r') + r' = x_1 + x_2 - x_3$$

следует, что

$$x_1 + x_2 - x_3 \in K(M). \tag{5.38}$$

Используя (5.38) и равенство

$$x_1 + x_2 + \cdots + x_{j+1} - x_{j+2} - x_{j+3} - \cdots - x_{2j+1} =$$
$$x_1 + x_2 + \cdots + x_{j-1} + (x_j + x_{j+1} - x_{j+2}) - x_{j+3} - x_{j+4} - \cdots - x_{2j+1},$$

справедливое для любого j, $j = 2, 3, \ldots$, получим:

$$\hat{f}_{2j+1} = x_1 + x_2 + \cdots + x_{j+1} - x_{j+2} - x_{j+3} - \cdots - x_{2j+1} \in K(M),$$

$j = 1, 2, \ldots$.

Применив к переменной x ЛАА $x + x + r'$ операцию обратной связи, получим константу $(-r')$.

Найдутся ЛАА f_0 и f_1,

$$f_0 \in M \setminus \tilde{T}_0, \;\; f_1 \in M \setminus \tilde{T}_1.$$

Множество

$$\{-r', f_0\left(-r', -r', \ldots, -r'\right), f_1\left(-r', -r', \ldots, -r'\right)\}$$

содержит константы $\tilde{r}_0$ и $\tilde{r}_1$,

$$\tilde{r}_0 \in 2\mathbb{Z}_{(2)}, \;\; \tilde{r}_1 \notin 2\mathbb{Z}_{(2)}.$$

Пусть $\tilde{r}_0 = \frac{\tilde{u}_0}{\tilde{v}_0}$, $\tilde{r}_1 = \frac{\tilde{u}_1}{\tilde{v}_1}$. Обозначим числа $\tilde{u}_1 \tilde{v}_0$ и $\tilde{u}_0 \tilde{v}_1$ через a и b, соответственно. Рассмотрим 2 случая.

Если числа $\tilde{r}_0$ и $\tilde{r}_1$ имеют одинаковые знаки, то, применив к переменной x ЛАА

$$\hat{f}_{2(|a|+|b|)+1}\left(\underbrace{\tilde{r}_0, \tilde{r}_0, \ldots, \tilde{r}_0}_{|a| \text{ раз } r}, \underbrace{x, x, \ldots, x}_{|b|+1 \text{ раз } x}, \underbrace{\tilde{r}_1, \tilde{r}_1, \ldots, \tilde{r}_1}_{|b| \text{ раз } r}, \underbrace{x, x, \ldots, x}_{|a| \text{ раз } x}\right)$$

операцию обратной связи, получим константу 0.

Если числа $\tilde{r}_0$ и $\tilde{r}_1$ имеют разные знаки, то константу 0 получим, применив операцию обратной связи к переменной x ЛАА

$$\hat{f}_{2(|a|+|b|)+1}\left(\underbrace{\tilde{r}_0, \tilde{r}_0, \ldots, \tilde{r}_0}_{|a| \text{ раз } r}, \underbrace{\tilde{r}_1, \tilde{r}_1, \ldots, \tilde{r}_1}_{|b| \text{ раз } r}, \underbrace{x, x, \ldots, x}_{|a|+|b|+1 \text{ раз } x}\right).$$

Таким образом,

$$0 \in K(M), \;\; x_1 + x_2 \in K(M).$$

ЛАА $\tilde{r}_1^{-1}x$ в случае $\tilde{r}_1 > 0$ получим, применив операцию обратной связи к переменной x' ЛАА

$$\hat{f}_{2(\tilde{u}_1+\tilde{v}_1)+1}\left(\underbrace{x', x', \ldots, x'}_{\tilde{u}_1+1 \text{ раз } x'}, \underbrace{0, 0, \ldots, 0}_{\tilde{v}_1+\tilde{u}_1 \text{ раз } 0}, \underbrace{x, x, \ldots, x}_{\tilde{v}_1 \text{ раз } x}\right).$$

А в случае $\tilde{r}_1 < 0$ этот ЛАА получим, применяя операцию обратной связи к переменной x' ЛАА

$$\hat{f}_{2(-\tilde{u}_1+\tilde{v}_1)+1}\left(\underbrace{x', x', \ldots, x'}_{-\tilde{u}_1+1 \text{ раз } x'}, \underbrace{x, x, \ldots, x}_{\tilde{v}_1 \text{ раз } x}, \underbrace{0, 0, \ldots, 0}_{\tilde{v}_1-\tilde{u}_1 \text{ раз } 0}\right).$$

Имеет место равенство:

$$\xi_1(x) = x + x + \tilde{r}_1^{-1}(\tilde{r}_1).$$

Поэтому

$$\{\ x_1 + x_2,\ \ \xi_1(x)\ \} \subseteq K(M).$$

Отсюда и из леммы 5.2.2 следует $K(M) = L_2$, то есть J_2^L - критериальная система в L_2. Приведенность этой системы следует из теоремы 5.2.1.

Как нетрудно видеть, каждый замкнутый класс системы J_2^L является предполным. Предполных классов, не содержащихся в J_2^L нет. Действительно, пусть такой класс Θ найдется. Тогда в Θ содержится ЛАА f_1 у которого не менее 2-х непосредственных переменных. Этот ЛАА может содержаться лишь в конечном подмножестве J_2' классов из множества J_2^L. Но для каждого Θ', $\Theta' \in J_2'$, в Θ найдется ЛАА $f_{\Theta'}$, не содержащийся в Θ'. По доказанному выше,

$$K\left(\{\ f_1,\ \ f_{\Theta'}\ \mid\ \Theta' \in J'_2\ \}\right) = L_2.$$

Поэтому $K(\Theta) = L_2$, что противоречит предположению, что Θ – предполный класс.

Теорема 5.2.3 доказана.

Теорема 5.2.4. *Задача проверки полноты конечных систем из L_2 алгоритмически разрешима.*

Доказательство. Очевидна конечность проверки соотношения $f \in \Theta$ для любых f и Θ, $f \in L_2$, $\Theta \in J_2^L$. Как отмечалось при доказательстве теоремы 5.2.3, для проверки полноты конечного множества ЛАА требуется выполнить конечное число таких проверок. Отсюда вытекает теорема 5.2.4.

Заключение

В работе для классов линейных автоматов над конечными полями найдены все K-предполные классы. Некоторые из этих классов определяются как обобщение для случая поля из двух элементов, остальные являются новыми. Существование нетривиальных автоморфизмов полей, не являющихся простыми, обусловило наличие двухпараметрических семейств K-предполных классов. При этом один из параметров соответствует автоморфизму, а другой — неприводимому приведенному многочлену из кольца многочленов над рассматриваемым полем.

Для классов линейных автоматов над конечными полями получен алгоритм проверки K-полноты конечных подмножеств, время работы которого по порядку оценивается произведением квадрата объема входных данных на количество элементов поля. При этом зависимость от количества задержек схем, задающих рассматриваемые автоматы, является квадратичной.

Для класса $\mathfrak{L}$ линейных автоматов над полем из двух элементов найдена структура K-замкнутых классов, содержащих сумматор. Для этого потребовалось изучить алгебру одноместных линейных автоматов, сохраняющих нулевую последовательность, вместе с операциями, индуцированными K-замыканием, что позволило получить алгоритм проверки выразимости через конечные множества линейных автоматов, содержащие сумматор, а также выразимости сумматора через конечные множества линейных автоматов

Найдена структура A-замкнутых классов в $\mathfrak{L}$, содержащих существенный автомат и все константы. Исследован вопрос о возможности A-выразимости всех констант через подмножества $\mathfrak{L}$, содержащие существенный автомат. Получены некоторые достаточные условия для A-выразимости. Выполнено сравнение операторов K- и A-замыкания.

В множестве $\mathfrak{L}$, рассматриваемого вместе с операциями суперпозиции, найдены все S-предполные классы. Выполнено сравнение структуры S-предполных классов со структурами A-предполных и K-предполных классов.

Техника, разработанная для класса $\mathfrak{L}$, позволила найти все предполные классы в классе линейных 2-адических автоматов и получить алгоритм проверки K-полноты конечных подмножеств этого класса.

Список сокращений и условных обозначений

ЛА — линейный автомат;

ЛАА — линейный 2-адический автомат;

1-глубина множества линейных автоматов M, $U(M) \not\subseteq E_2$ — наибольшее натуральное число r_0 такое, что для любого μ, $\mu \in U(M)$, выполнено:

$$\mu + \mu(0) \in \xi^{r_0}\mathfrak{L}_0^{(1)};$$

A-выразимость — аппроксимационная выразимость;

A-полнота — аппроксимационная полнота;

A-замкнутый класс — замкнутый по операциям аппроксимационного замыкания класс;

A-основание — для множества M, $M \subseteq \mathfrak{L}_0^{(1)}$, элемент μ, $\mu \in \xi\mathfrak{L} \setminus \{0\}$, удовлетворяющий равенству $A^{(1)}(M) = M' + \mu^{k'}\mathfrak{L}_0^{(1)}(\mu)$ для некоторого целого неотрицательного числа k' и множества M' степени меньшей k;

A-предполный класс — класс, являющийся предполным по операциям аппроксимационного замыкания;

A-критериальная система — система, являющаяся критериальной по операциям аппроксимационного замыкания;

$A(M)$ — A-замыкание множества M линейных автоматов;

$A^{(1)}$-замкнутый класс — подмножество $E_k'(\xi)$, замкнутое относительно $A^{(1)}$-замыкания;

$A^{(1)}$-замыкание — оператор аппроксимационного замыкания на $E_k'(\xi)$, индуцированный A-замыканием на $\mathfrak{L}_k$;

$A^{(1)}(M)$ — $A^{(1)}$-замыкание множества M, $M \subseteq E_k'(\xi)$;

$C(f)$ — константа $f(0, 0, \ldots, 0)$;

$C(M)$ — $\cup_{f\in M}C(f)$;

E_k — поле, состоящее из k элементов, где k — натуральная степень простого числа;

E_{k_s} — максимальное собственное подполе поля E_k с номером s;

$E'_k(\xi)$ — кольцо отношений многочленов переменной ξ над полем E_k, знаменатели которых не делятся на ξ;

$F(M)$ — расширение поля F элементами множеством M;

id — тождественный автоморфизм из Ω_k;

$\tilde{I}$ — множество всех автоматов из L_2, сумма модулей коэффициентов при переменных которых не превосходит 1;

J_k^A — множество, состоящее из всех A-предполных классов в $\mathfrak{L}_k$,

$$J_k^A = \{\ T_a,\ V_1,\ V_p,\ M_1\ \mid a \in E_k,\ \},$$

если k – простое число,

$$J_k^A = \{\ T_a,\ V_1,\ V_p,\ M_1,\ P_s\ \mid a \in E_k,\ s \in \{1, 2, \ldots, l\}\},$$

если k не является простым числом;

J_2^S — множество, состоящее из всех S-предполных классов в $\mathfrak{L}$,

$$\left\{\ T_0, T_1, V_1, V_2, M_1, \tilde{M}_i\ \mid\ i = 0, 2, 3, \ldots\ \right\};$$

$J_k^{(1)}$ — множество, состоящее из всех максимальных собственных подалгебр в $E'_k(\xi)$,

$$J_k^{(1)} = \left\{ M_i^{(1)}, R_i^{(1)} | i = 0, 1, \ldots \right\},$$

для простого k, где $M_i^{(1)} = M_{i,\mathrm{id}}^{(1)}$, и

$$J_k^{(1)} = \left\{\ M_{i,\omega}^{(1)}, M_1^{(1)}, R_i^{(1)}, P_s^{(1)}\ \mid\ \omega \in \Omega_k, i = 0, 2, 3, \ldots, s = 1, 2, \ldots, l,\ \right\}$$

для k, не являющегося простым;

J_k — множество, состоящее из всех K-предполных классов в $\mathfrak{L}_k$,

$$\left\{M_{i,\omega}, R_i^d, R_i^e | i = 0, 2, 3, \ldots, \omega \in \Omega_k\right\} \cup J_k^A;$$

J_2^L — множество, состоящее из всех K-предполных классов в L_2,

$$\left\{\ \tilde{T}_0, \tilde{T}_1, \tilde{V}_1, \tilde{V}_2, \tilde{I}, \tilde{R}_i^e, \tilde{R}_i^d\ \mid\ i = 2, 3, \ldots\ \right\};$$

$J_2^{L^0}$ — множество, состоящее из всех K-предполных классов в L_2^0

$$\left\{\ \Theta \cap L_2^0\ \mid\ \Theta \in\ J_2^L \setminus \left\{\tilde{T}_0, \tilde{T}_1\right\}\ \right\};$$

K-выразимость — выразимость при использовании операций композиции;

K-полнота — полнота при использовании операций композиции;

K-замкнутый класс — замкнутый по операциям композиции класс;

K-предполный класс — класс, являющийся предполным по операциям композиции;

K-критериальная система — система, являющаяся критериальной по операциям композиции;

$K(M)$ — замыкание множества линейных автоматов M по операциям композиции;

$K^{(1)}$-замкнутый класс — подмножество $E_k'(\xi)$, замкнутое относительно $K^{(1)}$-замыкания;

$K^{(1)}$-замыкание — оператор замыкания на $E_k'(\xi)$, индуцированный K-замыканием на $\mathfrak{L}_k$;

$K^{(1)}$-выразимость — выразимость в $E_k'(\xi)$ с использованием оператора $K^{(1)}$-замыкания;

$K^{(1)}$-полнота — полнота в $E_k'(\xi)$ с использованием оператора $K^{(1)}$-замыкания;

$K^{(1)}$-предполный класс — максимальный собственный $K^{(1)}$-замкнутый подкласс в $E_k'(\xi)$;

$K^{(1)}(M)$ — замыкание множества M, $M \subseteq E'_k(\xi)$, по операциям, индуцированным операциями K-замыкания на $\mathfrak{L}_k$;

L_2 — множество, состоящее из всех ЛАА;

L_2^0 — множество всех однородных автоматов из L_2;

M_1 — множество, состоящее из всех линейных автоматов рассматриваемого в контексте класса $\mathfrak{L}_k$, выход которых в следующем за начальным состоянии не зависит от входов в начальный момент времени;

$M_1^{(1)}$ — состоит из всех μ, $\mu \in E'_k(\xi)$, для которых имеет место включение: $\mu - \mu(0) \in \xi^2 E'_k(\xi)$;

$M_{0,\omega}$ — все дроби μ из $E'_k(\xi)$, для которых выполнено равенство $\mu'(0) = \omega(\mu(0))$, где $\mu'(\xi) = \mu(1/\xi)$ и $\mu'(\xi) \in E'_k(\xi)$;

$M_{i,\omega}^{(1)}$ — все дроби μ из $E'_k(\xi)$, которые можно представить в виде $p_i\mu' + u'$, где $\mu' \in E'_k(\xi)$, $u' \in E_k[\xi]$, $\deg u' < \deg p_i$ и $u' = \omega(\mu(0))$, i=2,3,...;

$\tilde{M}_i$ — $\left\{\ f \ \mid\ U(f) \subset \tilde{M}_i^{(1)}\ \right\}$;

$\tilde{M}_0^{(1)}$ — множество всех дробей кольца $E'_k(\xi)$, степень числителя которых не превосходит степени знаменателя;

$\tilde{M}_j^{(1)}$ — множество всех дробей из $E'_k(\xi)$, знаменатель которых не делится на p_j;

$M_{i,\omega}$ — множество всех линейных автоматов f таких, что $U(f) \subset M_{i,\omega}^{(1)}$, $i = 0, 2, 3, \ldots$, $\omega \in \Omega_k$;

$M^{(1)}(\mu, u_0)$ —

$$\left\{ a_0 + \mu u_0(\mu)\frac{u(\mu)}{v(\mu)} \middle| \; a_0 \in E_2, u(\xi) \in E_2[\xi], v(\xi) \in 1 + \xi E_2[\xi], (u_0(\xi), v(\xi)) = 1 \right\},$$

где $\mu \in \xi\mathfrak{L}_0^{(1)}$, $u_0 \in E_2[\xi] \setminus \{0\}$;

$\mathbb{N}$ — множество всех натуральных чисел;

Ω_k — множество всех автоморфизмов поля E_k;

P_k — класс всех функций k-значной логики, где k — натуральное число, $k \geq 3$;

P_s — множество, состоящее из всех линейных автоматов рассматриваемого в контексте класса $\mathfrak{L}_k$, свободный член каждого коэффициента при переменной которых содержится в E_{k_s};

$P_s^{(1)}$ — множество всех дробей μ из $E_k'(\xi)$, для которых выполнено включение $\mu(0) \in E_{k_s}$;

$P^{(1)}(\mu, u_0)$ —

$$\Big\{a_0 + \mu u_0(\mu)\frac{u(\mu)}{v(\mu)} | a_0 \in E_2, u(\xi) \in E_2[\xi],$$
$$v(\xi) \in 1 + \xi E_2[\xi], (u_0(\xi), v(\xi)) = 1,$$
$$\deg u(\xi) \leq \deg v(\xi) - 2(1 + \deg u_0(\xi))\Big\},$$

где $\mu \in \xi \mathfrak{L}_0^{(1)}$, $u_0 \in E_2[\xi] \setminus \{0\}$;

$E_k[\xi]$ — кольцо многочленов переменной ξ над полем E_k;

p_1, p_2, ... — последовательность всех (различных) приведенных неприводимых многочленов из $E_k[\xi]$, $p_1 = \xi$;

$\tilde{p}_1$, $\tilde{p}_2$, ... — последовательность всех (различных) простых чисел, $\tilde{p}_1 = 2$;

$R_k(\mu_0)$ — кольцо формальных степенных рядов переменной μ_0 над полем E_k;

$R_0^{(1)}$ — множество дробей из $E_k'(\xi)$, степень числителя которых меньше степени знаменателя;

$R_i^{(1)}$ — множество всех дробей из $E_k'(\xi)$, несократимый вид которых имеет числитель делящийся на p_i;

$\tilde{R}_i^e$ — множество всех ЛАА с не более чем одной существенной переменной, знаменатель коэффициента при существенной переменной которых не делятся на $\tilde{p}_i$, а также всех ЛАА, числители коэффициентов при переменных которых делятся на $\tilde{p}_i$;

$\tilde{R}_i^d$ — множество всех ЛАА, знаменатель коэффициента которой при единственной непосредственной переменной не делятся на $\tilde{p}_i$, а числители остальных коэффициентов при переменных делятся на $\tilde{p}_i$;

R_j^d —

$$\Bigg\{\ f\ \mid\ f \in \mathfrak{L}_k,\ \ f\left(x_1, x_2, \ldots, x_n\right)=\sum_{i=1}^n \mu_i x_i+\mu_0,$$
$\forall i, i=1,2,\ldots,n,$ если x_i — единственная непосредственная переменная ЛА $f,$ то $\mu_i \in \tilde{M}_j^{(1)},$ в противном случае: $\mu_i \in R_j^{(1)}$ $\Bigg\}$,

$j=0,2,3,\ldots;$

R_j^e —

$$\Bigg\{\ f\ \mid\ f \in \mathfrak{L}_k,\ \ f\left(x_1, x_2, \ldots, x_n\right)=\sum_{i=1}^n \mu_i x_i+\mu_0,$$
$\forall i, i=1,2,\ldots,n,$ если x_i — единственная существенная переменная ЛА $f,$ то $\mu_i \in \tilde{M}_j^{(1)},$ в противном случае: $\mu_i \in R_j^{(1)}$ $\Bigg\}$,

$j=0,2,3,\ldots;$

$R^{(1)}(\mu, u_0)$ —

$$\left\{u_0(\mu)\frac{u(\mu)}{v(\mu)} \mid u(\xi) \in E_2[\xi], v(\xi) \in 1+\xi E_2[\xi], (u_0(\xi), v(\xi))=1\right\},$$

где $\mu \in \xi\mathfrak{L}_0^{(1)}$, $u_0 \in E_2[\xi] \setminus \{0\}$;

S-полнота — полнота при использовании операций суперпозиции;

S-замкнутый класс — замкнутый по операциям суперпозиции класс;

S-предполный класс — класс, являющийся предполным по операциям суперпозиции;

S-система — Множество линейных автоматов, которое содержит существенный автомат, а его A-замыкание содержит все константы;

S_0-система — множество ЛА, содержащее существенный ЛА, и в K-замыкание которого входит нулевая константа;

S-критериальная система — система, являющаяся критериальной по операциям суперпозиции;

$S(M)$ — замыкание множества линейных автоматов M по операциям суперпозиции;

$S^{(1)}(M)$ — замыкание множества M, $M \subseteq E'_k(\xi)$, по операциям сложения и умножения;

$S(\hat{V})$ — замыкание множества векторов $\hat{V}$ по операции сложения;

$S(M, C)$ —

$$\left\{ \sum_{\substack{\gamma \in C',\\ \mu \in K^{(1)}(M)}} \mu\gamma \quad | \quad C' \subset C, \ |C'| < \infty \right\},$$

где $M \subseteq \mathfrak{L}_0^{(1)}$ и $C \subseteq \mathfrak{L}_c$;

T_a — множество, состоящее из всех линейных автоматов рассматриваемого в контексте класса $\mathfrak{L}_k$, сохраняющих элемент a поля E_k в начальный момент времени;

$\tilde{T}_a$ — множество, состоящее из всех ЛАА, сохраняющих элемент a множества E_2 в начальный момент времени;

$U(f)$ — множество коэффициентов при переменных линейного автомата f;

$U(M)$ — $\cup_{f \in M} U(M)$ для множества линейных автоматов M;

$\tilde{U}(f)$ — множество коэффициентов при переменных ЛАА f;

V_1 — множество, состоящее из всех линейных автоматов рассматриваемого в контексте класса $\mathfrak{L}_k$, имеющих не более одной непосредственной переменной;

$\tilde{V}_1$ — множество, состоящее из всех ЛАА, имеющих не более одной непосредственной переменной;

V_p — множество, состоящее из всех линейных автоматов рассматриваемого в контексте класса $\mathfrak{L}_k$, суммы (по простому модулю p) свободных членов коэффициентов при переменных которых равна 1;

$\tilde{V}_2$ — множество, состоящее из всех ЛАА, имеющих нечетное число непосредственных переменных;

$V^{(r_0)}(f)$ — $(b, a_0, a_1, \dots, a_{r_0-1})$, где $f(0,\dots,0) = \sum_{t=0}^{\infty} a_t \xi^t$, $b = 0$, если f имеет нечетное число непосредственных переменных, и $b = 1$, в противном случае;

$V^{(r_0)}(M)$ — $\cup_{f \in M} \left\{ V^{(r_0)}(f) \right\}$, где $M \subseteq \mathfrak{L}$;

$\tilde{V}^{(T_0)}(f)$ — $(a_0, a_1, \dots, a_{T_0-1})$, где $f(0,\dots,0) = \sum_{t=0}^{\infty} a_t \xi^t$;

$\tilde{V}^{(T_0)}(M)$ — $\cup_{f \in M} \left\{ \tilde{V}^{(T_0)}(f) \right\}$, где $M \subseteq \mathfrak{L}$;

$\Sigma(C)$ — замыкание по операциям сложения множества C, $C \subseteq \mathfrak{L}_c$;

τ-замкнутый класс — множество конечных автоматов, из которого нельзя получить отображений на словах длины τ, кроме тех, которые определяются автоматами из этого множества, τ — натуральное число;

τ-полнота — полнота на словах длины τ, где τ — натуральное число;

τ-предполный класс — максимальный собственный τ-замкнутый подкласс класса конечных автоматов, рассматриваемых как отображения на словах длины τ, τ — натуральное число;

$\mathfrak{L}_k$ — множество всех линейных автоматов над полем E_k;

$\mathfrak{L}$ — множество всех линейных автоматов над полем E_2;

$\mathfrak{L}_0^{(1)}$ — множество одноместных линейных автоматов, сохраняющих константу 0;

$\mathfrak{L}_c$ — множество ЛА, реализующих константы;

$\mathfrak{L}_0$ — множество, состоящее из всех ЛА f, для которых $C(f) = 0$.

Список литературы

1. Аблаев Ф. М. О сравнительной сложности вероятностных и детерминированных автоматов // Дискретная математика. — 1991. — Т. 3, № 2. С. 114–120.
2. Алексеев В. Б., Ложкин С. А. Элементы теории графов, схем и автоматов // М.: Изд. отдел ф-та ВМиК МГУ, 2000. — 58 с.
3. Алексеев Д. В. Приближение функций нескольких переменных нейронными сетями // Фундамент. и прикл. матем. — 2009. — Т. 15, вып. 3. — С. 9–21.
4. Алешин С. В. Конечные автоматы и проблема Бернсайда о периодических группах // Мат. заметки. — 1972. — Вып. 3. — С. 319–328.
5. Алешин С. В., Пантелеев П. А. Конечные автоматы и числа // Дискретная математика. — 2015. — Т. 27, вып. 4. — С. 3–20.
6. Алисейчик П. А., Вашик К., Кудрявцев В. Б., Перетрухин В. В., Строгалов А. С. Об автоматном моделировании процесса обучения // Дискретная математика — 1996. — Т. 8, вып. 4. — С. 3-–10.
7. Андреев А. Е., Часовских А. А. Автоматная сложность двуместных булевых базисов // Дискретная математика — 1996. — Т. 8, вып. 4. — С. 123-–133.
8. Бабин Д. Н. Разрешимый случай задачи о полноте автоматных функций // Дискретная математика. — 1992. — Т. 4, № 4. С. 41–55.
9. Бабин Д. Н. О классификации автоматных базисов Поста по разрешимости свойств полноты и А-полноты // Докл. РАН. — 1999. — Т. 367, № 4. — С. 439–441.
10. Бабин Д. Н. О классификации базисов в P_k по разрешимости проблемы полноты для автоматов // Фундамент. и прикл. матем. — 2009. — Т. 15, № 3. С. 33–47.
11. Бабин Д. Н. Автоматы с суперпозициями, пример нерасширяемости до предполного класса // Интеллектуальные системы. Теория и приложения. — 2015. — Т. 19, вып. 3. — С. 87–93.

12. Бабин Д. Н., Летуновский А. А. О возможностях суперпозиции, при наличии в базисе автоматов фиксированной добавки из булевых функций и задержки // Интеллектуальные системы. Теория и приложения. — 2015. — Т. 19, вып. 3. — С. 71—78.
13. Бабин Д. Н., Мазуренко И. Л., Холоденко А. Б. Автоматные языки с частотным свойством естественных языков // Интеллектуальные системы в производстве. — 2013/ — № 1. С. 9–13.
14. Богомолов А. М., Грунский И. С., Сперанский Д. В. Контроль и преобразования дискретных автоматов / М.: URSS, 1975. — 174 с.
15. Болотов А. А. О задачах сводимости и выразимости для однородных структур со входами и выходами // М.: ДАН СССР. — 1980.—Т. 254, № 1. — С. 14–16.
16. Боревич З. И., Шафаревич И. Р. Теория чисел / Изд. 3. — М: Наука, Гл. ред. физ.-мат. лит., 1985. — 504 с.
17. Буевич В. А. Об алгоритмической неразрешимости распознавания А-полноты для о.-д. функций // Мат. заметки. — 1972. — Вып. 6. — С. 687–697.
18. Будах Л. Лабиринты и автоматы // Проблемы кибернетики. — 1978. — Вып. 34. — С. 83–94.
19. Бухараев Р. Г. Основы теории вероятностных автоматов / М: Наука, 1985. — 288 с.
20. Ван дер Варден Б. Л. Алгебра / М.: Наука, 1976. — 648 с.
21. Ветренникова Е. В. Построение простейшей универсальной о.-д. функции // Математические вопросы кибернетики. — 1988. — Вып. 1. — С. 237–241.
22. Волков Н. Ю. Автоматная модель преследования // Интеллектуальные системы. — 2007.— Т. 11, вып. 1–4. — С. 749–752.
23. Гаврилов Г. П., Сапоженко А. А. Сборник задач по дискретной математике / М.: Наука, 1977. — 368 с.
24. Галатенко А. В. Автоматные модели защищенных компьютерных систем // Интеллектуальные системы. 2007. — Т. 11, вып. 1–4. — С. 403–418.

25. Гасанов Э. Э. Прогнозирование периодических сверхсобытий автоматами // Интеллектуальные системы. Теория и приложения. — 2015. — Т. 19, вып. 1. — С. 23–34.
26. Гасанов Э. Э., Мастихина А. А. Прогнозирование общерегулярных сверхсобытий автоматами // Интеллектуальные системы. Теория и приложения. — 2015. — Т. 19, вып. 3. — С. 127–154.
27. Гашков С. Б., Фролов А. Б. Дискретная математика / М.: Юрайт, 2018. — 448 с.
28. Гербуз В. Г. О связи функций автомата и автоматной функции // Интеллектуальные системы. Теория и приложения. — 2015. — Т. 19, вып. 2. — С. 135–142.
29. Гилл А. Линейные последовательностные машины / М.: Наука, 1974. — 288 с.
30. Глушков В. М. Синтез цифровых автоматов / М.: Физматгиз, 1962. — 476 с.
31. Елкин В. И., Высоцкий М. Н. О связи между декомпозициями автоматов и формальных грамматик // Моделирование, декомпозиция и оптимизация сложных динамических процессов. — 2011. — Т. 26, № 1. — С. 24-31.
32. Жук Д. Н. О неразрешимости проблемы полноты для дефинитных автоматов // Интеллектуальные системы. — 2008. — Т. 12. — С. 211–228.
33. Жук Д. Н. Континуальность множества предполных классов в классе дефинитных автоматов // Фундаментальная и прикладная математика. — 2009. — Т. 15, вып. 4. — С. 29—36.
34. Зарисский О., Самюэль П. Коммутативная алгебра: в 2 т. / М.: ИЛ, 1963. — 2 т. 444 с.
35. Карацуба А. А. Решение одной задачи из теории конечных автоматов // УМН. — 1960. — Т. 15, Вып. 3. — С. 157–159.
36. Клини С. К. Представление событий в нервных сетях и конечных автоматах // Автоматы. — М.: ИЛ, 1956. — С. 15-67.
37. Коршунов А. Д. О перечислении конечных автоматов // Проблемы кибер-

нетики. — 1978. — Вып. 34. — С. 5–82.

38. Кратко М. И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов // ДАН СССР. — 1964. — Т. 155, № 1. — С. 35–37.
39. Кудрявцев В. Б. Теорема полноты для одного класса автоматов без обратных связей // Проблемы кибернетики. — 1962. — Вып. 8. — С. 91–115.
40. Кудрявцев В. Б. О мощности множеств предполных множеств некоторых функциональных систем, связанных с автоматами // Проблемы кибернетики. — 1965. — Вып. 13. — С. 45–74.
41. Кудрявцев В. Б. О полноте для функциональных систем // ДАН СССР. — 1981. — Т. 257, № 2. — С. 274-278.
42. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов / М.: Наука, 1985. — 320 с.
43. Кучеренко И. В. О структуризации класса обратимых клеточных автоматов // Дискретная математика. — 2007. — Т. 19, № 3. С. 102–121.
44. Ленг С. Алгебра / М.: Мир, 1968. — 564 с.
45. Летичевский А. А. Условия полноты для конечных автоматов // ВМ и МФ. — 1961. — № 4. С. 702–710.
46. Летуновский А. А. Выразимость линейных автоматов относительно расширенной суперпозиции // Интеллектуальные системы. Теория и приложения. — 2015. — Т. 19, вып. 1. — С. 161–170.
47. Лидл Р., Нидеррайтер Г. Конечные поля: в 2 т. / М.: Мир, 1988. — Т. 1. 425 с.
48. Лунц А. Г. p-адический аппарат в теории конечных автоматов // Проблемы кибернетики. — 1965. — Вып. 14. — С. 17–30.
49. Мазуренко И. Л. Автоматные методы распознавания речи: диссертация на соискание ученой степени кандидата физ.-мат. наук. — М., 2001. — 119 с.
50. Михалев А. В., Нечаев А. А. Цикловые типы семейств полилинейных рекуррент и датчики псевдослучайных чисел // Математические вопросы крип-

тографии. — 2014. — Т. 5, вып. 1, — С. 95–125.

51. Минский М. Л. Некоторые универсальные элементы для конечных автоматов // Автоматы. — М.: ИЛ, 1956. — С. 163-178.
52. Миронов А. М. Морфизмы реакции для автоматов в категориях: диссертация на соискание ученой степени кандидата физ.-мат. наук. — М., 1992. — 151 с.
53. Мур Э. Ф. Умозрительные эксперименты с последовательными машинами // Автоматы. — М.: ИЛ, 1956. — С. 179-210.
54. Нейман Дж. Вероятностная логика и синтез надежных организмов из ненадежных компонент // Автоматы. — М.: ИЛ, 1956. — С. 68-139.
55. Носов В. А. О связи периодов состояний и периодов выходов автономных автоматов // Лесной вестник. — 2007. — Вып. 2. — С. 144-149.
56. Пантелеев П. А. Об отличимости состояний автоматов // Дискретная математика. — 2003.— Т. 15, вып. 3. — С. 76–90.
57. Пантелеев П. А. Об отличимости состояний решетчатых автоматов // Интеллектуальные системы. — 2005.— Т. 8, вып. 1–4. С. 529–542.
58. Пантелеев П. А. Об отличимости состояний автомата при искажениях на входе // Интеллектуальные системы. — 2007.— Т. 11, вып. 1–4. С. 653–678.
59. Подколзин А. С. О сложности моделирования в однородных структурах // Проблемы кибернетики. — М.: Наука, 1975. — Вып. 30. — С. 199–225.
60. Подколзин А. С. О поведениях однородных структур // Проблемы кибернетики. — М.: Наука, 1976. — Вып. 31. — С. 133–166.
61. Подколзин А. С. Об универсальных однородных структурах // Проблемы кибернетики. — М.: Наука, 1978. — Вып. 34. — С. 109–131.
62. Половников В. С. О некоторых характеристиках нейронных схем // Интеллектуальные системы. — 2004.— Т. 8, вып. 1–4. — С. 121–145.
63. Родин С. Б. Линейно реализуемые автоматы // Дискретная математика. — 2017. — Т. 29, № 1. — С. 59–79.
64. Саломаа А. Аксиоматизация алгебры событий, реализуемых логически-

ми сетями // Проблемы кибернетики. — М.: Наука, 1966. — Вып. 17. — С. 237–246.

65. Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста / М.: Наука, 1966. — 120 с.
66. Часовских А. А. Об алгоритмической разрешимости проблемы полноты для линейных автоматов // Вестник Московского университета сер. 1, мат., мех. — 1986. — № 3. — С. 82–84.
67. Часовских А. А. О выразимости систем с сумматором в классе линейных автоматов // Вестник Московского университета сер. 1, мат., мех. — 1990. — № 4. — С. 31–34.
68. Часовских А. А. О полноте в классе линейных автоматов // Математические вопросы кибернетики. — 1991. — Вып. 3. — С. 140–166.
69. Часовских А. А. Замкнутые классы линейно-автоматных функций // Математические вопросы кибернетики. — 2004. — Вып. 13. — С. 113–136.
70. Часовских А. А. Об A-выразимости в классе линейно автоматных функций // Математические вопросы кибернетики. — 2008. — Вып. 17. — С. 105–136.
71. Часовских А. А. О проблеме полноты в классе линейно-автоматных функций над простыми конечными полями // в сборнике Материалы международной конференции «Современные проблемы математики, механики и их приложений», посвященной 70-летию ректора МГУ академика В.А.Садовничего. — 2009. — С. 379–379.
72. Часовских А. А. О полноте в классе линейно-автоматных функций с операциями суперпозиции // в сборнике Материалы XI Международного семинара «Дискретная математика и ее приложения» (Москва, 18-23 июня 2012 г.), 2012 — С. 382–385.
73. Часовских А. А. Линейно-автоматные функции с операциями суперпозиции // Нейрокомпьютеры: разработка, применение. — 2013. — № 8. — С. 3–13.

74. Часовских А. А. О полноте в классе конечных автоматов, вычисляющих некоторые аффинные функции // Интеллектуальные системы. — 2013. — Т. 17, вып. 1–4. — С. 202–205.
75. Часовских А. А. Условия полноты линейно-р-автоматных функций // Интеллектуальные системы. Теория и приложения. — 2014. — Т. 18, вып. 3. — С. 203–252.
76. Часовских А. А. Проблема A-полноты линейно-автоматных функций над конечным полем // Интеллектуальные системы. Теория и приложения. — 2014. — Т. 18, вып. 1. — С. 253–257.
77. Часовских А. А. Проблема полноты для класса линейно-автоматных функций // Дискретная математика. — 2015. — Т. 27, № 2. — С. 134–151. Перевод: Chasovskikh A. A. Completeness problem for the class of linear automata functions // Discrete Mathematics and Applications. – 2016. – Vol. 26, Iss. 2. – Pp. 89–104.
78. Часовских А. А. Критериальные системы в классах линейно-автоматных функций над конечными полями // Интеллектуальные системы. Теория и приложения. — 2015. — Т. 19, вып. 3. — С. 195–207.
79. Часовских А. А. Сравнение операторов замыкания в классе линейно-автоматных функций // Интеллектуальные системы. Теория и приложения. — 2016. — Т. 20, вып. 3. — С. 120–124.
80. Часовских А. А. О полноте в классе линейных 2-адических автоматов // Интеллектуальные системы. Теория и приложения. — 2016. — Т. 20, вып. 4. — С. 209–227.
81. Часовских А. А. Проблема полноты в классах линейных автоматов // Интеллектуальные системы. Теория и приложения. — 2018. — Т. 22, вып. 2. — С. 151–154.
82. Часовских А. А. Приведенные критериальные системы предполных классов в классах линейных автоматов над конечными полями // Интеллектуальные системы. Теория и приложения. — 2018. — Т. 22, вып. 4. — С. 115–134.

83. Часовских А. А. О числе максимальных надклассов в классе линейных автоматов // Интеллектуальные системы. Теория и приложения. — 2019. — Т. 23, вып. 3. — С. 81–84.
84. Часовских А. А. О классах передаточных функций линейных автоматов // Интеллектуальные системы. Теория и приложения. — 2019. — Т. 23, вып. 3. — С. 135–142.
85. Часовских А. А. О проблеме полноты в классах линейных автоматов над конечными полями // в сборнике Материалы XIII Международного семинара «Дискретная математика и ее приложения» (Москва, 17-22 июня 2019 г.), 2019 — С. 50–59.
86. Часовских А. А. Максимальные подклассы в классах линейных автоматов над конечными полями // Дискретная математика. — 2019. — Т. 31, № 4. — С. 88–101. Перевод: Chasovskikh A. A. Maximum subclasses in classes of linear automata over finite fields // Discrete Mathematics and Applications. – 2020. – Vol. 30, Iss. 6. – Pp. 365–374.
87. Часовских А. А. Классы линейных p-автоматов с операциями суперпозиции // Интеллектуальные системы. Теория и приложения. — 2021. — Т. 25, вып. 2. — С. 155–156.
88. Hensel K. Zahlentheorie / Berlin und Leipzig: G.m.b.H., 1913. — 449 p.
89. Budach L. Automata and labyrinth // Mathematische Nachrichten. — 1978. — Vol. 86. — P. 195–282.
90. Chung J., Gulcehre C., KyungHyun C., Yoshua B. Empirical Evaluation of Gated Recurrent Neural Networks on Sequence Modeling // [Электронный ресурс]: Cornell University. URL: https://arxiv.org/pdf/1412.3555.pdf (дата обращения 05.01.2019).
91. Goto E. A Minimal Time Solution of the Firing Squad Problem // Dittoed course notes for Applied Mathematics, Harvard University 298. — 1962. — P. 52–59.
92. Hochreiter S., Schmidhuber J. Long Short-Term Memory // Neural

Computation. — 1997. — Vol. 9, № 8. P. 1735–1780.

93. Hopfield J. J. Neural networks and physical systems with emergent collective computational abilities // Proceedings of National Academy of Sciences. — 1982. — Vol. 79, № 8. P. 2554–2558.
94. Lau D. Function Algebras on Finite Sets. A Basic Course on Many-Valued Logic and Clone Theory / Rostok: Springer, 2006. — 668 p.
95. Moore E. F. Machine models of self-reproduction // Math. Soc. Proc. of Symposia in Applied Mathematics. — 1962. — Vol. 14. — P. 17–33.
96. Myhill J. The converse of Moore's Garden-of-Eden theorem // Proc. Amer. Math. Soc. — 1963. — Vol. 14. — P. 685–686.
97. Post E. L. The two-valued iterative systems of mathematical logic //Annals of Mathematics studies / Princeton: Princeton University Press, 1941. — № 5, —122 p. Post E. L. Introduction to a General Theory of Elementary Propositions // American Journal of Mathematics. — 1921. — Vol. 43, No 3. — P. 163–185.
98. Rabin M. O. Probabilistic automata // Information and Control, — 1963. — Vol. 6, № 3. — P. 230–245.
99. Rosenberg I. G. The number of maximal closed classes in the set of functions over a finite domain // Journal of Combinatorial Theory, — 1973. — Vol. 14. — P. 1–7.
100. Streich W. J., Rösner Th. / Theorie linearer Automaten / Berlin.: VEB Deutscher Verlag der Wissenschaften, 1978. — 158 p.
101. Szendrei Á. On closed classes of quasilinear functions // Chechoslovak Math. J. — 1980. — Vol. 30, No 3. — P. 498–509.
102. Von Neumann J. A., Burks W. Theory of Self-Reproducing Automata / Urbana, London: University of Illinois Press, 1966. — 388 p.