В.В. Скобелев

АВТОМАТЫ НА АЛГЕБРАИЧЕСКИХ СТРУКТУРАХ

Модели и методы их исследования

ИПММ НАНУ

НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК УКРАИНЫ

ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ И МЕХАНИКИ

В.В. Скобелев

АВТОМАТЫ НА АЛГЕБРАИЧЕСКИХ СТРУКТУРАХ

Модели и методы их исследования

Донецк

2013

УДК 512.7+519.7+681.3

Рецензенты:

Академик НАН Украины, зав. отделом теории цифровых автоматов ИК НАН Украины им. В.В. Глушкова *А.А. Летичевский*

Член-корреспондент НАН Украины, декан факультета кибернетики Киевского национального университета имени Тараса Шевченко, *А.В. Анисимов*

Автоматы на алгебраических структурах. Модели и методы их исследования
В.В. Скобелев. ИПММ НАН Украины, Донецк, 2013. – 307 с.

ISBN 978-966-02-7097-8

Монография посвящена разработке методов анализа семейств автоматов, заданных рекуррентными соотношениями на алгебраических структурах над конечным кольцом. Разработаны методы решения систем уравнений с параметрами над конечным кольцом. Построен решатель, предназначенный для проверки выполнимости формул линейной арифметики над конечным кольцом. Решены задачи построения имитационной модели для семейства автоматов и анализа вычислительной стойкости семейств хеш-функций, определяемых сильно-связанными автоматами без выхода. Исследованы семейства автоматов, заданных на многообразиях с алгеброй, на параметризованных многообразиях с выделенным множеством траекторий, а также на эллиптических кривых.

Для специалистов в областях алгебраической теории автоматов, прикладной теории алгоритмов, дискретной математики и защиты информации, а также для студентов и аспирантов, специализирующихся в этих областях. Монография также может быть использована преподавателями ВУЗов при разработке соответствующих спецкурсов.

Утверждено к печати Ученым советом Института прикладной математики и механики НАН Украины (*протокол № 11 от 20.12.2013*)

Автомати на алгебраїчних структурах. Моделі та методи їх дослідження
В.В. Скобелєв. ІПММ НАН України, Донецьк, 2013. – 307 с. (на російській мові)

ISBN 978-966-02-7097-8

Монографія присвячена розробці методів аналізу сімей автоматів, які визначено рекурентними співвідношеннями на алгебраїчних структурах над скінченним кільцем. Розроблено методи розв’язку систем рівнянь з параметрами над скінченним кільцем. Побудовано вирішувач, який призначено для перевірки виконуємості формул лінійної арифметики над скінченним кільцем. Вирішено задачі побудови імітаційної моделі для сім’ї автоматів та аналізу обчислювальної стійкості сімей геш-функцій, які визначено сильно зв’язаними автоматами без вихідної функції. Досліджено сім’ї автоматів, які визначено на многовидах з алгеброю, на параметризованих многовидах з виділеною множиною траєкторій, а також на еліптичних кривих.

Для спеціалістів в галузях алгебраїчної теорії автоматів, прикладної теорії алгоритмів, дискретної математики та захисту інформації, а також для студентів та аспірантів, які спеціалізуються у цих галузях. Монографію також може бути використано викладачами Вищих при розробці відповідних спецкурсів.

ISBN 978-966-02-7097-8

Предисловие

Внедрение информационных технологий практически во все сферы деятельности современного общества выделило ряд актуальных проблем, возникающих как в процессе их разработки, так и в процессе их применения. Одной из основных таких проблем является защита информации. Актуальность этой проблемы при массовом использовании информационных технологий явилась катализатором интенсивного развития криптографии.

Начиная с 80-х годов XX столетия развитие криптографии (см., напр., [4,30,113]) во-многом, определялось разработкой математических моделей шифров, совершенно различных по своей структуре. Такие модели часто были недостаточно исследованы с теоретических позиций. Как следствие, основным методом исследования в криптографии стал статистический анализ качества разрабатываемых шифров. Просчеты, допускаемые при таком анализе, а также интенсивное развитие средств вычислительной техники являются основными причинами достаточно частого пересмотра криптографических стандартов во всем мире.

В настоящее время наблюдается устойчивая тенденция перехода криптографии к моделям, построенным на основе конечных алгебраических систем. Эта тенденция подтверждается фрагментарным использованием вычислений в кольцах вычетов практически во всех кандидатах на современные шифры, становлением асимметричной криптографии на основе теоретико-числовых алгоритмов, а также интенсивным развитием эллиптической криптографии (см., напр., [10,12,14,33,109,110,207]).

Таким образом, на современном этапе развития криптографии созданы объективные предпосылки для формирования раздела теории дискретных преобразователей, предназначенного для исследования автоматно-алгебраических моделей, заданных на конечных алгебраических структурах. Фундамент для формирования такого раздела может быть охарактеризован следующим образом.

Во-первых, теория дискретных преобразователей, как раздел теории алгоритмов, достаточно интенсивно развивается с 70-х годов XX столетия (см., напр., [5,21]).

Во-вторых, именно под влиянием задач криптографии в настоящее время происходит переосмысление актуальности задач, решаемых в рамках теории (абстрактных) конечных автоматов. В частности, значительное внимание уделяется построению приближенных моделей конечного автомата (в [8] содержится обзор результатов, полученных в этом направлении), а также оценке числа прообразов выходной последовательности автомата (см., напр., [26,55-57,63]).

В-третьих, в 70-е годы XX столетия были исследованы линейные рекуррентные последовательности над конечными полями (см., напр., [228]). Именно под влиянием задач криптографии в настоящее время осуществляется исследование свойств линейных и полилинейных рекуррентных последовательностей над конечными кольцами (см., напр., [41,42]).

В четвертых, в 70-е годы XX столетия были исследованы свойства линейных последовательностных машин над конечными полями (см., напр., [1,2,9,12,16,54]). Результаты исследования нелинейных последовательностных машин специального типа над конечными полями представлены в [107]. В [66,80] исследованы свойства автоматов, заданных системами рекуррентных соотношений над конечными ассоциативно-коммутативными кольцами, с позиции их возможного применения в качестве математических моделей поточных шифров.

В пятых, в рамках алгебраической теории автоматов достаточно подробно исследована структура выходных полугрупп отображений, реализуемых абстрактными конечными автоматами (см., напр., [18,19,114,115,117,159,160]).

Из всего сказанного выше вытекает, что задачи криптографии естественно приводят к необходимости формирования нового раздела алгебраической теории автоматов, объектом исследования которого являются автоматы, заданные рекуррентными соотношениями на конечных алгебраических структурах, а предметом исследования – анализ вычислительной стойкости соответствующих автоматных отображений.

В качестве основной алгебраической структуры естественно выбрать ассоциативное конечное кольцо с ненулевым умножением. Такой выбор целесообразен в связи с тем, что конечные поля представляют собой специальный случай ассоциативно-коммутативных колец с единицей. Кроме того, такие особенности строения колец, как возможное отсутствие операции деления, единицы, свойства коммутативности умножения, а также возможное наличие делителей нуля существенно затрудняют анализ систем уравнений (особенно с параметрами) над кольцом. Это обстоятельство дает возможность обеспечить высокую сложность решения задач идентификации (параметрической и начального состояния) автомата, определенного рекуррентными соотношениями над ассоциативным кольцом.

Цель настоящей монографии состоит в построение семейств автоматов, заданных рекуррентными соотношениями на алгебраических структурах, определяемых над конечным ассоциативным кольцом, а также разработке методов анализа этих семейств автоматов, прежде всего, с позиции их возможного применения при решении задач защиты информации.

Монография состоит из шести разделов и заключения.

В разделе 1 содержится математический аппарат, необходимый для изложения материала в последующих разделах. Рассмотрены основные алгебраические системы, многообразия над кольцами, плоские алгебраические кривые, эллиптические кривые над полями. Охарактеризованы модели конечных автоматов, а также существующие подходы к решению задач идентификации конечных автоматов. Представлена общая схема построения семейств автоматов над конечным кольцом. Рассмотрено современное состояние проблемы выполнимости формул над разрешимыми теориями 1-го порядка. Очерчены задачи, рассматриваемые в последующих разделах.

В разделе 2 исследуются отображения абстрактных множеств в фактор-кольца. Построена и исследована комбинаторная схема, основанная на соотношении между множествами отображений абстрактного множества в полную систему вычетов по попарно взаимно простым идеалам ассоциативно-коммутативного кольца и множеством отображений этого же множества в полную систему вычетов по произведению этих идеалов. Рассмотрены применения этой комбинаторной схемы для решения модельных алгебраических задач. Построена «ленточная модель», представляющая собой интерпретацию предложенной комбинаторной схемы для кольца целых чисел. Рассмотрены применения «ленточной модели» для решения модельных теоретико-числовых и алгебраических задач. Доказано отсутствие непосредственного обобщения построенной комбинаторной схемы на бесконечное множество фактор-колец.

В разделе 3 предложена общая схема исследования строения множества решений системы полиномиальных уравнений с параметрами над конечным ассоциативным кольцом с единицей. В деталях рассмотрено применение этой схемы к анализу мно-

жества решений системы полиномиальных уравнений с параметрами над кольцом вычетов. Исследованы свойства делителей нуля в ассоциативных кольцах (именно на основе эффективного использования этих свойств осуществляется анализ множества решений уравнений вида «произведение равно нулю»).

В разделе 4 решена задача проверки выполнимости формул линейной арифметики над конечным кольцом. Охарактеризованы основные отличия линейной арифметики над произвольным ассоциативным конечным кольцом с ненулевым умножением от линейной арифметики над кольцом целых чисел. Предложена классификация конечных ассоциативных колец с ненулевым умножением, отражающая различия в построении основных модулей решателя в зависимости от типа рассматриваемого кольца. На основе «наслоения» (layering) построен решатель, предназначенный для проверки выполнимости формул линейной арифметики над любым конечным ассоциативным кольцом с ненулевым умножением. Исследована временная сложность построенного решателя.

В разделе 5 исследуются семейства автоматов, определенные системами рекуррентных соотношений с параметрами над конечным кольцом. Решена задача построения имитационной модели, моделирующей заданное семейство автоматов, определенное системой рекуррентных соотношений с параметрами над конечным кольцом. Для всех комбинаций понятий «в наихудшем случае» и «в среднем», представляющих интерес с позиции прикладной теории алгоритмов, определено понятие «точность имитационной модели». Выделено множество асимптотически точных имитационных моделей, представляющих, по своей сути, формируемый в процессе обучения автомат с конечной памятью. Построено семейство сильно-связанных автоматов без выхода, каждый из которых определяет семейство вычислительно-стойких хеш-функций. Исследованы свойства автоматов, функции переходов и выходов которых являются алгебраическими суммами функции от состояния автомата и функции от входного символа при условии, что значение каждой компоненты функции переходов принадлежит фиксированным идеалам кольца.

В разделе 6 исследуются семейства автоматов, заданные на многообразии, определенном над конечным кольцом. Охарактеризовано строение алгебраических кривых 2-го и 3-го порядков над конечным ассоциативно-коммутативным кольцом. Выделены 2 типа многообразий над конечным кольцом: многообразия с алгеброй и параметризованные многообразия с выделенными на них множествами траекторий. Построены и исследованы семейства автоматов Мили и Мура на многообразиях с алгебрами, а также на параметризованных многообразиях с выделенными на этих многообразиях множествами траекторий (охарактеризованы множества семейств групповых автоматов, автоматов, имеющих состояния-близнецы, автоматов, имеющих состояния-источники, автоматов, имеющих состояния-стоки, связных и сильно-связанных автоматов, а также приведенных автоматов). Охарактеризованы гомоморфизмы построенных множеств семейств автоматов при гомоморфизме рассматриваемых многообразий. Исследованы семейства автоматов Мили и Мура, заданных на эллиптической кривой над конечным полем (выделены множества семейств групповых автоматов, сильно связанных автоматов, автоматов, имеющих состояния-близнецы, обратимых и приведенных автоматов, решена задача идентификации начального состояния автомата, а также задача построения точной имитационной модели).

В заключении охарактеризованы полученные в монографии результаты и указа-

ны возможные направления дальнейших исследований.

Монография написана в замкнутой форме, т.е. определяются все, кроме общепринятых, понятия. В монографии принята нумерация вида «(a, b)», где a – номер раздела, а b – номер (по порядку) внутри данного раздела. Окончания формулировок теорем, лемм, следствий и утверждений, а также окончания доказательств обозначены символом «$\square$».

Представленные в монографии результаты получены автором в соответствии с планами научных исследований, проводимых в ИПММ НАН Украины в рамках следующих тем:

1. Сучасні алгебраїчні, логічні та еволюційні методи веріфікації, ідентифікації і керування дискретними та непервними системами (2009-2013) (НДР № 0109U002770).

2. Обернені задачі теорії керування і сучасні комунікаційні технології (2007-2011) (НДР № 0107U000466).

3. Розробка математичних моделей і методів аналізу динамічних систем із застосуваннями до задач створення нових інформаційних технологій (2012-2016) (НДР № 0111U007275).

Монография предназначена для специалистов в областях алгебраической теории автоматов, прикладной теории алгоритмов, дискретной математики и защиты информации, а также для студентов и аспирантов, специализирующихся в этих областях. Материал, изложенный в монографии также может быть использован преподавателями ВУЗов при разработке соответствующих спецкурсов.

Автор считает своим долгом выразить глубокую и искреннюю благодарность академику НАН Украины А.А. Летичевскому за его внимание и поддержку в процессе выполнения настоящего исследования.

Безусловно, что за все недостатки ответственность несет только автор, который будет благодарен за конструктивные замечания, касающиеся содержания книги.

АВТОР

Ноябрь, 2013 г.,
г. Донецк

СОДЕРЖАНИЕ

1. МОДЕЛИ И МЕТОДЫ

В настоящем разделе изложен математический аппарат, используемый в последующих разделах.

В п.1.1 охарактеризованы основные алгебраические системы, используемые в дальнейшем, а именно: полугруппы, группы, поля, кольца, а также кольца многочленов. В п.1.2 рассмотрены многообразия над кольцами (в том числе полиномиальная и рациональная параметризация этих многообразий), плоские алгебраические кривые (являющиеся специальным случаем многообразия) над кольцом, показана взаимосвязь между свойствами аффинных и проективных кривых над полем, охарактеризованы эллиптические кривые над полями. В п.1.3 представлены модели конечных автоматов, существующие подходы к решению задач идентификации конечных автоматов, а также общая схема построения семейств автоматов над конечным кольцом. П.1.4 содержит обзор современного состояния проблемы выполнимости формул над разрешимыми теориями 1-го порядка. Эта проблема является основой для построения решателей, т.е. программных средств автоматизированного решения задач. В п.1.5 очерчены задачи, рассматриваемые в последующих разделах.

1.1. Алгебраические системы.

В соответствии с [53] любая *алгебраическая система* $\mathfrak{S} = (A, \mathcal{F}, \mathcal{R})$ состоит из множества (основы) A, множества операций $\mathcal{F}$, т.е. отображений $f : A^n \to A$ $(n \in \mathbb{Z}_+)$ и множества отношений $\mathcal{R}$, т.е. подмножеств $\varrho \subset A^n$ $(n \in \mathbb{N})$. Число n называется *арностью* операции $f : A^n \to A$ и отношения $\varrho \subset A^n$. При $n = 2$, как правило, вместо $f(a, b)$ и $(a, b) \in \varrho$ пишут, соответственно, afb и $a\varrho b$. Алгебраическая система называется *алгеброй*, если $\mathcal{R} = \emptyset$, и *моделью*, если $\mathcal{F} = \emptyset$.

Рассмотрим алгебраические системы, в терминах которых будет осуществляться изложение результатов в последующих разделах. Эти алгебраические системы подробно рассмотрены в [13,27,28,36-38,44,45,49,50].

1.1.1. Алгебры с одной бинарной операцией.

Группоидом называется алгебра $\mathcal{G} = (G, \diamond)$, где $\diamond$ – бинарная операция. Величина $|G|$ – *порядок* группоида $\mathcal{G}$.

Пусть $c = a \diamond b$ $(a, b, c \in G)$. Тогда a (соответственно, b) – *левый* (соответственно, *правый*) *делитель* элемента c.

Если существует такой элемент $a \in G$, что:

1) $a \diamond x = x$ (соответственно, $x \diamond a = x$) для всех $x \in G$, то a – *левый* (соответственно, *правый*) *нейтральный элемент* группоида $\mathcal{G}$;

2) $a \diamond x = a$ (соответственно, $x \diamond a = a$) для всех $x \in G$, то a – *левый* (соответственно,*правый*) *нуль* группоида $\mathcal{G}$.

Замечание 1.1. Если существует двусторонний нейтральный элемент (соответственно, двусторонний нуль) группоида, то такой элемент единственный, и обозначается e (соответственно, 0). При этом, если $a \diamond b = e$, то a (соответственно, b) – *левый* (соответственно, *правый*) *обратный элемент* для b (соответственно, для a), а если $a \diamond b = 0$ ($a \neq 0, b \neq 0$), то a (соответственно, b) – *левый* (соответственно, *правый*) *делитель нуля*.

Группоид $\mathcal{G}_2 = (G_2, \diamond_2)$ – *гомоморфный образ* группоида $\mathcal{G}_1 = (G_1, \diamond_1)$, если существует такая сюръекция $h : G_1 \to G_2$, что $h(a \diamond_1 b) = h(a) \diamond_2 h(b)$ для всех $a, b \in G_1$. Такую сюръекцию h называют *гомоморфизмом* $\mathcal{G}_1$ на $\mathcal{G}_2$. Если при этом $h : G_1 \to G_2$ – биекция, то говорят, что группоиды $\mathcal{G}_1$ и $\mathcal{G}_2$ *изоморфны*, а биекцию h называют *изоморфизмом* между $\mathcal{G}_1$ и $\mathcal{G}_2$.

Замечание 1.2. При любом гомоморфизме h группоида $\mathcal{G}_1 = (G_1, \diamond_1)$ на группоид $\mathcal{G}_2 = (G_2, \diamond_2)$:

1) каждый левый (соответственно, правый) нейтральный элемент группоида $\mathcal{G}_1$ отображается в некоторый левый (соответственно, правый) нейтральный элемент группоида $\mathcal{G}_2$;

2) каждый левый (соответственно, правый) нуль группоида $\mathcal{G}_1$ отображается в некоторый левый (соответственно, правый) нуль группоида $\mathcal{G}_2$;

3) каждый левый (соответственно, правый) обратный для $a \in G_1$ элемент отображается в левый (соответственно, правый) обратный для $h(a) \in G_2$ элемент;

4) левые (соответственно, правые) делители нуля группоида $\mathcal{G}_1$ отображаются в левые (соответственно, правые) делители нуля группоида $\mathcal{G}_2$.

Группоид $\mathcal{G} = (G, \diamond)$ называется *абелевым*, если «$\diamond$» – *коммутативная* операция, т.е. $a \diamond b = b \diamond a$ для всех $a, b \in G$.

Говорят, что в группоиде $\mathcal{G} = (G, \diamond)$ выполнен *закон сокращения*, если

$$(\forall a, b, c \in G)((a \diamond c = b \diamond c \Longrightarrow a = b) \wedge (c \diamond a = c \diamond b \Longrightarrow a = b)).$$

Замечание 1.3. Если $|G| > 1$, то группоид $\mathcal{G} = (G, \diamond)$, удовлетворяющий закону сокращения, не содержит нуля.

Квазигруппой называется группоид $\mathcal{G} = (G, \diamond)$, в котором для любых $a, b \in G$ ($a \neq 0$) однозначно разрешимы уравнения $a \diamond x = b$ и $y \diamond a = b$. Квазигруппа $\mathcal{G}$ с нейтральным элементом называется *лупой*.

Полугруппой называется такой группоид $\mathcal{G} = (G, \diamond)$, что «$\diamond$» – *ассоциативная* операция, т.е. $a \diamond (b \diamond c) = (a \diamond b) \diamond c$ для всех $a, b, c \in G$. Степени элемента $a \in G$ определяются равенствами $a^n = \underbrace{a \diamond \cdots \diamond a}_{n \text{ раз}}$ ($n \in \mathbb{N}$). Элементы a^2 ($a \in G \backslash \{0, e\}$) называются *квадратами*, а элементом, *свободным от квадратов*, называется любой такой элемент $b \in G \backslash \{0, e\}$, что $b \notin \{v \diamond u^2 \diamond w, v \diamond u^2, u^2 \diamond w | u \in G \backslash \{0, e\}, v, w \in G\}$.

Замечание 1.4. Поиск квадратов полугруппы $\mathcal{G} = (G, \diamond)$ сводится к поиску решений уравнений вида $x^2 = b$ $(b \in G \backslash \{0, e\})$.

Пусть $\mathcal{G} = (G, \diamond)$ – полугруппа с нейтральным элементом. Если для элемента $a \in G$ существуют и левый, и правый обратные элементы, то они совпадают. Такой элемент a – *обратимый*, а обратный ему элемент обозначается a^{-1}. Элементы множества G^{inv} всех обратимых элементов полугруппы $\mathcal{G}$ называются *делителями нейтрального элемента*, а элементы множества $G \setminus G^{inv}$ – *необратимыми* элементами полугруппы $\mathcal{G}$.

Группой называется такая полугруппа $\mathcal{G} = (G, \diamond)$, что каждое из уравнений $a \diamond x = b$ и $y \diamond a = b$ однозначно разрешимо при любых $a, b \in G$.

Замечание 1.5. В группе выполняется закон сокращения, существует нейтральный элемент, и для каждого элемента существует обратный элемент. Если $|G| > 1$, то группа $\mathcal{G}$ не содержит нуля. Если $|G| = 1$, то единственный элемент множества G одновременно является и нулем, и нейтральным элементом группы $\mathcal{G}$.

Для элемента a группы $\mathcal{G}$ нулевая и отрицательная степени определены равенствами $a^0 = e$ и $a^{-n} = (a^{-1})^n$ $(n \in \mathbb{N})$. Элемент a группы $\mathcal{G}$ имеет *бесконечный* порядок, если все элементы a^n $(n \in \mathbb{N})$ попарно различны. В противном случае, *порядок* элемента a – это такое наименьшее число $n_0 \in \mathbb{N}$, что $a^{n_0} = e$.

Если подмножество H $(\emptyset \neq H \subseteq G)$ замкнуто относительно операции «$\diamond$», а алгебра $\mathcal{H} = (H, \diamond)$ является алгеброй того же типа, что и алгебра $\mathcal{G} = (G, \diamond)$, то имя алгебры $\mathcal{H}$ образуется из имени алгебры $\mathcal{G}$ с помощью приставки «под» (т.е. подгруппоид, подполугруппа, подгруппа и т.д.).

Отметим, что для полугруппы $\mathcal{G} = (G, \diamond)$ с нейтральным элементом подполугруппа $\mathcal{G}^{inv} = (G^{inv}, \diamond)$ является группой.

Пусть $\mathcal{G} = (G, \diamond)$ – группоид, а Ω – такое семейство отображений множества G в себя, что равенство $\omega(a \diamond b) = \omega(a) \diamond \omega(b)$ истинно для любых $\omega \in \Omega$ и $a, b \in G$. Тогда $\mathcal{G}$ называется Ω-*операторным* группоидом.

Замечание 1.6. Если элементам множества Ω соответствуют *эндоморфизмы* (т.е. гомоморфизмы в себя) группоида $\mathcal{G}$, то понятие «Ω-операторный группоид» дает возможность выделить в $\mathcal{G}$ подгруппоиды, которые отображаются в себя при каждом эндоморфизме $\omega \in \Omega$. Такие подгруппоиды называются Ω-*допустимыми*. Пересечение любого множества Ω-допустимых подгруппоидов группоида $\mathcal{G}$, если оно не пусто, является Ω-допустимых подгруппоидом.

Таким образом, понятие «Ω-операторный группоид» дает возможность с единых позиций исследовать не только внутренние свойства группоидов, но и различные их представления (достаточно в качестве Ω выбрать ту или иную подполугруппу полугруппы эндоморфизмов группоида $\mathcal{G}$).

Пусть $\mathcal{G} = (G, \diamond)$ – абелева полугруппа, а $\mathcal{S}_{\mathcal{G}} = (S_{\mathcal{G}}, \diamond)$ – такая ее подполугруппа, что в $\mathcal{G}$ можно выполнять сокращение на элементы из $S_{\mathcal{G}}$, т.е. если $a \diamond x = b \diamond x$ $(a, b \in G,\ x \in S_{\mathcal{G}})$, то $a = b$. Абелеву полугруппу $\mathcal{G}$ можно изоморфно вложить в такую абелеву полугруппу $\overline{\mathcal{G}} = (\overline{G}, \diamond)$ с нейтральным элементом, что каждый элемент $x \in S_{\mathcal{G}}$ имеет в полугруппе $\overline{\mathcal{G}}$ обратный элемент.

Замечание 1.7. Абелева полугруппа $\overline{\mathcal{G}} = (\overline{G}, \diamond)$ строится следующим образом.

Множеством *дробей* (говорят также, *множеством частных*) над абелевой полугруппой $\mathcal{G} = (G, \diamond)$ называется множество $R_{\mathcal{G}} = \left\{ \frac{a}{x} \middle| a \in G,\ x \in S_{\mathcal{G}} \right\}$ (дробь $\frac{a}{x}$ понимается просто как упорядоченная пара (a, x) элементов a и x). Определив на множестве $R_{\mathcal{G}}$ операцию «$\diamond$» равенством $\frac{a}{x} \diamond \frac{b}{y} = \frac{a \diamond b}{x \diamond y}$ $\left(\frac{a}{x}, \frac{b}{y} \in R_{\mathcal{G}} \right)$, получим абелеву полугруппу $\mathcal{R}_{\mathcal{G}} = (R_{\mathcal{G}}, \diamond)$. Обозначим через «$\equiv$» такое отношение эквивалентности на множестве $R_{\mathcal{G}}$, что $\frac{a}{x} \equiv \frac{b}{y}$ тогда и только тогда, когда $a \diamond y = b \diamond x$. Положим $\overline{G} = R_{\mathcal{G}}/_{\equiv}$, а операцию «$\diamond$» определим на множестве $\overline{G}$ следующим образом: если $H_1, H_2 \in \overline{G}$ $(\frac{a}{x} \in H_1, \frac{b}{y} \in H_2)$, то $H_1 \diamond H_2 = H$, где $\frac{a \diamond b}{x \diamond y} \in H$. Получим абелеву полугруппу $\overline{\mathcal{G}} = (\overline{G}, \diamond)$, которая называется *полугруппой дробей* (говорят также, *полугруппой частных*) над абелевой полугруппой $\mathcal{G}$. Нейтральным элементом полугруппы $\overline{\mathcal{G}}$ является элемент $\{\frac{x}{x} | x \in S_{\mathcal{G}}\}$. Элементу $a \in G$ соответствует элемент $\{\frac{a \diamond x}{x} | x \in S_{\mathcal{G}}\}$ полугруппы $\overline{\mathcal{G}}$, а элементом полугруппы $\overline{\mathcal{G}}$, обратным элементу $\{\frac{a \diamond x}{x} | x \in S_{\mathcal{G}}\}$ $(a \in S_{\mathcal{G}})$, является элемент $\{\frac{x}{a \diamond x} | x \in S_{\mathcal{G}}\}$.

Пусть $\mathcal{H} = (H, \diamond)$ – подгруппа группы $\mathcal{G} = (G, \diamond)$ (обозначается $\mathcal{H} \leq \mathcal{G}$). *Левые* (соответственно, *правые*) *смежные классы* группы $\mathcal{G}$ по подгруппе $\mathcal{H}$ – это множества $g \diamond H = \{g \diamond h | h \in H\}$ $(g \in G)$ (соответственно, множества $H \diamond g = \{h \diamond g | h \in H\}$ $(g \in G)$). При этом, $\pi_{\mathcal{H}}^{(l)} = \{g \diamond H | g \in G\}$ и $\pi_{\mathcal{H}}^{(r)} = \{H \diamond g | g \in G\}$ – разбиения множества G. Если $\mathcal{G}$ – конечная группа, то разбиения $\pi_{\mathcal{H}}^{(l)}$ и $\pi_{\mathcal{H}}^{(r)}$ содержат одно и тоже число блоков. Это число блоков называется *индексом* подгруппы $\mathcal{H}$ в группе $\mathcal{G}$. Имеет место теорема Лагранжа: порядок и индекс любой подгруппы конечной группы являются делителями порядка группы.

Подгруппа $\mathcal{H} = (H, \diamond)$ группы $\mathcal{G} = (G, \diamond)$ – *нормальная* (обозначается $\mathcal{H} \lhd \mathcal{G}$), если $g \diamond H = H \diamond g$ для всех $g \in G$. Пересечение любого множества нормальных подгрупп группы $\mathcal{G}$ является нормальной подгруппой группы $\mathcal{G}$. Множество $\{g \diamond H | g \in G\}$ называется *множеством смежных классов* группы $\mathcal{G}$ по нормальной подгруппе $\mathcal{H}$. Это множество является группой, если операцию «$*$» композиции определить равенством $(g_1 \diamond H) * (g_2 \diamond H) = (g_1 \diamond g_2) \diamond H$. Такая группа называется *фактор-группой* группы $\mathcal{G}$ по нормальной подгруппе $\mathcal{H}$ и обозначается $\mathcal{G}/_{\mathcal{H}}$.

Замечание 1.8. Существует следующая связь между нормальными подгруппами и гомоморфизмами групп: если $h : G \to H$ – гомоморфизм группы $\mathcal{G} = (G, \diamond_{\mathcal{G}})$ на группу $\mathcal{H} = (H, \diamond_{\mathcal{H}})$ то $(f^{-1}(e_{\mathcal{H}}), \diamond_{\mathcal{G}})$ – нормальная подгруппа группы $\mathcal{G}$ ($e_{\mathcal{H}}$ – нейтральный элемент группы $\mathcal{H}$). Множество $f^{-1}(e_{\mathcal{H}})$ – *ядро гомоморфизма* f (обозначается $\ker f$). Если $\mathcal{H}_1$ *и* $\mathcal{H}_2$ – такие нормальные подгруппы группы $\mathcal{G}$, что $\mathcal{H}_1 \lhd \mathcal{H}_2$, то существует гомоморфизм фактор-группы $\mathcal{G}/_{\mathcal{H}_1}$ на фактор-группу $\mathcal{G}/_{\mathcal{H}_2}$.

Множество всех *подстановок*, определенных на множестве X (т.е. биекций $f : X \to X$) вместе с операцией их суперпозиции образует *группу* $\mathcal{S}(X)$. Если $X = \mathbb{N}_n$, то эта группа называется *симметрической группой* и обозначается $\mathcal{S}(n)$. Имеет место теорема Кэли: любая конечная группа изоморфна некоторой подгруппе группы $\mathcal{S}(n)$ при подходящем выборе числа n.

Таким образом, симметрические группы $\mathcal{S}(n)$ ($n \in \mathbb{N}$) обеспечивают унифицированное представление конечных групп.

Для любой полугруппы $\mathcal{G} = (G, \diamond)$ абелева подполугруппа $(\langle a \rangle, \diamond)$ ($a \in G$), где $\langle a \rangle = \{a^n | n \in \mathbb{N}\}$, называется *циклической* полугруппой, порожденной элементом a.

Аналогичным образом, для любой группы $\mathcal{G} = (G, \diamond)$ абелева подгруппа $(\langle a \rangle, \diamond)$, где $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$ называется *циклической* группой, порожденной элементом $a \in G$.

В обоих случаях $a \in G$ – *образующий* элемент для $(\langle a \rangle, \diamond)$.

Замечание 1.9. В любой группе $\mathcal{G} = (G, \diamond)$ для подгруппы $(\langle a \rangle, \diamond)$ порядка n истинны следующие утверждения:

1) существует в точности $\varphi(n)$ (φ – функция Эйлера) образующих элементов подгруппы $(\langle a \rangle, \diamond)$;

2) элемент a^k ($k \in \mathbb{N}$) порождает подгруппу группы $(\langle a \rangle, \diamond)$, имеющую порядок $(n, k)^{-1} \cdot n$, где (n, k) – НОД чисел n и k;

3) для каждого делителя d числа n существует единственная подгруппа порядка d группы $(\langle a \rangle, \diamond)$, и единственная подгруппа индекса d группы $(\langle a \rangle, \diamond)$.

Пусть $\mathcal{G} = (G, \diamond)$ – абелева полугруппа с нейтральным элементом, удовлетворяющая закону сокращения. Элементы $a, b \in G$ называются *ассоциированными*, если каждый из них является делителем для другого. Истинно утверждение: $a, b \in G$ – ассоциированные элементы тогда и только тогда, когда существует такой элемент $c \in G^{inv}$, что $a = b \diamond c$.

Замечание 1.10. Множество G разбивается на классы ассоциированных элементов: один из этих классов – множество G^{inv}, а классом элементов, ассоциированных с элементом $a \in G \setminus G^{inv}$, является множество $a \diamond G^{inv}$.

Элемент $p \in G \setminus G^{inv}$ называется:

1) *неприводимым*, если из равенства $p = a \diamond b$ вытекает, что один из элементов a, b является делителем нейтрального элемента (и, следовательно, другой элемент ассоциирован с элементом p);

2) *простым*, если из того, что $a \diamond b$ делится на элемент p вытекает, что a или b делится на элемент p.

Замечание 1.11. Определим на множестве классов ассоциированных элементов полугруппы $\mathcal{G}$ следующее отношение «$\leq$» частичного порядка: $A \leq B$ тогда и только тогда, когда хотя бы один (а, следовательно, каждый) элемент класса A является делителем хотя бы одного (а, следовательно, каждого) элемента класса B. Ясно, что G^{inv} – наименьший элемент этого частично упорядоченного множества, а классы ассоциированных неприводимых элементов – минимальные элементы множества классов ассоциированных элементов, отличных от G^{inv}. Каждый простой элемент является неприводимым. Обратное утверждение истинно тогда и только тогда, когда для любых элементов $a, b \in G$ существует их наибольший общий делитель, т.е. такой делитель d элементов a и b, который делится на любой другой делитель d' этих элементов. Наибольшим общим делителем (если он существует) элементов a и b является любой элемент такого класса D ассоциированных элементов, что D – максимальный элемент множества всех таких классов X ассоциированных элементов, что $X \leq A$ (где $a \in A$) и $X \leq B$ (где $b \in B$).

Гауссовой полугруппой называется абелева полугруппа $\mathcal{G} = (G, \diamond)$ с нейтральным элементом, удовлетворяющая закону сокращения, в которой каждый элемент $a \in G \setminus G^{inv}$ разлагается в произведение неприводимых элементов, причем любые два такие разложения *ассоциированы* между собой, т.е. если $a = b_1 \dots b_m$ и $a = c_1 \dots c_l$ – разложения элемента a в произведения неприводимых элементов, то $l = m$ и существует такая подстановка f, принадлежащая симметрической группе $\mathcal{S}(m)$, что элементы b_i $(i = 1, \dots, m)$ и $c_{f(i)}$ ассоциированы. Любые два элемента гауссовой полугруппы имеют наибольший общий делитель.

Замечание 1.12. Существует класс конечных абелевых полугрупп $\mathcal{G} = (G, \diamond)$ с нейтральным элементом, которые не являются полугруппами с сокращением (а, следовательно, не являются гауссовыми полугруппами), но которые удовлетворяют следующим условиям:

1) $\mathcal{G}$ – полугруппа с нулем;

2) множества $a \diamond G^{inv}$ $(a \in G)$ – это классы *ассоциированных* элементов;

3) $p \in G \setminus G^{inv}$ – *неприводимый* элемент, если из равенства $p = a \diamond b$ вытекает, что один из элементов a, b – делитель нейтрального элемента;

4) каждый элемент $a \in G \setminus G^{inv}$ разлагается единственным образом (с точностью до ассоциированного разложения) в произведение неприводимых элементов (отсюда,

в частности, вытекает равенство множеств неприводимых и простых элементов, а также существование наибольшего общего делителя для любых элементов $a, b \in G$).

Этому классу полугрупп принадлежат полугруппы $\mathcal{Z}_n = (\mathbb{Z}_n, \circ)$ $(n \in \mathbb{N}, n \geq 2)$, где $a \circ b = ab\,(mod\,n)$. В этом случае $\mathbb{Z}_n^{inv}$ – множество всех чисел $m \in \mathbb{Z}_n$, взаимно-простых с числом n. Если $n = p^k$ (p – простое число, $k \in \mathbb{N}$ $(k \geq 2)$), то каждый элемент $a \in \mathbb{Z}_{p^k} \setminus \mathbb{Z}_{p^k}^{inv}$ – *нильпотентный*, т.е. существует такое $m \in \mathbb{N}$, что $a^m = 0$.

В дальнейшем, в соответствии с традицией, будем использовать следующие обозначения. Мультипликативное представление $\mathcal{G} = (G, \cdot)$ используется для обозначения произвольного группоида, полугруппы или группы. Вместо $a \cdot b$ пишут ab, а нейтральный элемент (если он существует) называется *единицей* (обозначается 1). Аддитивное представление $\mathcal{G} = (G, +)$ используется, когда хотят подчеркнуть, что $\mathcal{G}$ – абелева группа. Ее нейтральный элемент называется *нулем* (обозначается 0), обратный к $a \in G$ элемент называется *противоположным* элементом (обозначается $-a$). Запись na $(n \in \mathbb{Z}, a \in G)$ понимается в соответствии с равенствами $na = \underbrace{a + \cdots + a}_{n \text{ раз}}$ $(n \in \mathbb{N})$, $0a = 0$ и $(-n)a = -(na)$ $(n \in \mathbb{N})$.

Абелева полугруппа $\mathcal{Z}_n = (\mathbb{Z}_n, \circ)$ $(n \in \mathbb{N}, n \geq 2)$ определена в замечании 1.12, а запись $\mathcal{Z}_n = (\mathbb{Z}_n, \oplus)$ $(n \in \mathbb{N}, n \geq 2)$ используется для абелевой группы, в которой $a \oplus b = a + b\,(mod\,n)$.

1.1.2. Алгебры с двумя бинарными операциями.

Кольцом называется алгебра $\mathcal{K} = (K, +, \cdot)$, где $(K, \cdot)$ – группоид, $(K, +)$ – абелева группа, а операции «$\cdot$» и «$+$» связаны законами *дистрибутивности*: $a(b+c) = ab+ac$ и $(b+c)a = ba+ca$ для всех $a, b, c \in K$.

Замечание 1.13. В кольце $\mathcal{K} = (K, +, \cdot)$ через «$-$» обозначается операция, обратная операции «$+$», т.е. $a - b = c$ тогда и только тогда, когда $a = b + c$. Операции «$\cdot$» и «$-$» также связаны законами дистрибутивности, т.е. $a(b - c) = ab - ac$ и $(b - c)a = ba - ca$ для всех $a, b, c \in K$.

Для кольца $\mathcal{Z}_n = (\mathbb{Z}_n, \oplus, \circ)$ $(n \in \mathbf{N},\ n \geq 2)$ операция, обратная операции «$\oplus$» обозначается через «$\ominus$».

Группоид $(K, \cdot)$ называется *мультипликативным* группоидом, а абелева группа $(K, +)$ – *аддитивной* группой кольца $\mathcal{K}$. Для нуля $0 \in K$ аддитивной группы $(K, +)$ истинны равенства $0a = a0 = 0$ $(a \in K)$. Этот элемент называется *нулем* кольца $\mathcal{K}$.

Замечание 1.14. Из законов дистрибутивности непосредственно вытекает, что кольцо $\mathcal{K} = (K, +, \cdot)$ является $(\Omega_1 \cup \Omega_2)$-операторной абелевой группой $(K, +)$, где $\Omega_1 = \{\omega_a^{(1)} | a \in K \& \omega_a^{(1)}(x) = ax\ (x \in K)\}$ и $\Omega_2 = \{\omega_a^{(2)} | a \in K \& \omega_a^{(2)}(x) = xa\ (x \in K)\}$.

В зависимости от свойств мультипликативного группоида выделяют следующие типы колец. Кольцо $\mathcal{K} = (K, +, \cdot)$ называется:

1) *ассоциативным*, если $(K, \cdot)$ – полугруппа, и *не ассоциативным*, если группоид $(K, \cdot)$ не является полугруппой;

2) *коммутативным*, если группоид $(K, \cdot)$ – абелев, и *не коммутативным*, если группоид $(K, \cdot)$ не является абелевым;

3) *кольцом с единицей*, если группоид $(K, \cdot)$ содержит единицу $1 \in K$, и *кольцом без единицы*, если группоид $(K, \cdot)$ не содержит единицу.

Замечание 1.15. В кольце $\mathcal{K} = (K, +, \cdot)$ равенство $0 = 1$ истинно тогда и только тогда, когда $|K| = 1$. Всюду в дальнейшем будем рассматривать только такие кольца $\mathcal{K} = (K, +, \cdot)$, что $|K| \geq 2$, а $(K, \cdot)$ – группоид с ненулевым умножением, т.е. существуют такие $a, b \in K$, что $ab \neq 0$.

Если в кольце $\mathcal{K} = (K, +, \cdot)$ для элементов $a, b \in K \setminus \{0\}$ выполнено равенство $ab = 0$, то a называется *левым*, а b – *правым делителем нуля*. В случае, когда $\mathcal{K}$ – ассоциативно-коммутативное кольцо, указанные элементы a и b называются *делителями нуля*.

Пример 1.1. Пусть $\mathcal{P}_S$ – множество всех разбиений множества S. Запись $x \equiv y(\pi)$ означает утверждение «элементы x и y принадлежат одному блоку разбиения π». Умножение «$\cdot$» разбиений $\pi_1, \pi_2 \in \mathcal{P}_S$ определяется следующим образом: $\pi_1 \cdot \pi_2$ – разбиение, блоки которого – всевозможные непустые пересечения блоков разбиения π_1 с блоками разбиения π_2. Сложение «$+$» разбиений $\pi_1, \pi_2 \in \mathcal{P}_S$ определяется следующим образом: $\pi = \pi_1 + \pi_2$, где $s_1 \equiv s_2(\pi)$ тогда и только тогда, когда в множестве S существует такая конечная последовательность элементов $s_1 = x_1, \ldots, x_n = s_2$, что $x_i \equiv x_{i+1}(\pi_1)$ или $x_i \equiv x_{i+1}(\pi_2)$ для всех $i = 1, \ldots, n$. Разбиение $1_S = \{S\}$ – *единичное*, а разбиение $0_S = \{\{s\} | s \in S\}$ – *нулевое*. Таким образом $(\mathcal{P}_S, +, \cdot)$ – ассоциативно-коммутативное кольцо с единицей, которое содержит делители нуля, если $|S| \geq 3$.

Отношение частичного порядка $\leq$ на множестве разбиений множества S определяется следующим образом: $\pi_1 \leq \pi_2$ тогда и только тогда, когда каждый блок разбиения π_1 содержится в некотором блоке разбиения π_2.

Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативное кольцо с единицей. *Множеством обратимых элементов* кольца $\mathcal{K}$ называется множество K^{inv} обратимых элементов полугруппы $(K, \cdot)$. Группа $(K^{inv}, \cdot)$ называется *мультипликативной группой* кольца $\mathcal{K}$. Любой левый или правый делитель нуля кольца $\mathcal{K}$ принадлежит множеству $K \setminus (\{0\} \cup K^{inv})$. Если $K^{inv} = K \setminus \{0\}$, то $\mathcal{K}$ называется *телом*. Коммутативное тело называется *полем*.

Замечание 1.16. В кольце $\mathcal{Z}_n = (\mathbb{Z}_n, \oplus, \circ)$ $(n \in \mathbb{N}, n \geq 2)$ множество $\mathbb{Z}_n^{inv}$ состоит из всех чисел $a \in \mathbb{Z}_n$, взаимно-простых с числом n. Следовательно, $\mathcal{Z}_n$ $(n \in \mathbb{N}, n \geq 2)$ является полем тогда и только тогда, когда n – простое число.

Если для кольца $\mathcal{K} = (K, +, \cdot)$ существует такое число $n \in \mathbb{N}$, что $nx = 0$ для всех $x \in K$, то наименьшее из таких чисел $n \in \mathbb{N}$ называется *характеристикой* кольца $\mathcal{K}$. Если же указанное число $n \in \mathbb{N}$ не существует, то говорят, что $\mathcal{K}$ – кольцо *характеристики* 0.

Любая подалгебра $\mathcal{K}_1 = (K_1, +, \cdot)$ $(K_1 \subseteq K)$ кольца $\mathcal{K} = (K, +, \cdot)$, являющаяся кольцом, называется *подкольцом* кольца $\mathcal{K}$, а само кольцо $\mathcal{K}$ называется *надкольцом* (или *расширением* кольца $\mathcal{K}$).

Замечание 1.17. Подкольцами любого кольца $\mathcal{K} = (K, +, \cdot)$ являются *нуль-кольцо* $\mathcal{O} = (\{0\}, +, \cdot)$ и кольцо $\mathcal{K}$. Эти подкольца называются *несобственными*. Все остальные подкольца кольца $\mathcal{K}$ (если такие существуют) называются *собственными*. Пересечение любого множества подколец кольца $\mathcal{K}$ является подкольцом кольца $\mathcal{K}$. Кольцо, не содержащее ни одного собственного подкольца, называется *простым*.

Пусть $\mathcal{K}$ – ассоциативно-коммутативное кольцо, а $\mathcal{K}_1$ – подкольцо кольца $\mathcal{K}$. Возможны следующие три различные ситуации:

1. Оба кольца $\mathcal{K}$ и $\mathcal{K}_1$ не содержат единицы.

2. Оба кольца $\mathcal{K}$ и $\mathcal{K}_1$ содержат единицу и эти единицы совпадают. Тогда $\mathcal{K}_1$ называется *унитарным подкольцом* кольца $\mathcal{K}$, а само $\mathcal{K}$ – *унитарным надкольцом* кольца $\mathcal{K}_1$.

3. Кольцо $\mathcal{K}_1$ содержит единицу, а кольцо $\mathcal{K}$ либо не содержит единицы, либо единица кольца $\mathcal{K}$ отлична от единицы кольца $\mathcal{K}_1$. Тогда единица кольца $\mathcal{K}_1$ является делителем нуля в кольце $\mathcal{K}$.

Замечание 1.18. Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо с единицей $1 \in K$. Положим $\mathcal{K}(1) = (\{n1 | n \in \mathbb{Z}\}, +, \cdot)$, где $n_1 1 + n_2 1 = (n_1 + n_2)1$ и $(n_1 1)(n_2 1) = (n_1 n_2)1$ для любых $n_1, n_2 \in \mathbb{Z}$. Кольцо $\mathcal{K}(1)$ является наименьшим подкольцом кольца $\mathcal{K}$, содержащим единицу 1.

Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо, а $S_{\mathcal{K}}$ – множество всех элементов $x \in K \backslash \{0\}$, на которые допустимы сокращения. Ассоциативно-коммутативное кольцо $\mathcal{K}$ можно изоморфно вложить в такое ассоциативно-коммутативное кольцо дробей $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ с единицей, что каждый элемент $x \in S_{\mathcal{K}}$ имеет в кольце $\overline{\mathcal{K}}$ обратный элемент.

Замечание 1.19. Ассоциативно-коммутативное кольцо $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ строится в соответствии со схемой, представленной в замечании 1.7.

Пусть $R_{\mathcal{K}} = \{\frac{a}{x} | a \in K, x \in S_{\mathcal{K}}\}$ – множество *дробей* (*частных*) над кольцом $\mathcal{K}$. Положив $\frac{a}{x} + \frac{b}{y} = \frac{ay+bx}{xy}$ и $\frac{a}{x} \cdot \frac{b}{y} = \frac{ab}{xy}$, получим алгебру $\mathcal{R}_{\mathcal{K}} = (R_{\mathcal{K}}, +, \cdot)$. Пусть «$\equiv$» – такое отношение эквивалентности на множестве $R_{\mathcal{K}}$, что $\frac{a}{x} \equiv \frac{b}{y}$ тогда и только тогда, когда $ay = bx$. Положим $\overline{K} = R_{\mathcal{K}}/_{\equiv}$. Определим на множестве $\overline{K}$ операции «+» и «$\cdot$» следующим образом: если $H_1, H_2 \in \overline{K}$ $(\frac{a}{x} \in H_1, \frac{b}{y} \in H_2)$, то $H_1 + H_2 = H$, где

$\frac{ay+bx}{xy} \in H$ и $H_1H_2 = H$, где $\frac{ab}{xy} \in H$. Получим ассоциативно-коммутативное кольцо $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ дробей над кольцом $\mathcal{K}$. Единица кольца $\overline{\mathcal{K}}$ – элемент $\{\frac{x}{x}|x \in S_{\mathcal{K}}\}$, элементу $a \in K$ кольца $\mathcal{K}$ соответствует элемент $\{\frac{ax}{x}|x \in S_{\mathcal{K}}\}$ кольца $\overline{\mathcal{K}}$, а элементом кольца $\overline{\mathcal{K}}$, обратным элементу $\{\frac{ax}{x}|x \in S_{\mathcal{K}}\}$ $(a \in S_{\mathcal{K}})$ является элемент $\{\frac{x}{ax}|x \in S_{\mathcal{K}}\}$.

Областью целостности называется ассоциативно-коммутативное кольцо $\mathcal{K} = (K, +, \cdot)$ без делителей нуля. В этом случае $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ является *полем дробей* (над областью целостности $\mathcal{K}$).

Левым (соответственно, правым) идеалом кольца $\mathcal{K} = (K, +, \cdot)$ называется такое множество I $(\emptyset \neq I \subseteq K)$, что $(I, +)$ – подгруппа абелевой группы $(K, +)$ и истинно включение $KI \subseteq I$ (соответственно, $IK \subseteq I$).

Замечание 1.20. Если I – левый или правый идеал кольца $\mathcal{K}$, то $\mathcal{I} = (I, +, \cdot)$ – подкольцо кольца $\mathcal{K}$. Обратное утверждение не всегда истинно.

Если множество I одновременно является и левым, и правым идеалом кольца $\mathcal{K}$, то I называется (двусторонним) *идеалом* кольца $\mathcal{K}$.

Замечание 1.21. Идеалами любого кольца $\mathcal{K}$ являются $\{0\}$ (*нулевой* идеал) и множество K. Эти идеалы – *несобственные*. Остальные идеалы (если они существуют) – *собственные*. Кольцо $\mathcal{K}$ *простое*, если оно не имеет собственных идеалов.

Кольцо $\mathcal{K} = (K, +, \cdot)$ – *кольцо с делением*, если для любых $a, b \in K$ $(a \neq 0)$ уравнения $ax = b$ и $ya = b$ имеют решения, т.е. если $(K, \cdot)$ – квазигруппа. В кольце с делением отсутствуют как левые, так и правые собственные идеалы, а, следовательно, отсутствуют собственные идеалы, т.е. кольцо с делением – простое кольцо.

Базисом идеала I ассоциативно-коммутативного кольца $\mathcal{K} = (K, +, \cdot)$ называется любое такое подмножество $M \subseteq I$, что $M \not\subseteq I_1$ для любого идеала $I_1 \subset I$. Идеал I – *конечно-порожденный*, если он имеет конечный базис $M = \{a_1, \ldots, a_n\}$. В этом случае пишут $I = (a_1, \ldots, a_n)$. Ясно, что $I = \sum_{i=1}^{n} Ka_i + \sum_{i=1}^{n} \mathbb{Z}a_i$, причем если $\mathcal{K}$ – кольцо с единицей, то $I = \sum_{i=1}^{n} Ka_i$.

Замечание 1.22. Пусть I – конечно-порожденный идеал ассоциативно-коммутативного кольца $\mathcal{K}$. Базис $M = \{a_1, \ldots, a_n\}$ идеала I – *минимальный*, если никакое собственное подмножество множества M не является базисом идеала I. Идеал I может иметь минимальные базисы, состоящие из различного числа элементов.

Пусть I – идеал кольца $\mathcal{K} = (K, +, \cdot)$, а «$\equiv_I$» – такое отношение эквивалентности на множестве K, что $a \equiv_I b$ $(a, b \in K)$ тогда и только тогда, когда $a - b \in I$. Тогда кольцом является алгебра $\mathcal{K}/_{\equiv_I} = (K/_{\equiv_I}, +_I, \cdot_I)$, где $K/_{\equiv_I} = \{a + I|a \in K\}$, а операции $+_I$ и $\cdot_I$ определены равенствами $(a+I)+_I(b+I) = (a+b)+I$ и $(a+I)\cdot_I(b+I) = ab+I$. Кольцо $\mathcal{K}/_{\equiv_I}$ называется *фактор-кольцом* кольца $\mathcal{K}$ по идеалу I, а элементы множества

$K/_{\equiv_I}$ – *классами вычетов* по идеалу I. Запись $a \equiv b \,(\mathrm{mod}\, I)$ $(a, b \in K)$ означает утверждение «элементы a и b принадлежат одному и тому же классу вычетов по идеалу I».

Говорят, что кольцо $\mathcal{K}_2 = (K_2, +_2, \cdot_2)$ – *гомоморфный образ* кольца $\mathcal{K}_1 = (K_1, +_1, \cdot_1)$, если существует такая сюръекция $h : K_1 \to K_2$, что $h(a+_1 b) = h(a)+_2 h(b)$ и $h(a\cdot_1 b) = h(a)\cdot_2 h(b)$ для любых $a, b \in K_1$, а сюръекцию h называют *гомоморфизмом* кольца $\mathcal{K}_1$ на кольцо $\mathcal{K}_2$. Если при этом h – биекция, то говорят, что кольца $\mathcal{K}_1$ и $\mathcal{K}_2$ *изоморфны* (друг другу), а h называют *изоморфизмом* между кольцами $\mathcal{K}_1$ и $\mathcal{K}_2$.

Замечание 1.23. Существует следующая связь между идеалами и гомоморфизмами колец: если сюръекция $h : K_1 \to K_2$ – гомоморфизм кольца $\mathcal{K}_1$ на кольцо $\mathcal{K}_2$, то $h^{-1}(0_2)$ – идеал кольца $\mathcal{K}_1$ (0_2 – нуль кольца $\mathcal{K}_2$). Множество $f^{-1}(e_{\mathcal{H}})$ – ядро гомоморфизма f (обозначается $\ker f$). Если I_1 и I_2 – такие идеалы кольца $\mathcal{K} = (K, +, \cdot)$, что $I_1 \subseteq I_2$, то существует гомоморфизм фактор-кольца $\mathcal{K}/_{\equiv_{I_1}}$ на фактор-кольцо $\mathcal{K}/_{\equiv_{I_2}}$.

Для любых идеалов I_1 и I_2 кольца $\mathcal{K}$ *сумма* I_1+I_2, *пересечение* $I_1 \cap I_2$ и *произведение* $I = I_1 I_2 = \{\sum\limits_{i=1}^{n} a_i b_i | a_i \in I_1, b \in I_2 \ (n \in \mathbb{N})\}$ – идеалы кольца $\mathcal{K}$. Если $I = I_1 I_2$ и $I \neq I_1$ и $I \neq I_2$, то говорят, что идеал I *разложим*.

Простым идеалом ассоциативного кольца $\mathcal{K} = (K, +, \cdot)$ называется такой его собственный идеал I, что если $ab \in I$ $(a, b \in K)$, то $a \in I$ или $b \in I$. Собственный идеал I кольца $\mathcal{K}$ является простым тогда и только тогда, когда для любых идеалов A, B кольца $\mathcal{K}$ из $AB \subseteq I$ следует, что $A \subseteq I$ или $B \subseteq I$. Отсюда вытекает, что:

1) каждый максимальный (по включению) собственный идеал ассоциативного кольца является простым идеалом;

2) если ассоциативно-коммутативное кольцо $\mathcal{K}$ содержит единицу, а I простой идеал, то $\mathcal{K}/_{\equiv_I}$ является полем.

Пример 1.2. Если число $n \in \mathbb{N}$ $(n \geq 2)$ не является простым, а $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ $(\alpha_1, \dots \alpha_m \in \mathbb{N})$ – каноническое разложение числа n, то кольцо $\mathcal{Z}_n = (\mathbb{Z}_n, \oplus, \circ)$ содержит m простых идеалов, а именно: $(p_1), \dots, (p_m)$.

Дедекиндовым кольцом называется область целостности с единицей, в которой каждый собственный идеал единственным образом разложим в произведение конечного числа простых идеалов.

Нетеровым кольцом называется ассоциативно-коммутативное кольцо с единицей, в котором каждый идеал имеет конечный базис.

Замечание 1.24. Каждое конечное ассоциативно-коммутативное кольцо с единицей является нетеровым кольцом.

Ассоциативно-коммутативное кольцо с единицей называется *примарным*, если оно содержит единственный простой идеал.

Пример 1.3. В кольце $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (p – простое число, $k \in \mathbb{N}$ ($k \geq 2$)) единственным простым идеалом является (p), т.е. $\mathcal{Z}_{p^k}$ – примарное кольцо.

Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо. *Радикал* идеала I кольца $\mathcal{K}$ – идеал $\sqrt{I} = \{a \in K | (\exists n \in \mathbb{N})(a^n \in I)\}$. Идеал $\sqrt{(0)}$ состоит из всех нильпотентных элементов кольца $\mathcal{K}$ и называется *радикалом кольца* $\mathcal{K}$.

Замечание 1.25. Для любого идеала I ассоциативно-коммутативного кольца $I \subseteq \sqrt{I}$ (если $I = \sqrt{I}$, то I – *радикальный* идеал) и $\sqrt{\sqrt{I}} = \sqrt{I}$. Кроме того, если I_1 и I_2 такие идеалы ассоциативно-коммутативного кольца, что $I_1^n \subseteq I_2$ для некоторого $n \in \mathbf{N}$, то $\sqrt{I_1} \subseteq \sqrt{I_2}$, $\sqrt{I_1 I_2} = \sqrt{I_1 \cap I_2} = \sqrt{I_1} \cap \sqrt{I_2}$ и $\sqrt{I_1 + I_2} = \sqrt{\sqrt{I_1} + \sqrt{I_2}}$.

Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо. Идеал $(a) = \{ax + na | x \in K, n \in \mathbb{Z}\}$ называется *главным идеалом*, порождаемым элементом a. Этот идеал является наименьшим идеалом, содержащим элемент a. Если кольцо $\mathcal{K}$ содержит единицу, то $(a) = aK$.

Пример 1.4. Существует $k - 1$ собственный идеал кольца $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (p – простое число, $k \in \mathbb{N}$ ($k \geq 2$)), а именно: $(p), (p^2), \ldots, (p^{k-1})$, т.е. каждый собственный идеал кольца $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ – главный идеал.

Замечание 1.26. В любом ассоциативно-коммутативном кольце нулевой идеал является главным идеалом.

Пусть $\mathcal{K} = (K, +, \cdot)$ – область целостности с единицей, а элемент $a \in K \backslash K^{inv}$ $a \neq 0$) представлен в виде $a = a_1^{\alpha_1} \ldots a_l^{\alpha_l}$ ($\alpha_1, \ldots, \alpha_l \in \mathbb{N}$), где $a_1, \ldots, a_l$ – попарно не ассоциированные неприводимые элементы кольца $\mathcal{K}$. Тогда $\sqrt{(a)} = (a_1 \ldots, a_l)$. Если $a = a_1^{\alpha_1} \ldots a_l^{\alpha_l}$ ($\alpha_1, \ldots, \alpha_l \in \mathbb{Z}_+$) и $b = a_1^{\beta_1} \ldots a_l^{\beta_l}$ ($\beta_1, \ldots, \beta_l \in \mathbb{Z}_+$) – разложения элементов $a, b \in K \backslash K^{inv}$ в произведения попарно не ассоциированных неприводимых элементов, то $(a) \cap (b) = (c)$, где $c = a_1^{\gamma_1} \ldots a_l^{\gamma_l}$, а $\gamma_i = \max\{\alpha_i, \beta_i\}$ ($i = 1, \ldots, l$).

Гауссовым кольцом называется такая область целостности с единицей $\mathcal{K} = (K, +, \cdot)$, что $(K \setminus \{0\}, \cdot)$ гауссова полугруппа.

Кольцом главных идеалов называется область целостности с единицей, в которой каждый собственный идеал главный. Каждое кольцо главных идеалов является гауссовым кольцом. В кольце $\mathcal{K} = (K, +, \cdot)$ главных идеалов простые идеалы – это такие идеалы (p), что p – простой элемент абелевой полугруппы $(K, \cdot)$. При этом, если $a \in (K \setminus \{0\}) \setminus K^{inv}$ и $a = p_1 \ldots p_n$ – разложение элемента a в произведение простых множителей, то $(a) = (p_1) \ldots (p_n)$.

Замечание 1.27. Пусть число $n \in \mathbb{N}$ $(n \geq 2)$ не является простым. Тогда кольцо $\mathcal{Z}_n = (\mathbb{Z}_n, \oplus, \circ)$ не является кольцом главных идеалов (так как в этом случае $\mathcal{Z}_n$ не является областью целостности). Тем не менее, если $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ $(\alpha_1, \dots \alpha_m \in \mathbb{N})$ – каноническое разложение, а каноническое разложение числа $a \in (\mathbb{Z}_n \setminus \{0\}) \setminus \mathbb{Z}_n^{inv}$ имеет вид $a = \alpha p_{i_1}^{\beta_1} \dots p_{i_r}^{\beta_r}$ $(1 \leq i_1 < \dots < i_r \leq m, 1 \leq \beta_j \leq \alpha_{i_j} (j = 1, \dots, r))$, где $\alpha \in \mathbb{Z}_n^{inv}$, то $(a) = (p_{i_1})^{\beta_1} \dots (p_{i_r})^{\beta_r}$, т.е. в кольце $\mathcal{Z}_n$ каждый ненулевой главный идеал единственным образом представим в виде произведения простых идеалов.

Евклидовым кольцом называется область целостности $\mathcal{K} = (K, +, \cdot)$ с единицей, в которой каждому элементу $x \in K \setminus \{0\}$ можно поставить в соответствие такое число $n(x) \in \mathbb{Z}_+$, что:

1) если $b \in K$ – делитель элемента $a \in K \setminus \{0\}$, то $n(b) \leq n(a)$;

2) для любых элементов $a, b \in K$ $(b \neq 0)$ существуют такие элементы $q, r \in K$, что $a = bq + r$, причем либо $r = 0$, либо $n(r) < n(b)$.

Замечание 1.28. Евклидово кольцо является кольцом главных идеалов. В нем для поиска наибольшего общего делителя ненулевых элементов применим алгоритм Евклида.

Пусть $\mathcal{K} = (K, +, \cdot)$ – область целостности с единицей, а $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ – поле частных. *Дробным идеалом* кольца $\mathcal{K}$ называется такое множество $A \subseteq \overline{K}$, что:

1) $(A, +)$ – подгруппа абелевой группы $(\overline{K}, +)$;

2) если $a \in A$ и $x \in K$, то $ax \in A$;

3) существует такой элемент $d \in K \setminus \{0\}$ и такой идеал A_0 кольца $\mathcal{K}$, что $A = \frac{1}{d} A_0$, т.е. каждый элемент $a \in A$ – дробь с знаменателем d.

Замечание 1.29. Идеалы области целостности с единицей $\mathcal{K}$ (их называют *целыми идеалами*) принадлежат множеству дробных идеалов. Последнее является абелевой полугруппой, если операцию умножения определить следующим образом: если $A = \frac{1}{c} A_0$ и $B = \frac{1}{d} B_0$, то $AB = \frac{1}{cd} A_0 B_0$. Множество всех ненулевых дробных идеалов является подполугруппой этой полугруппы. Ненулевой дробный идеал A – *обратимый*, если существует такой дробный идеал A^{-1}, что $AA^{-1} = K$. Каждый ненулевой главный дробный идеал $\frac{1}{d}(a) = \left(\frac{a}{d}\right)$ обратим, так как $\left(\frac{a}{d}\right)^{-1} = \left(\frac{d}{a}\right)$. Каждый обратимый дробный идеал порождается конечным множеством элементов.

Область целостности с единицей является дедекиндовым кольцом тогда и только тогда, когда полугруппа ее ненулевых дробных идеалов является группой. Отсюда вытекает, что каждый ненулевой дробный идеал дедекиндового кольца раскладывается в произведение положительных или отрицательных степеней простых идеалов.

Кольцом дискретного нормирования называется примарное кольцо $\mathcal{K} = (K, +, \cdot)$ главных идеалов. Если (t) – простой идеал, то каждый элемент $x \in K \setminus \{0\}$ единственным образом представим в виде $x = t^r y$

$(r \in \mathbb{Z}_+)$, где $y \in K^{inv}$, а $t^0 = 1$. Элемент t – *локальный параметр*. В этом случае говорят, что кольцо $\mathcal{K}$ допускает *локальную параметризацию*.

Замечание 1.30. Кольцо дискретного нормирования $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (p – простое число, $k \in \mathbb{N}$ $(k \geq 2)$) допускает локальную параметризацию, так как любой элемент $x \in \mathbb{Z}_{p^k} \setminus \{0\}$ представим в виде $x = p^r y$, где $r \in \mathbb{Z}_k$ и $y \in \mathbb{Z}_{p^k}^{inv}$. Учитывая это обстоятельство, в [66] следующим образом определен *p-тип* $\mathtt{t}_p(z)$ элемента $z \in \mathbb{Z}_{p^k}$

$$\mathtt{t}_p(z) = \begin{cases} 0, & \text{если } z \in \mathbb{Z}_{p^k}^{inv} \\ r \ (1 \leq r \leq k-1), & \text{если } z \equiv 0 \,(mod\, p^r) \text{ и } z \not\equiv 0 \,(mod\, p^{r+1}) \,. \\ k, & \text{если } z = 0 \end{cases} \tag{1.1}$$

Из (1.1) вытекает, что:

1) $\mathtt{t}_p(u \circ v) = \min\{k, \mathtt{t}_p(u) + \mathtt{t}_p(v)\}$ $(u, v \in \mathbb{Z}_{p^k})$;

2) $\mathtt{t}_p(u \oplus v) = \min\{\mathtt{t}_p(u), \mathtt{t}_p(v)\}$ $(u, v \in \mathbb{Z}_{p^k})$, если $u \oplus v \neq 0$;

3) $\mathtt{t}_p(u) = \mathtt{t}_p(v)$ $(u, v \in \mathbf{Z}_{p^k})$ тогда и только тогда, когда элементы u и v принадлежат одному и тому же классу ассоциированных элементов кольца $\mathcal{Z}_{p^k}$.

В силу последнего свойства понятие «p-тип $\mathtt{t}_p(z)$ элемента кольца $\mathbb{Z}_{p^k}$» определяет биекцию классов ассоциированных элементов кольца $\mathcal{Z}_{p^k}$ на множество $\mathbb{Z}_{k+1}$: для того, чтобы задать класс ассоциированных элементов достаточно зафиксировать p-тип $\mathtt{t}_p(z)$ элемента, принадлежащего этому классу. Это обстоятельство дает возможность сокращать перебор в процессе решения уравнений над кольцом $\mathbb{Z}_{p^k}$.

Пусть $\mathcal{G} = (G, +)$ – абелева группа, а $\mathcal{K} = (K, +, \cdot)$ – кольцо отображений множества G в себя. Множество G называется $\mathcal{K}$-*модулем*, если выполнены следующие условия:

1) единица кольца $\mathcal{K}$, если она существует, является тождественным отображением множества G;

2) равенство $(a+b)(g) = a(g)+b(g)$ истинно для всех $a, b \in K$ и $g \in G$;

3) равенство $a(u+v) = a(u)+a(v)$ истинно для всех $a \in K$ и $u, v \in G$;

4) равенство $(ab)(g) = a(b(g))$ истинно для всех $a, b \in K$ и $g \in G$.

Замечание 1.31. В определении модуля первое свойство имеет значение только для колец с единицей. Модули над такими кольцами называются *унитарными*.

Подмодулем $\mathcal{K}$-модуля G называется такое подмножество $G_1 \subseteq G$, что $\mathcal{G} = (G_1, +)$ – подгруппа группы $\mathcal{G} = (G, +)$, причем $a(g) \in G_1$ для всех $a \in K$ и $g \in G_1$. При этом множество $G/_{G_1} = \{g + G_1 | g \in G\}$ называется *фактор-модулем*, а действие элементов кольца $\mathcal{K}$ на элементы множества $G/_{G_1}$ определяется равенством $a(g + G_1) = a(g) + G_1$.

Пусть U и V – $\mathcal{K}$-модули. $\mathcal{K}$-*гомоморфизмом* U в V называется такое отображение $\sigma : U \to V$, что $\sigma(u_1 + u_2) = \sigma(u_1) + \sigma(u_2)$ $(u_1, u_2 \in U)$ и

$\sigma(a(u)) = a(\sigma(u))$ $(a \in K, u \in U)$. Если $\sigma : U \to V$ – $\mathcal{K}$-гомоморфизм U в V, то $\ker\sigma = \{u \in U | \sigma(u) = 0\}$ является подмодулем модуля U.

Пример 1.5. 1. Любой левый (соответственно, правый) идеал I ассоциативного кольца $\mathcal{K} = (K, +, \cdot)$ является K-модулем, если действие элементов кольца на элементы идеала I определить равенством $a(x) = ax$ (соответственно, равенством $a(x) = xa$) для всех $a \in K$ и $x \in I$.

2. Для любого кольца $\mathcal{K} = (K, +, \cdot)$ абелевой группой является $(K^n, +)$ $(n \in \mathbb{N})$, где $\mathbf{a}+\mathbf{b} = (a_1+b_1, \ldots, a_n+b_n)$ для всех $\mathbf{a} = (a_1, \ldots, a_n) \in K^n$ и $\mathbf{b} = (b_1, \ldots, b_n) \in K^n$. Определим действие элементов кольца на элементы абелевой группы равенством $a(\mathbf{a}) = (aa_1, \ldots, aa_n)$ $(a \in K, \mathbf{a} = (a_1, \ldots, a_n) \in K^n)$. В этом случае вместо $a(\mathbf{a})$ $(\mathbf{a} \in K^n)$ пишут $a\mathbf{a}$.

Если $\mathcal{K}$ – ассоциативное кольцо, то множество K^n является $\mathcal{K}$-модулем, но не векторным пространством, если $\mathcal{K}$ не является телом (напомним, что *векторным* (или *линейным*) пространством называется унитарный модуль над телом, в частности, над полем).

Если $\mathcal{K} = (K, +, \cdot)$ – поле, то $\mathcal{K}$-модуль K^n $(n \in \mathbb{N})$ называется *n-мерным аффинным пространством* над полем $\mathcal{K}$. В частности, $K^1 = K$ называется *аффинной прямой*, а K^2 – *аффинной плоскостью*.

Далее в настоящем пункте под кольцом $\mathcal{K} = (K, +, \cdot)$ понимается ассоциативно-коммутативное кольцо с ненулевым умножением.

Многочленом над кольцом $\mathcal{K}$ от переменной x называется выражение $f(x) = a_0 + a_1x + \cdots + a_mx^m$ $(m \in \mathbb{Z}_+)$, где $a_0, a_1, \ldots, a_m \in K$ – *коэффициенты*. Если $a_0 = a_1 = \cdots = a_m = 0$, то $f(x)$ – *нулевой* многочлен, а если хотя бы один из коэффициентов отличен от нуля, то $f(x)$ – *ненулевой* многочлен. Степень нулевого многочлена не определена, а степень ненулевого многочлена – это такое максимальное число k, что $a_k \neq 0$ (a_k – *старший коэффициент*, а a_0 – *свободный член* многочлена $f(x)$).

Замечание 1.32. В дальнейшем нулевой многочлен обозначается 0, а в записи $f(x) = a_0 + a_1x + \cdots + a_mx^m$ ненулевого многочлена a_m – старший член. Два многочлена называются равными, если их коэффициенты совпадают.

Пусть $K[x]$ – множество всех многочленов над кольцом $\mathcal{K}$ от переменной x. Определив обычным образом сложение и умножение многочленов, получим ассоциативно-коммутативное кольцо $\mathcal{K}[x] = (K[x], +, \cdot)$ многочленов от переменной x над кольцом $\mathcal{K}$. Само кольцо $\mathcal{K}$ является подкольцом кольца $\mathcal{K}[x]$ (элементам множества $K \setminus \{0\}$ соответствуют многочлены 0-й степени, а элементу $0 \in K$ – нулевой многочлен).

Замечание 1.33. Если $\mathcal{K}$ – область целостности, то $\mathcal{K}[x]$ – область целостности.

Многочлен $f(x) \in K[x]$ степени $m \in \mathbb{N}$ называется *разложимым* (в кольце $\mathcal{K}[x]$), если существуют такие многочлены $f_i(x) \in K[x]$ $(i = 1, 2)$

степени $m_i \in \mathbb{N}$ ($m_i < m$ $(i = 1, 2)$), что $f(x) = f_1(x)f_2(x)$. В противном случае говорят, что многочлен $f(x) \in K[x]$ *не разложим* (в кольце $\mathcal{K}[x]$).

Замечание 1.34. Если $\mathcal{K}$ – область целостности, то $m = m_1 + m_2$. В противном случае можно только утверждать, что $m \leq m_1 + m_2$.

Подставим в многочлен $f(x) \in K[x]$ вместо переменной x элемент $a \in K$. Выполнив действия, получим элемент $f(a) \in K$, т.е. каждый многочлен $f(x) \in K[x]$ определяет отображение множества K в себя.

Замечание 1.35. Существуют такие кольца $\mathcal{K}$, что различные многочлены $f_1(x), f_2(x) \in K[x]$ определяют одно и то же отображение множества K в себя.

Обозначим через «$\equiv$» следующее отношение эквивалентности на множестве $K[x]$: $f_1(x) \equiv f_2(x)$ $(f_1(x), f_2(x) \in K[x])$ тогда и только тогда, когда многочлены $f_1(x)$ и $f_2(x)$ определяют одно и то же отображение множества K в себя. Тогда $\mathcal{K}[x]/_{\equiv} = (K[x]/_{\equiv}, +, \cdot)$ – ассоциативно-коммутативное фактор-кольцо всех полиномиальных отображений (от одной переменной) множества K в себя.

Элемент $a \in K$ – *корень* многочлена $f(x) \in \mathcal{K}[x]$, если $f(a) = 0$. Истинно утверждение: элемент $a \in K$ – корень многочлена $f(x)$ тогда и только тогда, когда $f(x) = (x - a)g(x)$, где $g(x) \in K[x]$ – многочлен, степень которого на единицу меньше степени многочлена $f(x)$. Если $f(x) = (x - a)^k g(x)$ $(k \in \mathbb{N})$, где $g(x) \in K[x]$ – такой многочлен, что $g(a) \neq 0$, то число k – *кратность* корня a. Корень a – *кратный*, если $k \geq 2$. Если $\mathcal{K}$ – область целостности, то любой многочлен $f(x) \in K[x]$ степени $m \in \mathbb{N}$ имеет не больше, чем m корней (с учетом их кратности).

Производная $\mathsf{D}f(x)$ многочлена $f(x) = a_0 + a_1x + \cdots + a_mx^m \in K[x]$ определяется равенством $\mathsf{D}f(x) = a_1 + 2a_2x + \cdots + ma_mx^{m-1}$. Ясно, что $a \in K$ – кратный корень многочлена $f(x) \in K[x]$ тогда и только тогда, когда a – корень многочлена $\mathsf{D}f(x)$.

Замечание 1.36. Проверку наличия общего корня любых ненулевых многочленов $f(x) = \sum\limits_{i=0}^{n} a_ix^i \in K[x]$ $(n \in \mathbb{N})$ и $g(x) = \sum\limits_{i=0}^{m} b_ix^i \in K[x]$ $(m \in \mathbb{N})$ можно осуществить с использованием их *результанта* $\mathrm{Res}(f, g, x) = \det(\mathrm{Syl}(f, g, x))$, где $\mathrm{Syl}(f, g, x)$ – *матрица Сильвестра*, т.е. $\mathrm{Syl}(f, g, x) = (\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(m)}, \mathbf{b}^{(1)}, \ldots, \mathbf{b}^{(n)})$, где $\mathbf{a}^{(i)} = (\underbrace{0, \ldots, 0}_{i-1 \text{ раз}}, a_n, \ldots, a_0, \underbrace{0, \ldots, 0}_{m-i \text{ раз}})^T$ $(i = 1, \ldots, m)$, $\mathbf{b}^{(j)} = (\underbrace{0, \ldots, 0}_{j-1 \text{ раз}}, b_m, \ldots, b_0, \underbrace{0, \ldots, 0}_{n-i \text{ раз}})^T$ $(j = 1, \ldots, n)$ (определитель $k \times k$-матрицы $A = (a_{ij})$ над кольцом $\mathcal{K}$ определяется равенством $\det(A) = \sum\limits_{\sigma \in \mathcal{S}(k)} \mathrm{sgn}(\sigma) a_{1\sigma(1)} \ldots a_{k\sigma(k)}$, где $\mathrm{sgn}(\sigma) = 1$, если σ – четная перестановка и $\mathrm{sgn}(\sigma) = -1$, если σ – нечетная перестановка). Если много-

члены $f(x)$ и $g(x)$ имеют общий корень, то $\mathrm{Res}(f,g,x) = 0$. В случае, когда $\mathcal{K}$ – поле, равенство $\mathrm{Res}(f,g,x) = 0$ истинно тогда и только тогда, когда многочлены $f(x)$ и $g(x)$ имеют общий корень. *Дискриминант* $\mathrm{disc}(f)$ ненулевого многочлена $f(x) = \sum\limits_{i=0}^{n} a_i x^i \in K[x]$ определяется равенством $a_n \mathrm{disc}(f) = (-1)^{0.5n(n-1)}\mathrm{Res}(f, \mathsf{D}f, x)$. Если многочлен $f(x) \in K[x]$ со старшим коэффициентом, не являющимся делителем нуля, имеет кратный корень, то $\mathrm{disc}(f) = 0$.

Пусть $\mathcal{K}_1 = (K_1, +, \cdot)$ – унитарное надкольцо кольца $\mathcal{K} = (K, +, \cdot)$. Элемент $a \in K_1$ называется *алгебраическим* элементом над $\mathcal{K}$, если существует такой ненулевой многочлен $f(x) \in K[x]$, что $f(a) = 0$. В противном случае $a \in K_1$ – *трансцендентный* элемент над $\mathcal{K}$. Для любого элемента $a \in K_1$ множество $\{f(a) | f(x) \in K[x]\}$ определяет наименьшее подкольцо кольца $\mathcal{K}_1$, содержащее кольцо $\mathcal{K}$ и элемент a. Если $\mathcal{K}_1$ – унитарное надкольцо области целостности $\mathcal{K}$, то для любого элемента $a \in K_1$, алгебраического над $\mathcal{K}$, многочлен $f(x) \in K[x]$ наименьшей степени, корнем которого является элемент a, неразложим в кольце $\mathcal{K}[x]$.

Замечание 1.37. Для любого кольца $\mathcal{K}$ с единицей $\mathcal{K}[x]$ является наименьшим унитарным надкольцом, содержащим кольцо $\mathcal{K}$ и трансцендентный элемент x.

Пусть $\mathcal{K}$ – гауссово кольцо. Многочлен $f(x) \in K[x]$ положительной степени называется *примитивным*, если его коэффициенты не имеют общих делителей, отличных от обратимых элементов.

Любой многочлен $f(x) \in K[x]$ степени $m \in \mathbb{N}$ единственным образом (с точностью до обратимых множителей, являющихся элементами кольца $\mathcal{K}$) может быть представлен в виде $f(x) = a\prod\limits_{i=1}^{k} f_i(x)$, где $a \in K$, а $f_i(x) \in K[x]$ $(i = 1, \ldots, k)$ – не разложимые примитивные многочлены, сумма степеней которых равна m, т.е. $\mathcal{K}[x]$ – гауссово кольцо.

Замечание 1.38. В гауссовом кольце $\mathcal{K}[x]$ разложение $f(x) = a\prod\limits_{i=1}^{k} f_i(x)$ многочлена $f(x) \in K[x]$ положительной степени в произведение не разложимых примитивных многочленов называется *каноническим разложением* $f(x)$.

Пусть $\mathcal{K}$ – поле. Тогда $\mathcal{K}[x]$ – евклидово кольцо (число $n(f(x))$ является степенью многочлена $f(x)$). Многочлен $f(x) \in K[x]$ положительной степени называется *приведенным*, если его старший коэффициент равен единице. Любой многочлен $f(x) \in K[x]$ степени $m \in \mathbb{N}$ единственным образом может быть представлен в виде $f(x) = a\prod\limits_{i=1}^{k} f_i(x)$, где $a \in K$ – старший коэффициент многочлена $f(x)$, а $f_i(x) \in K[x]$ $(i = 1, \ldots, k)$ –

не разложимые приведенные многочлены, сумма степеней которых равна m.

Поле $\mathcal{K}$ *алгебраически замкнуто*, если каждый не разложимый многочлен $f(x) \in K[x]$ имеет степень 1, т.е. каждый многочлен положительной степени раскладывается в $\mathcal{K}[x]$ в произведение многочленов 1-й степени.

Замечание 1.39. Известно, что алгебраически замкнутое поле – бесконечное поле. Поэтому, никакое конечное поле не является алгебраически замкнутым.

В кольце $\mathcal{K}[x] = (K[x], +, \cdot)$ допустимо сокращение на многочлены, принадлежащие множеству $S_{\mathcal{K}[x]} = \{f(x) \in K[x] | \mathrm{Val}\, f \subseteq S_{\mathcal{K}}\}$, т.е. $\mathcal{K}[x]$ можно изоморфно вложить в такое ассоциативно-коммутативное кольцо рациональных дробей $\overline{\mathcal{K}[x]} = (\overline{K[x]}, +, \cdot)$ с единицей, что каждый элемент $f(x) \in S_{\mathcal{K}[x]}$ имеет в кольце $\overline{\mathcal{K}[x]}$ обратный элемент.

Замечание 1.40. Ассоциативно-коммутативное кольцо $\overline{\mathcal{K}[x]} = (\overline{K[x]}, +, \cdot)$ строится в соответствии со схемой, представленной в замечании 1.19.

Пусть $R_{\mathcal{K}[x]} = \{\frac{f(x)}{g(x)} | f(x) \in K[x],\ g(x) \in S_{\mathcal{K}[x]}\}$ – множество дробей (частных) над кольцом $\mathcal{K}[x]$. Положив $\frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} = \frac{f_1(x)g_2(x)+f_2(x)g_1(x)}{g_1(x)g_2(x)}$ и $\frac{f_1(x)}{g_1(x)} \cdot \frac{f_2(x)}{g_2(x)} = \frac{f_1(x)f_2(x)}{g_1(x)g_2(x)}$ для любых $\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)} \in S_{\mathcal{K}[x]}$, получим алгебру $\mathcal{R}_{\mathcal{K}[x]} = (R_{\mathcal{K}[x]}, +, \cdot)$. Обозначим через «$\equiv$» такое отношение эквивалентности на множестве $R_{\mathcal{K}[x]}$, что $\frac{f_1(x)}{g_1(x)} \equiv \frac{f_2(x)}{g_2(x)}$ тогда и только тогда, когда $f_1(x)g_2(x) = f_2(x)g_1(x)$. Положим $\overline{K[x]} = R_{\mathcal{K}[x]}/_{\equiv}$ и определим на множестве $\overline{K[x]}$ операции «$+$» и «$\cdot$» следующим образом: если $H_1, H_2 \in \overline{K[x]}$ ($\frac{f_1(x)}{g_1(x)} \in H_1, \frac{f_2(x)}{g_2(x)} \in H_2$), то $H_1 + H_2 = H$, где $\frac{f_1(x)g_2(x)+f_2(x)g_1(x)}{g_1(x)g_2(x)} \in H$ и $H_1 H_2 = H$, где $\frac{f_1(x)f_2(x)}{g_1(x)g_2(x)} \in H$. Получим ассоциативно-коммутативное кольцо $\overline{\mathcal{K}[x]} = (\overline{K[x]}, +, \cdot)$ рациональных дробей от неизвестного x над кольцом $\mathcal{K}$. Единица кольца $\overline{\mathcal{K}[x]}$ – элемент $\{\frac{f(x)}{f(x)} | f(x) \in S_{\mathcal{K}[x]}\}$, элементу $f(x) \in K[x]$ кольца $\mathcal{K}[x]$ соответствует элемент $\{\frac{f(x)g(x)}{g(x)} | g(x) \in S_{\mathcal{K}[x]}\}$ кольца $\overline{\mathcal{K}[x]}$, а элементом кольца $\overline{\mathcal{K}[x]}$, обратным элементу $\{\frac{f(x)g(x)}{g(x)} | g(x) \in S_{\mathcal{K}[x]}\}$ ($f(x) \in S_{\mathcal{K}[x]}$) является элемент $\{\frac{g(x)}{f(x)g(x)} | g(x) \in S_{\mathcal{K}[x]}\}$.

Если $\mathcal{K}$ является областью целостности, то $\overline{\mathcal{K}[x]}$ является *полем рациональных дробей*.

Подставив вместо x элемент $a \in K$ в $\frac{f(x)}{g(x)} \in \overline{K[x]}$, получим элемент $\frac{f(a)}{g(a)} \in \overline{K}$, т.е. каждый элемент $\frac{f(x)}{g(x)} \in \overline{K[x]}$ определяет отображение множества K в множество $\overline{K}$. Определим на множестве $\overline{K[x]}$ отношение эквивалентности «$\equiv$» следующим образом: $\frac{f_1(x)}{g_1(x)} \equiv \frac{f_2(x)}{g_2(x)}$ ($\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)} \in \overline{K[x]}$) тогда и только тогда, когда дроби $\frac{f_1(x)}{g_1(x)}$ и $\frac{f_2(x)}{g_2(x)}$ определяют одно и то же отображение множества K в множество $\overline{K}$. Получим ассоциативно-коммутативное фактор-кольцо $\overline{\mathcal{K}[x]}/_{\equiv} = (\overline{K[x]}/_{\equiv}, +, \cdot)$ всех рациональных отображений (от одной переменной) множества K в множество $\overline{K}$.

Кольцо $\mathcal{K}[x_1,\ldots,x_n] = (K[x_1,\ldots,x_n],+,\cdot)$ $(n \in \mathbb{N}, n \geq 2)$ многочленов от переменных $x_1,\ldots,x_n$ над кольцом $\mathcal{K}$ определяется индуктивно, т.е. $\mathcal{K}[x_1,\ldots,x_n] = \mathcal{K}[x_1,\ldots,x_{n-1}][x_n]$. Ненулевой многочлен может быть представлен в виде $f(x_1,\ldots,x_n) = a_0 + \sum\limits_{1\leq i_1<\ldots i_r\leq n} a_{i_1\ldots i_r}x_{i_1}^{\alpha_1}\ldots x_{i_r}^{\alpha_r}$ $(\alpha_1,\ldots,\alpha_r \in \mathbb{N})$, где $a_0, a_{i_1\ldots i_r} \in K$ – коэффициенты. Его степень – это такое максимальное число $\alpha_1+\cdots+\alpha_r$, что $a_{i_1\ldots i_r} \neq 0$.

В кольце $\mathcal{K}[x_1,\ldots,x_n]$ производная $\mathsf{D}_{x_i}f(x_1,\ldots,x_n)$ $(i = 1,\ldots,n)$ многочлена $f(x_1,\ldots,x_n) \in K[x_1,\ldots,x_n]$ по переменной x_i определяется обычным образом, т.е. многочлен $f(x_1,\ldots,x_n)$ рассматривается как многочлен только от переменной x_i, и применяется правило дифференцирования, сформулированное для кольца многочленов от одной переменной.

Подставив в многочлен $f(x_1,\ldots,x_n)$ вместо каждой переменной x_i $(i = 1,\ldots,n)$ элемент $a_i \in K$ и выполнив действия, получим элемент $f(a_1,\ldots,a_n) \in K$. Таким образом, кольцо $\mathcal{K}[x_1,\ldots,x_n]$ определяет кольцо отображений множества K^n в множество K.

Если $\mathcal{K}_1 = (K_1,+,\cdot)$ – унитарное надкольцо кольца $\mathcal{K} = (K,+,\cdot)$, то для любых элементов $a_1,\ldots,a_n \in K_1$ наименьшее подкольцо кольца $\mathcal{K}_1$, содержащее эти элементы и кольцо $\mathcal{K}$, определяется множеством $\{f(a_1,\ldots,a_n)|f(x_1,\ldots,x_n) \in K[x_1,\ldots,x_n]\}$. Эти элементы *алгебраически зависимы* над кольцом $\mathcal{K}$, если существует такой ненулевой многочлен $f(x_1,\ldots,x_n) \in K[x_1,\ldots,x_n]$, что $f(a_1,\ldots,a_n) = 0$. В противном случае эти элементы *алгебраически независимы* над кольцом $\mathcal{K}$.

Замечание 1.41. Если $\mathcal{K}$ – кольцо с единицей, то $\mathcal{K}[x_1,\ldots,x_n]$ – наименьшее унитарное надкольцо, содержащее $\mathcal{K}$ и алгебраически независимые элементы $x_1,\ldots,x_n$.

Кольцо $\mathcal{K}[x_1,\ldots,x_n]$ $(n \geq 2)$ (в отличие от кольца $\mathcal{K}[x]$) не является кольцом главных идеалов.

Для любого фиксированного набора $\mathbf{a} = (a_1,\ldots,a_n) \in K^n$ $(n \in \mathbb{N})$ множество $I_{\mathbf{a}} = \{f(x_1,\ldots,x_n) \in K[x_1,\ldots,x_n]|f(a_1,\ldots,a_n) = 0\}$ является конечно порожденным идеалом кольца $\mathcal{K}[x_1,\ldots,x_n]$.

Замечание 1.42. Множество $M = \{x_1-a_1,\ldots,x_n-a_n\}$ – базис идеала $I_{\mathbf{a}}$.

Идеал $I_{\mathbf{a}}$ является простым идеалом, если $\mathcal{K} = (K,+,\cdot)$ – область целостности. Однако, для любых $\mathbf{a} \neq \mathbf{b}$ $(\mathbf{a},\mathbf{b} \in K^n)$ идеал $I_{\mathbf{a}} \cap I_{\mathbf{b}}$ не является простым идеалом кольца $\mathcal{K}[x_1,\ldots,x_n]$. Имеет место теорема Гильберта о базисе: если $\mathcal{K}$ – нетерово кольцо, то $\mathcal{K}[x_1,\ldots,x_n]$ $(n \in \mathbb{N})$ – нетерово кольцо, т.е. каждый идеал кольца $\mathcal{K}[x_1,\ldots,x_n]$ $(n \in \mathbb{N})$ является конечно порожденным.

Замечание 1.43. Пусть $\mathcal{K} = (K, +, \cdot)$ – область целостности с единицей. Многочлен $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n])$ положительной степени *неприводимый*, если он не может быть разложен в произведение двух многочленов положительной степени. Если $f(x_1, \ldots, x_n) = \prod\limits_{i=1}^{l} f_i^{\alpha_i}(x_1, \ldots, x_n)$ $(\alpha_1, \ldots, \alpha_n \in \mathbb{N})$ – разложение $f(x_1, \ldots, x_n)$ на попарно не ассоциированные неприводимые многочлены $f_i(x_1, \ldots, x_n)$ $(i = 1, \ldots, l)$, то $(f(x_1, \ldots, x_n)) = \prod\limits_{i=1}^{l}(f_i(x_1, \ldots, x_n))^{\alpha_i}$ и $\sqrt{(f(x_1, \ldots, x_n))} = \prod\limits_{i=1}^{l}(f_i(x_1, \ldots, x_n))$.

Кольцо рациональных дробей $\overline{\mathcal{K}[x_1, \ldots, x_n]} = (\overline{K[x_1, \ldots, x_n]}, +, \cdot)$ с единицей строится обычным образом (см. замечание 1.40). Если $\mathcal{K}$ – область целостности, то $\overline{\mathcal{K}[x_1, \ldots, x_n]}$ – поле рациональных дробей. Подставив в $\frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)} \in \overline{K[x_1, \ldots, x_n]}$ вместо переменных $x_1, \ldots, x_n$, соответственно, $a_1, \ldots, a_n \in K^n$, получим элемент $\frac{f(a_1,\ldots,a_n)}{g(a_1,\ldots,a_n)} \in \overline{K}$, т.е. каждый элемент $\frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)} \in \overline{K[x_1, \ldots, x_n]}$ определяет отображение множества K^n в множество $\overline{K}$. Определим на множестве $\overline{K[x_1, \ldots, x_n]}$ отношение эквивалентности «$\equiv$» следующим образом $\frac{f_1(x_1,\ldots,x_n)}{g_1(x_1,\ldots,x_n)} \equiv \frac{f_2(x_1,\ldots,x_n)}{g_2(x_1,\ldots,x_n)}$ тогда и только тогда, когда дроби $\frac{f_1(x_1,\ldots,x_n)}{g_1(x_1,\ldots,x_n)}$ и $\frac{f_2(x_1,\ldots,x_n)}{g_2(x_1,\ldots,x_n)}$ определяют одно и то же отображение множества K^n в множество $\overline{K}$. Получим ассоциативно-коммутативное фактор-кольцо $\overline{\mathcal{K}[x_1, \ldots, x_n]}/_{\equiv} = (\overline{K[x_1, \ldots, x_n]}/_{\equiv} +, \cdot)$ всех рациональных отображений (от n переменных) множества K^n в множество $\overline{K}$.

1.2. Многообразия над кольцами.

В настоящем пункте под кольцом $\mathcal{K} = (K, +, \cdot)$ понимается ассоциативно-коммутативное кольцо. Вместо записи «$f(x_1, \ldots, x_n)$» будем использовать запись «f», если это не вызывает недоразумений.

Рассмотрим основные понятия алгебраической геометрии, в терминах которых будет осуществляться изложение результатов в последующих разделах. Эти понятия подробно рассмотрены в [24,34,46,48,59,111,112].

1.2.1. Основные понятия.

Многообразием в множестве K^n $(n \in \mathbb{N})$, порожденным (ненулевыми) многочленами $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ $(m \in \mathbb{N})$ называется множество

$$V\{f_1, \ldots, f_m\} = \{(a_1, \ldots, a_n) \in K^n | (\forall i = 1, \ldots, m)(f_i(a_1, \ldots, a_n) = 0)\}.$$

Если $\mathcal{K}$ – поле, то многообразие называется *аффинным*.

Гиперповерхностью называется многообразие, порождаемое одним многочленом (если $m = 1$ и $n = 2$, то гиперповерхность называется *кривой* над кольцом $\mathcal{K}$). Таким образом, любое многообразие $V\{f_1, \ldots, f_m\}$ $(m \geq 2)$ – это пересечение гиперповерхностей $V\{f_i\}$ $(i = 1, \ldots, m)$.

Пример 1.6. 1. Если V_i $(i = 1, 2)$ – многообразие в множестве K^{n_i}, то $V_1 \times V_2$ также является многообразием в множестве $K^{n_1+n_2}$.

2. При всех значениях $m, n \in \mathbb{N}$ система линейных уравнений $a_{i1}x_1 + \cdots + a_{in}x_n = b_i$ $(i = 1, \ldots, m)$ определяет в множестве K^n *линейное многообразие*.

3. Если $\mathcal{K} = (K, +, \cdot)$ – область целостности, то каждое непустое конечное множество $S = \{a_1, \ldots, a_n\} \subseteq K$ является многообразием в K, так как $S = V\{\prod_{i=1}^{n}(x - a_i)\}$.

4. Пусть $\mathcal{K} = (K, +, \cdot)$ – конечное кольцо. Тогда $K = V\{\prod_{a \in K}(x - a)\}$, т.е. множество K является многообразием в K.

Более того, для любых чисел $n, r \in \mathbb{N}$ $(r \leq n)$ множество K^r также может рассматриваться как многообразие в K^n.

Действительно, для любых фиксированных элементов $b_1, \ldots, b_{n-r}$ кольца $\mathcal{K}$ истинно равенство

$$V\{\prod_{a_1 \in K}(x_1 - a_1), \ldots, \prod_{a_r \in K}(x_r - a_r), x_{r+1} - b_1, \ldots, x_n - b_{n-r}\} = K^r \times (\{b_1\} \times \cdots \times \{b_{n-r}\}).$$

Отождествив множество $K^r \times (\{b_1\} \times \cdots \times \{b_{n-r}\})$ с множеством K^r, получим требуемое.

В дальнейшем, при необходимости, для конечного кольца $\mathcal{K}$ будем рассматривать множество K^r $(r \in \mathbb{N})$ как многообразие, без уточнения, в каком множестве оно рассматривается.

Замечание 1.44. Для многообразий $V\{f_1, \ldots, f_s\}$ и $V\{g_1, \ldots, g_t\}$ в K^n равенство $V\{f_1, \ldots, f_s\} = V\{g_1, \ldots, g_t\}$ истинно тогда и только тогда, когда над кольцом $\mathcal{K}$ эквивалентны системы полиномиальных уравнений $f_i(x_1, \ldots, x_n) = 0$ $(i = 1, \ldots, s)$ и $g_i(x_1, \ldots, x_n) = 0$ $(i = 1, \ldots, t)$. Таким образом, любое многообразие в K^n – это множество решений класса всех эквивалентных над кольцом $\mathcal{K}$ систем полиномиальных уравнений от n неизвестных.

Если $\{f_1, \ldots, f_s\}$ и $\{g_1, \ldots, g_t\}$ – базисы одного и того же конечно-порожденного идеала кольца $\mathcal{K}[x_1, \ldots, x_n]$, то $V\{f_1, \ldots, f_s\} = V\{g_1, \ldots, g_t\}$. Поэтому говорят о многообразии V_I в K^n, ассоциированном с конечно-порожденным идеалом I кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$. Для любого кольца $\mathcal{K}$ отображение $\mathsf{v}_{\mathcal{K},n}$ $(n \in \mathbb{N})$, определенное на множестве всех конечно-порожденных идеалов кольца $\mathcal{K}[x_1, \ldots, x_n]$ равенством $\mathsf{v}_{\mathcal{K},n}(I) = V_I$, является сюръекцией этого множества на множество всех многообразий в K^n, т.е. на множество классов эквивалентных над кольцом $\mathcal{K}$ систем полиномиальных уравнений от n неизвестных. Отображение $\mathsf{v}_{\mathcal{K},n}$ может не быть инъекцией, так как в кольце $\mathcal{K}[x_1, \ldots, x_n]$ могут существовать такие конечно-порожденные идеалы I_1 и I_2 $(I_1 \neq I_2)$, что $\mathsf{v}_{\mathcal{K},n}(I_1) = \mathsf{v}_{\mathcal{K},n}(I_2)$.

Многообразие $V \subseteq K^n$ *неприводимое*, если для любых многообразий $V_1, V_2 \subseteq K^n$ из равенства $V = V_1 \cup V_2$ вытекает, что $V_1 = V$ или $V_2 = V$.

Пусть $V_1 = V\{f_1, \ldots, f_{m_1}\} \subseteq K^n$ и $V_2 = V\{g_1, \ldots, g_{m_2}\} \subseteq K^n$. Тогда $V_1 \cap V_2 = V\{f_1, \ldots, f_{m_1}, g_1, \ldots, g_{m_2}\}$ и $V_1 \cup V_2 \subseteq V\{f_i g_j | i \in \mathbb{N}_{m_1}, j \in \mathbb{N}_{m_2}\}$.

Замечание 1.45. Пусть $\mathcal{K}$ – область целостности. Если $V_1 = V\{f_1, \ldots, f_{m_1}\} \subseteq K^n$ и $V_2 = V\{g_1, \ldots, g_{m_2}\} \subseteq K^n$, то $V_1 \cup V_2 = V\{f_i g_j | i \in \mathbb{N}_{m_1}, j \in \mathbb{N}_{m_2}\}$. Следовательно, если I_1 и I_2 – конечно-порожденные идеалы кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$, то $\{\mathsf{v}_{\mathcal{K},n}(I_1)\} \cup \{\mathsf{v}_{\mathcal{K},n}(I_2)\} = \mathsf{v}_{\mathcal{K},n}(I_1 I_2)$. Отсюда вытекает, что для любого конечно-порожденного идеала I кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$ многообразие $\mathsf{v}_{\mathcal{K},n}(I)$ неприводимо тогда и только тогда, когда I – простой идеал.

Идеал многообразия $V = V\{f_1, \ldots, f_m\} \subseteq K^n$ определяется равенством $I(V) = \{f \in K[x_1, \ldots, x_n] | (\forall (a_1, \ldots, a_n) \in V)(f(a_1, \ldots, a_n) = 0\}$. Ясно, что $\{f_1, \ldots, f_m\} \subseteq I(V\{f_1, \ldots, f_m\})$.

Замечание 1.46. Таким образом, отображение $\mathsf{i}_{\mathcal{K},n}$ $(n \in \mathbb{N})$, определенное равенством $\mathsf{i}_{\mathcal{K},n}(V) = I(V)$, отображает множество всех многообразий $V \subseteq K^n$ в множество идеалов кольца $\mathcal{K}[x_1, \ldots, x_n]$. Следовательно, определено отображение $\mathsf{i}_{\mathcal{K},n} \circ \mathsf{v}_{\mathcal{K},n}$ множества конечно-порожденных идеалов кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$ в множество идеалов этого кольца. Это отображение обладает следующими свойствами:

1. Для любого конечно-порожденного идеала I кольца $\mathcal{K}[x_1, \ldots, x_n]$ истинно включение $I \subseteq \mathsf{i}_{\mathcal{K},n} \circ \mathsf{v}_{\mathcal{K},n}(I)$.

2. Если $f \in \mathsf{i}_{\mathcal{K},n} \circ \mathsf{v}_{\mathcal{K},n}(I)$ $(f \in K[x_1, \ldots, x_n])$, то $f^m \in \mathsf{i}_{\mathcal{K},n} \circ \mathsf{v}_{\mathcal{K},n}(I)$ для всех $m \in \mathbb{N}$, т.е. для любого конечно-порожденного идеала I кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$ истинно включение $\mathsf{i}_{\mathcal{K},n} \circ \mathsf{v}_{\mathcal{K},n}(I) \subseteq \sqrt{I}$. В частности, если $\mathcal{K}$ – алгебраически замкнутое поле, то $\mathsf{i}_{\mathcal{K},n} \circ \mathsf{v}_{\mathcal{K},n}(I) = \sqrt{I}$ (это равенство называется теоремой Гильберта о нулях).

3. Если $\mathcal{K}$ – область целостности и $f^m \in \mathsf{i}_{\mathcal{K},n} \circ \mathsf{v}_{\mathcal{K},n}(I)$ $(f \in K[x_1, \ldots, x_n])$ для некоторого $m \in \mathbb{N}$, то $f \in \mathsf{i}_{\mathcal{K},n} \circ \mathsf{v}_{\mathcal{K},n}(I)$, т.е. для любого конечно-порожденного идеала I кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$ идеал $\mathsf{i}_{\mathcal{K},n} \circ \mathsf{v}_{\mathcal{K},n}(I)$ – радикальный.

Полиномиальной параметризацией многообразия $V \subseteq K^n$ называется такой набор многочленов $h_1, \ldots, h_n \in K[t_1, \ldots, t_l]$, что точки с координатами

$$\begin{cases} x_1 = h_1(t_1, \ldots, t_l) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_n = h_n(t_1, \ldots, t_l) \end{cases} \qquad ((t_1, \ldots, t_l) \in K^l)$$

принадлежат многообразию V. Набор $\mathsf{h} = (h_1, \ldots, h_n)$ называется *полиномиальным* отображением множества K^l в множество K^n.

Замечание 1.47. Не для всякого многообразия $V \subseteq K^n$ существует полиномиальная параметризация h, удовлетворяющая условию $\mathrm{Val}\,\mathsf{h} = V$.

Обозначим через $P_{K^l\to K^m}$ $(l,m\in\mathbb{N})$ множество всех полиномиальных отображений $\mathsf{f}: K^l\to K^m$. Определим сумму и произведение отображений $\mathsf{f}=(f_1,\dots,f_m)\in P_{K^l\to K^m}$ и $\mathsf{g}=(g_1,\dots,g_m)\in P_{K^l\to K^m}$ равенствами $\mathsf{f}+\mathsf{g}=(f_1+g_1,\dots,f_m+g_m)$ и $\mathsf{fg}=(f_1g_1,\dots,f_mg_m)$. Получим кольцо $\mathcal{P}_{K^l\to K^m}=(P_{K^l\to K^m},+,\cdot)$ всех полиномиальных отображений множества K^l в множество K^m. Полиномиальные отображения $\mathsf{f},\mathsf{g}\in P_{K^l\to K^m}$ определяют одно и то же полиномиальное отображение многообразия $V\subseteq K^l$ в множество K^m, если $\mathsf{f}|_V=\mathsf{g}|_V$. Пусть $P_{V\to K^m}$ – множество всех полиномиальных отображений многообразия V в множество K^m. Тогда $\mathcal{P}_{V\to K^m}=(P_{V\to K^m},+,\cdot)$ – кольцо всех полиномиальных отображений многообразия V в множество K^m.

Замечание 1.48. *Подмногообразием* многообразия $V\subseteq K^l$ называется множество $\mathsf{v}_{V,l}(J)=\{(a_1,\dots,a_l)\in V|(\forall f\in J)(f(a_1,\dots,a_l)=0)\}$, где J – конечно-порожденный идеал кольца $\mathcal{P}_{V\to K}$. Для любого непустого множества $W\subseteq V$ положим $\mathsf{i}_{V,l}(W)=\{f\in P_{V\to K}|(\forall(a_1,\dots,a_l)\in W)(f(a_1,\dots,a_l)=0)\}$. Ясно, что $\mathsf{i}_{V,l}(W)$ – идеал кольца $\mathcal{P}_{V\to K}$. При этом:

1) $J\subseteq\mathsf{i}_{V,l}\circ\mathsf{v}_{V,l}(J)$ для любого конечно-порожденного идеала J кольца $\mathcal{P}_{V\to K}$;

2) $W\subseteq\mathsf{v}_{V,l}\circ\mathsf{i}_{V,l}(W)$ для любого подмногообразия W многообразия V (если $\mathcal{K}$ – алгебраически замкнутое поле, то $W=\mathsf{v}_{V,l}\circ\mathsf{i}_{V,l}(W)$).

Отображения $\mathsf{f}_i=(f_1^{(i)},\dots,f_m^{(i)})\in P_{K^l\to K^m}$ $(i=1,2)$ определяют одно и то же полиномиальное отображение $\mathsf{f}\in P_{V\to K^m}$ тогда и только тогда, когда $f_j^{(1)}\equiv f_j^{(2)}\pmod{\mathsf{i}_{\mathcal{K},l}(V)}$ для всех $j=1,\dots,l$, т.е. построение любого отображения $\mathsf{f}=(f_1,\dots,f_m)\in P_{V\to K^m}$, сводится к выбору компонент f_j $(j=1,\dots,l)$ из классов фактор-множества $K[t_1,\dots,t_l]/_{\equiv_{\mathsf{i}_{\mathcal{K},l}(V)}}$. Ясно, что алгебраические характеристики многообразия V могут быть сформулированы в терминах *координатного кольца*

$$\mathcal{K}[t_1,\dots,t_l]/_{\equiv_{\mathsf{i}_{\mathcal{K},l}(V)}}=(K[t_1,\dots,t_l]/_{\equiv_{\mathsf{i}_{\mathcal{K},l}(V)}},+_{\mathsf{i}_{\mathcal{K},l}(V)},\cdot_{\mathsf{i}_{\mathcal{K},l}(V)})$$

многообразия V, а сравнение многообразия $V\subseteq K^l$ с многообразием $W\subseteq K^m$ сводится к сравнению их координатных колец $\mathcal{K}[t_1,\dots,t_l]/_{\equiv_{\mathsf{i}_{\mathcal{K},l}(V)}}$ и $\mathcal{K}[t_1,\dots,t_m]/_{\equiv_{\mathsf{i}_{\mathcal{K},m}(W)}}$.

Пусть $P_{V\to W}$ – множество всех полиномиальных отображений многообразия $V\subseteq K^l$ в многообразие $W\subseteq K^m$. Многообразия $V\subseteq K^l$ и $W\subseteq K^m$ *изоморфны*, если существуют такие отображения $\mathsf{f}\in P_{V\to W}$ и $\mathsf{g}\in P_{W\to V}$, что $\mathsf{f}\circ\mathsf{g}$ – тождественное отображение на многообразии W, а $\mathsf{g}\circ\mathsf{f}$ – тождественное отображение на многообразии V.

Пусть $\widetilde{R}_{\mathcal{K}[t_1,\dots,t_l]}$ – множество всех таких дробей $\frac{f}{g}$ $(f,g\in K[t_1,\dots,t_l])$, что g – ненулевой многочлен. Элемент $\frac{f}{g}\in\widetilde{R}_{\mathcal{K}[t_1,\dots,t_l]}$ – *частичное ра-*

циональное отображение множества K^l в множество $\widetilde{R}_{\mathcal{K}} = \{\frac{a}{b} | b \neq 0\}$. При этом $Dom\,\frac{f}{g} = \{(a_1, \ldots, a_l) \in K^l | g(a_1, \ldots, a_l) \neq 0$. Для элемента $r \in \widetilde{R}_{\mathcal{K}[t_1,\ldots,t_l]}$ положим $\mathtt{S}_r = \{(a_1, \ldots, a_l) \in K^l | r(a_1, \ldots, a_l) \in K\}$.

Рациональная параметризация многообразия $V \subseteq K^n$ – такой набор элементов $r_1, \ldots, r_n \in \widetilde{R}_{\mathcal{K}[t_1,\ldots,t_l]}$, что $\bigcap\limits_{i=1}^{n} \mathtt{S}_{r_i} \neq \emptyset$ и точки с координатами

$$\begin{cases} x_1 = r_1(t_1, \ldots, t_l) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_n = r_n(t_1, \ldots, t_l) \end{cases} \qquad ((t_1, \ldots, t_l) \in \bigcap_{i=1}^{n} \mathtt{S}_{r_i})$$

принадлежат многообразию V. Набор $\mathsf{r} = (r_1, \ldots, r_n)$ называется частичным рациональным отображением множества K^l в множество $\widetilde{R}^n_{\mathcal{K}}$. При этом $Dom\,\mathsf{r} = \bigcap\limits_{i=1}^{n} Dom\,r_i$. Обозначим через $R_{K^l \mapsto \widetilde{R}^n_{\mathcal{K}}}$ $(l, n \in \mathbb{N})$ множество всех частичных рациональных отображений $\mathsf{r} : K^l \mapsto \widetilde{R}^n_{\mathcal{K}}$.

Пусть $V \subseteq K^l$ и $W \subseteq K^n$ – непустые неприводимые многообразия, а $R_{V \to W}$ – множество всех таких рациональных отображений $\mathsf{r} \in R_{K^l \mapsto \widetilde{R}^n_{\mathcal{K}}}$, что $\emptyset \neq \mathsf{r}(V \cap Dom\,\mathsf{r}) \subseteq W$. Многообразия $V \subseteq K^l$ и $W \subseteq K^n$ *бирационально эквивалентны*, если существуют такие отображения $\mathsf{r}_1 \in P_{V \to W}$ и $\mathsf{r}_2 \in P_{W \to V}$, что $\mathsf{r}_1 \circ \mathsf{r}_2$ – тождественное отображение на непустом подмножестве $\mathsf{r}_1(\mathsf{r}_2(W \cap Dom\,\mathsf{r}_2) \cap Dom\,\mathsf{r}_1) \subseteq W$, а $\mathsf{r}_2 \circ \mathsf{r}_1$ – тождественное отображение на непустом подмножестве $\mathsf{r}_2(\mathsf{r}_1(V \cap Dom\,\mathsf{r}_1) \cap Dom\,\mathsf{r}_2) \subseteq V$. Неприводимое многообразие $W \subseteq K^n$ – *рациональное*, если существует такое $l \in \mathbb{N}$, что W бирационально эквивалентно множеству K^l.

1.2.2. Кривые над кольцами.

В соответствии с традицией кольцо многочленов от двух переменных над кольцом $\mathcal{K}$ будем обозначать через $\mathcal{K}[x, y] = (K[x, y], +, \cdot)$.

Плоской алгебраической кривой Γ над кольцом $\mathcal{K} = (K, +, \cdot)$ называется многообразие $V(f)$ в K^2, где $f \in K[x, y]$ – многочлен положительной степени (в дальнейшем, для краткости, словосочетание «плоская алгебраическая» будет опускаться).

Замечание 1.49. Если $\mathcal{K}$ – поле, то $\Gamma = V(f)$ $(f \in K[x, y])$ – *аффинная кривая.*

Для кривой $\Gamma = V(f)$ $(f \in K[x, y])$ любое уравнение $g(x, y) = 0$ $(g \in \mathsf{i}_{\mathcal{K},2}(V(f)))$ называется *уравнением кривой* Γ.

Замечание 1.50. Пусть кольцо $\mathcal{K} = (K, +, \cdot)$ не содержит делителей нуля. Если существует разложение $g(x,y) = \prod\limits_{i=1}^{l} g_i^{\alpha_i}(x,y)$ $(\alpha_1, \ldots, \alpha_n \in \mathbb{N}, n \geq 2)$ многочлена $g(x,y)$ на попарно не ассоциированные неприводимые многочлены $g_i(x,y)$ $(i = 1, \ldots, l)$, то кривая $V(g)$ – объединение кривых $V(g_i)$ $(i = 1, \ldots, l)$. Если же $g \in K[x,y]$ – неприводимый многочлен, то кривая $V(g)$ – *неприводимая*.

В дальнейшем предполагается, что кривая $\Gamma = V(f)$ $(f \in K[x,y])$ задана таким уравнением $g(x,y) = 0$, что $g \in \mathsf{i}_{\mathcal{K},2}(V(f))$ – многочлен наименьшей положительной степени. Степень многочлена g называется *степенью кривой* $\Gamma = V(g)$, а корни уравнения $g(x,y) = 0$ – *точками* кривой Γ. Кривая $\Gamma = V(g)$ $(g \in K[x,y])$ называется *коникой*, если g – многочлен 2-й степени, и *кубикой*, если g – многочлен 3-й степени.

Замечание 1.51. Общее уравнение коники над кольцом $\mathcal{K} = (K, +, \cdot)$ имеет вид $ax^2 + bxy + cy^2 + dx + ey + f = 0$ $(a, b, c, d, e, f \in K)$. В зависимости от значений параметров $a, b, c, d, e, f \in K$ можно выделить различные типы коник над кольцом $\mathcal{K}$. Для поля $\mathcal{R}$ действительных чисел стандартная классификация имеет вид: эллипс, парабола, гипербола, изолированная точка, пустое множество, прямая, пара пересекающихся прямых, параллельные прямые, двойная прямая. Для произвольного кольца $\mathcal{K}$, классификация коник существенно зависит от структуры этого кольца и, чаще всего, осуществляется в зависимости от контекста решаемых задач.

Значительно сложнее ситуация с кубикой. Известна некоторая классификация кубик (с точностью до бирациональной эквивалентности многообразий) для поля $\mathcal{K} = (K, +, \cdot)$. В этом случае, как правило, рассматривают кубики вида $y^2 = f(x)$, где $f \in K[x]$ - многочлен 3-й степени. Это обусловлено тем, что над алгебраически замкнутым полем неприводимая кубика бирационально эквивалентна кривой именно этого вида. При этом, кривые $y^2 = f(x)$, для которых многочлен $f(x)$ не имеет кратных корней, называются *эллиптическими кривыми*.

Кривая $\Gamma = V(g)$ $(g \in K[x,y])$ – *рациональная*, если для многообразия $V(g)$ существует рациональная параметризация $\mathsf{r} : K \mapsto \widetilde{R}^2_{\mathcal{K}}$ $(\mathsf{r} = (\psi, \chi),\ \psi, \chi \in R_{K \mapsto \widetilde{R}_{\mathcal{K}}})$, т.е. $g(\psi(t), \chi(t)) = 0$ $(t \in Dom\,\psi \cap Dom\,\chi)$.

Замечание 1.52. Если $\mathcal{K} = (K, +, \cdot)$ – поле, то построение рациональной параметризации неприводимой рациональной кривой $\Gamma = V(g)$ $(g \in K[x,y])$ может быть осуществлено следующим образом: зафиксируем точку $(x_0, y_0) \in \Gamma$ и сопоставим точке $(x,y) \in \Gamma \backslash \{(x_0, y_0)\}$ угловой коэффициент t прямой, проходящей через точки (x_0, y_0) и (x,y). Этот метод, в частности, применим при поиске решений обычного рационального уравнения $f(x,y) = 0$ $(x, y \in \mathbb{Q})$, если известно одно из его решений. Однако если кольцо $\mathcal{K}$ не является областью целостности, то семейство отображений $y = ax$ $(a \in K)$ не может рассматриваться как проектирование из точки (x_0, y_0) на

множество K. Именно по этой причине и возникает сложность построения соответствия между значениями параметра и точками исследуемой кривой.

Точка (x_0, y_0) кривой $\Gamma = V(g)$ называется:
1) *особой*, если $\mathsf{D}_x g(x,y)|_{(x_0,y_0)} = 0$ и $\mathsf{D}_y g(x,y)|_{(x_0,y_0)} = 0$;
2) *простой*, если она не является особой точкой.
Кривая Γ – *гладкая*, если все ее точки простые.

Замечание 1.53. Любая эллиптическая кривая является гладкой.

Отметим, что любая неприводимая кривая над областью целостности может иметь только конечное число особых точек.

Замечание 1.54. Пусть (x_0, y_0) – особая точка неприводимой кривой $\Gamma = V(g)$ над областью целостности $\mathcal{K} = (K, +, \cdot)$. При замене $x \to x - x_0$, $y \to y - y_0$ (т.е. при сдвиге начала координат в точку (x_0, y_0)) точка $(0,0)$ – особая точка кривой Γ. При этом в уравнении кривой Γ младшие члены многочлена имеют степень r $(r \geq 2)$. В этом случае говорят, что $(0,0)$ – *r-кратная* особая точка кривой Γ. Рассмотрим следующие случаи.

1. Пусть $r = 2$, т.е. $(0,0)$ – 2-кратная особая точка. Тогда в уравнении неприводимой кривой Γ младшие члены многочлена имеют вид $ax^2 + bxy + cy^2$. Если при переходе к алгебраически замкнутому полю $\mathcal{K}' \supseteq \mathcal{K}$ многочлен $ax^2 + bxy + cy^2$:

1) разлагается на два различных линейных множителя, то особая точка $(0,0)$ называется *узлом*;

2) является полным квадратом, то особая точка $(0,0)$ называется *острием*.

2. Пусть Γ – неприводимая кривая степени $n \in \mathbb{N}$, а $(0,0)$ – $(n-1)$-кратная особая точка. Тогда при переходе к алгебраически замкнутому полю $\mathcal{K}' \supseteq \mathcal{K}$ кривая Γ является рациональной кривой.

3. Пусть Γ – неприводимая кривая степени $n \in \mathbb{N}$, а $(0,0)$ – $(n-2)$-кратная особая точка. Тогда кривая Γ называется *гиперэллиптической*.

Пусть $\mathcal{K} = (K, +, \cdot)$ – поле. Определим на множестве

$$\mathbf{S} = \{(\xi, \eta, \zeta) \in K^3 | (\xi, \eta, \zeta) \neq (0,0,0)\}$$

отношение эквивалентности «$\sim$» следующим образом:

$$(\forall (\xi_1, \eta_1, \zeta_1), (\xi_2, \eta_2, \zeta_2) \in \mathbf{S})((\xi_1, \eta_1, \zeta_1) \sim (\xi_2, \eta_2, \zeta_2) \Leftrightarrow$$

$$\Leftrightarrow (\exists \lambda \in K \backslash \{0\})(\xi_1 = \lambda \xi_2 \,\&\, \eta_1 = \lambda \eta_2 \,\&\, \zeta_2 = \lambda \zeta_1)).$$

Фактор-множество $\mathbf{P} = \mathbf{S}/_\sim$ называется *проективной плоскостью* над полем $\mathcal{K}$, а элементы множества $\mathbf{P}$ – *точками* проективной плоскости. Точка $M = \{(\lambda\xi, \lambda\eta, \lambda\zeta) | \lambda \in K \backslash \{0\}\} \in \mathbf{P}$ в *проективных координатах* записывается в виде $M = (\xi : \eta : \zeta)$.

Точки проективной плоскости $\mathbf{P}$ относительно координаты:

1) ξ делятся на точки аффинной плоскости $\mathbf{A}_1 = \{(y,z)|y,z \in K\}$, где $y = \frac{\eta}{\xi}$ и $z = \frac{\zeta}{\xi}$, и бесконечно удаленные точки, для которых $\xi = 0$;

2) η делятся на точки аффинной плоскости $\mathbf{A}_2 = \{(x,z)|x,z \in K\}$, где $x = \frac{\xi}{\eta}$ и $z = \frac{\zeta}{\eta}$, и бесконечно удаленные точки, для которых $\eta = 0$;

3) ζ делятся на точки аффинной плоскости $\mathbf{A}_3 = \{(x,y)|x,y \in K\}$, где $x = \frac{\xi}{\zeta}$ и $y = \frac{\eta}{\zeta}$, и бесконечно удаленные точки, для которых $\zeta = 0$.

Замечание 1.55. Аффинные плоскости $\mathbf{A}_1$, $\mathbf{A}_2$ и $\mathbf{A}_3$ попарно пересекаются. Действительно,точка $M = (\xi : \eta : \zeta) \in \mathbf{P}\ \xi \neq 0, \eta \neq 0, \zeta \neq 0)$ имеет:

1) в аффинной плоскости $\mathbf{A}_1$ координаты $(y,z) = (\frac{\eta}{\xi}, \frac{\zeta}{\xi})$;

2) в аффинной плоскости $\mathbf{A}_2$ координаты $(x',z') = (\frac{\xi}{\eta}, \frac{\zeta}{\eta})$;

3) в аффинной плоскости $\mathbf{A}_3$ координаты $(x'',y'') = (\frac{\xi}{\zeta}, \frac{\eta}{\zeta})$.

Преобразование $\mathbf{u}' = A\mathbf{u} + \mathbf{b}$, где $\mathbf{u} = (x,y)^T$, $\mathbf{b} = (b_1,b_2)^T$, а A – обратимая 2×2-матрица называется *аффинным преобразованием* аффинной плоскости (если A – ортогональная матрица, то преобразование – *евклидово*), а вектор $\mathbf{b} = (b_1,b_2)^T$ называется *вектором сдвига.*

Преобразование $\mathbf{U}' = D\mathbf{U}$, где D – обратимая 3×3-матрица, а $\mathbf{U} = (\xi,\eta,\zeta)^T$ называется *проективным преобразованием* проективной плоскости $\mathbf{P}$.

Замечание 1.56. Представим матрицу D в виде

$$D = \left(\begin{array}{cc|c} & A & \\ c & d & \mathbf{b} \\ \hline & & e \end{array}\right).$$

На аффинной плоскости $\mathbf{A}_3$ проективное преобразование совпадает с дробно-линейным преобразованием

$$\binom{x}{y} \mapsto \frac{1}{cx+dy+e}\left(A\binom{x}{y} + \mathbf{b}\right)\ \ (cx+dy+e \neq 0).$$

Проективная кривая (в проективной плоскости $\mathbf{P}$) задается уравнением $G(\xi,\eta,\zeta) = 0$, где G – однородный многочлен.

Замечание 1.57. Для любого $\lambda \neq 0$ равенство $G(\xi,\eta,\zeta) = 0$ сохраняется при замене $\xi' = \lambda\xi$, $\eta' = \lambda\eta$ и $\zeta' = \lambda\zeta$, т.е.задание алгебраической кривой в проективной плоскости не зависит от выбора однородных координат точки.

Аффинной кривой, определяемой уравнением $g(x,y) = 0$, где $g(x,y)$ – многочлен степени n, соответствует проективная кривая, определяемая уравнением $G(\xi,\eta,\zeta) = 0$, где $G(\xi,\eta,\zeta) = \zeta^n g\left(\frac{\xi}{\zeta}, \frac{\eta}{\zeta}\right)$ – однородный многочлен степени n. Обратно, проективная кривая, определяемая уравнением $G(\xi,\eta,\zeta) = 0$, где $G(\xi,\eta,\zeta)$ – однородный многочлен степени n состоит из аффинной кривой, определяемой уравнением $g(x,y) = 0$, где $g(x,y) = G(x,y,1)$ – многочлен степени n, и бесконечно удаленных точек, удовлетворяющих уравнению $G(\xi,\eta,0) = 0$.

Осуществив в частичном рациональном отображении $r(x,y) = \frac{p(x,y)}{q(x,y)}$ подстановку $x = \frac{\xi}{\zeta}$ и $y = \frac{\eta}{\zeta}$, получим частичное рациональное отображение $R(\xi,\eta,\zeta) = \frac{P(\xi,\eta,\zeta)}{Q(\xi,\eta,\zeta)}$, определенное на проективной плоскости $\mathbf{P}$, где P и Q – однородные многочлены.

Следовательно, каждому частичному рациональному отображению $(x,y) \mapsto (r_1(x,y), r_2(x,y))$ аффинной плоскости $\mathbf{A}_3$ соответствует такое частичное отображение $(\xi : \eta : \zeta) \mapsto (P(\xi,\eta,\zeta) : Q(\xi,\eta,\zeta) : H(\xi,\eta,\zeta))$ проективной плоскости $\mathbf{P}$ в себя, что P, Q и H – однородные многочлены одной и той же степени $n \in \mathbb{N}$. Это отображение определено в точке $M = (\xi : \eta : \zeta) \in \mathbf{P}$ тогда и только тогда, когда в этой точке хотя бы один из многочленов P, Q или H не обращается в нуль.

Пусть Γ – кривая в проективной плоскости $\mathbf{P}$, определяемая уравнением $G(\xi,\eta,\zeta) = 0$. Точка $M = (\xi_0 : \eta_0 : \zeta_0) \in \Gamma$ называется:

1) *особой*, если $\mathsf{D}_\xi G(\xi,\eta,\zeta)|_{(\xi_0,\eta_0,\zeta_0)} = 0$, $\mathsf{D}_\eta G(\xi,\eta,\zeta)|_{(\xi_0,\eta_0,\zeta_0)} = 0$ и $\mathsf{D}_\zeta G(\xi,\eta,\zeta)|_{(\xi_0,\eta_0,\zeta_0)} = 0$;

2) *простой*, если она не является особой точкой.

Кривая Γ в проективной плоскости $\mathbf{P}$, все точки которой – простые, называется *гладкой* кривой.

Замечание 1.58. Если $\mathcal{K} = (K,+,\cdot)$ – область целостности, то исследование кривой $\Gamma = V(g)$ $(g \in K[x,y])$ может быть осуществлено следующим образом.

Перейдем к полю частных $\overline{\mathcal{K}} = (\overline{K},+,\cdot)$. Рассмотрим над этим полем, кривую $\overline{\Gamma}$, определенную уравнением

$$g(x,y) = 0 \ (x,y \in \overline{K}).$$

Для ее исследования могут быть использованы все рассмотренные выше конструкции. Остается переформулировать эти результаты для кривой Γ, т.е. сформулировать их при дополнительном условии, что $x, y \in K$.

Если кольцо $\mathcal{K} = (K,+,\cdot)$ содержит делители нуля, то при исследовании кривой Γ возникают следующие обстоятельства.

Во-первых, при построении кольца частных $\overline{\mathcal{K}}$ обратимыми становятся только элементы множества $S_{\mathcal{K}}$, т.е. возникают сложности с построением рациональной параметризации кривой Γ.

Во-вторых, при построении проективной плоскости $\mathbf{P}$ естественно определить отношение эквивалентности «$\sim$» на множестве $\mathbf{S}$ следующим образом: $(\xi_1,\eta_1,\zeta_1) \sim (\xi_2,\eta_2,\zeta_2)$ тогда и только тогда, когда (ξ_1,ξ_2), (η_1,η_2) и (ζ_1,ζ_2) – пары ассоциированных элементов мультипликативной полугруппы $(\overline{K},\cdot)$. Однако, при этом в множестве $\mathbf{P}$ возникают точки вида $M = \{(\lambda\xi,\lambda\eta,\lambda\zeta) | \lambda \in \overline{K}^{inv}\}$, где ξ, η и ζ – делители нуля. Эти точки не являются ни точками аффинной плоскости, ни бесконечно удаленными точками.

Из-за наличия таких точек возникают сложности при интерпретации для кривой Γ свойств соответствующей ей кривой, определенной в множестве $\mathbf{P}$.

1.2.3. Эллиптические кривые над полями.

Уравнением Вейерштрасса для кубики Γ над полем $\mathcal{K}$ называется уравнение вида

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_1, a_2, a_3, a_4, a_6 \in K). \qquad (1.2)$$

Замечание 1.59. Уравнение (1.2) может рассматриваться над любым расширением $\widetilde{\mathcal{K}} = (\widetilde{K}, +, \cdot)$ поля $\mathcal{K}$. Чтобы подчеркнуть, что кубика Γ рассматривается над полем $\widetilde{\mathcal{K}}$, используют запись $\Gamma/\widetilde{\mathcal{K}}$. Решения уравнения (1.2) в поле $\widetilde{\mathcal{K}}$ называются *$\widetilde{\mathcal{K}}$-рациональными точками* кубики Γ. Множество всех точек кубики Γ над расширением $\widetilde{\mathcal{K}}$ обозначается через $\Gamma(\widetilde{\mathcal{K}})$.

Кубика Γ, определенная уравнением (1.2) – *эллиптическая кривая*, если ни для одного расширения $\widetilde{\mathcal{K}}$ поля $\mathcal{K}$ кубика $\Gamma/\widetilde{\mathcal{K}}$ не содержит особых точек. Критерий того, что кубика Γ, определенная уравнением (1.2), является эллиптической кривой состоит в том, что отличен от нуля ее дискриминант Δ_Γ.

Замечание 1.60. Дискриминант кривой (1.2) определяется формулой

$$\Delta_\Gamma = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6, \qquad (1.3)$$

где $d_2 = a_1^2 + 4a_2$, $d_4 = 2a_4 + a_1a_3$, $d_6 = a_3^2 + 4a_6$ и $d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$.

Эллиптические кривые Γ_1 и Γ_2, определенные над полем $\mathcal{K}$ уравнениями Вейерштрасса, *изоморфны*, если существуют такие $\alpha, \beta, \gamma, \delta \in K$ $(\alpha \neq 0)$, что в результате обратимого преобразования

$$\begin{cases} x = \alpha^2v + \beta \\ y = \alpha^3u + \alpha^2\gamma v + \delta \end{cases} \qquad (1.4)$$

эллиптическая кривая Γ_1 отображается на эллиптическую кривую Γ_2.

j-инвариант эллиптической кривой (1.2) определяется формулой

$$j(\Gamma) = (d_2^2 - 24d_4)^3\Delta_\Gamma^{-1} \qquad (1.5)$$

Критерий изоморфизма двух эллиптических кривых состоит в равенстве их j-инвариантов, т.е. эллиптические кривые Γ_1 и Γ_2 изоморфны тогда и только тогда, когда $j(\Gamma_1) = j(\Gamma_2)$.

Замечание 1.61. Для кольца $\mathcal{K} = (K, +, \cdot)$ формула (1.5) имеет смысл тогда и только тогда, когда $\Delta_\Gamma \in K^{inv}$. Если же $\Delta_\Gamma \notin K^{inv}$, но $\Delta_\Gamma \in S_\mathcal{K}$, то формула (1.5) имеет смысл над расширением $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ кольца $\mathcal{K}$.

Стандартные формы, к которым может быть приведено уравнение (1.2) эллиптической кривой Γ имеют следующий вид:

1) если $\mathcal{K}$ – поле характеристики 2, то (1.2) приводится либо к виду

$$y^2 + b_3 y = x^3 + b_4 x + b_6, \tag{1.6}$$

либо к виду

$$y^2 + xy = x^3 + b_2 x^2 + b_6; \tag{1.7}$$

2) если характеристика поля $\mathcal{K}$ не равна 2, то уравнение (1.2) приводится к виду

$$y^2 = x^3 + b_2 x^2 + b_4 x + b_6; \tag{1.8}$$

3) если характеристика поля $\mathcal{K}$ больше чем 3, то уравнение (1.2) приводится к виду

$$y^2 = x^3 + b_4 x + b_6. \tag{1.9}$$

Замечание 1.62. Эллиптические кривые над полем характеристики 2, заданные уравнением (1.6) называются *суперсингулярными*, а уравнением (1.7) – *несуперсингулярными*. Уравнение (1.9) для эллиптических кривых над полем характеристики большей, чем 3, называется *канонической формой Вейерштрасса*. Приведение уравнения (1.2) к стандартной форме осуществляется следующим образом.

Пусть $\mathcal{K}$ – поле характеристики 2. Возможны следующие два случая:

1. Пусть $a_1 = 0$. Обратимое преобразование

$$\begin{cases} x = v + a_2 \\ y = u \end{cases} \tag{1.10}$$

преобразует уравнение $y^2 + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ в эквивалентное уравнение $u^2 + b_3 u = v^3 + b_4 v + b_6$. Заменив v на x, а u на y, получим уравнение (1.6).

2. Пусть $a_1 \neq 0$. Обратимое преобразование

$$\begin{cases} x = a_1^2 v + a_1^{-1} a_3 \\ y = a_1^3 u \end{cases} \tag{1.11}$$

преобразует уравнение (1.2) в эквивалентное уравнение $u^2 + vu = v^3 + c_2 v^2 + c_4 v + c_6$. Это уравнение в результате обратимого преобразования

$$\begin{cases} v = x \\ u = y + c_4 \end{cases} \tag{1.12}$$

преобразуется в эквивалентное уравнение (1.7).

Пусть характеристика поля $\mathcal{K}$ не равна 2. Обратимое преобразование

$$\begin{cases} x = v \\ y = u - 2^{-1} a_1 v - 2^{-1} a_3 \end{cases} \tag{1.13}$$

преобразует уравнение (1.2) в эквивалентное уравнение $u^2 = v^3 + b_2v^2 + b_4v + b_6$. Заменив v на x, а u на y, получим уравнение (1.8).

Пусть характеристика поля $\mathcal{K}$ больше, чем 3. Обратимое преобразование

$$\begin{cases} v = x - 3^{-1}c_2 \\ u = y \end{cases} \tag{1.14}$$

преобразует уравнение $u^2 = v^3 + c_2v^2 + c_4v + c_6$ в эквивалентное уравнение (1.9).

Рассмотрим возможность применения изложенной выше техники в случае, когда $\mathcal{K} = (K, +, \cdot)$ – произвольное ассоциативно-коммутативное кольцо с единицей.

Пусть характеристика кольца $\mathcal{K}$ равна 2.

Преобразование (1.10) обратимое, т.е. уравнение $y^2 + a_3y = x^3 + a_2x^2 + a_4x + a_6$ может быть приведено к стандартной форме (1.6).

Преобразование (1.12) обратимое. Формула (1.11) имеет смысл (а определяемое ею преобразование обратимое) в кольце $\mathcal{K}$ тогда и только тогда, когда $a_1 \in K^{inv}$, т.е. если $a_1 \in K^{inv}$, то уравнение (1.2) может быть приведено к стандартной форме (1.7). Если $a_1 \notin K^{inv}$, но $a_1 \in S_{\mathcal{K}}$, то формула (1.11) имеет смысл (а определяемое ею преобразование обратимое) в кольце $\overline{\mathcal{K}}$, т.е. уравнение (1.2) может быть приведено к стандартной форме (1.7) в кольце $\overline{\mathcal{K}}$.

Пусть характеристика кольца $\mathcal{K}$ не равна 2.

Формула (1.13) имеет смысл (а определяемое ею преобразование обратимое) в кольце $\mathcal{K}$ тогда и только тогда, когда $2 \in K^{inv}$, т.е. если $2 \in K^{inv}$, то уравнение (1.2) может быть приведено к стандартной форме (1.8). Если $2 \notin K^{inv}$, но $2 \in S_{\mathcal{K}}$, то формула (1.13) имеет смысл (а определяемое ею преобразование обратимое) в кольце $\overline{\mathcal{K}}$, т.е. уравнение (1.2) может быть приведено к стандартной форме (1.8) в кольце $\overline{\mathcal{K}}$.

Пусть характеристика кольца больше, чем 3.

Формула (1.14) имеет смысл (а определяемое ею преобразование обратимое) в кольце $\mathcal{K}$ тогда и только тогда, когда $3 \in K^{inv}$, т.е. если $3 \in K^{inv}$, то уравнение (1.2) может быть приведено к стандартной форме (1.9). Если $3 \notin K^{inv}$, но $3 \in S_{\mathcal{K}}$, то формула (1.14) имеет смысл (а определяемое ею преобразование обратимое) в кольце $\overline{\mathcal{K}}$, т.е. уравнение (1.2) может быть приведено к стандартной форме (1.9) в кольце $\overline{\mathcal{K}}$.

Приложения эллиптических кривых основаны на том обстоятельстве, что множество их точек наделяется структурой абелевой группы.

Замечание 1.63. Построение абелевой группы $\mathfrak{G}_\Gamma$ на множестве точек эллиптической кривой Γ, определенной уравнением (1.2), осуществляется следующим образом. Рассмотрим в проективной плоскости $\mathbf{P}$ проективную кривую $G(\xi, \eta, \zeta) = 0$ (G – однородный многочлен, соответствующую эллиптической кривой Γ). Точки эллиптической кривой Γ лежат в аффинной плоскости $\mathbf{A}_3$, а нуль $\mathcal{O}$ группы $\mathfrak{G}_\Gamma$ – бесконечно удаленная точка $(0 : 1 : 0)$. Таким образом, $\mathfrak{G}_\Gamma = (\Gamma \cup \{\mathcal{O}\}, +_{\mathfrak{G}_\Gamma})$, где:

1) $P +_{\mathfrak{G}_\Gamma} \mathcal{O} = \mathcal{O} +_{\mathfrak{G}_\Gamma} P = P$ для всех $P \in \Gamma \cup \{\mathcal{O}\}$;

2) если $P = (x, y) \in \Gamma$, то $-_{\mathfrak{G}_\Gamma} P = (x, -y - a_1x - a_3)$, откуда, в частности вытекает, что $P +_{\mathfrak{G}_\Gamma} P = \mathcal{O}$ для любой точки $P = (x, -2^{-1}(a_1x + a_3)) \in \Gamma$;

3) $P_1 +_{\mathfrak{G}_\Gamma} P_2 +_{\mathfrak{G}_\Gamma} P_3 = \mathcal{O}$ для любых трех точек $P_1, P_2, P_3 \in \Gamma$, лежащих на одной прямой.

Для того, чтобы вывести формулы, по которым в абелевой группе $\mathfrak{G}_\Gamma$ вычисляются координаты суммы двух точек, достаточно учесть то обстоятельство, что в аффинной плоскости $\mathbf{A}_3$ бесконечно удаленной точке $(0:1:0)$ соответствует вертикальная прямая.

Пусть эллиптическая кривая Γ задана уравнением (1.2). Для любых двух таких точек $P_i = (x_i, y_i) \in \Gamma$ $(i = 1, 2)$, что $P_1 \neq -_{\mathfrak{G}_\Gamma} P_2$ точка $P_3 = P_1 +_{\mathfrak{G}_\Gamma} P_2 = (x_3, y_3)$ вычисляется по формулам

$$\begin{cases} x_3 = -x_1 - x_2 + \alpha^2 + \alpha a_1 - a_2 \\ y_3 = -y_1 + \alpha(x_1 - x_3) + a_1 x_3 - a_3 \end{cases}, \tag{1.15}$$

где

$$\alpha = \begin{cases} (3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1)(2y_1 + a_1 x_1 + a_3)^{-1}, & \text{если } x_1 = x_2 \\ (y_1 - y_2)(x_1 - x_2)^{-1}, & \text{если } x_1 \neq x_2 \end{cases}. \tag{1.16}$$

Так как $P_1 \neq -_{\mathfrak{G}_\Gamma} P_2$, то $P_1 = P_2$, если $x_1 = x_2$, т.е. значение α, определяемое 1-й строкой формулы (1.16), используется для вычисления точки $2P_1 = P_1 +_{\mathfrak{G}_\Gamma} P_1$ $(P_1 \in \Gamma, P_1 \neq -_{\mathfrak{G}_\Gamma} P_1)$ эллиптической кривой. Поэтому в абелевой группе $\mathfrak{G}_\Gamma$ для любой точки $P \in \Gamma$ $(P \neq -_{\mathfrak{G}_\Gamma} P)$ вычисление точки $nP = \underbrace{P +_{\mathfrak{G}_\Gamma} \cdots +_{\mathfrak{G}_\Gamma} P}_{n \text{ раз}}$ $(n \in \mathbb{N})$ может быть организовано с помощью стандартного алгоритма «удвоения элемента».

Если эллиптическая кривая приведена к стандартной форме, то формулы (1.15) и (1.16) принимают следующий вид.

Пусть характеристика поля $\mathcal{K}$ равна 2.

Если эллиптическая кривая Γ задана уравнением (1.6), то

$$\begin{cases} x_3 = -x_1 - x_2 + \alpha^2 \\ y_3 = -y_1 + \alpha(x_1 - x_3) - b_3 \end{cases},$$

где

$$\alpha = \begin{cases} b_3^{-1}(x_1^2 + b_4), & \text{если } x_1 = x_2 \\ (y_1 - y_2)(x_1 - x_2)^{-1}, & \text{если } x_1 \neq x_2 \end{cases}.$$

Если эллиптическая кривая Γ задана уравнением (1.7), то

$$\begin{cases} x_3 = -x_1 - x_2 + \alpha^2 + \alpha - b_2 \\ y_3 = -y_1 + \alpha(x_1 - x_3) + x_3 \end{cases},$$

где

$$\alpha = \begin{cases} x_1 - y_1 x_1^{-1}, & \text{если } x_1 = x_2 \\ (y_1 - y_2)(x_1 - x_2)^{-1}, & \text{если } x_1 \neq x_2 \end{cases}.$$

Пусть характеристика поля $\mathcal{K}$ не равна 2, а эллиптическая кривая Γ задана уравнением (1.8). Тогда

$$\begin{cases} x_3 = -x_1 - x_2 + \alpha^2 - b_2 \\ y_3 = -y_1 + \alpha(x_1 - x_3) \end{cases},$$

где

$$\alpha = \begin{cases} (2y_1)^{-1}(3x_1^2 + 2b_2 x_1 + b_4), & \text{если } x_1 = x_2 \\ (y_1 - y_2)(x_1 - x_2)^{-1}, & \text{если } x_1 \neq x_2 \end{cases}.$$

В частности, если характеристика поля $\mathcal{K}$ равна 3, то

$$\alpha = \begin{cases} y_1^{-1}(b_2 x_1 - b_4), & \text{если } x_1 = x_2 \\ (y_1 - y_2)(x_1 - x_2)^{-1}, & \text{если } x_1 \neq x_2 \end{cases}.$$

Пусть характеристика поля $\mathcal{K}$ больше, чем 3, а эллиптическая кривая Γ задана уравнением (1.9). Тогда

$$\begin{cases} x_3 = -x_1 - x_2 + \alpha^2 \\ y_3 = -y_1 + \alpha(x_1 - x_3) \end{cases},$$

где

$$\alpha = \begin{cases} (2y_1)^{-1}(3x_1^2 + b_4), & \text{если } x_1 = x_2 \\ (y_1 - y_2)(x_1 - x_2)^{-1}, & \text{если } x_1 \neq x_2 \end{cases}.$$

Эллиптическая кривая Γ над полем $\mathcal{Z}_p = (\mathbb{Z}_p, \oplus, \circ)$ (p – простое число, $p > 3$) может быть задана уравнением

$$y^2 = x^3 \oplus a \circ x \oplus b, \tag{1.17}$$

где $a, b \in \mathbb{Z}_p$, причем $4 \circ a^3 \oplus 27 \circ b^2 \neq 0$. Множество точек этой эллиптической кривой – множество решений сравнения $y^2 = x^3 + ax + b \,(mod\, p)$. Для фиксированного числа $x \in \mathbb{Z}$ число решений этого сравнения равно:

1) 1, если $x^3 + ax + b = 0$;

2) 0, если $x^3 + ax + b$ – квадратичный невычет по модулю p;

3) 2, если $x^3 + ax + b$ – квадратичный вычет по модулю p.

Используя символ Лежандра, определяемый для числа $c \in \mathbb{Z}$, взаимно простого с числом p (т.е. $(c, p) = 1$) формулой

$$\left(\frac{c}{p}\right) = \begin{cases} 1, & \text{если сравнение } x^2 = c \text{ имеет решения} \\ -1, & \text{если сравнение } x^2 = c \text{ не имеет решений} \end{cases},$$

и, положив по определению $\left(\frac{0}{p}\right) = 0$, получим, что для каждого фиксированного числа $x \in \mathbb{Z}$ число решений сравнения $y^2 = x^3 + ax + b \,(mod\, p)$ равно $1 + \left(\frac{x^3+ax+b}{p}\right)$ Следовательно, для числа точек эллиптической кривой Γ, заданной над полем $\mathcal{Z}_p$ (p – простое число, $p > 3$) уравнением (1.17), истинно равенство

$$|\Gamma| = \sum_{x=0}^{p-1} \left(1 + \left(\frac{x^3 + ax + b}{p}\right)\right) = p + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p}\right),$$

т.е.

$$|\Gamma \cup \{\mathcal{O}\}| = 1 + p + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p}\right). \tag{1.18}$$

Замечание 1.64. Для любого простого числа $p \in \mathbb{N}$ для каждого конечного расширения $\widetilde{\mathcal{Z}_p}$ поля $\mathcal{Z}_p$ существует такое число $k \in \mathbb{N}$, что поле $\widetilde{\mathcal{Z}_p}$ изоморфно полю многочленов от одной переменной с коэффициентами из поля $\mathcal{Z}_p$, степень которых не превосходит числа $k-1$. Такое поле называется *полем Галуа* и обозначается $\mathcal{GF}(p^k)$. Таким образом, $\mathcal{Z}_p = \mathcal{GF}(p)$. Известно, что множество всех конечных полей – это множество полей вида $\mathcal{GF}(p^k)$, где p – простое число, а $k \in \mathbb{N}$.

Рассмотрим эллиптическую кривую $\Gamma/\mathcal{GF}(p^k)$ ($k \in \mathbb{N}$), где эллиптическая кривая Γ задана над полем $\mathcal{GF}(p)$ ($p > 3$) уравнением (1.17). Известно (см., напр., [14]), что порядок абелевой группы $\mathfrak{G}_{\Gamma/\mathcal{GF}(p^k)}$ может быть вычислен по формуле

$$|\Gamma/\mathcal{GF}(p^k) \cup \{\mathcal{O}\}| = p^k + 1 - t_k, \tag{1.19}$$

где число t_k определяется рекуррентным соотношением $t_{j+1} = t_1 t_j - p t_{j-1}$ ($j \in \mathbb{N}$), а $t_0 = 2$ и $t_1 = \sum\limits_{x=0}^{p-1} \left(\frac{x^3+ax+b}{p}\right)$.

Хотя формулы (1.18) и (1.19) дают возможность вычислить порядки абелевых групп $\mathfrak{G}_{\Gamma/\mathcal{GF}(p^k)}$, их использование затруднительно. Кроме того, они не дают возможность оценить порядки указанных абелевых групп. Последний недостаток устраняется следующим образом.

Пусть $\mathcal{F}_q = \mathcal{GF}(p^k)$, где p – простое число ($p \geq 3$), а $k \in \mathbb{N}$. Хассе показал, что для порядка абелевой группы $\mathfrak{G}_\Gamma$ (Γ – эллиптическая кривая над полем $\mathcal{F}_q$) истинна оценка

$$\big|\,|\Gamma \cup \{\mathcal{O}\}| - (q+1)\big| \leq 2\sqrt{q}. \tag{1.20}$$

Замечание 1.65. Вывод оценки (1.20) осуществляется следующим образом.

Дзета-функцией эллиптической кривой Γ, определенной уравнением над полем $\mathcal{F}_q$, называется производящая функция

$$Z(\Gamma; T) = e^{\sum\limits_{l=1}^{\infty} \frac{N_l T^l}{l}}, \tag{1.21}$$

где N_l – порядок абелевой группы $\mathfrak{G}_{\Gamma/\mathcal{F}_{q^l}}$, а $\mathcal{F}_{q^l} = \mathcal{GF}(q^l) (= \mathcal{GF}(p^{kl}))$. Ряд (1.21) равномерно сходится на интервале $-q^{-1} < T < q^{-1}$, причем на этом интервале

$$Z(\Gamma; T) = \frac{1 - tT + qT^2}{(1-T)(1-qT)}, \tag{1.22}$$

где число t определяется равенством $N_1 = q + 1 - t$, а дискриминант числителя неположителен (т.е. уравнение $1 - tT + qT^2 = 0$ имеет комплексно сопряженные корни).

Из (1.21) и (1.22) вытекает, что

$$N_l = q^l + 1 - \omega^l - \overline{\omega}^l \ (l \in \mathbf{N}), \tag{1.23}$$

где ω и $\overline{\omega}$ – комплексно-сопряженные корни уравнения $T^2 - tT + q = 0$. Из (1.23) вытекает, что

$$|N_1 - (q+1)| = |\omega + \overline{\omega}| \le |\omega| + |\overline{\omega}|. \tag{1.24}$$

По теореме Виетта $\omega\overline{\omega} = q$. Следовательно,

$$|\omega| = |\overline{\omega}| = \sqrt{q}. \tag{1.25}$$

Из (1.24) и (1.25) вытекает (1.20).

Из (1.20) вытекает, что для порядка абелевой группы $\mathfrak{G}_\Gamma$, определенной для эллиптической кривой Γ, заданной над полем $\mathcal{GF}(p)$ $(p > 3)$ уравнением (1.17), истинны неравенства

$$p + 1 - 2\sqrt{p} \le |\Gamma \cup \{\mathcal{O}\}| \le p + 1 + 2\sqrt{p}.$$

В [180] показано, что порядки абелевых групп $\mathfrak{G}_\Gamma$ эллиптических кривых Γ, заданных над полем $\mathcal{GF}(p)$ $(p > 3)$ уравнением (1.17), имеют на этом отрезке распределение, близкое к равномерному распределению.

Замечание 1.66. Более точно, в [180] доказано, что существуют такие эффективно вычисляемые константы $c_1, c_2 > 0$, что для каждого простого числа $p > 3$ для любого такого подмножества S целых чисел, что $S \subseteq [p + 1 - 2\sqrt{p},\ p + 1 + 2\sqrt{p}]$ вероятность $\mathtt{p}_S$ того, что случайно выбранная пара $(a, b) \in \mathbb{Z}_p^2$ определяет такую эллиптическую кривую, заданную уравнением (1.17), что $|\Gamma \cup \{\mathcal{O}\}| \subseteq S$, удовлетворяет неравенствам

$$\tfrac{|S|-2}{2\lfloor\sqrt{p}\rfloor+1} c_1 \log^{-1} p \le \mathtt{p}_S \le \tfrac{|S|}{2\lfloor\sqrt{p}\rfloor+1} c_2 \log p (\log\log p)^2.$$

Пусть эллиптическая кривая Γ задана над полем $\mathcal{F}_q$ характеристики большей чем 3 уравнением $y^2 = x^3 + ax + b$, а ν – квадратичный невычет над полем $\mathcal{F}_q$, т.е. уравнение $x^2 = \nu$ не имеет решений в поле $\mathcal{F}_q$. Эллиптическая кривая Γ_1, заданная уравнением $y^2 = x^3 + a_1 x + b_1$, где $a_1 = \nu^2 a$ и $b_1 = \nu^3 b$ называется *скручиванием* эллиптической кривой Γ над полем $\mathcal{F}_q$. Известно, что:

1) $|\Gamma| + |\Gamma_1| = 2q$, и, следовательно, порядки абелевых групп $\mathfrak{G}_\Gamma$ и $\mathfrak{G}_{\Gamma_1}$ эллиптических кривых Γ и Γ_1 связаны соотношением

$$|\Gamma \cup \{\mathcal{O}\}| + |\Gamma_1 \cup \{\mathcal{O}\}| = 2q + 2;$$

2) эллиптические кривые Γ и Γ_1 не изоморфны над полем $\mathcal{F}_q$, но изоморфны над полем $\mathcal{F}_{q^2}$.

Для любого поля $\mathcal{F}_q$ структура абелевой группы $\mathfrak{G}_\Gamma$, определенной для эллиптической кривой Γ, заданной уравнением над полем $\mathcal{F}_q$, имеет следующий вид: либо $\mathfrak{G}_\Gamma$ – циклическая группа, либо $\mathfrak{G}_\Gamma$ изоморфна прямой сумме абелевых групп $\mathcal{Z}_{d_i} = (\mathbf{Z}_{d_i}, \oplus)$ $(i = 1, 2)$, где d_1 – делитель числа $q - 1$, а d_2 – делитель числа d_1.

Замечание 1.67. Прямой суммой групп $\mathcal{G}_1 = (G_1, +_{\mathcal{G}_1})$ и $\mathcal{G}_2 = (G_2, +_{\mathcal{G}_2})$ называется группа $\mathcal{G} = (G_1 \times G_2, +_{\mathcal{G}})$, где $(a_1, b_1) +_{\mathcal{G}} (a_2, b_2) = (a_1 +_{\mathcal{G}_1} a_2, b_1 +_{\mathcal{G}_2} b_2)$ для всех $(a_1, b_1), (a_2, b_2) \in G_1 \times G_2$.

1.3. Конечные автоматы.

Основы теории конечных автоматов были заложены в середине XX века. Эта теории была предназначена для исследование вычислений, которые могут быть осуществлены в реальное время на конечной памяти. Таким образом, конечный автомат, по своей сути, представляет собой формальную модель тех процессов, которые могут быть реализованы на компьютерах с учетом существующих ограничений на объем их памяти. Один из основных классов таких процессов – преобразование информации. Поэтому одно из основных направлений теории конечных автоматов – исследование моделей конечных автоматов с позиции их интерпретации как преобразователей информации.

Всюду в дальнейшем, для краткости, в словосочетании «конечный автомат» слово «конечный» будем опускать.

1.3.1. Модели абстрактных автоматов.

Теория абстрактных автоматов подробно изложена в [15,20,108,173]. Рассмотрим кратко модели таких автоматов.

Абстрактным автоматом называется система $M = (Q, X, Y, \delta, \lambda)$, где Q, X и Y – непустые конечные множество состояний, входной и выходной алфавиты, а $\delta : Q \times X \to Q$ и $\lambda : Q \times X \to Y$ – функции переходов и выходов (в дальнейшем, для краткости, в словосочетании «абстрактный автомат» слово «абстрактный» будем опускать). Если для отображения $\lambda : Q \times X \to Y$ обе переменные $q \in Q$ и $x \in X$ – существенные, то говорят, что M – автомат Мили. Если же для отображения $\lambda : Q \times X \to Y$ переменная $q \in Q$ – существенная, а переменная $x \in X$ – фиктивная, то говорят, что M – автомат Мура.

Замечание 1.68. Если $|X| = 1$, то M *автономный автомат*. Решение многих задач для автономных автоматов существенно отличается от решения этих же задач

в предположении, что $|X| = 2$, которое, в свою очередь, существенно отличается от решения этих же задач в предположении, что $|X| \geq 3$.

Если представляют интерес только переходы состояний, то автомат определяется как система $M = (Q, X, \delta)$ (т.е. выходной алфавит и функция выходов опускаются) и называется *автоматом без выхода*.

Замечание 1.69. Автомат без выхода $M = (Q, X, \delta)$ может быть представлен *графом переходов*, т.е. ориентированным размеченным мультиграфом, возможно с петлями [132], множество вершин которого – множество Q, множество дуг – множество $\{(q, q') \in Q^2 | (\exists x \in X)(\delta(q, x) = q')\}$, а отметка дуги (q, q') – множество $\{x \in X | \delta(q, x) = q'\}$. Автомат $M = (Q, X, Y, \delta, \lambda)$ может быть представлен *автоматным графом*, т.е. ориентированным размеченным мультиграфом, возможно с петлями, множество вершин которого – множество Q, множество дуг – множество $\{(q, q') \in Q^2 | (\exists x \in X)(\delta(q, x) = q')\}$, а отметка дуги (q, q') – множество $\{(x, y) \in X \times Y | \delta(q, x) = q' \& \lambda(q, x) = y\}$. В терминах этих графов естественно формулируются такие свойства автомата, как «быть связным», «быть сильно связным», «иметь данное число компонент связности (либо сильной связности)», «иметь данный диаметр» (т.е. *степень достижимости* [108]).

Автомат $M = (Q, X, Y, \delta, \lambda)$ – *групповой*, если для каждого фиксированного $x \in X$ отображение δ – подстановка на множестве Q.

Для конечного алфавита A положим $A^+ = \bigcup\limits_{i=1}^{\infty} A^i$ и $A^* = \{\Lambda\} \cup A^+$, где Λ – пустое слово. Слово $(a_1, \ldots, a_i) \in A^i$ записывается в виде $a_1 \ldots a_i$. Длина $d(w)$ слова $w \in A^*$ определяется равенствами: $d(\Lambda) = 0$ и $d(w) = i$ для всех $w \in A^i$ $(i \in \mathbb{N})$.

Замечание 1.70. Операция конкатенации слов в алфавите A определяется следующим образом:
1) если $w_j = a_1^{(j)} \ldots a_{i_j}^{(j)} \in A^+$ $(j = 1, 2)$, то $w_1 w_2 = a_1^{(1)} \ldots a_{i_1}^{(1)} a_1^{(2)} \ldots a_{i_2}^{(2)}$;
2) $\Lambda w = w \Lambda = w$ $(w \in A^*)$.

Множество A^+ с определенной на нем операцией конкатенации слов – *свободная полугруппа* над алфавитом A, а множество A^* с определенной на нем операцией конкатенации слов – *свободный моноид* (т.е. полугруппа с единицей) над A.

Функции δ и λ расширяются на множество $Q \times X^*$ следующим образом: для всех $q \in Q$, $u \in X^*$ и $x \in X$

$$\delta(q, \Lambda) = q, \quad \delta(q, ux) = \delta(\delta(q, u), x)),$$

$$\lambda(q, \Lambda) = \Lambda, \quad \lambda(q, ux) = \lambda(q, u)\lambda(\delta(q, u), x).$$

Замечание 1.71. *Степенью различимости* [108] автомата $M = (Q, X, Y, \delta, \lambda)$ называется такое наименьшее число $r \in \mathbb{N}$ (если оно существует), что для любых $q_1, q_2 \in Q$ $(q_1 \neq q_2)$ существует такое входное слово $u \in X^r$, что $\lambda(q_1, u) \neq \lambda(q_1, u)$.

Зафиксируем автоматы $M_i = (Q_i, X, Y, \delta_i, \lambda_i)$ $(i = 1, 2)$. Состояния $q_1 \in Q_1$ и $q_2 \in Q_2$ называются *эквивалентными*, если $\lambda_1(q_1, u) = \lambda_2(q_2, u)$ для любого входного слова $u \in X^+$.

Замечание 1.72. Состояния $q_1, q_2 \in Q$ $(q_1 \neq q_2)$ автомата $M = (Q, X, Y, \delta, \lambda)$ называются *близнецами*, если $\delta(q_1, x) = \delta(q_1, x)$ и $\lambda(q_1, x) = \lambda(q_1, x)$ для всех $x \in X$.

Автоматы $M_i = (Q_i, X, Y, \delta_i, \lambda_i)$ $(i = 1, 2)$ называются *эквивалентными* , если для каждого состояния $q_1 \in Q_1$ существует эквивалентное ему состояние $q_2 \in Q_2$, и для каждого состояния $q_2 \in Q_2$ существует эквивалентное ему состояние $q_1 \in Q_1$.

Говорят, что автомат $M_2 = (Q_2, X_2, Y_2, \delta_2, \lambda_2)$ – *гомоморфный образ* автомата $M_1 = (Q_1, X_1, Y_1, \delta_1, \lambda_1)$, если существует такая тройка сюръекций $\Phi = (\varphi_1, \varphi_2, \varphi_3)$ $(\varphi_1 : Q_1 \to Q_2, \varphi_2 : X_1 \to X_2, \varphi_3 : Y_1 \to Y_2)$, что $\delta_2(\varphi_1(q), \varphi_2(x)) = \varphi_1(\delta_1(q, x))$ и $\lambda_2(\varphi_1(q), \varphi_2(x)) = \varphi_3(\lambda_1(q, x))$ ($\Phi = (\varphi_1, \varphi_2, \varphi_3)$ называется *гомоморфизмом* автомата M_1 на автомат M_2). Если при этом $\Phi = (\varphi_1, \varphi_2, \varphi_3)$ – тройка биекций, то говорят, что автоматы $M_1 = (Q_1, X_1, Y_1, \delta_1, \lambda_1)$ и $M_2 = (Q_2, X_2, Y_2, \delta_2, \lambda_2)$ *изоморфны*, а $\Phi = (\varphi_1, \varphi_2, \varphi_3)$ называется *изоморфизмом* автоматов M_1 и M_2.

Автомат $M = (Q, X, Y, \delta, \lambda)$ называется *приведенным*, если любые два его различных состояния не являются эквивалентными.

Замечание 1.73. Пусть автомат $M = (Q, X, Y, \delta, \lambda)$ не является приведенным. Тогда существует нетривиальное отношение эквивалентности «$\equiv$» на множестве Q, определенное следующим образом: $q_1 \equiv q_2$ $(q_1, q_2 \in Q)$ тогда и только тогда, когда q_1 и q_2 – эквивалентные состояния автомата M. При переходе к фактор-множеству $Q/_{\equiv}$ получается (единственный с точностью до изоморфизма) автомат $M/_{\equiv}$, являющийся гомоморфным образом автомата M.

В [161,176] следующим образом определены *автоматы без потери информации* (БПИ-автоматы). Автомат $M = (Q, X, Y, \delta, \lambda)$ называется:

1) БПИ-автоматом 1-го типа, если для всех $q \in Q$ и $u \in X^+$ пара $(q, \lambda(q, u))$ однозначно идентифицирует входное слово u;

2) БПИ-автоматом 2-го типа, если для всех $q \in Q$ и $u \in X^+$ пара $(\delta(q, u), \lambda(q, u))$ однозначно идентифицирует входное слово u.

В [43] определены и исследованы обобщения этих моделей – БПИ-автоматы порядка n $(n \in \mathbb{N})$. Эти автоматы определяются следующим

образом. Автомат $M = (Q, X, Y, \delta, \lambda)$ называется:

1) БПИ-автоматом 1-го типа порядка n ($n \in \mathbb{N}$), если для всех $q \in Q$, $x \in X$ и всех $u \in X^n$ пара $(q, \lambda(q, xu))$ однозначно идентифицирует входной символ x;

2) БПИ-автоматом 2-го типа порядка n ($n \in \mathbb{N}$), если для всех $q \in Q$, $x \in X$ и всех $u \in X^n$ пара $(q, \lambda(q, ux))$ однозначно идентифицирует входной символ x и состояние $\delta(q, u)$.

Замечание 1.74. При использовании БПИ-автомата в качестве поточного шифра естественно возникает задача построения автомата, осуществляющего расшифрование. В [43] доказано существование таких автоматов для БПИ-автоматов порядка n ($n \in \mathbb{N}$). Однако такой автомат может иметь число состояний, существенно превышающее число состояний исходного БПИ-автомата.

Пусть $Q_0 \subseteq Q$ – непустое подмножество допустимых *начальных* состояний. Упорядоченная пара (M, Q_0) называется *слабоинициальным* автоматом. Если $Q_0 = \{q_0\}$ ($q_0 \in Q$), то упорядоченная пара (M, q_0) называется *инициальным* автоматом. Для автомата $M = (Q, X, Y, \delta, \lambda)$ каждый инициальный автомат (M, q_0) реализует отображение $f_{(M,q_0)} : X^* \to Y^*$, определяемое равенством $f_{(M,q_0)}(u) = \lambda(q, u)$ ($u \in X^*$).

Замечание 1.75. При интерпретации автомата как преобразователя информации, как правило, рассматривают сужение отображения $f_{(M,q_0)} : X^* \to Y^*$ на множество X^+, т.е. отображение $f_{(M,q_0)} : X^+ \to Y^+$.

Отображение $f_{(M,q_0)}$ называется *ограниченно-детерминированной функцией* (о.-д. функцией).

Замечание 1.76. О.-д. функция $f_{(M,q_0)}$ характеризуется следующим образом:

1) $f_{(M,q_0)}$ сохраняет длины слов, т.е. $d(f_{(M,q_0)}(u)) = d(u)$ ($u \in X^*$);

2) $f_{(M,q_0)}$ согласована с начальными отрезками слов, т.е. если $u_1 = uu_3$ и $u_2 = uu_4$ ($u, u_2, u_4 \in X^*$), то слова $f_{(M,q_0)}(u_1)$ и $f_{(M,q_0)}(u_2)$ совпадают на начальных отрезках длины $d(u)$.

Пусть $M = (Q, X, Y, \delta, \lambda)$ – такой автомат, что $X = Y$. Множество $S_{fxd}(M, q_0) = \{u \in X^+ | f_{(M,q_0)}(u) = u\}$ ($q_0 \in Q$) называется множеством *неподвижных точек* отображения $f_{(M,q_0)} : X^+ \to X^+$.

Замечание 1.77. Положим $S^{(i)}_{fxd}(M, q_0) = S_{fxd}(M, q_0) \cap X^i$ ($i \in \mathbb{N}$). Тогда:

1) истинно равенство $S_{fxd}(M, q_0) = \bigcup\limits_{i=1}^{\infty} S^{(i)}_{fxd}(M, q_0)$;

2) истинно равенство $S^{(i_1)}_{fxd}(M, q_0) \cap S^{(i_2)}_{fxd}(M, q_0) = \emptyset$ ($i_1, i_2 \in \mathbb{N}, i_1 \neq i_2$);

3) включение $S^{(i+1)}_{fxd}(M, q_0) \subseteq \{ux | u \in S^{(i)}_{fxd}(M, q_0), x \in X^n\}$ истинно для всех $i \in \mathbb{N}$;

4) если $S^{(i)}_{fxd}(M,q_0)=\emptyset$, то $S^{(i+k)}_{fxd}(M,q_0)=\emptyset$ $(k\in\mathbb{N})$;

5) $S_{fxd}(M,q_0)$ – конечное множество тогда и только тогда, когда существует такое $i\in\mathbb{N}$, что $S^{(i)}_{fxd}(M,q_0)=\emptyset$.

Из установленных свойств вытекает, что достаточно исследовать множества $S^{(1)}_{fxd}(M,q_0)$ $(q_0\in Q)$.

Пусть $M=(Q,X,Y,\delta,\lambda)$ – такой автомат, что инициальный автомат (M,q_0) реализует инъективное отображение. Тогда $f_{(M,q_0)}$ – *поточный шифр*, осуществляющий шифрование сообщений, представленных элементами свободной полугруппы X^+, в шифртексты, представленные элементами свободной полугруппы Y^+. При этом множество неподвижных точек шифра $f_{(M,q_0)}$ – это множество всех сообщений, которые идентичны своим шифртекстам.

Расшифрование сообщений осуществляется посредством любого такого отображения $g:Y^+\to X^+$, что $g|_{Val f_{(M,q_0)}}=f^{-1}_{(M,q_0)}$.

Замечание 1.78. Такая интерпретация допускает следующие два обобщения:

1. Пусть для автомата $M=(Q,X,Y,\delta,\lambda)$ существует такое подмножество состояний Q_0 $(\emptyset\neq Q_0\subseteq Q)$, что $f_{(M,q_0)}$ – инъекция для всех $q_0\in Q_0$. Тогда в качестве поточного шифра может быть выбрано семейство о.-д. функций $\{f_{(M,q_0)}\}_{q_0\in Q_0}$. При этом начальное состояние q_0 – секретный сеансовый ключ.

2. Пусть $\mathcal{M}=\{M_i=(Q^{(i)},X,Y,\delta^{(i)},\lambda^{(i)})\}_{i\in I}$ – такое семейство автоматов, что для каждого $i\in I$ существует такое подмножество состояний $Q^{(i)}_0$ $(\emptyset\neq Q^{(i)}_0\subseteq Q^{(i)})$, что $f_{(M_i,q^{(i)}_0)}$ – инъекция для всех $i\in I$ и $q^{(i)}_0\in Q_0$. Тогда в качестве поточного шифра может быть выбрано семейство о.-д. функций $\{f_{(M_i,q^{(i)}_0)}\}_{i\in I,q^{(i)}_0\in Q^{(i)}_0}$. При этом $i\in I$ – секретный ключ средней длительности, а начальное состояние $q^{(i)}_0$ – секретный сеансовый ключ.

Представление поточного шифра слабоинициальным автоматом (или семейством слабоинициальных автоматов) дает возможность охарактеризовать сложность и точность действий криптоаналитика в терминах сложности и точности решения задач идентификации (параметрической и начального состояния) автомата. В частности, посредством оценки числа прообразов выходной последовательности, которая может быть реализована автоматом [26,55-57,63].

Пусть $M=(Q,X,Y,\delta,\lambda)$ $(|X|=|Y|)$ – такой автомат, что $\{f_{(M,q_0)}\}_{q_0\in Q}$ – семейство биекций (ясно, что M – БПИ-автомат 1-го типа). Такой автомат M будем называть *обратимым*.

Для построения обратного автомата M^{-1} достаточно в автоматном графе автомата M поменять местами входные и выходные символы.

Это означает, что:

1) автоматы M и M^{-1} имеют одно и то же множество состояний Q;

2) при шифровании любого входного слова $u \in X^+$ инициальным автоматом (M, q_0) $(q_0 \in Q)$, а также при расшифровании слова $\lambda(q_0, u)$ автоматом (M^{-1}, q_0) оба автомата «движутся» в пространстве состояний Q по одной и той же «траектории» в одном и том же «направлении».

Функционирование автомата $M = (Q, X, Y, \delta, \lambda)$ осуществляется в дискретном времени и определяется рекуррентными соотношениями. Рассмотрим существующие подходы к выбору таких соотношений.

В [108] предполагается, что:

1) для автомата Мили $M = (Q, X, Y, \delta, \lambda)$

$$\begin{cases} q_{t+1} = \delta(q_t, x_t) \\ y_t = \lambda(q_t, x_t) \end{cases} \quad (t \in \mathbb{N});$$

2) для автомата Мура $M = (Q, X, Y, \delta, \lambda)$

$$\begin{cases} q_{t+1} = \delta(q_t, x_t) \\ y_t = \lambda(q_{t+1}) \end{cases} \quad (t \in \mathbb{N});$$

3) для автомата с задержкой $M = (Q, X, Y, \delta, \lambda)$

$$\begin{cases} q_{t+1} = \delta(q_t, x_t) \\ y_t = \lambda(q_t) \end{cases} \quad (t \in \mathbb{N}).$$

В [20] предполагается, что:

1) для автомата первого рода (автомата Мили) $M = (Q, X, Y, \delta, \lambda)$

$$\begin{cases} q_{t+1} = \delta(q_t, x_{t+1}) \\ y_{t+1} = \lambda(q_t, x_{t+1}) \end{cases} \quad (t \in \mathbb{N});$$

2) для автомата второго рода $M = (Q, X, Y, \delta, \lambda)$

$$\begin{cases} q_{t+1} = \delta(q_t, x_{t+1}) \\ y_{t+1} = \lambda(q_{t+1}, x_{t+1}) \end{cases} \quad (t \in \mathbb{N});$$

3) для автомата Мура $M = (Q, X, Y, \delta, \lambda)$

$$\begin{cases} q_{t+1} = \delta(q_t, x_{t+1}) \\ y_{t+1} = \lambda(q_{t+1}) \end{cases} \quad (t \in \mathbb{N}).$$

Замечание 1.79. При исследовании автоматов в качестве преобразователей информации подход, предложенный в [20], дает возможность избежать ряд сложностей, возникающих при использовании подхода, предложенного в [108]. Поэтому при исследовании функционирования автоматов во времени будет использоваться именно подход, предложенный в [20].

1.3.2. Задачи идентификации автоматов.

Эксперимент с автоматом состоит в подаче на автомат входных слов и анализе соответствующих реакций [15]. Многообразие экспериментов с автоматом определяется:

1) объектом идентификации: состояние заданного автомата, автомат, принадлежащий заданному семейству автоматов и т.д.;

2) числом экземпляров автомата: если используется один экземпляр, то эксперимент называется *простым*, а если не менее двух экземпляров, то эксперимент называется *кратным* (число используемых экземпляров автомата называется *кратностью* кратного эксперимента);

Замечание 1.80. Длина входного слова, подаваемого на автомат в процессе простого эксперимента называется *длиной* простого эксперимента, а максимальная из длин входных слов, подаваемых на автоматы в процессе кратного эксперимента называется *высотой* кратного эксперимента.

3) способом исполнения эксперимента: если при каждой реализации эксперимента подаются одни и те же слова, то эксперимент *безусловный*, а если каждый входной символ, начиная со второго, формируется в зависимости от реакции на предыдущие входные символы, то эксперимент называется *условным* (или *адаптивным*).

Замечание 1.81. Максимальная длина входного слова, подаваемого на автомат в процессе условного эксперимента называется *высотой* условного эксперимента.

Эксперимент, состоящий в идентификации начального состояния заданного слабоинициального автомата (M, Q_0) – *диагностический*.

Замечание 1.82. Выше было отмечено, что при использовании автомата в качестве поточного шифра начальное состояние автомата является секретным сеансовым ключом. Поэтому с позиции криптологии диагностический эксперимент с заданным слабоинициальным автоматом (M, Q_0) представляет собой атаку криптоаналитика на секретный сеансовый ключ. Сложность проведения безусловного диагностического эксперимента с автоматом характеризуется длиной диагностического слова.

Исследованию функции Шеннона $L_k^d(r)$ длины минимального диагностического слова для такого слабоинициального автомата M, что $|Q| = k$ и $|Q_0| = r$ посвящен ряд работ. В [105,106] показано, что истинны верхняя оценка

$$L_k^d(r) \le \begin{cases} (r-1)k^{0.5k(1+\varepsilon)}, & \text{если } r = 2, \dots, k-1 \\ \binom{k}{0.5k}, & \text{если } r = k \end{cases},$$

где $\varepsilon \to \infty$, если $r \to \infty$, а также нижняя оценка

$$L_k^d(r) \ge \begin{cases} \binom{k-1}{r-1}, & \text{если } r = 2, \dots, \lfloor 0.5k \rfloor \\ \binom{k-2}{\lfloor 0.5(k-2) \rfloor}, & \text{если } r = \lfloor 0.5k \rfloor + 1, \dots, k-1 \\ 3^{\lfloor \frac{k}{6} \rfloor}, & \text{если } r = k-1 \end{cases}.$$

В [60,61] показано, что если $r = k$, то истинна асимптотически точная оценка

$$\log_3 L_k^d(k) \sim \frac{k}{6} \ (k \to \infty).$$

Используемые в [60,61,105,106] автоматы имеют входной алфавит, мощность которого фактически совпадает с длиной минимального диагностического слова. В [103] показано, что в случае двух-буквенного входного алфавита при $r = O(\sqrt{k})$ $(k \to \infty)$ истинна нижняя оценка

$$L_k^d(\sqrt{k}) \geq e^{O(\sqrt{k})} \ (k \to \infty).$$

Из этой оценки вытекает, что любой алгоритм поиска минимального диагностического слова, который в единицу времени восстанавливает фрагмент слова, длина которого – полином от «площади» автоматной таблицы, имеет субэкспоненциальную сложность.

В настоящее время выделяют следующие четыре подхода к решению задачи идентификации автомата [8].

Подход 1. На множестве всех автоматов, у которых совпадают входные и выходные алфавиты, строится функция, оценивающая *близость* двух автоматов. Эта функция определяется в терминах расстояние Хемминга между выходными словами одной и той же длины и используется для поиска наилучшего приближения во множестве всех автоматов, число состояний которых не превосходит числа состояний исследуемого автомата.

Замечание 1.83. Успешное применение такого подхода известно только для класса групповых автоматов. Этот класс автоматов является достаточно «узким». Однако он имеет многочисленные приложения, в частности, при решении задач преобразования информации.

Подход 2. Для исследуемого автомата $M = (Q, X, Y, \delta, \lambda)$ строится такой автомат $M' = (Q, X, Y, \delta', \lambda')$ (называемый *статистическим аналогом* автомата M), что для любого состояния $q \in Q$ вероятности события $\delta(q, x) = \delta'(q, x)$ больше, чем $|Q|^{-1}$, а вероятность события $\lambda(q, x) = \lambda'(q, x)$ больше, чем $|Y|^{-1}$.

Подход 3. Предполагается, что задан (как правило, в неяном виде) автомат $M = (Q, X, Y, \delta, \lambda)$, определяющий эталонное поведение. Строится следствие M' автомата M, т.е. автомат, на вход которого поступает входная и выходная последовательность исследуемого дискретного преобразователя D. Автомат M', построенный на основе анализа поведения автомата M на конечном множестве слов, корректирует выход преобразователя D в соответствии с поведением эталона.

Подход 4. На прямом произведении (построенном, как правило, в неявном виде) возможных кандидатов определяется система обобщенных гомоморфизмов, т.е. гомоморфизмов, определенных в терминах отношений (а не отображений). Результат суперпозиции этих гомоморфизмов и является решением задачи.

Замечание 1.84. Если автомат задан системой рекуррентных соотношений над конечной алгебраической системой, то применение этого подхода является, по своей сути, решением задач идентификации соответствующей динамической системы. Отсюда, в частности, вытекает актуальность исследования задач параметрической идентификации и идентификации начального состояния автоматов, представленных системами рекуррентных соотношений над конечными алгебраическими системами.

1.3.3. Семейства автоматов над конечным кольцом.

Зафиксируем конечное кольцо $\mathcal{K} = (K, +, \cdot)$.

Для любых чисел $n_1, n_2, n_3, l \in \mathbb{N}$ при фиксированном множестве параметров $\mathbf{A}$ ($\emptyset \neq \mathbf{A} \subseteq K^l$) любые отображения $\mathbf{f}_1 : K^{n_1} \times K^{n_2} \times \mathbf{A} \to K^{n_1}$ и $\mathbf{f}_2 : K^{n_1} \times K^{n_2} \times \mathbf{A} \to K^{n_3}$ определяют семейство $\mathcal{M}_{\mathbf{f}_1,\mathbf{f}_2,\mathbf{A}} = \{M_{\mathbf{a}}\}_{\mathbf{a}\in\mathbf{A}}$ автоматов Мили

$$M_{\mathbf{a}} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \end{cases} \quad (t \in \mathbb{Z}_+), \tag{1.26}$$

а любые отображения $\mathbf{f}_1 : K^{n_1} \times K^{n_2} \times \mathbf{A} \to K^{n_1}$ и $\mathbf{f}_2 : K^{n_1} \times \mathbf{A} \to K^{n_3}$ – семейство $\mathcal{M}_{\mathbf{f}_1,\mathbf{f}_2,\mathbf{A}} = \{M_{\mathbf{a}}\}_{\mathbf{a}\in\mathbf{A}}$ автоматов Мура

$$M_{\mathbf{a}} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_{t+1}, \mathbf{a}) \end{cases} \quad (t \in \mathbb{Z}_+). \tag{1.27}$$

Замечание 1.85. При использовании автомата в качестве математической модели преобразователя информации часто считают, что $n_1 = n_2 = n_3 = n$.

Пример 1.7. Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо с единицей. Обозначим через M_n ($n \in \mathbb{N}$) множество всех $n \times n$-матриц над кольцом $\mathcal{K}$.

Семейства линейных автоматов (с лагом 1) Мили $\mathcal{M}_{n,1}$ и Мура $\mathcal{M}_{n,2}$ над кольцом $\mathcal{K}$, определяются, соответственно, системами рекуррентных соотношений

$$M_1 : \begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t + B\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C\mathbf{q}_t + D\mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+), \tag{1.28}$$

и

$$M_2 : \begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t + B\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C\mathbf{q}_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+), \tag{1.29}$$

где $A, B, C, D \in \mathsf{M}_n$ ($n \in \mathbb{N}$), а $\mathbf{q}_t, \mathbf{x}_t, \mathbf{y}_t \in K^n$ – вектор-столбцы, представляющие, соответственно, состояние автомата, входной и выходной символ в момент t.

Семейства автоматов $\mathcal{M}_{n,1}$ и $\mathcal{M}_{n,2}$ над кольцом $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (p – простое число, $k \in \mathbb{N}$) исследованы в [64-66]. Обобщения этих исследований для произвольного конечного ассоциативно-коммутативного кольца $\mathcal{K} = (K, +, \cdot)$ с единицей представлены в [80]. Перечислим кратко некоторые из этих результатов.

Обозначим через M_n^{inv} множество всех обратимых матриц $A \in \mathsf{M}_n$ и положим $\mathsf{M}_n^{n-inv} = \mathsf{M}_n \backslash \mathsf{M}_n^{inv}$. Истинны следующие утверждения.

Утверждение 1.1. Если $D \in \mathsf{M}_n^{inv}$, то $M_1 \in \mathcal{M}_{n,1}$ – обратимый автомат, причем обратный автомат имеет вид

$$M_1^{-1} : \begin{cases} \mathbf{q}_{t+1} = A_1\mathbf{q}_t + B_1\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C_1\mathbf{q}_t + D_1\mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+),$$

где $A_1 = A - BD^{-1}C$, $B_1 = BD^{-1}$, $C_1 = -D^{-1}C$ и $D_1 = D^{-1}$.□

Утверждение 1.2. Если $B, C \in \mathsf{M}_n^{inv}$, то $M_2 \in \mathcal{M}_{n,2}$ – обратимый автомат, причем обратный автомат имеет вид

$$M_2^{-1} : \begin{cases} \mathbf{q}_{t+1} = B_1\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C_1\mathbf{q}_t + D_1 + \mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+),$$

где $B_1 = C^{-1}$, $C_1 = -A$ и $D_1 = B^{-1}C^{-1}$.□

Утверждение 1.3. Если $B \in \mathsf{M}_n^{inv}$, то граф переходов автомата $M_i \in \mathcal{M}_{n,i}$ ($i = 1, 2$) – полный граф с петлями.□

Утверждение 1.4. Если $A \in \mathsf{M}_n^{inv}$, то $M_i \in \mathcal{M}_{n,i}$ ($i = 1, 2$) – групповой автомат.□

Утверждение 1.5. Если $C \in \mathsf{M}_n^{inv}$, то $M_1 \in \mathcal{M}_{n,1}$ – приведенный автомат, а его степень различимости равна 1.□

Утверждение 1.6. Если $A, C \in \mathsf{M}_n^{inv}$, то $M_2 \in \mathcal{M}_{n,2}$– приведенный автомат, а его степень различимости равна 1.□

Утверждение 1.7. В автомате $M_1 \in \mathcal{M}_{n,1}$ существуют состояния-близнецы тогда и только тогда, когда система уравнений

$$\begin{cases} A\mathbf{u} = \mathbf{0} \\ C\mathbf{u} = \mathbf{0} \end{cases}$$

имеет ненулевое решение.□

Утверждение 1.8. В автомате $M_2 \in \mathcal{M}_{n,2}$ существуют состояния-близнецы тогда и только тогда, когда уравнение$A\mathbf{u} = \mathbf{0}$ имеет ненулевое решение.□

Эквивалентность автоматов, принадлежащих семейству $\mathcal{M}_{n,i}$ ($i = 1, 2$) характеризуется следующим образом.

Утверждение 1.9. Автоматы $M_1, M_1' \in \mathcal{M}_{n,1}$ эквивалентны тогда и только тогда, когда выполнены следующие условия:

1) $D = D'$;

2) для каждого состояния $\mathbf{q}_0 \in K^n$ автомата M_1 существует такое состояние $\mathbf{q}_0' \in K^n$ автомата M_1' и, наоборот, для каждого состояния $\mathbf{q}_0' \in K^n$ автомата M_1' существует такое состояние $\mathbf{q}_0 \in K^n$ автомата M_1, что:

а) $C'\mathbf{q}_0' - C\mathbf{q}_0 = \mathbf{0}$;

б) $C'(A')^j\mathbf{q}_0' - CA^j\mathbf{q}_0 = \mathbf{0}$ ($j = 1, \ldots, 2|K|^n - 2$);

3) $C'(A')^jB' - CA^jB = O$ $(j = 1, \ldots, 2|K|^n - 3)$, где $O \in \mathsf{M}_n$ – нулевая матрица;

4) $C'B' - CB = O$.$\square$

Следствие 1.1. Состояния $\mathbf{q}_0, \mathbf{q}_0^{'} \in K^n$ автомата $M_1 \in \mathcal{M}_{n,1}$ эквивалентны тогда и только тогда, когда выполнены следующие условия:

1) $C(\mathbf{q}_0^{'} - \mathbf{q}_0) = \mathbf{0}$;

2) $C(A)^j(\mathbf{q}_0^{'} - \mathbf{q}_0) = \mathbf{0}$ $(j = 1, \ldots, |K|^n - 2)$.$\square$

Утверждение 1.10. Автоматы $M_2, M_2^{'} \in \mathcal{M}_{n,2}$ эквивалентны тогда и только тогда, когда выполнены следующие условия:

1) $C'B' - CB = O$;

2) для каждого состояния $\mathbf{q}_0 \in K^n$ автомата M_2 существует такое состояние $\mathbf{q}_0^{'} \in K^n$ автомата $M_2^{'}$ и, наоборот, для каждого состояния $\mathbf{q}_0^{'} \in K^n$ автомата $M_2^{'}$ существует такое состояние $\mathbf{q}_0 \in K^n$ автомата M_2, что $C'(A')^j\mathbf{q}_0^{'} - CA^j\mathbf{q}_0 = \mathbf{0}$ $(j = 1, \ldots, 2|K|^n - 1)$;

3) $C'(A')^jB' - CA^jB = O$ $(j = 1, \ldots, 2|K|^n - 2)$.$\square$

Следствие 1.2. Состояния $\mathbf{q}_0, \mathbf{q}_0^{'} \in K^n$ автомата $M_2 \in \mathcal{M}_{n,2}$ эквивалентны тогда и только тогда, когда $C(A)^j(\mathbf{q}_0^{'} - \mathbf{q}_0) = \mathbf{0}$ $(j = 1, \ldots, |K|^n - 2)$.$\square$

Сложность параметрической идентификации автомата $M_i \in \mathcal{M}_{n,i}$ $(i = 1, 2)$ характеризуется следующим образом.

Утверждение 1.11. Пусть экспериментатор полностью управляет входом и инициализацией автомата $M_1 \in \mathcal{M}_{n,1}$, а также полностью наблюдает выход автомата M_1. Тогда:

1) каждая из матриц C и D идентифицируется единственным образом посредством n-кратного эксперимента высоты 1;

2) если $C \in \mathsf{M}_n^{inv}$, то идентификация каждой из матриц A и B сводится к решению n систем линейных уравнений над кольцом $\mathcal{K}$, построенных в результате n-кратного эксперимента высоты 2.$\square$

Сложность параметрической идентификации автомата $M_1 \in \mathcal{M}_{n,1}$ существенно возрастает, если $C \in \mathsf{M}_n^{n-inv}$. Это обусловлено тем, что идентификация матриц A и B сводится к решению при известных матрицах C и D системы нелинейных уравнений

$$C(A^i\mathbf{q}_0 + \sum_{j=1}^{i-1} A^{i-j}B\mathbf{x}_j + B\mathbf{x}_i) = \mathbf{y}_{i+1} - D\mathbf{x}_{i+1}, \tag{1.30}$$

где $\mathbf{q}_0 \in K^n$ и $\mathbf{x}_1 \ldots \mathbf{x}_{i+1} \in (K^n)^{i+1}$ $(i = 1, \ldots, |K|^n - 1)$.

Для автомата $M_2 \in \mathcal{M}_{n,2}$ решение задачи параметрической идентификации всегда сводится к решению относительно матриц A, B и C системы нелинейных уравнений

$$C(A^{i+1}\mathbf{q}_0 + \sum_{j=0}^{i-1} A^{i-j}B\mathbf{x}_{j+1} + B\mathbf{x}_{i+1}) = \mathbf{y}_{i+1}, \tag{1.31}$$

где $\mathbf{q}_0 \in K^n$ и $\mathbf{x}_1 \ldots \mathbf{x}_{i+1} \in (K^n)^{i+1}$ $(i = 1, \ldots, |K|^n - 1)$.

Сложность идентификации начального состояния автомата $M_i \in \mathcal{M}_{n,i}$ $(i = 1, 2)$ в предположении, что экспериментатору известны параметры модели, но он не может управлять этими параметрами характеризуется следующим образом.

Положив $t = 0$ во 2-м уравнении системы (1.28), получим $C\mathbf{q}_0 = \mathbf{y}_1 - D\mathbf{x}_1$. Если $C \in \mathsf{M}_n^{inv}$, то $\mathbf{q}_0 = C^{-1}(\mathbf{y}_1 - D\mathbf{x}_1)$, т.е. идентификация начального состояния автомата

$M_1 \in \mathcal{M}_{n,1}$ сводится к решению системы линейных уравнений, полученной в результате любого простого эксперимента длины 1. Если же $C \in \mathsf{M}_n^{n-inv}$, то может быть найдено только множество возможных кандидатов на начальное состояние (которое может быть значительно шире класса эквивалентных состояний). Следовательно, идентификация начального состояния автомата $M_1 \in \mathcal{M}_{n,1}$ сводится к решению системы линейных уравнений (1.30) при известных матрицах A, B, C, D.

Положив $t = 0$ во 2-м уравнении системы (1.29), получим $C\mathbf{q}_0 = \mathbf{y}_1 - D\mathbf{x}_1$. Если $A, C \in \mathsf{M}_n^{inv}$, то $\mathbf{q}_0 = A^{-1}C^{-1}(\mathbf{y}_1 - CB\mathbf{x}_1)$, т.е. идентификация начального состояния автомата $M_2 \in \mathcal{M}_{n,2}$ сводится к решению системы линейных уравнений, полученной в результате любого простого эксперимента длины 1. Если же $A \in \mathsf{M}_n^{n-inv}$ или $C \in \mathsf{M}_n^{n-inv}$, то может быть найдено только множество возможных кандидатов на начальное состояние (которое может быть значительно шире класса эквивалентных состояний). Отсюда вытекает, что идентификация начального состояния автомата $M_2 \in \mathcal{M}_{n,2}$ сводится к решению системы линейных уравнений (1.31) при известных матрицах A, B, C.

Множество неподвижных точек, автоматных отображений, реализуемых автоматом $M_i \in \mathcal{M}_{n,i}$ $(i = 1, 2)$ характеризуется следующим образом.

Утверждение 1.12. Для автомата $M \in \mathcal{M}_{n,1} \cup \mathcal{M}_{n,2}$ множество $S_{fxd}^{(t+1)}(M, \mathbf{q}_0)$ $(\mathbf{q}_0 \in K^n, t \in \mathbb{Z}_+)$ состоит из всех таких входных слов $\mathbf{x}_1 \dots \mathbf{x}_{t+1} \in (K^n)^{t+1}$, что:

1) если $M \in \mathcal{M}_{n,1}$, то $(\mathbf{x}_1, \dots, \mathbf{x}_{t+1})$ – решение системы уравнений

$$\begin{cases} (I - D)\mathbf{x}_1 = C\mathbf{q}_0 \\ (I - D)\mathbf{x}_{i+1} = C(A^i\mathbf{q}_0 + \sum\limits_{j=1}^{i-1} A^{i-j}B\mathbf{x}_j + B\mathbf{x}_i) \ (i = 1, \dots, t) \end{cases},$$

где $I \in \mathsf{M}$ – единичная матрица;

2) если $M \in \mathcal{M}_{n,2}$, то $(\mathbf{x}_1, \dots, \mathbf{x}_{t+1})$ – решение системы уравнений

$$\begin{cases} (I - CB)\mathbf{x}_1 = CA\mathbf{q}_0 \\ (I - CB)\mathbf{x}_{i+1} = CA(A^i\mathbf{q}_0 + \sum\limits_{j=1}^{i-1} A^{i-j}B\mathbf{x}_j + B\mathbf{x}_i) \ (i = 1, \dots, t) \end{cases}.\square$$

Следствие 1.3. Если $I - D \in \mathsf{M}_n^{inv}$ для автомата $M_1 \in \mathcal{M}_{n,1}$, то для любого начального состояния $\mathbf{q}_0 \in K^n$ множество $S_{fxd}(M_1, \mathbf{q}_0)$ бесконечное, причем $S_{fxd}^{(t+1)}(M_1, \mathbf{q}_0)$ $(t \in \mathbb{Z}_+)$ – одноэлементное множество, содержащее такое входное слово $\mathbf{x}_1 \dots \mathbf{x}_{t+1} \in (K^n)^{t+1}$, что

$$\begin{cases} \mathbf{x}_1 = (I - D)^{-1}C\mathbf{q}_0 \\ \mathbf{x}_{i+1} = (I - D)^{-1}C(A^i\mathbf{q}_0 + \sum\limits_{j=1}^{i-1} A^{i-j}B\mathbf{x}_j + B\mathbf{x}_i) \ (i = 1, \dots, t) \end{cases}.\square$$

Следствие 1.4. Если $I - CB \in \mathsf{M}_n^{inv}$ для автомата $M_2 \in \mathcal{M}_{n,2}$, то для любого начального состояния $\mathbf{q}_0 \in K^n$ множество $S_{fxd}(M_2, \mathbf{q}_0)$ бесконечное, причем $S_{fxd}^{(t+1)}(M_2, \mathbf{q}_0)$ $(t \in \mathbb{Z}_+)$ – одноэлементное множество, содержащее такое входное слово $\mathbf{x}_1 \dots \mathbf{x}_{t+1} \in (K^n)^{t+1}$, что

$$\begin{cases} \mathbf{x}_1 = (I - CB)^{-1}CA\mathbf{q}_0 \\ \mathbf{x}_{i+1} = (I - CB)^{-1}CA(A^i\mathbf{q}_0 + \sum\limits_{j=1}^{i-1} A^{i-j}B\mathbf{x}_j + B\mathbf{x}_i) \ (i = 1, \dots, t) \end{cases}.\square$$

Следствие 1.5. Для каждого автомата $M \in \mathcal{M}_{n,1} \cup \mathcal{M}_{n,2}$ и начальных состояний $\mathbf{q}_0, \widetilde{\mathbf{q}}_0 \in K^n$ если $\mathbf{x} \in S^{(1)}_{fxd}(M, \mathbf{q}_0)$ и $\widetilde{\mathbf{x}} \in S^{(1)}_{fxd}(M, \widetilde{\mathbf{q}}_0)$, то $\mathbf{x} - \widetilde{\mathbf{x}} \in S^{(1)}_{fxd}(M, \mathbf{q}_0 - \widetilde{\mathbf{q}}_0)$.□

Следствие 1.6. Для каждого начального состояния $\mathbf{q}_0 \in K^n$ каждого автомата $M \in \mathcal{M}_{n,1} \cup \mathcal{M}_{n,2}$ и каждого входного символа $\mathbf{x} \in S^{(1)}_{fxd}(M, \mathbf{q}_0)$ истинно равенство $S^{(1)}_{fxd}(M, \mathbf{q}_0) = \{\mathbf{x} + \widetilde{\mathbf{x}} \mid \widetilde{\mathbf{x}} \in S^{(1)}_{fxd}(M, \mathbf{0})\}$.□

Пример 1.8. Семейства линейных одномерных автоматов с лагом l ($l \in \mathbb{N}$) Мили $\mathcal{M}^{(L)}_{l,1}$ и Мура $\mathcal{M}^{(L)}_{l,2}$ над кольцом $\mathcal{K}$, определяются, соответственно, системами рекуррентных соотношений

$$M_1 : \begin{cases} q_{t+l} = \sum\limits_{i=1}^{l} a_i q_{t+l-i} + b x_{t+1} \\ y_{t+1} = \sum\limits_{i=1}^{l} c_i q_{t+l-i} + d x_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+), \tag{1.32}$$

и

$$M_2 : \begin{cases} q_{t+l} = \sum\limits_{i=1}^{l} a_i q_{t+l-i} + b x_{t+1} \\ y_{t+1} = \sum\limits_{i=1}^{l} c_i q_{t+l+1-i} \end{cases} \quad (t \in \mathbb{Z}_+), \tag{1.33}$$

где $a_i, c_i, b, d \in K$ $(i = 1, \ldots, l)$, $x \in K$ – входная переменная, $y \in K$ – выходная переменная, q – переменная состояния, а $\mathbf{q}_0 = (q_{l-1}, \ldots, q_1, q_0)^T$ – начальное состояние автомата.

Перепишем (1.32) и (1.33) в матричном виде

$$M_1 : \begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t + B\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C\mathbf{q}_t + D\mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+),$$

$$M_2 : \begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t + B\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C\mathbf{q}_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+),$$

где $\mathbf{q}_t = (q_{t+l-1}, \ldots, q_{t+1}, q_t)^T$, $\mathbf{x}_{t+1} = (x_{t+1}, \underbrace{0, \ldots, 0}_{l-1 \text{ раз}})^T$ и $\mathbf{y}_{t+1} = (y_{t+1}, \underbrace{0, \ldots, 0}_{l-1 \text{ раз}})^T$ для всех $t \in \mathbf{Z}_+$, а $A, B, C, D \in \mathsf{M}_l$ – такие матрицы, что

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_{l-1} & a_l \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} c_1 & c_2 & \ldots & c_{l-1} & c_l \\ 0 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & 0 \end{pmatrix},$$

$$B = \begin{pmatrix} b & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix}, \quad D = \begin{pmatrix} d & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix}.$$

Отсюда вытекает, что для автоматов $M_i \in \mathcal{M}_{l,i}^{(L)}$ $(i = 1, 2)$ истинны перечисленные в примере 1.6 результаты, переформулированные заменой числа n числом l с учетом сужения входной и выходной полугрупп автоматов с множества $(K^n)^+$ до множества K^+. Перечислим основные из таких утверждений.

Утверждение 1.13. Если $d \in K^{inv}$, то $M_1 \in \mathcal{M}_{l,1}^{(L)}$ – обратимый автомат, причем обратный автомат имеет вид

$$M_1^{-1} : \begin{cases} q_{t+l} = \sum\limits_{i=1}^{l} \alpha_i q_{t+l-i} + \beta x_{t+1} \\ y_{t+1} = \sum\limits_{i=1}^{l} \gamma_i q_{t+l-i} + \delta x_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+),$$

где $\alpha_i = a_i - bd^{-1}c_i$, $\gamma_i = -d^{-1}c_i$ $(i = 1, \ldots, l)$ а $\beta = bd^{-1}$ и $\delta = d^{-1}$.□

Утверждение 1.14. Если $c_1, b \in K^{inv}$, то $M_2 \in \mathcal{M}_{l,2}^{(L)}$ – обратимый автомат, причем обратный автомат имеет вид

$$M_2^{-1} : \begin{cases} q_{t+l} = \sum\limits_{i=2}^{l} \alpha_i q_{t+l-i} + \beta x_{t+1} \\ y_{t+1} = \sum\limits_{i=1}^{l} \gamma_i q_{t+l-i} + \delta x_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+),$$

где $\alpha_i = c_1^{-1}c_i$ $(i = 2, \ldots, l)$, $\beta = c_1^{-1}$, $\gamma_i = -b^{-1}(c_1^{-1}c_{i+1} - a_i)$ $(i = 1, \ldots, l-1)$, $\gamma_l = -b^{-1}a_l$ и $\delta = b^{-1}c_1^{-1}$.□

Утверждение 1.15. Если $b \in K^{inv}$, то $M_i \in \mathcal{M}_{l,i}^{(L)}$ $(i = 1, 2)$ – сильно связный автомат, причем диаметр его графа переходов равен l.□

Утверждение 1.16. Если $a_l \in K^{inv}$, то $M_i \in \mathcal{M}_{l,i}^{(L)}$ $(i = 1, 2)$ – групповой автомат.□

Мощным источником построения семейств автоматов над конечными кольцами, являющихся математическими моделями поточных шифров, является теория хаотических динамических систем [40]. Общий подход к построению таких семейств автоматов предложен в [66] и, по своей сути, состоит в следующем.

Пусть хаотическая динамическая система представлена уравнением

$$\dot{\mathbf{q}} = \mathbf{g}(\mathbf{q}, \mathbf{a}), \tag{1.34}$$

где $\mathbf{g} : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ $(n, m \in \mathbb{N})$ – заданное алгебраическое отображение, вектор динамических переменных $\mathbf{q} = (q_1, \ldots, q_n)^T \in \mathbb{R}^n$ определяет состояние системы в момент $t \in \mathbb{R}_+$, а $\mathbf{a} = (a_1, \ldots, a_m)^T \in \mathbb{R}^m$ – вектор параметров.

Дискретизируем уравнение (1.34) с шагом $h \in \mathbb{R}_+$, аддитивно внесем внешнее управление $\mathbf{x}_{t+1} = (x_{t+1}^{(1)}, \ldots, x_{t+1}^{(n)})^T \in \mathbb{R}^n$ $(t \in \mathbb{Z}_+)$, интерпретируемое как информационная переменная, а также добавим рекуррентное

соотношение, определяющее преобразование информационной переменной в зависимости от состояния системы. В результате получим систему

$$\begin{cases} \mathbf{q}_{t+1} = \mathbf{g}_1(\mathbf{q}_t, \mathbf{a}_1, h) + \mathbf{g}_2(\mathbf{x}_{t+1}, \mathbf{a}_2) \\ \mathbf{y}_{t+1} = \mathbf{g}_3(\mathbf{q}_t, \mathbf{a}_3) + \mathbf{g}_4(\mathbf{x}_{t+1}, \mathbf{a}_4) \end{cases} \quad (t \in \mathbb{Z}_+) \tag{1.35}$$

или систему

$$\begin{cases} \mathbf{q}_{t+1} = \mathbf{g}_1(\mathbf{q}_t, \mathbf{a}_1, h) + \mathbf{g}_2(\mathbf{x}_{t+1}, \mathbf{a}_2) \\ \mathbf{y}_{t+1} = \mathbf{g}_3(\mathbf{q}_{t+1}, \mathbf{a}_3) \end{cases} \quad (t \in \mathbb{Z}_+), \tag{1.36}$$

где $\mathbf{g}_1 : \mathbb{R}^n \times \mathbb{R}^{m_1} \times \mathbb{R} \to \mathbb{R}^n$ и $\mathbf{g}_i : \mathbb{R}^n \times \mathbb{R}^{m_i} \to \mathbb{R}^n$ $(i = 2, 3, 4)$ – фиксированные отображения, $\mathbf{a}_i = (a_1^{(i)}, \ldots, a_{m_i}^{(i)})^T \in \mathbb{R}^{m_i}$ $(i = 1, \ldots, 4)$ – векторы параметров, а $h \in \mathbb{R}$ – параметр.

Замечание 1.86. Для хаотического отображения $\mathbf{q}_{t+1} = \mathbf{g}_1(\mathbf{q}_t, \mathbf{a})$ $(t \in \mathbb{Z}_+)$ непосредственно строится система

$$\begin{cases} \mathbf{q}_{t+1} = \mathbf{g}_1(\mathbf{q}_t, \mathbf{a}_1) + \mathbf{g}_2(\mathbf{x}_{t+1}, \mathbf{a}_2) \\ \mathbf{y}_{t+1} = \mathbf{g}_3(\mathbf{q}_t, \mathbf{a}_3) + \mathbf{g}_4(\mathbf{x}_{t+1}, \mathbf{a}_4) \end{cases} \quad (t \in \mathbb{Z}_+) \tag{1.37}$$

или система

$$\begin{cases} \mathbf{q}_{t+1} = \mathbf{g}_1(\mathbf{q}_t, \mathbf{a}_1) + \mathbf{g}_2(\mathbf{x}_{t+1}, \mathbf{a}_2) \\ \mathbf{y}_{t+1} = \mathbf{g}_3(\mathbf{q}_{t+1}, \mathbf{a}_3) \end{cases} \quad (t \in \mathbb{Z}_+). \tag{1.38}$$

Добавив в (1.35) и (1.36) параметр h к компонентам вектора $\mathbf{a}_1$, мы тем самым преобразуем (1.35) в (1.37), а (1.36) в (1.38).

Зафиксируем конечное кольцо $\mathcal{K} = (K, +, \cdot)$. Заменив отображения $\mathbf{g}_i$ $(i = 1, 2, 3, 4)$ их аналогами $\mathbf{f}_i$ над кольцом $\mathcal{K}$, и считая, что все переменные и параметры принадлежат множеству K, преобразуем (1.37) в семейство автоматов Мили над кольцом $\mathcal{K}$

$$\begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{a}_1) + \mathbf{f}_2(\mathbf{x}_{t+1}, \mathbf{a}_2) \\ \mathbf{y}_{t+1} = \mathbf{f}_3(\mathbf{q}_t, \mathbf{a}_3) + \mathbf{f}_4(\mathbf{x}_{t+1}, \mathbf{a}_4) \end{cases} \quad (t \in \mathbb{Z}_+), \tag{1.39}$$

а (1.38) – в семейство автоматов Мура над кольцом $\mathcal{K}$

$$\begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{a}_1) + \mathbf{f}_2(\mathbf{x}_{t+1}, \mathbf{a}_2) \\ \mathbf{y}_{t+1} = \mathbf{f}_3(\mathbf{q}_{t+1}, \mathbf{a}_3) \end{cases} \quad (t \in \mathbb{Z}_+). \tag{1.40}$$

Замечание 1.87. Семейства обратимых автоматов (1.39) и (1.40) могут быть использованы в качестве математических моделей поточных шифров. Именно это обстоятельство обосновывает актуальность исследования для семейств (1.39) и (1.40)

задачи параметрической идентификации автомата, принадлежащего заданному семейству, задачи идентификации начального состояния заданного автомата, задачи анализа множеств неподвижных точек о.-д. функций, реализуемых автоматами, принадлежащими заданному семейству, а также задачи построения и анализа семейств обратимых автоматов.

Пример 1.9. В [120] исследованы симметрические хаотические динамические системы Guckenheimer and Holmes cycle и free-running system. Эти системы имеют следующие особенности.

Во-первых, каждая из них имеет нетривиальную группу симметрий (как известно, теория симметрий [24] является мощным аппаратом анализа динамических систем).

Во-вторых, изменение динамических переменных Guckenheimer and Holmes cycle представлено многочленами третьей степени, а изменение динамических переменных free-running system осуществляется с помощью показательной функции (как известно, дискретное логарифмирование (т.е. операция обратная показательной функции) – одна из базовых конструкций современной криптографии).

Динамическая система Guckenheimer and Holmes cycle имеет следующий вид

$$\begin{cases} \dot{x} = x(l + ax^2 + by^2 + cz^2) \\ \dot{y} = y(l + ay^2 + bz^2 + cx^2) \\ \dot{z} = z(l + az^2 + bx^2 + cy^2) \end{cases}, \tag{1.41}$$

где $l, a, b, c \in \mathbb{R}\backslash\{0\}$ – параметры. Одни из наиболее простых семейств $\mathcal{M}_1^{(GH)}$ автоматов Мили и семейств $\mathcal{M}_2^{(GH)}$ и Мура над конечным ассоциативно-коммутативным кольцом $\mathcal{K} = (K, +, \cdot)$ с единицей, построенные для динамической системы (1.41), имеют, соответственно, вид

$$M_1 : \begin{cases} q_{t+1}^{(1)} = q_t^{(1)}(l + a(q_t^{(1)})^2 + b(q_t^{(2)})^2 + c(q_t^{(3)})^2) + \alpha_1 x_{t+1} \\ q_{t+1}^{(2)} = q_t^{(2)}(l + a(q_t^{(2)})^2 + b(q_t^{(3)})^2 + c(q_t^{(1)})^2) + \alpha_2 x_{t+1} \\ q_{t+1}^{(3)} = q_t^{(3)}(l + a(q_t^{(3)})^2 + b(q_t^{(1)})^2 + c(q_t^{(2)})^2) + \alpha_3 x_{t+1} \\ y_{t+1}^{(i)} = \beta_1^{(i)} q_t^{(1)} + \beta_2^{(i)} q_t^{(2)} + \beta_3^{(i)} q_t^{(3)} + \gamma_i x_{t+1} \ (i = 1, 2, 3) \end{cases} \quad (t \in \mathbb{Z}_+) \tag{1.42}$$

и

$$M_2 : \begin{cases} q_{t+1}^{(1)} = q_t^{(1)}(l + a(q_t^{(1)})^2 + b(q_t^{(2)})^2 + c(q_t^{(3)})^2) + \alpha_1 x_{t+1} \\ q_{t+1}^{(2)} = q_t^{(2)}(l + a(q_t^{(2)})^2 + b(q_t^{(3)})^2 + c(q_t^{(1)})^2) + \alpha_2 x_{t+1} \\ q_{t+1}^{(3)} = q_t^{(3)}(l + a(q_t^{(3)})^2 + b(q_t^{(1)})^2 + c(q_t^{(2)})^2) + \alpha_3 x_{t+1} \\ y_{t+1}^{(i)} = \beta_1^{(i)} q_{t+1}^{(1)} + \beta_2^{(i)} q_{t+1}^{(2)} + \beta_3^{(i)} q_{t+1}^{(3)} \ (i = 1, 2, 3) \end{cases} \quad (t \in \mathbb{Z}_+), \tag{1.43}$$

где $l, a, b, c \in K\backslash\{0\}$, $\alpha_i, \beta_j^{(i)}, \gamma_i \in K$ $(i, j = 1, 2, 3)$ – параметры, $x \in K$ – входная переменная, $y^{(i)} \in K$ $(i = 1, 2, 3)$ – выходные переменные, $q^{(i)} \in K$ $(i = 1, 2, 3)$ – переменные состояния автомата. Несложно доказать, что истинны следующие утверждения.

Утверждение 1.17. Если $a = b = c$ и $\alpha_1 = \alpha_2 = \alpha_3$, то автомат $M_i \in \mathcal{M}_i^{(GH)}$ $(i = 1, 2)$ не является сильно связным.□

Утверждение 1.18. Если $\gamma_1, \gamma_2, \gamma_3 \in K^{inv}$, то $M_1 \in \mathcal{M}_1^{(GH)}$ – обратимый автомат.□

Утверждение 1.19. Если $\alpha_1, \alpha_2, \alpha_3 \in K^{inv}$ и

$$B = \begin{pmatrix} \beta_1^{(1)} & \beta_2^{(1)} & \beta_3^{(1)} \\ \beta_1^{(2)} & \beta_2^{(2)} & \beta_3^{(2)} \\ \beta_1^{(3)} & \beta_2^{(3)} & \beta_3^{(3)} \end{pmatrix} \in \mathsf{M}_3^{inv},$$

то $M_2 \in \mathcal{M}_2^{(GH)}$ – обратимый автомат.□

Замечание 1.88. В [66] исследовано семейство автоматов $\mathcal{M}_2^{(GH)}$ над кольцом $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (p – простое число, $k \in \mathbb{N}$) в предположении, что $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}_{p^k}^{inv}$, $\beta_1^{(1)} = \beta_2^{(2)} = \beta_3^{(3)} = 1$ и $\beta_j^{(i)} = 0$ $(i, j = 1, 2, 3; i \neq j)$.

Динамическая система free running system имеет следующий вид

$$\begin{cases} x_{t+1} = f(x_t)e^{-\gamma z_n} \\ y_{t+1} = f(y_t)e^{-\gamma x_n} \quad (t \in \mathbb{Z}_+), \\ z_{t+1} = f(z_t)e^{-\gamma y_n} \end{cases} \tag{1.44}$$

где $\gamma > 0$, а $f(x) = ax(1-x)$ – логистическое отображение с параметром $a \in (0; 4)$. Одни из наиболее простых семейств $\mathcal{M}_1^{(FR)}$ автоматов Мили и семейств $\mathcal{M}_2^{(FR)}$ и Мура над конечным ассоциативно-коммутативным кольцом $\mathcal{K} = (K, +, \cdot)$ с единицей, построенные для хаотического отображения (1.44), имеют, соответственно, вид

$$M_1 : \begin{cases} q_{t+1}^{(1)} = f(q_t^{(1)})\zeta^{q_t^{(3)}} + \alpha_1 x_{t+1} \\ q_{t+1}^{(2)} = f(q_t^{(2)})\zeta^{q_t^{(1)}} + \alpha_2 x_{t+1} \\ q_{t+1}^{(3)} = f(q_t^{(3)})\zeta^{q_t^{(2)}} + \alpha_3 x_{t+1} \\ y_{t+1}^{(i)} = \beta_1^{(i)} q_t^{(1)} + \beta_2^{(i)} q_t^{(2)} + \beta_3^{(i)} q_t^{(3)} + \gamma_i x_{t+1} \ (i = 1, 2, 3) \end{cases} (t \in \mathbb{Z}_+), \tag{1.45}$$

и

$$M_2 : \begin{cases} q_{t+1}^{(1)} = f(q_t^{(1)})\zeta^{q_t^{(3)}} + \alpha_1 x_{t+1} \\ q_{t+1}^{(2)} = f(q_t^{(2)})\zeta^{q_t^{(1)}} + \alpha_2 x_{t+1} \\ q_{t+1}^{(3)} = f(q_t^{(3)})\zeta^{q_t^{(2)}} + \alpha_3 x_{t+1} \\ y_{t+1}^{(i)} = \beta_1^{(i)} q_{t+1}^{(1)} + \beta_2^{(i)} q_{t+1}^{(2)} + \beta_3^{(i)} q_{t+1}^{(3)} \ (i = 1, 2, 3) \end{cases} (t \in \mathbb{Z}_+), \tag{1.46}$$

где $a \in K \backslash \{0\}$, $\zeta \in K^{inv}$, $\alpha_i, \beta_j^{(i)}, \gamma_i \in K$ $(i, j = 1, 2, 3)$ – параметры, $x \in K$ – входная переменная, $y^{(i)} \in K$ $(i = 1, 2, 3)$ – выходные переменные, $q^{(i)} \in K$ $(i = 1, 2, 3)$ – переменные состояния автомата. Истинны следующие утверждения.

Утверждение 1.20. Если $\alpha_1 = \alpha_2 = \alpha_3$, то автомат $M_i \in \mathcal{M}_i^{(FR)}$ $(i = 1, 2)$ не является сильно связным.□

Утверждение 1.21. Если $\gamma_1, \gamma_2, \gamma_3 \in K^{inv}$, то $M_1 \in \mathcal{M}_1^{(FR)}$ – обратимый автомат.□

Утверждение 1.22. Если $\alpha_1, \alpha_2, \alpha_3 \in K^{inv}$ и

$$B = \begin{pmatrix} \beta_1^{(1)} & \beta_2^{(1)} & \beta_3^{(1)} \\ \beta_1^{(2)} & \beta_2^{(2)} & \beta_3^{(2)} \\ \beta_1^{(3)} & \beta_2^{(3)} & \beta_3^{(3)} \end{pmatrix} \in \mathsf{M}_3^{inv},$$

то $M_2 \in \mathcal{M}_2^{(FR)}$ – обратимый автомат.□

Замечание 1.89. В [66,71] исследовано семейство автоматов $\mathcal{M}_2^{(FR)}$ над кольцом $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (p – простое число, $k \in \mathbb{N}$) в предположении, что $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}_{p^k}^{inv}$, $\beta_1^{(1)} = \beta_2^{(2)} = \beta_3^{(3)} = 1$ и $\beta_j^{(i)} = 0$ $(i, j = 1, 2, 3; i \neq j)$.

Пример 1.10. В рамки рекуррентного соотношение

$$q_{t+2} = a_1 + a_2 q_{t+1}^2 + a_3 q_t \ (t \in \mathbb{Z}_+) \tag{1.47}$$

укладывается ряд хаотических отображений, в том числе такие модельные хаотические отображения, как отображение Эно (см., напр., [40]). Одни из наиболее простых семейств $\mathcal{M}_1$ автоматов Мили и семейств $\mathcal{M}_2$ автоматов Мура над конечным ассоциативно-коммутативным кольцом с единицей $\mathcal{K} = (K, +, \cdot)$, построенные для отображения (1.47), имеют, соответственно, вид

$$M_1 : \begin{cases} q_{t+2} = a_1 + a_2 q_{t+1}^2 + a_3 q_t + a_4 x_{t+1} \\ y_{t+1} = b_1 q_{t+1} + b_2 q_t + b_3 x_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+) \tag{1.48}$$

и

$$M_2 : \begin{cases} q_{t+2} = a_1 + a_2 q_{t+1}^2 + a_3 q_t + a_4 x_{t+1} \\ y_{t+1} = b_1 q_{t+2} + b_2 q_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+), \tag{1.49}$$

где $a_i \in K$ $(i = 1, 2, 3, 4)$ и $b_i \in K$ $(i = 1, 2, 3)$ – параметры, $x \in K$ – входная переменная, $y \in K$ – выходная переменная, $q \in K$ – переменная состояния автомата, а $\mathbf{q}_0 = (q_1, q_0)^T$ – начальное состояние автомата. Несложно доказать, что истинны следующие утверждения.

Утверждение 1.23. Если $b_3 \in K^{inv}$, то $M_1 \in \mathcal{M}_1$ – обратимый автомат.□

Утверждение 1.24. Если $a_4, b_1 \in K^{inv}$, то $M_2 \in \mathcal{M}_2$ – обратимый автомат.□

Замечание 1.90. В [70,80,82] исследовано семейство автоматов $\mathcal{M}_2$ в предположении, что $b_2 = 0$.

1.4. Проверка выполнимости формул разрешимых теорий.

Применение информационных технологий практически во всех сферах деятельности человечества привело к необходимости автоматизации процессов управления, проектирования и сопровождения реальных (в том числе, информационных) систем, особенно систем с критической областью применения.

Широкий класс реальных задач (организация потоков информации в компьютерных сетях, формальная верификация систем, представление и обработка знаний, планирование, исследование операций, тестирование дискретных устройств и т.д.), а также задач дискретной математики (основанных на использовании теоретико-множественных, теоретико-числовых, логических, теоретико-графовых и сетевых моделей) имеет

следующее общее свойство: решение задачи естественно сводится к проверке выполнимости формулы некоторой разрешимой теории 1-го порядка (см., напр., [141,155,177,181,196,215,216,218,221,222]). Именно это свойство и лежит в основе разработки средств автоматизированного решения (т.е. *решателей*) всех таких задач.

Рассмотрим современное состояние решения проблемы проверки выполнимости формул разрешимых теорий.

1.4.1. Выполнимость формул математической логики.

Выполнимость формулы математической логики означает существование *интерпретации* (говорят также, *модели*), в которой она истинна (см., напр., [39,138]).

Проверку выполнимости формулы F исчисления высказываний можно осуществить с помощью следующей рекурсивной схемы.

Рассмотрим двоичное размеченное ориентированное ранжированное дерево $\mathfrak{D}_F$, построенное в соответствии со следующими правилами (это дерево называется *семантическим деревом* формулы F):

1. Корень дерева $\mathfrak{D}_F$ отмечен формулой F.

2. Осуществляется выбор висячей вершины v дерева $\mathfrak{D}_F$ и переменной x, входящей в формулу F_v, являющуюся отметкой вершины v.

3. Из вершины v выходят две дуги, ведущие в вершины v_l и v_r следующего уровня. Дуга, ведущая в вершину v_l (соответственно, в вершину v_r), имеет отметку $x \mapsto \top$ (соответственно, $x \mapsto \bot$).

Замечание 1.91. Символы $\top$ и $\bot$ обозначают, соответственно, логические значения `true` и `false`.

Отметка вершины v_l (соответственно, вершины v_r) – формула, полученная из F_v подстановкой $x \mapsto \top$ (соответственно, $x \mapsto \bot$), и упрощенная на основе тождеств исчисления высказываний.

Построение дерева $\mathfrak{D}_F$ осуществляется до тех пор, пока либо не появится вершина с отметкой $\top$, либо каждая висячая вершина имеет отметку $\bot$. В 1-м случае F – выполнимая формула, а во 2-м случае невыполнимая (т.е. тождественно ложная во всех интерпретациях) формула.

Замечание 1.92. Семантическое дерево, в отличие от таблиц истинности, осуществляет, вообще говоря, частичное присвоение истинностных значений булевым переменным с целью поиска одной (безразлично, какой именно) интерпретации, в которой выполнима исследуемая формула исчисления высказываний.

Рассмотренная выше схема представляет собой класс рекурсивных алгоритмов, каждый из которых определяется правилами выбора раскрываемой вершины v и переменной x, входящей в формулу F_v. Известно, что (см., напр., [25]) проверка выполнимости формул исчисления высказываний – NP-полная задача.

Значительные усилия были затрачены на разработку методов, позволяющих упростить решение этой задачи на практике. Один из классов таких методов основан на применении *правила резолюции*: следствием дизъюнктов $A \vee B$ и $\overline{A} \vee C$ является дизъюнкт $B \vee C$ (этот дизъюнкт называется *резольвентой*). Известно, что формула невыполнима тогда и только тогда, когда конечным числом применений правила резолюции из нее выводится значение $\perp$.

Комбинация построения семантического дерева и применения правила резолюции лежит в основе DPLL-процедуры [149,150] (DPLL – сокращение от Davis-Putnam-Logemann-Loveland).

Для исчисления предикатов ситуация иная. Известно, что не существует алгоритм проверки выполнимости формул исчисления предикатов. Однако существуют алгоритмы, которые для любой выполнимой формулы исчисления предикатов за конечное число шагов устанавливает ее выполнимость (т.е., строго говоря, исчисление предикатов является *полу-разрешимой теорией*). Идея их построения состоит в следующем.

Замкнутая (т.е. не содержащая свободных переменных) формула F_1 преобразуется в эквивалентную формулу F_2, не содержащую логические связки, отличные от $\vee$, $\wedge$ и $^-$.

Формула F_2 приводится к *предваренной нормальной форме*

$$F_4 = (Q_1 x_1) \dots (Q_n x_n) F_3,$$

где $Q_1, \dots, Q_n$ – кванторы, а F_3 – бескванторная формула.

Элиминацией кванторов существования формула F_4 приводится к *сколемовской нормальной форме*

$$F_6 = (\forall y_1) \dots (\forall y_m) F_5,$$

где F_5 – бескванторная формула.

В силу теоремы Эрбрана не выполнимость формулы F_6 (т.е. используется метод доказательства «от противного») эквивалентна существованию конечного невыполнимого подмножества множества формул, полученных подстановкой в F_5 всевозможных термов, которые можно построить при помощи предметных констант и функциональных символов, встречающихся в F_5.

Замечание 1.93. Таким образом, проверка не выполнимости формулы F_6, по своей сути, сводится к проверке не выполнимости конечного множества формул исчисления высказываний.

Задача, представленная формулой математической логики, может быть решена применением SAT-решателя, т.е. программной системы, предназначенной для проверки выполнимости формул математической логики.

Если задача представлена формулой разрешимой теории 1-го порядка $\mathcal{T}$, то говорят о *выполнимости по модулю этой теории*. В этом случае используется обозначение $SMT(\mathcal{T})$ (SMT – сокращение фразы «Satisfiability Modulo Theory»). Для решения таких задач применяется $\mathcal{T}$-решатель, т.е. программная система, осуществляющих анализ совместности ограничений, представленных атомами теории $\mathcal{T}$. Основы построения $\mathcal{T}$-решателей заложены в [118,181,187,188,195,204-206].

В течение последнего десятилетия значительные усилия были направлены на исследование методов интеграции SAT-решателей и $\mathcal{T}$-решателей, что дает возможность «кодировать» задачу формулой математической логики и применить для анализа выполнимости последней SAT-решатель. При этом $\mathcal{T}$-решатели применяются только для проверки совместности (в теории $\mathcal{T}$) множеств литералов, кодирующих ограничения, представленные атомами теории $\mathcal{T}$. Такой подход (он получил имя «ленивый подход» – lazy approach) дает возможность существенно расширить класс решаемых задач. В настоящее время «ленивый подход» считается наиболее перспективным при разработке средств автоматизированного решения задач (см., напр., [151,153,164,193,194,198-202]).

Рассмотрим современное состояние исследования проблемы $SMT(\mathcal{T})$ на основе «ленивого подхода».

1.4.2. SAT-решатели.

Успехи в разработке методов повышения эффективности анализа выполнимости формул исчисления высказываний [123,143,174,184,185] привели к появлению ряда достаточно мощных SAT-решателей, основанных на использовании DPLL-процедуры (см., напр., [157,168,186,225,227]). Такие SAT-решатели, для краткости, называют DPLL.

Существующие DPLL можно разбить на следующие два класса:

1. DPLL, основанные на методе ветвей и границ [58] (они получили имя look-ahead DPLL [143]). В этих DPLL с каждой вершиной v дере-

ва ассоциируется множество S_v литералов, которым еще не присвоено истинностное значение.

Замечание 1.94. *Литералом* называют переменную или ее отрицание.

Каждый раз раскрывается вершина v, для которой множество S_v содержит «наиболее перспективный» литерал l. Раскрытие вершины состоит в присвоении истинностного значения $l \mapsto \top$, т.е. в построении вершины v' следующего уровня, в которую из v идет дуга с отметкой $l \mapsto \top$, и в ассоциировании с вершиной v' множества $S_{v'} = S_v \setminus \{l, \bar{l}\}$.

2. DPLL, управляющие конфликтами (они получили имя conflict driven DPLL [184,185]). В этих DPLL реализован поиск с возвращением [58], основанный на анализе и устранении конфликтов, возникающих при каждом раскрытии вершины дерева, приводящем к невыполнимости анализируемой формулы.

Замечание 1.95. В настоящее время не известны успешные применения DPLL, основанных на методе ветвей и границ, при исследований проблемы $SMT(\mathcal{T})$ на основе «ленивого подхода».

Тем не менее, для проверки выполнимости формул исчисления высказываний DPLL, основанные на методе ветвей и границ, более эффективны (по затрачиваемому времени), чем DPLL, управляющие конфликтами.

Таким образом, затраты, связанные с управлением конфликтами, являются, по-видимому, той «ценой», которую приходится платить за возможность применения «ленивого подхода» к исследованию проблемы $SMT(\mathcal{T})$.

Охарактеризуем структуру DPLL, управляющих конфликтами.

С анализируемой формулой исчисления высказываний, представленной в виде КНФ, ассоциируется упорядоченная пара (φ, μ), где φ – множество дизъюнктов, входящих в КНФ, а μ – множество значений истинности, присвоенных переменным (первоначально, $\mu = \emptyset$). DPLL, управляющая конфликтами, состоит из следующих трех процедур.

1. *Препроцессорная обработка данных.* Эта процедура предназначена для упрощения анализируемого множества дизъюнктов φ. Основана на комбинации следующих методов [122,139,158]:

а) для каждой переменной x, встречающейся в множестве φ либо только без отрицания, либо только с отрицанием из множества φ удаляются все дизъюнкты, содержащие эту переменную (так как эти дизъюнкты являются выполнимыми), а в множество μ добавляется соответствующее истинностное значение этой переменной (а именно, $x \mapsto \top$, если переменная x входит в φ без отрицания, и $x \mapsto \bot$, если переменная x входит в φ с отрицанием);

б) для каждого дизъюнкта, принадлежащего множеству φ, удаляются все дизъюнкты, частью которых является этот дизъюнкт;

в) пары дизъюнктов, принадлежащих множеству φ, к которым применимо правило резолюции, заменяются их резольвентами, а истинностные значение переменных, по которым осуществляется свертка, добавляются в множество μ.

Замечание 1.96. После препроцессорной обработки данных исходная пара (φ, μ) преобразуется в экви-выполнимую пару (φ', μ'), т.е. формула $\varphi \wedge \mu$ выполнима тогда и только тогда, когда выполнима формула $\varphi' \wedge \mu'$.

2. *Ветвление*. Эта процедура реализует *прямой ход* поиска с возвращением и предназначена для присвоения истинностных значений литералам, встречающихся в обрабатываемом множестве дизъюнктов. Процедура основана на использовании того или иного *эвристического метода* (или комбинации эвристических методов). На практике используются следующие эвристические методы:

а) выбор литерала, наиболее часто встречающегося в дизъюнктах минимальной длины, и присвоение этому литералу истинностного значения $\top$ [174,177];

б) выбор литерала, приводящего к минимальному (по мощности) анализируемому множеству дизъюнктов, и присвоение этому литералу истинностного значения $\top$ [144];

в) выбор литерала в соответствии со списком приоритетов переменных, и присвоение этому литералу истинностного значения $\top$ [171,126];

Замечание 1.97. Список приоритетов переменных составляется с участием пользователя при кодировании реальной задачи формулой математической логики, исходя из значения этих переменных для решаемой задачи.

г) выбор литерала из списка литералов, входящих в дизъюнкты, рассмотренные на предыдущем шаге, в соответствии со значением той или иной меры, оценивающей вклад литерала в построение решения задачи, и присвоение этому литералу истинностного значения $\top$ [157,168,186];

д) выбор литералов на основе дедукции [145,158,186], т.е. на итеративном анализе, направленном на выделение множества ψ эквивалентных (для выполнимости анализируемой формулы) под-дизъюнктов, подстановке в обрабатываемое множество дизъюнктов новой пропозициональной переменной вместо элементов множества ψ, и присвоение этой переменной истинностного значения $\top$.

3. *Анализ конфликтов.* Эта процедура реализует *обратный ход* (backtracking) поиска с возвращением, предназначена для модификации множества значений истинности, присвоенных переменным, и состоит в следующем [123,182,226,227].

Представим текущее состояние поиска с возвращением (см., напр., [58]) в виде пути

$$\overset{v_0}{\emptyset} \to \overset{v_1}{(l_1, D_1)} \to \overset{v_2}{(l_2, D_2)} \to \cdots \to \overset{v_n}{(l_n, D_n)}, \tag{1.50}$$

идущего из корня v_0 дерева поиска в вершину v_n, где l_i $(i = 1, \ldots, n)$ – такой литерал, что присвоение значения истинности $l_i \mapsto \top$ порождает вершину v_i, а D_i – дизъюнкт, на основе которого присвоено это значение.

Анализ вершины v_n состоит в следующем.

Проверяется, существует ли среди дизъюнктов, которые предстоит обработать дизъюнкт, имеющий значение $\bot$. Если такого дизъюнкта нет, то из вершины v_n продолжается прямой ход. Если же существует такой дизъюнкт D, то следующим образом реализуется обратный ход (через $Rslvnt(D', D'')$ обозначена резольвента дизъюнктов D' и D''). Последовательно вычисляются резольвенты $R_1, R_2, \ldots$, где

$$R_i = \begin{cases} Rslvnt(D, D_n), \text{ если } i = 1 \\ Rslvnt(R_{i-1}, D_{n-i+1}), \text{ если } i \geq 2 \end{cases}.$$

Эти вычисления осуществляются до тех пор, пока не будет получена резольвента

$$R_j = \overline{l_r} \vee D',$$

где $r \in \{j+1, \ldots, n\}$, а $D' = \bigvee\limits_{j=1}^{h} \overline{l_{i_j}}$ $(1 \leq i_1 \cdots < i_h \leq n - j)$.

Обратный ход состоит в том, что текущее состояние (1.50) поиска с возвращением заменяется текущим состоянием

$$\overset{v_0}{\emptyset} \to \overset{v_1}{(l_1, D_1)} \to \overset{v_2}{(l_2, D_2)} \to \cdots \to \overset{v_h}{(l_h, D_h)} \to \overset{v_{h+1}}{(\overline{l_r}, D)}.$$

После этого осуществляется анализ вершины v_{h+1}.

Замечание 1.98. В программных реализациях DPLL, управляющих конфликтами, для сокращения временных и емкостных затрат используются также дополнительные приемы, в том числе и псевдо-случайный выбор объектов (см., напр., [169]).

В последнее десятилетие значительные усилия были направлены на разработку формальных моделей DPLL и SMT-систем, построенных на

основе «ленивого подхода». Такие модели определяются системой продукций (rule-based systems) (см., напр., [191-193,220]). Их значение определяется следующими двумя факторами.

Во-первых, они являются частью математического аппарата, предназначенного для унифицированного построения решателей на основе «ленивого подхода».

Во вторых, появляется возможность доказать для разрабатываемых решателей такие основные с позиции теории алгоритмов свойства, как *корректность* (soundness), *полнота* и *остановка*.

Замечание 1.99. По-видимому, одной из первых таких формальных моделей является (построенная на основе модели, разработанной В. Аккерманом в середине XX века) *теория равенства и не интерпретируемых функций* $\mathcal{EUF}$ (equality and uninterpreted functions) [155,183,189,190]. Эта теория является бесквантворной теорией 1-го порядка, определяемой обычными аксиомами равенства

$$x = x,\ \ (x = y) \to (y = x),\ \ (x = y) \wedge (y = z) \to (x = z)$$

и аксиомами конгруэтности (f – функциональный, а P – предикатный символы)

$$\bigwedge_{i=1}^{n}(x_i = y_i) \to (f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)),$$

$$\bigwedge_{i=1}^{n}(x_i = y_i) \to (P(x_1, \ldots, x_n) = P(y_1, \ldots, y_n)).$$

Существующие $\mathcal{EUF}$-решатели имеют полиномиальную сложность. Их внедрение на верхний уровень обработки замкнутых относительно конгруэнции структур данных является мощным средством выявления конфликтов.

1.4.3. $\mathcal{T}$-решатели.

Построение современных $\mathcal{T}$-решателей осуществляется на основе следующего подхода, получившего имя *наслоение* (layering) [134,136].

Выделяется такая последовательность подтеорий

$$\mathcal{T}_1 \subset \mathcal{T}_2 \subset \cdots \subset \mathcal{T}_n = \mathcal{T},$$

что проверка совместности ограничений для теории $\mathcal{T}_i$ $(i = 1, \ldots, n-1)$ проще, чем соответствующая проверка для теории $\mathcal{T}_{i+1}$. Далее конструируется последовательность $S_1, \ldots, S_n$ решателей возрастающей выразительности (и, как следствие, сложности), где S_i $(i = 1, \ldots, n)$ – $\mathcal{T}_i$-решатель. Если $\mathcal{T}_i$-решатель S_i установил, что исследуемое множество ограничений является не совместным множеством, то $\mathcal{T}$-решатель выдает `unsat` без обращения к решателям $S_{i+1}, \ldots, S_n$.

Кроме ответа `sat` (множество ограничений совместно) или `unknown` (вывод о совместности множества ограничений не сделан) предусмотрена возможность выдачи $\mathcal{T}$-решателем следствий, установленных в процессе анализа исследуемого множества ограничений, представленных атомами теории $\mathcal{T}$. В случае ответа `sat` эти следствия называются *леммами* теории $\mathcal{T}$. Аналогичным образом, кроме ответа `unsat` предусмотрена возможность выдачи $\mathcal{T}$-решателем *конфликтных множеств*, т.е. тех или иных подмножеств ограничений, наличие которых приводит к невыполнимости исследуемого множества ограничений.

Проиллюстрируем особенности построения $\mathcal{T}$-решателей на примере задачи проверки выполнимости формул линейной арифметики $\mathcal{LA}$, т.е. атомы этой теории – это формулы вида

$$\sum_{i=1}^{n} a_i x_i \diamondsuit b \quad (\diamondsuit \in \{\leq, <, \neq, =, \geq, >\}).$$

Замечание 1.100. Эта задача наиболее полно проработана на текущий момент.

Пример 1.11. Для проверки выполнимости бесквантворных формул линейной рациональной арифметики $\mathcal{LA}(\mathbb{Q})$ разработан ряд эффективных на практике $\mathcal{LA}(\mathbb{Q})$-решателей, каждый из которых основан на использовании симплекс-метода (см., напр., [127,133,154,156]).

Иная ситуация имеет место в случае проверки выполнимости бесквантворных формул линейной целочисленной арифметики $\mathcal{LA}(\mathbb{Z})$. Известно, что эта задача NP-полная, а $\mathcal{LA}(\mathbb{Z})$-решатели, аналогичные предложенным в [163,197], далеко не всегда справляются с решением реальных задач.

В [170] предложен следующий достаточно эффективный на практике $\mathcal{LA}(\mathbb{Z})$-решатель в предположении, что атомы имеют вид

$$\sum_{i=1}^{n} a_i x_i \diamondsuit b \quad (\diamondsuit \in \{=, \leq\}).$$

Вначале применяется $\mathcal{LA}(\mathbb{Q})$-решатель. Если он выдает `unsat`, то $\mathcal{LA}(\mathbb{Z})$-решатель также выдает `unsat` и прекращает работу. Если же $\mathcal{LA}(\mathbb{Q})$-решатель выдает `sat` (т.е. конфликты не обнаружены), то осуществляется проверка целочисленности значений переменных. В случае положительного ответа $\mathcal{LA}(\mathbb{Z})$-решатель выдает `sat` и прекращает работу. В случае отрицательного ответа активируется следующий модуль, предназначенный для анализа системы линейных диофантовых уравнений.

Первая процедура проверяет, есть ли среди анализируемых уравнений такое уравнение

$$\sum_{i} a_{hi} x_i + b_h = 0,$$

что НОД чисел a_{hi} не является делителем числа b_h. В случае положительного ответа $\mathcal{LA}(\mathbb{Z})$-решатель выдает `unsat` (так как анализируемая система линейных диофантовых уравнений является не совместной системой уравнений) и прекращает работу. В случае отрицательного ответа активируется процедура, которая следующим образом последовательно преобразует каждое из анализируемых уравнений.

В уравнении

$$\sum_i a_{hi}x_i + b_h = 0 \tag{1.51}$$

выбирается наименьший по модулю ненулевой коэффициент a_{hk}.

Возможны следующие два случая:

1. Пусть $|a_{hk}| = 1$. Тогда уравнение (1.51) приводится к виду

$$x_k = -\sum_{i\neq k} \alpha_{kh}a_{hi}x_i - \alpha_{hk}b_h,$$

где

$$\alpha_{hk} = a_{hk}|a_{hk}|^{-1}.$$

Эта подстановка осуществляется во все остальные уравнения.

2. Пусть $|a_{hk}| > 1$. Тогда уравнение (1.51) приводится к виду

$$a_{hk}(x_k + \sum_{i\neq k} a_{hi}^{(q)}x_i + b_h^{(q)}) + \sum_{i\neq k} a_{hi}^{(r)}x_i + b_h^{(r)} = 0,$$

где $a_{hi}^{(q)}$ и $a_{hi}^{(r)}$ (соответственно, $b_h^{(q)}$ и $b_h^{(r)}$) – частное и остаток от деления a_{hi} на a_{hk} (соответственно, b_h на a_{hk}). Вводится новая переменная

$$x_t = x_k + \sum_{i\neq k} a_{hi}^{(q)}x_i + b_h^{(q)}.$$

Эта подстановка осуществляется во все уравнения.

Такое преобразование применяется к анализируемому уравнению (1.51) до тех пор, пока не возникнет 1-й случай (что всегда происходит через конечное число шагов).

Если при выполнении рассмотренной процедуры обнаружены конфликты, то $\mathcal{LA}(\mathbb{Z})$-решатель выдает `unsat` и прекращает работу. Если же конфликты не обнаружены, то полученная система

$$x_j = \sum_{i\neq j} a_{ji}x_i + c_j$$

линейных диофантовых уравнений используется в качестве подстановки в анализируемую систему неравенств и активируется модуль, предназначенный для анализа системы линейных неравенств.

Вначале каждое такое неравенство

$$\sum_i a_i x_i + b \leq 0,$$

что НОД g чисел a_i не является делителем числа b преобразуется в неравенство

$$\sum_i a_i g^{-1}x_i + \lceil bg^{-1}\rceil \leq 0.$$

Затем активируется $\mathcal{LA}(\mathbb{Q})$-решатель. Если он выдает `sat` , то осуществляется проверка целочисленности значений переменных. В случае положительного ответа

$\mathcal{LA}(\mathbb{Z})$-решатель также выдает `sat` и прекращает работу. В случае отрицательного ответа активируется модуль, реализующий метод ветвей и границ.

Этот модуль следующим образом рекурсивно разбивает анализируемую задачу на две подзадачи добавлением дополнительных ограничений в исследуемую формулу.

Пусть $\mathcal{LA}(\mathbb{Q})$-решатель ассоциировал с переменной x_k значение α_k, не являющееся целым числом. Дополнительное ограничение для 1-й подзадачи является неравенство

$$x_k - \lfloor \alpha_k \rfloor \leq 0,$$

а для 2-й подзадачи является неравенство

$$-x_k + \lceil \alpha_k \rceil \leq 0.$$

После этого к каждой из подзадач применяется $\mathcal{LA}(\mathbb{Q})$-решатель.

Такие вычисления осуществляются до тех пор, пока либо $\mathcal{LA}(\mathbb{Z})$-решатель выдает `sat`, либо будет установлено, что все подзадачи невыполнимы. В последнем случае $\mathcal{LA}(\mathbb{Z})$-решатель выдает `unsat`.

Исследования, связанные с разработкой процедур анализа формул $\mathcal{LA}$ естественно привели к выделению следующих двух подтеорий.

1. *Разностная логика* $\mathcal{DL}$ (difference logic) [146,182,191,223]. Атомы этой теории – это формулы вида

$$x - y \diamondsuit a \ (\diamondsuit \in \{\leq, <, \neq, =, \geq, >\}.$$

Существующие решатели для $\mathcal{DL}(\mathbb{Q})$ и $\mathcal{DL}(\mathbb{Z})$ имеют полиномиальную сложность. Большинство из них основано на сведении проверки выполнимости множества неравенств к проверке отсутствия отрицательных циклов в графе ограничений (constraint graph) [142]. Последний определяется следующим образом. Вершины отмечены переменными. Из вершины с отметкой «x» идет дуга в вершину с отметкой «y» тогда и только тогда, когда анализируемое множество неравенств содержит неравенство $x - y \leq a$. Эта дуга имеет отметку «a».

2. *Теория двух целых переменных на неравенство* $\mathcal{UTVPI}$ (unit-two-variable-per-inequality) [172,179]. Эта теория является подтеорией теории $\mathcal{LA}(\mathbb{Z})$, а ее атомы имеют вид

$$\pm x \pm y \leq a.$$

Существующие $\mathcal{UTVPI}$-решатели имеют полиномиальную сложность. Большинство из них основано на итеративном построении транзитивного замыкания: при добавлении нового ограничения выводятся всевозможные следствия до тех пор, пока либо будет получено противоречие, либо будет достигнута неподвижная точка.

Анализ $\mathcal{EUF}$ и $\mathcal{LA}$ показал, что сложность решателей, во-многом, характеризуется такими свойствами теории $\mathcal{T}$, как «быть выпуклой» (convex) и «быть бесконечно устойчивой» (stably-infinite) [195]. Эти свойства определяются следующим образом.

Теория $\mathcal{T}$ *выпукла*, если для любой конъюнкции K ее литералов и для любой дизъюнкции $\bigvee\limits_{i=1}^{n}(x_i = y_i)$ (где x_i и y_i – переменные теории $\mathcal{T}$)

$$\left(K \models_{\mathcal{T}} \bigvee_{i=1}^{n}(x_i = y_i)\right) \Leftrightarrow (\exists i \in \mathbb{N}_n)(K \models_{\mathcal{T}} (x_i = y_i)).$$

Теория $\mathcal{T}$ *бесконечно устойчива*, если для любой $\mathcal{T}$-выполнимой формулы φ существует модель с бесконечной областью, в которой формула φ выполнима.

Замечание 1.101. $\mathcal{EUF}$, $\mathcal{LA}(\mathbb{Q})$ и $\mathcal{DL}(\mathbb{Q})$ – бесконечно устойчивые и выпуклые теории, а $\mathcal{LA}(\mathbb{Z})$, $\mathcal{DL}(\mathbb{Z})$ и $\mathcal{UTVPI}$ – бесконечно устойчивые не выпуклые теории.

Значительные усилия исследователей были направлены на построение решателей для работы с основными структурами данных. Рассмотрим их кратко.

Теория битовых векторов $\mathcal{BV}$ [124,131,137,140,148,162,166,178,183] является теорией 1-го порядка с равенством. Она предназначена для анализа дискретных устройств, представленных на языке регистровых передач, а также для верификации программ.

Основные операции теории $\mathcal{BV}$ – конкатенация, выбор подслова, сложение и умножение по заданному модулю, а также побитовые логические операции над векторами одной и той же длины. Эта теория не является ни выпуклой, ни бесконечно устойчивой. Известно, что проверка выполнимости безквантворных формул теории $\mathcal{BV}$ является NP-полной задачей. Большинство существующих $\mathcal{BV}$-решателей, используя препроцессорные вычисления, кодируют исследуемую задачу в виде данных либо для SAT-решателя, либо для $\mathcal{LA}(\mathbb{Z})$-решателя.

Замечание 1.102. Выбор приемлемых на практике алгоритмов для $\mathcal{BV}$-решателя является одной из наиболее актуальных проблем в настоящее время.

Теория массивов $\mathcal{AR}$ [183,187,196,218] является теорией 1-го порядка с равенством. Она предназначена для анализа поведения на уровне «массив/память» (что, в частности, актуально как при верификации программ, так и при организации тестирования программных систем).

Сигнатура $\mathcal{AR}$ содержит два интерпретированных функциональных символа: $read$ и $write$ ($read(a,i)$ – это элемент элемент, записанный в массив a по адресу i, а $write(a,i,e)$ – это результат записи элемента e в массив a по адресу i). Аксиомы $\mathcal{AR}$ имеют следующий вид

$$(\forall a)(\forall i)(\forall e)(read(write(a,i,e),i)=e),$$

$$(\forall a)(\forall i,j)(\forall e)((i\neq j)\rightarrow read(write(a,i,e),j)=read(a,j)),$$

$$(\forall a,b)((\forall i)(read(a,i)=read(b,i))\rightarrow(a=b)).$$

Известно, что проверка выполнимости безкванторных формул теории $\mathcal{AR}$ является NP-полной задачей.

Замечание 1.103. Существующие $\mathcal{AR}$-решатели применяются, как правило, в комбинации с решателями, предназначенными для других теорий.

Теория списков $\mathcal{LI}$ [183] представляет собой теорию 1-го порядка с равенством.

Замечание 1.104. Эта теория является подтеорией *теории рекурсивных типов данных* $\mathcal{RDT}$ [196].

Сигнатура $\mathcal{LI}$ содержит три интерпретированных функциональных символа, представляющих основные операторы языка LISP: функцию $cons$, конструирующую в памяти объект, содержащий два значения или указатели на эти значения, а также функции car и cdr, осуществляющие выбор, соответственно, 1-го и 2-го элементов объекта.

Аксиомы $\mathcal{LI}$ имеют следующий вид

$$(\forall x)(cons(cad(x),cdr(x))=x),$$

$$(\forall x,y)(car(cons(x,y))=x),\quad(\forall x,y)(cdr(cons(x,y))=y),$$
$$(\forall x)(f^n(x)\neq x)\quad(f\in\{car,cdr\},n\in\mathbb{N}). \tag{1.52}$$

Замечание 1.105. Аксиомы (1.52) обеспечивают отсутствие «зацикливания» при формировании списков.

Известно, что проверка выполнимости бесквантворных формул $\mathcal{LI}$ осуществима за линейное время. Это обосновывает целесообразность применения существующих $\mathcal{LI}$-решателей при решении задач проверки корректности любых алгоритмов, использующих списки в качестве основных структур данных (в частности, при верификации программ и анализе алгоритмов обработки моделей с сетевой структурой).

1.4.4. Интеграция DPLL и $\mathcal{T}$-решателей.

Обозначим через $\mathcal{T}$-DPLL систему, состоящую из взаимодействующих DPLL и $\mathcal{T}$-решателя, предназначенную для решения задачи $SMT(\mathcal{T})$ на основе «ленивого подхода». Входными данными для $\mathcal{T}$-DPLL системы является исследуемая $\mathcal{T}$-формула φ. Система автоматически конструирует (посредством кодировки атомов теории $\mathcal{T}$ пропозициональными переменными) пропозициональное представление $\varphi^{(p)}$ формулы φ.

Все многообразие взаимодействий DPLL и $\mathcal{T}$-решателя в системе $\mathcal{T}$-DPLL естественно разбивается на следующие два класса.

1. *Off-line взаимодействие.* При таком взаимодействии функционирование $\mathcal{T}$-DPLL системы осуществляется следующим образом.

Формула $\varphi^{(p)}$ подается на вход DPLL. Если установлено, что $\varphi^{(p)}$ – невыполнимая формула, то система $\mathcal{T}$-DPLL выдает `unsat` и останавливается. Если же построена модель $\mu^{(p)}$ формулы $\varphi^{(p)}$, то множество η атомов теории $\mathcal{T}$, построенных в соответствии с литералами, входящими в $\mu^{(p)}$, подается на вход $\mathcal{T}$-решателя.

Если $\mathcal{T}$-решатель устанавливает, что множество атомов η выполнимо, то система $\mathcal{T}$-DPLL выдает `sat` и останавливается. Если же $\mathcal{T}$-решатель устанавливает, что множество атомов η является не выполнимым, то выбирается конфликтное подмножество η_0 множества η. Множество $\overline{\eta_0}$, состоящее из отрицаний атомов, принадлежащих множеству η_0, кодируется дизъюнкцией D литералов, и формула $\varphi^{(p)} \wedge D$ подается на вход DPLL.

Замечание 1.106. Процесс перехода от пропозициональной формулы $\varphi^{(p)}$ к формуле $\varphi^{(p)} \wedge D$ называют построением *лемм по требованию* (lemmas on demand) [126].

Таким образом, при off-line взаимодействии DPLL рассматривается как «черный ящик» в системе $\mathcal{T}$-DPLL.

2. *On-line взаимодействие.* При таком взаимодействии $\mathcal{T}$-DPLL система представляет собой вариант DPLL, функционирующий как *перечислитель* (enumerator) моделей пропозициональной формулы, выполнимость интерпретаций в теории $\mathcal{T}$ которых проверяется $\mathcal{T}$-решателем. С исследуемой формулой φ такая $\mathcal{T}$-DPLL система ассоциирует множество $\mathcal{T}$-литералов μ, которым присвоены значения (первоначально, $\mu = \emptyset$).

Замечание 1.107. $\mathcal{T}$-литералом называется атом теории $\mathcal{T}$ или его отрицание.

Структура $\mathcal{T}$-DPLL системы, основанной на on-line взаимодействии, во многом, аналогична структуре DPLL, управляющей конфликтами. Основными являются следующие три процедуры.

1. *$\mathcal{T}$-препроцессорная обработка данных.* Эта процедура предназначена для упрощения формулы φ, а также для преобразования (если возникает необходимость) множества μ, сохраняющего $\mathcal{T}$-выполнимость формулы $\varphi \wedge \mu$. Большинство ее шагов является комбинацией шагов соответствующей процедуры для DPLL с определяемыми теорией $\mathcal{T}$ правилами вывода, применяемыми к $\mathcal{T}$-литералам формулы φ.

Среди методов упрощения формулы φ выделяют *нормализацию* $\mathcal{T}$-атомов и *статическое изучение* (static learning) [119,121,134,203,217].

Под *нормализацией* $\mathcal{T}$-атомов понимают их приведение к стандартному виду.

Замечание 1.108. В зависимости от теории $\mathcal{T}$ в процессе *нормализации* могут применяться замена некоторых операций и отношений на двойственные, использоваться свойства ассоциативности, коммутативности, дистрибутивности, поглощения, та или иная сортировка, и т.д.

Статическое изучение состоит в проверке совместности рассматриваемого множества $\mathcal{T}$-атомов посредством анализа ограничений, определяемых простейшими эквивалентностями и конгруэнциями.

Если при выполнении $\mathcal{T}$-препроцессорной обработки данных обнаружен конфликт, то $\mathcal{T}$-DPLL система выдает `unsat` и останавливается.

2. *$\mathcal{T}$-ветвление.* Эта процедура реализует *прямой ход* поиска с возвращением. Большинство ее шагов является комбинацией шагов соответствующей процедуры для DPLL с основанными на учете семантики теории $\mathcal{T}$ методами *раннего отсечения* (early pruning) и *$\mathcal{T}$-продвижения* ($\mathcal{T}$-propagating) [119,121,125,134,167,191,220].

Методы *раннего отсечения* предназначены для сужения пространства поиска при выборе литералов, которым присваиваются значения. Их суть состоит в том, что при обнаружении не совместности в теории $\mathcal{T}$ (иными словами, $\mathcal{T}$-несовместности) множества $\mathcal{T}$-литералов μ нет необходимости рассматривать никакое расширение множества μ.

Реализация этих методов основана на том обстоятельстве, что построение современных $\mathcal{T}$-решателей на основе техники наслоения дает возможность эффективно использовать последовательность соответствующих $\mathcal{T}_i$-решателей.

Кроме того, могут применяться такие эвристические методы, как отсечение множества μ при отсутствии его расширения на протяжении заданного числа шагов, или при присвоении в течение данного числа шагов значений только чисто пропозициональным литералам.

Методы $\mathcal{T}$-*продвижения* состоят в следующем. При текущем вызове $\mathcal{T}$-решателя осуществляется попытка выводов вида $\eta \models_{\mathcal{T}} l$, где $\eta \subseteq \mu$, а l – $\mathcal{T}$-литерал, значение которому еще не присвоено. Если такие $\mathcal{T}$-литералы найдены, то они добавляются в множество μ.

3. $\mathcal{T}$-*анализ конфликтов*. Эта процедура реализует *обратный ход* поиска с возвращением. Большинство ее шагов является комбинацией шагов соответствующей процедуры для DPLL с основанными на учете семантики теории $\mathcal{T}$ методами $\mathcal{T}$-*возврата* ($\mathcal{T}$-backjumping) и $\mathcal{T}$-*изучения* ($\mathcal{T}$-learning) [123,135,136,152,164,167,175,219,214].

Методы $\mathcal{T}$-*возврата* основаны на следующем предположении: если $\mathcal{T}$-решатель активируется на множестве $\mathcal{T}$-литералов μ, то при установлении $\mathcal{T}$-несовместности множества μ он строит конфликтное подмножество $\eta \subset \mu$. В этом случае система $\mathcal{T}$-DPLL использует пропозициональное представление $\eta^{(p)}$ в качестве источника конфликта. При этом активируется режим возврата DPLL (т.е. $\varphi^{(p)} := \varphi^{(p)} \wedge D$, где D – дизъюнкция отрицаний пропозициональных литералов, принадлежащих $\eta^{(p)}$ и осуществляется возврат в вершину дерева поиска (какую именно, зависит от выбранной стратегии), в которой не присвоены значения ни одному из литералов, принадлежащих множеству $\eta^{(p)}$).

Методы $\mathcal{T}$-*изучения* предназначены для выделения суб-минимальных по мощности конфликтных множеств $\mathcal{T}$-литералов, объединение которых содержит как можно больше $\mathcal{T}$-литералов, значения которым не присвоены на текущий момент. Именно такие системы множеств $\mathcal{T}$-литералов, а также аналогичные системы множеств чисто пропозициональных литералов используются при построении стратегии ветвления и возврата $\mathcal{T}$-DPLL системы в вершины дерева поиска, расположенные в как можно ранее построенных уровнях, что, в конечном итоге, обеспечивают наиболее существенное сужение пространства поиска.

Замечание 1.109. Наиболее простой такой стратегий ветвления и возврата $\mathcal{T}$-DPLL системы является следующая (см. процедуру анализа конфликтов для DPLL).

Пусть S – множество $\mathcal{T}$-литералов, которым на текущий момент присвоены значения $\top$. Для каждого множества η, принадлежащего построенной на текущий момент системе суб-минимальных по мощности конфликтных множеств $\mathcal{T}$-литералов проверяется условие

$$|S \cap \eta| = |\eta| - 1.$$

Если это условие выполнено, то $\mathcal{T}$-литералу $l \in \eta \backslash S$ автоматически присваивается значение $\bot$.

После окончания этого процесса происходит активация процедуры $\mathcal{T}$-анализа конфликтов.

В заключение отметим следующее. В настоящее время достаточно хорошо проработаны теоретические основы построения $\mathcal{T}$-DPLL систем в терминах разрешимых теорий 1-го порядка. При этом созданы общие методы синтеза $\mathcal{T}$-DPLL систем на основе сведения предназначенных для различных теорий решателей в единый решатель с последующей его интеграцией с DPLL [154,155,168,187,205].

Построение приемлемых на практике $\mathcal{T}$-решателей дает возможность конструировать на основе наслоения такие программные системы с достаточно широкой областью применения, как MathSAT [134], представляющий собой взаимодействующую с DPLL иерархию решателей, предназначенных, для проверки выполнимости формул, соответственно, теорий $\mathcal{EUF}$, $\mathcal{DL}$, $\mathcal{LA}(\mathbb{Q})$ и $\mathcal{LA}(\mathbb{Z})$.

Возможности таких программных систем могут быть существенно расширены за счет включения в иерархию решателей, предназначенных для проверки выполнимости формул других теорий. Например, предложенного в [165] решателя, основанного на интервальной арифметике и предназначенного для проверки выполнимости системы нелинейных ограничений (в том числе построенных с помощью трансцендентных функций).

1.5. Выводы.

В настоящее время наблюдается устойчивая тенденция к применению алгебраических моделей и методов при решении задач преобразования информации, в частности, защиты информации. Подтверждением этого является использование вычислений, осуществляемых в конечных кольцах, при построении современных стандартов шифрования. Такая ситуация обосновывает актуальность разработки нового раздела алгебраической теории автоматов, предметом исследования которого являются автоматные модели, представленные системами рекуррентных соотношений над конечными алгебраическими структурами. При этом основными становятся задачи исследования сложности идентификации автоматов, принадлежащих этим семействам, исследования сложности идентификации начальных состояний автоматов, принадлежащих этим семействам, анализа множеств неподвижных точек о.-д. функций, реализуемых автоматами, принадлежащими этим семействам, а также задачи выделения и исследования семейств обратимых автоматов.

В качестве основной конечной алгебраической структуры естественно выбрать конечное кольцо. Решение перечисленных выше задач для семейств автоматов, представленных системами рекуррентных соотношений над конечным кольцом, естественно сводится к анализу систем уравнений над этим кольцом. Поэтому актуальна задача исследования методов решения систем уравнений над конечными кольцами (известно, что даже решение системы уравнений второй степени от многих переменных над полем $\mathcal{GF}(2^k)$ ($k \in \mathbb{N}$) является NP-полной задачей). Кроме того, актуальной является разработка методов проверки выполнимости формул над конечным кольцом, что является основой для создания соответствующих решателей, приемлемых на практике.

Известно, что многообразие является одним из основных понятий алгебраической геометрии [24,111,112]. При этом естественно возникают параметризованные многообразия и многообразия с определенной на них алгебраической системой (к последним, в частности, относятся эллиптические кривые). Таким образом, естественно возникают семейства автоматов, заданных на многообразии над конечным кольцом. Исследование таких семейств автоматов актуально в связи со следующими обстоятельствами.

Во-первых, они определяют новый класс дискретных конечных динамических систем.

Во-вторых, эллиптическая криптография [12,14,33] считается одним из наиболее перспективных направлений современной криптографии.

Решение всех перечисленных выше задач и рассматривается в последующих разделах.

2. ОТОБРАЖЕНИЯ МНОЖЕСТВА В ФАКТОР-КОЛЬЦА

Применение алгебраических моделей и методов в процессе решения прикладных задач обосновывает актуальность разработки комбинаторных схем, предназначенных для подсчета числа тех или иных объектов, построенных в терминах теории колец. Любую такую схему можно представить в терминах отображений абстрактного множества в соответствующее кольцо. Такое представление дает возможность установить внутренние связи между теорией колец, комбинаторным анализом и прикладными задачами, в том числе, задачами преобразования информации и криптографии.

В настоящем разделе построена и исследована комбинаторная схема, основанная на соотношении между множествами отображений абстрактного множества в полную систему вычетов по попарно взаимно простым идеалам ассоциативно-коммутативного кольца и множеством отображений этого же множества в полную систему вычетов по произведению этих идеалов.

В п.2.1 введены необходимые понятия. Построена и исследована комбинаторная схема. Рассмотрены ее применения для решения модельных алгебраических задач. В п.2.2 построена «ленточная модель», представляющая собой интерпретацию предложенной схемы для кольца целых чисел. Рассмотрены ее применения для решения модельных теоретико-числовых и алгебраических задач. Доказано отсутствие непосредственного обобщения построенной комбинаторной схемы на бесконечное множество фактор-колец. П.2.3 содержит ряд заключительных замечаний.

Результаты автора, представленные в настоящем разделе, опубликованы в работах [67,68,78-80,87].

2.1. Исследуемая модель.

Охарактеризуем соотношения между множествами отображений абстрактного множества в полную систему вычетов по попарно взаимно простым идеалам ассоциативно-коммутативного кольца и множеством отображений этого же множества в полную систему вычетов по произведению этих идеалов.

2.1.1. Свойства разбиений, определяемых идеалами.

Пусть $\mathcal{K} = (K, +, \cdot)$ – произвольное ассоциативно-коммутативное кольцо. Обозначим через $\mathcal{I}_{\mathcal{K}}$ множество всех идеалов кольца $\mathcal{K}$.

Замечание 2.1. Для любого ассоциативно-коммутативного кольца $\mathcal{K}$ множество $\mathcal{I}_{\mathcal{K}}$ является коммутативной полугруппой относительно операции умножения идеалов, т.е. $I_1 I_2 = I_2 I_1$ для всех $I_1, I_2 \in \mathcal{I}_{\mathcal{K}}$. Идеал $I_1 \cap I_2$ называется *наименьшим общим кратным* идеалов I_1 и I_2. При этом включение

$$I_1 I_2 \subseteq I_1 \cap I_2 \tag{2.1}$$

истинно для всех $I_1, I_2 \in \mathcal{I}_{\mathcal{K}}$.

Утверждение 2.1. В каждом ассоциативно-коммутативном кольце $\mathcal{K}$ включение

$$I_1(I_2 \cap I_3) \subseteq I_1 I_2 \cap I_1 I_3 \tag{2.2}$$

истинно для всех идеалов $I_1, I_2, I_3 \in \mathcal{I}_{\mathcal{K}}$.□

Доказательство. Пусть $\mathcal{K}$ – ассоциативно-коммутативное кольцо и $I_1, I_2, I_3 \in \mathcal{I}_{\mathcal{K}}$.

Так как $I_2 \cap I_3 \subseteq I_2$, то $I_1(I_2 \cap I_3) \subseteq I_1 I_2$, а так как $I_2 \cap I_3 \subseteq I_3$, то $I_1(I_2 \cap I_3) \subseteq I_1 I_3$.

Из включений $I_1(I_2 \cap I_3) \subseteq I_1 I_2$ и $I_1(I_2 \cap I_3) \subseteq I_1 I_3$ вытекает, что включение (2.2) истинно.□

Утверждение 2.2. В каждом ассоциативно-коммутативном кольце $\mathcal{K}$ для каждого числа $m \in \mathbb{N}$ $(m \geq 3)$ включение

$$\prod_{i=1}^{m} I_i \subseteq \bigcap_{i=1}^{m} I_i \tag{2.3}$$

истинно для всех идеалов $I_1, \ldots, I_m \in \mathcal{I}_{\mathcal{K}}$.□

Доказательство. Пусть $\mathcal{K}$ – ассоциативно-коммутативное кольцо, $m \in \mathbb{N}$ $(m \geq 3)$ и $I_1, \ldots, I_m \in \mathcal{I}_{\mathcal{K}}$.

Докажем включение (2.3) индукцией по числу $m \in \mathbb{N}$ $(m \geq 3)$.

Пусть $m = 3$. Из включений (2.1) и (2.2) вытекает, что

$$I_1 I_2 I_3 \subseteq I_1(I_2 \cap I_3) \subseteq I_1 I_2 \cap I_1 I_3 \subseteq (I_1 \cap I_2) \cap (I_2 \cap I_3) = I_1 \cap I_2 \cap I_3,$$

что и требовалось доказать.

Предположим, что включение (2.3) истинно для всех $m = 3, \ldots, n$, т.е.

$$\prod_{i=1}^{m} I_i \subseteq \bigcap_{i=1}^{m} I_i \ (m = 3, \ldots, n). \tag{2.4}$$

Докажем включение (2.3) для $m = n + 1$.

Из включений (2.1) и (2.4) вытекает, что

$$\prod_{i=1}^{m} I_i = \prod_{i=1}^{n+1} I_i = \left(\prod_{i=1}^{n} I_i\right) I_{n+1} \subseteq \left(\bigcap_{i=1}^{n} I_i\right) I_{n+1} \subseteq$$

$$\subseteq \left(\bigcap_{i=1}^{n} I_i\right) \cap I_{n+1} = \bigcap_{i=1}^{n+1} I_i = \bigcap_{i=1}^{m} I_i,$$

что и требовалось доказать.□

Следствие 2.1. В каждом ассоциативно-коммутативном кольце $\mathcal{K}$ включение

$$\prod_{i=1}^{m} I_i \subseteq \bigcap_{i=1}^{m} I_i \ (m \in \mathbb{N}, m \geq 2) \tag{2.5}$$

истинно для всех идеалов $I_1, \ldots, I_m \in \mathcal{I}_{\mathcal{K}}$.□

Доказательство. При $m = 2$ включение (2.5) совпадает с (2.1), а при $m \geq 3$ включение (2.5) представляет собой включение (2.3).□

Фактор-множество $K/_{\equiv_I}$ $(I \in \mathcal{I}_{\mathcal{K}})$, рассматриваемое как разбиение множества K обозначим через через $\pi(K, I)$, т.е. $x \equiv y(\pi(K, I))$ тогда и только тогда, когда $x \equiv y \,(mod\, I)$.

Замечание 2.2. Таким образом,

$$\pi(K, I) = \{I + a | a \in K\} \ (I \in \mathcal{I}_{\mathcal{K}}).$$

При этом $\pi(K, I_1) \leq \pi(K, I_2)$ $(I_1, I_2 \in \mathcal{I}_{\mathcal{K}})$ тогда и только тогда, когда $I_1 \subseteq I_2$.

Положим

$$\mathcal{P}_{\mathcal{K}} = \{\pi(K, I) | I \in \mathcal{I}_{\mathcal{K}}\}.$$

Множество $\mathcal{P}_{\mathcal{K}}$ характеризуется следующим образом.

Лемма 2.1. Для каждого ассоциативно-коммутативного кольца $\mathcal{K}$ и для каждого числа $m \in \mathbb{N}$ неравенство

$$\pi\left(K, \prod_{i=1}^{m} I_i\right) \leq \prod_{i=1}^{m} \pi(K, I_i) \tag{2.6}$$

истинно для всех идеалов $I_1, \ldots, I_m \in \mathcal{I}_{\mathcal{K}}$.□

Доказательство. Предположим, что $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо, $m \in \mathbb{N}$ и $I_1, \ldots, I_m \in \mathcal{I}_{\mathcal{K}}$.

При $m = 1$ неравенство (2.6) имеет вид $\pi(K, I_1) \leq \pi(K, I_1)$, и, следовательно, является истинным для всех $I_1 \in \mathcal{I}_{\mathcal{K}}$.

Пусть $m \geq 2$. Для любых элементов $x, y \in K$

$$x \equiv y \left(\pi\left(K, \prod_{i=1}^{m} I_i\right)\right) \Leftrightarrow x \equiv y \left(mod \prod_{i=1}^{m} I_i\right). \tag{2.7}$$

Так как $\prod\limits_{i=1}^{m} I_i \subseteq \bigcap\limits_{i=1}^{m} I_i$, то

$$x \equiv y \left(mod \prod_{i=1}^{m} I_i\right) \Rightarrow x \equiv y \left(mod \bigcap_{i=1}^{m} I_i\right) \Leftrightarrow$$

$$\Leftrightarrow x-y\in\bigcap_{i=1}^{m}I_i\Leftrightarrow(\forall i=1,\ldots,m)(x-y\in I_i)\Leftrightarrow$$
$$\Leftrightarrow(\forall i=1,\ldots,m)(x\equiv y\,(mod\,I_i))\Leftrightarrow$$
$$\Leftrightarrow(\forall i=1,\ldots,m)(x\equiv y\,(\pi(K,I_i)))\Leftrightarrow$$
$$\Leftrightarrow x\equiv y\left(\prod_{i=1}^{m}\pi(K,I_i)\right). \tag{2.8}$$

Из (2.7) и (2.8) вытекает (2.6). □

Следствие 2.2. Для каждого ассоциативно-коммутативного кольца $\mathcal{K}$ равенство

$$\pi\left(K,\prod_{i=1}^{m}I_i\right)=\prod_{i=1}^{m}\pi(K,I_i)\ (m\in\mathbb{N}) \tag{2.9}$$

истинно для всех таких идеалов $I_1,\ldots,I_m\in\mathcal{I}_{\mathcal{K}}$, что $\prod\limits_{i=1}^{m}I_i=\bigcap\limits_{i=1}^{m}I_i$.□

Доказательство. Предположим, что $\mathcal{K}=(K,+,\cdot)$ – ассоциативно-коммутативное кольцо, $m\in\mathbb{N}$, $I_1,\ldots,I_m\in\mathcal{I}_{\mathcal{K}}$ и $\prod\limits_{i=1}^{m}I_i=\bigcap\limits_{i=1}^{m}I_i$.

При $m=1$ равенство (2.9) имеет вид $\pi(K,I_1)=\pi(K,I_1)$, и, следовательно, является истинным для всех $I_1\in\mathcal{I}_{\mathcal{K}}$.

Пусть $m\geq 2$. Из равенства $\prod\limits_{i=1}^{m}I_i=\bigcap\limits_{i=1}^{m}I_i$ $(I_1,\ldots,I_m\in\mathcal{I}_{\mathcal{K}})$ вытекает, что

$$x\equiv y\left(mod\prod_{i=1}^{m}I_i\right)\Leftrightarrow x\equiv y\left(mod\bigcap_{i=1}^{m}I_j\right). \tag{2.10}$$

Заменим в (2.8) фрагмент

$$x\equiv y\left(mod\prod_{i=1}^{m}I_i\right)\Rightarrow x\equiv y\left(mod\bigcap_{i=1}^{m}I_j\right)$$

фрагментом (2.10). Получим, что

$$x\equiv y\left(mod\prod_{i=1}^{m}I_i\right)\Leftrightarrow x\equiv y\left(\prod_{i=1}^{m}\pi(K,I_i)\right). \tag{2.11}$$

Из (2.7) и (2.11) вытекает (2.9). □

Теорема 2.1. Для каждого ассоциативно-коммутативного кольца $\mathcal{K}$ и для каждого числа $m \in \mathbb{N}$ $(m \geq 2)$ равенство

$$\pi\left(K, \prod_{i=1}^{m} I_i\right) = \left\{ \bigcap_{i=1}^{m} B_i \middle| B_i \in \pi(K, I_i)\ (i = 1, \ldots, m) \right\} \tag{2.12}$$

истинно для всех таких идеалов $I_1, \ldots, I_m \in \mathcal{I}_{\mathcal{K}}$, что $\prod\limits_{i=1}^{r} I_i + I_{r+1} = K$ для всех $r = 1, \ldots, m-1$ и $\prod\limits_{i=1}^{h} I_i = \bigcap\limits_{i=1}^{h} I_i$ для всех $h = 2, \ldots, m$.$\square$

Доказательство. Предположим, что $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо, $m \in \mathbb{N}$ $(m \geq 2)$, а $I_1, \ldots, I_m \in \mathcal{I}_{\mathcal{K}}$ $(m \in \mathbb{N}, m \geq 2)$ – такие идеалы, что истинны равенства $\prod\limits_{i=1}^{r} I_i + I_{r+1} = K$ $(r = 1, \ldots, m-1)$ и $\prod\limits_{i=1}^{h} I_i = \bigcap\limits_{i=1}^{h} I_i$ $(h = 2, \ldots, m)$.

Равенство (2.12) эквивалентно утверждению о том, что

$$\bigcap_{i=1}^{m} B_i \neq \emptyset\ (m \in \mathbb{N}; m \geq 2) \tag{2.13}$$

для всех $B_i \in \pi(K, I_i)$ $(i = 1, \ldots, m)$.

Докажем это утверждение индукцией по числу $m \in \mathbb{N}$ $(m \geq 2)$.

Пусть $m = 2$. Так как $I_1 I_2 = I_1 \cap I_2$, то $\pi(K, I_1 I_2) = \pi(K, I_1)\pi(K, I_2)$. Пусть $B_1 \in \pi(K, I_1)$ и $B_2 \in \pi(K, I_2)$. Тогда $B_1 = I_1 + a$ и $B_2 = I_2 + b$, где $a, b \in K$ – фиксированные элементы.

Из равенства $I_1 + I_2 = K$ вытекает, что существуют такие элементы $\alpha_1 \in I_1$ и $\alpha_2 \in I_2$, что $a - b = \alpha_2 - \alpha_1$. Следовательно, $a + \alpha_1 = b + \alpha_2$.

Так как $\alpha_1 \in I_1$ и $\alpha_2 \in I_2$, то $\alpha_1 + a \in B_1$ и $\alpha_2 + b \in B_2$.

Из условий $a + \alpha_1 \in B_1$, $b + \alpha_2 \in B_2$ и $a + \alpha_1 = b + \alpha_2$ вытекает, что $B_1 \cap B_2 \neq \emptyset$, что и требовалось доказать.

Предположим, что формула (2.13) истинна для всех $m = 2, \ldots, n$.

Докажем, что формула (2.13) истинна при $m = n + 1$.

Так как $\prod\limits_{i=1}^{m} I_i = \bigcap\limits_{i=1}^{m} I_i$, то

$$\pi\left(K, \prod_{i=1}^{m} I_i\right) = \pi\left(K, \prod_{i=1}^{n+1} I_i\right) = \left(\prod_{i=1}^{n} \pi(K, I_i)\right) \pi(K, I_{n+1}).$$

Пусть $B \in \prod\limits_{i=1}^{n} \pi(K, I_i)$ и $B_{n+1} \in \pi(K, I_{n+1})$. Тогда $B = \prod\limits_{i=1}^{m} I_i + a_1$ и $B_{n+1} = I_{n+1} + a_2$, где $a, b \in K$ – фиксированные элементы.

Из равенства $\prod\limits_{i=1}^{n} I_i + I_{n+1} = K$ вытекает, что существуют такие элементы $\alpha_1 \in \prod\limits_{i=1}^{n} I_i$ и $\alpha_2 \in I_{n+1}$, что $a_1 - a_2 = \alpha_2 - \alpha_1$. Следовательно, $a_1 + \alpha_1 = \alpha_2 + a_2$.

Так как $\alpha_1 \in \prod\limits_{i=1}^{n} I_i$ и $\alpha_2 \in I_{n+1}$, то $\alpha_1 + a_1 \in B$ и $\alpha_2 + a_2 \in B_{n+1}$.

Из условий $\alpha_1 + a_1 \in B$, $\alpha_2 + a_2 \in B_{n+1}$ и $a_1 + \alpha_1 = \alpha_2 + a_2$ вытекает, что $B \cap B_{n+1} \neq \emptyset$, что и требовалось доказать.□

2.1.2. Основное равенство.

Пусть S – произвольное непустое множество, $\mathcal{K}$ – ассоциативно-коммутативное кольцо, а $I_1, \ldots, I_m \in \mathcal{I}_{\mathcal{K}}$ $(m \in \mathbb{N}; m \geq 2)$ – такие идеалы, что $\prod\limits_{i=1}^{r} I_i + I_{r+1} = K$ для всех $r = 1, \ldots, m-1$ и $\prod\limits_{i=1}^{h} I_i = \bigcap\limits_{i=1}^{h} I_i$ для всех $h = 2, \ldots, m$. Положим

$$F_{I_i}(S) = \{f | f : S \to \pi(K, I_i)\} \ (i = 1, \ldots m) \tag{2.14}$$

и

$$F(S) = \left\{ f \middle| f : S \to \pi\left(K, \prod_{i=1}^{m} I_i\right) \right\}. \tag{2.15}$$

Замечание 2.3. Из равенства $\prod\limits_{i=1}^{m} I_i = \bigcap\limits_{i=1}^{m} I_i$ вытекает (см. следствие 2.2), что $\pi\left(K, \prod\limits_{i=1}^{m} I_i\right) = \prod\limits_{i=1}^{m} \pi(K, I_i)$, т.е. $F(S) = \left\{ f \middle| f : S \to \prod\limits_{i=1}^{m} \pi(K, I_i) \right\}$.

Зафиксируем подмножества отображений

$$\widehat{F}_{I_i}(S) \subseteq F_{I_i}(S) \ (i = 1, \ldots m)$$

и положим

$$\widetilde{F}_{I_i}(S) = \{f \in F(S) | f_{I_i} \in \widehat{F}_{I_i}(S)\} \ (i = 1, \ldots m),$$

где отображение f_{I_i} $(i = 1, \ldots m)$ определяется следующим образом: если $f(s) = B$ $(s \in S)$ (где $B \in \prod\limits_{i=1}^{m} \pi(K, I_i)$), то $f_{I_i}(s) = B'$, где B' – такой (единственный) блок разбиения $\pi(K, I_i)$, что $B \subseteq B'$.

Теорема 2.2. Для каждого ассоциативно-коммутативного кольца $\mathcal{K} = (K, +, \cdot)$, каждого непустого множества S и каждого числа $m \in \mathbb{N}$ $(m \geq 2)$ равенство

$$|\widehat{F}_{I_1}(S) \times \cdots \times \widehat{F}_{I_m}(S)| = \left| \bigcap_{i=1}^{m} \widetilde{F}_{I_i}(S) \right| \tag{2.16}$$

истинно для любых таких идеалов $I_1, \ldots, I_m \in \mathcal{I}_{\mathcal{K}}$, что $\prod\limits_{i=1}^{r} I_i + I_{r+1} = K$ для всех $r = 1, \ldots, m-1$ и $\prod\limits_{i=1}^{h} I_i = \bigcap\limits_{i=1}^{h} I_i$ для всех $h = 2, \ldots, m$.□

Доказательство. Предположим, что $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо, $m \in \mathbb{N}$ $(m \geq 2)$, а $I_1, \ldots, I_m \in \mathcal{I}_{\mathcal{K}}$ $(m \in \mathbb{N}, m \geq 2)$ – такие идеалы, что истинны равенства $\prod\limits_{i=1}^{r} I_i + I_{r+1} = K$ $(r = 1, \ldots, m-1)$ и $\prod\limits_{i=1}^{h} I_i = \bigcap\limits_{i=1}^{h} I_i$ $(h = 2, \ldots, m)$.

Для доказательства равенства (2.16) достаточно построить инъекции

$$\varphi : \widehat{F}_{I_1}(S) \times \cdots \times \widehat{F}_{I_m}(S) \to \bigcap_{i=1}^{m} \widetilde{F}_{I_i}(S) \tag{2.17}$$

и

$$\psi : \bigcap_{i=1}^{m} \widetilde{F}_{I_i}(S) \to \widehat{F}_{I_1}(S) \times \cdots \times \widehat{F}_{I_m}(S). \tag{2.18}$$

Построим инъекцию φ.

Для каждого элемента $\mathbf{f} = (f_1, \ldots f_m) \in \widehat{F}_{I_1}(S) \times \cdots \times \widehat{F}_{I_m}(S)$ положим $\varphi(\mathbf{f}) = f$, где отображение f определяется равенством

$$f(s) = \bigcap_{i=1}^{m} f_i(s) \ (s \in S). \tag{2.19}$$

Из теоремы 2.1 вытекает, что $f \in F(S)$.

Докажем, что отображение (2.19) является отображением вида (2.17).

Из (2.19) вытекает, что $f_{I_i}(s) = f_i(s)$ $(i = 1, \ldots, m)$ для всех $s \in S$, т.е. $f_{I_i} = f_i \in \widehat{F}_{I_i}(S)$ для всех $i = 1, \ldots, m$.

Следовательно, $f \in \widetilde{F}_{I_i}(S)$ для всех $i = 1, \ldots, m$, т.е. $f \in \bigcap\limits_{i=1}^{m} \widetilde{F}_{I_i}(S)$, что и требовалось доказать.

Докажем, что отображение (2.19) инъекция.

Пусть $\mathbf{f}_r = (f_1^{(r)}, \dots f_m^{(r)}) \in \widehat{F}_{a_1}(S) \times \dots \times \widehat{F}_{a_m}(S)$ $(r = 1, 2)$ и $\mathbf{f}_1 \neq \mathbf{f}_2$. Докажем, что $\varphi(\mathbf{f}_1) \neq \varphi(\mathbf{f}_2)$.

Так как $\mathbf{f}_1 \neq \mathbf{f}_2$, то существует такое $j \in \mathbb{N}_m$, что $f_j^{(1)} \neq f_j^{(2)}$.

Следовательно, существует такой элемент $s \in S$, что $f_j^{(1)}(s) \neq f_j^{(2)}(s)$, т.е. $f_j^{(1)}(s)$ и $f_j^{(2)}(s)$ – различные блоки разбиения $\pi(K, I_j)$. Отсюда вытекает, что $\bigcap\limits_{i=1}^{m} f_i^{(1)}(s)$ и $\bigcap\limits_{i=1}^{m} f_i^{(2)}(s)$ – различные блоки разбиения $\prod\limits_{i=1}^{m} \pi(K, I_i)$.

Так как

$$\varphi(\mathbf{f}_1)(s) = \bigcap_{i=1}^{m} f_i^{(1)}(s) \neq \bigcap_{i=1}^{m} f_i^{(2)}(s) = \varphi(\mathbf{f}_2)(s)$$

то $\varphi(\mathbf{f}_1) \neq \varphi(\mathbf{f}_2)$, что и требовалось доказать.

Построим инъекцию ψ.

Для любого $f \in \bigcap\limits_{i=1}^{m} \widetilde{F}_{I_i}(S)$ положим

$$\psi(f) = (f_{I_1}, \dots, f_{I_m}). \tag{2.20}$$

Из (2.20) непосредственно вытекает, что для любого $f \in \bigcap\limits_{i=1}^{m} \widetilde{F}_{I_i}(S)$ равенство $f(s) = \bigcap\limits_{i=1}^{m} f_{I_i}(s)$ истинно для всех $s \in S$.

Докажем, что отображение (2.20) является отображением вида (2.18).

Так как $f \in \bigcap\limits_{i=1}^{m} \widetilde{F}_{I_i}(S)$, то $f \in \widetilde{F}_{I_i}(S)$ для всех $i = 1, \dots, m$.

Следовательно, $f_{I_i} \in \widehat{F}_{I_i}(S)$ для всех $i = 1, \dots, m$. Отсюда вытекает, что $(f_{I_1}, \dots, f_{I_m}) \in \widehat{F}_{I_1}(S) \times \dots \times \widehat{F}_{I_m}(S)$, что и требовалось доказать.

Докажем, что отображение (2.20) инъекция.

Пусть $f^{(1)}, f^{(2)} \in \bigcap\limits_{i=1}^{m} \widetilde{F}_{I_i}(S)$ и $f^{(1)} \neq f^{(2)}$. Докажем, что

$$\psi(f^{(1)}) = (f_{I_1}^{(1)}, \dots, f_{I_m}^{(1)}) \neq (f_{I_1}^{(2)}, \dots, f_{I_m}^{(2)}) = \psi(f^{(2)}).$$

Так как $f^{(1)} \neq f^{(2)} \left(f^{(1)}, f^{(2)} \in \bigcap\limits_{i=1}^{m} \widetilde{F}_{I_i}(S) \right)$, то существует такой элемент $s \in S$, что $f^{(1)}(s) \neq f^{(2)}(s)$, т.е. элементы $f^{(1)}(s)$ и $f^{(2)}(s)$ принадлежат разным блокам $B^{(1)}$ и $B^{(2)}$ разбиения $\prod\limits_{i=1}^{m} \pi(K, I_i)$. Следовательно,

$$\bigcap_{i=1}^{m} f_{I_i}^{(1)}(s) = f^{(1)}(s) \neq f^{(2)}(s) = \bigcap_{i=1}^{m} f_{I_i}^{(2)}(s).$$

Отсюда вытекает, что существует такое $j \in \mathbb{N}_m$, что $f^{(1)}_{I_j}(s) \neq f^{(2)}_{I_j}(s)$, т.е. $f^{(1)}_{I_j} \neq f^{(2)}_{I_j}$.

Так как $f^{(1)}_{I_j} \neq f^{(2)}_{I_j}$, то $\psi(f^{(1)}) \neq \psi(f^{(2)})$, что и требовалось доказать.$\square$

Если $\widehat{F}_{I_i}(S)$ $(i = 1, \ldots, m)$ – конечные множества, то равенство (2.16) естественно записать в виде

$$\prod_{i=1}^{m} |\widehat{F}_{I_i}(S)| = \left| \bigcap_{i=1}^{m} \widetilde{F}_{I_i}(S) \right|. \tag{2.21}$$

При этом из доказательства теоремы 2.2 непосредственно вытекает, что истинно следующее следствие.

Следствие 2.3. Если $\widehat{F}_{a_i}(S)$ $(i = 1, \ldots, m)$ – конечные множества, то отображения

$$\varphi : \widehat{F}_{I_1}(S) \times \cdots \times \widehat{F}_{I_m}(S) \to \bigcap_{i=1}^{m} \widetilde{F}_{I_i}(S)$$

и

$$\psi : \bigcap_{i=1}^{m} \widetilde{F}_{I_i}(S) \to \widehat{F}_{I_1}(S) \times \cdots \times \widehat{F}_{I_m}(S),$$

построенные в процессе доказательства теоремы 2.2, являются взаимно-обратными биекциями, т.е. $\varphi^{-1} = \psi$ и $\psi^{-1} = \varphi$.$\square$

Отметим, что именно равенство (2.21) и является основой для построения комбинаторных схем, предназначенных для для подсчета числа комбинаторных объектов, построенных в терминах ассоциативно-коммутативных колец.

Рассмотрим детализацию полученных результатов для ассоциативно-коммутативных колец с единицей.

Пусть $\mathcal{K} = (K, +, \cdot)$ – произвольное ассоциативно-коммутативное кольцо с единицей.

Собственные идеалы $I_1, \ldots, I_m \in \mathcal{I}_\mathcal{K}$ $(m \in \mathbb{N}, m \geq 2)$ называются *попарно комаксимальными*, если равенство $I_i + I_j = K$ истинно для всех $i, j = 1, \ldots, m$ $(i \neq j)$.

Следствие 2.4. Если $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо с единицей, то для каждого непустого множества S и каждого числа $m \in \mathbb{N}$ $(m \geq 2)$ равенство (2.16) истинно для любых попарно комаксимальных идеалов $I_1, \ldots, I_m \in \mathcal{I}_\mathcal{K}$.$\square$

Доказательство. Если $I_1, \ldots, I_m \in \mathcal{I}_{\mathcal{K}}$ $(m \in \mathbb{N}, m \geq 2)$ – попарно комаксимальные идеалы, то (см., напр., [27]) $\prod\limits_{i=1}^{r} I_i + I_{r+1} = K$ для всех $r = 1, \ldots, m-1$ и $\prod\limits_{i=1}^{h} I_i = \bigcap\limits_{i=1}^{h} I_i$ для всех $h = 2, \ldots, m$.

Таким образом, в любом ассоциативно-коммутативном кольце с единицей для любых попарно комаксимальных идеалов $I_1, \ldots, I_m \in \mathcal{I}_{\mathcal{K}}$ $(m \in \mathbb{N}, m \geq 2)$ выполнены условия теоремы 2.2.

Отсюда вытекает, что равенство (2.16) истинно для любых попарно комаксимальных идеалов $I_1, \ldots, I_m \in \mathcal{I}_{\mathcal{K}}$, что и требовалось доказать.□

Пусть $\mathcal{K} = (K, +, \cdot)$ – произвольное кольцо главных идеалов. Элементы $a, b \in K \backslash (K^{inv} \cup \{0\})$ называются *взаимно простыми*, если идеалы (a) и (b) являются взаимно-простыми.

Замечание 2.4. Идеалы I_1 и I_2 называются *взаимно-простыми*, если их наибольший общий делитель (т.е. идеал, порожденный теоретико-множественным объединением идеалов I_1 и I_2) совпадает с множеством K.

Следствие 2.5. Пусть $\mathcal{K} = (K, +, \cdot)$ – кольцо главных идеалов. Тогда для каждого непустого множества S и каждого числа $m \in \mathbb{N}$ $(m \geq 2)$ равенство

$$|\widehat{F}_{(a_1)}(S) \times \cdots \times \widehat{F}_{(a_m)}(S)| = \left| \bigcap_{i=1}^{m} \widetilde{F}_{(a_i)}(S) \right|. \tag{2.22}$$

истинно для всех попарно взаимно простых элементов $a_1, \ldots, a_m \in K$.□

Доказательство. Так как $a_1, \ldots, a_m \in K$ $(m \in \mathbb{N}, m \geq 2)$ являются попарно взаимно простыми элементами, то $(a_1), \ldots, (a_m)$ – собственные идеалы кольца $\mathcal{K}$.

При этом (см., напр., [13]) равенство $(a_i) + (a_j) = K$ истинно для всех $i, j = 1, \ldots, m$ $(i \neq j)$. Следовательно, $(a_1), \ldots, (a_m)$ – попарно комаксимальные идеалы.

Из следствия 2.4 вытекает, что следствие 2.5 истинно, что и требовалось доказать.□

Если $\widehat{F}_{(a_i)}(S)$ $(i = 1, \ldots, m)$ – конечные множества, то (по аналогии с равенством (2.21)) равенство (2.22) естественно записать в виде

$$\prod_{i=1}^{m} |\widehat{F}_{(a_i)}(S)| = \left| \bigcap_{i=1}^{m} \widetilde{F}_{(a_i)}(S) \right|. \tag{2.23}$$

При использовании равенства (2.23) в процессе решения прикладных задач для попарно взаимно простых элементов $a_1, \ldots, a_m \in K$ коль-

ца главных идеалов $\mathcal{K} = (K, +, \cdot)$ удобнее рассматривать отображения, принадлежащие множествам $F_{(a_i)}(S)$ $(m \in \mathbb{N}, m \geq 2)$ и $F(S)$, как отображения множества S в множество K.

Переопределим множества $F_{(a_i)}(S)$ $(m \in \mathbb{N}, m \geq 2)$ и $F(S)$ следующим образом.

Зафиксировав в каждом блоке разбиения $\pi(K, (a))$ $(a \in K)$ по одному элементу, получим *полную систему вычетов* $\mathrm{MOD}(a)$ по модулю a. Обозначим через $b < \mathrm{mod}\, a > (a, b \in K)$ такой единственный элемент $c \in \mathrm{MOD}(a)$, что элементы b и c принадлежат одному и тому же блоку разбиения $\pi(K, (a))$.

Пусть S – произвольное множество, а $a_1, \ldots, a_m$ $(m \in \mathbb{N}, m \geq 2)$ – попарно взаимно простые элементы кольца главных идеалов $\mathcal{K} = (K, +, \cdot)$. Положим

$$F_{(a_i)}(S) = \{f | f : S \to \mathrm{MOD}(a_i)\} \ (i = 1, \ldots m) \tag{2.24}$$

и

$$F(S) = \left\{ f \middle| f : S \to \mathrm{MOD}\left(\prod_{i=1}^{m} a_i\right) \right\}. \tag{2.25}$$

Нетрудно убедиться в том, что для любых попарно взаимно простых элементов $a_1, \ldots, a_m$ $(m \in \mathbb{N}, m \geq 2)$ кольца главных идеалов $\mathcal{K} = (K, +, \cdot)$ определение множеств $F_{(a_i)}(S)$ $(m \in \mathbb{N}, m \geq 2)$ и $F(S)$ формулами, соответственно, (2.24) и (2.25) эквивалентно определению этих множеств формулами, соответственно, (2.14) и (2.15).

Пусть $\mathcal{K} = (K, +, \cdot)$ – произвольное дедекиндово кольцо. Элементы $a, b \in K \backslash (K^{inv} \cup \{0\})$ назовем *взаимно простыми*, если $(a) + (b) = K$.

Следствие 2.6. Если $\mathcal{K} = (K, +, \cdot)$ – дедекиндово кольцо, то для каждого непустого множества S, каждого числа $m \in \mathbb{N}$ $(m \geq 2)$ равенство (2.22) истинно для всех попарно взаимно простых элементов $a_1, \ldots, a_m \in K$.□

Доказательство аналогично доказательству следствия 2.5.

В дальнейшем для упрощения обозначений вместо $F_{(a)}(S)$, $\widehat{F}_{(a)}(S)$ и $\widetilde{F}_{(a)}(S)$ будем писать, соответственно $F_a(S)$, $\widehat{F}_a(S)$ и $\widetilde{F}_a(S)$. При этом равенство (2.23) будем записывать в виде

$$\prod_{i=1}^{m} |\widehat{F}_{a_i}(S)| = \left| \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S) \right|. \tag{2.26}$$

2.1.3. Решение модельных задач.

Рассмотрим применение равенства (2.26) для решения модельных алгебраических задач.

Пример 2.1. Предположим, что кольцо $\mathcal{K} = (K, +, \cdot)$ является кольцом главных идеалов или дедекиндовым кольцом, а $a_1, \ldots, a_m \in K$ $(m \in \mathbb{N}, m \geq 2)$ являются попарно взаимно простыми элементами кольца $\mathcal{K}$.

В [45] установлен изоморфизм фактор-колец, специальным случаем которого является изоморфизм $\mathcal{K}/_{\equiv \prod\limits_{i=1}^{m}(a_i)} \leftrightarrow \prod\limits_{i=1}^{m} \mathcal{K}/_{\equiv(a_i)}$.

Пусть $|S| = 1$. Тогда множество $F_{a_i}(S)$ $(i = 1, \ldots, m)$ можно отождествить с множеством $\mathrm{MOD}(a_i)$.

Положив $\widehat{F}_{a_i}(S) = F_{a_i}(S)$ $(i = 1, \ldots, m)$, заключаем, что если $|S| = 1$, то равенство (2.26) устанавливает равномощность фактор-колец $\mathcal{K}/_{\equiv \prod\limits_{i=1}^{m}(a_i)}$ и $\prod\limits_{i=1}^{m} \mathcal{K}/_{\equiv(a_i)}$, а отображения φ и $\psi = \varphi^{-1}$, построенные при доказательстве теоремы 2.2, устанавливают изоморфизм этих фактор-колец.

Пример 2.2. Предположим, что кольцо $\mathcal{K} = (K, +, \cdot)$ является кольцом главных идеалов или дедекиндовым кольцом, $a_1, \ldots, a_m$ $(m \in \mathbb{N}, m \geq 2)$ являются попарно взаимно простыми элементами кольца $\mathcal{K}$, а $|S| = 1$.

Зафиксируем произвольные элементы $b_1, \ldots, b_m \in K$ кольца $\mathcal{K}$ и положим $\widehat{F}_{a_i}(S) = \{f_i\}$ $(i = 1, \ldots, m)$, где $f_i(s) = b_i < \mathrm{mod}\, a_i >$ $(i = 1, \ldots, m)$.

В рассматриваемом случае равенство (2.26) принимает вид

$$\left| \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S) \right| = 1.$$

При этом $f \in \bigcap\limits_{i=1}^{m} \widetilde{F}_{a_i}(S)$ представляет собой такое отображение, что $f(s)$ – это такой единственный элемент $c \in \mathrm{MOD}\left(\prod\limits_{i=1}^{m} a_i\right)$, что $c = b_i < \mathrm{mod}\, a_i >$ для всех $i = 1, \ldots, m$.

Таким образом, показано, что система сравнений

$$x \equiv b_i \ (\mathrm{mod}\ (a_i)) \ \ (i = 1, \ldots, m)$$

имеет единственное решение, принадлежащее множеству $\mathrm{MOD}\left(\prod\limits_{i=1}^{m} a_i\right)$, т.е. доказан вариант китайской теоремы об остатках для кольца $\mathcal{K}$.

Пример 2.3. Обратимые матрицы над кольцом $\mathcal{Z}_n = (\mathbb{Z}_n, \oplus, \circ)$ $(n \in \mathbb{N}, n \geq 2)$ играют важную роль при поиске множеств решений некоторых систем (в том числе и нелинейных) уравнений над этим кольцом. Кроме того, в [66,67,80] показано, что в терминах таких матриц могут быть охарактеризованы основные нетривиальные множества обратимых автоматов над кольцом $\mathcal{Z}_n$. Таким образом, число обратимых матриц над кольцом $\mathcal{Z}_n$ используется при оценке мощности достаточно широкого класса множеств объектов, определенных в терминах кольца $\mathcal{Z}_n$ $(n \in \mathbb{N}, n \geq 2)$.

В [67] предложена следующая схема подсчета числа обратимых $l \times l$-матриц над кольцом $\mathcal{Z}_n$ ($n \in \mathbb{N}, n \geq 2$).

Обозначим через $\mathsf{M}_l(p,k)$ (где p – простое число, а $k \in \mathbb{N}$) множество всех $l \times l$-матриц над кольцом $\mathcal{Z}_{p^k}$, а через $\mathsf{M}_l^{inv}(p,k)$ – множество всех обратимых матриц $A \in \mathsf{M}_l(p,k)$. Ясно, что

$$|\mathsf{M}_l(p,k)| = p^{kl^2}. \tag{2.27}$$

Лемма 2.2. Для любого простого числа p равенство

$$|\mathsf{M}_l^{inv}(p,1)| = |\mathsf{M}_l(p,1)| \prod_{i=1}^{l}(1-p^{-l}) \tag{2.28}$$

истинно для всех $l \in \mathbb{N}$.□

Доказательство. Зафиксируем простое число p и число $l \in \mathbb{N}$.

Так как $\mathcal{Z}_p = \mathcal{GF}(p)$, то $A = [\mathbf{a}_1, \ldots, \mathbf{a}_l] \in \mathsf{M}_l^{inv}(p,1)$ (где $\mathbf{a}_i \in \mathbb{Z}_p^l$ $(i = 1, \ldots, l)$) тогда и только тогда, когда $\mathbf{a}_1$ – ненулевой вектор-столбец и для всех $i = 2, \ldots, l$ вектор-столбец $\mathbf{a}_i$ не является линейной комбинацией вектор-столбцов $\mathbf{a}_1, \ldots, \mathbf{a}_{i-1}$.

Так как число линейных комбинаций векторов $\mathbf{a}_1, \ldots, \mathbf{a}_{i-1}$ $(i = 2, \ldots, l)$ равно p^{i-1}, то

$$|\mathsf{M}_l^{inv}(p,1)| = (p^l - 1)(p^l - p)\ldots(p^l - p^{l-1}) = p^{l^2}\prod_{i=1}^{l}(1-p^{-i}). \tag{2.29}$$

Положив $k = 1$ в (2.27), получим

$$|\mathsf{M}_l(p,1)| = p^{l^2}. \tag{2.30}$$

Из (2.29) и (2.30) вытекает, что равенство (2.28) истинно.□

Лемма 2.3. Для любого простого числа p и любого числа $k \in \mathbb{N}$ $(k \geq 2)$ равенство

$$|\mathsf{M}_l^{inv}(p,k)| = |\mathsf{M}_l(p,k)| \prod_{i=1}^{l}(1-p^{-i}) \tag{2.31}$$

истинно для всех $l \in \mathbb{N}$.□

Доказательство. Зафиксируем простое число p и числа $k, l \in \mathbb{N}$ $(k \geq 2)$.

Любая матрица $A \in \mathsf{M}_l^{inv}(p,k)$ может быть представлена в виде $A = B \oplus C$, где $B \in \mathsf{M}_l^{inv}(p,1)$, а C – $l \times l$-матрица над кольцом $\mathcal{Z}_{p^k}$, все элементы которой – необратимые элементы кольца $\mathcal{Z}_{p^k}$. При этом, $\det(A)\ (mod\ p) = \det B\ (mod\ p)$. Кроме того, если $B_1 \neq B_2$ $(B_1, B_2 \in \mathsf{M}_l(p,1))$, то $B_1 + C_1 \neq B_2 + C_2$ для любых матриц $C_1, C_2 \in \mathsf{M}_l(p,k)$, каждый элемент которых – необратимый элемент кольца $\mathcal{Z}_{p^k}$.

Следовательно, число $|\mathsf{M}_l^{inv}(p,k)|$ равно числу матриц $B + C$, где $B \in \mathsf{M}_l^{inv}(p,1)$, а C – $l \times l$-матрица над кольцом $\mathcal{Z}_{p^k}$, все элементы которой – необратимые элементы кольца $\mathcal{Z}_{p^k}$. Число таких матриц C равно $p^{(k-1)l^2}$.

Поэтому, принимая во внимание равенства (2.29) и (2.27), получим, что

$$|\mathsf{M}_l^{inv}(p,k)| = p^{l^2}\prod_{i=1}^{l}(1-p^{-i})p^{(k-1)l^2} = p^{kl^2}\prod_{i=1}^{l}(1-p^{-i}) = |\mathsf{M}_l(p,k)|\prod_{i=1}^{l}(1-p^{-i}),$$

что и требовалось доказать.□

Следствие 2.7. Для любого простого числа p равенство

$$|\mathsf{M}_l^{inv}(p,k)| = |\mathsf{M}_l(p,k)| \prod_{i=1}^{l}(1-p^{-i}) \ (k \in \mathbb{N}) \tag{2.32}$$

истинно для всех $l \in \mathbb{N}$.□

Доказательство. Если $k = 1$, то равенство (2.32) совпадает с равенством (2.28). При $k \in \mathbb{N}$ $(k \geq 2)$ равенство (2.32) совпадает с равенством (2.31).□

Обозначим через $\mathsf{M}_l^{inv}(n)$ множество всех обратимых $l \times l$-матриц над кольцом $\mathcal{Z}_n = (\mathbb{Z}_n, \oplus, \circ)$, где $n = p_1^{k_1} \dots p_m^{k_m}$ $(m \geq 2)$, $p_1, \dots, p_m$ – попарно-различные простые числа, а $k_1, \dots, k_m \in \mathbb{N}$.

Теорема 2.3. Для каждого числа $n = p_1^{k_1} \dots p_m^{k_m}$ $(m \geq 2)$, где $p_1, \dots, p_m$ – попарно-различные простые числа, а $k_1, \dots, k_m \in \mathbb{N}$ равенство

$$|\mathsf{M}_l^{inv}(n)| = \left(\prod_{j=1}^{m} |\mathsf{M}_l(p_j,k_j)|\right) \prod_{j=1}^{m}\prod_{i=1}^{l}(1-p_j^{-i}) \tag{2.33}$$

истинно для всех $l \in \mathbb{N}$.□

Доказательство. Выберем в качестве дедекиндового кольца $\mathcal{K}$ кольцо целых чисел $\mathcal{Z} = (\mathbb{Z}, +, \cdot)$, а в качестве множества S выберем множество, состоящее из l^2 элементов.

Ясно, что в рассматриваемом случае множество отображений $F_{p_j^{k_j}}(S)$ $(j = 1, \dots, m)$ может быть отождествлено с множеством матриц $\mathsf{M}_l(p_j, k_j)$.

Выберем в качестве множества отображений $\widehat{F}_{p_j^{k_j}}(S)$ $(j = 1, \dots, m)$ множество всех матриц $\mathsf{M}_l^{inv}(p_j, k_j)$.

Тогда множество $\widetilde{F}_{p_j^{k_j}}(S)$ $(j = 1, \dots, m)$ состоит из всех $l \times l$-матриц над кольцом $\mathcal{Z}_n$, определитель которых не сравним с нулем по модулю p_j.

Следовательно,

$$\mathsf{M}_l^{inv}(n) = \bigcap_{j=1}^{m} \widetilde{F}_{p_i^{k_i}}(S). \tag{2.34}$$

Из равенства (2.32) вытекает, что

$$|\widehat{F}_{p_j^{k_j}}(S)| = |\mathsf{M}_l(p_j,k_j)| \prod_{i=1}^{l}(1-p_j^{-i}). \tag{2.35}$$

Из равенств (2.26), (2.34) и (2.35) вытекает, что

$$|\mathsf{M}_l^{inv}(n)| = \left|\bigcap_{j=1}^{m} \widetilde{F}_{p_j^{k_j}}(S)\right| = \prod_{j=1}^{m} |\widehat{F}_{p_j^{k_j}}(S)| =$$

$$= \prod_{j=1}^{m}\left(|\mathsf{M}_l(p_j,k_j)| \prod_{i=1}^{l}(1-p_j^{-i})\right) = \left(\prod_{j=1}^{m} |\mathsf{M}_l(p_j,k_j)|\right) \prod_{j=1}^{m}\prod_{i=1}^{l}(1-p_j^{-i}),$$

что и требовалось доказать.□

2.2. Интерпретация исследуемой модели для кольца $\mathcal{Z}$.

Пусть в качестве дедекиндового кольца $\mathcal{K}$ выбрано кольцо целых чисел $\mathcal{Z} = (\mathbb{Z}, +, \cdot)$, а в качестве множества S выбрано одноэлементное множество. Построим наглядную «геометрическую» модель, представляющую равенство (2.26).

2.2.1. Ленточная модель.

Зафиксируем попарно взаимно простые числа $a_1, \ldots, a_m \in \mathbb{N}\backslash\{1\}$ $(m \in \mathbb{N})$. Положим $\mathrm{MOD}(a_i) = \{0, 1, \ldots, a_i - 1\}$ $(i = 1, \ldots, m)$.

Выберем любые такие неотрицательные целые числа $b_1, \ldots, b_m$, что $b_i \leq a_i$ для всех $i = 1, \ldots, m$. Пусть $|\widehat{F}_{a_i}(S)| = b_i$ $(i = 1, \ldots, m)$. Тогда равенство (2.26) принимает следующий вид

$$\left|\bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S)\right| = \prod_{i=1}^{m} b_i. \tag{2.36}$$

Равенство (2.36) имеет содержательную интерпретацию в терминах следующей «геометрической» модели, впервые исследованной в [68], которую назовем ленточной моделью.

Под *лентой* будем понимать одностороннюю бесконечную вправо ленту, разбитую на клетки, занумерованные неотрицательными целыми числами. Расположив $m + 1$ лент одну над другой, занумеруем их сверху вниз неотрицательными целыми числами. Ленты с номерами $1, \ldots, m$ назовем *рабочими*, а ленту с номером 0 – *результирующей*.

Осуществим разметку лент маркером в соответствии со следующими тремя правилами.

Правило 2.1. Среди первых a_i $(i = 1, \ldots, m)$ клеток рабочей ленты с номером i отметим маркером те и только те b_i клеток, номера которых являются значениями отображений, принадлежащих множеству $\widehat{F}_{a_i}(S)$.

Правило 2.2. На рабочей ленте с номером i $(i = 1, \ldots, m)$ клетка с номером h $(h \geq a_i)$ отмечена маркером тогда и только тогда, когда маркером отмечена клетка с номером $h <\mathrm{mod}\, a_i>$ этой ленты.

Замечание 2.5. В кольце целых чисел $\mathcal{Z} = (\mathbb{Z}, +, \cdot)$ для любого фиксированного числа $a \in \mathbb{N}$ равенство $h <\mathrm{mod}\, a >= h\ (mod\, a)$ истинно для всех чисел $h \in \mathbb{Z}_+$.

Правило 2.3. На результирующей ленте клетка с номером j $(j \in \mathbb{Z}_+)$ отмечена маркером тогда и только тогда, когда на каждой рабочей ленте клетка с номером j отмечена маркером.

Замечание 2.6. Из правил 2.1-2.3 вытекает, что все многообразие разметок лент определяется выбором семейства множеств отображений $\widehat{F}_{a_i}(S)$ $(i = 1, \ldots, m)$.

Обозначим через $\mathtt{L}_i$ $(i = 0, 1, \ldots, m)$ начальный отрезок ленты с номером i, состоящий из первых $\prod\limits_{i=1}^{m} a_i$ клеток.

Назовем *ленточной моделью* упорядоченный набор лент

$$(\mathtt{L}_0; \mathtt{L}_1, \ldots, \mathtt{L}_m). \tag{2.37}$$

Из (2.36) вытекает, что в терминах ленточной модели формулировка равенства (2.26) имеет следующий вид.

Теорема 2.4. (*Ленточная теорема*). Для любых попарно взаимно простых чисел $a_1, \ldots, a_m \in \mathbb{N}\backslash\{1\}$ $(m \in \mathbb{N})$ при любых таких неотрицательных целых числах $b_1, \ldots, b_m$, что $b_i \leq a_i$ для всех $i = 1, \ldots, m$, в точности $\prod\limits_{i=1}^{m} b_i$ клеток результирующей ленты $\mathtt{L}_0$ отмечено маркером.□

Замечание 2.7. В [68] ленточная модель исследована непосредственно, без использования разработанного в предыдущем пункте математического аппарата. Содержащееся в [68] ad hoc доказательство теоремы 2.2 достаточно длинное, громоздкое, основано на комбинации метода решета и индукции по числу рабочих лент.

2.2.2. Решение модельных задач.

Проиллюстрируем применение ленточной модели при решении модельных теоретико-числовых задач.

Пример 2.4. Пусть φ – функции Эйлера, т.е. $\varphi(1) = 1$ и $\varphi(n)$ $(n \in \mathbb{N}\backslash\{1\})$ – это количество натуральных чисел, меньших числа n, и взаимно простых с числом n.

Докажем следующее свойство мультипликативности функции φ: для любых взаимно простых чисел $k_1, k_2 \in \mathbb{N}\backslash\{1\}$ истинно равенство

$$\varphi(k_1 k_2) = \varphi(k_1)\varphi(k_2).$$

Положив $m = 2$ в (2.37), построим такую ленточную модель

$$(\mathtt{L}_0; \mathtt{L}_1, \mathtt{L}_2),$$

что $a_i = k_i$ $(i = 1, 2)$, а множество $\widehat{F}_{a_i}(S)$ $(i = 1, 2)$ состоит из всех отображений $f \in F_{a_i}(S)$, значением которых является число, взаимно простое с числом a_i.

Для построенной модели

$$b_i = \varphi(a_i) \ (i = 1, 2),$$

а среди первых a_i $(i = 1, 2)$ клеток рабочей ленты $\mathtt{L}_i$ маркером отмечены те и только те b_i клеток, номерами которых являются числа, взаимно простые с числом a_i.

Так как a_1 и a_2 – взаимно простые числа, то число $a \in \mathbb{N}$ взаимно просто с произведением $a_1 a_2$ тогда и только тогда, когда оно взаимно просто с каждым из чисел a_1 и a_2.

Следовательно, клетка результирующей ленты $\mathtt{L}_0$ отмечена маркером тогда и только тогда, когда ее номер – число, взаимно простое с произведением a_1a_2.

Отсюда вытекает, что число клеток результирующей ленты $\mathtt{L}_0$, отмеченных маркером, равно $\varphi(a_1a_2)$.

Применяя ленточную теорему, получим, что

$$\varphi(k_1k_2) = \varphi(a_1a_2) = b_1b_2 = \varphi(k_1)\varphi(k_2),$$

что и требовалось доказать.

Пример 2.5. Пусть φ – функции Эйлера.

Докажем формулу Эйлера: если $n = p_1^{k_1} \dots p_m^{k_m}$ $(n \in \mathbb{N}\backslash\{1\})$ – каноническое разложение числа n, то

$$\varphi(n) = n\prod_{i=1}^{m}(1 - p_i^{-1}). \tag{2.38}$$

По условию, числа $p_1^{k_1}, \dots, p_m^{k_m}$ являются взаимно простыми.

Построим такую ленточную модель (2.37), что $a_i = p_i^{k_i}$ $(i = 1, \dots, m)$, а множество $\widehat{F}_{a_i}(S)$ $(i = 1, \dots, m)$ состоит из всех отображений $f \in F_{a_i}(S)$, значением которых является число, взаимно простое с числом a_i.

Для построенной модели

$$b_i = \varphi(a_i) \ (i = 1, \dots, m),$$

а среди первых a_i $(i = 1, \dots, m)$ клеток рабочей ленты $\mathtt{L}_i$ маркером отмечены те и только те b_i клеток, номера которых – числа, взаимно простые с числом a_i.

Так как $a_1, \dots, a_m$ – взаимно простые числа, то число $a \in \mathbb{N}$ взаимно просто с произведением $\prod\limits_{i=1}^{m} a_i$ тогда и только тогда, когда оно взаимно просто с каждым из чисел $a_1, \dots, a_m$.

Следовательно, клетка результирующей ленты $\mathtt{L}_0$ отмечена маркером тогда и только тогда, когда ее номер – число, взаимно простое с произведением $\prod\limits_{i=1}^{m} a_i$.

Отсюда вытекает, что число клеток результирующей ленты $\mathtt{L}_0$, отмеченных маркером, равно $\varphi(\prod\limits_{i=1}^{m} a_i)$.

Применяя ленточную теорему, получим, что

$$\varphi(n) = \varphi\left(\prod_{i=1}^{m} a_i\right) = \prod_{i=1}^{m} b_i = \prod_{i=1}^{m} \varphi(p_i^{k_i}). \tag{2.39}$$

Воспользовавшись в (2.39) равенствами

$$\varphi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i-1} \ (i = 1, \dots, m),$$

получим

$$\varphi(n) = \prod_{i=1}^{m}(p_i^{k_i} - p_i^{k_i-1}) = \left(\prod_{i=1}^{m} p_i^{k_i}\right)\prod_{i=1}^{m}(1 - p_i^{-1}) = n\prod_{i=1}^{m}(1 - p_i^{-1}),$$

т.е. равенство (4.11) истинно.

Пример 2.6. Докажем следующий вариант китайской теоремы об остатках: если числа $k_1, \dots k_m \in \mathbb{N}\backslash\{1\}$ являются попарно взаимно простыми числами, то для любых чисел $c_1, \dots, c_m \in \mathbf{Z}$ система сравнений

$$x \equiv c_i \ (mod\ k_i) \ \ (i = 1, \dots, m) \tag{2.40}$$

имеет единственное решение по модулю $\prod\limits_{i=1}^{m} k_i$.

Обозначив через r_i $(i = 1, \dots, m)$ остаток от деления числа c_i на число k_i, перейдем от системы сравнений (2.40) к эквивалентной системе сравнений

$$x \equiv r_i \ (mod\ k_i) \ \ (i = 1, \dots, m). \tag{2.41}$$

Построим такую ленточную модель (2.37), что $a_i = k_i$ $(i = 1, \dots, m)$, а множество $\widehat{F}_{a_i}(S)$ $(i = 1, \dots, m)$ состоит из единственного отображения $f \in F_{a_i}(S)$, значением которого является число r_i.

Для построенной модели

$$b_i = 1 \ \ (i = 1, \dots, m),$$

а среди первых a_i $(i = 1, \dots, m)$ клеток рабочей ленты $\mathtt{L}_i$ маркером отмечена единственная клетка, номер которой равен r_i.

Следовательно, клетка с номером j $(j = 0, 1, \dots, \prod\limits_{i=1}^{m} a_i - 1)$ результирующей ленты $\mathtt{L}_0$ отмечена маркером тогда и только тогда, когда число j сравнимо с каждым из чисел r_i $(i = 1, \dots, m)$ по модулю a_i.

Отсюда вытекает, что число j является решением системы сравнений (2.41), т.е. решением системы сравнений (2.40).

Применяя ленточную теорему, получим, что число решений системы сравнений (2.40) по модулю $\prod\limits_{i=1}^{m} k_i$ равно

$$\prod_{i=1}^{m} b_i = \prod_{i=1}^{m} 1 = 1,$$

что и требовалось доказать.

2.2.3. Об отсутствии одного обобщения исследуемой модели.

В формулировке теоремы 2.2 используется конечное множество идеалов ассоциативно-коммутативного кольца $\mathcal{K}$. Ленточная модель дает возможность достаточно просто доказать, что эта теорема не может быть непосредственно обобщена на бесконечное множество идеалов, т.е. что ложно следующее утверждение:

Утверждение 2.3. Для каждого ассоциативно-коммутативного кольца $\mathcal{K} = (K, +, \cdot)$ и каждого непустого множества S равенство

$$|\widehat{F}_{I_1}(S) \times \dots \times \widehat{F}_{I_m}(S) \times \dots| = \left| \bigcap_{i=1}^{\infty} \widetilde{F}_{I_i}(S) \right| \tag{2.42}$$

истинно для любой такой бесконечной последовательности $\{I_i\}_{i\in\mathbb{N}}$ попарно различных собственных идеалов кольца $\mathcal{K}$, что $\prod\limits_{i=1}^{r} I_i + I_{r+1} = K$ для всех $r \in \mathbb{N}$ и $\prod\limits_{i=1}^{h} I_i = \bigcap\limits_{i=1}^{h} I_i$ для всех $h \in \mathbb{N}$ $(h \geq 2)$.$\square$

Для того, чтобы доказать, что утверждение 2.3 не является истинным, достаточно доказать, что для обобщения ленточной модели на бесконечное число лент, т.е. для ленточной модели

$$(\mathtt{L}_0; \mathtt{L}_1, \ldots, \mathtt{L}_m, \ldots) \tag{2.43}$$

не является истинным следующее обобщение теоремы 2.4:

Утверждение 2.4. Для любой бесконечной последовательности попарно взаимно простых чисел $a_i \in \mathbb{N}\backslash\{1\}$ $(i \in \mathbb{N})$ и любой такой бесконечной последовательности неотрицательных целых чисел b_i $(i \in \mathbb{N})$, что $b_i \leq a_i$ для всех $i \in \mathbb{N}$ в точности $\prod\limits_{r=1}^{\infty} b_r$ клеток результирующей ленты $\mathtt{L}_0$ отмечено маркером.$\square$

Построим следующую обобщенную ленточную модель (2.43).

Зафиксируем бесконечную возрастающую последовательность попарно взаимно простых чисел $a_i \in \mathbb{N}\backslash\{1\}$ $(i \in \mathbb{N})$, а одноэлементные множества отображений $\widehat{F}_{a_i}(S)$ $(i \in \mathbb{N})$ выберем так, что:

1) $\widehat{F}_{a_1}(S) = \{f\}$, где f – любое отображение, принадлежащее множеству $F_{a_1}(S)$;

2) $\widehat{F}_{a_i}(S) = \{f\}$ $(i \geq 2)$, где f – любое такое отображение, принадлежащее множеству $F_{a_i}(S)$, что $a_{i-1} \leq f(s) < a_i$.

Так как $b_i = 1$ для всех $i \in \mathbb{N}$, то

$$\prod_{i=1}^{\infty} b_i = 1.$$

Покажем, что ни одна из клеток результирующей ленты $\mathtt{L}_0$ не отмечена маркером.

Предположим противное, т.е. что существует такое число $j \in \mathbb{Z}_+$, что клетка с номером j результирующей ленты отмечена маркером.

Так как $\{a_i\}_{i\in\mathbb{N}}$ – бесконечная возрастающая последовательность натуральных чисел, то существует такое число $i_0 \in \mathbb{N}$, что $a_{i_0} > j$.

Клетка с номером j рабочей ленты $\mathtt{L}_{i_0+1}$ не отмечена маркером. Следовательно, клетка с номером j результирующей ленты также не отмечена маркером. Получено противоречие.

Полученное противоречие показывает, что не является истинным предположение о том, что существует такое число $j \in \mathbb{Z}_+$, что клетка с номером j результирующей ленты отмечена маркером.

Следовательно, ни одна из клеток результирующей ленты не отмечена маркером, откуда вытекает,что утверждение 2.4 не является истинным, что и требовалось доказать.

2.3. Выводы.

В настоящем разделе исследованы множества отображений абстрактного множества в фактор-кольца ассоциативно-коммутативного кольца. Основные результаты состоят в следующем:

1. Построена и исследована комбинаторная схема, основанная на соотношении между множествами отображений абстрактного множества в полную систему вычетов по попарно взаимно простым идеалам ассоциативно-коммутативного кольца и множеством отображений этого же множества в полную систему вычетов по произведению этих идеалов.

2. Построена «ленточная модель», представляющая собой наглядную «геометрическую» интерпретацию предложенной схемы для кольца целых чисел.

3. Показана применимость предложенной схемы для решения модельных алгебраических и теоретико-числовых задач.

4. Доказано отсутствие непосредственного обобщения построенной комбинаторной схемы на бесконечное множество фактор-колец.

Полученные результаты показывают, что рассмотренные классы отображений абстрактных множеств в фактор-кольца ассоциативно-коммутативных колец дают возможность с единых позиций исследовать прикладные задачи, в которых применяются структуры, построенные в терминах этих колец. Класс таких прикладных задач определяется выбором ассоциативно-коммутативного кольца $\mathcal{K}$, а также выбором абстрактного множества S и множеств отображений $\widehat{F}_{I_i}(S)$ $(i = 1, \ldots, m)$.

Детальное исследование предложенной комбинаторной схемы при дополнительных ограничениях на множество идеалов I_i $(i = 1, \ldots, m)$ и/или на множества отображений $\widehat{F}_{I_i}(S)$ $(i = 1, \ldots, m)$ представляет собой возможное направление дальнейших исследований.

3. СИСТЕМЫ УРАВНЕНИЙ НАД КОЛЬЦАМИ

Широкий класс задач анализа объектов, определенных над кольцом, естественно сводится к исследованию множества решений системы уравнений с параметрами над этим кольцом. К таким задачам относится анализ строения алгебраических многообразий (в частности, алгебраических кривых), определенных над кольцом, а также построение (для конечных колец) таких многообразий в явном виде. Кроме того, как показано в [66,80], к таким задачам относится анализ структуры, анализ тех или иных аспектов поведения, а также задачи идентификации (параметрической и начального состояния) автоматно-алгебраических моделей, определенных системами уравнений над конечным кольцом. Как было отмечено ранее, именно автоматно-алгебраические модели в последнее время начинают интенсивно применяться при решении задач преобразования (в частности, задач защиты) информации.

Таким образом, разработка математического аппарата, предназначенного для исследования строения множества решений системы алгебраических уравнений с параметрами, определенной над кольцом, актуальна как с теоретической, так и с прикладной точки зрения.

В п.3.1 предложена общая схема исследования строения множества решений системы полиномиальных уравнений с параметрами над конечным ассоциативным кольцом $\mathcal{K}$ с единицей. В деталях рассмотрено применение этой схемы к анализу множества решений системы полиномиальных уравнений с параметрами над кольцом вычетов $\mathcal{Z}_{p^k}$. В п.3.2 исследованы свойства делителей нуля в ассоциативных кольцах (именно на основе эффективного использования этих свойств осуществляется анализ множества решений уравнений вида «произведение равно нулю»). П.3.3 содержит ряд заключительных замечаний.

Результаты автора, представленные в настоящем разделе, опубликованы в работах [66,70,72,80,82,83,102,210].

3.1. Анализ системы полиномиальных уравнений.

Решение систем линейных уравнений над полем $\mathcal{GF}(p^k)$ (где p – простое число, а $k \in \mathbb{N}$) не вызывает особых затруднений. Однако ситуация в корне изменяется при решении систем нелинейных уравнений над этим полем. Известно, что над полем $\mathcal{GF}(p^k)$ решение систем квадратных уравнений от многих переменных, даже в случае, когда $p = 2$, является NP-полной задачей (см., напр., [3]).

При этом, ни один метод решения систем полиномиальных уравнений над полем $\mathcal{GF}(p^k)$ не может быть непосредственно применен для решения систем полиномиальных уравнений над кольцом с делителями нуля.

Ситуация еще более усложняется при исследовании системы уравнений с параметрами, определенной над кольцом, так как в дополнение к сложности поиска множества решений появляется сложность представления этого множества (такая ситуация, например, типична для любого кольца $n \times n$-матриц ($n \geq 2$) над любым кольцом с единицей).

Таким образом, разработка схемы, предназначенной для унифицированного представления множества решений системы уравнений с параметрами, определенной над кольцом, является актуальной задачей. Рассмотрим решение этой задачи.

3.1.1. Постановка задачи.

Пусть над конечным ассоциативным кольцом $\mathcal{K} = (K, +, \cdot)$ с единицей задана система уравнений

$$\begin{cases} f_1(u_1, \ldots, u_n, a_1, \ldots, a_h) = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_m(u_1, \ldots, u_n, a_1, \ldots, a_h) = 0 \end{cases}, \tag{3.1}$$

где $f_1, \ldots, f_m$ $(m \in \mathbb{N})$ – многочлены над кольцом $\mathcal{K}$, $u_1, \ldots, u_n$ $(n \in \mathbb{N})$ – переменные, а $a_1, \ldots, a_h \in K$ $(h \in \mathbb{N})$ – параметры.

Обозначим через S множество решений системы уравнений (3.1).

Строение множества S может существенно зависеть от значений параметров $a_1, \ldots, a_h \in K$. Поэтому разработку схемы, предназначенной для унифицированного представления множества S, естественно осуществить так, чтобы были выполнены следующие три условия:

1) осуществляется построение такого конечного семейства $\{S_i\}_{i \in I}$ непустых множеств, что $S = \bigcup\limits_{i \in I} S_i$;

2) каждое множество S_i $(i \in I)$ представлено в неявном виде посредством теоретико-множественной формулы, построенной с учетом строения кольца $\mathcal{K}$;

3) сложность представления каждого множества S_i $(i \in I)$ в явном виде зависит, в основном, от строения кольца $\mathcal{K}$.

Отметим, что эти условия отражают внутреннюю сложность построения и хранения множества решений S системы уравнений (3.1).

Основная идея предлагаемого в настоящем разделе подхода к построению схемы, предназначенной для унифицированного представления множества S, состоит в следующем.

Известно, что для любого многочлена

$$f(x) = \sum_{i=0}^{k} a_i x^i \ (a_0, a_1, \ldots, a_k \in \mathbb{Z})$$

и любого числа $m = p_1^{\beta_1} \ldots p_n^{\beta_n}$ (где $p_1, \ldots, p_n$ – попарно различные простые числа, а $\beta_1, \ldots, \beta_n \in \mathbb{N}$) решение сравнения

$$f(x) \equiv 0 \ (mod\, m)$$

сводится к решению системы сравнений

$$\begin{cases} f(x) \equiv 0 \ (mod\, p_1^{\beta_1}) \\ \cdots\cdots\cdots\cdots\cdots \\ f(x) \equiv 0 \ (mod\, p_n^{\beta_n}) \end{cases}.$$

В свою очередь, решение любого сравнения

$$f(x) \equiv 0 \ (mod\, p^{\beta})$$

(где p – простое число, а $\beta \in \mathbb{N}$) сводится к построению всех сумм вида

$$x = \sum_{j=1}^{\beta-1} b_j p^j,$$

где числа $b_0, b_1, \ldots, b_{\beta-1} \in \mathbb{Z}_p$ вычисляются следующим образом:

1) число $p_0 \in \mathbb{Z}_p$ является решением сравнения

$$f(x) \equiv 0 \ (mod\, p);$$

2) для каждого $s = 1, \ldots, \beta-1$ число $p_s \in \mathbb{Z}_p$ – это любое такое число, что число

$$x = \sum_{j=1}^{s} b_j p^j$$

является решением сравнения

$$f(x) \equiv 0 \ (mod\, p^{s+1}).$$

В кольце вычетов $\mathcal{Z}_{p^\beta} = (\mathbb{Z}_{p^\beta}, \oplus, \circ)$ каждая сумма

$$x = \sum_{j=1}^{\beta-1} b_j p^j$$

является элементом однозначно определенного класса ассоциированных элементов.

Поэтому для системы уравнений (3.1) естественно определить семейство множеств $\{S_i\}_{i \in I}$ в терминах классов ассоциированных элементов ассоциативного кольца $\mathcal{K}$ с единицей.

Именно эта идея и лежит в основе предлагаемого в настоящем разделе подхода к построению схемы, предназначенной для унифицированного представления множества S.

3.1.2. Классы ассоциированных элементов кольца $\mathcal{K}$.

Пусть $\mathcal{K} = (K, +, \cdot)$ – произвольное (не обязательно конечное) ассоциативное кольцо с единицей. Так как кольцо $\mathcal{K}$ содержит единицу, то множество K^{inv} обратимых элементов кольца $\mathcal{K}$ непусто.

Определим на множестве K отношения эквивалентности $\equiv_l$ и $\equiv_r$ следующим образом:

$$\forall x, y \in K)(x \equiv_l y \Leftrightarrow (\exists \alpha \in K^{inv})(x = \alpha y)),$$
$$(\forall x, y \in K)(x \equiv_r y \Leftrightarrow (\exists \alpha \in K^{inv})(x = y\alpha)).$$

Элементы фактор-множества $\mathtt{B}_l = K/_{\equiv_l}$ (соответственно, фактор-множества $\mathtt{B}_r = K/_{\equiv_r}$) назовем классами l-ассоциированных (соответственно, классами r-ассоциированных) элементов кольца $\mathcal{K} = (K, +, \cdot)$.

Замечание 3.1. Если $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо с единицей, то истинны равенства

$$\equiv_l = \equiv_r = \equiv, \tag{3.2}$$

где $\equiv$ – это обычное отношение эквивалентности «быть ассоциированными элементами кольца $\mathcal{K}$». Следовательно, в этом случае

$$\mathtt{B}_l = \mathtt{B}_r = \mathtt{B}, \tag{3.3}$$

где $\mathtt{B} = K/_{\equiv}$ – фактор-множество классов ассоциированных (в обычном смысле) элементов кольца $\mathcal{K}$.

Центр кольца $\mathcal{K}$ определяется равенством

$$K^{cntr} = \{x \in K | (\forall y \in K)(xy = yx\}. \tag{3.4}$$

Равенства (3.2) и (3.3) истинны для любого такого ассоциативного не коммутативного кольца $\mathcal{K} = (K, +, \cdot)$ с единицей, что $K^{inv} \subseteq K^{cntr}$.

Для любого элемента $x \in K$ обозначим через $\langle x \rangle_l$ и $\langle x \rangle_r$ классы l-ассоциированных и r-ассоциированных элементов кольца $\mathcal{K} = (K, +, \cdot)$, определенные равенствами

$$\langle x \rangle_l = \{y \in K | (\exists \alpha \in K^{inv})(y = \alpha x)\} \tag{3.5}$$

и

$$\langle x \rangle_r = \{y \in K | (\exists \alpha \in K^{inv})(y = x\alpha)\}. \tag{3.6}$$

Замечание 3.2. Из (3.5) и (3.6) непосредственно вытекает, что если $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо с единицей, то для любого элемента $x \in K$ истинны равенства $\langle x \rangle_l = \langle x \rangle_r = \langle x \rangle$, где $\langle x \rangle$ – класс элементов кольца $\mathcal{K}$, ассоциированных (в обычном смысле) с элементом x.

Из равенства (3.5) (соответственно, (3.6)) вытекает, что для того, чтобы определить конкретный элемент $y \in \langle x\rangle_l$ (соответственно, $y \in \langle x\rangle_r$) достаточно указать такой элемент $\alpha \in K^{inv}$, что $y = \alpha x$ (соответственно, $y = x\alpha$).

Исследуем свойства классов $\langle x\rangle_l$ и $\langle x\rangle_r$.

Утверждение 3.1. Равенства

$$\langle 0\rangle_l = \langle 0\rangle_r = \{0\} \tag{3.7}$$

истинны для любого ассоциативного кольца $\mathcal{K} = (K, +, \cdot)$ с единицей.□

Доказательство. Так как $a0 = 0a = 0$ для всех $a \in K$, то из (3.5) вытекает, что $\langle 0\rangle_l = \{0\}$, а из (3.6) вытекает, что $\langle 0\rangle_r = \{0\}$.□

Утверждение 3.2. Для любого ассоциативного кольца $\mathcal{K} = (K, +, \cdot)$ с единицей равенства

$$\langle x\rangle_l = \langle x\rangle_r = K^{inv} \tag{3.8}$$

истинны для каждого элемента $x \in K^{inv}$.□

Доказательство. Пусть $x \in K^{inv}$. Тогда $\alpha x \in K^{inv}$ и $x\alpha \in K^{inv}$ для всех $\alpha \in K^{inv}$. Следовательно, для каждого элемента $x \in K^{inv}$ истинны включения $\langle x\rangle_l \subseteq K^{inv}$ и $\langle x\rangle_r \subseteq K^{inv}$.

Так как $x \in K^{inv}$, то для любого элемента $y \in K^{inv}$ равенство $y = \alpha x$ истинно для элемента $\alpha = yx^{-1} \in K^{inv}$, а равенство $y = x\alpha$ истинно для элемента $\alpha = x^{-1}y \in K^{inv}$. Следовательно, для каждого элемента $x \in K^{inv}$ истинны включения $K^{inv} \subseteq \langle x\rangle_l$ и $K^{inv} \subseteq \langle x\rangle_r$.

Из включений $\langle x\rangle_l \subseteq K^{inv}$ и $K^{inv} \subseteq \langle x\rangle_l$ вытекает, что истинно равенство $\langle x\rangle_l = K^{inv}$, а из включений $\langle x\rangle_r \subseteq K^{inv}$ и $K^{inv} \subseteq \langle x\rangle_r$ вытекает, что истинно равенство $K^{inv} = \langle x\rangle_r$.□

Утверждение 3.3. Для любого ассоциативного кольца $\mathcal{K} = (K, +, \cdot)$ с единицей равенство

$$\langle x\rangle_l = \langle x\rangle_r \tag{3.9}$$

истинно для каждого элемента $x \in K^{cntr}$.□

Доказательство. Пусть $x \in K^{cntr}$. Из равенств (3.4)-(3.6) вытекает, что

$$y \in \langle x\rangle_l \Leftrightarrow (\exists \alpha \in K^{inv})(y = \alpha x) \Leftrightarrow (\exists \alpha \in K^{inv})(y = x\alpha) \Leftrightarrow y \in \langle x\rangle_r,$$

что и требовалось доказать.□

Для любых множеств $A, B \in K$ положим

$$A * B = \{ab | a \in A, b \in B\}. \tag{3.10}$$

Утверждение 3.4. Равенство

$$K^{inv} * K^{inv} = K^{inv} \tag{3.11}$$

истинно для любого ассоциативного кольца $\mathcal{K} = (K, +, \cdot)$ с единицей.□

Доказательство. Если $a, b \in K^{inv}$, то $ab \in K^{inv}$. Следовательно, $K^{inv} * K^{inv} \subseteq K^{inv}$. Из равенства (3.10) вытекает, что

$$K^{inv} * K^{inv} \supseteq \{1 \cdot b | b \in K^{inv}\} = K^{inv}.$$

Из включений $K^{inv} * K^{inv} \subseteq K^{inv}$ и $K^{inv} * K^{inv} \supseteq K^{inv}$ вытекает, что равенство (3.11) истинно.□

Если $A = \{a\}$ (соответственно, $B = \{b\}$), то вместо $\{a\} * B$ (соответственно, вместо $A * \{b\}$), для краткости, будем писать $a * B$ (соответственно, $A * b$).

Утверждение 3.5. Для любого ассоциативного кольца $\mathcal{K} = (K, +, \cdot)$ с единицей равенства

$$\langle x \rangle_l = K^{inv} * x \tag{3.12}$$

и

$$\langle x \rangle_r = x * K^{inv} \tag{3.13}$$

истинны для каждого элемента $x \in K$.□

Доказательство. Равенство (3.12) вытекает из равенств (3.5) и (3.10), а равенство (3.13) вытекает из равенств (3.6) и (3.10).□

Положим

$$K^{c-inv} = \{x \in K | (\forall \alpha \in K^{inv})(x\alpha = \alpha x)\}. \tag{3.14}$$

Замечание 3.3. В любом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$ множество K^{c-inv} непусто, так как $0 \in K^{c-inv}$. Кроме того, если $\mathcal{K}$ – кольцо с единицей, то $1 \in K^{c-inv}$.

Для любого элемента $x \in K^{c-inv}$ истинны равенства

$$\langle x \rangle_l = \langle x \rangle_r = \langle x \rangle,$$

где $\langle x \rangle$ – класс элементов кольца $\mathcal{K}$, ассоциированных (в обычном смысле) с элементом x. Более того, для любых элементов $x, y \in K^{c-inv}$ истинно равенство

$$\langle x \rangle * \langle y \rangle = \langle xy \rangle.$$

Следовательно, алгебра $(\{\langle x \rangle | x \in K^{c-inv}\}, *)$ является полугруппой.

Замечание 3.4. Пусть $\mathcal{K} = (K, +, \cdot)$ – любое такое ассоциативное не коммутативное кольцо с единицей, что $K^{c-inv} = K$. Тогда для любого элемента $x \in K$ истинны равенства

$$\langle x \rangle_l = \langle x \rangle_r = \langle x \rangle,$$

где $\langle x \rangle$ – класс элементов кольца $\mathcal{K}$, ассоциированных (в обычном смысле) с элементом x. Кроме того, для любых элементов $x, y \in K$ истинно равенство

$$\langle x \rangle * \langle y \rangle = \langle xy \rangle.$$

Отсюда вытекает, что алгебра $(\{\langle x \rangle | x \in K\}, *)$ является полугруппой.

Следующая теорема показывает, что возможна иная ситуация для такого ассоциативного не коммутативного кольца $\mathcal{K} = (K, +, \cdot)$ с единицей, что $K^{c-inv} \neq K$.

Теорема 3.1. Для любого ассоциативного кольца $\mathcal{K} = (K, +, \cdot)$ с единицей включения

$$\langle xy \rangle_l \subseteq \langle x \rangle_l * \langle y \rangle_l \tag{3.15}$$

и

$$\langle xy \rangle_r \subseteq \langle x \rangle_r * \langle y \rangle_r \tag{3.16}$$

истинны для любых элементов $x, y \in K \backslash K^{c-inv}$.□

Доказательство. Пусть $x, y \in K \backslash K^{c-inv}$. Так как $\mathcal{K}$ – ассоциативное кольцо с единицей, то

$$\langle x \rangle_l * \langle y \rangle_l = \{(\alpha x)(\beta y) | \alpha, \beta \in K^{inv}\} =$$

$$= \{\alpha((x\beta)y) | \alpha, \beta \in K^{inv}\} \supseteq \{\alpha(xy) | \alpha \in K^{inv}\} = \langle xy \rangle_l,$$

и

$$\langle x \rangle_r * \langle y \rangle_r = \{(x\alpha)(y\beta) | \alpha, \beta \in K^{inv}\} =$$

$$= \{(x(\alpha y))\beta | \alpha, \beta \in K^{inv}\} \supseteq \{(xy)\beta | \beta \in K^{inv}\} = \langle xy \rangle_r,$$

что и требовалось доказать.□

Теорема 3.2. Для любого ассоциативного кольца $\mathcal{K} = (K, +, \cdot)$ с единицей равенства

$$\langle x \rangle_l * \langle y \rangle_r = \langle xy \rangle_r * K^{inv} = K^{inv} * \langle xy \rangle_r \tag{3.17}$$

истинны для любых элементов $x, y \in K$.□

Доказательство. Так как $\mathcal{K}$ – ассоциативное кольцо с единицей, то

$$\langle x \rangle_l * \langle y \rangle_r = \{(\alpha x)(y\beta) | \alpha, \beta \in K^{inv}\} = \{(\alpha(xy))\beta | \alpha, \beta \in K^{inv}\} \tag{3.18}$$

и

$$\langle x \rangle_l * \langle y \rangle_r = \{(\alpha x)(y\beta) | \alpha, \beta \in K^{inv}\} = \{\alpha((xy)\beta) | \alpha, \beta \in K^{inv}\}. \tag{3.19}$$

При этом

$$\{\alpha(xy)|\alpha \in K^{inv}\} = \langle xy\rangle_l \tag{3.20}$$

и

$$\{(xy)\beta|\beta \in K^{inv}\} = \langle xy\rangle_r. \tag{3.21}$$

Из равенств (3.18) и (3.20) вытекает, что

$$\langle x\rangle_l * \langle y\rangle_r = \{u\beta|u \in \langle xy\rangle_l, \beta \in K^{inv}\} = \langle xy\rangle_l * K^{inv},$$

а из равенств (3.19) и (3.21) вытекает, что

$$\langle x\rangle_l * \langle y\rangle_r = \{\alpha v|\alpha \in K^{inv}, v \in \langle xy\rangle_r\} = K^{inv} * \langle xy\rangle_r,$$

что и требовалось доказать.□

Для любых множеств $A, B \in K$ положим

$$A + B = \{a + b|a \in A, b \in B\}. \tag{3.22}$$

Отметим, что:

1) $A + B = B + A$ для любых множеств $A, B \in K$, т.е. сложение подмножеств множества K – коммутативная операция;

2) $\{0\} + A = A$ для любого множества $A \in K$.

Следующая теорема показывает, что сложение подмножеств множества K, определенное формулой (3.22), может не являться операцией на классах l-ассоциированных, а также классах r-ассоциированных элементов ассоциативного кольца $\mathcal{K} = (K, +, \cdot)$ с единицей.

Теорема 3.3. В каждом ассоциативном кольца $\mathcal{K} = (K, +, \cdot)$ с единицей для любого элемента $x \in K$ включения

$$\langle x\rangle_l + K^{inv} \supseteq \langle x + n1\rangle_l \tag{3.23}$$

и

$$\langle x\rangle_r + K^{inv} \supseteq \langle x + n1\rangle_r \tag{3.24}$$

истинны для всех таких чисел $n \in \mathbb{N}$, что $n1 \in K^{inv}$.□

Доказательство. Так как $\mathcal{K}$ – ассоциативное кольцо с единицей, то для любого элемента $x \in K$ и любого такого числа $n \in \mathbb{N}$, что $n1 \in K^{inv}$

$$\langle x\rangle_l + K^{inv} = \{\alpha x + \beta|\alpha, \beta \in K^{inv}\} \supseteq$$

$$\supseteq \{\alpha x + \alpha(n1)|\alpha \in K^{inv}\} =$$

$$= \{\alpha(x + (n1))|\alpha \in K^{inv}\} = \langle x + n1\rangle_l$$

и

$$\langle x\rangle_r + K^{inv} = \{x\alpha + \beta | \alpha, \beta \in K^{inv}\} \supseteq$$
$$\supseteq \{x\alpha + (n1)\alpha | \alpha \in K^{inv}\} =$$
$$= \{(x + (n1))\alpha | \alpha \in K^{inv}\} = \langle x + n1\rangle_r,$$

что и требовалось доказать.□

Рассмотрим детализацию полученных результатов для кольца вычетов $\mathcal{Z}_{p^k} = (\mathbf{Z}_{p^k}, \oplus, \circ)$ (где p простое число, а $k \in \mathbb{N}$ $(k \geq 2)$).

3.1.3. Классы ассоциированных элементов кольца $\mathcal{Z}_{p^k}$ $(k \geq 2)$.

Так как $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (где p – простое число, а $k \in \mathbb{N}$ $(k \geq 2)$) – ассоциативно-коммутативное кольцо с единицей, то $\mathtt{B}_l = \mathtt{B}_r = \mathtt{B}$.

В замечании 1.30 определен (см. формулу (1.1)) p-тип $\mathtt{t}_p(z)$ элемента $z \in \mathbb{Z}_{p^k}$ кольца $\mathcal{Z}_{p^k}$ и отмечено, что для того, чтобы задать класс C_r $(r = 0, 1, \ldots, k)$ ассоциированных элементов кольца $\mathcal{Z}_{p^k}$, достаточно зафиксировать p-тип $\mathtt{t}_p(z)$ элемента, принадлежащего этому классу. При этом:

1) p-тип, равный 0, определяет класс C_0 ассоциированных элементов, состоящий из обратимых элементов кольца $\mathcal{Z}_{p^k}$, т.е. $C_0 = \mathbb{Z}_{p^k}^{inv}$;

2) p-тип, равный k, определяет одно-элементный класс ассоциированных элементов, состоящий из нуля 0 кольца $\mathcal{Z}_{p^k}$, т.е. $C_k = \{0\}$.

Следующее утверждение характеризует класс C_r $(r = 1, \ldots, k-1)$ ассоциированных элементов кольца $\mathcal{Z}_{p^k}$, для которых p-тип равен r.

Утверждение 3.6. Для любого кольца $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (где p – простое число, а $k \in \mathbb{N}$ $(k \geq 2)$) равенство

$$C_r = \{\alpha \circ p^r | \alpha \in \mathbb{Z}_{p^{k-r}}^{inv}\}$$

истинно для всех чисел $r = 1, \ldots, k-1$.□

Доказательство. Представим элемент $a \in \mathbb{Z}_{p^k}$ $(a \neq 0)$ в виде

$$a = \sum_{i=0}^{k-1} \beta_i p^i, \tag{3.25}$$

$\beta_i \in \mathbb{Z}_p$ $(i = 0, 1, \ldots, k-1)$.

Так как $\beta_i \in \mathbb{Z}_p$ $(i = 0, 1, \ldots, k-1)$, то $\beta_i \in \mathbb{Z}_p^{inv}$ (а, следовательно, $\beta_i \in \mathbb{Z}_{p^k}^{inv}$) тогда и только тогда, когда $\beta_i \neq 0$. Из определения p-типа элемента кольца $\mathcal{Z}_{p^k}$ вытекает, что если элемент $a \in \mathbb{Z}_{p^k}$ представлен в виде (3.25), то

$$(\forall r = 1, \ldots, k-1)(\mathtt{t}_p(a) = r) \Leftrightarrow (\forall j = 0, 1, \ldots, r-1)(\beta_j = 0 \& \beta_r \neq 0).$$

Следовательно, если элемент $a \in \mathbb{Z}_{p^k}$ представлен в виде (3.25), то

$$\mathtt{t}_p(a) = r \Leftrightarrow \beta_r \neq 0 \& a = \sum_{i=r}^{k-1} \beta_i p^i \Leftrightarrow$$

$$\Leftrightarrow \beta_r \neq 0 \& a = p^r \circ \sum_{i=0}^{k-r-1} \beta_{i+r} p^i \Leftrightarrow$$

$$\Leftrightarrow \sum_{i=0}^{k-r-1} \beta_{i+r} p^i \in \mathbb{Z}_{p^{k-r}}^{inv} \& a = p^r \circ \sum_{i=0}^{k-r-1} \beta_{i+r} p^i,$$

что и требовалось доказать.$\square$

Из коммутативности кольца $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (где p – простое число, а $k \in \mathbb{N}$ $(k \geq 2)$) вытекает, что алгебра $(\{C_r | r = 0, 1, \ldots, k\}, *)$ является коммутативной полугруппой. При этом

$$C_r * C_0 = C_0 * C_r = C_r \ (r = 0, 1, \ldots, k), \tag{3.26}$$

$$C_r * C_k = C_k * C_r = C_k \ (r = 0, 1, \ldots, k), \tag{3.27}$$

$$C_{r_1} * C_{r_2} = \begin{cases} C_{r_1+r_2}, & \text{если } r_1 + r_2 < k \\ C_k, & \text{если } r_1 + r_2 \geq k \end{cases} \ (r_1, r_2 = 1, \ldots, k-1), \tag{3.28}$$

$$C_{r_1} * p^{r_2} = p^{r_2} * C_{r_1} = \begin{cases} C_{r_1+r_2}, & \text{если } r_1 + r_2 \leq k \\ C_k, & \text{если } r_1 + r_2 > k \end{cases} \tag{3.29}$$

Несложно убедиться в том, что истинны следующие соотношения, связанные со сложением классов C_r $(r = 0, 1, \ldots, k)$ ассоциированных элементов кольца $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (где p – простое число, а $k \in \mathbb{N}$ $(k \geq 2)$)

$$C_r \oplus C_0 = C_0 \oplus C_r = C_0 \ (r = 1, \ldots, k), \tag{3.30}$$

$$(C_0 \oplus C_0) \cap \langle x \rangle \neq \emptyset \ (x \in \mathbb{Z}_{p^k}), \tag{3.31}$$

$$C_r \oplus C_k = C_k \oplus C_r = C_r \ (r = 0, 1, \ldots, k), \tag{3.32}$$

$$C_i \oplus C_j = C_i \ (1 \leq i < j \leq k-1), \tag{3.33}$$

$$C_i \oplus C_i \supseteq C_i \ (i = 1, \ldots, k-1), \tag{3.34}$$

$$C_i \oplus C_i \supseteq C_k \ (i = 1, \ldots, k-1), \tag{3.35}$$

$$(C_i + C_i) \cap C_j \neq \emptyset \ (i = 1, \ldots, k-2; j = i+1, \ldots, k-1). \tag{3.36}$$

Кроме того, операция сложения классов C_r $(r = 0, 1, \ldots, k)$ ассоциированных элементов кольца $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (где p – простое число, а $k \in \mathbb{N}$ $(k \geq 2)$) связана с операцией $*$ следующим равенством

$$C_{r_1} \oplus C_{r_2} = C_{r_2} \oplus C_{r_1} = \begin{cases} p^{r_1} * (C_0 \oplus C_{r_2 - r_1}), & \text{если } r_1 \leq r_2 \\ p^{r_2} * (C_0 \oplus C_{r_1 - r_2}), & \text{если } r_1 > r_2 \end{cases} \tag{3.37}$$

для любых чисел $r_1, r_2 = 1, \ldots, k-1$.

Отметим, что именно равенства (3.26)-(3.37) и дают возможность эффективно представлять множества решений систем полиномиальных уравнений с параметрами над кольцом вычетов $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (где p – простое число, а $k \in \mathbb{N}$ $(k \geq 2)$).

3.1.4. Схема построения множества решений.

В п.3.1.2 установлены свойства классов l-ассоциированных и r-ассоциированных элементов ассоциативного кольца $\mathcal{K} = (K, +, \cdot)$ с единицей. Эти свойства дают возможность осуществлять построение множества решений системы уравнений (3.1) над конечным ассоциативным кольцом $\mathcal{K}$ с единицей в соответствии со следующей схемой.

Схема 3.1

Шаг 1. $S := \emptyset$.

Шаг 2. Вычисляем множество I наборов элементов, принадлежащих множеству $\mathtt{B}_l \cup \mathtt{B}_r$, которые являются допустимыми для значений параметров a_j $(j = 1, \ldots, h)$.

Замечание 3.5. В силу равенств (3.12) и (3.13) замена параметра a_j $(j = 1, \ldots, h)$ классом $\langle x \rangle_l$ l-ассоциированных (соответственно, классом $\langle x \rangle_r$ r-ассоциированных) элементов сводится к представлению параметра a_j в виде $b_j x$ (соответственно, в виде $x b_j$), где $b_j \in K^{inv}$ – переменная.

Шаг 3. Если $I = \emptyset$, то конец, иначе переход к шагу 4.

Шаг 4. Выбираем элемент $i \in I$, $I := I \backslash \{i\}$, $S_i = \emptyset$.

Шаг 5. Вычисляем множество $Q(i)$ наборов элементов, принадлежащих множеству $\mathtt{B}_l \cup \mathtt{B}_r$, которые являются допустимыми для значений переменных u_j $(j = 1, \ldots, n)$ при значениях параметров, характеризуемых набором $i \in I$ элементов множества $\mathtt{B}_l \cup \mathtt{B}_r$.

Шаг 6. Если $Q(i) = \emptyset$, то переход к шагу 4, иначе – к шагу 7.

Шаг 7. Выбираем элемент $q \in Q(i)$, $Q(i) := Q(i) \backslash \{q\}$.

Шаг 8. Вычисляем множество S_{iq} всех решений, значения которых принадлежат элементу q.

Шаг 9. $S_i := S_i \cup S_{iq}$.

Шаг 10. Если $Q(i) \neq \emptyset$, то переход к шагу 7, иначе – к шагу 11.

Шаг 11. $S := S \cup S_i$.

Шаг 12. Если $I = \emptyset$, то конец, иначе переход к шагу 4.

Корректность схемы 3.1 обусловлена следующими обстоятельствами.

Каждое из множеств $\mathtt{B}_l$ и $\mathtt{B}_r$ является разбиением множества K. Поэтому любой набор значений параметров a_j $(j = 1, \ldots, h)$, а также любой набор значений переменных u_j $(j = 1, \ldots, n)$ принадлежит той или иной комбинации элементов множества $\mathtt{B}_l \cup \mathtt{B}_r$.

Замечание 3.6. Из равенств (3.12) и (3.13) вытекает, что для любого ассоциативного кольца $\mathcal{K} = (K, +, \cdot)$ с единицей неравенства

$$|\langle x \rangle_l| \leq |K^{inv}|$$

и

$$|\langle x \rangle_r| \leq |K^{inv}|$$

истинны для каждого элемента $x \in K \backslash \{0\}$. При этом, если элемент $x \in K \backslash \{0\}$ не является делителем нуля, то истинны равенства

$$|\langle x \rangle_l| = |K^{inv}|$$

и

$$|\langle x \rangle_r| = |K^{inv}|.$$

Следовательно, в результате перехода к допустимым наборам элементов множества $\mathtt{B}_l \cup \mathtt{B}_r$ схема 3.1 может обеспечить существенный выигрыш во времени по сравнению с решением системы уравнений (3.1) непосредственным перебором вариантов.

Вычисления, осуществляемые на шагах 2 и 5, приводят к появлению переменных, значения которых принадлежат множеству K^{inv}.

Вычисления, осуществляемые на шаге 8, по своей сути, устанавливают условия, которым должны удовлетворять значения этих переменных, с тем, чтобы набор значений переменных u_j $(j = 1, \ldots, n)$ являлся решением системы уравнений (3.1).

Циклы, присутствующие в схеме 3.1, гарантируют анализ всех наборов элементов множества $\mathtt{B}_l \cup \mathtt{B}_r$, допустимых для значений параметров a_j $(j = 1, \ldots, h)$ и переменных u_j $(j = 1, \ldots, n)$.

А так как $\mathcal{K}$ – конечное кольцо, то вычисления, осуществляемые в соответствии со схемой 3.1, всегда завершаются за конечное время.

Сложность вычислений, которые осуществляются в соответствии со схемой 3.1, в значительной мере определяется сложностью вычислений, осуществляемыми при выполнении шагов 2, 5 и 8.

В ряде случаев сложность вычисления множеств I и $Q(i)$ $(i \in I)$ наборов элементов множества $\mathtt{B}_l \cup \mathtt{B}_r$, которые являются допустимыми для значений параметров a_j $(j = 1, \ldots, h)$ и переменных u_j $(j = 1, \ldots, n)$, может быть существенно понижена (по сравнению с полным перебором вариантов) за счет представления этих множеств в неявном виде. Каждое такое представление является, по своей сути, формулой, построенной с использованием соотношений между классами l-ассоциированных и r-ассоциированных элементов кольца $\mathcal{K}$.

Представление множеств I и $Q(i)$ $(i \in I)$ в неявном виде дает возможность одновременно рассматривать все наборы элементов множества $\mathtt{B}_l \cup \mathtt{B}_r$, которые удовлетворяют данному соотношению.

Сложность вычислений, осуществляемых при выполнении шага 8, существенно зависит от строения множества K^{inv} обратимых элементов кольца $\mathcal{K}$. Использование особенностей этого строения дает возможность одновременно рассматривать все варианты, удовлетворяющие заданному набору условий для переменных, принадлежащих множеству K^{inv}.

Анализ схемы 3.1 показывает, что шаги 2 и 5 могут быть объединены в один шаг. В результате мы получим следующую схему, предназначенную для построения множества решений системы уравнений (3.1) над конечным ассоциативным кольцом $\mathcal{K}$ с единицей.

Схема 3.2

Шаг 1. $S := \emptyset$.

Шаг 2. Заменяя каждый параметр a_j $(j = 1, \ldots, h)$ и каждую переменную u_j $(j = 1, \ldots, n)$ всевозможными элементами множества $\mathtt{B}_l \cup \mathtt{B}_r$, вычисляем множество $\widetilde{S} = \{(i, q) | i \in I, q \in Q(i)\}$ наборов элементов, допустимых для значений параметров и переменных.

Шаг 3. Если $\widetilde{S} = \emptyset$, то конец, иначе переход к шагу 4.

Шаг 4. Выбираем элемент $i \in I$, $I := I \backslash \{i\}$, $S_i = \emptyset$.

Шаг 5. Выбираем элемент $q \in Q(i)$, $Q(i) := Q(i) \backslash \{q\}$.

Шаг 6. Вычисляем множество S_{iq} всех решений, значения которых принадлежат элементу q.

Шаг 7. $S_i := S_i \cup S_{iq}$.

Шаг 8. Если $Q(i) \neq \emptyset$, то переход к шагу 5, иначе – к шагу 9.

Шаг 9. $S := S \cup S_i$.

Шаг 10. Если $I = \emptyset$, то конец, иначе переход к шагу 4.

Проиллюстрируем применение схем 3.1 и 3.2 в случае кольца вычетов $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (где p – простое число, а $k \in \mathbb{N}$ $(k \geq 2)$).

Пример 3.1. Рассмотрим над кольцом $\mathcal{Z}_{p^2} = (\mathbb{Z}_{p^2}, \oplus, \circ)$ (где p – простое число) решение нелинейного уравнения

$$a_1 \circ u_1 \circ u_2 = a_2,$$

где $a_1, a_2 \in \mathbb{Z}_{p^2}$ – параметры.

После выполнения шага 2 схемы 3.1 получим, что множество допустимых наборов классов ассоциированных элементов кольца $\mathcal{Z}_{p^2}$ для значений параметров a_1 и a_2 имеет следующий вид:

$$I = \{(C_0, C_0), (C_0, C_1), (C_0, C_2), (C_1, C_1), (C_1, C_2), (C_2, C_2)\}.$$

В результате выполнения шагов 3-12 схемы 3.1 получим

$$S_{(C_2,C_2)} = \mathbb{Z}_{p^2}^2,$$

$$S_{(C_0,C_0)} = \{(d, d^{-1}a_1^{-1}a_2) | d \in \mathbb{Z}_{p^2}^{inv}\},$$

$$S_{(C_0,C_1)} = \{(d, d^{-1}a_1^{-1}a_2) | d \in \mathbb{Z}_{p^2}^{inv}\} \cup \{(d^{-1}a_1^{-1}a_2, d) | d \in \mathbb{Z}_{p^2}^{inv}\},$$

$$S_{(C_0,C_2)} = \{0\} \times \mathbb{Z}_{p^2} \cup \mathbb{Z}_{p^2} \times \{0\} \cup C_1 \times C_1,$$

$$S_{(C_1,C_2)} = \{0\} \times \mathbb{Z}_{p^2} \cup \mathbb{Z}_{p^2} \times \{0\} \cup$$

$$\cup\{(d_1, d_2 p) | d_1, d_2 \in \mathbb{Z}_{p^2}^{inv}\} \cup \{(d_1 p, d_2) | d_1, d_2 \in \mathbb{Z}_{p^2}^{inv}\} \cup \{(d_1 p, d_2 p) | d_1, d_2 \in \mathbb{Z}_{p^2}^{inv}\},$$

$$S_{(C_1,C_1)} = \{(d, d^{-1}b_1^{-1}b_2) | d \in \mathbb{Z}_{p^2}^{inv}\} \cup \{(d, d^{-1}b_1^{-1}b_2 + \alpha p) | d, \alpha \in \mathbb{Z}_{p^2}^{inv}\} \cup$$

$$\cup\{(d^{-1}b_1^{-1}b_2, d) | d \in \mathbb{Z}_{p^2}^{inv}\} \cup \{(d^{-1}b_1^{-1}b_2 + \alpha p, d) | d, \alpha \in \mathbb{Z}_{p^2}^{inv}\},$$

где $a_1 = b_1 p$ ($b_1 \in \mathbb{Z}_{p^2}^{inv}$) и $a_2 = b_2 p$ ($b_2 \in \mathbb{Z}_{p^2}^{inv}$).

Пример 3.2. Рассмотрим над кольцом $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (где p – простое число, а $k \in \mathbb{N}$ ($k \geq 2$)) решение линейного уравнения

$$a \circ u = b, \tag{3.38}$$

где $a, b \in \mathbb{Z}_{p^k}$ – параметры.

Воспользуемся схемой 3.2. Переходя от параметров и переменной к классами ассоциированных элементов, получим

$$C_{r_1} * C_{r_2} = C_{r_3}. \tag{3.39}$$

где $r_1, r_2, r_3 \in \mathbb{Z}_{k+1}$.

Из (3.26)-(3.28) вытекает, что:

1) если $r_3 < r_1$, то уравнение (3.39) (следовательно, и уравнение (3.38)) решений не имеет;

2) если $r_1 = 0$, то $r_2 = r_3$;

3) если $r_1 = k$, то $r_3 = k$, а r_2 – любой элемент множества $\mathbb{Z}_{k+1}$;

4) если $r_1, r_3 \in \mathbb{N}_{k-1}$, то $r_3 \geq r_1$ и $r_2 = r_3 - r_1$;

5) если $r_1 \in \mathbb{N}_{k-1}$ и $r_3 = k$, то r_2 – любой элемент множества $\mathbb{N}_k \backslash \mathbb{N}_{k-r_1-1}$.

Таким образом, для построения множества S решений уравнения (3.38) необходимо рассмотреть следующие ситуации.

1. Пусть $a \in \mathbb{Z}_{p^k}^{inv}$. Тогда уравнение (3.38) имеет единственное решение $u = a^{-1} \circ b$, т.е. $S = \{a^{-1} \circ b\}$.

2. Пусть $a = 0$. Тогда при $b \neq 0$ уравнение (3.38) решений не имеет, а при $b = 0$ любой элемент множества $\mathbb{Z}_{p^k}$ является решением уравнения (3.38), т.е. $S = \mathbb{Z}_{p^k}$.

3. Пусть $a = \alpha \circ p^{r_1}$ ($r_1 \in \mathbb{N}_{k-1}, \alpha \in \mathbb{Z}^{inv}_{p^{k-r_1}}$) и $b = \beta \circ p^{r_3}$ ($r_3 \in \mathbb{N}_{k-1} \backslash \mathbb{N}_{r_1-1}, \beta \in \mathbb{Z}^{inv}_{p^{k-r_3}}$). Тогда:

1) если $r_1 = r_3$, то $u = \gamma$ или $u = \gamma \oplus \delta \circ p^{k-i}$ ($i \in \mathbb{N}_{k-1} \backslash \mathbb{N}_{k-r_1-1}$), где $\gamma \in \mathbb{Z}^{inv}_{p^k}$, а $\delta \in \mathbb{Z}^{inv}_{p^i}$;

2) если $r_1 < r_3$, то $u = \gamma \circ p^{r_3-r_1}$ или $u = \gamma \circ p^{r_3-r_1} \oplus \delta \circ p^{k-i}$ ($i \in \mathbb{N}_{k-1} \backslash \mathbb{N}_{k-r_1-1}$), где $\gamma \in \mathbb{Z}^{inv}_{p^{k-r_3+r_1}}$, а $\delta \in \mathbb{Z}^{inv}_{p^i}$.

Подставив эти значения a, b и u в уравнение (3.38), получим,

$$\alpha \circ \gamma \circ p^{r_3} = \beta \circ p^{r_3} \Leftrightarrow (\alpha \circ \gamma \ominus \beta) \circ p^{r_3} = 0.$$

Следовательно, либо

$$\alpha \circ \gamma \ominus \beta = 0 \Leftrightarrow \gamma = \alpha^{-1} \circ \beta,$$

либо

$$\alpha \circ \gamma \ominus \beta = \varepsilon \circ p^j \Leftrightarrow \gamma = \alpha^{-1} \circ (\beta \oplus \varepsilon \circ p^j) \ (j \in \mathbb{N}_{k-1} \backslash \mathbb{N}_{k-r_3-1}, \varepsilon \in \mathbb{Z}^{inv}_{p^{k-j}}).$$

Таким образом:

1) если $a = \alpha \circ p^{r_1}$ и $b = \beta \circ p^{r_1}$, где $r_1 \in \mathbb{N}_{k-1}$ и $\alpha, \beta \in \mathbb{Z}^{inv}_{p^{k-r_1}}$, то $S = \bigcup\limits_{i=1}^{4} S_i$, где

$$S_1 = \{\alpha^{-1} \circ \beta\},$$

$$S_2 = \bigcup_{j=k-r_1}^{k-1} \{\alpha^{-1} \circ (\beta \oplus \varepsilon \circ p^j) | \varepsilon \in \mathbb{Z}^{inv}_{p^{k-j}}\},$$

$$S_3 = \bigcup_{i=k-r_1}^{k-1} \{\alpha^{-1} \circ \beta \oplus \delta \circ p^{k-i} | \delta \in \mathbb{Z}^{inv}_{p^i}\},$$

$$S_4 = \bigcup_{i=k-r_1}^{k-1} \bigcup_{j=k-r_1}^{k-1} \{\alpha^{-1} \circ (\beta \oplus \varepsilon \circ p^j) \oplus \delta \circ p^{k-i} | \delta \in \mathbb{Z}^{inv}_{p^i}, \varepsilon \in \mathbb{Z}^{inv}_{p^{k-j}}\};$$

2) если $a = \alpha \circ p^{r_1}$ и $b = \beta \circ p^{r_3}$, где $r_1, r_3 \in \mathbb{N}_{k-1}$ и $r_1 < r_3$, то $S = \bigcup\limits_{i=1}^{4} S_i$, где

$$S_1 = \{\alpha^{-1} \circ \beta \circ p^{r_3-r_1}\},$$

$$S_2 = \bigcup_{j=k-r_1}^{k-1} \{(\alpha^{-1} \circ (\beta \oplus \varepsilon \circ p^j) \circ p^{r_3-r_1}) | \varepsilon \in \mathbb{Z}^{inv}_{p^{k-j}}\},$$

$$S_3 = \bigcup_{i=k-r_1}^{k-1} \{\alpha^{-1} \circ \beta \circ p^{r_3-r_1} \oplus \delta \circ p^{k-i} | \delta \in \mathbb{Z}^{inv}_{p^i}\},$$

$$S_4 = \bigcup_{i=k-r_1}^{k-1} \bigcup_{j=k-r_1}^{k-1} \{(\alpha^{-1} \circ (\beta \oplus \varepsilon \circ p^j) \circ p^{r_3-r_1}) \oplus \delta \circ p^{k-i} | \delta \in \mathbb{Z}^{inv}_{p^i}, \varepsilon \in \mathbb{Z}^{inv}_{p^{k-j}}\}.$$

4. Пусть $a = \alpha \circ p^{r_1}$, где $r_1 \in \mathbb{N}_{k-1}$ и $\alpha \in \mathbb{Z}_{p^{k-r_1}}^{inv}$, а $b = 0$. Тогда либо $u = 0$, либо $u = \gamma \circ p^i$, где $i \in \mathbb{N}_{k-1} \backslash \mathbb{N}_{k-r_1-1}$ и $\gamma \in \mathbb{Z}_{p^{k-i}}^{inv}$, т.е. $S = \{0\} \cup \bigcup\limits_{i=k-r_1}^{k-1} \{\gamma \circ p^i | \gamma \in \mathbb{Z}_{p^{k-i}}^{inv}\}$.

Пример 3.3. Рассмотрим над кольцом $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (где p – простое число, а $k \in \mathbb{N}$ $(k \geq 2)$) решение систем линейных уравнений.

Рассмотрим вначале систему n линейных уравнений с n неизвестными

$$\begin{cases} a_{11} \circ u_1 \oplus \cdots \oplus a_{1n} \circ u_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1} \circ u_1 \oplus \cdots \oplus a_{nn} \circ u_n = b_n \end{cases}, \tag{3.40}$$

где $a_{ij}, b_i \in \mathbb{Z}_{p^k}$ $(i, j \in \mathbb{N}_n)$ – параметры.

Запишем систему (3.40) в матричном виде

$$A \circ \mathbf{u} = \mathbf{b}. \tag{3.41}$$

Известно (см., напр., [13]), что посредством элементарных преобразований и, возможно, изменения нумерации переменных (т.е., по сути, с помощью метода Гаусса) система уравнений (3.41) может быть преобразована в такую эквивалентную систему уравнений

$$D \circ \mathbf{u} = \mathbf{c}, \tag{3.42}$$

что $\mathbf{c} = (c_1, \ldots, c_n)^T$, где $c_1, \ldots, c_n \in \mathbb{Z}_{p^k}$ и

$$D = \begin{pmatrix} d_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & d_n \end{pmatrix},$$

где $d_1, \ldots, d_l \in \mathbb{Z}_{p^k}^{inv}$ $(0 \leq l \leq n)$ и $d_{l+1}, \ldots, d_n \in \mathbb{Z}_{p^k} \backslash \mathbb{Z}_{p^k}^{inv}$.

Запишем систему (3.42) в явном виде

$$\begin{cases} d_1 \circ u_1 = c_1 \\ \cdots\cdots\cdots\cdots \\ d_n \circ u_n = c_n \end{cases}. \tag{3.43}$$

Множество решений S_i $(i \in \mathbb{N}_n)$ i-го уравнения системы уравнений (3.43) может быть найдено методом, рассмотренным в примере 3.2. Множество $S = S_1 \times \cdots \times S_n$ представляет собой множество решений системы уравнений (3.43) (а, следовательно, множество решений системы уравнений (3.40)).

Рассмотрим недоопределенную систему m линейных уравнений с n $(m < n)$ неизвестными над кольцом $\mathcal{Z}_{p^k}$

$$\begin{cases} a_{11} \circ u_1 \oplus \cdots \oplus a_{1n} \circ u_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1} \circ u_1 \oplus \cdots \oplus a_{mn} \circ u_n = b_m \end{cases}, \tag{3.44}$$

где $a_{ij}, b_i \in \mathbb{Z}_{p^k}$ $(i \in \mathbb{N}_m, j \in \mathbb{N}_n)$ – параметры.

Посредством элементарных преобразований и, возможно, перенумерации переменных) система уравнений (3.44) может быть приведена к виду

$$\begin{cases} d_1 \circ u_1 = c_{1,m+1} \circ u_{m+1} \oplus \cdots \oplus c_{1,n} \circ u_n \\ \cdots\cdots\cdots\cdots\cdots \\ d_m \circ u_m = c_{m,m+1} \circ u_{m+1} \oplus \cdots \oplus c_{m,n} \circ u_n \end{cases}, \tag{3.45}$$

где $d_i, c_{ij} \in \mathbb{Z}_{p^k}$ $(i \in \mathbb{N}_m, j \in \mathbb{N}_n \backslash \mathbb{N}_m)$.

Множество решений $S^{(i)}_{u_{m+1},\ldots,u_n}$ $(i \in \mathbb{N}_m)$ i-го уравнения системы уравнений (3.45) может быть найдено методом, рассмотренным в примере 3.1. Множество

$$S = \bigcup_{(u_{m+1},\ldots,u_n) \in \mathbb{Z}_{p^k}^{n-m}} S^{(1)}_{u_{m+1},\ldots,u_n} \times \cdots \times S^{(m)}_{u_{m+1},\ldots,u_n} \times (u_{m+1}, \ldots, u_n)$$

представляет собой множество решений системы уравнений (3.45), а, следовательно, множество решений системы уравнений (3.44).

Рассмотрим переопределенную систему m линейных уравнений с n $(m > n)$ неизвестными над кольцом $\mathcal{Z}_{p^k}$

$$\begin{cases} a_{11} \circ u_1 \oplus \cdots \oplus a_{1n} \circ u_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ u_{m1} \circ u_1 \oplus \cdots \oplus a_{mn} \circ u_n = b_m \end{cases}, \tag{3.46}$$

где $a_{ij}, b_i \in \mathbb{Z}_{p^k}$ $(i \in \mathbb{N}_m, j \in \mathbb{N}_n)$ – параметры.

Без ограничения общности считаем, что ни одно из уравнений системы (3.46) не является линейной комбинацией остальных уравнений. С помощью элементарных преобразований и, возможно, перенумерации переменных, представим систему линейных уравнений (3.46) в виде двух систем линейных уравнений

$$\begin{cases} d_1 \circ u_1 = c_1 \\ \cdots\cdots\cdots \\ d_n \circ u_n = c_n \end{cases} \tag{3.47}$$

и

$$\begin{cases} d_{n+1,1} \circ u_1 \oplus \cdots \oplus d_{n+1,n} \circ u_n = c_{n+1} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ d_{m,1} \circ u_1 \oplus \cdots \oplus d_{m,n} \circ u_n = c_m \end{cases}. \tag{3.48}$$

Метод поиска множества решений S' системы линейный уравнений (3.47) был рассмотрен выше. Далее из множества S' необходимо выделить множество S решений системы линейный уравнений (3.48). Это множество S и представляет собой множество решений системы линейных уравнений (3.46).

Пример 3.4. Рассмотрим над кольцом $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (где p – простое число, а $k \in \mathbb{N}$ $(k \geq 2)$) решение системы нелинейных уравнений

$$\begin{cases} a_1 \circ u_1 \circ u_2 \oplus a_2 \circ u_3 = 0 \\ a_2 \circ u_1 = 0 \end{cases}, \tag{3.49}$$

где $a_1, a_2 \in \mathbb{Z}_{p^k}$ – параметры.

Применяем схему 3.2. Переходя от параметров и переменных к классами ассоциированных элементов, получим

$$\begin{cases} C_{r_1} * C_{r_2} * C_{r_3} \oplus C_{r_4} * C_{r_5} = C_k \\ C_{r_4} * C_{r_2} = C_k \end{cases}, \tag{3.50}$$

Из (3.26)-(3.37) вытекает, что допустимыми являются следующие случаи (во всех остальных случаях система уравнений (3.50) (а, следовательно, и система уравнений (3.49)) не имеет решений):

1) если $r_1 = k$, то $r_5 \geq k - r_4$, $r_2 \geq k - r_4$, а $r_3 \in \mathbb{N}_{k+1}$;

2) если $r_1 \neq k$ и $r_4 = 0$, то $r_2 = k$, $r_5 = k$, а $r_3 \in \mathbb{N}_{k+1}$;

3) если $r_1 \neq k$ и $r_4 = k$, то $r_2 + r_3 \geq k - r_1$, а $r_5 \in \mathbb{N}_{k+1}$;

4) если $r_1 \neq k$ и $r_4 \in \mathbb{N}_{k-1}$, то $r_2 \geq k - r_4$, а это означает, что:

а) если $r_2 = k$, то $r_5 \geq k - r_4$, а $r_3 \in \mathbb{N}_{k+1}$;

б) если $k - r_4 \leq r_2 \leq k-1$, то либо $r_2 + r_3 \geq k - r_1$ и $r_5 \geq k - r_4$, либо $r_2 + r_3 < k - r_1$ и $r_2 + r_3 - r_5 = r_4 - r_1$.

Таким образом, для построения множества S решений системы уравнений (3.49) необходимо рассмотреть следующие ситуации.

1. Пусть $a_1 = 0$. Тогда система уравнений (4.40) принимает вид

$$\begin{cases} 0 \circ u_1 \circ u_2 \oplus a_2 \circ u_3 = 0 \\ a_2 \circ u_1 = 0 \end{cases} \Leftrightarrow \begin{cases} a_2 \circ u_3 = 0 \\ a_2 \circ u_1 = 0 \end{cases}.$$

Следовательно:

1) если $a_2 \in \mathbb{Z}_{p^k}^{inv}$, то $S = \{(0, u_2, 0) | u_2 \in \mathbb{Z}_{p^k}\}$;

2) если $a_2 = \alpha_4 \circ p^{r_4}$ $(\alpha_4 \in \mathbb{Z}_{p^{k-r_4}}^{inv}, r_4 \in \mathbb{N}_{k-1})$, то $S = \bigcup\limits_{i=1}^{4} S_i$, где

$$S_1 = \{(0, u_2, 0) | u_2 \in \mathbb{Z}_{p^k}\},$$

$$S_2 = \bigcup_{r_5 = k - r_4}^{k-1} \{(0, u_2, \alpha_5 \circ p^{r_5}) | u_2 \in \mathbb{Z}_{p^k}, \alpha_5 \in \mathbb{Z}_{p^{k-r_5}}^{inv}\},$$

$$S_3 = \bigcup_{r_2 = k - r_4}^{k-1} \{(\alpha_2 \circ p^{r_2}, u_2, 0) | u_2 \in \mathbb{Z}_{p^k}, \alpha_2 \in \mathbb{Z}_{p^{k-r_2}}^{inv}\},$$

а

$$S_4 = \bigcup_{r_5 = k - r_4}^{k-1} \bigcup_{r_2 = k - r_4}^{k-1} S_{r_2, r_5}^{(1)},$$

где $S_{r_2, r_5}^{(1)} = \{(\alpha_2 \circ p^{r_2}, u_2, \alpha_5 \circ p^{r_5}) | u_2 \in \mathbb{Z}_{p^k}, \alpha_i \in \mathbb{Z}_{p^{k-r_i}}^{inv} \ (i = 2, 5)\}$;

3) если $a_2 = 0$, то $S = \mathbb{Z}_{p^k}^3$.

2. Пусть $a_1 \neq 0$ и $a_2 \in \mathbb{Z}_{p^k}^{inv}$. Тогда система уравнений (4.49) принимает вид

$$\begin{cases} a_2^{-1} \circ a_1 \circ u_1 \circ u_2 \oplus u_3 = 0 \\ u_1 = 0 \end{cases}.$$

Следовательно, $S = \{(0, u_2, 0) | u_2 \in \mathbb{Z}_{p^k}\}$.

3. Пусть $a_1 \neq 0$ и $a_2 = 0$. Тогда система уравнений (4.49) принимает вид

$$\begin{cases} a_1 \circ u_1 \circ u_2 \oplus 0 \circ u_3 = 0 \\ 0 \circ u_1 = 0 \end{cases}.$$

Следовательно:

1) если $a_1 \in \mathbb{Z}_{p^k}^{inv}$, то $S = S_1 \cup S_2 \cup S_3$, где

$$S_1 = \{(u_1, 0, u_3) | u_1, u_3 \in \mathbb{Z}_{p^k}\},$$

$$S_2 = \{(0, u_2, u_3) | u_2 \in \mathbb{Z}_{p^k} \backslash \{0\}, u_3 \in \mathbb{Z}_{p^k}\},$$

а

$$S_3 = \bigcup_{r_3=1}^{k-1} \bigcup_{r_2=k-r_3}^{k-1} S_{r_2,r_3}^{(2)},$$

где $S_{r_2,r_3}^{(2)} = \{(\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, u_3) | \alpha_i \in \mathbb{Z}_{p^{k-r_i}}^{inv} \ (i = 2, 3), u_3 \in \mathbb{Z}_{p^k}\}$;

2) если $a_1 = \alpha_1 \circ p^{r_1}$ $(\alpha_1 \in \mathbb{Z}_{p^{k-r_1}}^{inv}, r_1 \in \mathbb{N}_{k-1})$, то $S = \bigcup_{i=1}^{5} S_i$, где

$$S_1 = \{(u_1, 0, u_3) | u_1, u_3 \in \mathbb{Z}_{p^k}\},$$

$$S_2 = \{(0, u_2, u_3) | u_2 \in \mathbb{Z}_{p^k} \backslash \{0\}, u_3 \in \mathbb{Z}_{p^k}\},$$

$$S_3 = \bigcup_{r_2=k-r_1}^{k-1} \{(\alpha_2 \circ p^{r_2}, u_2, u_3) | \alpha_2 \in \mathbb{Z}_{p^{k-r_2}}^{inv}, u_2 \in \mathbb{Z}_{p^k}^{inv}, u_3 \in \mathbb{Z}_{p^k}\},$$

$$S_4 = \bigcup_{r_3=k-r_1}^{k-1} \{(u_1, \alpha_3 \circ p^{r_3}, u_3) | u_1 \in \mathbb{Z}_{p^k}^{inv}, \alpha_3 \in \mathbb{Z}_{p^{k-r_3}}^{inv}, u_3 \in \mathbb{Z}_{p^k}\},$$

а

$$S_5 = \bigcup_{r_2=1}^{k-1} \bigcup_{r_3=\max\{k-r_1-r_2,1\}}^{k-1} S_{r_2,r_3}^{(3)},$$

где $S_{r_2,r_3}^{(3)} = \{(\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, u_3) | \alpha_i \in \mathbb{Z}_{p^{k-r_i}}^{inv} \ (i = 2, 3), u_3 \in \mathbb{Z}_{p^k}\}$.

4. Пусть $a_1 \neq 0$ и $a_2 = \alpha_4 \circ p^{r_4}$ $(\alpha_4 \in \mathbb{Z}_{p^{k-r_4}}^{inv}, r_4 \in \mathbb{N}_{k-1})$.

1) если $a_1 \in \mathbb{Z}_{p^k}^{inv}$, то $S = \bigcup_{i=1}^{7} S_i$, где

$$S_1 = \{(0, u_2, 0) | u_2 \in \mathbb{Z}_{p^k}\},$$

$$S_2 = \bigcup_{r_5=k-r_4}^{k-1} \{(0, u_2, \alpha_5 \circ p^{r_5}) | u_2 \in \mathbb{Z}_{p^k}, \alpha_5 \in \mathbb{Z}_{p^{k-r_5}}^{inv}\},$$

$$S_3 = \bigcup_{r_2=k-r_4}^{k-1} \{(\alpha_2 \circ p^{r_2}, 0, 0) | \alpha_2 \in \mathbb{Z}_{p^{k-r_2}}^{inv}\},$$

$$S_4 = \bigcup_{r_2=k-r_4}^{k-1} \bigcup_{r_5=k-r_4}^{k-1} S^{(4)}_{r_2,r_5},$$

где $S^{(4)}_{r_2,r_5} = \{(\alpha_2 \circ p^{r_2}, 0, \alpha_5 \circ p^{r_5}) | \alpha_i \in \mathbb{Z}^{inv}_{p^{k-r_i}} \ (i = 2,5)\}$,

$$S_5 = \bigcup_{r_2=k-r_4}^{k-1} \bigcup_{r_3=k-r_2}^{k-1} S^{(5)}_{r_2,r_3},$$

где $S^{(5)}_{r_2,r_3} = \{(\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, 0) | \alpha_i \in \mathbb{Z}^{inv}_{p^{k-r_i}} \ (i = 2,3)\}$,

$$S_6 = \bigcup_{r_2=k-r_4}^{k-1} \bigcup_{r_3=k-r_2}^{k-1} \bigcup_{r_5=k-r_4}^{k-1} S^{(6)}_{r_2,r_3,r_5},$$

где $S^{(6)}_{r_2,r_3,r_5} = \{(\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, \alpha_5 \circ p^{r_5}) | \alpha_i \in \mathbb{Z}^{inv}_{p^{k-r_i}} \ (i = 2,3,5)\}$,

$$S_7 = \bigcup_{r_2=k-r_4}^{k-2} \bigcup_{r_3=1}^{k-1-r_2} \left(\widetilde{S}^{(7)}_{r_2,r_3} \cup \bigcup_{r_6=\max\{1,k-r_2-r_3\}}^{k-1} \widehat{S}^{(7)}_{r_2,r_3,r_6} \right),$$

где:

а) $\widetilde{S}^{(7)}_{r_2,r_3} = \emptyset$, если $r_2 + r_3 < r_4 + 1$, а при $r_2 + r_3 \geq r_4 + 1$ множество $\widetilde{S}^{(7)}_{r_2,r_3}$ состоит из всех таких упорядоченных троек $(\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, \alpha_5 \circ p^{r_2+r_3-r_4})$, что $\alpha_i \in \mathbb{Z}^{inv}_{p^{k-r_i}}$ $(i = 2,3)$ и $\alpha_5 = (\ominus a_1 \circ {\alpha_4}^{-1} \circ \alpha_2 \circ \alpha_3) \ (mod\ p^{r_2+r_3-r_4})$;

б) $\widehat{S}^{(7)}_{r_2,r_3,r_6} = \emptyset$, если $r_2 + r_3 < r_4 + 1$, а при $r_2 + r_3 \geq r_4 + 1$ множество $\widehat{S}^{(7)}_{r_2,r_3,r_6}$ состоит из всех таких упорядоченных троек $(\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, \alpha_5 \circ p^{r_2+r_3-r_4})$, что $\alpha_i \in \mathbb{Z}^{inv}_{p^{k-r_i}}$ $(i = 2,3)$, а $\alpha_5 = (a_1 \circ {\alpha_4}^{-1} \circ (\alpha_6 \circ p^{r_6} \ominus \alpha_2 \circ \alpha_3)) \ (mod\ p^{r_2+r_3-r_4})$ $(\alpha_6 \in \mathbb{Z}^{inv}_{p^{k-r_6}})$;

2) если $a_1 = \alpha_1 \circ p^{r_1}$ $(\alpha_1 \in \mathbb{Z}^{inv}_{p^{k-r_1}}, r_1 \in \mathbb{N}_{k-1}$, то $S = \bigcup_{i=1}^{8} S_i$, где

$$S_1 = \{(0, u_2, 0) | u_2 \in \mathbb{Z}_{p^k}\},$$

$$S_2 = \bigcup_{r_5=k-r_4}^{k-1} \{(0, u_2, \alpha_5 \circ p^{r_5}) | u_2 \in \mathbb{Z}_{p^k}, \alpha_5 \in \mathbb{Z}^{inv}_{p^{k-r_5}}\},$$

$$S_3 = \bigcup_{r_2=k-r_4}^{k-1} \{(\alpha_2 \circ p^{r_2}, 0, 0) | \alpha_2 \in \mathbb{Z}^{inv}_{p^{k-r_2}}\},$$

$$S_4 = \bigcup_{r_2=k-r_4}^{k-1} \bigcup_{r_5=k-r_4}^{k-1} S^{(4)}_{r_2,r_5},$$

где $S^{(4)}_{r_2,r_5} = \{(\alpha_2 \circ p^{r_2}, 0, \alpha_5 \circ p^{r_5}) | \alpha_i \in \mathbb{Z}^{inv}_{p^{k-r_i}} \ (i = 2,5)\}$,

$$S_5 = \bigcup_{r_2=\max\{k-r_1,k-r_4\}}^{k-1} \{\alpha_2 \circ p^{r_2}, u_2, 0) | \alpha_2 \in \mathbb{Z}^{inv}_{p^{k-r_2}}, u_2 \in \mathbb{Z}^{inv}_{p^k}\},$$

$$S_6 = \bigcup_{r_2=k-r_4}^{k-1} \bigcup_{r_3=\max\{1,k-r_1-r_2\}}^{k-1} S^{(6)}_{r_2,r_3},$$

где $S^{(6)}_{r_2,r_3} = \{(\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, 0) | \alpha_i \in \mathbb{Z}^{inv}_{p^{k-r_i}} \ (i = 2,3)\}$,

$$S_7 = \bigcup_{r_2=k-r_4}^{k-1} \bigcup_{r_3=\max\{1,k-r_1-r_2\}}^{k-1} \bigcup_{r_5=k-r_4}^{k-1} S^{(7)}_{r_2,r_3,r_5},$$

где $S^{(7)}_{r_2,r_3,r_5} = \{(\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, \alpha_5 \circ p^{r_5}) | \alpha_i \in \mathbb{Z}^{inv}_{p^{k-r_i}} \ (i = 2,3,5)\}$,

$$S_8 = \bigcup_{r_2=k-r_4}^{k-1} \bigcup_{r_3=1}^{k-1-r_1-r_2} \left(\widetilde{S}^{(8)}_{r_2,r_3} \cup \bigcup_{r_6=\max\{1,k-r_1-r_2-r_3\}}^{k-1} \widehat{S}^{(8)}_{r_2,r_3,r_6} \right),$$

где

а) $\widetilde{S}^{(8)}_{r_2,r_3} = \emptyset$, если $r_2 + r_3 < r_4 - r_1 + 1$, а при $r_2 + r_3 \geq r_4 - r_1 + 1$ множество $\widetilde{S}^{(8)}_{r_2,r_3}$ состоит из всех таких упорядоченных троек $(\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, \alpha_5 \circ p^{r_1+r_2+r_3-r_4})$, что $\alpha_i \in \mathbb{Z}^{inv}_{p^{k-r_i}}$ $(i = 2,3)$, а $\alpha_5 = (\ominus\alpha_1 \circ {\alpha_4}^{-1} \circ \alpha_2 \circ \alpha_3) \ (mod\, p^{r_1+r_2+r_3-r_4})$;

б) $\widehat{S}^{(8)}_{r_2,r_3,r_6} = \emptyset$, если $r_2 + r_3 < r_4 - r_1 + 1$, а при $r_2 + r_3 \geq r_4 - r_1 + 1$ множество $\widehat{S}^{(8)}_{r_2,r_3,r_6}$ состоит из всех таких упорядоченных троек $(\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, \alpha_5 \circ p^{r_1+r_2+r_3-r_4})$, что $\alpha_i \in \mathbb{Z}^{inv}_{p^{k-r_i}}$ $(i = 2,3)$, а $\alpha_5 = (\alpha_1 \circ {\alpha_4}^{-1} \circ (\alpha_6 \circ p^{r_6} \ominus \alpha_2 \circ \alpha_3)) \ (mod\, p^{r_1+r_2+r_3-r_4})$ $(\alpha_6 \in \mathbb{Z}^{inv}_{p^{k-r_6}})$.

3.2. Свойства делителей нуля в ассоциативном кольце.

Исследование множества решений уравнения с параметрами, имеющего вид «произведение равно нулю» является одной из модельных задач, возникающих при анализе различных конструкций, построенных над ассоциативным кольцом. Целью настоящего пункта является исследование свойств делителей нуля в ассоциативных кольцах с целью разработки математического аппарата, применимого при решении таких уравнений.

3.2.1. Основные понятия и обозначения.

Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо. Тогда $K = K^{inv} \cup K^{non-inv}$, где K^{inv} и $K^{non-inv} = K \backslash K^{inv}$ – множество, соответственно, обратимых и необратимых элементов кольца $\mathcal{K}$.

Замечание 3.7. Так как $0 \in K^{non-inv}$, то $K^{non-inv} \neq \emptyset$. Отметим, что если $\mathcal{K}$ – кольцо с единицей и $u \in K^{non-inv}$, то $u^l \neq 1$ для всех $l \in \mathbb{N}$.

При этом, если $\mathcal{K}$ – кольцо без единицы, то $K^{inv} = \emptyset$, а если $\mathcal{K}$ – кольцо с единицей, то

$$K^{inv} = \{x \in K | (\exists x^{-1} \in K)(xx^{-1} = x^{-1}x = 1)\}. \qquad (3.51)$$

Элементы $a, b \in K^{non-inv}\backslash\{0\}$ называются делителями нуля кольца $\mathcal{K}$, если $ab = 0$.

Обозначим через $K^{z.d}$ множество всех делителей нуля кольца $\mathcal{K}$ и положим $K^{non-z.d} = K\backslash(K^{z.d} \cup \{0\})$.

Рассмотрим теперь аналоги этих понятий для ассоциативного не коммутативного кольца $\mathcal{K} = (K, +, \cdot)$.

Множество $K^{l.inv}$ обратимых слева элементов кольца $\mathcal{K}$ определяется следующим образом:

$$K^{l.inv} = \begin{cases} \emptyset, & \text{если } \mathcal{K} \text{ – кольцо без единицы} \\ \{x \in K | (\exists a \in K)(ax = 1)\}, & \text{если } \mathcal{K} \text{ – кольцо с единицей} \end{cases}.$$

Аналогичным образом определяется множество $K^{r.inv}$ обратимых справа элементов кольца $\mathcal{K}$, а именно:

$$K^{r.inv} = \begin{cases} \emptyset, & \text{если } \mathcal{K} \text{ – кольцо без единицы} \\ \{x \in K | (\exists a \in K)(xa = 1)\}, & \text{если } \mathcal{K} \text{ – кольцо с единицей} \end{cases}.$$

Множество $K^{non-l.inv} = K\backslash K^{l.inv}$ называется множеством необратимых слева, а множество $K^{non-r.inv} = K\backslash K^{r.inv}$ – множеством необратимых справа элементов кольца $\mathcal{K}$.

Замечание 3.8. Таким образом, относительно понятия «обратимость элемента» ассоциативные не коммутативные кольца имеют «более тонкое строение», чем ассоциативно-коммутативные кольца, характеризуемое следующим образом.

В ассоциативно-коммутативном кольце $\mathcal{K} = (K, +, \cdot)$ выделяются непересекающиеся подмножества K^{inv} обратимых и $K^{non-inv}$ необратимых элементов, объединение которых – множество K.

В ассоциативном не коммутативном кольце $\mathcal{K} = (K, +, \cdot)$ выделяются следующие четыре непересекающиеся подмножества, объединение которых – множество K:

1) подмножество $K^{inv} = K^{l.inv} \cap K^{r.inv}$ обратимых (в обычном смысле этого слова) элементов кольца $\mathcal{K}$, т.е. для этого множества истинно равенство (3.51);

2) подмножество $K^{l.inv}\backslash K^{r.inv} = K^{l.inv} \cap K^{non-r.inv}$ обратимых слева, но не обратимых справа элементов;

3) подмножество $K^{r.inv}\backslash K^{l.inv} = K^{r.inv} \cap K^{non-l.inv}$ обратимых справа, но не обратимых слева элементов;

4) подмножество $K^{non-l.inv} \cap K^{non-r.inv} = K\backslash(K^{l.inv} \cup K^{r.inv})$ элементов, которые не обратимы ни слева, ни справа.

Элемент $x \in K^{non-l.inv}\backslash\{0\}$ (соответственно, $y \in K^{non-r.inv}\backslash\{0\}$) называется левым (соответственно, правым) делителем нуля кольца $\mathcal{K}$, если существует такой элемент $u \in K\backslash\{0\}$ (соответственно, $v \in K\backslash\{0\}$), что $xu = 0$ (соответственно, $vy = 0$).

Обозначим через $K^{z.l.d}$ множество всех левых делителей нуля кольца $\mathcal{K}$, а через $K^{z.r.d}$ множество всех правых делителей нуля кольца $\mathcal{K}$ и положим $K^{non-z.l.d} = K\backslash(K^{z.l.d} \cup \{0\})$ и $K^{non-z.r.d} = K\backslash(K^{z.r.d} \cup \{0\})$.

Замечание 3.9. Таким образом, относительно понятия «быть делителем нуля» ассоциативные не коммутативные кольца имеют «более тонкое строение», чем ассоциативно-коммутативные кольца, характеризуемое следующим образом.

В ассоциативно-коммутативном кольце $\mathcal{K} = (K, +, \cdot)$ выделяются непересекающиеся подмножества $K^{z.d}$ делителей нуля и $K^{non-z.d}$ ненулевых элементов, не являющихся делителями нуля, причем объединение этих подмножеств – множество $K\backslash\{0\}$.

В ассоциативном не коммутативном кольце $\mathcal{K} = (K, +, \cdot)$ выделяются следующие четыре непересекающиеся подмножества, объединение которых – множество $K\backslash\{0\}$:

1) подмножество $K^{z.d} = K^{z.l.d} \cap K^{z.r.d}$ (двусторонних) делителей нуля;

2) подмножество $K^{z.l.d}\backslash K^{z.r.d} = K^{z.l.d} \cap K^{non-z.r.d}$ элементов, являющихся левыми делителями нуля, но не являющихся правыми делителями нуля;

3) подмножество $K^{z.r.d}\backslash K^{z.l.d} = K^{z.r.d} \cap K^{non-z.l.d}$ элементов, являющихся правыми делителями нуля, но не являющихся левыми делителями нуля;

4) подмножество $K^{non-z.l.d} \cap K^{non-z.r.d} = K\backslash(K^{z.l.d} \cup K^{z.r.d} \cup \{0\})$ элементов, которые не являются ни левыми, ни правыми делителями нуля.

Из замечаний 3.8 и 3.9 вытекает, что относительно понятий «обратимость элемента» и «быть делителем нуля» ассоциативные не коммутативные кольца и ассоциативно-коммутативные кольца можно рассматривать с единой точки зрения, просто полагая, что в последнем случае истинны равенства

$$K^{l.inv} = K^{r.inv} = K^{inv}$$

и

$$K^{z.l.d} = K^{z.r.d} = K^{z.d}.$$

Поэтому в дальнейшем, до конца данного раздела, если в явном виде не оговорено противное, то под кольцом $\mathcal{K} = (K, +, \cdot)$ понимается ассоциативное (возможно, не коммутативное) кольцо.

Из определения множеств левых и правых делителей нуля ассоциативного кольца $\mathcal{K} = (K, +, \cdot)$ непосредственно вытекает, что истинны следующие утверждения.

Утверждение 3.7. Если $\mathcal{K} = (K, +, \cdot)$ – ассоциативное кольцо, то $K^{z.l.d} \neq \emptyset$ тогда и только тогда, когда $K^{z.r.d} \neq \emptyset$.□

Утверждение 3.8. В каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$ если $x \in K^{z.l.d}$, то $-x \in K^{z.l.d}$, а если $y \in K^{z.r.d}$, то $-y \in K^{z.r.d}$.□

Утверждение 3.9. В каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$ если $x \neq 0$, то $x \in K^{z.d}$ тогда и только тогда, когда существуют такие элементы $a \in K^{z.l.d}$ и $b \in K^{z.r.d}$, что $ax = 0$ и $xb = 0$.□

Утверждение 3.10. Формулы

$$ax \in \begin{cases} K^{z.l.d}, & \text{если } a \in K^{non-z.l.d} \cup \{0\}) \\ K^{z.l.d} \cup \{0\}, & \text{иначе,} \end{cases} \quad (x \in K^{z.l.d})$$

и

$$ya \in \begin{cases} K^{z.r.d}, & \text{если } a \in K^{non-z.r.d} \cup \{0\}) \\ K^{z.r.d} \cup \{0\}, & \text{иначе.} \end{cases} \quad (y \in K^{z.r.d})$$

истинны в каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$.□

Из утверждения 3.10 вытекает, что истинны следующие три следствия.

Следствие 3.1. В каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$ с единицей если $a \in K^{l.inv}$, то $ax \in K^{z.l.d}$ $(x \in K^{z.l.d})$, а если $a \in K^{r.inv}$, то $ya \in K^{z.r.d}$ $(y \in K^{z.r.d})$.□

Следствие 3.2. В каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$ если $x \in K^{z.l.d} \backslash K^{z.r.d}$ (соответственно, $y \in K^{z.r.d} \backslash K^{z.l.d}$), то $ax \in K^{z.l.d}$ (соответственно, $yb \in K^{z.r.d}$) для любого элемента $a \neq 0$ (соответственно, для любого элемента $b \neq 0$).□

Следствие 3.3. В каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$ если $x \in K^{z.l.d}$ и $y \in K^{z.r.d}$, то $yx \in K^{z.d} \cup \{0\}$.□

Утверждение 3.11. В каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$ если $K^{z.l.d} \neq \emptyset$ (или, что то же самое, $K^{z.r.d} \neq \emptyset$), то $K^{z.d} = \emptyset$ тогда и только тогда, когда $(K^{z.l.d}, \cdot)$ и $(K^{z.r.d}, \cdot)$ являются подполугруппами полугруппы $(K, \cdot)$.□

Утверждение 3.12. Для любого подкольца $\mathcal{U} = (U, +, \cdot)$ ассоциативного кольца $\mathcal{K} = (K, +, \cdot)$ истинны равенства $K^{z.l.d} \cap U = U^{z.l.d}$ и $K^{z.r.d} \cap U = U^{z.r.d}$.□

Следствие 3.4. Если $\mathcal{U}$ – коммутативное подкольцо ассоциативного кольца $\mathcal{K}$, то истинны равенства $K^{z.l.d} \cap U = K^{z.r.d} \cap U = U^{d}$.□

Нетрудно убедиться в том, что истинны следующие утверждения, характеризующие множества левых и правых делителей нуля ассоциативного кольца в терминах его центра.

Утверждение 3.13. В каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$ истинно равенство $K^{z.l.d} \cap K^{cntr} = K^{z.r.d} \cap K^{cntr} = K^{z.d}$.□

Утверждение 3.14. Если $\mathcal{K} = (K, +, \cdot)$ – ассоциативное кольцо, то $K^{z.l.d} \subseteq K^{cntr}$ тогда и только тогда, когда $K^{z.r.d} \subseteq K^{cntr}$.□

Утверждение 3.15. В каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$ если $K^{z.l.d} \subseteq K^{cntr}$ (или, что то же самое, $K^{z.r.d} \subseteq K^{cntr}$), то истинны равенства $K^{z.l.d} = K^{z.r.d} = K^{z.d}$.□

Нетрудно убедиться в том, что истинны следующие утверждения, характеризующие множества левых и правых делителей нуля в терминах гомоморфизмов колец.

Утверждение 3.16. Если φ – гомоморфизм ассоциативного кольца $\mathcal{K}_1 = (K_1, +_1, \cdot_1)$ в кольцо $\mathcal{K}_2 = (K_2, +_2, \cdot_2)$, то истинны включения $\varphi(K_1^{z.l.d}) \subseteq K_2^{z.l.d} \cup \{0\}$ и $\varphi(K_1^{z.r.d}) \subseteq K_2^{z.r.d} \cup \{0\}$.$\square$

Следствие 3.5. Для любого эндоморфизма φ ассоциативного кольца $\mathcal{K}$ истинны включения $\varphi(K^{z.l.d}) \subseteq K^{z.l.d} \cup \{0\}$ и $\varphi(K^{z.r.d}) \subseteq K^{z.r.d} \cup \{0\}$.$\square$

Утверждение 3.17. Если φ – изоморфизм ассоциативного кольца $\mathcal{K}_1 = (K_1, +_1, \cdot_1)$ в кольцо $\mathcal{K}_2 = (K_2, +_2, \cdot_2)$, то истинны включения $\varphi(K_1^{z.l.d}) \subseteq K_2^{z.l.d}$ и $\varphi(K_1^{z.r.d}) \subseteq K_2^{z.r.d}$.$\square$

Следствие 3.6. Для любого изоморфизма φ ассоциативного кольца $\mathcal{K}$ в себя истинны включения $\varphi(K^{z.l.d}) \subseteq K^{z.l.d}$ и $\varphi(K^{z.r.d}) \subseteq K^{rd}$.$\square$

Утверждение 3.18. Если φ – автоморфизм ассоциативного кольца $\mathcal{K}$, то истинны равенства $\varphi(K^{z.l.d}) = K^{z.l.d}$ и $\varphi(K^{z.r.d}) = K^{z.r.d}$.

В дальнейшем, до конца данного раздела, если в явном виде не оговорено противное, считаем, что $\mathcal{K} = (K, +, \cdot)$ – такое ассоциативное кольцо, что $K^{z.l.d} \neq \emptyset$ (и, следовательно, $K^{z.r.d} \neq \emptyset$).

Множества $K^{z.l.d}$ и $K^{z.r.d}$ однозначно определяют в ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$ семейства множеств

$$A_x^r = \{u \in K^{z.r.d} | xu = 0\} \ (x \in K \backslash \{0\}) \tag{3.52}$$

и

$$A_y^l = \{v \in K^{z.l.d} | vy = 0\} \ (y \in K \backslash \{0\}). \tag{3.53}$$

Из (3.52) и (3.53) непосредственно вытекает, что

$$(\forall x \in K \backslash \{0\})(A_x^r \neq \emptyset \Leftrightarrow x \in K^{z.l.d}),$$

$$(\forall y \in K \backslash \{0\})(A_y^l \neq \emptyset \Leftrightarrow y \in K^{z.r.d})$$

и

$$(\forall a, b \in K \backslash \{0\})((ab = 0) \Leftrightarrow (a \in A_b^l) \& (b \in A_a^r)).$$

Замечание 3.10. Если $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо, то

$$A_x^r = A_x^l = A_x \ (x \in K \backslash \{0\}),$$

где

$$A_x = \{u \in K^{z.d} | xu = 0\}.$$

Семейства множеств (3.52) и (3.53) играют важную роль при решении уравнений вида «произведение равно нулю» над ассоциативном кольцом $\mathcal{K} = (K, +, \cdot)$. Проиллюстрируем это обстоятельство на примере.

Пример 3.5. Предположим, что кольцо $\mathcal{K} = (K, +, \cdot)$ является ассоциативным кольцом.

1. Пусть $n \in \mathbb{N}$ и $a_1, \ldots, a_n \in K \backslash \{0\}$.

Решение системы уравнений

$$a_i x = 0 \ (i = 1, \ldots, n)$$

имеет вид

$$x \in \{0\} \cup \bigcap_{i=1}^{n} A^r_{a_i}.$$

Аналогичным образом, решение системы уравнений

$$x a_i = 0 \ (i = 1, \ldots, n)$$

имеет вид

$$x \in \{0\} \cup \bigcap_{i=1}^{n} A^l_{a_i}.$$

2. Пусть $n \in \mathbb{N}$ и $a \in K \backslash \{0\}$.

Решение уравнения

$$a x^n = 0$$

имеет вид

$$x \in \{0\} \cup \{y \in K^{non-r.inv} \backslash \{0\} | y^n \in A^r_a\}.$$

Аналогичным образом, решение уравнения

$$x^n a = 0$$

имеет вид

$$x \in \{0\} \cup \{y \in K^{non-l.inv} \backslash \{0\} | y^n \in A^l_a\}.$$

3. Пусть $a \in K$.

Решение уравнения

$$x^2 + ax = 0$$

имеет вид

$$x \in \{0, -a\} \cup \{b \in K^{non-r.inv} | (b + a \in K^{non-l.inv}) \& (b \in (A^l_b - a) \cap A^r_{b+a})\}.$$

Аналогичным образом, решение уравнения

$$x^2 + xa = 0$$

имеет вид

$$x \in \{0, -a\} \cup \{b \in K^{non-l.inv} | (b + a \in K^{non-r.inv}) \& (b \in (A^r_b - a) \cap A^l_{b+a})\}.$$

4. Решение уравнения

$$f_1(x)f_2(y) = 0$$

имеет вид

$$(x,y) \in \{(a,b) \in K^2 | (f_1(a) = 0) \vee (f_2(b) = 0)\} \cup$$
$$\cup \{(a,b) \in K^2 | (f_1(a) \neq 0) \& (f_2(b) \neq 0) \& (f_1(a) \in A^l_{f_2(b)}) \& (f_2(b) \in A^r_{f_1(a)})\}.$$

Рассмотренный пример показывает, что исследование теоретико-множественных и алгебраических свойств семейств множеств (3.52) и (3.53) имеет важное значение для анализа строения множества решений уравнений с параметрами, имеющих вид «произведение равно нулю».

3.2.2. Свойства множеств I^r_x $(x \in K^{z.l.d})$ и I^l_y $(y \in K^{z.r.d})$.

Зафиксируем ассоциативное кольцо $\mathcal{K} = (K, +, \cdot)$.

Так как

$$\bigcup_{x \in K^{z.l.d}} A^r_x = K^{z.r.d}$$

и

$$\bigcup_{y \in K^{z.r.d}} A^l_y = K^{z.l.d},$$

то семейство множеств A^r_x $(x \in K^{z.l.d})$ (соответственно, семейство множеств A^l_y $(y \in K^{z.r.d})$) представляет собой покрытие множества $K^{z.r.d}$ (соответственно, множества $K^{z.l.d}$) не пустыми подмножествами.

Следующее утверждение характеризует соотношение между этими покрытиями.

Утверждение 3.19. Формулы

$$x \in \bigcap_{u \in A^r_x} A^l_u \ (x \in K^{z.l.d}) \tag{3.54}$$

и

$$y \in \bigcap_{v \in A^l_y} A^r_v \ (y \in K^{z.r.d}). \tag{3.55}$$

истинны в каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$.□

Доказательство. Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативное кольцо.

Из (3.52) вытекает, что истинна формула

$$(\forall x \in K^{z.l.d})(\forall u \in A^r_x)(x \in A^l_u),$$

откуда следует, что истинна формула (3.54).

Аналогичным образом, из (3.53) вытекает, что истинна формула

$$(\forall y \in K^{z.r.d})(\forall v \in A_y^l)(y \in A_v^r),$$

откуда следует, что истинна формула (3.55).□

Назовем множество

$$I_x^r = A_x^r \cup \{0\} \ (x \in K^{z.l.d})$$

правым аннулятором элемента x, а множество

$$I_y^l = A_y^l \cup \{0\} \ (y \in K^{z.r.d})$$

назовем левым аннулятором элемента y.

Отметим, что если $\mathcal{K}$ – ассоциативно-коммутативное кольцо, то

$$I_x^r = I_x^l = I_x \ (x \in K^{z.d}),$$

где множество I_x $(x \in K^{z.d})$ – аннулятор элемента x.

Утверждение 3.20. В каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$ каждое множество I_x^r $(x \in K^{z.l.d})$ является правым идеалом, а каждое множество I_y^l $(y \in K^{z.r.d})$ является левым идеалом.□

Доказательство. Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативное кольцо.

Для любого элемента $x \in K^{z.l.d}$ и для любых элементов $a, b \in I_x^r$

$$x(a \pm b) = xa \pm xb = 0 \pm 0 = 0,$$

откуда вытекает, что $a \pm b \in I_x^r$.

Следовательно, $(I_x^r, +)$ $(x \in K^{z.l.d})$ – подгруппа аддитивной группы кольца $\mathcal{K}$.

Аналогичным образом, для любого элемента $y \in K^{z.r.d}$ и для любых элементов $a, b \in I_y^l$

$$(a \pm b)y = ay \pm by = 0 \pm 0 = 0,$$

откуда вытекает, что $a \pm b \in I_y^l$.

Следовательно, $(I_y^l, +)$ $(y \in K^{z.r.d})$ – подгруппа аддитивной группы кольца $\mathcal{K}$.

Для любого элемента $x \in K^{z.l.d}$ и для любых элементов $a \in I_x^r$ и $b \in K$

$$x(ab) = (xa)b = 0b = 0,$$

откуда вытекает, что $ab \in I_x^r$ для любых $a \in I_x^r$ и $b \in K$.

Следовательно, каждое множество I_x^r $(x \in K^{z.l.d})$ является правым идеалом кольца $\mathcal{K}$.

Аналогичным образом, для любого элемента $y \in K^{z.r.d}$ и для любых элементов $a \in I_y^l$ и $b \in K$

$$(ba)y = b(ay) = b0 = 0,$$

откуда вытекает, что $ba \in I_y^l$ для любых $a \in I_y^l$ и $b \in K$.

Следовательно, каждое множество I_y^l $(y \in K^{z.r.d})$ является левым идеалом кольца $\mathcal{K}$.□

Таким образом, в ассоциативном кольце $\mathcal{K}$ семейство множеств A_x^r $(x \in K^{z.l.d})$ определяет семейство правых идеалов I_x^r $(x \in K^{z.l.d})$, а семейство множеств A_y^l $(y \in K^{z.r.d})$ – семейство левых идеалов I_y^l $(y \in K^{z.r.d})$.

Охарактеризуем эти семейства идеалов.

Утверждение 3.21. Равенства

$$I_{-x}^r = I_x^r \quad (x \in K^{z.l.d}), \tag{3.56}$$

$$I_{-y}^l = I_y^l \quad (y \in K^{z.r.d}). \tag{3.57}$$

истинны в каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$.□

Доказательство. Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативное кольцо.

Зафиксируем элемент $x \in K^{z.l.d}$. Из утверждения 3.8 вытекает, что $-x \in K^{z.l.d}$.

Пусть $a \in I_x^r$. Тогда $xa = 0$.

Следовательно,

$$(-x)a = -xa = -0 = 0,$$

т.е. $a \in I_{-x}^r$.

Итак, показано, что истинно включение

$$I_x^r \subseteq I_{-x}^r.$$

Пусть $a \in I_{-x}^r$. Тогда $(-x)a = 0$.

Следовательно,

$$xa = -(-x)a = -0 = 0,$$

т.е. $a \in I_x^r$.

Итак, показано, что истинно включение

$$I_{-x}^r \subseteq I_x^r.$$

Из включений $I_x^r \subseteq I_{-x}^r$ и $I_{-x}^r \subseteq I_x^r$ вытекает равенство (3.56).

Равенство (3.57) доказывается аналогично.□

Утверждение 3.22. Включения

$$I_u^l \cap I_v^l \subseteq I_{u+v}^l \quad (u, v, u+v \in K^{z.r.d}), \tag{3.58}$$

$$I_u^l \cap I_v^l \subseteq I_{u-v}^l \quad (u, v, u-v \in K^{z.r.d}), \tag{3.59}$$

$$I_u^r \cap I_v^r \subseteq I_{u+v}^r \quad (u, v, u+v \in K^{z.l.d}), \tag{3.60}$$

$$I_u^r \cap I_v^r \subseteq I_{u-v}^r \quad (u, v, u-v \in K^{z.l.d}). \tag{3.61}$$

истинны в каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$.□

Доказательство. Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативное кольцо.

Зафиксируем элементы $u, v \in K^{z.r.d}$.

Пусть $a \in I_u^l \cap I_v^l$. Тогда $au = 0$ и $av = 0$.

Следовательно,

$$a(u \pm v) = au \pm av = 0 \pm 0 = 0.$$

Из равенств $a(u \pm v) = 0$ вытекает, что если $u+v \in K^{z.r.d}$, то $a \in I_{u+v}^l$, т.е. истинно включение (3.58), а если $u - v \in K^{z.r.d}$, то $a \in I_{u-v}^l$, т.е. истинно включение (3.59).

Включения (3.60) и (3.61) доказываются аналогичным образом.□

Напомним, что произведением подмножеств $X, Y \subseteq K$ (взятых именно в этом порядке) называется множество XY, состоящее из всех таких конечных сумм $\sum\limits_{i=1}^{n} x_i y_i$ $(n \in \mathbb{N})$, что $x_i \in X$ и $y_i \in Y$ для всех $i = 1, \ldots, n$.

Утверждение 3.23. В каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$ для любых элементов $x \in K^{z.l.d}$ и $y \in K^{z.r.d}$ множество $I_y^l I_x^r$ является двусторонним идеалом.□

Доказательство. Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативное кольцо.

Так как $(I_x^r, +)$ $(x \in K^{z.l.d})$ и $(I_y^l, +)$ $(y \in K^{z.r.d})$ – подгруппы аддитивной группы кольца $\mathcal{K}$, то $(I_y^l I_x^r, +)$ также является подгруппой аддитивной группы кольца $\mathcal{K}$.

Пусть $u \in I_y^l I_x^r$. Тогда существует такое $n \in \mathbb{N}$, что $u = \sum\limits_{i=1}^{n} v_i w_i$, где $v_i \in I_y^l$ и $w_i \in I_x^r$ для всех $i = 1, \ldots, n$.

Так как множество I_y^l – левый идеал кольца $\mathcal{K}$ и $v_i \in I_y^l$ $(i = 1, \ldots, n)$, то $av_i = \alpha_i \in I_y^l$ $(i = 1, \ldots, n)$ для любого элемента $a \in K$.

Следовательно,

$$au = a \sum_{i=1}^{n} v_i w_i = \sum_{i=1}^{n} (av_i) w_i = \sum_{i=1}^{n} \alpha_i w_i \in I_y^l I_x^r$$

для любого элемента $a \in K$, т.е. множество $I_y^l I_x^r$ является левым идеалом кольца $\mathcal{K}$.

Аналогичным образом доказывается, что множество $I_y^l I_x^r$ – правый идеал кольца $\mathcal{K}$.

Так как множество $I_y^l I_x^r$ является как левым, так и правым идеалом кольца $\mathcal{K}$, то оно является двусторонним идеалом кольца $\mathcal{K}$.□

Элементы семейства I_y^l $(y \in K^{z.r.d})$, а так же элементы семейства I_x^r $(x \in K^{z.l.d})$ могут не быть попарно различными, соответственно, левыми или правыми идеалами кольца $\mathcal{K}$.

Проиллюстрируем это обстоятельство следующим примером.

Пример 3.6. Для кольца вычетов $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ (где p – простое число, а $k \in \mathbb{N}$ $(k \geq 2)$), которое, как известно, является ассоциативно-коммутативным кольцом с единицей, множество $\mathbb{Z}_{p^k}^{inv}$ состоит из всех чисел $a \in \mathbb{Z}_{p^k} \backslash \{0\}$, взаимно-простых с числом p, а

$$\mathbb{Z}_{p^k}^{z.d} = \mathbb{Z}_{p^k} \backslash (\mathbb{Z}_{p^k}^{inv} \cup \{0\}) = \{ap^i | a \in \mathbb{Z}_{p^k}^{inv};\ i = 1, \ldots, k-1\}.$$

Множества A_{ap^i} $(a \in \mathbb{Z}_{p^k}^{inv};\ i = 1, \ldots, k-1)$ имеют вид

$$A_{ap^i} = \{bp^j | b \in \mathbb{Z}_{p^k}^{inv};\ j = k-i, \ldots, k-1\}, \tag{3.62}$$

а идеалы

$$I_{ap^i} = A_{ap^i} \cup \{0\}\ (a \in \mathbb{Z}_{p^k}^{inv};\ i = 1, \ldots, k-1)$$

определяют все собственные идеалы кольца $\mathcal{Z}_{p^k}$.

Из (3.62) вытекает, что $A_{a_1 p^i} = A_{a_2 p^i}$ $(i = 1, \ldots, k-1)$ для любых $a_1, a_2 \in \mathbb{Z}_{p^k}^{inv}$. Следовательно, $I_{a_1 p^i} = I_{a_2 p^i}$ $(i = 1, \ldots, k-1)$ для любых $a_1, a_2 \in \mathbb{Z}_{p^k}^{inv}$.

Определив на множестве $K^{z.l.d}$ отношение эквивалентности $\sim_l$ формулой

$$x_1 \sim_l x_2 \Leftrightarrow A_{x_1}^r = A_{x_2}^r\ (x_1, x_2 \in K^{z.l.d}),$$

и выбрав по одному представителю a из каждого класса фактор-множества $K^{z.l.d}/_{\sim_l}$, получим все попарно-различные правые идеалы I_a^r, принадлежащие семейству правых идеалов I_x^r $(x \in K^{z.l.d})$.

Аналогичным образом, определив на множестве $K^{z.r.d}$ отношение эквивалентности $\sim_r$ формулой

$$y_1 \sim_r y_2 \Leftrightarrow A_{y_1}^l = A_{y_2}^l\ (y_1, y_2 \in K^{z.r.d}),$$

и выбрав по одному представителю b из каждого класса фактор-множества $K^{z.r.d}/_{\sim_r}$, получим все попарно-различные левые идеалы I_b^l, принадлежащие семейству левых идеалов I_y^l $(y \in K^{z.r.d})$.

Известно, что в каждом ассоциативном кольце $\mathcal{K}$ для любого элемента $u \in K\backslash\{0\}$ последовательность элементов

$$u, u^2, \ldots, u^n, \ldots$$

удовлетворяет в точности одному из следующих трех условий:

Условие 3.1. Все элементы u^n $(n \in \mathbb{N})$ попарно различны (что возможно только в бесконечном кольце $\mathcal{K}$).

Условие 3.2. Существует такое натуральное число $n_u \geq 2$, что $u, \ldots, u^{n_u-1}$ – попарно различные элементы множества $K\backslash\{0\}$ и $u^{n_u} = 0$ (т.е. u – нильпотентный элемент).

Условие 3.3. Существует такое натуральное число $n_u \geq 2$, что $u, \ldots, u^{n_u-1}$ – попарно различные элементы множества $K\backslash\{0\}$ и $u^{n_u} = u^i$ для некоторого числа $i \in \mathbb{N}_{n_u-1}$.

Теорема 3.4. В каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$ включения

$$I^r_u \subseteq I^r_{u^2} \subseteq \cdots \subseteq I^r_{u^k} \ (u \in K^{ld}), \tag{3.63}$$

и

$$I^l_u \subseteq I^l_{u^2} \subseteq \cdots \subseteq I^l_{u^k} \ (u \in K^{rd}) \tag{3.64}$$

истинны для каждого такого элемента $u \in K^{z.l.d} \cup K^{z.r.d}$, что $u, u^2, \ldots, u^k$ $(k \geq 2)$ – элементы множества $K\backslash\{0\}$.□

Доказательство. Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативное кольцо.

Предположим, что $u \in K^{z.l.d}$ и $u, u^2, \ldots, u^k$ $(k \geq 2)$ – элементы множества $K\backslash\{0\}$.

Пусть $a \in I^r_{u^i}$ для некоторого $i \in \mathbb{N}_{k-1}$. Тогда $u^i a = 0$. Следовательно, $u^{i+1}a = u(u^i a) = u0 = 0$, т.е. $a \in I^r_{u^{i+1}}$. Итак, показано, что $I^r_{u^i} \subseteq I^r_{u^{i+1}}$ для всех $i \in \mathbb{N}_{k-1}$. Отсюда вытекает, что включения (3.63) истинны.

Включения (3.64) доказываются аналогичным образом.□

Для элементов множества $K^{z.l.d} \cup K^{z.r.d}$ ситуацию, определяемую условием 3.3, характеризует следующая теорема.

Теорема 3.5. В каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$ с единицей формулы

$$u^i \in A^l_{u^{n_u-i}-1} \cap A^r_{u^{n_u-i}-1} \tag{3.65}$$

и

$$u^{n_u-1} \in (A^l_{u^i} + 1) \cap (A^r_{u^i} + 1) \tag{3.66}$$

истинны для каждого такого элемента $u \in K^{z.l.d} \cup K^{z.r.d}$, что $u, \ldots, u^{n_u-1}$ $(n_u \geq 2)$ – попарно различные элементы множества $K\backslash\{0\}$ и $u^{n_u} = u^i$ для некоторого числа $i \in \mathbb{N}_{n_u-1}$.□

Доказательство. Пусть выполнены условия теоремы.

Так как $u^{n_u} = u^i$, то $u^i(u^{n_u-i} - 1) = 0$ и $(u^{n_u-i} - 1)u^i = 0$.

По условию теоремы $u^i \neq 0$. Кроме того, так как $u \in K^{non-inv}$, то $u^{n_u-i} \neq 1$, т.е. $u^{n_u-i} - 1 \neq 0$.

Поэтому, из равенства $u^i(u^{n_u-i} - 1) = 0$ вытекает, что $u^i \in A^l_{u^{n_u-i}-1}$ и $u^{n_u-1} \in A^r_{u^i}+1$, а из равенства $(u^{n_u-i}-1)u^i = 0$ вытекает, что $u^i \in A^r_{u^{n_u-i}-1}$ и $u^{n_u-1} \in A^l_{u^i} + 1$.

Из соотношений $u^i \in A^l_{u^{n_u-i}-1}$ и $u^i \in A^r_{u^{n_u-i}-1}$ вытекает, что истинна формула (3.65), а из соотношений $u^{n_u-1} \in A^r_{u^i} + 1$ и $u^{n_u-1} \in A^l_{u^i} + 1$ вытекает, что истинна формула (3.66).□

Из теоремы 3.5 непосредственно вытекает, что истинно следующее следствие.

Следствие 3.7. В каждом ассоциативном кольце $\mathcal{K} = (K, +, \cdot)$ с единицей формулы

$$u^i \in (I^l_{u^{l_u-i}-1} \cap I^r_{u^{l_u-i}-1})\backslash\{0\}$$

и

$$u^{l_u-1} \in ((I^l_{u^i}\backslash\{0\}) + 1) \cap ((I^r_{u^i}\backslash\{0\}) + 1)$$

истинны для каждого такого элемента $u \in K^{z.l.d} \cup K^{z.r.d}$, что $u, \ldots, u^{n_u-1}$ $(n_u \geq 2)$ – попарно различные элементы множества $K\backslash\{0\}$ и $u^{n_u} = u^i$ для некоторого числа $i \in \mathbb{N}_{n_u-1}$.□

3.3. Выводы.

В настоящем разделе разработаны основы математического аппарата, предназначенного для исследования строения множества решений системы алгебраических уравнений с параметрами, заданной над ассоциативным (не обязательно коммутативным) кольцом. Основные результаты состоят в следующем:

1. Исследованы свойства классов ассоциированных слева (l-ассоциированных) и ассоциированных справа (r-ассоциированных) элементов ассоциативного кольца.

2. На основе использования этих классов элементов разработана схема унифицированного представления в неявном виде множества решений системы алгебраических уравнений с параметрами, заданной над ассоциативным кольцом.

3. Построена детализация разработанной схемы для представления в неявном виде множества решений системы алгебраических уравнений с

параметрами, заданной над кольцом вычетов $\mathcal{Z}_{p^k}$ (p – простое число, $k \in \mathbb{N}$ ($k \geq 2$)).

4. Исследованы свойства множеств левых и правых делителей нуля ассоциативного кольца.

В своей совокупности полученные в настоящем разделе результаты представляют собой фрагмент теории, которая может быть использована при построении решателей, предназначенных для проверки выполнимости формул над ассоциативным кольцом.

Построение таких решателей актуально с теоретической и с прикладной точки зрения.

Одним из возможных направлений дальнейших исследований является выделение нетривиальных классов систем алгебраических уравнений с параметрами, заданных над ассоциативным кольцом, характеризуемых с позиции сложности представления множеств их решений в терминах классов l-ассоциированных и r-ассоциированных классов элементов.

Другое направление связано с детальным исследованием свойств семейств подмножеств, определяемых, соответственно, правыми и левыми делителями нуля, для тех или иных классов ассоциативных не коммутативных колец с ненулевым умножением.

4. ПРОВЕРКА ВЫПОЛНИМОСТИ ФОРМУЛ ЛИНЕЙНОЙ АРИФМЕТИКИ НАД КОНЕЧНЫМ КОЛЬЦОМ

Известно, что широкий класс как теоретических, так и прикладных задач естественно сводится к проверке выполнимости формулы той или иной разрешимой теории $\mathcal{T}$ 1-го порядка. Такая ситуация, в частности, имеет место в процессе решения ряда модельных задач анализа автоматно-алгебраических моделей, определенных над конечным кольцом (проверка различимости двух фиксированных состояний входным словом заданной длины, проверка достижимости того или иного состояния из заданного состояния, проверка наличия состояний-близнецов, проверка наличия эквивалентных состояний, проверка эквивалентности двух автоматов, проверка наличия неподвижных точек автоматного отображения и т.д.).

Унифицированным средством автоматизированного решения таких задач является решатель, предназначенный для проверки выполнимости формул теории 1-го порядка, построенной над конечными кольцами.

Проблема построения решателя, предназначенного для проверки выполнимости формул теории 1-го порядка, построенной над конечными кольцами, из-за большой ее внутренней сложности, является в настоящее время практически не исследованной.

В п.1.4 было отмечено, что в настоящее время наиболее перспективным является «ленивый подход» к построению решателей, т.е. подход, основанный на интеграции SAT-решателей и $\mathcal{T}$-решателей. При таком подходе основная задача состоит в разработке $\mathcal{T}$-решателя, т.е. комплекса алгоритмов, предназначенных именно для анализа формул теории $\mathcal{T}$, имеющих тот или иной вид. С этой точки зрения методы построения множества решений систем уравнений с параметрами, разработанные в разделе 3, представляют собой фрагмент теории, которая может быть использована при построении решателя, предназначенного для проверки выполнимости формул над ассоциативным кольцом, являющихся конъюнкцией равенств термов.

Целью настоящего раздела является разработка структуры $\mathcal{LA}(\mathcal{K})$-решателя, предназначенного для проверки формул линейной арифметики над конечным ассоциативным кольцом $\mathcal{K} = (K, +, \cdot)$ с ненулевым умножением. Эта задача актуальна как с теоретической, так и с прикладной точки зрения. Последнее, в частности, обусловлено потенциальными применениями автоматно-алгебраических моделей, определенных над конечным ассоциативным кольцом, в процессе решения задач преобразования и защиты информации (в том числе, задач криптографии).

В п.4.1 охарактеризованы основные отличия линейной арифметики над конечным кольцом $\mathcal{K} = (K, +, \cdot)$ от линейной арифметики над кольцом $\mathcal{Z} = (\mathbb{Z}, +, \cdot)$ целых чисел. Построена классификация конечных ассоциативных колец с ненулевым умножением, отражающая различия в построении основных модулей $\mathcal{LA}(\mathcal{K})$-решателя в зависимости от типа рассматриваемого конечного ассоциативного кольца $\mathcal{K}$. В п.4.2 на основе «наслоения» (layering) построен решатель, предназначенный для проверки выполнимости формул линейной арифметики над любым конечным ассоциативным кольцом с ненулевым умножением. Охарактеризована временная сложность построенного решателя. П.4.3 содержит ряд заключительных замечаний.

Результаты автора, представленные в разделе, опубликованы в [101,214].

4.1. Анализ свойств конечных колец.

Выделим те свойства конечных ассоциативных колец $\mathcal{K} = (K, +, \cdot)$, которые существенны для построения $\mathcal{LA}(\mathcal{K})$-решателя. На основании этих свойств построим классификацию конечных ассоциативных колец и охарактеризуем те факторы, которые существенно влияют на структуру основных модулей $\mathcal{LA}(\mathcal{K})$-решателя в зависимости от типа рассматриваемого конечного ассоциативного кольца $\mathcal{K}$.

4.1.1. Особенности исследуемой проблемы.

Известно, что конечные кольца имеют ряд существенных отличий по сравнению с кольцом $\mathcal{Z} = (\mathbb{Z}, +, \cdot)$ целых чисел. Эти отличия, в частности, проявляются для линейной арифметики над произвольным конечным кольцом $\mathcal{K} = (K, +, \cdot)$, т.е. в случае, когда $\mathcal{T} = \mathcal{LA}(\mathcal{K})$. Для линейной арифметики над конечным ассоциативным кольцом наиболее важными из таких отличий являются следующие:

1. В кольце $\mathcal{K}$ умножение может быть некоммутативной операцией. В этом случае необходимо различать термы ab и ba.

2. В любом конечном кольце $\mathcal{K}$ невозможно определить отношение линейного порядка $\leq$, согласованное с операциями в этом кольце. Поэтому в конечном кольце могут рассматриваться только атомы вида

$$\sum_{i=1}^{n} a_i x_i + b_i \diamond 0,\ \sum_{i=1}^{n} x_i a_i + b_i \diamond 0,\ \sum_{i=1}^{n} a'_i x_i a''_i + b_i \diamond 0\ (\diamond \in \{=, \neq\}).$$

3. Любое конечное кольцо $\mathcal{K}$ с ненулевым умножением не является алгебраической подсистемой ни кольца целых чисел $\mathcal{Z} = (\mathbb{Z}, +, \cdot)$, ни кольца рациональных чисел $\mathcal{Q} = (\mathbb{Q}, +, \cdot)$. Поэтому для конечных колец в принципе не могут быть использованы $\mathcal{LA}(\mathcal{Q})$-решатели, а также модули, предназначенные для анализа систем линейных диофантовых уравнений над кольцом целых чисел.

4. Деление в кольце $\mathcal{K}$ может быть частичной операцией. Поэтому для конечного кольца в процессе анализа систем атомов, построенных из линейных термов, необходимо отдельно рассматривать ситуацию, когда выбранный коэффициент является обратимым элементом и ситуацию, когда выбранный коэффициент является необратимым элементом.

5. В кольце $\mathcal{K}$ могут быть делители нуля. В этом случае в процессе анализа систем атомов, построенных из линейных термов, необходимо детально исследовать влияние возможности наличия делителей нуля на выполнимость исследуемых систем атомов.

Исходя из перечисленных выше факторов, рассмотрим классификацию конечных колец, отражающую различия в построении основных модулей $\mathcal{LA}(\mathcal{K})$-решателя в зависимости от типа рассматриваемого конечного кольца $\mathcal{K}$.

Всюду в дальнейшем в настоящем разделе предполагается, что кольцо $\mathcal{K} = (K, +, \cdot)$ является кольцом с ненулевым умножением.

Замечание 4.1. Арифметика любого кольца $\mathcal{K} = (K, +, \cdot)$ с нулевым умножение непосредственно сводится к арифметике абелевой группы $(K, +)$.

4.1.2. Некоторые свойства колец с ненулевым умножением.

Так как $\mathcal{K} = (K, +, \cdot)$ – кольцо с ненулевым умножением, то $|K| \geq 2$.

Если $|K| = 2$, то $\mathcal{K} = \mathcal{GF}(2)$.

Если $|K| \geq 3$, то для как конечных, так и бесконечных колец с ненулевым умножением истинны следующие утверждения.

Лемма 4.1. Пусть $\mathcal{K} = (K, +, \cdot)$ ($|K| \geq 3$) – кольцо с ненулевым умножением. Если для элемента $a \in K$ существует такой элемент $b \in K$, что $ax = b$ для всех $x \in K \backslash \{0\}$, то $b = 0$.□

Доказательство. Пусть $\mathcal{K} = (K, +, \cdot)$ ($|K| \geq 3$) – кольцо с ненулевым умножением и $a \in K$ – элемент, для которого существует такой элемент $b \in K$, что $ax = b$ для всех $x \in K \backslash \{0\}$.

Если $a = 0$, то $b = ax = 0x = 0$, что и требовалось доказать.

Предположим, что $a \neq 0$. Так как $|K| \geq 3$, то существуют такие элементы $x_1, x_2 \in K \backslash \{0\}$, что $x_1 \neq x_2$.

По условию теоремы $ax_1 = 0$ и $ax_2 = 0$. Вычитая из 1-го равенства 2-е равенство, получим

$$ax_1 - ax_2 = 0. \tag{4.1}$$

Из равенства (4.1) и из закона дистрибутивности для кольца $\mathcal{K}$ вытекает, что

$$a(x_1 - x_2) = 0.$$

Так как $x_1 \neq x_2$, то $x_1 - x_2 \neq 0$. Следовательно, по условию теоремы, существует такой элемент $b \in K$, что $a(x_1 - x_2) = b$.

Из равенств $a(x_1 - x_2) = 0$ и $a(x_1 - x_2) = b$ вытекает, что $b = 0$, что и требовалось доказать. □

Лемма 4.2. Пусть $\mathcal{K} = (K, +, \cdot)$ ($|K| \geq 3$) – кольцо с ненулевым умножением. Если для элемента $a \in K$ существует такой элемент $b \in K$, что $xa = b$ для всех $x \in K \backslash \{0\}$, то $b = 0$.□

Доказательство леммы 4.2 аналогично доказательству леммы 4.1.

Лемма 4.3. Пусть $\mathcal{K} = (K, +, \cdot)$ ($|K| \geq 3$) – ассоциативное кольцо с ненулевым умножением. Если для элементов $a_1, a_2 \in K$ существует такой элемент $b \in K$, что $a_1 x a_2 = b$ для всех $x \in K \backslash \{0\}$, то $b = 0$.□

Доказательство. Пусть $\mathcal{K} = (K, +, \cdot)$ ($|K| \geq 3$) – кольцо с ненулевым умножением и $a_1, a_2 \in K$ – элементы, для которых существует такой элемент $b \in K$, что $a_1 x a_2 = b$ для всех $x \in K \backslash \{0\}$.

Если $a_1 = 0$, то, используя ассоциативность операции умножения, получим

$$b = a_1 x a_2 = a_1(x a_2) = 0(x a_2) = 0.$$

Аналогичным образом, если $a_2 = 0$, то, используя ассоциативность операции умножения, получим

$$b = a_1 x a_2 = (a_1 x) a_2 = (a_1 x) 0 = 0.$$

Предположим, что $a_1 \neq 0$ и $a_2 \neq 0$. Так как $|K| \geq 3$, то существуют такие элементы $x_1, x_2 \in K \backslash \{0\}$, что $x_1 \neq x_2$.

По условию теоремы $a_1 x_1 a_2 = 0$ и $a_1 x a_2 = 0$. Используя ассоциативность операции умножения, получим, что $(a_1 x_1) a_2 = 0$ и $(a_1 x_2) a_2 = 0$. Вычитая из 1-го равенства 2-е равенство, получим

$$(a_1 x_1) a_2 - (a_1 x_2) a_2 = 0. \tag{4.2}$$

Из (4.2) и из закона дистрибутивности для кольца $\mathcal{K}$ вытекает, что

$$(a_1 x_1 - a_1 x_2) a_2 = 0. \tag{4.3}$$

Из закона дистрибутивности для кольца $\mathcal{K}$ вытекает, что

$$a_1 x_1 - a_1 x_2 = a_1(x_1 - x_2). \tag{4.4}$$

Подставив (4.4) в (4.3), получим

$$(a_1(x_1 - x_2)) a_2 = 0,$$

откуда, в силу ассоциативности операции умножения, вытекает, что

$$a_1(x_1 - x_2) a_2 = 0.$$

Так как $x_1 \neq x_2$, то $x_1 - x_2 \neq 0$. Следовательно, по условию теоремы существует такой элемент $b \in K$, что $a_1(x_1 - x_2) a_2 = b$.

Из равенств $a_1(x_1 - x_2) a_2 = 0$ и $a_1(x_1 - x_2) a_2 = b$ вытекает, что $b = 0$, что и требовалось доказать.□

Охарактеризуем множество решений линейного уравнения в кольцах с ненулевым умножением.

Лемма 4.4. Для любого кольца $\mathcal{K} = (K, +, \cdot)$ ($|K| \geq 3$) с ненулевым умножением множество решений уравнения

$$ax = b \tag{4.5}$$

имеет вид

$$S_{ax=b} = \begin{cases} K, & \text{если } a = 0 \text{ и } b = 0 \\ \emptyset, & \text{если } a = 0 \text{ и } b \neq 0 \\ x_0 + I_a^r, & \text{если } a \neq 0 \end{cases}, \tag{4.6}$$

где x_0 – любое решение уравнения (4.5).□

Замечание 4.2. Множество I_a^r определено и исследовано в п.3.2.2.

Доказательство. Пусть $\mathcal{K} = (K, +, \cdot)$ ($|K| \geq 3$) – кольцо с ненулевым умножением.

Если $a = 0$, то из (4.5) вытекает, что $0 = b$ для всех $x \in K$. Отсюда, в свою очередь, вытекает, что

$$S_{0x=b} = \begin{cases} K, & \text{если } b = 0 \\ \emptyset, & \text{если } b \neq 0 \end{cases}.$$

Пусть $a \neq 0$ и x_0, x_1 – решения уравнения (4.5). Тогда истинны равенства $ax_1 = b$ и $ax_0 = b$. Вычитая из 1-го равенства 2-е равенство, получим, что истинно равенство

$$ax_1 - ax_0 = 0. \tag{4.7}$$

Из (4.7) и из закона дистрибутивности для кольца $\mathcal{K}$ вытекает, что истинно равенство

$$a(x_1 - x_0) = 0. \tag{4.8}$$

Из равенства (4.8) вытекает, что $x_1 - x_0 \in I_a^r$, т.е. $x_1 \in x_0 + I_a^r$.

Следовательно, если $a \neq 0$, то истинно включение $S_{ax=b} \subseteq x_0 + I_a^r$.

Пусть $a \neq 0$ и x_0 – решение уравнения (4.5). Тогда истинно равенство $ax_0 = b$. Подставим в (4.5) произвольный элемент $x_1 = x_0 + y$, где $y \in I_a^r$. Получим

$$a(x_0 + y) = b. \tag{4.9}$$

Применив в (4.9) закон дистрибутивности для кольца $\mathcal{K}$, получим эквивалентное равенство

$$ax_0 + ay = b. \tag{4.10}$$

Так как $y \in I_a^r$, то $ay = 0$. Это означает, что равенство (4.10) эквивалентно истинному равенству $ax_0 = 0$, т.е. равенство (4.9) истинно. Отсюда вытекает, что $x_0 + y \in S_{ax=b}$.

Итак, показано, что если $a \neq 0$, то истинно включение $x_0 + I_a^r \subseteq S_{ax=b}$.

Из включений $S_{ax=b} \subseteq x_0 + I_a^r$ $(a \neq 0)$ и $x_0 + I_a^r \subseteq S_{ax=b}$ $(a \neq 0)$, где x_0 – решение уравнения (4.5) вытекает, что для всех $a \neq 0$ истинно равенство и $x_0 + I_a^r = S_{ax=b}$, что и требовалось доказать.□

Следствие 4.1. Для любого кольца $\mathcal{K} = (K, +, \cdot)$ $(|K| \geq 3)$ с ненулевым умножением множество решений терма

$$ax \neq b \tag{4.11}$$

имеет вид

$$S_{ax\neq b} = \begin{cases} \emptyset, & \text{если } a = 0 \text{ и } b = 0 \\ K, & \text{если } a = 0 \text{ и } b \neq 0 \\ K \backslash (x_0 + I_a^r), & \text{если } a \neq 0 \end{cases}, \tag{4.12}$$

где x_0 – любое решение уравнения $ax = b$.□

Доказательство. Пусть $\mathcal{K} = (K, +, \cdot)$ $(|K| \geq 3)$ – кольцо с ненулевым умножением.

Так как истинны равенства

$$S_{ax=b} \cup S_{ax\neq b} = K$$

и

$$S_{ax=b} \cap S_{ax\neq b} = \emptyset,$$

то из истинности формулы (4.6) вытекает, что формула (4.12) истинна.□

Лемма 4.5. Для любого кольца $\mathcal{K} = (K, +, \cdot)$ $(|K| \geq 3)$ с ненулевым умножением множество решений уравнения

$$xa = b \tag{4.13}$$

имеет вид

$$S_{xa=b} = \begin{cases} K, & \text{если } a = 0 \text{ и } b = 0 \\ \emptyset, & \text{если } a = 0 \text{ и } b \neq 0 \\ x_0 + I_a^l, & \text{если } a \neq 0 \end{cases}, \tag{4.14}$$

где x_0 – любое решение уравнения (4.13).□

Замечание 4.3. Множество I_a^l определено и исследовано в п.3.2.2.

Доказательство леммы 4.5 аналогично доказательству леммы 4.4.

Следствие 4.2. Для любого кольца $\mathcal{K} = (K, +, \cdot)$ ($|K| \geq 3$) с ненулевым умножением множество решений терма

$$xa \neq b \tag{4.15}$$

имеет вид

$$S_{xa\neq b} = \begin{cases} \emptyset, & \text{если } a = 0 \text{ и } b = 0 \\ K, & \text{если } a = 0 \text{ и } b \neq 0 \\ K \backslash (x_0 + I_a^l), & \text{если } a \neq 0 \end{cases}, \tag{4.16}$$

где x_0 – любое решение уравнения $xa = b$.$\square$

Доказательство следствия 4.2 аналогично доказательству следствия 4.1.

Лемма 4.6. Для любого ассоциативного не коммутативного кольца $\mathcal{K} = (K, +, \cdot)$ ($|K| \geq 3$) с ненулевым умножением множество решений уравнения

$$a_1 x a_2 = b \tag{4.17}$$

имеет вид

$$S_{a_1 x a_2 = b} = \begin{cases} K, & \text{если } a_1 = 0 \text{ или } a_2 = 0, \text{ и } b = 0 \\ \emptyset, & \text{если } a_1 = 0 \text{ или } a_2 = 0, \text{ и } b \neq 0 \\ S_{a_1,a_2,b}(x_0), & \text{если } a_1 \neq 0 \text{ и } a_2 \neq 0 \end{cases}, \tag{4.18}$$

где x_0 – любое решение уравнения (4.17),

$$S_{a_1,a_2,b}(x_0) = S'_{a_1,a_2,b}(x_0) \cup S''_{a_1,a_2,b}(x_0), \tag{4.19}$$

а

$$S'_{a_1,a_2,b}(x_0) = (x_0 + I_{a_1}^r) \cup (x_0 + I_{a_2}^l) \tag{4.20}$$

и

$$S''_{a_1,a_2,b}(x_0) = \{x | a_1(x - x_0) \in I_{a_2}^l\} \cup \{x | (x - x_0)a_2 \in I_{a_1}^r\} \tag{4.21}$$

для любого решения x_0 уравнения (4.17).$\square$

Доказательство. Пусть $\mathcal{K} = (K, +, \cdot)$ ($|K| \geq 3$) – ассоциативное не коммутативное кольцо с ненулевым умножением.

Подставив $a_1 = 0$ в равенство (4.17) и применив свойство ассоциативности операции умножения, получим, что для любого элемента $x \in K$

$$b = 0xa_2 = (0x)a_2 = 0a_2 = 0. \tag{4.22}$$

Подставив $a_2 = 0$ в равенство (4.17) и применив свойство ассоциативности операции умножения, получим, что для любого элемента $x \in K$

$$b = a_1 x 0 = (a_1 x)0 = 0. \tag{4.23}$$

Из равенств (4.22) и (4.23) вытекает, что

$$S_{a_1 x a_2 = b} = \begin{cases} K, & \text{если } a_1 = 0 \text{ или } a_2 = 0, \text{ и } b = 0 \\ \emptyset, & \text{если } a_1 = 0 \text{ или } a_2 = 0, \text{ и } b \neq 0 \end{cases}.$$

Предположим, что $a_1 \neq 0$ и $a_2 \neq 0$.

Пусть x_0 и x_1 – решения уравнения (4.17). Тогда истинны равенства $a_1 x_1 a_2 = b$ и $a_1 x_0 a_2 = b$. Вычитая из 1-го равенства 2-е равенство, получим, что истинно равенство

$$a_1 x_1 a_2 - a_1 x_0 a_2 = 0. \tag{4.24}$$

Из равенства (4.24) и из закона дистрибутивности для кольца $\mathcal{K}$ вытекает, что истинно равенство

$$(a_1 x_1 - a_1 x_0) a_2 = 0. \tag{4.25}$$

Из равенства (4.25) и из закона дистрибутивности для кольца $\mathcal{K}$ вытекает, что истинно равенство

$$(a_1 (x_1 - x_0)) a_2 = 0. \tag{4.26}$$

Так как равенство (4.26) истинно то $a_1(x_1 - x_0) = 0$ (т.е. $x_1 \in x_0 + I^r_{a_1}$) или $a_1(x_1 - x_0) \in I^l_{a_2}$. Следовательно,

$$x_1 \in (x_0 + I^r_{a_1}) \cup \{x | a_1(x - x_0) \in I^l_{a_2}\}. \tag{4.27}$$

Из (4.19)-(4.21) и (4.27) вытекает, что $x_1 \in S_{a_1,a_2,b}(x_0)$.

Итак, доказано, что истинно включение $S_{a_1 x a_2 = b} \subseteq S_{a_1,a_2,b}(x_0)$.

Пусть x_0 – любое решение уравнения (4.17). Тогда истинно равенство $a_1 x_0 a_2 = 0$.

Рассмотрим произвольный элемент $x \in S'_{a_1,a_2,b}(x_0)$.

Если $x \in x_0 + I^r_{a_1}$, то $x = x_0 + y$, где $y \in I^r_{a_1}$. Следовательно,

$$a_1(x_0 + y)a_2 = (a_1(x_0 + y))a_2 = (a_1 x_0 + a_1 y)a_2 =$$
$$= (a_1 x_0 + 0)a_2 = (a_1 x_0)a_2 = a_1 x_0 a_2 = 0,$$

откуда вытекает, что $x \in S_{a_1 x a_2 = b}$.

Если $x \in x_0 + I^l_{a_2}$, то $x = x_0 + y$, где $y \in I^l_{a_2}$. Следовательно,

$$a_1(x_0+y)a_2 = a_1((x_0+y)a_2) = a_1(x_0a_2+ya_2) =$$
$$= a_1(x_0a_2+0) = a_1(x_0a_2) = a_1x_0a_2 = 0,$$

откуда вытекает, что $x \in S_{a_1xa_2=b}$.

Рассмотрим произвольный элемент $x \in S''_{a_1,a_2,b}(x_0)$.

Если $a_1(x-x_0) \in I^l_{a_2}$, то

$$a_1xa_2 = a_1((x-x_0)+x_0)a_2 = (a_1(x-x_0)+a_1x_0)a_2 =$$
$$= (a_1(x-x_0))a_2 + (a_1x_0)a_2 = 0 + (a_1x_0)a_2 = (a_1(x_0)a_2 = a_1x_0a_2 = 0,$$

откуда вытекает, что $x \in S_{a_1xa_2=b}$.

Если $(x-x_0)a_2 \in I^r_{a_1}$, то

$$a_1xa_2 = a_1((x-x_0)+x_0)a_2 = a_1((x-x_0)a_2+x_0a_2) =$$
$$= a_1((x-x_0)a_2) + a_1(x_0a_2) = 0 + a_1(x_0a_2) = a_1(x_0a_2) = a_1x_0a_2 = 0,$$

откуда вытекает, что $x \in S_{a_1xa_2=b}$.

Итак, доказано, что истинно включение $S_{a_1,a_2,b}(x_0) \subseteq S_{a_1xa_2=b}$.

Так как включения $S_{a_1xa_2=b} \subseteq S_{a_1,a_2,b}(x_0)$ и $S_{a_1,a_2,b}(x_0) \subseteq S_{a_1xa_2=b}$ истинны для любых $a_1 \neq 0$ и $a_2 \neq 0$, то равенство $S_{a_1xa_2=b} = S_{a_1,a_2,b}(x_0)$ истинно для любых $a_1 \neq 0$ и $a_2 \neq 0$.□

Следствие 4.3. Для любого ассоциативного не коммутативного кольца $\mathcal{K} = (K,+,\cdot)$ ($|K| \geq 3$) с ненулевым умножением множество решений терма

$$a_1xa_2 \neq b \tag{4.28}$$

имеет вид

$$S_{a_1xa_2\neq b} = \begin{cases} \emptyset, & \text{если } a_1 = 0 \text{ или } a_2 = 0, \text{ и } b = 0 \\ K, & \text{если } a_1 = 0 \text{ или } a_2 = 0, \text{ и } b \neq 0 \\ K \backslash S_{a_1,a_2,b}(x_0), & \text{если } a_1 \neq 0 \text{ и } a_2 \neq 0 \end{cases}, \tag{4.29}$$

где где x_0 – любое решение уравнения $a_1xa_2 = b$,

$$S_{a_1,a_2,b}(x_0) = S'_{a_1,a_2,b}(x_0) \cup S''_{a_1,a_2,b}(x_0), \tag{4.30}$$

а

$$S'_{a_1,a_2,b}(x_0) = (x_0 + I^r_{a_1}) \cup (x_0 + I^l_{a_2}) \tag{4.31}$$

и

$$S''_{a_1,a_2,b}(x_0) = \{x | a_1(x-x_0) \in I^l_{a_2}\} \cup \{x | (x-x_0)a_2 \in I^r_{a_1}\} \tag{4.32}$$

для любого решения x_0 уравнения (4.17).□

Доказательство. Пусть $\mathcal{K} = (K, +, \cdot)$ ($|K| \geq 3$) – кольцо с ненулевым умножением.

Так как истинны равенства

$$S_{a_1 x a_2 = b} \cup S_{a_1 x a_2 \neq b} = K$$

и

$$S_{a_1 x_2 = b} \cap S_{a_1 x a_2 \neq b} = \emptyset,$$

то из истинности формулы (4.18) вытекает, что формула (4.29) истинна.□

4.1.3. Классификация конечных ассоциативных колец.

Обозначим через $\mathfrak{K}^{fnt}$ множество всех конечных ассоциативных колец $\mathcal{K} = (K, +, \cdot)$ с ненулевым умножением.

Относительно понятия «деление элемента на элемент» во множестве $\mathfrak{K}^{fnt}$ могут быть выделены следующие три непустые множества колец:

1) множество $\mathfrak{K}^{l.d-fnt}$ всех колец $\mathcal{K} \in \mathfrak{K}^{fnt}$ с «делением слева», т.е. $\mathcal{K} \in \mathfrak{K}^{l.d-fnt}$ тогда и только тогда, когда множество решений уравнения $ax = b$ непусто для всех $a \in K \backslash \{0\}$ и $b \in K$.

2) множество $\mathfrak{K}^{r.d-fnt}$ всех колец $\mathcal{K} \in \mathfrak{K}^{fnt}$ с «делением справа», т.е. $\mathcal{K} \in \mathfrak{K}^{r.d-fnt}$ тогда и только тогда, когда множество решений уравнения $xa = b$ непусто для всех $a \in K \backslash \{0\}$ и $b \in K$.

3) множество $\mathfrak{K}^{d-fnt}$ всех колец $\mathcal{K} \in \mathfrak{K}^{fnt}$ с «делением».

Замечание 4.4. Истинны включения $\mathfrak{K}^{l.d-fnt} \cup \mathfrak{K}^{r.d-fnt} \subset \mathfrak{K}^{fnt}$, $\mathfrak{K}^{d-fnt} \subset \mathfrak{K}^{l.d-fnt}$ и $\mathfrak{K}^{d-fnt} \subset \mathfrak{K}^{r.d-fnt}$. Из этих включений непосредственно вытекает, что $\mathfrak{K}^{fnt} \backslash \mathfrak{K}^{l.d-fnt} \neq \emptyset$, $\mathfrak{K}^{fnt} \backslash \mathfrak{K}^{r.d-fnt} \neq \emptyset$, $\mathfrak{K}^{l.d-fnt} \backslash \mathfrak{K}^{d-fnt} \neq \emptyset$ и $\mathfrak{K}^{r.d-fnt} \backslash \mathfrak{K}^{d-fnt} \neq \emptyset$.

Относительно понятия «единица» множество $\mathfrak{K}^{fnt}$ разбивается на следующие шесть непустых множеств колец:

1) множество $\mathfrak{K}_1^{fnt}$ всех коммутативных колец $\mathcal{K} \in \mathfrak{K}^{fnt}$ с единицей, т.е. существует такой элемент $1 \in K$, что $1x = x1 = x$ для всех $x \in K$.

2) множество $\mathfrak{K}_2^{fnt}$ всех коммутативных колец $\mathcal{K} \in \mathfrak{K}^{fnt}$ без единицы.

3) множество $\mathfrak{K}_3^{fnt}$ всех не коммутативных колец $\mathcal{K} \in \mathfrak{K}^{fnt}$ с единицей.

4. Множество $\mathfrak{K}_4^{fnt}$всех не коммутативных колец $\mathcal{K} \in \mathfrak{K}^{fnt}$, в которых существует левая единица (т.е. такой элемент $1_l \in K$, что $1_l x = x$ для всех элементов $x \in K$), но не существует правая единица (т.е. такой элемент $1_r \in K$, что $x1_r = x$ для всех элементов $x \in K$).

5. Множество $\mathfrak{K}_5^{fnt}$ всех не коммутативных колец $\mathcal{K} \in \mathfrak{K}^{fnt}$, в которых существует правая единица, но не существует левая единица.

6. Множество $\mathfrak{K}_5^{fnt}$ всех не коммутативных колец $\mathcal{K} \in \mathfrak{K}^{fnt}$, в которых не существует ни левой единицы, ни правой единицы.

Замечание 4.5. В кольце $\mathcal{K} \in \mathfrak{K}_4^{fnt} \cup \mathfrak{K}_5^{fnt}$ может существовать несколько односторонних единиц.

Простейшее кольцо $\mathcal{K} \in \mathfrak{K}_4^{fnt}$ с двумя левыми единицами содержит четыре элемента, а таблицы, определяющие операции в нем, представлены на рис. 4.1.

+	0	a	b	c	•	0	a	b	c
0	0	a	b	c	0	0	0	0	0
a	a	0	c	b	a	0	a	b	c
b	b	c	0	a	b	0	a	b	c
c	c	b	a	0	c	0	0	0	0

Рис. 4.1. Простейшее кольцо без правой единицы с двумя левыми единицами.

Для того, чтобы получить простейшее кольцо $\mathcal{K} \in \mathfrak{K}_5^{fnt}$ с двумя правыми единицами, достаточно транспонировать таблицу, определяющую операцию умножения.

Лемма 4.7. Истинно следующее равенство

$$(\mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}) \cap \mathfrak{K}^{\alpha.d-fnt} = (\mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}) \cap \mathfrak{K}^{d-fnt}, \tag{4.33}$$

где $\alpha \in \{l, d\}$. $\square$

Доказательство. Так как $\mathfrak{K}^{d-fnt} \subset \mathfrak{K}^{l.d-fnt}$ и $\mathfrak{K}^{d-fnt} \subset \mathfrak{K}^{r.d-fnt}$, то истинны включения

$$(\mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}) \cap \mathfrak{K}^{d-fnt} \subseteq (\mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}) \cap \mathfrak{K}^{l.d-fnt} \tag{4.34}$$

и

$$(\mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}) \cap \mathfrak{K}^{d-fnt} \subseteq (\mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}) \cap \mathfrak{K}^{r.d-fnt}. \tag{4.35}$$

Докажем обратные включения.

Пусть $\mathcal{K} = (K, +, \cdot) \in (\mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}) \cap \mathfrak{K}^{l.d-fnt}$. Тогда множество решений любого уравнения $ax = b$ $(a \in K \backslash \{0\}, b \in K)$ непусто.

Так как $\mathcal{K} \in \mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}$, то уравнение $ax = b$ эквивалентно уравнению $xa = b$. Следовательно, для кольца $\mathcal{K}$ множество решений любого уравнения $xa = b$ $(a \in K \backslash \{0\}, b \in K)$ также непусто.

Так как в кольце $\mathcal{K}$ для любых $a \in K \backslash \{0\}$ и $b \in K$ множество решений каждого из уравнений $ax = b$ и $xa = b$ является непустым множеством, то $\mathcal{K} \in (\mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}) \cap \mathfrak{K}^{d-fnt}$.

Таким образом, доказано, что истинно включение

$$(\mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}) \cap \mathfrak{K}^{l.d-fnt} \subseteq (\mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}) \cap \mathfrak{K}^{d-fnt}. \tag{4.36}$$

Включение

$$(\mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}) \cap \mathfrak{K}^{r.d-fnt} \subseteq (\mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}) \cap \mathfrak{K}^{d-fnt} \tag{4.37}$$

доказывается аналогичным образом.

Из включений (4.34)-(4.37) вытекает, что равенства (4.33) истинны. □

Из леммы 4.7 непосредственно вытекает, что истинно следующее следствие.

Следствие 4.4. Истинно следующее равенство

$$(\mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}) \backslash \mathfrak{K}^{\alpha.d-fnt} = (\mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}) \backslash \mathfrak{K}^{d-fnt}, \tag{4.38}$$

где $\alpha \in \{l, d\}$. □

В дальнейшем в настоящем разделе мы будем использовать следующие понятия и обозначения:

1. Если $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}_1^{fnt}$, то K^{inv} – множество всех обратимых элементов кольца $\mathcal{K}$. Таким образом, $(K^{inv}, \cdot)$ – мультипликативная коммутативная группа кольца $\mathcal{K}$.

2. Если $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}_3^{fnt}$, то множество

$$K^{l.inv} = \{x \in K | (\exists a \in K)(ax = 1)\}$$

является множеством всех обратимых слева элементов кольца $\mathcal{K}$, а множество

$$K^{r.inv} = \{x \in K | (\exists a \in K)(xa = 1)\}$$

является множеством всех обратимых справа элементов кольца $\mathcal{K}$. Множество $K^{inv} = K^{l.inv} \cap K^{r.inv}$ является множеством всех обратимых (в обычном смысле этого слова) элементов кольца $\mathcal{K}$, а $(K^{inv}, \cdot)$ – мультипликативная (возможно, не коммутативная) группа кольца $\mathcal{K}$.

3. Если $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}_4^{fnt}$, то для каждой левой единицы $1_l \in K$ множество

$$K^{l.inv}(1_l) = \{x \in K | (\exists a \in K)(ax = 1_l)\}$$

является множеством всех элементов кольца $\mathcal{K}$, обратимых слева относительно левой единицы 1_l.

4. Если $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}_5^{fnt}$, то для каждой правой единицы $1_r \in K$ множество

$$K^{r.inv}(1_r) = \{x \in K | (\exists a \in K)(xa = 1_r)\}$$

является множеством всех элементов кольца $\mathcal{K}$, обратимых справа относительно правой единицы 1_r.

4.2. Структура $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}$ ($\mathcal{K} \in \mathfrak{K}^{fnt}$).

Охарактеризуем структуру $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}$, предназначенного для проверки выполнимости формул линейной арифметики над любым кольцом $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$.

4.2.1. Проверка выполнимости простейших атомов.

В любом кольце $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$ простейшими атомами являются формулы вида $ax \diamond b$, $xa \diamond b$ и $a_1 x a_2 \diamond b$, где $a, a_1, a_2, b \in K$ – фиксированные элементы, а $\diamond \in \{=, \neq\}$.

Замечание 4.6. В коммутативном кольце произведения ax, xa и $a_1 x a_2$ считаются неразличимыми. Поэтому в коммутативном кольце рассматриваются только атомы вида $ax \diamond b$, где $a, b \in K$ – фиксированные элементы, а $\diamond \in \{=, \neq\}$.

Построим на основе «наслоения» (layering) $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$, предназначенный для проверки выполнимости атомов

$$ax = b, \tag{4.39}$$

$$xa = b \tag{4.40}$$

и

$$a_1 x a_2 = b, \tag{4.41}$$

где $a, a_1, a_2, b \in K$ – фиксированные элементы.

$\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ представляет собой иерархию следующих трех модулей $\mathfrak{M}^{(1)}_1$, $\mathfrak{M}^{(1)}_2$ и $\mathfrak{M}^{(1)}_3$.

Вначале активируется модуль $\mathfrak{M}^{(1)}_1$. Осуществляемые им вычисления состоят в следующем.

Если исследуется атом (4.39) или (4.40) (соответственно, атом (4.41)), то модуль $\mathfrak{M}^{(1)}_1$ проверяет условие «$a = 0$» (соответственно, условие «$a_1 = 0$ или $a_2 = 0$»).

Пусть для атома (4.39) или (4.40) (соответственно, для атома (4.41)) выполнено условие «$a = 0$» (соответственно, выполнено условие «$a_1 = 0$ или $a_2 = 0$»). Тогда модуль $\mathfrak{M}^{(1)}_1$ проверяет условие «$b = 0$».

Если условие «$b = 0$» выполнено, то модуль $\mathfrak{M}^{(1)}_1$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `sat` и прекращает работу.

Если же условие «$b = 0$» не выполнено, то модуль $\mathfrak{M}^{(1)}_1$ возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `unsat` и прекращает работу.

Пусть для атома (4.39) или (4.40) (соответственно, для атома (4.41)) не выполнено условие «$a = 0$» (соответственно, не выполнено условие «$a_1 = 0$ или $a_2 = 0$»), т.е. $a \neq 0$ (соответственно, $a_1 \neq 0$ и $a_2 \neq 0$).

Замечание 4.7. Предположим, что атом (4.41) исследуется при условии, что $a_1 \neq 0$ и $a_2 \neq 0$. Если $\mathcal{K} \in \mathfrak{K}^{r.d-fnt} \backslash \mathfrak{K}^{l.d-fnt}$, то атом (4.41) может быть преобразован в атом вида (4.39). Если же $\mathcal{K} \in \mathfrak{K}^{l.d-fnt} \backslash \mathfrak{K}^{r.d-fnt}$, то атом (4.41) может быть преобразован в атом вида (4.40). А если $\mathcal{K} \in \mathfrak{K}^{d-fnt}$, то атом (4.41) может быть преобразован как в атом вида (4.39), так и в атом вида (4.40).

Могут иметь место следующие две ситуации:

1. Предположим, что, или $\mathcal{K} \in \mathfrak{K}^{l.d-fnt}$ и исследуется атом (4.39), или $\mathcal{K} \in \mathfrak{K}^{r.d-fnt}$ и исследуется атом (4.40). Тогда модуль $\mathfrak{M}_1^{(1)}$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `sat` и прекращает работу.

2. Предположим, что, или $\mathcal{K} \notin \mathfrak{K}^{l.d-fnt}$ и исследуется атом (4.39), или $\mathcal{K} \notin \mathfrak{K}^{r.d-fnt}$ и исследуется атом (4.40), или $\mathcal{K} \notin \mathfrak{K}^{l.d-fnt} \cup \mathfrak{K}^{r.d-fnt}$ и исследуется атом (4.41).

Если $\mathcal{K} \in \mathfrak{K}_1^{fnt} \cup \mathfrak{K}_3^{fnt} \cup \mathfrak{K}_4^{fnt} \cup \mathfrak{K}_5^{fnt}$, то модуль $\mathfrak{M}_1^{(1)}$ активирует модуль $\mathfrak{M}_2^{(1)}$. Если же $\mathcal{K} \in \mathfrak{K}_2^{fnt} \cup \mathfrak{K}_6^{fnt}$, то модуль $\mathfrak{M}_1^{(1)}$ активирует модуль $\mathfrak{M}_3^{(1)}$.

Модуль $\mathfrak{M}_2^{(1)}$ осуществляет вычисления в следующих четырех случаях (во всех остальных случаях модуль $\mathfrak{M}_2^{(1)}$ просто активирует модуль $\mathfrak{M}_3^{(1)}$):

1. Предположим, что $\mathcal{K} \in \mathfrak{K}_1^{fnt}$.

Замечание 4.8. Из замечаний 4.6 и 4.7 вытекает, что, не ограничивая общность рассуждений, мы можем считать, что осуществляется исследование атома (4.39).

Модуль $\mathfrak{M}_2^{(1)}$ проверяет условие «$a \in K^{inv}$».

Если условие «$a \in K^{inv}$» выполнено, то модуль $\mathfrak{M}_2^{(1)}$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `sat` и прекращает работу.

Если же условие «$a \in K^{inv}$» не выполнено, то модуль $\mathfrak{M}_2^{(1)}$ активирует модуль $\mathfrak{M}_3^{(1)}$.

2. Предположим, что $\mathcal{K} \in \mathfrak{K}_3^{fnt}$.

Замечание 4.9. Из замечания 4.7 вытекает, что, не ограничивая общность рассуждений, мы можем считать, что если исследуется атом (4.39), то $\mathcal{K} \in \mathfrak{K}_3^{fnt} \backslash \mathfrak{K}^{l.d-fnt}$, если же исследуется атом (4.40), то $\mathcal{K} \in \mathfrak{K}_3^{fnt} \backslash \mathfrak{K}^{r.d-fnt}$, а если исследуется атом (4.41), то $\mathcal{K} \in \mathfrak{K}_3^{fnt} \backslash (\mathfrak{K}^{l.d-fnt} \cup \mathfrak{K}^{r.d-fnt})$.

Если исследуется атом (4.39), то модуль $\mathfrak{M}_2^{(1)}$ проверяет условие «$a \in K^{l.inv}$». Если же исследуется атом (4.40), то модуль $\mathfrak{M}_2^{(1)}$ проверяет условие «$a \in K^{r.inv}$». А если исследуется атом (4.41), то модуль $\mathfrak{M}_2^{(1)}$ проверяет условие «$a_1 \in K^{l.inv}$ и $a_2 \in K^{r.inv}$».

Если проверяемое условие выполнено, то модуль $\mathfrak{M}_2^{(1)}$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}$ также возвращает `sat` и прекращает работу.

Если же проверяемое условие не выполнено, то модуль $\mathfrak{M}_2^{(1)}$ активирует модуль $\mathfrak{M}_3^{(1)}$.

3. Предположим, что $\mathcal{K} \in \mathfrak{K}_4^{fnt} \backslash \mathfrak{K}^{l.d-fnt}$. Модуль $\mathfrak{M}_2^{(1)}$ осуществляет следующие вычисления.

Пусть исследуется атом (4.39). Тогда модуль $\mathfrak{M}_2^{(1)}$ проверяет условие «существует такая левая единица $1_l \in K$, что $a \in K^{l.inv}(1_l)$».

Если проверяемое условие выполнено, то модуль $\mathfrak{M}_2^{(1)}$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}$ также возвращает `sat` и прекращает работу.

Если же проверяемое условие не выполнено, то модуль $\mathfrak{M}_2^{(1)}$ активирует модуль $\mathfrak{M}_3^{(1)}$.

Пусть исследуется атом (4.40). Модуль $\mathfrak{M}_2^{(1)}$ активирует модуль $\mathfrak{M}_3^{(1)}$.

Пусть исследуется атом (4.41). Тогда модуль $\mathfrak{M}_2^{(1)}$ проверяет условие «существует такая левая единица $1_l \in K$, что $a_1 \in K^{l.inv}(1_l)$».

Если проверяемое условие выполнено, то атом (4.41) преобразуется в атом вида (4.40) и модуль $\mathfrak{M}_2^{(1)}$ активирует модуль $\mathfrak{M}_3^{(1)}$.

Если же проверяемое условие не выполнено, то модуль $\mathfrak{M}_2^{(1)}$ активирует модуль $\mathfrak{M}_3^{(1)}$.

4. Предположим, что $\mathcal{K} \in \mathfrak{K}_5^{fnt} \backslash \mathfrak{K}^{r.d-fnt}$. Модуль $\mathfrak{M}_2^{(1)}$ осуществляет следующие вычисления.

Пусть исследуется атом (4.39). Модуль $\mathfrak{M}_2^{(1)}$ активирует модуль $\mathfrak{M}_3^{(1)}$.

Пусть исследуется атом (4.40). Тогда модуль $\mathfrak{M}_2^{(1)}$ проверяет условие «существует такая правая единица $1_r \in K$, что $a \in K^{r.inv}(1_r)$».

Если проверяемое условие выполнено, то модуль $\mathfrak{M}_2^{(1)}$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}$ также возвращает `sat` и прекращает работу.

Если же проверяемое условие не выполнено, то модуль $\mathfrak{M}_2^{(1)}$ активирует модуль $\mathfrak{M}_3^{(1)}$.

Пусть исследуется атом (4.41). Тогда модуль $\mathfrak{M}_2^{(1)}$ проверяет условие «существует такая правая единица $1_r \in K$, что $a_2 \in K^{r.inv}(1_r)$».

Если проверяемое условие выполнено, то атом (4.41) преобразуется в атом вида (4.39) и модуль $\mathfrak{M}_2^{(1)}$ активирует модуль $\mathfrak{M}_3^{(1)}$.

Если же проверяемое условие не выполнено, то модуль $\mathfrak{M}_2^{(1)}$ активирует модуль $\mathfrak{M}_3^{(1)}$.

Структура модуля $\mathfrak{M}_3^{(1)}$ существенно зависит от структуры рассматриваемого кольца $\mathcal{K}$.

Наиболее простой является ситуация, когда $\mathcal{K} \in \mathfrak{K}_1^{fnt} \cup \mathfrak{K}_3^{fnt}$. В этом случае при построении модуля $\mathfrak{M}_3^{(1)}$ могут быть использованы, по крайней мере, следующие два подхода.

Первый подход основан на непосредственной проверке выполнимости атомов (4.39)-(4.41) на основе использования алгебраических свойств кольца $\mathcal{K}$ (см. леммы 4.4-4.6).

Если модуль $\mathfrak{M}_3^{(1)}$ установил, что исследуемый атом выполним, то он возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}$ также возвращает `sat` и прекращает работу.

Если же модуль $\mathfrak{M}_3^{(1)}$ установил, что исследуемый атом не выполним, то он возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}$ также возвращает `unsat` и прекращает работу.

Второй подход основан на использовании понятия «ассоциированные элементы кольца» (см. пп.3.1.2 и 3.1.4) и состоит в следующем.

Предположим, что $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}_1^{fnt}$.

Замечание 4.10. Из замечания 4.6 вытекает, что, не ограничивая общность рассуждений, мы можем считать, что исследуется атом (4.39).

Проверка выполнимости атома (4.39) сводится к проверке выполнимости атома $\langle a\rangle * \langle x\rangle = \langle b\rangle$ в полугруппе $(\{\langle x\rangle | x \in K\}, *)$.

Если модуль $\mathfrak{M}_3^{(1)}$ установил, что последний атом выполним, то он возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}$ также возвращает `sat` и прекращает работу.

Если же модуль $\mathfrak{M}_3^{(1)}$ установил, что исследуемый атом не выполним, то он возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}$ также возвращает `unsat` и прекращает работу.

Предположим, что $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}_3^{fnt}$.

Проверка выполнимости атома (4.39) сводится к проверке выполнимости формулы $b \in \langle a\rangle_l * \langle x\rangle_r$, проверка выполнимости атома (4.40) сводится

к проверке выполнимости формулы $b \in \langle x\rangle_l * \langle a\rangle_r$, а проверка выполнимости атома (4.41) сводится к проверке выполнимости любой из формул $b \in \langle a_1\rangle_l * \langle x\rangle_r * \langle a_2\rangle_l$, $b \in \langle a_1\rangle_l * \langle x\rangle_r * \langle a_2\rangle_r$, $b \in \langle a_1\rangle_r * \langle x\rangle_l * \langle a_2\rangle_r$ или $b \in \langle a_1\rangle_l * \langle x\rangle_l * \langle a_2\rangle_r$.

Если модуль $\mathfrak{M}_3^{(1)}$ установил, что анализируемая формула выполнима, то он возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `sat` и прекращает работу.

Если же модуль $\mathfrak{M}_3^{(1)}$ установил, что анализируемая формула не выполнима, то он возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `unsat` и прекращает работу.

Предположим, что $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}_2^{fnt} \cup \mathfrak{K}_4^{fnt} \cup \mathfrak{K}_5^{fnt} \cup \mathfrak{K}_6^{fnt}$. Тогда (особенно при отсутствии в кольце $\mathcal{K}$ эффективных методов разложения элементов кольца в произведение простых элементов) модуль $\mathfrak{M}_3^{(1)}$ осуществляет исчерпывающий поиск по некоторому подмножеству $S \subseteq K$, определяемым исходя из структуры кольца $\mathcal{K}$ (отметим, что мощность множества S может быть сравнима с мощностью множества K).

Так как $\{\mathfrak{K}_1^{fnt}, \mathfrak{K}_2^{fnt}, \mathfrak{K}_3^{fnt}, \mathfrak{K}_4^{fnt}, \mathfrak{K}_5^{fnt}, \mathfrak{K}_6^{fnt}\}$ является разбиением множества $\mathfrak{K}^{fnt}$, то изложенный выше метод построения $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$, по своей сути, является доказательством следующей теоремы.

Теорема 4.1. $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ является полным и непротиворечивым для любого кольца $\mathcal{K} \in \mathfrak{K}^{fnt}$.□

Построим на основе «наслоения» (layering) $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$, предназначенный для проверки выполнимости атомов

$$ax \neq b, \tag{4.42}$$

$$xa \neq b \tag{4.43}$$

и

$$a_1 x a_2 \neq b, \tag{4.44}$$

где $a, a_1, a_2, b \in K$ – фиксированные элементы.

$\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$ представляет собой иерархию следующих трех модулей $\mathfrak{M}_1^{(2)}$, $\mathfrak{M}_2^{(2)}$ и $\mathfrak{M}_3^{(2)}$.

Замечание 4.11. Принимая во внимание замечание 4.6, считаем, что в коммутативном кольце $\mathcal{K}$ рассматриваются только атомы вида (4.42).

Вначале активируется модуль $\mathfrak{M}_1^{(2)}$. Осуществляемые им вычисления состоят в следующем.

Если исследуется атом (4.42) или (4.43) (соответственно, атом (4.44)), то модуль $\mathfrak{M}_1^{(2)}$ проверяет условие «$a = 0$» (соответственно, условие «$a_1 = 0$ или $a_2 = 0$»).

Пусть для атома (4.42) или (4.43) (соответственно, для атома (4.44)) выполнено условие «$a = 0$» (соответственно, выполнено условие «$a_1 = 0$ или $a_2 = 0$»). Тогда модуль $\mathfrak{M}_1^{(2)}$ проверяет условие «$b = 0$».

Если условие «$b = 0$» выполнено, то модуль $\mathfrak{M}_1^{(2)}$ возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(2)}$ также возвращает `unsat` и прекращает работу.

Если же условие «$b = 0$» не выполнено, то модуль $\mathfrak{M}_1^{(2)}$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(2)}$ также возвращает `sat` и прекращает работу.

Пусть для атома (4.42) или (4.43) (соответственно, для атома (4.44) не выполнено условие «$a = 0$» (соответственно, не выполнено условие «$a_1 = 0$ или $a_2 = 0$»), т.е. $a \neq 0$ (соответственно, $a_1 \neq 0$ и $a_2 \neq 0$). Тогда модуль $\mathfrak{M}_1^{(2)}$ активирует модуль $\mathfrak{M}_2^{(2)}$.

Вычисления, осуществляемые модулем $\mathfrak{M}_2^{(2)}$, состоят в проверке условия «$b = 0$».

Если условие «$b = 0$» не выполнено, то модуль $\mathfrak{M}_2^{(2)}$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(2)}$ также возвращает `sat` и прекращает работу. Если же условие «$b = 0$» выполнено, то модуль $\mathfrak{M}_2^{(2)}$ активирует модуль $\mathfrak{M}_3^{(2)}$.

Вычисления, осуществляемые модулем $\mathfrak{M}_3^{(2)}$, состоят в следующем.

Пусть исследуется атом (4.42). Тогда модуль $\mathfrak{M}_3^{(2)}$ проверяет условие «$a \in K^{z.l.d}$».

Если условие «$a \in K^{z.l.d}$» выполнено, то модуль $\mathfrak{M}_3^{(2)}$ проверяет условие «$I_a^r = K$».

Если условие «$I_a^r = K$» выполнено, то модуль $\mathfrak{M}_3^{(2)}$ возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(2)}$ также возвращает `unsat` и прекращает работу.

Если условие «$I_a^r = K$» не выполнено, то модуль $\mathfrak{M}_3^{(2)}$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(2)}$ также возвращает `sat` и прекращает работу.

Если же условие «$a \in K^{z.l.d}$» не выполнено, то модуль $\mathfrak{M}_3^{(2)}$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(2)}$ также возвращает `sat` и прекращает работу.

Пусть исследуется атом (4.43). Тогда модуль $\mathfrak{M}_3^{(2)}$ проверяет условие «$a \in K^{z.r.d}$».

Предположим, что условие «$a \in K^{z.r.d}$» выполнено. Тогда модуль $\mathfrak{M}_3^{(2)}$ осуществляет проверку условия «$I_a^l = K$».

Если условие «$I_a^l = K$» выполнено, то модуль $\mathfrak{M}_3^{(2)}$ возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(2)}$ также возвращает `unsat` и прекращает работу.

Если условие «$I_a^l = K$» не выполнено, то модуль $\mathfrak{M}_3^{(2)}$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(2)}$ также возвращает `sat` и прекращает работу.

Предположим, что условие «$a \in K^{z.r.d}$» не выполнено. Тогда модуль $\mathfrak{M}_3^{(2)}$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(2)}$ также возвращает `sat` и прекращает работу.

Пусть исследуется атом (4.44). Тогда модуль $\mathfrak{M}_3^{(2)}$ проверяет условие «$a_1 \in K^{z.l.d}$».

Предположим, что условие «$a_1 \in K^{z.l.d}$» выполнено. Тогда модуль $\mathfrak{M}_3^{(2)}$ проверяет условие «$I_{a_1}^r = K$».

Если условие «$I_{a_1}^r = K$» выполнено, то модуль $\mathfrak{M}_3^{(2)}$ возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(2)}$ также возвращает `unsat` и прекращает работу.

Если условие «$I_{a_1}^r = K$» не выполнено, то модуль $\mathfrak{M}_3^{(2)}$ проверяет условие «$\{x \in K | xa_2 \in I_{a_1}^r\} = K$».

Если условие «$\{x \in K | xa_2 \in I_{a_1}^r\} = K$» выполнено, то модуль $\mathfrak{M}_3^{(2)}$ возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(2)}$ также возвращает `unsat` и прекращает работу.

Если условие «$\{x \in K | xa_2 \in I_{a_1}^r\} = K$» не выполнено, то модуль $\mathfrak{M}_3^{(2)}$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(2)}$ также возвращает `sat` и прекращает работу.

Предположим, что условие «$a_1 \in K^{z.l.d}$» не выполнено. Тогда модуль $\mathfrak{M}_3^{(2)}$ проверяет условие «$a_2 \in K^{z.r.d}$».

Пусть условие «$a_2 \in K^{z.r.d}$» выполнено. Тогда модуль $\mathfrak{M}_3^{(2)}$ проверяет условие «$I_{a_2}^l = K$».

Если условие «$I_{a_2}^l = K$» выполнено, то модуль $\mathfrak{M}_3^{(2)}$ возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(2)}$ также возвращает `unsat` и прекращает работу.

Если условие «$I^l_{a_2} = K$» не выполнено, то модуль $\mathfrak{M}^{(2)}_3$ проверяет условие «$\{x \in K | a_1 x \in I^l_{a_2}\} = K$».

Если условие «$\{x \in K | a_1 x \in I^l_{a_2}\} = K$» выполнено, то модуль $\mathfrak{M}^{(2)}_3$ возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `unsat` и прекращает работу.

Если условие «$\{x \in K | a_1 x \in I^l_{a_2}\} = K$» не выполнено, то модуль $\mathfrak{M}^{(2)}_3$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `sat` и прекращает работу.

Пусть условие «$a_2 \in K^{z.r.d}$» не выполнено. Тогда модуль $\mathfrak{M}^{(2)}_3$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `sat` и прекращает работу.

Из лемм 4.1-4.3 и следствий 4.1-4.3 вытекает, что изложенный выше метод построения $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$, по своей сути, является доказательством следующей теоремы.

Теорема 4.2. $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$ является полным и непротиворечивым для любого кольца $\mathcal{K} \in \mathfrak{K}^{fnt}$.$\square$

4.2.2. Проверка выполнимости системы линейных уравнений.

Пусть $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$. Построим на основе «наслоения» (layering) $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$, предназначенный для проверки выполнимости систем линейных уравнений

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{4.45}$$

и

$$\begin{cases} x_1a_{11} + \cdots + x_na_{1n} = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x_1a_{m1} + \cdots + x_na_{mn} = b_m \end{cases}, \tag{4.46}$$

где $a_{ij} \in K$ $(i \in \mathbb{N}_m, j \in \mathbb{N}_n)$ – фиксированные элементы кольца $\mathcal{K}$, а также системы линейных уравнений

$$\begin{cases} u_{11} + \cdots + u_{1n} = b_1 \\ \cdots\cdots\cdots\cdots\cdots \\ u_{m1} + \cdots + u_{mn} = b_m \end{cases}, \tag{4.47}$$

где каждое u_{ij} $(i \in \mathbb{N}_m, j \in \mathbb{N}_n)$ – терм одного из следующих трех типов: $a_{ij}x_j$, $x_j a_{ij}$ или $a'_{ij}x_j a''_{ij}$ $(a_{ij}, a'_{ij}, a''_{ij} \in K$ – фиксированные элементы кольца $\mathcal{K})$, причем в системе (4.37) присутствует, по крайней мере, два из указанных трех типов термов.

Замечание 4.12. Принимая во внимание замечание 4.6, считаем, что в коммутативном кольце $\mathcal{K}$ рассматриваются только атомы вида (4.45).

$\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ представляет собой иерархию следующих трех модулей $\mathfrak{M}^{(3)}_1$, $\mathfrak{M}^{(3)}_2$ и $\mathfrak{M}^{(3)}_3$.

Вначале активируется модуль $\mathfrak{M}^{(3)}_1$. Этот модуль основан на использовании метода Гаусса и предназначен для преобразования:

1) системы уравнений (4.45) в эквивалентную диагональную форму

$$\begin{cases} e_{i_1}x_{i_1} = \sum\limits_{j\in\mathbb{N}_n\setminus\{i_1,\ldots,i_r\}} c_{i_1 j}x_j + d_{i_1} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ e_{i_r}x_{i_r} = \sum\limits_{j\in\mathbb{N}_n\setminus\{i_1,\ldots,i_r\}} c_{i_r j}x_j + d_{i_r} \end{cases}; \tag{4.48}$$

2) системы уравнений (4.46) в эквивалентную диагональную форму

$$\begin{cases} x_{i_1}e_{i_1} = \sum\limits_{j\in\mathbb{N}_n\setminus\{i_1,\ldots,i_r\}} x_j c_{i_1 j} + d_{i_1} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_{i_r}e_{i_r} = \sum\limits_{j\in\mathbb{N}_n\setminus\{i_1,\ldots,i_r\}} x_j c_{i_r j} + d_{i_r} \end{cases}; \tag{4.49}$$

3) системы уравнений (4.47) в эквивалентную диагональную форму

$$\begin{cases} e'_{i_1}x_{i_1}e''_{i_1} = \sum\limits_{j\in\mathbb{N}_n\setminus\{i_1,\ldots,i_r\}} c'_{i_1 j}x_j c''_{i_1 j} + d_{i_1} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ e'_{i_r}x_{i_r}e''_{i_r} = \sum\limits_{j\in\mathbb{N}_n\setminus\{i_1,\ldots,i_r\}} c'_{i_r j}x_j c''_{i_r j} + d_{i_r} \end{cases}. \tag{4.50}$$

Если в процессе указанных преобразований обнаружены противоречия, то модуль $\mathfrak{M}^{(3)}_1$ возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `unsat` и прекращает работу.

Если же в процессе указанных преобразований не обнаружено никаких противоречий, то возможны следующие две ситуации:

1. Исследуемая система линейных уравнений приведена к эквивалентной диагональной форме. Тогда модуль $\mathfrak{M}_1^{(3)}$ активирует модуль $\mathfrak{M}_2^{(3)}$.

2. В результате преобразования исследуемая система линейных уравнений приведена к эквивалентной форме, отличной от диагональной формы. Тогда модуль $\mathfrak{M}_1^{(3)}$ активирует модуль $\mathfrak{M}_3^{(3)}$.

Замечание 4.13. Очевидно, что (4.48)-(4.50) могут рассматриваться как системы линейных уравнений с параметрами x_j ($j \in \mathbb{N}_n \backslash \{i_1, \ldots, i_r\}$).

Модуль $\mathfrak{M}_2^{(3)}$ предназначен для проверки выполнимости системы линейных уравнений, представленной в диагональной форме. Осуществляемые им вычисления основаны на следующем последовательном анализе уравнений этой системы линейных уравнений.

Для очередного исследуемого уравнения модуль $\mathfrak{M}_2^{(3)}$ осуществляет следующие вычисления.

Вначале на основе алгебраических свойств кольца $\mathcal{K}$ модуль $\mathfrak{M}_2^{(3)}$ выделяет множество S всех таких наборов значений параметров x_j ($j \in \mathbb{N}_n \backslash \{i_1, \ldots, i_r\}$), что множество решений системы, состоящей из предыдущих уравнений и исследуемого уравнения может быть непустым множеством.

Замечание 4.14. С целью обеспечения эффективности функционирования $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(3)}$ построение множества S (за исключением таких хорошо проработанных колец $\mathcal{K} \in \mathfrak{K}^{fnt}$, как, например, кольца вычетов) осуществляется некоторой совокупностью достаточно быстрых эвристических методов, основанных на алгебраических свойствах кольца $\mathcal{K}$.

Далее модуль $\mathfrak{M}_2^{(3)}$ проверяет условие «$S = \emptyset$».

Если модуль $\mathfrak{M}_2^{(3)}$ установил, что условие «$S = \emptyset$» выполнено, то он возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(3)}$ также возвращает `unsat` и прекращает работу.

Если же модуль $\mathfrak{M}_2^{(3)}$ установил, что условие «$S = \emptyset$» не выполнено, то он осуществляет следующие вычисления.

Модуль $\mathfrak{M}_2^{(3)}$ выбирает из множества S очередной набор значений параметров x_j ($j \in \mathbb{N}_n \backslash \{i_1, \ldots, i_r\}$) и вызывает $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}$.

Если $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}$ установил, что на данном наборе значений параметров x_j ($j \in \mathbb{N}_n \backslash \{i_1, \ldots, i_r\}$) исследуемое уравнение выполнимо (т.е. $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}$ возвратил `sat`), то модуль $\mathfrak{M}_2^{(3)}$ переходит к исследованию следующего уравнения.

Если $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ установил, что на данном наборе значений параметров x_j $(j \in \mathbb{N}_n \backslash \{i_1, \ldots, i_r\})$ исследуемое уравнение невыполнимо (т.е. $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ возвратил `unsat`), то модуль $\mathfrak{M}^{(3)}_2$ выбирает из множества S следующий набор значений параметров x_j $(j \in \mathbb{N}_n \backslash \{i_1, \ldots, i_r\})$ и вызывает $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$.

Если $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ установил, что для всех наборов значений параметров x_j $(j \in \mathbb{N}_n \backslash \{i_1, \ldots, i_r\})$, принадлежащих множеству S, исследуемое уравнение невыполнимо (т.е. для всех наборов значений параметров, принадлежащих множеству S, $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ возвратил `unsat`), то модуль $\mathfrak{M}^{(3)}_2$ возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `unsat` и прекращает работу.

Если по окончанию исследования последнего уравнения $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ возвращает `sat`, то модуль $\mathfrak{M}^{(3)}_2$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `sat` и прекращает работу.

Модуль $\mathfrak{M}^{(3)}_3$ предназначен для проверки выполнимости системы линейных уравнений, полученной в результате работы модуля $\mathfrak{M}^{(3)}_1$, в случае, когда полученная система не представлена в диагональной форме.

Вычисления, осуществляемые модулем $\mathfrak{M}^{(3)}_3$, основаны на исчерпывающем поиске (возможно сокращенным за счет использования алгебраических свойств кольца $\mathcal{K} \in \mathfrak{K}^{fnt}$).

Если модуль $\mathfrak{M}^{(3)}_3$ установил, что множество решений исследуемой системы линейных уравнений является непустым множеством, то он возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `sat` и прекращает работу.

Если же модуль $\mathfrak{M}^{(3)}_3$ установил, что множество решений исследуемой системы линейных уравнений является пустым множеством, то он возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `unsat` и прекращает работу.

Из теоремы 4.1 вытекает, что изложенный выше метод построения $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$, по своей сути, является доказательством следующей теоремы.

Теорема 4.3. $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ является полным и непротиворечивым для любого кольца $\mathcal{K} \in \mathfrak{K}^{fnt}$.$\square$

4.2.3. Проверка выполнимости системы линейных неравенств.

Пусть $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$. Построим на основе «наслоения» (layering) $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$, предназначенный для проверки выполнимости систем линейных неравенств

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n \neq b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \neq b_m \end{cases} \tag{4.51}$$

и

$$\begin{cases} x_1a_{11} + \cdots + x_na_{1n} \neq b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x_1a_{m1} + \cdots + x_na_{mn} \neq b_m \end{cases}, \tag{4.52}$$

где $a_{ij} \in K$ $(i \in \mathbb{N}_m, j \in \mathbb{N}_n)$ – фиксированные элементы кольца $\mathcal{K}$, а также системы линейных неравенств

$$\begin{cases} u_{11} + \cdots + u_{1n} \neq b_1 \\ \cdots\cdots\cdots\cdots\cdots \\ u_{m1} + \cdots + u_{mn} \neq b_m \end{cases}, \tag{4.53}$$

где каждое u_{ij} $(i \in \mathbb{N}_m, j \in \mathbb{N}_n)$ – терм одного из следующих трех типов: $a_{ij}x_j$, x_ja_{ij} или $a'_{ij}x_ja''_{ij}$ $(a_{ij}, a'_{ij}, a''_{ij} \in K$ – фиксированные элементы кольца $\mathcal{K})$, причем в системе (4.37) присутствует, по крайней мере, два из указанных трех типов термов.

С системами линейных неравенств (4.51)-(4.53) могут быть ассоциированы, соответственно, системы линейных уравнений с параметрами

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 + \alpha_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m + \alpha_m \end{cases}, \tag{4.54}$$

$$\begin{cases} x_1a_{11} + \cdots + x_na_{1n} = b_1 + \alpha_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x_1a_{m1} + \cdots + x_na_{mn} = b_m + \alpha_m \end{cases} \tag{4.55}$$

и

$$\begin{cases} u_{11} + \cdots + u_{1n} = b_1 + \alpha_1 \\ \cdots\cdots\cdots\cdots\cdots \\ u_{m1} + \cdots + u_{mn} = b_m + \alpha_m \end{cases}, \tag{4.56}$$

где $\alpha_i \in K\backslash\{0\}$ $(i = 1, \ldots, m)$ – параметры. При этом:

1) система линейных неравенств (4.51) выполнима тогда и только тогда, когда выполнима система линейных уравнений (4.54);

2) система линейных неравенств (4.52) выполнима тогда и только тогда, когда выполнима система линейных уравнений (4.55);

3) система линейных неравенств (4.53) выполнима тогда и только тогда, когда выполнима система линейных уравнений (4.56).

Отсюда вытекает, что $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(4)}_{\mathcal{LA}(\mathcal{K})}$ может быть построен в виде иерархии следующих двух модулей $\mathfrak{M}^{(4)}_1$ и $\mathfrak{M}^{(4)}_2$.

Вначале активируется модуль $\mathfrak{M}^{(4)}_1$. Этот модуль предназначен для преобразования исследуемой системы линейных неравенств в ассоциированную систему линейных уравнений с параметрами. По завершению этого преобразования модуль $\mathfrak{M}^{(4)}_1$ активирует модуль $\mathfrak{M}^{(4)}_2$.

Модуль $\mathfrak{M}^{(4)}_2$ предназначен для проверки выполнимости исследуемой ассоциированной системы линейных уравнений. Осуществляемые им вычисления состоят в следующем.

Вначале на основе алгебраических свойств кольца $\mathcal{K}$ модуль $\mathfrak{M}^{(4)}_2$ выделяет множество S всех наборов значений параметров $\alpha_i \in K\backslash\{0\}$ $(i = 1, \ldots, m)$, для которых множество решений ассоциированной системы линейных уравнений может быть непустым множеством.

Замечание 4.15. С целью обеспечения эффективности функционирования $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(4)}_{\mathcal{LA}(\mathcal{K})}$ построение множества S (за исключением таких хорошо проработанных типов колец $\mathcal{K} \in \mathfrak{K}^{fnt}$, как, например, кольца вычетов) осуществляется некоторой совокупностью достаточно быстрых эвристических методов, основанных на алгебраических свойствах кольца $\mathcal{K}$.

Далее модуль $\mathfrak{M}^{(4)}_2$ проверяет условие «$S = \emptyset$».

Если модуль $\mathfrak{M}^{(4)}_2$ установил, что выполнено условие «$S = \emptyset$», то он возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(4)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `unsat` и прекращает работу.

Если же модуль $\mathfrak{M}^{(4)}_2$ установил, что не выполнено условие «$S = \emptyset$», то он осуществляет следующие вычисления.

Модуль $\mathfrak{M}^{(4)}_2$ выбирает из множества S очередной набор значений параметров $\alpha_i \in K\backslash\{0\}$ $(i = 1, \ldots, m)$ и вызывает $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$.

Если $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ установил, что исследуемая ассоциированная система линейных уравнений на данном наборе значений параметров $\alpha_i \in K\backslash\{0\}$ $(i = 1, \ldots, m)$ является выполнимой (т.е. $\mathcal{LA}(\mathcal{K})$-

решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ возвратил `sat`), то модуль $\mathfrak{M}^{(4)}_2$ возвращает `sat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(4)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `sat` и прекращает работу.

Если $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ установил, что исследуемая ассоциированная система линейных уравнений на данном наборе значений параметров $\alpha_i \in K\backslash\{0\}$ $(i = 1, \ldots, m)$ является невыполнимой (т.е. $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ возвратил `unsat`), то модуль $\mathfrak{M}^{(4)}_2$ выбирает из множества S следующий набор параметров $\alpha_i \in K\backslash\{0\}$ $(i = 1, \ldots, m)$ и вызывает $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$.

Если $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ установил, что для всех наборов значений параметров $\alpha_i \in K\backslash\{0\}$ $(i = 1, \ldots, m)$ исследуемая ассоциированная система линейных уравнений является невыполнимой (т.е. для всех наборов значений параметров, принадлежащих множеству S, $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ возвратил `unsat`), то модуль $\mathfrak{M}^{(4)}_2$ возвращает `unsat` и прекращает работу. При этом $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(4)}_{\mathcal{LA}(\mathcal{K})}$ также возвращает `unsat` и прекращает работу.

Из теоремы 4.3 вытекает, что изложенный выше метод построения $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(4)}_{\mathcal{LA}(\mathcal{K})}$, по своей сути, является доказательством следующей теоремы.

Теорема 4.4. $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(4)}_{\mathcal{LA}(\mathcal{K})}$ является полным и непротиворечивым для любого кольца $\mathcal{K} \in \mathfrak{K}^{fnt}$.$\square$

Из теорем 4.1-4.4 непосредственно вытекает, что $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}$, представляющий собой систему, состоящую из взаимодействующих $\mathcal{LA}(\mathcal{K})$-решателей $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$, $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$, $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ и $\mathfrak{S}^{(4)}_{\mathcal{LA}(\mathcal{K})}$ (каждый из которых построен на основе «наслоения» (layering)) является полным и непротиворечивым для любого кольца $\mathcal{K} \in \mathfrak{K}^{fnt}$.

4.2.4. Анализ сложности $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}$ $(\mathcal{K} \in \mathfrak{K}^{fnt})$.

Исследуем временную сложность построенных $\mathcal{LA}(\mathcal{K})$-решателей $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$, $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$, $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ и $\mathfrak{S}^{(4)}_{\mathcal{LA}(\mathcal{K})}$ при логарифмическом весе [7].

Рассмотрим $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$.

Наиболее простой случай имеет место, когда кольцо $\mathcal{K} \in \mathfrak{K}^{fnt}$ – конечное поле, т.е. $\mathcal{K} = \mathcal{GF}(p^k)$, где p – простое число и $k \in \mathbb{N}$. В этом случае временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ характеризуется следующим образом.

Теорема 4.5. Временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ имеет вид

$$T_{\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}} = \begin{cases} O(\log p), & \text{если } p \to \infty \text{ и число } k \text{ фиксировано} \\ O(k), & \text{если } k \to \infty \text{ и число } p \text{ фиксировано} \\ O(k \log p), & \text{если } p \to \infty \text{ и } k \to \infty \end{cases}, \quad (4.57)$$

если $\mathcal{K} = \mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$).$\square$

Доказательство. Временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ равна

$$T_{\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}} = T_1 + T_2 + T_3, \quad (4.58)$$

где T_i $(i = 1, 2, 3)$ – временная сложность модуля $\mathfrak{M}^{(1)}_i$.

Пусть $\mathcal{K} = \mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$).

Временная сложность T' проверки каждого из условий «$a = 0$» и «$b = 0$» определяется формулой

$$T' = \begin{cases} O(\log p), & \text{если } p \to \infty \text{ и число } k \text{ фиксировано} \\ O(k), & \text{если } k \to \infty \text{ и число } p \text{ фиксировано} \\ O(k \log p), & \text{если } p \to \infty \text{ и } k \to \infty \end{cases}. \quad (4.59)$$

Модуль $\mathfrak{M}^{(1)}_1$ осуществляет проверку условий «$a = 0$» и «$b = 0$».

Следовательно, если $\mathcal{K} = \mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$), то $T_1 = T' + T'$, где T' определяется формулой (4.59). Отсюда вытекает, что если $\mathcal{K} = \mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$), то

$$T_1 = \begin{cases} O(\log p), & \text{если } p \to \infty \text{ и число } k \text{ фиксировано} \\ O(k), & \text{если } k \to \infty \text{ и число } p \text{ фиксировано} \\ O(k \log p), & \text{если } p \to \infty \text{ и } k \to \infty \end{cases}. \quad (4.60)$$

Если $\mathcal{K} = \mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$), то в процессе функционирования $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ не происходит ни активация модуля $\mathfrak{M}^{(1)}_2$, ни активация модуля $\mathfrak{M}^{(1)}_3$. Следовательно, если $\mathcal{K} = \mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$), то

$$T_2 = O(1) \ (p \to \infty \text{ или } k \to \infty) \quad (4.61)$$

и

$$T_3 = O(1) \ (p \to \infty \text{ или } k \to \infty). \quad (4.62)$$

Из (4.58)и (4.60)-(4.62) вытекает, что если $\mathcal{K} = \mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$), то временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ определяется формулой (4.57).$\square$

Наиболее простыми кольцами $\mathcal{K} \in \mathfrak{K}_1^{fnt} \backslash \mathfrak{K}^{d-fnt}$, являются кольца вычетов, т.е. кольца $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$, где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$. В этом случае временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ характеризуется следующим образом.

Теорема 4.6. Временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ имеет вид

$$T_{\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}} = \begin{cases} O(\log p), & \text{если } p \to \infty \text{ и число } k \text{ фиксировано} \\ O(\log k), & \text{если } k \to \infty \text{ и число } p \text{ фиксировано} \\ O(\log pk), & \text{если } p \to \infty \text{ и } k \to \infty \end{cases}, \quad (4.63)$$

если $\mathcal{K} = \mathcal{Z}_{p^k}$, где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$.$\square$

Доказательство. Временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ равна

$$T_{\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}} = T_1 + T_2 + T_3, \quad (4.64)$$

где T_i $(i = 1, 2, 3)$ – временная сложность модуля $\mathfrak{M}_i^{(1)}$.

Пусть $\mathcal{K} = \mathcal{Z}_{p^k}$, где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$.

Замечание 4.16. Представим ненулевые элементы кольца $\mathcal{Z}_{p^k}$ в виде $\gamma \circ p^i$, где $\gamma \in \mathbb{Z}^{inv}_{p^{k-i}}$ $(i \in \mathbb{Z}_k)$, а нуль кольца $\mathcal{Z}_{p^k}$ представим в виде $0 \circ p^0$.

Представим элемент $\gamma \in \mathbb{Z}_{p^{k-i}} \backslash \{0\}$ в виде

$$\gamma = \sum_{j=0}^{k-i-1} \gamma_j p^j,$$

где $\gamma_j \in \mathbb{Z}_p$ $(j \in \mathbb{Z}_{k-i})$.

При таком представлении проверка условия «$\gamma \in \mathbb{Z}^{inv}_{p^k}$» (т.е. проверка условия «$\gamma \not\equiv 0 \,(mod\, p)$») сводится к проверке условия «$\gamma_0 \neq 0$».

Для унификации обозначений вместо «$\gamma_0 = 0$» будем писать «$\gamma \equiv 0 \,(mod\, p)$», а вместо «$\gamma_0 \neq 0$» будем писать «$\gamma \not\equiv 0 \,(mod\, p)$» (что не вызывает недоразумений).

Принимая во внимание все сказанное выше, заключаем, что проверка условия «$\gamma \circ p^i = 0$» сводится к проверке условия «$\gamma \equiv 0 \,(mod\, p)$ и $i = 0$», а проверка условия «$\gamma \circ p^i \in \mathbb{Z}^{inv}_{p^k}$» – к проверке условия «$\gamma \not\equiv 0 \,(mod\, p)$ и $i = 0$».

Следовательно, временная сложность проверки каждого из условий «$\gamma \circ p^i = 0$» и «$\gamma \circ p^i \in \mathbb{Z}^{inv}_{p^k}$» определяется формулой

$$T'' = \begin{cases} O(\log p), & \text{если } p \to \infty \text{ и число } k \text{ фиксировано} \\ O(\log k), & \text{если } k \to \infty \text{ и число } p \text{ фиксировано} \\ O(\log pk), & \text{если } p \to \infty \text{ и } k \to \infty \end{cases}. \quad (4.65)$$

Охарактеризуем временную сложность модуля $\mathfrak{M}_1^{(1)}$.

Если $\mathcal{K} = \mathcal{Z}_{p^k}$, где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$, то модуль $\mathfrak{M}_1^{(1)}$ осуществляет проверку условия «$\alpha \equiv 0\,(mod\, p)$ и $i = 0$» (где $a = \alpha \circ p^i$), а также проверку условия «$\beta \equiv 0\,(mod\, p)$ и $j = 0$» (где $b = \beta \circ p^j$). Следовательно, $T_1 = T'' + T''$, где T'' определяется формулой (4.65), т.е.

$$T_1 = \begin{cases} O(\log p), & \text{если } p \to \infty \text{ и число } k \text{ фиксировано} \\ O(\log k), & \text{если } k \to \infty \text{ и число } p \text{ фиксировано} \\ O(\log pk), & \text{если } p \to \infty \text{ и } k \to \infty \end{cases}. \tag{4.66}$$

Охарактеризуем временную сложность модуля $\mathfrak{M}_2^{(1)}$.

Если $\mathcal{K} = \mathcal{Z}_{p^k}$, где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$, то модуль $\mathfrak{M}_1^{(2)}$ осуществляет проверку условия «$\alpha \equiv 0\,(mod\, p)$ и $i = 0$» (где $a = \alpha \circ p^i$).

Следовательно, $T_2 = T''$, где T'' определяется формулой (4.65), т.е.

$$T_2 = \begin{cases} O(\log p), & \text{если } p \to \infty \text{ и число } k \text{ фиксировано} \\ O(\log k), & \text{если } k \to \infty \text{ и число } p \text{ фиксировано} \\ O(\log pk), & \text{если } p \to \infty \text{ и } k \to \infty \end{cases}. \tag{4.67}$$

Охарактеризуем временную сложность модуля $\mathfrak{M}_3^{(1)}$.

Классами ассоциированных элементов кольца $\mathcal{Z}_{p^k}$, где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$ (см. п.3.1.3), являются множества $C_0 = \mathbb{Z}_{p^k}^{inv}$, $C_k = \{0\}$ и $C_r = \{\alpha \circ p^r | \alpha \in \mathbb{Z}_{p^{k-r}}^{inv}\}$ $(r = 1, \ldots, k-1)$.

Любой атом $a \circ x = b$, где $a \in C_i$ $(i \in \mathbb{N}_{k-1})$ и $b \in C_j$ $(j \in \mathbb{N}_{k-1})$ может быть преобразован в атом $C_i * \langle x \rangle = C_j$ за время $O(k)$ $(k \to \infty)$.

Отсюда вытекает, что проверка выполнимости атома $C_i * \langle x \rangle = C_j$ сводится к проверке условия «$i \leq j$».

Следовательно, если $\mathcal{K} = \mathcal{Z}_{p^k}$, где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$, то временная сложность модуля $\mathfrak{M}_3^{(1)}$ определяется формулой

$$T_3 = \begin{cases} O(1), & \text{если число } k \text{ фиксировано} \\ O(k), & \text{если } k \to \infty \end{cases}. \tag{4.68}$$

Из (4.64) и (4.66)-(4.68) вытекает, что если $\mathcal{K} = \mathcal{Z}_{p^k}$, где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$, то временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}$ определяется формулой (4.63).$\square$

Охарактеризуем временную сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ в множестве колец $\mathfrak{K}^{fnt}$.

Вычисления, осуществляемые модулем $\mathfrak{M}^{(1)}_1$, состоят в проверке коэффициентов на их равенство нулю.

Следовательно, временная сложность модуля $\mathfrak{M}^{(1)}_1$ в множестве колец $\mathfrak{K}^{fnt}$ имеет вид

$$T^{(1)}_1 = O(\log |K|) \ (|K| \to \infty). \tag{4.69}$$

Вычисления, осуществляемые модулем $\mathfrak{M}^{(1)}_2$ сводятся к проверке принадлежности коэффициентов множествам (односторонних для не коммутативного кольца, и двусторонних для коммутативного кольца) обратимых элементов.

Если отсутствует эффективная техника разложения элементов кольца $\mathcal{K} \in \mathfrak{K}^{fnt}$ в произведение простых элементов, то такая проверка может представлять собой исчерпывающий поиск по некоторому представленному в неявном виде подмножеству множества K, мощность которого может быть сравнима с мощностью множества K.

Следовательно, временная сложность модуля $\mathfrak{M}^{(1)}_2$ в множестве колец $\mathfrak{K}^{fnt}$ имеет вид

$$T^{(1)}_2 = O(|K|) \ (|K| \to \infty). \tag{4.70}$$

Если отсутствует эффективная техника разложения элементов кольца $\mathcal{K} \in \mathfrak{K}^{fnt}$ в произведение простых элементов, то вычисления, осуществляемые модулем $\mathfrak{M}^{(1)}_3$, могут, по своей сути, представлять собой исчерпывающий поиск по подтаблице таблицы умножения в кольце $\mathcal{K} \in \mathfrak{K}^{fnt}$, определяемой некоторым представленным в неявном виде подмножеством множества K. При этом мощность такого подмножества множества K может быть сравнима с мощностью самого множества K.

Следовательно, временная сложность модуля $\mathfrak{M}^{(1)}_3$ в множестве колец $\mathfrak{K}^{fnt}$ имеет вид

$$T^{(1)}_3 = O(|K| \cdot t_{mult}(\mathcal{K})) \ (|K| \to \infty), \tag{4.71}$$

где $t_{mult}(\mathcal{K})$ – время, необходимое для вычисления произведения двух элементов кольца $\mathcal{K} \in \mathfrak{K}^{fnt}$.

Так как $T_{\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}} = T^{(1)}_1 + T^{(1)}_2 + T^{(1)}_3$, то из (4.69)-(4.71) вытекает, что

$$T_{\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}} = O(|K| \cdot t_{mult}(\mathcal{K})) \ (|K| \to \infty). \tag{4.72}$$

Рассмотрим $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$.

Теорема 4.7. Временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$ имеет вид

$$T_{\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}} = \begin{cases} O(\log p), & \text{если } p \to \infty \text{ и число } k \text{ фиксировано} \\ O(k), & \text{если } k \to \infty \text{ и число } p \text{ фиксировано} \\ O(k \log p), & \text{если } p \to \infty \text{ и } k \to \infty \end{cases}, \quad (4.73)$$

если $\mathcal{K} = \mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$).□

Доказательство. Временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$ равна

$$T_{\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}} = T_1 + T_2 + T_3, \quad (4.74)$$

где T_i $(i = 1, 2, 3)$ – временная сложность модуля $\mathfrak{M}^{(2)}_i$.

Пусть $\mathcal{K} = \mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$).

Так как вычисления, осуществляемые модулями $\mathfrak{M}^{(2)}_1$ и $\mathfrak{M}^{(2)}_2$, состоят в проверке коэффициентов a и b на их равенство нулю, то при $i = 1, 2$

$$T_i = \begin{cases} O(\log p), & \text{если } p \to \infty \text{ и число } k \text{ фиксировано} \\ O(k), & \text{если } k \to \infty \text{ и число } p \text{ фиксировано} \\ O(k \log p), & \text{если } p \to \infty \text{ и } k \to \infty \end{cases}. \quad (4.75)$$

В поле $\mathcal{GF}(p^k)$ отсутствуют делители нуля.

Следовательно, если $\mathcal{K} = \mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$), то в процессе функционирования $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$ не происходит активация модуля $\mathfrak{M}^{(2)}_3$, т.е.

$$T_3 = O(1) \ (p \to \infty \text{ или } k \to \infty). \quad (4.76)$$

Из (4.74)-(4.76) вытекает, что если $\mathcal{K} = \mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$), то временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$ определяется формулой (4.73).□

Теорема 4.8. Временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$ имеет вид

$$T_{\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}} = \begin{cases} O(\log p), & \text{если } p \to \infty \text{ и число } k \text{ фиксировано} \\ O(\log k), & \text{если } k \to \infty \text{ и число } p \text{ фиксировано} \\ O(\log pk), & \text{если } p \to \infty \text{ и } k \to \infty \end{cases}, \quad (4.77)$$

если $\mathcal{K} = \mathcal{Z}_{p^k}$, где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$.□

Доказательство. Временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$ равна

$$T_{\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}} = T_1 + T_2 + T_3, \tag{4.78}$$

где T_i $(i = 1, 2, 3)$ – временная сложность модуля $\mathfrak{M}^{(2)}_i$.

Пусть $\mathcal{K} = \mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$, где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$.

Так как вычисления, осуществляемые модулями $\mathfrak{M}^{(2)}_1$ и $\mathfrak{M}^{(2)}_2$, состоят в проверке коэффициентов a и b на их равенство нулю, то при $i = 1, 2$

$$T_i = \begin{cases} O(\log p), & \text{если } p \to \infty \text{ и число } k \text{ фиксировано} \\ O(\log k), & \text{если } k \to \infty \text{ и число } p \text{ фиксировано} \\ O(\log pk), & \text{если } p \to \infty \text{ и } k \to \infty \end{cases}. \tag{4.79}$$

В кольце $\mathcal{Z}_{p^k}$ (где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$) истинно равенство $\mathbb{Z}^{z.d}_{p^k} = \mathbb{Z}_{p^k} \backslash (\mathbb{Z}^{inv}_{p^k} \cup \{0\})$, а также неравенство $I_a \neq K$ для всех $a \in \mathbb{Z}^{z.d}_{p^k}$.

Следовательно, если $\mathcal{K} = \mathcal{Z}_{p^k}$, где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$, то в процессе функционирования $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$ не происходит активация модуля $\mathfrak{M}^{(2)}_3$, т.е.

$$T_3 = O(1) \ (p \to \infty \text{ или } k \to \infty). \tag{4.80}$$

Из (4.78)-(4.80) вытекает, что если $\mathcal{K} = \mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$), то временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$ определяется формулой (4.77).□

Охарактеризуем временную сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(2)}_{\mathcal{LA}(\mathcal{K})}$ в множестве колец $\mathfrak{K}^{fnt}$.

Вычисления, осуществляемые модулем $\mathfrak{M}^{(2)}_1$, состоят в проверке коэффициентов на их равенство нулю. Следовательно, временная сложность модуля $\mathfrak{M}^{(2)}_1$ в множестве колец $\mathfrak{K}^{fnt}$ определяется формулой

$$T^{(2)}_1 = O(\log |K|) \ (|K| \to \infty). \tag{4.81}$$

Вычисления, осуществляемые модулем $\mathfrak{M}^{(2)}_2$ сводятся к проверке условия «$b = 0$». Следовательно, временная сложность модуля $\mathfrak{M}^{(2)}_2$ в множестве колец $\mathfrak{K}^{fnt}$ определяется формулой

$$T^{(2)}_2 = O(\log |K|) \ (|K| \to \infty). \tag{4.82}$$

Если в кольце $\mathcal{K} \in \mathfrak{K}^{fnt}$ отсутствует эффективная техника разложения элементов кольца в произведение простых элементов, то проверка

принадлежности коэффициентов множеству (односторонних для не коммутативного кольца, и двусторонних для коммутативного кольца) делителей нуля может представлять собой исчерпывающий поиск по некоторому представленному в неявном виде подмножеству множества K, мощность которого может быть сравнима с мощностью множества K.

Аналогичным образом, если в кольце $\mathcal{K} \in \mathfrak{K}^{fnt}$ отсутствует эффективная техника разложения элементов кольца в произведение простых элементов, то проверка совпадения (одностороннего для не коммутативного кольца, и двустороннего для коммутативного кольца) аннулятора элемента кольца с множеством K, может представлять собой исчерпывающий поиск по некоторому представленному в неявном виде подмножеству множества K, мощность которого может быть сравнима с мощностью множества K.

Следовательно, временная сложность модуля $\mathfrak{M}_3^{(2)}$ в множестве колец $\mathfrak{K}^{fnt}$ имеет вид

$$T_3^{(2)} = O(\log |K|) \ (|K| \to \infty). \tag{4.83}$$

Так как $T_{\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(2)}} = T_1^{(2)} + T_2^{(2)} + T_3^{(2)}$, то из (4.81)-(4.83) вытекает, что

$$T_{\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(2)}} = O(|K|) \ (|K| \to \infty). \tag{4.84}$$

Рассмотрим $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(3)}$.

Теорема 4.9. Временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(3)}$ имеет вид

$$T_{\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(3)}} = \begin{cases} O(mn\log^2 p + \min\{m,n\}\log p), & \text{если } p \to \infty \text{ и } k \text{ фиксировано} \\ O(mnk^2 + \min\{m,n\}k), & \text{если } k \to \infty \text{ и } p \text{ фиксировано} \\ O(mnk^2\log^2 p + \min\{m,n\}k\log p), & \text{если } p \to \infty \text{ и } k \to \infty \end{cases}, \tag{4.85}$$

если $\mathcal{K} = \mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$).□

Доказательство. Временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(3)}$ равна

$$T_{\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(3)}} = T_1 + \max\{T_2, T_3\}, \tag{4.86}$$

где T_i $(i = 1, 2, 3)$ – временная сложность модуля $\mathfrak{M}_i^{(3)}$.

Пусть $\mathcal{K} = \mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$).

В поле $\mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$) любая система линейных уравнений

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{4.87}$$

может быть приведена к эквивалентной диагональной форме

$$\begin{cases} e_{i_1}x_{i_1} = \sum\limits_{j \in \mathbb{N}_n \setminus \{i_1,\ldots,i_r\}} c_{i_1 j}x_j + d_{i_1} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ e_{i_r}x_{i_r} = \sum\limits_{j \in \mathbb{N}_n \setminus \{i_1,\ldots,i_r\}} c_{i_r j}x_j + d_{i_r} \end{cases} . \tag{4.88}$$

Следовательно, если $\mathcal{K} = \mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$), то в процессе функционирования $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ не происходит активация модуля $\mathfrak{M}^{(3)}_3$, т.е.

$$T_3 = O(1) \ (p \to \infty \text{ или } k \to \infty). \tag{4.89}$$

Используя оценку $O(l^2)$ $(l \to \infty)$ временной сложности умножения двух l-разрядных чисел, получим, что при преобразовании (4.87) в (4.88) методом Гаусса временная сложность модуля $\mathfrak{M}^{(3)}_1$ определяется формулой

$$T_1 = O(mnk^2\log^2 p) \ (p \to \infty \text{ или } k \to \infty). \tag{4.90}$$

В процессе вычислений, осуществляемых модулем $\mathfrak{M}^{(3)}_2$, активация $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(1)}_{\mathcal{LA}(\mathcal{K})}$ осуществляется не более, чем $\min\{m, n\}$ раз. Следовательно, из (4.57) вытекает, что

$$T_2 = \begin{cases} O(\min\{m,n\}\log p), & \text{если } p \to \infty \text{ и } k \text{ фиксировано} \\ O(\min\{m,n\}k), & \text{если } k \to \infty \text{ и } \ p \text{ фиксировано} \\ O(\min\{m,n\}k\log p), & \text{если } p \to \infty \text{ и } k \to \infty \end{cases} , \tag{4.91}$$

Из (4.86) и (4.89)-(4.91) вытекает, что если $\mathcal{K} = \mathcal{GF}(p^k)$ (где p – простое число и $k \in \mathbb{N}$), то временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ определяется формулой (4.85).□

Теорема 4.10. Временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ имеет вид

$$T_{\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}} = \begin{cases} O(mn\log^2 p + \min\{m,n\}\log p), & \text{если } p \to \infty \text{ и } k \text{ фиксировано} \\ O(mnk^2 + \min\{m,n\}\log k), & \text{если } k \to \infty \text{ и } p \text{ фиксировано} \\ O(mnk^2\log^2 p + \min\{m,n\}\log pk), & \text{если } p \to \infty \text{ и } k \to \infty \end{cases}, \quad (4.92)$$

если $\mathcal{K} = \mathcal{Z}_{p^k}$, где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$.□

Доказательство. Временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ равна

$$T_{\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}} = T_1 + \max\{T_2, T_3\}, \quad (4.93)$$

где T_i $(i = 1,2,3)$ – временная сложность модуля $\mathfrak{M}^{(3)}_i$.

Пусть $\mathcal{K} = \mathcal{Z}_{p^k}$, где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$.

В кольце $\mathcal{K} = \mathcal{Z}_{p^k}$ любая система линейных уравнений

$$\begin{cases} a_{11} \circ x_1 \oplus \cdots \oplus a_{1n} \circ x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1} \circ x_1 \oplus \cdots \oplus a_{mn} \circ x_n = b_m \end{cases} \quad (4.94)$$

может быть приведена к эквивалентной диагональной форме

$$\begin{cases} e_{i_1} \circ x_{i_1} = \bigoplus\limits_{j \in \mathbb{N}_n \setminus \{i_1,\ldots,i_r\}} c_{i_1 j} \circ x_j \oplus d_{i_1} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ e_{i_r} \circ x_{i_r} = \bigoplus\limits_{j \in \mathbb{N}_n \setminus \{i_1,\ldots,i_r\}} c_{i_r j} \circ x_j \oplus d_{i_r} \end{cases}. \quad (4.95)$$

Следовательно, если $\mathcal{K} = \mathcal{Z}_{p^k}$, где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$, то в процессе функционирования $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}^{(3)}_{\mathcal{LA}(\mathcal{K})}$ не происходит активация модуля $\mathfrak{M}^{(3)}_3$, т.е.

$$T_3 = O(1) \ (p \to \infty \text{ или } k \to \infty). \quad (4.96)$$

Используя оценку $O(l^2)$ $(l \to \infty)$ временной сложности умножения двух l-разрядных чисел, получим, что при преобразовании (4.94) в (4.95)

методом Гаусса временная сложность модуля $\mathfrak{M}_1^{(3)}$ определяется формулой

$$T_1 = O(mnk^2\log^2 p)\ (p \to \infty \text{ или } k \to \infty). \tag{4.97}$$

В процессе вычислений, осуществляемых модулем $\mathfrak{M}_2^{(3)}$, активация $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}$ осуществляется не более, чем $\min\{m,n\}$ раз. Следовательно, из (4.63) вытекает, что

$$T_2 = \begin{cases} O(\min\{m,n\}\log p), & \text{если } p \to \infty \text{ и } k \text{ фиксировано} \\ O(\min\{m,n\}\log k), & \text{если } k \to \infty \text{ и } p \text{ фиксировано} \\ O(\min\{m,n\}\log pk), & \text{если } p \to \infty \text{ и } k \to \infty \end{cases}, \tag{4.99}$$

Из (4.93) и (4.96)-(4.99) вытекает, что если $\mathcal{K} = \mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$, где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$, то временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(3)}$ определяется формулой (4.92).□

Охарактеризуем временную сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(3)}$ в множестве колец $\mathfrak{K}^{fnt}$.

Временная сложность модуля $\mathfrak{M}_1^{(3)}$ (т.е. временная сложность приведения исследуемой системы линейных уравнений к эквивалентной диагональной форме), при отсутствии в кольце $\mathcal{K} \in \mathfrak{K}^{fnt}$ эффективной техники разложения элементов кольца в произведение простых элементов, определяется формулой

$$T_1^{(3)} = O(mn \cdot t_{mult}(\mathcal{K})),\ (|K| \to \infty) \tag{4.100}$$

где $t_{mult}(\mathcal{K})$ – время, необходимое для вычисления произведения двух элементов кольца $\mathcal{K} \in \mathfrak{K}^{fnt}$.

Найдем временную сложность модуля $\mathfrak{M}_2^{(3)}$.

Из (4.48)-(4.50) вытекает, что число вариантов системы линейных уравнений, представленной в диагональной форме, получаемых при подстановке всевозможных значений параметров, не превосходит величины $|K|^{n-r}$. При анализе каждого варианта диагональной формы осуществляется вызов $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}$. Следовательно, временная сложность модуля $\mathfrak{M}_2^{(3)}$ имеет вид

$$T_2^{(3)} = O(|K|^{n-r} \cdot T_{\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}})\ (|K| \to \infty), \tag{4.101}$$

где величина $T_{\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}}$ определяется формулой (4.72).

Найдем временную сложность модуля $\mathfrak{M}_3^{(3)}$.

Если в кольце $\mathcal{K} \in \mathfrak{K}^{fnt}$ отсутствует эффективная техника разложения элементов кольца в произведение простых элементов, то вычисления, осуществляемые модулем $\mathfrak{M}_3^{(3)}$, могут представлять собой, по своей сути, исчерпывающий поиск по всему множеству $\underbrace{K \times \cdots \times K}_{n \text{ раз}}$. При этом временная сложность проверки для каждого набора $x_i = c_i$ $(i = 1, \ldots, n)$ значений переменных свойства «быть решением исследуемой системы линейных уравнений» равна $O(mn \cdot t_{mult}(\mathcal{K}))$ $(|K| \to \infty)$. Следовательно, временная сложность модуля $\mathfrak{M}_3^{(3)}$ имеет вид

$$T_3^{(3)} = O(|K|^n \cdot mn \cdot t_{mult}(\mathcal{K})) \ (|K| \to \infty). \tag{4.102}$$

Так как $T_{\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(3)}} = T_1^{(3)} + \max\{T_2^{(3)}, T_3^{(3)}\}$, то из (4.100)-(4.102) вытекает, что

$$T_{\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(3)}} = O(mn \cdot t_{mult}(\mathcal{K}) +$$
$$+ \max\{|K|^{n-r} \cdot T_{\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}}, |K|^n \cdot mn \cdot t_{mult}(\mathcal{K})\}) \ (|K| \to \infty). \tag{4.103}$$

Временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(4)}$ в множестве колец $\mathfrak{K}^{fnt}$ определяется временной сложностью модуля $\mathfrak{M}_2^{(4)}$.

Если в кольце $\mathcal{K} \in \mathfrak{K}^{fnt}$ отсутствует эффективная техника разложения элементов кольца в произведение простых элементов, то вычисления, осуществляемые модулем $\mathfrak{M}_2^{(4)}$, могут представлять собой, по своей сути, исчерпывающий поиск по всему множеству $\underbrace{(K \backslash \{0\}) \times \cdots \times (K \backslash \{0\})}_{n \text{ раз}}$. При этом для каждого набора значений параметров $(\alpha_1, \ldots, \alpha_n)$ осуществляется вызов $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(3)}$. Отсюда и из (4.103) вытекает, что временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(4)}$ в множестве колец $\mathfrak{K}^{fnt}$ имеет вид

$$T_{\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(4)}} = O((|K| - 1)^n (mn \cdot t_{mult}(\mathcal{K}) +$$
$$+ \max\{|K|^{n-r} \cdot T_{\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}^{(1)}}, |K|^n \cdot mn \cdot t_{mult}(\mathcal{K})\})) \ (|K| \to \infty). \tag{4.104}$$

В своей совокупности формулы (4.72), (4.84), (4.103) и (4.104) характеризуют в множестве колец $\mathfrak{K}^{fnt}$ временную сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}$ в зависимости от типа атомов, исследуемых им.

4.3. Выводы.

В настоящем разделе исследована задача проверки выполнимости формул линейной арифметики над любым конечным ассоциативным кольцом $\mathcal{K} = (K, +, \cdot)$ с ненулевым умножением. Основные результаты состоят в следующем:

1. Охарактеризовано множество $\mathfrak{K}^{fnt}$ всех конечных ассоциативных колец с ненулевым умножением.

2. В терминах (односторонних для не коммутативных колец и двусторонних для коммутативных колец) аннуляторов ненулевых элементов кольца охарактеризованы множества решений простейших атомов линейной арифметики над любым кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$.

3. На основе техники «наслоения» (layering) впервые построен $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}$, предназначенный для проверки выполнимости формул линейной арифметики над любым кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$.

4. Охарактеризована временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}$.

В своей совокупности полученные в настоящем разделе результаты представляют собой фрагмент теории, которая может быть использована при построении приемлемых на практике программных реализаций решателей, предназначенных для анализа и верификации математических моделей, построенных в терминах конечных колец.

Построение таких программных реализаций решателей актуально с теоретической и с прикладной точки зрения.

Одним из возможных направлений дальнейших исследований является детализация полученных результатов для не коммутативных колец квадратных матриц над конечным полем $\mathcal{GF}(p^k)$ или кольцом вычетов $\mathcal{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$, где p – простое число и $k \in \mathbb{N}$ $(k \geq 2)$. Такие кольца имеют многочисленные применения при решении как теоретических, так и прикладных задач.

Другое направление связано с выделением нетривиальных подмножеств колец $\mathcal{K} \in \mathfrak{K}^{fnt}$, для которых имеют место высокие оценки временной сложности анализа простейших атомов линейной арифметики.

Третье направление связано с построением решателей, предназначенных для проверки выполнимости простейших атомов нелинейной арифметики над теми или иными классами колец $\mathcal{K} \in \mathfrak{K}^{fnt}$.

5. АВТОМАТЫ НАД КОНЕЧНЫМ КОЛЬЦОМ

Анализ свойств семейств автоматов, заданных системами рекуррентных соотношений с параметрами (см. п.1.3.3) над конечным кольцом, является предметом исследования нового раздела алгебраической теории автоматов. Объект исследования (т.е. система рекуррентных соотношений с параметрами над конечным кольцом) дает возможность установить глубокие внутренние связи между моделями и методами теории автоматов, теории систем, теории алгебраических систем и комбинаторного анализа, а также открывает широкие возможности для взаимопроникновения этих моделей и методов.

Именно разработке основ математического аппарата, предназначенного для анализа семейств автоматов, заданных системами рекуррентных соотношений с параметрами над конечным кольцом, посвящены разделы 2-4.

Со своей стороны, потенциальные приложения семейств автоматов, заданных системами рекуррентных соотношений с параметрами над конечным кольцом, в процессе решения задач защиты информации (в частности, криптографии) определяют ряд основных модельных задач. Такими задачами являются выделение множества обратимых автоматов и построение обратного автомата, анализ сложности параметрической идентификации и идентификации начального состояния автомата, принадлежащего заданному семейству, анализ множества неподвижных точек автоматных отображений, реализуемых инициальными автоматами, принадлежащими заданному семейству.

При этом, как с позиции алгебраической теории автоматов, так и с позиции потенциальных приложений семейств автоматов, заданных системами рекуррентных соотношений с параметрами над конечным кольцом, в процессе решения задач защиты информации актуальным является вопрос о том, насколько переход к семействам обратимых автоматов упрощает решение перечисленных выше задач.

Цель настоящего раздела и состоит в исследовании семейств автоматов, заданных системами рекуррентных соотношений с параметрами над конечным кольцом, с позиции перечисленных выше модельных задач.

В п.5.1 определены исследуемые модели и охарактеризованы особенности решения перечисленных выше задач. В п.5.2 исследуется задача построения имитационной модели, моделирующей семейство автоматов, заданное системой рекуррентных соотношений с параметрами над конечным кольцом. Актуальность этой задачи обусловлена тем, что одной из наиболее опасных и наименее изученных атак является «атака на алгоритм шифрования». При такой атаке целью криптоаналитика является не идентификация ключа, а попытка построения в результате эксперимента своего алгоритма шифрования, дающего ему возможность успешно решать поставленную им задачу. В п.5.3 исследуется задача использования семейства автоматов без выхода, заданного системой рекуррентных соотношений с параметрами над конечным кольцом, в качестве семейства хеш-функций. Актуальность этой задачи обусловлена тем, что в основе практически всех используемых в настоящее время хеш-функций лежит применение рекуррентного соотношения, преобразующего двоичную последовательность фиксированной длины в двоичную последовательность этой же длины. В п.5.4 исследуются автоматы над конечным кольцом, функции переходов и выходов которых являются алгебраическими суммами функции от состояния автомата и функ-

ции от входного символа при условии, что значение каждой компоненты функции переходов принадлежит фиксированным идеалам кольца. Актуальность этой задачи обусловлена тем, что имеется глубокая внутренняя связь между понятием «идеал кольца» и понятием «многообразие» в алгебраической геометрии (см. п.1.2.1). П.5.5 содержит ряд заключительных замечаний.

Результаты автора, представленные в настоящем разделе, опубликованы в работах [70,72-74,82,84,86,88,89,91,95,96,99,211].

5.1. Анализ модельных задач.

Определим исследуемые модели семейств автоматов и рассмотрим особенности решения основных модельных задач, определяющих потенциальную возможность применения этих семейств автоматов в процессе решения задач защиты информации.

5.1.1. Основные модели.

Зафиксируем кольцо $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$.

В п.1.3.3 было отмечено, что для любых чисел $n_1, n_2, n_3, l \in \mathbb{N}$ при фиксированном множестве параметров $\mathbf{A}$ ($\emptyset \neq \mathbf{A} \subseteq K^l$) любые отображения $\mathbf{f}_1 : K^{n_1} \times K^{n_2} \times \mathbf{A} \to K^{n_1}$ и $\mathbf{f}_2 : K^{n_1} \times K^{n_2} \times \mathbf{A} \to K^{n_3}$ задают над кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$ семейство $\mathcal{M}_{\mathbf{f}_1,\mathbf{f}_2,\mathbf{A}} = \{M_{\mathbf{a}}\}_{\mathbf{a}\in\mathbf{A}}$ автоматов Мили

$$M_{\mathbf{a}} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \end{cases} \quad (t \in \mathbb{Z}_+), \tag{5.1}$$

а любые отображения $\mathbf{f}_1 : K^{n_1} \times K^{n_2} \times \mathbf{A} \to K^{n_1}$ и $\mathbf{f}_2 : K^{n_1} \times \mathbf{A} \to K^{n_3}$ – семейство $\mathcal{M}_{\mathbf{f}_1,\mathbf{f}_2,\mathbf{A}} = \{M_{\mathbf{a}}\}_{\mathbf{a}\in\mathbf{A}}$ автоматов Мура

$$M_{\mathbf{a}} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_{t+1}, \mathbf{a}) \end{cases} \quad (t \in \mathbb{Z}_+). \tag{5.2}$$

В п.1.3.3 также было отмечено, что построение над кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$ аналогов хаотических динамических систем естественно приводит к выделению в множестве определенных выше семейств автоматов таких подмножеств семейств $\mathcal{M}_{\mathbf{f}_1,\mathbf{f}_2,\mathbf{f}_3,\mathbf{f}_4,\mathbf{A}} = \{M_{\mathbf{a}}\}_{\mathbf{a}\in\mathbf{A}}$ автоматов Мили

$$M_{\mathbf{a}} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{a}_1) + \mathbf{f}_2(\mathbf{x}_{t+1}, \mathbf{a}_2) \\ \mathbf{y}_{t+1} = \mathbf{f}_3(\mathbf{q}_t, \mathbf{a}_3) + \mathbf{f}_4(\mathbf{x}_{t+1}, \mathbf{a}_4) \end{cases} \quad (t \in \mathbb{Z}_+), \tag{5.3}$$

и подмножеств семейств $\mathcal{M}_{\mathbf{f}_1,\mathbf{f}_2,\mathbf{f}_3,\mathbf{A}} = \{M_{\mathbf{a}}\}_{\mathbf{a}\in\mathbf{A}}$ автоматов Мура

$$M_{\mathbf{a}} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{a}_1) + \mathbf{f}_2(\mathbf{x}_{t+1}, \mathbf{a}_2) \\ \mathbf{y}_{t+1} = \mathbf{f}_3(\mathbf{q}_{t+1}, \mathbf{a}_3) \end{cases} \quad (t \in \mathbb{Z}_+), \tag{5.4}$$

что:

1) для автоматов Мили вектор параметров $\mathbf{a} \in \mathbf{A}$ представлен в виде $\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_4)$, причем $\mathbf{a}_i \in \mathbf{A}_i$ $(i = 1, \ldots, 4)$, где $\emptyset \neq \mathbf{A}_i \subseteq K^{l_i}$, а $l_i \in \mathbb{Z}_+$ $(i = 1, \ldots, 4)$ и $l = l_1 + l_2 + l_3 + l_4$;

2) для автоматов Мура вектор параметров $\mathbf{a} \in \mathbf{A}$ представлен в виде $\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)$, причем $\mathbf{a}_i \in \mathbf{A}_i$ $(i = 1, 2, 3)$, где $\emptyset \neq \mathbf{A}_i \subseteq K^{l_i}$, а $l_i \in \mathbb{Z}_+$ $(i = 1, 2, 3)$ и $l = l_1 + l_2 + l_3$;

3) $\mathbf{f}_1 : K^{n_1} \times \mathbf{A}_1 \to K^{n_1}$, $\mathbf{f}_2 : K^{n_2} \times \mathbf{A}_2 \to K^{n_1}$, $\mathbf{f}_3 : K^{n_1} \times \mathbf{A}_3 \to K^{n_3}$ и $\mathbf{f}_4 : K^{n_2} \times \mathbf{A}_4 \to K^{n_3}$ – произвольные фиксированные отображения.

Замечание 5.1. В дальнейшем считаем, что отображения $\mathbf{f}_i$ $(i = 1, \ldots, 4)$ фиксированы, и будем опускать их при обозначении семейства автоматов, т.е. будем обозначать семейство автоматов через $\mathcal{M}_{\mathbf{A}}$.

Отметим, что:

1. Для автомата $M_{\mathbf{a}}$, определенного любым из соотношений (5.1)-(5.4) множества $\mathbf{Q} = K^{n_1}$, $\mathbf{X} = K^{n_2}$ и $\mathbf{Y} = K^{n_3}$ являются, соответственно, множеством состояний, входным и выходным алфавитом.

2. Если для семейства автоматов (5.1) (соответственно, (5.2)) переменная $\mathbf{q}_t$ (соответственно, $\mathbf{q}_{t+1}$) является фиктивной переменной для отображения $\mathbf{f}_2$, то соотношение (5.1) (соответственно, (5.2)) задает семейство автоматов без памяти. При этом каждый автомат, заданный соотношением (5.2), генерирует постоянную последовательность в алфавите $\mathbf{Y}$.

3. Если для семейства автоматов (5.1) (соответственно, (5.2)) переменная $\mathbf{x}_{t+1}$ является фиктивной переменной для отображений $\mathbf{f}_1$ и $\mathbf{f}_2$ (соответственно, для отображения $\mathbf{f}_1$), то соотношение (5.1) (соответственно, (5.2)) задает семейство автономных автоматов (или, иными словами, семейство рекуррентных генераторов последовательностей в алфавите $\mathbf{Y}$).

4. Если для семейства автоматов (5.3) (соответственно, (5.4)) переменная $\mathbf{q}_t$ (соответственно, $\mathbf{q}_{t+1}$) является фиктивной переменной для отображения $\mathbf{f}_3$, то соотношение (5.3) (соответственно, (5.4)) задает семейство автоматов без памяти. При этом каждый автомат, заданный соотношением (5.4), генерирует постоянную последовательность в алфавите $\mathbf{Y}$.

5. Если для семейства автоматов (5.3) (соответственно, (5.4)) переменная $\mathbf{x}_{t+1}$ является фиктивной переменной для отображений $\mathbf{f}_2$ и $\mathbf{f}_4$ (соответственно, для отображения $\mathbf{f}_2$), то соотношение (5.3) (соответственно, (5.4)) задает семейство автономных автоматов.

В п.1.3.1 было отмечено, что семейство обратимых автоматов представляет, по своей сути, математическую модель поточного шифра. Оха-

рактеризуем семейства обратимых автоматов, определяемых соотношениями (5.1)-(5.4).

Пусть семейство автоматов задано соотношением (5.1). Автомат $M_{\mathbf{a}}$ обратимый тогда и только тогда, когда $n_2 \leq n_3$, и существует такое отображение $\mathbf{h} : \mathbf{A} \to K^{l'}$, а также такое отображение

$$\mathbf{g} : \mathbf{Q} \times Val\, \mathbf{f}_2 \times \mathbf{h}(\mathbf{A}) \to \mathbf{X},$$

что равенство $\mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a})$ $(t \in \mathbb{Z}_+)$ может быть преобразовано в эквивалентное равенство $\mathbf{x}_{t+1} = \mathbf{g}(\mathbf{q}_t, \mathbf{y}_{t+1}, \mathbf{h}(\mathbf{a}))$. При этом обратный автомат $M_{\mathbf{a}}^{-1}$ имеет вид

$$M_{\mathbf{a}}^{-1} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{g}(\mathbf{q}_t, \mathbf{y}_{t+1}, \mathbf{h}(\mathbf{a})), \mathbf{a}) \\ \mathbf{x}_{t+1} = \mathbf{g}(\mathbf{q}_t, \mathbf{y}_{t+1}, \mathbf{h}(\mathbf{a})) \end{cases} \quad (t \in \mathbb{Z}_+). \tag{5.5}$$

Пусть семейство автоматов задано соотношением (5.2). Автомат $M_{\mathbf{a}}$ обратимый тогда и только тогда, когда $n_2 \leq n_3$, и существуют такие отображения $\mathbf{h}_1 : \mathbf{A} \to K^{l'}$ и $\mathbf{h}_2 : \mathbf{A} \to K^{l''}$, а также такие отображения

$$\mathbf{g}_1 : Val\, \mathbf{f}_1 \times \mathbf{Q} \times \mathbf{h}_1(\mathbf{A}) \to \mathbf{X}$$

и

$$\mathbf{g}_2 : Val\, \mathbf{f}_2 \times \mathbf{h}_2(\mathbf{A}) \to Val\, \mathbf{f}_1,$$

что равенство $\mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a})$ $(t \in \mathbb{Z}_+)$ может быть представлено в виде эквивалентного равенства $\mathbf{x}_{t+1} = \mathbf{g}_1(\mathbf{q}_{t+1}, \mathbf{q}_t, \mathbf{h}_1(\mathbf{a}))$, а равенство $\mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_{t+1}, \mathbf{a})$ $(t \in \mathbb{Z}_+)$ может быть представлено в виде эквивалентного равенства $\mathbf{q}_{t+1} = \mathbf{g}_2(\mathbf{y}_{t+1}, \mathbf{h}_2(\mathbf{a}))$. При этом обратный автомат $M_{\mathbf{a}}^{-1}$ имеет вид

$$M_{\mathbf{a}}^{-1} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{g}_2(\mathbf{y}_{t+1}, \mathbf{h}_2(\mathbf{a})) \\ \mathbf{x}_{t+1} = \mathbf{g}_1(\mathbf{g}_2(\mathbf{y}_{t+1}, \mathbf{h}_2(\mathbf{a})), \mathbf{q}_t, \mathbf{h}_1(\mathbf{a})) \end{cases} \quad (t \in \mathbb{Z}_+). \tag{5.6}$$

Пусть семейство автоматов задано соотношением (5.3). Автомат $M_{\mathbf{a}}$ обратимый тогда и только тогда, когда $n_2 \leq n_3$, и существует такое отображения $\mathbf{h} : \mathbf{A}_3 \times \mathbf{A}_4 \to K^{l'}$, а также такое отображение

$$\mathbf{g} : \mathbf{Q} \times (Val\, \mathbf{f}_3 + Val\, \mathbf{f}_4) \times \mathbf{h}(\mathbf{A}_3 \times \mathbf{A}_4) \to \mathbf{X},$$

что равенство $\mathbf{y}_{t+1} = \mathbf{f}_3(\mathbf{q}_t, \mathbf{a}_3) + \mathbf{f}_4(\mathbf{x}_{t+1}, \mathbf{a}_4)$ $(t \in \mathbb{Z}_+)$ может быть преобразовано в эквивалентное равенство $\mathbf{x}_{t+1} = \mathbf{g}(\mathbf{q}_t, \mathbf{y}_{t+1}, \mathbf{h}(\mathbf{a}_3, \mathbf{a}_4))$. При

этом обратный автомат $M_{\mathbf{a}}^{-1}$ имеет вид

$$M_{\mathbf{a}}^{-1}:\begin{cases}\mathbf{q}_{t+1}=\mathbf{f}_1(\mathbf{q}_t,\mathbf{a}_1)+\mathbf{f}_2(\mathbf{g}(\mathbf{q}_t,\mathbf{y}_{t+1},\mathbf{h}(\mathbf{a}_3,\mathbf{a}_4)),\mathbf{a}_2)\\ \mathbf{x}_{t+1}=\mathbf{g}(\mathbf{q}_t,\mathbf{y}_{t+1},\mathbf{h}(\mathbf{a}_3,\mathbf{a}_4))\end{cases}\quad(t\in\mathbb{Z}_+).\quad(5.7)$$

Пусть семейство автоматов задано соотношением (5.4). Автомат $M_{\mathbf{a}}$ обратимый тогда и только тогда, когда $n_2 \le n_3$, и существуют такие отображения $\mathbf{h}_1 : \mathbf{A}_1 \times \mathbf{A}_2 \to K^{l'}$ и $\mathbf{h}_2 : \mathbf{A}_3 \to K^{l''}$, а также такие отображения

$$\mathbf{g}_1 : (Val\,\mathbf{f}_1 + Val\,\mathbf{f}_2) \times \mathbf{Q} \times \mathbf{h}(\mathbf{A}_1 \times \mathbf{A}_2) \to \mathbf{X}$$

и

$$\mathbf{g}_2 : Val\,\mathbf{f}_3 \times \mathbf{h}_2(\mathbf{A}_3) \to Val\,\mathbf{f}_1 + Val\,\mathbf{f}_2,$$

что равенство $\mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{a}_1) + \mathbf{f}_2(\mathbf{x}_{t+1}, \mathbf{a}_2)$ $(t \in \mathbb{Z}_+)$ может быть представлено в виде в эквивалентного равенства $\mathbf{x}_{t+1} = \mathbf{g}_1(\mathbf{q}_{t+1}, \mathbf{q}_t, \mathbf{h}_1(\mathbf{a}_1, \mathbf{a}_2))$, а равенство $\mathbf{y}_{t+1} = \mathbf{f}_3(\mathbf{q}_{t+1}, \mathbf{a}_3)$ $(t \in \mathbb{Z}_+)$ может быть представлено в виде в эквивалентного равенства $\mathbf{q}_{t+1} = \mathbf{g}_2(\mathbf{y}_{t+1}, \mathbf{h}_2(\mathbf{a}_3)$. При этом обратный автомат $M_{\mathbf{a}}^{-1}$ имеет вид

$$M_{\mathbf{a}}^{-1}:\begin{cases}\mathbf{q}_{t+1}=\mathbf{g}_2(\mathbf{y}_{t+1},\mathbf{h}_2(\mathbf{a}_3))\\ \mathbf{x}_{t+1}=\mathbf{g}_1(\mathbf{g}_2(\mathbf{y}_{t+1},\mathbf{h}_2(\mathbf{a}_3)),\mathbf{q}_t,\mathbf{h}_1(\mathbf{a}_1,\mathbf{a}_2))\end{cases}\quad(t\in\mathbb{Z}_+).\qquad(5.8)$$

Замечание 5.2. Выходным алфавитом автомата $M_{\mathbf{a}}^{-1}$, заданного любым из соотношений (5.5)-(5.8), является множество $\mathbf{X}$. Входным алфавитом автомата $M_{\mathbf{a}}^{-1}$, заданного соотношением (5.5) или (5.6), является множество $Val\,\mathbf{f}_2$, входным алфавитом автомата $M_{\mathbf{a}}^{-1}$, заданного соотношением (5.7), является множество $Val\,\mathbf{f}_3 + Val\,\mathbf{f}_4$, а входным алфавитом автомата $M_{\mathbf{a}}^{-1}$, заданного соотношением (5.8), является множество $Val\,\mathbf{f}_3$.

5.1.2. Особенности решения модельных задач.

Рассмотрим вначале задачу анализа множества неподвижных точек $S_{fxd}(M_{\mathbf{a}}, \mathbf{q}_0)$ $(M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}, \mathbf{q}_0 \in \mathbf{Q})$ отображения $f_{(M_{\mathbf{a}},\mathbf{q}_0)}$, реализуемого инициальным автоматом $(M_{\mathbf{a}}, \mathbf{q}_0)$, где $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ – автомат, заданный любой из систем рекуррентных соотношений (5.1)-(5.4).

Решение этой задачи актуально в процессе анализа возможности использования обратимого автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ в качестве математической модели поточного шифра, так для обеспечения для шифра условия «быть вычислительно стойким шифром» необходимо, чтобы, по крайней

мере, почти все входные последовательности не принадлежали множеству $S_{fxd}(M_{\mathbf{a}}, \mathbf{q}_0)$.

Замечание 5.3. В п.1.3.1 было показано, что при исследовании множества $S_{fxd}(M_{\mathbf{a}}, \mathbf{q}_0)$ достаточно ограничиться анализом множества $S^{(1)}_{fxd}(M_{\mathbf{a}}, \mathbf{q}_0)$ входных символов, являющихся неподвижными точками отображения $f_{(M_{\mathbf{a}}, \mathbf{q}_0)}$.

Из (5.1)-(5.4) вытекает, что проверка условия «$S_{fxd}(M_{\mathbf{a}}, \mathbf{q}_0) = \emptyset$» ($M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}, \mathbf{q}_0 \in \mathbf{Q}$) сводится:

1) к проверке выполнимости формулы

$$\mathbf{x} = \mathbf{f}_2(\mathbf{q}_0, \mathbf{x}, \mathbf{a}), \tag{5.9}$$

если автомат $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ задан соотношением (5.1);

2) к проверке выполнимости формулы

$$\mathbf{x} = \mathbf{f}_2(\mathbf{f}_1(\mathbf{q}_0, \mathbf{x}, \mathbf{a}), \mathbf{a}), \tag{5.10}$$

если автомат $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ задан соотношением (5.2);

3) к проверке выполнимости формулы

$$\mathbf{x} = \mathbf{f}_3(\mathbf{q}_0, \mathbf{a}_3) + \mathbf{f}_4(\mathbf{x}, \mathbf{a}_4), \tag{5.11}$$

если автомат $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ задан соотношением (5.3);

4) к проверке выполнимости формулы

$$\mathbf{x} = \mathbf{f}_3(\mathbf{f}_1(\mathbf{q}_0, \mathbf{a}_1) + \mathbf{f}_2(\mathbf{x}, \mathbf{a}_2), \mathbf{a}_3), \tag{5.12}$$

если автомат $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ задан соотношением (5.4).

Из равенств (5.9)-(5.12) вытекает, что:

1. Проверка условия «$S_{fxd}(M_{\mathbf{a}}, \mathbf{q}_0) = \emptyset$» ($M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}, \mathbf{q}_0 \in \mathbf{Q}$) может быть выполнена непосредственным применением $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}$, построенного в п.4.2, в следующих случаях:

Случай 5.1. Автомат $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$, заданный соотношением (5.1) или соотношением (5.3), является автоматом с линейной функцией выхода.

Случай 5.2. Автомат $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$, заданный соотношением (5.2) или соотношением (5.4), является линейным автоматом.

2. Проверка условия «$S_{fxd}(M_{\mathbf{a}}, \mathbf{q}_0) = \emptyset$» ($M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}, \mathbf{q}_0 \in \mathbf{Q}$) может быть выполнена непосредственным применением предложенной в п.3.1.4 схемы построения множества решений системы полиномиальных уравнений (причем вычисления сразу же оканчиваются, если установлено, что множество решений исследуемой системы полиномиальных уравнений непусто) в следующих случаях:

Случай 5.3. Автомат $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$, заданный соотношением (5.1) или соотношением (5.3), представляет собой автомат, функция выходов которого является системой полиномиальных рекуррентных соотношений.

Случай 5.4. Автомат $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$, заданный соотношением (5.2) или соотношением (5.4), представляет собой автомат, у которого как функция выходов, так и функция переходов являются системами полиномиальных рекуррентных соотношений.

В остальных случаях для проверки условия «$S_{fxd}(M_{\mathbf{a}}, \mathbf{q}_0) = \emptyset$» ($M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}, \mathbf{q}_0 \in \mathbf{Q}$) требуется разработка специальных методов анализа выполнимости формул (5.9)-(5.12), т.е. методов, существенно зависящих как от вида отображений, определяющих автомат $M_{\mathbf{a}}$, так и от алгебраических свойств кольца $\mathcal{K} \in \mathfrak{K}^{fnt}$.

Рассмотрим теперь задачи идентификации автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$, определенного любой из систем рекуррентных соотношений (5.1)-(5.4), в предположении, что экспериментатору известны значения параметров (т.е. известен исследуемый автомат).

С помощью последовательной подстановки 1-го рекуррентного соотношения во 2-е рекуррентное соотношение, последнее всегда может быть преобразовано в формулу, которая содержит входную последовательность, подаваемую на автомат, а из состояний автомата – только его начальное состояние, т.е. в рекуррентное соотношение вида

$$\mathbf{y}_{t+1} = \mathbf{F}(\mathbf{q}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{t+1}) \ (t \in \mathbb{Z}_+). \tag{5.13}$$

Именно рекуррентное соотношение (5.13) и используется в процессе решения задач идентификации автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$, определенного любой из систем рекуррентных соотношений (5.1)-(5.4).

Задача идентификации начального состояния $\mathbf{q}_0 \in \mathbf{Q}$ (с точностью до множества эквивалентных ему состояний) в предположении, что экспериментатору известен автомат $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ (т.е. известна система рекуррентных соотношений, определяющих автомат $M_{\mathbf{a}}$) всегда разрешима кратным экспериментом.

Замечание 5.4. Известно, что (см., напр., [15]) идентификация начального состояния (с точностью до множества эквивалентных ему состояний) заданного автомата с k состояниями ($k \geq 2$) и m-элементным входным алфавитом всегда разрешима кратным экспериментом высоты $k-1$ и кратности m^{k-1}. Также известно, что эта задача не всегда разрешима простым экспериментом.

Решение задачи идентификации начального состояния $\mathbf{q}_0 \in \mathbf{Q}$ заданного автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ осуществляется следующим образом.

В результате подстановок в (5.13) всевозможных начальных отрезков вход-выходных пар, полученных в ходе эксперимента, формируется система уравнений, для которой переменной является начальное состояние $\mathbf{q}_0$ автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$. Решение этой системы уравнений и является решением задачи идентификации начального состояния $\mathbf{q}_0 \in \mathbf{Q}$ заданного автомата $M_{\mathbf{a}}$.

Отметим, что даже над кольцом $\mathcal{K} \in \mathfrak{K}_1^{fnt}$ (т.е. ассоциативно-коммутативным кольцом с единицей) решение задачи идентификации начального состояния $\mathbf{q}_0 \in \mathbf{Q}$ заданного автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ сводится к решению достаточно сложных систем уравнений над кольцом $\mathcal{K}$. Сказанное, в частности, истинно уже для семейства линейных автоматов над кольцом $\mathcal{K} \in \mathfrak{K}_1^{fnt}$ (см. пример 1.7).

Более того, в [80] показано, что если $\mathcal{M}_{\mathbf{A}}$ – семейство автоматов с нелинейной функцией переходов над кольцом $\mathcal{K} \in \mathfrak{K}_1^{fnt}$, то решение задачи идентификации начального состояния $\mathbf{q}_0 \in \mathbf{Q}$ заданного автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ сводится к решению достаточно сложных нелинейных систем уравнений над кольцом $\mathcal{K}$.

Замечание 5.5. Ясно, что сложность решения задачи идентификации начального состояния $\mathbf{q}_0 \in \mathbf{Q}$ заданного автомата $M_{\mathbf{a}}$, принадлежащего семейству автоматов $\mathcal{M}_{\mathbf{A}}$, существенно возрастает, если $K \in \mathfrak{K}^{fnt} \backslash \mathfrak{K}_1^{fnt}$.

При этом в [80] показано, что даже над кольцом $\mathcal{K} \in \mathfrak{K}_1^{fnt}$ переход к семействам обратимых автоматов не упрощает решение задачи идентификации начального состояния автомата. Именно это обстоятельство и является обоснованием целесообразности выбора начального состояния обратимого автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ в качестве секретного сеансового ключа соответствующего поточного шифра.

Значительно более сложным является решение задачи параметрической идентификации автомата $M_{\mathbf{a}}$, принадлежащего заданному семейству автоматов $\mathcal{M}_{\mathbf{A}}$.

Замечание 5.6. Эта задача, по своей сути, является задачей идентификации автомата $M_{\mathbf{a}}$, принадлежащего заданному семейству автоматов $\mathcal{M}_{\mathbf{A}}$ (см. п.1.3.2).

При исследовании задачи параметрической идентификации автомата $M_{\mathbf{a}}$, принадлежащего заданному семейству автоматов $\mathcal{M}_{\mathbf{A}}$, естественно выделяются следующие три случая.

Случай 5.5. Экспериментатору не известно начальное состояние $\mathbf{q}_0$ исследуемого автомата.

В этом случае в результате подстановок в (5.13) всевозможных начальных отрезков вход-выходных пар, полученных в ходе эксперимента, формируется система уравнений, для которой переменными являются параметры и неизвестное начальное состояние $\mathbf{q}_0$. Решение этой системы уравнений представляется множеством утверждений вида «если начальное состояние $\mathbf{q}_0$ принадлежит множеству ..., то значениями параметров являются ...».

Это множество утверждений и является решением задачи параметрической идентификации автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$.

Случай 5.6. Экспериментатору известно начальное состояние $\mathbf{q}_0$ исследуемого автомата.

В этом случае в результате подстановок в (5.13) всевозможных начальных отрезков вход-выходных пар, полученных в ходе эксперимента, формируется система уравнений, для которой переменными являются только параметры. Решение этой системы уравнений и является решением задачи параметрической идентификации автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$.

Случай 5.7. Экспериментатор может принудительно устанавливать исследуемый автомат в любое известное ему начальное состояние требуемое число раз.

В этом случае в результате подстановок в (5.13) всевозможных начальных отрезков вход-выходных пар, полученных в ходе каждого из экспериментов, формируются подсистемы уравнений, для которой переменными являются только параметры. Эти подсистемы объединяются в одну систему уравнений. Решение полученной системы уравнений и является решением задачи параметрической идентификации автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$.

Замечание 5.7. Несложно заметить, что случаи 5.5-5.7 упорядочены в порядке усиления возможностей экспериментатора в процессе решения задачи параметрической идентификации автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$.

Действительно, наименее слабыми являются возможности экспериментатора в случае 5.5, так как число утверждений, являющихся решением задачи параметрической идентификации автомата (т.е. число допустимых автоматов) может быть достаточно большим. В случае 5.6 возможности экспериментатора несколько возрастают по сравнению со случаем 5.5 (насколько именно возрастают эти возможности, зависит от структуры автоматов, принадлежащих семейству $\mathcal{M}_{\mathbf{A}}$). В случае 5.7 возможности экспериментатора существенно возрастают по сравнению с его возможностями в

случае 5.6, так как экспериментатор потенциально имеет возможность осуществить полный анализ исследуемого автомата на основе кратных экспериментов, проводимых в каждом начальном состоянии автомата.

В [80] показано, что даже в случае 5.7 решение задачи параметрической идентификации автомата $M_{\mathbf{a}}$, принадлежащего заданному семейству автоматов $\mathcal{M}_{\mathbf{A}}$ над кольцом $\mathcal{K} \in \mathfrak{K}_1^{fnt}$, сводится к решению достаточно сложных систем нелинейных уравнений над кольцом $\mathcal{K}$. При этом в множестве параметров, определяющих автомат $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$, может быть выделено подмножество параметров, идентификация которых осуществляется достаточно легко, а также подмножество параметров, идентификация которых является сложной задачей.

Замечание 5.8. Ясно, что сложность решения задачи параметрической идентификации автомата $M_{\mathbf{a}}$, принадлежащего заданному семейству автоматов $\mathcal{M}_{\mathbf{A}}$, существенно возрастает, если $K \in \mathfrak{K}^{fnt} \backslash \mathfrak{K}_1^{fnt}$.

Кроме того, в [80] показано, что даже в случае 5.7 переход к семействам обратимых автоматов не упрощает решение задачи параметрической идентификации автомата, принадлежащего заданному семейству автоматов $\mathcal{M}_{\mathbf{A}}$ над кольцом $\mathcal{K} \in \mathfrak{K}_1^{fnt}$.

Именно этот результат и является обоснованием целесообразности выбора параметров, определяющих обратимый автомат $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ в качестве секретного ключа средней длительности для соответствующего поточного шифра (при этом может быть выделено подмножество параметров, обеспечению секретности которых следует уделить особое внимание, т.е. параметры идентификация которых является сложной задачей).

Следует особо отметить и следующее обстоятельство. В процессе решения задачи параметрической идентификации автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ множество значений параметров не всегда вычисляется в явном виде. Это означает, что в результате решения системы уравнений может быть получено множество некоторых комбинаций значений параметров, из которого сложно (а иногда и невозможно) однозначно определить конкретный автомат $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$.

Указанная выше ситуация, по-видимому, является типичной для таких семейств нелинейных автоматов с лагом l ($l \geq 2$), что в рекуррентных соотношениях, определяющих автомат $M_{\mathbf{a}}$, состояние $\mathbf{q}_{t+1}$ и/или выходной символ $\mathbf{y}_{t+1}$ при $t \geq l-1$ существенно (и нелинейно) зависят от последовательности состояний $\mathbf{q}_t, \ldots, \mathbf{q}_{t-l+1}$.

Проиллюстрируем сказанное следующим простым примером.

Пример 5.1. Пусть $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}_1^{fnt}$ и

$$\mathbf{A} = \{\mathbf{a} = (a, b, c, d, e) \in K^5 | a, b, c \in K \backslash \{0\} \& d, e \in K^{inv}\},$$

а семейство $\mathcal{M}_{\mathbf{A}}$ нелинейных одномерных автоматов Мура с лагом 2 определено над кольцом $\mathcal{K}$ системой рекуррентных соотношений

$$M_{\mathbf{a}} : \begin{cases} q_{t+2} = a + bq_{t+1}^2 + cq_t + dx_{t+1} \\ y_{t+1} = eq_{t+2} \end{cases} \quad (t \in \mathbb{Z}_+), \tag{5.14}$$

где x_{t+1} и y_{t+1} являются, соответственно, входным и выходным символом в момент $t+1$, а $\mathbf{q}_t = (q_{t+1}, q_t)$ – состояние в момент t.

Рассмотрим задачу параметрической идентификации автомата $M_{\mathbf{a}}$ ($\mathbf{a} \in \mathbf{A}$).

Из (5.14) вытекает, что

$$y_{t+1} = e(a + bq_{t+1}^2 + cq_t + dx_{t+1}) \ (t \in \mathbb{Z}_+). \tag{5.15}$$

Подставив $t = 0, 1, \ldots, l$ ($l > 2$) в (5.15), и используя 2-е рекуррентное соотношение системы (5.14), получим следующую систему уравнений

$$\begin{cases} y_1 = ae + beq_1^2 + ceq_0 + dex_1 \\ y_2 = ae + be^{-1}y_1^2 + ceq_1 + dex_2 \\ y_i = ae + be^{-1}y_{i-1}^2 + cy_{i-2} + dex_i \ (i = 3, \ldots, l) \end{cases}. \tag{5.16}$$

Предположим вначале, что начальное состояние автомата $M_{\mathbf{a}}$ ($\mathbf{a} \in \mathbf{A}$) известно экспериментатору. Тогда возможны следующие два случая.

1. Пусть $\mathbf{q}_0 = (0, 0)$. Тогда система уравнений (5.16) принимает следующий вид

$$\begin{cases} u_1 + x_1u_4 = y_1 \\ u_1 + y_1^2u_2 + x_2u_4 = y_2 \\ u_1 + y_{i-1}^2u_2 + y_{i-2}u_3 + x_iu_4 = y_i \ (i = 3, \ldots, l) \end{cases}, \tag{5.17}$$

где u_i ($i = 1, \ldots, 4$) – такие неизвестные, что

$$(u_1, u_2, u_3, u_4) = (ae, be^{-1}, c, de). \tag{5.18}$$

Матрица линейной системы уравнений (5.17) имеет следующий вид

$$A = \begin{pmatrix} 1 & 0 & 0 & x_1 \\ 1 & y_1^2 & 0 & x_2 \\ 1 & y_2^2 & y_1 & x_3 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & y_{l-1}^2 & y_{l-2} & x_l \end{pmatrix}.$$

Если существует такое входное слово $x_1 \ldots x_l \in K^l$ заранее неизвестной длины $l \geq 4$, что матрица A содержит обратимую матрицу 4-го порядка, то может быть вычислено единственное решение (u_1, u_2, u_3, u_4) системы уравнений (5.17).

Из (5.18) вытекает, что тем самым будут вычислены величины ae, be^{-1}, c и de, т.е. только параметр c автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ будет вычислен точно.

При этом, из (5.17) вытекает, что

$$\begin{cases} y_1 = u_1 & + x_1 u_4 \\ y_2 = u_1 + y_1^2 u_2 & + x_2 u_4 \\ y_i = u_1 + y_{i-1}^2 u_2 + y_{i-2} u_3 + x_i u_4 \ (i = 3, \ldots, l) \end{cases}, \tag{5.19}$$

где значения u_j $(j = 1, \ldots, 4)$ определены равенством (5.18).

2. Пусть $\mathbf{q}_0 \neq (0, 0)$. Тогда система уравнений (5.16) принимает вид

$$\begin{cases} v_1 + q_1^2 v_2 & + q_0 v_4 & + x_1 v_6 = y_1 \\ v_1 & + y_1^2 v_3 \ + q_1 v_4 & + x_2 v_6 = y_2 \\ v_1 & + y_{i-1}^2 v_3 & + y_{i-2} v_5 + x_i v_6 = y_i \ (i = 3, \ldots, l) \end{cases}, \tag{5.20}$$

где v_i $(i = 1, \ldots, 6)$ – такие неизвестные, что

$$(v_1, v_2, v_3, v_4, v_5, v_6) = (ae, be, be^{-1}, ce, c, de). \tag{5.21}$$

Матрица системы уравнений (5.20) имеет вид

$$B = \begin{pmatrix} 1 & q_1^2 & 0 & q_0 & 0 & x_1 \\ 1 & 0 & y_1^2 & q_1 & 0 & x_2 \\ 1 & 0 & y_2^2 & 0 & y_1 & x_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & y_{l-1}^2 & 0 & y_{l-2} & x_l \end{pmatrix}.$$

Если существует такое входное слово $x_1 \ldots x_l \in K^l$ заранее неизвестной длины $l \geq 6$, что матрица B содержит обратимую матрицу 6-го порядка, то может быть вычислено единственное решение $(v_1, \ldots, v_6)$ системы уравнений (5.20).

Из (5.21) вытекает, что тем самым будут вычислены величины ae, be, be^{-1}, ce, c и de, т.е. только параметр c автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ будет вычислен точно.

При этом, из (5.20) вытекает, что

$$\begin{cases} y_1 = v_1 + q_1^2 v_2 & + q_0 v_4 & + x_1 v_6 \\ y_2 = v_1 & + y_1^2 v_3 \ + q_1 v_4 & + x_2 v_6 \\ y_i = v_1 & + y_{i-1}^2 v_3 & + y_{i-2} v_5 + x_i v_6 \ (i = 3, \ldots, l) \end{cases}, \tag{5.22}$$

где значения v_j $(j = 1, \ldots, 6)$ определены равенством (5.21).

Предположим теперь, что начальное состояние автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ не известно экспериментатору.

Сравнивая системы уравнений (5.17) и (5.20), мы видим, что при $\mathbf{q}_0 = (0, 0)$ и $\mathbf{q}_0 \neq (0, 0)$ ситуации различаются именно из-за первых 2-х уравнений этих систем (это различие характеризуется формулами (5.19) и (5.23)).

Поэтому отбросим первые два уравнения в системе уравнений (5.17) (или, что тоже самое, в системе уравнений (5.20). Получим систему уравнений

$$w_1 + y_{i-1}^2 w_2 + y_{i-2} w_3 + x_i w_4 = y_i \ (i = 3, \ldots, l), \tag{5.23}$$

где

$$(w_1, w_2, w_3, w_4) = (ae, be^{-1}, c, de). \tag{5.24}$$

Матрица системы уравнений (5.24) имеет вид

$$C = \begin{pmatrix} 1 & y_2^2 & y_1 & x_3 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & y_{l-1}^2 & y_{l-2} & x_l \end{pmatrix}.$$

Если существует такое входное слово $x_1 \dots x_l \in K^l$ заранее неизвестной длины $l \geq 6$, что матрица C содержит обратимую матрицу 4-го порядка, то может быть вычислено единственное решение (w_1, w_2, w_3, w_4) системы уравнений (5.23).

Из (5.24) вытекает, что тем самым будут вычислены величины ae, be^{-1}, c и de, т.е. только параметр c автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ будет вычислен точно.

При этом, из (5.23) вытекает, что

$$y_i = w_1 + y_{i-1}^2 w_2 + y_{i-2} w_3 + x_i w_4 \ (i = 3, \dots, l), \tag{5.25}$$

где значения w_j $(j = 1, \dots, 4)$ определены равенством (5.24).

В заключение отметим, что алгоритм, осуществляющий вычисления в соответствии с формулами (5.16), (5.19) и (5.25) является, по своей сути, алгоритмом, моделирующим любой автомат $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$. Именно это обстоятельство и стимулировало разработку общего подхода к построению имитационной модели заданного семейства автоматов, который рассмотрен в следующем пункте.

5.2. Имитационная модель семейства автоматов.

Решение задачи параметрической идентификации семейства обратимых автоматов, определенного рекуррентными соотношениями над кольцом $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$, характеризует сложность атаки криптоаналитика на секретный ключ средней длительности для соответствующего поточного шифра.

С позиции теории автоматов наиболее сильная формулировка задачи параметрической идентификации семейства автоматов, определенного рекуррентными соотношениями над кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$, имеет следующий вид.

Известно, что автомат M принадлежит семейству автоматов $\mathcal{M}_{\mathbf{A}}$, определенного заданными рекуррентными соотношениями над кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$. Требуется на основе эксперимента с автоматом M вычислить такой набор параметров $\mathbf{a} \in \mathbf{A}$, что $M = M_{\mathbf{a}}$.

При такой постановке задача параметрической идентификации автомата не всегда имеет решение, даже если экспериментатор может проводить с исследуемым автоматом эксперимент любой кратности, а также

управлять выбором начального состояния исследуемого автомата (что, в частности, проиллюстрировано примером 5.1).

Задача параметрической идентификации семейства автоматов, определенного рекуррентными соотношениями над кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$, характеризует сложность распознавания автомата, принадлежащего этому семейству автоматов. Однако в отличие от решения задачи параметрической идентификации для динамических систем над полем действительных или рациональных чисел [52], при решении этой задачи для семейства автоматов над кольцом отсутствует обычное понятие «точность идентификации, обусловленная выбором приближения или ошибками измерений». Это обусловлено тем, что кольцо $\mathcal{K} \in \mathfrak{K}^{fnt}$ является конечной алгебраической системой, а также тем, что кольцо – это настолько «жесткая» структура, что любая ошибка приводит к непредсказуемым последствиям (именно в этом и состоит одно из основных отличий конечных колец от поля характеристики нуль).

Из всего сказанного выше вытекает, что актуальной является задача разработки математического аппарата, предназначенного для построения для заданного семейства автоматов $\mathcal{M}_{\mathbf{A}}$ ($\mathbf{A} \in K^l, |\mathbf{A}| \geq 1$), определенного рекуррентными соотношениями над кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$, имитационной модели, т.е. алгоритма, который (после некоторого обучения) с некоторой заданной точностью имитирует поведение любого автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ на суффиксах входных слов, получаемых отбрасыванием префиксов фиксированной длины. Рассмотрим решение этой задачи.

5.2.1. Построение имитационной модели.

Пусть $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$ – фиксированное кольцо.
Зафиксируем числа $l, n_1, n_2, n_3 \in \mathbb{N}$ и множество $\mathbf{A} \subseteq K^l$ ($|\mathbf{A}| \geq 1$).
Система рекуррентных соотношений

$$\begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \end{cases} \quad (t \in \mathbb{Z}_+), \tag{5.26}$$

где $\mathbf{f}_1 : K^{n_1} \times K^{n_2} \times \mathbf{A} \to K^{n_1}$ и $\mathbf{f}_2 : K^{n_1} \times K^{n_2} \times \mathbf{A} \to K^{n_3}$, определяет над кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$ некоторое такое семейство конечных автоматов Мили $\mathcal{M}_{\mathbf{A}} = \{M_{\mathbf{a}}\}_{\mathbf{a} \in \mathbf{A}}$, что для каждого набора $\mathbf{a} \in \mathbf{A}$ значений параметров элементы $\mathbf{q}_t \in K^{n_1}$, $\mathbf{x}_t \in K^{n_2}$ и $\mathbf{y}_t \in K^{n_3}$ являются, соответственно, состоянием, входным символом и выходным символом автомата $M_{\mathbf{a}}$ в момент t.

Аналогичным образом, система рекуррентных соотношений

$$M_{\mathbf{a}} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_{t+1}, \mathbf{a}) \end{cases} \quad (t \in \mathbb{Z}_+), \tag{5.27}$$

где $\mathbf{f}_1 : K^{n_1} \times K^{n_2} \times \mathbf{A} \to K^{n_1}$ и $\mathbf{f}_2 : K^{n_1} \times \mathbf{A} \to K^{n_3}$, определяет над кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$ некоторое такое семейство конечных автоматов Мура $\mathcal{M}_{\mathbf{A}} = \{M_{\mathbf{a}}\}_{\mathbf{a}\in\mathbf{A}}$, что для каждого набора значения параметров $\mathbf{a} \in \mathbf{A}$ элементы $\mathbf{q}_t \in K^{n_1}$, $\mathbf{x}_t \in K^{n_2}$ и $\mathbf{y}_t \in K^{n_3}$ являются, соответственно, состоянием, входным символом и выходным символом автомата $M_{\mathbf{a}}$ в момент t.

Рассмотрим семейство автоматов $\mathcal{M}_{\mathbf{A}}$, определенное либо рекуррентными соотношениями (5.26), либо рекуррентными соотношениями (5.27).

Обозначим через $F_{\mathbf{a},\mathbf{q}_0}$ ($\mathbf{a} \in \mathbf{A}, \mathbf{q}_0 \in K^{n_1}$) отображение множества входных слов $(K^{n_2})^+$ в множество выходных слов $(K^{n_3})^+$, реализуемое инициальным автоматом $(M_{\mathbf{a}}, \mathbf{q}_0)$ (т.е. $F_{\mathbf{a},\mathbf{q}_0}$ – это ограниченно детерминированная функция, или, иными словами, автоматное отображение $f_{(M_{\mathbf{a}},\mathbf{q}_0)}$). Таким образом, каждому автомату $M_{\mathbf{a}}$ ($\mathbf{a} \in \mathbf{A}$) поставлено в соответствие семейство автоматных отображений $\mathcal{F}_{\mathbf{a}} = \{F_{\mathbf{a},\mathbf{q}_0}\}_{\mathbf{q}_0\in K^{n_1}}$.

Зафиксируем числа $r, l_1 \in \mathbb{N}$, непустое множество $\mathbf{B} \subseteq K^{l_1}$ ($|\mathbf{B}| \le |\mathbf{A}|$) и три семейства отображений

$$\{\varphi^{(1)}_{\mathbf{b}} : K^{n_1} \times K^{n_2} \to K^{n_3}\}_{\mathbf{b}\in\mathbf{B}},$$

$$\left\{\varphi^{(2)}_{\mathbf{b}} : K^{n_1} \times \left(\bigcup_{j=1}^{r-1} K^{n_3}\right)^j \times K^{n_2} \to K^{n_3}\right\}_{\mathbf{b}\in\mathbf{B}},$$

$$\{\varphi^{(3)}_{\mathbf{b}} : K^{n_1} \times (K^{n_3})^r \times K^{n_2} \to K^{n_3}\}_{\mathbf{b}\in\mathbf{B}}.$$

Рассмотрим семейство таких отображений

$$\mathcal{G}_{\mathbf{B}} = \{G_{\mathbf{b}} : K^{n_1} \times (K^{n_2})^+ \to (K^{n_3})^+\}_{\mathbf{b}\in\mathbf{B}},$$

что

$$G_{\mathbf{b}}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_m) = \mathbf{y}_1 \dots \mathbf{y}_m \ (\mathbf{b} \in \mathbf{B}, m \in \mathbb{N}), \tag{5.28}$$

где

$$\mathbf{y}_i = \begin{cases} \varphi^{(1)}_{\mathbf{b}}(\mathbf{q}_0, \mathbf{x}_1), \text{ если } i = 1 \\ \varphi^{(2)}_{\mathbf{b}}(\mathbf{q}_0, \mathbf{y}_1 \dots \mathbf{y}_{i-1}, \mathbf{x}_i), \text{ если } i = 2, \dots, r \\ \varphi^{(3)}_{\mathbf{b}}(\mathbf{q}_0, \mathbf{y}_{i-r} \dots \mathbf{y}_{i-1}, \mathbf{x}_i), \text{ если } r < i \le m \end{cases} \tag{5.29}$$

для любых $\mathbf{q}_0 \in K^{n_1}$ и $\mathbf{x}_1 \dots \mathbf{x}_m \in (K^{n_2})^+$.

Определим отображения

$$H_{\mathbf{b},\mathbf{q}_0} : (K^{n_2})^+ \to (K^{n_3})^+ \ (\mathbf{b} \in \mathbf{B}, \mathbf{q}_0 \in K^{n_1})$$

следующим образом:

$$H_{\mathbf{b},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_m) = G_{\mathbf{b}}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_m) \tag{5.30}$$

для всех входных слов $\mathbf{x}_1 \dots \mathbf{x}_m \in (K^{n_2})^+$ $(m \in \mathbb{N})$.

Из равенств (5.28)-(5.30) вытекает, что каждое отображение $H_{\mathbf{b},\mathbf{q}_0}$ $(\mathbf{b} \in \mathbf{B}, \mathbf{q}_0 \in K^{n_1})$ является автоматным отображением, причем каждое семейство автоматных отображений $\mathcal{H}_{\mathbf{b}} = \{H_{\mathbf{b},\mathbf{q}_0}\}_{\mathbf{q}_0 \in K^{n_1}}$ $(\mathbf{b} \in \mathbf{B})$ определяет конечный автомат над кольцом $\mathcal{K}$.

Зафиксировав сюръекцию $h : \mathbf{A} \to \mathbf{B}$ мы можем каждому автомату $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ поставить в соответствие автомат, заданный семейством автоматных отображений $\mathcal{H}_{h(\mathbf{a})}$.

Таким образом, упорядоченная пара $(\mathcal{G}_{\mathbf{B}}, h)$ может быть выбрана в качестве имитационной модели семейства автоматов $\mathcal{M}_{\mathbf{A}}$, если выполнены следующие три условия:

1) построение как семейства отображений $\mathcal{G}_{\mathbf{B}}$, так и сюръекции h осуществляется только на основе анализа системы рекуррентных соотношений, определяющих семейство автоматов $\mathcal{M}_{\mathbf{A}}$, без каких-либо дополнительных ограничений на значения параметра $\mathbf{a} \in \mathbf{A}$;

2) для каждого фиксированного значения параметра $\mathbf{a} \in \mathbf{A}$ сложность вычислений в соответствии с семейством отображений $\mathcal{F}_{\mathbf{a}}$ не меньше, чем сложность вычислений в соответствии с семейством отображений $\mathcal{H}_{h(\mathbf{a})}$;

3) для каждого фиксированного значения параметра $\mathbf{a} \in \mathbf{A}$ автомат, определяемый семейством автоматных отображений $\mathcal{H}_{h(\mathbf{a})}$, моделирует поведение автомата $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$ с заданной точностью.

Ясно, что те или иные дополнительные ограничения на структуру отображений $\varphi^{(1)}_{\mathbf{b}}$, $\varphi^{(2)}_{\mathbf{b}}$, $\varphi^{(3)}_{\mathbf{b}}$ $(\mathbf{b} \in \mathbf{B})$ накладывают соответствующие ограничения на каждое семейство автоматных отображений $\mathcal{H}_{\mathbf{b}}$ и, следовательно, на структуру автомата, определяемого этим семейством.

Естественно потребовать, чтобы для имитационной модели $(\mathcal{G}_{\mathbf{B}}, h)$ отображения $\varphi^{(1)}_{h(\mathbf{a})}$ и $\varphi^{(2)}_{h(\mathbf{a})}$ были выбраны так, чтобы истинными были равенства

$$H_{h(\mathbf{a}),\mathbf{q}_0}\big|_{\bigcup\limits_{i=1}^{r} K^{n_2}} = F_{\mathbf{a},\mathbf{q}_0}\big|_{\bigcup\limits_{i=1}^{r} K^{n_2}} \quad (\mathbf{a} \in \mathbf{A}, \mathbf{q}_0 \in K^{n_1}). \tag{5.31}$$

Содержательный смысл требования выполнения равенств (5.31) состоит в следующем.

Имитационная модель $(\mathcal{G}_{\mathbf{B}}, h)$, подсоединенная к входу и выходу исследуемого автомата $M_{\mathbf{a}}$ ($\mathbf{a} \in \mathbf{A}$) пропускает первые r выходных символов. При этом в процессе наблюдения первых r входных символов и соответствующих им выходных символов происходит обучение (или, иными словами, настройка) имитационной модели. После этого имитационная модель блокирует выход автомата $M_{\mathbf{a}}$ и начинает моделировать его поведение на оставшейся части входного слова.

Всюду в дальнейшем считаем, что условие (5.31) выполнено.

Среди ограничений на структуру отображений $\varphi_{\mathbf{b}}^{(3)}$ ($\mathbf{b} \in \mathbf{B}$) с прикладной точки зрения особый интерес представляет следующее ограничение: для каждого отображения $\varphi_{\mathbf{b}}^{(3)}$ ($\mathbf{b} \in \mathbf{B}$) переменная $\mathbf{q}_0$ является фиктивной. Это ограничение означает, что имитационная модель $(\mathcal{G}_{\mathbf{B}}, h)$ осуществляет моделирование поведения каждого автомата $M_{\mathbf{a}}$ ($\mathbf{a} \in \mathbf{A}$) посредством использования автоматов с конечной памятью.

5.2.2. Точность имитационной модели.

Определим точность имитационной модели $(\mathcal{G}_{\mathbf{B}}, h)$ семейства автоматов $\mathcal{M}_{\mathbf{A}}$, используя стандартный подход, принятый в прикладной теории алгоритмов [7,58].

Пусть

$$F_{\mathbf{a},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_m) = \mathbf{y}_1 \dots \mathbf{y}_m$$

и

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

где $\mathbf{q}_0 \in K^{n_1}$, $\mathbf{a} \in \mathbf{A}$ и $\mathbf{x}_1 \dots \mathbf{x}_m \in (K^{n_2})^m$ ($m \in \mathbb{N}$).

Число $m - \varrho(\mathbf{y}_1 \dots \mathbf{y}_m, \widetilde{\mathbf{y}}_1 \dots \widetilde{\mathbf{y}}_m)$ (где ϱ – расстояние по Хеммингу) является количеством букв в выходных словах $\mathbf{y}_1 \dots \mathbf{y}_m$ и $\widetilde{\mathbf{y}}_1 \dots \widetilde{\mathbf{y}}_m$, на которых отображения $F_{\mathbf{a},\mathbf{q}_0}$ и $H_{h(\mathbf{a}),\mathbf{q}_0}$ совпадают на входном слове $\mathbf{x}_1 \dots \mathbf{x}_m \in (K^{n_2})^m$.

Замечание 5.9. Пусть U ($U \neq \emptyset$) – произвольный конечный алфавит. Расстоянием по Хеммингу между словами $v = u_1^{(1)} \dots u_m^{(1)}$ и $w = u_1^{(2)} \dots u_m^{(2)}$, где $u_j^{(i)} \in U$ ($i = 1, 2$; $j = 1, \dots, m$) называется количество $\varrho(v, w)$ таких позиций i ($1 \leq i \leq m$), что $u_i^{(1)} \neq u_i^{(2)}$.

Следовательно, число

$$\alpha_{\mathbf{a},\mathbf{q}_0,m} = \frac{1}{|K^{n_2}|^m} \sum_{\mathbf{x}_1 \ldots \mathbf{x}_m \in (K^{n_2})^m} (m - \varrho(\mathbf{y}_1 \ldots \mathbf{y}_m, \widetilde{\mathbf{y}}_1 \ldots \widetilde{\mathbf{y}}_m)) \ (m \in \mathbb{N}), \quad (5.32)$$

является средним количеством букв в выходных словах, на которых отображения $F_{\mathbf{a},\mathbf{q}_0}$ и $H_{h(\mathbf{a}),\mathbf{q}_0}$ совпадают на множестве всех входных слов длины m.

Из (5.32) вытекает, что число

$$\beta_{\mathbf{a},\mathbf{q}_0,m} = m^{-1}\alpha_{\mathbf{a},\mathbf{q}_0,m} \ (m \in \mathbb{N}) \quad (5.33)$$

является средним количеством букв в выходных словах, приходящимся на одну букву входного слова, на которых отображения $F_{\mathbf{a},\mathbf{q}_0}$ и $H_{h(\mathbf{a}),\mathbf{q}_0}$ совпадают на множестве всех входных слов длины m.

Так как множества $K^{n_2}, (K^{n_2})^2, \ldots, (K^{n_2})^m$ $(m \in \mathbb{N})$ попарно не пересекаются, то

$$\left| \bigcup_{i=1}^{m} (K^{n_2})^i \right| = \frac{|K^{n_2}|^{m+1} - |K|^{n_2}}{|K^{n_2}| - 1} \ (m \in \mathbb{N}).$$

Следовательно, число

$$\gamma_{\mathbf{a},\mathbf{q}_0,m} = \frac{|K^{n_2}| - 1}{|K^{n_2}|^{m+1} - |K^{n_2}|} \sum_{i=1}^{m} |K^{n_2}|^i \beta_{\mathbf{a},\mathbf{q}_0,i} \ (m \in \mathbb{N}) \quad (5.34)$$

является средним количеством букв в выходных словах, приходящимся на одну букву входного слова, на которых отображения $F_{\mathbf{a},\mathbf{q}_0}$ и $H_{h(\mathbf{a}),\mathbf{q}_0}$ совпадают на множестве всех входных слов длины, не превосходящей число m.

Отсюда вытекает, что числа

$$\underline{\gamma}_{\mathbf{a},\mathbf{q}_0} = \underline{\lim}\gamma_{\mathbf{a},\mathbf{q}_0,m} = \lim_{m\to\infty} \inf\{\gamma_{\mathbf{a},\mathbf{q}_0,i} | i \in \mathbb{N}_m\} \ (\mathbf{a} \in \mathbf{A}, \mathbf{q}_0 \in K^{n_1}) \quad (5.35)$$

и

$$\overline{\gamma}_{\mathbf{a},\mathbf{q}_0} = \overline{\lim}\gamma_{\mathbf{a},\mathbf{q}_0,m} = \lim_{m\to\infty} \sup\{\gamma_{\mathbf{a},\mathbf{q}_0,i} | i \in \mathbb{N}_m\} \ (\mathbf{a} \in \mathbf{A}, \mathbf{q}_0 \in K^{n_1}) \quad (5.36)$$

являются, соответственно, нижней и верхней границей для среднего количества букв в выходных словах, приходящегося на одну букву входного слова, на которых отображения $F_{\mathbf{a},\mathbf{q}_0}$ и $H_{h(\mathbf{a}),\mathbf{q}_0}$ совпадают на всей своей области определения $(K^{n_2})^+$.

Следовательно, числа

$$\underline{\eta}_{\mathbf{a}} = \min_{\mathbf{q}_0 \in K^{n_1}} \underline{\gamma}_{\mathbf{a},\mathbf{q}_0} \ (\mathbf{a} \in \mathbf{A}) \tag{5.37}$$

и

$$\overline{\eta}_{\mathbf{a}} = \max_{\mathbf{q}_0 \in K^{n_1}} \overline{\gamma}_{\mathbf{a},\mathbf{q}_0} \ (\mathbf{a} \in \mathbf{A}) \tag{5.38}$$

являются, соответственно, нижней и верхней границей для среднего количества букв в выходных словах, приходящегося на одну букву входного слова, на которых отображения, принадлежащие семейству отображений $\mathcal{F}_{\mathbf{a}}$, реализуемых автоматом $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$, совпадают с соответствующими отображениями, принадлежащими семейству отображений $\mathcal{H}_{h(\mathbf{a})}$.

Таким образом, числа

$$\underline{\eta} = \min_{\mathbf{a} \in \mathbf{A}} \underline{\eta}_{\mathbf{a}} \tag{5.39}$$

и

$$\overline{\eta} = \max_{\mathbf{a} \in \mathbf{A}} \underline{\eta}_{\mathbf{a}} \tag{5.40}$$

определяют, соответственно, нижнюю и верхнюю границу для среднего количества букв в выходных словах, приходящегося на одну букву входного слова, на которых автоматные отображения, реализуемые семейством автоматов $\mathcal{M}_{\mathbf{A}}$, совпадают с автоматными отображениями, реализуемыми имитационной моделью $(\mathcal{G}_{\mathbf{B}}, h)$.

Из (5.34)-(5.40) вытекает, что упорядоченная пара $(\mathcal{G}_{\mathbf{B}}, h)$ может быть охарактеризована как $[\underline{\eta}, \overline{\eta}]$-точная имитационная модель семейства автоматов $\mathcal{M}_{\mathbf{A}}$.

Естественно определить $[\underline{\eta}, \overline{\eta}]$-точную имитационную модель $(\mathcal{G}_{\mathbf{B}}, h)$ как асимптотически точную имитационную модель семейства автоматов $\mathcal{M}_{\mathbf{A}}$, если $\underline{\eta} = \overline{\eta} = 1$.

Рассмотрим теперь случай, когда для всех $\mathbf{a} \in \mathbf{A}$ и $\mathbf{q}_0 \in K^{n_1}$ существует предел

$$\gamma_{\mathbf{a},\mathbf{q}_0} = \lim_{m \to \infty} \gamma_{\mathbf{a},\mathbf{q}_0,m}. \tag{5.41}$$

Число $\gamma_{\mathbf{a},\mathbf{q}_0}$ $(\mathbf{a} \in \mathbf{A}, \mathbf{q}_0 \in K^{n_1})$, определяемое равенством (5.41), равно среднему количеству букв в выходных словах, приходящихся на одну букву входного слова, на которых отображения $F_{\mathbf{a},\mathbf{q}_0}$ и $H_{h(\mathbf{a}),\mathbf{q}_0}$ совпадают на всей своей области определения $(K^{n_2})^+$.

Следовательно, число

$$\eta_{\mathbf{a}} = \min_{\mathbf{q}_0 \in K^{n_1}} \gamma_{\mathbf{a},\mathbf{q}_0} \ (\mathbf{a} \in \mathbf{A}) \tag{5.42}$$

определяет в наихудшем случае среднее количество букв в выходных словах, приходящееся на одну букву входного слова, на которых отображения, принадлежащие семейству отображений $\mathcal{F}_{\mathbf{a}}$, реализуемых автоматом $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$, совпадают с соответствующими отображениями, принадлежащими семейству отображений $\mathcal{H}_{h(\mathbf{a})}$, а число

$$\zeta_{\mathbf{a}} = |K^{n_1}|^{-1} \sum_{\mathbf{q}_0 \in K^{n_1}} \gamma_{\mathbf{a},\mathbf{q}_0} \ (\mathbf{a} \in \mathbf{A}) \tag{5.43}$$

определяет в среднем количество букв в выходных словах, приходящееся на одну букву входного слова, на которых отображения, принадлежащие семейству отображений $\mathcal{F}_{\mathbf{a}}$, реализуемых автоматом $M_{\mathbf{a}} \in \mathcal{M}_{\mathbf{A}}$, совпадают с соответствующими отображениями, принадлежащими семейству отображений $\mathcal{H}_{h(\mathbf{a})}$.

Из (5.42) и (5.43) вытекает, что:

а) число

$$\nu_1 = \min_{\mathbf{a} \in \mathbf{A}} \eta_{\mathbf{a}} \tag{5.44}$$

представляет собой в наихудшем случае среднее количество букв в выходных словах, приходящееся на одну букву входного слова, на которых автоматные отображения, реализуемые семейством автоматов $\mathcal{M}_{\mathbf{A}}$, совпадают с автоматными отображениями, реализуемыми имитационной моделью $(\mathcal{G}_{\mathbf{B}}, h)$;

б) число

$$\nu_2 = |\mathbf{A}|^{-1} \sum_{\mathbf{a} \in \mathbf{A}} \eta_{\mathbf{a}} \tag{5.45}$$

представляет собой среднее для наихудших случаев от средних количеств букв в выходных словах, приходящихся на одну букву входного слова, на которых автоматные отображения, реализуемые семейством автоматов $\mathcal{M}_{\mathbf{A}}$, совпадают с автоматными отображениями, реализуемыми имитационной моделью $(\mathcal{G}_{\mathbf{B}}, h)$;

в) число

$$\nu_3 = \min_{\mathbf{a} \in \mathbf{A}} \zeta_{\mathbf{a}} \tag{5.46}$$

представляет собой наихудший случай для средних от средних количеств букв в выходных словах, приходящееся на одну букву входного слова, на которых автоматные отображения, реализуемые семейством автоматов $\mathcal{M}_{\mathbf{A}}$, совпадают с автоматными отображениями, реализуемыми имитационной моделью $(\mathcal{G}_{\mathbf{B}}, h)$;

г) число

$$\nu_4 = |\mathbf{A}|^{-1} \sum_{\mathbf{a} \in \mathbf{A}} \zeta_{\mathbf{a}} \tag{5.47}$$

представляет собой среднее от средних количеств букв в выходных словах, приходящееся на одну букву входного слова, на которых автоматные отображения, реализуемые семейством автоматов $\mathcal{M}_{\mathbf{A}}$, совпадают с автоматными отображениями, реализуемыми имитационной моделью $(\mathcal{G}_{\mathbf{B}}, h)$.

Эти четыре случая охватывают все представляющие интерес комбинации понятий «в наихудшем случае» и «в среднем», и дают возможность охарактеризовать имитационную модель $(\mathcal{G}_{\mathbf{B}}, h)$ семейства автоматов $\mathcal{M}_{\mathbf{A}}$ как ν-точную, где ν – любое из чисел ν_1, ν_2, ν_3 или ν_4.

Естественно определить ν-точную ($\nu \in \{\nu_1, \nu_2, \nu_3, \nu_4\}$) имитационную модель $(\mathcal{G}_{\mathbf{B}}, h)$ как асимптотически точную имитационную модель семейства автоматов $\mathcal{M}_{\mathbf{A}}$, если $\nu = 1$.

Следующая теорема выделяет над кольцом $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$ важный нетривиальный класс имитационных моделей $(\mathcal{G}_{\mathbf{B}}, h)$ семейств автоматов $\mathcal{M}_{\mathbf{A}}$ ($\emptyset \neq \mathbf{A} \subseteq K^l$).

Теорема 5.1. Пусть $(\mathcal{G}_{\mathbf{B}}, h)$ – такая имитационная модель семейства автоматов $\mathcal{M}_{\mathbf{A}}$ ($\emptyset \neq \mathbf{A} \subseteq K^l$) над кольцом $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$, что существует предел $\gamma_{\mathbf{a},\mathbf{q}_0} = \lim\limits_{m \to \infty} \gamma_{\mathbf{a},\mathbf{q}_0,m}$.

Пусть существует такое число $r_0 \in \mathbb{N}$ ($r_0 \geq r$), что при всех $\mathbf{q}_0 \in K^{n_1}$, $\mathbf{a} \in \mathbf{A}$ и $\mathbf{x}_1 \ldots \mathbf{x}_m \in (K^{n_2})^m$ ($m > r_0$) для выходных слов

$$F_{\mathbf{a},\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_m) = \mathbf{y}_1 \ldots \mathbf{y}_m$$

и

$$H_{h(\mathbf{a}),\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_m) = \widetilde{\mathbf{y}}_1 \ldots \widetilde{\mathbf{y}}_m$$

равенства $\mathbf{y}_i = \widetilde{\mathbf{y}}_i$ имеют место для всех $i = r_0 + 1, \ldots, m$. Тогда

$$\nu_1 = \nu_2 = \nu_3 = \nu_4 = 1, \tag{5.48}$$

т.е. $(\mathcal{G}_{\mathbf{B}}, h)$ – асимптотически точная имитационная модель семейства автоматов $\mathcal{M}_{\mathbf{A}}$ для всех $\nu \in \{\nu_1, \nu_2, \nu_3, \nu_4\}$.□

Доказательство. Предположим, что имитационная модель $(\mathcal{G}_{\mathbf{B}}, h)$ семейства автоматов $\mathcal{M}_{\mathbf{A}}$ ($\emptyset \neq \mathbf{A} \subseteq K^l$) над кольцом $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$ удовлетворяет условиям теоремы.

Из (5.32) вытекает, что для всех $\mathbf{q}_0 \in K^{n_1}$, $\mathbf{a} \in \mathbf{A}$ и $m \geq r_0$

$$\alpha_{\mathbf{a},\mathbf{q}_0,m} = \frac{1}{|K^{n_2}|^m} \sum_{\mathbf{x}_1 \dots \mathbf{x}_m \in (K^{n_2})^m} (m - \varrho(\mathbf{y}_1 \dots \mathbf{y}_m, \widetilde{\mathbf{y}}_1 \dots \widetilde{\mathbf{y}}_m)) \geq$$

$$\geq \frac{1}{|K^{n_2}|^m} \sum_{\mathbf{x}_1 \dots \mathbf{x}_m \in (K^{n_2})^m} (m - (r_0 - r)) =$$

$$= \frac{m - (r_0 - r)}{|K^{n_2}|^m} \sum_{\mathbf{x}_1 \dots \mathbf{x}_m \in (K^{n_2})^m} 1 =$$

$$= \frac{m - (r_0 - r)}{|K^{n_2}|^m} |K^{n_2}|^m = m - (r_0 - r). \tag{5.49}$$

Из (5.33) и (5.49) вытекает, что для всех $\mathbf{q}_0 \in K^{n_1}$, $\mathbf{a} \in \mathbf{A}$ и $m \geq r_0$

$$\beta_{\mathbf{a},\mathbf{q}_0,m} = m^{-1} \alpha_{\mathbf{a},\mathbf{q}_0,m} \geq m^{-1}(m - (r_0 - r)) = 1 - m^{-1}(r_0 - r). \tag{5.50}$$

Из (5.34) и (5.50) вытекает, что для всех $\mathbf{q}_0 \in K^{n_1}$, $\mathbf{a} \in \mathbf{A}$ и $m \geq r_0$

$$\gamma_{\mathbf{a},\mathbf{q}_0,m} = \frac{|K^{n_2}| - 1}{|K^{n_2}|^{m+1} - |K^{n_2}|} \sum_{i=1}^{m} |K^{n_2}|^i \beta_{\mathbf{a},\mathbf{q}_0,i} \geq$$

$$\geq \frac{|K^{n_2}| - 1}{|K^{n_2}|^{m+1} - |K^{n_2}|} \sum_{i=1}^{m} |K^{n_2}|^i (1 - m^{-1}(r_0 - r)) =$$

$$= (1 - m^{-1}(r_0 - r)) \frac{|K^{n_2}| - 1}{|K^{n_2}|^{m+1} - |K^{n_2}|} \sum_{i=1}^{m} |K^{n_2}|^i =$$

$$= (1 - m^{-1}(r_0 - r)) \frac{|K^{n_2}| - 1}{|K^{n_2}|^{m+1} - |K^{n_2}|} \frac{|K^{n_2}|^{m+1} - |K^{n_2}|}{|K^{n_2}| - 1} =$$

$$= (1 - m^{-1}(r_0 - r)). \tag{5.51}$$

Из (5.41) и (5.51) вытекает, что для всех $\mathbf{q}_0 \in K^{n_1}$ и $\mathbf{a} \in \mathbf{A}$

$$\gamma_{\mathbf{a},\mathbf{q}_0} = \lim_{m \to \infty} \gamma_{\mathbf{a},\mathbf{q}_0,m} = \lim_{m \to \infty} (1 - m^{-1}(r_0 - r)) = 1. \tag{5.52}$$

Из (5.42), (5.43) и (5.52) вытекает, что для всех $\mathbf{a} \in \mathbf{A}$

$$\eta_{\mathbf{a}} = \min_{\mathbf{q}_0 \in K^{n_1}} \gamma_{\mathbf{a},\mathbf{q}_0} = \min_{\mathbf{q}_0 \in K^{n_1}} 1 = 1 \tag{5.53}$$

и

$$\zeta_{\mathbf{a}} = |K^{n_1}|^{-1} \sum_{\mathbf{q}_0 \in K^{n_1}} \gamma_{\mathbf{a},\mathbf{q}_0} = |K^{n_1}|^{-1} \sum_{\mathbf{q}_0 \in K^{n_1}} 1 = |K^{n_1}|^{-1} |K^{n_1}| = 1. \quad (5.54)$$

Следовательно, из (5.53), (5.54) и (5.44)-(5.47) вытекает, что

$$\nu_1 = \min_{\mathbf{a} \in \mathbf{A}} \eta_{\mathbf{a}} = \min_{\mathbf{a} \in \mathbf{A}} 1 = 1,$$

$$\nu_2 = |\mathbf{A}|^{-1} \sum_{\mathbf{a} \in \mathbf{A}} \eta_{\mathbf{a}} = |\mathbf{A}|^{-1} \sum_{\mathbf{a} \in \mathbf{A}} 1 = |\mathbf{A}|^{-1} |\mathbf{A}| = 1,$$

$$\nu_3 = \min_{\mathbf{a} \in \mathbf{A}} \zeta_{\mathbf{a}} = \min_{\mathbf{a} \in \mathbf{A}} 1 = 1$$

и

$$\nu_4 = |\mathbf{A}|^{-1} \sum_{\mathbf{a} \in \mathbf{A}} \zeta_{\mathbf{a}} = |\mathbf{A}|^{-1} \sum_{\mathbf{a} \in \mathbf{A}} 1 = |\mathbf{A}|^{-1} |\mathbf{A}| = 1,$$

т.е. равенства (5.48) истинны.□

5.3. Семейства хэш-функций.

Известно, что задача компактного представления информации имеет многочисленные приложения как в процессе разработки программных систем, так и в процессе разработки средств защиты информации (в частности, криптографии).

Для обеспечения компактного представления информации определяющую роль играет процесс хеширования, суть которого состоит в преобразовании входного массива данных в выходную строку фиксированной длины. Такие преобразования называются хэш-функциями.

С математической точки зрения хэш-функция представляет собой отображение

$$H : X^+ \to Y,$$

где X и Y – такие непустые конечные множества, что $|X| \geq |Y|$.

Выше было отмечено, что хэш-функции применяются при решении задач, связанных с защитой информации (см., напр., [4,30,109,113]). Формально требования, которым должна удовлетворять такая хэш-функция $H : X^+ \to Y$, могут быть сформулированы следующим образом:

1) сложность вычисления значений функции H является полиномом от длины входа (т.е. H – легко вычислимая функция);

2) для каждого фиксированного элемента $y \in Y$ поиск такого слова $u \in X^+$, что $H(u) = y$ является трудной задачей (отсюда, в частности, вытекает, что для каждого фиксированного слова $u \in X^+$ поиск такого слова $u' \in X^+$, что $H(u) = H(u')$ является трудной задачей);

3) поиск двух таких случайных слов $u, u' \in X^+$, что $H(u) = H(u')$ имеет, по крайней мере, субэкспоненциальную сложность.

Первые два требования означают, что H является однонаправленной функцией, а третье требования называются устойчивостью к коллизиям.

В настоящее время не известно ни одной функции, для которой доказано, что она удовлетворяет требованиям 1 и 2. Поэтому при решении прикладных задач под однонаправленной хэш-функцией понимают такую легко вычислимую функцию $H : X^+ \to Y$, что для каждого фиксированного элемента $y \in Y$ любой известный алгоритм решения уравнения $H(u) = y$ имеет субэкспоненциальную сложность.

Исходя из этого, под криптостойкой хэш-функцией понимают однонаправленную функцию $H : X^+ \to Y$ (в указанном выше прикладном значении этого понятия), для которой любой известный алгоритм нахождения коллизий имеет, по крайней мере, субэкспоненциальную сложность.

Замечание 5.10. В настоящее время в криптографии принято считать (см., напр., [113]), что хэш-функция $H : (\mathbb{E}^m)^+ \to \mathbb{E}^k$ (где $\mathbb{E} = \{0, 1\}$, а $k, m \in \mathbb{N}$ $(k \leq m)$ – фиксированные числа) является криптостойкой, если для каждого фиксированного элемента $\mathbf{y} \in \mathbb{E}^k$ асимптотическая сложность любого известного алгоритма поиска такого слова $\mathbf{u} \in (\mathbb{E}^m)^n$, что $H(\mathbf{u}) = \mathbf{y}$, а также асимптотическая сложность любого известного алгоритма поиска двух таких случайных слов $\mathbf{u}, \mathbf{u}' \in (\mathbb{E}^m)^n$, что $H(\mathbf{u}) = H(\mathbf{u}')$ равна $O(2^{0.5n})$ $(n \to \infty)$.

Любая хэш-функция представляет, по своей сути, автомат без выхода. Поэтому естественно возникает задача исследования семейства хэш-функций, определяемого автоматом без выходов, заданным системой рекуррентных соотношений над кольцом $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$.

Актуальность этой задачи с теоретической точки зрения обусловлена тем, что исследуется достаточно общий класс математических моделей, предназначенных для унифицированного представления семейств хэш-функций, а с прикладной точки зрения – тем, что анализ криптостойкости указанного семейства хэш-функций дает возможность обосновать целесообразность их применения при решении задач защиты информации (в частности, задач криптографии).

Рассмотрим решение этой задачи.

5.3.1. Исследуемая модель.

Зафиксируем числа $k, m \in \mathbb{N}$ $(k \leq m)$. Обозначим через $\mathcal{F}_{k,m}$ множество всех отображений $\mathbf{f} : K^k \times K^m \to K^k$, удовлетворяющих следующим двум условиям:

1) для любых $\mathbf{q}, \mathbf{q}' \in K^k$ истинно равенство

$$|\{\mathbf{x} \in K^m | \mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{q}'\}| = K^{m-k}; \tag{5.55}$$

2) для любых $\mathbf{q}, \mathbf{q}', \mathbf{q}'' \in K^k$ $(\mathbf{q} \neq \mathbf{q}')$ истинно равенство

$$\{\mathbf{x} \in K^m | \mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{q}''\} \cap \{\mathbf{x} \in K^m | \mathbf{f}(\mathbf{q}', \mathbf{x}) = \mathbf{q}''\} = \emptyset. \tag{5.56}$$

Из (5.55) вытекает, что множество отображений $\mathcal{F}_{k,m}$ определяет над кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$ такое семейство

$$\mathcal{M}_{\mathcal{F}_{k,m}} = \{M_{\mathbf{f}}\}_{\mathbf{f} \in \mathcal{F}_{k,m}}$$

сильно связных автоматов без выхода, что

$$M_{\mathbf{f}} : \mathbf{q}_{t+1} = \mathbf{f}(\mathbf{q}_t, \mathbf{x}_{t+1}) \ (\mathbf{f} \in \mathcal{F}_{k,m}, t \in \mathbb{Z}_+), \tag{5.57}$$

имеющих множество состояний $\mathbf{Q} = K^k$ и входной алфавит $\mathbf{X} = K^m$, т.е. $\mathbf{q}_t \in K^k$ и $\mathbf{x}_t \in K^m$ являются, соответственно, состоянием автомата $M_{\mathbf{f}}$ и входным символом в момент $t \in \mathbb{Z}_+$.

Замечание 5.11. В терминах теории графов [132] каждый автомат $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ $(\mathbf{f} \in \mathcal{F}_{k,m})$ характеризуется следующим образом.

Рассмотрим автоматный граф $G_{\mathbf{f}}$ автомата $M_{\mathbf{f}}$. Удалим отметки всех дуг. Для каждой пары состояний $\mathbf{q}, \widetilde{\mathbf{q}} \in K^k$ отождествим (иными словами, склеим) все дуги, идущие из вершины с отметкой $\mathbf{q}$ в вершину с отметкой $\widetilde{\mathbf{q}}$. Получим полный направленный граф G с петлями, имеющий $|K^k|$ вершин.

Следующий пример показывает, что множество отображений $\mathcal{F}_{k,m}$ $(k, m \in \mathbb{N}; k \leq m)$ определяет нетривиальное множество сильно связных автоматов без выхода над любым таким кольцом $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$, что $|K| \geq 2$.

Пример 5.2. Обозначим через $\mathcal{F}^{(0)}_{k,m}$ $(k, m \in \mathbb{N}; k \leq m)$ множество всех отображений $\mathbf{f} : K^k \times K^m \to K^k$, имеющих вид

$$\mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{g}(\mathbf{q}) + \mathbf{h}(\mathbf{x}), \tag{5.58}$$

где $\mathbf{h} : K^m \to K^k$ – такая сюръекция, что $|\mathbf{h}^{-1}(\mathbf{q})| = |K|^{m-k}$ для всех $\mathbf{q} \in K^k$, а $\mathbf{g} : K^k \to K^k$ – биекция.

Так как для каждого отображения $\mathbf{f} \in \mathcal{F}_{k,m}^{(0)}$ истинны равенства (5.55) и (5.56), то истинно включение $\mathcal{F}_{k,m}^{(0)} \subseteq \mathcal{F}_{k,m}$.

Следовательно, из (5.58) вытекает, что отображения, принадлежащие множеству $\mathcal{F}_{k,m}^{(0)}$, определяют над кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$ такое подсемейство

$$\mathcal{M}_{\mathcal{F}_{k,m}^{(0)}} = \{M_{\mathbf{f}}\}_{\mathbf{f} \in \mathcal{F}_{k,m}^{(0)}}$$

семейства сильно связных автоматов без выхода $\mathcal{M}_{\mathcal{F}_{k,m}}$, что

$$M_{\mathbf{f}} : \mathbf{q}_{t+1} = \mathbf{g}(\mathbf{q}_t) + \mathbf{h}(\mathbf{x}_{t+1}) \ (t \in \mathbb{Z}_+). \tag{5.59}$$

Если $\mathcal{K} \in \mathfrak{K}_1^{fnt}$ и $k = m$, то рекуррентное соотношение (5.59) определяет функцию переходов некоторого нетривиального семейства автоматов, являющегося подсемейством семейства автоматов над кольцом $\mathcal{K} \in \mathfrak{K}_1^{fnt}$, исследованного в [66,80].

В частности, если $\mathcal{K} \in \mathfrak{K}_1^{fnt}$ и $k = m$, то рекуррентному соотношению (5.59) удовлетворяет также функция переходов некоторого нетривиального подсемейства семейства линейных автоматов над кольцом $\mathcal{K} \in \mathfrak{K}_1^{fnt}$, исследованного в [64,65].

Кроме того, при $\mathcal{K} \in \mathfrak{K}_1^{fnt}$ и $k = m$ рекуррентному соотношению (5.59) удовлетворяет каждое семейство таких нелинейных автоматов без выхода

$$M_{\mathbf{f}} : \mathbf{q}_{t+1} = \mathbf{g}(\mathbf{q}_t) + A\mathbf{x}_{t+1} \ (t \in \mathbb{Z}_+). \tag{5.60}$$

что $\mathbf{g} : K^m \to K^m$ – биекция, а $A \in \mathsf{M}_m^{inv}$.

Как это обычно принято в теории автоматов, расширим отображение $\mathbf{f} \in \mathcal{F}_{k,m}$ на множество $K^k \times (K^m)^+$ равенством

$$\mathbf{f}(\mathbf{q}, \mathbf{x}_1 \dots \mathbf{x}_{t+1}) = \mathbf{f}(\mathbf{f}(\dots \mathbf{f}(\mathbf{f}(\mathbf{q}, \mathbf{x}_1), \mathbf{x}_2), \dots, \mathbf{x}_t), \mathbf{x}_{t+1}). \tag{5.61}$$

Всюду в дальнейшем считаем, что каждое отображение $\mathbf{f} \in \mathcal{F}_{k,m}$ определено на множестве $K^k \times (K^m)^+$.

Каждый инициальный автомат $(M_{\mathbf{f}}, \mathbf{q}_0)$ $(\mathbf{f} \in \mathcal{F}_{k,m}, \mathbf{q}_0 \in K^k)$ определяет отображение $H_{\mathbf{f},\mathbf{q}_0} : (K^m)^+ \to K^k$ свободной входной полугруппы $(K^m)^+$ во множество K^k состояний автомата $M_{\mathbf{f}}$, значения которого на входном слове $\mathbf{x}_1 \dots \mathbf{x}_t \in (K^m)^t$ $(t \in \mathbb{N})$ вычисляются в соответствии с формулой

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_t) = \mathbf{f}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_t). \tag{5.62}$$

Отметим, что из (5.61) и (5.62) вытекает, что для каждого отображения $\mathbf{f} \in \mathcal{F}_{k,m}$ и каждого начального состояния $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ равенство

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_t \mathbf{x}_{t+1}) = H_{\mathbf{f},H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_t)}(\mathbf{x}_{t+1}) \tag{5.63}$$

истинно для всех входных слов $\mathbf{x}_1 \dots \mathbf{x}_t \mathbf{x}_{t+1} \in (K^m)^{t+1}$ $(t \in \mathbb{N})$.

Таким образом, каждый автомат $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ ($\mathbf{f} \in \mathcal{F}_{k,m}$) определяет семейство хэш-функций

$$\mathcal{H}_{\mathbf{f}} = \{H_{\mathbf{f},\mathbf{q}_0}\}_{\mathbf{q}_0 \in K^k},$$

каждая из которых отображает множество всех входных слов $(K^m)^+$ во множество K^k состояний автомата $M_{\mathbf{f}}$.

5.3.2. Анализ исследуемой модели.

Основные свойства семейства хэш-функций $\mathcal{H}_{\mathbf{f}}$ ($\mathbf{f} \in \mathcal{F}_{k,m}$) характеризуются следующим образом.

Теорема 5.2. Для каждого отображения $\mathbf{f} \in \mathcal{F}_{k,m}$ при любых таких состояниях $\mathbf{q}_0, \mathbf{q}'_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$, что $\mathbf{q}_0 \neq \mathbf{q}'_0$ неравенство

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) \neq H_{\mathbf{f},\mathbf{q}'_0}(\mathbf{u}) \tag{5.64}$$

истинно для каждого входного слова $\mathbf{u} \in (K^m)^+$.□

Доказательство. Зафиксируем отображение $\mathbf{f} \in \mathcal{F}_{k,m}$. Докажем теорему индукцией по длине t входного слова.

Пусть $t = 1$.

Из (5.56) вытекает, что

$$\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) \neq \mathbf{f}(\mathbf{q}'_0, \mathbf{x}_1) \tag{5.65}$$

для любых состояний $\mathbf{q}_0, \mathbf{q}'_0 \in K^k$ ($\mathbf{q}_0 \neq \mathbf{q}'_0$) автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ и любого входного символа $\mathbf{x}_1 \in K^m$.

В силу равенства (5.62)

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1) = \mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) \tag{5.66}$$

и

$$H_{\mathbf{f},\mathbf{q}'_0}(\mathbf{x}_1) = \mathbf{f}(\mathbf{q}'_0, \mathbf{x}_1). \tag{5.67}$$

Из (5.65)-(5.67) вытекает, что

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1) \neq H_{\mathbf{f},\mathbf{q}'_0}(\mathbf{x}_1)$$

для любых состояний $\mathbf{q}_0, \mathbf{q}'_0 \in K^k$ ($\mathbf{q}_0 \neq \mathbf{q}'_0$) автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ и любого входного символа $\mathbf{x}_1 \in K^m$, что и требовалось доказать.

Предположим, что теорема истинна для всех $t \leq n$.

Докажем теорему для $t = n + 1$.

В силу равенства (5.63) мы получаем, что

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_n\mathbf{x}_{n+1}) = H_{\mathbf{f},H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_n)}(\mathbf{x}_{n+1}) \tag{5.68}$$

и

$$H_{\mathbf{f},\mathbf{q}'_0}(\mathbf{x}_1 \dots \mathbf{x}_n\mathbf{x}_{n+1}) = H_{\mathbf{f},H_{\mathbf{f},\mathbf{q}'_0}(\mathbf{x}_1 \dots \mathbf{x}_n)}(\mathbf{x}_{n+1}). \tag{5.69}$$

для любых состояний $\mathbf{q}_0, \mathbf{q}'_0 \in K^k$ $(\mathbf{q}_0 \neq \mathbf{q}'_0)$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ и любого входного слова $\mathbf{x}_1 \dots \mathbf{x}_n \in (K^m)^n$.

Из предположения индукции вытекает, что

$$\mathbf{q}_n = H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_n) \neq H_{\mathbf{f},\mathbf{q}'_0}(\mathbf{x}_1 \dots \mathbf{x}_n) = \mathbf{q}_n \tag{5.70}$$

для любых состояний $\mathbf{q}_0, \mathbf{q}'_0 \in K^k$ $(\mathbf{q}_0 \neq \mathbf{q}'_0)$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ и любого входного слова $\mathbf{x}_1 \dots \mathbf{x}_n \in (K^m)^n$.

А так как теорема истинна при $t = 1$, то из (5.63) и (5.68)-(5.70) вытекает, что

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_n\mathbf{x}_{n+1}) = H_{\mathbf{f},H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_n)}(\mathbf{x}_{n+1}) \neq$$

$$\neq H_{\mathbf{f},H_{\mathbf{f},\mathbf{q}'_0}(\mathbf{x}_1 \dots \mathbf{x}_n)}(\mathbf{x}_{n+1}) = H_{\mathbf{f},\mathbf{q}'_0}(\mathbf{x}_1 \dots \mathbf{x}_n\mathbf{x}_{n+1}),$$

что и требовалось доказать.□

В силу теоремы 5.2 элементы каждого семейства хэш-функций $\mathcal{H}_{\mathbf{f}}$ $(\mathbf{f} \in \mathcal{F}_{k,m})$ являются такими отображениями множества всех входных слов $(K^m)^+$ во множество K^k состояний автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$, что их значения попарно различны на каждом входном слове $\mathbf{u} \in (K^m)^+$.

Таким образом, из теоремы 5.2 непосредственно вытекает, что истинно следующее следствие.

Следствие 5.1. Для каждого отображения $\mathbf{f} \in \mathcal{F}_{k,m}$ если $\mathbf{q}_0 \neq \mathbf{q}'_0$ $(\mathbf{q}_0, \mathbf{q}'_0 \in K^k)$, то

$$H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}) \cap H^{-1}_{\mathbf{f},\mathbf{q}'_0}(\mathbf{q}) = \emptyset$$

для любого состояния $\mathbf{q} \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$.□

Теорема 5.3. Для каждого отображения $\mathbf{f} \in \mathcal{F}_{k,m}$ и каждого начального состояния $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ равенства

$$|H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_t) \cap (K^m)^t| = |K|^{tm-k} \ (\mathbf{q}_t \in K^k) \tag{5.71}$$

истинны для всех чисел $t \in \mathbb{N}$.□

Доказательство. Зафиксируем отображение $\mathbf{f} \in \mathcal{F}_{k,m}$. Докажем теорему индукцией по длине t входного слова.

Пусть $t = 1$.

Из определения отображения $H_{\mathbf{f},\mathbf{q}_0}$ ($\mathbf{f} \in \mathcal{F}_{k,m}, \mathbf{q}_0 \in K^k$) вытекает, что для любого состояния $\mathbf{q}_1 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ истинно равенство

$$H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_1) \cap K^m = \{\mathbf{x}_1 \in K^m | \mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) = \mathbf{q}_1\}. \tag{5.72}$$

Следовательно, в силу равенства (5.55) для любого состояния $\mathbf{q}_1 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ истинно равенство

$$|\{\mathbf{x}_1 \in K^m | \mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) = \mathbf{q}_1\}| = |K|^{m-k}. \tag{5.73}$$

Из (5.72) и (5.73) вытекает, что если $t = 1$, то равенство (5.71) истинно для любого состояния $\mathbf{q}_1 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$, что и требовалось доказать.

Предположим, что теорема истинна для всех $t \leq n$.

Докажем теорему для $t = n + 1$.

Воспользуемся определением отображения $H_{\mathbf{f},\mathbf{q}_0}$ ($\mathbf{f} \in \mathcal{F}_{k,m}, \mathbf{q}_0 \in K^k$), а также равенствами (5.62) и (5.63). Получим, что для любого состояния $\mathbf{q}_{n+1} \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$

$$H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_{n+1}) \cap (K^m)^{n+1} =$$

$$= \{\mathbf{x}_1 \dots \mathbf{x}_{n+1} \in (K^m)^{n+1} | \mathbf{f}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_{n+1}) = \mathbf{q}_{n+1}\} =$$

$$= \bigcup_{\mathbf{q}_n \in K^k} \{\mathbf{x}_1 \dots \mathbf{x}_{n+1} \in (K^m)^{n+1} | H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_n) = \mathbf{q}_n \&$$

$$\& H_{\mathbf{f},\mathbf{q}_n}(\mathbf{x}_{n+1}) = \mathbf{q}_{n+1}\} =$$

$$= \bigcup_{\mathbf{q}_n \in K^k} (H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_n) \cap (K^m)^n) \times (H^{-1}_{\mathbf{f},\mathbf{q}_n}(\mathbf{q}_{n+1}) \cap K^m). \tag{5.74}$$

В силу равенства (5.56) для любого состояния $\mathbf{q}_{n+1} \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ множества $H^{-1}_{\mathbf{f},\mathbf{q}_n}(\mathbf{q}_{n+1}) \cap K^m$ ($\mathbf{q}_n \in K^k$) попарно не пересекаются. Поэтому, из (5.74) вытекает, что

$$|H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_{n+1}) \cap (K^m)^{n+1}| =$$

$$= \sum_{\mathbf{q}_n \in K^k} |H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_n) \cap (K^m)^n| \cdot |H^{-1}_{\mathbf{f},\mathbf{q}_n}(\mathbf{q}_{n+1}) \cap K^m|. \tag{5.75}$$

Из предположения индукции вытекает, что для любых состояний $\mathbf{q}_0, \mathbf{q}_n \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ истинно равенство

$$|H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_n) \cap (K^m)^n| = |K|^{nm-k}. \tag{5.76}$$

Кроме того, было показано, что истинна при $t = 1$, т.е. для любых состояний $\mathbf{q}_n, \mathbf{q}_{n+1} \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ истинно равенство

$$|H^{-1}_{\mathbf{f},\mathbf{q}_n}(\mathbf{q}_{n+1}) \cap K^m| = |K|^{m-k}. \tag{5.77}$$

Из (5.75)-(5.77) вытекает, что

$$|H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_{n+1}) \cap (K^m)^{n+1}| = \sum_{\mathbf{q}_n \in K^k} |K|^{nm-k} \cdot |K|^{m-k} =$$

$$= |K|^{(n+1)m-2k} \sum_{\mathbf{q}_n \in K^k} 1 = |K|^{(n+1)m-2k} \cdot |K|^k = |K|^{(n+1)m-k},$$

что и требовалось доказать.□

Для исследования вычислительной стойкости семейства хэш-функций $\mathcal{H}_{\mathbf{f}} = \{H_{\mathbf{f},\mathbf{q}_0}\}_{\mathbf{q}_0 \in K^k}$ $(\mathbf{f} \in \mathcal{F}_{k,m})$ нам понадобятся следующие обозначения:

1) $\mathtt{P}^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q})$ $(\mathbf{f} \in \mathcal{F}_{k,m}; \mathbf{q}_0, \mathbf{q} \in K^k; t \in \mathbb{N})$ – вероятность того, что случайно выбранное из множества $(K^m)^t$ входное слово $\mathbf{u}$ – решение уравнения $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = \mathbf{q}$;

2) $\mathtt{P}^{(2)}_{\mathbf{f},\mathbf{q}_0,t}$ $(\mathbf{f} \in \mathcal{F}_{k,m}; \mathbf{q}_0, \mathbf{q} \in K^k; t \in \mathbb{N})$ – вероятность того, что для двух различных входных слов $\mathbf{u}$ и $\mathbf{u}'$, случайно выбранных из множества $(K^m)^t$, истинно равенство $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}')$.

Следствие 5.2. Для каждого отображения $\mathbf{f} \in \mathcal{F}_{k,m}$ при любых состояниях $\mathbf{q}_0, \mathbf{q} \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ равенство

$$\mathtt{P}^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q}) = |K|^{-k} \tag{5.78}$$

истинно для всех чисел $t \in \mathbb{N}$.□

Доказательство. Зафиксируем отображение $\mathbf{f} \in \mathcal{F}_{k,m}$ и состояния $\mathbf{q}_0, \mathbf{q} \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$.

Из (5.71) вытекает, что для всех чисел $t \in \mathbb{N}$

$$\mathtt{P}^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q}) = \frac{|H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_t) \cap (K^m)^t|}{|(K^m)^t|} = \frac{|K|^{tm-k}}{|(K^m)^t|} = |K|^{-k},$$

что и требовалось доказать.□

Из (5.78) вытекает, что истинны следующие два утверждения.

Утверждение 5.1. Для всех отображений $\mathbf{f} \in \mathcal{F}_{k,m}$ и состояний $\mathbf{q}_0, \mathbf{q} \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ вероятность $\mathsf{P}^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q})$ не зависит ни от мощности $|K^m|$ входного алфавита автомата $M_{\mathbf{f}}$ (т.е. не зависит от числа $m \in \mathbb{N}$ $(m \geq k)$), ни от длины $t \in \mathbb{N}$ входного слова.$\square$

Утверждение 5.2. Для всех отображений $\mathbf{f} \in \mathcal{F}_{k,m}$, состояний $\mathbf{q}_0, \mathbf{q} \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ и чисел $t \in \mathbb{N}$ вероятность $\mathsf{P}^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q})$ монотонно убывает при росте параметра $k \in \mathbb{N}$, причем

$$\lim_{k\to\infty} \mathsf{P}^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q}) = 0$$

для всех $\mathbf{f} \in \mathcal{F}_{k,m}$, $\mathbf{q}_0 \in K^k$ и $t \in \mathbb{N}$.$\square$

Следствие 5.3. Для каждого отображения $\mathbf{f} \in \mathcal{F}_{k,m}$ и каждого начального состояния $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ равенства

$$\mathsf{P}^{(2)}_{\mathbf{f},\mathbf{q}_0,t} = |K|^{-k}\left(1 - \frac{|K|^k - 1}{|K|^{mt} - 1}\right) \tag{5.79}$$

истинны для всех чисел $t \in \mathbb{N}$.$\square$

Доказательство. Зафиксируем отображение $\mathbf{f} \in \mathcal{F}_{k,m}$ и начальное состояние $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ и число $t \in \mathbb{N}$.

Для каждого числа $t \in \mathbb{N}$ множества входных слов $H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_t) \cap (K^m)^t$ $(\mathbf{q}_t \in K^k)$ попарно не пересекаются. Поэтому, принимая во внимание равенство (5.71), получим, что для всех чисел $t \in \mathbb{N}$

$$\mathsf{P}^{(2)}_{\mathbf{f},\mathbf{q}_0,t} = \frac{\sum\limits_{\mathbf{q}_t\in K^k} \binom{H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_t)\cap(K^m)^t}{2}}{\binom{(K^m)^t}{2}} = \frac{\sum\limits_{\mathbf{q}_t\in K^k} 0.5|K|^{tm-k}(|K|^{tm-k}-1)}{0.5|K|^{tm}(|K|^{tm}-1)} =$$

$$= \frac{0.5|K|^{tm-k}(|K|^{tm-k}-1)\sum\limits_{\mathbf{q}_t\in K^k} 1}{0.5|K|^{tm}(|K|^{tm}-1)} = \frac{0.5|K|^{tm-k}(|K|^{tm-k}-1)|K^k}{0.5|K|^{tm}(|K|^{tm}-1)} =$$

$$= \frac{|K|^{tm-k}-1}{|K|^{tm}-1} = |K|^{-k}\frac{|K|^{tm}-|K|^k}{|K|^{tm}-1} = |K|^{-k}\frac{|K|^{tm}-1+1-|K|^k}{|K|^{tm}-1} =$$

$$= |K|^{-k}\left(1 - \frac{|K|^k-1}{|K|^{mt}-1}\right),$$

что и требовалось доказать.$\square$

Из (5.79) вытекает, что истинны следующие три утверждения.

УТВЕРЖДЕНИЕ 5.3. Для всех отображений $\mathbf{f} \in \mathcal{F}_{k,m}$ и всех начальных состояний $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ вероятность $\mathtt{P}^{(2)}_{\mathbf{f},\mathbf{q}_0,t}$ монотонно возрастает при росте длины $t \in \mathbb{N}$ входного слова, причем

$$\lim_{t\to\infty} \mathtt{P}^{(2)}_{\mathbf{f},\mathbf{q}_0,t} = |K|^{-k}$$

для всех $\mathbf{f} \in \mathcal{F}_{k,m}$, $\mathbf{q}_0 \in K^k$ и $k, m \in \mathbb{N}$ $(k \le m)$.$\square$

УТВЕРЖДЕНИЕ 5.4. Для всех отображений $\mathbf{f} \in \mathcal{F}_{k,m}$, всех начальных состояний $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ и всех чисел $t \in \mathbb{N}$ вероятность $\mathtt{P}^{(2)}_{\mathbf{f},\mathbf{q}_0,t}$ монотонно возрастает при росте параметра $m \in \mathbb{N}$ $(m \ge k)$, причем

$$\lim_{m\to\infty} \mathtt{P}^{(2)}_{\mathbf{f},\mathbf{q}_0,t} = |K|^{-k}$$

для всех $\mathbf{f} \in \mathcal{F}_{k,m}$, $\mathbf{q}_0 \in K^k$, $k \in \mathbb{N}$ $(k \le m)$ и $t \in \mathbb{N}$.$\square$

УТВЕРЖДЕНИЕ 5.5. Для всех отображений $\mathbf{f} \in \mathcal{F}_{k,m}$ и всех начальных состояний $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ число $|K|^{-k}$ является верхней границей для вероятности $\mathtt{P}^{(2)}_{\mathbf{f},\mathbf{q}_0,t}$ при всех значениях параметров $k, m \in \mathbb{N}$ $(k \le m)$ и при любой длине $t \in \mathbb{N}$ входного слова.$\square$

5.3.3. Вычислительная стойкость исследуемой модели.

Охарактеризуем вначале для произвольного $t \in \mathbb{N}$ сложность поиска такого входного слова $\mathbf{u} \in (K^m)^t$, что при заданном значении $\mathbf{q} \in K^k$ истинно равенство

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = \mathbf{q}, \tag{5.80}$$

а также сложность поиска таких входных слов $\mathbf{u}, \widetilde{\mathbf{u}} \in (K^m)^t$ $(\mathbf{u} \ne \widetilde{\mathbf{u}})$, что истинно равенство

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = H_{\mathbf{f},\mathbf{q}_0}(\widetilde{\mathbf{u}}) \tag{5.81}$$

в предположении, что экспериментатору известно семейство хэш-функций $\mathcal{H}_{\mathbf{f}}$, т.е. известно отображение $\mathbf{f} \in \mathcal{F}_{k,m}$ для системы уравнений (5.57).

Возможны следующие две ситуации.

Ситуация 5.1. Экспериментатору известна хэш-функция $H_{\mathbf{f},\mathbf{q}_0}$, т.е. известно начальное состояние $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$.

Охарактеризуем для произвольного $t \in \mathbb{N}$ сложность поиска одного (не важно, какого именно) решения уравнения (5.80), т.е. сложность поиска такого входного слова $\mathbf{x}_1 \dots \mathbf{x}_t \in (K^m)^t$ $(t \in \mathbb{N})$, что

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_t) = \mathbf{q},$$

где $\mathbf{q} \in K^k$ – фиксированное состояние автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$.

Пусть $t = 1$.

Тогда сложность поиска решения уравнения (5.80) совпадает со сложностью поиска одного (не важно, какого именно) решения $\mathbf{x}_1 \in K^m$ уравнения

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1) = \mathbf{q},$$

т.е., иными словами, со сложностью поиска одного (не важно, какого именно) решения $\mathbf{x}_1 \in K^m$ уравнения

$$\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) = \mathbf{q}$$

при известных значениях $\mathbf{q}_0, \mathbf{q} \in K^k$.

Пусть $t > 1$.

Тогда в качестве $\mathbf{x}_1 \dots \mathbf{x}_{t-1}$ достаточно выбрать любое входное слово, а в качестве входного символа $\mathbf{x}_t$ – любое решение уравнения

$$\mathbf{f}(H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_{t-1}), \mathbf{x}_t) = \mathbf{q}$$

при известных значениях $\mathbf{q}_0, \mathbf{q} \in K^k$.

Таким образом, если экспериментатору известно начальное состояние $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$, то при любом $t \in \mathbb{N}$ сложность поиска одного (не важно, какого именно) решения уравнения (5.80) (без учета сложности вычисления значения функции $H_{\mathbf{f},\mathbf{q}_0}$) совпадает со сложностью поиска одного (не важно, какого именно) решения уравнения

$$\mathbf{f}(\mathbf{q}, \mathbf{x}) = \widetilde{\mathbf{q}}$$

при известных значениях $\mathbf{q}, \widetilde{\mathbf{q}} \in K^k$.

Охарактеризуем для произвольного $t \in \mathbb{N}$ сложность поиска одного (не важно, какого именно) решения уравнения (5.81), т.е. сложность поиска двух таких различных входных слов $\mathbf{x}_1 \dots \mathbf{x}_t \in (K^m)^t$ и $\widetilde{\mathbf{x}}_1 \dots \widetilde{\mathbf{x}}_t \in (K^m)^t$, что

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_t) = H_{\mathbf{f},\mathbf{q}_0}(\widetilde{\mathbf{x}}_1 \dots \widetilde{\mathbf{x}}_t).$$

Пусть $t = 1$.

Если $k = m$, то из (5.55) вытекает, что

$$\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) \neq \mathbf{f}(\mathbf{q}_0, \widetilde{\mathbf{x}}_1)$$

для любых входных символов $\mathbf{x}_1, \widetilde{\mathbf{x}}_1 \in K^m$ $(\mathbf{x}_1 \neq \widetilde{\mathbf{x}}_1)$, т.е. уравнение (5.81) не имеет решений для любого отображения $\mathbf{f} \in \mathcal{F}_{k,m}$ и любого начального состояния $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$.

Если же $k < m$, то сложность поиска одного (не важно, какого именно) решения уравнения (5.81) совпадает со сложностью поиска одного (не важно, какого именно) решения $(\mathbf{x}_1, \widetilde{\mathbf{x}}_1) \in K^m \times K^m$ $(\mathbf{x}_1 \neq \widetilde{\mathbf{x}}_1)$ уравнения

$$\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) = \mathbf{f}(\mathbf{q}_0, \widetilde{\mathbf{x}}_1)$$

при известном значении $\mathbf{q}_0 \in K^k$.

Пусть $t > 1$.

Если $k = m$, то в качестве $\mathbf{x}_1 \dots \mathbf{x}_{t-1}$ и $\widetilde{\mathbf{x}}_1 \dots \widetilde{\mathbf{x}}_{t-1}$ достаточно выбрать любые такие входные слова, что при известном значении $\mathbf{q}_0 \in K^k$

$$\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_{t-1}) \neq \mathbf{f}(\mathbf{q}_0, \widetilde{\mathbf{x}}_1 \dots \widetilde{\mathbf{x}}_{t-1}),$$

а в качестве $\mathbf{x}_t$ и $\widetilde{\mathbf{x}}_t$ – любые такие входные символы, что

$$\mathbf{f}(\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_{t-1}), \mathbf{x}_t) = \mathbf{f}(\mathbf{f}(\mathbf{q}_0, \widetilde{\mathbf{x}}_1 \dots \widetilde{\mathbf{x}}_{t-1}), \widetilde{\mathbf{x}}_t).$$

при известном значении $\mathbf{q}_0 \in K^k$.

Замечание 5.12. Так как $\mathbf{x}_1 \dots \mathbf{x}_{t-1} \neq \widetilde{\mathbf{x}}_1 \dots \widetilde{\mathbf{x}}_{t-1}$, то допускается, что $\mathbf{x}_t = \widetilde{\mathbf{x}}_t$.

Если же $k < m$, то в качестве $\mathbf{x}_1 \dots \mathbf{x}_{t-1}$ достаточно выбрать любое входное слово, положить $\widetilde{\mathbf{x}}_1 \dots \widetilde{\mathbf{x}}_{t-1} = \mathbf{x}_1 \dots \mathbf{x}_{t-1}$, а в качестве $\widetilde{\mathbf{x}}_t$ выбрать любые два такие различные входные символы, что

$$\mathbf{f}(\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_{t-1}), \mathbf{x}_t) = \mathbf{f}(\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_{t-1}), \widetilde{\mathbf{x}}_t)$$

при известном значении $\mathbf{q}_0 \in K^k$.

Таким образом, если экспериментатору известно начальное состояние $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$, то при любом $t \in \mathbb{N}$ сложность поиска двух таких различных входных слов $\mathbf{u} = \mathbf{x}_1 \dots \mathbf{x}_t \in (K^m)^t$ и $\widetilde{\mathbf{u}} = \widetilde{\mathbf{x}}_1 \dots \widetilde{\mathbf{x}}_t \in (K^m)^t$, что $(\mathbf{u}, \widetilde{\mathbf{u}})$ является решением уравнения (5.81), совпадает со сложностью поиска одного (не важно, какого именно) решения $(\mathbf{x}, \widetilde{\mathbf{x}}) \in K^m \times K^m$ (возможно при дополнительном условии $\mathbf{x} \neq \widetilde{\mathbf{x}}$) уравнения

$$\mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{f}(\widetilde{\mathbf{q}}, \widetilde{\mathbf{x}})$$

при известных значениях $\mathbf{q}, \widetilde{\mathbf{q}} \in K^k$.

Замечание 5.13. Если $k < m$, то число скалярных уравнений, определяемых как векторным уравнением $\mathbf{f}(\mathbf{q}, \mathbf{x}) = \widetilde{\mathbf{q}}$, так и векторным уравнением $\mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{f}(\widetilde{\mathbf{q}}, \widetilde{\mathbf{x}})$ меньше числа неизвестных. Это обстоятельство существенно усложняет перебор в процессе поиска решений уравнений над конечным кольцом с делителями нуля (см., напр., [80]).

Ситуация 5.2. Экспериментатору не известна хэш-функция $H_{\mathbf{f},\mathbf{q}_0}$, т.е. не известно начальное состояние $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$.

Замечание 5.14. При этом, как обычно, предполагается, что любое состояние $\mathbf{q}_0 \in K^k$ может быть выбрано в качестве начального состояния автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ с одной и той же вероятностью $|K^k|^{-1}$.

Пусть $t = 1$.

Единственным способом поиска (при известных значениях $\mathbf{q}_0, \mathbf{q} \in K^k$) такого входного символа $\mathbf{x}_1 \in K^k$, что

$$\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) = \mathbf{q} \tag{5.82}$$

является случайный выбор входного символа.

Аналогичным образом, при условии, что $k < m$, единственным способом поиска (при известном значении $\mathbf{q}_0 \in K^k$) таких входных символов $\mathbf{x}_1, \widetilde{\mathbf{x}}_1 \in K^k$ $(\mathbf{x}_1 \neq \widetilde{\mathbf{x}}_1)$, что

$$\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) = \mathbf{f}(\mathbf{q}_0, \widetilde{\mathbf{x}}_1) \tag{5.83}$$

также является случайный выбор входных символов.

Замечание 5.15. При $k = m$ не существуют такие входные символы $\mathbf{x}_1, \widetilde{\mathbf{x}}_1 \in K^k$ $(\mathbf{x}_1 \neq \widetilde{\mathbf{x}}_1)$, что $\mathbf{f}(\mathbf{q}_0, \mathbf{x}) = \mathbf{f}(\mathbf{q}_0, \widetilde{\mathbf{x}}_1)$.

Вероятность того, что равенство (5.82) истинно при случайном выборе входного символа $\mathbf{x}_1 \in K^k$ определяется формулой (5.78).

Аналогичным образом, вероятность того, что равенство (5.83) истинно при случайном выборе входных символов $\mathbf{x}_1, \widetilde{\mathbf{x}}_1 \in K^k$ $(\mathbf{x}_1 \neq \widetilde{\mathbf{x}}_1)$ определяется формулой (5.79).

Пусть $t > 1$.

Предположим, что экспериментатор, кроме возможности наблюдать финальное состояние автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$, имеет также возможность наблюдать состояние исследуемого автомата $M_{\mathbf{f}}$ на всех промежуточных вычислениях.

Тогда, выбрав произвольный входной символ $\mathbf{x}_1 \in K^k$, экспериментатор определяет текущее состояние $\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1)$ исследуемого автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$, и ситуация сводится к рассмотренному выше случаю.

Предположим, что экспериментатор не имеет возможности наблюдать состояние исследуемого автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ ни на одном промежуточном вычислении, а имеет возможность наблюдать только финальное состояние автомата $M_{\mathbf{f}}$.

Тогда единственным способом поиска одного (не важно, какого именно) решения $\mathbf{u} \in (K^m)^t$ уравнения (5.80) является случайный выбор входного слова. При этом, вероятность того, что при случайном выборе входного слова $\mathbf{u} \in (K^m)^t$ истинно равенство (5.80), определяется формулой (5.78).

Аналогичным образом, единственным способом поиска одного (не важно, какого именно) решения $(\mathbf{u}, \widetilde{\mathbf{u}}) \in (K^m)^t \times (K^m)^t$ $(\mathbf{u} \neq \widetilde{\mathbf{u}})$ уравнения (5.81) является случайный выбор входных слов. При этом, вероятность того, что при случайном выборе входных слов $\mathbf{u}, \widetilde{\mathbf{u}} \in (K^m)^t$ $(\mathbf{u} \neq \widetilde{\mathbf{u}})$ истинно равенство (5.81), определяется формулой (5.79).

Высокая сложность поиска входного слова $\mathbf{u} \in (K^m)^t$, для которого истинно равенство (5.80), а также поиска входных слов $\mathbf{u}, \widetilde{\mathbf{u}} \in (K^m)^t$ $(\mathbf{u} \neq \widetilde{\mathbf{u}})$, для которых истинно равенство (5.81), обосновывают возможность использования семейства хэш-функций $\mathcal{H}_{\mathbf{f}}$ $(\mathbf{f} \in \mathcal{F}_{k,m})$ в алгоритмах защиты информации. При этом начальное состояние $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$ целесообразно использовать в качестве секретного сеансового ключа используемой хэш-функции.

Рассмотрим теперь задачу параметрической идентификации семейства хэш-функций $\mathcal{H}_{\mathbf{f}}$ $(\mathbf{f} \in \mathcal{F}_{k,m})$.

Пусть $\mathbf{f} \in \mathcal{F}_{k,m}$ – такое отображение, что

$$\mathbf{f}(\mathbf{q}_t, \mathbf{x}_{t+1}) = \mathbf{F}(a_1, \ldots, a_r, \mathbf{q}_t, \mathbf{x}_{t+1}) \ (t \in \mathbb{Z}_+),$$

где $a_1, \ldots, a_r \in K$ – параметры, т.е. система уравнений (5.57) имеет вид

$$M_{\mathbf{f}} : \mathbf{q}_{t+1} = \mathbf{F}(a_1, \ldots, a_r, \mathbf{q}_t, \mathbf{x}_{t+1}) \ (t \in \mathbb{Z}_+), \tag{5.84}$$

где отображение $\mathbf{F}$ известно экспериментатору.

Предположим, что экспериментатору не известны значения параметров, входящих в систему уравнений (5.84), но экспериментатор, кроме возможности наблюдать финальное состояние автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$, имеет также возможность наблюдать состояние исследуемого автомата $M_{\mathbf{f}}$ на всех промежуточных вычислениях.

Тогда идентификация семейства хэш-функций (5.84) является задачей параметрической идентификации автомата, принадлежащего заданному семейству автоматов над кольцом $\mathcal{K}$.

При возможности экспериментатора проводить только простой эксперимент решение задачи параметрической идентификации автомата сводится к поиску входного слова $\mathbf{x}_1 \ldots \mathbf{x}_n \in (K^m)^n$ заранее неизвестной

длины $n \in \mathbb{N}$ с целью формирования и решения над кольцом $\mathcal{K}$ системы уравнений

$$\mathbf{q}_i = \mathbf{F}(a_1, \ldots, a_r, \mathbf{q}_{i-1}, \mathbf{x}_i) \ (i = 1, \ldots, n) \tag{5.85}$$

относительно неизвестных $a_1, \ldots, a_r \in K$.

При возможности экспериментатора проводить l-кратный эксперимент (где $l \in \mathbb{N}$ $(l \geq 2)$ – фиксированное число) решение задачи параметрической идентификации автомата сводится к поиску l-элементного множества входных слов $\mathbf{x}_1^{(i)} \ldots \mathbf{x}_{n_i}^{(i)} \in (K^m)^{n_i}$ $(i = 1, \ldots, l)$, длины n_i которых заранее неизвестны, с целью формирования и решения над кольцом $\mathcal{K}$ системы уравнений

$$\mathbf{q}_j^{(i)} = \mathbf{F}(a_1, \ldots, a_r, \mathbf{q}_0, \mathbf{x}_1^{(i)} \ldots \mathbf{x}_1^{(i)}) \ (i = 1, \ldots, l; j = 1, \ldots, n_i) \tag{5.86}$$

относительно неизвестных $a_1, \ldots, a_r \in K$.

Ситуация несколько отличается, если экспериментатор может любое число раз устанавливать исследуемый автомат в любое требуемое начальное состояние, и при каждой установке начального состояния проводить с исследуемым автоматом кратный эксперимент любой кратности.

В этом случае для решения задачи параметрической идентификации автомата достаточно сформировать и решить над кольцом систему уравнений

$$\widetilde{\mathbf{q}} = \mathbf{F}(a_1, \ldots, a_r, \mathbf{q}, \mathbf{x}) \ (\mathbf{q} \in K^k, \mathbf{x} \in K^m) \tag{5.87}$$

относительно неизвестных $a_1, \ldots, a_r \in K$.

Отметим, что в кольце с делителями нуля при достаточно большом значении $k \in \mathbb{N}$ решение любой из систем уравнений (5.85)-(5.87) является сложной задачей из-за перебора, обусловленного именно наличием делителей нуля.

Поэтому, при использовании семейства хэш-функций $\mathcal{H}_{\mathbf{f}}$ $(\mathbf{f} \in \mathcal{F}_{k,m})$ в алгоритмах защиты информации параметры $a_1, \ldots, a_r$, входящие в уравнение (5.84), целесообразно использовать либо в качестве секретного ключа средней длительности, либо в качестве долговременного секретного ключа.

Замечание 5.16. Если экспериментатор, кроме возможности наблюдать финальное состояние автомата $M_{\mathbf{f}} \in \mathcal{M}_{\mathcal{F}_{k,m}}$, имеет также возможность наблюдать состояние исследуемого автомата $M_{\mathbf{f}}$ на всех промежуточных вычислениях, то методом, изложенным в п.5.2, может быть построена имитационная модель заданного семейства хеш-функций. Оценка сложности построения и точности такой модели осуществляется на основе алгебраических свойств отображения $\mathbf{F}$.

5.4. Автоматы, определенные в терминах идеалов кольца.

В процессе исследования различных объектов, определенных над конечным кольцом, естественно возникает необходимость анализа их свойств при наличии тех или иных дополнительных ограничений, сформулированных в терминах этого кольца. Именно такой, по своей сути, подход и применялся (в явном или неявном виде) при исследовании, представленном в разделах 2-5.

Одним из основных понятий теории колец является понятие идеала кольца. Поэтому естественным является анализ свойств автоматных моделей, определенных системой рекуррентных соотношений над конечным кольцом, при наличии ограничений, сформулированных в терминах идеалов этого кольца. Актуальность таких исследований обусловлена тем, что существует тесная связь между идеалами колец и многообразиями над кольцами. В результате устанавливается внутренняя связь между алгебраической теорией автоматов и алгебраической геометрией на конечных кольцах.

Исходя из сказанного выше, исследуем свойства автоматов Мили и Мура над кольцом $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}$ ($|K| \geq 2$), функции переходов и выходов которых являются алгебраическими суммами функции от состояния автомата и функции от входного символа при условии, что значение каждой компоненты функции переходов принадлежит фиксированным идеалам кольца.

5.4.1. Исследуемые модели.

Для каждого числа $n \in \mathbb{N}$ обозначим через $\mathcal{A}_{n,1}$ семейство автоматов Мили, определенных системой рекуррентных соотношений

$$M_1 : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t) + \mathbf{f}_3(\mathbf{x}_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_t) + \mathbf{f}_4(\mathbf{x}_{t+1}) \end{cases} \quad (t \in \mathbb{Z}_+), \tag{5.88}$$

а через $\mathcal{A}_{n,2}$ семейство автоматов Мура, определенных системой рекуррентных соотношений

$$M_2 : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t) + \mathbf{f}_3(\mathbf{x}_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_{t+1}) \end{cases} \quad (t \in \mathbb{Z}_+), \tag{5.89}$$

где $\mathbf{f}_i : K^n \to K^n$ ($i = 1, 2, 3, 4$), а $\mathbf{q}_t \in K^n$, $\mathbf{x}_t \in K^n$ и $\mathbf{y}_t \in K^n$ являются, соответственно, состоянием автомата, входным и выходным символом в момент t.

Если множество K^n интерпретируется, соответственно, как входной алфавит, как множество состояний или как выходной алфавит автомата $M_i \in \mathcal{A}_{n,i}$ $(i = 1, 2)$, то будем обозначать множество K^n, соответственно, через $\mathbf{X}_n$, $\mathbf{Q}_n$ и $\mathbf{Y}_n$.

Обозначим через $\mathcal{A}_{n,i}^{inv}$ $(i = 1, 2)$ семейство всех обратимых автоматов $M_i \in \mathcal{A}_{n,i}$. Известно, что (см., напр., [80]):

1) $M_1 \in \mathcal{A}_{n,1}^{inv}$ тогда и только тогда, когда $\mathbf{f}_4$ является биекцией множества K^n на себя;

2) $M_2 \in \mathcal{A}_{n,2}^{inv}$ тогда и только тогда, когда $\mathbf{f}_2$ и $\mathbf{f}_3$ являются биекциями множества K^n на себя.

При этом, для автомата $M_1 \in \mathcal{A}_{n,1}^{inv}$ обратным автоматом является автомат

$$M_1^{-1} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t) + \mathbf{f}_3(\mathbf{f}_4^{-1}(\mathbf{x}_{t+1} - \mathbf{f}_2(\mathbf{q}_t))) \\ \mathbf{y}_{t+1} = \mathbf{f}_4^{-1}(\mathbf{x}_{t+1} - \mathbf{f}_2(\mathbf{q}_t)) \end{cases} \qquad (t \in \mathbb{Z}_+),$$

а для автомата $M_2 \in \mathcal{A}_{n,2}^{inv}$ обратным автоматом является автомат

$$M_1^{-1} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_2^{-1}(\mathbf{x}_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{f}_3^{-1}(\mathbf{f}_2^{-1}(\mathbf{x}_{t+1}) - \mathbf{f}_1(\mathbf{q}_t)) \end{cases} \qquad (t \in \mathbb{Z}_+).$$

Замечание 5.17. Отметим, что если пара обратимых автоматов (M_i, M_i^{-1}) $(i = 1, 2)$ рассматривается в качестве математической модели поточного шифра, то в процессе «шифрование-расшифрование» автоматы M_i и M_i^{-1} движутся в пространстве состояний по одной и той же траектории в одном и том же направлении.

Для каждого идеала I кольца $\mathcal{K}$ в фактор-кольце

$$\mathcal{K}/_{\equiv_I} = (K/_{\equiv_I}, +_I, \cdot_I)$$

множество $K/_{\equiv_I}$ является разбиением множества K на $|K| \cdot |I|^{-1}$ блоков, каждый из которых содержит $|I|$ элементов.

Отсюда вытекает, что для каждого вектора $\mathbf{I} = (I_1, \ldots, I_n)$, где I_j $(j = 1, \ldots, n)$ – идеал кольца $\mathcal{K}$, в фактор-кольце

$$\mathcal{K}^n/_{\equiv_{\mathbf{I}}} = (K/_{\equiv_{I_1}} \times \cdots \times K/_{\equiv_{I_n}}, +_{\mathbf{I}}, \cdot_{\mathbf{I}})$$

множество $K/_{\equiv_{I_1}} \times \cdots \times K/_{\equiv_{I_n}}$ является разбиением множества K^n на $|K|^n \cdot \prod\limits_{j=1}^{n} |I_j|^{-1}$ блоков, каждый из которых содержит $\prod\limits_{j=1}^{n} |I_j|$ элементов.

При этом для любых элементов $\mathbf{a}_i = (a_1^{(i)}, \ldots, a_n^{(i)}) \in K^n$ $(i = 1, 2)$ истинна формула

$$\mathbf{a}_1 \equiv \mathbf{a}_2 \,(mod\, \mathbf{I}) \Leftrightarrow (\forall 1 \leq j \leq n)(a_j^{(1)} \equiv a_j^{(1)} \,(mod\, I_j)).$$

Каждые два вектора

$$\mathbf{I}_r = (I_1^{(r)}, \ldots, I_n^{(r)}) \ (r = 1, 2), \tag{5.90}$$

где $I_j^{(r)}$ $(r = 1, 2; j = 1, \ldots, n)$ – идеал кольца $\mathcal{K}$, определяют семейства автоматов

$$\mathcal{A}_{n,i}(\mathbf{I}_1, \mathbf{I}_2) = \{M_i \in \mathcal{A}_{n,i} \mid Val\, \mathbf{f}_1 = \mathbf{I}_1 \& Val\, \mathbf{f}_2 = \mathbf{I}_2\} \ (i = 1, 2).$$

Отметим, что для каждого автомата $M \in \mathcal{A}_{n,1}(\mathbf{I}_1, \mathbf{I}_2) \cup \mathcal{A}_{n,2}(\mathbf{I}_1, \mathbf{I}_2)$ истинны равенства

$$|\mathbf{Q}_n/_{\ker \mathbf{f}_1}| = |\mathbf{I}_1| \tag{5.91}$$

и

$$|\mathbf{Q}_n/_{\ker \mathbf{f}_2}| = |\mathbf{I}_2|. \tag{5.92}$$

Обозначим через $\mathcal{A}_{n,i}^{inv}(\mathbf{I}_1, \mathbf{I}_2)$ $(i = 1, 2)$ семейство всех обратимых автоматов $M_i \in \mathcal{A}_{n,i}(\mathbf{I}_1, \mathbf{I}_2)$.

Замечание 5.18. Так как

$$\mathbf{I}_2 \neq (\underbrace{K, \ldots, K}_{n \text{ раз}}) \Rightarrow \mathcal{A}_{n,2}^{inv}(\mathbf{I}_1, \mathbf{I}_2) = \emptyset,$$

то при $\mathbf{I}_2 = (\underbrace{K, \ldots, K}_{n \text{ раз}})$ для упрощения обозначений будем писать $\mathcal{A}_{n,2}^{inv}(\mathbf{I}_1)$ вместо $\mathcal{A}_{n,2}^{inv}(\mathbf{I}_1, \mathbf{I}_2)$.

Исследуем свойства семейств автоматов $\mathcal{A}_{n,i}(\mathbf{I}_1, \mathbf{I}_2)$ $(i = 1, 2)$ и $\mathcal{A}_{n,i}^{inv}(\mathbf{I}_1, \mathbf{I}_2)$ $(i = 1, 2)$.

5.4.2. Комбинаторные характеристики исследуемых моделей.

Оценим мощности семейств автоматов $\mathcal{A}_{n,i}(\mathbf{I}_1, \mathbf{I}_2)$ $(i = 1, 2)$ и $\mathcal{A}_{n,i}^{inv}(\mathbf{I}_1, \mathbf{I}_2)$ $(i = 1, 2)$.

Утверждение 5.6. Равенства

$$|\mathcal{A}_{n,i}| = |K|^{(5-i)n|K|} \ (i = 1, 2) \tag{5.93}$$

истинны для всех чисел $n \in \mathbb{N}$.□

Доказательство. Для каждого числа $n \in \mathbb{N}$ число отображений $\mathbf{f} : K^n \to K^n$ равно $|K|^{n|K|}$.

При построении автомата $M_1 \in \mathcal{A}_{n,1}$ осуществляется независимый выбор отображений $\mathbf{f}_i : K^n \to K^n$ $(i = 1, 2, 3, 4)$. Поэтому,

$$|\mathcal{A}_{n,1}| = (|K|^{n|K|})^4 = |K|^{4n|K|}. \tag{5.94}$$

При построении автомата $M_2 \in \mathcal{A}_{n,2}$ осуществляется независимый выбор отображений $\mathbf{f}_i : K^n \to K^n$ $(i = 1, 2, 3)$. Следовательно,

$$|\mathcal{A}_{n,2}| = (|K|^{n|K|})^3 = |K|^{3n|K|}. \tag{5.95}$$

Из истинности равенств (5.94) и (5.95) вытекает, что для всех чисел $n \in \mathbb{N}$ истинны равенства (5.93).□

Утверждение 5.7. Равенства

$$|\mathcal{A}^{inv}_{n,i}| = |\mathcal{A}_{n,i}| \left(\frac{|K|!}{|K|^{|K|}} \right)^{in} \quad (i = 1, 2) \tag{5.96}$$

истинны для всех чисел $n \in \mathbb{N}$.□

Доказательство. Для каждого числа $n \in \mathbb{N}$ число отображений $\mathbf{f} : K^n \to K^n$, являющихся биекциями, равно $(|K|!)^n$.

При построении автомата $M_1 \in \mathcal{A}^{inv}_{n,1}$ осуществляется независимый выбор отображений $\mathbf{f}_i : K^n \to K^n$ $(i = 1, 2, 3, 4)$. Следовательно, используя равенство (5.94), получим

$$|\mathcal{A}^{inv}_{n,1}| = (|K|^{n|K|})^3 (|K|!)^n = |\mathcal{A}_{n,1}| \left(\frac{|K|!}{|K|^{|K|}} \right)^n. \tag{5.97}$$

Аналогичным образом, при построении автомата $M_2 \in \mathcal{A}^{inv}_{n,2}$ осуществляется независимый выбор отображений $\mathbf{f}_i$ $(i = 1, 2, 3)$. Следовательно, используя равенство (5.95), получим

$$|\mathcal{A}^{inv}_{n,2}| = |K|^{n|K|} ((|K|!)^n)^2 = |\mathcal{A}_{n,2}| \left(\frac{|K|!}{|K|^{|K|}} \right)^2. \tag{5.98}$$

Из истинности равенств (5.97) и (5.98) вытекает, что для всех чисел $n \in \mathbb{N}$ истинны равенства (5.96).□

Следствие 5.4. При $i = 1, 2$ асимптотическое равенство

$$|\mathcal{A}^{inv}_{n,i}| = |\mathcal{A}_{n,i}| (\sqrt{2\pi|K|} \cdot e^{-|K|} (1 + O(|K|^{-1})))^{in} \ (|K| \to \infty) \tag{5.99}$$

истинно для всех чисел $n \in \mathbb{N}$.□

Доказательство. Из формулы Стирлинга вытекает, что

$$|K|! = \sqrt{2\pi|K|} \cdot |K|^{|K|} e^{-|K|}(1 + O(|K|^{-1})) \ (|K| \to \infty). \qquad (5.100)$$

Из истинности равенств (5.96) и (5.100) вытекает, что для всех чисел $i \in \{1, 2\}$ и $n \in \mathbb{N}$ истинны равенства (5.99).□

Теорема 5.4. Для каждых векторов $\mathbf{I}_r = (I_1^{(r)}, \ldots, I_n^{(r)})$ $(r = 1, 2)$, где $I_j^{(r)}$ $(r = 1, 2; j = 1, \ldots, n)$ – идеал кольца $\mathcal{K}$, равенства

$$|\mathcal{A}_{n,i}(\mathbf{I}_1, \mathbf{I}_2)| =$$

$$= \frac{|\mathcal{A}_{n,i}|}{|K|^{2n|K|}} \cdot \prod_{r=1}^{2} \prod_{j=1}^{n} \left(\sum_{h=0}^{|I_j^{(r)}|} (-1)^h \binom{|I_j^{(r)}|}{h} (|I_j^{(r)}| - h)^{|K|} \right) \ (i = 1, 2) \ (5.101)$$

истинны для всех чисел $n \in \mathbb{N}$.□

Доказательство. Известно, что (см., напр., [51]) для каждых чисел $l, m \in \mathbb{N}$ $(m < l)$ число сюръекций l-элементного множества на m-элементное множество равно

$$s_{l,m} = \sum_{h=0}^{m} (-1)^h \binom{m}{h} (m - h)^l. \qquad (5.102)$$

Из формулы (5.102) вытекает, что для каждого вектора

$$\mathbf{I}_r = (I_1^{(r)}, \ldots, I_n^{(r)}) \ (r = 1, 2),$$

где $I_j^{(r)}$ $(r = 1, 2; j = 1, \ldots, n)$ – идеал кольца $\mathcal{K}$ число всех таких отображений $\mathbf{f}_r : K^n \to K^n$ $(r = 1, 2)$, что $Val\, \mathbf{f}_r = \mathbf{I}_r$, равно

$$t_{\mathbf{I}_r} = \prod_{j=1}^{n} s_{|K|,|I_j^{(r)}|} =$$

$$= \prod_{j=1}^{n} \left(\sum_{h=0}^{|I_j^{(r)}|} (-1)^h \binom{|I_j^{(r)}|}{h} (|I_j^{(r)}| - h)^{|K|} \right) \ (r = 1, 2). \qquad (5.103)$$

При построении автомата $M_1 \in \mathcal{A}_{n,1}(\mathbf{I}_1, \mathbf{I}_2)$ осуществляется независимый выбор отображений $\mathbf{f}_i$ $(i = 1, 2, 3, 4)$. Следовательно, из равенств (5.94) и (5.103) вытекает, что

$$|\mathcal{A}_{n,1}(\mathbf{I}_1, \mathbf{I}_2)| = |K|^{2n|K|} \prod_{r=1}^{2} t_{\mathbf{I}_r} =$$

$$= |K|^{2n|K|} \prod_{r=1}^{2} \prod_{j=1}^{n} \left(\sum_{h=0}^{|I_j^{(r)}|} (-1)^h \binom{|I_j^{(r)}|}{h} (|I_j^{(r)}| - h)^{|K|} \right) =$$

$$= \frac{|\mathcal{A}_{n,1}|}{|K|^{2n|K|}} \cdot \prod_{r=1}^{2} \prod_{j=1}^{n} \left(\sum_{h=0}^{|I_j^{(r)}|} (-1)^h \binom{|I_j^{(r)}|}{h} (|I_j^{(r)}| - h)^{|K|} \right). \qquad (5.104)$$

При построении автомата $M_2 \in \mathcal{A}_{n,2}(\mathbf{I}_1, \mathbf{I}_2)$ осуществляется независимый выбор отображений $\mathbf{f}_i$ $(i = 1, 2, 3)$.

Следовательно, из равенств (5.95) и (5.103) вытекает, что

$$|\mathcal{A}_{n,2}(\mathbf{I}_1, \mathbf{I}_2)| = |K|^{n|K|} \prod_{r=1}^{2} t_{\mathbf{I}_r} =$$

$$= |K|^{n|K|} \prod_{r=1}^{2} \prod_{j=1}^{n} \left(\sum_{h=0}^{|I_j^{(r)}|} (-1)^h \binom{|I_j^{(r)}|}{h} (|I_j^{(r)}| - h)^{|K|} \right) =$$

$$= \frac{|\mathcal{A}_{n,2}|}{|K|^{2n|K|}} \cdot \prod_{r=1}^{2} \prod_{j=1}^{n} \left(\sum_{h=0}^{|I_j^{(r)}|} (-1)^h \binom{|I_j^{(r)}|}{h} (|I_j^{(r)}| - h)^{|K|} \right). \qquad (5.105)$$

Из истинности равенств (5.104) и (5.105) вытекает, что для всех чисел $n \in \mathbb{N}$ истинны равенства (5.103).□

Теорема 5.5. Для каждых векторов $\mathbf{I}_r = (I_1^{(r)}, \ldots, I_n^{(r)})$ $(r = 1, 2)$, где $I_j^{(r)}$ $(r = 1, 2; j = 1, \ldots, n)$ – идеал кольца $\mathcal{K}$, равенства

$$|\mathcal{A}_{n,1}^{inv}(\mathbf{I}_1, \mathbf{I}_2)| =$$

$$= \frac{|\mathcal{A}_{n,1}^{inv}|}{|K|^{2n|K|}} \cdot \prod_{r=1}^{2} \prod_{j=1}^{n} \left(\sum_{h=0}^{|I_j^{(r)}|} (-1)^h \binom{|I_j^{(r)}|}{h} (|I_j^{(r)}| - h)^{|K|} \right) \qquad (5.106)$$

истинны для всех чисел $n \in \mathbb{N}$.□

Доказательство. Так как при построении автомата $M_1 \in \mathcal{A}_{n,1}^{inv}$ осуществляется независимый выбор отображений $\mathbf{f}_i$ $(i = 1, 2, 3, 4)$, то из равенств (5.97) и (5.103) вытекает, что

$$|\mathcal{A}_{n,1}^{inv}(\mathbf{I}_1, \mathbf{I}_2)| = (|K|!)^n K^{n|K|} \prod_{r=1}^{2} t_{\mathbf{I}_r} = \frac{(|K|!)^n K^{3n|K|}}{K^{2n|K|}} \prod_{r=1}^{2} t_{\mathbf{I}_r} =$$

$$= \frac{|\mathcal{A}_{n,1}^{inv}|}{K^{2n|K|}} \prod_{r=1}^{2} t_{\mathbf{I}_r} = \frac{|\mathcal{A}_{n,1}^{inv}|}{K^{2n|K|}} \prod_{r=1}^{2} \prod_{j=1}^{n} \left(\sum_{h=0}^{|I_j^{(r)}|} (-1)^h \binom{|I_j^{(r)}|}{h} (|I_j^{(r)}| - h)^{|K|} \right),$$

что и требовалось доказать.□

Теорема 5.6. Для каждого вектора $\mathbf{I}_1 = (I_1^{(1)}, \ldots, I_n^{(1)})$ $(r = 1, 2)$, где $I_j^{(1)}$ $(j = 1, \ldots, n)$ – идеал кольца $\mathcal{K}$, равенства

$$|\mathcal{A}_{n,2}^{inv}(\mathbf{I}_1)| = \frac{|\mathcal{A}_{n,2}^{inv}|}{|K|^{n|K|}} \prod_{j=1}^{n} \left(\sum_{h=0}^{|I_j^{(1)}|} (-1)^h \binom{|I_j^{(1)}|}{h} (|I_j^{(1)}| - h)^{|K|} \right) \qquad (5.107)$$

истинны для всех чисел $n \in \mathbb{N}$.□

Доказательство. Так как при построении автомата $M_2 \in \mathcal{A}_{n,2}^{inv}$ осуществляется независимый выбор отображений $\mathbf{f}_i$ $(i = 1, 2, 3)$, то из равенств (5.97) и (5.103) вытекает, что

$$|\mathcal{A}_{n,2}^{inv}(\mathbf{I}_1)| = (|K|!)^{2n} t_{\mathbf{I}_1} = \frac{(|K|!)^{2n} K^{n|K|}}{K^{n|K|}} t_{\mathbf{I}_1} = \frac{|\mathcal{A}_{n,1}^{inv}|}{K^{n|K|}} t_{\mathbf{I}_1} =$$

$$= \frac{|\mathcal{A}_{n,1}^{inv}|}{K^{n|K|}} \prod_{j=1}^{n} \left(\sum_{h=0}^{|I_j^{(1)}|} (-1)^h \binom{|I_j^{(1)}|}{h} (|I_j^{(1)}| - h)^{|K|} \right),$$

что и требовалось доказать.□

Из установленных выше оценок мощностей семейств автоматов $\mathcal{A}_{n,i}(\mathbf{I}_1, \mathbf{I}_2)$ $(i = 1, 2)$, $\mathcal{A}_{n,1}^{inv}(\mathbf{I}_1, \mathbf{I}_2)$ и $\mathcal{A}_{n,2}^{inv}(\mathbf{I}_1)$ вытекает, что исследуемые модели определяют достаточно обширные множества семейств автоматов, содержащие нетривиальные подмножества семейств обратимых автоматов. Это обстоятельство обосновывает актуальность исследования рассматриваемых семейств автоматов с теоретической и с прикладной точки зрения.

5.4.3. Структурные свойства исследуемых моделей.

Обозначим через $\mathbf{f}_{M,\mathbf{q}_0}$ $(M \in \mathcal{A}_{n,1}(\mathbf{I}_1,\mathbf{I}_2) \cup \mathcal{A}_{n,2}(\mathbf{I}_1,\mathbf{I}_2), \mathbf{q}_0 \in \mathbf{Q}_n)$ отображение входной полугруппы $\mathbf{X}_n^+$ в выходную полугруппу, реализуемое инициальным автоматом $(M,\mathbf{q}_0)$.

Состояния автомата называются близнецами, если по каждому входному символу они переходят в одно и то же состояние, а выходные символы, которые автомат выдает при этих переходах совпадают.

Из (5.88) и (5.89) вытекает, что:

1) множества состояний-близнецов автомата $M_1 \in \mathcal{A}_{n,1}(\mathbf{I}_1,\mathbf{I}_2)$ совпадают с элементами фактор-множества $\mathbf{Q}_n/_{\ker \mathbf{f}_1 \cap \ker \mathbf{f}_2}$;

2) множества состояний-близнецов автомата $M_2 \in \mathcal{A}_{n,2}(\mathbf{I}_1,\mathbf{I}_2)$ совпадают с элементами фактор-множества $\mathbf{Q}_n/_{\ker \mathbf{f}_1}$.

Отсюда вытекает, что мощность множества автоматных отображений

$$\mathbf{F}_M = \{\mathbf{f}_{M,\mathbf{q}_0} \mid \mathbf{q}_0 \in \mathbf{Q}_n\} \ (M \in \mathcal{A}_{n,1}(\mathbf{I}_1,\mathbf{I}_2) \cup \mathcal{A}_{n,2}(\mathbf{I}_1,\mathbf{I}_2)),$$

реализуемых автоматом M, удовлетворяет следующим неравенствам:

$$|\mathbf{F}_M| \le |\mathbf{Q}_n/_{\ker \mathbf{f}_1 \cap \ker \mathbf{f}_2}|, \tag{5.108}$$

если $M \in \mathcal{A}_{n,1}(\mathbf{I}_1,\mathbf{I}_2)$, и

$$|\mathbf{F}_M| \le |\mathbf{Q}_n/_{\ker \mathbf{f}_1}|, \tag{5.109}$$

если $M \in \mathcal{A}_{n,2}(\mathbf{I}_1,\mathbf{I}_2)$.

Из (5.91), (5.92), (5.108) и (5.109) вытекает, что

$$|\mathbf{F}_M| \le \min\{|\mathbf{Q}_n|, |\mathbf{I}_1| \cdot |\mathbf{I}_2|\},$$

если $M \in \mathcal{A}_{n,1}(\mathbf{I}_1,\mathbf{I}_2)$, и

$$|\mathbf{F}_M| \le |\mathbf{I}_1|,$$

если $M \in \mathcal{A}_{n,2}(\mathbf{I}_1,\mathbf{I}_2)$.

Охарактеризуем более подробно структуру множества отображений $\mathbf{F}_M$ $(M \in \mathcal{A}_{n,1}(\mathbf{I}_1,\mathbf{I}_2) \cup \mathcal{A}_{n,2}(\mathbf{I}_1,\mathbf{I}_2))$.

Рассмотрим автомат $M_1 \in \mathcal{A}_{n,1}(\mathbf{I}_1,\mathbf{I}_2)$.

Определим на входном алфавите $\mathbf{X}_n$ отношения эквивалентности $\sim_{n,1}$ и $\sim_{n,2}$ следующим образом: для всех $\mathbf{x}', \mathbf{x}'' \in \mathbf{X}_n$:

$$\mathbf{x}' \sim_{n,1} \mathbf{x}'' \Leftrightarrow \mathbf{f}_3(\mathbf{x}') \equiv \mathbf{f}_3(\mathbf{x}'') \ (mod\, \mathbf{I}_1) \tag{5.110}$$

и

$$\mathbf{x}' \sim_{n,2} \mathbf{x}'' \Leftrightarrow \mathbf{f}_4(\mathbf{x}') \equiv \mathbf{f}_4(\mathbf{x}'') \ (mod\, \mathbf{I}_2). \tag{5.111}$$

Из (5.110) и (5.111) вытекает, что

$$\ker \mathbf{f}_3 \subseteq \sim_{n,1} \tag{5.112}$$

и

$$\ker \mathbf{f}_4 \subseteq \sim_{n,2}, \tag{5.113}$$

Положим

$$\sim_{n,12} = \sim_{n,1} \cap \sim_{n,2}. \tag{5.114}$$

Замечание 5.19. Из (5.112)-(5.114) вытекает, что $\ker \mathbf{f}_3 \cap \ker \mathbf{f}_4 \subseteq \sim_{n,12}$.

Распространим отношения эквивалентности $\sim_{n,i}$ $(i = 1, 2)$ и $\sim_{n,12}$ на входную полугруппу $\mathbf{X}_n^+$ следующим образом: для каждого числа $k \in \mathbb{N}$ и для всех входных слов $\mathbf{u}' = \mathbf{x}'_1 \dots \mathbf{x}'_k \in \mathbf{X}_n^k$ и $\mathbf{u}'' = \mathbf{x}''_1 \dots \mathbf{x}''_k \in \mathbf{X}_n^k$

$$\mathbf{u}' \sim_{n,i} \mathbf{u}'' \Leftrightarrow (\forall 1 \leq j \leq k)(\mathbf{x}'_j \sim_{n,i} \mathbf{x}''_j) \ (i = 1, 2) \tag{5.115}$$

и

$$\mathbf{u}' \sim_{n,12} \mathbf{u}'' \Leftrightarrow (\forall 1 \leq j \leq k)(\mathbf{x}'_j \sim_{n,12} \mathbf{x}''_j). \tag{5.116}$$

Теорема 5.7. Пусть $n \in \mathbb{N}$ и $\mathbf{I}_r = (I_1^{(r)}, \dots, I_n^{(r)})$ $(r = 1, 2)$, где $I_j^{(r)}$ $(r = 1, 2; j = 1, \dots, n)$ – идеал кольца $\mathcal{K}$. Тогда для каждого автомата $M_1 \in \mathcal{A}_{n,1}(\mathbf{I}_1, \mathbf{I}_2)$ и каждого числа $k \in \mathbb{N}$ формула

$$\mathbf{u}' \sim_{n,12} \mathbf{u}'' \Leftrightarrow (\forall \mathbf{q}'_0, \mathbf{q}''_0 \in \mathbf{Q}_n)(\forall 1 \leq j \leq k)(\mathbf{q}'_j \equiv \mathbf{q}''_j \ (mod\, \mathbf{I}_1) \&$$

$$\& \mathbf{y}'_j \equiv \mathbf{y}''_j \ (mod\, \mathbf{I}_2)) \tag{5.117}$$

истинна для всех $\mathbf{u}' = \mathbf{x}'_1 \dots \mathbf{x}'_k \in \mathbf{X}_n^k$ и $\mathbf{u}'' = \mathbf{x}''_1 \dots \mathbf{x}''_k \in \mathbf{X}_n^k$.□

Доказательство. Пусть $\mathbf{u}' = \mathbf{x}'_1 \dots \mathbf{x}'_k \in \mathbf{X}_n^k$ и $\mathbf{u}'' = \mathbf{x}''_1 \dots \mathbf{x}''_k \in \mathbf{X}_n^k$.

Из 1-го рекуррентного соотношения системы рекуррентных соотношений (5.88) находим, что для всех чисел $j = 0, 1, \dots, k-1$

$$\mathbf{q}''_{j+1} - \mathbf{q}'_{j+1} = (\mathbf{f}_1(\mathbf{q}''_j) - \mathbf{f}_1(\mathbf{q}'_j)) + (\mathbf{f}_3(\mathbf{x}''_{j+1}) - \mathbf{f}_3(\mathbf{x}'_{j+1})). \tag{5.118}$$

Так как $\mathbf{f}_1(\mathbf{q}''_j) - \mathbf{f}_1(\mathbf{q}'_j) \in \mathbf{I}_1$ $(j = 0, 1, \dots, k-1)$ для всех $\mathbf{q}'_j, \mathbf{q}''_j \in \mathbf{Q}_n$, то из (5.110), (5.115) и (5.118) вытекает, что

$$(\forall \mathbf{q}'_0, \mathbf{q}''_0 \in \mathbf{Q}_n)(\forall 1 \leq j \leq k)(\mathbf{q}'_j \equiv \mathbf{q}''_j \ (mod\, \mathbf{I}_1)) \Leftrightarrow$$

$$\Leftrightarrow (\forall \mathbf{q}'_0, \mathbf{q}''_0 \in \mathbf{Q}_n)(\forall 1 \leq j \leq k)(\mathbf{f}_3(\mathbf{x}'_j) \equiv \mathbf{f}_3(\mathbf{x}''_j) \ (mod\, \mathbf{I}_1)) \Leftrightarrow$$

$$\Leftrightarrow \mathbf{u}' \sim_{n,1} \mathbf{u}''. \tag{5.119}$$

Аналогичным образом, из 2-го рекуррентного соотношения системы рекуррентных соотношений (5.88) находим, что для всех чисел $j = 0, 1, \ldots, k-1$

$$\mathbf{y}''_{j+1} - \mathbf{y}'_{j+1} = (\mathbf{f}_2(\mathbf{q}''_j) - \mathbf{f}_2(\mathbf{q}'_j)) + (\mathbf{f}_4(\mathbf{x}''_{j+1}) - \mathbf{f}_4(\mathbf{x}'_{j+1})). \tag{5.120}$$

Так как $\mathbf{f}_2(\mathbf{q}''_j) - \mathbf{f}_2(\mathbf{q}'_j) \in \mathbf{I}_1$ $(j = 0, 1, \ldots, k-1)$ для всех $\mathbf{q}'_j, \mathbf{q}''_j \in \mathbf{Q}_n$, то из (5.111), (5.115) и (5.120) вытекает, что

$$(\forall \mathbf{q}'_0, \mathbf{q}''_0 \in \mathbf{Q}_n)(\forall 1 \le j \le k)(\mathbf{y}'_j \equiv \mathbf{y}''_j \,(mod\, \mathbf{I}_2)) \Leftrightarrow$$

$$\Leftrightarrow (\forall \mathbf{q}'_0, \mathbf{q}''_0 \in \mathbf{Q}_n)(\forall 1 \le j \le k)(\mathbf{f}_4(\mathbf{x}'_j) \equiv \mathbf{f}_4(\mathbf{x}''_j) \,(mod\, \mathbf{I}_2)) \Leftrightarrow$$

$$\Leftrightarrow \mathbf{u}' \sim_{n,2} \mathbf{u}''. \tag{5.121}$$

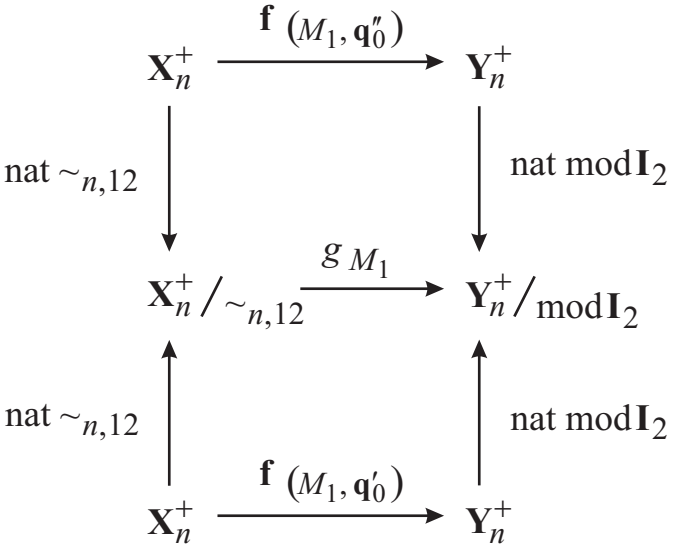
Из (5.114), (5.119) и (5.121) вытекает, что формула (5.117) истинна.□

Обозначим через $\mathbf{Y}_n^+ /_{mod\, \mathbf{I}_2}$ фактор-множество множества $\mathbf{Y}^+$, определенное следующим образом: для каждого числа $k \in \mathbb{N}$ и всех выходных слов $\mathbf{v}' = \mathbf{y}'_1 \ldots \mathbf{y}'_k \in \mathbf{Y}_n^k$ и $\mathbf{v}'' = \mathbf{y}''_1 \ldots \mathbf{y}''_k \in \mathbf{Y}_n^k$

$$\mathbf{v}' \equiv \mathbf{v}'' \,(mod\, \mathbf{I}_2) \Leftrightarrow (\forall 1 \le j \le k)(\mathbf{y}'_j \equiv \mathbf{y}''_j \,(mod\, \mathbf{I}_2)).$$

Из теоремы 5.7 вытекает, что истинно следующее следствие.

Следствие 5.5. Пусть $n \in \mathbb{N}$ и $\mathbf{I}_r = (I_1^{(r)}, \ldots, I_n^{(r)})$ $(r = 1, 2)$, где $I_j^{(r)}$ $(r = 1, 2; j = 1, \ldots, n)$ – идеал кольца $\mathcal{K}$. Тогда для каждого автомата $M_1 \in \mathcal{A}_{n,1}(\mathbf{I}_1, \mathbf{I}_2)$ и любых его начальных состояний $\mathbf{q}'_0, \mathbf{q}''_0 \in \mathbf{Q}_n$ истинна диаграмма



где отображение g_{M_1} определяется автоматом M_1.□

Таким образом, для каждого автомата $M_1 \in \mathcal{A}_{n,1}(\mathbf{I}_1, \mathbf{I}_2)$ при любых его начальных состояниях $\mathbf{q}'_0, \mathbf{q}''_0 \in \mathbf{Q}_n$ отображения $\mathbf{f}_{(M_1,\mathbf{q}'_0)}$ и $\mathbf{f}_{(M_1,\mathbf{q}''_0)}$ реализуют одно и то же отображение g_{M_1} фактор-множества $\mathbf{X}_n^+/_{\sim_{n,12}}$ в фактор-множество $\mathbf{Y}_n^+/_{mod\,\mathbf{I}_2}$.

Рассмотрим автомат $M_2 \in \mathcal{A}_{n,1}(\mathbf{I}_1, \mathbf{I}_2)$.

Определим на множестве $\mathbf{X}_n^+$ отношение эквивалентности $\sim'_{n,1}$ следующим образом: для каждого числа $k \in \mathbb{N}$ и для всех входных слов $\mathbf{u}' = \mathbf{x}'_1 \dots \mathbf{x}'_k \in \mathbf{X}_n^k$ и $\mathbf{u}'' = \mathbf{x}''_1 \dots \mathbf{x}''_k \in \mathbf{X}_n^k$

$$\mathbf{u}' \sim'_{n,1} \mathbf{u}'' \Leftrightarrow \mathbf{u}' \sim_{n,1} \mathbf{u}'' \&$$

$$\&(\forall \mathbf{q}'_0, \mathbf{q}''_0 \in \mathbf{Q}_n)(\forall 1 \le j \le k)(\mathbf{q}'_j \equiv \mathbf{q}''_j \,(\ker \mathbf{f}_2)), \tag{5.122}$$

где $\sim_{n,1}$ – отношение эквивалентности на множестве $\mathbf{X}_n^+$, определенное в соответствии с формулами (5.110) и (5.115).

Теорема 5.8. Пусть $n \in \mathbb{N}$ и $\mathbf{I}_r = (I_1^{(r)}, \dots, I_n^{(r)})$ $(r = 1, 2)$, где $I_j^{(r)}$ $(r = 1, 2; j = 1, \dots, n)$ – идеал кольца $\mathcal{K}$. Тогда для каждого автомата $M_2 \in \mathcal{A}_{n,2}(\mathbf{I}_1, \mathbf{I}_2)$ и каждого числа $k \in \mathbb{N}$ формула

$$\mathbf{u}' \sim'_{n,1} \mathbf{u}'' \Leftrightarrow (\forall \mathbf{q}'_0, \mathbf{q}''_0 \in \mathbf{Q}_n)(\forall 1 \le j \le k)(\mathbf{q}'_j \equiv \mathbf{q}''_j \,(mod\,\mathbf{I}_1) \&$$

$$\&\mathbf{y}'_j = \mathbf{y}''_j) \tag{5.123}$$

истинна для всех $\mathbf{u}' = \mathbf{x}'_1 \dots \mathbf{x}'_k \in \mathbf{X}_n^k$ и $\mathbf{u}'' = \mathbf{x}''_1 \dots \mathbf{x}''_k \in \mathbf{X}_n^k$.□

Доказательство. В системах рекуррентных соотношений (5.88) и (5.89) первые рекуррентные соотношения совпадают. Поэтому из формул (5.119) и (5.122) вытекает, что

$$\mathbf{u}' \sim'_{n,1} \mathbf{u}'' \Leftrightarrow (\forall \mathbf{q}'_0, \mathbf{q}''_0 \in \mathbf{Q}_n)(\forall 1 \le j \le k)(\mathbf{q}'_j \equiv \mathbf{q}''_j \,(mod\,\mathbf{I}_1)) \&$$

$$\&(\forall \mathbf{q}'_0, \mathbf{q}''_0 \in \mathbf{Q}_n)(\forall 1 \le j \le k)(\mathbf{q}'_j \equiv \mathbf{q}''_j \,(\ker \mathbf{f}_2)) \Leftrightarrow$$

$$\Leftrightarrow (\forall \mathbf{q}'_0, \mathbf{q}''_0 \in \mathbf{Q}_n)(\forall 1 \le j \le k)(\mathbf{q}'_j \equiv \mathbf{q}''_j \,(mod\,\mathbf{I}_1)) \&$$

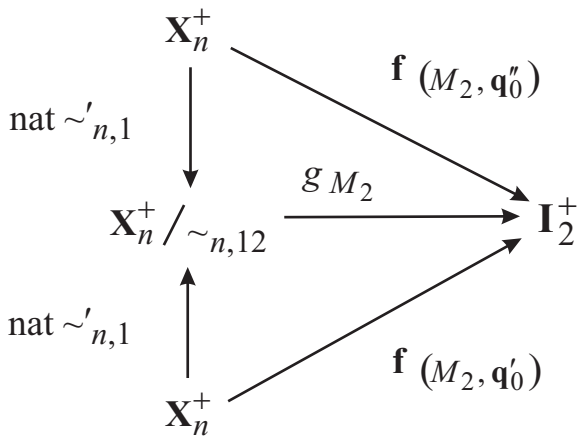
$$\&(\forall \mathbf{q}'_0, \mathbf{q}''_0 \in \mathbf{Q}_n)(\forall 1 \le j \le k)(\mathbf{y}'_j = \mathbf{y}''_j) \Leftrightarrow$$

$$\Leftrightarrow (\forall \mathbf{q}'_0, \mathbf{q}''_0 \in \mathbf{Q}_n)(\forall 1 \le j \le k)(\mathbf{q}'_j \equiv \mathbf{q}''_j \,(mod\,\mathbf{I}_1) \& \mathbf{y}'_j = \mathbf{y}''_j),$$

что и требовалось доказать.□

Из теоремы 5.8 вытекает, что истинно следующее следствие.

Следствие 5.6. Пусть $n \in \mathbb{N}$ и $\mathbf{I}_r = (I_1^{(r)}, \dots, I_n^{(r)})$ $(r = 1, 2)$, где $I_j^{(r)}$ $(r = 1, 2; j = 1, \dots, n)$ – идеал кольца $\mathcal{K}$. Тогда для каждого автомата $M_2 \in \mathcal{A}_{n,2}(\mathbf{I}_1, \mathbf{I}_2)$ и любых его начальных состояний $\mathbf{q}'_0, \mathbf{q}''_0 \in \mathbf{Q}_n$ истинна диаграмма



где отображение g_{M_2} определяется автоматом M_2.$\square$

Таким образом, для каждого автомата $M_2 \in \mathcal{A}_{n,2}(\mathbf{I}_1, \mathbf{I}_2)$ при любых его начальных состояниях $\mathbf{q}_0', \mathbf{q}_0'' \in \mathbf{Q}_n$ отображения $\mathbf{f}_{(M_2,\mathbf{q}_0')}$ и $\mathbf{f}_{(M_2,\mathbf{q}_0'')}$ реализуют одно и то же отображение g_{M_1} фактор-множества $\mathbf{X}_n^+/_{\sim'_{n,1}}$ в множество $\mathbf{I}_2^+$.

5.5. Выводы.

В настоящем разделе исследованы семейства автоматов Мили и Мура, заданные системами рекуррентных соотношений с параметрами над конечным кольцом. Основные результаты состоят в следующем:

1. Разработан математический аппарат, предназначенный для построения имитационной модели семейства автоматов, заданного системой рекуррентных соотношений над конечным кольцом.

2. Для всех комбинаций понятий «в наихудшем случае» и «в среднем», представляющих интерес с позиции прикладной теории алгоритмов, определено понятие «точность имитационной модели» семейства автоматов, заданного системой рекуррентных соотношений над конечным кольцом.

3. Выделено множество асимптотически точных имитационных моделей семейства автоматов, заданного системой рекуррентных соотношений над конечным кольцом, представляющих, по своей сути, формируемый в процессе обучения автомат с конечной памятью.

4. Построены семейства хэш-функций, реализуемые сильно-связными автоматами без выхода, определенными системой рекуррентных соотношений над конечным кольцом.

5. Исследована вычислительная стойкость семейств хэш-функций, реализуемых сильно-связными автоматами без выхода, определенными си-

стемой рекуррентных соотношений над конечным кольцом.

6. С позиции универсальной алгебры исследованы автоматы над конечным кольцом, для которых функции переходов и выходов являются алгебраическими суммами функции от состояния автомата и функции от входного символа при условии, что значение каждой компоненты функции переходов принадлежит фиксированным идеалам кольца.

В своей совокупности полученные в настоящем разделе результаты представляют собой фрагмент теории, которая может быть использована при разработке программных систем, предназначенных для построения и анализа автоматных моделей, применяемых в процессе решения задач защиты информации.

Возможных следующие направления дальнейших исследований.

Во-первых, это выделение нетривиальных классов семейств автоматов над конечным кольцом, для которых любая ν-точная имитационная модель при всех значениях числа ν, достаточно близких к единице, существенно сложнее, чем система рекуррентных соотношений, определяющая семейство автоматов.

Во-вторых, это детальный анализ свойств семейства хэш-функций, определяемого рекуррентными соотношениями того или иного вида над ассоциативно-коммутативными и матричными кольцами.

В-третьих, это детальный анализ для конкретных типов конечных колец при наличии тех или иных соотношений между векторами идеалов $\mathbf{I}_1$ и $\mathbf{I}_2$ свойств автоматов, функции переходов и выходов которых являются алгебраическими суммами функции от состояния автомата и функции от входного символа при условии, что значение каждой компоненты функции переходов принадлежит фиксированным идеалам кольца.

6. АВТОМАТЫ НА МНОГООБРАЗИИ НАД КОНЕЧНЫМ КОЛЬЦОМ

Понятие «многообразие» является одним из основных понятий алгебраической геометрии [24.34,59,111,112], которая детально проработана над алгебраически замкнутыми полями. Последние, как известно, являются бесконечными полями.

Специальным видом многообразия являются алгебраические кривые. Среди них важную роль играют эллиптические кривые [32,46-48,128,129,207], имеющие многочисленные применения при решении теоретических и прикладных задач. Успешные применения эллиптических кривых над конечными полями в процессе решения задач защиты информации привели к формированию эллиптической криптографии [10,12,14,110] – одного из наиболее перспективных в настоящее время разделов современной криптографии.

Кроме того, в последнее время при решении задач защиты информации фрагментарно начинают использоваться вычисления над кольцами вычетов.

Все сказанное выше обосновывает актуальность, как с теоретической, так и с прикладной точки зрения, исследования свойств автоматных моделей, определенных на многообразиях над конечными кольцами. Решению этой задачи и посвящен настоящий раздел.

В п.6.1 исследовано строение алгебраических кривых 2-го и 3-го порядков над конечным ассоциативно-коммутативным кольцом. Найдены множества разложимых линий. Охарактеризованы множества особых точек исследуемых линий. Исследуются методы приведения линии 2-го порядка к каноническому виду. Установлены условия существования кратных корней для некоторых линий 3-го порядка. В п.6.2 выделены 2 типа многообразий над произвольным конечным кольцом: многообразия с алгеброй и параметризованные многообразия. В п.6.3 исследуются автоматы Мили и Мура, определенные на многообразии с алгеброй, а в п.6.4 – автоматы Мили и Мура, определенные на параметризованном многообразии. Установлены автоматные характеристики исследуемых моделей. Охарактеризованы гомоморфизмы исследуемых моделей в терминах гомоморфизмов рассматриваемых многообразий. В п.6.5 исследованы множества автоматов Мили и Мура, определенные на группах точек эллиптических кривых над конечным полем. Охарактеризованы множества групповых и приведенных автоматов, а также множества эквивалентных состояний не приведенных автоматов. Найдены достаточные условия, при которых автомат не является сильно связным. Решены задача идентификации начального состояния автомата, а также задача построения точной асимптотически имитационной модели автомата. П.6.6 содержит ряд заключительных замечаний.

Результаты автора, представленные в настоящем разделе, опубликованы в работах [76,77,80,85,90,92-94,97,98,100,102,212,213].

6.1. Кривые 2-го и 3-го порядков над конечным кольцом.

Простейшими нелинейными многообразиями над кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$ являются кривые линии 2-го и 3-го порядков, определенные уравнением над этим кольцом. Исследуем строение таких кривых в предположении, что $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}_1^{fnt} \cup \mathfrak{K}_2^{fnt}$.

6.1.1. Анализ кривых 2-го порядка.

Общее уравнение кривой 2-го порядка Γ над кольцом $\mathcal{K}$ имеет вид

$$a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0 = 0, \tag{6.1}$$

где $a_{11}, a_{12}, a_{22}, a_1, a_2, a_0 \in K$, причем $(a_{11}, a_{12}, a_{22}) \neq (0, 0, 0)$.

Для многочлена $f(x, y) = a_{11}x^2+a_{12}xy+a_{22}y^2+a_1x+a_2y+a_0$ возможны следующие три ситуации.

Ситуация 6.1. Многочлен $f(x, y)$ неразложим над кольцом $\mathcal{K}$.

Ситуация 6.2. Для любых многочленов $f_i \in \mathcal{K}[x, y]$ $(i = 1, 2)$ степени $m_i \geq 1$ $(i = 1, 2)$, удовлетворяющих равенству $f(x, y) = f_1(x, y)f_2(x, y)$, истинно неравенство $m_1 + m_2 > 2$.

Ситуация 6.3. Существуют многочлены $f_i \in \mathcal{K}[x, y]$ $(i = 1, 2)$ степени $m_i = 1$ $(i = 1, 2)$, удовлетворяющие равенству $f(x, y) = f_1(x, y)f_2(x, y)$.

Предположим, что имеет место ситуация 6.2. Тогда $f(x, y)$ – многочлен наименьшей степени, определяющий кривую 2-го порядка Γ. Анализ кривой Γ осуществляется непосредственно на основе уравнения (6.1).

Предположим, что имеет место ситуация 6.3. При известном разложении многочлена $f(x, y)$ уравнение (6.1) естественно представить в виде

$$(b_1x + b_2y + b_0)(c_1x + c_2y + c_0) = 0. \tag{6.2}$$

Из (6.2) вытекает, что множество точек кривой Γ может быть представлено в виде

$$\Gamma = S_1 \cup S_2 \cup S_3,$$

где S_1 – объединение множеств решений одно-параметрического семейства систем линейных уравнений

$$\mathtt{A}_\alpha : \begin{cases} b_1x + b_2y + b_0 = 0 \\ c_1x + c_2y + c_0 = \alpha \end{cases} \qquad (\alpha \in K),$$

S_2 – объединение множеств решений одно-параметрического семейства систем линейных уравнений

$$\mathtt{B}_\beta : \begin{cases} b_1x + b_2y + b_0 = \beta \\ c_1x + c_2y + c_0 = 0 \end{cases} \qquad (\beta \in K\backslash\{0\}),$$

а S_3 – объединение множеств решений двух-параметрического семейства систем линейных уравнений

$$\mathtt{C}_{\alpha,\beta} : \begin{cases} b_1x + b_2y + b_0 = \alpha \\ c_1x + c_2y + c_0 = \beta \end{cases} \qquad (\alpha, \beta \in K\backslash\{0\}, \alpha\beta = 0).$$

Замечание 6.1. Таким образом, построение в явном виде множества точек кривой 2-го порядка Γ в ситуациях 6.1 и 6.2 эквивалентно поиску множества решений нелинейного уравнения (6.1) от двух переменных, а в ситуации 6.3 – поиску множеств решений трех семейств $\mathtt{A}_\alpha$ ($\alpha \in K$), $\mathtt{B}_\beta$ ($\beta \in K\backslash\{0\}$) и $\mathtt{C}_{\alpha,\beta}$ ($\alpha, \beta \in K\backslash\{0\}, \alpha\beta = 0$) систем линейных уравнений. Если кольцо $\mathcal{K}$ не содержит делителей нуля, то $S_3 = \emptyset$.

Охарактеризуем особые точки кривой (6.1).

Множеством особых точек кривой (6.1) является множество решений системы уравнений

$$\begin{cases} \mathsf{D}_x(a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0) = 0 \\ \mathsf{D}_y(a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0) = 0 \\ a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0 = 0 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} 2a_{11}x + a_{12}y + a_1 = 0 \\ a_{12}x + 2a_{22}y + a_2 = 0 \\ a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0 = 0 \end{cases}.$$

Отсюда вытекает, что истинно следующее утверждение.

Утверждение 6.1. Кривая Γ, определенная уравнением (6.1), имеет особые точки тогда и только тогда, когда существует такое решение (x_0, y_0) системы линейных уравнений

$$\begin{cases} 2a_{11}x + a_{12}y = -a_1 \\ a_{12}x + 2a_{22}y = -a_2 \end{cases}, \tag{6.3}$$

что (x_0, y_0) – точка кривой Γ.$\square$

Замечание 6.2. Иными словами, когда для решения (x_0, y_0) системы линейных уравнений (6.3) истинно равенство $a_{11}x_0^2 + a_{12}x_0y_0 + a_{22}y_0^2 + a_1x_0 + a_2y_0 + a_0 = 0$.

Если характеристика кольца $\mathcal{K}$ равна 2, то система уравнений (6.3) принимает вид

$$\begin{cases} a_{12}y = -a_1 \\ a_{12}x = -a_2 \end{cases}.$$

Отсюда вытекает, что истинно следующее утверждение.

Утверждение 6.2. Пусть характеристика кольца $\mathcal{K}$ равна 2. Тогда кривая Γ, определенная уравнением (6.1):

1) имеет единственную особую точку, если $a_{12} \in K^{inv}$ и

$$a_{11}a_2^2 + a_{12}a_1a_2 + a_{22}a_1^2 + a_0a_{12}^2 = 0;$$

2) является гладкой кривой, если либо $a_{12} \in K^{inv}$ и

$$a_{11}a_2^2 + a_{12}a_1a_2 + a_{22}a_1^2 + a_0a_{12}^2 \neq 0,$$

либо $a_{12} \notin K^{inv}$ и, кроме того, $a_1 \in K^{inv}$ или $a_2 \in K^{inv}$.□

Охарактеризуем множество точек кривой (6.1).

1. Пусть

$$\begin{cases} a_{3-i,3-i} \neq 0 \\ a_{ii} = a_{12} = a_i = 0 \end{cases}. \tag{6.4}$$

где либо $i = 1$, либо $i = 2$.

Если (6.4) истинно при $i = 1$, то уравнение (6.1) принимает вид

$$a_{22}y^2 + a_2y + a_0 = 0, \tag{6.5}$$

а если при $i = 2$, то уравнение (6.1) принимает вид

$$a_{11}x^2 + a_1x + a_0 = 0. \tag{6.6}$$

Следовательно, кривая Γ состоит из всех таких точек $(x_0, y_0) \in K^2$, что при $i = 1$ (соответственно, при $i = 2$) элемент y_0 (соответственно, элемент x_0) – корень уравнения (6.5) (соответственно, уравнения (6.6)) над кольцом $\mathcal{K}$. В частности, если уравнение (6.5) (соответственно, уравнение (6.6)) не имеет решений над кольцом $\mathcal{K}$, то $\Gamma = \emptyset$.

2. Пусть

$$\begin{cases} a_{3-i,3-i} \neq 0 \\ a_{ii} = a_{12} = 0 \\ a_i \neq 0 \end{cases}. \tag{6.7}$$

где либо $i = 1$, либо $i = 2$.

Если (6.7) истинно при $i = 1$, то имеет место следующая теорема.

Теорема 6.1. Если характеристика кольца $\mathcal{K}$ отлична от 2, $a_1 \neq 0$, $a_{22} \neq 0$, $a_{11} = a_{12} = 0$ и существуют такие элементы $b, c \in K\backslash\{0\}$, что

$$\begin{cases} a_{22} = cb^2 \\ a_2 = 2cb \end{cases}, \tag{6.8}$$

то кривая Γ, определенная уравнением (6.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что $(w_0, u_0) = (by_0 + 1, x_0)$ является корнем уравнения

$$cw^2 + a_1u + (a_0 - c) = 0 \tag{6.9}$$

над кольцом $\mathcal{K}$.□

Доказательство. Пусть характеристика кольца $\mathcal{K}$ отлична от 2.

Если $a_1 \neq 0$, $a_{22} \neq 0$, $a_{11} = a_{12} = 0$, то уравнение (6.1) принимает вид

$$a_{22}y^2 + a_1x + a_2y + a_0 = 0. \tag{6.10}$$

Подставив (6.8) в (6.10), получим

$$c(by + 1)^2 + a_1x + (a_0 - c) = 0. \tag{6.11}$$

Положив $w = by + 1$ и $u = x$ в (6.11), получим уравнение (6.9).

Отсюда вытекает, что $(x_0, y_0) \in \Gamma$ тогда и только тогда, когда $(w_0, u_0) = (by_0 + 1, x_0)$ – корень уравнения (6.9) над кольцом $\mathcal{K}$.□

Если (6.7) истинно при $i = 2$, то имеет место следующая теорема.

Теорема 6.2. Если характеристика кольца $\mathcal{K}$ отлична от 2, $a_2 \neq 0$, $a_{11} \neq 0$, $a_{11} = a_{12} = 0$ и существуют такие элементы $b, c \in K\backslash\{0\}$, что $a_{11} = cb^2$ и $a_1 = 2cb$, то кривая Γ, определенная уравнением (6.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что $(w_0, u_0) = (bx_0 + 1, y_0)$ является корнем уравнения $cw^2 + a_1u + (a_0 - c) = 0$ над кольцом $\mathcal{K}$.□

Доказательство теоремы 6.2 аналогично доказательству теоремы 6.1.

3. Пусть $a_{11} = a_{22} = 0$ и $a_{12} \neq 0$. Имеет место следующая теорема.

Теорема 6.3. Пусть $a_{11} = a_{22} = 0$ и $a_{12} \neq 0$. Тогда:

1) если $a_1 = a_2 = 0$, то кривая Γ, определенная уравнением (6.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что (x_0, y_0) – корень уравнения

$$a_{12}xy + a_0 = 0 \tag{6.12}$$

над кольцом $\mathcal{K}$;

2) если $a_2 \neq 0$ и существует такой элемент $c \in K\backslash\{0\}$, что $a_2 = ca_{12}$, то кривая Γ, определенная уравнением (6.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что $(u_0, v_0) = (a_{12}y_0 + a_1, x_0 + c)$ является корнем уравнения

$$uv + (a_0 - ca_1) = 0 \tag{6.13}$$

над кольцом $\mathcal{K}$;

3) если $a_1 \neq 0$ и существует такой элемент $c \in K\backslash\{0\}$, что $a_1 = ca_{12}$, то кривая Γ, определенная уравнением (6.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что $(u_0, v_0) = (a_{12}x_0 + a_2, y_0 + c)$ является корнем уравнения

$$uv + (a_0 - ca_2) = 0 \tag{6.14}$$

над кольцом $\mathcal{K}$.□

Доказательство. Если $a_{11} = a_{22} = 0$ и $a_{12} \neq 0$, то уравнение (6.1) принимает вид

$$a_{12}xy + a_1x + a_2y + a_0 = 0. \tag{6.15}$$

Если $a_1 = a_2 = 0$, то уравнение (6.15) совпадает с уравнением (6.12). Отсюда вытекает, что кривая Γ, определенная уравнением (6.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что (x_0, y_0) – корень уравнения (6.12) над кольцом $\mathcal{K}$, что и требовалось доказать.

Пусть $a_2 \neq 0$ и существует такой элемент $c \in K\backslash\{0\}$, что $a_2 = ca_{12}$. Тогда

$$a_{12}xy + a_1x + a_2y + a_0 = x(a_{12}y + a_1) + ca_{12}y + a_0 =$$

$$= x(a_{12}y + a_1) + c(a_{12}y + a_1) + (a_0 - ca_1) = (a_{12}y + a_1)(x + c) + (a_0 - ca_1).$$

Следовательно, уравнение (6.15) принимает вид

$$(a_{12}y + a_1)(x + c) + (a_0 - ca_1) = 0. \tag{6.16}$$

Положив $u = a_{12}y + a_1$ и $v = x + c$ в (6.16), получим уравнение (6.13).

Отсюда вытекает, что кривая Γ, определенная уравнением (6.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что $(u_0, v_0) = (a_{12}y_0 + a_1, x_0 + c)$ – корень уравнения (6.13) над кольцом $\mathcal{K}$, что и требовалось доказать.

Пусть $a_1 \neq 0$ и существует такой элемент $c \in K\backslash\{0\}$, что $a_1 = ca_{12}$. Тогда

$$a_{12}xy + a_1x + a_2y + a_0 = y(a_{12}x + a_2) + ca_{12}x + a_0 =$$

$$= y(a_{12}x + a_2) + c(a_{12}x + a_2) + (a_0 - ca_2) =$$

$$= (a_{12}x + a_2)(y + c) + (a_0 - ca_2).$$

Отсюда вытекает, что уравнение (6.15) принимает вид

$$(a_{12}x + a_2)(y + c) + (a_0 - ca_2) = 0. \tag{6.17}$$

Положив $u = a_{12}x + a_2$ и $v = y + c$ в (6.17), получим уравнение (6.14).

Следовательно, кривая Γ, определенная уравнением (6.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что $(u_0, v_0) = (a_{12}x_0 + a_2, y_0 + c)$ – корень уравнения (6.14) над кольцом $\mathcal{K}$, что и требовалось доказать.□

4. Пусть

$$\begin{cases} a_{ii} \neq 0 \ (i = 1, 2) \\ a_j \neq 0 \ (j = 1, 2) \end{cases}.$$

Имеет место следующая теорема.

Теорема 6.4. Пусть характеристика кольца $\mathcal{K}$ отлична от 2. Если $a_{ii} \neq 0$ $(i = 1, 2)$, $a_j \neq 0$ $(j = 1, 2)$ и существуют такие элементы $b_1, b_2, c, d \in K \backslash \{0\}$, что

$$\begin{cases} a_{11} = cb_1^2 \\ a_{12} = 2cb_1b_2 \\ a_{22} = cb_2^2 \\ a_1 = db_1 \\ a_2 = db_2 \end{cases}, \tag{6.18}$$

то кривая Γ, определенная уравнением (6.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что $w_0 = b_1x_0 + b_2y_0$ является корнем уравнения

$$cw^2 + dw + a_0 = 0 \tag{6.19}$$

над кольцом $\mathcal{K}$.□

Доказательство. Пусть характеристика кольца $\mathcal{K}$ отлична от 2, $a_{ii} \neq 0$ $(i = 1, 2)$ и $a_j \neq 0$ $(j = 1, 2)$.

Подставив (6.18) в (6.1), получим

$$a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0 = 0 \Leftrightarrow$$

$$\Leftrightarrow cb_1^2x^2 + 2cb_1b_2xy + cb_2^2y^2 + db_1x + db_2y + a_0 = 0 \Leftrightarrow$$

$$\Leftrightarrow c(b_1^2x^2 + 2b_1b_2xy + b_2^2y^2) + d(b_1x + b_2y) + a_0 = 0 \Leftrightarrow$$

$$\Leftrightarrow c(b_1x + b_2y)^2 + d(b_1x + b_2y) + a_0 = 0. \tag{6.20}$$

Положив $w = b_1x + b_2y$ в (6.20), получим уравнение (6.19).

Отсюда вытекает, что кривая Γ, определенная уравнением (6.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что $w_0 = b_1x_0 + b_2y_0$ – корень уравнения (6.19) над кольцом $\mathcal{K}$.□

5. Пусть

$$\begin{cases} a_{ii} \neq 0 \\ a_{3-i,3-i} = 0 \\ a_{12} \neq 0 \end{cases}, \tag{6.21}$$

где либо $i = 1$, либо $i = 2$.

Если (6.21) истинно при $i = 1$, то уравнение (6.1) принимает вид

$$x(a_{11}x + a_{12}y) + a_1x + a_2y + a_0 = 0, \tag{6.22}$$

а если при $i = 2$, то уравнение (6.1) принимает вид

$$y(a_{22}y + a_{12}x) + a_1x + a_2y + a_0 = 0. \tag{6.23}$$

Следовательно, если (6.21) истинно при $i = 1$ (соответственно, при $i = 2$), то кривая Γ, определенная уравнением (6.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что (x_0, y_0) – корень уравнения (6.22) (соответственно, уравнения (6.23)) над кольцом $\mathcal{K}$. В частности, если уравнение (6.22) (соответственно, уравнение (6.23)) не имеет решений над кольцом $\mathcal{K}$, то $\Gamma = \emptyset$.

6. Пусть $a_{ii} \neq 0$ $(i = 1, 2)$ и либо $a_1 = 0$, либо $a_2 = 0$.

Если $a_1 = 0$, то уравнение (6.1) принимает вид

$$x(a_{11}x + a_{12}y) + a_{22}y^2 + a_2y + a_0 = 0, \tag{6.24}$$

а если $a_2 = 0$, то уравнение (6.1) принимает вид

$$y(a_{22}y + a_{12}x) + a_{11}x^2 + a_1x + a_0 = 0. \tag{6.25}$$

Пусть характеристика кольца $\mathcal{K}$ отлична от 2.

Если существуют такие элементы $b, c, d \in K$, что $a_{22} = db^2$, $a_2 = 2dbc$ и $a_0 = dc^2$, то уравнение (6.24) принимает вид

$$x(a_{11}x + a_{12}y) + d(by + c)^2 = 0, \tag{6.26}$$

а если же существуют такие элементы $b, c, d \in K$, что $a_{11} = db^2$, $a_1 = 2dbc$ и $a_0 = dc^2$, то уравнение (6.25) принимает вид

$$y(a_{22}y + a_{12}x) + d(bx + c)^2 = 0. \tag{6.27}$$

Отсюда вытекает, что если $a_{ii} \neq 0$ $(i = 1, 2)$ и $a_1 = 0$ (соответственно, $a_2 = 0$), то кривая Γ, определенная уравнением (6.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что (x_0, y_0) – корень уравнения (6.26) (соответственно, уравнения (6.27)) над кольцом $\mathcal{K}$.

Построим канонические формы кривых 2-го порядка над кольцом $\mathcal{K}$.

Рассмотрим линейное преобразование

$$\begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} u \\ v \end{pmatrix}, \tag{6.28}$$

где

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}. \tag{6.29}$$

Подставив (6.29) в (6.28) и выполнив действия, получим

$$\begin{cases} x = \alpha_{11}u + \alpha_{12}v \\ y = \alpha_{21}u + \alpha_{22}v \end{cases}. \tag{6.30}$$

Будем говорить,что линейная форма $h(x, y) = a_1x + a_2y$ аннулируется в результате применения линейного преобразования (6.30) тогда и только тогда, когда $h(\alpha_{11}u + \alpha_{12}v, \alpha_{21}u + \alpha_{22}v) = 0u + 0v$.

Лемма 6.1. Линейная форма

$$h(x, y) = a_1x + a_2y \tag{6.31}$$

над кольцом $\mathcal{K}$ аннулируется в результате применения линейного преобразования (6.30) тогда и только тогда, когда равенства

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \end{cases}. \tag{6.32}$$

истинны кольцом $\mathcal{K}$.□

Доказательство. Подставив (6.30) в (6.31), получим

$$h(\alpha_{11}u + \alpha_{12}v, \alpha_{21}u + \alpha_{22}v) = a_1(\alpha_{11}u + \alpha_{12}v) + a_2(\alpha_{21}u + \alpha_{22}v) =$$

$$= (a_1\alpha_{11} + a_2\alpha_{21})u + (a_1\alpha_{12} + a_2\alpha_{22})v. \tag{6.33}$$

Из (6.33) вытекает, что равенство $h(\alpha_{11}u+\alpha_{12}v, \alpha_{21}u+\alpha_{22}v) = 0u+0v$ истинно тогда и только тогда, когда истинны равенства (6.32).□

Следствие 6.1. Если $a_1 \in K^{inv}$ или $a_2 \in K^{inv}$, то любое линейное преобразование (6.30), аннулирующее линейную форму (6.31), является необратимым линейным преобразованием над кольцом $\mathcal{K}$.□

Доказательство. Пусть линейное преобразование (6.30) аннулирует линейную форму (6.31).

Предположим, что $a_1 \in K^{inv}$. Тогда

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \end{cases} \Leftrightarrow \begin{cases} \alpha_{11} = -a_1^{-1}a_2\alpha_{21} \\ \alpha_{12} = -a_1^{-1}a_2\alpha_{22} \end{cases}.$$

Следовательно,

$$\det(A) = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21} = -a_1^{-1}a_2\alpha_{21}\alpha_{22} + a_1^{-1}a_2\alpha_{22}\alpha_{21} = 0,$$

откуда вытекает, что линейное преобразование (6.30), аннулирующее линейную форму (6.31), является необратимым над кольцом $\mathcal{K}$.

В случае, когда $a_2 \in K^{inv}$, доказательство осуществляется аналогичным образом.□

Выясним, к какому виду в результате применения линейного преобразования (6.30) может быть приведена квадратичная форма

$$f(x, y) = a_{11}x^2 + a_{12}xy + a_{22}y^2, \tag{6.34}$$

где $a_{11}, a_{12}, a_{22} \in K$ $((a_{11}, a_{12}, a_{22}) \neq (0, 0, 0))$.

Теорема 6.5. Над кольцом $\mathcal{K}$ в результате линейного преобразования (6.30) квадратичная форма (6.34) может быть приведена к виду

$$g(u, v) = b_{11}u^2 + b_{22}v^2 \tag{6.35}$$

тогда и только тогда, когда существуют такие $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in K$, что

$$2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0. \tag{6.36}$$

При этом коэффициенты b_{11} и b_{22} определяются равенствами

$$b_{11} = a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2 \tag{6.37}$$

и

$$b_{22} = a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2. \tag{6.38}$$

над кольцом $\mathcal{K}$.□

Доказательство. Применив линейное преобразование (6.30) к квадратичной форме (6.34), получим

$$\begin{gathered} g(u, v) = f(\alpha_{11}u + \alpha_{12}v, \alpha_{21}u + \alpha_{22}v) = a_{11}(\alpha_{11}^2u^2 + 2\alpha_{11}\alpha_{12}uv + \alpha_{12}^2v^2) + \\ + a_{12}(\alpha_{11}\alpha_{21}u^2 + (\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21})uv + \alpha_{12}\alpha_{22}v^2) + \\ + a_{22}(\alpha_{21}^2u^2 + 2\alpha_{21}\alpha_{22}uv + \alpha_{22}^2v^2) = (a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2)u^2 + \\ + (2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}))uv + \\ + (a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2)v^2. \end{gathered} \tag{6.39}$$

Из (6.39) вытекает, что истинность равенства (6.36) является необходимым и достаточным условием приведения квадратичной формы (6.34) к виду (6.35). При этом, коэффициенты b_{11} и b_{22} определяются, соответственно, равенством (6.37) и (6.38).□

Из теоремы 6.5 непосредственно вытекает, что истинны следующие три следствия.

Следствие 6.2. Над кольцом $\mathcal{K}$ в результате линейного преобразования (6.30) квадратичная форма (6.34) может быть приведена к виду

$$g(u,v) = b_{11}u^2 \tag{6.40}$$

тогда и только тогда, когда существуют такие $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in K$, что

$$\begin{cases} 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0 \\ a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2 = 0 \end{cases}. \tag{6.41}$$

При этом, коэффициент b_{11} определяется равенством (6.37).□

Следствие 6.3. Над кольцом $\mathcal{K}$ в результате линейного преобразования (6.30) квадратичная форма (6.34) может быть приведена к виду

$$g(u,v) = b_{22}v^2 \tag{6.42}$$

тогда и только тогда, когда

$$\begin{cases} 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0 \\ a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2 = 0 \end{cases}. \tag{6.43}$$

При этом, коэффициент b_{22} определяется равенством (6.38).□

Следствие 6.4. Над кольцом $\mathcal{K}$ в результате линейного преобразования (6.30) квадратичная форма (6.34) может быть приведена к виду

$$g(u,v) = b_{12}uv \tag{6.44}$$

тогда и только тогда, когда

$$\begin{cases} a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2 = 0 \\ a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2 = 0 \end{cases}. \tag{6.45}$$

При этом, коэффициент b_{22} определяется равенством

$$b_{12} = 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) \tag{6.46}$$

над кольцом $\mathcal{K}$.□

Необходимость выделения в отдельный случай выражения $b_{12}uv$ обусловлена тем, что не всегда в кольце $\mathcal{K}$ это выражение с помощью обратимого линейного преобразования

$$\begin{cases} u = \gamma U + \delta V \\ v = \varphi U + \psi V \end{cases}$$

может быть приведен к виду $\gamma\varphi U^2 + \delta\psi V^2$.

Критерием возможности такого приведения является существование таких элементов $\gamma, \delta, \varphi, \psi \in K$, что

$$\gamma\psi - \delta\varphi \neq 0$$

и

$$\gamma\psi + \delta\varphi = 0.$$

Замечание 6.3. Некоторые из установленных выше равенств упрощаются, если $\mathcal{K}$ – кольцо характеристики 2.

Действительно, равенство (6.36) принимает вид

$$a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0, \tag{6.47}$$

а равенство (6.46) принимает вид

$$b_{12} = a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}). \tag{6.48}$$

Из леммы 6.1, теоремы 6.5 и следствий 6.2-6.4 вытекают следующие достаточные условия приведения к каноническому виду кривой Γ, определенной над кольцом $\mathcal{K}$ уравнением (6.1), в результате применения линейного преобразования (6.30).

Кривая Γ, определяемая над кольцом $\mathcal{K}$ уравнением (6.1), применением линейного преобразования (6.30):

1) может быть приведена к виду

$$b_{11}u^2 + b_{22}v^2 + a_0 = 0, \tag{6.49}$$

если

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \\ 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0 \end{cases}; \tag{6.50}$$

2) может быть приведена к виду

$$b_{11}u^2 + a_0 = 0, \tag{6.51}$$

если

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \\ 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0 \\ a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2 = 0 \end{cases}; \tag{6.52}$$

3) может быть приведена к виду

$$b_{22}v^2 + a_0 = 0, \tag{6.53}$$

если

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \\ 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0 \\ a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2 = 0 \end{cases}; \tag{6.54}$$

4) может быть приведена к виду

$$b_{12}uv + a_0 = 0, \tag{6.55}$$

если

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \\ a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2 = 0 \\ a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2 = 0 \end{cases}. \tag{6.56}$$

Таким образом, системы нелинейных уравнений (6.50), (6.52), (6.54) и (6.56) могут быть использованы для поиска линейного преобразования, осуществляющего приведение кривой Γ, определенной над кольцом $\mathcal{K}$ уравнением (6.1), соответственно, к виду (6.49), (6.51), (6.53) или (6.55).

Линейное преобразование (6.28) является биекцией множества K^2 на себя тогда и только тогда, когда 2×2-матрица (6.29) обратима над кольцом $\mathcal{K}$. Последнее имеет место тогда и только тогда, когда

$$\alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21} \in K^{inv}. \tag{6.57}$$

Теорема 6.6. Если характеристика кольца $\mathcal{K}$ равна 2, а $a_{12} \in K^{inv}$, то никаким обратимым линейным преобразованием (6.28) квадратичная форма (6.34) не может быть приведена ни к виду (6.40), ни к виду (6.42).

Доказательство. Предположим, что характеристика кольца $\mathcal{K}$ равна 2, $a_{12} \in K^{inv}$ и существует обратимое линейное преобразование (6.28), приводящее квадратичную форму (6.34) к виду (6.40) или (6.42). Тогда истинно равенство (6.47).

Так как $a_{12} \in K^{inv}$, то равенство (6.47) эквивалентно равенству

$$\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21} = 0. \tag{6.58}$$

А так как 2×2-матрица (6.29) обратима над кольцом $\mathcal{K}$, то истинно условие (6.57).

Из (6.57) и (6.58) вытекает, что

$$2\alpha_{11}\alpha_{22} \in K^{inv} \Leftrightarrow 0 \in K^{inv}.$$

Полученное противоречие показывает, что предположение – ложное.

Отсюда вытекает, что если характеристика кольца $\mathcal{K}$ равна 2, а $a_{12} \in K^{inv}$, то никаким обратимым линейным преобразованием (6.28) квадратичная форма (6.34) не может быть приведена ни к виду (6.40), ни к виду (6.42).$\square$

6.1.2. Анализ кривых 3-го порядка.

Рассмотрим над кольцом $\mathcal{K} = (K, +, \cdot)$ кривую 3-го порядка Γ, определенную уравнением

$$ay^2 = b_3x^3 + b_2x^2 + b_1x + b_0, \tag{6.59}$$

где $a, b_3 \in K\backslash\{0\}$ и $b_2, b_1, b_0 \in K$.

Для многочлена $f(x) = b_3x^3 + b_2x^2 + b_1x + b_0$, являющегося правой частью уравнения (6.59), возможны следующие три ситуации.

Ситуация 6.4. Многочлен $f(x)$ неразложим над кольцом $\mathcal{K}$.

Ситуация 6.5. Для любых многочленов $f_i \in \mathcal{K}[x]$ $(i = 1, 2)$ степени $m_i \geq 1$ $(i = 1, 2)$, удовлетворяющих равенству $f(x) = f_1(x)f_2(x)$, истинно неравенство $m_1 + m_2 > 3$.

Ситуация 6.6. Существуют многочлены $f_i \in \mathcal{K}[x]$ $(i = 1, 2)$ степени $m_i \geq 1$ $(i = 1, 2)$, удовлетворяющие равенству $f(x) = f_1(x)f_2(x)$, для которых $m_1 + m_2 = 3$.

Пусть имеет место ситуация 6.5. Тогда $f(x, y)$ – многочлен наименьшей степени, определяющий кривую 3-го порядка Γ. Анализ кривой Γ осуществляется непосредственно на основе уравнения (6.59).

Пусть имеет место ситуация 2.6. Тогда либо

$$f(x) = (\alpha_2x^2 + \alpha_1x + \alpha_0)(\beta_1x + \beta_0),$$

где $\alpha_2, \alpha_1, \alpha_0, \beta_1, \beta_0 \in K$, причем $\alpha_2\beta_1 \neq 0$, либо

$$f(x) = (\gamma_1x + \delta_1)(\gamma_2x + \delta_2)(\gamma_3x + \delta_3),$$

где $\gamma_i, \delta_i \in K$ $(i = 1, 2, 3)$, причем $\gamma_1\gamma_2\gamma_3 \neq 0$.

Следовательно, уравнение (6.59) принимает либо вид

$$ay^2 = (\alpha_2 x^2 + \alpha_1 x + \alpha_0)(\beta_1 x + \beta_0), \tag{6.60}$$

либо вид

$$ay^2 = (\gamma_1 x + \delta_1)(\gamma_2 x + \delta_2)(\gamma_3 x + \delta_3). \tag{6.61}$$

Положим

$$S_a = \{ay^2 | y \in K\},$$
$$S_a^{(2)} = \{(\mu_1, \mu_2) \in K^2 | \mu_1\mu_2 \in S_a\}$$

и

$$S_a^{(3)} = \{(\nu_1, \nu_2, \nu_3) \in K^3 | \nu_1\nu_2\nu_3 \in S_a\}.$$

Пусть кривая Γ определена уравнением (6.60). Тогда множество ее точек представляет собой объединение множеств решений двухпараметрического семейства систем нелинейных уравнений

$$\mathtt{A}_{\mu_1,\mu_2} : \begin{cases} ay^2 = \mu_1\mu_2 \\ \alpha_2 x^2 + \alpha_1 x + \alpha_0 = \mu_1 \\ \beta_1 x + \beta_0 = \mu_2 \end{cases} \qquad ((\mu_1, \mu_2) \in S_a^{(2)}).$$

Пусть кривая Γ определена уравнением (6.61). Тогда множество ее точек представляет собой объединение множеств решений трехпараметрического семейства систем нелинейных уравнений

$$\mathtt{B}_{\nu_1,\nu_2,\nu_3} : \begin{cases} ay^2 = \nu_1\nu_2\nu_3 \\ \gamma_1 x + \delta_1 = \nu_1 \\ \gamma_2 x + \delta_2 = \nu_2 \\ \gamma_3 x + \delta_3 = \nu_3 \end{cases} \qquad ((\nu_1, \nu_2, \nu_3) \in S_a^{(3)}).$$

Замечание 6.4. Таким образом, построение в явном виде множества точек кривой 3-го порядка Γ в ситуациях 6.4 и 6.5 эквивалентно поиску множества решений нелинейного уравнения (6.59) от двух переменных, а в ситуации 6.6 – поиску множества решений двух-параметрического семейства $\mathtt{A}_{\mu_1,\mu_2}$ $((\mu_1, \mu_2) \in S_a^{(2)})$ или трехпараметрического семейства $\mathtt{B}_{\nu_1,\nu_2,\nu_3}$ $((\nu_1, \nu_2, \nu_3) \in S_a^{(3)})$ систем нелинейных уравнений.

При этом в ситуации 6.6 возникает необходимость построения в явном виде всех факторизаций всех элементов множества S_a либо на два, либо на три сомножителя.

Отметим, что наилучший из известных алгоритмов факторизации для конечных колец имеет субэкспоненциальную сложность.

Охарактеризуем особые точки кривой (6.59).

Из определения особой точки кривой вытекает, что множеством особых точек кривой (6.59) является множество решений системы уравнений

$$\begin{cases} \mathsf{D}_x(b_3x^3+b_2x^2+b_1x+b_0-ay^2)=0 \\ \mathsf{D}_x(ay^2-b_3x^3-b_2x^2-b_1x-b_0)=0 \\ ay^2=b_3x^3+b_2x^2+b_1x+b_0 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} 3b_3x^2+2b_2x+b_1=0 \\ 2ay=0 \\ ay^2=b_3x^3+b_2x^2+b_1x+b_0 \end{cases}.$$

Отсюда вытекает, что истинно следующее утверждение.

Утверждение 6.3. Кривая Γ, определенная уравнением (6.59), имеет особые точки тогда и только тогда, когда существует такое решение (x_0, y_0) системы уравнений

$$\begin{cases} 3b_3x^2+2b_2x+b_1=0 \\ 2ay=0 \end{cases}, \tag{6.62}$$

что истинно равенство $ay_0^2=b_3x_0^3+b_2x_0^2+b_1x_0+b_0$.□

Пусть характеристика кольца $\mathcal{K}$ равна 2.

Тогда система уравнений (6.62) принимает вид

$$\begin{cases} b_3x^2+b_1=0 \\ y\in K \end{cases}. \tag{6.63}$$

Отсюда вытекает, что истинно следующее утверждение.

Утверждение 6.4. Пусть характеристика кольца $\mathcal{K}$ равна 2. Тогда:

1) кривая Γ, определенная уравнением (6.59), является гладкой кривой, если над кольцом $\mathcal{K}$ уравнение $b_3x^2+b_1=0$ не имеет решений;

2) если $b_3\in K^{inv}$, то множеством особых точек кривой Γ, определенной уравнением (6.59), является множество решений системы нелинейных уравнений

$$\begin{cases} x^2=b_3^{-1}b_1 \\ ay^2=b_0-b_1b_2b_3^{-1} \end{cases} \Leftrightarrow \begin{cases} x^2=b_3^{-1}b_1 \\ ay^2=b_0+b_1b_2b_3^{-1} \end{cases}$$

над кольцом $\mathcal{K}$;

3) если $b_3 \in K \backslash K^{inv}$, то множеством особых точек кривой Γ, определенной уравнением (6.59), является множество решений системы нелинейных уравнений

$$\begin{cases} b_3 x^2 + b_1 = 0 \\ ay^2 = b_2 x^2 + b_0 \end{cases}$$

над кольцом $\mathcal{K}$.$\square$

Пусть характеристика кольца $\mathcal{K}$ равна 3.

Тогда система уравнений (6.62) принимает вид

$$\begin{cases} 2b_2 x + b_1 = 0 \\ 2ay = 0 \end{cases} \Leftrightarrow \begin{cases} b_2 x = b_1 \\ ay = 0 \end{cases} . \tag{6.64}$$

Отсюда вытекает, что истинно следующее утверждение.

Утверждение 6.5. Пусть характеристика кольца $\mathcal{K}$ равна 3. Тогда:

1) кривая Γ, определенная уравнением (6.59), является гладкой кривой, если над кольцом $\mathcal{K}$ уравнение $b_3 x^3 - b_1 x + b_0 = 0$ не имеет решений;

2) если $b_2 \in K^{inv}$ и $b_1^3 b_2^{-3} b_3 - b_1^2 b_2^{-1} + b_0 = 0$, то множеством особых точек кривой Γ, определенной уравнением (6.59), является множество точек $\{(b_1 b_2^{-1}, y) | ay = 0\}$;

3) если $b_2 \in K \backslash K^{inv}$, то множеством особых точек кривой Γ, определенной уравнением (6.59), является множество решений системы нелинейных уравнений

$$\begin{cases} b_2 x = b_1 \\ b_3 x^3 - b_1 x + b_0 = 0 \\ ay = 0 \end{cases}$$

над кольцом $\mathcal{K}$.$\square$

Найдем условия, при которых многочлен, являющийся правой частью уравнения (6.59), имеет кратный корень, т.е. когда

$$b_3 x^3 + b_2 x^2 + b_1 x + b_0 = (x - \alpha)^2 (b_3 x + \beta) \tag{6.65}$$

или

$$b_3 x^3 + b_2 x^2 + b_1 x + b_0 = b_3 (x - \alpha)^3. \tag{6.66}$$

Пусть характеристика кольца $\mathcal{K}$ равна 2. Тогда истинно следующее утверждение.

Утверждение 6.6. Если характеристика кольца $\mathcal{K}$ равна 2, то:

1) разложение (6.65) существует тогда и только тогда, когда существует решение α системы нелинейных уравнений

$$\begin{cases} b_3\alpha^2 = b_1 \\ b_2\alpha^2 = b_0 \end{cases}$$

над кольцом $\mathcal{K}$;

2) разложение (6.66) существует тогда и только тогда, когда существует решение α системы линейных уравнений

$$\begin{cases} b_3\alpha = -b_2 \\ b_3\alpha^2 = b_1 \\ b_3\alpha^3 = -b_0 \end{cases} \Leftrightarrow \begin{cases} b_3\alpha = b_2 \\ b_3\alpha^2 = b_1 \\ b_3\alpha^3 = b_0 \end{cases} \Leftrightarrow \begin{cases} b_3\alpha = b_2 \\ b_2\alpha = b_1 \\ b_1\alpha = b_0 \end{cases}$$

над кольцом $\mathcal{K}$.$\square$

Пусть характеристика кольца $\mathcal{K}$ равна 3. Тогда истинно следующее утверждение.

Утверждение 6.7. Если характеристика кольца $\mathcal{K}$ равна 3, то:

1) разложение (6.65) существует тогда и только тогда, когда существует решение (α, β) системы нелинейных уравнений

$$\begin{cases} \alpha b_3 + \beta = b_2 \\ \alpha b_2 = b_1 \\ \alpha^2\beta = b_0 \end{cases};$$

2) разложение (6.66) существует тогда и только тогда, когда существует решение α нелинейного уравнения $b_3\alpha^3 = -b_0$ и $b_2 = b_1 = 0$.$\square$

Замечание 6.5. Для кольца (в отличие от поля) равенство нулю результанта двух многочленов является необходимым условием существования их общего корня. Поэтому с использованием понятия «результант двух многочленов» может быть установлено только необходимое условие существования разложений (6.65) и (6.66).

Теорема 6.7. Если характеристика кольца $\mathcal{K}$ отлична от 2 и 3, то:

1) если существует разложение (6.65), то равенство

$$b_3(4b_0b_2^3 + 27b_0^2b_3^2 - 18b_0b_1b_2b_3 + 4b_1^3b_3 - b_1^2b_2^2) = 0 \qquad (6.67)$$

истинно над кольцом $\mathcal{K}$;

2) если существует разложение (6.66), то истинны равенства

$$\begin{cases} b_3(4b_0b_2^3 + 27b_0^2b_3^2 - 18b_0b_1b_2b_3 + 4b_1^3b_3 - b_1^2b_2^2) = 0 \\ 12b_3(3b_1b_3 - b_2) = 0 \end{cases} \tag{6.68}$$

над кольцом $\mathcal{K}$.$\square$

Доказательство. Производная многочлена $f(x)$, являющегося правой частью уравнения (6.59), равна $\mathsf{D}f(x) = 3b_3x^2 + 2b_2x + b_1$.

Вычислим результант многочленов $f(x)$ и $\mathsf{D}f(x)$.

$$\operatorname{Res}(f, \mathsf{D}f, x) = \det(\operatorname{Syl}(f, \mathsf{D}f, x)) = \begin{vmatrix} b_3 & 0 & 3b_3 & 0 & 0 \\ b_2 & b_3 & 2b_2 & 3b_3 & 0 \\ b_1 & b_2 & b_1 & 2b_2 & 3b_3 \\ b_0 & b_1 & 0 & b_1 & 2b_2 \\ 0 & b_0 & 0 & 0 & b_1 \end{vmatrix} =$$

$$= b_3 \begin{vmatrix} b_3 & 2b_2 & 3b_3 & 0 \\ b_2 & b_1 & 2b_2 & 3b_3 \\ b_1 & 0 & b_1 & 2b_2 \\ b_0 & 0 & 0 & b_1 \end{vmatrix} + 3b_3 \begin{vmatrix} b_2 & b_3 & 3b_3 & 0 \\ b_1 & b_2 & 2b_2 & 3b_3 \\ b_0 & b_1 & b_1 & 2b_2 \\ 0 & b_0 & 0 & b_1 \end{vmatrix} =$$

$$= b_3 \begin{vmatrix} -2b_3 & 2b_2 & 3b_3 & 0 \\ -b_2 & b_1 & 2b_2 & 3b_3 \\ 0 & 0 & b_1 & 2b_2 \\ b_0 & 0 & 0 & b_1 \end{vmatrix} + 3b_3 \begin{vmatrix} b_2 & -2b_3 & 3b_3 & 0 \\ b_1 & -b_2 & 2b_2 & 3b_3 \\ b_0 & 0 & b_1 & 2b_2 \\ 0 & b_0 & 0 & b_1 \end{vmatrix}. \tag{6.69}$$

Вычислим по отдельности определители 4-го порядка.

$$\begin{vmatrix} -2b_3 & 2b_2 & 3b_3 & 0 \\ -b_2 & b_1 & 2b_2 & 3b_3 \\ 0 & 0 & b_1 & 2b_2 \\ b_0 & 0 & 0 & b_1 \end{vmatrix} = -b_0 \begin{vmatrix} 2b_2 & 3b_3 & 0 \\ b_1 & 2b_2 & 3b_3 \\ 0 & b_1 & 2b_2 \end{vmatrix} + b_1 \begin{vmatrix} -2b_3 & 2b_2 & 3b_3 \\ -b_2 & b_1 & 2b_2 \\ 0 & 0 & b_1 \end{vmatrix} =$$

$$= -b_0(8b_2^3 - 12b_1b_2b_3) + b_1^2(-2b_1b_3 + 2b_2^2) =$$

$$= -8b_0b_2^3 + 12b_0b_1b_2b_3 - 2b_1^3b_3 + 2b_1^2b_2^2, \tag{6.70}$$

$$\begin{vmatrix} b_2 & -2b_3 & 3b_3 & 0 \\ b_1 & -b_2 & 2b_2 & 3b_3 \\ b_0 & 0 & b_1 & 2b_2 \\ 0 & b_0 & 0 & b_1 \end{vmatrix} = b_0 \begin{vmatrix} b_2 & 3b_3 & 0 \\ b_1 & 2b_2 & 3b_3 \\ b_0 & b_1 & 2b_2 \end{vmatrix} + b_1 \begin{vmatrix} b_2 & -2b_3 & 3b_3 \\ b_1 & -b_2 & 2b_2 \\ b_0 & 0 & b_1 \end{vmatrix} =$$

$$= b_0(4b_2^3 + 9b_0b_3^2 - 9b_1b_2b_3) + b_1(-b_1b_2^2 - b_0b_2b_3 + 2b_1^2b_3) =$$
$$= 4b_0b_2^3 + 9b_0^2b_3^2 - 10b_0b_1b_2b_3 - b_1^2b_2^2 + 2b_1^3b_3. \qquad (6.71)$$

Подставив (6.70) и (6.71) в (6.69), получим

$$\mathrm{Res}(f, \mathsf{D}f, x) = b_3(-8b_0b_2^3 + 12b_0b_1b_2b_3 - 2b_1^3b_3 + 2b_1^2b_2^2) +$$
$$+3b_3(4b_0b_2^3 + 9b_0^2b_3^2 - 10b_0b_1b_2b_3 - b_1^2b_2^2 + 2b_1^3b_3) =$$
$$= b_3(-8b_0b_2^3 + 12b_0b_1b_2b_3 - 2b_1^3b_3 + 2b_1^2b_2^2 +$$
$$+12b_0b_2^3 + 27b_0^2b_3^2 - 30b_0b_1b_2b_3 - 3b_1^2b_2^2 + 6b_1^3b_3) =$$
$$= b_3(4b_0b_2^3 + 27b_0^2b_3^2 - 18b_0b_1b_2b_3 + 4b_1^3b_3 - b_1^2b_2^2). \qquad (6.72)$$

Из (6.72) вытекает, что если существует разложение (6.65), то истинно равенство (6.67), что и требовалось показать.

Производная многочлена $\mathsf{D}f(x)$ равна $\mathsf{D}^2f(x) = 6b_3x + 2b_2$.

Вычислим результант многочленов $\mathsf{D}f(x)$ и $\mathsf{D}^2f(x)$.

$$\mathrm{Res}(\mathsf{D}f, \mathsf{D}^2f, x) = \det(\mathrm{Syl}(\mathsf{D}f, \mathsf{D}^2f, x)) =$$

$$= \begin{vmatrix} 3b_3 & 6b_3 & 0 \\ 2b_2 & 2b_2 & 6b_3 \\ b_1 & 0 & 2b_2 \end{vmatrix} = \begin{vmatrix} -3b_3 & 6b_3 & 0 \\ 0 & 2b_2 & 6b_3 \\ b_1 & 0 & 2b_2 \end{vmatrix} = 12b_3(3b_1b_3 - b_2^2). \qquad (6.73)$$

Из (6.72) и (6.73) вытекает, что если существует разложение (6.66), то истинны равенства (6.68), что и требовалось показать.□

Замечание 6.6. Пусть характеристика кольца $\mathcal{K}$ равна 4. Из (6.73) вытекает, что $\mathrm{Res}(\mathsf{D}f, \mathsf{D}^2f, x) \equiv 0$, т.е. необходимое условие существования разложения (6.66), устанавливаемое равенствами (6.68), тривиально для кольца характеристики 4.

Из (6.72) вытекает, что

$$b_3\mathrm{disc}(f) = -b_3(4b_0b_2^3 + 27b_0^2b_3^2 - 18b_0b_1b_2b_3 + 4b_1^3b_3 - b_1^2b_2^2). \qquad (6.74)$$

Из (6.74) непосредственно вытекает, что истинно утверждение.

Утверждение 6.8. Пусть либо $b_3 \in K^{inv}$, либо $\mathcal{K}$ – гауссово кольцо. Тогда достаточное условие отсутствия разложения (6.65) для многочлена $f(x) = b_3x^3 + b_2x^2 + b_1x + b_0$ состоит в том, что

$$4b_0b_2^3 + 27b_0^2b_3^2 - 18b_0b_1b_2b_3 + 4b_1^3b_3 - b_1^2b_2^2 \neq 0$$

над кольцом $\mathcal{K}$.□

6.2. Два типа многообразий над конечным кольцом.

Рассмотрим над кольцом $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$ автомат Мили

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

где $\mathbf{f}_1 : K^{n_1} \times K^{n_2} \to K^{n_1}$ и $\mathbf{f}_2 : K^{n_1} \times K^{n_2} \to K^{n_3}$, или автомат Мура

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

где $\mathbf{f}_1 : K^{n_1} \times K^{n_2} \to K^{n_1}$ и $\mathbf{f}_2 : K^{n_1} \to K^{n_3}$ (элементы $\mathbf{q}_t \in K^{n_1}$, $\mathbf{x}_t \in K^{n_2}$ и $\mathbf{y}_t \in K^{n_3}$ являются, соответственно, состоянием, входным символом и выходным символом автомата в момент t).

Если при любом начальном состоянии $\mathbf{q}_0$, принадлежащем многообразию $\mathbf{V} \in K^{n_1}$, для любого входного слова $\mathbf{x}_1 \dots \mathbf{x}_i \in (K^{n_2})^i$ $(i \in \mathbb{N})$ все состояния $\mathbf{q}_j$ также принадлежат этому многообразию, то естественно говорить, что автомат определен на многообразии $\mathbf{V}$.

Само по себе определение многообразия над кольцом $\mathcal{K}$ формулой

$$\mathbf{V} = \{(v_1, \dots, v_n) \in K^n | f_i(v_1, \dots, v_n) = 0 \text{ для всех } i = 1, \dots, m\},$$

где $f_1, \dots, f_m \in K[\tau_1, \dots, \tau_n]$ – попарно различные ненулевые многочлены, мало что дает при исследовании свойств отображений, определенных на многообразии $\mathbf{V}$ (напомним, что даже над полем $GF(2^k)$ $(k \in \mathbb{N})$ поиск решений уравнения $f(\tau_1, \dots, \tau_n) = 0$, где f – квадратичная форма, является NP-полной задачей).

Поэтому при исследования отображений, определенных на многообразии, естественно ограничиться такими многообразиями $\mathbf{V}$ над кольцом $\mathcal{K}$, которые представляют интерес как с теоретической, так и с прикладной точки зрения, и свойства которых могут быть эффективно использованы в процессе анализа автоматных моделей, определенных на этих многообразиях. Рассмотрим два основных типа таких многообразий над кольцом $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$.

6.2.1. Многообразия с алгеброй.

Рассмотрим вначале следующий пример.

Пример 6.1. Пусть γ – эллиптическая кривая над конечным полем $\mathcal{K}$. Известно, что множество точек G_γ этой кривой (включая бесконечно удаленную точку $\mathcal{O}$) является абелевой группой

$$\mathcal{G}_\gamma = (G_\gamma, +_\gamma, \cdot_\gamma).$$

Зафиксируем на множестве G_γ множество унарных операций

$$\mathcal{F}_1 = \{\alpha_0, \alpha_1, \ldots, \alpha_{k_1}\} \ (k_1 \in \mathbb{N}),$$

где

$$\alpha_0(P) = \mathcal{O}$$

и

$$\alpha_i(P) = \underbrace{P +_\gamma \cdots +_\gamma P}_{i \text{ раз}} \ (i \in \mathbb{N}_{k_1})$$

для всех $P \in G_\gamma$.

Положим

$$\mathcal{F}_2 = \{+_\gamma\}.$$

Таким образом, построена алгебра

$$\mathfrak{A}_{G_\gamma} = (G_\gamma, \mathcal{F}_1, \mathcal{F}_2),$$

основой которой является множество G_γ точек эллиптической кривой γ.

Рассмотренная в примере 6.1 конструкция допускает следующее естественное обобщение.

Пусть $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$.

Во множестве всех многообразий в K^n $(n \in \mathbb{N})$ выделим множество $\mathcal{V}_{1,n}(\mathcal{K})$ всех таких многообразий $\mathbf{V} \subseteq K^n$, что задана некоторая алгебра

$$\mathfrak{A}_{\mathbf{V}} = (\mathbf{V}, \mathcal{F}_{1,\mathbf{V}}, \mathcal{F}_{2,\mathbf{V}}),$$

где

$$\mathcal{F}_{1,\mathbf{V}} = \{\alpha_0, \alpha_1, \ldots, \alpha_{k_1}\} \ (k_1 \in \mathbb{Z}_+)$$

и

$$\mathcal{F}_{2,\mathbf{V}} = \{\beta_1, \ldots, \beta_{k_2}\} \ (k_2 \in \mathbb{N})$$

есть множество, соответственно, унарных и бинарных операций, определенных на множестве $\mathbf{V}$.

Замечание 6.7. Целесообразность выделения множества многообразий $\mathcal{V}_{1,n}(\mathcal{K})$ $(n \in \mathbb{N})$ над кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$ обосновывается, по крайней мере, тем, что эллиптические кривые над конечными полями имеют многочисленные применения в процессе решения как теоретических, так и прикладных задач.

Пусть $\mathbf{V}_i \in \mathcal{V}_{1,n_i}(\mathcal{K}_i)$ $(i = 1, 2)$ (где $n_1, n_2 \in \mathbb{N}$ и $\mathcal{K}_1, \mathcal{K}_2 \in \mathfrak{K}^{fnt}$) – такие многообразия, что для алгебр

$$\mathfrak{A}_{\mathbf{V}_i} = (\mathbf{V}_i, \mathcal{F}_{1,\mathbf{V}_i}, \mathcal{F}_{2,\mathbf{V}_i}) \ (i = 1, 2),$$

где

$$\mathcal{F}_{1,\mathbf{V}_i} = \{\alpha_0^{(i)}, \alpha_1^{(i)}, \ldots, \alpha_{k_1^{(i)}}^{(i)}\}\ (k_1^{(i)} \in \mathbb{Z}_+)$$

есть множество унарных операций алгебры $\mathfrak{A}_{\mathbf{V}_i}$, а

$$\mathcal{F}_{2,\mathbf{V}_i} = \{\beta_1^{(i)}, \ldots, \beta_{k_2^{(i)}}^{(i)}\}\ (k_2^{(i)} \in \mathbb{N})$$

есть множество бинарных операций алгебры $\mathfrak{A}_{\mathbf{V}_i}$, истинны равенства

$$k_1^{(1)} = k_1^{(2)} = k_1$$

и

$$k_2^{(1)} = k_2^{(2)} = k_2.$$

Предположим, что существует тройка отображений

$$\Phi = \varphi_1, \varphi_2, \varphi_3),$$

где $\varphi_1 : \mathbf{V}_1 \to \mathbf{V}_2$ – сюръекция, а $\varphi_2 : \mathcal{F}_{1,\mathbf{V}_1} \to \mathcal{F}_{1,\mathbf{V}_2}$ и $\varphi_3 : \mathcal{F}_{2,\mathbf{V}_1} \to \mathcal{F}_{2,\mathbf{V}_2}$ – биекции, для которой равенства

$$\varphi_1(\alpha(\mathbf{v}_1)) = \varphi_2(\alpha)(\varphi_1(\mathbf{v}_1)) \tag{6.75}$$

и

$$\varphi_1(\beta(\mathbf{v}_1, \mathbf{v}_2)) = \varphi_3(\beta)(\varphi_1(\mathbf{v}_1), \varphi_1(\mathbf{v}_2)) \tag{6.76}$$

истинны для всех $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}_1$, $\alpha \in \mathcal{F}_{1,\mathbf{V}_1}$ и $\beta \in \mathcal{F}_{2,\mathbf{V}_1}$.

Тогда будем говорить, что:

1) многообразие $\mathbf{V}_2$ – гомоморфный образ многообразия $\mathbf{V}_1$;

2) многообразия $\mathbf{V}_1$ и $\mathbf{V}_2$ изоморфны, если отображение φ_1 – биекция.

Иными словами:

1) многообразие $\mathbf{V}_2 \in \mathcal{V}_{1,n_2}(\mathcal{K}_2)$ – гомоморфный образ многообразия $\mathbf{V}_1 \in \mathcal{V}_{1,n_1}(\mathcal{K}_1)$ тогда и только тогда, когда алгебра

$$\mathfrak{A}_{\mathbf{V}_2} = (\mathbf{V}_2, \mathcal{F}_{1,\mathbf{V}_2}, \mathcal{F}_{2,\mathbf{V}_2})$$

является гомоморфным образом алгебры

$$\mathfrak{A}_{\mathbf{V}_1} = (\mathbf{V}_1, \mathcal{F}_{1,\mathbf{V}_1}, \mathcal{F}_{2,\mathbf{V}_1});$$

2) многообразия $\mathbf{V}_1 \in \mathcal{V}_{1,n_1}(\mathcal{K}_1)$ и $\mathbf{V}_2 \in \mathcal{V}_{1,n_2}(\mathcal{K}_2)$ изоморфны тогда и только тогда, когда изоморфны алгебры

$$\mathfrak{A}_{\mathbf{V}_1} = (\mathbf{V}_1, \mathcal{F}_{1,\mathbf{V}_1}, \mathcal{F}_{2,\mathbf{V}_1})$$

и

$$\mathfrak{A}_{\mathbf{V}_2} = (\mathbf{V}_2, \mathcal{F}_{1,\mathbf{V}_2}, \mathcal{F}_{2,\mathbf{V}_2}).$$

Замечание 6.8. Подчеркнем, что приведенное выше определение гомоморфизма (соответственно, изоморфизма) для многообразий с алгеброй представляет, по своей сути, определение гомоморфизма (соответственно, изоморфизма) для упорядоченных пар $(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1})$ $(\mathbf{V}_1 \in \mathcal{V}_{1,n_1}(\mathcal{K}_1))$ и $(\mathbf{V}_2, \mathfrak{A}_{\mathbf{V}_2})$ $(\mathbf{V}_2 \in \mathcal{V}_{1,n_2}(\mathcal{K}_2))$.

Пример 6.2. Пусть γ_1 и γ_2 – эллиптические кривые, заданные над областью целостности $\mathcal{K}$. Говорят, что:

1) эллиптическая кривая γ_2 является гомоморфным образом эллиптической кривой γ_1, если абелева группа $(\widetilde{\mathcal{K}}(\gamma_2), +_{\gamma_2})$ является гомоморфным образом абелевой группы $(\widetilde{\mathcal{K}}(\gamma_1), +_{\gamma_1})$;

2) эллиптические кривые γ_1 и γ_2 изоморфны, если абелевы группы $(\widetilde{\mathcal{K}}(\gamma_1), +_{\gamma_1})$ и $(\widetilde{\mathcal{K}}(\gamma_2), +_{\gamma_2})$ изоморфны.

Пусть $\varphi_1 : \widetilde{\mathcal{K}}(\gamma_1) \to \widetilde{\mathcal{K}}(\gamma_2)$ – гомоморфизм эллиптической кривой γ_1 на эллиптическую кривую γ_2.

Тогда для любого числа $k_1 \in \{1, \ldots, |\widetilde{\mathcal{K}}(\gamma_2)| - 1\}$ алгебра

$$\mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_2)} = (\widetilde{\mathcal{K}}(\gamma_2), \mathcal{F}_1^{(2)}, \mathcal{F}_2^{(2)}),$$

где

$$\mathcal{F}_1^{(2)} = \{\alpha_0^{(2)}, \alpha_1^{(2)}, \ldots, \alpha_{k_1}^{(2)}\}$$

и

$$\mathcal{F}_2^{(2)} = \{+_{\gamma_2}\},$$

является гомоморфным образом алгебры

$$\mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_1)} = (\widetilde{\mathcal{K}}(\gamma_1), \mathcal{F}_1^{(1)}, \mathcal{F}_2^{(1)}),$$

где

$$\mathcal{F}_1^{(1)} = \{\alpha_0^{(1)}, \alpha_1^{(1)}, \ldots, \alpha_{k_1}^{(1)}\}$$

и

$$\mathcal{F}_2^{(1)} = \{+_{\gamma_1}\}.$$

При этом для гомоморфизма

$$\Phi = (\varphi_1, \varphi_2, \varphi_3)$$

алгебры $\mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_1)}$ на алгебру $\mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_2)}$ биекции $\varphi_2 : \mathcal{F}_1^{(1)} \to \mathcal{F}_1^{(2)}$ и $\varphi_3 : \mathcal{F}_2^{(1)} \to \mathcal{F}_2^{(2)}$ определяются равенствами

$$\varphi_2(\alpha_i^{(1)}) = \alpha_i^{(2)} \ \ (i \in \mathbb{Z}_{k_1+1})$$

и

$$\varphi_3(+_{\gamma_1}) = +_{\gamma_2}.$$

В частности, если φ_1 – биекция, то алгебры $\mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_1)}$ и $\mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_2)}$ изоморфны.

Таким образом, если эллиптическая кривая γ_2 – гомоморфный образ эллиптической кривой γ_1, то упорядоченная пара $(\widetilde{\mathcal{K}}(\gamma_2), \mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_2)})$ $(\widetilde{\mathcal{K}}(\gamma_2) \in \mathcal{V}_{1,2}(\widetilde{\mathcal{K}}))$ является гомоморфным образом упорядоченной пары $(\widetilde{\mathcal{K}}(\gamma_1), \mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_1)})$ $(\widetilde{\mathcal{K}}(\gamma_1) \in \mathcal{V}_{1,2}(\widetilde{\mathcal{K}}))$.

В частности, если эллиптические кривые γ_1 и γ_2 изоморфны, то упорядоченные пары $(\widetilde{\mathcal{K}}(\gamma_1), \mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_1)})$ $(\widetilde{\mathcal{K}}(\gamma_1) \in \mathcal{V}_{1,2}(\widetilde{\mathcal{K}}))$ и $(\widetilde{\mathcal{K}}(\gamma_2), \mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_2)})$ $(\widetilde{\mathcal{K}}(\gamma_2) \in \mathcal{V}_{1,2}(\widetilde{\mathcal{K}}))$ изоморфны.

6.2.2. Параметризованные многообразия.

Пусть $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$.

Во множестве всех многообразий в K^n $(n \in \mathbb{N})$ выделим множество $\mathcal{V}_{2,n}(\mathcal{K})$ всех многообразий $\mathbf{V} \subseteq K^n$, для которых существует параметризация

$$\mathbf{v} = \mathbf{h}(\mathbf{t}),$$

где $\mathbf{t} \in K^m$ $(m < n)$, а $\mathbf{h} = (h_1, \ldots, h_n)^T$ – набор многочленов от m переменных $t_1, \ldots, t_m$ над кольцом $\mathcal{K}$.

Замечание 6.9. Целесообразность выделения множества многообразий $\mathcal{V}_{2,n}(\mathcal{K})$ $(n \in \mathbb{N})$ над кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$ обосновывается тем, что параметризованные многообразия над полями имеют многочисленные применения в процессе решения как теоретических, так и прикладных задач.

Параметризация $\mathbf{v} = \mathbf{h}(\mathbf{t})$ $(\mathbf{t} \in K^m)$ дает возможность выделить на многообразии $\mathbf{V} \in \mathcal{V}_{2,n}(\mathcal{K})$ множество траекторий, т.е. последовательностей точек.

Действительно (см. рис. 6.1), любое отображение $f : K^m \to K^m$ определяет во множестве K^m множество траекторий

$$\mathbf{t}, f(\mathbf{t}), f^2(\mathbf{t}), \ldots \quad (\mathbf{t} \in K^m),$$

где

$$f^i = \underbrace{f \circ \cdots \circ f}_{i \text{ раз}} \quad (i \in \mathbb{N}),$$

а «$\circ$» является операцией суперпозиции.

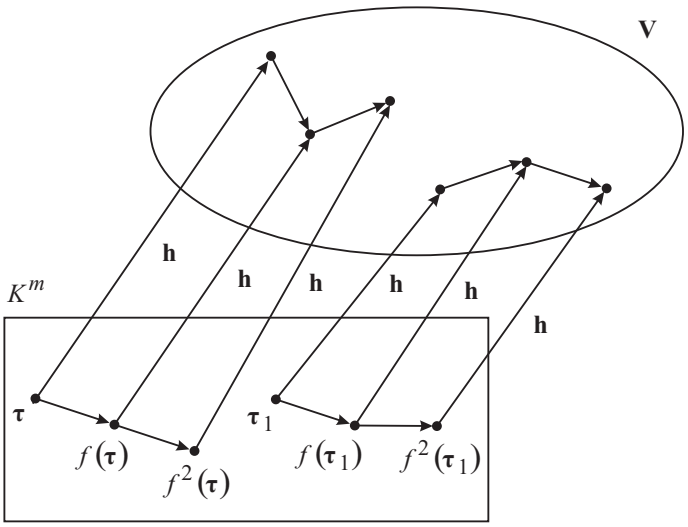


Рис. 6.1. Траектории в многообразии $\mathbf{V} \in \mathcal{V}_{2,n}(\mathcal{K})$.

Следовательно, для любого многообразия $\mathbf{V} \in \mathcal{V}_{2,n}(\mathcal{K})$ отображение $f : K^m \to K^m$ и параметризация $\mathbf{v} = \mathbf{h}(\mathbf{t})$ $(\mathbf{t} \in K^m)$ определяют на многообразии $\mathbf{V}$ множество траекторий

$$\mathbf{h}(\mathbf{t}), \mathbf{h}(f(\mathbf{t})), \mathbf{h}(f^2(\mathbf{t})), \ldots \quad (\mathbf{t} \in K^m).$$

Пусть параметризация многообразия $\mathbf{V}_j \in \mathcal{V}_{2,n_j}(\mathcal{K}_j)$ $(j = 1, 2)$ (где $n_1, n_2 \in \mathbb{N}$ и $\mathcal{K}_j = (K_j, +_j, \cdot_j) \in \mathfrak{K}^{fnt}$ $(j = 1, 2)$) имеет вид

$$\mathbf{v} = \mathbf{h}_j(\mathbf{t}) \ (\mathbf{t} \in K_j^{m_i}),$$

где $\mathbf{h}_j = (h_1^{(j)}, \ldots, h_{n_j}^{(j)})^T$ $(j = 1, 2)$ представляет собой набор многочленов от m_j переменных $t_1^{(j)}, \ldots, t_{m_j}^{(j)}$ над кольцом $\mathcal{K}_j$

Зафиксируем такие семейства отображений

$$\Theta^{(j)} = \{\theta_i^{(j)}\}_{i \in \mathbb{N}_{k_j}} \ (j = 1, 2),$$

где $\theta_i^{(j)} : K_j^{m_j} \to K_j^{m_j}$ для всех $i \in \mathbb{N}_{k_j}$, что истинно равенство

$$k_1 = k_2 = k.$$

Предположим, что существует такая упорядоченная пара сюръекций

$$\Phi = (\varphi_1, \varphi_2),$$

где $\varphi_1 : \mathbf{V}_1 \to \mathbf{V}_2$ и $\varphi_2 : K_1^{m_1} \to K_2^{m_2}$, что равенства

$$\varphi_1(\mathbf{h}_1(\mathbf{t})) = \mathbf{h}_2(\varphi_2(\mathbf{t})) \tag{6.77}$$

и

$$\varphi_2(\theta_i^{(1)}(\mathbf{t})) = \theta_i^{(2)}(\varphi_2(\mathbf{t})) \tag{6.78}$$

истинны для всех $\mathbf{t} \in K_1^{m_1}$ и $i \in \mathbb{N}_k$.

Тогда будем говорить, что:

1) упорядоченная пара $(\mathbf{V}_2, \Theta^{(2)})$ – гомоморфный образ упорядоченной пары $(\mathbf{V}_1, \Theta^{(1)})$;

2) упорядоченные пары $(\mathbf{V}_1, \Theta^{(1)})$ и $(\mathbf{V}_2, \Theta^{(2)})$ изоморфны, если отображения φ_1 и φ_2 – биекции.

Пример 6.3. Любая алгебраическая кривая

$$v_2 = a_0 v_1^n + a_1 v_1^{n-1} + \cdots + a_n$$

над кольцом $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}_1^{fnt}$ может рассматриваться как полиномиально параметризованное многообразие

$$\begin{cases} v_1 = \tau \\ v_2 = a_0\tau^n + a_1\tau^{n-1} + \cdots + a_n \end{cases} \qquad (\tau \in K)$$

в K^2, т.е. как элемент множества $\mathcal{V}_{2,2}(\mathcal{K})$.

Алгебраические кривые

$$v_2 = a_0 v_1^{n_1} + a_1 v_1^{n_1-1} + \cdots + a_{n_1}$$

и

$$u_2 = b_0 u_1^{n_2} + b_1 u_1^{n_2-1} + \cdots + b_{n_2}$$

над кольцом $\mathcal{K}$ определяют в K^2 многообразия

$$\mathbf{V}_1 = \{(\tau_1, a_0\tau_1^{n_1} + a_1\tau_1^{n_1-1} + \cdots + a_{n_1}) \mid \tau_1 \in K\}$$

и

$$\mathbf{V}_2 = \{(\tau_2, b_0\tau_2^{n_2} + b_1\tau_2^{n_2-1} + \cdots + b_{n_2}) \mid \tau_2 \in K\}.$$

Зафиксируем элементы $c, c_1, \ldots, c_k \in K^{inv}$.

Определим семейство

$$\Theta = \{\theta_i\}_{i \in \mathbb{Z}_k}$$

отображений $\theta_i : K \to K$ следующим образом

$$\theta_i(\tau) = c_i\tau \quad (i \in \mathbb{Z}_k, \tau \in K),$$

а пару биекций

$$\Phi = (\varphi_1, \varphi_2) \quad (\varphi_1 : \mathbf{V}_1 \to \mathbf{V}_2, \varphi_2 : K \to K)$$

определим равенствами

$$\varphi_1((\tau, a_0\tau^{n_1} + a_1\tau^{n_1-1} + \cdots + a_{n_1})) =$$

$$= (c\tau, b_0c^{n_2}\tau^{n_2} + b_1c^{n_2-1}\tau^{n_2-1} + \cdots + b_{n_2}) \quad (\tau \in K),$$

$$\varphi_2(\tau) = c\tau \quad (\tau \in K).$$

Так как для биекций $\Phi = (\varphi_1, \varphi_2)$ истинны равенства (6.77) и (6.78), то упорядоченные пары $(\mathbf{V}_1, \Theta)$ и $(\mathbf{V}_2, \Theta)$ изоморфны.

6.3. Автоматы на многообразии с алгеброй.

Определим автоматы Мили и Мура на многообразии $\mathbf{V} \in \mathcal{V}_{1,n}(\mathcal{K})$, где $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$ и $n \in \mathbb{N}$, и исследуем свойства таких автоматов.

6.3.1. Исследуемые модели.

Для каждого многообразия $\mathbf{V} \in \mathcal{V}_{1,n}(\mathcal{K})$ может быть задана некоторая алгебра

$$\mathfrak{A}_{\mathbf{V}} = (\mathbf{V}, \mathcal{F}_{1,\mathbf{V}}, \mathcal{F}_{2,\mathbf{V}}),$$

где $\mathcal{F}_{1,\mathbf{V}} = \{\alpha_0, \alpha_1, \ldots, \alpha_{k_1}\}$ $(k_1 \in \mathbb{Z}_+)$ и $\mathcal{F}_{2,\mathbf{V}} = \{\beta_1, \ldots, \beta_{k_2}\}$ $(k_2 \in \mathbb{N})$ есть множество, соответственно, унарных и бинарных операций, определенных на множестве $\mathbf{V}$. Таким образом, может быть задана упорядоченная пара $(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$.

Системы рекуррентных соотношений

$$\begin{cases} \mathbf{q}_{t+1} = \beta_{j_1}(\alpha_{i_1}(\mathbf{q}_t), \alpha_{x_{t+1}}(\mathbf{v}_1)) \\ \mathbf{y}_{t+1} = \beta_{j_2}(\alpha_{i_2}(\mathbf{q}_t), \alpha_{x_{t+1}}(\mathbf{v}_2)) \end{cases} \quad (t \in \mathbb{Z}_+) \tag{6.79}$$

и

$$\begin{cases} \mathbf{q}_{t+1} = \beta_{j_1}(\alpha_{i_1}(\mathbf{q}_t), \alpha_{x_{t+1}}(\mathbf{v}_1)) \\ \mathbf{y}_{t+1} = \beta_{j_2}(\alpha_{i_2}(\mathbf{q}_{t+1}), \mathbf{v}_2) \end{cases} \quad (t \in \mathbb{Z}_+), \tag{6.80}$$

где $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}$ – фиксированные точки, $i_1, i_2 \in \mathbb{Z}_{k_1+1}$ и $j_1, j_2 \in \mathbb{N}_{k_2}$ – фиксированные числа, а $\mathbf{q}_0 \in \mathbf{V}$ и $x_{t+1} \in \mathbb{Z}_{k_1+1}$ $(t \in \mathbb{Z}_+)$, определяют, соответственно, семейство автоматов Мили $\mathcal{M}^{(1)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$ и семейство автоматов Мура $\mathcal{M}^{(2)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$.

Для каждого автомата $M \in \mathcal{M}^{(1)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}}) \cup \mathcal{M}^{(2)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$ элементы x_t, $\mathbf{q}_t$ и $\mathbf{y}_t$ являются, соответственно, входным символом, состоянием и выходным символом в момент t.

Поэтому, для каждого автомата $M \in \mathcal{M}^{(1)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}}) \cup \mathcal{M}^{(2)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$ множество чисел $\mathbb{Z}_{k_1+1}$ является входным алфавитом, а многообразие $\mathbf{V}$ – как множеством состояний, так и выходным алфавитом.

Пример 6.4. Пусть γ – эллиптическая кривая, заданная над областью целостности $\mathcal{K}$.

Тогда для любого числа $k_1 \in \{1, \ldots, |\widetilde{\mathcal{K}}(\gamma)| - 1\}$ может быть задана алгебра

$$\mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma)} = (\widetilde{\mathcal{K}}(\gamma), \mathcal{F}_1, \mathcal{F}_2),$$

где $\mathcal{F}_1 = \{\alpha_0, \alpha_1, \ldots, \alpha_{k_1}\}$ и $\mathcal{F}_2 = \{+_\gamma\}$ являются множествами, соответственно, унарных и бинарных операций, определенных на множестве $\widetilde{\mathcal{K}}(\gamma)$.

Из (6.79) и (6.80) вытекает, что упорядоченная пара $(\widetilde{\mathcal{K}}(\gamma), \mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma)})$ дает возможность определить системами рекуррентных соотношений

$$\begin{cases} q_{t+1} = \alpha_{i_1}(q_t) +_\gamma \alpha_{x_{t+1}}(P_1) \\ y_{t+1} = \alpha_{i_2}(q_t) +_\gamma \alpha_{x_{t+1}}(P_2) \end{cases} \quad (t \in \mathbb{Z}_+) \tag{6.81}$$

и

$$\begin{cases} q_{t+1} = \alpha_{i_1}(q_t) +_\gamma \alpha_{x_{t+1}}(P_1) \\ y_{t+1} = \alpha_{i_2}(q_{t+1}) +_\gamma P_2 \end{cases} \quad (t \in \mathbb{Z}_+), \tag{6.82}$$

соответственно, семейство автоматов Мили $\mathcal{M}^{(1)}(\widetilde{\mathcal{K}}(\gamma), \mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma)})$ и семейство автоматов Мура $\mathcal{M}^{(2)}(\widetilde{\mathcal{K}}(\gamma), \mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma)})$, где $i_1, i_2 \in \mathbb{Z}_{k_1+1}$ – фиксированные числа, $P_1, P_2 \in \widetilde{\mathcal{K}}(\gamma)$ – фиксированные точки, $q_0 \in \widetilde{\mathcal{K}}(\gamma)$ и $x_{t+1} \in \mathbb{Z}_{k_1+1}$ $(t \in \mathbb{Z}_+)$.

6.3.2. Автоматные характеристики исследуемых моделей.

Пусть на многообразии $\mathbf{V} \in \mathcal{V}_{1,n}(\mathcal{K})$ $(n \in \mathbb{N})$ задана алгебра

$$\mathfrak{A}_{\mathbf{V}} = (\mathbf{V}, \mathcal{F}_{1,\mathbf{V}}, \mathcal{F}_{2,\mathbf{V}}),$$

где $\mathcal{F}_{1,\mathbf{V}} = \{\alpha_0, \alpha_1, \ldots, \alpha_{k_1}\}$ $(k_1 \in \mathbb{Z}_+)$ и $\mathcal{F}_{2,\mathbf{V}} = \{\beta_1, \ldots, \beta_{k_2}\}$ $(k_2 \in \mathbb{N})$ есть множество, соответственно, унарных и бинарных операций, определенных на множестве $\mathbf{V}$.

Из (6.79) и (6.80) вытекает, что истинны равенства

$$|\mathcal{M}^{(1)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})| = |\mathcal{M}^{(2)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})| = (k_1+1)^2 k_2^2 |\mathbf{V}|.$$

Положим

$$Val_{\mathbf{v}}\, \mathcal{F}_{1,\mathbf{V}} = \{\alpha_r(\mathbf{v}) \mid r \in \mathbb{N}_{k_1}\}\ (\mathbf{v} \in \mathbf{V}). \tag{6.83}$$

Охарактеризуем свойства автомата $M \in \mathcal{M}^{(1)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}}) \cup \mathcal{M}^{(2)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$, которые формулируются только в терминах функции переходов автомата, т.е. в терминах рекуррентного соотношения

$$\mathbf{q}_{t+1} = \beta_{j_1}(\alpha_{i_1}(\mathbf{q}_t), \alpha_{x_{t+1}}(\mathbf{v}_1)).$$

Напомним, что автомат называется групповым, если для каждого фиксированного входного символа функция переходов является подстановкой на множестве состояний.

Утверждение 6.9. Для многообразия $\mathbf{V} \in \mathcal{V}_{1,n}(\mathcal{K})$ $(n \in \mathbb{N})$ и алгебры $\mathfrak{A}_{\mathbf{V}} = (\mathbf{V}, \mathcal{F}_{1,\mathbf{V}}, \mathcal{F}_{2,\mathbf{V}})$ семейство всех групповых автоматов $M \in \mathcal{M}^{(1)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}}) \cup \mathcal{M}^{(2)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$ определяется множеством всех таких упорядоченных пар $(\alpha_{i_1}, \beta_{j_1}) \in \mathcal{F}_{1,\mathbf{V}} \times \mathcal{F}_{2,\mathbf{V}}$, что $Val\, \alpha_{i_1} = \mathbf{V}$ и $Val\, \beta_{j_1}|_{\mathbf{V}\times\{\mathbf{v}\}} = \mathbf{V}$ для каждого $\mathbf{v} \in Val_{\mathbf{v}_1}\, \mathcal{F}_{1,\mathbf{V}}$.□

Доказательство. Для каждых фиксированных $\mathbf{v}_1 \in \mathbf{V}$ и $x \in \mathbb{Z}_{k_1+1}$ формула

$$\beta_{j_1}(\alpha_{i_1}(\mathbf{q}), \alpha_x(\mathbf{v}_1)) \neq \beta_{j_1}(\alpha_{i_1}(\widetilde{\mathbf{q}}), \alpha_x(\mathbf{v}_1))$$

истинна для всех состояний $\mathbf{q}, \widetilde{\mathbf{q}} \in \mathbf{V}$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ тогда и только тогда, когда

$$Val\, \alpha_{i_1} = \mathbf{V}$$

и

$$Val\, \beta_{j_1}|_{\mathbf{V}\times\{\alpha_x(\mathbf{v}_1)\}} = \mathbf{V}.$$

Следовательно, автомат $M \in \mathcal{M}^{(1)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}}) \cup \mathcal{M}^{(2)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$ является групповым автоматом тогда и только тогда, когда $Val\, \alpha_{i_1} = \mathbf{V}$ и $Val\, \beta_{j_1}|_{\mathbf{V}\times\{\alpha_x(\mathbf{v}_1)\}} = \mathbf{V}$.

Отсюда и из формулы (6.83) вытекает, что утверждение истинно.□

Состояние $\mathbf{q} \in \mathbf{V}$ автомата $M \in \mathcal{M}^{(1)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}}) \cup \mathcal{M}^{(2)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$ называется:

1) источником, если из любого состояния $\widetilde{\mathbf{q}} \in \mathbf{V}$ автомата M невозможен переход в состояние $\mathbf{q}$;

2) стоком, если из состояния $\mathbf{q}$ невозможно перейти ни в какое другое состояние автомата M.

УТВЕРЖДЕНИЕ 6.10. Для автомата $M \in \mathcal{M}^{(1)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}}) \cup \mathcal{M}^{(2)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$ множество

$$\mathbf{V}_{\text{ист}} = \mathbf{V} \backslash Val\,(\beta_{j_1}|_{Val\,\alpha_{i_1} \times Val_{\mathbf{v}_1} \mathcal{F}_{1,\mathbf{V}}}) \tag{6.84}$$

является множеством состояний-источников.□

ДОКАЗАТЕЛЬСТВО. Для любых фиксированных элементов $\mathbf{q}, \mathbf{v}_1 \in \mathbf{V}$ уравнение

$$\mathbf{q} = \beta_{j_1}(\alpha_{i_1}(\widetilde{\mathbf{q}}), \alpha_x(\mathbf{v}_1)) \tag{6.85}$$

имеет решение относительно переменных $\widetilde{\mathbf{q}} \in \mathbf{V}$ и $x \in \mathbb{Z}_{k_1+1}$ тогда и только тогда, когда

$$\mathbf{q} \in \bigcup_{\widetilde{\mathbf{q}} \in \mathbf{V}, x \in \mathbb{Z}_{k_1+1}} Val\,(\beta_{j_1}|_{\{(\alpha_{i_1}(\widetilde{\mathbf{q}}), \alpha_x(\mathbf{v}_1))\}}).$$

При этом

$$\bigcup_{\widetilde{\mathbf{q}} \in \mathbf{V}, x \in \mathbb{Z}_{k_1+1}} Val\,(\beta_{j_1}|_{\{(\alpha_{i_1}(\widetilde{\mathbf{q}}), \alpha_x(\mathbf{v}_1))\}}) =$$

$$= \bigcup_{\widetilde{\mathbf{q}} \in \mathbf{V}} \Bigg(\bigcup_{x \in \mathbb{Z}_{k_1+1}} Val\,(\beta_{j_1}|_{\{(\alpha_{i_1}(\widetilde{\mathbf{q}}), \alpha_x(\mathbf{v}_1))\}}) \Bigg) =$$

$$= \bigcup_{\widetilde{\mathbf{q}} \in \mathbf{V}} \Big(Val\,(\beta_{j_1}|_{\{\alpha_{i_1}(\widetilde{\mathbf{q}})\} \times Val_{\mathbf{v}_1} \mathcal{F}_{1,\mathbf{V}}}) \Big) = Val\,(\beta_{j_1}|_{Val\,\alpha_{i_1} \times Val_{\mathbf{v}_1} \mathcal{F}_{1,\mathbf{V}}}).$$

Таким образом, для любых фиксированных элементов $\mathbf{q}, \mathbf{v}_1 \in \mathbf{V}$ уравнение (6.85) имеет решение относительно переменных $\widetilde{\mathbf{q}} \in \mathbf{V}$ и $x \in \mathbb{Z}_{k_1+1}$ тогда и только тогда, когда $\mathbf{q} \in Val\,(\beta_{j_1}|_{Val\,\alpha_{i_1} \times Val_{\mathbf{v}_1} \mathcal{F}_{1,\mathbf{V}}})$. Отсюда и из определения состояния-источника вытекает равенство (6.84).□

УТВЕРЖДЕНИЕ 6.11. Для автомата $M \in \mathcal{M}^{(1)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}}) \cup \mathcal{M}^{(2)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$ множество

$$\mathbf{V}_{\text{ст}} = \{\mathbf{q} \in \mathbf{V} \mid \{\mathbf{q}\} = Val\,(\beta_{j_1}|_{Val\,\alpha_{i_1} \times Val_{\mathbf{v}_1} \mathcal{F}_{1,\mathbf{V}}})\} \tag{6.86}$$

является множеством состояний-стоков.□

Доказательство. Для любых фиксированных элементов $\mathbf{q}, \mathbf{v}_1 \in \mathbf{V}$ уравнение

$$\widetilde{\mathbf{q}} = \beta_{j_1}(\alpha_{i_1}(\mathbf{q}), \alpha_x(\mathbf{v}_1)) \tag{6.87}$$

не имеет решения относительно переменных $\widetilde{\mathbf{q}} \in \mathbf{V}\backslash\{\mathbf{q}\}$ и $x \in \mathbb{Z}_{k_1+1}$ тогда и только тогда, когда

$$\bigcup_{x \in \mathbb{Z}_{k_1+1}} Val\,(\beta_{j_1}|_{\{(\alpha_{i_1}(\mathbf{q}), \alpha_x(\mathbf{v}_1))\}}) = \{\mathbf{q}\}.$$

При этом

$$\bigcup_{x \in \mathbb{Z}_{k_1+1}} Val\,(\beta_{j_1}|_{\{(\alpha_{i_1}(\mathbf{q}), \alpha_x(\mathbf{v}_1))\}}) = Val\,(\beta_{j_1}|_{\{\alpha_{i_1}(\mathbf{q})\} \times Val_{\mathbf{v}_1} \mathcal{F}_{1,\mathbf{V}}}).$$

Следовательно, для любых фиксированных элементов $\mathbf{q}, \mathbf{v}_1 \in \mathbf{V}$ уравнение (6.87) не имеет решения относительно переменных $\widetilde{\mathbf{q}} \in \mathbf{V}\backslash\{\mathbf{q}\}$ и $x \in \mathbb{Z}_{k_1+1}$ тогда и только тогда, когда $Val\,(\beta_{j_1}|_{\{\alpha_{i_1}(\mathbf{q})\} \times Val_{\mathbf{v}_1} \mathcal{F}_{1,\mathbf{V}}}) = \mathbf{q}$. Отсюда и из определения состояния-стока вытекает равенство (6.86).□

Охарактеризуем свойства автомата $M \in \mathcal{M}^{(1)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}}) \cup \mathcal{M}^{(2)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$, при формулировке которых существенно используется функция выходов автомата.

Для автомата $M \in \mathcal{M}^{(1)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}}) \cup \mathcal{M}^{(2)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$ определим на многообразии $\mathbf{V} \in \mathcal{V}_{1,n}(\mathcal{K})$ $(n \in \mathbb{N})$ такие отношения эквивалентности $\varepsilon_1(\mathbf{v})$ $(\mathbf{v} \in Val_{\mathbf{v}_1} \mathcal{F}_{1,\mathbf{V}})$, $\varepsilon_2(\mathbf{v})$ $(\mathbf{v} \in Val_{\mathbf{v}_2} \mathcal{F}_{1,\mathbf{V}})$ и $\varepsilon_3(\mathbf{v})$ $(\mathbf{v} \in Val_{\mathbf{v}_1} \mathcal{F}_{1,\mathbf{V}})$, что:

$$(\mathbf{q}, \widetilde{\mathbf{q}}) \in \varepsilon_1(\mathbf{v}) \Leftrightarrow \beta_{j_1}(\alpha_{i_1}(\mathbf{q}), \mathbf{v}) = \beta_{j_1}(\alpha_{i_1}(\widetilde{\mathbf{q}}), \mathbf{v}), \tag{6.88}$$

$$(\mathbf{q}, \widetilde{\mathbf{q}}) \in \varepsilon_2(\mathbf{v}) \Leftrightarrow \beta_{j_2}(\alpha_{i_2}(\mathbf{q}), \mathbf{v}) = \beta_{j_2}(\alpha_{i_2}(\widetilde{\mathbf{q}}), \mathbf{v}) \tag{6.89}$$

и

$$(\mathbf{q}, \widetilde{\mathbf{q}}) \in \varepsilon_3(\mathbf{v}) \Leftrightarrow$$

$$\Leftrightarrow \beta_{j_2}(\alpha_{i_2}(\beta_{j_1}(\alpha_{i_1}(\mathbf{q}), \mathbf{v})), \mathbf{v}_2) = \beta_{j_2}(\alpha_{i_2}(\beta_{j_1}(\alpha_{i_1}(\widetilde{\mathbf{q}}), \mathbf{v})), \mathbf{v}_2). \tag{6.90}$$

Положим

$$\varepsilon_1 = \bigcap_{\mathbf{v} \in Val_{\mathbf{v}_1} \mathcal{F}_{1,\mathbf{V}}} \varepsilon_1(\mathbf{v}), \tag{6.91}$$

$$\varepsilon_2 = \bigcap_{\mathbf{v} \in Val_{\mathbf{v}_2} \mathcal{F}_{1,\mathbf{V}}} \varepsilon_2(\mathbf{v}) \tag{6.92}$$

и

$$\varepsilon_3 = \bigcap_{\mathbf{v} \in Val_{\mathbf{v}_1} \mathcal{F}_{1,\mathbf{V}}} \varepsilon_3(\mathbf{v}). \tag{6.93}$$

Напомним, что два различных состояния автомата называются близнецами, если каждый входной символ переводит их в одно и то же состояние, и при этом автомат выдает одинаковые выходные символы.

Из (6.88), (6.89), (6.91) и (6.92) непосредственно вытекает, что истинно следующее утверждение.

Утверждение 6.12. Для автомата $M \in \mathcal{M}^{(1)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$ состояния $\mathbf{q}, \widetilde{\mathbf{q}} \in \mathbf{V}$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ являются близнецами тогда и только тогда, когда $(\mathbf{q}, \widetilde{\mathbf{q}}) \in \varepsilon_1 \cap \varepsilon_2$.□

Аналогичным образом, из (6.88), (6.90), (6.91) и (6.93) непосредственно вытекает, что истинно следующее утверждение.

Утверждение 6.13. Для автомата $M \in \mathcal{M}^{(2)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$ состояния $\mathbf{q}, \widetilde{\mathbf{q}} \in \mathbf{V}$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ являются близнецами тогда и только тогда, когда $(\mathbf{q}, \widetilde{\mathbf{q}}) \in \varepsilon_1 \cap \varepsilon_3$.□

Замечание 6.10. Из утверждений 6.12 и 6.13 вытекает, что:

1) максимальными множествами состояний-близнецов автомата $M \in \mathcal{M}^{(1)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$ являются такие элементы $\mathbf{S}$ фактор-множества $\mathbf{V}/_{\varepsilon_1 \cap \varepsilon_2}$, что $|\mathbf{S}| \geq 2$;

2) максимальными множествами состояний-близнецов автомата $M \in \mathcal{M}^{(2)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$ являются такие элементы $\mathbf{S}$ фактор-множества $\mathbf{V}/_{\varepsilon_1 \cap \varepsilon_3}$, что $|\mathbf{S}| \geq 2$.

Автомат называется явно приведенным (говорят также, что автомат является 1-диагностируемым), если для любых двух его различных состояний существует входной символ, который различает эти состояния.

Из (6.89) и (6.92) непосредственно вытекает, что истинно следующее утверждение.

Утверждение 6.14. Автомат $M \in \mathcal{M}^{(1)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$ является явно приведенным тогда и только тогда, когда отношение эквивалентности ε_2 является отношением равенства на множестве $\mathbf{V}$.□

Аналогичным образом, из (6.90) и (6.93) непосредственно вытекает, что истинно следующее утверждение.

Утверждение 6.15. Автомат $M \in \mathcal{M}^{(2)}(\mathbf{V}, \mathfrak{A}_{\mathbf{V}})$ является явно приведенным тогда и только тогда, когда отношение эквивалентности ε_3 является отношением равенства на множестве $\mathbf{V}$.□

6.3.3. Гомоморфизмы исследуемых моделей.

Напомним, что понятие «гомоморфизм» для абстрактных автоматов определяется следующим образом.

Гомоморфным образом автомата $M = (Q, X, Y, \delta, \lambda)$ называется такой автомат $M' = (Q', X', Y', \delta', \lambda')$, что существует такая тройка сюръекций (χ_1, χ_2, χ_3) (где $\chi_1 : Q \to Q'$, $\chi_2 : X \to X'$ и $\chi_3 : Q \to Y'$), что равенства

$$\chi_1(\delta(q,x)) = \delta'(\chi_1(q),\chi_2(x))$$

и

$$\chi_3(\lambda(q,x)) = \lambda'(\chi_1(q),\chi_2(x))$$

истинны для всех $q \in Q$ и $x \in X$. В частности, если χ_1, χ_2, χ_3 – биекции, то автоматы M и M' называются изоморфными.

Гомоморфизм упорядоченной пары $(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1})$ ($\mathbf{V}_1 \in \mathcal{V}_{1,n_1}(\mathcal{K}_1)$) на упорядоченную пару $(\mathbf{V}_2, \mathfrak{A}_{\mathbf{V}_2})$ ($\mathbf{V}_2 \in \mathcal{V}_{1,n_2}(\mathcal{K}_2)$), где $\mathfrak{A}_{\mathbf{V}_r} = (\mathbf{V}_r, \mathcal{F}_{1,\mathbf{V}_r}, \mathcal{F}_{2,\mathbf{V}_r})$ $(r = 1, 2)$ – алгебра, а

$$\mathcal{F}_{1,\mathbf{V}_r} = \{\alpha_0^{(r)}, \alpha_1^{(r)}, \ldots, \alpha_{k_1}^{(r)}\}$$

и

$$\mathcal{F}_{2,\mathbf{V}_r} = \{\beta_1^{(r)}, \ldots, \beta_{k_2}^{(r)}\}$$

есть множество, соответственно, унарных и бинарных операций, определен в п.6.2.1 как тройка отображений

$$\Phi = (\varphi_1, \varphi_2, \varphi_3)$$

где $\varphi_1 : \mathbf{V}_1 \to \mathbf{V}_2$ – сюръекция, а $\varphi_2 : \mathcal{F}_{1,\mathbf{V}_1} \to \mathcal{F}_{1,\mathbf{V}_2}$ и $\varphi_3 : \mathcal{F}_{2,\mathbf{V}_1} \to \mathcal{F}_{2,\mathbf{V}_2}$ – биекции, удовлетворяющих равенствам (6.75) и (6.76).

Следующая теорема устанавливает, каким образом связаны между собой гомоморфизм

$$\Phi = (\varphi_1, \varphi_2, \varphi_3)$$

упорядоченной пары $(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1})$ на упорядоченную пару $(\mathbf{V}_2, \mathfrak{A}_{\mathbf{V}_2})$ и гомоморфные образы автоматов $M_r \in \mathcal{M}^{(r)}(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1})$ $(r = 1, 2)$, которые принадлежат семейству автоматов $\mathcal{M}^{(r)}(\mathbf{V}_2, \mathfrak{A}_{\mathbf{V}_2})$.

Теорема 6.8. Если упорядоченная пара $(\mathbf{V}_2, \mathfrak{A}_{\mathbf{V}_2})$ ($\mathbf{V}_2 \in \mathcal{V}_{1,n_2}(\mathcal{K}_2)$) – гомоморфный образ упорядоченной пары $(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1})$ ($\mathbf{V}_1 \in \mathcal{V}_{1,n_1}(\mathcal{K}_1)$), то существуют такие отображения

$$\Psi_r : \mathcal{M}^{(r)}(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1}) \to \mathcal{M}^{(r)}(\mathbf{V}_2, \mathfrak{A}_{\mathbf{V}_2}) \ (r = 1, 2), \tag{6.94}$$

что автомат $\Psi_r(M_r)$ ($M_r \in \mathcal{M}^{(r)}(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1})$) – гомоморфный образ автомата M_r.□

Доказательство. Предположим, что упорядоченная пара $(\mathbf{V}_2, \mathfrak{A}_{\mathbf{V}_2})$ ($\mathbf{V}_2 \in \mathcal{V}_{1,n_2}(\mathcal{K}_2)$) – гомоморфный образ упорядоченной пары $(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1})$ ($\mathbf{V}_1 \in \mathcal{V}_{1,n_1}(\mathcal{K}_1)$), а тройка отображений

$$\Phi = (\varphi_1, \varphi_2, \varphi_3),$$

где $\varphi_1 : \mathbf{V}_1 \to \mathbf{V}_2$, $\varphi_2 : \mathcal{F}_1^{(1)} \to \mathcal{F}_1^{(2)}$ и $\varphi_3 : \mathcal{F}_2^{(1)} \to \mathcal{F}_2^{(2)}$, определяет гомоморфизм упорядоченной пары $(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1})$ на упорядоченную пару $(\mathbf{V}_2, \mathfrak{A}_{\mathbf{V}_2})$.

Рассмотрим такие отображения (6.94), что:

1) для автомата $M_1 \in \mathcal{M}^{(1)}(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1})$, заданного системой рекуррентных соотношений

$$\begin{cases} \mathbf{q}_{t+1}^{(1)} = \beta_{j_1}^{(1)}(\alpha_{i_1}^{(1)}(\mathbf{q}_t^{(1)}), \alpha_{x_{t+1}}^{(1)}(\mathbf{v}_1^{(1)})) \\ \mathbf{y}_{t+1}^{(1)} = \beta_{j_2}^{(1)}(\alpha_{i_2}^{(1)}(\mathbf{q}_t^{(1)}), \alpha_{x_{t+1}}^{(1)}(\mathbf{v}_2^{(1)})) \end{cases} \quad (t \in \mathbb{Z}_+), \tag{6.95}$$

автомат $\Psi_1(M_1) \in \mathcal{M}^{(1)}(\mathbf{V}_2, \mathfrak{A}_{\mathbf{V}_2})$ задан системой рекуррентных соотношений

$$\begin{cases} \mathbf{q}_{t+1}^{(2)} = \varphi_3(\beta_{j_1}^{(1)})(\varphi_2(\alpha_{i_1}^{(1)})(\mathbf{q}_t^{(2)}), \varphi_2(\alpha_{x_{t+1}}^{(1)})(\mathbf{v}_1^{(2)})) \\ \mathbf{y}_{t+1}^{(2)} = \varphi_3(\beta_{j_2}^{(1)})(\varphi_2(\alpha_{i_2}^{(1)})(\mathbf{q}_t^{(2)}), \varphi_2(\alpha_{x_{t+1}}^{(1)})(\mathbf{v}_2^{(2)})) \end{cases} \quad (t \in \mathbb{Z}_+); \tag{6.96}$$

2) для автомата $M_2 \in \mathcal{M}^{(2)}(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1})$, заданного системой рекуррентных соотношений

$$\begin{cases} \mathbf{q}_{t+1}^{(1)} = \beta_{j_1}^{(1)}(\alpha_{i_1}^{(1)}(\mathbf{q}_t^{(1)}), \alpha_{x_{t+1}}^{(1)}(\mathbf{v}_1^{(1)})) \\ \mathbf{y}_{t+1}^{(1)} = \beta_{j_2}^{(1)}(\alpha_{i_2}^{(1)}(\mathbf{q}_{t+1}^{(1)}), \mathbf{v}_2^{(1)}) \end{cases} \quad (t \in \mathbb{Z}_+), \tag{6.97}$$

автомат $\Psi_2(M_2) \in \mathcal{M}^{(2)}(\mathbf{V}_2, \mathfrak{A}_{\mathbf{V}_2})$ задан системой рекуррентных соотношений

$$\begin{cases} \mathbf{q}_{t+1}^{(2)} = \varphi_3(\beta_{j_1}^{(1)})(\varphi_2(\alpha_{i_1}^{(1)})(\mathbf{q}_t^{(2)}), \varphi_2(\alpha_{x_{t+1}}^{(1)})(\mathbf{v}_1^{(2)})) \\ \mathbf{y}_{t+1}^{(2)} = \varphi_3(\beta_{j_2}^{(1)})(\varphi_2(\alpha_{i_2}^{(1)})(\mathbf{q}_{t+1}^{(2)}), \mathbf{v}_2^{(2)})) \end{cases} \quad (t \in \mathbb{Z}_+). \tag{6.98}$$

Из (6.95)-(6.98) вытекает, что для всех $t \in \mathbb{Z}_+$ истинны равенства

$$\varphi_1(\beta_{j_1}^{(1)}(\alpha_{i_1}^{(1)}(\mathbf{q}_t^{(1)}), \alpha_{x_{t+1}}^{(1)}(\mathbf{v}_1^{(1)}))) =$$

$$= \varphi_3(\beta_{j_1}^{(1)})(\varphi_2(\alpha_{i_1}^{(1)})(\varphi_1(\mathbf{q}_t^{(1)})), \varphi_2(\alpha_{x_{t+1}}^{(1)})(\varphi_1(\mathbf{v}_1^{(1)}))), \tag{6.99}$$

$$\varphi_1(\beta_{j_2}^{(1)}(\alpha_{i_2}^{(1)}(\mathbf{q}_t^{(1)}), \alpha_{x_{t+1}}^{(1)}(\mathbf{v}_2^{(1)}))) =$$

$$= \varphi_3(\beta_{j_2}^{(1)})(\varphi_2(\alpha_{i_2}^{(1)})(\varphi_1(\mathbf{q}_t^{(1)})), \varphi_2(\alpha_{x_{t+1}}^{(1)})(\varphi_1(\mathbf{v}_2^{(1)}))) \tag{6.100}$$

и

$$\varphi_1(\beta_{j_2}^{(1)}(\alpha_{i_2}^{(1)}(\mathbf{q}_{t+1}^{(1)}), \mathbf{v}_2^{(1)})) = \varphi_3(\beta_{j_2}^{(1)})(\varphi_2(\alpha_{i_2}^{(1)})(\varphi_1(\mathbf{q}_{t+1}^{(1)})), \varphi_1(\mathbf{v}_2^{(1)})). \tag{6.101}$$

Из (6.99) и (6.100) вытекает, что автомат $\Psi_1(M_1) \in \mathcal{M}^{(1)}(\mathbf{V}_2, \mathfrak{A}_{\mathbf{V}_2})$ – гомоморфный образ автомата $M_1 \in \mathcal{M}^{(1)}(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1})$, а из (6.99) и (6.101)

вытекает, что автомат $\Psi_2(M_2) \in \mathcal{M}^{(2)}(\mathbf{V}_2, \mathfrak{A}_{\mathbf{V}_2})$ – гомоморфный образ автомата $M_2 \in \mathcal{M}^{(2)}(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1})$.$\square$

Замечание 6.11. Из равенств (6.99)-(6.101) вытекает, что для тройки сюръекций (χ_1, χ_2, χ_3), определяющей гомоморфизм автомата $M_r \in \mathcal{M}^{(r)}(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1})$ $(r = 1, 2)$ на автомат $\Psi_r(M_r) \in \mathcal{M}^{(r)}(\mathbf{V}_2, \mathfrak{A}_{\mathbf{V}_2})$ истинно равенство $\chi_1 = \chi_3 = \varphi_1$, а значения $\chi_2(i) \in \mathbb{Z}_{k_1+1}$ $(i \in \mathbb{Z}_{k_1+1})$ определяются равенствами

$$\alpha^{(2)}_{\chi_2(i)}(\varphi_1(\mathbf{v}^{(1)}_1)) = \alpha^{(1)}_i(\mathbf{v}^{(1)}_1).$$

Из теоремы 6.8 непосредственно вытекает, что истинно следующее следствие.

Следствие 6.5. Если упорядоченные пары $(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1})$ $(\mathbf{V}_1 \in \mathcal{V}_{1,n_1}(\mathcal{K}_1))$ и $(\mathbf{V}_2, \mathfrak{A}_{\mathbf{V}_2})$ $(\mathbf{V}_2 \in \mathcal{V}_{1,n_2}(\mathcal{K}_2))$ изоморфны, то существуют такие отображения $\Psi_r : \mathcal{M}^{(r)}(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1}) \to \mathcal{M}^{(r)}(\mathbf{V}_2, \mathfrak{A}_{\mathbf{V}_2})$ $(r = 1, 2)$, что автоматы $M_r \in \mathcal{M}^{(r)}(\mathbf{V}_1, \mathfrak{A}_{\mathbf{V}_1})$ и $\Psi_r(M_r)$ изоморфны.$\square$

Пример 6.5. Пусть γ_1 и γ_2 – такие эллиптические кривые, заданные над областью целостности $\mathcal{K}$, что упорядоченная пара $(\widetilde{\mathcal{K}}(\gamma_2), \mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_2)})$ изоморфна упорядоченной паре $(\widetilde{\mathcal{K}}(\gamma_1), \mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_1)})$, где $\mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_r)} = (\widetilde{\mathcal{K}}(\gamma_r), \mathcal{F}^{(r)}_1, \mathcal{F}^{(r)}_2)$ $(r = 1, 2)$, а $\mathcal{F}^{(r)}_1 = \{\alpha^{(r)}_0, \alpha^{(r)}_1, \ldots, \alpha^{(r)}_{k_1}\}$ и $\mathcal{F}^{(r)}_2 = \{+_{\gamma_r}\}$ являются множествами, соответственно, унарных и бинарных операций, определенных на множестве $\widetilde{\mathcal{K}}(\gamma_r)$.

Из теоремы 6.8 вытекает, что существуют такие отображения

$$\Psi_r : \mathcal{M}^{(r)}(\widetilde{\mathcal{K}}(\gamma_1), \mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_1)}) \to \mathcal{M}^{(r)}(\widetilde{\mathcal{K}}(\gamma_2), \mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_2)}) \ (r = 1, 2)$$

что автомат $\Psi_r(M_r)$ $(M_r \in \mathcal{M}^{(r)}(\widetilde{\mathcal{K}}(\gamma_1), \mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_1)})$ – гомоморфный образ автомата M_r.

При этом, из доказательства теоремы 6.8 вытекает, что:

1) для автомата $M_1 \in \mathcal{M}^{(1)}(\widetilde{\mathcal{K}}(\gamma_1), \mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_1)})$, заданного системой рекуррентных соотношений

$$\begin{cases} q^{(1)}_{t+1} = \alpha^{(1)}_{i_1}(q^{(1)}_t) +_{\gamma_1} \alpha^{(1)}_{x_{t+1}}(P^{(1)}_1) \\ y^{(1)}_{t+1} = \alpha^{(1)}_{i_2}(q^{(1)}_t) +_{\gamma_1} \alpha^{(1)}_{x_{t+1}}(P^{(1)}_2) \end{cases} \quad (t \in \mathbb{Z}_+),$$

автомат $\Psi_1(M_1) \in \mathcal{M}^{(1)}(\widetilde{\mathcal{K}}(\gamma_2), \mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_2)})$ задан системой рекуррентных соотношений

$$\begin{cases} q^{(2)}_{t+1} = \alpha^{(2)}_{i_1}(q^{(2)}_t) +_{\gamma_2} \alpha^{(2)}_{x_{t+1}}(P^{(2)}_1) \\ y^{(2)}_{t+1} = \alpha^{(2)}_{i_2}(q^{(2)}_t) +_{\gamma_2} \alpha^{(2)}_{x_{t+1}}(P^{(2)}_2) \end{cases} \quad (t \in \mathbb{Z}_+);$$

2) для автомата $M_2 \in \mathcal{M}^{(2)}(\widetilde{\mathcal{K}}(\gamma_1), \mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_1)})$, заданного системой рекуррентных соотношений

$$\begin{cases} q^{(1)}_{t+1} = \alpha^{(1)}_{i_1}(q^{(1)}_t) +_{\gamma_1} \alpha^{(1)}_{x_{t+1}}(P^{(1)}_1) \\ y^{(1)}_{t+1} = \alpha^{(1)}_{i_2}(q^{(1)}_{t+1}) +_{\gamma_1} P^{(1)}_2 \end{cases} \quad (t \in \mathbb{Z}_+),$$

автомат $\Psi_2(M_2) \in \mathcal{M}^{(2)}(\widetilde{\mathcal{K}}(\gamma_2), \mathfrak{A}_{\widetilde{\mathcal{K}}(\gamma_2)})$ задан системой рекуррентных соотношений

$$\begin{cases} q^{(2)}_{t+1} = \alpha^{(2)}_{i_1}(q^{(2)}_t) +_{\gamma_2} \alpha^{(2)}_{x_{t+1}}(P^{(2)}_1) \\ y^{(2)}_{t+1} = \alpha^{(2)}_{i_2}(q^{(2)}_{t+1}) +_{\gamma_2} P^{(2)}_2 \end{cases} \quad (t \in \mathbb{Z}_+).$$

6.4. Автоматы на параметризованных многообразиях.

Определим автоматы Мили и Мура на многообразии $\mathbf{V} \in \mathcal{V}_{2,n}(\mathcal{K})$, где $\mathcal{K} = (K, +, \cdot) \in \mathfrak{K}^{fnt}$ и $n \in \mathbb{N}$, и исследуем свойства таких автоматов.

6.4.1. Исследуемые модели.

Пусть $\mathbf{V} \in \mathcal{V}_{2,n}(\mathcal{K})$ и $\mathbf{v} = \mathbf{h}(\mathbf{t})$ $(\mathbf{t} \in K^m)$ – параметризация многообразия $\mathbf{V}$ (где $\mathbf{h} = (h_1, \ldots, h_n)^T$ – набор многочленов от m $(m < n)$ переменных $t_1, \ldots, t_m$ над кольцом $\mathcal{K}$). Зафиксировав семейство отображений $\Theta = \{\theta_i\}_{i \in \mathbb{N}_k}$ (где $\theta_i : K^m \to K^m$ для всех $i \in \mathbb{N}_k$), мы определяем упорядоченную пару $(\mathbf{V}, \Theta)$.

Упорядоченная пара $(\mathbf{V}, \Theta)$ дает возможность для любого числа $l \in \mathbb{N}$ определить семейство автоматов Мили $\mathcal{M}^{(1)}_{n,k,l}(\mathbf{V}, \Theta)$ и семейство автоматов Мура $\mathcal{M}^{(2)}_{n,k,l}(\mathbf{V}, \Theta)$, соответственно, системой рекуррентных соотношений

$$\begin{cases} \mathbf{q}_{t+1} = \mathbf{h}(\theta_{x_{t+1}}(\mathbf{t}_t)) \\ \mathbf{y}_{t+1} = \mathbf{g}_{x_{t+1}}(\mathbf{q}_t) \end{cases} \quad (t \in \mathbb{N}) \tag{6.102}$$

и системой рекуррентных соотношений

$$\begin{cases} \mathbf{q}_{t+1} = \mathbf{h}(\theta_{x_{t+1}}(\mathbf{t}_t)) \\ \mathbf{y}_{t+1} = \mathbf{g}(\mathbf{q}_{t+1}) \end{cases} \quad (t \in \mathbb{N}), \tag{6.103}$$

где $\mathbf{t}_0 \in K^m$, $\mathbf{q}_0 = \mathbf{h}(\mathbf{t}_0)$, $\mathbf{t}_{t+1} = \theta_{x_{t+1}}(\mathbf{t}_t)$ $(t \in \mathbb{Z}_+)$, $\mathbf{g}_i : K^n \to K^l$ $(i \in \mathbb{N}_k)$, $\mathbf{g} : K^n \to K^l$ $(i \in \mathbb{N}_k)$ и $x_{t+1} \in \mathbb{N}_k$ $(t \in \mathbb{Z}_+)$.

Для каждого автомата $M \in \mathcal{M}^{(1)}_{n,k,l}(\mathbf{V}, \Theta) \cup \mathcal{M}^{(2)}_{n,k,l}(\mathbf{V}, \Theta)$ элементы x_t, $\mathbf{q}_t$ и $\mathbf{y}_t$ являются, соответственно, входным символом, состоянием и выходным символом в момент t.

Поэтому, для каждого автомата $M \in \mathcal{M}^{(1)}_{n,k,l}(\mathbf{V}, \Theta) \cup \mathcal{M}^{(2)}_{n,k,l}(\mathbf{V}, \Theta)$ множество чисел $\mathbb{N}_k$ является входным алфавитом, а многообразие $\mathbf{V}$ – множеством состояний.

Выходным алфавитом автомата $M \in \mathcal{M}^{(1)}_{n,k,l}(\mathbf{V}, \Theta)$ является множество $\bigcup\limits_{i \in \mathbb{Z}_k} Val\,(\mathbf{g}_i|_{\mathbf{V}})$, а выходным алфавитом автомата $M \in \mathcal{M}^{(2)}_{n,k,l}(\mathbf{V}, \Theta)$ – множество $Val\,(\mathbf{g}|_{\mathbf{V}})$.

Положим

$$\mathcal{M}^{(r)}_{n,k}(\mathbf{V}, \Theta) = \bigcup_{l=1}^{\infty} \mathcal{M}^{(r)}_{n,k,l}(\mathbf{V}, \Theta) \ (r = 1, 2).$$

Обозначим через $\mathcal{F}_m(\mathcal{K})$ множество всех отображений $f : K^m \to K^m$.

При определении семейства автоматов Мили $\mathcal{M}^{(1)}_{n,k,l}(\mathbf{V}, \Theta)$ и семейства автоматов Мура $\mathcal{M}^{(2)}_{n,k,l}(\mathbf{V}, \Theta)$ не было наложено никаких ограничений на отображения, принадлежащие семейству $\Theta = \{\theta_i\}_{i\in\mathbb{N}_k}$, т.е. элементами семейства Θ могут быть любые элементы множества $\mathcal{F}_m(\mathcal{K})$.

Такая общность естественно приводит к широкому классу семейств автоматов, определяемых формулами (6.102) и (6.103).

Охарактеризуем этот класс семейств автоматов.

Как было отмечено в п.6.2.2, каждое отображение $f \in \mathcal{F}_m$ определяет на многообразии $\mathbf{V}$ множество $\mathcal{T}_{\mathbf{V},f}$ траекторий

$$\mathbf{h}(\mathbf{t}_0), \mathbf{h}(\mathbf{t}_1), \ldots, \mathbf{h}(\mathbf{t}_j), \ldots \quad (\mathbf{t}_0 \in K^m), \tag{6.104}$$

где $\mathbf{t}_{j+1} = f(\mathbf{t}_j)$ для всех $j \in \mathbb{Z}_+$. Будем говорить, что траектория (6.104) исходит из точки $\mathbf{h}(P_0)$ многообразия $\mathbf{V}$.

Имеет место следующая теорема.

Теорема 6.9. Пусть $\mathbf{v} = \mathbf{h}(\mathbf{t})$ $(\mathbf{t} \in K^m)$ – параметризация многообразия $\mathbf{V} \in \mathcal{V}_{2,n}(\mathcal{K})$, а $f \in \mathcal{F}_m(\mathcal{K})$. Любые две различные траектории, принадлежащие множеству $\mathcal{T}_{\mathbf{V},f}$, исходят из различных точек многообразия $\mathbf{V}$ тогда и только тогда, когда не существуют такие точки $\mathbf{t}_0^{(1)}, \mathbf{t}_0^{(2)} \in K^m$, что $\mathbf{t}_0^{(1)} \equiv \mathbf{t}_0^{(2)}$ $(\ker \mathbf{h})$ и $\mathbf{t}_0^{(1)} \not\equiv \mathbf{t}_0^{(2)}$ $(\ker(\mathbf{h} \circ f))$.□

Доказательство. Из (6.104) вытекает, что точки $\mathbf{t}_0^{(1)}, \mathbf{t}_0^{(2)} \in K^m$ определяют, соответственно, принадлежащие множеству $\mathcal{T}_{\mathbf{V},f}$ траектории

$$\mathbf{h}(\mathbf{t}_0^{(1)}), \mathbf{h}(\mathbf{t}_1^{(1)}), \ldots, \mathbf{h}(\mathbf{t}_j^{(1)}), \ldots, \tag{6.105}$$

и

$$\mathbf{h}(\mathbf{t}_0^{(2)}), \mathbf{h}(\mathbf{t}_1^{(2)}), \ldots, \mathbf{h}(\mathbf{t}_j^{(2)}), \ldots, \tag{6.106}$$

где

$$\mathbf{t}_{j+1}^{(i)} = f(\mathbf{t}_j^{(i)}) \ (i = 1, 2)$$

для всех $j \in \mathbf{Z}_+$.

Предположим, что существуют точки $\mathbf{t}_0^{(1)}, \mathbf{t}_0^{(2)} \in K^m$, удовлетворяющие условию «$\mathbf{t}_0^{(1)} \equiv \mathbf{t}_0^{(2)}$ $(\ker \mathbf{h})$ и $\mathbf{t}_0^{(1)} \not\equiv \mathbf{t}_0^{(2)}$ $(\ker(\mathbf{h} \circ f))$».

Так как $\mathbf{t}_0^{(1)} \equiv \mathbf{t}_0^{(2)}$ $(\ker \mathbf{h})$, то $\mathbf{h}(\mathbf{t}_0^{(1)}) = \mathbf{h}(\mathbf{t}_0^{(2)})$.

А так как $\mathbf{t}_0^{(1)} \not\equiv \mathbf{t}_0^{(2)}$ $(\ker(\mathbf{h} \circ f))$, то

$$\mathbf{h}(\mathbf{t}_1^{(1)}) = (\mathbf{h} \circ f)(\mathbf{t}_0^{(1)}) \neq (\mathbf{h} \circ f)(\mathbf{t}_0^{(2)}) = \mathbf{h}(\mathbf{t}_1^{(2)}).$$

Из соотношений

$$\mathbf{h}(\mathbf{t}_0^{(1)}) = \mathbf{h}(\mathbf{t}_0^{(2)})$$

и

$$\mathbf{h}(\mathbf{t}_1^{(1)}) \neq \mathbf{h}(\mathbf{t}_1^{(2)})$$

вытекает, что (6.105) и (6.106) являются двумя различными траекториями, принадлежащими множеству $\mathcal{T}_{\mathbf{V},f}$, и исходящие из одной и той же точки многообразия $\mathbf{V}$, что и требовалось доказать.

Рассмотренная выше ситуация схематически представлена на рис. 6.2.

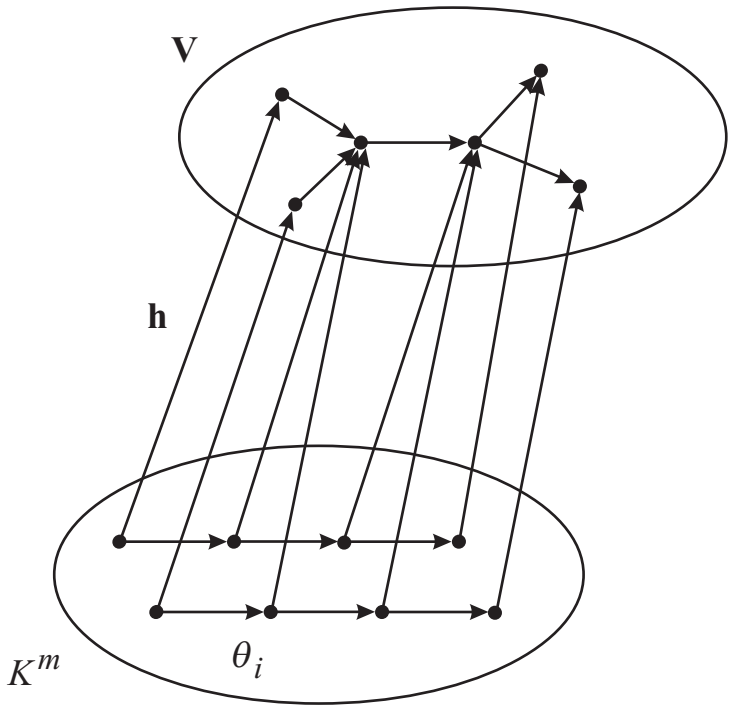


Рис. 6.2. Различные траектории в многообразии $\mathbf{V} \in \mathcal{V}_{2,n}(\mathcal{K})$, исходящие из одной точки.

Предположим теперь, что любые точки $\mathbf{t}_0^{(1)}, \mathbf{t}_0^{(2)} \in K^m$ $(\mathbf{t}_0^{(1)} \neq \mathbf{t}_0^{(2)})$ не удовлетворяют условию «$\mathbf{t}_0^{(1)} \equiv \mathbf{t}_0^{(2)}\,(\ker \mathbf{h})$ и $\mathbf{t}_0^{(1)} \not\equiv \mathbf{t}_0^{(2)}\,(\ker(\mathbf{h} \circ f))$». Такое предположение эквивалентно тому, что для любых двух различных точек $\mathbf{t}_0^{(1)}, \mathbf{t}_0^{(2)} \in K^m$ выполнено условие «$\mathbf{t}_0^{(1)} \not\equiv \mathbf{t}_0^{(2)}\,(\ker \mathbf{h})$ или $\mathbf{t}_0^{(1)} \equiv \mathbf{t}_0^{(2)}\,(\ker(\mathbf{h} \circ f))$».

Возможны следующие два случая.

Случай 6.1. Пусть $\mathbf{t}_0^{(1)} \not\equiv \mathbf{t}_0^{(2)}\,(\ker \mathbf{h})$.

Так как $\mathbf{h}(\mathbf{t}_0^{(1)}) \neq \mathbf{h}(\mathbf{t}_0^{(2)})$, то (6.105) и (6.106) являются двумя различными траекториями, принадлежащими множеству $\mathcal{T}_{\mathbf{V},f}$, и исходящими из различных точек многообразия $\mathbf{V}$, что и требовалось доказать.

Случай 6.2. Пусть $\mathbf{t}_0^{(1)} \equiv \mathbf{t}_0^{(2)}\ (\ker \mathbf{h})$.

Тогда $\mathbf{t}_0^{(1)} \equiv \mathbf{t}_0^{(2)}\ (\ker(\mathbf{h} \circ f))$.

Так как $\mathbf{t}_0^{(1)} \equiv \mathbf{t}_0^{(2)}\ (\ker \mathbf{h})$, то $\mathbf{h}(\mathbf{t}_0^{(1)}) = \mathbf{h}(\mathbf{t}_0^{(2)})$, т.е. (6.105) и (6.106) являются траекториями, принадлежащими множеству $\mathcal{T}_{\mathbf{V},f}$, и исходящими из одной и той же точки многообразия $\mathbf{V}$.

Докажем, что траектории траекториями совпадают.

Для этого достаточно доказать, что для каждого числа $j \in \mathbb{N}$ из равенства $\mathbf{h}(\mathbf{t}_i^{(1)}) = \mathbf{h}(\mathbf{t}_i^{(2)})$ $(i \in \mathbb{Z}_j)$ вытекает, равенство $\mathbf{h}(\mathbf{t}_j^{(1)}) = \mathbf{h}(\mathbf{t}_j^{(2)})$.

1. Пусть $j = 1$. Так как $\mathbf{h}(\mathbf{t}_0^{(1)}) = \mathbf{h}(\mathbf{t}_0^{(2)})$ и $\mathbf{t}_0^{(1)} \equiv \mathbf{t}_0^{(2)}\ (\ker(\mathbf{h} \circ f))$, то

$$\mathbf{h}(\mathbf{t}_1^{(1)}) = (\mathbf{h} \circ f)(\mathbf{t}_0^{(1)}) = (\mathbf{h} \circ f)(\mathbf{t}_0^{(2)}) = \mathbf{h}(\mathbf{t}_1^{(2)}),$$

что и требовалось доказать.

2. Предположим, что равенства $\mathbf{h}(\mathbf{t}_i^{(1)}) = \mathbf{h}(\mathbf{t}_i^{(2)})$ $(i \in \mathbb{Z}_j)$ истинны для некоторого числа $j \in \mathbb{N}$.

3. Покажем, что истинно равенство $\mathbf{h}(\mathbf{t}_j^{(1)}) = \mathbf{h}(\mathbf{t}_j^{(2)})$.

Пусть $\mathbf{t}_{j-1}^{(1)} = \mathbf{t}_{j-1}^{(2)}$. Тогда

$$\mathbf{t}_j^{(1)} = f(\mathbf{t}_{j-1}^{(1)}) = f(\mathbf{t}_{j-1}^{(2)}) = \mathbf{t}_j^{(2)}.$$

Следовательно, $\mathbf{h}(\mathbf{t}_j^{(1)}) = \mathbf{h}(\mathbf{t}_j^{(2)})$, что и требовалось доказать.

Пусть $\mathbf{t}_{j-1}^{(1)} \neq \mathbf{t}_{j-1}^{(2)}$. Так как $\mathbf{h}(\mathbf{t}_{j-1}^{(1)}) = \mathbf{h}(\mathbf{t}_{j-1}^{(2)})$, то $\mathbf{t}_{j-1}^{(1)} \equiv \mathbf{t}_{j-1}^{(2)}\ (\ker \mathbf{h})$. А так как $\mathbf{t}_{j-1}^{(1)} \equiv \mathbf{t}_{j-1}^{(2)}\ (\ker \mathbf{h})$ и $\mathbf{t}_{j-1}^{(1)} \neq \mathbf{t}_{j-1}^{(2)}$, то, по предположению индукции, $\mathbf{t}_{j-1}^{(1)} \equiv \mathbf{t}_{j-1}^{(2)}\ (\ker(\mathbf{h} \circ f))$.

Следовательно,

$$\mathbf{h}(\mathbf{t}_j^{(1)}) = (\mathbf{h} \circ f)(\mathbf{t}_{j-1}^{(1)}) = (\mathbf{h} \circ f)(\mathbf{t}_{j-1}^{(2)}) = \mathbf{h}(\mathbf{t}_j^{(2)}),$$

что и требовалось доказать.□

Условие «$\mathbf{t} \not\equiv \mathbf{t}'\ (\ker \mathbf{h})$ или $\mathbf{t} \equiv \mathbf{t}'\ (\ker(\mathbf{h} \circ f))$» формально может быть записано в виде

$$(\forall \mathbf{t}, \mathbf{t}' \in K^m)(\mathbf{t} \equiv \mathbf{t}'\ (\ker \mathbf{h}) \Rightarrow \mathbf{t} \equiv \mathbf{t}'\ (\ker(\mathbf{h} \circ f))). \tag{6.107}$$

Обозначим через $\mathcal{F}_{m,\mathbf{h}}(\mathcal{K})$ множество всех отображений $f \in \mathcal{F}_m(\mathcal{K})$, удовлетворяющих формуле (6.107).

Замечание 6.12. Таким образом, из теоремы 6.9 вытекает, что именно отображения $f \in \mathcal{F}_{m,\mathbf{h}}(\mathcal{K})$ определяют такие множества траекторий $\mathcal{T}_{\mathbf{V},f}$, что любые две различные траектории, принадлежащие множеству $\mathcal{T}_{\mathbf{V},f}$, исходят из различных точек многообразия $\mathbf{V}$.

Из теоремы 6.9 непосредственно вытекает следующее следствие.

Следствие 6.6. Пусть $\mathbf{v} = \mathbf{h}(\mathbf{t})$ $(\mathbf{t} \in K^m)$ – параметризация многообразия $\mathbf{V} \in \mathcal{V}_{2,n}(\mathcal{K})$. Тогда:

1) семейство $\mathcal{M}^{(r)}_{n,k}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ состоит из детерминированных автоматов тогда и только тогда, когда семейство Θ состоит только из элементов, принадлежащих множеству $\mathcal{F}_{m,\mathbf{h}}(\mathcal{K})$;

2) семейство $\mathcal{M}^{(r)}_{n,k}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ состоит из недетерминированных автоматов тогда и только тогда, когда семейство Θ содержит хотя бы один элемент, принадлежащий множеству $\mathcal{F}_m(\mathcal{K}) \backslash \mathcal{F}_{m,\mathbf{h}}(\mathcal{K})$.$\square$

Обозначим через $\mathfrak{I}_{m,k}(\mathcal{K})$ множество всех семейств $\Theta = \{\theta_i\}_{i \in \mathbb{N}_k}$, состоящих только из элементов, принадлежащих множеству $\mathcal{F}_{m,\mathbf{h}}(\mathcal{K})$.

В дальнейшем будем рассматривать только семейства $\mathcal{M}^{(r)}_{n,k}(\mathbf{V}, \Theta)$ $(r = 1, 2)$, состоящие из детерминированных автоматов, т.е. всюду в дальнейшем предполагается, что $\Theta \in \mathfrak{I}_{m,k}(\mathcal{K})$.

6.4.2. Автоматные характеристики исследуемых моделей.

Охарактеризуем те свойства автоматов $M_r \in \mathcal{M}^{(r)}_{n,k}(\mathbf{V}, \Theta)$ $(r = 1, 2)$, которые формулируются только в терминах функции переходов автомата, т.е. в терминах рекуррентного соотношения

$$\mathbf{q}_{t+1} = \mathbf{h}(\theta_{x_{t+1}}(\mathbf{t}_t)). \tag{6.108}$$

Напомним, что автомат называется групповым, если для каждого фиксированного входного символа функция переходов является подстановкой на множестве состояний.

Обозначим через $\mathcal{F}^{(0)}_{m,\mathbf{h}}(\mathcal{K})$ множество всех отображений $f \in \mathcal{F}_{m,\mathbf{h}}(\mathcal{K})$, удовлетворяющих условию

$$(\forall \mathbf{t}, \mathbf{t}' \in K^m)(\mathbf{t} \not\equiv \mathbf{t}' \,(\ker \mathbf{h}) \Rightarrow \mathbf{t} \not\equiv \mathbf{t}' \,(\ker(\mathbf{h} \circ f))). \tag{6.109}$$

Теорема 6.10. Пусть $\mathbf{v} = \mathbf{h}(\mathbf{t})$ $(\mathbf{t} \in K^m)$ – параметризация многообразия $\mathbf{V} \in \mathcal{V}_{2,n}(\mathcal{K})$. Тогда:

1) семейство $\mathcal{M}^{(r)}_{n,k}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ состоит из групповых автоматов тогда и только тогда, когда семейство Θ $(\Theta \in \mathfrak{I}_{m,k}(\mathcal{K}))$ состоит только из элементов, принадлежащих множеству $\mathcal{F}^{(0)}_{m,\mathbf{h}}(\mathcal{K})$;

2) семейство $\mathcal{M}^{(r)}_{n,k}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ состоит из автоматов, не являющихся групповыми автоматами тогда и только тогда, когда семейство Θ $(\Theta \in \mathfrak{I}_{m,k}(\mathcal{K}))$ содержит хотя бы один элемент, принадлежащий множеству $\mathcal{F}_{m,\mathbf{h}}(\mathcal{K}) \backslash \mathcal{F}^{(0)}_{m,\mathbf{h}}(\mathcal{K})$.$\square$

Доказательство. Из формулы (6.108) вытекает, что любые состояния $\mathbf{q} = \mathbf{h}(\mathbf{t})$ $(\mathbf{t} \in K^m)$ и $\mathbf{q}' = \mathbf{h}(\mathbf{t}')$ $(\mathbf{t}' \in K^m)$ автомата $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ под действием любого входного символа $i \in \mathbb{N}_k$ переходят, соответственно, в состояния $\widetilde{\mathbf{q}} = \mathbf{h}(\theta_i(\mathbf{t}))$ и $\widetilde{\mathbf{q}}' = \mathbf{h}(\theta_i(\mathbf{t}'))$.

Для доказательства теоремы докажем следующие две леммы.

Лемма 6.2. Семейство $\mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ состоит из групповых автоматов, если семейство Θ состоит только из элементов, принадлежащих множеству $\mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K})$.□

Доказательство. Предположим, что семейство Θ состоит только из элементов, принадлежащих множеству $\mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K})$.

Рассмотрим произвольный автомат $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$.

Для любых двух состояний $\mathbf{q}, \mathbf{q}' \in \mathbf{V}$ $(\mathbf{q} \neq \mathbf{q}')$ автомата M существуют такие $\mathbf{t}, \mathbf{t}' \in K^m$ $(\mathbf{t} \neq \mathbf{t}')$, что $\mathbf{q} = \mathbf{h}(\mathbf{t})$ и $\mathbf{q}' = \mathbf{h}(\mathbf{t}')$.

Так как $\mathbf{t} \not\equiv \mathbf{t}' (\ker \mathbf{h})$, а семейство $\Theta = \{\theta_i\}_{i \in \mathbb{Z}_k}$ состоит только из элементов, принадлежащих множеству $\mathcal{F}_{m,\mathbf{h}}^{(0)}$, то из условия (6.109) вытекает, что $\mathbf{t} \not\equiv \mathbf{t}' (\ker(\mathbf{h} \circ \theta_i))$ для каждого входного символа $i \in \mathbb{Z}_k$, т.е. $\mathbf{h}(\theta_i(\mathbf{t})) \neq \mathbf{h}(\theta_i(\mathbf{t}'))$ для каждого входного символа $i \in \mathbf{Z}_k$.

Так как любые два состояния $\mathbf{q}, \mathbf{q}' \in \mathbf{V}$ $(\mathbf{q} \neq \mathbf{q}')$ автомата M под действием каждого входного символа $i \in \mathbb{Z}_k$ переходят в различные состояния, то M – групповой автомат, что и требовалось доказать.□

Лемма 6.3. Семейство $\mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ состоит из автоматов, не являющихся групповыми автоматами, если семейство Θ содержит хотя бы один элемент, принадлежащий множеству $\mathcal{F}_{m,\mathbf{h}}(\mathcal{K}) \backslash \mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K})$.□

Доказательство. Предположим, что семейство $\Theta = \{\theta_i\}_{i \in \mathbb{Z}_k}$ содержит элемент θ_j, принадлежащий множеству $\mathcal{F}_{m,\mathbf{h}}(\mathcal{K}) \backslash \mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K})$.

Так как $\theta_j \in \mathcal{F}_{m,\mathbf{h}}(\mathcal{K}) \backslash \mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K})$, то $\theta_j \notin \mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K})$.

Из условия $\theta_j \notin \mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K})$ и условия (6.109), определяющего множество $\mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K})$, вытекает, что

$$(\exists \mathbf{t}, \mathbf{t}' \in K^m)(\mathbf{t} \not\equiv \mathbf{t}' (\ker \mathbf{h}) \,\&\, \mathbf{t} \equiv \mathbf{t}' (\ker(\mathbf{h} \circ \theta_j))).$$

Так как $\mathbf{t} \not\equiv \mathbf{t}' (\ker \mathbf{h})$, то $\mathbf{q} = \mathbf{h}(\mathbf{t})$ и $\mathbf{q}' = \mathbf{h}(\mathbf{t}')$ различные состояния любого автомата $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$.

А так как $\mathbf{t} \equiv \mathbf{t}' (\ker(\mathbf{h} \circ \theta_j))$, то $\mathbf{h}(\theta_j(\mathbf{t})) = \mathbf{h}(\theta_j(\mathbf{t}'))$, т.е. для любого автомата $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ различные состояния $\mathbf{q} = \mathbf{h}(\mathbf{t})$ и $\mathbf{q}' = \mathbf{h}(\mathbf{t}')$ под действием входного символа j переходят в одно и тоже состояние.

Отсюда вытекает, что ни один автомат $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ не является групповым автоматом, что и требовалось доказать.□

Так как

$$\{\mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K}), \mathcal{F}_{m,\mathbf{h}}(\mathcal{K}) \backslash \mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K})\}$$

является разбиением множества $\mathcal{F}_{m,\mathbf{h}}$, то из лемм 6.2 и 6.3 вытекает, что теорема 6.10 истинна.□

Напомним, что состояние автомата называется:

1) источником, если это состояние не достижимо ни из какого состояния автомата;

2) стоком, если из этого состояния невозможен переход ни в какое другое состояние автомата.

Положим $K^m / \ker \mathbf{h} = \{B_1, \ldots, B_{|\mathbf{V}|}\}$.

Утверждение 6.16. Семейство $\mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ состоит из автоматов, имеющих состояния-источники, тогда и только тогда, когда $\Theta = \{\theta_i\}_{i \in \mathbb{N}_k}$ – такое семейство элементов множества $\mathcal{F}_{m,\mathbf{h}}(\mathcal{K}) \backslash \mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K})$, что включение

$$\bigcup_{i \in \mathbb{N}_k} Val\, \theta_i \subseteq K^m \backslash B_j. \tag{6.110}$$

истинно для некоторого числа $j \in \mathbb{N}_{|\mathbf{V}|}$.□

Доказательство. Предположим, что семейство $\Theta = \{\theta_i\}_{i \in \mathbb{N}_k}$ элементов множества $\mathcal{F}_{m,\mathbf{h}}(\mathcal{K})$ содержит элемент $\theta_x \in \mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K})$.

Из теоремы 6.10 вытекает, что входной символ x является подстановкой на множестве состояний любого автомата $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$.

Следовательно, ни один автомат $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ не имеет состояний-источников, что и требовалось доказать.

Предположим, что семейство $\Theta = \{\theta_i\}_{i \in \mathbb{N}_k}$ состоит из элементов, принадлежащих множеству $\mathcal{F}_{m,\mathbf{h}}(\mathcal{K}) \backslash \mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K})$.

Пусть включение (6.110) ложно для всех $j \in \mathbb{N}_{|\mathbf{V}|}$.

Рассмотрим произвольное состояние $\mathbf{q} = \mathbf{h}(\mathbf{t})$ $(\mathbf{t} \in K^m)$ любого автомата $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$.

Пусть B_j – такой элемент фактор-множества $K^m / \ker \mathbf{h}$, что $\mathbf{t} \in B_j$.

Так как (6.110) ложно,то существуют $\widetilde{\mathbf{t}} \in K^m$ и $x \in \mathbb{N}_k$, для которых $\theta_x(\widetilde{\mathbf{t}}) \in B_j$. Отсюда вытекает, что $\mathbf{h}(\theta_x(\widetilde{\mathbf{t}})) = \mathbf{h}(\mathbf{t})$, т.е. состояние $\widetilde{\mathbf{q}} = \mathbf{h}(\widetilde{\mathbf{t}})$ автомата M под действием входного символа x переходит в состояние $\mathbf{q}$.

Следовательно, ни один автомат $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ не имеет состояний-источников, что и требовалось доказать.

Пусть существует число $j \in \mathbb{N}_{|\mathbf{V}|}$, для которого включение (6.110) истинно.

Рассмотрим в произвольном автомате $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ такое состояние $\mathbf{q} = \mathbf{h}(\mathbf{t})$, что $\mathbf{t} \in B_j$.

Так как включение (6.110) истинно, то $\theta_x(\widetilde{\mathbf{t}}) \notin B_j$ для всех $\widetilde{\mathbf{t}} \in K^m$ и $x \in \mathbb{N}_k$, т.е.

$$\mathbf{h}(\theta_x(\widetilde{\mathbf{t}})) \neq \mathbf{h}(\mathbf{t}) = \mathbf{q}$$

для всех $\widetilde{\mathbf{t}} \in K^m$ и $x \in \mathbb{N}_k$.

Следовательно, любое состояние $\widetilde{\mathbf{q}} = \mathbf{h}(\widetilde{\mathbf{t}})$ $(\widetilde{\mathbf{t}} \in K^m)$ автомата M под действием любого входного символа $x \in \mathbb{N}_k$ переходит в состояние, отличное от состояния $\mathbf{q}$.

Отсюда вытекает, что $\mathbf{q}$ – состояние-источник для любого автомата $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$, что и требовалось доказать.□

Утверждение 6.17. Семейство $\mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ состоит из автоматов, имеющих состояния-стоки, тогда и только тогда, когда для семейства $\Theta = \{\theta_i\}_{i \in \mathbb{N}_k}$ элементов множества $\mathcal{F}_{m,\mathbf{h}}(\mathcal{K})$ существует такое число $j \in \mathbb{N}_{|\mathbf{V}|}$, что истинно включение (6.110).□

Доказательство. Предположим, что включение (6.110) истинно для некоторого числа $j \in \mathbb{N}_{|\mathbf{V}|}$.

Рассмотрим в произвольном автомате $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ состояние $\mathbf{q} = \mathbf{h}(\mathbf{t})$ $(\mathbf{t} \in B_j)$.

Из истинности включения (6.110) вытекает, что $\theta_x(\widetilde{\mathbf{t}}) \in B_j$ для всех $\widetilde{\mathbf{t}} \in B_j$ и $x \in \mathbb{N}_k$. Это означает, что под действием любого входного символа $x \in \mathbb{N}_k$ состояние $\mathbf{q}$ переходит в себя.

Следовательно, состояние $\mathbf{q}$ является состоянием-стоком для любого автомата $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$, что и требовалось доказать.

Предположим, что включение (6.110) ложно для всех чисел $j \in \mathbb{N}_{|\mathbf{V}|}$.

Рассмотрим произвольное состояние $\mathbf{q} = \mathbf{h}(\mathbf{t})$ $(\mathbf{t} \in K^m)$ любого автомата $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$.

Пусть B_j – такой элемент фактор-множества $K^m / \ker \mathbf{h}$, что $\mathbf{t} \in B_j$.

Так как включение (6.110) ложно, то существуют такие $\widetilde{\mathbf{t}} \in B_j$ и $x \in \mathbb{Z}_k$, что $\theta_x(\widetilde{\mathbf{t}}) \notin B_j$.

Отсюда вытекает, что $\mathbf{h}(\theta_x(\widetilde{\mathbf{t}})) \neq \mathbf{q}$, т.е. состояние $\mathbf{q}$ автомата M под действием входного символа x переходит в состояние, отличное от состояния $\mathbf{q}$.

Следовательно, ни один автомат $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ не имеет состояний-стоков, что и требовалось доказать.□

Из доказательства утверждений 6.16 и 6.17 вытекает, что структура графа переходов автомата $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ может быть исследована в терминах следующей теоретико-графовой конструкции.

Назовем следом автомата $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ направленный граф (возможно, с петлями) [132]

$$G_M = (K^m / \ker \mathbf{h}, \Gamma_M),$$

где $(B_{j_1}, B_{j_2}) \in \Gamma_M$ $(j_1, j_2 \in \mathbb{N}_{|\mathbf{V}|})$ тогда и только тогда, когда существует такое число $x \in \mathbb{N}_k$, что истинно включение $\theta_x(B_{j_1}) \subseteq B_{j_2}$.

Ясно, что направленный граф G_M изоморфен направленному графу, полученному из графа переходов автомата M в результате удаления отметок всех дуг (изоморфизм этих направленных графов устанавливает отображение $\mathbf{h}$).

Отсюда вытекает, что истинны следующие утверждения о свойствах автомата $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ (при условии, что $(\Theta \in \mathfrak{I}_k)(\mathcal{K})$):

1) автомат $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ связный (соответственно, сильно связный) тогда и только тогда, когда граф G_M связный (соответственно, сильно связный);

2) число компонент связности (соответственно, сильной связности) автомата $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ совпадает с числом компонент связности (соответственно, сильной связности) графа G_M;

3) диаметр графа переходов автомата $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ совпадает с диаметром графа G_M;

3) радиус графа переходов автомата $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ совпадает с радиусом графа G_M

Охарактеризуем те свойства автоматов $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$, которые существенно зависят как от функции переходов, так и от функции выходов автомата.

Напомним, что два различных состояния автомата называются близнецами, если по любому входному символу они переходят в одно и то же состояние и при этом переходе автомат выдает один и тот же выходной символ.

Утверждение 6.18. Семейство $\mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ состоит из автоматов, не имеющих состояний-близнецов, если семейство Θ содержит хотя бы один элемент, принадлежащий множеству $\mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K})$.□

Доказательство. Предположим, что семейство $\Theta = \{\theta_i\}_{i \in \mathbb{N}_k}$ содержит элемент θ_x, принадлежащий множеству $\mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K})$.

Из теоремы 6.10 вытекает, что входной символ x является подстановкой на множестве состояний любого автомата $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$.

Следовательно, ни один автомат $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ не имеет состояний-близнецов, что и требовалось доказать.□

Установим условия, при которых автомат $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ имеет состояния-близнецы.

Утверждение 6.19. Пусть $\mathbf{V} \in \mathcal{V}_{2,n}(\mathcal{K})$, $\mathbf{v} = \mathbf{h}(\mathbf{t})$ $(\mathbf{t} \in K^m)$ – параметризация многообразия $\mathbf{V}$, а $\Theta = \{\theta_i\}_{i \in \mathbb{N}_k}$ – семейство элементов множества $\mathcal{F}_{m,\mathbf{h}}(\mathcal{K}) \backslash \mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K})$.

Автомат $M \in \mathcal{M}_{n,k}^{(1)}(\mathbf{V}, \Theta)$ имеет состояния-близнецы тогда и только тогда, когда существуют такие $\mathbf{t}, \widetilde{\mathbf{t}} \in K^m$, что выполнены следующие три условия:

1) $\mathbf{t} \not\equiv \widetilde{\mathbf{t}}$ $(\ker \mathbf{h})$;

2) $\theta_i(\mathbf{t}) \equiv \theta_i(\widetilde{\mathbf{t}})$ $(\ker \mathbf{h})$ для всех $i \in \mathbb{N}_k$;

3) $\mathbf{t} \equiv \widetilde{\mathbf{t}}$ $(\bigcap\limits_{i \in \mathbb{N}_k} \ker(\mathbf{g}_i \circ \mathbf{h}))$,

где $\mathbf{g}_i : K^n \to K^l$ $(i \in \mathbb{N}_k)$ – отображения, определяющие функцию выхода автомата M.□

Доказательство. Первое условие означает, что $\mathbf{q} = \mathbf{h}(\mathbf{t})$ и $\widetilde{\mathbf{q}} = \mathbf{h}(\widetilde{\mathbf{t}})$ являются различными состояниями автомата M.

Второе условие означает, что состояния $\mathbf{q}$ и $\widetilde{\mathbf{q}}$ автомата M по каждому входному символу $i \in \mathbb{N}_k$ переходят в одно и то же состояние.

Третье условие означает, что при переходе из состояний $\mathbf{q}$ и $\widetilde{\mathbf{q}}$ под действием любого входного символа $i \in \mathbb{N}_k$ автомат M выдает один и тот же выходной символ.□

Аналогично доказывается и следующее утверждение.

Утверждение 6.20. Пусть $\mathbf{V} \in \mathcal{V}_{2,n}(\mathcal{K})$, $\mathbf{v} = \mathbf{h}(\mathbf{t})$ $(\mathbf{t} \in K^m)$ – параметризация многообразия $\mathbf{V}$, а $\Theta = \{\theta_i\}_{i \in \mathbb{N}_k}$ – семейство элементов множества $\mathcal{F}_{m,\mathbf{h}}(\mathcal{K}) \backslash \mathcal{F}_{m,\mathbf{h}}^{(0)}(\mathcal{K})$.

Автомат $M \in \mathcal{M}_{n,k}^{(2)}(\mathbf{V}, \Theta)$ имеет состояния-близнецы тогда и только тогда, когда существуют такие $\mathbf{t}, \widetilde{\mathbf{t}} \in K^m$, что выполнены следующие два условия:

1) $\mathbf{t} \not\equiv \widetilde{\mathbf{t}}$ $(\ker \mathbf{h})$;

2) $\theta_i(\mathbf{t}) \equiv \theta_i(\widetilde{\mathbf{t}})$ $(\ker \mathbf{h})$ для всех $i \in \mathbb{N}_k$.□

Напомним, что автомат называется явно приведенным, если любые два его различных состояния различимы некоторым входным символом.

Установим условия, при которых автомат $M \in \mathcal{M}_{n,k}^{(r)}(\mathbf{V}, \Theta)$ $(r = 1, 2)$ является явно приведенным.

Утверждение 6.21. Пусть $\mathbf{V} \in \mathcal{V}_{2,n}(\mathcal{K})$, а $\mathbf{v} = \mathbf{h}(\mathbf{t})$ $(\mathbf{t} \in K^m)$ – параметризация многообразия $\mathbf{V}$.

Автомат $M \in \mathcal{M}_{n,k}^{(1)}(\mathbf{V}, \Theta)$ является явно приведенным тогда и только тогда, когда истинно равенство

$$\ker \mathbf{h} = \bigcap_{i \in \mathbb{N}_k} \ker(\mathbf{g}_i \circ \mathbf{h}), \tag{6.111}$$

где $\mathbf{g}_i : K^n \to K^l$ $(i \in \mathbb{N}_k)$ – отображения, определяющие функцию выхода автомата M.□

Доказательство. Из 2-го рекуррентного соотношения системы рекуррентных соотношений (6.102) вытекает, что автомат $M \in \mathcal{M}_{n,k}^{(1)}(\mathbf{V}, \Theta)$ является явно приведенным тогда и только тогда, когда бинарное отношение $\bigcap\limits_{i \in \mathbb{N}_k} \ker(\mathbf{g}_i|_{\mathbf{V}})$ является отношением равенства на множестве $\mathbf{V}$, т.е. когда

$$(\forall \mathbf{t}, \mathbf{t}' \in K^m)(\mathbf{t} \not\equiv \mathbf{t}' \,(\ker \mathbf{h}) \Leftrightarrow (\exists i \in \mathbb{N}_k)(\mathbf{t} \not\equiv \mathbf{t}' \,(\ker(\mathbf{g}_i \circ \mathbf{h})))) \Leftrightarrow$$

$$\Leftrightarrow (\forall \mathbf{t}, \mathbf{t}' \in K^m)(\mathbf{t} \not\equiv \mathbf{t}' \,(\ker \mathbf{h}) \Leftrightarrow \mathbf{t} \not\equiv \mathbf{t}' \,(\bigcap_{i \in \mathbb{N}_k} \ker(\mathbf{g}_i \circ \mathbf{h}))). \tag{6.112}$$

Формула (6.112) эквивалентна формуле (6.111).

Следовательно, автомат $M \in \mathcal{M}_{n,k}^{(1)}(\mathbf{V}, \Theta)$ является явно приведенным тогда и только тогда, когда истинно равенство (6.111), что и требовалось доказать.□

Утверждение 6.22. Пусть $\mathbf{V} \in \mathcal{V}_{2,n}(\mathcal{K})$, $\mathbf{v} = \mathbf{h}(\mathbf{t})$ $(\mathbf{t} \in K^m)$ – параметризация многообразия $\mathbf{V}$, а $\Theta = \{\theta_i\}_{i \in \mathbb{N}_k}$.

Автомат $M \in \mathcal{M}_{n,k}^{(2)}(\mathbf{V}, \Theta)$ является явно приведенным тогда и только тогда, когда истинно равенство

$$\ker \mathbf{h} = \bigcap_{i \in \mathbb{N}_k} \ker(\mathbf{g} \circ \mathbf{h} \circ \theta_i), \tag{6.113}$$

где $\mathbf{g} : K^n \to K^l$ – отображение, определяющее функцию выхода автомата M.□

Доказательство. Из 2-го рекуррентного соотношения системы рекуррентных соотношений (6.103) вытекает, что автомат $M \in \mathcal{M}_{n,k}^{(2)}(\mathbf{V}, \Theta)$

является явно приведенным тогда и только тогда, когда выполнено условие

$$(\forall \mathbf{t}, \mathbf{t}' \in K^m)(\mathbf{t} \not\equiv \mathbf{t}' (\ker \mathbf{h}) \Leftrightarrow (\exists i \in \mathbb{N}_k)(\mathbf{t} \not\equiv \mathbf{t}' (\ker(\mathbf{g} \circ \mathbf{h} \circ \theta_i)))) \Leftrightarrow$$

$$\Leftrightarrow (\forall \mathbf{t}, \mathbf{t}' \in K^m)(\mathbf{t} \not\equiv \mathbf{t}' (\ker \mathbf{h}) \Leftrightarrow \mathbf{t} \not\equiv \mathbf{t}' (\bigcap_{i \in \mathbb{N}_k} \ker(\mathbf{g} \circ \mathbf{h} \circ \theta_i))). \quad (6.114)$$

Формула (6.114) эквивалентна формуле (6.113).

Следовательно, автомат $M \in \mathcal{M}^{(2)}_{n,k}(\mathbf{V}, \Theta)$ является явно приведенным тогда и только тогда, когда истинно равенство (6.113), что и требовалось доказать.□

6.4.3. Гомоморфизмы исследуемых моделей.

Пусть $\mathbf{V}_r \in \mathcal{V}_{2,n_1}(\mathcal{K}_r)$, а $\mathbf{h}_r$ – параметризация многообразия $\mathbf{V}_r$.

Гомоморфизм упорядоченной пары $(\mathbf{V}_1, \Theta_1)$ на упорядоченную пару $(\mathbf{V}_2, \Theta_2)$, где $\Theta^{(r)} = \{\theta_i^{(r)}\}_{i \in \mathbb{N}_k}$ $(r = 1, 2)$ – фиксированное семейство отображений $\theta_i^{(r)} : K_r^{m_r} \to K_r^{m_r}$ $(i \in \mathbb{N}_k)$ определен в п.6.2.1 как упорядоченная пара сюръекций $\Phi = (\varphi_1, \varphi_2)$ (где $\varphi_1 : \mathbf{V}_1 \to \mathbf{V}_2$ и $\varphi_2 : K_1^{m_1} \to K_2^{m_2}$), удовлетворяющая равенствам (6.77) и (6.78).

Следующая теорема устанавливает, как связаны между собой гомоморфизм $\Phi = (\varphi_1, \varphi_2)$ упорядоченной пары $(\mathbf{V}_1, \Theta_1)$ на упорядоченную пару $(\mathbf{V}_2, \Theta_2)$ и гомоморфные образы автоматов $M_r \in \mathcal{M}^{(r)}_{n_1,k}(\mathbf{V}_1, \Theta_1)$ $(r = 1, 2)$, которые принадлежат семейству автоматов $\mathcal{M}^{(r)}_{n_2,k}(\mathbf{V}_2, \Theta_2)$.

Теорема 6.11. Если упорядоченная пара $(\mathbf{V}_2, \Theta_2)$ $(\mathbf{V}_2 \in \mathcal{V}_{2,n_2}(\mathcal{K}_2))$ – гомоморфный образ упорядоченной пары $(\mathbf{V}_1, \Theta_1)$ $(\mathbf{V}_1 \in \mathcal{V}_{2,n_1}(\mathcal{K}_1))$, то существуют такие отображения

$$\Psi_r : \mathcal{M}^{(r)}_{n_1,k}(\mathbf{V}_1, \Theta_1) \to \mathcal{M}^{(r)}_{n_2,k}(\mathbf{V}_2, \Theta_2), \quad (6.115)$$

что автомат $\Psi_r(M_r)$ $(M_r \in \mathcal{M}^{(r)}_{n_1,k}(\mathbf{V}_1, \Theta_1)$ является гомоморфным образом автомата M_r.□

Доказательство. Предположим, что упорядоченная пара $(\mathbf{V}_2, \Theta_2)$ $(\mathbf{V}_2 \in \mathcal{V}_{2,n_2}(\mathcal{K}_2))$ – гомоморфный образ упорядоченной пары $(\mathbf{V}_1, \Theta_1)$ $(\mathbf{V}_1 \in \mathcal{V}_{2,n_1}(\mathcal{K}_1))$, а упорядоченная пара сюръекций

$$\Phi = (\varphi_1, \varphi_2),$$

где $\varphi_1 : \mathbf{V}_1 \to \mathbf{V}_2$ и $\varphi_2 : K_1^{m_1} \to K_2^{m_2}$, определяет гомоморфизм упорядоченной пары $(\mathbf{V}_1, \Theta_1)$ на упорядоченную пару $(\mathbf{V}_2, \Theta_2)$.

Определим отображения (6.115) следующим образом:

1) для автомата $M_1 \in \mathcal{M}^{(1)}_{n_1,k,l_1}(\mathbf{V}_1, \Theta_1)$ ($l_1 \in \mathbb{N}$), заданного системой рекуррентных соотношений

$$\begin{cases} \mathbf{q}^{(1)}_{t+1} = \mathbf{h}_1(\theta^{(1)}_{x_{t+1}}(\mathbf{t}_t)) \\ \mathbf{y}^{(1)}_{t+1} = \mathbf{g}^{(1)}_{x_{t+1}}(\mathbf{q}^{(1)}_t) \end{cases} \quad (t \in \mathbb{N}) \tag{6.116}$$

где $\mathbf{g}^{(1)}_i : K_1^{n_1} \to K_1^{l_1}$ ($i \in \mathbb{N}_k$), автомат $\Psi_1(M_1) \in \mathcal{M}^{(1)}_{n_2,k,l_2}(\mathbf{V}_2, \Theta_2)$ задан системой рекуррентных соотношений

$$\begin{cases} \mathbf{q}^{(2)}_{t+1} = \mathbf{h}_2(\theta^{(2)}_{x_{t+1}}(\varphi_2(\mathbf{t}_t))) \\ \mathbf{y}^{(2)}_{t+1} = \mathbf{g}^{(2)}_{x_{t+1}}(\varphi_1(\mathbf{q}^{(1)}_t)) \end{cases} \quad (t \in \mathbb{N}), \tag{6.117}$$

где число $l_2 \in \mathbb{N}$ и отображения $\mathbf{g}^{(2)}_i : K_2^{n_2} \to K_2^{l_2}$ ($i \in \mathbb{N}_k$) будут определены ниже;

2) для автомата $M_2 \in \mathcal{M}^{(2)}_{n_1,k,l_1}(\mathbf{V}_1, \Theta_1)$ ($l_1 \in \mathbb{N}$), заданного системой рекуррентных соотношений

$$\begin{cases} \mathbf{q}^{(1)}_{t+1} = \mathbf{h}_1(\theta^{(1)}_{x_{t+1}}(\mathbf{t}_t)) \\ \mathbf{y}^{(1)}_{t+1} = \mathbf{g}^{(1)}(\mathbf{q}^{(1)}_{t+1}) \end{cases} \quad (t \in \mathbb{N}), \tag{6.118}$$

где $\mathbf{g}^{(1)} : K_1^{n_1} \to K_1^{l_1}$, автомат $\Psi_1(M_2) \in \mathcal{M}^{(2)}_{n_2,k,l_2}(\mathbf{V}_2, \Theta_2)$ задан системой рекуррентных соотношений

$$\begin{cases} \mathbf{q}^{(2)}_{t+1} = \mathbf{h}_2(\theta^{(2)}_{x_{t+1}}(\varphi_2(\mathbf{t}_t))) \\ \mathbf{y}^{(2)}_{t+1} = \mathbf{g}^{(2)}(\varphi_1(\mathbf{q}^{(1)}_{t+1})) \end{cases} \quad (t \in \mathbb{N}), \tag{6.119}$$

где число $l_2 \in \mathbb{N}$ и отображение $\mathbf{g}^{(2)} : K_2^{n_2} \to K_2^{l_2}$ будут определены ниже.

Из (6.77) и (6.78) вытекает, что функция переходов автомата (6.117) (соответственно, автомата (6.119) удовлетворяет требованиям, предъявляемым к функции переходов гомоморфного образа автомата (6.116) (соответственно, автомата (6.118)) в случае, когда $\chi_1 = \varphi_1$, а χ_2 – тождественное отображение.

Определим теперь функции выходов автоматов (6.117) и (6.119).

Рассмотрим автомат (6.117).

Положим

$$\mathcal{S}_{M_1} = \bigcup_{i \in \mathbb{N}_k} \mathcal{S}_{M_1,i},$$

где

$$\mathcal{S}_{M_1,i} = \{S_{\mathbf{v},i} | \mathbf{v} \in \mathbf{V}_2\} \ (i \in \mathbb{N}_k),$$

а множество $S_{\mathbf{v},i}$ $(i \in \mathbb{N}_k)$ определено равенством

$$S_{\mathbf{v},i} = \mathbf{g}_i^{(1)}(\varphi_1^{-1}(\mathbf{v})) \ (i \in \mathbb{N}_k).$$

Определим на множестве $\mathcal{S}_{M_1}$ отношение эквивалентности $\equiv_{M_1}$ следующим образом: $S_{\mathbf{v}',i_1} \equiv_{M_1} S_{\mathbf{v}'',i_2}$ $(\mathbf{v}', \mathbf{v}'' \in \mathbf{V}_2; i_1, i_2 \in \mathbb{N}_k)$ тогда и только тогда, когда существуют такая последовательность элементов

$$\mathbf{v}_1 = \mathbf{v}', \mathbf{v}_2, \ldots, \mathbf{v}_d = \mathbf{v}''$$

многообразия $\mathbf{V}_2$ и такая последовательность

$$c_1 = i_1, c_2, \ldots, c_d = i_2$$

элементов множества $\mathbb{N}_k$, что

$$S_{\mathbf{v}_j,r_j} \cap S_{\mathbf{v}_{i+1},r_{j+1}} \neq \emptyset$$

для всех $j = 1, \ldots, d-1$.

Обозначим через ξ_{M_1} такую сюръекцию множества $\bigcup\limits_{i \in \mathbb{N}_k} Val\, \mathbf{g}_i^{(1)}$ в фактор-множество $\mathcal{S}_{M_1}/_{\equiv_{M_1}}$, что $\xi_{M_1}(\mathbf{y}) = \mathtt{S}$ тогда и только тогда, когда существует такое $S_{\mathbf{v},i} \in \mathtt{S}$, что $\mathbf{y} \in S_{\mathbf{v},i}$.

Положим

$$l_2 = \lceil (\log |\mathcal{S}_{M_1}|) \cdot (\log |K_2|)^{-1} \rceil.$$

Зафиксируем любую инъекцию η_{M_1} фактор-множества $\mathcal{S}_{M_1}/_{\equiv_{M_1}}$ в множество $K_2^{l_2}$.

Определим отображения $\mathbf{g}_i^{(2)}$ $(i \in \mathbb{N}_k)$ равенствами

$$\mathbf{g}_i^{(2)}(\mathbf{v}) = (\eta_{M_1} \circ \xi_{M_1})(\mathbf{g}_i^{(1)}(\varphi_1^{-1}(\mathbf{v}))) \ (\mathbf{v} \in \mathbf{V}_2, i \in \mathbb{N}_k). \tag{6.120}$$

Из (6.120) вытекает, что истинны равенства

$$(\eta_{M_1} \circ \xi_{M_1})(\mathbf{g}_i^{(1)}(\mathbf{q}_t^{(1)})) = \mathbf{g}_i^{(2)}(\varphi_1(\mathbf{q}_t^{(1)})) \ (i \in \mathbb{N}_k),$$

т.е. функции выходов автомата (6.117), определенная равенствами (6.120), удовлетворяет требованиям, предъявляемым к функции выходов гомоморфного образа автомата (6.116), если $\chi_1 = \varphi_1$, χ_2 – тождественное отображение, а $\chi_3 = \eta_{M_1} \circ \xi_{M_2}$.

Таким образом, автомат $\Psi_1(M_1) \in \mathcal{M}^{(1)}_{n_1,k,l_2}(\mathbf{V}_2, \Theta_2)$ является гомоморфным образом автомата $M_1 \in \mathcal{M}^{(1)}_{n_1,k,l_1}(\mathbf{V}_1, \Theta_1)$, что и требовалось доказать.

Рассмотрим автомат (6.119).

Положим

$$\mathcal{S}_{M_2} = \{S_{\mathbf{v}} | \mathbf{v} \in \mathbf{V}_2\},$$

где

$$S_{\mathbf{v}} = \mathbf{g}^{(1)}(\varphi_1^{-1}(\mathbf{v}))\ (\mathbf{v} \in \mathbf{V}_2).$$

Определим на множестве $\mathcal{S}_{M_2}$ отношение эквивалентности $\equiv_{M_2}$ следующим образом: $S_{\mathbf{v}'} \equiv_{M_2} S_{\mathbf{v}''}$ $(\mathbf{v}', \mathbf{v}'' \in \mathbf{V}_2)$ тогда и только тогда, когда существует такая последовательность

$$\mathbf{v}_1 = \mathbf{v}', \mathbf{v}_2, \ldots, \mathbf{v}_d = \mathbf{v}''$$

элементов многообразия $\mathbf{V}_2$, что

$$S_{\mathbf{v}_i} \cap S_{\mathbf{v}_{i+1}} \neq \emptyset$$

для всех $i = 1, \ldots, d-1$.

Обозначим через ξ_{M_2} такую сюръекцию множества $Val\ \mathbf{g}^{(1)}$ в фактормножество $\mathcal{S}_{M_2}/_{\equiv_{M_2}}$, что $\xi_{M_2}(\mathbf{y}) = \mathtt{S}$ тогда и только тогда, когда существует такое $S_{\mathbf{u}} \in \mathtt{S}$, что $\mathbf{y} \in S_{\mathbf{u}}$.

Положим

$$l_2 = \lceil (\log |\mathcal{S}_{M_2}|) \cdot (\log |K_2|)^{-1} \rceil.$$

Зафиксируем любую инъекцию η_{M_2} фактор-множества $\mathcal{S}_{M_2}/_{\equiv_{M_2}}$ в множество $K_2^{l_2}$.

Определим отображение $\mathbf{g}^{(2)}$ равенством

$$\mathbf{g}^{(2)}(\mathbf{u}) = (\eta_{M_2} \circ \xi_{M_2})(\mathbf{g}^{(1)}(\varphi_1^{-1}(\mathbf{v})))\ (\mathbf{v} \in \mathbf{V}_2). \tag{6.121}$$

Из (6.121) вытекает, что истинно равенство

$$(\eta_{M_2} \circ \xi_{M_2})(\mathbf{r}^{(1)}(\mathbf{q}_{t+1}^{(1)})) = \mathbf{g}^{(2)}(\varphi_1(\mathbf{q}_{t+1}^{(1)})),$$

т.е. функции выходов автомата (6.119), определенная равенством (6.110), удовлетворяет требованиям, предъявляемым к функции выходов гомоморфного образа автомата (6.118), если $\chi_1 = \varphi_1$, χ_2 – тождественное отображение, а $\chi_3 = \eta_{M_2} \circ \xi_{M_2}$.□

6.5. Автоматы на эллиптических кривых.

Раннее было отмечено, что эллиптические кривые над конечным полем $\mathcal{GF}(q)$, где $q = p^k$ (где p – простое число, а $k \in \mathbb{N}$) имеют многочисленные применения при решении как теоретических, так и прикладных

задач. Среди последних в настоящее время особое внимание уделяется задачам преобразования информации, в частности, задачам криптографии (напомним, что в настоящее время эллиптическая криптография считается одним из наиболее перспективных направлений современной криптографии).

По-видимому, именно эти обстоятельства послужили основной причиной исследования свойств эллиптических кривых, заданных уравнениями над областью целостности $\mathcal{K} = (K, +, \cdot)$, а также свойств эллиптических кривых, которые характеризуются в терминах расширения полей.

Все сказанное выше обосновывает актуальность исследования автоматных моделей, заданных системами рекуррентных соотношений на эллиптических кривых над конечными полями.

В примерах 6.4 и 6.5 были определены семейства автоматов Мили и Мура, заданные системой рекуррентных соотношений на эллиптической кривой над конечным полем или конечной областью целостности, а также охарактеризованы гомоморфизмы автоматов, принадлежащих этим семействам, с позиции гомоморфизма многообразий с алгеброй.

Ниже мы исследуем свойства семейств автоматов Мили и Мура, заданных системой рекуррентных соотношений на эллиптической кривой над конечным полем, с позиции теории автоматов.

6.5.1. Исследуемые модели.

Зафиксируем конечное поле $\mathsf{F} = \mathcal{GF}(q)$, где $q = p^k$ (где p – простое число, а $k \in \mathbb{N}$) и обозначим через Γ_{F} множество всех эллиптических кривых над полем F.

Как это было сделано раннее, обозначим через G_γ множество всех точек (включая бесконечно удаленную точку $\mathcal{O}$) эллиптической кривой $\gamma \in \Gamma_{\mathsf{F}}$, а через $\mathcal{G}_\gamma = (G_\gamma, +_\gamma, \cdot_\gamma)$ – абелеву группу, определяемую эллиптической кривой γ.

Для любой точки $P \in G_\gamma$ и любого числа $a \in \mathbb{N}$ положим

$$aP = \underbrace{P +_\gamma \ldots +_\gamma P}_{a \text{ раз}}.$$

Напомним, что абелева группа $\mathcal{G}_\gamma$ является либо циклической группой, либо изоморфна прямой сумме двух циклических групп.

Представим семейства автоматов Мили и Мура, определенные, соответственно, формулами (6.81) и (6.82) в более удобном для исследования их свойств виде.

Зафиксируем эллиптическую кривую $\gamma \in \Gamma_{\mathbf{F}}$ и число $l \in \mathbb{N}_{|G_\gamma|}$.

При фиксированных числах $n, m \in \mathbb{Z}_{|G_\gamma|}$ и точках $P_1, P_2 \in G_\gamma$ системы рекуррентных соотношений

$$\begin{cases} q_{t+1} = nq_t +_\gamma x_{t+1}P_1 \\ y_{t+1} = mq_t +_\gamma x_{t+1}P_2 \end{cases} \quad (t \in \mathbb{Z}_+) \tag{6.122}$$

и

$$\begin{cases} q_{t+1} = nq_t +_\gamma x_{t+1}P_1 \\ y_{t+1} = mq_{t+1} +_\gamma P_2 \end{cases} \quad (t \in \mathbb{Z}_+), \tag{6.123}$$

где $q_0 \in G_\gamma$ и $x_{t+1} \in \mathbb{Z}_l$, определяют, соответственно, автомат Мили и автомат Мура на эллиптической кривой γ.

Отметим, что для этих автоматов множество $\mathbb{Z}_l$ является входным алфавитом, а множество G_γ – множеством состояний, а также выходным алфавитом.

Очевидно, что каждый автомат (6.123) изоморфен соответствующему автомату

$$\begin{cases} q_{t+1} = nq_t +_\gamma x_{t+1}P_1 \\ y_{t+1} = mq_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+). \tag{6.124}$$

Поэтому всюду в дальнейшем будем считать, что автомат Мура на эллиптической кривой γ определен именно системой рекуррентных соотношений (6.124). Такое предположение не снижает общность рассуждений, а только уменьшает громоздкость формул.

Обозначим через $\mathcal{M}_{1,\gamma,l}$ семейство автоматов Мили, заданное системой рекуррентных соотношений (6.122), а через $\mathcal{M}_{2,\gamma,l}$ – семейство автоматов Мура, заданное системой рекуррентных соотношений (6.124).

Исследуем свойства автоматов, принадлежащих семействам автоматов $\mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$.

6.5.2. Автоматные характеристики исследуемых моделей.

Из определения семейств автоматов $\mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$ вытекает, что

$$|\mathcal{M}_{r,\gamma,l}| = |G_\gamma|^{5-r} \ (r = 1, 2). \tag{6.125}$$

Из (1.20) и (6.125) вытекает, что для любого числа $q = p^k$, где p $(p > 3)$ – простое число, а $k \in \mathbb{N}$ истинны оценки

$$(q + 1 - 2\sqrt{q})^{5-r} \leq |\mathcal{M}_{r,\gamma,l}| \leq (q + 1 + 2\sqrt{q})^{5-r} \ (r = 1, 2). \tag{6.126}$$

Из 2-го рекуррентного соотношения системы рекуррентных соотношений (6.122) вытекает, что для каждого автомата $M_1 \in \mathcal{M}_{1,\gamma,l}$ при каждом его начальном состоянии $q_0 \in G_\gamma$ для всех входных символов $x, \widetilde{x} \in \mathbb{Z}_l$ истинно равенство

$$(x - \widetilde{x})P_2 = y -_\gamma \widetilde{y}.$$

Таким образом, автомат $M_1 \in \mathcal{M}_{1,\gamma,l}$:

1) при каждом начальном состоянии $q_0 \in G_\gamma$ реализует инъективное отображение свободной входной полугруппы $\mathbb{Z}_l^+$ в свободную полугруппу G_γ^+ тогда и только тогда, когда $P_2 \in G_\gamma \backslash \{\mathcal{O}\}$ и число $l-1$ меньше порядка элемента P_2 группы $\mathcal{G}_\gamma$;

2) при каждом начальном состоянии $q_0 \in G_\gamma$ реализует отображение свободной входной полугруппы $\mathbb{Z}_l^+$ в свободную полугруппу G_γ^+, не являющееся инъекцией, тогда и только тогда, когда $P_2 = \mathcal{O}$ или число $l-1$ не меньше порядка элемента P_2 группы $\mathcal{G}_\gamma$.

Аналогичным образом, из 2-го рекуррентного соотношения системы рекуррентных соотношений (6.124) вытекает, что для каждого автомата $M_2 \in \mathcal{M}_{2,\gamma,l}$ при каждом его начальном состоянии $q_0 \in G_\gamma$ для всех входных символов $x, \widetilde{x} \in \mathbb{Z}_l$ истинно равенство

$$m(x - \widetilde{x})P_1 = y -_\gamma \widetilde{y}.$$

Таким образом, автомат $M_2 \in \mathcal{M}_{2,\gamma,l}$:

1) при каждом начальном состоянии $q_0 \in G_\gamma$ реализует инъективное отображение свободной входной полугруппы $\mathbb{Z}_l^+$ в свободную полугруппу G_γ^+ тогда и только тогда, когда $P_1 \in G_\gamma \backslash \{\mathcal{O}\}$, $m \neq 0$ и число $m(l-1)$ меньше порядка элемента P_1 группы $\mathcal{G}_\gamma$;

2) при каждом начальном состоянии $q_0 \in G_\gamma$ реализует отображение свободной входной полугруппы $\mathbb{Z}_l^+$ в свободную полугруппу G_γ^+, не являющееся инъекцией, тогда и только тогда, когда $P_1 = \mathcal{O}$ или $m = 0$, или число $m(l-1)$ не меньше порядка элемента P_1 группы $\mathcal{G}_\gamma$.

Напомним, что автомат называется групповым, если , если для каждого фиксированного входного символа функция переходов является подстановкой на множестве состояний.

Обозначим через $\mathcal{M}_{r,\gamma,l}^{gr}$ $(r = 1, 2)$ семейство, состоящее из всех групповых автоматов $M_r \in \mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$.

Теорема 6.12. Семейство автоматов $\mathcal{M}_{r,\gamma,l}^{gr}$ $(r = 1, 2)$ состоит из всех таких автоматов $M_r \in \mathcal{M}_{r,\gamma,l}$, что $n \in \mathbb{N}_{|G_\gamma|-1}$ и число n не является кратным порядка ни для какого элемента $P \in G_\gamma \backslash \{\mathcal{O}\}$ группы $\mathcal{G}_\gamma$.□

Доказательство. Первое рекуррентное соотношение систем рекуррентных соотношений (6.122) и (6.124) имеет вид

$$q_{t+1} = nq_t +_\gamma x_{t+1}P_1 \ (t \in \mathbb{Z}_+). \tag{6.127}$$

Из (6.127) вытекает, что для любых начальных состояний $q_0, \widetilde{q}_0 \in G_\gamma$ автомата $M_r \in \mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$ и любого входного символа $x_1 \in \mathbb{Z}_l$ истинны равенства

$$\widetilde{q}_1 = n\widetilde{q}_0 +_\gamma x_1 P_1$$

и

$$q_1 = nq_0 +_\gamma x_1 P_1.$$

Вычитая из 1-го равенства 2-е равенство, получим

$$\widetilde{q}_1 -_\gamma q_1 = n(\widetilde{q}_0 -_\gamma q_0). \tag{6.128}$$

Для каждого элемента $q_0 \in G_\gamma$ если элемент $\widetilde{q}_0$ пробегает (без повторений) множество $G_\gamma \backslash \{q_0\}$, то элемент $\widetilde{q}_0 -_\gamma q_0$ пробегает (без повторений) множество $G_\gamma \backslash \{\mathcal{O}\}$.

Следовательно, из равенства (6.128) вытекает, что входной символ $x_1 \in \mathbb{Z}_l$ является подстановкой на множестве состояний G_γ автомата $M_r \in \mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$ тогда и только тогда, когда $n \in \mathbb{N}_{|G_\gamma|-1}$ и $nP \neq \mathcal{O}$ для всех $P \in G_\gamma \backslash \{\mathcal{O}\}$, т.е. при условии, что число $n \in \mathbb{N}_{|G_\gamma|-1}$ не является кратным порядка ни для какого элемента $P \in G_\gamma \backslash \{\mathcal{O}\}$ группы $\mathcal{G}_\gamma$.□

Из равенства (6.128) непосредственно вытекает, что истинны следующие два следствия.

Следствие 6.7. Каждый входной символ $x \in \mathbb{Z}_l$ переводит состояния $q_0, \widetilde{q}_0 \in G_\gamma$ $(q_0 \neq \widetilde{q}_0)$ автомата $M_r \in \mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$ в одно и то же состояние тогда и только тогда, когда либо $n = 0$, либо $n \in \mathbb{N}_{|G_\gamma|-1}$ и число n – кратное порядка элемента $\widetilde{q}_0 -_\gamma q_0 \in G_\gamma \backslash \{\mathcal{O}\}$ группы $\mathcal{G}_\gamma$.□

Следствие 6.8. Каждый входной символ $x \in \mathbb{Z}_l$ переводит состояния $q_0, \widetilde{q}_0 \in G_\gamma$ $(q_0 \neq \widetilde{q}_0)$ автомата $M_r \in \mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$ в различные состояния тогда и только тогда, когда $n \in \mathbb{N}_{|G_\gamma|-1}$ и число n не является кратным порядка элемента $\widetilde{q}_0 -_\gamma q_0 \in G_\gamma \backslash \{\mathcal{O}\}$ группы $\mathcal{G}_\gamma$.□

В дальнейшем нам понадобится следующее обозначение

$$\mathtt{n}_t = \begin{cases} 1, & \text{если } n = 0 \text{ и } t = 0 \\ n^t, & \text{если } n \in \mathbb{N}_{|G_\gamma|-1} \text{ и } t \in \mathbb{N} \end{cases}.$$

Напомним, что автомат является приведенным, если каждые два его различных состояния не являются эквивалентными.

Обозначим через $\mathcal{M}_{r,\gamma,l}^{rdcd}$ $(r=1,2)$ семейство, состоящее из всех приведенных автоматов $M_r \in \mathcal{M}_{r,\gamma,l}$ $(r=1,2)$.

Теорема 6.13. Семейство автоматов $\mathcal{M}_{1,\gamma,l}^{rdcd}$ состоит из всех таких автоматов $M_1 \in \mathcal{M}_{1,\gamma,l}$, что $m \in \mathbb{N}_{|G_\gamma|-1}$ и число m не является кратным порядка ни для какого элемента $P \in G_\gamma \backslash \{\mathcal{O}\}$ группы $\mathcal{G}_\gamma$.$\square$

Доказательство. Из 1-го рекуррентного соотношения системы рекуррентных соотношений (6.122) вытекает, что

$$q_{t+1} = \mathtt{n}_{t+1} q_0 +_\gamma \left(\sum_{i=0}^{t} \mathtt{n}_{t-i} x_{i+1} \right) P_1 \quad (t \in \mathbb{Z}_+). \tag{6.129}$$

Из 2-го рекуррентного соотношения системы рекуррентных соотношений (6.122) и равенства (6.129) вытекает, что

$$y_{t+1} = m\mathtt{n}_t q_0 +_\gamma m \left(\sum_{i=0}^{t-1} \mathtt{n}_{t-1-i} x_{i+1} \right) P_1 +_\gamma x_{t+1} P_2 \quad (t \in \mathbb{Z}_+). \tag{6.130}$$

Как известно, состояния $q_0, \widetilde{q}_0 \in G_\gamma$ $(q_0 \neq \widetilde{q}_0)$ автомата $M_1 \in \mathcal{M}_{1,\gamma,l}$ эквивалентны тогда и только тогда, когда реакции инициальных автоматов (M_1, q_0) и $(M_1, \widetilde{q}_0)$ одинаковы на каждое входное слово $u \in (\mathbb{Z}_l)^{|G_\gamma|-1}$.

Следовательно, из (6.130) вытекает, что состояния $q_0, \widetilde{q}_0 \in G_\gamma$ $(q_0 \neq \widetilde{q}_0)$ автомата $M_1 \in \mathcal{M}_{1,\gamma,l}$ эквивалентны тогда и только тогда, когда

$$m\mathtt{n}_t(\widetilde{q}_0 -_\gamma q_0) = \mathcal{O} \ (t = 0, 1, \ldots, |G_\gamma| - 2). \tag{6.131}$$

Ясно, что равенства (6.131) эквивалентны равенству

$$m(\widetilde{q}_0 -_\gamma q_0) = \mathcal{O}. \tag{6.132}$$

Из (6.132) вытекает, что либо $m = 0$, либо $m \in \mathbb{N}_{|G_\gamma|-1}$ и число m является кратным порядка элемента $\widetilde{q}_0 -_\gamma q_0 \in G_\gamma \backslash \{\mathcal{O}\}$ группы $\mathcal{G}_\gamma$.

Для каждого элемента $q_0 \in G_\gamma$ если элемент $\widetilde{q}_0$ пробегает (без повторений) множество $G_\gamma \backslash \{q_0\}$, то элемент $\widetilde{q}_0 -_\gamma q_0$ пробегает (без повторений) множество $G_\gamma \backslash \{\mathcal{O}\}$.

Следовательно, из равенства (6.132) вытекает, что каждые два состояния $q_0, \widetilde{q}_0 \in G_\gamma$ $(q_0 \neq \widetilde{q}_0)$ автомата $M_1 \in \mathcal{M}_{1,\gamma,l}$ не эквивалентны тогда и только тогда, когда $mP \neq \mathcal{O}$ для всех элементов $P \in G_\gamma \backslash \{\mathcal{O}\}$, т.е. при условии, что число $m \in \mathbb{N}_{|G_\gamma|-1}$ не является кратным порядка ни для какого элемента $P \in G_\gamma \backslash \{\mathcal{O}\}$ группы $\mathcal{G}_\gamma$.$\square$

Из доказательства теоремы 6.13 непосредственно вытекает, что истинны следующие два следствия.

Следствие 6.9. Каждые два состояния $q_0, \widetilde{q_0} \in G_\gamma$ $(q_0 \neq \widetilde{q_0})$ автомата $M_1 \in \mathcal{M}_{1,\gamma,l}^{rdcd}$ различаются каждым входным символом $x \in \mathbb{Z}_l$.$\square$

Следствие 6.10. Пусть $M_1 \in \mathcal{M}_{1,\gamma,l} \backslash \mathcal{M}_{1,\gamma,l}^{rdcd}$ и $m \in \mathbb{N}_{|G_\gamma|-1}$. Для каждого состояния $q_0 \in G_\gamma$ автомата M_1 множество S_{q_0} всех состояний, эквивалентных состоянию q_0, имеет вид

$$S_{q_0} = \{q_0\} \cup S'_{q_0},$$

где S'_{q_0} является множеством всех таких элементов $q \in G_\gamma \backslash \{q_0\}$, что порядок элемента $q - q_0$ группы $\mathcal{G}_\gamma$ является делителем числа m.$\square$

Теорема 6.14. Семейство автоматов $\mathcal{M}_{2,\gamma,l}^{rdcd}$ состоит из всех таких автоматов $M_2 \in \mathcal{M}_{2,\gamma,l}$, что $n, m \in \mathbb{N}_{|G_\gamma|-1}$ и число mn не является кратным порядка ни для какого элемента $P \in G_\gamma \backslash \{\mathcal{O}\}$ группы $\mathcal{G}_\gamma$.$\square$

Доказательство. Из 1-го рекуррентного соотношения системы рекуррентных соотношений (6.124) вытекает, что истинно равенство (6.129).

Из 2-го рекуррентного соотношения системы рекуррентных соотношений (6.124) и равенства (6.129) вытекает, что

$$y_{t+1} = m\mathtt{n}_{t+1}q_0 +_\gamma m\left(\sum_{i=0}^{t} \mathtt{n}_{t-i}x_{i+1}\right)P_1 \quad (t \in \mathbb{Z}_+). \tag{6.133}$$

Как известно, состояния $q_0, \widetilde{q_0} \in G_\gamma$ $(q_0 \neq \widetilde{q_0})$ автомата $M_2 \in \mathcal{M}_{2,\gamma,l}$ эквивалентны тогда и только тогда, когда реакции инициальных автоматов (M_2, q_0) и $(M_2, \widetilde{q_0})$ одинаковы на каждое входное слово $u \in (\mathbb{Z}_l)^{|G_\gamma|-1}$.

Следовательно, из (6.133) вытекает, что состояния $q_0, \widetilde{q_0} \in G_\gamma$ $(q_0 \neq \widetilde{q_0})$ автомата $M_2 \in \mathcal{M}_{2,\gamma,l}$ эквивалентны тогда и только тогда, когда

$$m\mathtt{n}_{t+1}(\widetilde{q_0} -_\gamma q_0) = \mathcal{O} \ (t = 0, 1, \ldots, |G_\gamma| - 2). \tag{6.134}$$

Ясно, что равенства (6.134) эквивалентны равенству

$$mn(\widetilde{q_0} -_\gamma q_0) = \mathcal{O}. \tag{6.135}$$

Из (6.135) вытекает, что либо $mn = 0$, либо $n, m \in \mathbb{N}_{|G_\gamma|-1}$ и число mn является кратным порядка элемента $\widetilde{q_0} -_\gamma q_0 \in G_\gamma \backslash \{\mathcal{O}\}$ группы $\mathcal{G}_\gamma$.

Для каждого элемента $q_0 \in G_\gamma$ если элемент $\widetilde{q_0}$ пробегает (без повторений) множество $G_\gamma \backslash \{q_0\}$, то элемент $\widetilde{q_0} -_\gamma q_0$ пробегает (без повторений) множество $G_\gamma \backslash \{\mathcal{O}\}$.

Следовательно, из равенства (6.135) вытекает, что каждые два состояния $q_0, \widetilde{q}_0 \in G_\gamma$ $(q_0 \neq \widetilde{q}_0)$ автомата $M_2 \in \mathcal{M}_{2,\gamma,l}$ не эквивалентны тогда и только тогда, когда $mnP \neq \mathcal{O}$ для всех элементов $P \in G_\gamma \backslash \{\mathcal{O}\}$, т.е. при условии, что $n, m \in \mathbb{N}_{|G_\gamma|-1}$ и число mn не является кратным порядка ни для какого элемента $P \in G_\gamma \backslash \{\mathcal{O}\}$ группы $\mathcal{G}_\gamma$.$\square$

Из доказательства теоремы 6.14 непосредственно вытекает, что истинны следующие два следствия.

Следствие 6.11. Каждые два состояния $q_0, \widetilde{q}_0 \in G_\gamma$ $(q_0 \neq \widetilde{q}_0)$ автомата $M_2 \in \mathcal{M}^{rdcd}_{2,\gamma,l}$ различаются каждым входным символом $x \in \mathbb{Z}_l$.$\square$

Следствие 6.12. Пусть $M_2 \in \mathcal{M}_{2,\gamma,l} \backslash \mathcal{M}^{rdcd}_{2,\gamma,l}$ и $n, m \in \mathbb{N}_{|G_\gamma|-1}$. Для каждого состояния $q_0 \in G_\gamma$ автомата M_2 множество S_{q_0} всех состояний, эквивалентных состоянию q_0, имеет вид

$$S_{q_0} = \{q_0\} \cup S''_{q_0},$$

где S''_{q_0} является множеством всех таких элементов $q \in G_\gamma \backslash \{q_0\}$, что порядок элемента $q - q_0$ группы $\mathcal{G}_\gamma$ является делителем числа mn.$\square$

Напомним, что два различных состояния автомата – близнецы, если по любому входному символу они переходят в одно и то же состояние и при этом переходе автомат выдает один и тот же выходной символ.

Замечание 6.13. Ясно, что состояния-близнецы являются эквивалентными состояниями автомата. При этом все автоматы, не являющиеся приведенными, можно разбить на два множества: 1-е множество состоит из всех автоматов, имеющих состояния-близнецы, а 2-е множество состоит из всех автоматов, не являющихся приведенными, у которых каждые два различные эквивалентные состояния переводятся каждым входным словом в различные эквивалентные состояния.

Из следствий 6.7, 6.10 и 6.12 непосредственно вытекает, что истинны следующие два следствия.

Следствие 6.13. Пусть $M_1 \in \mathcal{M}_{1,\gamma,l}$. Состояния $q_0, \widetilde{q}_0 \in G_\gamma$ $(q_0 \neq \widetilde{q}_0)$ автомата M_1 являются близнецами тогда и только тогда, когда выполнено одно из следующих четырех условий:

1) $n = m = 0$;

2) $n = 0$, $m \in \mathbb{N}_{|G_\gamma|-1}$ и порядок элемента $\widetilde{q}_0 - q_0 \in G_\gamma \backslash \{\mathcal{O}\}$ группы $\mathcal{G}_\gamma$ является делителем числа m;

3) $m = 0$, $n \in \mathbb{N}_{|G_\gamma|-1}$ и порядок элемента $\widetilde{q}_0 - q_0 \in G_\gamma \backslash \{\mathcal{O}\}$ группы $\mathcal{G}_\gamma$ является делителем числа n;

4) $n, m \in \mathbb{N}_{|G_\gamma|-1}$ и каждое из чисел n и m является кратным порядка элемента $\widetilde{q}_0 - q_0 \in G_\gamma \backslash \{\mathcal{O}\}$ группы $\mathcal{G}_\gamma$.$\square$

Следствие 6.14. Пусть $M_2 \in \mathcal{M}_{2,\gamma,l}$. Состояния $q_0, \widetilde{q_0} \in G_\gamma$ $(q_0 \neq \widetilde{q_0})$ автомата M_2 являются близнецами тогда и только тогда, когда выполнено одно из следующих двух условий:

1) $n = 0$;

2) $n \in \mathbb{N}_{|G_\gamma|-1}$ и порядок элемента $\widetilde{q_0} - q_0 \in G_\gamma \backslash \{\mathcal{O}\}$ группы $\mathcal{G}_\gamma$ является делителем числа n.

Напомним, что автомат называется сильно связанным тогда и только тогда, когда для каждой упорядоченной пары его состояний существует входное слово, переводящее 1-е состояние во 2-е состояние.

Теорема 6.15. Автомат $M_r \in \mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$ не является сильно связанным, если либо $P_1 = \mathcal{O}$, либо $P_1 \in G_\gamma \backslash \{\mathcal{O}\}$ и порядок элемента P_1 отличается от порядка $|G_\gamma|$ группы $\mathcal{G}_\gamma$.$\square$

Доказательство. Предположим, что $P_1 = \mathcal{O}$.

Подставив $P_1 = \mathcal{O}$ и $q_0 = \mathcal{O}$ в равенство (6.129), получим, что

$$q_{t+1} = \mathtt{n}_{t+1}\mathcal{O} +_\gamma \left(\sum_{i=0}^{t} \mathtt{n}_{t-i}x_{i+1}\right)\mathcal{O} =$$

$$= \left(\mathtt{n}_{t+1} + \left(\sum_{i=0}^{t} \mathtt{n}_{t-i}x_{i+1}\right)\right)\mathcal{O} \quad (t \in \mathbb{Z}_+). \tag{6.136}$$

Из (6.136) вытекает, что если $P_1 = \mathcal{O}$, то каждое входное слово $x_1 \dots x_{t+1} \in (\mathbb{N}_l)^+$ переводит состояние $q_0 = \mathcal{O}$ автомата $M_r \in \mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$ в себя, т.е. $q_0 = \mathcal{O}$ является состоянием-стоком автомата M_r.

Следовательно, если $P_1 = \mathcal{O}$, то подавтомат автомата $M_r \in \mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$, определяемый состоянием $q = \mathcal{O}$, является собственным подавтоматом автомата M_r.

Это означает, что если $P_1 = \mathcal{O}$, то автомат $M_r \in \mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$ не является сильно связанным автоматом, что и требовалось доказать.

Предположим, что $P_1 \in G_\gamma \backslash \{\mathcal{O}\}$ и порядок элемента P_1 отличается от порядка $|G_\gamma|$ группы $\mathcal{G}_\gamma$.

Тогда циклическая подгруппа

$$\langle P_1 \rangle = (\{kP_1 | k \in \mathbb{Z}\}, +_\gamma)$$

является собственной подгруппой группы $\mathcal{G}_\gamma$.

Подставив $q_0 = P_1$ в равенство (6.129), получим, что

$$q_{t+1} = \mathtt{n}_{t+1}P_1 +_\gamma \left(\sum_{i=0}^{t} \mathtt{n}_{t-i}x_{i+1}\right)P_1 =$$

$$= \left(\mathtt{n}_{t+1} + \left(\sum_{i=0}^{t} \mathtt{n}_{t-i} x_{i+1}\right)\right) P_1 \quad (t \in \mathbb{Z}_+). \tag{6.137}$$

Из (6.137) вытекает, что каждое входное слово $x_1 \dots x_{t+1} \in (\mathbb{N}_l)^+$ переводит состояние $q_0 = P_1$ автомата $M_r \in \mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$ в состояние $q_{t+1} \in \{kP_1 | k \in \mathbb{Z}\}$.

Следовательно, если $P_1 \in G_\gamma \backslash \{\mathcal{O}\}$ и порядок элемента P_1 отличается от порядка $|G_\gamma|$ группы $\mathcal{G}_\gamma$, то подавтомат автомата $M_r \in \mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$, определяемый множеством состояний $\{kP_1 | k \in \mathbb{Z}\}$, является собственным подавтоматом автомата M_r.

Это означает, что если $P_1 \in G_\gamma \backslash \{\mathcal{O}\}$ и порядок элемента P_1 отличается от порядка $|G_\gamma|$ группы $\mathcal{G}_\gamma$, то автомат $M_r \in \mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$ не является сильно связанным автоматом, что и требовалось доказать.□

6.5.3. Идентификация исследуемых моделей.

Всюду в дальнейшем считаем, что $n, m \in \mathbb{N}_{|G_\gamma|-1}$ и $P_1, P_2 \in G_\gamma \backslash \{\mathcal{O}\}$.

Рассмотрим вначале задачу идентификации начального состояния автомата $M_r \in \mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$ при условии, что экспериментатору известны числа $n, m \in \mathbb{N}_{|G_\gamma|-1}$ и точки $P_1, P_2 \in G_\gamma \backslash \{\mathcal{O}\}$.

Теорема 6.16. Для каждого автомата $M_1 \in \mathcal{M}_{1,\gamma,l}$ идентификация начального состояния (с точностью до множества эквивалентных состояний) сводится к поиску любого решения $u \in G_\gamma$ уравнения

$$mu = a_0, \tag{6.138}$$

где элемент $a_0 \in G_\gamma$ определяется в результате простого эксперимента длины 1 с автоматом M_1.□

Доказательство. Пусть $M_1 \in \mathcal{M}_{1,\gamma,l}$.

Из равенства (6.130) вытекает, что

$$mn^t q_0 = a_t \ (t \in \mathbb{Z}_+),$$

где

$$a_t = y_{t+1} -_\gamma m\left(\sum_{i=0}^{t-1} n^{t-1-i} x_{i+1}\right) P_1 -_\gamma x_{t+1} P_2 \quad (t \in \mathbb{Z}_+),$$

т.е. начальное состояние автомата $M_1 \in \mathcal{M}_{1,\gamma,l}$ является решением системы уравнений

$$mn^t u = a_t \ (t \in \mathbb{Z}_+). \tag{6.139}$$

Так как при $t \in \mathbb{N}$ каждое уравнение системы уравнений (6.139) является следствием уравнения (6.138), то достаточно ограничиться именно уравнением (6.138).

Если $M_1 \in \mathcal{M}_{1,\gamma,l}^{rdcd}$, то из следствия 6.9 вытекает, что при всех $x \in \mathbb{Z}_l$ уравнение (6.138) имеет одно и то же единственное решение.

Если же $M_1 \in \mathcal{M}_{1,\gamma,l} \backslash \mathcal{M}_{1,\gamma,l}^{rdcd}$, то при всех $x \in \mathbb{Z}_l$ уравнение (6.138) имеет одно и то же непустое множество решений S_{q_0}, состоящее из всех состояний, эквивалентных состоянию q_0 (см. следствие 6.10).

Из сказанного выше также вытекает, что для вычисления элемента $a_0 \in G_\gamma$ достаточно провести с автоматом $M_1 \in \mathcal{M}_{1,\gamma,l}$ простой эксперимент длины 1, состоящий в подаче на автомат M_1 любого входного символа $x \in \mathbb{Z}_l$ и наблюдении соответствующей реакции автомата.□

Замечание 6.14. Из доказательства теоремы 6.16 вытекает, что

$$a_0 = y_1 -_\gamma x_1 P_2.$$

Таким образом, при идентификации (с точностью до множества эквивалентных состояний) начального состояния автомата $M_1 \in \mathcal{M}_{1,\gamma,l}$ из четырех параметров $m, n \in \mathbb{N}_{|G_\gamma|-1}$ и $P_1, P_2 \in G_\gamma \backslash \{\mathcal{O}\}$, определяющих автомат M_1, экспериментатор существенно использует только параметры $m \in \mathbb{N}_{|G_\gamma|-1}$ и $P_2 \in G_\gamma \backslash \{\mathcal{O}\}$, и вообще не использует никакой информации о параметрах $n \in \mathbb{N}_{|G_\gamma|-1}$ и $P_1 \in G_\gamma \backslash \{\mathcal{O}\}$.

Теорема 6.17. Для каждого автомата $M_2 \in \mathcal{M}_{2,\gamma,l}$ идентификация начального состояния (с точностью до множества эквивалентных состояний) сводится к поиску любого решения $v \in G_\gamma$ уравнения

$$mnv = b_0, \tag{6.140}$$

где элемент $b_0 \in G_\gamma$ определяется в результате простого эксперимента длины 1 с автоматом M_2.□

Доказательство. Пусть $M_2 \in \mathcal{M}_{2,\gamma,l}$.

Из равенства (6.133) вытекает, что

$$mn^{t+1} q_0 = b_t \ (t \in \mathbb{Z}_+),$$

где

$$b_t = y_{t+1} -_\gamma m\left(\sum_{i=0}^{t} n^{t-i} x_{i+1}\right) P_1 \quad (t \in \mathbb{Z}_+),$$

т.е. начальное состояние автомата $M_2 \in \mathcal{M}_{2,\gamma,l}$ является решением системы уравнений

$$mn^{t+1} v = b_t \ (t \in \mathbb{Z}_+). \tag{6.141}$$

Так как при $t \in \mathbb{N}$ каждое уравнение системы уравнений (6.141) является следствием уравнения (6.140), то достаточно ограничиться именно уравнением (6.140).

Если $M_2 \in \mathcal{M}_{2,\gamma,l}^{rdcd}$, то из следствия 6.11 вытекает, что при всех $x \in \mathbb{Z}_l$ уравнение (6.140) имеет одно и то же единственное решение.

Если же $M_2 \in \mathcal{M}_{2,\gamma,l} \backslash \mathcal{M}_{2,\gamma,l}^{rdcd}$, то при всех $x \in \mathbb{Z}_l$ уравнение (6.140) имеет одно и то же непустое множество решений S_{q_0}, состоящее из всех состояний, эквивалентных состоянию q_0 (см. следствие 6.12).

Из сказанного выше также вытекает, что для вычисления элемента $b_0 \in G_\gamma$ достаточно провести с автоматом $M_2 \in \mathcal{M}_{2,\gamma,l}$ простой эксперимент длины 1, состоящий в подаче на автомат M_2 любого входного символа $x \in \mathbb{Z}_l$ и наблюдении соответствующей реакции автомата.□

Замечание 6.15. Из доказательства теоремы 6.17 вытекает, что

$$b_0 = y_1 -_\gamma m x_1 P_1.$$

Таким образом, при идентификации (с точностью до множества эквивалентных состояний) начального состояния автомата $M_2 \in \mathcal{M}_{2,\gamma,l}$ экспериментатор существенно использует все три параметра $m, n \in \mathbb{N}_{|G_\gamma|-1}$ и $P_1 \in G_\gamma \backslash \{\mathcal{O}\}$, определяющие автомат M_2.

Рассмотрим теперь задачу параметрической идентификации для семейства автоматов $\mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$ в предположении, что экспериментатор, не имея никакой информации о начальном состоянии автомата, может проводить с исследуемым (неизвестным) инициальным автоматом (M_r, q_0) $(M_r \in \mathcal{M}_{r,\gamma,l}, q_0 \in G_\gamma)$ эксперимент любой кратности и любой высоты.

Под решением задачи параметрической идентификации для семейства автоматов $M_r \in \mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$ будем понимать построение точной имитационной модели.

Последнее означает, что в результате эксперимента с исследуемым (неизвестным) инициальным автоматом (M_r, q_0) $(M_r \in \mathcal{M}_{r,\gamma,l}, q_0 \in G_\gamma)$ осуществляется поиск такой комбинации начального состояния автомата M_r и параметров, определяющих автомат M_r, которая полностью определяет отображение свободной входной полугруппы $\mathbb{Z}_l^+$ в свободную выходную полугруппу G_γ^+, реализуемое неизвестным инициальным автоматом (M_r, q_0).

В процессе построения имитационной модели для семейства автоматов $\mathcal{M}_{r,\gamma,l}$ $(r = 1, 2)$ будем учитывать следующее обстоятельство.

Рассмотрим последовательность

$$\mathcal{F} = \{a^i P\}_{i \in I},$$

где $a \in \mathbb{N}$ – фиксированное число, $P \in G_\gamma$ – фиксированная точка, а $I = \mathbb{N}$, либо $I = \mathbb{Z}_+$.

Обозначим через $\mathcal{F}_b$ ($b \in \mathbb{N}$) подпоследовательность, состоящую из первых b элементов последовательности $\mathcal{F}$.

Так как $\mathcal{G}_\gamma$ – конечная группа, то существует такое наименьшее положительное число $b_{id} \in \mathbb{N}$, что для подпоследовательности $\mathcal{F}_{b_{id}}$ имеет место один из следующих двух случаев:

1) первые $b_{id} - 1$ элементов подпоследовательности $\mathcal{F}_{b_{id}}$ являются попарно различными элементами множества $G_\gamma \backslash \{\mathcal{O}\}$, а последним ее элементом является точка $\mathcal{O}$;

2) первые $b_{id} - 1$ элементов подпоследовательности $\mathcal{F}_{b_{id}}$ являются попарно различными элементами множества $G_\gamma \backslash \{\mathcal{O}\}$, а последний ее элемент равен некоторому предыдущему элементу.

Ясно, что подпоследовательность $\mathcal{F}_{b_{id}}$ полностью определяет последовательность $\mathcal{F}$.

Поэтому назовем подпоследовательность $\mathcal{F}_{b_{id}}$ идентификатором последовательности $\mathcal{F}$.

Отметим, что для каждой последовательности $\mathcal{F} = \{a^i P\}_{i \in I}$ истинно равенство

$$1 \le b_{id} \le |G_\gamma|. \tag{6.142}$$

Теорема 6.18. Построение точной имитационной модели для семейства автоматов $\mathcal{M}_{1,\gamma,l}$ может быть осуществлено в результате кратного эксперимента, кратность которого равна 3, и высота которого не превосходит число $|G_\gamma| + 1$. Суммарная длина всех входных слов, подаваемых на исследуемый автомат в процессе этого эксперимента не превосходит число $|G_\gamma| + 1 + 0.5|G_\gamma|(|G_\gamma| + 3)$.□

Доказательство. Пусть $M_1 \in \mathcal{M}_{1,\gamma,l}$.

Представим равенство (6.130) в виде

$$y_{t+1} = n^t(mq_0) +_\gamma \left(\sum_{i=0}^{t-1} x_{i+1}(n^{t-1-i}(mP_1)) \right) +_\gamma x_{t+1} P_2 \quad (t \in \mathbb{Z}_+). \tag{6.143}$$

Из равенства (6.143) вытекает, что для построения точной имитационной модели для семейства автоматов $\mathcal{M}_{1,\gamma,l}$ достаточно выполнить следующие три действия:

1) идентифицировать элемент $P_2 \in G_\gamma \backslash \{\mathcal{O}\}$ группы $\mathcal{G}_\gamma$;
2) найти идентификатор $\mathcal{F}^{(1)}_{k^{(1)}_{id}}$ последовательности

$$\mathcal{F}^{(1)} = \{n^t(mq_0)\}_{t\in\mathbb{Z}_+};$$

3) найти идентификатор $\mathcal{F}^{(2)}_{k^{(2)}_{id}}$ последовательности

$$\mathcal{F}^{(2)} = \{n^t(mP_1)\}_{t\in\mathbb{Z}_+}.$$

Для того, чтобы найти идентификатор

$$mq_0, n(mq_0), \ldots, n^{k^{(1)}_{id}-1}(mq_0)$$

последовательности

$$\mathcal{F}^{(1)} = \{n^t(mq_0)\}_{t\in\mathbb{Z}_+}$$

достаточно на исследуемый (неизвестный) инициальный автомат (M_1, q_0) $(M_1 \in \mathcal{M}_{1,\gamma,l}, q_0 \in G_\gamma)$ подать входное слово $0^{k^{(1)}_{id}}$, так как при этом

$$n^{t-1}(mq_0) = y_t \ (t = 1, \ldots, k^{(1)}_{id}).$$

После идентификации элемента mq_0, для того, чтобы идентифицировать элемент $P_2 \in G_\gamma \backslash \{\mathcal{O}\}$ достаточно на исследуемый (неизвестный) инициальный автомат (M_1, q_0) $(M_1 \in \mathcal{M}_{1,\gamma,l}, q_0 \in G_\gamma)$ подать входной символ $x_1 = 1$, так как при этом

$$P_2 = y_1 -_\gamma mq_0.$$

После вычисления идентификатора $\mathcal{F}^{(1)}_{k^{(1)}_{id}}$ последовательности $\mathcal{F}^{(1)}$ для того, чтобы найти t-й элемент $(t = 1, \ldots, k^{(2)}_{id})$ идентификатора

$$mP_1, n(mP_1), \ldots, n^{k^{(2)}_{id}-1}(mP_1)$$

последовательности

$$\mathcal{F}^{(2)} = \{n^t(mP_1)\}_{t\in\mathbb{Z}_+},$$

достаточно на исследуемый (неизвестный) инициальный автомат (M_1, q_0) $(M_1 \in \mathcal{M}_{1,\gamma,l}, q_0 \in G_\gamma)$ подать входное слово 10^t, так как при этом

$$n^{t-1}(mP_1) = y_{t+1} -_\gamma n^t(mq_0) \ (t = 1, \ldots, k^{(2)}_{id}).$$

Таким образом, построение точной имитационной модели для семейства автоматов $\mathcal{M}_{1,\gamma,l}$ может быть осуществлено в результате кратного эксперимента, кратности

$$L_1^{(1)} = 1 + 1 + 1 = 3 \tag{6.144}$$

и высоты

$$L_2^{(1)} = \max\{k_{id}^{(1)}, k_{id}^{(2)} + 1\}. \tag{6.145}$$

Суммарная длина всех входных слов, подаваемых в процессе построенного кратного эксперимента на исследуемый (неизвестный) инициальный автомат (M_1, q_0) $(M_1 \in \mathcal{M}_{1,\gamma,l}, q_0 \in G_\gamma)$, равна

$$L_3^{(1)} = k_{id}^{(1)} + 1 + (2 + \cdots + (k_{id}^{(2)} + 1)) =$$

$$= k_{id}^{(1)} + 1 + 0.5k_{id}^{(2)}(k_{id}^{(2)} + 3). \tag{6.146}$$

Из (6.142), (6.144)-(6.146) вытекают оценки, приведенные в формулировке теоремы.□

Теорема 6.19. Построение точной имитационной модели для семейства автоматов $\mathcal{M}_{2,\gamma,l}$ может быть осуществлено в результате кратного эксперимента, кратность которого равна 2, и высота которого не превосходит число $|G_\gamma|$. Суммарная длина всех входных слов, подаваемых на исследуемый автомат в процессе этого эксперимента не превосходит число $|G_\gamma| + 0.5|G_\gamma|(|G_\gamma| + 1)$.□

Доказательство. Пусть $M_2 \in \mathcal{M}_{2,\gamma,l}$.

Представим равенство (6.133) в виде

$$y_{t+1} = mn^{t+1}q_0 +_\gamma \left(\sum_{i=0}^{t} x_{i+1}(n^{t-i}(mP_1))\right) \quad (t \in \mathbb{Z}_+). \tag{6.147}$$

Из (6.147) вытекает, что для построения точной имитационной модели для семейства автоматов $\mathcal{M}_{2,\gamma,l}$ достаточно выполнить следующие два действия:

1) найти идентификатор $\mathcal{F}^{(3)}_{k_{id}^{(3)}}$ последовательности

$$\mathcal{F}^{(3)} = \{n^{t+1}(mq_0)\}_{t\in\mathbb{Z}_+};$$

2) найти идентификатор $\mathcal{F}^{(4)}_{k_{id}^{(4)}}$, последовательности

$$\mathcal{F}^{(4)} = \{n^t(mP_1)\}_{t\in\mathbb{Z}_+}.$$

Для того, чтобы найти идентификатор

$$n(mq_0), n^2(mq_0), \ldots, n^{k_{id}^{(3)}}(mq_0)$$

последовательности

$$\mathcal{F}^{(3)} = \{n^{t+1}(mq_0)\}_{t\in\mathbb{Z}_+}$$

достаточно на исследуемый (неизвестный) инициальный автомат (M_2, q_0) $(M_2 \in \mathcal{M}_{2,\gamma,l}, q_0 \in G_\gamma)$ подать входное слово $0^{k_{id}^{(3)}}$, так как при этом

$$n^t(mq_0) = y_t \ (t = 1, \ldots, k_{id}^{(3)}).$$

После вычисления идентификатора $\mathcal{F}^{(3)}_{k_{id}^{(1)}}$ последовательности $\mathcal{F}^{(3)}$ для того, чтобы найти t-й элемент $(t = 1, \ldots, k_{id}^{(4)})$ идентификатора

$$mP_1, n(mP_1), \ldots, n^{k_{id}^{(4)}-1}(mP_1)$$

последовательности

$$\mathcal{F}^{(4)} = \{n^t(mP_1)\}_{t\in\mathbb{Z}_+},$$

достаточно на исследуемый (неизвестный) инициальный автомат (M_2, q_0) $(M_2 \in \mathcal{M}_{2,\gamma,l}, q_0 \in G_\gamma)$ подать входное слово 10^{t-1}, так как при этом

$$n^{t-1}(mP_1) = y_t -_\gamma n^t(mq_0) \ (t = 1, \ldots, k_{id}^{(4)}).$$

Таким образом, построение точной имитационной модели для семейства автоматов $\mathcal{M}_{2,\gamma,l}$ может быть осуществлено в результате кратного эксперимента, кратности

$$L_1^{(2)} = 1 + 1 = 2 \tag{6.148}$$

и высоты

$$L_2^{(2)} = \max\{k_{id}^{(3)}, k_{id}^{(4)}\}. \tag{6.149}$$

Суммарная длина всех входных слов, подаваемых в процессе построенного кратного эксперимента на исследуемый (неизвестный) инициальный автомат (M_2, q_0) $(M_2 \in \mathcal{M}_{2,\gamma,l}, q_0 \in G_\gamma)$, равна

$$L_3^{(2)} = k_{id}^{(3)} + (1 + \cdots + k_{id}^{(4)}) =$$

$$= k_{id}^{(3)} + 0.5k_{id}^{(4)}(k_{id}^{(4)} + 1). \tag{6.150}$$

Из (6.142), (6.148)-(6.150) вытекают оценки, приведенные в формулировке теоремы.□

6.6. Выводы.

Настоящий раздел посвящен исследованию семейств автоматов Мили и Мура, определенных на многообразиях над конечным кольцом с ненулевым умножением.

Выделены следующие два типа многообразий над конечным кольцом. Во-первых, это многообразия, с заданными на них алгебрами, содержащими унарные и бинарные операции (к этому типу многообразий, в частности, относятся эллиптические кривые, имеющие многочисленные приложения при решении теоретических и прикладных задач). Во-вторых, это параметризованные многообразия, в которых заданы некоторые множества траекторий. Определены гомоморфизмы и изоморфизмы многообразий, принадлежащих указанным выше типам многообразий.

Исследованы свойства кривых 2-го и 3-го порядков, заданных уравнением $y = f(x)$ над конечным ассоциативно-коммутативным кольцом. С одной стороны, такие кривые являются простейшим средством задания множества нелинейных легко вычислимых траекторий в конечном кольце. С другой стороны, эти кривые представляют собой простейшие нелинейные параметризованные многообразия, точки которых легко вычислимы.

Таким образом, в разделе разработан математический аппарат, который (с учетом результатов, полученных в п.5.4) устанавливает глубокую внутреннюю связь между алгебраической теорией автоматов и алгебраической геометрией.

Основные результаты, представленные в настоящем разделе, состоят в следующем:

1. Впервые для конечного кольца с ненулевым умножением построены семейства автоматов Мили и Мура, заданных на многообразии с алгеброй, а также на параметризованном многообразии с выделенным на нем множеством траекторий.

2. Впервые с позиции теории автоматов исследовано строение указанных выше семейств автоматов (охарактеризованы множества семейств групповых автоматов, автоматов, имеющих состояния-близнецы, автоматов, имеющих состояния-источники, автоматов, имеющих состояния-стоки, связных и сильно-связанных автоматов, а также приведенных автоматов).

3. Охарактеризованы гомоморфизмы множеств построенных семейств автоматов при гомоморфизме рассматриваемых многообразий.

4. Впервые построены и исследованы семейства автоматов Мили и Мура, заданных на эллиптической кривой над конечным полем (выделены множества семейств групповых автоматов, сильно связанных автоматов, автоматов, имеющих состояния-близнецы, а также обратимых и приведенных автоматов).

5. Впервые для семейства автоматов, заданного на эллиптической кривой над конечным полем, решена задача идентификации начального состояния автомата, а также задача построения точной имитационной модели.

Таким образом, результаты, полученные в настоящем разделе, в своей совокупности представляют собой фрагмент алгебраической теории автоматов, которая может быть использована при разработке программных систем, предназначенных для построения и анализа автоматных моделей, применяемых в процессе решения задач защиты информации.

Возможны следующие направления дальнейших исследований.

Первое направление исследований связано с анализом свойств кривых 2-го и 3-го порядков, заданных уравнением $y = f(x)$ над конечным кольцом с ненулевым умножением. Здесь естественно возникают следующие три задачи.

Во-первых, это задача исследования свойств генераторов случайных последовательностей элементов кольца, построенных на основе этих кривых.

Во-вторых, это задача исследования свойств семейств автоматов Мили и Мура, заданных на этих кривых (такие семейства автоматов являются простейшими семействами автоматов, заданных на нелинейных параметризованных многообразиях).

В-третьих, это задача исследования свойств этих кривых над конечным ассоциативным не коммутативным кольцом (в частности, над кольцом, изоморфным матричному кольцу над конечным полем).

Второе направление исследований связано с анализом для конечного кольца с ненулевым умножением семейств автоматов Мили и Мура, заданных на многообразии с алгеброй, а также на параметризованном многообразии с выделенным на нем множеством траекторий. Здесь естественно возникают следующие три задачи.

Во-первых, это задача исследования свойств указанных семейств автоматов при наличии тех или иных дополнительных ограничений на многообразие и/или на определенную на нем алгебру, либо на структуру

заданных на многообразии множестве траекторий.

Во-вторых, это задача исследования множеств неподвижных точек автоматных отображений, определяемых автоматами, принадлежащими указанным семействам автоматов.

В-третьих, это задача исследования свойств указанных семейств автоматов при условии, что многообразие является той или иной композицией многообразий с алгеброй и/или параметризованных многообразий с выделенными на них множествами траекторий.

Третье направление исследований связано с анализом семейств автоматов Мили и Мура, заданных на эллиптической кривой γ над конечным полем. Здесь естественно возникают следующие две задачи.

Во-первых, это задача детального исследования свойств указанных семейств автоматов в терминах структуры группы $\mathcal{G}_\gamma$.

Во-вторых, это задача выделения таких семейств автоматов Мили и Мура, заданных на эллиптической кривой γ над конечным полем, для которых суммарная длина входных слов, подаваемых на исследуемый автомат в процессе эксперимента, предназначенного для построения точной имитационной модели, не превосходит величину $O(|G_\gamma|)$ $(|G_\gamma| \to \infty)$, а также таких семейств автоматов, для которых указанная суммарная длина входных слов равна $O(|G_\gamma|^2)$ $(|G_\gamma| \to \infty)$.

ЗАКЛЮЧЕНИЕ

В настоящей монографии разработан фрагмент теории, предназначенной для исследования семейств автоматов, заданных на конечных алгебраических структурах, определенных над конечным кольцом.

Актуальность такого исследования обусловлена следующими обстоятельствами.

Во-первых, автоматы, заданные на конечных алгебраических структурах, определенных над конечным кольцом, формируют новый раздел алгебраической теории автоматов, предметом исследования которого является анализ свойств автоматных отображений конечных алгебраических структур в конечные алгебраические структуры.

Таким образом, тематика исследований, представленных в монографии, актуальна с теоретической точки зрения, так как разработанный математический аппарат дает возможность установить глубокие внутренние связи между алгебраической теорией автоматов, современной алгеброй, алгебраической геометрией и теорией систем.

Во-вторых, применение комбинаторно-алгебраических моделей в процессе решения актуальных для разработки современных информационных технологий задач защиты информации (в том числе, задач криптографии) естественно приводят к задачам анализа автоматов, заданных на конечных алгебраических структурах, определенных над конечным кольцом.

При этом основными становятся задача выделения семейств обратимых автоматов, задача анализа сложности идентификации начального состояния исследуемого автомата, задача анализа сложности параметрической идентификации семейства автоматов и задача анализа множеств неподвижных точек, автоматных отображений.

Таким образом, тематика исследований, представленных в монографии, актуальна с прикладной точки зрения, так разработанный математический аппарат дает возможность теоретически обосновать на основе взаимопроникновения методов теории автоматов, современной алгебры, теории систем и теории алгоритмов вычислительную стойкость автоматных моделей в процессе их применения для решения задач защиты информации (в том числе, задач криптографии).

Основные результаты, представленные в настоящей монографии, состоят в следующем:

I. Разработан математический аппарат, предназначенный для исследования систем уравнений и неравенств над произвольным конечным кольцом с ненулевым умножением. С этой целью:

1. Впервые исследованы множества отображений абстрактного множества в фактор-кольца ассоциативно-коммутативного кольца. Построена комбинаторная схема, основанная на соотношении между множествами отображений абстрактного множества в полную систему вычетов по попарно взаимно простым идеалам и множеством отображений этого же множества в полную систему вычетов по произведению этих идеалов. Показана применимость предложенной комбинаторной схемы для решения модельных алгебраических и теоретико-числовых задач. Построена «ленточная модель», представляющая собой наглядную «геометрическую» интерпретацию предложенной комбинаторной схемы для кольца целых чисел. Доказано отсутствие непосредственного обобщения построенной комбинаторной схемы на бесконечное множество фактор-колец.

2. Охарактеризовано множество $\mathfrak{K}^{fnt}$ всех конечных ассоциативных колец с ненулевым умножением. Для ассоциативного кольца исследованы свойства классов ассоциированных слева и ассоциированных справа элементов, а также свойства множеств левых и правых делителей нуля.

3. Разработана схема, основанная на классах ассоциированных слева и ассоциированных справа элементов, предназначенная для унифицированного представления в неявном виде множества решений системы алгебраических уравнений с параметрами, определенной над ассоциативным кольцом. Построена детализация разработанной схемы для представления в неявном виде множества решений системы алгебраических уравнений с параметрами, определенной над кольцом вычетов $\mathcal{Z}_{p^k}$ (p – простое число, $k \in \mathbb{N}$ ($k \geq 2$)).

4. В терминах (односторонних для не коммутативных колец и двусторонних для коммутативных колец) аннуляторов ненулевых элементов кольца охарактеризованы множества решений простейших атомов линейной арифметики над любым кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$.

5. Впервые построен $\mathcal{LA}(\mathcal{K})$-решатель $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}$, основанный на использовании техники «наслоения» (layering), предназначенный для проверки выполнимости формул линейной арифметики над любым кольцом $\mathcal{K} \in \mathfrak{K}^{fnt}$. Исследована временная сложность $\mathcal{LA}(\mathcal{K})$-решателя $\mathfrak{S}_{\mathcal{LA}(\mathcal{K})}$.

II. Разработаны методы исследования семейств автоматов, заданных системами рекуррентных соотношений с параметрами над конечным кольцом. С этой целью:

1. Решена задача построения имитационной модели семейства автоматов, заданного системой рекуррентных соотношений над конечным кольцом. Для всех комбинаций понятий «в наихудшем случае» и «в среднем», представляющих интерес с позиции прикладной теории алгоритмов, определено понятие «точность имитационной модели». Выделено множество асимптотически точных имитационных моделей, представляющих, по своей сути, формируемый в процессе обучения автомат с конечной памятью.

2. Построены семейства хэш-функций, реализуемые сильно-связными автоматами без выхода, заданными системой рекуррентных соотношений над конечным кольцом. Исследована вычислительная стойкость этих семейств хэш-функций.

III. Построены и исследованы автоматные модели, заданные на алгебраических структурах над конечным кольцом. С этой целью:

1. С позиции универсальной алгебры исследованы семейства автоматов Мили и Мура над конечным ассоциативно-коммутативным кольцом, для которых функции переходов и выходов являются алгебраическими суммами функции от состояния автомата и функции от входного символа при условии, что значение каждой компоненты функции переходов принадлежит фиксированным идеалам кольца.

2. Впервые над конечным кольцом построены семейства автоматов Мили и Мура на многообразиях с алгебрами, а также на параметризованных многообразиях с выделенными на них множествами траекторий. Исследована структура построенных семейств автоматов (охарактеризованы множества семейств групповых автоматов, автоматов, имеющих состояния-близнецы, автоматов, имеющих состояния-источники, автоматов, имеющих состояния-стоки, связных и сильно-связанных автоматов, а также приведенных автоматов). Охарактеризованы гомоморфизмы построенных множеств семейств автоматов при гомоморфизме рассматриваемых многообразий.

3. Впервые построены и исследованы семейства автоматов Мили и Мура, заданных на эллиптической кривой над конечным полем (выделены множества семейств групповых автоматов, сильно связанных автоматов, автоматов, имеющих состояния-близнецы, а также обратимых

и приведенных автоматов). Решена задача идентификации начального состояния автомата, а также задача построения точной имитационной модели для рассматриваемых семейств автоматов.

В своей совокупности перечисленные выше результаты представляют собой фрагмент теории, которая может быть использована при разработке программных систем, предназначенных для построения и анализа автоматных моделей, применяемых в процессе решения задач защиты информации (в том числе, задач криптографии).

Возможные направления развития этой теории, представляющие интерес как с теоретической, так и с прикладной точки зрения, перечислены в выводах к разделам. Кратко эти направления могут быть сформулированы следующим образом.

Во-первых, это построение и исследование решателя, предназначенного для проверки формул нелинейной арифметики, хотя бы для некоторых узких классов конечных колец с ненулевым умножением.

Во-вторых, это исследование для конечных ассоциативных не коммутативных колец, изоморфных матричному кольцу над конечным полем, тех задач, которые решены в монографии для конечных ассоциативно-коммутативных колец.

В-третьих, это построение в явном виде над конечными алгебраическими структурами семейств автоматов, для которых множества неподвижных точек, реализуемых автоматными отображениями, являются достаточно узкими, а решение задач идентификации начального состояния автомата и параметрической идентификации семейства автоматов является достаточно сложным.

В-четвертых, это детальное исследование (прежде всего с позиции универсальной алгебры) множеств семейств автоматов на эллиптических кривых, заданных уравнением над конечной областью целостности.

СПИСОК ЛИТЕРАТУРЫ

1. *Агибалов Г.П.* Распознавание операторов, реализуемых в линейных автономных автоматах // Известия АН СССР. Техническая кибернетика. – 1970. – № 3. – С. 99-108.
2. *Агибалов Г.П., Юфит Я.Г.* О простых экспериментах для линейных инициальных автоматов // Автоматика и вычислительная техника. – 1972. – № 2. – С. 17-19.
3. *Агибалов Г.П.* Методы решения систем полиномиальных уравнений над конечным полем // Вестник Томского государственного университета. Приложение. – 2006. – № 17. – С. 4-9.
4. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. – М.: Гелиос АРВ, 2002. – 480 с.
5. *Анисимов А.В.* Рекурсивные преобразователи информации. – Киев: Вища школа, 1987. – 230 с.
6. *Антонов А.В.* Оценка вычислительных затрат на функционирование криптосистемы, использующей методы хаотической динамики, при решении задач защиты информации в информационно-коммуникационных системах и сетях // Прикладная радиоэлектроника. – 2007. – № 2. – С. 105-109.
7. *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. – М.: Мир, 1979. – 536 с.
8. *Бабаш А.В.* Приближенные модели конечных автоматов // Обозрение прикладной и промышленной математики. – М.: Научное изд-во «ТВП». – 2005. – Т. 12. – № 2. – С. 108-117.
9. *Бернштейн А.С., Попков Ю.С., Фараджев Р.Г.* Аналитическое описание нелинейных последовательностных машин // Автоматика и телемеханика. – 1971. – № 12. – С. 69-77.
10. *Бессалов А.В., Телижненко А.Б.* Криптосистемы на эллиптических кривых. – Киев: Политехника, 2004. – 223 с.
11. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576 с.
12. *Болотов А.А., Гашков С.Б., Фролов А.Б.* Элементарное введение в эллиптическую криптографию: протоколы криптографии на эллиптических кривых. – М.: КомКнига, 2006. – 280 с.
13. *Ван дер Варден Б.Л.* Алгебра. – М.: Наука, 1976. – 624 с.
14. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – 328 с.
15. *Гилл А.* Введение в теорию конечных автоматов. – М.: Наука, 1966. – 272 с.
16. *Гилл А.* Линейные последовательностные машины. – М.: Наука, 1974. – 298 с.
17. *Глухов М.М.* О применении квазигрупп в криптографии // Прикладная дискретная математика. – 2008. – № 2. – С. 28-32.

18. *Глушков В.М.* Абстрактная теория автоматов // Успехи мат. наук. – 1961. – № 5. – С. 3-62.

19. *Глушков В.М.* Абстрактные автоматы и разбиение свободных полугрупп // Докл. АН СССР. – 1961. – № 4. – С. 765-768.

20. *Глушков В.М.* Синтез цифровых автоматов. – М.: Физматлит, 1962. – 476 с.

21. *Глушков В.М., Летичевский А.А.* Теория дискретных преобразователей // Избранные вопросы алгебры и логики. – Новосибирск: Наука, 1973. – С. 5-39.

22. *Голод П.И., Климык А.У.* Математические основы теории симметрий. – Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. – 528 с.

23. *Горяшко А.П.* Проектирование легко тестируемых дискретных устройств: идеи, методы, реализация // Автоматика и телемеханика. – 1984. – № 7. – С. 5-35.

24. *Гриффитс Ф., Харрис Дж.* Принципы алгебраической геометрии.Т. 1,2. – М.: Мир, 1982. – 862 с.

25. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. – М.: Мир, 1982. – 416 с.

26. *Жуков А.Е., Чистяков В.П.* Матричный подход к исследованию прообразов выходной последовательности автомата // Обозрение прикладной и промышленной математики. – М.: Научное изд-во «ТВП». – 1994. – Т. 1. – № 1. – С. 108-117.

27. *Зарисский О., Самюэль П.* Коммутативная алгебра. Т. 1. – М.: ИЛ, 1963. – 374с.

28. *Зарисский О., Самюэль П.* Коммутативная алгебра. Т. 2. – М.: ИЛ, 1963. – 438с.

29. *Зачесов Ю.Л., Салихов Н.П.* Алгоритм решения полиномиального сравнения $P(x) \equiv 0\ (modN)$ и его экспериментальное подтверждение // Вестник Томского государственного университета. Приложение. – 2007. – № 23. – С. 95-98.

30. *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.

31. *Калман Р., Фалб П., Арбиб М.* Очерки по математической теории систем. – М.: Мир, 1971. – 400 с.

32. *Коблиц Н.* Введение в эллиптические и модулярные формы. – М.: Мир, 1988. – 320 с.

33. *Коблиц Н.* Курс теории чисел и криптография. – М.: Научное изд-во «ТВП», 2001. – 262 с.

34. *Кокс Д., Литтл Дж., О'Ши Д.* Идеалы, многообразия и алгоритмы. – М.: Мир, 2000. – 687 с.

35. *Кон П.М.* Универсальная алгебра. – М. Мир, 1968. – 352 с.

36. *Кострикин А.И.* Введение в алгебру. Ч. 1. Основы алгебры. – М.: Физматлит, 2000. – 272 с.

37. *Кострикин А.И.* Введение в алгебру. Ч. 2. Линейная алгебра. – М.: Физматлит, 2000. – 368 с.

38. *Кострикин А.И.* Введение в алгебру. Ч. 3. Основные структуры алгебры. – М.: Физматлит, 2000. – 272 с.

39. *Кудрявцев В.Б., Гассанов Э.Э., Подколзин А.С.* Введение в теорию интеллектуальных систем. – М.: МАКС Пресс, 2006. – 208 с.

40. *Кузнецов С.П.* Динамический хаос. – М.: Физматлит, 2001. – 296 с.

41. *Кузьмин А.С., Куракин В.Л., Нечаев А.А.* Псевдослучайные и полилинейные последовательности. – Труды по дискретной математике. Т. 1. – М.: Научное изд-во «ТВП». – 1997. – С. 139-202.

42. *Кузьмин А.С., Куракин В.Л., Нечаев А.А.* Свойства линейных и полилинейных рекуррент над кольцами Галуа (I). - Труды по дискретной математике. Т. 2. – М.: Научное изд-во «ТВП». – 1998. – С. 191-222.

43. *Курмит А.* Автоматы без потери информации конечного порядка. – Рига: Зинатне, 1972. – 266 с.

44. *Курош А.Г.* Лекции по общей алгебре. – М.: Наука, 1973. – 400 с.

45. *Ленг С.* Алгебра. – М.: Мир, 1968. – 564 с.

46. *Ленг С.* Введение в алгебраические и абелевы функции. – М.: Мир, 1976. – 136с.

47. *Ленг С.* Эллиптические функции. – М.: Наука, 1984. – 312 с.

48. *Ленг С.* Основы диофантовой геометрии. – М.: Мир, 1986. – 446 с.

49. *Лиддл Р., Нидеррайтер Г.* Конечные поля. Т. 1. – М.: Мир, 1988. – 428 с.

50. *Лиддл Р., Нидеррайтер Г.* Конечные поля. Т. 2. – М.: Мир, 1988. – 394 с.

51. *Липский В.* Комбинаторика для программистов. – М.: Мир, 1988. – 213 с.

52. *Льюнг Л.* Идентификация систем. Теория для пользователя. – М.: Наука, 1991. – 432 с.

53. *Мальцев А.И.* Алгебраические системы. – М.: Наука, 1970. – 329 с.

54. *Медведев И.Л., Фараджев Р.Г., Чуйко А.С.* Применение модулярных линейных уравнений для описания линейных последовательностных машин // Автоматика и телемеханика. – 1971. – № 8. – С. 63-71.

55. *Михайлов В.Г., Чистяков В.П.* О задачах теории конечных автоматов, связанных с числом прообразов выходной последовательности // Обозрение прикладной и промышленной математики. – М.: Научное изд-во «ТВП». – 1994. – Т. 1. – № 1. – С. 7-31.

56. *Михайлов В.Г.* Обобщение теоремы о числе прообразов выходной последовательности автомата // Обозрение прикладной и промышленной математики. – М.: Научное изд-во «ТВП». – 1994. – Т. 1. – № 1. – С. 122-125.

57. *Михайлов В.Г.* Асимптотическая нормальность числа прообразов выходной последовательности автомата // Обозрение прикладной и промышленной математики. – М.: Научное изд-во «ТВП». – 1994. – Т. 1. – № 1. – С. 126-135.

58. *Рейнгольд Э., Нивергельт Ю., Део Н.* Комбинаторные алгоритмы. Теория и практика. – М.: Мир, 1980. – 476 с.

59. *Рид М.* Алгебраическая геометрия для всех. – М.: Мир, 1991. – 151 с.

60. *Рысцов И.К.* Оценка длины кратчайшего диагностического слова для конечного автомата // Кибернетика. – 1978. – № 6. – С. 40-45.

61. *Рысцов И.К.* Асимптотическая оценка длины кратчайшего диагностического слова для конечного автомата // Доклады АН СССР. – 1978. – № 6. – С. 40-45.

62. *Сачков В.Н.* Введение в комбинаторные методы дискретной математики. – М.: Наука, 1982. – 384 с.

63. *Севостьянов Б.А., Чистяков В.П.* О числе входных последовательностей, соответствующих выходной последовательности автомата // Обозрение прикладной и промышленной математики. – М.: Научное изд-во «ТВП». – 1994. – Т. 1. – № 1. – С. 96-107.

64. *Скобелев В.В.* Исследование структуры множества линейных БПИ-автоматов над кольцом $\mathcal{Z}_{p^k}$ // Доповіді НАНУ. – 2007. – № 10. – С. 44-49.

65. *Скобелев В.В.* Анализ структуры класса линейных автоматов над кольцом $\mathcal{Z}_{p^k}$ // Кибернетика и системный анализ. – 2008. – № 3. – С. 60-74.

66. *Скобелев В.В., Скобелев В.Г.* Анализ шифрсистем. – Донецк: ИПММ НАНУ. – 2009. – 479 с.

67. *Скобелев В.В.* Точная формула для числа обратимых матриц над конечным кольцом // Труды ИПММ НАНУ. – 2009. – Т. 18. – С. 155-158.

68. *Скобелев В.В.* «Ленточная теорема» и ее приложения // Прикладная дискретная математика. – 2009. – № 4. – С. 84-89.

69. *Скобелев В.В., Скобелев В.Г.* Анализ автоматов над конечным кольцом // Праці Міжнародного симпозіума «Питання оптимізації обчислень (ПОО-XXXVI)». Т. 2. – Київ: ІК НАНУ. – 2009. – С. 310-315.

70. *Скобелев В.В., Скобелев В.Г.* Анализ нелинейных автоматов с лагом 2 над конечным кольцом // Прикладная дискретная математика. – 2010. – № 1. – С. 68-85.

71. *Скобелев В.В.* Анализ free-running автомата над конечным кольцом // Системні дослідження та інформаційні технології. – 2010. – № 3. – С. 130-142.

72. *Скобелев В.В., Скобелев В.Г.* О сложности анализа автоматов над конечным кольцом // Кибернетика и системный анализ. – 2010. – № 4. – С. 17-30.

73. *Скобелев В.В.* Сложность задач идентификации для нелинейных одномерных автоматов с лагом 2 над конечным кольцом // Материали 12-ї Міжнародної науково-технічної конференції «Системний аналіз та інформаційні технології (SAIT 2010)». – Київ: ННК ІПСА «НТУУ КПІ». – 2010. – С. 489.

74. *Скобелев В.В.* О сложности идентификации нелинейных автоматов над кольцом // Proc. of the International Conference of Students and Young Scientists «Theoretical and Applied Aspects of Cybernetics (TAAC 2011)». – Kyiv: Bukrek. – 2011. – С. 180-181.

75. *Скобелев В.В.* Об одной схеме решения систем полиномиальных уравнений над конечным кольцом // Праці Міжнародної молодіжної математичної школи «Питання оптимізації обчислень (ПОО-XXXVII)». – Київ: ІК НАНУ. – 2011. – С. 178-179.

76. *Скобелев В.В.* Анализ кривых 2-го порядка над конечным кольцом // Труды ИПММ НАНУ. – 2011. – Т. 22. – С. 184-196.

77. *Скобелєв В.В.* Про деякі властивості кубічних кривих ліній над кільцями // Вісник Київського університету. Серія: фізико-математичні науки. – 2011. – Вип. 2. – С. 147-150.

78. *Скобелев В.В.* Анализ некоторых отображений множеств в дедекиндовы кольца // Доповіді НАНУ. – 2011. – № 3. – С. 41-45.

79. *Скобелев В.В.* Об одном классе отображений абстрактных множеств в кольца // Тезисы докладов Международной конференции «Современные проблемы математики и ее приложения в естественных науках и информационных технологиях». – Харьков: Апостроф. – 2011. – С. 189-190.

80. *Скобелев В.В., Глазунов Н.М., Скобелев В.Г.* Многообразия над кольцами. Теория и приложения. – Донецк: ИПММ НАН Украины, 2011. – 323 с.

81. *Скобелєв В.В.* Про множини автоматів над скінченним кільцем, які визначено у термінах ідеалів // Вісник Київського університету. Сер.: фіз.-мат. науки. – 2011. – Вип. 3. – С. 212-218.

82. *Скобелев В.В.* Сложность идентификации нелинейных одномерных автоматов с лагом 2 над конечным кольцом // Компьютерная математика. – 2011. – Вып. 2. – С. 81-89.

83. *Скобелев В.В.* Свойства делителей нуля в ассоциативных кольцах // Труды ИПММ НАНУ. – 2011. – Т. 23. – С. 192-201.

84. *Скобелев В.В.* О построении имитационной модели нелинейного обратимого автомата над конечным кольцом // Матеріали XVIII Міжнародної конференції з автоматичного управління «AUTOMATICS-2011» . – Львів: Видавництво Львівської політехніки. – 2011. – С. 289-290.

85. *Скобелєв В.В.* Аналіз задачі ідентифікації для автоматів на еліптичних кривих над скінченним полем // Матеріали XIX Міжнародної конференції з автоматичного управління «AUTOMATICS-2012». – Київ: НУХТ. – 2012. – С. 126-127.

86. *Скобелєв В.В., Скобелєв В.Г.* Нерухомі точки автоматних відображень над скінченним кільцем // Матеріали XIX Міжнародної конференції з автоматичного управління «AUTOMATICS-2012». – Київ: НУХТ. – 2012. – С. 128-129.

87. *Скобелев В.В.* О двух последовательностях множеств отображений абстрактных множеств в дедекиндовы кольца // Кибернетика и системный анализ. – 2012. – № 2. – С. 105-112.

88. *Скобелев В.В.* Моделирование автоматов над кольцом автоматами с конечной памятью // Проблемы управления и информатики. – 2012. – № 3. – С.114-122.

89. *Скобелев В.В.* О задаче построения имитационной модели для автоматов над кольцами // Материалы Международной научной конференции «Компьютерные науки и информационные технологи (КНИТ 2012)». – Саратов: СГУ. – 2012. – С. 289-290.

90. *Скобелєв В.В.* Аналіз автоматів, які визначено на еліптичних кривих // Вісник Київського університету. Сер.: фіз.-мат. науки. – 2012. – Вип. 1. – С. 223-230.

91. *Скобелев В.В.* Анализ задачи распознавания автомата над кольцом // Доповіді НАНУ. – 2012. – № 9. – С. 29-35.

92. *Скобелев В.В.* Об автоматах на многообразиях над кольцом // Труды ИПММ НАНУ. – 2012. – Т. 24. – С. 190-201.

93. *Скобелев В.В.* Автомати на многовидах з алгеброю // Вісник Київського університету. Сер.: фіз.-мат. науки. – 2012. – Вип. 2. – С. 234-238.

94. *Скобелев В.В.* Об автоматах на полиномиально параметризованном многообразии над конечным кольцом // Труды ИПММ НАНУ. – 2012. – Т. 25. – С. 185-195.

95. *Скобелєв В.В.* Про один клас геш-функцій для задач захисту інформації // Матеріали 1-ої Міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем». – Львів: Видавництво Львівської політехніки. – 2012. – С. 128-129.

96. *Скобелев В.В.* О хэш-функциях, реализуемых автоматами над алгебраическими структурами // Праці 9-ої Міжнародної науково-практичної конференції «Теоретичні та прикладні аспекти побудови програмних систем (TAAPSD'2012)». – 2012. – С. 268-270.

97. *Скобелєв В.В.* Автомати на еліптичних кривих над скінченним полем // Матеріали II-ої Міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем». – Львів: Видавництво Львівської політехніки, 2013. – С. 12-13.

98. *Скобелев В.В.* О гомоморфизмах автоматов на многообразиях над кольцом // Доповіді НАНУ. – 2013. – № 1. – С. 42-46.

99. *Скобелев В.В.* Анализ семейств хэш-функций, определяемых автоматами над конечным кольцом // Кибернетика и системный анализ. – 2013. – № 2. – С. 46-55.

100. *Скобелев В.В.* Анализ автоматных моделей, определенных над конечным кольцом // Проблемы управления и информатики. – 2013. – № 4. – С. 147-156.

101. *Скобелев В.В.* Проверка выполнимости формул линейной арифметики над конечным кольцом // Праці 10-ої Міжнародної науково-практичної конференції «Теоретичні та прикладні аспекти побудови програмних систем (TAAPSD'2013)». – 2013. – С. 154-158.

102. *Скобелев В.В.* Автоматы на алгебраических структурах // Вестник Саратовского университета. Сер.: математика, механика, информатика. – 2013. – Т. 13. – Вып. 2. – Ч. 2. – С. 58-66.

103. *Скобелев В.Г.* Об оценках длин диагностических и возвратных слов для автоматов // Кибернетика. – 1987. – № 4. – С. 114-116.

104. *Скобелев В.Г.* Нелинейные автоматы над конечным кольцом // Кибернетика и системный анализ. – 2006. – № 6. – С. 29-42.

105. *Соколовский М.Н.* Сложность порождения подстановок и эксперименты с автоматами // Методы дискретного анализа в теории кодов и схем. – 1976. – Вып. 29. – С. 68-86.

106. *Соколовский М.Н.* Оценка длины диагностического слова для конечного автомата // Кибернетика. – 1976. – № 2. – С. 16-21.

107. *Сперанский Д.В.* Эксперименты с линейными и билинейными конечными автоматами. – Саратов: СГУ, 2004. – 144 с.

108. *Трахтенброт Б.А., Барздинь Я.М.* Конечные автоматы (поведение и синтез). – М.: Наука, 1970. – 400 с.

109. *Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В.* Математические и компьютерные основы криптологии. – Минск: Новое знание, 2003. – 382 с.

110. *Черемушкин А.В.* Лекции по арифметическим алгоритмам в криптографии. – М.: МЦНМО, 2002. – 104 с.

111. *Шафаревич И.Р.* Основы алгебраической геометрии. Т. 1. – М.: Наука, 1988. – 352 с.

112. *Шафаревич И.Р.* Основы алгебраической геометрии. Т. 2. – М.: Наука, 1988. – 304 с.

113. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. – М.: ТРИУМФ, 2003. – 816 с.

114. *Adamec J.* Realization theory for automata in categories // J. Pure and Appl. Algebra. – 1977. – Vol. 9. – № 3. – P. 281-296.

115. *Adamec J.* Functional algebra and automata // Kybernetika. – 1977. – Vol. 13. – № 4. – P. 245-260.

116. *Aldeman L.* A sub-exponential algorithm for the discrete logarithm problem with applications to cryptography // Proc. of IEEE 18^{th} Annual Symposium on Foundations of Computer Science. – 1979. – P. 55-60.

117. *Arbib M.A.* Machines in a category // SIAM Review. – 1974. – Vol. 16. – № 2. – P. 163.

118. *Armando A., Guinchiglia E.* Embedding complex decision problems inside an interactive theorem prover // Annals of Mathematics and Artificial Intelligence. – 1993. – N 3-4. – P. 475-502.

119. *Armando A., Castellini C., Guinchiglia E.* SAT-based procedures for temporal reasoning // LNCS. – 2000. – Vol. 1809. – P.97-108.

120. *Ashwin P., Rucklidge A.M., Sturman R.* Cyclic attractors of coupled cell systems and dynamics with symmetry // Synchronization: Theory and application. NATO Science Series. – Vol. 109. – 2003. – P. 5-23.

121. *Audermand G., Bertolli P., Cimatti A., at all.* A SAT based approach for solving formulae over Boolean and linear mathematical propositions // LNCS. – 2002. – Vol. 2392. – P. 195-210.

122. *Bacchus F., Winter J.* Effective prepocessing with hyper-resolution and equality reduction // Proceedings of the 6^{th} International Symposium on Theory and Applications of Satisfiability Testing. – 2003. – http://www.cs.toronto.edu/∼fbacchus/Parers/BSAT2003.pdf

123. *Bajardo R.J., Schrag R.C.* Using CSP look-back techniques to solve real-world SAT instances // Proc. of AAAI'97. – 1997. – P. 203-208.

124. *Barret C. W., Dill D.L., Levitt J.R.* A decision procedure for bit-vector arithmetic // Proc. of The 35^{th} Design Automation Conference. – 1998. – P. 522-527.

125. *Barret C., Dill D., Stump A.* Checking satisfiability of first-order formulae by incremental translation to SAT // LNCS. – 2002. – Vol. 2404. – P. 236-249.

126. *Barret C., Nieuwenhuis R., Oliveras A., at all.* Splitting on demand in SAT modulo theories // LNCS. – 2006. – Vol. 4246. – P. 512-526.

127. *Berezin S., Ganesh V., Dill D.L.* An online proof-producing decision procedure for mixed-integer linear arithmetic // LNCS. – 2003. – Vol. 2619. – P. 521-536.

128. *Birch B.J., Swinnerton-Dyer H.P.F.* Notes on elliptic curves I // Journ. Rein. Angew. Math. – 1963. – Vol. 212. – P. 7-25.

129. *Birch B.J., Swinnerton-Dyer H.P.F.* Notes on elliptic curves II // Journ. Rein. Angew. Math. – 1965. – Vol. 218. – P. 79-108.

130. *Birch B.J.* How the number of points of elliptic curves over a fixed prime field varies // Journ. London Math. Soc. – 1968. – Vol. 43. – p. 57-60.

131. *Bjorner N., Pichora M.C.* Deciding fixed and non-fixed size bit vectors // LNCS. – 1998. – Vol. 1384. – P. 376-392.

132. *Bollobás B.* Modern graph theory. – NY: Springer-Verlag, 1998. – 394 p.

133. *Borning A., Mariott K., Stuckey P.* Solving linear arithmetic constraints for user interface applications // Proc. of UIST'97. – 1997. – P. 87-96.

134. *Bozzano M., Bruttomesso R., Cimatti A., at all.* MathSAT: A tight integration of SAT and mathematical decision procedures // Journal of Automated Reasoning. – 2005. – N 1-3. – P. 265-293.

135. *Bozzano M., Bruttomesso R., Cimatti A., at all.* Efficient satisfiability modulo theories via delayed theory combination // LNCS. – 2005. – Vol. 3576. – P. 335-349.

136. *Bozzano M., Bruttomesso R., Cimatti A., at all.* An icremental and layered procedure for the satisfiability of linear arithmetic logic // LNCS. – 2005. – Vol. 3440. – P. 317-333.

137. *Bozzano M., Bruttomesso R., Cimatti A., at all.* Encoding RTL Constructs for MathSAT // Electr. Notes Theor. Comput. Sci. – 2006. – N 2. – P. 3-14.

138. *Bradley A.R., Manna Z.* The calculus of computation. Desicion procedures with applications to verification. – Berlin-Heidelberg: Springer-Verlag, 2010. – 366 p.

139. *Brafman R.* A simplifier for propositional formulae with many binary clauses // IEEE Transactions on Systems, Man and Cybernetics. – 2004. – N 1. – P. 52-59.

140. *Brinkmann R., Drechsler R.* RTL-datapath verification using integer linear programming // Proc. of DAC'02. – 2002. – P. 741-746.

141. *Castellini C., Guinchiglia E., Tacchella A.* SAT-based planning in complex domains: concurrency, constraints and nondeterminism // Artificial Intelligence. – 2003. – N 1-2. – P. 85-117.

142. *Cherkassky B.V., Goldgerg A.V.* Negative cycle detection algorithms // Mathematical Programming. – 1999. – N 2. – P. 277 - 311.

143. *Chu M.L., Anbulagan.* Look-ahead versus look-back for satisfiability problems // LNCS. – 1997. – Vol. 1330. – P. 341-355.

144. *Chu M.L., Anbulagan.* Heuristics based on unit propagation for satisfiability problems // Proc. of IJCAI'97. – 1997. – P. 366-371.

145. *Chu M.L.* Integrating equivalency reasoning into davis-putnam procedure // Proc. of AAAI'00. – 2000. – P. 291-296.

146. *Cotton S., Maler O.* Fast and flexible difference constraint propagation for DPLL(T) // LNCS. – 2006. – Vol. 4121. – P. 170-183.

147. *Courtois N., Meier W.* Algebraic attack on stream ciphers with linear feedback // LNCS. – 2003. – Vol. 2656. – P. 345-349.

148. *Cyrluk D., Moller M.O., Ruess H.* An efficient decision procedure for the theory of fixed-sized bit-vectors // LNCS. – 1997. – Vol. 1254. – P. 60-71.

149. *Davis M., Putnam H.* A computing procedure for quantification theory // Journal of the ACM. – 1960. – N 3. – P. 201-215.

150. *Davis M., Logemann G., Loveland D.* A machine programm for theorem proving // Journal of the ACM. – 1962. – N 7. – P. 394-397.

151. *de Moura L., Ruass H., Sorea M.* Lazy theorem proving for bounded model checking over infinite domains // LNCS. – 2002. – Vol. 2392. – P. 438-455.

152. *de Moura L., Ruess H.* Lemmas on demand for satisfiability solvers // Proc. of SAT'02. – 2002. – P. 244-251.

153. *de Moura L., Duterte B., Shankar N.* A tutorial on satisfiability modulo theoris // LNCS. – 2007. – Vol. 4590. – P. 20-36.

154. *de Moura L., Bjorner N.* Model based theory combination // Proc. of the 5^{th} Workshop on SMT (SMT'07). – 2007. – http://www.lsi.upc.edu/oliveras/smt07/.

155. *Detlefs D., Nelson G., Saxe J.* Simplify: a theorem prover for program-checking // Journal of the ACM. – 2005. – N 3. – P. 365-473.

156. *Duterte B., de Moura L.* A fast linear-arithmetic solver for DPLL(T) // LNCS. – 2006. – Vol. 4144. – P. 81-94.

157. *Een N., Sorenson N.* An extensible SAT-solver // LNCS. – 2004. – Vol. 2919. – P. 502-518.

158. *Een N., Biere A.* Effective prepocessing in SAT through variable and clause elimination // Proc. of SAT'05. – 2005. – http://mimisat.se/dounloads/SatELite.pdf

159. *Eilenberg S.* Automata, laguages and machines. Vol. A. – NY: Academic Press, 1974. – 451 p.

160. *Eilenberg S.* Automata, laguages and machines. Vol. B. – NY: Academic Press, 1976. – 387 p.

161. *Even S.* On information lossless automata of finite order // IEEE Trans. Elect. Comput. – 1965. – Vol. C-14. – № 4. – P. 561-569.

162. *Fallah F., Devadas S., Keutzer K.* Functional vector generation for HDL models using linear programming and 3-satisfiability // Proc. of DAC'98. – 1998. – P. 355-367.

163. *Faure G., Nieuwenhuis R., Oliveras A., at all.* SAT modulo the theory of linear arithmetic: exact, inexact and commersial solvers // LNCS. – 2008. – Vol. 4996. – P. 77-90.

164. *Flanagan C., Joshi R., Ou X., at all.* Theorem proving using lazy proof explication // LNCS. – 2003. – Vol. 2725. – P. 438-455.

165. *Franzle M., Herde C., Tiege T., at all.* Efficient solving of large non-linear arithmetic constraint systems with complex Boolean structure // Journal of Satisfiability, Boolen Modeling and Computation. – 2007. – N 1. – P. 209-236.

166. *Ganesh V., Dill D.L.* A desicion procedure for bit-vectors and arrays // LNCS. – 2007. – Vol. 4590. – P. 519-531.

167. *Ganzinger H., Hagen G., Nieuwenhus R., at all.* DPLL(T): Fast decision procedures // LNCS. – 2004. – Vol. 3114. – P. 175-188.

168. *Goldberg E., Novikov Y.* BerkMin: a fast and robust SAT-solver // Proc. of DATE'02. – 2002. – P. 142.

169. *Gomes C.P., Selman B., Kautz H.* Boosting combinational search through randomization. // Proc. of AAAI'98. – 1998. – P. 431-437.

170. *Griggio A.* A practical approach to satisfiability modulo linear arithmetic // Journal on Satisfiability, Boolean Modeling and Computation. – 2012. – N 8. – P. 1-27.

171. *Guinchiglia E., Massarotto A., Sebastiani R.* Act, and the rest will follow: exploiting determinism in planning of satisfiability // Proc. of AAAI'98. – 1998. – P. 948-953.

172. *Harvey W., Stuckey P.* A unit two variable per inequality integer constraint solver for constraint logic programming // Proc. of ICAPS'05. – 2005. – P. 71-80.

173. *Hennie F.C.* Finite state models for logical machines. – NY: John Wiley&Sons, Inc., 1962. – 466 p.

174. *Hooker J.N., Vinay V.* Branching rules for satisfiability // Journal of Automated Reasoning. – 1995. – N 3. – P. 359-383.

175. *Horrocks I., Patel-Schneider P.F.* Optimizing propositional modal satisfiability for description logic subsumption // LNAI. – 1998. – Vol. 1476. – P. 234-246.

176. *Huffman D.A.* Canonical forms for information-lossless finite stste logical machines // IRE Trans. Circuit Theory. Special Supplement. – 1959. – Vol. CT-6. – P. 41-59.

177. *Jeroslow R.G., Wang J.* Solving propositional satisfiability problems // Annals of Mathematics and Artificial Intelligence. – 1990. – **1**. – N 1-4. – P. 167-187.

178. *Kovasznai G., Frohlich A., Biere A.* On the complexity of fixed-size bit-vectors logics with binary encoded bit-width // Proc. of SMT'12. – 2012. – P. 44-55.

179. *Lahiri S.K., Musuvathi M.* An efficient decision prosedure for UTVPI constraints // LNCS. – 2005. – Vol. 3717. – P. 168-183.

180. *Lensta H.W.* Factorizing integers with elliptic curves // Ann. of Math. – 1987. – Vol. 126. – P. 649-673.

181. *Lin F., Zhao Y.* ASSAT: computing answer sets of logic program by SAT solvers // Artificial Intelligence. – 2004. – N 1-2. – P. 115-137.

182. *Mahfoudh M., Miebert P., Asarin E, at all.* A satisfiability checker for difference logic // Proc. of SAT'02. – 2002. – P. 222-230.

183. *Manna Z., Zarba C.* Combining decision procerures // LNCS. – 2003. – Vol. 2787. – P. 453-468.

184. *Marques-Silva J., Sakallah K.* GRASP: a search algorithm for satisfiability // Proc. of ICCAD'96. – 1996. – P. 220-227.

185. *Marques-Silva J., Sakallah K.* GRASP: a search algorithm for propositional satisfiability // IEEE Transactions on Computers. – 1999. – N 5. – P. 506-521.

186. *Moskewich M.,W., Madigan C.F., Zhang Y.Z. at all.* Chaff: engineering an efficient SAT solver // Proc. of DAC'01. – 2001. – P. 530-535.

187. *Nelson G., Oppen D.C.* Simplification by cooperating decision procedures // ACM Transactions on Programming Languages and Systems. – 1979. – N 2. – P. 245-257.

188. *Nelson G., Oppen D.C.* Fast decision procedures based on congruence closure // Journal of the ACM. – 1980. – N 2. – P. 356-364.

189. *Nieuwenhuis R., Oliveras A., Tinelli C.* Congruence closure with integer offsets // LNAI. – 2003. – Vol.2850. – P. 381-422.

190. *Nieuwenhuis R., Oliveras A.* Proof-producing congruence closure // LNCS. – 2005. – Vol. 3467. – P. 453-468.

191. *Nieuwenhuis R., Oliveras A.* DPLL($\mathcal{T}$) with exhaustive theory propagation and its application to difference logic // LNCS. – 2005. – Vol. 3576. – P. 321-334.

192. *Nieuwenhuis R., Oliveras A., Tinelli C.* Abstract DPLL and abstract DPLL modulo theories // LNCS. – 2005. – Vol. 3452. – P. 36-50.

193. *Nieuwenhuis R., Oliveras A., Tinelli C.* Solving SAT and SAT Modulo theories: from an abstract Davis-Putnam-Logemann-Loveland procedure to DPLL($\mathcal{T}$) // Journal of the ACM. – 2006. – N 6. – P. 937-977.

194. *Nieuwenhuis R., Oliveras A.* On SAT Modulo theories and optimisation problems // LNCS. – 2006. – Vol. 4121. – P. 156-169.

195. *Oppen D.C.* Complexity, convexity and combinations of theories // Theoretical Computer Science. – 1980. – N 12. – P. 291-302.

196. *Oppen D.C.* Reasoning about recursively defined data structures // Journal of the ACM. – 1980. – N 3. – P. 403-411.

197. *Pugh W.* The omega test: a fast and practical integer programming algorithm for dependence analysis //Proc. of ACM/IEEE Conference on Supercomputing. – 1991. – P. 4-13.

198. *Ranise S., Tinelli C.* Satisfiability modulo theories // IEEE Intelligent Systems Magazine. – 2006. – N 6. – P. 71-81.

199. *Ranise S., Tinelli C.* Satisfiability modulo theories library (SMT-LIB). – 2006. – http://www.SMT-LIB.org.

200. *Ranise S., Tinelli C.* The SMT-LIB Standard: Version 1.2. Technical Report, Department of Computer Science, The Univ. of Iowa, 2006. – http://www.SMT-LIB.org.

201. *Sebasttiani R.* Integrating SAT solvers with Math reasoners: Foundations and basic algorithms. // Technical Report 0111-22, ITC-IRST, Trento, Italy, 2001. – http://sra.itc.it/tr/Seb01.pdf.

202. *Sebasttiani R.* Lazy satisfiability modulo theories // Journal on Satisfiability, Boolean Modeling and Computation. – 2007. – N 3. – P. 141-224.

203. *Seshia S., Lahiri S., Bryant R.* A hybrid SAT-based decision procedure for separation logic with uninterpreted functions // Proc. of DAC'03. – 2003. – P.425-430.

204. *Shostak R.* An algorithm for reasoning about equality // Com. ACM. – 1978. – N 3. – P. 583-585.

205. *Shostak R.* A practical decision procedure for arithmetic with function symbols // Journal of the ACM. – 1979. – N 2. – P. 351-360.

206. *Shostak R.* Deciding combinations of theories // Journal of the ACM. – 1984. – N 1. – P. 1-12.

207. *Silverman J.* Advanced topics in the arithmetic of elliptic curves. – NY: Springer-Verlag, 1994. – 430 p.

208. *Skobelev V.V.* On automata over elliptic curves // Proc. of the VIth International Conference on Computer Science and Information Technologies (CSIT 2011). – Львів: Вежа і Ко. – 2011. – С. 29.

209. *Skobelev V.V.* On the 2^d order curves over finite ring // Материалы X Международной конференции «Интеллектуальные системы и компьютерные науки». – М.: МГУ. – 2011. – С. 327-329.

210. *Skobelev V.V.* On systems of polynomial equations over finite rings // Наукові записки НаУ-КМА. Серія: Комп'ютерні науки. – 2012. – Т. 138. – С. 15-19.

211. *Skobelev V.V.* On simulation of automata over finite ring // Book of abstracts of the International Scientific Conference «Computer Algebra and Information Technology». – Odessa: ONU. – 2012. – P. 93-95.

212. *Skobelev V.V.* Analysis of automata determined over parametric varieties over an associative ring. // Вісник Київського університету. Сер.: фіз.-мат. науки. – 2012. – Вип. 3. – С. 239-244.

213. *Skobelev V.V.* Automata over parametric varieties in a finite ring. – Proceedings of the 2nd International Conference of Students and Young Scientists «Theoretical and Applied Aspects of Cybernetics (TAAC 2012)». – Kyiv: Bukrek. – 2012. – P.79-81.

214. *Skobelev V.V.* Satisfiability modulo linear arithmetic over a finite ring // Вісник Київського університету. Сер.: фіз.-мат. науки. – 2013. – Вип. 2. – С. 95-106.

215. *Stephan P., Brayton R., Sangiovanni-Vincentelli A.* Combinational test generation using satisfiability // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. – 1996. – N 12. – P. 1167-1176.

216. *Strichman O.* Tuning SAT checkers for bounded model checking // LNCS. – 2000. – Vol. 1885. – P. 480-494.

217. *Strichman O., Seshia S.A., Bryant R.E.* Deciding separation formulae with SAT // LNCS. – 2004. – Vol. 2404. – P. 209-222.

218. *Stump A., Dill D.L., Barret C.W. at all.* A decision procedure for an extensional theory of arrays // Proc. of LICS'01. – 2001. – P. 29-37.

219. *Stump A., Barret C.W., Dill D.L.* CVC: a cooperative validity checker // LNCS. – 2002. – Vol. 2404. – P. 500-504.

220. *Tinelli C.* A DPLL-based calculus for ground satisfiability modulo theories // LNAI. – 2002. – Vol. 2424. – P. 308-319.

221. *Velev M.N., Bryant R.E.* Exploating positive equality and partial non-consistency in the formal verification of pipelined microprocessors // Proc. of DAC'99. – 1999. – P. 397-401.

222. *Velev M.N., Bryant R.E.* Effective use of Boolean satisfiabiliry procedures in the formal verification of superscalar and VLIW microptocessors // Journal of Symbolic Computation. – 2003. – N 2. – P. 73-106.

223. *Wang C., Ivancic F., Canai M.K., at all.* Deciding separation logic formulae by SAT and incremental negative cycle elimination // LNCS. – 2005. – Vol. 3835. – P. 322-336.

224. *Wang C., Gupta A., Ganai M.* Predicate learning and selective theory deduction for a difference logic solver // Proc. of DAC'06. – 2006. – P. 235-240.

225. *Zhang H.* SATO: an efficient propositional prover // Proc. of DAC'97. – 1997. – P. 272-275.

226. *Zhang L., Madigan C.F., Moskewicz M.W., al all.* Efficient conflict-driven learning in boolean satisfiability // Proc. of ICCAD'01. – 2001. – P. 279-285.

227. *Zhang L., Malic S.* The quest for efficient boolean satisfiability solvers // LNCS. – 2002. – Vol. 2404. – P. 17-36.

228. *Zierler N.* Products of linear recurring sequences // Journal of Algebra. – 1973. – Vol. 27. – № 1. – P. 147-157.