МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2021 № 54

Зарегистрирован в Федеральной службе по надзору
в сфере связи и массовых коммуникаций

Свидетельство о регистрации ПИ № ФС 77-33762 от 16 октября 2008 г.

Подписной индекс в объединённом каталоге «Пресса России» 38696

УЧРЕДИТЕЛЬ
Томский государственный университет

Адрес редакции и издателя: 634050, г. Томск, пр. Ленина, 36
E-mail: pank@mail.tsu.ru

В журнале публикуются результаты фундаментальных и прикладных научных исследований отечественных и зарубежных ученых, включая студентов и аспирантов, в области дискретной математики и её приложений в криптографии, компьютерной безопасности, кибернетике, информатике, программировании, теории надёжности, интеллектуальных системах.

Периодичность выхода журнала: 4 номера в год.

Редактор *Н. И. Шидловская*
Верстка *И. А. Панкратовой*

Подписано к печати 01.12.2021. Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 14,55. Тираж 300 экз.
Заказ № 4865. Цена свободная. Дата выхода в свет 10.12.2021.

Отпечатано на оборудовании
Издательства Томского государственного университета
634050, г. Томск, пр. Ленина, 36
Тел.: 8(3822)53-15-28, 52-98-49

СОДЕРЖАНИЕ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

CONTENTS

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 512.572 DOI 10.17223/20710410/54/1

ИССЛЕДОВАНИЯ ПОЛУГРУПП С ПЛАНАРНЫМИ ГРАФАМИ КЭЛИ: РЕЗУЛЬТАТЫ И ПРОБЛЕМЫ

Д. В. Соломатин

Омский государственный педагогический университет, г. Омск, Россия

E-mail: solomatin_dv@omgpu.ru

Классические графы Кэли для групп давно и основательно зарекомендовали себя в решении прикладных задач, найдя применение в различных научных сферах, от криптографии до кампанологии. В последнее время всё большее внимание привлекает изучение прикладных аспектов графов Кэли полугрупп. В настоящей работе дан обзор результатов, полученных при исследованиях полугрупп с планарными графами Кэли, и результатов по изучению ранга планарности многообразий полугрупп. Сформулирован ряд нерешённых проблем, решение которых найдёт применение в комбинаторной теории полугрупп. В заключении даётся понятие спектра рангов планарности многообразий полугрупп, с помощью которого появляется возможность хеширования полугрупповых многообразий.

Ключевые слова: *полугруппа, граф Кэли полугруппы, планарный граф, многообразие полугрупп, ранг планарности.*

RESEARCHES OF SEMIGROUPS WITH PLANAR CAYLEY GRAPHS: RESULTS AND PROBLEMS

D. V. Solomatin

Omsk State Pedagogical University, Omsk, Russia

The classical Cayley graphs for groups have long and thoroughly proven themselves in solving applied problems, finding application in various scientific fields, from cryptography to campanology. Recently, more and more attention has been paid to the researching the applied aspects of Cayley graphs of semigroups. In this paper, we survey a result obtained in investigations on semigroups with planar Cayley graphs and results on the study of planarity rank of a semigroup varieties. A number of unsolved problems are formulated, the solution of which finds application in the combinatorial theory of semigroups. Just as Cayley graphs of semigroups are used for constructing hash functions, the concluding part of the paper introduces the concept of the spectrum of planarity ranks for varieties of semigroups, with the help of which it becomes possible to hash semigroup varieties.

Keywords: *semigroup, Cayley graph of semigroup, planar graph, semigroup variety, planarity rank.*

Введение

Данная работа представляет собой критический анализ результатов в обозначенном заглавием направлении, их обобщение и решение новых задач планаризации для многообразий полугрупп в ходе зарождения спектральной теории рангов планарности полугрупповых многообразий. Постепенно подводя читателя к понятию коспектральных многообразий полугрупп, находящих применение в широком круге задач построения хэш-функций, в заключительном разделе приведён краткий список открытых проблем этой теории. Последнее обобщает существующую ныне геометрическую теорию групп [1] и вносит вклад в развитие теории полугрупп с планарными графами Кэли, определяемый критическим анализом результатов, их систематизацией и помещением в более широкий контекст, вычленением потенциальных точек для дальнейшего роста активно развивающейся геометрической теории полугрупп [2].

Понятие графа Кэли предложено Артуром Кэли в 1878 г. [3] как наглядная интерпретация абстрактных групп. С тех пор получено много интересных результатов, опирающихся на саму концепцию графов Кэли групп как таковую. Вдохновлённые обилием результатов о графах Кэли для групп, многие авторы изучали графы Кэли для полугрупп. Что касается исследований планарных графов, то их традиционно относят к вопросам топологии, которые представляют определённый интерес и с инженерной точки зрения. Рассматриваемый нами алгебраический подход значительно шире.

При этом классические графы Кэли для групп давно [4] и основательно [5] зарекомендовали себя в решении прикладных задач, они применяются в различных научных сферах, от криптографии [6] до кампанологии [7]. В последнее время активно изучаются прикладные аспекты графов Кэли полугрупп. В настоящей работе дан обзор результатов, полученных при исследованиях конечных полугрупп с планарными графами Кэли, и результатов по изучению ранга планарности многообразий полугрупп. Сформулирован ряд открытых проблем, решение которых найдёт применение в комбинаторной теории полугрупп. Подобно тому, как в [8] графам Кэли полугрупп находят приложение для построения хэш-функций, в заключении даётся понятие спектра рангов планарности многообразий полугрупп, с помощью которого появляется возможность хеширования полугрупповых многообразий.

Описание допускающих плоские графы Кэли конечных групп известно давно [9]. Но исследования групп, допускающих плоские графы Кэли, продолжаются [10 – 13], в том числе и зарубежными авторами [14 – 23], и эти работы имеют дело уже с бесконечными конечно порождёнными группами.

Первое упоминание используемого определения конструкции графов Кэли для полугрупп относительно множества образующих её элементов, как ориентированного мультиграфа с помеченными (раскрашенными) дугами, встречается в [24]. При этом исследование полугрупп методами теории графов проводилось и ранее, например в [25], а в дальнейшем широкое развитие, видоизменение и обобщение тех идей с приложением к теории графов было отражено в систематических работах, выполняемых под руководством профессора Зелинка [26, 27] и опубликованных Институтом математики Чешской академии наук. Более точно, в [25] рассматривается граф подполугрупп полугруппы, вершинами которого являются подполугруппы наперёд заданной полугруппы, а две различные вершины графа соединяются ребром тогда и только тогда, когда пересечение соответствующих подполугрупп не пусто. Работа [26] относится именно к таким графам подполугрупп, несмотря на название, закрепившееся ныне за графами Кэли полугрупп.

Известно, что можно фиксировать свойства графов, получая тем самым описание связанных с ними алгебраических структур, и наоборот, фиксируя алгебраические свойства, получать уникальные серии графов, наглядно отражающих внутреннюю природу некоторой алгебраической структуры. Это продемонстрировано, в частности, в приводимых далее результатах.

Вопрос описания конечных полугрупп с планарными графами Кэли оказался весьма трудным и по сей день остаётся открытым. Наши исследования позволяют говорить о том, что вопрос является трансцендентным. При этом поднимаемые в работах [28, 29] вопросы различной вложимости графов Кэли для полугрупп лежат на стыке теории графов, алгебры и топологии, а ведь именно на стыке наук рождаются новые идеи.

Основной целью данной работы является обзор результатов многолетних научных исследований, проводимых в следующих двух направлениях. Первое направление сопряжено с исследованиями конечных полугрупп, допускающих планарные графы Кэли. Второе направление исследования инспирировано тесно связанными между собой понятиями ранга планарности и спектра рангов планарности многообразий полугрупп. Предложенное Л. М. Мартыновым, это направление базируется на оценке наибольшего числа образующих элементов свободных полугрупп в многообразиях полугрупп, относительно которых граф Кэли этих полугрупп является планарным. Так как свободные полугруппы в многообразиях играют важную роль (хотя бы потому, что любая полугруппа многообразия является гомоморфным образом подходящей свободной в нём полугруппы), изучение этого понятия является весьма актуальной задачей. При изучении свойства планарности графов Кэли для многообразий полугрупп принципиальный характер имеет проблема описания рангов планарности многообразий полугрупп, сформулированная Л. М. Мартыновым в 2015 г. [30].

В завершающем разделе обзора приведён новый результат, полученный в процессе написания. Прежде чем дать определение ключевого для понимания этого результата понятия (ранга планарности многообразия полугрупп), перечислим некоторые определения понятий, связанных со свойством планарности графов Кэли полугрупп.

В качестве небольшого исторического экскурса всё же напомним, что изучение планарных графов Кэли уходит корнями к известной работе 1896 г. [9]. В 1955 г. [31] показана алгоритмическая нераспознаваемость почти всех нетривиальных свойств группы по её заданию конечным числом определяющих соотношений, позднее этот результат независимо был получен в [32], и с того времени по теореме Адяна — Рабина о неразрешимости марковских свойств групп свойство планарности графов Кэли «официально» получило статус трудного для изучения. Дело в том, что свойство группы, заключающееся в наличии планарного графа Кэли, — марковское, поэтому не существует алгоритма, который по заданному представлению определит планарность графа Кэли соответствующей группы, в лучшем случае можно рассчитывать лишь на «каталоги» планарных групп. Далее, в 1980 г. [33] предпринимались попытки перечисления планарных групп как групп, сохраняющих ориентацию автоморфизмов плоского комплекса. Группы с планарными графами Кэли таковыми являются, потому что группа действует автоморфизмами на своём графе Кэли.

На этом исследования не были остановлены, так, например, в 1997 г. изучались регулярные замощения плоскости как графы Кэли [10]. Из сравнительно недавних работ можно упомянуть исследования операций над группами, сохраняющих свойства связности и планарности их графов [14]. Как видим, изучение графов Кэли востребовано для групп. Более того, с 1981 г. это понятие систематически исследовалось в виде аналогичной конструкции на полугруппах [27]. Важность этого понятия для комбина-

торной теории полугрупп продемонстрирована в работах многих авторов. Например, в [34] изучаются E-унитарные инверсные моноиды и графы Кэли, а в [35, 36] — свойства полноты, двудольности, транзитивности графов Кэли групп и полугрупп. В [37] описываются полугруппы, удовлетворяющие различным комбинаторным свойствам, определённым в терминах графов Кэли, а в [38] — все периодические (и, следовательно, все конечные) полугруппы G, для которых существует непустое подмножество S, такое, что граф Кэли группы G относительно S является неориентированным графом Кэли. Кроме того, из [39] известно описание конечных инверсных полугрупп, коммутативных инверсных полугрупп с двудольными графами Кэли и инверсных эпигрупп с графами Кэли, являющимися дизъюнктными объединениями полных графов. Алгебраисты интересовались также и графами Кэли полурешёток полугрупп на предмет характеризации цветовых автоморфизмов вершинно-транзитивных графов Кэли полурешёток полугрупп [40], вершинной транзитивностью графов Кэли полугрупп Брандта [41], вершинной транзитивностью графов Кэли левых групп [42] и конечных связок (полугрупп идемпотентов) [43]. Что касается важного свойства планарности, то, как видим, ранее оно исследовалось в основном для групп, а ныне проводятся исследования полугрупп с ациклическими [44], внешнепланарными [45] графами Кэли. Изучаются и более общие вопросы, о полугруппах с планарными графами Кэли, результаты в этой области принадлежат автору, они приведены далее.

Отметим, что после пионерских работ свойство планарности для графов Кэли полугрупп стало использоваться и в работах других авторов, так как развитие тематики, помимо фундаментального значения, находит отражение в прикладных исследованиях [2, 44, 46 – 55].

В частности, известна классификация плоских вполне регулярных полугрупп, понятие которых близко к понятию групп, так как вполне регулярные полугруппы являются объединением групп. Расскажем обо всём этом по порядку в соответствующих разделах.

1. Основные определения и обозначения

Напомним определения основных понятий и условимся относительно некоторых обозначений. Определения других понятий теории полугрупп можно найти в [56], а теории графов — в [57].

Определение 1. Пусть S — полугруппа, X — множество порождающих её элементов. Через $Cay(S, X)$ обозначим [правый] граф Кэли полугруппы S относительно X. Граф $Cay(S, X)$ состоит из множества вершин S и множества помеченных дуг — всевозможных троек (a, x, b), где $a, b \in S$, $x \in X$ и $ax = b$.

Заметим, что в данном случае граф Кэли является ориентированным мультиграфом с помеченными дугами. Вершины графа обычно изображаются точками на плоскости, а дуга (a, x, b) — линией, направленной от a к b и помеченной элементом x.

Существует несколько небольших разновидностей данного определения, например в некоторых контекстах вместо правого умножения используется левое. Тем самым можно разделять правые и левые графы Кэли. Очевидно, что данные понятия совпадают для случая коммутативных полугрупп, в противном случае их можно исследовать с точностью до антиизоморфизма, а принцип двойственности позволяет не воспроизводить соответствующие утверждения для одного из взаимно двойственных случаев.

Определение 2. Основой ориентированного мультиграфа с помеченными дугами называем (обыкновенный) граф, полученный из данного графа удалением петель,

меток и заменой всех дуг, соединяющих две вершины, одним ребром, соединяющим эти вершины.

Естественным будет называть полугруппу *допускающей планарный граф Кэли*, если относительно некоторого минимального множества образующих её элементов основа графа Кэли данной полугруппы является планарным графом.

Определение 3. Ориентированный помеченный мультиграф называем планарным [внешнепланарным], если его основа является планарным [внешнепланарным] графом. Будем говорить, что полугруппа S допускает планарный [внешнепланарный] граф Кэли, если для некоторого множества X её образующих основа $SCay(S, X)$ графа $Cay(S, X)$ является планарным [внешнепланарным] графом.

Напомним, что граф называется внешнепланарным, если внешняя грань его плоской укладки содержит все его вершины.

Систему полугрупповых тождеств $\{xw \approx w, wx \approx w\}$ при любом слове w, не содержащем переменную x, будем записывать в эквивалентном виде тождеством $w \approx 0$. Полугрупповые тождества вида $w \approx 0$ при $w \neq 0$, а также многообразия полугрупп с нулём, задаваемые системами тождеств такого вида, называются 0-*приведёнными*. Такие многообразия обладают неприводимым базисом тождеств вида $w \approx 0$, и их множество имеет мощность континуума [58].

Определение 4. Многообразие, каждая полугруппа которого допускает планарный граф Кэли, называется планарным.

Приведём определение конечных свободных коммутативных полугрупп [моноидов, полугрупп с нулём], так как будем ссылаться на ранее выполненные исследования вопросов планарности их графов Кэли. Конечную полугруппу [моноид, полугруппу с нулём], являющуюся коммутативно-свободным произведением циклических полугрупп [моноидов, полугрупп с нулём], условимся называть *конечной свободной коммутативной полугруппой* [*моноидом, полугруппой с нулём*]. В частности, в классе коммутативных моноидов такой моноид имеет следующее копредставление:

$$S = \left\langle a_1, a_2, \ldots, a_n \mid a_j^{m_j} = 1,\ a_i^{r_i+m_i} = a_i^{r_i},\ i \in I,\ j \in J \right\rangle,$$
$$I \cup J = \{1, \ldots, n\},\ I \cap J = \varnothing,\ J \neq \varnothing.$$

Под *множеством свободных образующих* коммутативно-свободного произведения циклических полугрупп [моноидов, полугрупп с нулём] мы понимаем множество полугрупповых образующих соответствующих циклических сомножителей.

Кроме того, в обозначениях моноидов [полугрупп с нулём] условимся различать операции присоединения единицы [нуля] и внешнего присоединения единицы [нуля] к полугруппе S. В первом случае единицу [нуль] будем добавлять только в случае, когда она [он] отсутствует в полугруппе S, и соответствующую полугруппу обозначать, как обычно, через S^1 [S^0]. Во втором случае единицу [нуль] будем присоединять всегда и полученную полугруппу обозначать через S^{+1} [S^{+0}].

Важнейший класс полугрупп формируют вполне регулярные полугруппы, по определению являющиеся объединением групп. Типичные ситуации возникновения групп в теории полугрупп перечислены в [56], где можно почерпнуть дополнительные определения, а также краткий перечень современных понятий и актуальных фактов теории полугрупп. Среди прочего из упомянутой фундаментальной монографии напомним, что полугруппа S называется *регулярной*, если для любого элемента a из S найдётся элемент $x \in S$, такой, что $axa = a$. Другими словами, полугруппа называется регулярной, если в ней для любого элемента a разрешимо уравнение $axa = a$. Два элемента a

и b полугруппы S называются *инверсными*, если $aba = a$ и $bab = b$. В результате тесно связанными с понятием регулярности оказываются инверсные полугруппы. *Инверсной полугруппой* называется полугруппа, в которой каждый элемент имеет единственный инверсный к нему элемент.

Как мы упомянули выше, полугруппа, которая является объединением групп, называется *вполне регулярной*. Напомним, что *полурешёткой* называется коммутативная полугруппа идемпотентов, а *прямоугольная связка* — это полугруппа идемпотентов, элементы которой удовлетворяют тождеству $xyx \approx x$. Известно, что всякая вполне регулярная полугруппа является полурешёткой прямоугольных связок групп. Таким образом, если элементы полугруппы, принадлежащие максимальным подгруппам, называть *групповыми*, то соответственно полугруппы, все элементы которых групповые, являются вполне регулярными.

Инверсные вполне регулярные полугруппы получили название *клиффордовых*. Важно отметить, что в клиффордовых полугруппах идемпотенты перестановочны. Как видим, понятие клиффордовых полугрупп близко к понятию группы. Устоявшийся в научной литературе термин для этих полугрупп выбран в честь американского математика А. Клиффорда, одного из пионеров теории полугрупп, выявившего среди прочего основополагающие свойства обсуждаемых полугрупп [59].

Для понимания дальнейшего изложения уместно вспомнить, что клиффордова полугруппа является полурешёткой групп, более того, для неё можно указать детальное строение, описываемое в [59, теорема 4.11].

В 2012 г. [60] начато изучение предложенного Л. М. Мартыновым понятия ранга планарности многообразия полугрупп. Третий раздел настоящей работы содержит детальное изложение актуальных результатов и текущего положения дел в данной области.

Условимся буквой $\boldsymbol{O}$ обозначать многообразие одноэлементных полугрупп и называть его *тривиальным*.

Определение 5. Пусть $\boldsymbol{V}$ — нетривиальное многообразие полугрупп. Если существует такое натуральное число r, что все $\boldsymbol{V}$-свободные полугруппы ранга $\leqslant r$ допускают планарные графы Кэли (относительно множеств их свободных образующих), а $\boldsymbol{V}$-свободная полугруппа ранга $r+1$ уже не допускает планарный граф Кэли, то рангом планарности многообразия $\boldsymbol{V}$ называется это число $r = r_\pi(\boldsymbol{V})$. Если для многообразия $\boldsymbol{V}$ такого натурального числа не существует, то говорят, что многообразие $\boldsymbol{V}$ имеет бесконечный ранг планарности, и пишут $r_\pi(\boldsymbol{V}) = \infty$.

Заметим, что ранг планарности для любого нетривиального многообразия $\boldsymbol{V}$ ограничен снизу, а именно $r_\pi(\boldsymbol{V}) \geqslant 1$, так как очевидно, что любая циклическая (моногенная) полугруппа допускает планарный граф Кэли. С другой стороны, вырожденный случай формирует тривиальное многообразие $\boldsymbol{O}$, для которого в целях повышения информативности понятия спектра рангов планарности удобно считать в дальнейшем, что ранг планарности $r_\pi(\boldsymbol{O}) = 0$.

Определение 6. Спектром рангов планарности многообразия $\boldsymbol{V}$ называется множество $\mathrm{Spec}_{r\pi}(\boldsymbol{V})$ всех возможных значений рангов планарности подмногообразий $\boldsymbol{X}$ многообразия $\boldsymbol{V}$.

Если через $L(\boldsymbol{V})$ обозначить решётку подмногообразий многообразия $\boldsymbol{V}$, то $\mathrm{Spec}_{r\pi}(\boldsymbol{V}) = \{r_\pi(\boldsymbol{X}) : \boldsymbol{X} \in L(\boldsymbol{V})\}$. Кроме того, зафиксируем обозначение $\mathbb{N}^\infty = \{0, 1, 2, 3, \ldots, \infty\}$.

Определение 7. Спектр рангов планарности полугруппового многообразия $\boldsymbol{V}$ называется полным, если он содержит все натуральные числа и символ ∞, то есть $\mathrm{Spec}_{r\pi}(\boldsymbol{V}) = \mathbb{N}^{\infty}$.

Коль скоро всякое многообразие полугрупп содержит тривиальное многообразие в качестве подмногообразия, то спектр любого многообразия содержит число 0, а $\mathrm{Spec}_{r\pi}(\boldsymbol{O}) = \{0\}$.

При получении сформулированных далее результатов для обоснования планарности обыкновенного графа использованы различные критерии. Наиболее часто применялся известный *критерий Понтрягина — Куратовского*: обыкновенный граф планарен тогда и только тогда, когда он не содержит подграфов, гомеоморфных полному двудольному графу $K_{3,3}$ или полному пятиэлементному графу K_5.

Кроме того, применялся *критерий Вагнера*: обыкновенный граф планарен тогда и только тогда, когда он не содержит подграфов, стягиваемых к графам K_5 или $K_{3,3}$.

Для полугруппы, удовлетворяющей условиям соответствующего утверждения, строится плоская укладка её графа Кэли. Если полугруппа не удовлетворяет этим условиям, то основа её графа Кэли содержит подграф, либо гомеоморфный K_5 или $K_{3,3}$, либо стягиваемый к ним. Графы K_5 и $K_{3,3}$ детально исследованы в [61].

Существуют эффективные методы распознавания планарности графа. Например, в [62] предложен работающий за линейное время $O(n)$ алгоритм, использующий специальные структуры данных (PQ-деревья) для представления графа порядка n; на его базе в [63] построен параллельный алгоритм с $O(\log^2 n)$ операциями; последний, в свою очередь, оптимизирован в [64] для параллельных вычислений на $p \leqslant n$ процессорах с CREW PRAM (это одна из разновидностей оперативной памяти для мультипроцессорных систем, которая допускает одновременное чтение, но запрещает одновременную запись), в результате получена более точная оценка эффективности $O(n \log^2 n/p)$.

В [65] все известные способы определения планарности графа условно разделены на следующие группы:

1. Критерии планарности графа:
   1.1) критерий Маклейна;
   1.2) критерий Уитни;
   1.3) критерий Понтрягина — Куратовского (вариация для схем — условия Линского) или Вагнера;
   1.4) критерий Харари — Татта.
2. Алгоритмические методы определения планарности графа:
   2.1) циклические;
   2.2) матричные;
   2.3) смешанные.

Заметим, что к критерию 1.3 можно адаптировать представленный в [66] вероятностный алгоритм поиска подграфа, гомеоморфного заданному.

С применением функционала Маклейна и структурных чисел можно предложить более алгоритмизируемый критерий, хотя и менее эффективный, чем использующий PQ-деревья, но легче реализуемый. Для поиска базиса пространства циклов в графе можно использовать структурные числа. Вообще говоря, задача поиска циклов для полугрупп заслуживает отдельного внимания [67].

В целом задача распознавания планарности графа Кэли полугруппы разбивается на следующие последовательные этапы:

1) подготовительный этап;

2) эвристический анализ;
3) предварительный выбор;
4) окончательный выбор.

На подготовительном этапе фиксируется класс исследуемых полугрупп и метод проверки планарности основы их графа Кэли, после чего эвристический анализ позволяет предопределить эффективность выбранного метода. Выбор из всех полугрупп лишь допускающих планарные графы завершает решение задачи. Очевидно, что число всех неориентированных графов порядка n без петель и кратных рёбер равно $2^{(n^2-n)/2}$, известны также оценки числа заведомо планарных и заведомо непланарных из них [68]. Естественно, далеко не каждый из них планерен и может служить основой некоторого графа Кэли полугруппы. Тем не менее решение задачи перебором сопряжено со значительными вычислительными трудностями. Например, число всех неориентированных графов порядка 6 равно 32 768, заведомо непланарных из них — 121, а заведомо планарных — 22 818, поэтому дополнительная проверка требуется ещё для 9 829 графов.

В связи с этим имеет смысл индуктивно строить цепь полугрупп, в которой граф Кэли каждой предшествующей содержался бы в следующем планарном графе. Получится, аналогично пифагоровым полям, своеобразная цепочка расширений. При её построении следует учитывать, что любую петлю можно провести без пересечений. Более того, для кратных рёбер справедливо утверждение: если одно из кратных рёбер расположено без пересечений, то и другие не пересекаются.

Таким образом, если строить цепочки планарных графов Кэли, то можно ограничиться описанием соотношений, приводящих к появлению кратных рёбер и петель в конечном случае, либо фрактальных графов в бесконечном случае. Добавление иных рёбер, в пределе, инспирирует наибольшие по включению планарные графы, так называемые триангуляции, исследованные в [61].

2. О группах с планарными графами Кэли

Прежде всего укажем на фундаментальную взаимосвязь между понятиями графа Кэли полугруппы и графа Кэли группы, благодаря которой в дальнейшем для изучения спектров рангов планарности многообразий полугрупп можно будет использовать групповые результаты, так как группы являются частным случаем полугрупп. Свойство планарности графов Кэли для групп оказалось существенным ещё и потому, что, как показано в [69], если бесконечный граф Кэли не является планарным, то он не может быть вложен ни в одну из поверхностей конечного рода. Говоря о бесконечных конечно порождённых группах с планарными графами Кэли, отметим важные публикации последних лет [16 – 19, 22]. Работы по графам Кэли групп релевантны и в теории графов Кэли полугрупп, поскольку конечно порождённая группа конечно порождена и как полугруппа. Среди работ по графам Кэли конечно порождённых групп есть весьма глубокие, вскрывающие интересные взаимосвязи между алгеброй, комбинаторикой и маломерной топологией. Поэтому дадим содержательный обзор таких работ. На языке современной топологии связный граф является планарным, если он служит разрезающим графом для некоторой склейки сферы, а началось исследование групп с графами Кэли, обладающими свойством планарности, с известной теоремы Машке (теорема 1).

Перед тем как привести данную теорему, напомним необходимые обозначения из теории групп: $\mathbb{Z}_n = \{0, \ldots, n-1\}$ — аддитивная группа кольца вычетов по модулю n. Заметим, что $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ при взаимно простых m и n. В частности, $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong D_2$. Здесь $D_n = \langle x, y \mid x^n = y^2 = (xy)^2 = 1 \rangle$ — диэдральная группа. Элементами D_n являют-

ся автоморфизмы графа, состоящего только из цикла с n вершинами, таким образом, $|D_n| = 2n$. Очевидно, что $\mathbb{Z}_2 \times D_n \cong D_{2n}$ при нечётном n. Наконец, A_n и S_n — знакопеременная группа и симметрическая группа подстановок степени n, содержащая только чётные и соответственно все возможные подстановки данной степени.

Теорема 1 [9, §5]. Конечная группа G планарна тогда и только тогда, когда $G = G_1 \times G_2$, где $G_1 = \mathbb{Z}_1$ или $\mathbb{Z}_2$, а $G_2 = \mathbb{Z}_n$, D_n, S_4, A_4 или A_5.

2.1. О плоских графах Кэли в терминах копредставлений групп

Изучением возможностей, при которых одна и та же группа обладает неизоморфными плоскими графами Кэли, и изучением неизоморфных групп, допускающих изоморфные графы Кэли, занималась Ж. Т. Беленкова [12]. Кроме того, всестороннее исследование графов Кэли групп провели В. А. Романьков и Ж. Т. Беленкова в [11, 10]. Ими описаны всевозможные варианты выбора групп и их порождающих множеств, приводящие к регулярным замощениям как графам Кэли. Проведён полный и детальный анализ групп, допускающих в качестве графа Кэли регулярное замощение плоскости. В результате подробных рассмотрений получены 6 групп с графом Кэли, составленным из треугольников, 16 групп с графом из квадратов и 6 групп с графом из шестиугольников. С точностью до изоморфизма, полученные графы исчерпывают 14 кристаллографических групп (из 17 возможных). Кроме того, приведены некоторые общие свойства плоских графов Кэли конечных групп. В частности, охарактеризованы нециклические абелевы группы, вложимые в плоскость. Приведены примеры неабелевых групп, невложимых в плоскость. В [12] описаны все плоские графы Кэли группы S_4. Оказалось, что группа S_4 обладает четырьмя плоскими графами Кэли, два из которых являются графами Кэли двух групп, не изоморфных группе S_4. Кроме того, выписаны все минимальные по включению порождающие множества группы S_4. Их 10 штук: 3 из них состоят из двух элементов, а 7 — из трёх элементов.

В [17] доказано, что граф Кэли вкладывается в евклидову плоскость без точек аккумулирования вершин (другими словами, имеет локально конечное вложение) тогда и только тогда, когда он является 1-остовом комплекса Кэли, который может быть вложен в плоскость после удаления лишних симплексов. Там же приводится характеристика планарных графов Кэли в терминах копредставлений групп и делается вывод о том, что их можно эффективно перечислить.

Теорема 2 [17, теорема 1.1]. Планарный граф Кэли группы Γ не имеет точек аккумулирования тогда и только тогда, когда он является 1-остовом плоского комплекса Кэли группы Γ.

С другой стороны, локальная конечность не является теоретико-групповым инвариантом планарности графа Кэли в общем случае, однако становится таковым, если рассматривать лишь 3-связные графы Кэли.

Теорема 3 [17, теорема 4.1]. Если группа Γ имеет 3-связный планарный граф Кэли, являющийся локально конечным, а группа Δ имеет 3-связный планарный граф Кэли, таковым не являющийся, то Γ не изоморфна Δ.

Например, планарный граф Кэли группы $\langle a, b, c, d \mid a^4 = 1, b^4 = 1, c = ab, d = a^2b^2a^2\rangle$ является 3-связным, но не локально конечным. Тот факт, что никакое вложение этого графа не является локально конечным, вытекает из следующей теоремы.

Теорема 4 [17, теорема 4.3]. Пусть G — трёхсвязный граф, вложенный в плоскость. Тогда каждый автоморфизм графа G отображает границу грани в границу грани.

В [17] для групп введено копредставление специального вида (выходящее за рамки данной работы), тесным образом связанное с гранями плоского графа; в результате оказалось возможным охарактеризовать плоские графы Кэли в терминах таких копредставлений.

Теорема 5 [17, теорема 5.1]. Граф Кэли, соответствующий любому граниевому копредставлению, является плоским и допускает устойчивое локально конечное вложение.

Заметим, что адаптировать описанным способом критерий Маклейна к проверке планарности графов Кэли групп в терминах копредставления групп оказалось возможным благодаря именно групповой специфике копредставления — наличию нейтрального и симметричных элементов.

Более того, очевидно, что изучение планарных графов существенно упрощается, если известна их локальная конечность, примером тому служит теорема Томассена (теорема 6), которая справедлива только в локально конечном случае.

Теорема 6 [17, теорема 5.2]. Двусвязный граф имеет 2-базис (то есть такое порождающее множество пространства циклов, что никакое ребро не принадлежит более чем двум его элементам) тогда и только тогда, когда он плоский и имеет локально конечное вложение.

Дело в том, что планарность локально конечных графов можно охарактеризовать условием, аналогичным условию Понтрягина — Куратовского, но нам удалось преодолеть это ограничение в ходе доказательства теоремы 43, столкнувшись с фрактальными графами.

Для сравнения отметим почерпнутые из [15] необходимые условия планарности графа Кэли конечно порождённой группы с более чем одним концом в представляемом ею топологическом пространстве. Напомним, используя вспомогательные обозначения, что для всякой пятёрки (G, A, H, B, φ), где G и H — группы с подгруппами A и B соответственно, а $\varphi : A \to B$ — изоморфизм, *свободным произведением с амальгамированием* называется группа $\mathrm{FPA}(G, A, H, B, \varphi) = (G{*}H)/N$, где N — нормальное в $G{*}H$ замыкание множества $\{a^{-1}\varphi(a) : a \in A\}$. Здесь G и H называются *базовыми группами*, а A и B — *амальгамированными подгруппами*. Для всякой четвёрки (G, A, B, ψ), где G — группа, A и B — подгруппы группы G, а $\psi : A \to B$ — изоморфизм, HNN-*расширение* — это группа $\mathrm{HNN}(G, A, B, \psi) = (G{*}\mathbb{Z})/N$, где N — нормальное в $G{*}\mathbb{Z}$ замыкание множества $\{t^{-1}a^{-1}t\psi(a) \mid a \in A\}$; t — образующий бесконечного циклического множителя $\mathbb{Z}$. Здесь также G называется *базовой группой*, а A и B — *ассоциированными подгруппами* HNN-расширения.

Теорема 7 [15, теорема 4.1]. Пусть G — группа, допускающая планарный граф Кэли с более чем одним концом. Тогда G является либо свободным произведением с амальгамированием $\mathrm{FPA}(H, A, K, B, \varphi)$, где (H, A, K, B, φ) — планарная пятёрка, либо это HNN-расширение $\mathrm{HNN}(H, A, B, \psi)$, где (H, A, B, ψ) — планарная четвёрка.

Достаточные условия, которые гарантируют, что свободное произведение с конечным амальгамированием или HNN-расширение с конечными ассоциированными подгруппами обладает планарным графом Кэли, приведены там же, но они носят более технический характер и не имеют принципиального значения в теоретическом плане.

2.2. О группах с планарными кубическими графами Кэли

Как и планарность, связность является одним из фундаментальных свойств в теории графов. Наличие графа Кэли со связностью меньше чем 3 имеет серьёзные по-

следствия для структуры соответствующей группы. В планарном случае задача декомпозиции (заключающаяся в таком разбиении множества вершин на подмножества, чтобы вес вершин в этих подмножествах был сбалансирован, а суммарный вес разрезанных рёбер минимизирован), трудно решаемая при низкой связности графа, может сводиться к случаю, когда граф Кэли является 3-связным, а в нём могут использоваться геометрические методы.

Напомним, что граф $G = (VG, EG)$ называется κ-связным, если $G - X$ связен для любого множества $X \subseteq VG$ при $|X| < \kappa$. Заметим, что если граф G κ-связен, то он также является $(\kappa - 1)$-связным. Число связности $\kappa(G)$ графа G — это наибольшее целое число κ, такое, что G k-связен.

Теоретическими предпосылками к основным результатам данного пункта являются следующие теоремы:

Теорема 8 [14, теорема 2.2]. Любая подгруппа планарной группы является планарной.

Теорема 9 [14, теорема 4.1]. Группа G имеет 1-связный планарный граф Кэли тогда и только тогда, когда она является либо бесконечной циклической, либо нетривиальным свободным произведением планарных групп.

Теорема 10 [14, теорема 4.4]. Если группа G имеет планарный 2-связный граф Кэли, то G либо является конечной циклической группой или группой диэдра, либо это фундаментальная группа графа групп, все рёберные группы которых имеют порядок два или менее, а группы вершин допускают планарную связность как минимум 3. В последнем случае группы вершин имеют планарные порождающие множества, включающие нетривиальные элементы, инцидентные группе рёбер.

Теорема 11 [14, теорема 4.5]. Пусть Γ — 3-связный планарный граф, а c — простой цикл в нём. Если c является границей диска в некоторой плоской укладке графа Γ, то он будет таким в любой плоской укладке графа Γ.

В [18] классифицируются плоские 2-связные (то есть наименьшая мощность множества вершин, разделяющих граф, равна 2) кубические графы Кэли, описывая явное копредставление и вложение в плоскость для каждого из них. В сочетании с [19] это даёт полное описание всех плоских кубических графов Кэли.

Теорема 12 [18, теорема 1.1]. Пусть G — плоский кубический граф Кэли связности 2. Тогда верно одно из следующих утверждений:

(i) $G \cong Cay\,\langle a, b \mid b^2 = 1, (ab)^n = 1\rangle$, $n \geqslant 2$;
(ii) $G \cong Cay\,\langle a, b \mid b^2 = 1, (aba^{-1}b^{-1})^n = 1\rangle$, $n \geqslant 1$;
(iii) $G \cong Cay\,\langle a, b \mid b^2 = 1, a^4 = 1, (a^2b)^n = 1\rangle$, $n \geqslant 2$;
(iv) $G \cong Cay\,\langle b, c, d \mid b^2 = 1, c^2 = 1, d^2 = 1, (bc)^2 = 1, (bcd)^m = 1\rangle$, $m \geqslant 2$;
(v) $G \cong Cay\,\langle b, c, d \mid b^2 = 1, c^2 = 1, d^2 = 1, (bc)^{2n} = 1, (cbcd)^m = 1\rangle$, $n, m \geqslant 2$;
(vi) $G \cong Cay\,\langle b, c, d \mid b^2 = 1, c^2 = 1, d^2 = 1, (bc)^n = 1, (bd)^m = 1\rangle$, $n, m \geqslant 2$;
(vii) $G \cong Cay\,\langle b, c, d \mid b^2 = 1, c^2 = 1, d^2 = 1, (b(cb)^n d)^m = 1\rangle$, $n, m \geqslant 2$;
(viii) $G \cong Cay\,\langle b, c, d \mid b^2 = 1, c^2 = 1, d^2 = 1, (bcbd)^m = 1\rangle$, $m \geqslant 1$;
(ix) $G \cong Cay\,\langle b, c, d \mid b^2 = 1, c^2 = 1, d^2 = 1, (bc)^n = 1, cd = 1\rangle$, $n \geqslant 1$ (вырожденные случаи с избыточным числом образующих и конечным G).

И наоборот, каждое из данных копредставлений с параметрами, выбранными в указанных интервалах, имеет плоский двусвязный кубический граф Кэли.

Вложение графа называется устойчивым, если любые две его вершины имеют либо одинаковый спин, либо все вершины имеют разные спины. Интуитивно это значит,

что каждая вершина вкладывается «одинаково» в том смысле, что групповое действие отображает грани в грани. В свою очередь, ребро графа называется сохраняющим спин, если его концевые вершины имеют одинаковый спин, в противном случае ребро изменяет спин. Более точно, спином вершины x называется циклический порядок множества $L = \{xy^{-1} : y \in N(x)\}$, где $N(x)$ — окружение вершины x, а вершина xy_1^{-1} является концом ребра, начинающегося в вершине xy_2^{-1}, при том, что ребро xy_2 идёт сразу после ребра xy_1 в обходе по часовой стрелке вокруг вершины x.

Следующая теорема содержит характеристическое свойство плоских двусвязных графов Кэли групп, порождённых двумя элементами, один из которых имеет бесконечный порядок.

Теорема 13 [18, теорема 3.2]. Пусть $G = Cay\,\langle a, b \,|\, b^2 = 1, \ldots\rangle$ — двусвязный граф Кэли, в котором a имеет бесконечный порядок. Тогда $\Gamma(G) \cong \langle a, b \mid b^2 = 1, (ab)^n = 1\rangle$, $n \geqslant 2$, либо $\Gamma(G) \cong \langle a, b \mid b^2 = 1, (aba^{-1}b^{-1})^n = 1\rangle$, $n \geqslant 1$. При этом G планарен и имеет устойчивое вложение, в котором ребро a сохраняет спин. И наоборот, каждое из данных копредставлений с параметрами, выбранными в указанных интервалах, имеет плоский двусвязный кубический граф Кэли, в котором a бесконечного порядка.

Следующая теорема содержит характеристическое свойство плоских двусвязных графов Кэли групп, порождённых двумя элементами, оба из которых конечного порядка.

Теорема 14 [18, теорема 3.3]. Пусть $G = Cay\,\langle a, b \mid b^2 = 1, a^n = 1, \ldots\rangle$ — плоский двусвязный граф Кэли. Тогда $G \cong Cay\,\langle a, b \mid b^2 = 1, a^4 = 1, (a^2b)^n = 1\rangle$, $n \geqslant 2$. При этом G имеет устойчивое вложение, в котором a меняет спин, а b сохраняет. И наоборот, для любого $n \geqslant 2$ данное копредставление имеет плоский двусвязный кубический граф Кэли, в котором a порядка 4.

Наконец, рассмотрим ситуацию, когда группа G определяется тремя образующими элементами b, c, d, каждый из которых удовлетворяет соотношениям $b^2 = 1$, $c^2 = 1$, $d^2 = 1$, поскольку G кубическая. Выделим два случая в зависимости от того, есть ли у графа G шарнир, то есть ребро $e = xy$, такое, что удаление пары вершин x, y приводит к потере связности графа G.

Граф с шарнирами описывается в следующей теореме.

Теорема 15 [18, теорема 4.1]. Пусть $G = Cay\,\langle b, c, d \mid b^2 = 1, c^2 = 1, d^2 = 1, \ldots\rangle$ — двусвязный граф Кэли, имеющий шарнир. Тогда либо $G \cong Cay\langle b, c, d \mid b^2 = 1, c^2 = 1, d^2 = 1, (bc)^n = 1, (bd)^m = 1\rangle$ для любых значений $m, n \geqslant 2$, либо $G \cong Cay\langle b, c, d \mid b^2 = 1, c^2 = 1, d^2 = 1, (bcbd)^n = 1\rangle$ для $n \geqslant 1$, но не одновременно. В обоих случаях граф G плоский. В первом случае он имеет вложение, каждое ребро которого меняет спин, а во втором — вложение, у которого ровно одно из рёбер (являющееся шарниром) сохраняет спин. И наоборот, каждое из приведённых копредставлений с параметрами, выбранными в указанных интервалах, допускает плоский двусвязный кубический граф Кэли с шарнирами.

Следующий результат завершает характеризацию плоских двусвязных кубических графов Кэли. Единственный оставшийся случай — когда G не имеет шарнира, но в нём есть двухцветный цикл. Заметим, исходя из комбинаторных соображений, что конечные простые графы Кэли степени не менее 3 будут 3-связны, поэтому для обеспечения свойства двусвязности граф G должен иметь параллельные рёбра. Отсюда следует, что если удовлетворяющий условию двусвязности граф $G = Cay(\Gamma)$ конечен, то $\Gamma \cong$ $\cong \langle b, c, d \mid b^2 = 1, c^2 = 1, d^2 = 1, (bc)^n = 1, cd = 1\rangle$, где $n \geqslant 1$. Будем изначально выбирать граф G бесконечным.

Граф без шарниров описывается следующей теоремой.

Теорема 16 [18, теорема 4.6]. Пусть $G = Cay\,\langle b, c, d \mid b^2 = 1, c^2 = 1, d^2 = 1, \ldots\rangle$ — плоский двусвязный бесконечный граф Кэли с двухцветным циклом и без шарнира. Тогда имеет место изоморфизм $\Gamma \cong \langle b, c, d \mid b^2 = 1, c^2 = 1, d^2 = 1, (bc)^2 = 1, (bcd)^m = 1\rangle$, где $m \geqslant 2$, в этом случае граф $G = Cay(\Gamma)$ допускает устойчивое вложение с одним фиксированным спином, либо $\Gamma \cong \langle b, c, d \mid b^2 = 1, c^2 = 1, d^2 = 1, (bc)^{2k} = 1, (cbcd)^m = 1\rangle$, где $k, m \geqslant 2$ и $G = Cay(\Gamma)$ допускает устойчивое вложение, в котором только рёбра, помеченные элементом c, сохраняют спин. И наоборот, каждое из указанных копредставлений с параметрами m и k в заданных интервалах имеет плоский граф Кэли с числом связности 2 без шарниров.

Для полноты картины отметим, что в [19] опубликован список всех 37 возможных копредставлений групп из теоремы о классификации плоских кубических графов Кэли. Акцентируем внимание читателя на том факте, что среди бесконечных плоских графов Кэли особый интерес исследователей вызывают графы, соответствующие разрывному действию на плоскости. Их группы (так называемые разрывные группы) находят приложения в комплексном анализе и тесным образом связаны с поверхностными группами. Эти графы и группы хорошо изучены. С остальными ситуация сложнее, интерес к ним проявился позже, и они до сих пор полностью не классифицированы, в частности, не известно даже, можно ли их эффективно перечислить. В то же время класс плоских кубических графов Кэли оказался достаточно хорошо устроен для того, чтобы получить полное описание всех его элементов, и достаточно разнообразен для того, чтобы дать общее представление о планарных графах Кэли бесконечных групп.

Систематизация и дальнейшее обобщение изложенных результатов привели к появлению в [20] концепции *представления планарных групп*, а в [21] — *обобщённого представления планарных групп*, это тип группового представления, который гарантирует планарность соответствующего графа Кэли, и наоборот, каждый планарный конечно порождённый граф Кэли допускает такое групповое представление. Авторы работ [20, 21] показывают, что группа допускает планарный конечно порождённый граф Кэли тогда и только тогда, когда она допускает особый вид группового представления, называемого планарным. Планарные представления могут быть распознаны алгоритмически. Как следствие, получается эффективное перечисление планарных графов Кэли и, в частности, утвердительный ответ на вопрос о том, могут ли планарные группы быть эффективно перечислимы.

2.3. О планарности графов Кэли графового произведения групп

Упомянутое во введении перемещение вопросов планарности графов Кэли в более широкий контекст послужило толчком к получению новых результатов о таких, казалось бы, всесторонне изученных классических объектах, как функциональные клейновы группы, основная теория которых была заложена в фундаментальных работах Х. Пуанкаре и Ф. Клейна в XIX в. А именно: если G — конечно порождённая группа, действующая точно и правильно разрывно гомеоморфизмами на плоской поверхности $X \subseteq \mathbb{S}^2$, то в [23] инструментами теории графов доказывается, что G допускает ко-компактное преобразование при условии, что можно заменить X другой поверхностью $Y \subseteq \mathbb{S}^2$. Также в [23] доказано, что если группа H имеет конечно порождённый (мульти-)граф Кэли, эквивариантно вложимый в $\mathbb{S}^2$, то его можно задать так, чтобы граница любой грани была конечна. Доказательства этих двух фактов из далёких друг от друга областей математики тесным образом переплетены, а определяемые ими

классы групп совпадают. При сохранении ориентации эти классы с точностью до изоморфизма совпадают с классом конечно порождённых клейновых функциональных групп. Но, к сожалению, существует конечно порождённый планарный граф Кэли, группа которого не принадлежит данному классу, поэтому завершённой классификации не сформировалось, тем не менее в ходе попыток её получения обнаружилось, что компактификация Фрейденталя каждой плоской поверхности гомеоморфна сфере.

Предтечей появления основных результатов данного пункта была изложенная в [16] классификация конечно определённых групп с плоскими графами Кэли, опирающаяся на классификацию плоских покрытий компактных поверхностей.

Вслед за определением из [22] положим, что $\Gamma = (V, E)$ — конечный простой граф (неориентированный и без петель). Зададим разметку вершин графа Γ отображением φ, ставящим в соответствие каждой вершине из множества вершин V некоторую нетривиальную конечную абелеву группу. Граф Γ с описанной разметкой вершин называется умножающим. Графовое произведение групп $G(\Gamma)$ — это группа, полученная из свободного произведения абелевых групп $\varphi(v)$ путём добавления к нему коммутаторных соотношений $[g, h] = 1$ для всех $g \in \varphi(v)$, $h \in \varphi(w)$, таких, что $\{v, w\} \in E$. Эти группы были введены для $\varphi(v) \cong \mathbb{Z}$ по всем $v \in V$, а позже неоднократно обобщались на случай произвольных групп, маркирующих вершины умножающего графа. В частности, свободные [прямые] произведения конечных абелевых групп являются графовыми произведениями групп, в которых умножающий граф пустой [полный].

В [70, 71] исследовано свойство планарности графов Кэли некоторых из таких групп на более высоком уровне абстракции — на языке частично коммутативных полугрупп. Следующая теорема даёт полную характеризацию графовых произведений конечных абелевых групп, графы Кэли которых относительно минимального множества образующих плоские.

Теорема 17 [22, теорема A]. Пусть Γ — умножающий граф графового произведения конечных циклических групп, $\Gamma_{=2}$ — подграф графа Γ, порождённый вершинами, помеченными группами порядка 2, а $\Gamma_{>2}$ — подграф графа Γ, порождённый вершинами, помеченными группами порядка > 2. Граф Кэли $Cay(G(\Gamma))$ плоский тогда и только тогда, когда выполнено каждое из следующих условий:

(i) $\Gamma_{=2}$ внешнепланарен;
(ii) $\Gamma_{>2}$ — пустой граф;
(iii) если $v \in \Gamma_{>2}$, то порождённый смежными с v вершинами подграф графа Γ не содержит вершин, либо состоит из одной вершины, либо является дизъюнктным объединением двух вершин;
(iv) если $\Gamma' \subseteq \Gamma$ — порождённый цикл, то $\Gamma' \subseteq \Gamma_{=2}$.

Отметим, что на языке частично коммутативных полугрупп аналогичная теорема 43 сформулирована лаконичнее, но содержит труднее проверяемые условия в случае их переноса на группы.

3. О полугруппах с планарными графами Кэли

Пионерские работы в обозначенном направлении, инициированные в 2001 г. Л. М. Мартыновым, можно условно разделить по следующим категориям в зависимости от класса решаемой задачи:

1) критерий планарности графов Кэли коммутативно-свободных произведений циклических полугрупп, моноидов и полугрупп с нулём;

2) критерий планарности графов Кэли прямых произведений циклических полугрупп, моноидов и полугрупп с нулём;
3) задача о допустимости плоских триангуляций, полного пятиэлементного графа K_5 и полного двудольного графа $K_{3,3}$ с некоторой ориентацией рёбер в качестве графов Кэли полугрупп;
4) рассыпчатые полугруппы с планарными графами Кэли.

А именно: в [72] охарактеризованы полугруппы, являющиеся коммутативно-свободными произведениями [56, с. 69] циклических полугрупп, циклических моноидов и циклических полугрупп с нулём с планарными графами Кэли. При этом мы рассматриваем сначала случаи конечных полугрупп, а затем в качестве следствий получаем описания бесконечных полугрупп с указанным свойством.

3.1. О коммутативных полугруппах с планарными графами Кэли

Выбор тематики данного подраздела объясняется исключительной ролью коммутативных полугрупп в теории полугрупп, сравнимой по уровню развития со структурной теорией абелевых групп.

Основным результатом о конечных свободных коммутативных полугруппах с планарными графами Кэли является следующая

Теорема 18 [72, теорема 1]. Граф Кэли конечной свободной коммутативной полугруппы S относительно множества свободных образующих планарен тогда и только тогда, когда S задана копредставлением одного из следующих видов:

1. $S = \langle a \mid a^{r+m} = a^r \rangle$, где r и m — любые натуральные числа.
2. $S = \langle a, b \mid ab = ba,\ a^{r+m} = a^r,\ b^{h+t} = b^h \rangle$, где для натуральных чисел r, m, h, t выполняется одно из следующих ограничений:
   а) $m \leqslant 2$, $t \leqslant 2$;
   б) $r = 1$, $h = 1$, $t = 2$; или $r = 1$, $h = 2$, $t = 1$;
   в) $r = 1$, $h = 1$, $m = 2$; или $r = 2$, $h = 1$, $m = 1$;
   г) $r = 1$, $m = 1$; или $h = 1$, $t = 1$.
3. $S = \langle a, b, c \mid ab = ba,\ ac = ca,\ bc = cb,\ a^2 = a,\ b^2 = b,\ c^{k+l} = c^k \rangle$, где k и l — натуральные числа, $l \leqslant 2$.

Заметим, что в каждом условии теоремы присутствуют бесконечные серии полугрупп.

Тем не менее число образующих соответствующих полугрупп с планарными графами Кэли в данном случае ограничено числом 3. Позднее [73] были охарактеризованы конечные свободные коммутативные моноиды, допускающие планарный граф Кэли.

Теорема 19 [73, теорема 1]. Граф Кэли конечного свободного коммутативного моноида S относительно множества свободных образующих планарен тогда и только тогда, когда S задан копредставлением одного из следующих видов:

1. $S = \langle a \mid a^m = 1 \rangle$, где m — любое натуральное число.

2.1) $S = \langle a, b \mid ab = ba,\ a^{r+m} = a^r,\ b^t = 1 \rangle$, где для натуральных чисел r, m, t выполнено одно из следующих ограничений:
   а) $t \leqslant 2$;
   б) $m \leqslant 2$, $t > 2$;

2.2) $S = \langle a, b \mid ab = ba,\ a^m = 1,\ b^t = 1 \rangle$, где m и t — натуральные числа, $t \leqslant 2$;

3.1) $S = \langle a, b, c \mid ab = ba,\ ac = ca,\ bc = cb,\ a^{r+m} = a^r,\ b^{h+t} = b^h,\ c^k = 1 \rangle$, где для натуральных чисел r, m, h, t, k выполнено одно из следующих условий:

а) $h = 1$, $t = 1$, $k = 1$;
б) $m \leqslant 2$, $t \leqslant 2$, $k = 1$;
в) $m \leqslant 2$, $h = 1$, $t = 1$, $k = 2$;

3.2) $S = \langle a, b, c \mid ab = ba,\ ac = ca,\ bc = cb,\ a^{r+m} = a^r,\ b^2 = 1,\ c^2 = 1\rangle$, где r и m — натуральные числа, $m \leqslant 2$;

3.3) $S = \langle a, b, c \mid ab = ba,\ ac = ca,\ bc = cb,\ a^2 = 1,\ b^2 = 1,\ c^2 = 1\rangle$.

4. $S = \langle a, b, c, d \mid ab = ba,\ ac = ca,\ ad = da,\ bc = cb,\ bd = db,\ cd = dc,\ a^{r+m} = a^r,\ b^2 = b,\ c^2 = c,\ d = 1\rangle$, где r и m — натуральные числа, $m \leqslant 2$.

Для полноты изложения приведём соответствующий результат из [72] о конечных свободных коммутативных полугруппах с нулём, допускающих планарный граф Кэли.

Теорема 20 [72, теорема 2]. Граф Кэли конечной свободной коммутативной полугруппы S с нулём относительно множества свободных образующих планарен тогда и только тогда, когда S задана копредставлением одного из следующих видов:

1) $S = \langle a \mid a^r = 0\rangle$, где r — любое натуральное число;
2) $S = \langle a, b \mid ab = ba,\ a^r = 0,\ b^h = 0\rangle$, где r, h — любые натуральные числа;
3) $S = \langle a, b \mid ab = ba,\ a^{r+m} = a^r,\ b^h = 0\rangle$, где r, m, h — натуральные числа, причём $m \leqslant 2$ либо $r = 1$ и $h = 1$;
4) $S = \langle a, b, c \mid ab = ba,\ ac = ca,\ bc = cb,\ a^2 = a,\ b^2 = b,\ c^k = 0\rangle$, где k — любое натуральное число.

Коль скоро, согласно теореме Биркгофа [74], многообразия полугрупп замкнуты относительно операций взятия подполугрупп, прямых произведений и гомоморфных образов полугрупп, то вторым естественным этапом эволюции познания структуры полугрупп, допускающих планарные графы Кэли, является анализ прямых произведений оных. Полугруппы, являющиеся прямыми произведениями циклических полугрупп, моноидов и полугрупп с нулём, допускающие планарные графы Кэли, охарактеризованы в [75, 76] теоремами 21–23.

Так как граф Кэли конечной циклической полугруппы является планарным, то предполагается, что число сомножителей в прямых произведениях более одного.

Теорема 21 [75]. Конечная полугруппа S, являющаяся прямым произведением неодноэлементных циклических полугрупп, допускает планарный граф Кэли тогда и только тогда, когда выполнено одно из условий:

1. $S \cong \langle a \mid a^{r+m} = a^r\rangle \times \langle b \mid b^{h+t} = b^h\rangle$, где для натуральных чисел r, m, h, t выполняется одно из следующих ограничений:
   1.1) $r = 1$, $h = 1$, $(m, t) < 3$;
   1.2) $r = 1$, $m = 2$, $t < 3$;
   1.3) $r = 2$, $m = 1$, $h < 4$, $t < 3$;
   1.4) $r = 2$, $m = 1$, $h < 5$, $t = 1$;
   1.5) $r = 3$, $m = 1$, $h = 3$, $t = 1$.
2. $S \cong \langle a \mid a^{r+m} = a^r\rangle \times \langle b \mid b^{h+t} = b^h\rangle \times \langle c \mid c^{k+l} = c^k\rangle$, где для натуральных чисел r, m, h, t, k, l выполняется одно из следующих ограничений:
   2.1) $r = 1$, $m = 2$, $h = 1$, $t = 2$, $k = 1$, $l = 2$;
   2.2) $r = 1$, $m = 2$, $h = 2$, $t = 1$, $k = 2$, $l = 1$;
   2.3) $r = 2$, $m = 1$, $h = 2$, $t = 1$, $k = 2$, $l < 3$;
   2.4) $r = 2$, $m = 1$, $h = 2$, $t = 1$, $k = 3$, $l = 1$.
3. $S \cong \langle a_0 \mid a_0^{r+m} = a_0^r\rangle \times \prod\limits_{i=1}^{n} \langle a_i \mid a_i^{2+1} = a_i^2\rangle$, где для натуральных чисел r и m выполняется одно из следующих ограничений:

3.1) $r = 1$, $m = 2$;
3.2) $r = 2$, $m < 3$;
3.3) $r = 3$, $m = 1$.

Теорема 22 [76, теорема 1]. Конечный моноид S, являющийся прямым произведением неодноэлементных циклических моноидов, допускает планарный граф Кэли тогда и только тогда, когда выполняется одно из следующих условий:

1. $S \cong \langle a \mid a^{r+m} = a^r \rangle^1 \times \langle b \mid b^{h+t} = b^h \rangle^1$, где для натуральных r, m, h, t выполняется одно из следующих ограничений:
   1.1) $r = 1$, $m = 2$;
   1.2) $m \leqslant 2$, $t \leqslant 2$;
   1.3) $r = 1$, $m > 2$, $t \leqslant 2$.
2. $S \cong \langle a \mid a^3 = a \rangle \times \langle b \mid b^3 = b \rangle \times \langle c \mid c^{k+l} = c^k \rangle^i$, где для натуральных i, k, l выполняется одно из следующих условий:
   2.1) $i = 1$, $l \leqslant 2$;
   2.2) $i = +1$, $k = 1$, $l \leqslant 2$.
3. $S \cong \langle a \mid a^{1+m} = a^1 \rangle^{+1} \times \langle b \mid b^{h+t} = b^h \rangle^i$, где m, h, t — натуральные числа; $i \in \{1, +1\}$ и выполняется одно из следующих ограничений:
   3.1) $m = 1$;
   3.2) $i = 1$, $h = 1$, $t = 2$;
   3.3) $m = 2$, $h = 1$, $i = 1$;
   3.4) $m = 2$, $h = 1$, $t = 2$, $i = +1$.
4. $S \cong \langle a_0 \mid a_0^{r+m} = a_0^r \rangle^1 \times \prod_{i=1}^{n} \langle a_i \mid a_i^2 = a_i \rangle^{+1}$, где $m \leqslant 2$, $n \leqslant 2$; или $r = 1$, $m = 1$, $n \leqslant 3$.

Заметим, что условия теоремы 22 практически повторяют условия теоремы 19, с учётом неодноэлементности перемножаемых моноидов.

Теорема 23 [76, теорема 2]. Конечная полугруппа S с нулём, являющаяся прямым произведением неодноэлементных циклических полугрупп с нулём, допускает планарный граф Кэли тогда и только тогда, когда выполняется одно из следующих условий:

1. $S \cong \langle a \mid a^{r+m} = a^r \rangle^0 \times \langle b \mid b^{h+t} = b^h \rangle^0$, где для натуральных чисел r, m, h, t выполняется одно из следующих ограничений:
   1.1) $r = 2$, $m = 1$, $h < 5$, $t = 1$;
   1.2) $r = 3$, $m = 1$, $h = 3$, $t = 1$;
   1.3) $r = 2$, $m = 1$, $h = 1$, $t = 2$.
2. $S \cong \langle a_0 \mid a_0^{r+1} = a_0^r \rangle \times \prod_{i=1}^{n} \langle a_i \mid a_i^{2+1} = a_i^2 \rangle$, где r — натуральное число, $r \leqslant 3$.

3.1) $S \cong \langle a \mid a^{2+1} = a^2 \rangle \times \langle b \mid b^{2+1} = b^2 \rangle^{+0}$;
3.2) $S \cong \langle a \mid a^{r+m} = a^r \rangle^{+0} \times \langle b \mid b^2 = b \rangle^{+0}$, где r и m — натуральные числа, $m \leqslant 2$.

4. $S \cong \langle a_0 \mid a_0^{r+1} = a_0^r \rangle \times \prod_{i=1}^{n} \langle a_i \mid a_i^2 = a_i \rangle^{+0}$, где $n \leqslant 2$; или $r = 1$, $n \leqslant 3$.

3.2. О полугруппах с ациклическими графами Кэли

Остановимся подробнее на полугруппах с ациклическими графами Кэли. Их изучением систематически занимался А. Л. Макарьев с 2006 г., и на этом пути получены интересные результаты.

Теорема 24 [46, теорема 1]. Основа графа Кэли нильпотентной полугруппы S ступени $n \geqslant 2$ с минимальным порождающим множеством X является деревом то-

гда и только тогда, когда для любых элементов x, y из множества X справедливо равенство $xy = x^2$.

Опираясь на данную теорему, её следствия и ряд ценных предложений, была доказана следующая теорема, характеризующая конечное дерево, которое может быть основой графа Кэли некоторой нильпотентной полугруппы, и позволяющая указать такие полугруппы, если они имеются.

Теорема 25 [46, теорема 2]. Для того чтобы конечное дерево было основой графа Кэли некоторой нильпотентной полугруппы ступени $n \geqslant 2$, необходимо и достаточно, чтобы среди центральных или висячих вершин этого дерева имелась хотя бы одна вершина ω, удалённая от каждой висячей вершины дерева (отличной от ω) на расстояние $(n-1)$ или $(n-2)$, и все простые цепи, соединяющие произвольную висячую вершину с вершиной ω, либо не имели общих вершин (кроме ω), либо имели одинаковую длину (или, в частности, совпадали). При этом все висячие вершины дерева (кроме вершины ω, если она является висячей) соответствуют порождающим элементам, а вершина ω соответствует нулю этой полугруппы.

Годом позднее были охарактеризованы рассыпчатые и прямоугольные полугруппы с ациклическими графами Кэли (в частности, деревьями), а также найдены условия, при которых ациклический неорграф (в частности, дерево) может служить основой графа Кэли некоторой прямоугольной или рассыпчатой полугруппы.

Основным результатом, касающимся рассыпчатых полугрупп, является следующая

Теорема 26 [44, теорема 1]. Ординальная сумма $S = \bigcup\limits_{e \in P} S_e$ сингулярных полугрупп имеет ациклический граф Кэли тогда и только тогда, когда выполняется одно из следующих условий:

1) $|P| = 1$ и $|S| \leqslant 2$, причём S — любая сингулярная полугруппа;
2) $|P| = 1$ и $S > 2$, причём S — полугруппа левых нулей;
3) $|P| = 2$, причём одна из компонент — произвольная полугруппа левых нулей, а вторая — одноэлементная полугруппа.

Следующий результат касается прямоугольных полугрупп.

Теорема 27 [44, теорема 2]. Основа графа Кэли прямоугольной полугруппы $S = L \times R$ является ациклическим графом тогда и только тогда, когда $|R| \leqslant 2$.

Естественным образом формулируемая, но нетривиально доказываемая, следующая теорема характеризует ациклический неорграф, который может быть основой графа Кэли некоторой прямоугольной полугруппы.

Теорема 28 [44, теорема 3]. Для того чтобы ациклический неорграф мог служить основой графа Кэли некоторой прямоугольной полугруппы, необходимо и достаточно, чтобы выполнялось только одно из условий:

1) каждая вершина графа изолирована;
2) все вершины графа являются висячими.

Из теоремы 28 следует, что для того чтобы неориентированное дерево могло служить основой графа Кэли некоторой прямоугольной полугруппы, необходимо и достаточно, чтобы это дерево имело не больше двух вершин.

В 2008 г. продолжилось рассмотрение полугрупп с ациклическими графами Кэли, начатое в [46, 44], а именно рассмотрен важный класс полугрупп идемпотентов — полурешётки. Характеризацию полурешёток, имеющих ациклический граф Кэли, даёт следующая

Теорема 29 [47]. Для полурешётки S следующие условия эквивалентны:

1) основа графа Кэли полугруппы S является ациклическим графом;
2) S — веерная полугруппа;
3) основа графа Кэли полугруппы S является нуль- или одноярусным деревом.

Заключительным результатом в данной серии явилась теорема 30, значительно усиливающая результат теоремы 26. Заметим, что ранее найдены условия, при которых ординальная сумма сингулярных полугрупп имеет ациклический граф Кэли, а в следующей теореме рассматриваются условия, при которых ациклический граф Кэли имеет ординальная сумма произвольных полугрупп.

Теорема 30 [48]. Ординальная сумма $\overline{S} = \bigcup\limits_{e \in P} S_e$ полугрупп имеет ациклический граф Кэли тогда и только тогда, когда выполняется одно из следующих условий:

1. $|P| = 1$ и $\overline{S}$ — любая полугруппа с ациклическим графом Кэли.
2. $|P| = 2$, причём выполняется одно из условий:
   а) первая компонента — циклическая полугруппа с периодом 1 или 2, а вторая — левосингулярная полугруппа;
   б) вторая компонента — одноэлементная полугруппа, а первая — любая нециклическая полугруппа S с минимальным порождающим множеством X, в которой выполняется следующее условие: если $xa = yb$ или $xa = y$, то $x = y$, где $x, y \in X$ и $a, b \in S$.

3.3. О вполне регулярных полугруппах с планарными графами Кэли

Напомним, что вполне регулярной называется полугруппа, являющаяся объединением групп. В свою очередь, группы представляют собой частный случай полугрупп. Исторически сложилось так, что изучение групп было начало раньше, чем полугрупп, исходя из геометрических приложений первых. Несмотря на их более сложную структуру, многие проблемы теории полугрупп ныне решаются по модулю теории групп. В частности, исследователям вопросов планарности графов Кэли для конечных групп удалось получить завершённые результаты.

Родом графа G называется наименьшее число ручек, которые нужно добавить к сфере, чтобы уложить G на этой сфере.

С опорой на приведённое в теореме Машке (теорема 1) описание плоских групп в работе [28] найдена следующая характеризация полугрупп, графы Кэли которых допускают укладку на торе, то есть являются графами минимального рода, равного 1. Центральное место в этой характеризации заняли так называемые *правые группы*, по определению представимые прямым произведением группы G на полугруппу правых нулей R_n порядка n.

Теорема 31 [28, теорема 3.6]. Пусть $G \times R_r$ — конечная правая группа, $r \geqslant 2$. Минимальный род графа $Cay(G \times R_r, C \times R_r)$ среди всех порождающих множеств $C \subseteq G$ группы G равен 1 тогда и только тогда, когда $G \times R_r$ изоморфна одной из следующих правых групп: $\mathbb{Z}_n \times R_r$ с $(n, r) \in \{(2,3), (2,4), (3,3), (i,2)\}$ для $i \geqslant 4$; $D_n \times R_2$ для всех $n \geqslant 2$. Обратим внимание, что этот список включает в себя $\mathbb{Z}_2 \times D_n \times R_2$ и $\mathbb{Z}_2 \times \mathbb{Z}_n \times R_2$ для нечётного $n \geqslant 3$.

Данный результат позднее был дополнен перечислением всех правых групп, графы Кэли которых являются планарными, то есть минимального рода, равного нулю.

Теорема 32 [29, теорема 7.1]. Любая плоская правая группа представима в виде произведения $G \times R_k$ с $k \geqslant 2$, где один из множителей равен $G \in \{\{e\}, \mathbb{Z}_n, D_n, S_4, A_4, A_5\}$

при $k \leqslant 3$, либо в виде произведения $\{e\} \times R_4$. Здесь $\{e\}$ означает одноэлементную группу.

Приведём известную классификацию плоских клиффордовых полугрупп в простейшем частном случае, когда полугруппа является полурешёткой двух групп. Прежде чем сформулировать результат, разъясним используемые в [55] обозначения. Запись $G_\alpha \xrightarrow{f} G_\beta$ применяется для обозначения групп и соответствующего гомоморфизма $f_{\alpha,\beta}$, описанного в теореме 33.

Теорема 33 [59, теорема 4.11]. Пусть Y — полурешётка. Каждому элементу α из Y поставим в соответствие группу G_α таким образом, что G_α и G_β не пересекаются при $\alpha \neq \beta$. Каждой паре элементов α, β из Y, для которых $\alpha > \beta$, поставим в соответствие гомоморфизм $f_{\alpha,\beta}$ группы G_α в G_β таким образом, что если $\alpha > \beta > \gamma$, то $f_{\alpha,\beta} f_{\beta,\gamma} = f_{\alpha,\gamma}$. Через $f_{\alpha,\alpha}$ обозначим тождественный автоморфизм группы G_α. Пусть S — объединение всех групп G_α ($\alpha \in Y$). Определим произведение в S, полагая для двух элементов $a_\alpha, b_\beta \in S$ ($a_\alpha \in G_\alpha$, $b_\beta \in G_\beta$) $a_\alpha a_\beta = (a_\alpha f_{\alpha,\gamma})(b_\beta f_{\beta,\gamma})$, где γ равно произведению $\alpha\beta$ элементов α и β полурешётки Y. Тогда S — полугруппа с коммутирующими идемпотентами, являющаяся объединением групп, или (что эквивалентно) инверсная полугруппа, являющаяся объединением групп. Обратно, каждая такая полугруппа может быть построена указанным способом.

Запись $G_\alpha \xrightarrow{(f,f')} G_\beta$ содержит соответствующие ограниченные отображения $f_{\alpha,\beta}$ на каждой из компонент G_α, если G_α имеет два образующих; 0 обозначает нулевое отображение, id — тождественное. Например, в п. 2, *б* теоремы 34 первый множитель отображается тождественно, а второй — нулевым отображением. Инъективное и биективное отображения обозначаются «injective» и «bijective» соответственно. Наконец, заметим, что если k и m взаимно просты, то группы $\mathbb{Z}_k \times \mathbb{Z}_m$ и $\mathbb{Z}_{km}$ изоморфны.

Теорема 34 [55, теорема 2.5]. Пусть $S = G_\alpha \cup G_\beta$ — конечная клиффордова полугруппа с $\alpha > \beta$. Тогда S планарна тогда и только тогда, когда выполнено одно из следующих условий:

1. $G_\alpha = \mathbb{Z}_m$, $G_\beta = \mathbb{Z}_n$ при
   - а) $\mathbb{Z}_m \xrightarrow{0} \mathbb{Z}_n$, или
   - б) $m = n$, $\mathbb{Z}_m \xrightarrow{\text{bijective}} \mathbb{Z}_m$, или
   - в) $n = 2m$, $\mathbb{Z}_m \xrightarrow{\text{injective}} \mathbb{Z}_{2m}$.
2. $G_\alpha = \mathbb{Z}_2 \times \mathbb{Z}_2$ при
   - а) $\mathbb{Z}_2 \times \mathbb{Z}_2 \xrightarrow{0} \mathbb{Z}_n$, или
   - б) $\mathbb{Z}_2 \times \mathbb{Z}_2 \xrightarrow{(\mathrm{id},0)} \mathbb{Z}_2$, или
   - в) $\mathbb{Z}_2 \times \mathbb{Z}_2 \xrightarrow{(\text{injective},0)} \mathbb{Z}_4$.
3. $G_\alpha = \mathbb{Z}_2$, $G_\beta = \mathbb{Z}_2 \times \mathbb{Z}_2$ или D_2.
4. $G_\beta = \mathbb{Z}_n$, $\mathbb{Z}_2 \times \mathbb{Z}_{2n}$, D_n, где $n > 2$, A_4, A_5, S_4 или $\mathbb{Z}_2 \times A_4$ и
   - а) $G_\alpha = \{0\}$ или
   - б) $G_\alpha = \mathbb{Z}_2$ с $f_{\alpha,\beta}$, являющимся нулевым отображением.

3.4. О полугруппах с внешнепланарными графами Кэли

Выбор тематики данного подраздела обусловлен следующим наблюдением, анонсированным в [77]. В [27] изучается граф правого сдвига полугруппы S относительно её элемента a, то есть граф, вершины которого являются элементами S, а ребро соединяет вершины s и t тогда и только тогда, когда $t = sa$. Если a порождает S, то такой граф является графом Кэли полугруппы S, более того, граф правого сдвига всегда плана-

рен. Но как оказалось, свойство планарности графа Кэли полугрупп не сохраняется при переходе к следующим теоретико-полугрупповым конструкциям: коммутативно-свободному произведению [73], ординальной сумме [78], прямому произведению [75] циклических полугрупп, моноидов и полугрупп с нулём. В связи с этим возникает естественная задача характеризации полугрупп с планарными графами Кэли тех или иных классов $\mathcal{K}$ полугрупп, применение к которым наиболее используемых в теории полугрупп конструкций наследует свойство планарности. В настоящем исследовании в качестве $\mathcal{K}$ выбран класс нильпотентных полугрупп, а в качестве конструкции — 0-прямое объединение. Напомним, что 0-прямым объединением дизъюнктного семейства полугрупп S_i $(i \in I)$ с нулём называется полугруппа S с нулём, определённая на объединении полугрупп S_i с последующим отождествлением нулей всех S_i и операцией умножения, совпадающей с исходными операциями на каждой полугруппе S_i, и $xy = 0$, если $x \in S_i$, $y \in S_j$ и $i \neq j$.

Ключевым результатом, мотивирующим к исследованию полугрупп, допускающих внешнепланарные графы Кэли, является

Теорема 35 [77]. Свойство планарности графа Кэли полугруппы наследуется 0-прямым объединением нильпотентных полугрупп, если и только если основа графа Кэли каждой из объединяемых полугрупп в результате удаления нулевого элемента допускает такую плоскую укладку, что все её вершины принадлежат одной грани.

Основная цель данного подраздела — обзор исследований полугрупп, допускающих внешнепланарные графы Кэли. Приведены решения вопросов внешнепланарности графов Кэли для следующих классов:

1) конечные свободные коммутативные полугруппы;
2) конечные свободные коммутативные моноиды;
3) рассыпчатые полугруппы;
4) конечно порождённые полугруппы с одним определяющим соотношением и с тождеством;
5) свободные частично коммутативные полугруппы и n-веерные полурешётки.

Особый интерес представляет вопрос о допустимости графов, взятых с некоторой ориентацией и пометкой рёбер, в качестве графов Кэли полугрупп.

Описываются конечные свободные коммутативные полугруппы, а также конечные свободные коммутативные полугруппы с нулём, графы Кэли которых являются внешнепланарными.

Теорема 36 [45, теорема 2.1]. Граф Кэли конечной свободной коммутативной полугруппы S относительно множества свободных образующих внешнепланарен тогда и только тогда, когда S задана копредставлением одного из следующих видов:

1. $S = \langle a \mid ; a^{r+m} = a^r \rangle$, где r и m — любые натуральные числа.
2. $S = \langle a, b \mid ab = ba,\ a^{r+m} = a^r,\ b^{h+t} = b^h \rangle$, где для натуральных r, m, h, t выполняется одно из следующих условий:
   а) $h = 1$, $m \leqslant 2$, $t = 1$; или $r = 1$, $m = 1$, $t \leqslant 2$;
   б) $r \leqslant 2$, $h \leqslant 2$, $m \leqslant 2$, $t \leqslant 2$ при $r + m \leqslant 3$, $h + t \leqslant 3$.

Перейдём к рассмотрению полугрупп с нулём.

Теорема 37 [45, теорема 2.2]. Граф Кэли конечной свободной коммутативной полугруппы S с нулём относительно множества свободных образующих внешнепланарен тогда и только тогда, когда S задана копредставлением одного из следующих видов:

1. $S = \langle a \mid a^r = 0 \rangle$, где r — любое натуральное число.

2. $S = \langle a, b \mid ab = ba,\ a^r = 0,\ b^h = 0\rangle$, где r, h — натуральные числа, $r \leqslant 2$, $h \leqslant 2$.
3. $S = \langle a, b \mid ab = ba,\ a^{r+m} = a^r,\ b^h = 0\rangle$, где для натуральных r, m, h выполняется хотя бы одно из следующих условий:
   а) $h = 1$;
   б) $r + m = 3$, $h = 2$;
   в) $r + m = 2$, $h > 2$.
4. $S = \langle a, b, c \mid ab = ba,\ ac = ca,\ bc = cb,\ a^2 = a,\ b^2 = b,\ c^1 = 0\rangle$.

Перечислим конечные свободные коммутативные моноиды, допускающие внешнепланарные графы Кэли:

Теорема 38 [45, теорема 3.1]. Граф Кэли свободного коммутативного моноида S с циклическими соотношениями внешнепланарен тогда и только тогда, когда выполнено одно из следующих условий:

1. $S = \langle a \mid a^m = 1\rangle$, где m — любое натуральное число.
2. $S = \langle a, b \mid ab = ba,\ a^{r+m} = a^r,\ b^t = 1\rangle$ либо полугруппа S имеет копредставление $S = \langle a, b \mid ab = ba,\ a^m = 1,\ b^t = 1\rangle$, где для натуральных r, m, t выполнено одно из следующих ограничений:
   а) $t = 1$;
   б) $m \leqslant 2$, $t = 2$.
3. $S = \langle a, b, c \mid ab = ba,\ ac = ca,\ bc = cb,\ a^{r+m} = a^r,\ b^2 = b,\ c = 1\rangle$, где r и m — натуральные числа, $m \leqslant 2$.

Решена и задача описания рассыпчатых полугрупп, допускающих внешнепланарный граф Кэли. Любая рассыпчатая полугруппа является ординальной суммой сингулярных полугрупп [56, с. 50]. Напомним, что ординальной суммой попарно непересекающихся полугрупп S_e, где e пробегает цепь P, называется полугруппа $S = \bigcup\limits_{e \in P} S_e$, в которой при $e < f$ для любых $a \in S_e$ и $b \in S_f$ действует правило умножения $ab = ba = a$. Полугруппа называется *сингулярной*, если она является полугруппой левых или правых нулей.

Теорема 39 [45, теорема 4.1]. Пусть S — рассыпчатая полугруппа и $S = \bigcup\limits_{e \in P} S_e$ — соответствующая ординальная сумма сингулярных полугрупп. Тогда S допускает внешнепланарный граф Кэли, если и только если выполняется одно из следующих условий:

1. $|P| = 1$ и $|S| < 4$, если S — полугруппа правых нулей.
2. $|P| = 2$ и выполнено одно из следующих условий:
   а) обе компоненты — полугруппы правых нулей и $|S| < 4$;
   б) только одна из компонент S_e является полугруппой правых нулей, при этом $|S_e| \leqslant 2$ и другая компонента содержит менее трёх элементов;
   в) обе компоненты — полугруппы левых нулей и одна из них одноэлементная, либо каждая содержит не более двух элементов.
3. $|P| = 3$ и выполнено одно из условий:
   а) все компоненты — полугруппы правых нулей и $|S| < 4$;
   б) все компоненты являются полугруппами левых нулей и $|S| < 5$.

Приведённое во введении определение графа Кэли задает ориентированный мультиграф с помеченными рёбрами. Но существует несколько небольших разновидностей, например в некоторых контекстах вместо правого умножения используется левое. Тем самым можно разделять правые и левые графы Кэли. Очевидно, что данные понятия

совпадают для случая коммутативных полугрупп, в противном случае их можно исследовать с точностью до антиизоморфизма, а принцип двойственности позволяет не воспроизводить соответствующие утверждения для одного из взаимно двойственных случаев. В связи с этим верна

Теорема 40 [45, теорема 5.1]. Нециклическая полугруппа с одним определяющим соотношением и с тождеством допускает внешнепланарный граф Кэли тогда и только тогда, когда она антиизоморфна одной из полугрупп $S_{2,k} = \langle a, b \mid ab = b^k \rangle$ при $k \leqslant 3$, $S_3 = \langle a, b \mid aba = ba \rangle$ или изоморфна полугруппе $S_{2,1} = \langle a, b \mid ab = b \rangle$.

Напомним [79, с. 1269; 80, с. 460], что если дан обыкновенный граф Γ с множеством вершин $V\Gamma = \{a_1, \ldots, a_n\}$, то можно определить свободную частично коммутативную полугруппу как полугруппу $S(\Gamma)$, заданную множеством $\{a_1, \ldots, a_n\}$ образующих элементов и множеством определяющих соотношений вида $a_i a_j = a_j a_i$ для тех и только тех a_i и a_j, которые соединены ребром в графе Γ.

В следующей теореме описывается влияние графа коммутативности множества образующих элементов частично коммутативной свободной полугруппы на внешнепланарность графа Кэли последней. Как оказалось, существенной является валентность вершин графа коммутативности, то есть не только число элементов множества образующих, но и количество коммутирующих пар влияет на внешнепланарность графа Кэли полугруппы.

Теорема 41 [45, теорема 6.1]. Граф Кэли частично коммутативной свободной полугруппы $S(\Gamma)$, соответствующей графу коммутативности Γ множества образующих её элементов, внешнепланарен тогда и только тогда, когда степень любой вершины в графе Γ равна нулю, то есть полугруппа $S(\Gamma)$ некоммутативная.

Перейдем теперь к n-веерным полурешёткам. Напомним, что полурешёткой называется коммутативная полугруппа идемпотентов [56, с. 31].

Будем называть *n-веерной* полурешётку S_k^n с нулём, $1 \leqslant n \leqslant k$, заданную копредставлением

$$\langle a_1, a_2, \ldots, a_k \mid a_i^2 = a_i,\ a_i a_j = a_j a_i,\ a_{i_1} a_{i_2} \ldots a_{i_n} = 0 \rangle,$$

где $(i_1, i_2, \ldots, i_n)$ пробегают все размещения без повторений из k элементов $1, 2, \ldots, k$ по n, а i, j принимают всевозможные значения от 1 до k. Следующая теорема выделяет в классе таких полугрупп все допускающие внешнепланарные графы Кэли полугруппы на языке ограничений количества элементов фиксированной длины.

Теорема 42 [45, теорема 6.2]. n-Веерная полурешётка $S = S_k^n$ допускает внешнепланарный граф Кэли тогда и только тогда, когда $n \leqslant 2$.

Для сравнения приведём полученные в [70] аналогичные характеристические свойства свободных частично коммутативных полугрупп и n-веерных полурешёток с планарными графами Кэли. Приводим этот результат в разделе, посвящённом внешнепланарности, отчасти выбиваясь из общей канвы повествования, потому что, с одной стороны, он не относится ни к одной из ранее выделенных категорий полугрупп с планарными графами Кэли, но с другой — не упомянуть его нельзя, результат интересен оригинальностью доказательства, там есть свежие идеи, связанные с появлением фрактальных графов.

Теорема 43 [70, теорема 1]. Граф Кэли частично коммутативной свободной полугруппы $S(\Gamma)$, соответствующей графу коммутативности Γ множества образующих её элементов, планарен тогда и только тогда, когда степень любой вершины в графе Γ не превосходит единицы.

Теорема 44 [70, теорема 2]. n-Веерная полурешётка $S = S_k^n$ допускает планарный граф Кэли тогда и только тогда, когда $|S^{(2)}| \leqslant 3$, где $S^{(2)}$ — множество всех ненулевых слов полугруппы S вида $a_i a_j$, $i \neq j$.

При изучении вопросов планарности важную роль играют графы K_5 и $K_{3,3}$. В [61] доказано, что если $Cay(S, E)$ — граф Кэли конечной полугруппы S, то $Cay(S, E)$:

1) не изоморфен полному двудольному графу $K_{3,3}$ с любой ориентацией и раскраской (разметкой) рёбер;
2) изоморфен полному графу K_5 с единственной ориентацией рёбер тогда и только тогда, когда S имеет копредставление $S = \langle a, b \mid ab = ba,\ a = b^2 = a^3 b,\ a^2 = ab^2,\ b = a^3 = a^2 b^2 \rangle$.

Продолжая обзор исследований в данном направлении, заметим, что при изучении вопросов внешнепланарности на основании критерия Чартрэнда — Харари ключевая роль отводится графам K_4 и $K_{2,3}$. В следующей теореме показано, что не существует полугрупп, графы Кэли которых изоморфны полному графу K_4 или полному двудольному графу $K_{2,3}$ с некоторой ориентацией и раскраской рёбер.

Теорема 45 [45, теорема 7.1]. Если $Cay(S, E)$ — граф Кэли конечной полугруппы S, то $Cay(S, E)$:

1) не изоморфен полному графу K_4 с любой ориентацией и раскраской рёбер;
2) не изоморфен полному двудольному графу $K_{2,3}$ с любой ориентацией и раскраской рёбер.

Таков список основных результатов, полученных в ходе исследования полугрупп, допускающих внешнепланарные графы Кэли.

3.5. О полугруппах с обобщёнными внешнепланарными графами Кэли

Напомним, что *обобщённым внешнепланарным графом* называется планарный граф, который можно уложить на плоскости таким образом, что каждое ребро обладает хотя бы одной концевой вершиной на границе внешней грани. Обобщённые внешнепланарные графы впервые ввёл в рассмотрение И. Седлачек [81]. Данное понятие сыграло важную роль при изучении локальных свойств графов. Кроме того, Седлачек нашел характеризацию обобщённых внешнепланарных графов в терминах запрещённых подграфов.

Статья [50] открыла цикл работ, посвящённых перечислению полугрупп, допускающих обобщённые внешнепланарные графы Кэли. Первым результатом является теорема, содержащая характеристическое свойство конечных свободных коммутативных полугрупп, графы Кэли которых являются обобщённо внешнепланарными.

Теорема 46 [50, теорема 1]. Граф Кэли конечной свободной коммутативной полугруппы S относительно множества свободных образующих обобщённо внешнепланарен тогда и только тогда, когда S задана копредставлением одного из следующих видов:

1. $S = \langle a \mid a^{r+m} = a^r \rangle$, где r и m — любые натуральные числа.
2. $S = \langle a, b \mid ab = ba,\ a^{r+m} = a^r,\ b^{h+t} = b^h \rangle$, где для натуральных r, m, h, t выполняется хотя бы одно из следующих условий:
   а) $h = 1$, $t = 1$, $m \leqslant 2$; или $r = 1$, $m = 1$, $t \leqslant 2$;
   б) $((h \leqslant 2,\ t = 2)$ или $(h \leqslant 3,\ t = 1))$ при $r + m = 3$; или $((r \leqslant 2,\ m = 2)$ или $(r \leqslant 3,\ m = 1))$ при $h + t = 3$.
3. $S = \langle a, b, c \mid ab = ba,\ ac = ca,\ bc = cb,\ a^2 = a,\ b^2 = b,\ c^2 = c \rangle$.

Заметим, что условие данной теоремы содержит все конечные свободные коммутативные полугруппы, допускающие внешнепланарные графы Кэли, согласно [45, теорема 2.1]. Более того, свободными коммутативными полугруппами, допускающими обобщённо внешнепланарные графы Кэли, но не допускающими внешнепланарные графы Кэли, являются полугруппы, имеющие копредставления

$$S = \langle a, b \mid ab = ba,\ a^{r+m} = a^r,\ b^{h+t} = b^h \rangle,$$

где ($(h = 2,\ t = 2)$ или $(h = 3,\ t = 1)$) при $r + m = 3$; либо ($(r = 2,\ m = 2)$ или $(r = 3,\ m = 1)$) при $h + t = 3$; или

$$S = \langle a, b, c \mid ab = ba,\ ac = ca,\ bc = cb,\ a^2 = a,\ b^2 = b,\ c^2 = c \rangle,$$

и только они.

Далее под циклической полугруппой с нулём понимается любой гомоморфный образ свободной однопорождённой полугруппы с нулём. Очевидно, что любая циклическая полугруппа с нулём изоморфна либо циклической ниль-полугруппе, либо получена из циклической полугруппы внешним присоединением нуля. Конечная полугруппа с нулём называется свободной коммутативной, если она является коммутативно-свободным произведением циклических полугрупп с нулём.

Следующая теорема содержит характеристическое свойство конечных свободных коммутативных полугрупп с нулём, графы Кэли которых являются обобщённо внешнепланарными.

Теорема 47 [50, теорема 2]. Граф Кэли конечной свободной коммутативной полугруппы S с нулём относительно множества свободных образующих обобщённо внешнепланарен тогда и только тогда, когда S задана копредставлением одного из следующих видов:

1. $S = \langle a \mid a^r = 0 \rangle$, где r — любое натуральное число.
2. $S = \langle a, b \mid ab = ba,\ a^r = 0,\ b^h = 0 \rangle$, где r, h — натуральные числа, причём $r = 1$, или $h = 1$, или $r + h \leqslant 5$.
3. $S = \langle a, b \mid ab = ba,\ a^{r+m} = a^r,\ b^h = 0 \rangle$, где для натуральных r, m, h выполняется хотя бы одно из следующих условий:
   а) при $m = 1$ имеем $h = 1$, или $r = 1$, или $r + h \leqslant 5$;
   б) при $m = 2$ имеем $h = 1$, или $r + h \leqslant 4$;
   в) при $m = 3$ имеем $h = 1$;
   г) при $m \geqslant 4$ имеем $r = 1$ и $h = 1$.
4. $S = \langle a, b, c \mid ab = ba,\ ac = ca,\ bc = cb,\ a^2 = a,\ b^2 = b,\ c = 0 \rangle$.

Далее перечислены все конечные свободные коммутативные моноиды, допускающие обобщённые внешнепланарные графы Кэли.

Теорема 48 [51, теорема 2]. Граф Кэли конечного свободного коммутативного моноида S обобщённо внешнепланарен тогда и только тогда, когда S в классе всех коммутативных моноидов имеет копредставление одного из следующих видов:

1. $S = \langle a \mid a^m = 1 \rangle$, где m — любое натуральное число.
2. $S = \langle a, b \mid a^{r+m} = a^r,\ b^t = 1 \rangle$, либо $S = \langle a, b \mid a^m = 1,\ b^t = 1 \rangle$, где для натуральных r, m, t выполнено одно из следующих ограничений:
   а) $t = 1$;
   б) $m \leqslant 2$, $t = 2$.
3. $S = \langle a, b, c \mid a^{r+m} = a^r,\ b^2 = b,\ c = 1 \rangle$, где r, m — натуральные числа, $m \leqslant 2$.

Ранее приведены условия, при которых рассыпчатые полугруппы допускают планарные и, в частности, внешнепланарные графы Кэли. Следующая теорема характеризует рассыпчатые полугруппы, допускающие обобщённые внешнепланарные графы Кэли.

Теорема 49 [52, теорема 1]. Пусть S — рассыпчатая полугруппа и $S = \bigcup\limits_{e\in P} S_e$ — соответствующая ординальная сумма сингулярных полугрупп. Тогда S допускает обобщённый внешнепланарный граф Кэли тогда и только тогда, когда выполняется одно из следующих условий:

1. $|P| = 1$ и $|S| < 5$, если S — полугруппа правых нулей или S — полугруппа левых нулей.
2. $|P| = 2$ и выполнено одно из условий:
   а) обе компоненты являются полугруппами правых нулей и $|S| < 5$;
   б) только одна из компонент S_e является полугруппой правых нулей и $|S_e| \leqslant 3$, а другая компонента одноэлементная (при $|S_e| = 3$);
   в) обе компоненты — полугруппы левых нулей и одна из них содержит менее трёх элементов.
3. $|P| = 3$ и выполнено одно из условий:
   а) все компоненты — полугруппы правых нулей и $|S| < 5$;
   б) две из компонент содержат по одному элементу, а третья компонента — полугруппа левых нулей;
   в) все компоненты являются полугруппами левых нулей и $|S| \leqslant 5$.
4. $|P| = 4$ и $|S| = 4$.

3.6. О гиперграфах полугрупп

На пути исследования вопросов планарности графов Кэли полугрупп могут появляться комбинаторные проблемы, например имеет место

Гипотеза 1 [82]. Граф Кэли мультипликативной полугруппы кольца вычетов по модулю n планарен тогда и только тогда, когда $n < 9$ или n — простое число.

В то же время подобные утверждения носят частный характер, поэтому удобнее распространить известное понятие графов Кэли до гиперграфов алгебр. В частности, оказалось возможным всякой модели сопоставить гиперграф, множеством вершин которого служит основное множество модели, а гиперрёбрами — элементы (кортежи) отношений модели [83].

Так как всякая n-местная алгебраическая операция представляется $(n+1)$-местным отношением, то данное определение применимо и для алгебр [84], более того, установлен механизм структурного описания моделей теорий по семействам гиперграфов простых моделей произвольной малой теории [85]; поэтому, направление видится весьма перспективным. Кёнигово представление гиперграфов [86, с. 93] алгебр при таком подходе является двудольным графом, следовательно, более доступно для изучения свойств ацикличности и внешнепланарности. Особый интерес вызывают гиперграфы полугрупп, обладающие перечисленными далее свойствами 1°–3°, отражающими их тесную связь с графами Кэли. Необходимый минимум понятий теории гиперграфов можно почерпнуть из работы [86].

Дадим конструктивное определение гиперграфа полугруппы S относительно множества образующих её элементов X: каждой полугруппе сопоставлен гиперграф $HCay(S, X)$, множеством вершин которого служит основное множество элементов по-

лугруппы S, а гиперрёбрами — всевозможные тройки вида (a, x, b), где $a, b \in S$, $x \in X$ и $ax = b$.

Некоторые свойства гиперграфа устанавливаются через одноименные свойства кёнигова представления. Напомним, что кёниговым представлением гиперграфа называется двудольный граф, отражающий отношение инцидентности элементов гиперграфа. Этот граф несёт полную информацию о гиперграфе и однозначно его определяет. Поэтому вполне естественно называть гиперграф плоским или планарным, если его кёнигово представление является планарным графом.

Таким образом, *гиперграф* $HCay(S, X)$ *полугруппы* S относительно множества образующих её элементов X представляется кёниговым двудольным графом, у которого множество вершин одной из долей является основным множеством элементов s_i полугруппы S, а множество вершин другой доли исчерпывается всевозможными тройками $e_j = (a_j, x_j, b_j)$, где $a_j, b_j \in S$, $x_j \in X$ и $a_j x_j = b_j$; при этом вершина s_i соединена дугой с вершиной $e_j = (a_j, x_j, b_j)$ тогда и только тогда, когда $s_i \in (a_j, x_j, b_j)$, то есть гипервершина s_i принадлежит гиперребру e_j в гиперграфе $HCay(S, X)$. Для удобства восприятия дуга $(s_i;\ e_j)$ помечается порядковым номером компоненты s_i в упорядоченной тройке e_j. *Основой* ориентированного помеченного мультиграфа мы называем обыкновенный граф, полученный из данного удалением меток, петель и заменой всех дуг, соединяющих две вершины, одним ребром, соединяющим эти вершины.

Некоторые свойства гиперграфов полугрупп:

1°) Гиперграф моногенной полугруппы планарен.

2°) Существуют полугруппы, допускающие планарный граф Кэли, но не допускающие планарный гиперграф.
Примером может служить мультипликативная полугруппа кольца вычетов по модулю 8, порождаемая тремя элементами ($\mathbb{Z}_8 = \langle 2, 3, 5\rangle$) и допускающая планарный граф Кэли, в то время как её гиперграф планарным не является, в силу теоремы о них.

3°) Если гиперграф полугруппы планарен, то её граф Кэли тоже планарен.
В самом деле, каждому ребру графа Кэли соответствует подграф кёнигова представления гиперграфа. Следовательно, если в кёниговом представлении гиперграфа отсутствует подграф, гомеоморфный K_5 или $K_{3,3}$, то он отсутствует и в графе Кэли, то есть планарность наследуется.

Таким образом, полугруппы с планарными гиперграфами образуют класс более узкий, чем полугруппы, допускающие планарные графы Кэли. Более того, имеет место следующая

Теорема 50 [82]. Гиперграф мультипликативной полугруппы $\mathbb{Z}_n$ кольца вычетов по модулю n планарен тогда и только тогда, когда $n = 1$ или $\mathbb{Z}_n = \big\langle a, b \mid a^l = 0,\ b^k = 1,\ ab = a\big\rangle$, $l, k \in \mathbb{N}$.

Заметим, что примером допускающей планарный гиперграф 2-порождённой мультипликативной полугруппы кольца вычетов по модулю n, порождающие элементы a, b которой удовлетворяют равенству $ab = a$, служит $\mathbb{Z}_4 = \langle 2, 3\rangle$. Кроме того, условие теоремы выполнено, если n — простое число, так как $0\beta = 0$ и $\mathbb{Z}_p = \langle 0, \beta\rangle$ для любого простого p, где β — первообразный корень сравнения $\beta^{p-1} \equiv 1 \pmod p$.

Следствие 1 [82]. Гиперграф мультипликативной полугруппы кольца вычетов по модулю n внешнепланарен тогда и только тогда, когда $n < 3$.

3.7. О других полугруппах с планарными графами Кэли

В [71] изучаются свободные частично коммутативные нильпотентные полугруппы, допускающие планарные графы Кэли. Если дан обыкновенный граф Γ с множеством вершин $V\Gamma = \{a_1, \ldots, a_t\}$, то можно определить свободную частично коммутативную полугруппу как полугруппу $S(\Gamma)$, заданную множеством $\{a_1, \ldots, a_t\}$ образующих элементов и множеством определяющих соотношений вида $a_i \cdot a_j = a_j \cdot a_i$ для тех и только тех a_i и a_j, которые соединены ребром в графе Γ. Для любого натурального числа n фактор-полугруппу Риса $S(\Gamma)/S^n$ назовём *свободной частично коммутативной n-нильпотентной полугруппой, определяемой графом* Γ *порядка* t; условимся обозначать эту полугруппу через $S_t^n(\Gamma)$. Справедлива следующая теорема, приближающая нас к исследованию вопросов планарности графов Кэли свободных полугрупп квазимногообразий.

Теорема 51 [71, теорема 1]. Полугруппа $S_t^n(\Gamma)$ допускает планарный граф Кэли, если и только если выполнено хотя бы одно из следующих условий:

1) Γ — пустой граф;
2) связными компонентами графа Γ являются паросочетания или изолированные вершины и $n \leqslant 5$;
3) связными компонентами графа Γ являются цепи или изолированные вершины и $n \leqslant 4$;
4) связными компонентами графа Γ являются «деревья» из простых циклов (кактусы) или изолированные вершины и $n \leqslant 3$;
5) Γ — любой граф и $n \leqslant 2$, либо $n > 2$ и $t \leqslant 2$.

Для полноты картины о разнообразии результатов в данной области и в качестве иллюстрации к вариациям на тему основного определения графа Кэли полугруппы приведём следующую теорему.

Теорема 52 [87]. Нециклическая полугруппа с одним определяющим соотношением и с тождеством допускает планарный граф Кэли тогда и только тогда, когда она антиизоморфна одной из полугрупп: $S_1 = \langle a, b \mid ab = ba\rangle$, $S_{2,k} = \langle a, b \mid ab = b^k\rangle$, $k = 1, 2, \ldots$, $S_3 = \langle a, b \mid aba = ba\rangle$, $S_4 = \langle a, b \mid aba = b\rangle$, $S_5 = \langle a, b \mid a^2 = b^2\rangle$, $S_6 = \langle a, b \mid aba^2 = ba\rangle$, или изоморфна одной из полугрупп: S_1, $S_{2,1}$, S_4, S_5.

При исследовании вопроса планарности графов важную роль играют непланарные графы K_5 или $K_{3,3}$. С другой стороны, максимальными плоскими графами (графами, которые перестают быть плоскими при добавлении любого ребра) являются плоские триангуляции (графы, каждая грань которых — треугольник). Поэтому при изучении конечных полугрупп со свойством планарности графов Кэли возникает задача перечисления всех полугрупп, графы Кэли которых являются упомянутыми с некоторой ориентацией рёбер.

В [61], в частности, решена задача о допустимости графов $K_{3,3}$, K_5 и плоских триангуляций в качестве графов Кэли конечных полугрупп.

Теорема 53 [61]. Если $Cay(S, X)$ — граф Кэли конечной полугруппы S, то $Cay(S, X)$:

1) не изоморфен полному двудольному графу $K_{3,3}$ с любой ориентацией и пометкой рёбер;
2) изоморфен плоской триангуляции с единственной ориентацией рёбер тогда и только тогда, когда S имеет копредставление

$$S = \langle a \mid a^4 = a\rangle;$$

3) изоморфен полному графу K_5 с единственной ориентацией рёбер тогда и только тогда, когда S имеет копредставление

$$S = \langle a, b \mid ab = ba,\ a = b^2 = a^3b,\ a^2 = ab^2,\ b = a^3 = a^2b^2 \rangle.$$

Заметим, что, в продолжение начатого в [61] исследования вопроса о допустимости некоторых графов в качестве графов Кэли полугрупп, в [88] показано, что графом Кэли полугруппы S является плоская триангуляция, изоморфная графу октаэдра, с некоторой (не единственной) ориентацией и пометкой рёбер тогда и только тогда, когда полугруппа S является циклической полугруппой $S \cong \langle a \mid a^7 = a \rangle$ относительно множества образующих элементов $\{a, a^2\}$ или $\{a, a^4\}$, либо полугруппой $S \cong \langle a, b \mid a^4 = a,\ b^4 = b,\ a^2 = ba,\ b^2 = ab \rangle$.

Кроме того, полугруппа S, указанная в условии 3 теоремы 53, является циклической группой порядка 5 (при выборе одного образующего она имеет копредставление $S = \langle a \mid a^6 = a \rangle$) и поэтому допускает планарный граф Кэли. Данное замечание иллюстрирует известный факт, что свойство планарности графа Кэли полугруппы существенно зависит от выбора множества образующих. В связи с этим естественно рассматривать графы относительно минимального по включению множества образующих.

Изучению свойства планарности графов Кэли в классе полугрупп, совпадающих с любым своим минимальным множеством образующих, посвящена работа [78]. Нетрудно показать, что этот класс совпадает с классом всех рассыпчатых полугрупп, то есть таких полугрупп S, в которых для любых элементов a, b из S выполняется $ab = a$ или $ab = b$.

Результатом из данной серии является

Теорема 54 [78, теорема 1]. Пусть S — рассыпчатая полугруппа и $S = \bigcup\limits_{e \in P} S_e$ — соответствующая ординальная сумма сингулярных полугрупп. Тогда S допускает планарный граф Кэли, если и только если выполняется одно из следующих условий:

1. $|P| = 1$ и $|S| < 5$, если S — полугруппа правых нулей.
2. $|P| = 2$ и выполнено одно из условий:
   а) обе компоненты — полугруппы правых нулей и $|S| < 5$;
   б) только одна из компонент S_e является полугруппой правых нулей и $|S_e| \leqslant 3$, а другая компонента содержит менее трёх элементов (при $|S_e| = 3$);
   в) обе компоненты — полугруппы левых нулей, и одна из них содержит менее трёх элементов.
3. $|P| = 3$ и выполнено одно из условий:
   а) все компоненты — полугруппы правых нулей и $|S| < 5$;
   б) две из компонент содержат по одному элементу, а третья компонента — полугруппа левых нулей;
   в) все компоненты являются полугруппами левых нулей и $|S| \leqslant 5$ или $|S_e| = 2$ для любого $e \in P$.
4. $|P| = 4$ и $|S| \leqslant 5$.

Прямоугольной полугруппой называется полугруппа, изоморфная прямому произведению $L \times R$, где L — левосингулярная, а R — правосингулярная полугруппа.

Теорема 55 [88]. Пусть S — ординальная сумма прямоугольных полугрупп. Тогда S допускает планарный граф Кэли, если и только если выполняется одно из следующих условий:

1. $|P| = 1$ и $S = (L_i \times R_j)$, где $1 \leqslant j < 5,\ i \geqslant 1$.
2. $|P| = 2$ и выполнено хотя бы одно из условий:
   а) одна из компонент — R_1, а другая — $(L_i \times R_j)$, где $1 \leqslant j \leqslant 3$, $i \geqslant 1$;
   б) одна из компонент — R_2, а другая — $(L_i \times R_j)$, где $1 \leqslant j \leqslant 2$, $i \geqslant 1$, причём если R_2 — бóльшая, то возможно $j = 3$, $i \geqslant 2$;
   в) одна из компонент — L_2 либо $(L_2 \times R_2)$ — является меньшей, а другая — $(L_i \times R_j)$, где $1 \leqslant j \leqslant 2$, $i \geqslant 1$ либо $j = 3$, $i = 1$, причём если L_2 — бóльшая, то возможно $j = 3$, $i \geqslant 2$;
   г) меньшая из компонент является произведением $(L_i \times R_j)$, где $1 \leqslant j \leqslant 4$, $i \geqslant 2$, бóльшая — R_1, R_2 либо L_2.
3. $|P| = 3$ и выполнено хотя бы одно из условий:
   а) две из компонент одноэлементные, а третья — $(L_i \times R_j)$, где $1 \leqslant j \leqslant 4$, $i \geqslant 2$ для меньшей компоненты, $1 \leqslant j \leqslant 3$, $i \geqslant 2$ — для средней, $1 \leqslant j \leqslant 2$, $i \geqslant 1$ — для большей;
   б) компонентами ординальной суммы одновременно являются R_1, R_2 (либо L_2) и L_2, причём вместо L_2 меньшей или средней компонентой возможна $(L_2 \times R_2)$;
   в) все компоненты — L_2, либо меньшая из них — $(L_2 \times R_2)$.
4. $|P| = 4$ и выполнено хотя бы одно из условий:
   а) все компоненты — полугруппы левых нулей и $|S| \leqslant 5$;
   б) три из компонент одноэлементные, а $(L_2 \times R_2)$ — не наибольшая.

4. О рангах планарности многообразий полугрупп

Результаты этого раздела принадлежат исключительно автору.

За время всестороннего исследования понятия ранга планарности многообразия полугрупп сделано много открытий, среди которых можно выделить следующие теориообразующие:

1) описаны ранги планарности многообразий коммутативных моноидов и приведена классификация многообразий коммутативных моноидов по рангам планарности [60];
2) найдены все планарные многообразия полугрупп, в частности вычислены ранги планарности многообразий из решётки, порождённой негрупповыми атомами [89];
3) описаны ранги планарности коммутативных полугрупп и вычислены ранги планарности некоторых серий многообразий коммутативных полугрупп [90, 91];
4) найдены ранги планарности многообразия всех полугрупп идемпотентов и многообразий полугрупп, заданных перестановочным тождеством [92];
5) в классе многообразий ниль-полугрупп указана континуальная серия многообразий бесконечного ранга планарности и континуальная серия многообразий конечного ранга планарности [93];
6) описаны ранги планарности многообразий полугрупп [94].

Определённый интерес представляет также вопрос о том, какие составленные из натуральных чисел и символа ∞ наборы значений могут быть наборами значений рангов планарности нетривиальных подмногообразий $\boldsymbol{X}$ произвольного многообразия $\boldsymbol{V}$ полугрупп. Л. М. Мартынов предложил называть этот вопрос «Проблема спектров рангов планарности многообразий полугрупп».

Например, в силу теоремы 60, спектр рангов планарности многообразия всех полугрупп является полным. Последнее открывает обширные горизонты для дальнейших

исследований. В частности, в процессе написания обзора были найдены ранги планарности каждого из многообразий бесконечной счётной решётки всех многообразий связок.

4.1. Ранги планарности многообразий коммутативных моноидов и полугрупп

При доказательстве результатов данного подраздела использованы методы структурной теории полугрупп, теории многообразий и теории графов.

В частности, широко применяется критерий Понтрягина — Куратовского. Первый эффективный алгоритм (линейной временной сложности) для проверки графа на планарность принадлежит Д. Хопкрофту и Р. Тарьяну [95], и как рисовать планарные графы за линейное время, известно давно [96].

Автором получен результат, касающийся моноидов. Для его формулировки приведём некоторые обозначения из [60]:

- $\mathbf{M}$ — многообразие всех коммутативных моноидов;
- $\mathbf{A}_m = \mathrm{var}\{x^m \approx 1\}$ — многообразие всех абелевых групп экспоненты m, являющееся подмногообразием многообразия $\mathbf{M}$;
- $\mathbf{S}^1_{i,m} = \mathrm{var}\{x^{i+m} \approx x^i\}$ — многообразие коммутативных моноидов типа (i, m), являющееся подмногообразием многообразия $\mathbf{M}$.

С использованием развитого в [73] инструментария в [60] доказана следующая

Теорема 56 [60]. Пусть $\boldsymbol{V}$ — нетривиальное многообразие коммутативных моноидов, $r_\pi(\boldsymbol{V})$ — его ранг планарности. Тогда $r_\pi(\boldsymbol{V}) \leqslant 3$. Более того:

1) $r_\pi(\boldsymbol{V}) = 1$ тогда и только тогда, когда $\boldsymbol{V} = \mathbf{A}_m$ или $\boldsymbol{V} = \mathbf{S}^1_{i,m}$, где $m > 2$, $i \geqslant 1$, $n > 2$;
2) $r_\pi(\boldsymbol{V}) = 2$ тогда и только тогда, когда $\boldsymbol{V} = \mathbf{M}$, или $\boldsymbol{V} = \mathbf{S}^1_{i_1,1}$, или $\boldsymbol{V} = \mathbf{S}^1_{i_2,2}$, где $i_1 \geqslant 2$, $i_2 \geqslant 1$;
3) $r_\pi(\boldsymbol{V}) = 3$ тогда и только тогда, когда $\boldsymbol{V} = \mathbf{A}_2$ или $\boldsymbol{V} = \mathbf{S}^1_{1,1}$.

Таким образом, из теоремы 56 вытекает, что $\mathrm{Spec}_{r\pi}(\mathbf{M}) = \{0, 1, 2, 3\}$. Эта теорема не только решает проблему рангов планарности для многообразий коммутативных моноидов [97], но и приводит классификацию многообразий коммутативных моноидов по рангам планарности.

Следующая теорема посвящена указанию рангов планарности некоторых многообразий коммутативных полугрупп. Для формулировки результата приведём следующие обозначения:

- $\mathbf{C} = \mathrm{var}\{xy \approx yx\}$ — многообразие всех коммутативных полугрупп;
- $\mathbf{A}_n = \mathrm{var}\{x^n y \approx y, xy \approx yx\}$ — многообразие всех абелевых групп экспоненты $n > 1$;
- $\mathbf{CB}_{r,m} = \mathrm{var}\{x^{r+m} \approx x^r, xy \approx yx\}$ — многообразие всех коммутативных полугрупп бернсайдовского типа, где $r > 0$, $m > 0$;
- $\mathbf{CN}_s = \mathrm{var}\{x_1 x_2 \dots x_s y \approx x_1 x_2 \dots x_s, xy \approx yx\}$ — многообразие коммутативных нильпотентных полугрупп ступени $s > 1$;
- $\mathbf{CNil}_r = \mathrm{var}\{x^r y \approx x^r, xy \approx yx\}$ — многообразие всех коммутативных ниль-полугрупп индекса $r > 1$.

Справедлива следующая

Теорема 57 [90, 91, теорема 1]. Нетривиальное многообразие коммутативных полугрупп либо имеет бесконечный ранг планарности и при этом совпадает с многообразием полугрупп с нулевым умножением, либо имеет ранг планарности 1, 2 или 3:

1) $r_\pi(\mathbf{C}) = 2$;

2) $r_\pi(\mathbf{A}_2) = 3$ и $r_\pi(\mathbf{A}_n) = 1$ при $n > 2$;
3) $r_\pi(\mathbf{CB}_{1,1}) = 3$, $r_\pi(\mathbf{CB}_{r,m}) = 1$ при $r > 0$, $m > 2$, и $r_\pi(\mathbf{CB}_{r,m}) = \infty$ в остальных случаях;
4) $r_\pi(\mathbf{CN}_2) = \infty$, $r_\pi(\mathbf{CN}_3) = 3$, $r_\pi(\mathbf{CN}_s) = 2$ при $s > 3$;
5) $r_\pi(\mathbf{CNil}_r) = 2$ при любом $r > 1$.

Приведём несколько конфигураций, возникающих в процессе доказательства теоремы 57. Условимся обозначать свободную n-порождённую полугруппу многообразия $\boldsymbol{V}$ над n-элементным множеством образующих $X \subseteq \{x, y, z, t, x_1, x_2, \ldots, x_n, \ldots\}$, являющимся подмножеством бесконечного счётного алфавита, как $F_{\boldsymbol{V}}\langle X\rangle$. Граф Кэли свободной полугруппы многообразия $\operatorname{var}\{xy \approx yx, x^{1+m} \approx x^1\}$ с тремя образующими содержит изображённый на рис. 1 подграф, основа которого гомеоморфна графу $K_{3,3}$. Следовательно, этот граф не является планарным, а ранг планарности такого многообразия не превышает 2 и тем более 3.

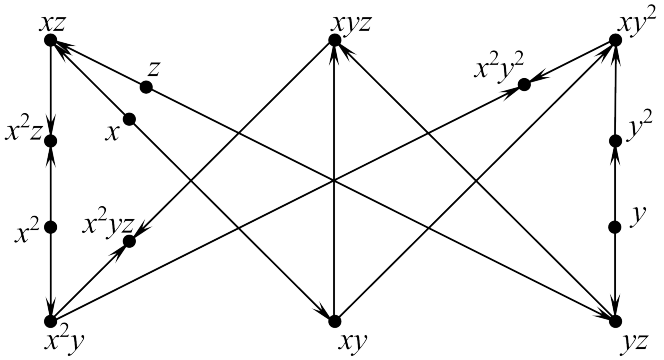


Рис. 1. Подграф графа Кэли свободной 3-порождённой полугруппы $F_{\boldsymbol{V}}\langle\{x, y, z\}\rangle$ коммутативного многообразия $\boldsymbol{V} = \operatorname{var}\{xy \approx yx, x^{1+m} \approx x^1\}$ при $m > 1$

Выполнение хотя бы одного из соотношений $x^2z = z$, $x^2y = y$ или $x = xy^2$ приводит к тому, что выполнено тождество $x^2y = y$, из которого следует $x^2z = z$, что приводит к $x^2 = xxy^2 = x^2yy = y^2$ — многообразию полугрупп, задаваемых системой тождеств $\operatorname{var}\{xy \approx yx, x^{1+m} \approx x, x^2 \approx y^2\}$, ранг планарности которого ограничен 3, согласно рис. 2, на котором изображён подграф, основа которого гомеоморфна графу K_5.

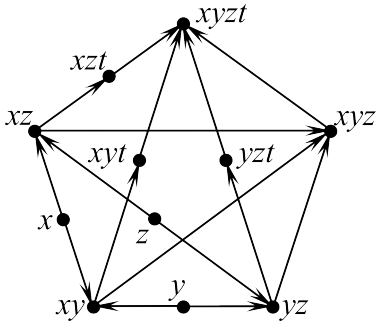


Рис. 2. Подграф графа Кэли свободной 4-порождённой полугруппы $F_{\boldsymbol{V}}\langle\{x, y, z, t\}\rangle$ коммутативного многообразия $\boldsymbol{V} = \operatorname{var}\{xy \approx yx, x^{1+m} \approx x^1\}$ при $m \geqslant 1$

При доказательстве теоремы 57 существенным образом использованы результаты из работы [60].

Следующая теорема посвящена нахождению рангов планарности многообразий полугрупп идемпотентов, ниль-полугрупп и полугрупп с перестановочным тождеством.

Теорема 58 [92]. Ранг планарности многообразия всех полугрупп идемпотентов равен 3; ранг планарности многообразия ниль-полугрупп, заданного тождеством $w \approx 0$, равен бесконечности; ранг планарности любого перестановочного многообразия полугрупп равен 1 или 2.

Позже был получен более общий результат о ниль-многообразиях, приведём его в подразделе 4.2.

В случае многообразий всех нильпотентных полугрупп $\mathbf{N}_l$ данной ступени нильпотентности l легко видеть, что $\mathrm{Spec}_{r\pi}(\mathbf{N}_2) = \{0, \infty\}$, так как многообразие $\mathbf{N}_2$ является планарным и является атомом решётки многообразий полугрупп (аналогично $\mathrm{Spec}_{r\pi}(\mathbf{L}_0) = \{0, \infty\}$, $\mathrm{Spec}_{r\pi}(\mathbf{R}_0) = \{0, 4\}$, $\mathrm{Spec}_{r\pi}(\mathbf{A}_2) = \{0, 3\}$, $\mathrm{Spec}_{r\pi}(\mathbf{A}_{p>2}) = \{0, 1\}$).

Кроме того, $\mathrm{Spec}_{r\pi}(\mathbf{N}_3) = \{0, 3, \infty\}$, так как не 0-приведённые подмногообразия многообразия $\mathbf{N}_3$ исчерпываются многообразиями: $\mathbf{CN}_3 = \mathrm{var}\{xyz \approx 0; xy \approx yx\}$ всех коммутативных нильпотентных полугрупп ступени 3, для которого ранг планарности $r_\pi(\mathbf{CN}_3) = 3$, и $\mathrm{var}\{xyz \approx 0; x^2 \approx 0; xy \approx yx\}$, ранг планарности которого также равен 3; каждое из оставшихся 0-приведённых подмногообразий многообразия $\mathbf{N}_3$ имеет бесконечный ранг планарности.

Разнообразие ситуации с рангами демонстрирует теорема 57: $\mathrm{Spec}_{r\pi}(\mathbf{C}) = \{0, 1, 2, 3, \infty\}$.

4.2. О рангах планарности ниль-многообразий

В следующей теореме приведены бесконечные серии многообразий ниль-полугрупп бесконечного и конечного рангов планарности.

Теорема 59 [93]. Ранг планарности 0-приведённого многообразия ниль-полугрупп бесконечен. Кроме того, если система тождеств, определяющая многообразие ниль-полугрупп, среди не эквивалентных системе 0-приведённых тождеств имеет только одно тождество минимальной длины вида $u_1xu_2yu_3 \approx v_1yv_2xv_3$, где слова u_i, v_j — не обязательно различные, возможно, пустые для некоторых многообразий, а u_1v_1 не содержит символы x и y, то ранг планарности такого многообразия конечен.

Доказательство теоремы 59 опирается на следующие утверждения:

Лемма 1 [93, лемма 1]. Фактор-полугруппа Риса свободной полугруппы по любому идеалу допускает планарный граф Кэли.

Следствие 2 [93, следствие 1]. Ранг планарности любого 0-приведённого многообразия равен бесконечности.

Множество 0-приведённых многообразий имеет мощность континуума, поэтому справедливо

Следствие 3 [93, следствие 2]. Множество полугрупповых многообразий бесконечного ранга планарности имеет континуальную мощность.

Кроме того, из теоремы 59 вытекает и обслуживаемое одной конфигурацией следующее

Следствие 4 [93, следствие 3]. Множество полугрупповых ниль-многообразий конечного ранга планарности имеет континуальную мощность.

Заметим, что бывают и не 0-приведённые многообразия ниль-полугрупп бесконечного ранга, например $r_\pi(\mathrm{var}\{xyy \approx xyx, x^m \approx 0\}) = \infty$, где $m > 2$. Однако до настоящего времени не было известно ни одного многообразия полугрупп с конечным рангом

планарности более чем 4. Тем неожиданнее оказалась справедливость результата [94], из которого вытекает существование полугрупповых многообразий любого наперёд заданного конечного ранга планарности, что вместе с предыдущими результатами автора решает проблему описания рангов планарности подмногообразий многообразия всех полугрупп, сформулированную Л. М. Мартыновым в [30].

Теорема 60 [94]. Ранг планарности любого многообразия полугрупп либо бесконечен, либо может быть любым натуральным числом.

Из теоремы 60, в частности, вытекает, что спектр рангов планарности многообразий всех полугрупп является полным, то есть $\mathrm{Spec}_{r\pi}(\mathbf{S}) = \mathbb{N}^\infty$, где $\mathbf{S}$ — это многообразие всех полугрупп.

Многообразие всех ниль-полугрупп данного конечного ниль-индекса k с одним перестановочным тождеством длины n, переставляющим элементы в позициях i, j, обозначим через $\mathbf{Nil}_k\mathbf{P}_n^{(i;j)}$. Тогда из того, что при доказательстве теоремы 59 обнаруживаются конфигурации, содержащие вхождения элементов в степени не выше 4, вытекает

Следствие 5 [94, следствие 1]. При $k > 4$ существуют подмногообразия многообразия всех ниль-полугрупп $\mathbf{Nil}_k$ ранга планарности 1 и 2, примеры которых доставляют многообразия $\mathbf{Nil}_k\mathbf{P}_3^{(1;2)}$ и $\mathbf{Nil}_k\mathbf{P}_3^{(2;3)}$ с соответствующим перестановочным тождеством.

В качестве комментария к теореме 60 напомним, что многообразия бесконечного ранга планарности присутствуют в теоремах 59 и 60. Многообразия полугрупп конечных рангов планарности 1, 2, 3 содержат предыдущие результаты автора. Наконец, многообразия полугрупп

$$\mathbf{Nil}_2\mathbf{P}_n^{(1;2)} = \mathrm{var}\{x^2 \approx 0,\ xyx \approx 0,\ x_1x_2x_3x_4\dots x_n \approx x_2x_1x_3x_4\dots x_n\}$$

при каждом $n > 3$ имеют ранг планарности $n - 1$.

Плоская укладка основы графа Кэли свободной $(n-1)$-порождённой полугруппы этого многообразия получается следующим образом: отправной точкой берётся лес, как для всякого 0-приведённого многообразия; в силу внешнепланарности леса можно добавить к нему изолированную вершину 0 и все остальные вершины леса соединить ребром с 0 так, чтобы планарность сохранилась [45]. Теперь рассмотрим свободную n-порождённую полугруппу многообразия $\mathbf{Nil}_2\mathbf{P}_n^{(1;2)}$. При достаточном количестве образующих начинает работать тождество вида $x_1x_2x_3x_4\dots x_n \approx x_2x_1x_3x_4\dots x_n$, которое в случае $(n-1)$-порождённой полугруппы вырождается, поскольку в любой $(n-1)$-порождённой полугруппе многообразия $\mathbf{Nil}_2\mathbf{P}_n^{(1;2)}$ любое слово длины n равно 0. В результате образуется достаточно склеек слов длины n в свободной n-порождённой полугруппе $F_n(\mathbf{Nil}_2\mathbf{P}_n^{(1;2)})$ многообразия $\mathbf{Nil}_2\mathbf{P}_n^{(1;2)}$, при $n > 3$ приводящих к появлению в основе графа Кэли этой полугруппы относительно множества образующих $X_n = \{x_1, x_2, \dots, x_n\}$ подграфа, гомеоморфного полному двудольному графу $K_{3,3}$.

Непосредственно из доказательства теоремы 60 вытекает

Следствие 6 [94, следствие 2]. Натуральное число $n \geqslant 3$ и значение ∞ могут быть рангами планарности подмногообразий многообразия $\mathbf{Nil}_k = \mathrm{var}\{x^k \approx 0\}$ всех ниль-полугрупп данного конечного ниль-индекса k при любом $k \geqslant 2$.

Ввиду следствия 6 и того факта, что примеры, обеспечивающие ранги планарности 1 и 2, описаны в следствии 5 из теоремы 58, спектр рангов планарности многообразий всех ниль-полугрупп $\mathbf{Nil}_k$ данного конечного ниль-индекса $k > 4$ является полным, то есть $\mathrm{Spec}_{r\pi}(\mathbf{Nil}_k) = \mathbb{N}^\infty$.

Отметим, что многообразия $\mathbf{Nil}_2\mathbf{P}_n^{(1;2)}$ при $n > 3$ не единственны в своём роде. Примеры иных серий полугрупповых многообразий конечного наперёд заданного ранга планарности получаются по аналогии добавлением к тождествам $x^2 \approx 0$, $xyx \approx 0$ других перестановочных тождеств фиксированного порядка $n > 3$ и их наборов, а именно: справедливо

Предложение 1 [94]. Для любого натурального числа $n > 3$ справедливы следующие утверждения:

1) ранг планарности многообразия $\mathbf{Nil}_2\mathbf{P}_n^{(n-1;n)}$ полугрупп, заданного системой тождеств $\{x^2 \approx 0,\ xyx \approx 0,\ x_1 \dots x_{n-2}x_{n-1}x_n \approx x_1 \dots x_{n-2}x_nx_{n-1}\}$, равен n;
2) ранг планарности многообразия $\mathbf{Nil}_2\mathbf{P}_n^{(i;j)}$ полугрупп, заданного системой тождеств

$$\{x^2 \approx 0,\ xyx \approx 0,\ x_1 \dots x_{i-1}x_ix_{i+1} \dots x_{j-1}x_j \dots x_n \approx x_1 \dots x_{i-1}x_jx_{i+1} \dots x_{j-1}x_i \dots x_n\} \tag{1}$$

при $i + 1 \neq n$, равен $n - 1$;
3) ранг планарности многообразия $\mathbf{Nil}_2\mathbf{P}_n^{(i;j)}$ полугрупп, заданного системой тождеств (1) при $j \neq n$, равен $n - 1$;
4) ранг планарности многообразия $\mathbf{Nil}_2\mathbf{P}_n^{S_{n-1}}$ полугрупп, заданного системой тождеств $\{x^2 \approx 0,\ xyx \approx 0,\ x_1x_2 \dots x_{n-1}x_n \approx x_{\pi(1)}x_{\pi(2)} \dots x_{\pi(n-1)}x_n : \pi \in S_{n-1}\}$, где S_{n-1} — симметрическая группа подстановок на $(n-1)$-элементном множестве, равен $n - 1$;
5) ранг планарности многообразия $\mathbf{Nil}_2\mathbf{P}_n^{S_n}$ полугрупп, заданного системой тождеств $\{x^2 \approx 0,\ xyx \approx 0,\ x_1x_2 \dots x_{n-1}x_n \approx x_{\pi(1)}x_{\pi(2)} \dots x_{\pi(n-1)}x_{\pi(n)} : \pi \in S_n\}$, равен $n - 1$.

В связи с результатами предложения 1 ещё более актуальной становится проблема классификации многообразий полугрупп по рангам планарности, в частности задача описания многообразий полугрупп бесконечного ранга планарности.

4.3. О рангах планарности других многообразий полугрупп

Принципиальная новизна серии многообразий, описанных в данном подразделе, заключается в том, что впервые поднимается вопрос о рангах планарности для многообразий вполне регулярных полугрупп, то есть являющихся объединением групп, причём соответствующие группы не обязательно являются абелевыми. Из теоремы 56 для абелевых групп известно и независимо доказано позднее для произвольных групп в [98], что ранг планарности многообразия $\mathrm{var}\{x^n \approx 1\}$ при любом $n \geqslant 3$ равен 1. Но в более общем случае при нахождении рангов планарности многообразий полугрупп, заданных тождеством $x^n \approx x$, в полугрупповой сигнатуре, на этом пути возникает проблема Туэ равенства слов. Удалось обойти эту проблему при доказательстве следующей теоремы.

Теорема 61 [98]. Ранг планарности многообразия $\mathrm{var}\{x^n \approx x\}$ при любом $n \geqslant 3$ равен 1, а при $n = 2$ равен 3.

Позднее всех стали известны планарные многообразия полугрупп [89].

Теорема 62 [89, теорема 1]. Нетривиальные планарные многообразия полугрупп исчерпываются:

— многообразием полугрупп левых нулей $\mathbf{L}_0 = \mathrm{var}\{xy \approx x\}$;
— многообразием полугрупп с нулевым умножением $\mathbf{N}_2 = \mathrm{var}\{xy \approx zt\}$;
— и их покрывающим многообразием $\mathbf{L}_0 \vee \mathbf{N}_2 = \mathrm{var}\{xy \approx xz\}$.

Как следствие, из данной теоремы легко вытекает перечисление всех планарных многообразий коммутативных полугрупп:

Следствие 7 [90, теорема 1]. Единственным нетривиальным планарным многообразием коммутативных полугрупп является многообразие полугрупп с нулевым умножением.

При доказательстве теоремы 62 найдены многообразия полугрупп бесконечного ранга планарности и рангов 2, 3, 4 (приведены в [89] на примере известной решётки из [99], порождённой негрупповыми атомами).

В завершение приведём новый результат, полученный в процессе написания обзора.

Теорема 63. $\mathrm{Spec}_{r\pi}(\mathrm{var}\{x^2 = x\}) = \{0, 2, 3, 4, \infty\}$.

Несмотря на столь краткую формулировку, доказательство теоремы 63 показательно тем, что опирается на обширные результаты прежних исследований и в процессе доказательства были существенно задействованы машинные вычисления, согласно описанной в [100] общей методологии.

Доказательство. В [101] приведено такое множество $\mathcal{G}$, которое содержит все тождества многообразий связок с точностью до эквивалентности, при этом каждое тождество из $\mathcal{G}$ неприводимо (то есть любое тождество из $\mathcal{G}$ не эквивалентно некоторому тождеству от меньшего числа переменных) и каждое многообразие связок задается системой тождеств, образованной тождеством $x^2 = x$ и одним из тождеств множества $\mathcal{G}$. Данное множество $\mathcal{G} = \bigcup\limits_{i=1}^{4} (a_i \cup \overline{a_i} \cup \mathcal{b}_i \cup \overline{\mathcal{b}_i}) \cup c \cup \mathcal{d}$ является дизъюнктным объединением следующих подмножеств, состоящих из тождеств, в словах которых d — это переменная, отличная от переменных a, x, y, x_i, $i = 1, \ldots, \infty$:

$a_1 = \{R_n = Q_n : n = 3, 5, \ldots\}$, $\quad a_2 = \{R_n = S_n : n = 3, 5, \ldots\}$,
$a_3 = \{R_n = Q_n : n = 4, 6, \ldots\}$, $\quad a_4 = \{R_n = S_n : n = 4, 6, \ldots\}$,
$\mathcal{b}_1 = \{R_n dx_n R_{n-1} = Q_n dx_n S_{n-1} : n = 5, 7, \ldots\}$,
$\mathcal{b}_2 = \{R_n d\overline{R_n} = S_n d\overline{Q_n} : n = 3, 5, \ldots\}$,
$\mathcal{b}_3 = \{\overline{R_n} dx_n \overline{R_{n-1}} = \overline{Q_n} dx_n \overline{S_{n-1}} : n = 4, 6, \ldots\}$,
$\mathcal{b}_4 = \{\overline{R_n} dR_n = \overline{S_n} dQ_n : n = 4, 6, \ldots\}$,
$c = \{Ad\overline{A} = Bd\overline{B} : A = B \in a_1 \cup a_2 \cup \overline{a_3} \cup \overline{a_4}\} \cup \{R_3 dR_2 = Q_3 dS_2, \overline{R_2} d\overline{R_3} = \overline{S_2} d\overline{Q_3}\}$,
$\mathcal{d} = \{x = y, ax = a, xa = a, axya = ayxa, R_2 = Q_2, \overline{R_2} = \overline{Q_2}, ax = axa, axya = axaya, xa = axa, a = a, R_2 = S_2, \overline{R_2} = \overline{S_2}, xy = yx, a = axa\}$,

где

$$R_n = \begin{cases} x_3x_2x_1 & \text{при } n = 2, \\ x_1x_2x_3 & \text{при } n = 3, \\ R_{n-1}x_n & \text{при } n = 4, 6, \ldots, \\ x_nR_{n-1} & \text{при } n = 5, 7, \ldots; \end{cases} \qquad Q_n = \begin{cases} x_2x_3x_1 & \text{при } n = 2, \\ x_1x_2x_3x_1x_3 & \text{при } n = 3, \\ Q_{n-1}x_nR_n & \text{при } n = 4, 6, \ldots, \\ R_nx_nQ_{n-1} & \text{при } n = 5, 7, \ldots; \end{cases}$$

$$S_n = \begin{cases} x_3x_1x_2x_1 & \text{при } n = 2, \\ x_1x_2x_3x_1x_3x_2x_3 & \text{при } n = 3, \\ S_{n-1}x_nR_n & \text{при } n = 4, 6, \ldots, \\ R_nx_nS_{n-1} & \text{при } n = 5, 7, \ldots, \end{cases}$$

а слово $\bar{A}$ обозначает зеркальное отражение слова $A \in \{R_n, Q_n, S_n : n = 2, 3, 4, 5, 6, 7, \ldots\}$ и для каждого множества тождеств $f \in \cup_{i=1}^{4}\{a_i, \mathcal{b}_i\}$ однозначно определено соответствующее множество зеркальных тождеств $\overline{f} = \{\overline{P} = \overline{Q} : P = Q \in f\}$.

Таким образом, многообразия связок формируют решётку счётного порядка. Она приведена на рис. 3 с обозначениями из [101] и указанием рангов планарности соответствующих многообразий. Ранги планарности восьми многообразий нижних этажей решётки и самого верхнего вычислены в [89] и [92] соответственно, они принимают все возможные значения из множества $\{0, 3, 4, \infty\}$. Кроме того, нетрудно убедиться, что в классе многообразий связок $r_\pi(\mathrm{var}\{xa \approx axa\}) = r_\pi(\mathrm{var}\{R_2 \approx S_2\}) = r_\pi(\mathrm{var}\{\overline{R_3} \approx \overline{Q_3}\}) = 2$, $r_\pi(\mathrm{var}\{axya \approx axaya\}) = r_\pi(\mathrm{var}\{R_3 \approx S_3\}) = r_\pi(\mathrm{var}\{\overline{R_3} \approx \overline{S_3}\}) = 3$, $r_\pi(\mathrm{var}\{\overline{R_2} \approx \overline{S_2}\}) = r_\pi(\mathrm{var}\{R_3 \approx Q_3\}) = 4$, а $r_\pi(\mathrm{var}\{ax \approx axa\}) = \infty$ (так как основа графа Кэли свободной полугруппы данного многообразия относительно любого числа образующих является лесом). Следовательно, каждое из значений рангов планарности в множестве $\{0, 2, 3, 4, \infty\}$ достижимо.

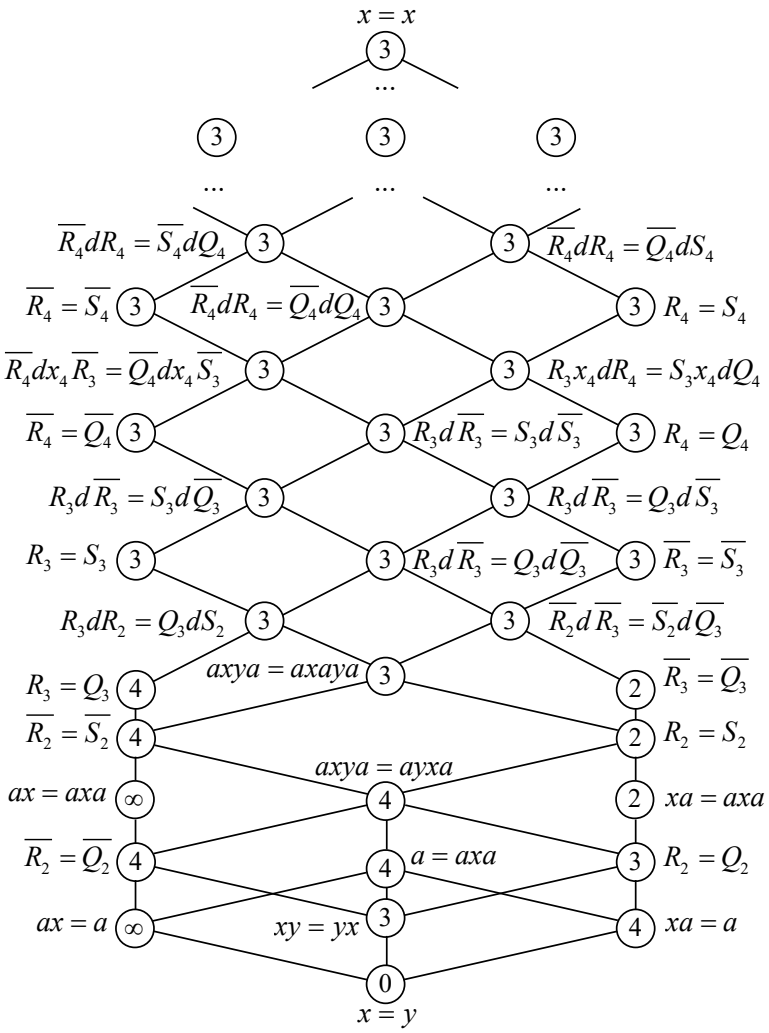


Рис. 3. Бесконечная счётная решётка всех многообразий связок с указанием в кружочках значений их рангов планарности

Заметим, что длина отождествляемых слов в свободной полугруппе указанных многообразий не превосходит восьми. Остаётся показать, что ранги планарности оставшихся из ранее не исследованных на предмет значения рангов планарности многообразий связок (в свободной полугруппе которых длина отождествляемых слов более восьми) принимают значения из множества $\{2, 3, 4, \infty\}$, а именно равны 3. В самом деле, плоская укладка графа Кэли 3-порождённой свободной полугруппы каждого

из этих многообразий совпадает с приведённой в [92] плоской укладкой графа Кэли 3-порождённой свободной полугруппы многообразия $\mathrm{var}\{a \approx a\}$ в классе многообразий связок, поскольку каждый из 159 элементов этой полугруппы является словом длины не более 8.

При выборе четырёх и более образующих свободная полугруппа каждого из анализируемых многообразий не допускает плоской укладки по теореме Понтрягина — Куратовского, так как в основе её графа Кэли содержится подграф, гомеоморфный графу $K_{3,3}$, содержащий в одной из долей вершины $xyzuxyz$, $xyzuy$, $xyzuzy$, а в другой — вершины $xyzu$, $xyzuyu$, $xyzuyz$, соединённые следующими непересекающимися маршрутами: $xyzuxyz$–$xyzu$, $xyzuxyz$–$xyzuxy$–$xyzuxyux$–$xyzuyuxz$–$xyzuyux$–$xyzuyu$, $xyzuxyz$–$xyzuxyzx$–$xyzuyzxu$–$xyzuyzx$–$xyzuyz$, $xyzuy$–$xyzu$, $xyzuy$–$xyzuyu$, $xyzuy$––$xyzuyz$, $xyzuzy$–$xyzuz$–$xyzu$, $xyzuzy$–$xyzuyuz$–$xyzuyu$, $xyzuzy$–$xyzuzyu$–$xyzuyzy$––$xyzuyz$. Принципиальное значение имеет тот факт, что каждая из вершин данного графа является словом, длина которого не превосходит восьми.

Типовой подзадачей, возникающей в поисках минимальной конфигурации $K_{3,3}$, является доказательство либо опровержение равенства слов. Доказательство равенства $xyzuxyuxz = xyzuyuxz$ в свободной полугруппе многообразия, заданного тождеством $x^2 \approx x$, используемого для обоснования существования ребра $xyzuxyux$–$xyzuyuxz$, помеченного элементом z в графе Кэли свободной полугруппы данного многообразия, можно осуществить разными способами. С одной стороны, равенство верно, так как если взять в качестве отправной точки $(((((((xy)z)u)x)y)u)x)z = (((((((xy)z)u)y)u)x)z$ — доказываемое тождество, выполняемое для всех допустимых значений пропозициональных переменных x, y, z, u; $x^2 = x$ — исходное тождество идемпотентности; $(xy)z = x(yz)$ — исходное тождество ассоциативности, и предположить, что $(((((((c_1c_2)c_3)c_4)c_1)c_2)c_4)c_1)c_3 \neq ((((((c_1c_2)c_3)c_4)c_2)c_4)c_1)c_3$ — противное к доказываемому, что существуют такие константы c_1, c_2, c_3, c_4, для которых тождество неверно, то в результате серии из 320 тождественных преобразований будет получено противоречие. Следовательно, предположение неверно. С другой стороны, достаточно вспомнить некоторые классические факты о равенстве слов в свободной связке B_X над алфавитом X, установленные в [102], примеры использования которых можно найти в [103, с. 121]. Один из этих фактов состоит в следующем. Обозначим через $c(w)$ содержание слова w, т. е. множество букв из X, участвующих в записи w. Тогда если $c(w_1) = c(w_3) \supseteq c(w_2)$, то $w_1w_2w_3 = w_1w_3$ в B_X. Если положить $w_1 = xyzu$, $w_2 = x$, $w_3 = yuxz$, то становится очевидным, что тождество $xyzu \cdot x \cdot yuxz = xyzu \cdot yuxz$ является специальным случаем указанного общего факта и не нуждается в отдельном доказательстве. Аналогично, из решения проблемы равенства слов в свободной связке сразу следует неравенство $xyzuyux \neq xyzuxyux$ в B_X.

Тем не менее при доказательстве неравенств, необходимых для обоснования того, что все вершины найденной конфигурации различны в исследуемом многообразии, можно построить конкретные модели эквациональной логики первого порядка. В качестве типового нетривиального примера покажем, что $xyzuyux \neq xyzuxyux$ в свободной полугруппе многообразия, заданного тождеством $x^2 \approx x$, для обоснования существования двух различных вершин $xyzuyux$, $xyzuxyux$ в графе Кэли свободной полугруппы данного многообразия.

В самом деле, равенство $xyzuyux = xyzuxyux$ не выполняется в свободной полугруппе исследуемого многообразия связок, возможно, удовлетворяющей тождеству, не эквивалентному тождеству идемпотентности, но отождествляющее слово из более

чем восьми символов с любым другим словом, так как оно обращается в ложное, при интерпретации умножения по следующей таблице Кэли:

$\cdot$	0	1	2	3	4	5
0	0	0	2	0	4	5
1	1	1	2	1	4	5
2	4	5	2	2	4	5
3	0	1	2	3	4	5
4	4	4	2	4	4	5
5	5	5	2	5	4	5

Для такого умножения выполнены тождества идемпотентности и ассоциативности, последнее эффективно проверяется тестом ассоциативности по Лайту, впервые опубликованным в [104] на английском и независимо в первой в мировой литературе монографии по теории полугрупп на русском языке [105], но, взяв $x = 0$, $y = 1$, $z = 2$, $u = 3$, получим противоречие: $xyzuyux = 0123130 = 023130 = 23130 = 2130 = 530 = 50 = 5$, $xyzuxyux = 01230130 = 0230130 = 230130 = 20130 = 4130 = 430 = 40 = 4$. Что и требовалось доказать. ■

Заключение

Подводя итоги обзора результатов исследований по изучению свойства планарности графов Кэли для полугрупп, напомним, что было выделено два основных направления: первое (классическое) посвящено описанию полугрупп с планарными графами Кэли; второе (новое) — инспирировано тесно связанными между собой понятиями ранга планарности и спектра рангов планарности многообразий полугрупп, предложенными Л. М. Мартыновым.

В планах развития первого направления адресуем проблему описания конечных полугрупп с планарными графами Кэли для тех или иных классов полугрупп, в которых, на наш взгляд, решение этой проблемы имеет шансы на успех. Например, в [29] перед описанием планарных правых групп отмечается, что можно зафиксировать полугруппу левых нулей $L_k = \{l_1, \ldots, l_k\}$ на k элементах, таких, что $l_i l_j = l_i$ при всех $i, j \in \{1, \ldots, k\}$, и рассмотреть левую группу $L_k \times G$, система образующих которой всегда имеет вид $L_k \times C$, где C — система образующих элементов группы G. Правый граф Кэли $Cay(L_k \times G, L_k \times C)$ левой группы состоит из k копий $Cay(G, C)$. Следовательно, левая группа $L_k \times G$ плоская тогда и только тогда, когда группа G плоская для произвольного $k \in \mathbb{N}$. После этого естественным образом возникает задача описания планарных правых групп и её решение. В дальнейшем данная задача может быть перенесена на случай прямоугольных групп (прямое произведение группы и прямоугольной полугруппы) в противовес более сложным образом устроенным клиффордовым полугруппам. Описание клиффордовых полугрупп с планарными графами Кэли сдерживается значительными вычислительными трудностями, но является лишь одним из многих путей первого направления.

Помимо этого, с одной стороны, можно налагать дополнительные ограничения на планарные графы Кэли полугрупп, а именно: известна идея описания полугрупп, допускающих ациклические графы Кэли (в основе которых запрещены подграфы, гомеоморфные полному графу третьего порядка K_3, соответствующее исследование полугрупп, основа графа Кэли которых является деревом, начато в [46]), внешнепланарные графы Кэли (запрещены K_4 и $K_{2,3}$, большая часть основных классов таких полугрупп рассмотрена в монографии [106]), обобщённые внешнепланарные графы

Кэли (без подграфов, гомеоморфных графам Седлачека, изучение которых начато в [50]), последовательно-параллельные графы Кэли (без K_4) и незацепленные вложения (без K_6 и других графов Петерсенова семейства в качестве миноров). Каждый из упомянутых классов графов, согласно общей теории миноров, хорошо описывается на языке запрещённых конфигураций, аналогично планарным (без K_5 и $K_{3,3}$), а поиск характеризации полугрупп, допускающих графы Кэли без подграфов, выбираемых с точностью до гомеоморфизма из непустого наперёд заданного множества не обязательно конечных графов, ещё ждёт своего исследователя.

С другой стороны, можно варьировать класс полугрупп, например весьма актуальной представляется задача исчерпывающего описания нильпотентных полугрупп с планарными графами Кэли. Известно лишь описание плоских свободных нильпотентных полугрупп, плоских нильпотентных частично коммутативных полугрупп, но результаты не распространены на бесконечный случай частично коммутативных полугрупп. В настоящее время предпринимаются попытки классифицировать изучаемые объекты на языке количества элементов в квадрате соответствующей полугруппы (по количеству ненулевых двухэлементных произведений из множества образующих). Попутно могут быть описаны графы Кэли полугрупп круглых порядков (n — круглое, если существует натуральная степень основания некоторой системы счисления, равная n). По мере продвижения предстоит исследовать возникающие алгоритмические проблемы. Так, например, проблема равенства слов в классе полугрупп с планарными графами Кэли ещё не решена. С одной стороны, мы располагаем примерами полугрупп с разрешимой проблемой равенства слов, но не планарными графами Кэли; с другой стороны — на сегодняшний день неизвестен ответ на вопрос: «Существует ли полугруппа с планарным графом Кэли и с неразрешимой проблемой равенства слов», — при том что в [107] доказана неразрешимость узкой проблемы равенства слов для рассмотренных классов конечных, периодических, ниль- и нильпотентных полугрупп.

Кроме того, интересен вопрос о допустимости графа в качестве графа Кэли полугруппы (когда по графу требуется сказать, может ли он быть графом Кэли полугруппы; при этом эффективные алгоритмы в случае групп известны). Преодоление этих трудностей видится в применении параметрических алгоритмов и построении цепочек полугрупп, в которых граф Кэли каждой предшествующей содержался бы в следующем планарном графе, с использованием рекуррентных соотношений. Тогда будут исследованы возможности получения новых полугрупп, ведь остаётся открытым вопрос о влиянии различных произведений графов на свойство результирующего графа быть графом Кэли некоторой полугруппы. В частности, могут исследоваться произведения графов Кэли матричных полугрупп Риса или полугрупп Брандта, либо графов Кэли как графов пяти платоновых тел с некоторой ориентацией и пометкой рёбер.

Известные попытки классификации полугрупп не вписываются в рамки исследования полугрупп с планарными графами Кэли (в отличие от групп), поэтому имеет смысл построение новой классификации полугрупп, отталкиваясь от свойства планарности. Необходимо систематизировать «хорошие» и «плохие» полугруппы в смысле планарности их графов Кэли, с учётом различных характеристик непланарных графов, что, возможно, повлечёт появление нового подхода к понятию чистоты полугрупп и продемонстрирует высокую степень продуктивности использования графов Кэли полугрупп в решении задач, основанных на планарности. Так, например, описание допустимых перестановок компонентов может быть использовано для разработки сетей параллельных вычислений и проектирования интегральных схем. Предполагается, что результаты могут позволить выйти на качественно новый уровень технических

решений в схемотехнике. С другой стороны, результаты косвенно повлияют на получение решения открытой проблемы поиска гамильтонова цикла в графе, поскольку известно, что многие задачи на графах класса NP имеют полиномиальное решение в планарном случае. Более того, упомянутые в обзоре результаты, продолжающие исследования в этом направлении, обосновали, в частности, практическую значимость графов Кэли валентности 3 (так называемых кубических графов) для решения трудоёмких комбинаторных задач проектирования без использования групповых структур.

Основным направлением дальнейшего использования получаемых результатов является их применение для классификации полугрупп с планарными графами Кэли. Предвидя трудность решения проблемы классификации, желательно получить ответы на ряд конкретных вопросов: найти условия, при которых свободное коммутативное произведение двух конечных полугрупп с планарными графами Кэли обладает тем же свойством; прямое произведение двух полугрупп с планарными графами Кэли обладает тем же свойством; раздувание (inflation) полугруппы с планарным графом Кэли обладает тем же свойством; описать планарные графы Кэли полугруппы, полученной раздуванием полугруппы правых нулей; описать конечные коммутативные клиффордовы полугруппы (в частности, полурешётки), допускающие планарный граф Кэли (с точностью до групп); найти абстрактную характеристику графов Кэли полугрупп; описать полугруппы, полученные добавлением соотношения (не являющегося следствием исходных соотношений), допускающие планарный граф; описать полугруппы Фибоначчи, допускающие планарный граф Кэли.

Для второго направления приведём более конкретные открытые проблемы, постановка которых возникла при обсуждении результатов с Л. М. Мартыновым, и укажем на перспективы развития данной проблематики. Актуальной становится, по-видимому, весьма трудная следующая проблема.

Проблема 1. Описать многообразия полугрупп, имеющие бесконечный ранг планарности.

На подступах к решению этой проблемы интересно получить ответы на следующие два вопроса:

В о п р о с 1 . Какие из тождеств определяют многообразия полугрупп, имеющие бесконечный ранг планарности?

В о п р о с 2 . Какие системы из двух тождеств определяют многообразия полугрупп, имеющие бесконечный ранг планарности?

Дело в том, что некоторые ключевые многообразия полугрупп задаются именно двумя тождествами в полугрупповой сигнатуре, соответствующие примеры можно найти среди многообразий групп и 0-приведённых многообразий.

Первую задачу можно свести к не менее трудной проблеме задания матрицы смежности основы графа Кэли соответствующей свободной полугруппы. Опираясь на доказанное в [108], можно получить эквивалентность $r_\pi(\boldsymbol{V}) = \infty \Leftrightarrow$ $\Leftrightarrow \lim\limits_{n\to\infty} \mu(SCay(F_n(\boldsymbol{V}))) \leqslant 3$, где μ — инвариант Колен де Вердьера. Напомним: если $G = (V, E)$ — неориентированный граф (положим $V = \{1, \ldots, n\}$), то $\mu(G)$ является наибольшим корангом (дефектом) такой матрицы $M = (M_{i,j}) \in R^{(n)}$, для которой выполнены следующие три условия: 1) для всех i, j при $i \neq j$ имеет место неравенство $M_{i,j} < 0$, если i и j являются смежными, и равенство $M_{i,j} = 0$ в противном случае; 2) M имеет ровно одно отрицательное собственное значение кратности 1; 3) не существует ненулевой матрицы $X = (X_{i,j}) \in R^{(n)}$, такой, что $MX = 0$, в которой $X_{i,j} = 0$,

когда $i = j$ или $M_{i,j} \neq 0$ (то есть вершины i и j являются смежными). Данную эквивалентность можно раскрыть, используя методы работ [109, 110].

Например, для многообразия полугрупп правых нулей $\mathbf{R}_0 = \mathrm{var}\{xy \approx y\}$ имеет место неравенство $\lim\limits_{n\to\infty} \mu(SCay(F_n(\mathbf{R}_0))) = \lim\limits_{n\to\infty}(n-1) = \infty > 3$. В самом деле, $F_n(\mathbf{R}_0) = \langle a_1, a_2, \ldots, a_n \mid xy \approx y\rangle$, $SCay(F_n(\mathbf{R}_0)) = K_n$, $\mu(K_n) = n - 1$. Следовательно, данное многообразие имеет конечный ранг планарности.

Для многообразия полугрупп с нулевым умножением $\mathbf{N}_2 = \mathrm{var}\{xy \approx zt\}$ имеет место неравенство $\lim\limits_{n\to\infty} \mu(SCay(F_n(\mathbf{N}_2))) = \lim\limits_{n\to\infty}(2) = 2 \leqslant 3$. В самом деле, $F_n(\mathbf{N}_2) = \langle a_1, a_2, \ldots, a_n \mid xy \approx zt\rangle$, $SCay(F_n(\mathbf{N}_2)) = K_{1,n}$, $\mu(K_{1,n}) = \min\{1, n\}+1 = 2$ при $n \geqslant 4$. Следовательно, данное многообразие имеет бесконечный ранг планарности.

Определённый интерес представляет ещё более трудная проблема классификации многообразий полугрупп по рангам планарности.

Проблема 2. Описать многообразия полугрупп, имеющих ранг планарности r, где r – фиксированный элемент из $\mathbb{N}^\infty$.

На сегодняшний день классифицированы по рангам планарности лишь многообразия коммутативных моноидов (теорема 56) и многообразия связок (рис. 3). Кроме того, отдельный интерес представляет также проблема спектров рангов планарности многообразий полугрупп.

Проблема 3. Описать спектры рангов планарности многообразий полугрупп.

При решении этой проблемы возникнет более трудная задача классификации многообразий полугрупп по спектрам рангов планарности и откроются приложения спектральной теории многообразий полугрупп к построению хэш-функций.

Проблема 4. Описать многообразия полугрупп, имеющих данный спектр рангов планарности S, где S — фиксированное подмножество множества $\mathbb{N}^\infty$.

Отдельный интерес представляет здесь следующий вопрос:

В о п р о с 3 . Для каких многообразий полугрупп спектр рангов планарности является полным?

Конкретные примеры многообразий полного спектра рангов планарности представлены в обзоре. Ранее отмечалось (теорема 60), что спектр рангов планарности многообразия всех полугрупп полный, кроме того, обнаружена бесконечная серия многообразий ниль-полугрупп с полным спектром рангов планарности (следствие 6).

При этом из групповых многообразий в обзоре охвачены только многообразия абелевых групп. Тем интереснее адресовать к произвольным многообразиям вполне регулярных полугрупп следующую проблему.

Проблема 5. Описать ранги планарности многообразий вполне регулярных полугрупп, в частности клиффордовых.

Любая вполне регулярная полугруппа является полурешёткой прямоугольных связок групп. В таком многообразии выполняется тождество $x^n \approx x$ для некоторого натурального числа $n > 1$. Ясно, что любое многообразие связок является многообразием вполне регулярных полугрупп. Среди многообразий связок, согласно тереме 63, лишь два многообразия $\mathrm{var}\{x^2 \approx x; xy \approx x\}$ и $\mathrm{var}\{x^2 \approx x; xy \approx xyx\}$ имеют бесконечный ранг планарности. Примеры других многообразий вполне регулярных полугрупп бесконечного ранга планарности нам неизвестны. В связи с этим интересно получить ответы на следующие два вопроса:

В о п р о с 4 . Имеется ли многообразие вполне регулярных полугрупп бесконечного ранга планарности, содержащее неодноэлементную группу?

На подступах к решению этого вопроса отметим очевидную конечность ранга планарности любого локально конечного многообразия групп. Это вытекает из того, что перечисленные в теореме Машке (теорема 1) конечные группы с планарными графами Кэли порождаются не более чем тремя элементами, поэтому любая $\boldsymbol{V}$-свободная группа с четырьмя и более образующими не принадлежит этому списку.

В о п р о с 5 . Конечен ли ранг планарности любого нетривиального многообразия групп?

Ответ на последний вопрос приблизит решение вопроса 4. Обратим внимание, что здесь речь идёт о многообразии групп, рассматриваемых в полугрупповой сигнатуре, как алгебр с одной бинарной операцией умножения. В частности, любое многообразие групп является периодическим.

Итак, ещё раз подчеркнем важность изучения свойства планарности для графов Кэли полугрупп. В настоящее время в практических приложениях (в криптографии, теории кодирования и других) широко востребованы классические алгебры: группы, полугруппы. И не представляется возможным предвидеть, какие свойства тех или иных алгебраических структур понадобятся в дальнейшем. Поэтому мы солидарны с автором обзора [111] в мысли о том, что необходимо развивать структурные теории классических алгебр, используя различные подходы, методами теории графов в том числе.

Автор выражает глубокую признательность научному консультанту профессору Л. М. Мартынову за постановку задачи, постоянное внимание к работе и полезные обсуждения результатов, а также профессору М. В. Волкову за конструктивные критические замечания, высказанные после доклада автора на екатеринбургском семинаре «Алгебраические системы».

ЛИТЕРАТУРА

1. *Druţu C. and Kapovich M.* Geometric Group Theory. Colloquium Publ. AMS. 2018. V. 63. 819 p.
2. *McCammond J., Rhodes J., and Steinberg B.* Geometric Semigroup Theory. arXiv:1104.2301 [math.GR]. 2011.
3. *Cayley A.* The theory of groups: graphical representation // Amer. J. Math. 1878. V. 1. P. 174–176.
4. *Cooperman G., Finkelstein L., and Sarawagi N.* Applications of Cayley graphs // LNCS. 1991. V. 508. P. 367–378.
5. *Horwitz J. A.* Applications of Cayley Graphs, Bilinearity, and Higher-Order Residues to Cryptology. Diss. for the Degree of Doctor of Philosophy. Stanford, 2004. 100 p.
6. *Zémor G.* Hash functions and Cayley graphs // Des. Codes Crypt. 1994. V. 4. P. 381–394.
7. *Tripi A.* Cayley Graphs of Groups and Their Applications. MSU Graduate Theses. 2017. V. 3133. 47 p.
8. *Sosnovski B.* Cayley Graphs of Semigroups and Applications to Hashing. Diss. for the Degree of Doctor of Philosophy. City University of New York, 2016. 111 p.
9. *Maschke H.* The representation of finite groups, especially of the rotation groups of the regular bodies of three- and four-dimensional space, by Cayley's color diagrams // Amer. J. Math. 1896. V. 18. No. 2. P. 156–194.
10. *Беленкова Ж. Т., Романьков В. А.* Регулярные графы Кэли. Деп. ВИНИТИ. 1997. № 802–V97. 37 с.
11. *Беленкова Ж. Т., Романьков В. А.* Плоские графы Кэли конечных групп. Препринт. Омск: ОмГУ, 1997. 8 с.

12. *Беленкова Ж. Т.* Все плоские графы Кэли группы S_4. Препринт. Омск: ОмГУ, 1997. 12 с.
13. *Беленкова Ж. Т.* Плоские графы Кэли: дис. ... канд. физ.-мат. наук. Омск: ОмГУ, 1998.
14. *Droms C., Servatius B., and Servatius H.* Connectivity and planarity of Cayley graphs // Beiträge zur Algebra und Geometrie. 1998. V. 39. No. 2. P. 269–282.
15. *Droms C.* Infinite-ended groups with planar Cayley graphs // J. Group Theory. 2006. V. 9. No. 4. P. 487–496.
16. *Dunwoody M. J.* Planar Graphs and Covers. `https://arxiv.org/abs/0708.0920`. 2009.
17. *Georgakopoulos A.* Characterising planar Cayley graphs and Cayley complexes in terms of group presentations // Europ. J. Combinatorics. 2014. V. 36. P. 282–293.
18. *Georgakopoulos A.* The planar cubic Cayley graphs of connectivity 2 // Europ. J. Combinatorics. 2017. V. 64. P. 152–169.
19. *Georgakopoulos A.* The planar cubic Cayley graphs // Mem. Amer. Math. Soc. 2017. V. 250. No. 1190. 82 p.
20. *Georgakopoulos A. and Hamann M.* The planar Cayley graphs are effectively enumerable I: Consistently planar graphs // Combinatorica. 2019. V. 39. No. 5. P. 993–1019.
21. *Georgakopoulos A. and Hamann M.* The Planar Cayley Graphs are Effectively Enumerable II. `https://arxiv.org/abs/1901.00347`. 2019.
22. *Varghese O.* Planarity of Cayley graphs of graph products of groups // Discrete Math. 2019. V. 342. No. 6. P. 1812–1819.
23. *Georgakopoulos A.* On planar Cayley graphs and Kleinian groups // Trans. Amer. Math. Soc. 2020. V. 373. No. 7. P. 4649–4684.
24. *Paalman A. B.* Topological representation of semigroups // General Topology and its Relations to Modern Analysis and Algebra. Praha: Academia Publishing House AS CR, 1967. P. 276–282.
25. *Bosák J.* The graphs of semigroups // Proc. Symp. "Theory of Graphs and its Applications". Praha, 1964. P. 119–125.
26. *Zelinka B.* The diameter of the graph of the system of proper semigroups of a commutative semigroup // Mat.-Fyz. Cas. SAV. 1965. V. 15. P. 143–144.
27. *Zelinka B.* Graphs of semigroups // Cas. Pest. Mat. 1981. P. 407–408.
28. *Knauer K. and Knauer U.* Toroidal embeddings of right groups // Thai J. Math. 2010. V. 8. No. 3. P. 483–490.
29. *Knauer K. and Knauer U.* On planar right groups // Semigroup Forum. 2016. V. 92. No. 1. P. 142–157.
30. `http://www.mathnet.ru/php/seminars.phtml?presentid=12900` — Новые проблемы алгебры и логики. Юбилейное 900-е заседание семинара: Омский алгебраический семинар, 12 ноября 2015.
31. *Адян С. И.* Алгоритмическая неразрешимость проблем распознавания некоторых свойств групп // Докл. АН СССР. 1955. Т. 103. № 4. С. 533–535.
32. *Rabin M. O.* Recursive unsolvability of group theoretic problems // Ann. Math. 1958. V. 67. P. 172–174.
33. *Zieschang H., Vogt E., and Coldewey H. D.* Surfaces and Planar Discontinuous Groups. Berlin: Springer Verlag, 1980. 336 p.
34. *Margolis S. W. and Meakin J. C.* E-unitary inverse monoids and the Cayley graph of a group representation // J. Pure Appl. Algebra. 1989. V. 58. P. 45–76.
35. *Kelarev A. V. and Quinn S. J.* On complete and bipartite Cayley graphs // Arbeitstagung Allgemeine Algebra 62, June 14–17, 2001. Abstracts. Linz: Austria, 2001. P. 25.

36. *Kelarev A. V. and Praeger C. E.* On transitive Cayley graphs of groups and semigroups // Europ. J. Combinatorics. 2003. V. 24. P. 59–72.
37. *Kelarev A. V. and Quinn S. J.* A combinatorial property and Cayley graphs of semigroups // Semigroup Forum. 2002. V. 66. No. 1. P. 89–96.
38. *Kelarev A. V.* On undirected Cayley graphs // Australasian J. Combinatorics. 2002. V. 25. P. 73–78.
39. *Kelarev A. V.* On Cayley graphs of inverse semigroups // Semigroup Forum. 2006. V. 72. P. 411–418.
40. *Khosravi Be. and Khosravi Ba.* On Cayley graphs of semilattices of semigroups // Semigroup Forum. 2013. V. 86. P. 114–132.
41. *Khosravi Be. and Khosravi Ba.* A characterization of Cayley graphs of Brandt semigroups // Bull. Malaysian Math. Sci. Soc. 2012. V. 2. No. 2. P. 12–18.
42. *Khosravi B.* On Cayley graphs of left groups // Houston J. Math. 2009. V. 35. No. 3. P. 745–755.
43. *Fan S. and Zeng Y.* On Cayley graphs of Bands // Semigroup Forum. 2007. V. 74. P. 99–105.
44. *Макарьев А. Л.* О полугруппах идемпотентов с ациклическими графами Кэли // Математика и информатика: Наука и образование. 2007. Т. 6. С. 26–34.
45. *Соломатин Д. В.* Строение полугрупп, допускающих внешнепланарные графы Кэли // Сиб. электрон. матем. изв. 2011. Т. 8. С. 191–212.
46. *Макарьев А. Л.* Нильпотентные полугруппы, основа графа Кэли которых является деревом // Математика и информатика: Наука и образование. 2006. Т. 5. С. 40–46.
47. *Макарьев А. Л.* Полурешётки с ациклическими графами Кэли // Математика и информатика: Наука и образование. 2008. Т. 7. С. 28–33.
48. *Макарьев А. Л.* Ординальные суммы полугрупп с ациклическими графами Кэли // Вестник Омского университета. 2008. Т. 4. С. 12–17.
49. *Мартынов Л. М., Соломатин Д. В.* Полугруппы вычетов с циклическими группами обратимых элементов, допускающие планарные графы Кэли // Вестник Омского университета. 2012. Т. 2. С. 57–62.
50. *Мартынов П. О., Соломатин Д. В.* Конечные свободные коммутативные полугруппы и полугруппы с нулём, допускающие обобщенные внешнепланарные графы Кэли // Вестник Омского университета. 2014. Т. 3. С. 22–26.
51. *Мартынов П. О.* Конечные свободные коммутативные моноиды, допускающие обобщенно внешнепланарные графы Кэли // Вестник Омского университета. 2015. Т. 4. С. 6–9.
52. *Мартынов П. О.* Рассыпчатые полугруппы, допускающие обобщенные внешнепланарные графы Кэли // Вестник Омского университета. 2018. Т. 3. С. 6–9.
53. *Khosravi B.* Comparison of Cayley graphs of semigroups and Cayley graphs of groups // Book of Abstracts Caucasian Math. Conf. CMC II. Turkish Math. Society, 2007. P. 18–19.
54. *Molchanov V. A.* A universal planar automaton is determined by its semigroup of input symbols // Semigroup Forum. 2011. V. 82. P. 1–9.
55. *Zhang X.* Clifford semigroups with genus zero // Proc. Intern. Conf. Semigroups, Acts and Categories with Applications to Graphs. University of Tartu, June 27–30, 2007. Tartu: EMS, 2008. P. 151–160.
56. *Шеврин Л. Н.* Полугруппы // Общая алгебра (ред. Л. А. Скорняков). Гл. IV. М.: Наука, 1991. Т. 2. С. 11–191.
57. *Емеличев В. А., Мельников О. И., Сарванов В. И., Тышкевич Р. И.* Лекции по теории графов. М.: Наука, 1990. 384 с.
58. *Martynova T. A.* The groupoid of 0-reduced varieties of semigroups // Semigroup Forum. 1983. V. 26. P. 249–274.

59. *Preston G. and Clifford A.* The Algebraic Theory of Semigroups // Amer. Math. Soc. 1964. V. 1. No. 7. P. 169–174.
60. *Соломатин Д. В.* Ранги планарности многообразий коммутативных моноидов // Вестник Омского университета. 2012. Т. 4. С. 41–45.
61. *Соломатин Д. В.* О допустимости некоторых графов в качестве графов Кэли полугрупп // Математика и информатика: Наука и образование. 2004. Т. 4. С. 32–34.
62. *Lempel A., Even S., and Cederbaum I.* An algorithm for planarity testing of graphs // Proc. Int. Symp. Theory Graphs. New York, 1967. P. 215–232.
63. *Klein P. N. and Reif J. H.* An efficient parallel algorithm for planarity // J. Computer System Sci. 1988. V. 37. P. 190–246.
64. *Bader D. A. and Sreshta S. A.* A New Parallel Algorithm for Planarity Testing. `https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.65.2914&rep=rep1&type=pdf`. 2003.
65. *Соломатин Д. В.* О критериях планарности графов Кэли полугрупп // Математика и информатика: Наука и образование. 2010. Т. 9. С. 44–46.
66. *Соломатин Д. В.* Стохастический алгоритм поиска подграфа, гомеоморфного заданному // Стохастические модели в биологии и предельные алгебры (Омск, 2–7 августа 2010). Омск: ИМ им. С. Л. Соболева СО РАН, 2010. С. 98–100.
67. *Kambites M.* The loop problem for Rees matrix semigroups // Semigroup Forum. 2008. V. 76. No. 2. P. 204–216.
68. *Мелихов А. Н., Берштейн Л. С., Курейчик В. М.* Применение графов для проектирования дискретных устройств. М.: Наука, 1974. 304 с.
69. *Levinson H.* On the genera of graphs of group presentations // Ann. New York Acad. Sci. 1970. V. 175. P. 277–284.
70. *Соломатин Д. В.* Свободные частично коммутативные n-веерные полурешетки с планарными графами Кэли // Математика и информатика: Наука и образование. 2009. Т. 8. С. 36–39.
71. *Соломатин Д. В.* Свободные частично коммутативные нильпотентные полугруппы с планарными графами Кэли // Вестник Омского университета. 2014. Т. 3. С. 28–36.
72. *Соломатин Д. В.* Конечные свободные коммутативные полугруппы с планарными графами Кэли // Математика и информатика: Наука и образование. 2003. Т. 3. С. 32–38.
73. *Соломатин Д. В.* Конечные свободные коммутативные моноиды, допускающие планарный граф Кэли // Вестник Омского университета. 2005. Т. 4. С. 36–38.
74. *Birkhoff G.* On the structure of abstract algebras // Proc. Camb. Phil. Soc. 1935. V. 31. P. 433–454.
75. *Соломатин Д. В.* Прямые произведения циклических полугрупп, допускающие планарный граф Кэли // Сиб. электрон. матем. изв. 2006. Т. 3. С. 238–252.
76. *Соломатин Д. В.* Прямые произведения циклических моноидов и полугрупп с нулем, допускающие планарные графы Кэли // Математика и информатика: Наука и образование. 2006. Т. 5. С. 51–64.
77. *Соломатин Д. В.* Критерий планарности для графов Кэли 0-прямых объединений нильпотентных полугрупп // Мальцевские чтения (2–6 мая 2010). Новосибирск: ИМ им. С. Л. Соболева СО РАН, 2010. С. 144.
78. *Соломатин Д. В.* Рассыпчатые полугруппы с планарными графами Кэли // Вестник Волгоградского государственного педагогического университета. 2005. Т. 4. С. 27–31.
79. *Полякова Л. Ю.* Резольвенты для свободных частично коммутативных моноидов // Сиб. матем. журн. 2007. Т. 48. С. 1295–1304.

80. *Diekert V. and Métivier Y.* Partial commutation and traces // Handbook of Formal Languages. Berlin: Springer Verlag, 1997. V. 3. P. 457–533.
81. *Sedláček J.* On a generalization of outerplanar graphs // Časopis Pěst. Mat. 1988. V. 2. No. 113. P. 213–218.
82. *Соломатин Д. В.* Планарные гиперграфы мультипликативных полугрупп вычетов // Математика и информатика: Наука и образование. 2011. Т. 10. С. 30–34.
83. *Булатов А. А.* Алгебраические методы исследования комбинаторных задач: дис. ... докт. физ.-мат. наук. Екатеринбург, 2008.
84. *Zinbiel G. W.* Encyclopedia of Types of Algebras 2010. arXiv:1101.0267v1. 2010.
85. *Sudoplatov S. V.* Hypergraphs of prime models and distributions of countable models of small theories // J. Math. Sci. 2010. V. 169. No. 5. P. 680–695.
86. *Зыков А. А.* Гиперграфы // Успехи матем. наук. 1974. Т. 29. № 6(180). С. 89–154.
87. *Соломатин Д. В.* Конечно порожденные полугруппы с одним определяющим соотношением и тождеством, допускающие планарный граф Кэли // Математика и информатика: Наука и образование. 2007. Т. 6. С. 42–48.
88. *Соломатин Д. В.* Ординальные суммы прямоугольных полугрупп, допускающие планарные графы Кэли // Математика и информатика: Наука и образование. 2008. Т. 7. С. 33–41.
89. *Соломатин Д. В.* Планарные многообразия полугрупп // Сиб. электрон. матем. изв. 2015. Т. 12. С. 232–247.
90. *Соломатин Д. В.* Планарные многообразия коммутативных полугрупп // Вестник Омского университета. 2015. Т. 2. С. 17–22.
91. *Соломатин Д. В.* Ранги планарности многообразий коммутативных полугрупп // Прикладная дискретная математика. 2016. № 4(34). С. 50–64.
92. *Соломатин Д. В.* О рангах планарности многообразий полугрупп идемпотентов, нильполугрупп и полугрупп с перестановочным тождеством // Вестник Омского университета. 2017. Т. 4. № 86. С. 11–21.
93. *Соломатин Д. В.* О рангах планарности многообразий нильполугрупп // Вестник Омского университета. 2019. Т. 2. № 24. С. 17–22.
94. *Соломатин Д. В.* Ранги планарности многообразий полугрупп // Вестник Омского университета. 2019. Т. 4. С. 9–15.
95. *Hopcroft J. and Tarjan R.* Efficient planarity testing // J. ACM. 1974. V. 21. No. 4. P. 549–568.
96. *Chiba N., Yamanouchi T., and Nishizeki T.* Linear algorithms for convex drawings of planar graphs // J. A. Bondy, U. S. R. Murty (eds.). Progress in Graph Theory. London: Academic Press, P. 153–173.
97. *Head T. J.* The varieties of commutative monoids // Nieuw Archief voor Wiskunde. 1968. V. 3. No. 16. P. 203–206.
98. *Соломатин Д. В.* Ранги планарности многообразий полугрупп, заданных тождеством $x \approx x^n$ // Вестник Омского Университета. 2020. Т. 3. № 25. С. 13–17.
99. *Evans T.* The lattice of semigroup varieties // Semigroup Forum. 1971. V. 2. P. 1–43.
100. *Arthan R. and Oliva P.* Studying algebraic structures using Prover9 and Mace4 // G. Hanna et al. (eds.) Proof Technology in Mathematics Research and Teaching. Ch. 5. Springer, 2020.
101. *Fennemore C.* All varieties of bands // Semigroup Forum. 1970. V. 1. P. 172–179.
102. *Green J. A. and Rees D.* On semigroups in which $x^r = x$, Proc. Cambridge Philos. Soc. 1952. V. 48. P. 35–40.

103. *Howie J. M.* Fundamentals of Semigroup Theory. London Math. Society Monographs. New Series, 12. Oxford Science Publ. N.Y.: Clarendon Press, Oxford University Press, 1995. 351 p.
104. *Preston G. and Clifford A.* The algebraic theory of semigroups // Amer. Math. Soc. 1961. V. 1. No. 1. P. 12–31.
105. *Ljapin E. S.* Semigroups. Amer. Math. Soc. 4th ed. 1963. 519 p.
106. *Соломатин Д. В.* Теория представлений: учеб. пособие. Омск: ОмГПУ, 2015. 64 с.
107. *Гуревич Ю. Ш.* Проблема равенства слов для некоторых классов полугрупп // Алгебра и логика. 1966. Т. 5. № 5. С. 25–35.
108. *De Verdière Y. C.* Sur un Nouvel Invariant des Graphes et un Critère de Planarité // J. Combinat. Theory. Ser. B. 1990. No. 50. P. 11–21.
109. *Канторович Л. В., Крылов В. И.* Приближенные методы высшего анализа. 5-е изд. М., Л.: Физматгиз, 1962. 708 с.
110. *Fedorov F. M.* On the theory of infinite systems of linear algebraic equations // TWMS J. Pure Appl. Math. 2015. V. 2. No. 6. P. 202–212.
111. *Мартынов Л. М.* Полнота, редуцированность, примарность и чистота для алгебр: результаты и проблемы // Сиб. электрон. матем. изв. 2016. Т. 13. С. 181–241.

REFERENCES

1. *Druţu C. and Kapovich M.* Geometric Group Theory. Colloquium Publ., AMS, 2018, vol. 63. 819 p.
2. *McCammond J., Rhodes J., and Steinberg B.* Geometric Semigroup Theory. arXiv:1104.2301 [math.GR], 2011.
3. *Cayley A.* The theory of groups: Graphical representation. Amer. J. Math., 1878, vol. 1, pp. 174–176.
4. *Cooperman G., Finkelstein L., and Sarawagi N.* Applications of Cayley graphs // LNCS, 1991, vol. 508, pp. 367–378.
5. *Horwitz J. A.* Applications of Cayley Graphs, Bilinearity, and Higher-Order Residues to Cryptology. Diss. for the Degree of Doctor of Philosophy. Stanford, 2004. 100 p.
6. *Zémor G.* Hash functions and Cayley graphs. Des. Codes Cryptogr., 1994, vol. 4, pp. 381–394.
7. *Tripi A.* Cayley Graphs of Groups and Their Applications. MSU Graduate Theses, 2017, vol. 3133. 47 p.
8. *Sosnovski B.* Cayley Graphs of Semigroups and Applications to Hashing. Diss. for the Degree of Doctor of Philosophy, City University of New York, 2016. 111 p.
9. *Maschke H.* The representation of finite groups, especially of the rotation groups of the regular bodies of three- and four-dimensional space, by Cayley's color diagrams. Amer. J. Math., 1896, vol. 18, no. 2, pp. 156–194.
10. *Belenkova Zh. T. and Roman'kov V. A.* Regulyarnye grafy Keli. [Regular Cayley graphs]. Dep. VINITI, 1997, no. 802–V97. (in Russian)
11. *Belenkova Zh. T. and Roman'kov V. A.* Ploskie grafy Keli konechnykh grupp [Plane Cayley graphs of finite groups]. Preprint, Omsk, OmSU, 1997. 8 p. (in Russian)
12. *Belenkova Zh. T.* Vse ploskie grafy Keli gruppy S_4 [All plane Cayley graphs of the group S_4]. Preprint, Omsk, OmSU, 1997. 12 p. (in Russian)
13. *Belenkova Zh. T.* Ploskie grafy Keli [Plane Cayley graphs]. PhD Thesis, Omsk, OmSU, 1998. (in Russian)
14. *Droms C., Servatius B., and Servatius H.* Connectivity and planarity of Cayley graphs. Beiträge zur Algebra und Geometrie, 1998, vol. 39, no. 2, pp. 269–282.
15. *Droms C.* Infinite-ended groups with planar Cayley graphs. J. Group Theory, 2006, vol. 9, no. 4, pp. 487–496.

16. *Dunwoody M. J.* Planar Graphs and Covers. `https://arxiv.org/abs/0708.0920`, 2009.
17. *Georgakopoulos A.* Characterising planar Cayley graphs and Cayley complexes in terms of group presentations. Europ. J. Combinatorics, 2014, vol. 36, pp. 282–293.
18. *Georgakopoulos A.* The planar cubic Cayley graphs of connectivity 2. Europ. J. Combinatorics, 2017, vol. 64, pp. 152–169.
19. *Georgakopoulos A.* The planar cubic Cayley graphs. Mem. Amer. Math. Soc., 2017, vol. 250, no. 1190. 82 p.
20. *Georgakopoulos A. and Hamann M.* The planar Cayley graphs are effectively enumerable I: Consistently planar graphs. Combinatorica, 2019, vol. 39, no. 5, pp. 993–1019.
21. *Georgakopoulos A. and Hamann M.* The Planar Cayley Graphs are Effectively Enumerable II. `https://arxiv.org/abs/1901.00347`, 2019.
22. *Varghese O.* Planarity of Cayley graphs of graph products of groups. Discrete Math., 2019, vol. 342, no. 6, pp. 1812–1819.
23. *Georgakopoulos A.* On planar Cayley graphs and Kleinian groups. Trans. Amer. Math. Soc., 2020, vol. 373, no. 7, pp. 4649–4684.
24. *Paalman A. B.* Topological representation of semigroups. General Topology and its Relations to Modern Analysis and Algebra, Praha, Academia Publishing House AS CR, 1967, pp. 276–282.
25. *Bosák J.* The graphs of semigroups. Proc. Symp. "Theory of Graphs and its Applications", Praha, 1964, pp. 119–125.
26. *Zelinka B.* The diameter of the graph of the system of proper semigroups of a commutative semigroup. Mat.-Fyz. Cas. SAV, 1965, vol. 15, pp. 143–144.
27. *Zelinka B.* Graphs of semigroups. Cas. Pest. Mat., 1981, pp. 407–408.
28. *Knauer K. and Knauer U.* Toroidal embeddings of right groups. Thai J. Math., 2010, vol. 8, no. 3, pp. 483–490.
29. *Knauer K. and Knauer U.* On planar right groups. Semigroup Forum, 2016, vol. 92, no. 1, pp. 142–157.
30. `http://www.mathnet.ru/php/seminars.phtml?presentid=12900`.
31. *Adian S. I.* Algoritmicheskaya nerazreshimost' problem raspoznavaniya nekotorykh svoystv grupp [Algorithmic unsolvability of problems of recognition of certain properties of groups]. Dokl. USSR Academy of Sciences, 1955, vol. 103, no. 4, pp. 533–535. (in Russian)
32. *Rabin M. O.* Recursive unsolvability of group theoretic problems. Ann. of Math., 1958, vol. 67, pp. 172–174.
33. *Zieschang H., Vogt E., and Coldewey H. D.* Surfaces and Planar Discontinuous Groups. Berlin, Springer Verlag, 1980. 336 p.
34. *Margolis S. W. and Meakin J. C.* E-unitary inverse monoids and the Cayley graph of a group representation. J. Pure Appl. Algebra, 1989, vol. 58, pp. 45–76.
35. *Kelarev A. V. and Quinn S. J.* On complete and bipartite Cayley graphs. Arbeitstagung Allgemeine Algebra 62, June 14–17, 2001. Abstracts. Linz, Austria, 2001, pp. 25.
36. *Kelarev A. V. and Praeger C. E.* On transitive Cayley graphs of groups and semigroups. Europ. J. Combinatorics, 2003, vol. 24, pp. 59–72.
37. *Kelarev A. V. and Quinn S. J.* A combinatorial property and Cayley graphs of semigroups. Semigroup Forum, 2002, vol. 66, no. 1, pp. 89–96.
38. *Kelarev A. V.* On undirected Cayley graphs. Australasian J. Combinatorics, 2002, vol. 25, pp. 73–78.
39. *Kelarev A. V.* On Cayley graphs of inverse semigroups. Semigroup Forum, 2006, vol. 72, pp. 411–418.

40. *Khosravi Be. and Khosravi Ba.* On Cayley graphs of semilattices of semigroups. Semigroup Forum, 2013, vol. 86, pp. 114–132.
41. *Khosravi Be. and Khosravi Ba.* A characterization of Cayley graphs of Brandt semigroups. Bull. Malaysian Math. Sci. Soc., 2012, vol. 2, no. 2, pp. 12–18.
42. *Khosravi B.* On Cayley graphs of left groups. Houston J. Math., 2009, vol. 35, no. 3, pp. 745–755.
43. *Fan S. and Zeng Y.* On Cayley graphs of Bands, Semigroup Forum, 2007, vol. 74, pp. 99–105.
44. *Makarjev A. L.* O polugruppakh idempotentov s atsiklicheskimi grafami Keli [About semigroups of idempotents with Cayley acyclic graphs]. Mathematics and Computer Science: Science and Education, 2007, vol. 6, pp. 26–34. (in Russian)
45. *Solomatin D. V.* Stroenie polugrupp, dopuskayushchikh vneshneplanarnye grafy Keli [Semigroups with outerplanar Cayley graphs]. Sib. Elektron. Mat. Izv., 2011, vol. 8, pp. 191–212. (in Russian)
46. *Makar'ev A. L.* Nil'potentnye polugruppy, osnova grafa Keli kotorykh yavlyaetsya derevom [Nilpotent semigroups whose Cayley graph base is a tree]. Mathematics and Computer Science: Science and Education, 2006, vol. 5, pp. 40–46. (in Russian)
47. *Makar'ev A. L.* Polureshetki s atsiklicheskimi grafami Keli [Semilattices with Cayley acyclic graphs]. Mathematics and Computer Science: Science and Education, 2008, vol. 7, pp. 28–33. (in Russian)
48. *Makar'ev A. L.* Ordinal'nye summy polugrupp s atsiklicheskimi grafami Keli [Ordinal sums of semigroups with Cayley acyclic graphs]. Herald of Omsk University, 2008, vol. 4, pp. 12–17. (in Russian)
49. *Martynov L. M. and Solomatin D. V.* Polugruppy vychetov s tsiklicheskimi gruppami obratimykh elementov, dopuskayushchie planarnye grafy Keli [Semigroups of residues with cyclic groups of invertible elements admitting planar Cayley graphs]. Herald of Omsk University, 2012, vol. 2, pp. 57–62. (in Russian)
50. *Martynov P. O. and Solomatin D. V.* Konechnye svobodnye kommutativnye polugruppy i polugruppy s nulem, dopuskayushchie obobshchennye vneshneplanarnye grafy Keli [Finite free commutative semigroups and semigroups with zero how admitting generalized outerplanar Cayley graphs]. Herald of Omsk University, 2014, vol. 3, pp. 22–26. (in Russian)
51. *Martynov P. O.* Konechnye svobodnye kommutativnye monoidy, dopuskayushchie obobshchenno vneshneplanarnye grafy Keli [Finite free commutative monoids who admitted generalized outerplanar Cayley graphs]. Herald of Omsk University, 2015, vol. 4, pp. 6–9. (in Russian)
52. *Martynov P. O.* Rassypchatye polugruppy, dopuskayushchie obobshchennye vneshneplanarnye grafy Keli [Crisp semigroups admit generalized outerplanar Cayley graphs]. Herald of Omsk University, 2018, vol. 3, pp. 6–9. (in Russian)
53. *Khosravi B.* Comparison of Cayley graphs of semigroups and Cayley graphs of groups. Book of Abstracts Caucasian Math. Conf. CMC II, Turkish Math. Society, 2007, pp. 18–19.
54. *Molchanov V. A.* A universal planar automaton is determined by its semigroup of input symbols. Semigroup Forum, 2011, vol. 82, pp. 1–9.
55. *Zhang X.* Clifford semigroups with genus zero. Proc. Intern. Conf. Semigroups, Acts and Categories with Applications to Graphs. University of Tartu, June 27–30, 2007. Tartu, EMS, 2008, pp. 151–160.
56. *Shevrin L. N.* Polugruppy [Semigroups]. Algebra (ed. L. A. Skornyakov), Ch. IV, Moscow, Nauka Publ., 1991, vol. 2, pp. 11–191. (in Russian)
57. *Emelichev V. A., Melnikov O. I., Sarvanov V. I., and Tyshkevich R. I.* Lekcii po eorii grafov [Lectures on Graph Theory]. Moscow, Nauka Publ., 1990. 384 p. (in Russian)

58. *Martynova T. A.* The groupoid of 0-reduced varieties of Semigroups. Semigroup Forum, 1983, vol. 26, pp. 249–274.
59. *Preston G. and Clifford A.* The Algebraic Theory of Semigroups. Amer. Math. Soc., 1964, vol. 1, no. 7, pp. 169–174.
60. *Solomatin D. V.* Rangi planarnosti mnogoobraziy kommutativnykh monoidov [Planarity ranks of the varieties of commutative monoids]. Herald of Omsk University, 2012, vol. 4, pp. 41–45. (in Russian)
61. *Solomatin D. V.* O dopustimosti nekotorykh grafov v kachestve grafov Keli polugrupp [On the admissibility of some graphs as Cayley graphs of semigroups]. Mathematics and Computer Science: Science and Education, 2004, vol. 4, pp. 32–34. (in Russian)
62. *Lempel A., Even S., and Cederbaum I.* An algorithm for planarity testing of graphs. Proc. Int. Symp. Theory Graphs, New York, 1967, pp. 215–232.
63. *Klein P. N. and Reif J. H.* An efficient parallel algorithm for planarity. J. Computer System Sci., 1988, vol. 37, pp. 190–246.
64. *Bader D. A. and Sreshta S. A.* New Parallel Algorithm for Planarity Testing. `https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.65.2914&rep=rep1&type=pdf`, 2003.
65. *Solomatin D. V.* O kriteriyakh planarnosti grafov Keli polugrupp [About the criteria of planarity for Cayley graphs of semigroups]. Mathematics and Computer Science: Science and Education, 2010, vol. 9, pp. 44–46. (in Russian)
66. *Solomatin D. V.* Stokhasticheskiy algoritm poiska podgrafa, gomeomorfnogo zadannomu [Stochastic algorithm for search a homeomorphic subgraph]. Conference paper: Stochastic Models in Biology and Limit Algebras (Omsk, 2–7 August 2010), Sobolev Institute of Mathematics SB RAS, 2010, pp. 98–100. (in Russian)
67. *Kambites M.* The loop problem for Rees matrix semigroups. Semigroup Forum, 2008, vol. 76, no. 2, pp. 204–216.
68. *Melikhov A. N., Bershtein L. S., and Kureichik V. M.* Primenenie grafov dlya proektirovaniya diskretnykh ustroystv [Application of Graphs in the Design of Discrete Devices]. Moscow, Nauka, 1974. 304 p. (in Russian)
69. *Levinson H.* On the genera of graphs of group presentations. Ann. New York Acad. Sci., 1970, vol. 175, pp. 277–284.
70. *Solomatin D. V.* Svobodnye chastichno kommutativnye n-veernye polureshetki s planarnymi grafami Keli [Free partially commutative semigroups and the n-fan semilattices with planar Cayley graphs]. Mathematics and Computer Science: Science and Education, 2009, vol. 8, pp. 36–39. (in Russian)
71. *Solomatin D. V.* Svobodnye chastichno kommutativnye nil'potentnye polugruppy s planarnymi grafami Keli [Free partially commutative nilpotent semigroups with planar Cayley graphs]. Herald of Omsk University, 2014, vol. 3, pp. 28–36. (in Russian)
72. *Solomatin D. V.* Konechnye svobodnye kommutativnye polugruppy s planarnymi grafami Keli [Finite free commutative semigroups with planar Cayley graphs]. Mathematics and Computer Science: Science and Education, 2003, vol. 3, pp. 32–38. (in Russian)
73. *Solomatin D. V.* Konechnye svobodnye kommutativnye monoidy, dopuskayushchie planarnyy graf Keli [Finite free commutative monoids admitting planar Cayley graph]. Herald of Omsk University, 2005, vol. 4, pp. 36–38. (in Russian)
74. *Birkhoff G.* On the structure of abstract algebras. Proc. Camb. Phil. Soc., 1935, vol. 31, pp. 433–454.

75. *Solomatin D. V.* Pryamye proizvedeniya tsiklicheskikh polugrupp, dopuskayushchie planarnyy graf Keli [Direct products of cyclic semigroups admitting a planar Caley graph]. Sib. Elektron. Mat. Izv., 2006, vol. 3, pp. 238–252. (in Russian)
76. *Solomatin D. V.* Pryamye proizvedeniya tsiklicheskikh monoidov i polugrupp s nulem, dopuskayushchie planarnye grafy Keli [Direct products of cyclic monoids and semigroups with zero admitting planar Cayley graphs]. Mathematics and Computer Science: Science and Education, 2006, vol. 5, pp. 51–64. (in Russian)
77. *Solomatin D. V.* Kriteriy planarnosti dlya grafov Keli 0-pryamykh ob"edineniy nil'potentnykh polugrupp [A planarity criterion for Cayley graphs of 0-direct unions of nilpotent semigroups]. Conf. paper: Maltsev Meeting 2010 (Novosibirsk, May 2–6, 2010), Sobolev Institute of Mathematics SB RAS, 2010, pp. 144. (in Russian)
78. *Solomatin D. V.* Rassypchatye polugruppy s planarnymi grafami Keli [Crisp semigroups with planar Cayley graphs]. Herald of Volgograd State Pedagogical University, 2005, vol. 4, pp. 27–31. (in Russian)
79. *Polyakova L. Yu.* Rezol'venty dlya svobodnykh chastichno kommutativnykh monoidov [Resolutions of free partially commutative monoids]. Siberian Math. J., 2007, vol. 48, pp. 1295–1304. (in Russian)
80. *Diekert V. and Métivier Y.* Partial commutation and traces. Handbook of Formal Languages. Berlin, Springer Verlag, 1997, vol. 3, pp. 457–533.
81. *Sedláček J.* On a generalization of outerplanar graphs. Časopis Pěst. Mat., 1988, vol. 2, no. 113, pp. 213–218. (in Czech)
82. *Solomatin D. V.* Planarnye gipergrafy mul'tiplikativnykh polugrupp vychetov [Planar hypergraphs of the multiplicative semigroup of residues]. Mathematics and Computer Science: Science and Education, 2011, vol. 10, pp. 30–34. (in Russian)
83. *Bulatov A. A.* Algebraicheskie metody issledovaniya kombinatornykh zadach [Algebraic methods in the study of combinatorial problems]. Diss. of the Doctor Phys.-Mat. Sci., Ekaterinburg, 2008. (in Russian)
84. *Zinbiel G. W.* Encyclopedia of Types of Algebras. arXiv:1101.0267v1, 2010.
85. *Sudoplatov S. V.* Hypergraphs of prime models and distributions of countable models of small theories. J. Math. Sci., 2010, vol. 169, no. 5, pp. 680–695.
86. *Zykov A. A.* Gipergrafy [Hypergraphs]. Uspekhi Mat. Nauk, 1974, vol. 29, no. 6(180), pp. 89–154. (in Russian)
87. *Solomatin D. V.* Konechno porozhdennye polugruppy s odnim opredelyayushchim sootnosheniem i tozhdestvom, dopuskayushchie planarnyy graf Keli [Finitely generated semigroups with one defining relation and identity admitting planar Cayley graph]. Mathematics and Computer Science: Science and Education, 2007, vol. 6, pp. 42–48. (in Russian)
88. *Solomatin D. V.* Ordinal'nye summy pryamougol'nykh polugrupp, dopuskayushchie planarnye grafy Keli [Ordinal sums of rectangular semigroups admitting a planar Cayley graph]. Mathematics and Computer Science: Science and Education, 2008, vol. 7, pp. 33–41. (in Russian)
89. *Solomatin D. V.* Planarnye mnogoobraziya polugrupp [Planar varieties of semigroups]. Sib. Elektron. Mat. Izv., 2015, vol. 12, pp. 232–247. (in Russian)
90. *Solomatin D. V.* Planarnye mnogoobraziya kommutativnykh polugrupp [Planar varieties of commutative semigroups]. Herald of Omsk University, 2015, vol. 2, pp. 17–22. (in Russian)
91. *Solomatin D. V.* Rangi planarnosti mnogoobraziy kommutativnykh polugrupp [The ranks of planarity for varieties of commutative semigroups]. Prikladnaya Diskretnaya Matematika, 2016, no. 4(34), pp. 50–64. (in Russian)

92. *Solomatin D. V.* O rangakh planarnosti mnogoobraziy polugrupp idempotentov, nil'polugrupp i polugrupp s perestanovochnym tozhdestvom [On ranks of the planarity of varieties of all idempotent semigroups, nilsemigroups, and semigroups with the permutation identity]. Herald of Omsk University, 2017, vol. 4, no. 86, pp. 11–21. (in Russian)
93. *Solomatin D. V.* O rangakh planarnosti mnogoobraziy nil'polugrupp [On ranks of planarity of nil-semigroups varieties]. Herald of Omsk University, 2019, vol. 2, no. 24, pp. 17–22. (in Russian)
94. *Solomatin D. V.* Rangi planarnosti mnogoobraziy polugrupp [The ranks of the planarity for varieties of semigroups]. Herald of Omsk University, 2019, vol. 4, pp. 9–15. (in Russian)
95. *Hopcroft J. and Tarjan R.* Efficient Planarity Testing, J. ACM, 1974, vol. 21, no. 4, pp. 549–568.
96. *Chiba N., Yamanouchi T., and Nishizeki T.* Linear algorithms for convex drawings of planar graphs. J. A. Bondy, U. S. R. Murty (eds.). Progress in Graph Theory. London, Academic Press, 1984, pp. 153–173.
97. *Head T. J.* The varieties of commutative monoids. Nieuw Archief voor Wiskunde, 1968, vol. 3, no. 16, pp. 203–206.
98. *Solomatin D. V.* Rangi planarnosti mnogoobraziy polugrupp, zadannykh tozhdestvom $x \approx x^n$ [Ranks of planarity for the variety of semigroups defined by the identity $x \approx x^n$]. Herald of Omsk University, 2020, vol. 25, no. 3, pp. 13–17. (in Russian)
99. *Evans T.* The lattice of semigroup varieties. Semigroup Forum, 1971, vol. 2, pp. 1–43.
100. *Arthan R. and Oliva P.* Studying algebraic structures using Prover9 and Mace4. G. Hanna et al. (eds.) Proof Technology in Mathematics Research and Teaching, Ch. 5, Springer, 2020.
101. *Fennemore C.* All varieties of bands. Semigroup Forum, 1970, vol. 1, pp. 172–179.
102. *Green J. A. and Rees D.* On semigroups in which $x^r = x$. Proc. Cambridge Philos. Soc., 1952, vol. 48, pp. 35–40.
103. *Howie J. M.* Fundamentals of Semigroup Theory. London Math. Society Monographs, New Series, 12, Oxford Science Publ., N.Y., Clarendon Press, Oxford University Press, 1995. 351 p.
104. *Preston G. and Clifford A.* The Algebraic Theory of Semigroups. Amer. Math. Soc., 1961, vol. 1, no. 1, pp. 12–31.
105. *Ljapin E. S.* Semigroups. Amer. Math. Soc., 4th ed., 1963. 519 p.
106. *Solomatin D. V.* Teoriya predstavleniy [Representation Theory]. Tutorial. Omsk, OmSPU Publ., 2015. 64 p. (in Russian)
107. *Gurevich Yu. Sh.* Problema ravenstva slov dlya nekotorykh klassov polugrupp [The word problem for some classes of semigroups]. Algebra and Logic, 1966, vol. 5, no. 5, pp. 25–35. (in Russian)
108. *De Verdière Y. C.* Sur un Nouvel Invariant des Graphes et un Critère de Planarité. J. Combinat. Theory, Ser. B, 1990, no. 50, pp. 11–21.
109. *Kantorovich L. V. and Krylov V. I.* Approximate Methods of Higher Analysis. Noordhoff, Interscience Interscience, 1958. 704 p.
110. *Fedorov F. M.* On the theory of infinite systems of linear algebraic equations. TWMS J. Pure Appl. Math., 2015, vol. 2, no. 6, pp. 202–212.
111. *Martynov L. M.* Polnota, redutsirovannost', primarnost' i chistota dlya algebr: rezul'taty i problemy [Completeness, reducibility, primarity and purity for algebras: results and problems]. Sib. Elektron. Mat. Izv., 2016, vol. 13, pp. 181–241. (in Russian)

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.719.2+512.542.74 DOI 10.17223/20710410/54/2

ОБ ИНВАРИАНТНЫХ ПОДПРОСТРАНСТВАХ В XSL-ШИФРАХ

Д. И. Трифонов*, Д. Б. Фомин**

*Технический комитет по стандартизации «Криптографическая защита информации», г. Москва, Россия,

**Национальный исследовательский университет «Высшая школа экономики», г. Москва, Россия

E-mail: d.arlekino@gmail.com, dfomin@hse.ru

Исследуется рассеивание подпространств, инвариантных относительно нелинейного преобразования XSL-шифра, линейным преобразованием. Приведён конструктивный способ поиска подпространств, инвариантных относительно одной итерации XSL-шифра. Показано, что подпространства, инвариантные относительно нелинейных преобразований из некоторых классов, не сохраняются любой матрицей, построенной из ненулевых элементов расширения поля $\mathbb{F}_2$. На основании теоретико-графового и группового подходов доказан ряд свойств множеств специального вида, инвариантных относительно раундовой функции XSL-шифра.

Ключевые слова: *XSL-шифр, SP-сеть, инвариантное подпространство.*

INVARIANT SUBSPACES IN SPN BLOCK CIPHER

D. I. Trifonov*, D. B. Fomin**

*Technical committee «Cryptography and Security Mechanism», Moscow, Russia,

**Higher School of Economics, Moscow, Russia

Let there exist subsets of $\mathbb{F}_2^n$ that the non-linear layer of an SP-network maps to some other subset of $\mathbb{F}_2^n$. We study the possibility of existence of subsets of $\mathbb{F}_2^n$ that are invariant under the SP-layer. It is shown that subspaces invariant under nonlinear transformations from some classes are not preserved by any matrix without nonzero elements of the field extension $\mathbb{F}_2$. The paper also studies the question of the existence of invariant subsets of the form $A_{i_1} \times \ldots \times A_{i_m}$, where $n = m \cdot n'$, $A_{i_j} \subseteq \mathbb{F}_2^{n'}$, $j = 1, \ldots, m$. Some properties of such invariant sets of the round function of the SP-layer are proved on the basis of the graph-theoretic and group-theoretic approaches. We study the capacity of these sets and, using additional assumptions, show that A_{i_j}, $j = 1, \ldots, m$, should be cosets of some subspaces of $\left(\mathbb{F}_2^{n'}, +\right)$ of equal size. A constructive way of constructing such sets is proposed.

Keywords: *SP-network, SPN, invariant subspaces.*

Введение

С конца XX в. широкое распространение получили блочные криптографические алгоритмы. Большинство из них построено по итеративному принципу, где каждая итерация представляет собой чередование линейных и локальных нелинейных преобразований информационного блока.

В связи с появлением линейного и разностного методов криптографического анализа [1, 2] были сформулированы требования на выбор нелинейных и линейных рассеивающих преобразований для обеспечения стойкости относительно этих методов (см., например, [1, 3, 4] и др.). Изучению линейных и нелинейных преобразований посвящено много работ отечественных и зарубежных специалистов [2–26].

Таким образом, сформировался уже устоявшийся подход к построению блочных шифров, стойких относительно линейного и разностного методов: в качестве нелинейных необходимо использовать преобразования, обеспечивающие необходимые характеристики относительно линейного и разностного методов, а в качестве линейных — преобразования с достаточно высокими коэффициентами рассеивания. По такому принципу построено много криптографических алгоритмов, среди которых можно отметить российский стандарт блочного шифрования «Кузнечик» [27].

Вопрос о влиянии приводимости линейных преобразований на стойкость блочных криптографических алгоритмов поставлен в обзоре [28]. Изучению структурных свойств линейных преобразований посвящены работы [29–32].

В работе [32] наличие инвариантных подпространств у линейного преобразования позволило усилить разностную атаку на криптографический алгоритм ICEBERG (Involution Cipher Efficient for Block Encryption in Reconfigurable Hardware) [33]. В [34] построена атака на алгоритм Khazad [21], существенно использующая приводимость линейного преобразования. При этом в алгоритме используется максимально рассеивающее линейное преобразование и локальные нелинейные преобразования (подстановки) с высокими криптографическими характеристиками.

Наличие инвариантных подпространств у линейного преобразования делает необходимым при синтезе XSL-шифра исследовать вопрос, насколько хорошо данные подпространства рассеиваются нелинейным слоем. В данной работе предлагается несколько другой подход: сначала выделить подпространства, инвариантные для нелинейных преобразований, а затем изучить вопрос, насколько хорошо данные подпространства рассеиваются линейным слоем. Частично этот вопрос исследован в [35, 36].

1. Основные определения и обозначения

В работе используются следующие определения и обозначения. Через $\mathbb{F}_q$ обозначим конечное поле из q элементов, где $q = p^n$, p — простое число, $n \in \mathbb{N}$. Пусть $V_n(2^d)$ — векторное пространство размерности $n \in \mathbb{N}$ над полем $\mathbb{F}_{2^d}$. Обозначим полную линейную группу в её естественном действии на пространстве $V_n(2^d)$ через $\mathrm{GL}_n(2^d)$, при этом если $d = 1$, то будем писать $\mathrm{GL}_n = \mathrm{GL}_n(2)$.

Множество всех матриц из m строк и n столбцов с элементами из поля $\mathbb{F}_q$ обозначим $(\mathbb{F}_q)_{m,n}$, в случае поля $\mathbb{F}_2$ будем использовать обозначение $(\mathbb{F}_2)_{n,n} = M_n$. Кольцо многочленов от одного переменного x над полем $\mathbb{F}_q$ обозначим $\mathbb{F}_q[x]$; множество всех подстановок множества U — $S(U)$; $\mathbf{0}^{(l)} \in V_l$ — вектор $\mathbf{0}^{(l)} = (0, \ldots, 0)$.

Прежде чем сформулировать основные результаты, напомним несколько фактов из теории конечных полей [37].

Рассмотрим способ представления элементов конечного поля $\mathbb{F}_q$ с помощью матриц. Пусть $f(x) = x^n + f_{n-1}x^{n-1} + \ldots + f_1 x + f_0 \in \mathbb{F}_q[x]$ есть унитарный многочлен степени

$n \in \mathbb{N}$. Его сопровождающей матрицей называется следующая квадратная матрица порядка n:

$$S(f(x)) = \begin{pmatrix} 0 & 0 & \dots & -f_0 \\ 1 & 0 & \dots & -f_1 \\ \dots & \dots & \dots & \dots \\ \dots & 1 & 0 & -f_{n-2} \\ 0 & \dots & 1 & -f_{n-1} \end{pmatrix}.$$

Из теоремы Гамильтона — Кэли (см., например, [38, с. 62, теорема 8]) следует, что матрица $A = S(f(x))$ удовлетворяет уравнению $f(A) = \mathbf{O}_{n,n}$, то есть

$$A^n + f_{n-1}A^{n-1} + \ldots + f_1 A + f_0 \mathbf{I}_{n,n} = \mathbf{O}_{n,n},$$

где $\mathbf{O}_{n,n}$ — нулевая матрица порядка n; $\mathbf{I}_{n,n}$ — единичная матрица порядка n.

Элементы поля $\mathbb{F}_{p^n}$ могут быть представлены всевозможными многочленами над $\mathbb{F}_p$ от матрицы $A = S(f(x))$ степеней меньше n. Далее многочлен $f(x)$ и соответствующую ему матрицу $S(f(x)) = A$ будем считать фиксированными.

Рассмотрим только случай $p = 2$. Элементы поля $\mathbb{F}_{2^{n'}}$, $n' \in \mathbb{N}$, могут быть представлены в виде матриц размера $n' \times n'$ над полем $\mathbb{F}_2$ следующим образом:

$$a_{n'-1} \cdot A^{n'-1} \oplus \ldots \oplus a_1 \cdot A \oplus a_0 \cdot \mathbf{I}_{n',n'}, \tag{1}$$

где $a_k \in \{0, 1\}$, $k = 0, \ldots, n' - 1$.

Пусть $\mathbb{F}_{2^{n'}} = \mathbb{F}_2[x]/f(x)$, $n' \in \mathbb{N}$, $\deg f(x) = n'$, $f[x] \in \mathbb{F}_2[x]$ неприводим и θ — класс вычетов по модулю $f(x)$, содержащий x. Пусть также $A = S(f(x))$. Элементам поля $\mathbb{F}_{2^{n'}}$ поставим во взаимно однозначное соответствие элементы вида (1) следующим образом: элементу $z_0 \oplus z_1 \cdot \theta \oplus \ldots \oplus z_{n'-1} \cdot \theta^{n'-1}$, $z_i \in \{0, 1\}$, $i = 0, 1, \ldots, n'-1$, соответствует элемент $z_0 \cdot \mathbf{I}_{n',n'} \oplus z_1 \cdot A \oplus \ldots \oplus z_{n'-1} \cdot A^{n'-1}$.

Через $\overline{\mathbb{F}}_{2^{n'}}$ будем обозначать описанное выше матричное представление поля из $2^{n'}$ элементов.

2. Постановка задачи

Рассмотрим XSL-шифр со следующими параметрами: n — размер блока в битах, m — число нелинейных биективных преобразований (подстановок) на подвекторах длины n', $n = n' \cdot m$.

При реализации изучаемых алгоритмов используются следующие преобразования:

- *наложение ключа* $\mathrm{X}[K] \colon V_n \to V_n$, где $\mathrm{X}[K](a) = K \oplus a$; $a, K \in V_n$;
- *нелинейное преобразование* $\mathrm{S} \colon V_n \to V_n$, $\mathrm{S}(a) = \mathrm{S}(a_1, \ldots, a_m) = (\pi(a_1), \ldots, \pi(a_m))$, $a_i \in V_{n'}$, $\pi \in S(V_{n'})$, $i = 1, \ldots, m$;
- *линейное преобразование* $\mathrm{L} \colon V_n \to V_n$, $\mathrm{L}(a) = a \cdot L'$, где $L' \in \mathrm{GL}_n$.

В [3, 4] отмечено, что для противодействия линейному и разностному методам криптографического анализа линейное преобразование должно обладать достаточно высоким коэффициентом рассеивания. Большинство способов построения максимально рассеивающих матриц из GL_n сводится к построению матриц из $\mathrm{GL}_m\left(2^{n'}\right)$ в известных классах: циркулянты, матрицы Коши, матрицы Коши — Адамара [3, 39] и некоторых других. Отметим также возможность построения при помощи направленного поиска максимально рассеивающих матриц с примитивным характеристическим многочленом [40]. Таким образом, широкое распространение получают матрицы из GL_n, полученные из матриц $\mathrm{GL}_m\left(2^{n'}\right)$. В рассматриваемом XSL-шифре будем использовать два типа матриц. Для их описания приведём необходимые определения.

Рассмотрим отображение $\varphi\colon \mathbb{F}_{2^{n'}} \to M_{n'}$, которое элементу $\alpha \in \mathbb{F}_{2^{n'}}$ ставит в соответствие матрицу из $M_{n'}$, определяемую равенством (1). Зададим также отображение $\psi\colon \mathrm{GL}_m(2^{n'}) \to \mathrm{GL}_{n'm}$, которое матрице $B = (\mathbf{B}_{i,j})_{m,m} \in \mathrm{GL}_m(2^{n'})$ ставит в соответствие следующую матрицу $\psi(B) \in \mathrm{GL}_{n'm}$:

$$\psi(B) = \begin{pmatrix} \varphi(\mathbf{B}_{1,1}) & \dots & \varphi(\mathbf{B}_{1,m}) \\ \vdots & \ddots & \vdots \\ \varphi(\mathbf{B}_{m,1}) & \dots & \varphi(\mathbf{B}_{m,m}) \end{pmatrix}.$$

Матрицами типа I будем называть матрицы $\psi(B)$, такие, что $\mathbf{B}_{i,j} \neq 0$ для всех $i, j = 1, \dots, m$.

Матрицами типа II будем называть матрицы $C \in M_{n'm}$ вида

$$C = \begin{pmatrix} C_{1,1} & \dots & C_{1,m} \\ \vdots & \ddots & \vdots \\ C_{m,1} & \dots & C_{m,m} \end{pmatrix},$$

где $C_{i,j} \in M_{n'}$ невырождены, $i, j = 1, \dots, m$.

Замечание 1. Матрицы типа I являются матрицами типа II. Обратное, вообще говоря, неверно.

Большинство нелинейных биективных преобразований, используемых в современных криптографических алгоритмах, имеют достаточно простую алгебраическую структуру. Например, в AES [4], Grand-Cru [41], Mugi [42], Scream [43], Camelia [44], Square [45] используются подстановки, аффинно эквивалентные подстановке обращения ненулевых элементов поля $\mathbb{F}_{2^8}$. Подстановки белорусского стандарта [46] аффинно эквивалентны экспоненциальной подстановке, а подстановки российских стандартизированных алгоритмов «Кузнечик» [27] и «Стрибог» [47] имеют так называемую TU-декомпозицию, как и подстановки, рассматриваемые в [13, 14, 48, 49].

Наличие простой алгебраической структуры подстановки часто влечёт наличие смежных классов, инвариантных относительно данной подстановки. Например, нетрудно убедиться, что для подстановки обращения ненулевых элементов поля инвариантным подпространством будет любое подполе данного поля. Данное свойство подстановки может являться потенциальной слабостью относительно методов, использующих различные гомоморфизмы [50].

3. Основные результаты

Одним из основных вопросов, рассматриваемых в данной работе, является изучение случая, когда подмножество множества $V_{n'}^m$, которое является инвариантным относительно действия слоя подстановок, сохраняется линейным преобразованием.

Множество $W \subseteq V_n$ будем называть инвариантным относительно преобразования $g\colon V_n \to V_n$, если для любого $x \in W$ выполнено включение $g(x) \in W$. Для преобразования g определим множество $g(W)$, равное множеству образов всех элементов из W под действием преобразования g, то есть

$$g(W) = \{g(x)\colon x \in W\}.$$

В данных обозначениях множество W инвариантно относительно преобразования g, если $g(W) \subseteq W$. Будем использовать экспоненциальную форму записи действия произвольного отображения: $g(a) = a^g$, $a \in V_n$.

Пусть $K \in V_{n'}^m \cong V_n$ — раундовый ключ рассматриваемого блочного криптографического алгоритма. Интересен вопрос поиска множеств $G_K \subset V_n$, инвариантных относительно произведения преобразований $\mathrm{L} \circ \mathrm{S} \circ \mathrm{X}[K]$:

$$G_K = G_K^{\mathrm{L} \circ \mathrm{S} \circ \mathrm{X}[K]}.$$

Наличие таких множеств для большого числа ключей может говорить о возможных слабостях в раундовом преобразовании шифра [36].

Пусть множество $U \subset V_{n'}$ инвариантно относительно подстановки π. Рассмотрим множество

$$W = W_1 \times \ldots \times W_m,$$

где $W_i \in \{U, V_{n'}\}$, которое, очевидно, инвариантно относительно преобразования S. При фиксированном ключе $K \in V_{n'}^m$ для построения множества G_K необходимо изучить вопрос, в каких случаях множество W является инвариантным относительно линейного преобразования L.

Случай, когда для всех $i = 1, \ldots, m$ выполнено равенство $W_i = V_{n'}$, является тривиальным и не представляет интереса для построения множества G_K. Поэтому будем рассматривать следующие варианты построения множества W:

С л у ч а й 1. Существует единственный $i \in \{1, \ldots, m\}$, такой, что $W_i = U$.

С л у ч а й 2. Существуют $i_1 < \ldots < i_j$, $i_1, \ldots, i_j \in \{1, \ldots, m\}$, $j \in 1, \ldots, m-1$, такие, что $W_{i_1} = \ldots = W_{i_j} = U$.

С л у ч а й 3. Для всех $i = 1, \ldots, m$ выполнено равенство $W_i = U$.

Утверждение 1. Пусть подпространство $U < V_{n'}$, $U \neq V_{n'}$, инвариантно относительно подстановки π. Пусть для множества $W = W_1 \times \ldots \times W_m$, где $W_i \in \{U, V_{n'}\}$, не для всех $i = 1, \ldots, m$ выполнено $W_i = V_{n'}$. Кроме того, пусть в преобразовании L используется матрица $C = (C_{i,j})_{m,m} \in \mathrm{GL}_{n'm}$ типа II. Тогда справедливы следующие утверждения:

1) если существует $i \in \{1, \ldots, m\}$, такое, что $W_i = V_{n'}$, то множество W не является инвариантным относительно матрицы C;
2) если для любого $i = 1, \ldots, m$ выполнено $W_i = U$ и существуют $j_1, j_2 \in \in \{1, \ldots, m\}$, такие, что $C_{j_1,j_2}(U) \neq U$, то множество W не является инвариантным относительно матрицы C;
3) если для любого $i = 1, \ldots, m$ выполнено $W_i = U$ и $C_{j_1,j_2}(U) = U$ при всех $j_1, j_2 = 1, \ldots, m$, то $C(W) = W$.

Доказательство.

1) Покажем, что в данном случае при $C(W) = W'$, $W = W_1 \times \ldots \times W_i \times \ldots \times W_m$, $W' = W_1' \times \ldots \times W_i' \times \ldots \times W_m'$ и $W_i = V_{n'}$ получается, что для любых $j = 1, \ldots, m$ выполнено $W_j' \neq U$.

Во введённых обозначениях

$$W_j' = C_{1,j}(W_1) \oplus C_{2,j}(W_2) \oplus \ldots \oplus C_{m,j}(W_m),$$

где для множеств $A, B \subseteq V_n$ под множеством $A \oplus B$ будем понимать множество различных векторов $a \oplus b$ при всех $a \in A$ и $b \in B$.

Следовательно, в силу того, что $U \neq V_{n'}$, равенство $W_j' = U$, $j = 1, \ldots, m$ возможно лишь когда матрица $C_{i,j}$ вырождена, что противоречит условию утверждения. Таким образом, подпространство W не является инвариантным относительно матрицы C.

2) Пусть $C(W) = W'$, $W = W_1 \times \ldots \times W_{j_1} \times \ldots \times W_m$, $W' = W'_1 \times \ldots \times W'_{j_1} \times \ldots \times W'_m$ и $W_i = U$, $i = 1, \ldots, m$. Тогда

$$W'_{j_2} = C_{1,j_2}(W_1) \oplus C_{2,j_2}(W_2) \oplus \ldots \oplus C_{m,j_2}(W_m).$$

В силу того, что $C_{j_1,j_2}(U) \neq U$, $W'_{j_2} \neq U$ при всех $j_2 = 1, \ldots, m$. Таким образом, подпространство W не является инвариантным относительно матрицы C.

3) В справедливости данного утверждения можно убедиться, рассмотрев доказательство п. 2 с условием $C_{j_1,j_2}(U) = U$ при всех $j_1, j_2 = 1, \ldots, m$. ■

Рассмотрим следующий случай. Пусть в рассматриваемом XSL-шифре $n' = 2n''$ и множество R_1 векторов вида

$$(\underbrace{0, \ldots, 0}_{n''}, x_{n''+1}, \ldots, x_{2n''}) \in V_{n'},$$

где $(x_{n''+1}, \ldots, x_{2n''}) \in V_{n''}$, инвариантно относительно преобразования π. При фиксированном ключе K шифра рассмотрим вопрос построения множества G_K, инвариантного относительно преобразования $\mathrm{L} \circ \mathrm{S} \circ \mathrm{X}[K]$.

Нетрудно убедиться, что множество

$$W = W_1 \times \ldots \times W_m,$$

где $W_i = R_1$, $i = 1, \ldots, m$, инвариантно относительно преобразования S. Для построения множества G_K необходимо рассмотреть условия, которым должна удовлетворять матрица $C = (C_{i,j})_{m,m}$, используемая в линейном преобразовании L. Согласно п. 3 утверждения 1, должны быть выполнены равенства $C_{i,j}(R_1) = R_1$, $i, j = 1, \ldots, m$. Ответ на вопрос, выполнимо ли последнее равенство при использовании матриц типа I, даёт следующая

Теорема 1. Пусть $\mathbf{B} \in \overline{\mathbb{F}}_{2^{n'}}$, $\mathbf{B} \neq 0$, $\mathbf{B} \neq 1$. Тогда множество R_1 не является инвариантным относительно матрицы $\varphi(\mathbf{B})$.

Доказательство. Введём следующее обозначение: $A \begin{pmatrix} i_1, \ldots, i_k \\ j_1, \ldots, j_l \end{pmatrix}$ — подматрица матрицы $A \in \mathrm{GL}_{n'}$, полученная из A удалением всех строк, кроме строк с номерами $i_1 < \ldots < i_k$, и всех столбцов, кроме столбцов с номерами $j_1 < \ldots < j_l$.

Переформулируем утверждение теоремы. Необходимо показать, что существует $x \in V_{n''}$, такой, что

$$(\mathbf{0}^{(n'')}, x) \cdot \varphi(\mathbf{B}) = (y_1, y_2),$$

где $y_1 \neq \mathbf{0}^{(n'')}$.

Доказательство теоремы будем проводить методом от противного. Предположим, что для любого $x \in V_{n''}$ выполнено

$$(\mathbf{0}^{(n'')}, x) \cdot \varphi(\mathbf{B}) = (\mathbf{0}^{(n'')}, y_2) \tag{2}$$

при некотором $y_2 \in V_{n''}$.

Рассмотрим первые n'' столбцов матрицы $\varphi(\mathbf{B})$, т. е. подматрицу $\varphi(\mathbf{B}) \begin{pmatrix} 1, \ldots, 2n'' \\ 1, \ldots, n'' \end{pmatrix}$. Заметим, что для выполнения равенства (2) для любых $x \in V_{n''}$ необходимо и достаточно, чтобы $\varphi(\mathbf{B}) \begin{pmatrix} n''+1, & \ldots, & 2n'' \\ 1, & \ldots, & n'' \end{pmatrix} = \mathbf{O}_{n'',n''}$.

Рассмотрим для элемента $\mathbf{B}$ поля $\overline{\mathbb{F}}_{2^{2n''}}$, которое задаётся неприводимым над $\mathbb{F}_2$ многочленом $f(x)$ степени $2n''$, представление в виде (1):

$$b_{2n''-1} \cdot S(f(x))^{2n''-1} \oplus \ldots \oplus b_1 \cdot S(f(x)) \oplus b_0 \cdot \mathbf{I}_{2n'',2n''}.$$

Непосредственной проверкой можно убедиться в следующем:

— при возведении матрицы $S(f(x))$ в степень i матрица $S(f(x))^i$ получается из матрицы $S(f(x))^{i-1}$ сдвигом всех столбцов на один влево и дописыванием последнего столбца, вид которого полностью определяется коэффициентами многочлена $f(x)$, $i = 2, \ldots, 2n'' - 1$;

— в матрицах $\mathbf{I}_{2n'',2n''}, S(f(x)), S(f(x))^2, \ldots, S(f(x))^{2n''-1}$ в первом столбце присутствует ровно одна единица, которая для матрицы $S(f(x))^i$ стоит в $(i+1)$-й строке, $i = 0, \ldots, 2n'' - 1$.

Таким образом, если рассмотреть элемент $\mathbf{B}$ поля $\mathbb{F}_{2^{2n''}}$ в виде (1), то равенство $\varphi(\mathbf{B}) \begin{pmatrix} n''+1, \ldots, 2n'' \\ 1, \ldots, n'' \end{pmatrix} = \mathbf{O}_{n'',n''}$ верно тогда и только тогда, когда выполнено одно из следующих условий:

1) $b_k = 0$, $k = 0, \ldots, 2n'' - 1$. Однако в этом случае $\mathbf{B} = 0$, что противоречит условию теоремы;
2) $b_0 = 1$, $b_k = 0$, $k = 1, \ldots, 2n'' - 1$. Однако в этом случае $\mathbf{B} = 1$, что противоречит условию теоремы.

Полученные противоречия завершают доказательство теоремы. ■

Замечание 2. Пусть $\mathbf{B} \in \overline{\mathbb{F}}_{2^{n'}}$, $\mathbf{B} = 1$. Тогда множество R_1 является инвариантным относительно матрицы $\varphi(\mathbf{B})$.

Утверждение 2. Пусть $n' = 2n''$, $n'' \in \mathbb{N}$, $m \geqslant 2$, $B = (\mathbf{B}_{i,j})_{m,m} \in \mathrm{GL}_m(2^{2n''})$ и матрица $\psi(B)$ является матрицей типа I. Тогда множества $W^{(1)}, W^{(2)}, W^{(3)}$ не являются инвариантными относительно преобразования $\psi(B)$, где

1) $W^{(1)} = W_1 \times \ldots \times W_m$ и существует единственный $i \in \{1, \ldots, m\}$, такой, что $W_i = R_1$;
2) $W^{(2)} = W_1 \times \ldots \times W_m$ и существуют $i_1 < \ldots < i_j$, $i_1, \ldots, i_j \in \{1, \ldots, m\}$, $j \in \in \{1, \ldots, m-1\}$, такие, что $W_{i_1} = \ldots = W_{i_j} = R_1$;
3) $W^{(3)} = W_1 \times \ldots \times W_m$ и для всех $i = 1, \ldots, m$ выполнено равенство $W_i = R_1$.

Доказательство. Справедливость утверждения следует из теоремы 1, а также п. 3 утверждения 1. ■

Аналогичные результаты можно сформулировать и для XSL-шифров, где в качестве линейного преобразования используется матрица типа II.

Утверждение 3. Пусть $n' \in \mathbb{N}$, $C = (c_{i,j}) \in M_{n'}$, $R_2 < V_{n'}$,

$$R_2 = \{(x_1, \ldots, x_{n'})\colon x_{j_1} = \ldots = x_{j_l} = 0, j_1 < \ldots < j_l; j_1, \ldots, j_l \in \{1, \ldots, n'\}; 1 \leqslant l < n'\}.$$

Тогда множество R_2 является инвариантным относительно матрицы C тогда и только тогда, когда $C \begin{pmatrix} \{1, \ldots, n'\} \setminus \{j_1, \ldots, j_l\} \\ j_1, \ldots, j_l \end{pmatrix} = \mathbf{O}_{n'-l,l}$.

Доказательство. Аналогично доказательству теоремы 1 с учётом того, что выполнимость условия утверждения означает существование в матрице C нулевой подматрицы $C \begin{pmatrix} \{1, \ldots, n'\} \setminus \{j_1, \ldots, j_l\} \\ j_1, \ldots, j_l \end{pmatrix}$. ■

Пример 1. Для иллюстрации теоремы 1 приведём конкретный пример. Пусть $n'' = 4$ и $\mathbf{B} \in \overline{\mathbb{F}}_{2^8}$, $\mathbf{B} \neq 0$, $\mathbf{B} \neq 1$. Поле $\overline{\mathbb{F}}_{2^8}$ задаётся неприводимым над $\mathbb{F}_2$ многочленом $f(x) = x^8 + \sum\limits_{i=0}^{7} f_i x_i$. Приведём в явном виде матрицы $A^i = (S(f(x)))^i$, $i = 0, \ldots, 7$:

$$E = \left(\begin{array}{cccc|cccc} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ \hline 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1 \end{array}\right), \quad A = \left(\begin{array}{cccc|cccc} 0&0&0&0&0&0&0&f_0\\ 1&0&0&0&0&0&0&f_1\\ 0&1&0&0&0&0&0&f_2\\ 0&0&1&0&0&0&0&f_3\\ \hline 0&0&0&1&0&0&0&f_4\\ 0&0&0&0&1&0&0&f_5\\ 0&0&0&0&0&1&0&f_6\\ 0&0&0&0&0&0&1&f_7 \end{array}\right),$$

$$A^2 = \left(\begin{array}{cccc|cccc} 0&0&0&0&0&0&f_0&*\\ 0&0&0&0&0&0&f_1&*\\ 1&0&0&0&0&0&f_2&*\\ 0&1&0&0&0&0&f_3&*\\ \hline 0&0&1&0&0&0&f_4&*\\ 0&0&0&1&0&0&f_5&*\\ 0&0&0&0&1&0&f_6&*\\ 0&0&0&0&0&1&f_7&* \end{array}\right), \quad A^3 = \left(\begin{array}{cccc|cccc} 0&0&0&0&0&f_0&*&*\\ 0&0&0&0&0&f_1&*&*\\ 0&0&0&0&0&f_2&*&*\\ 1&0&0&0&0&f_3&*&*\\ \hline 0&1&0&0&0&f_4&*&*\\ 0&0&1&0&0&f_5&*&*\\ 0&0&0&1&0&f_6&*&*\\ 0&0&0&0&1&f_7&*&* \end{array}\right),$$

$$A^4 = \left(\begin{array}{cccc|cccc} 0&0&0&0&f_0&*&*&*\\ 0&0&0&0&f_1&*&*&*\\ 0&0&0&0&f_2&*&*&*\\ 0&0&0&0&f_3&*&*&*\\ \hline 1&0&0&0&f_4&*&*&*\\ 0&1&0&0&f_5&*&*&*\\ 0&0&1&0&f_6&*&*&*\\ 0&0&0&1&f_7&*&*&* \end{array}\right), \quad A^5 = \left(\begin{array}{cccc|cccc} 0&0&0&f_0&*&*&*&*\\ 0&0&0&f_1&*&*&*&*\\ 0&0&0&f_2&*&*&*&*\\ 0&0&0&f_3&*&*&*&*\\ \hline 0&0&0&f_4&*&*&*&*\\ 1&0&0&f_5&*&*&*&*\\ 0&1&0&f_6&*&*&*&*\\ 0&0&1&f_7&*&*&*&* \end{array}\right),$$

$$A^6 = \left(\begin{array}{cccc|cccc} 0&0&f_0&*&*&*&*&*\\ 0&0&f_1&*&*&*&*&*\\ 0&0&f_2&*&*&*&*&*\\ 0&0&f_3&*&*&*&*&*\\ \hline 0&0&f_4&*&*&*&*&*\\ 0&0&f_5&*&*&*&*&*\\ 1&0&f_6&*&*&*&*&*\\ 0&1&f_7&*&*&*&*&* \end{array}\right), \quad A^7 = \left(\begin{array}{cccc|cccc} 0&f_0&*&*&*&*&*&*\\ 0&f_1&*&*&*&*&*&*\\ 0&f_2&*&*&*&*&*&*\\ 0&f_3&*&*&*&*&*&*\\ \hline 0&f_4&*&*&*&*&*&*\\ 0&f_5&*&*&*&*&*&*\\ 0&f_6&*&*&*&*&*&*\\ 1&f_7&*&*&*&*&*&* \end{array}\right).$$

Здесь элементы, обозначенные «$*$», полностью определяются коэффициентами многочлена $f(x)$ и не приводятся из-за громоздкости их записи.

Покажем, что множество R_1 не инвариантно относительно матрицы $\varphi(\mathbf{B})$. Действительно, согласно доказательству теоремы 1, для того, чтобы множество R_1 было инвариантным относительно преобразования $\varphi(\mathbf{B})$, необходимо и достаточно, чтобы $\varphi(\mathbf{B}) \binom{5, \ldots, 8}{1, \ldots, 4} = \mathbf{O}_{n'', n''}$.

Рассмотрим элемент $\mathbf{B}$ в виде (1):

$$\mathbf{B} = a_7 \cdot A^7 \ \oplus \ a_6 \cdot A^6 \ \oplus \ \ldots \ \oplus \ a_1 \cdot A \ \oplus \ a_0 \cdot \mathbf{I}_{8,8},$$

$a_k \in \{0, 1\}$, $k = 0, \ldots, 7$. Отметим, что в первом столбце матрицы A^i присутствует ровно одна единица в строке с номером $i + 1$, $i = 0, \ldots, 7$. Таким образом,

$\varphi(\mathbf{B})\binom{5,\ldots,8}{1,\ldots,4} = \mathbf{O}_{n'',n''}$ тогда и только тогда, когда $a_k = 0$, $k = 0,\ldots,7$. Однако в этом случае $\varphi(\mathbf{B}) = \mathbf{O}_{8,8}$. Полученное противоречие подтверждает теорему 1.

Замечание 3. Существуют подстановки, обладающие высокими криптографическими характеристиками, относительно которых множество R_1 будет инвариантным. Примерами могут служить подстановки, исследуемые в [13, 14]. Ещё одним примером являются подстановки обращения ненулевых элементов поля $\mathbb{F}_{2^{2n'}}$. По теореме о башне полей [37], в поле $\mathbb{F}_{2^{2n'}}$ существует подполе $\mathbb{F}_{2^{n'}}$. Тогда можно подобрать подстановку, аффинно эквивалентную заданной, относительно которой множество R_1 будет инвариантным.

Рассмотрим XSL-шифр с линейным преобразованием, задаваемым матрицей типа II. Опишем один подход к поиску множеств $G_K \subset V_n$, инвариантных относительно композиции преобразований $\mathrm{X}[K]\circ\mathrm{L}\circ\mathrm{S}$. Пусть имеется пара семейств множеств $(\mathcal{A},\mathcal{B})$:

$$\mathcal{A} = \{A_1, A_2, \ldots, A_{e_a}\},\ A_i \subseteq V_{n'},$$
$$\mathcal{B} = \{B_1, B_2, \ldots, B_{e_b}\},\ B_i \subseteq V_{n'},$$

и для любого $i \in \{1,\ldots,e_a\}$ существует $j \in \{1,\ldots,e_b\}$, такой, что $A_i^{\pi} \subseteq B_j$. Рассмотрим семейства $\mathcal{A}^m$ и $\mathcal{B}^m$ — декартовы степени множеств $\mathcal{A}$ и $\mathcal{B}$. Тогда для любого элемента $A_{i_1} \times \ldots \times A_{i_m} \in \mathcal{A}^m$ существует элемент $B_{j_1} \times \ldots \times B_{j_m} \in \mathcal{B}^m$, такой, что

$$(A_{i_1} \times \ldots \times A_{i_m})^{\mathrm{S}} = \left(A_{i_1}^{\pi} \times \ldots \times A_{i_m}^{\pi}\right) \subseteq B_{j_1} \times \ldots \times B_{j_m}.$$

Множество G_K будем искать среди подмножеств множества $\mathcal{A}^m$, то есть его элементами являются множества вида $A_{i_1} \times A_{i_2} \times \ldots \times A_{i_m} \in \mathcal{A}^m$.

Пусть $\mathcal{C}$ — такое семейство множеств, что для любого элемента $B_{j_1} \times \ldots \times B_{j_m} \in \mathcal{B}^m$ существует элемент C семейства $\mathcal{C}$, для которого выполняется включение

$$(B_{j_1} \times \ldots \times B_{j_m})^{\mathrm{L}} \subseteq C.$$

Пусть также существует такой $K \in V_{n'}^m$, что $\mathcal{C}^{\mathrm{X}[K]} = \mathcal{A}^m$, то есть верна следующая диаграмма:

$$\mathcal{A}^m \xrightarrow{\mathrm{S}} \mathcal{B}^m \xrightarrow{\mathrm{L}} \mathcal{C} \xrightarrow{\mathrm{X}[K]} \mathcal{A}^m. \tag{3}$$

Все дальнейшие рассуждения будем проводить в предположении выполнимости диаграммы (3). В этом случае, очевидно, выполняется равенство $|\mathcal{C}| = |\mathcal{A}^m|$. Действительно, рассмотрим элемент $A_{i_1} \times A_{i_2} \times \ldots \times A_{i_m} \in \mathcal{A}^m$, $i_1,\ldots,i_m \in \{1,\ldots,e_a\}$. Пусть $K = (k_1, k_2, \ldots, k_m)$. Тогда

$$(A_{i_1} \oplus k_1) \times (A_{i_2} \oplus k_2) \times \ldots \times (A_{i_m} \oplus k_m) \in \mathcal{C}.$$

Таким образом, множество C состоит из прямого произведения множеств вида $A_j \oplus k_i$, $j \in \{1,\ldots,e_a\}$, $i \in \{1,\ldots,m\}$.

Утверждение 4. Пусть имеется XSL-шифр, линейное преобразование которого $L = (l_{a,b})_{m\times m}$, $l_{a,b} \in GL_{n'}(2)$, $a,b = 1,\ldots,m$, задаётся матрицей типа II. Рассмотрим множества

$$B = B_{i_1} \times B_{i_2} \times \ldots \times B_{i_m} \in \mathcal{B}^m, \quad i_1,\ldots,i_m \in \{1,\ldots,e_b\},$$
$$C = C_{j_1} \times C_{j_2} \times \ldots \times C_{j_m} \in \mathcal{C}, \quad j_1,\ldots,j_m \in \{1,\ldots,e_a\},$$

такие, что $B^{\mathrm{L}} \subseteq C$, и для некоторого ключа $K \in V_{n'}^m$ выполнена диаграмма (3). Тогда для любого $j \in \{j_1,\ldots,j_m\}$ выполнено неравенство $|C_j| \geqslant \max\limits_{i\in\{i_1,\ldots,i_m\}} |B_i|$.

Доказательство. Пусть $x_v \in B_{i_v}$, $v = 1, \ldots, m$. Для произвольного $w \in \in \{1, \ldots, m\}$ рассмотрим следующую сумму:

$$S = \sum_{v=1}^{m} x_v \cdot l_{v,w}. \tag{4}$$

Так как $B^{\mathrm{L}} \subseteq C$, то $S \in C_{j_w}$ при любой фиксации $x_v \in B_{i_v}$, $v \in \{1, \ldots, m\}$.

Заметим, что $|C_{j_w}|$ не меньше мощности множества различных значений сумм вида (4), получаемых при различных фиксациях значений $x_v \in B_{i_v}$, $v = 1, \ldots, m$. Фиксируем произвольное $v' \in \{1, \ldots, m\}$, а также $x_v \in B_{i_v}$, $v \in \{1, \ldots, m\} \setminus \{v'\}$ и рассмотрим сумму

$$S_{v'} = \sum_{v \in \{1,\ldots,m\} \setminus \{v'\}} x_v \cdot l_{v,w}.$$

Тогда мощность множества

$$\left\{ S_{v'} + x_{v'} \cdot l_{v',w} : x_{v'} \in B_{i_{v'}} \right\},$$

во-первых, не больше мощности множества C_{j_w} и, во-вторых, равна мощности множества $B_{i_{v'}}$. Действительно, так как L — матрица типа II, то $l_{v',w}$ обратима и мощность множества

$$\left\{ x_{v'} \cdot l_{v',w} : x_{v'} \in B_{i_{v'}} \right\}$$

равна мощности множества $B_{i_{v'}}$. Отсюда для любого $v' \in \{1, \ldots, m\}$ выполняется равенство

$$|C_{j_w}| \geqslant \left| \left\{ x_{v'} \cdot l_{v',w} \in B_{i_{v'}} \right\} \right|,$$

которое завершает доказательство утверждения 4. ■

Из верности диаграммы 3 следует, что для любых $i_1, \ldots, i_m \in \{1, \ldots, e_a\}$ существуют такие $j_1, \ldots, j_m \in \{1, \ldots, e_a\}$, что верна диаграмма

$$A_{i_1} \times \ldots \times A_{i_m} \xrightarrow{\mathrm{X}[K] \circ \mathrm{L} \circ \mathrm{S}} A_{j_1} \times \ldots \times A_{j_m}.$$

Зададим на семействе $\mathcal{A}^m$ ориентированный граф Γ с помеченными дугами следующим образом. Вершинами этого графа являются элементы семейства $\mathcal{A}^m$, при этом вершины $X, Y \in \mathcal{A}^m$ соединены дугой с пометкой K тогда и только тогда, когда существует ключ K, такой, что $X^{\mathrm{X}[K] \circ \mathrm{L} \circ \mathrm{S}} \to Y$. Если $V_{n'} \in \mathcal{A}$, то очевидно, что для произвольного ключа K

$$(V_{n'}^m)^{\mathrm{X}[K] \circ \mathrm{L} \circ \mathrm{S}} = V_{n'}^m$$

есть цикл, который будем называть тривиальным. Для построения множества G_K необходимо уметь искать нетривиальные циклы в графе Γ. В частности, G_K — множество вершин графа Γ, лежащих на циклах длины 1 (петлях) с пометкой K. Однако далее рассмотрим и более общий случай, когда цикл состоит из более чем одной вершины. Предположим, что в графе Γ существует нетривиальный цикл длины r, задаваемый подсемейством семейства $\mathcal{A}^m$. Это эквивалентно тому, что некоторое подмножество $\mathcal{A}^m$ является инвариантным относительно r раундов рассматриваемого блочного шифра для некоторых ключей $K_1, \ldots, K_r$. Найдём необходимые условия существования нетривиального цикла и предложим конструктивный алгоритм его поиска.

Пусть здесь и далее $\mathcal{A}' \subset \mathcal{A}^m$ — множество вершин графа Γ, задающее некоторый нетривиальный цикл длины r. Обозначим $\mathcal{B}' = (\mathcal{A}')^{\mathrm{S}}$, $\mathcal{C}' = (\mathcal{B}')^{\mathrm{L}}$. При этом для каждого $A \in \mathcal{A}'$ существуют ключ K и множество $C \in \mathcal{C}'$, такие, что $C^{\mathrm{X}[K]} = A$.

Утверждение 5. Пусть имеется XSL-шифр, линейное преобразование которого $L = (l_{a,b})_{m\times m}$, $l_{a,b} \in GL_{n'}(2)$, $a, b = 1, \ldots, m$, задаётся матрицей типа II, элементы семейства $\mathcal{A}'$ задают некоторый нетривиальный цикл графа Γ, $A_{a_1} \times \ldots \times A_{a_m} \in \mathcal{A}'$, и

$$B_{b_1} \times \ldots \times B_{b_m} \in \mathcal{B}',\ B_{b_1} \times \ldots \times B_{b_m} = \mathrm{S}\left(A_{a_1} \times \ldots \times A_{a_m}\right),$$
$$C_{c_1} \times \ldots \times C_{c_m} \in \mathcal{C}',\ C_{c_1} \times \ldots \times C_{c_m} = \mathrm{L}\left(B_{b_1} \times \ldots \times B_{b_m}\right).$$

Тогда:

1) $|A_{a_1}| = |B_{b_1}| = |C_{c_1}|$;
2) $|A_{a_1}| = |A_{a_2}| = \ldots = |A_{a_m}|$;
3) $|B_{b_1}| = |B_{b_2}| = \ldots = |B_{b_m}|$;
4) $|C_{c_1}| = |C_{c_2}| = \ldots = |C_{c_m}|$.

Доказательство. Множество $A_{a_1} \times \ldots \times A_{a_m} \in \mathcal{A}'$ лежит на цикле длины r. Тогда для некоторых ключей $K_1, \ldots, K_r$ верна следующая диаграмма, описывающая действие функций на соответствующие множества:

$$A_{a_1} \times \ldots \times A_{a_m} \xrightarrow{\mathrm{S}} \underbrace{B_{b_1} \times \ldots \times B_{b_m}}_{\in\mathcal{B}} \xrightarrow{\mathrm{L}} \underbrace{C_{c_1} \times \ldots \times C_{c_m}}_{\in\mathcal{C}'} \xrightarrow{\mathrm{X}[K_1]}$$
$$\xrightarrow{\mathrm{X}[K_1]} \underbrace{A_{d_1} \times \ldots \times A_{d_m}}_{\in\mathcal{A}'} \xrightarrow{\mathrm{X}[K_2]} \ldots \xrightarrow{\mathrm{X}[K_r]} \underbrace{A_{a_1} \times \ldots \times A_{a_m}}.$$

Отсюда следует, что $|C_{c_v}| = |A_{d_v}|$, $v = 1, \ldots, m$. Заметим, что по построению множеств $\mathcal{A}'$ и $\mathcal{B}'$ выполнено неравенство $|B_{b_v}| \geqslant |A_{a_v}|$, $v = 1, \ldots, m$, а по утверждению 4 — $|C_{c_v}| \geqslant |B_{b_w}|$, $v, w = 1, \ldots, m$.

Тогда, так как вершина $A_{a_1} \times \ldots \times A_{a_m}$ лежит на цикле в графе Γ, для любого $v = 1, \ldots, m$ имеет место

$$|A_{a_v}| \leqslant |B_{b_v}| \leqslant |C_{c_v}| = |A_{d_v}| \leqslant \ldots \leqslant |A_{a_v}|,$$

откуда следует доказательство п. 1 утверждения 5.

Для доказательства п. 2–4 достаточно доказать только один из них и воспользоваться цепочкой неравенств выше. Не теряя общности, покажем, что $|C_{c_1}| = |C_{c_2}|$. Для остальных пар индексов равенство доказывается аналогично.

Воспользуемся утверждением 4, а также фактом, что произвольное множество $A_{a_1} \times \ldots \times A_{a_m}$ лежит на цикле в графе Γ:

$$|C_{c_1}| = |A_{a_1}| \leqslant |B_{b_1}| \leqslant |C_{c_2}| = |A_{a_2}| \leqslant |B_{b_2}| \leqslant |C_{c_1}| \leqslant \ldots \leqslant |C_{c_1}|.$$

Утверждение доказано. ■

Следующее утверждение позволяет сформулировать алгоритм поиска циклов в графе Γ или доказать, что нетривиальных циклов нет.

Утверждение 6. Пусть для XSL-шифра, линейное преобразование которого $L = (l_{a,b})_{m\times m}$, $l_{a,b} \in GL_{n'}(2)$, $a, b = 1, \ldots, m$, задаётся матрицей типа II, элементы семейства $\mathcal{A}'$ образуют некоторый нетривиальный цикл графа Γ. Пусть также

$$B = B_{i_1} \times B_{i_2} \times \ldots \times B_{i_m} \in \mathcal{B}', \quad C = C_{j_1} \times C_{j_2} \times \ldots \times C_{j_m} \in \mathcal{C}',$$

где $C = B^{\mathrm{L}}$. Тогда:

1) для произвольного $v \in \{1, \ldots, m\}$ множество B_{i_v} является смежным классом по некоторому подпространству пространства $V_{n'}$;
2) для произвольного $v \in \{1, \ldots, m\}$ множество C_{j_v} является смежным классом по некоторому подпространству пространства $V_{n'}$.

Доказательство. По п. 1 утверждения 5 верно равенство

$$C_{j_w} = \left\{ \sum_{v=1}^{m} b_v \cdot l_{v,w} : b_v \in B_{i_v},\ v \in \{1, \ldots, m\} \right\}.$$

Зафиксируем произвольные $v', v'' \in \{1, \ldots, m\}$, $x_v \in B_{i_v}$, $v \in \{1, \ldots, m\}$. Пользуясь п. 1 и 3 утверждения 5, запишем:

$$C_{j_w} = \left\{ \sum_{v \in \{1,\ldots,m\} \setminus \{v'\}} x_v \cdot l_{v,w} \oplus y_{v'} \cdot l_{v',w} : y_{v'} \in B_{i_{v'}} \right\},$$

$$C_{j_w} = \left\{ \sum_{v \in \{1,\ldots,m\} \setminus \{v''\}} x_v \cdot l_{v,w} \oplus y_{v''} \cdot l_{v'',w} : y_{v''} \in B_{i_{v''}} \right\}.$$

Отсюда следует, что множества

$$C'(x_{v''}) = \left\{ x_{v''} \cdot l_{v'',w} \oplus y_{v'} \cdot l_{v',w} : y_{v'} \in B_{i_{v'}} \right\} \text{ и } C''(x_{v'}) = \left\{ x_{v'} \cdot l_{v',w} \oplus y_{v''} \cdot l_{v'',w} : y_{v''} \in B_{i_{v''}} \right\}$$

равны. Запишем их в следующем виде:

$$C'\left(x_{v''}\right) = B_{i_{v'}} \cdot l_{v',w} \oplus x_{v''} \cdot l_{v'',w}, \quad C''\left(x_{v'}\right) = B_{i_{v''}} \cdot l_{v'',w} \oplus x_{v'} \cdot l_{v',w}.$$

Тогда

$$\forall\ x_{v'} \in B_{i_{v'}} \forall x_{v''} \in B_{i_{v''}} \left(C'(x_{v''}) = C''(x_{v'}) \right). \tag{5}$$

Из (5) следует, что

$$\left(B_{i'_v} + x_{v'}\right) \cdot l_{v',w} = \left(B_{i''_v} + x_{v''}\right) \cdot l_{v'',w}.$$

Так как $l_{v',w}$ невырождена, то

$$\forall x_1, x_2 \in B_{i_{v'}} \left(B_{i_{v'}} \oplus x_1 = B_{i_{v'}} \oplus x_2 \right). \tag{6}$$

Рассмотрим случай, когда $0 \in B_{i_{v'}}$. Пользуясь (6), получим

$$\forall x_1 \in B_{i_{v'}} \left(B_{i_{v'}} = B_{i_{v'}} \oplus x_1 \right).$$

Отсюда следует, что $B_{i_{v'}}$ замкнуто относительно операции сложения и является группой по сложению (векторным пространством).

Пусть теперь $0 \notin B_{i_{v'}}$. Фиксируем произвольное $x_1 \in B_{i_{v'}}$ и рассмотрим множество $H = x_1 \oplus B_{i_{v'}}$. Очевидно, что $0 \in H$. Покажем, что множество H замкнуто относительно операции сложения. Для этого покажем, что для любых $x_1, x_2 \in B_{i_{v'}}$ их сумма лежит в множестве $B_{i_{v'}}$. Действительно, пользуясь формулой (6), запишем:

$$B_{i_{v'}} = B_{i_{v'}} \oplus (x_1 \oplus x_2).$$

Таким образом, $B_{i_{v'}}$ является либо подпространством пространства $V_{n'}^m$, либо смежным классом по некоторому подпространству пространства $V_{n'}^m$. Для остальных индексов доказательство аналогично.

Для множеств C_{j_w} доказательство аналогично ввиду обратимости матрицы L. ■

Следствие 1. Пусть в условиях утверждения 6

$$A = A'_{i_1} \times A'_{i_2} \times \ldots \times A'_{i_m} \in \mathcal{A}'.$$

Тогда для любого $j \in \{1, \ldots, m\}$ множество A'_{i_j} является смежным классом по некоторому подпространству пространства $V_{n'}$.

Таким образом, нас в первую очередь интересуют такие пары множеств (A, B), что $A^{\pi} = B$, $A = H_A \oplus h_A$, $B = H_B \oplus h_B$, и H_A, H_B — подпространства пространства $V_{n'}$, $h_A, h_B \in V_{n'}$.

Предположим, имеется M пар таких множеств (A_i, B_i), $i \in \{1, \ldots, M\}$, при этом $A_i = H_{A,i} \oplus h_{A,i}$, $B_i = H_{B,i} \oplus h_{B,i}$, $|A_i| = |A_j|$ для всех $i, j \in \{1, \ldots, M\}$. Необходимость одинаковости мощностей множеств A_i обусловлена аналогичным требованием для множеств, образующих цикл в графе Γ. Рассмотрим вектор $h \in V_{n'}^m$:

$$h = (h_{B,i_1}, h_{B,i_2}, \ldots, h_{B,i_m}),\ i_1, \ldots, i_m \in \{1, \ldots, M\}.$$

Всего таких векторов $|M|^m$.

Для каждых $v, w = 1, \ldots, m$ вычислим множество $C(h, v, w) \subset V_{n'}$:

$$C(h, v, w) = \left\{ \sum_{b=1}^{m} h_{B,i_b} \cdot l_{b,w} + y \cdot l_{v,w} : y \in H_{B,v} \right\}$$

— и проверим, существуют ли такие $g(w) \in V_{n'}$ и $j(w) \in \{1, \ldots, M\}$, зависящие от w, что

$$C(h, v, w) \oplus g(w) = A_{j(w)}.$$

То есть при разных v, но одинаковых w множество $A_{j(w)}$ и элемент $g(w)$ должны быть одинаковыми. Докажем следующую теорему.

Теорема 2. Пусть для XSL-шифра, линейное преобразование которого $L = (l_{a,b})_{m \times m}$, $l_{a,b} \in GL_{n'}(2)$, $a, b = 1, \ldots, m$, задаётся матрицей типа II, элементы семейства $\mathcal{A}'$ образуют некоторый нетривиальный цикл в графе Γ. Пусть также $A_i = H_{A,i} \oplus h_{A,i}$, $H_{A,i}$ — подпространство пространства $V_{n'}$, $h_{A,i} \in V_{n'}$, $i \in \{1, \ldots, M\}$, при этом $|A_i| = |A_j|$ для всех $i, j \in \{1, \ldots, M\}$. Для множества $A \in \mathcal{A}'$,

$$A = A_{i_1} \times A_{i_2} \times \ldots \times A_{i_m},\ i_1, \ldots, i_m \in \{1, \ldots, M\},$$

существует такой ключ K, что $A^{\mathrm{L} \circ \mathrm{S} \circ \mathrm{X}[K]} = A' \in \mathcal{A}'$,

$$A' = A_{j_1} \times A_{j_2} \times \ldots \times A_{j_m},\ j_1, \ldots, j_m \in \{1, \ldots, M\},$$

тогда и только тогда, когда для каждого $w \in \{1, \ldots, m\}$ существуют вектор $g(w) \in V_{n'}$ и номер $j(w) \in \{1, \ldots, M\}$, такие, что для любого $v \in \{1, \ldots, m\}$ выполнено равенство

$$C(h, v, w) \oplus g(w) = A_{j(w)},$$

где

$$C(h, v, w) = \left\{ \sum_{b=1}^{m} h_{B,i_b} \cdot l_{b,w} \oplus y \cdot l_{v,w} : y \in H_{B,v} \right\}.$$

Доказательство.

Докажем в прямую сторону методом от противного. Возможны два случая:

1) существует v, для которого не существует такого $g \in V_{n'}$, что $C(h, v, w) \oplus g \neq A_j$ хотя бы для одного $j \in \{1, \ldots, M\}$;
2) для некоторого w не существуют такие $g(w)$ и $A_{j(w)}$, что $C(h, v, w) \oplus g(w) = A_{j(w)}$.

В первом случае получаем противоречие с условием теоремы. Рассмотрим подробно второй случай.

Возьмём произвольный $x \in B$, $x = (x_1, x_2, \ldots, x_m)$. Так как для каждого $i \in \in \{1, \ldots, M\}$ верно $A_i = H_{A,i} \oplus h_{A,i}$, то $x = y \oplus h$, где $h = (h_{A,i_1}, h_{A,i_2}, \ldots, h_{A,i_m})$; $y = (y_1, y_2, \ldots, y_m)$; $y_i \in H_{A,i}$. Тогда

$$x \cdot L = y \cdot L \oplus h \cdot L.$$

Рассмотрим множество

$$Y_w = \left\{ y \cdot L_w^{\downarrow} : y \in H_{A,i_1} \times \ldots \times H_{A,i_m} \right\},$$

где $L_w^{\downarrow}$ — столбец матрицы L с номером w. Так как по условию теоремы $(Y_w \oplus h \cdot L) \oplus \oplus k = A_{j_w}$ для некоторого $k \in V_{n'}$, то $|A_{j_w}| = |Y_w|$; и по условию $|A_{i_a}| = |A_{j_b}|$ для всех $a, b \in \{1, \ldots, m\}$. Из мощностных соображений и того факта, что $0 \in H_{A,i_v}$ для всех $v \in \{1, \ldots, m\}$, получаем

$$\forall v \in \{1, \ldots, m\} \left(Y_w = \{ y_v \cdot l_{i_v,w} : y \in H_{A,i_v} \} \right).$$

Это противоречит тому, что для фиксированного w не существует таких $g(w)$ и $A_{j(w)}$, так как множество $\{ y_v \cdot l_{i_v,w} : y \in H_{A,i_v} \}$ одинаково для всех v.

Обратное очевидно. ■

С помощью теоремы 2 можно конструктивно строить инварианты для раундового преобразования XSL-шифра рассматриваемого вида. В общем случае можно воспользоваться методом нелинейных инвариантов [51]: функция $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ называется нелинейным инвариантом преобразования $g \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, если для любого $x \in \mathbb{F}_2^n$ и некоторой константы $c \in \mathbb{F}_2$ выполняется равенство

$$f(x) + f(g(x)) = c.$$

В работе [52] исследуются нелинейные инварианты раундовых преобразований XSL-алгоритмов и указаны условия на нелинейные биективные преобразования и матрицы, необходимые для существования таких инвариантов.

Авторы выражают благодарность Д. А. Довганю и Д. А. Бурову за конструктивные замечания в ходе обсуждения данной работы.

ЛИТЕРАТУРА

1. *Малышев Ф. М.* Двойственность разностного и линейного методов в криптографии // Матем. вопр. криптогр. 2014. Т. 5. Вып. 3. С. 35–48.
2. *Matsui M.* Linear cryptanalysis method for DES Cipher // LNCS. 1994. V. 765. P. 386–397.
3. *Малышев Ф. М., Трифонов Д. И.* Рассеивающие свойства XSLP-шифров // Матем. вопр. криптогр. 2016. Т. 7. Вып. 3. С. 47–60.
4. *Daemon J. and Rijmen V.* The Design of Rijndael: AES — The Advanced Encryption Standard. Berlin; Heidelberg: Springer, 2002. 238 p.
5. *Сидельников В. М.* О взаимной корреляции последовательностей // Проблемы кибернетики. 1971. Вып. 24. С. 15–42.

6. *Nyberg K.* Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 55–64.
7. *Bilgin B., Nikova S., Nikov V., et al.* Threshold Implementations of all 3×3 and 4×4 S-boxes. IACR Cryptology ePrint Archive. 2012. http://eprint.iacr.org/2012/300.
8. *Bora A., Tolga M. S., and Ercan B.* Classifying 8-bit to 8-bit S-boxes based on power mappings from the point of DDT and LAT distributions // LNCS. 2008. V. 5130. P. 123–133.
9. *Biryukov A., De Cannière C., Braeken A., and Preneel B.* A toolbox for cryptanalysis: Linear and affine equivalence algorithms // LNCS. 2003. V. 2656. P. 33–50.
10. *Leander G. and Poschmann A.* On the classification of 4 bit S-boxes // LNCS. 2007. V. 4547. P. 159–176.
11. *Saarinen M. J. O.* Cryptographic analysis of all 4×4-bit S-boxes // LNCS. 2012. V. 7118. P. 118–133.
12. *Menyachikhin A. V.* Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters // Матем. вопр. криптогр. 2017. Т. 8. Вып. 2. С. 97–116.
13. *Fomin D. B.* New classes of 8-bit permutations based on a butterfly structure // Матем. вопр. криптогр. 2019. Т. 10. Вып. 2. С. 169–180.
14. *Фомин Д. Б.* Построение подстановок пространства V_{2m} с использованием $(2m, m)$-функций // Матем. вопр. криптогр. 2020. Т. 11. Вып. 3. С. 121–138.
15. *Фомин Д. Б.* Об алгебраической степени и дифференциальной равномерности подстановок пространства V_{2m}, построенных с использованием $(2m, m)$-функций // Матем. вопр. криптогр. 2020. Т. 11. Вып. 4. С. 133–149.
16. *Feistel H.* Cryptography and computer privacy // Scientific American. 1973. V. 225(5). P. 15–23.
17. *Feistel H., Notz W. A., and Smith J. L.* Some cryptographic techniques for machine to machine data communications // Proc. IEEE. 1975. V. 63(11). P. 1545–1554.
18. *Webster A. F. and Tavares S. E.* On the design of S-boxes // LNCS. 1986. V. 218. P. 523–534.
19. *Augot D. and Finiasz M.* Direct Construction of Recursive MDS Diffusion Layers using Shortened BCH Codes. IACR Cryptology ePrint Archive. 2014. http://eprint.iacr.org/2014/566.
20. *Augot D. and Finiasz M.* Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions // IEEE Intern. Symp. Inform. Theory. 2013. P. 1551–1555.
21. *Barreto P. and Rijmen V.* The KHAZAD Legacy-Level Block Cipher. Submission to NESSIE. 2000. https://www.researchgate.net/publication/228924670_The_Khazad_legacy-level_block_cipher.
22. *Gupta K. C. and Ray I. G.* On constructions of involutory MDS matrices // LNCS. 2013. V. 7918. P. 43–60.
23. *Junod P. and Vaudenay S.* Perfect diffusion primitives for block ciphers building efficient MDS matrices // LNCS. 2004. V. 3357. P. 84–99.
24. *Nakahara J. Jr. and Abrahao E.* A new involutory MDS matrix for the AES // Intern. J. Network Security. 2009. V. 9(2). P. 109–116.
25. *Poschmann A.* Lightweight Cryptography — Cryptographic Engineering for a Pervasive World. IACR Cryptology ePrint Archive. 2009. http://eprint.iacr.org/2009/516.
26. *Анашкин А. В.* Полное описание одного класса MDS-матриц над конечным полем характеристики 2 // Матем. вопр. криптогр. 2017. Т. 8. Вып. 4. С. 5–28.
27. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015.
28. D.STVL.9 — Ongoing Research Areas in Symmetric Cryptography. ECRYPT, 2008. 108 p.

29. *Погорелов Б. А., Пудовкина М. А.* Комбинаторная характеризация XL-слоёв // Матем. вопр. криптогр. 2013. Т. 4. Вып. 3. С. 99–129.
30. *Погорелов Б. А., Пудовкина М. А.* О расстояниях от подстановок до импримитивных групп при фиксированной системе импримитивности // Дискретная математика. 2013. Т. 25. № 3. С. 78–95.
31. *Погорелов Б. А., Пудовкина М. А.* О расстоянии от подстановок до объединения всех импримитивных групп с равными параметрами систем импримитивности // Дискретная математика. 2014. Т. 26. № 1. С. 103–117.
32. *Пудовкина М. А.* О вероятностях r-раундовых пар разностей XSL-алгоритма блочного шифрования Маркова с приводимым линейным преобразованием // Прикладная дискретная математика. Приложение. 2014. № 7. С. 52–54.
33. *Standaert F. X., Piret G., Rouvroy G., et al.* ICEBERG : An involutional cipher efficient for block encryption in reconfigurable hardware // LNCS. 2004. V. 3017. С. 279–299.
34. *Burov D. A. and Pogorelov B. A.* An attack on 6 rounds of KHAZAD // Матем. вопр. криптогр. 2016. Т. 7. Вып. 2. С. 35–46.
35. *Burov D. A. and Pogorelov B. A.* The permutation group insight on the diffusion property of linear mappings // Матем. вопр. криптогр. 2018. Т. 9. Вып. 2. С. 47–58.
36. *Буров Д. А.* Подгруппы прямого произведения групп, инвариантные относительно действия подстановок на сомножителях // Дискретная математика. 2019. Т. 31. № 4. С. 3–19.
37. *Лидл Р., Нидеррайтер Г.* Конечные поля. В 2-х т. Пер. с англ. М.: Мир, 1988.
38. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра: учебник. В 2-х т. Т. 2. М.: Гелиос АРВ, 2003.
39. *Sim S. M., Khoo K., Oggier F. E., and Peyrin T.* Lightweight MDS involution matrices // FSE. 2015. P. 471–493.
40. *Coy Puente O. and de la Cruz Jiménez R. A.* Construction of orthomorphic MDS matrices with primitive characteristic polynomial // CTCrypt'20. 2020. `https://ctcrypt.ru/files/files/Oliver\CTCrypt2020.pdf`.
41. *Khan A. A. and Murtaza G.* Efficient Implementation of Grand Cru with TI C6x+ Processor. IACR Cryptology ePrint Archive. 2011. `http://eprint.iacr.org/2011/385`.
42. *Watanabe D., Furuya S., Yoshida H., et al.* A new keystream generator MUGI // LNCS. 2002. V. 2365. P. 179–194.
43. *Halevi S., Coppersmith D., and Jutla C. S.* Scream: A Software-Efficient Stream Cipher. IACR Cryptology ePrint Archive. 2002. `http://eprint.iacr.org/2002/019`.
44. `http://www.cryptonessie.org` — The New European Schemes for Signatures, Integrity and Encryption (NESSIE). 2003.
45. *Daeman J., Knudsen L. R., and Rijmen V.* The block cipher SQUARE // FSE'97. 1997. V. 1267. P. 149–156.
46. *Агиевич С. В., Галинский В. А., Микулич Н. Д., Харин Ю. С.* Алгоритм блочного шифрования BelT. `elib.bsu.by`.
47. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Стандартинформ, 2012.
48. *Biryukov A., Perrin L., and Udovenko A.* Reverse-engineering the S-box of Streebog, Kuznyechik and STRIBOBr1 // LNCS. 2016. V. 9665. P. 372–402.
49. *Perrin L.* Partitions in the S-Box of Streebog and Kuznyechik. Cryptology ePrint Archive. 2019. `https://eprint.iacr.org/2019/092`.
50. *Горчинский Ю. Н.* О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями // Труды по дискретной математике. 1997. Т. 1. С. 67–84.

51. *Todo Y., Leander G., and Sasaki Y.* Nonlinear Invariant Attack — Practical Attack on Full SCREAM, iSCREAM, and Midori64. Cryptology ePrint Archive. 2016. https://eprint.iacr.org/2016/732.

52. *Буров Д. А.* О существовании нелинейных инвариантов специального вида для раундовых преобразований XSL-алгоритмов // Дискретная математика. 2021. Т. 33. № 2. С. 31–45.

REFERENCES

1. *Malyshev F. M.* Dvoystvennost' raznostnogo i lineynogo metodov v kriptografii [The duality of differential and linear methods in cryptography]. Matem. Vopr. Kriptogr., 2014, vol. 5, no. 3, pp. 35–48. (in Russian)
2. *Matsui M.* Linear cryptanalysis method for DES cipher. LNCS, 1994, vol. 765, pp. 386–397.
3. *Malyshev F. M. Trifonov D. I.* Rasseivayushchiye svoystva XSLP-shifrov [Diffusion properties of XSLP-ciphers]. Matem. Vopr. Kriptogr., 2016, vol. 7, no. 3, pp. 47–60. (in Russian)
4. *Daemon J. and Rijmen V.* The Design of Rijndael: AES — The Advanced Encryption Standard. Berlin; Heidelberg, Springer, 2002. 238 p.
5. *Sidel'nikov V. M.* O vzaimnoy korrelyatsii posledovatel'nostey [Cross-correlation of sequences]. Problemy Kibernetiki, 1971, no. 24, pp. 15–42. (in Russian)
6. *Nyberg K.* Differentially uniform mappings for cryptography. LNCS, 1994, vol. 765, pp. 55–64.
7. *Bilgin B., Nikova S., Nikov V., et al.* Threshold Implementations of all 3×3 and 4×4 S-boxes. IACR Cryptology ePrint Archive. 2012. http://eprint.iacr.org/2012/300.
8. *Bora A., Tolga M. S., and Ercan B.* Classifying 8-bit to 8-bit S-boxes based on power mappings from the point of DDT and LAT distributions. LNCS, 2008, vol. 5130, pp. 123–133.
9. *Biryukov A., De Cannière C., Braeken A., and Preneel B.* A toolbox for cryptanalysis: Linear and affine equivalence algorithms. LNCS, 2003, vol. 2656, pp. 33–50.
10. *Leander G. and Poschmann A.* On the classification of 4 bit S-boxes. LNCS, 2007, vol. 4547, pp. 159–176.
11. *Saarinen M. J. O.* Cryptographic analysis of all 4×4-bit S-boxes. LNCS, 2012, vol. 7118, pp. 118–133.
12. *Menyachikhin A. V.* Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters. Matem. Vopr. Kriptogr., 2017, vol. 8, no. 2, pp. 97–116.
13. *Fomin D. B.* New classes of 8-bit permutations based on a butterfly structure. Matem. Vopr. Kriptogr., 2019, vol. 10, no. 2, pp. 169–180.
14. *Fomin D. B.* Postroenie podstanovok prostranstva V_{2m} s ispol'zovaniem $(2m, m)$-funktsiy [Construction of permutations on the space V_{2m} by means of $(2m, m)$-functions]. Matem. Vopr. Kriptogr., 2020, vol. 11, no. 3, pp. 121–138. (in Russian)
15. *Fomin D. B.* Ob algebraicheskoy stepeni i differentsial'noy ravnomernosti podstanovok prostranstva V_{2m}, postroennykh s ispol'zovaniem $(2m, m)$-funktsiy [On the algebraic degree and differential uniformity of permutations on the space V_{2m} constructed via $(2m, m)$-functions]. Matem. Vopr. Kriptogr., 2020, vol. 11, no. 4, pp. 133–149. (in Russian)
16. *Feistel H.* Cryptography and computer privacy. Scientific American, 1973, vol. 225(5), pp. 15–23.
17. *Feistel H., Notz W. A., and Smith J. L.* Some cryptographic techniques for machine to machine data communications. Proc. IEEE, 1975, vol. 63(11), pp. 1545–1554.
18. *Webster A. F. and Tavares S. E.* On the design of S-boxes. LNCS, 1986, vol. 218, pp. 523–534.

19. *Augot D. and Finiasz M.* Direct Construction of Recursive MDS Diffusion Layers using Shortened BCH Codes. IACR Cryptology ePrint Archive. 2014. http://eprint.iacr.org/2014/566.
20. *Augot D. and Finiasz M.* Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions. IEEE Intern. Symp. Inform. Theory, 2013, pp. 1551–1555.
21. *Barreto P. and Rijmen V.* The KHAZAD Legacy-Level Block Cipher. Submission to NESSIE. 2000. https://www.researchgate.net/publication/228924670_The_Khazad_legacy-level_block_cipher.
22. *Gupta K. C. and Ray I. G.* On constructions of involutory MDS matrices. LNCS, 2013, vol. 7918, pp. 43–60.
23. *Junod P. and Vaudenay S.* Perfect diffusion primitives for block ciphers building efficient MDS matrices. LNCS, 2004, vol. 3357, pp. 84–99.
24. *Nakahara J. Jr. and Abrahao E.* A new involutory MDS matrix for the AES. Intern. J. Network Security, 2009, vol. 9(2), pp. 109–116.
25. *Poschmann A.* Lightweight Cryptography — Cryptographic Engineering for a Pervasive World. IACR Cryptology ePrint Archive, 2009. http://eprint.iacr.org/2009/516.
26. *Anashkin A. V.* Polnoe opisanie odnogo klassa MDS-matrits nad konechnym polem kharakteristiki 2 [Complete description of a class of MDS-matrices over finite field of characteristic 2]. Matem. Vopr. Kriptogr., 2017, vol. 8, no. 4, pp. 5–28. (in Russian)
27. GOST R 34.12-2015. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Blochnye shifry. [GOST P 34.12-2015. Information Technology. Cryptographic Data Security. Block Ciphers]. Moscow, Standartinform, 2015. (in Russian)
28. D.STVL.9 — Ongoing Research Areas in Symmetric Cryptography. ECRYPT, 2008. 108 p.
29. *Pogorelov B. A. and Pudovkina M. A.* Kombinatornaya kharakterizatsiya XL-sloyov [Combinatorial characterization of XL-layers]. Matem. Vopr. Kriptogr., 2013, vol. 4, no. 3, pp. 99–129. (in Russian)
30. *Pogorelov B. A. and Pudovkina M. A.* On the distance from permutations to imprimitive groups for a fixed system of imprimitivity. Discr. Math. Appl., 2013, vol. 24(2), pp. 95–108.
31. *Pogorelov B. A. and Pudovkina M. A.* On the distance from permutations to the union of all imprimitive groups with identical parameters of imprimitivity systems. Discr. Math. Appl., 2014, vol. 24(3), pp. 163–173.
32. *Pudovkina M. A.* O veroyatnostyakh r-raundovykh par raznostey XSL-algoritma blochnogo shifrovaniya Markova s privodimym lineynym preobrazovaniyem [On probabilities of r-round differences of a Markov XSL block cipher with a reducible linear transformation]. Prikladnaya Diskretnaya Matematika. Prilozheniye, 2014, no. 7, pp. 52–54. (in Russian)
33. *Standaert F. X., Piret G., Rouvroy G., et al.* ICEBERG : An involutional cipher efficient for block encryption in reconfigurable hardware. LNCS, 2004, vol. 3017, pp. 279–299.
34. *Burov D. A. and Pogorelov B. A.* An attack on 6 rounds of KHAZAD. Matem. Vopr. Kriptogr., 2016, vol. 7, no. 2, pp. 35–46.
35. *Burov D. A. and Pogorelov B. A.* The permutation group insight on the diffusion property of linear mappings. Matem. Vopr. Kriptogr., 2018, vol. 9, no. 2, pp. 47–58.
36. *Burov D. A.* Podgruppy pryamogo proizvedeniya grupp, invariantnyye otnositel'no deystviya podstanovok na somnozhitelyakh [Subgroups of Cartesian Product of Groups that are Invariant on Nonlinear Layer]. Diskretnaya Matematika, 2019, vol. 31, no. 4, pp. 3–19. (in Russian)
37. *Lidl R. and Niederreiter H.* Finite Fields. Cambridge, Cambridge University Press, 1984.

38. *Gluhov M. M., Elizarov V. P., and Nechaev A. A.* Algebra: Study Book. Moscow, Gelous ARV, 2003. (in Russian)
39. *Sim S. M., Khoo K., Oggier F. E., and Peyrin T.* Lightweight MDS involution matrices. FSE, 2015, pp. 471–493.
40. *Coy Puente O. and de la Cruz Jiménez R. A.* Construction of orthomorphic MDS matrices with primitive characteristic polynomial. CTCrypt'20, 2020. `https://ctcrypt.ru/files/files/Oliver\CTCrypt2020.pdf`.
41. *Khan A. A. and Murtaza G.* Efficient Implementation of Grand Cru with TI C6x+ Processor. IACR Cryptology ePrint Archive. 2011. `http://eprint.iacr.org/2011/385`.
42. *Watanabe D., Furuya S., Yoshida H., et al.* A new keystream generator MUGI. LNCS, 2002, vol. 2365, pp. 179–194.
43. *Halevi S., Coppersmith D., and Jutla C. S.* Scream: A Software-Efficient Stream Cipher. IACR Cryptology ePrint Archive. 2002. `http://eprint.iacr.org/2002/019`.
44. `http://www.cryptonessie.org` — The New European Schemes for Signatures, Integrity and Encryption (NESSIE), 2003.
45. *Daeman J., Knudsen L. R., and Rijmen V.* The block cipher SQUARE. FSE'97, 1997, vol. 1267, pp. 149–156.
46. *Agievich S. V., Galinskiy V. A., Mikulich N. D., and Kharin Yu. S.* Algoritm blochnogo shifrovaniya BelT. [BelT Block Cipher]. `elib.bsu.by`. (in Russian)
47. GOST R 34.11-2012. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Funktsiya kheshirovaniya. [GOST P 34.11-2012. Information Technology. Cryptographic Data Security. Hash Function]. Moscow, Standartinform, 2012. (in Russian)
48. *Biryukov A., Perrin L., and Udovenko A.* Reverse-engineering the S-box of Streebog, Kuznyechik and STRIBOBr1. LNCS, 2016, vol. 9665, pp. 372–402.
49. *Perrin L.* Partitions in the S-box of Streebog and Kuznyechik. Cryptology ePrint Archive, 2019. `https://eprint.iacr.org/2019/092`.
50. *Gorchinskiy Yu. N.* O gomomorfizmakh mnogoosnovnykh universal'nykh algebr v svyazi s kriptograficheskimi primeneniyami [On homomorphisms of multibase universal algebras in connection with cryptographic applications]. Trudy po Diskretnoy Matematike, 1997, vol. 1, pp. 67–84. (in Russian)
51. *Todo Y., Leander G., and Sasaki Y.* Nonlinear Invariant Attack — Practical Attack on Full SCREAM, iSCREAM, and Midori64. Cryptology ePrint Archive. 2016. `https://eprint.iacr.org/2016/732`.
52. *Burov D. A.* O sushchestvovanii nelineynykh invariantov spetsial'nogo vida dlya raundovykh preobrazovaniy XSL-algoritmov [About existence of the special nonlinear invariants for round functions of XSL-ciphers]. Diskretnaya Matematika, 2021, vol. 33, no. 2, pp. 31–45. (in Russian)

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 519.7 DOI 10.17223/20710410/54/3

ВЛИЯНИЕ РАНДОМИЗАЦИИ В МЕХАНИЗМАХ VKO НА БЕЗОПАСНОСТЬ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Е. К. Алексеев, В. Д. Николаев, С. В. Смышляев

ООО «КРИПТО-ПРО», г. Москва, Россия

E-mail: alekseev@cryptopro.ru, nikolaev@cryptopro.ru, svs@cryptopro.ru

Одним из широко применяемых на практике при работе в условиях слабодоверенного окружения механизмов противодействия атакам на используемые в процедурах выработки общих секретов долговременные ключи является умножение на рандомизирующие множители с последующим применением хэш-функций. Данный подход применяется в механизмах семейства VKO, на основе которых строятся российские криптонаборы основных протоколов криптографической защиты информации (в том числе IPsec, TLS, CMS), стандартизированных в Российской Федерации. В частности, таким образом устроена выработка общих параметров в российских механизмах протокола TLS 1.2, повсеместно применяемого в массовых программных средствах защиты информации. В работе рассмотрены некоторые аспекты результирующей безопасности процедур выработки общих параметров в случае ошибок реализации, из-за которых возможны сбои при вычислениях в группах точек скрученных кривых Эдвардса составного порядка, а также в случае отсутствия гарантий константного времени вычисления кратных точек.

Ключевые слова: *модели и методы защиты информации, криптографические протоколы.*

IMPACT OF RANDOMIZATION IN VKO MECHANISMS ON OVERALL SECURITY LEVEL

E. K. Alekseev, V. D. Nikolaev, S. V. Smyshlyaev

CryptoPro, Moscow, Russia

Multiplier randomization techniques with hashing of the results is one of widely used (especially for semi-trusted environment) countermeasures against attacks on key agreement protocols in practice. This approach is used, for instance, in VKO mechanisms, which are used as building blocks for Russian cipher suites for main cryptographic protocols (including IPsec, TLS, CMS), standardized in Russia. As an important example, shared keys are produced with this technique in TLS 1.2 cipher suites, which are widespread in cryptographic software for citizens of Russia. In this paper, we consider overall security of procedures of shared key computation in the practically significant cases of implementation errors in computations on twisted Edwards elliptic curves and non-constant time of scalar multiplication operations.

Keywords: *models and methods in information security, cryptographic protocols.*

Введение

В рамках решения важной для систем защиты информации проблемы обеспечения информационной безопасности в случае неполного доверия к окружению применяются механизмы, компенсирующие потенциальные уязвимости среды. В частности, для повышения безопасности программных средств криптографической защиты в условиях аппаратного окружения, не проходящего исследования в части побочных каналов, применяется приём умножения закрытых величин на рандомизирующие множители — в этом случае многократное использование одного и того же закрытого значения не будет приводить к одним и тем же вычислениям, а некоторые методы анализа с использованием побочных каналов не будут применимы из-за невозможности получения выборки достаточного объёма. Одними из стандартизированных в России механизмов, в которых данный приём учтён непосредственно в математической конструкции, являются определённые в рекомендациях по стандартизации Р 50.1.113-2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования» механизмы выработки ключей обмена VKO.

В настоящей работе исследуются свойства данных механизмов, которые при наличии ошибок в программной реализации могут привести к падению уровня защищённости средств. В частности, изучаются вопросы построения методов криптографического анализа, применимых к реализациям VKO в случае таких недостатков реализации, как ошибки при вычислениях в группах точек скрученных кривых Эдвардса составного порядка (стандартизированных в России) и зависимость времени вычислений от закрытых величин.

Показано, что положительные свойства данных механизмов, крайне желательные для использования в предназначенных для работы в слабодоверенном окружении средствах защиты информации, неразрывно связаны с существенным повышением критичности последствий уязвимостей при реализации для результирующей безопасности. Рандомизирующие множители позволяют «размывать» влияние закрытых величин на значения, которые противник может перехватывать по побочным каналам, предотвращая атаки, требующие накопления существенной статистики для уменьшения перебора закрытых величин. Однако одновременно с этим существенно опаснее становятся методы атак, предполагающие получение информации о закрытых величинах по одному значению, без необходимости накопления. В этих случаях умножение на рандомизирующие множители может приводить к тому, что малозначимые на практике атаки, позволявшие сокращать перебор долговременного секрета всего лишь в 2–4 раза, могут превращаться в применимые на практике для полного восстановления долговременных секретов. Таким образом, обратной стороной методов обеспечения безопасности в слабодоверенном окружении может становиться абсолютная недопустимость ошибок реализации программной части, защитные механизмы при ошибках разработки превращаются в оружие против самих защищаемых объектов.

В п. 1 приводится описание механизмов VKO и порядок применения в них рандомизирующего множителя UKM, а также типичные схемы применения данных механизмов в криптографических протоколах. Пункт 2 посвящён подходам к эксплуатации ошибок при работе на эллиптических кривых составного порядка с целью восстановления долговременного секрета и влиянию рандомизации на последствия таких ошибок для безопасности. В п. 3 рассмотрены некоторые подходы к восстановлению информации о долговременном секрете с помощью побочного канала по времени и их развитие в случае применения рандомизирующих множителей.

В работе использованы следующие обозначения:

— p — характеристика конечного поля, над которым задана кривая;
— m — порядок группы точек эллиптической кривой;
— q — простое число, порядок простой подгруппы группы точек эллиптической кривой;
— P — базовая точка простой подгруппы группы точек эллиптической кривой;
— O — нейтральный элемент группы точек эллиптической кривой;
— $\oplus$ — операция сложения двух точек эллиптической кривой;
— $[a]P$ — операция скалярного умножения точки на число (точка P умножается на целое a).

1. Применение рандомизации при вычислении общего секрета в протоколах

1.1. Механизмы VKO

Вычисление общего ключа по схеме Диффи — Хеллмана [1] является одним из основных базовых механизмов криптографии с открытым ключом. В современных протоколах данная процедура применяется в группе точек эллиптической кривой (как правило, эллиптическая кривая задаётся над простым конечным полем $\mathbb{F}_p$): для вычисления общего секрета закрытый ключ x одного из участников протокола умножается на открытый ключ $Y = [y]P$ второго участника: элемент группы Y умножается на скалярное значение x. Результатом операции скалярного умножения точки кривой является также точка на эллиптической кривой — в общем случае представимая вовсе не битовой строкой, претендующей на неотличимость от равновероятно выбранной из множества строк той же длины. Следовательно, для использования результата операции в качестве криптографического параметра (например, симметричного ключа блочного шифра) над ним требуется произвести некоторое преобразование. В соответствии со стандартной практикой, отражённой, например, в рекомендациях [2], таким преобразованием является хэширование. Отметим, что в некоторых случаях, например в протоколе TLS 1.3 [3], оно применяется не непосредственно к результату процедуры Диффи — Хеллмана, а сразу к набору данных (в этом случае общий ключевой материал используется в HMAC для получения основных ключей безопасности).

Схема выработки общего ключа VKO является в некотором смысле расширением схемы Диффи — Хеллмана. Помимо точки эллиптической кривой Y, соответствующей открытому ключу одного из участников, и закрытого ключа x другого участника, схема получает на вход ненулевое число UKM. Итоговое общее ключевое значение, вырабатываемое схемой, рассчитывается по формуле

$$\mathrm{VKO}(x, Y, UKM) = \mathrm{HASH}\left(\left[\frac{m}{q}(x \cdot UKM \bmod q)\right] Y\right),$$

где m, q — порядок группы точек и порядок простой подгруппы точек используемой эллиптической кривой; $HASH$ — хэш-функция ГОСТ Р 34.11-2012 [4]. Первым документом в области стандартизации, определяющим механизм семейства VKO, является RFC 4357 [5]. В 2016 г. рабочей группой по сопутствующим криптографическим алгоритмам, определяющим ключевые системы, входящей в состав Технического комитета 26 «Криптографическая защита информации», были разработаны рекомендации [6], которые описывают механизм VKO для ключей ГОСТ Р 34.10-2012 [7]. Соответствующий документ в системе IETF — RFC 7836 [8] — появился также в 2016 г.

Необходимо отметить, что процедуры выработки общего ключа по схемам Диффи — Хеллмана и VKO могут применяться в протоколах к различным с точки зрения срока жизни ключевым парам участников:

1. Оба ключа участников одноразовые («эфемерные», «ephemeral»). Так, например, в протоколе TLS 1.3 одноразовые ключевые пары вырабатываются и клиентом, и сервером в начале соединения и используются однократно для выработки общего секрета по схеме Диффи — Хеллмана. Аутентификация клиента и сервера производится при помощи механизма электронной подписи, использующего отдельные ключевые пары.
2. Один из ключей эфемерный, а другой долговременный («ephemeral – static»). Такая схема используется, например, при выработке ключа шифрования ключа в сообщениях формата CMS, а также в протоколе TLS 1.2. В первом случае отправитель генерирует эфемерную ключевую пару, использует её в схеме VKO, а затем вместе с сообщением передаёт свой эфемерный открытый ключ. Получатель использует для выполнения схемы VKO полученный открытый ключ и свой долговременный закрытый ключ. В случае протокола TLS 1.2 эфемерная ключевая пара используется клиентом, а сервер применяет долговременную пару. Открытый эфемерный ключ клиента передаётся серверу в сообщении ClientKeyExchange. Аутентификация сервера при этом производится по долговременному ключу VKO (сервер доказывает факт владения соответствующим закрытым ключом, выработав ключевое хэш-значение с использованием выработанного общего ключа), а аутентификация клиента — средствами электронной подписи с применением отдельной ключевой пары.
3. Оба ключа участников долговременные («static – static»). Такая схема может применяться в устаревших криптонаборах протокола TLS 1.0, TLS 1.1 и TLS 1.2 (например, TLS_GOSTR341001_WITH_28147_CNT_IMIT, устаревшая версия набора TLS_GOSTR341112_256_WITH_28147_CNT_IMIT) при установлении соединения с двусторонней аутентификацией. Аутентификация и клиента, и сервера производится по долговременным ключам VKO; механизм электронной подписи при этом не применяется. Это позволяет не использовать при анализе стойкости протокола подписывающий оракул.

Использование нетривиального значения UKM обязательно для случая «static – static» (в противном случае при повторных операциях VKO будут производиться одинаковые ключи). Хэширование в этом случае помогает избежать угадывания ключей согласования разных сессий. Предположим, что схема VKO не применяла бы хэширование. В этом случае компрометация одного общего сеансового ключа могла бы привести к компрометации всех общих ключей, полученных на двух данных долговременных ключевых парах. Действительно, пусть был скомпрометирован ключ $K_1 = \left[\frac{m}{q}((x \cdot UKM_1) \bmod q)\right] Y$ и при выработке общего ключа K_2 использовалось новое значение UKM_2. Тогда противник легко восстанавливает ключ K_2:

$$K_2 = \left[\frac{UKM_2}{UKM_1} \bmod q\right] K_1.$$

1.2. Типичные способы применения VKO в протоколах

Прикладные протоколы используют механизмы VKO для установления общего секретного ключа сторон взаимодействия. Этот ключ может использоваться как непо-

средственно для создания основного ключевого материала, так и как ключ шифрования мастер-ключей. Рассмотрим эти сценарии:

1. Протокол TLS 1.2 [9]. Механизм VKO в этом случае используется с одной эфемерной парой ключей (со стороны клиента) и одной долговременной парой ключей (со стороны сервера). В качестве значения UKM применяется число, задаваемое в формате BigEndian первыми 16 байтами значения HASH(ClientRandom|ServerRandom), где HASH — хэш-функция ГОСТ Р 34.11-2012 с длиной выхода 256 бит. Полученный ключ используется для шифрования премастер-ключа, вырабатываемого клиентом и передаваемого в зашифрованном виде серверу. Пассивный противник, наблюдающий за каналом, может получить случайные значения ClientRandom, ServerRandom в открытом виде и, таким образом, получить значение UKM. Активный противник, действующий от имени клиента, может в некоторой степени управлять значениями UKM, выбирая разные значения ClientRandom по своему усмотрению, однако не имеет возможности навязать конкретное значение. Следует отдельно подчеркнуть, что вместо схемы VKO в новой версии протокола TLS 1.3 используется непосредственно схема Диффи — Хеллмана.
2. Сообщения формата CMS [10]. Механизм VKO используется для выработки ключа шифрования ключа данных в сообщениях типа EnvelopedData. Может поддерживаться один из двух режимов работы: со статическим VKO (и отправитель, и получатель используют долговременные ключи) и «полустатическим» VKO (ключ отправителя — эфемерный, получателя — долговременный). UKM при этом указывается в сообщении в открытом виде и может быть известен пассивному противнику. Активный противник, отправляющий сообщения, может вырабатывать UKM полностью по своему усмотрению.
3. Протоколы IKEv1 и IKEv2 [11, 12]). Механизм VKO используется для выработки общего ключа сторон, из которого потом выращивается базовый ключ SKEYSEED. И инициатор соединения, и ответчик применяют эфемерные ключи. В качестве UKM при этом используется константное значение 1, поэтому активный противник не может навязывать значения UKM.

2. Влияние рандомизации в случае ошибок проверки входной точки

2.1. Особенности работы схем выработки общего ключа на эллиптических кривых составного порядка

При использовании эллиптических кривых, аддитивные группы которых имеют составной порядок (например, стандартизированные в России скрученные кривые Эдвардса id-tc26-gost-3410-2012-256-paramSetA и id-tc26-gost-3410-2012-512-paramSetC [13, 14], кофактор m/q равен 4), принципиально важным для безопасности закрытых ключей является противодействие методам проведения атак с помощью навязывания точек малых порядков. Подробная информация о данных методах криптоанализа представлена в [15, 16]; напомним основные идеи.

В модели, в которой противник имеет возможность передать свой открытый ключ Y атакуемому серверу с закрытым ключом x для вычисления ключа согласования SK по формуле $SK = [x]Y$, этот противник может в качестве Y передать не точку основной подгруппы кривой (порядка q), а точку из малой подгруппы (например, порядка m/q). Если сервер при этом не проверит принадлежность Y основной подгруппе, вычислит SK (который будет иметь одно из m/q возможных значений) и передаст данные, зависящие от SK (например, полученный с использованием SK

шифртекст), то противник, перебрав и сравнив с вычисленным на сервере SK значения $[1]Y, [2]Y, \ldots, [(m/q-1)]Y$, сможет получить значение $x \bmod m/q$, т. е. получить $\log_2(m/q)$ бит о ключе x.

2.2. Расширение атак с использованием вспомогательных кривых

Атака, описанная выше, может быть модифицирована для случая кривых с кофактором, равным 1. Предположим, что сервер не только не проверяет принадлежность получаемой точки группе нужного порядка, но и принадлежность целевой эллиптической кривой вообще. Противник может воспользоваться тем фактом, что большинство реально используемых в прикладной криптографии эллиптических кривых в краткой форме Вейерштрасса задаются уравнением вида $y^2 = x^3 - 3x + b$, $b \in \mathbb{F}_p$. В этом случае противник может, перебирая значения b, находить произвольные кривые, порядки групп точек которых имеют малые делители. Поскольку некоторые формулы скалярного умножения точек эллиптической кривой в краткой форме Вейерштрасса не зависят от коэффициента b, сервер при выполнении операции умножения не получит результат в виде точки, не лежащей на целевой кривой. Противник в этом случае может последовательно высылать точки Q_2 порядка 2, Q_3 порядка 3, Q_5 порядка 5 с разных кривых, тем самым получая значения $x \bmod 2$, $x \bmod 3$, $x \bmod 5$ и так далее, что позволит определить многие биты закрытого ключа x. Атака такого рода впервые описана в [17].

2.3. Расширение атак в случае применения рандомизации

Атака для кривых составного порядка может быть расширена, если противник может управлять значениями UKM, а также получать информацию об успехе или неуспехе операции, проводимой с помощью общего ключа.

Предположим, что противник передаёт точку эллиптической кривой $Y = Q \oplus T$, где Q — точка, принадлежащая подгруппе порядка q (Q может быть равно O), а T — точка малого порядка (в случае российских стандартизированных скрученных кривых в форме Эдвардса это может быть точка T_2 порядка 2 или точка T_4 порядка 4). Если операция VKO на стороне получателя реализована правильным образом, а именно по формуле $\left[\frac{m}{q}(UKM \cdot x \bmod q)\right] Y$ (где x — долговременный закрытый ключ сервера), то будет получена результирующая точка

$$\left[\frac{m}{q}(UKM \cdot x \bmod q)\right] Q \oplus \left[\frac{m}{q}(UKM \cdot x \bmod q)\right] T = \left[\frac{m}{q}(UKM \cdot x \bmod q)\right] Q,$$

принадлежащая целевой подгруппе порядка q группы точек эллиптической кривой. В случае неправильной реализации, заключающейся в умножении на кофактор $\frac{m}{q}$ по модулю q, в ходе операции VKO будет получен следующий результат:

$$\left[\left(\left(\frac{m}{q} \cdot UKM \cdot x\right) \bmod q\right)\right] Q \oplus \left[\left(\left(\frac{m}{q} \cdot UKM \cdot x\right) \bmod q\right)\right] T = \left[\left(\left(\frac{m}{q} \cdot UKM \cdot x\right) \bmod q\right)\right] Q \oplus U,$$

где U — точка группы малого порядка, равная $[((m/q) \cdot UKM \cdot x) \bmod q]T$. Такой ход выполнения операции VKO позволит противнику проводить следующую атаку, направленную на полное определение закрытого ключа сервера x:

1. Противник вырабатывает открытый ключ Y, который не принадлежит целевой подгруппе порядка q. Сделать это он может, выработав ключевую пару $(y, [y]P)$, где $y \in \{1, \dots q-1\}$ — закрытый ключ, а далее положив $Y = [y]P \oplus T$, где T — точка малого порядка.
2. Противник передаёт Y получателю в рамках используемого протокольного решения для проведения операции VKO.
3. Противник получает значение общего ключа $K = [((m/q) \cdot UKM \cdot x) \bmod q]Q \oplus \oplus [((m/q) \cdot UKM \cdot x) \bmod q]T$.
4. Противник ожидает уведомления о корректной выработке общего ключа получателем.

   а) В случае протокола TLS версий 1.0–1.2 данное уведомление может быть получено следующим образом. В рамках сообщения ClientKeyExchange противник пересылает свой открытый ключ Y, а также зашифрованный на ключе K премастер-ключ PMS. Противник вырабатывает из премастер-ключа мастер-ключ MS, после чего вырабатывает значение ClientFinished, равное выходу ключевой хэш-функции, ключом которой является MS. Отметим, что данное сообщение пересылается в защищённом виде (будучи зашифрованным и совместно со значением имитовставки). Ключи шифрования и имитозащиты для данного сообщения также вырабатываются на основе ключа MS. В свою очередь, сервер, получив сообщение ClientKeyExchange и, следовательно, точку Y, может выполнить операцию VKO, получить ключ K, расшифровать зашифрованный ключ PMS, получить ключ MS, расшифровать и проверить целостность сообщения ClientFinished и проверить его. Если хотя бы одна из этих операций завершается с ошибкой, сервер пересылает клиенту уведомление об ошибке (alert) и прерывает исполнение протокола. В противном случае сервер формирует сообщение ServerFinished и успешно завершает исполнение протокола. Таким образом, у противника получается чёткий критерий выработки общего ключа K сервером.

   б) В случае использования зашифрованных сообщений формата CMS противник вырабатывает случайное значение ключа KEK, используемого для шифрования и имитозащиты данных, и шифрует его на общем ключе K. Получатель расшифровывает ключ KEK, а затем расшифровывает и проверяет целостность данных. Если хотя бы одна из этих операций завершается с ошибкой, получатель отвергает сообщение, иначе сообщение принимается. Если получатель сигнализирует отправителю о факте ошибки или успеха, противник получает чёткий критерий выработки общего ключа K получателем.
5. Противник, зная общий ключ и удостоверившись в его знании получателем, определяет значение

$$U = K \oplus \left[-1 \cdot \left(\frac{m}{q} \cdot UKM \cdot x\right) \bmod q\right] Q = \left[\frac{m}{q} \cdot UKM \cdot x \bmod \frac{m}{q}\right] T.$$

   Так как точка U имеет малый порядок, он перебором определяет l, такое, что $U = [l]T$, при этом $l = ((m/q) \cdot UKM \cdot x) \bmod q$. Для российских стандартизированных скрученных кривых в формате Эдвардса $m/q = 4$, это означает получение информации о двух битах закрытого ключа сервера. Отметим, что в корректной реализации протокола VKO (даже если реализация сервера не осуществляет проверку принадлежности точки Y целевой подгруппе) атака бу-

дет прервана именно на этом пункте — противник получит $U = O$, что не даст ему никакой информации о ключе x.

6. При проведении атаки на схему VKO в рамках конкретного прикладного протокола противник может повторять шаги 2.3–2.3 N раз (где N определяется битовым размером задачи и вычислительными возможностями противника), каждый раз используя новое значение UKM. Для сообщений CMS он имеет возможность полностью управлять значением UKM, в случае протокола TLS — рандомизировать (конкретное значение UKM будет зависеть ещё и от случайного значения, выбираемого сервером), отбрасывая неподходящие для проведения атаки значения (например, случайно совпавшие с прошлыми). Получаемые значения $a_i = ((m/q) \cdot UKM_i \cdot x \bmod q) \bmod (m/q)$, $1 \leqslant i \leqslant N$, для случая $m/q = 4$ будут иметь два содержательных бита, которые обозначим $a_{i,0}, a_{i,1}$. Информация, полученная противником, может быть представлена в виде системы двух булевых уравнений

$$\begin{cases} a_{i,0} = f_0(q, x_1, \ldots, x_n, UKM_{i,1}, \ldots, UKM_{i,n}), \\ a_{i,1} = f_1(q, x_1, \ldots, x_n, UKM_{i,1}, \ldots, UKM_{i,n}). \end{cases}$$

Здесь через n обозначена битовая длина закрытого ключа; $x_1, \ldots, x_n$ — переменные, соответствующие битам закрытого ключа; $UKM_{i,j}$ — константные биты, составляющие представление чисел UKM_i, $1 \leqslant i \leqslant N$, $1 \leqslant j \leqslant n$. Функции f_i, $i = 1, 2$, являются булевыми многочленами, определяемыми операцией приведения по модулю q.

7. Искомое значение закрытого ключа можно определить из полученной системы N уравнений с единственным неизвестным x вида

$$\begin{cases} \left(\dfrac{m}{q} \cdot UKM_1 \cdot x \bmod q\right) \bmod \dfrac{m}{q} = a_1, \\ \ldots \\ \left(\dfrac{m}{q} \cdot UKM_N \cdot x \bmod q\right) \bmod \dfrac{m}{q} = a_N \end{cases} \tag{1}$$

либо из представления этой системы в виде $2N$ булевых уравнений с n неизвестными $x_1, \ldots, x_n$:

$$\begin{cases} a_{1,0} = f_0(q, x_1, \ldots, x_n, UKM_{1,1}, \ldots, UKM_{1,n}), \\ a_{1,1} = f_1(q, x_1, \ldots, x_n, UKM_{1,1}, \ldots, UKM_{1,n}), \\ \ldots \\ a_{N,0} = f_0(q, x_1, \ldots, x_n, UKM_{N,1}, \ldots, UKM_{N,n}), \\ a_{N,1} = f_1(q, x_1, \ldots, x_n, UKM_{N,1}, \ldots, UKM_{N,n}). \end{cases}$$

Замечание 1. Системы такого вида могут решаться в общем виде с использованием SAT-решателей и алгоритмов, основанных на построении базисов Грёбнера. Такой подход, однако, при первом рассмотрении представляется неэффективным, так как трудоёмкость этих алгоритмов, по-видимому, будет значительно превышать трудоёмкость задачи дискретного логарифмирования в группах точек практически применяемых эллиптических кривых.

В некоторых аналогичных случаях находятся способы использовать структурные особенности систем для построения более эффективных алгоритмов. В качестве примера результативного подхода к анализу структур систем уравнений для уменьшения

трудоёмкости их решения алгоритмами, основанными на применении аппарата базисов Грёбнера, приведём случай систем уравнений, получаемых при решении задачи дискретного логарифмирования в группах точек эллиптических кривых над конечными полями с использованием многочленов Семаева (впервые предложенными в [18]). Различные подходы [19 – 22], использующие структурные особенности систем, в отдельных случаях понижают асимптотическую сложность итоговых алгоритмов дискретного логарифмирования до теоретически субэкспоненциальной.

По мнению авторов, существенно более перспективным является подход, связанный с рассмотрением уравнения (1).

С точки зрения теоретико-информационного подхода представляется возможным, что построенные таким образом системы при правильном выборе параметров будут разрешимы и иметь единственное решение. Для демонстрации наличия такой возможности проведён следующий эксперимент:

1) для $q = 2^{32} - 5$ были выработаны случайные битовые векторы x_i, $1 \leqslant x_i < q$, $1 \leqslant i \leqslant 20$, играющие роль закрытых ключей;
2) каждый из этих битовых векторов умножался по модулю q на случайные значения $UKM_{i,j}$, $1 \leqslant UKM_{i,j} < q$, $1 \leqslant i \leqslant 20$, $1 \leqslant j \leqslant 32$;
3) полученные значения приводились по модулю 4. Набор из 32 значений по модулю 4 для вектора x_i далее будем называть спектром вектора x_i по $(UKM_{i,1}, \ldots, UKM_{i,32})$;
4) для каждого x', такого, что $1 \leqslant x' < q$, и для всех i, таких, что $1 \leqslant i \leqslant 20$, строились спектры x' по $(UKM_{i,1}, \ldots, UKM_{i,32})$;
5) построенные спектры для векторов x' сравнивались с соответствующими спектрами для векторов x_i, $1 \leqslant i \leqslant 20$.

Целью эксперимента являлась проверка гипотезы о том, что спектр вектора x_i однозначно определяет этот вектор среди всех возможных. Если бы спектр x' по $(UKM_{i,1}, \ldots, UKM_{i,32})$ для некоторого i совпал со спектром x_i по тому же кортежу значений UKM, но при этом $x' \neq x_i$, гипотеза была бы опровергнута. Экспериментально, однако, таких случаев выявлено не было, откуда следует, что во всех случаях целевой вектор x_i определялся однозначно своим спектром, что, в свою очередь, является свидетельством в пользу того, что в спектре содержится достаточно информации для восстановления искомого закрытого ключа.

3. Влияние рандомизации в случае неконстантного времени вычисления кратной точки

3.1. Механизмы вычисления кратных точек и побочные каналы по времени

Потребность в высокопроизводительных криптографических системах привела к необходимости разработки эффективных алгоритмов выполнения базовых криптографических операций. Одной из таких операций является задача скалярного умножения точки эллиптической кривой на множитель (или вычисления кратной точки). В последние десятилетия эта задача получила большое число решений для использования в разных криптографических примитивах и с разными представлениями эллиптических кривых. Интересный обзор таких решений можно найти в [23].

Время выполнения операции скалярного умножения зависит от битового вектора, представляющего множитель. Поэтому при выборе алгоритма вычисления кратной точки важно учитывать наличие побочного канала по времени. Кратко рассмотрим

два классических представителя семейств алгоритмов вычисления кратных точек и оценим возможность утечки данных по временному каналу при использовании таких методов.

Введём следующие обозначения:

— умножаемую точку будем обозначать через P (точка на эллиптической кривой), множитель — через m (неотрицательное целое число). Таким образом, требуется по P и m найти точку $[m]P$;
— бинарное разложение m будем обозначать $m_{(2)} = (m_{n-1}, \ldots, m_1, m_0)$, где $m_i \in \in \{0, 1\}$, $i = 0, 1, 2, \ldots, n-1$; n — длина бинарного разложения. С точностью до старших нулей бинарное разложение однозначно. Через $\mathrm{wt}_2(m)$ будем обозначать вес бинарного разложения числа m.

Для всякого алгоритма умножения точки на число будем использовать следующие обозначения:

— ID — число удвоений точек на этапе предварительных вычислений;
— IA — число сложений точек на этапе предварительных вычислений;
— IS — объём хранимых предвычисленных данных (в точках на кривой);
— $D_{\max}, D_{\min}, D_{\exp}$ — максимальное, минимальное и среднее (по всем m длины n бит) количество требуемых удвоений точек;
— $A_{\max}$, $A_{\min}$, $A_{\exp}$ — максимальное, минимальное и среднее (по всем m длины n бит) количество требуемых сложений точек.

Классическая схема Горнера

Выражение $[m]P$ можно представить в следующем виде:

$$[m]P = \Big[\underbrace{\sum_{i=0}^{n-1} 2^i m_i}_{=m}\Big] P = [2]([2](\ldots[2]([2]([2][m_{n-1}]P \oplus [m_{n-2}]P) \oplus [m_{n-3}]P) \oplus \ldots) \oplus [m_1]P) \oplus [m_0]P.$$

Обозначим для $k = 0, 1, \ldots, n-1$ через P_k точку $\left[\sum\limits_{i=k}^{n-1} 2^{i-k} m_i\right] P$. Тогда $[m]P = P_0$, $P_{n-1} = [m_{n-1}]P$, $P_{k-1} = [2]P_k \oplus [m_{k-1}]P$, $k = n-1, \ldots, 2, 1$. Теперь

$$[m]P = \overbrace{[2](\overbrace{[2](\ldots[2]([2]([2]\underbrace{[m_{n-1}]P}_{P_{n-1}} \oplus [m_{n-2}]P) \oplus [m_{n-3}]P) \oplus \ldots) \oplus [m_1]P}^{P_1}) \oplus [m_0]P}^{P_0}.$$

$$\underbrace{\qquad\qquad\qquad\qquad}_{P_{n-2}}$$

Алгоритм 1 описывает действия по этой схеме. Предварительные вычисления отсутствуют.

Заметим, что количество удвоений (D) в алгоритме GornerClassic совпадает с номером старшей единицы бинарного разложения числа m и равно $\lfloor \log_2(m) \rfloor$; на шаге 5 сложение осуществляется только при $m_k = 1$, поэтому количество сложений точек (A) на 1 меньше количества единиц в бинарном разложении числа m. Таким образом, для алгоритма 1 точные количества сложений и удвоений точек зависят от m:

$$A = \mathrm{wt}_2(m) - 1, \quad D = \lfloor \log_2(m) \rfloor.$$

Алгоритм 1. GornerClassic

Вход: $m = \sum\limits_{i=0}^{n-1} m_i 2^i$ — натуральное число; P — элемент некоторой аддитивной группы.
Выход: $Q = [m]P$ — элемент, m-кратный элементу P.
1: $Q := P$;
2: $n' :=$ номер старшей единицы в бинарном разложении $m_{(2)}$;
3: $k := n' - 1$.
4: **Пока** $k \geqslant 0$:
5: $\quad Q := [2]Q \oplus [m_k]P$;
6: $\quad k := k - 1$.
7: **Вернуть** Q

Основные вычисления:

— $D_{\max} = n - 1$, $D_{\min} = 0$, $D_{\exp} = n - 2 + \dfrac{1}{2^{n-1}} = \sum\limits_{k=0}^{n-1} \dfrac{k}{2^{n-k}}$;

— $A_{\max} = n - 1$, $A_{\min} = 0$, $A_{\exp} = \dfrac{n}{2} - 1$.

Обратим внимание на то, что время выполнения алгоритма напрямую зависит от веса двоичного разложения m. Таким образом, в случае применения схемы Горнера по времени вычисления можно получить информацию о весе ключа, тем самым резко ограничив размер класса возможных закрытых ключей. Простейшим приёмом, позволяющим избавиться от подобного побочного канала по времени, является добавление лишнего сложения при $m_k = 0$, результат которого игнорируется. На рис. 1 показано влияние веса w, $0 \leqslant w < 512$, для исходного (чёрный график) и доработанного с помощью указанного приёма (серый график) алгоритмов на время выполнения скалярного умножения точки эллиптической кривой.

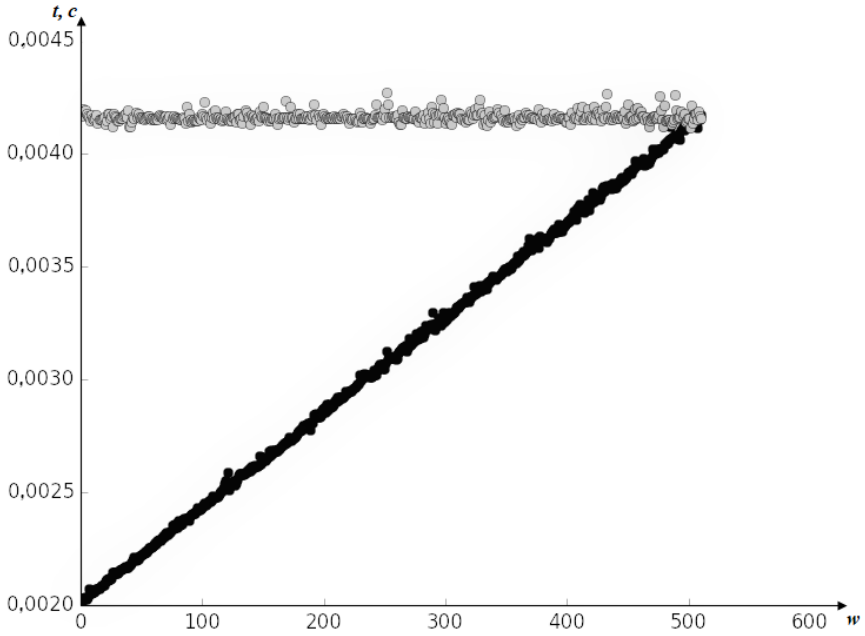


Рис. 1. Зависимость времени вычисления кратной точки методом Горнера от битового веса множителя

Алгоритм WTNAF

Алгоритм WTNAF является представителем семейства так называемых оконных алгоритмов и основан на w-TNAF-представлении числа m, которым называется набор

$$((m^{(s-1)}, p^{(s-1)}), (m^{(s-2)}, p^{(s-2)}), \ldots, (m^{(1)}, p^{(1)}), (m^{(0)}, p^{(0)})),$$

$m^{(i)} \in \{-2^{w+1}+1, -2^{w+1}+3, \ldots, 2^{w+1}-3, 2^{w+1}-1\}$, $p^{(i)} \in \mathbb{N}$, $i = 0, 1, \ldots, s-1$, такой, что $m = \sum\limits_{i=0}^{s-1} 2^{\sum\limits_{j=0}^{i} p^{(j)}} m^{(i)}$; $m^{(s-1)} \neq 0$.

В этом случае

$$[m]P = \sum_{i=0}^{s-1} \left[2^{\sum\limits_{j=0}^{i} p^{(j)}} m^{(i)} \right] P.$$

Заметим, что можно заранее вычислить значения $[r]P$ для всех $r \in \{1, 3, \ldots, 2^{w+1}-3, 2^{w+1}-1\}$. При необходимости сложения произвольной точки с точкой $[r']P$, где $r' = -r$ для $r \in \{1, 3, \ldots, 2^{w+1}-3, 2^{w+1}-1\}$, сложение заменяется на вычитание точки $[r]P$.

Эти действия описаны в алгоритме 2.

Алгоритм 2. WTNAF

Вход: m — натуральное число вместе с его w-TNAF-представлением $((m^{(s-1)}, p^{(s-1)}), (m^{(s-2)}, p^{(s-2)}), \ldots, (m^{(1)}, p^{(1)}), (m^{(0)}, p^{(0)}))$,
P — элемент некоторой аддитивной группы,
таблица точек $[r]P$ для всех $r \in \{1, 3, \ldots, 2^{w+1}-3, 2^{w+1}-1\}$.
Выход: $Q = [m]P$ — элемент, m-кратный P.
1: $k := s-1$; $Q := O$.
2: **Пока** $k \neq 0$:
3: $Q := [2^{p^{(k)}}](Q \oplus [m^{(k)}]P)$;
4: $k := k-1$.
5: **Вернуть** Q

Предварительные вычисления: $ID = 1$; $IA = 2^w - 1$; $IS = 2^w$.

Основные вычисления:

— $D_{\max} = n-1$, $D_{\min} = 0$, $D_{\exp} \approx n-2$;
— $A_{\max} = \left\lceil \dfrac{n}{w+2} \right\rceil$, $A_{\min} = 0$, $A_{\exp} \approx \dfrac{n}{w+3}$.

На каждой итерации алгоритма происходит одна операция удвоения точки и максимум одна операция сложения. При этом разное время исполнения итераций может быть получено только за счёт того, что на некоторых итерациях $m^{(k)} = 0$ и сложения не требуется. Этого можно избежать одним из двух способов:

1) в некоторых представлениях точка O может быть представлена в аффинных координатах и при $m^{(k)} = 0$ можно осуществлять полноценную операцию сложения с такой точкой;
2) в таблице можно хранить не точки $[m^{(k)}]P$ непосредственно, а точки $[m^{(k)}]P \oplus M$, где M — маскирующая точка, такая, что $[m^{(k)}]P \oplus M \neq O$ для любых $0 \leqslant k \leqslant s-1$. Такой подход потребует дополнительного вычитания константной точки в конце алгоритма.

3.2. Влияние рандомизации на атаки

Подход, приводящий к возможности построения атаки на схему выработки общего ключа VKO при некорректном умножении на кофактор подгруппы точек эллиптической кривой при применении случайных значений UKM, может быть применён и при анализе информации, поступающей по побочным каналам при использовании специальных алгоритмов вычисления кратных точек. Далее через x будем обозначать закрытый ключ честной стороны, который пытается определить противник.

Как было показано, при фиксированном значении UKM в конечном протоколе противник может (при применении честной стороной схемы Горнера) определить вес вектора $UKM \cdot x \bmod q$, однако дополнительной информации он более не получит. Если используются рандомизированные значения UKM, противник может получить битовые веса ряда векторов вида $x \cdot UKM_i \bmod q$, $1 \leqslant i \leqslant N$, где N — параметр, определяемый вычислительными ресурсами противника и ограничениями протокола. Отметим, что, в отличие от случая некорректной реализации схемы VKO, в данном случае нужно учитывать «зашумлённость» получаемых значений битовых весов. Для избавления от «шума» необходимо сделать несколько повторов операций с каждым конкретным значением UKM_i, что возможно в случае сообщений формата CMS (где значения UKM выбираются противником), но крайне затруднено в случае протокола TLS (противник может рандомизировать значение UKM, но не контролирует его выработку полностью). Фактически противник получает следующую систему уравнений (через $a_1, \ldots, a_N$ обозначим конкретные полученные противником значения весов):

$$\begin{cases} \mathrm{wt}(x \cdot UKM_1 \bmod q) = a_1, \\ \ldots \\ \mathrm{wt}(x \cdot UKM_N \bmod q) = a_N. \end{cases} \tag{2}$$

Вопрос существования эффективного алгоритма, который позволяет находить единственное значение x по данным значениям UKM_i и полученным весам a_i множителей вида $x \cdot UKM_i \bmod q$, остаётся открытым, но можно сделать предположение о достаточности информации в полученных противником данных для восстановления закрытого ключа x с точки зрения теоретико-информационного подхода. Для иллюстрации этого предположения был проведён эксперимент, сходный с экспериментом для случая некорректной реализации схемы VKO.

Цель эксперимента — проверка гипотезы о том, что по весам множителей вида $x \cdot UKM_i \bmod q$ однозначно определяется подходящее значение x из ключевого пространства. Эксперимент проводился для q длин 24, 28 и 32 бита и состоял из следующих шагов:

- вырабатывались битовые векторы x_i, $1 \leqslant x_i < q$, $1 \leqslant i \leqslant 20$, играющие роль закрытых ключей;
- каждый из векторов x_i умножался на случайные значения $UKM_{i,j}$, $1 \leqslant UKM_{i,j} < q$, $1 \leqslant i \leqslant 20$, $1 \leqslant j \leqslant 32$;
- для каждого из векторов $x_i \cdot UKM_{i,j} \bmod q$ считался его битовый вес a_i. Далее для фиксированного i совокупность 32 таких весовых значений будем называть спектром вектора x_i по $(UKM_{i,1}, \ldots, UKM_{i,32})$;
- для каждого x', $1 \leqslant x' < q$, и для всех i, $1 \leqslant i \leqslant 20$, строились спектры x' по $(UKM_{i,1}, \ldots, UKM_{i,32})$;
- построенные спектры для векторов x' сравнивались с соответствующими спектрами для векторов $x_i, 1 \leqslant i \leqslant 20$.

Если бы спектр x' по $(UKM_{i,1}, \ldots, UKM_{i,32})$ для некоторого i совпал со спектром x_i по тому же кортежу значений UKM, но при этом $x' \neq x_i$, гипотеза была бы опровергнута. Экспериментально, однако, таких случаев выявлено не было, откуда следует, что во всех случаях целевой вектор x_i определялся однозначно своим спектром, что, в свою очередь, свидетельствует в пользу истинности предположения о наличии в спектре достаточной информации для восстановления искомого закрытого ключа.

Данные эксперимента показывают, что в случае появления математического алгоритма, восстанавливающего значение закрытого x по его весовому спектру по кортежу значений UKM небольшой длины, рандомизацию в схеме VKO следует использовать только совместно с методами противодействия побочным каналам по времени.

4. Задачи для дальнейших исследований

Построение эффективных методов решения систем уравнений (1) и (2), определяемых в соответствии с описанными сценариями атак, представляется весьма сложной и важной задачей для дальнейших исследований. Она может оказаться интересной, например, для специалистов в области теории решёток.

Отметим, что разбиение процесса построения законченных методов криптоанализа реальных систем на два самоценных этапа является распространённой практикой. Первым является этап сведения задачи реализации актуальной для системы угрозы к некоторой формальной математической задаче, а за ним следует этап исследования методов решения этой задачи. При этом в ряде случаев эти этапы исследуются независимо в разных, разнесённых во времени и авторству работах. Ярким примером является история криптографического анализа схемы подписи вслепую Шнорра. В 2001 г. в работе [24] Шнорр свёл задачу криптоанализа этой схемы к решению так называемой «ROS-задачи», не предложив эффективного алгоритма её решения. И только в 2021 г. в работе [25] другой группой исследователей предложен полиномиальный алгоритм решения этой задачи. Учитывая широту спектра применяемых сегодня в криптоанализе математических методов и постоянное усложнение исследуемых криптосистем, тенденция к разделению задачи оценки стойкости таких систем на два указанных этапа вполне естественна. Другие примеры подобного характера можно найти в [26, разд. 4.1].

Заключение

Рассмотренные аспекты позволяют сделать следующий общий вывод о принципах обеспечения защиты информации в слабодоверенном окружении. Применение механизмов, позволяющих в ряде случаев обеспечивать защищённость программных компонент средств защиты информации при отсутствии полного доверия к программному и аппаратному окружению, требует максимально внимательной разработки самих этих компонент. Цена за возможность обеспечивать защиту программных модулей в слабодоверенном окружении — недопустимость ошибок в самих этих модулях, предельно высокие требования к качеству и глубине исследований программных средств защиты информации, предполагающих применение в средах, которые не подвергаются полноценному анализу.

Авторы благодарят Владимира Пузырёва за существенную помощь в организации вычислительных экспериментов.

Авторы выражают глубокую признательность рецензенту за детальные и содержательные комментарии о подходах к решению получаемых в результате описанных сценариев атак систем уравнений.

ЛИТЕРАТУРА

1. *Diffie W. and Hellman M.* New directions in cryptography // IEEE Trans. Inform. Theory. 1976. V. 22. No. 6. P. 644–654.
2. Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. NIST Special Publication 800-56A Revision 3. `https://doi.org/10.6028/NIST.SP.800-56Ar3`. 2018.
3. *Rescorla E.* The Transport Layer Security (TLS) Protocol Version 1.3. `https://tools.ietf.org/html/rfc8446`. 2018.
4. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования». М.: Стандартинформ, 2012.
5. *Popov V., Kurepkin I., and Leontiev S.* Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms. `https://tools.ietf.org/html/rfc4357`. 2006.
6. Рекомендации по стандартизации Р 50.1.113–2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования». М.: Стандартинформ, 2016.
7. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». М.: Стандартинформ, 2012.
8. *Smyshlyaev S., Alekseev E., Popov V., and Leontiev S.* Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012. `https://tools.ietf.org/html/rfc7836`. 2016.
9. Рекомендации по стандартизации Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)». М.: Стандартинформ, 2020.
10. Методические рекомендации МР 26.2.002-2013 «Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.10 и ГОСТ Р 34.11 в криптографических сообщениях формата CMS». М.: Стандартинформ, 2013.
11. Техническая спецификация ТС 26.2.001-2015 «Использование ГОСТ 28147-89, ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 в протоколах обмена ключами IKE и ISAKMP». М.: Стандартинформ, 2015.
12. Рекомендации по стандартизации «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в сети Интернет версии 2 (IKEv2)» (проект).
13. *Алексеев Е. К., Ошкин И. Б., Попов В. О. и др.* О перспективах использования скрученных эллиптических кривых Эдвардса со стандартом ГОСТ Р 34.10-2012 и алгоритмом ключевого обмена на его основе // Проблемы информационной безопасности. Компьютерные системы. 2014. № 3. С. 60–66.
14. *Alekseev E. K., Nikolaev V. D., and Smyshlyaev S. V.* On the security properties of Russian standardized elliptic curves // Матем. вопр. криптогр. 2018. Т. 9. № 3. С. 5–32.
15. SafeCurves: Choosing Safe Curves for Elliptic-Curve Cryptography. `https://safecurves.cr.yp.to/index.html`.
16. *Lim C. H. and Lee P. J.* A key recovery attack on discrete log-based schemes using a prime order subgroup // LNCS. 1997. V. 1294. P. 249–263.
17. *Biehl I., Meyer B., and Muller V.* Differential fault attacks on elliptic curve cryptosystems (extended abstract) // LNCS. 2000. V. 1880. P. 131–146.

18. *Semaev I. A.* Summation Polynomials and the Discrete Logarithm Problem on Elliptic Curves. Cryptology ePrint Archive: Report 2004/031. https://eprint.iacr.org/2004/031.pdf.
19. *Petit C. and Quisquater J.-J.* On polynomial systems arising from a Weil descent // LNCS. 2012. V. 7658. P. 451–466.
20. *Semaev I. A.* New Algorithm for the Discrete Logarithm Problem on Elliptic Curves. Cryptology ePrint Archive: Report 2015/310. https://eprint.iacr.org/2015/310.pdf.
21. *Courtois N.* On Splitting a Point with Summation Polynomials in Binary Elliptic Curves. Cryptology ePrint Archive: Report 2016/003. https://eprint.iacr.org/2016/003.pdf.
22. *Petit C., Kosters M., and Messeng A.* Algebraic approaches for the elliptic curve discrete logarithm problem over prime fields // LNCS. 2016. V. 9615. P. 3–18.
23. *Hankerson D., Menezes A. J., and Vanstone S.* Guide to Elliptic Curve Cryptography. N.Y.: Springer Verlag, 2004.
24. *Schnorr C.-P.* Security of blind discrete log signatures against interactive attacks // LNCS. 2001. V. 2229. P. 1–12.
25. *Benhamouda F., Lepoint T., Loss J., et al.* On the (in)security of ROS' // LNCS. 2021. V. 12696. P. 33–53.
26. *Koblitz N. and Menezes A.* Critical perspectives on provable security: Fifteen years of "another look" papers // Adv. Math. Commun. 2019. V. 13. P. 517–558.

REFERENCES

1. *Diffie W. and Hellman M.* New directions in cryptography. IEEE Trans. Inform. Theory, 1976, vol. 22, no. 6, pp. 644–654.
2. Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. NIST Special Publication 800-56A Revision 3. https://doi.org/10.6028/NIST.SP.800-56Ar3, 2018.
3. *Rescorla E.* The Transport Layer Security (TLS) Protocol Version 1.3. https://tools.ietf.org/html/rfc8446, 2018.
4. GOST R 34.11-2012 "Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Funktsiya kheshirovaniya" [GOST R 34.11-2012 "Information Technology. Cryptographic Data Security. Hash Function"]. Moscow, Standartinform, 2012. (in Russian)
5. *Popov V., Kurepkin I., and Leontiev S.* Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms. https://tools.ietf.org/html/rfc4357. 2006.
6. Rekomendatsii po standartizatsii R 50.1.113–2016 "Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Kriptograficheskie algoritmy, soputstvuyushchie primeneniyu algoritmov elektronnoy tsifrovoy podpisi i funktsii kheshirovaniya" [Recommendations for Standardization R 50.1.113–2016 "Information Technology. Cryptographic Data Security. Additional Cryptographic Algorithms for Digital Signature Algorithms and Hash Function"]. Moscow, Standartinform, 2016. (in Russian)
7. GOST R 34.10-2012 "Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Protsessy formirovaniya i proverki elektronnoy tsifrovoy podpisi" [GOST R 34.10-2012 "Information Technology. Cryptographic Data Security. Processes of Digital Signature Creation and Verification"]. Moscow, Standartinform, 2012. (in Russian)
8. *Smyshlyaev S., Alekseev E., Popov V., and Leontiev S.* Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012. https://tools.ietf.org/html/rfc7836. 2016.
9. Rekomendatsii po standartizatsii R 1323565.1.020-2020 "Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Ispol'zovanie rossiyskikh kriptograficheskikh algoritmov v protokole bezopasnosti transportnogo urovnya (TLS 1.2)" [Recommendations

for Standardization R 1323565.1.020-2020 “Information Technology. Cryptographic Data Security. Usage of Russian Cryptographic Algorithms in TLS 1.2 Protocol”]. Moscow, Standartinform, 2020. (in Russian)

10. Metodicheskie rekomendatsii MR 26.2.002-2013 “Ispol’zovanie algoritmov GOST 28147-89, GOST R 34.10 i GOST R 34.11 v kriptograficheskikh soobshcheniyakh formata CMS” [Methodical Recommendations MR 26.2.002-2013 “Usage of GOST 28147-89, GOST R 34.10 and GOST R 34.11 in CMS”]. Moscow, Standartinform, 2013. (in Russian)
11. Tekhnicheskaya spetsifikatsiya TS 26.2.001-2015 “Ispol’zovanie GOST 28147-89, GOST R 34.11-2012 i GOST R 34.10-2012 v protokolakh obmena klyuchami IKE i ISAKMP” [Technical Specification TS 26.2.001-2015 “Usage of GOST 28147-89, GOST R 34.11-2012 and GOST R 34.10-2001 for Key Agreement in IKE and ISAKMP Protocols”]. Moscow, Standartinform, 2015. (in Russian)
12. Rekomendatsii po standartizatsii “Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Ispol’zovanie rossiyskikh kriptograficheskikh algoritmov v seti Internet versii 2 (IKEv2)” (proekt) [Recommendations for Standardization “Information technology. Cryptographic data security. Usage of Russian cryptographic algorithms in Internet key exchange protocol version 2 (IKEv2)” (proekt)]. (in Russian)
13. *Alekseev E. K., Oshkin I. B., Popov V. O., et al.* O perspektivakh ispol’zovaniya skruchennykh ellipticheskikh krivykh Edvardsa so standartom GOST R 34.10-2012 i algoritmom klyuchevogo obmena na ego osnove [On the prospects of using twisted Edwards elliptic curves with the GOST R 34.10-2012 standard and the key exchange algorithm based on it]. Problemy Informatsionnoy Bezopasnosti. Komp’yuternye Sistemy, 2014, no. 3, pp. 60–66. (in Russian)
14. *Alekseev E. K., Nikolaev V. D., and Smyshlyaev S. V.* On the security properties of Russian standardized elliptic curves // Matem. Vopr. Kriptogr., 2018, vol. 9, iss. 3, pp. 5–32.
15. SafeCurves: Choosing Safe Curves for Elliptic-Curve Cryptography. `https://safecurves.cr.yp.to/index.html`.
16. *Lim C. H. and Lee P. J.* A key recovery attack on discrete log-based schemes using a prime order subgroup. LNCS, 1997, vol. 1294, pp. 249–263.
17. *Biehl I., Meyer B., and Muller V.* Differential fault attacks on elliptic curve cryptosystems (extended abstract). LNCS, 2000, vol. 1880, pp. 131–146.
18. *Semaev I. A.* Summation Polynomials and the Discrete Logarithm Problem on Elliptic Curves. Cryptology ePrint Archive: Report 2004/031. `https://eprint.iacr.org/2004/031.pdf`.
19. *Petit C. and Quisquater J.-J.* On polynomial systems arising from a Weil descent. LNCS, 2012, vol. 7658, pp. 451–466.
20. *Semaev I. A.* New Algorithm for the Discrete Logarithm Problem on Elliptic Curves. Cryptology ePrint Archive: Report 2015/310. `https://eprint.iacr.org/2015/310.pdf`.
21. *Courtois N.* On Splitting a Point with Summation Polynomials in Binary Elliptic Curves. Cryptology ePrint Archive: Report 2016/003. `https://eprint.iacr.org/2016/003.pdf`.
22. *Petit C., Kosters M., and Messeng A.* Algebraic approaches for the elliptic curve discrete logarithm problem over prime fields. LNCS, 2016, vol. 9615, pp. 3–18.
23. *Hankerson D., Menezes A. J., and Vanstone S.* Guide to Elliptic Curve Cryptography. N.Y., Springer Verlag, 2004.
24. *Schnorr C.-P.* Security of blind discrete log signatures against interactive attacks. LNCS, 2001, vol. 2229, pp. 1–12.
25. *Benhamouda F., Lepoint T., Loss J., et al.* On the (in)security of ROS’. LNCS, 2021, vol. 12696, pp. 33–53.
26. *Koblitz N. and Menezes A.* Critical perspectives on provable security: Fifteen years of “another look” papers. Adv. Math. Commun., 2019, vol. 13, pp. 517–558.

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

УДК 519.246.5, 519.218.5 DOI 10.17223/20710410/54/4

ОПТИМАЛЬНЫЙ АЛГОРИТМ ПРЕОБРАЗОВАНИЯ АЦИКЛИЧЕСКОГО ОРГРАФА В СИЛЬНОСВЯЗНЫЙ

Г. Ш. Цициашвили*, М. А. Осипова*,**

*Институт прикладной математики ДВО РАН, г. Владивосток, Россия
**Дальневосточный федеральный университет, г. Владивосток, Россия

E-mail: guram@iam.dvo.ru, mao1975@list.ru

Для двудольного орграфа G, в котором все дуги выходят из первой доли во вторую, решена задача нахождения минимального набора дуг, дополнение которых преобразует его в сильносвязный орграф. Доказано, что минимальное число дополнительных дуг, преобразующих двудольный орграф G в сильносвязный, равно максимуму из числа вершин первой и второй долей. Построен алгоритм определения минимального набора дополнительных дуг, преобразующих данный орграф в сильносвязный. Этот алгоритм основан на выделении минимального рёберного покрытия, как совокупности несвязанных между собой звезд в орграфе G, и на построении дуг, соединяющих эти звезды. Полученный результат использован для нахождения минимального набора дуг, преобразующих произвольный ациклический орграф в сильносвязный орграф путём выделения рёбер, соединяющих звёзды в минимальном рёберном покрытии. Данная задача возникла при анализе биотехнологических решений, повышающих стабильность функционирования белковых сетей за счёт введения в них обратных связей.

Ключевые слова: *ациклический орграф, двудольный орграф, сильная связность, гамильтонов цикл, обратная связь, минимальное рёберное покрытие.*

OPTIMAL ALGORITHM FOR CONVERTING AN ACYCLIC DIGRAPH TO A CLUSTER

G. Sh. Tsitsiashvili*, M. A. Osipova*,**

*Institute for Applied Mathematics, FEB RAS, Vladivostok, Russia
**Far Eastern Federal University, Vladivostok, Russia

A bipartite digraph $\widehat{G}$ with edges from the first part V_1 to the second part V_2 is considered. The minimum edge cover in the digraph $\widehat{G}$ consists of a set of unrelated stars $G_1^1, \ldots, G_1^M$ with a root in V_1 and stars $G_2^1, \ldots, G_2^N$ with a root in V_2. Denote by m the number of leaves in the stars $G_1^1, \ldots, G_1^M$ and by n the number of leaves in the stars $G_2^1, \ldots, G_2^N$ and put $p(\widehat{G})$ the minimum number of additional edges, the introduction of which into the digraph $\widehat{G}$ transforms it into a strongly connected digraph. It is proved that: 1) $p(\widehat{G}) = \max(m+N, n+M)$; 2) $p(\widehat{G}) = \max(|V_1|, |V_2|)$; 3) $p(\mathcal{G}) = \max(|\mathcal{V}_1|, |\mathcal{V}_2|)$ for an acyclic digraph $\mathcal{G}$, where $\mathcal{V}_1$ is the set of vertices of $\mathcal{G}$, from which the arcs only leave, $\mathcal{V}_2$ — the set of vertices of $\mathcal{G}$, into which the arcs only

enter. Algorithms for determining the minimum set of additional edges have been proposed. They are based on finding the minimum edge coverage in a bipartite graph and connecting unconnected stars with the minimum number of edges.

Keywords: *acyclic digraph, bipartite digraph, cluster, Hamiltonian cycle, feedback, minimal edge cover.*

Введение

В [1, 2] построен алгоритм выделения в орграфе компонент сильной связности и преобразования исходного орграфа в ациклический орграф, вершинами которого являются эти компоненты. В настоящей работе рассматривается в определённом смысле обратная задача добавления к ациклическому орграфу минимального числа дуг, превращающих его в сильносвязный орграф. Эта процедура нужна, чтобы включить все вершины ациклического орграфа, моделирующего белковую сеть, в систему обратных связей, которые стабилизируют функционирование этой сети. Такая постановка задачи предложена авторам биотехнологом, чл.-корр. РАН В. П. Булгаковым. Авторы подобрали математический эквивалент решения этой задачи в терминах теории графов, которое планируется использовать в дальнейших совместных исследованиях.

Предположим, что сложная система, например белковая сеть, представима ациклическим орграфом $\mathcal{G}$ без петель и изолированных вершин. Обозначим V_1 множество вершин, из которых дуги только выходят, а V_2 — множество вершин, в которые дуги только входят. Построим двудольный орграф G, в котором V_1 — множество вершин первой доли, а V_2 — второй, и вершина $v_1 \in V_1$ соединена дугой с вершиной $v_2 \in V_2$, если между ними в ациклическом орграфе $\mathcal{G}$ существует путь.

Преобразуем двудольный орграф G в неориентированный удалением ориентации рёбер и найдем в нём минимальное рёберное покрытие [3–5]. Для этого алгоритмом увеличивающих чередующихся путей находим максимальное паросочетание, которое можно преобразовать в минимальное рёберное покрытие, компонентами связности которого являются графы-звёзды (все дуги выходят из одной вершины или входят в одну вершину, называемую корнем). В минимальном рёберном покрытии восстановим ориентацию рёбер и обозначим полученный двудольный орграф $\widehat{G}$.

Основным результатом работы является алгоритм построения минимального набора дополнительных дуг, превращающих $\widehat{G}$ в сильносвязный орграф. Доказано, что число дуг в этом минимальном наборе $p(\widehat{G}) = \max(|V_1|, |V_2|)$. Данное равенство распространяется на двудольный орграф G с долями V_1, V_2 и на ациклический орграф $\mathcal{G}$.

1. Основные результаты

Рассмотрим двудольный орграф $\widehat{G}$, состоящий из совокупности несвязанных между собой M звёзд $G_1^1, \ldots, G_1^M$ с корнем в первой доле и N звёзд $G_2^1, \ldots, G_2^N$ с корнем во второй доле. Обозначим m количество листьев в звёздах $G_1^1, \ldots, G_1^M$ и n — в звёздах $G_2^1, \ldots, G_2^N$. На рис. 1 приведен пример орграфа $\widehat{G}$, состоящего из звезд $G_1^1,\ G_1^2,\ G_2^1,\ G_2^2$ в случае $m = n = 6$.

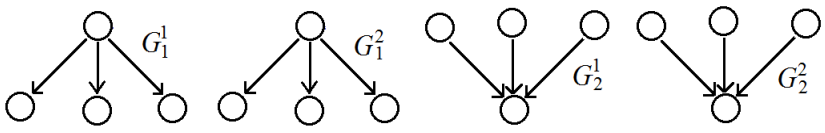


Рис. 1. Несвязанные звёзды $G_1^1,\ G_1^2,\ G_2^1,\ G_2^2,\ M = N = 2,\ m = n = 6$

Теорема 1. Справедливо равенство $p(\widehat{G}) = \max(m+N, n+M)$.

Доказательство. При преобразовании орграфа $\widehat{G}$ число дополнительных дуг, входящих в корни звёзд $G_1^1, \ldots, G_1^M$, должно быть не меньше M, а входящих в листья звёзд $G_2^1, \ldots, G_2^N$ — не меньше n. Число дополнительных дуг, выходящих из листьев звёзд $G_1^1, \ldots, G_1^M$, должно быть не меньше m, а выходящих из корней звёзд $G_2^1, \ldots, G_2^N$ — не меньше N. Поэтому число дополнительных дуг, входящих в вершины первой доли, не меньше чем $M+n$, а выходящих из вершин второй доли — не меньше чем $m+N$. Дополнительные входящие и выходящие дуги могут совпадать. Поэтому минимальное число дополнительных дуг $p(\widehat{G}) \geqslant \max(m+N, n+M)$. Докажем, что $p(\widehat{G}) = \max(m+N, n+M)$.

Рассмотрим сначала случай, когда орграф $\widehat{G}$ состоит только из звёзд $G_1^1, \ldots, G_1^M$ или только из звёзд $G_2^1, \ldots, G_2^N$. Дополним звёзды $G_1^1, \ldots, G_1^M$ дугами, последовательно соединяющими их листья. Из последнего листа звезды G_1^k проведём дополнительную дугу в корень G_1^{k+1}, $k = 1, \ldots, M-1$, а из последнего листа звезды G_1^M — в корень G_1^1. В звёздах $G_1^1, \ldots, G_1^M$ с дополнительными дугами укажем гамильтонов цикл. Он начинается в корне звезды G_1^1, проходит последовательно через все её листья и направляется в корень G_1^2 и т. д.; из последнего листа звезды G_1^M — в корень G_1^1. В результате преобразуем звёзды $G_1^1, \ldots, G_1^M$ в сильносвязный орграф с числом дополнительных дуг $m = \max(m+0, 0+M)$ (рис. 2).

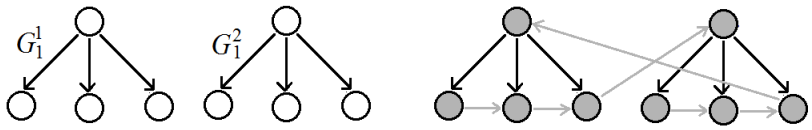


Рис. 2. Сильносвязный орграф (справа), построенный из звёзд G_1^1, G_1^2 (слева)

Аналогично орграф $\widehat{G}$, состоящий только из звёзд $G_2^1, \ldots, G_2^N$, дополним дугами, последовательно соединяющими их листья. Кроме того, из корня звезды G_2^k проведём дополнительную дугу в первый лист G_2^{k+1}, $k = 1, \ldots, N-1$, а из корня звезды G_2^N — в первый лист G_2^1. В звёздах $G_2^1, \ldots, G_2^N$ с дополнительными дугами укажем гамильтонов цикл. Он начинается в первом листе звезды G_2^1, проходит последовательно через все её листья и направляется в корень, затем идёт в первый лист звезды G_2^2, и т. д. Из корня звезды G_2^N путь продолжается в первый лист G_2^1. В результате преобразуем звёзды $G_2^1, \ldots, G_2^N$ в сильносвязный орграф с числом дополнительных дуг $n = \max(0+N, n+0)$ (рис. 3).

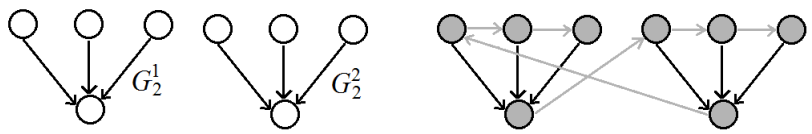


Рис. 3. Сильносвязный орграф, построенный из звёзд G_2^1, G_2^2

Рассмотрим теперь случай, когда $MN > 0$. Обозначим W_1 множество всех вершин в звёздах $G_1^1, \ldots, G_1^M$ и W_2 — в звёздах $G_2^1, \ldots, G_2^N$. Введём дополнительную дугу из корня G_2^N в какой-либо лист звезды G_2^{N-1}, дугу из корня G_2^{N-1} — в какой-либо лист звезды G_2^{N-2} и т. д., дугу из корня G_2^1 — в корень G_1^M, дугу из какого-либо листа G_1^M — в корень G_1^{M-1}, дугу из какого-либо листа G_1^{M-1} — в корень G_1^{M-2} и т. д., дугу из какого-либо листа G_1^2 — в корень G_1^1. Назовём введённые дуги и инцидентные им вершины

помеченными (на рис. 4 выделены серым цветом). Очевидно, что из любой помеченной, а значит, и из любой вершины звезды набора $G_2^1, \ldots, G_2^N$ существует путь в любую вершину звезды набора $G_1^1, \ldots, G_1^M$. Будем это утверждение обозначать $W_2 \Rightarrow W_1$.

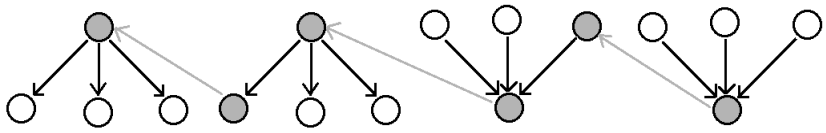


Рис. 4. Введение $M + N - 1$ дополнительных дуг

Число помеченных дуг, соединяющих вершины звёзд $G_1^1, \ldots, G_1^M$, равно $M-1$, а дуг, соединяющих вершины звёзд $G_2^1, \ldots, G_2^N$, равно $N-1$. Тогда общее число помеченных дуг с учётом дуги из G_2^1 в G_1^M равно $M-1+N-1+1 = M+N-1$.

Общее число непомеченных вершин в звёздах $G_1^1, \ldots, G_1^M$ равно $(m-(M-1))$, в звёздах $G_2^1, \ldots, G_2^N$ их $(n-(N-1))$. Из каждой непомеченной вершины множества W_1 проведём дополнительную дугу в какую-либо непомеченную вершину множества W_2 так, чтобы в каждую непомеченную вершину множества W_2 входила дуга из какой-либо вершины множества W_1 (рис. 5). Таким образом, число дополнительно введённых дуг равно $\max(m-(M-1), n-(N-1))$. Следовательно, общее число дополнительных дуг равно $\max(m-(M-1), n-(N-1)) + M + N - 1 = \max(m+N, n+M)$.

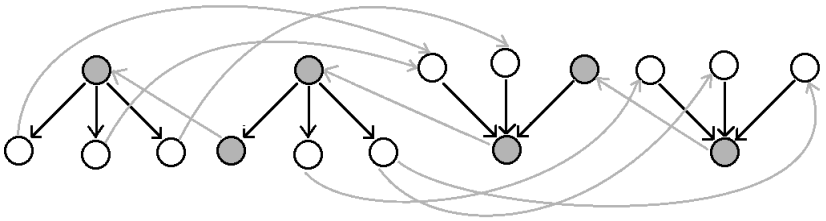


Рис. 5. Введение дополнительных дуг

Докажем, что введение дополнительных дуг в звёзды $G_1^1, \ldots, G_1^M$, $G_2^1, \ldots, G_2^N$ преобразует их в сильносвязный орграф. Возьмём произвольные непомеченные вершины $v_1 \in W_1$, $v_2 \in W_2$ и проведём путь через непомеченные вершины v_1, v_2', v_1', v_2, где $v_2' \in W_2$ — вершина, соединённая с v_1, а $v_1' \in W_1$ — вершина, соединённая с v_2. Поскольку из любой помеченной вершины множества W_1 можно провести путь в некоторую непомеченную вершину этого множества и из любой непомеченной вершины множества W_2 можно провести дугу в некоторую помеченную вершину этого множества, то можно провести путь из любой вершины множества W_1 в любую вершину множества W_2, т. е. $W_1 \Rightarrow W_2$. Тогда из соотношений $W_1 \Rightarrow W_2$, $W_2 \Rightarrow W_1$ получаем $W_1 \cup W_2 \Rightarrow W_1 \cup W_2$. Следовательно, построенный из звёзд $G_1^1, \ldots, G_1^M$, $G_2^1, \ldots, G_2^N$ орграф с введёнными $\max(m+N, n+M)$ дугами является сильносвязным. ■

Теорема 2. Для двудольного орграфа G, в котором дуги идут только из первой доли V_1 во вторую долю V_2, минимальное число дополнительных дуг, превращающих его в сильносвязный орграф, равно

$$p(G) = \max(|V_1|, |V_2|). \tag{1}$$

Доказательство. Из теоремы 1 следуют равенства $|V_1| = n + M$, $|V_2| = m + N$, $p(\widehat{G}) = \max(|V_1|, |V_2|)$. В свою очередь, из определения $p(G)$ и включения $\widehat{G} \subseteq G$

следует $p(\widehat{G}) \geqslant p(G)$. В то же время очевидно неравенство $p(G) \geqslant \max(|V_1|, |V_2|)$. Тогда выполняется (1). ■

Замечание 1. С помощью алгоритма, приведённого при доказательстве теоремы 1, можно построить минимальный набор из $p(G)$ дополнительных дуг, преобразующих двудольный орграф G в сильносвязный орграф $\widetilde{G}$. Таким образом, дано конструктивное решение задачи определения минимального набора дополняющих дуг в двудольном орграфе G.

Теорема 3. Для произвольного ациклического орграфа $\mathcal{G}$ обозначим V_1 — множество вершин, из которых дуги только выходят, V_2 — множество вершин, в которые дуги только входят. Тогда минимальное число дополнительных дуг, превращающих $\mathcal{G}$ в сильносвязный, определяется равенством

$$p(\mathcal{G}) = \max(|V_1|, |V_2|).$$

Доказательство. Преобразуем орграф $\mathcal{G}$ в двудольный ациклический орграф G с долями V_1 и V_2 и дугами (v_1, v_2), $v_1 \in V_1$, $v_2 \in V_2$, такими, что в орграфе $\mathcal{G}$ существует путь из v_1 в v_2. Дугами из минимального набора $p(G)$ дополнительных дуг соединим в $\mathcal{G}$ вершины множеств V_1, V_2. Получим сильносвязный орграф, в котором число дополнительных дуг равно $p(\mathcal{G}) = \max(|V_1|, |V_2|)$. ■

Авторы благодарят В. П. Булгакова и А. С. Бурундукова за помощь в постановке задачи.

ЛИТЕРАТУРА

1. *Tarjan R.* Dehpt-first search and linear graph algorithms // SIAM J. Comput. 1972. V. 1. No. 2. P. 146–160.
2. *Цициашвили Г. Ш., Осипова М. А., Лосев А. С.* Алгоритмы кластеризации графов // Вестник Воронежского государственного университета. Сер. Физика. Математика. 2016. № 1. С. 145–149.
3. *Алексеев В. Е., Захарова Д. В.* Теория графов: учеб. пособие. Н. Новгород: Нижегородский госуниверситет, 2017. 119 с.
4. `https://logic.pdmi.ras.ru/~dvk/graphs_dk.pdf` — Теория графов. 2017.
5. *Cormen T. H., Leiserson Ch. E., Rivest R. L., and Stein Cl.* Introduction to Algorithms. 3rd Ed. Cambridge: MIT Press, 2009. 499 p.

REFERENCES

1. *Tarjan R.* Dehpt-first search and linear graph algorithms. SIAM J. Comput., 1972, vol. 1, no. 2, pp. 146–160.
2. *Tsitsiashvili G. Sh., Osipova M. A., and Losev A. S.* Algoritmy klasterizatsii grafov [Graph clustering algorithms]. Bull. Voronezh State University. Ser. Physics, Math., 2016, no. 1, pp. 145–149. (in Russian)
3. *Alekseev V. E., Zakharova D. V.* Teoriya grafov [Graph Theory], tutorial. N. Novgorod, Nizhny Novgorod State University, 2017. 119 p. (in Russian)
4. `https://logic.pdmi.ras.ru/~dvk/graphs_dk.pdf` — Graph Theory, 2017.
5. *Cormen T. H., Leiserson Ch. E., Rivest R. L., and Stein Cl.* Introduction to Algorithms, 3rd Ed. Cambridge, MIT Press, 2009. 499 p.

УДК 519.174.7 DOI 10.17223/20710410/54/5

THE PALETTE INDEX OF SIERPIŃSKI TRIANGLE GRAPHS AND SIERPIŃSKI GRAPHS

A. Ghazaryan

Yerevan State University, Yerevan, Armenia

E-mail: ghazaryan.aghasi@gmail.com

The palette of a vertex v of a graph G in a proper edge coloring is the set of colors assigned to the edges which are incident to v. The palette index of G is the minimum number of palettes occurring among all proper edge colorings of G. In this paper, we consider the palette index of Sierpiński graphs S_p^n and Sierpiński triangle graphs $\widehat{S}_3^n$. In particular, we determine the exact value of the palette index of Sierpiński triangle graphs. We also determine the palette index of Sierpiński graphs S_p^n where p is even, $p = 3$, or $n = 2$ and $p = 4l + 3$.

Keywords: *palette index, Sierpiński triangle graph, Sierpiński graph.*

ОБ ИНДЕКСЕ ПАЛИТРЫ ТРЕУГОЛЬНИКА СЕРПИНСКОГО И ГРАФА СЕРПИНСКОГО

А. Газарян

Ереванский государственный университет, г. Ереван, Армения

Палитра вершины v графа G в правильной раскраске рёбер — это набор цветов, присвоенных рёбрам, инцидентным v. Индекс палитры G — это минимальное количество палитр из всех правильных рёберных раскрасок G. Рассматриваются индексы палитры графов Серпинского S_p^n и треугольников Серпинского $\widehat{S}_3^n$. Доказано, что индекс палитры треугольника Серпинского $\widehat{S}_3^n$ равен 3, если n чётное, и 4 иначе; индекс палитры графа S_p^n равен 2 для чётного p и равен 3 для $p = 3$ или $n = 2$ и $p = 4l + 3$.

Ключевые слова: *индекс палитры графа, треугольник Серпинского, граф Серпинского.*

1. Introduction

In this paper, we use the standard notations of graph theory [1]. Graph coloring problems are even more challenging when there are some constraints on them, such as proper edge or proper vertex colorings. Usually, such constraints are naturally motivated by different applications in scheduling theory.

In [2], a new chromatic parameter is called the *palette index* of a graph and is defined as follows: for a given proper edge coloring of a graph G, we define the *palette* of a vertex $v \in V(G)$ as the set of all colors appearing on edges incident to v. The palette index $\check{s}(G)$ of G is the minimum number of distinct palettes occurring in a proper edge coloring of G.

Mainly, the palette index was studied for regular graphs. In [2], it is shown that the palette index of a regular graph is 1 if and only if the graph is of Class 1, and it is different from 2. The palette index of complete graphs is also determined in [2].

Theorem 1 [2]. For every positive integer $n > 1$, we have

$$\check{s}(K_n) = \begin{cases} 1, & \text{if } n \text{ is even,} \\ 3, & \text{if } n = 4l + 3, \\ 4, & \text{if } n = 4l + 1. \end{cases}$$

In [2], the authors also studied the palette index of cubic graphs. More specifically,

$$\check{s}(G) = \begin{cases} 1, & \text{if } G \text{ is of Class 1,} \\ 3, & \text{if } G \text{ is of Class 2 and has a perfect matching,} \\ 4, & \text{if } G \text{ is of Class 2 and has no perfect matching.} \end{cases}$$

As mentioned in [3], the palette index of a d-regular graph of Class 2 satisfies the inequality $3 \leqslant \check{s}(G) \leqslant d + 1$.

The paper [3] investigates 4-regular graphs and proves that $\check{s}(G) \in \{3, 4, 5\}$ if G is 4-regular and of Class 2, and that all these values are, in fact, attained.

Since the computing of the chromatic index of cubic graphs is NP-complete [4], determining the palette index of a given graph is also NP-complete, even for cubic graphs [2]. This means that even determining, if a given graph has a palette index 1, is an NP-complete problem.

Vizing's edge coloring theorem yields an upper bound for the palette index of a general graph G with the maximum degree Δ, namely $\check{s}(G) \leqslant 2^{\Delta+1} - 2$. It is not hard to construct graphs whose palette index is quite smaller than $2^{\Delta+1} - 2$. In [5], an infinite family of multigraphs is described, whose palette index grows asymptotically as Δ^2; however, it is an open question whether there are such examples without multiple edges. Furthermore, in [5] it is conjectured that there is a polynomial $p(\Delta)$ so that for any graph with the maximum degree Δ, it holds the bound $\check{s}(G) \leqslant p(\Delta)$.

There are few results about the palette index of non-regular graphs. In [6], M. Horňák and J. Hudák have completely determined the palette index of the complete bipartite graphs $K_{a,b}$ with $\min\{a, b\} \leqslant 5$.

In [7], C. Casselgren and P. Petrosyan studied the palette index of bipartite graphs. In particular, they have determined the exact value of the palette index of grids and characterized the class of graphs whose palette index equals the number of vertices.

In [8], the palette index of trees is considered. In particular, the authors have proved that $\check{s}(T) \leqslant \sum_{i=1}^{\Delta} \left\lceil \frac{\Delta}{i} \right\rceil$. Moreover, they also have showed the sharpness of the bound by constructing trees T^{Δ} for which the palette index is is equal to this value.

One of the fascinating graph families is *Sierpiński graphs* S_p^n. It has been introduced in [9] as a result of the study of the topological properties of the Lipscomb space, and it is still being studied extensively. An interesting fact is that S_3^n is isomorphic to the graph of the Tower of Hanoi with n disks [9].

Sierpiński triangle graphs $\widehat{S}_3^n$ are quite similar to Sierpiński graphs S_3^{n+1} and are obtained from S_3^{n+1} by a finite number of steps. These graphs are usually studied in conjunction with Sierpiński graphs and have quite interesting properties. Sierpiński triangle graphs are fractals of dimension $d = \log 3 / \log 2 \approx 1.585$ and have been introduced in [10].

For Sierpiński graphs and other Sierpiński-type graphs, [11] is a good survey.

In [12], S. Klavžar has introduced an explicit labeling of the vertices of $\widehat{S}_3^n$. Also, he has proved that $\widehat{S}_3^n$ is uniquely 3-colorable and S_3^n is uniquely 3-edge-colorable.

In [13], the authors have studied and summarized vertex, edge, and total colorings of the Sierpiński triangle graphs $\widehat{S}_3^n$ and Sierpiński graphs S_p^n.

In [14], some properties of graphs $\widehat{S}_3^n$ are given, including their cycle structure, domination number, and pebbling number.

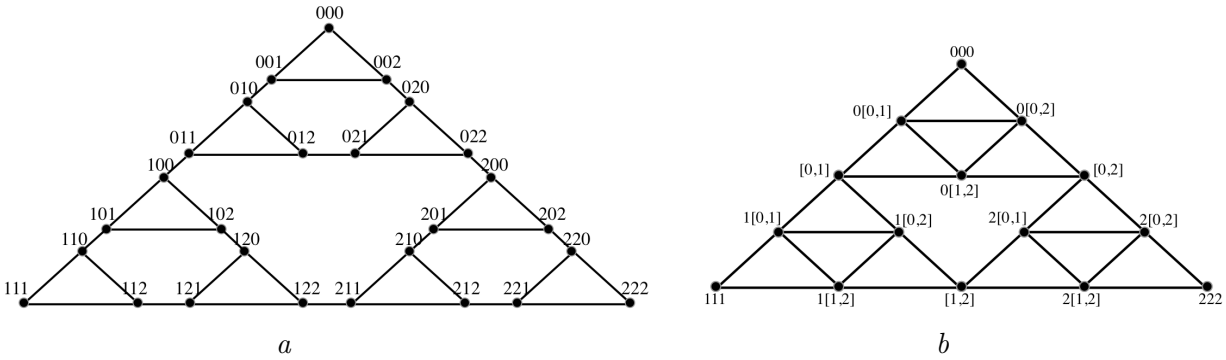
These graphs are beneficial to other theories such as probability theory [15], dynamical systems theory [16], topology [17], etc.

Let us now give explicit definitions of Sierpiński graphs S_p^n and Sierpiński triangle graphs $\widehat{S}_3^n$, where $n \geqslant 0$ and $p > 0$ are integers. The graphs are defined as follows. The vertex set of S_p^n is the set of all n-tuples of integers $0, 1, \ldots, p-1$, namely, $V(S_p^n) = \{0, 1, \ldots, p-1\}^n$. Two different vertices $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ are adjacent if and only if there exists an $h \in \{1, \ldots, n\}$ such that:

1) $u_t = v_t$ for $t = 1, \ldots, h-1$;
2) $u_h \neq v_h$;
3) $u_t = v_h$ and $v_t = u_h$ for $t = h+1, \ldots, n$.

We will denote a vertex $(u_1, u_2, \ldots, u_n)$ by $\langle u_1 u_2 \ldots u_n \rangle$ or even $u_1 u_2 \ldots u_n$. The vertices $\langle i \ldots i \rangle$, $i \in \{0, \ldots, p-1\}$, are called the *extreme vertices* of S_p^n. We will denote by $iS_p^n = S_p^n[\{v : v = \langle i \ldots i \rangle\}]$ the subgraph of S_p^n, where $i = 0, 1, \ldots, p-1$. Obviously, iS_p^{n+1} is isomorphic to S_p^n. Consequently, S_p^n contains p^{n-1} copies of the graph $S_p^1 = K_p$. We will call *link edges* all the edges of S_p^n that do not belong to the above-mentioned K_p.

As a result of contracting all the link edges of S_3^{n+1}, we will get the Sierpiński triangle graph $\widehat{S}_3^n$ where $n \geqslant 0$. We label the vertices of $\widehat{S}_3^n$ as follows. Let $\langle u_1 \ldots u_r ij \ldots j \rangle$ and $\langle u_1 \ldots u_r ji \ldots i \rangle$ be the endvertices of a link edge of S_3^{n+1} that is contracted to a vertex x of $\widehat{S}_3^n$. Then we label x with $\langle u_1 \ldots u_r \rangle [i, j]$ or $u_1 \ldots u_r [i, j]$ where $r \leqslant n-2$. $\widehat{S}_3^{n+1}$ contains three isomorphic copies of $\widehat{S}_3^n$, and we denote these copies with $i\widehat{S}_3^{n+1}$, where $i\widehat{S}_3^{n+1}$ is the subgraph which contains $\langle i \ldots i \rangle$, $0 \leqslant i \leqslant 2$; see Fig. 1.



a *b*

Fig. 1. Labeling of S_3^3 (a) and of $\widehat{S}_3^2$ (b)

In this paper, the palette indices of Sierpiński triangle graphs $\widehat{S}_3^n$ and Sierpiński graphs S_3^n are determined. Next, the palette index of S_p^n is determined, where p is even, or $n = 2$ and $p = 4l + 3$.

2. The palette index of Sierpiński triangle graphs

Let $\widehat{S}_3^n$ be the Sierpiński triangle graph. When $n = 0$, then $\widehat{S}_3^n$ is isomorphic to K_3, whose palette index is determined (Theorem 1). Below we consider the case $n > 0$. The graph has two kinds of vertices in terms of vertex degree: three vertices with degree 2 and the remaining vertices with degree 4. To color $\widehat{S}_3^n$, we need at least four colors as $\Delta = 4$.

Let us define edge coloring functions ϕ_n for the graph $\widehat{S}_3^1$ as follows:

$$\phi_n(e) = \begin{cases} n, & \text{if } e \in \{[0,1]00, [1,2]11, [0,2]22\}, \\ n \bmod 4 + 1, & \text{if } e \in \{[0,1]11, [1,2][0,2]\}, \\ (n+1) \bmod 4 + 1, & \text{if } e \in \{[1,2]22, [0,1][0,2]\}, \\ (n+2) \bmod 4 + 1, & \text{if } e \in \{[0,2]00, [0,1][1,2]\}, \end{cases}$$

where $n \in \{1,2,3,4\}$. Thus, for all colorings ϕ_n, we have 4 different sets of palettes and we call this group A:

1) $\{\{1,2,3,4\},\{1,2\},\{1,3\},\{1,4\}\}$;
2) $\{\{1,2,3,4\},\{2,1\},\{2,3\},\{2,4\}\}$;
3) $\{\{1,2,3,4\},\{3,1\},\{3,2\},\{3,4\}\}$;
4) $\{\{1,2,3,4\},\{1,4\},\{2,4\},\{3,4\}\}$.

We will identify two edge colorings if one is obtained by rotating or reflecting the other. Clearly, if we color $\widehat{S}_3^1$ in a manner that all vertices with cardinality 4 have the palette $\{1,2,3,4\}$, then we will get a coloring ϕ_n. After this, let us color the graph $\widehat{S}_3^2$ so that all 4 degree vertices are colored with the palette $\{1,2,3,4\}$. That means we must use ϕ_n colorings to color $i\widehat{S}_3^2$, where $i = 0,1,2$. By considering all possible cases, we have four different sets of palettes and we call that group B:

1) $\{\{1,2,3,4\},\{1,2\},\{1,3\},\{2,3\}\}$;
2) $\{\{1,2,3,4\},\{1,2\},\{1,4\},\{2,4\}\}$;
3) $\{\{1,2,3,4\},\{1,3\},\{1,4\},\{3,4\}\}$;
4) $\{\{1,2,3,4\},\{2,3\},\{2,4\},\{3,4\}\}$.

Proposition 1. For every positive integer n, we have

$$\check{s}(\widehat{S}_3^n) \leqslant 4.$$

Proof. If n is 1 or 2, then we can color $\widehat{S}_3^n$ using a set of palettes from group A or B. If we try to color $\widehat{S}_3^3$ so that each $i\widehat{S}_3^3$ is colored the same as we colored $\widehat{S}_3^2$, where $i = 0,1,2$, and the vertices $[0,1],[0,2],[1,2]$ have the palette $\{1,2,3,4\}$, then we will have all the possible sets of palettes of group A. We now prove the following stronger lemma:

Lemma 1. For every positive integer n, we can color $\widehat{S}_3^n$ using every set of palettes from group A, if n is odd, and every set of palettes from group B, if n is even.

As we have seen, the lemma is true for $\widehat{S}_3^n$, where $n = 1,2,3$. Assume the lemma holds for $n > 0$. We wish to find a satisfying coloring of $\widehat{S}_3^{n+1}$. By the induction assumption, we can color $\widehat{S}_3^n$ using every set of palettes from group A or B depending on whether n is odd or not. In general, if we have colorings for $i\widehat{S}_3^m$, then the palettes of vertices of degree two of $i\widehat{S}_3^m$ are the only essentials for coloring $\widehat{S}_3^m$, where $i = 0,1,2$, $m > 1$. As we saw above in the process of coloring $\widehat{S}_3^2$ ($\widehat{S}_3^3$), if we can color $i\widehat{S}_3^2$ ($i\widehat{S}_3^3$) using every set of palettes from group A (B), then we can color $\widehat{S}_3^2(\widehat{S}_3^3)$ using every set of palettes from group B (A). So we can color $\widehat{S}_3^{n+1}$ by using $\widehat{S}_3^n$ colorings as we did for $\widehat{S}_3^2$ or $\widehat{S}_3^3$. ■

Proposition 2. For every positive integer n, we have

$$\check{s}(\widehat{S}_3^n) \geqslant 3.$$

Proof. Clearly, $\check{s}(\widehat{S}_3^n) \geqslant 2$, since there are vertices with only two different degrees. If we try to color $\widehat{S}_3^1$ with one palette with cardinality 4 ($\{1,2,3,4\}$), then we will get a

coloring ϕ_n. In Proposition 1 for coloring $\widehat{S}_3^n$, we used only colorings ϕ_n for any subgraph $\widehat{S}_3^1$ and tried all possible cases. That means that if we want to have only one palette with cardinality 4, we must use a set of palettes from group A or B, where each set of palettes contains three palettes with cardinality 2. Hence, $\check{s}(\widehat{S}_3^n) \geqslant 3$. ■

Proposition 2 means that if we are looking for a coloring with three palettes, then we should have one palette with cardinality 2 and two palettes with cardinality 4.

Proposition 3. For every positive integer n, if $\check{s}(\widehat{S}_3^n) = 3$, then the palettes for vertices with degree 4 should differ in only one color.

Proof. All possible cases for two palettes with degree 4 are described below:

1) $\{1, 2, 3, 4\}$ and $\{1, 2, 3, 5\}$;
2) $\{1, 2, 3, 4\}$ and $\{1, 2, 5, 6\}$;
3) $\{1, 2, 3, 4\}$ and $\{1, 5, 6, 7\}$;
4) $\{1, 2, 3, 4\}$ and $\{5, 6, 7, 8\}$.

In Fig. 2, we show an example of the coloring of $\widehat{S}_3^2$ with three palettes, where the palettes of cardinality 4 correspond to the first case.

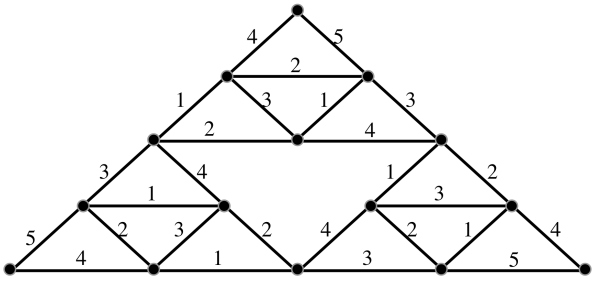


Fig. 2. A coloring of $\widehat{S}_3^2$ with three palettes

We now show that the last three cases are impossible. Suppose we have colored $\widehat{S}_3^n$ with three palettes. If $\check{s}(\widehat{S}_3^n) = 3$, then we have only one palette with cardinality 2. Let's denote that palette by $\{a, b\}$, where $1 \leqslant a < b \leqslant 8$. We will call the colors $5, 6, 7, 8$ the *extra colors*. Now, we change each extra color c with the color $9 - c$ from the set $\{1, 2, 3, 4\}$. The proper edge coloring of $\widehat{S}_3^n$ might be broken only on edges adjacent to the vertices of degree 2 if b is an extra color and $9 - b = a$. But in cases 2–4, we can change the color b with another color different from a. So for the cases 2–4, we can color $\widehat{S}_3^n$ with two palettes, which is a contradiction to Proposition 2. ■

By Proposition 3 and its proof, we may assume that if we have a coloring with three palettes, then the palettes are $\{1, 2, 3, 4\}$, $\{1, 2, 3, 5\}$, and $\{4, 5\}$. Moreover, it is possible to use the palette $\{1, 2, 3, 5\}$ exactly three times.

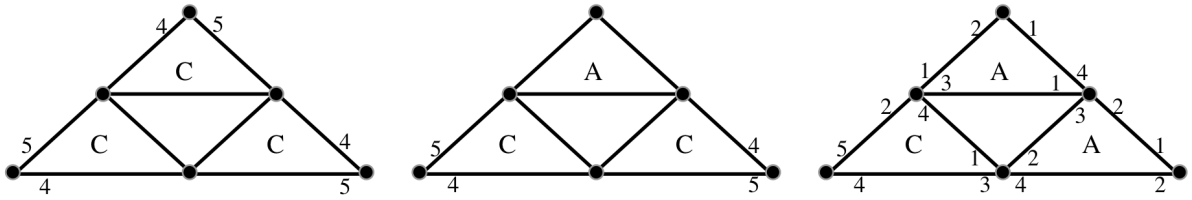
Let us now expose all possible colorings of $\widehat{S}_3^1$, where the palettes $\{1, 2, 3, 4\}$, $\{1, 2, 3, 5\}$, and $\{4, 5\}$ are used. After this, we will have this group of sets of palettes, and we will call this group C:

1) $\{\{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \{4, 5\}, \{1, 2\}, \{3, 4\}\}$;
2) $\{\{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \{4, 5\}, \{1, 3\}, \{2, 4\}\}$;
3) $\{\{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \{4, 5\}, \{1, 4\}, \{2, 3\}\}$.

To find colorings with three palettes of $\widehat{S}_3^n$, as a set of palettes of $\widehat{S}_3^1$, it is enough for us to use only sets of palettes of groups A and C, as we can use the palette $\{1, 2, 3, 5\}$ three times.

There is no coloring of $\widehat{S}_3^1$ with three palettes; thus, $\check{s}(\widehat{S}_3^1) = 4$. As shown in Fig. 2, we can color $\widehat{S}_3^2$ by coloring each $i\widehat{S}_3^2$ using a set of palettes from group C, where $i = 0, 1, 2$.

Let us see what sets of palettes we can have for $\widehat{S}_3^2$ by coloring each $i\widehat{S}_3^2$ using a set of palettes from group A and C, where $i = 0, 1, 2$. We have three cases shown in Fig. 3.



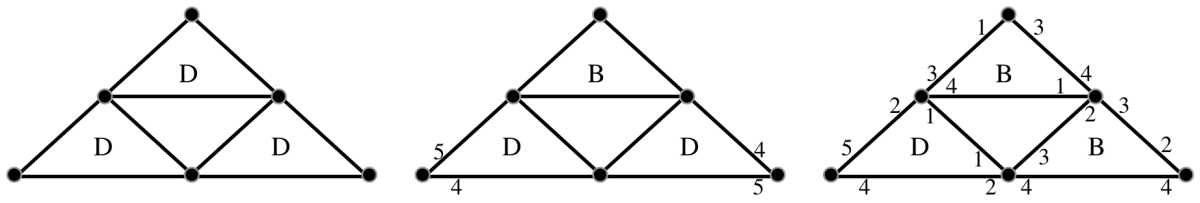
a *b* *c*

Fig. 3. Cases *a*, *b*, *c*

For the case a, the possible combination is the following: all $i\widehat{S}_3^2$ have the same set of palettes from group C, where $i = 0, 1, 2$, and that gives us a coloring with three palettes. Let us notice that we can not use this coloring of $\widehat{S}_3^2$ for coloring a subgraph of $\widehat{S}_3^n$, where $n > 2$, because we do not have a palette with cardinality 4 that has colors 4 and 5. The case b does not give a coloring with three palettes, and we can not use it for coloring $\widehat{S}_3^n$, where $n > 2$, because there are two vertices with the palette $\{4, 5\}$. The case c gives a new group of sets of palettes, and we will call this group D:

1) $\{\{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \{4, 5\}, \{1, 2\}\}$;
2) $\{\{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \{4, 5\}, \{1, 3\}\}$;
3) $\{\{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \{4, 5\}, \{1, 4\}\}$;
4) $\{\{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \{4, 5\}, \{2, 3\}\}$;
5) $\{\{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \{4, 5\}, \{2, 4\}\}$;
6) $\{\{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \{4, 5\}, \{3, 4\}\}$.

Let us now see what sets of palettes we can have for $\widehat{S}_3^3$ by coloring each $i\widehat{S}_3^3$ using a set of palettes from group B and D, where $i = 0, 1, 2$. We have three cases (Fig. 4).



a *b* *c*

Fig. 4. Cases *a*, *b*, *c*

For the case a, there is no possibility to construct a proper edge coloring. The case b does not give a coloring with three palettes, and we can not use it for coloring $\widehat{S}_3^n$, where $n > 3$, because there are two vertices with the palette $\{4, 5\}$. And finally, the case c gives the same sets of palettes of group C that close the chain. Thus, depending on whether the number $n > 0$ is even or odd, we can color $\widehat{S}_3^n$ with the palettes of any set of groups C or D, respectively.

Theorem 2. For every non-negative integer n, the palette index of $\widehat{S}_3^n$ is determined by the formula

$$\check{s}(\widehat{S}_3^n) = \begin{cases} 3, & \text{if } n \text{ is even,} \\ 4, & \text{if } n \text{ is odd.} \end{cases}$$

Proof. Clearly, $\check{s}(\widehat{S}_3^0) = 3$, so we will consider the cases when $n > 0$.

We have shown that we can color $\widehat{S}_3^n$ using any set of palettes from groups A and C if n is odd, and from groups B and D if n is even. Also, we have shown that we can color $\widehat{S}_3^n$ with three palettes if each $i\widehat{S}_3^n$ is colored with palettes of a set of group C, where $i = 0, 1, 2$. Since we have considered all possible cases of coloring $\widehat{S}_3^n$ with three palettes, and it is possible only if $i\widehat{S}_3^n$ is colored using a set of palettes from group C, then $\check{s}(\widehat{S}_3^n) > 3$ for odd n. Consequently, by Proposition 1, $\check{s}(\widehat{S}_3^n) = 4$ if n is odd. ■

3. The palette index of Sierpiński graphs

In this section, we will examine the palette index of Sierpiński graphs S_p^n, where $p > 1$.

If $n = 1$, then S_p^n is isomorphic to K_p, whose palette index was determined (Theorem 1). Now, let us consider the cases when $n > 1$. Here, we have two kinds of vertices in terms of vertex degree: extreme vertices with degree $n-1$ and the remaining vertices with degree n. So $\check{s}(S_p^n) \geqslant 2$.

Theorem 3. For every even integer $p > 1$ and every integer $n > 1$, we have

$$\check{s}(S_p^n) = 2.$$

Proof. Since $\check{s}(S_p^n) \geqslant 2$, we just need a coloring of S_p^n with two palettes. We color all p^{n-1} copies of $S_p^1 = K_p$ in S_p^n with the palette $\{1, \ldots, p-1\}$. Then we color all link edges with the color p. In this way all extreme vertices have the palette $\{1, \ldots, p-1\}$, and the other vertices have the palette $\{1, \ldots, p\}$. ■

Now, consider the case when p is odd.

Proposition 4. For every odd integer $p > 1$ and every integer $n > 1$, we have

$$\check{s}(S_p^n) \geqslant 3.$$

Proof. In [13, Claim in Theorem 4.1], it has been proved for any integer $n \geqslant 1$ and any odd integer $p > 1$, that $\chi'(S_p^n) = p$ and the palettes of extreme vertices of S_p^n are pairwise different. If we try to color S_p^n with two palettes, then we must use a single palette for coloring vertices with degree p, which means that we use only p colors. So we will have p palettes for extreme vertices [13, Claim in Theorem 4.1]. Hence, $\check{s}(S_p^n) \geqslant 3$. ■

Proposition 5. For every odd integer $p > 1$ and every integer $n > 1$, we have

$$\check{s}(S_p^n) \leqslant \begin{cases} \check{s}(K_p), & \text{if } n = 2, \\ \check{s}(K_p) + 1, & \text{if } n > 2. \end{cases}$$

Proof. As shown in [2], if p is odd, then we can always color K_p with three or four palettes, and there is only one vertex s with a unique palette P_s. For a coloring S_p^2, we color each complete graph iS_p^2, and we keep the vertex s as the extreme vertex $(0 \leqslant i \leqslant p-1)$. At this moment, we have these palettes: P_s and $P_1, \ldots, P_m$, where m is 2 or 3. Then we color all link edges with a new color c. Thus, we have these $\check{s}(K_p)$ palettes: P_s and $P_1 \cup \{c\}, \ldots, P_m \cup \{c\}$. To color S_p^3, we color each iS_p^3 as mentioned above, and again, we color uncolored link edges with the same color c. Thus, we have $\check{s}(K_p) + 1$ palettes: P_s and $P_s \cup \{c\}, P_1 \cup \{c\}, \ldots, P_m \cup \{c\}$. To color S_p^n, where $n > 3$, we can do the same steps. In that case, we do not create a new palette. ■

Corollary 1. For every integer p, we have

$$\check{s}(S_{4p+3}^2) = 3.$$

Proof. This result follows from Proposition 4, Proposition 5, and Theorem 1. ■

Theorem 4. For every positive integer n, we have

$$\check{s}(S_3^n) = 3.$$

Proof. By Proposition 4, we obtain $\check{s}(S_3^n) \geqslant 3$. So we just need a coloring with three palettes to prove the theorem. If $n = 1$, then we have K_3, whose palette index is 3. If $n = 2$, we can color S_3^2 as shown in Fig. 5.

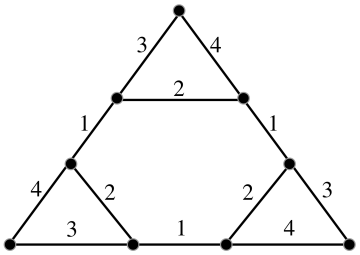


Fig. 5. A coloring of S_3^2 with three palettes

Now, let us consider the two colorings of S_3^2 from Fig. 6.

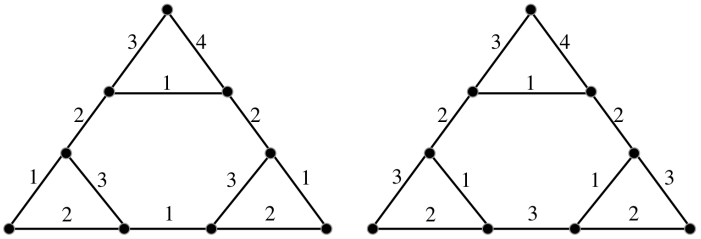
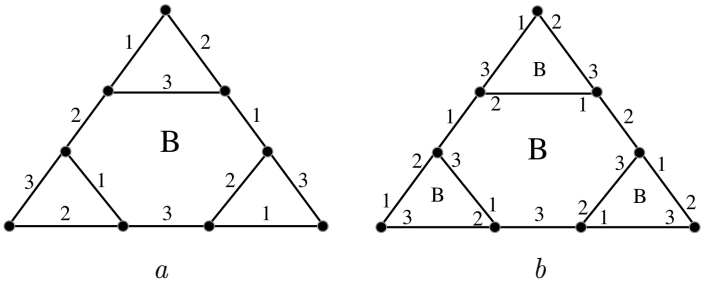


Fig. 6. Group A

Let us denote this group of sets of palettes by A:

1) $\{\{1,2,3\},\{1,2,4\},\{1,2\},\{3,4\}\}$;
2) $\{\{1,2,3\},\{1,2,4\},\{2,3\},\{3,4\}\}$.

Next, let us consider the coloring of S_3^n in Fig. 7.



a *b*

Fig. 7. Group B

Figure 7, *a* gives a coloring of S_3^2. We denote this single element group of sets of palettes by B:

1) $\{\{1,2,3\},\{1,2\},\{1,3\},\{2,3\}\}$.

Figure 7, *b* shows how we can color S_3^n using palettes from group B, where $n > 1$.

In Fig. 8, we can see that, for any integer $n \geqslant 2$, we can color S_3^n using each set of palettes from group A by coloring one of iS_3^n using a set of palettes from group A, two others using a set of palettes from group B, and link edges that connect these iS_3^n with colors 1, 2 or 3, where $i = 0, 1, 2$. We can also see that for S_3^n we can color it with three palettes by coloring all iS_3^n using a set of palettes from group A, and link edges that connect these iS_3^n with colors 1 or 3, where $i = 0, 1, 2$. The theorem is proved. ■

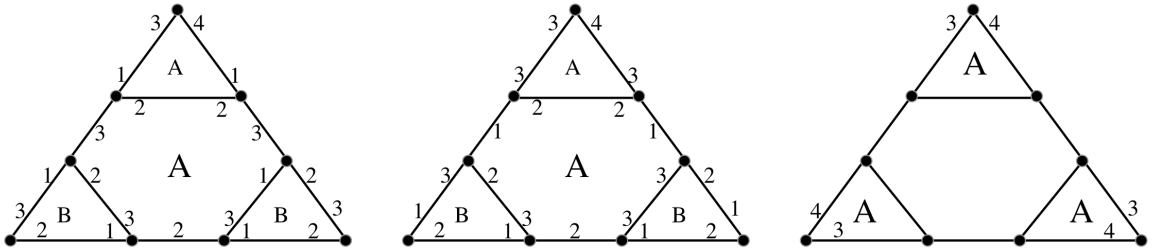


Fig. 8. The coloring of S_3^n with three palettes

Acknowledgement. The author thanks P. A. Petrosyan for many useful comments and suggestions.

REFERENCES

1. *West D.* Introduction to Graph Theory. Prentice-Hall, 2014.
2. *Horňák M., Kalinowski R., Meszka M., and Woźniak M.* Minimum number of palettes in edge colorings. Graphs Combin., 2014, vol. 30, pp. 619–626.
3. *Bonvicini S. and Mazzuoccolo G.* Edge-colorings of 4-regular graphs with the minimum number of palettes. Graphs Combin., 2016, vol. 32, pp. 1293–1311.
4. *Holyer I.* The NP-completeness of edge-coloring. Siam J. Comput., 1981, vol. 10, pp. 718–720.
5. *Avesani M., Bonisoli A., and Mazzuoccolo G.* A family of multigraphs with large palette index. Ars Math. Contemp., 2019, vol. 17, pp. 115–124.
6. *Horňák M. and Hudák J.* On the palette index of complete bipartite graphs. Discussiones Mathematicae Graph Theory, 2018, vol. 38, pp. 463–476.
7. *Casselgren C. and Petrosyan P.* Some results on the palette index of graphs. Discrete Math. Theor. Comput. Sci., 2019, vol. 21, no. 3, A2.
8. *Bonisoli A., Bonvicini S., and Mazzuoccolo G.* On the palette index of a graph: the case of trees. Lecture Notes of Seminario Interdisciplinare di Matematica, 2017, vol. 14, pp. 49–55.
9. *Klavžar S. and Milutinović U.* Graphs $S(n, k)$ and a variant of the Tower of Hanoi problem. Czechoslovak Math. J., 1997, vol. 47, no. 122, pp. 95–104.
10. *Scorer R., Grundy P., and Smith C.* Some binary games. Math. Gaz., 1944, vol. 28, pp. 96–103.
11. *Hinz A., Klavžar S., and Zemljič S.* A survey and classification of Sierpiński-type graphs. Discrete Math., 2017, vol. 217, no. 3, pp. 565–600.
12. *Klavžar S.* Coloring Sierpiński graphs and Sierpiński triangle graphs. Taiwan J. Math., 2008, vol. 12, pp. 513–522.
13. *Jakovac M. and Klavžar S.* Vertex-, edge-, and total-colorings of Sierpiński-like graphs. Discrete Math., 2009, vol. 309, no. 6, pp. 1548–1556.
14. *Teguia A. and Godbole A.* Sierpiński triangle graphs and some of their properties. Australas. J. Combin., 2006, vol. 35, pp. 181–192.

15. *Hinz A. and Schief A.* The average distance on the Sierpiński gasket. Probab. Theory Related Fields, 1990, vol. 87, pp. 129–138.
16. *Kaimanovich V.* Random walks on Sierpiński graphs: hyperbolicity and stochastic homogenization. P. Grabner, W. Woess (eds.) Fractals in Graz 2001. Trends in Mathematics. Birkhäuser, Basel, 2003, pp. 145–183.
17. *Imran M., Hafi S., Gao W., and Farahani M. R.* On topological properties of Sierpiński networks. Chaos Soliton. Fract., 2017, vol. 98, pp. 199–204.

УДК 519.176 DOI 10.17223/20710410/54/6

SERIES OF FAMILIES OF DEGREE SIX CIRCULANT GRAPHS[1]

E. A. Monakhova

Institute of Computational Mathematics and Mathematical Geophysics SB RAS, Novosibirsk, Russia

E-mail: emilia@rav.sscc.ru

An approach for constructing and optimizing graphs of series of analytically described circulant graphs of degree six with general topological properties is proposed. The paper presents three series of families of undirected circulants having the form $C(N(d,p);1,s_2(d,p),s_3(d,p))$, with an arbitrary diameter $d>1$ and a variable parameter $p(d)$, $1\leqslant p(d)\leqslant d$. The orders N of each graph in the families are determined by a cubic polynomial function of the diameter, and generators s_2 and s_3 are defined by polynomials of the diameter of various orders. We have proved that the found series of families include degree six extremal circulant graphs with the largest known orders for all diameters. By specifying the functions $p(d)$, new infinite families of circulant graphs including solutions close to extremal graphs are obtained.

Keywords: *Abelian Cayley graph, degree/diameter problem, families of degree six circulant graphs, triple loop graphs, extremal circulant graphs.*

СЕРИИ СЕМЕЙСТВ ЦИРКУЛЯНТНЫХ ГРАФОВ СТЕПЕНИ ШЕСТЬ

Э. А. Монахова

Институт вычислительной математики и математической геофизики СО РАН, г. Новосибирск, Россия

Предложен подход к построению и оптимизации графов серий аналитически описываемых циркулянтных графов степени шесть с общими топологическими свойствами. Представлены три серии семейств неориентированных циркулянтов вида $C(N(d,p);1,s_2(d,p),s_3(d,p))$ произвольного диаметра $d>1$ с переменным параметром $p(d)$, $1\leqslant p(d)\leqslant d$. Порядки N каждого графа в семействах определяются кубическим полиномом от диаметра, а образующие s_2 — полиномами от диаметра различных порядков. Доказано, что найденные серии семейств включают экстремальные циркулянтные графы степени 6 с самыми большими известными порядками для всех диаметров. Посредством задания функций $p(d)$ построены новые бесконечные семейства циркулянтных графов, включая решения, близкие к экстремальным графам.

Ключевые слова: *граф Кэли абелевой группы, проблема d/k графов, семейства циркулянтных графов степени 6, трёхмерные кольцевые циркулянтные графы, экстремальные циркулянтные графы.*

[1]The work was supported by ICMMG SB RAS budget project no. 0251-2021-0005.

1. Introduction

Circulant graphs are Cayley graphs of Abelian groups. They are widely studied in graph theory and discrete mathematics and play an important role in various applications including network design, see surveys [1 – 4] and references in them.

Let $s_1, s_2, \ldots, s_k, N$ be a set of integers such that $1 \leqslant s_1 < s_2 < \ldots < s_k < N$, and let $S = (s_1, s_2, \ldots, s_k)$ be a generator set. An undirected graph $C(N; S)$ with sets of vertices $V = \{0, 1, \ldots, N-1\}$ and edges $E = \{(v, (v \pm s_l) \bmod N) : v \in V, l = 1, \ldots, k\}$, is called *circulant graph*, k is the dimension, N is the order of the graph. The diameter of C is $\mathrm{dia}(C) = \max\limits_{i,j \in V} D(i,j)$, where $D(i,j)$ is the length of a shortest path from vertex i to vertex j. In the paper, we consider the class of even-degree multi-loop circulants when $s_1 = 1$ and $s_k \neq N/2$ for even N [1 – 7].

For any given k and d, the function $M(d,k)$ defines the maximum number of vertices that can be reached from any vertex of a circulant graph of dimension k in at most d steps. It is known [8] that

$$M(d,k) = \sum_{i=0}^{k} 2^i \binom{k}{i} \binom{d}{i},$$

where the value of $M(d,k)$ can be viewed as the Moore bound for circulant graphs of dimension k. This is a polynomial in d of order k:

$$M(d,k) = \frac{2^k}{k!} d^k + \frac{2^{k-1}}{(k-1)!} d^{k-1} + O(d^{k-2}).$$

Following [5], we define for any natural d and k the extremal function $P(d,k)$ as maximum possible (attainable) natural number N such that there is a set of generators $S = (1, s_2, \ldots, s_k)$ for which $\mathrm{dia}(C(N;S)) \leqslant d$. We have $P(d,k) = M(d,k)$ for $k \leqslant 2$, namely,

$$P(d,1) = 2d + 1, \quad P(d,2) = 2d^2 + 2d + 1,$$

and $P(d,k) < M(d,k)$ for $k > 2$ [5, 9 – 11], including

$$P(d,3) < M(d,3) = \frac{4d^3}{3} + 2d^2 + \frac{8d}{3} + 1.$$

It is difficult to obtain the exact value of $P(d,k)$ for $k \geqslant 3$ and large d. This is a solution to the degree/diameter problem [12 – 14] in the class of circulant networks and it leads to an exhaustive computer search. The lower bounds for $P(d,k)$ in each individual case may depend on the diameter under consideration and are usually obtained by finding infinite families of graphs with these estimates (see also the table of the orders of the largest known circulant graphs [15]). Note that for a given dimension and diameter, circulant graphs with the maximum possible order (or the nearest to it), taken as a model of interconnection networks of multiprocessor systems, have the maximum reliability and connectivity and the minimum number of steps in the implementation of routing algorithms. Using circulant graphs as a network-on-chip (NoC) topology [16, 17] becomes relevant due to their better structural properties and high scalability compared to standard NoC topologies (2D-mesh, 2D-torus). Three-dimensional circulant topologies for NoCs [18, 19] are a promising alternative to the classic 3D-mesh and 3D-torus topologies [20, 21] due to the best characteristics of the diameter and average distance between nodes. An urgent task for NoCs with three-dimensional circulant topology is the development of effective routing

algorithms related to the peculiarities of the requirements for the use of chip resources in NoCs.

The following infinite families of degree 6 circulant graphs with an analytical description are known in the literature. The family of circulant graphs of diameter d

$$C(3d^2+3d+1; 1, 3d+1, 3d+2), \quad d \geqslant 1,$$

was obtained in [22] as a solution to the optimization problem for hexagonal tessellation on the plane of circulants of the form $C(N; s_1, s_2, s_1+s_2)$ with diameter d. Note that the family is a subset of the family of Eisenstein — Jacobi graphs [23] introduced for constructing perfect codes. Shortest path search algorithms for this family were given in [24, 25]. In [26], the family of three-dimensional circulants has been found as a solution to the optimization problem when considering the Kronecker product of two circulants of degrees 2 and 3. The family has diameter $d \equiv 3, 5 \pmod 6$ and order $N = 4d^2 - 2d - 2$.

Families of the so-called multiplicative circulant graphs of dimension $k \geqslant 3$ have been obtained in [5, 6, 8, 27]. In [6, 27], the diameter and shortest path search algorithms were also given for the families. Below for $k = 3$, we give the orders of graphs of these families represented as a function of diameter d; for diameter $d \geqslant 3$, $d \equiv 0 \pmod 3$ [8, 27]:

$$N = \left(\frac{2d+3}{3}\right)^3 = \frac{8}{27}d^3 + O(d^2);$$

for diameter $d \geqslant 5$, $d \equiv 2 \pmod 3$ [6]:

$$N = \left(\frac{2d+2}{3}\right)^3 = \frac{8}{27}d^3 + O(d^2);$$

and for diameter $d \geqslant 3$, $d \equiv 0 \pmod 3$ [5]:

$$N = \frac{32}{27}d^3 + \frac{8}{9}d^2 + \frac{2}{3}d.$$

The families of the largest known degree 6 circulant graphs (extremal circulants) were discovered by E. A. Monakhova [9] and in [28] (for Cayley graphs of Abelian groups).

For dimension $k > 3$, R. R. Lewis have recently obtained families of the largest known circulant graphs of degrees 8 and 10 with an analytical description [10, 11]. Formulas for the order N in diameter $d \geqslant 3$ of degree 8 graphs are shown below:

$$N = \begin{cases} d^4/2 + d^3 + 3d^2 + 2d & \text{for} \quad d \equiv 0 \pmod 2, \\ d^4/2 + d^3 + 3d^2 + 3d + 1/2 & \text{for} \quad d \equiv 1 \pmod 2. \end{cases}$$

As we can see, only individual families of circulants have been obtained earlier, and their topological properties and the possibility of obtaining good routing algorithms for some of them have been studied.

In [29], the author introduced the concept of a series of families of three-dimensional circulant graphs defined by two parameters, one of which is their common diameter and the second is a function of the diameter. This paper is an extension of the previous one. We introduce three series of parametrically described infinite families of circulant graphs that differ in the set of graph generators. We prove that these series include extremal triple loop graphs with the maximum number of vertices for any diameter and have common

topological and communicative properties (Sections 2–4). This result makes it possible to create previously unknown infinite families of dense circulant graphs with varying the diameter and also to construct a series of d graphs for a fixed diameter $d > 1$. Section 5 presents examples of constructing new infinite families of triple loop networks in all the series based on specifying functions $p = p(d)$. The results of constructing the three series of circulants are presented in Section 6 and the Appendix. Another important property is the existence of a general structure of the graphs of the found families, which leads to the construction of a general analytical method for finding the shortest paths and routing algorithm for them.

2. A series of circulants with generators $s_2 = f(d)$

Consider a set of circulant graphs of the form $C(N; 1, s_2, s_3)$ with $s_1 = 1$ and $1 < s_2 < s_3 \leqslant \lfloor N/2 \rfloor$. Denote $\Delta = s_3 - s_2$. We place the vertices of a graph C on the line, as shown in Fig. 1 and 2. They are labeled from 0 to N (the vertex N is understood to be the same vertex as 0). Define $+s_3$- and $-s_3$-jumps from i, if we travel to $(i + s_3)$ mod N or $(i - s_3)$ mod N, respectively. Similarly, define $+s_2$- and $-s_2$-jumps and +1- and −1-jumps. In the paper, we also use $\pm\Delta$-jumps of length 2. Since the circulant graphs are vertex transitive, it is sufficient to consider 0 as the initial vertex. For simplicity, we will use the notation $D(v)$ instead of $D(0, v)$.

The following slightly modified Lemma from [29] is used in the proofs of Theorems.

Lemma 1 [29]. In a triple loop graph $C(N; 1, s_2, s_3)$, let $0 \leqslant i < j < N$ be any two vertices, and let $D(i)$, $D(j)$ be the values of their distances from 0. Then, using +1-jumps from i and −1-jumps from j, we have

$$\max_{i \leqslant v \leqslant j} D(v) = \lfloor (j - i + D(i) + D(j))/2 \rfloor.$$

The maximum is reached at the vertex $v = \lfloor (j + i + D(j) - D(i))/2 \rfloor$.

At first, we will consider the case when generators s_2 and s_3 of $C(N; 1, s_2, s_3)$ are polynomials in d of orders 1 and 2, respectively. We have the following result.

Theorem 1. Let $1 \leqslant p \leqslant d$ for any integer $d > 1$. Then any circulant graph $C(N; 1, s_2, s_3)$, where

$$\begin{cases} N = p^3 - (4d + 1/2)p^2 + 4d^2p + 2d^2 + 2d + 1 & \text{for even } p, \\ N = p^3 - (4d + 1/2)p^2 + 4d^2p + 2d^2 + 2d + 1/2 & \text{for odd } p, \\ s_2 = 2(d - \lceil p/2 \rceil) + 1, \\ s_3 = 2(d - \lfloor p/2 \rfloor)s_2 + 1, \end{cases} \tag{1}$$

has diameter d.

Proof. Consider a graph $C(N; 1, s_2, s_3)$, where N, s_2 and s_3 are given by (1), $d > 1$ and $1 \leqslant p \leqslant d$. The representation of vertices of C is shown in Fig. 1.

From (1) it follows that $r = N \bmod s_3 = (s_3 + s_2)/2$ and hence

$$N = ps_3 + (s_3 + s_2)/2. \tag{2}$$

We need to prove that the graphs given by (1) have the diameter d. We will divide all the vertices $0 \leqslant v \leqslant N$ into the following segments $A_i = [is_3, (i + 1)s_3]$, $i = 0, 1, \ldots, p$, which in turn are divided into the subsegments:

$$A_i^l = [is_3, N - (p - i)s_3], \quad A_i^r = [N - (p - i)s_3, (i + 1)s_3].$$

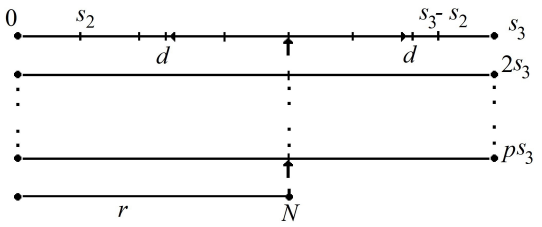


Fig. 1. The representation of vertices of a graph defined by (1)

We have

$$D(is_3) = i, \quad D((i+1)s_3) = i+1, \quad D(N-(p-i)s_3) = p-i.$$

All vertices in A_i^l can be reached from is_3 by $+s_2$-jumps and ± 1-jumps or from $N-(p-i)s_3$ by $-s_2$-jumps and ± 1-jumps. Similarly, all vertices in A_i^r can be reached from $N-(p-i)s_3$ by $+s_2$-jumps and ± 1-jumps or from $(i+1)s_3$ by $-s_2$-jumps and ± 1-jumps. From the structure of the graphs, it follows that $|A_i^l| = |A_i^r| + s_2$, and in A_i^r distances $D(v)$ of vertices v are the same as in $[is_3 + s_2, N-(p-i)s_3]$. Hence, it is sufficient only to consider the segments A_i^l. In turn, they are divided into the subsegments

$$A_{ik}^l = [is_3 + ks_2, is_3 + ks_2 + \lceil s_2/2 \rceil],$$
$$A_{ik}^r = [is_3 + ks_2 + \lceil s_2/2 \rceil, is_3 + (k+1)s_2],$$

where $k = 0, 1, \ldots, d - \lfloor p/2 \rfloor$, since we have $\lfloor (s_3 + s_2)/2s_2 \rfloor = d - \lfloor p/2 \rfloor$ by (1). Note that for $k = d - \lfloor p/2 \rfloor$ the segment A_{ik}^r is not considered. We have $|A_{ik}^l| = \lceil s_2/2 \rceil = |A_{ik}^r| + 1$ and accordingly in A_{ik}^r the values of $D(v)$ of the vertices v are the same as in $[is_3 + ks_2 + 1, is_3 + ks_2 + \lceil s_2/2 \rceil]$. Hence, it is sufficient only to consider the segments A_{ik}^l to determine the maximum distance in the graph. We have

$$D(is_3+ks_2) = i+k, \quad D(is_3+ks_2+\lceil s_2/2 \rceil) = d+\lceil p/2 \rceil - i-k, \quad D(is_3+(k+1)s_2) = i+k+1.$$

To obtain in A_{ik}^l the maximum distance of vertices from 0, we use Lemma 1:

$$\max_{v \in A_{ik}^l} D(v) = \lfloor (i+k+d+\lceil p/2 \rceil - (i+k) + \lceil s_2/2 \rceil)/2 \rfloor = d.$$

Now we will show that there is a vertex v at the distance $D(v) = d$ from 0. Let $v = N - ps_3 - (d-p)s_2$. For it, as we can see, there is a path with the number of steps d using $-s_3$-jumps and $-s_2$-jumps. On the other hand, using (2) and substituting s_3 from (1) into v, we obtain $v = \lfloor s_3/2 \rfloor + \lceil s_2/2 \rceil - (d-p)s_2 = \lceil p/2 \rceil s_2 + d - \lceil p/2 \rceil + 1$. It follows that the length of the path from 0 to v through the nearest vertex of the form $\lceil p/2 \rceil s_2$ is $d+1$. Similarly, we have $v = (\lceil p/2 \rceil + 1)s_2 - (d - \lceil p/2 \rceil)$ and hence the length of the path from 0 to v through another nearest vertex $(\lceil p/2 \rceil + 1)s_2$ is also equal to $d+1$. The lengths of other paths from 0 to v are greater than d. Therefore, the graphs prescribed by (1) have diameter d. ■

We introduce the concept of a series of graphs of Γ. For any integer $d > 1$, let $p = 1, 2, \ldots, d$. Then we have an infinitive set (*series*) Γ of triple loop graphs with diameters $d = 2, 3, \ldots$:

$$\Gamma = \bigcup_{(d>1) \wedge (1 \leqslant p \leqslant d)} C(N; 1, s_2, s_3),$$

where N, s_2 and s_3 are defined using (1).

Now consider the optimization problem for Γ: to find a function $p = p(d)$ giving the maximum of $N = N(p)$ for all $d > 1$ among graphs of Γ with diameter $d > 1$.

Theorem 2. Let $d > 1$ be an integer. The maximum order of circulant graphs $C(N; 1, s_2, s_3) \in \Gamma$ with diameter d is

$$N = \begin{cases} 32d^3/27 + 16d^2/9 + 2d + 1 & \text{for } d \equiv 0 \pmod 3, \\ 32\lfloor d/3 \rfloor^3 + 48\lfloor d/3 \rfloor^2 + 26\lfloor d/3 \rfloor + 5 & \text{for } d \equiv 1 \pmod 3, \\ 32\lfloor d/3 \rfloor^3 + 80\lfloor d/3 \rfloor^2 + 70\lfloor d/3 \rfloor + 21 & \text{for } d \equiv 2 \pmod 3. \end{cases} \tag{3}$$

The maximum is achieved with the following generators:

$$(s_2, s_3) = \begin{cases} (4d/3 + 1, 16d^2/9 + 4d/3 + 1) & \text{for } d \equiv 0 \pmod 3, \\ (4\lfloor d/3 \rfloor + 2 \pm 1, 16\lfloor d/3 \rfloor^2 + 16\lfloor d/3 \rfloor + 5 \pm (4\lfloor d/3 \rfloor + 2)) & \text{for } d \equiv 1 \pmod 3, \\ (4\lfloor d/3 \rfloor + 3, 16\lfloor d/3 \rfloor^2 + 28\lfloor d/3 \rfloor + 13) & \text{for } d \equiv 2 \pmod 3. \end{cases} \tag{4}$$

Proof.

C a s e 1. Let p be an even number. Our goal is to find the maximum function $N = N(p)$ for a given $d > 1$. The function N is a cubic polynomial in p with the following coefficients: $a = 1 > 0$, $b = -4d - 1/2$, $c = 4d^2$. We will find a valued-integer function $p(d)$ such that N defined by (1) has a maximum for any $d > 1$. The discriminant $D = 3ac - b^2 = -4d^2 - 4d - 1/4 < 0$. Hence, $N(p)$ has one maximum when

$$p = -\frac{b + \sqrt{-D}}{3a} = \frac{4}{3}d - \frac{2}{3}\sqrt{d^2 + d + \frac{1}{16}} + \frac{1}{6}.$$

Since $d + 1/4 < \sqrt{d^2 + d + 1/16} < d + 1/2$, we have $\dfrac{2}{3}d - \dfrac{1}{6} < p < \dfrac{2}{3}d$. Since $p(d)$ is a valued-integer function with even values, we take the nearest even integer and obtain

$$p = 2\lfloor d/3 \rfloor, \quad \text{if} \quad d \equiv 0, 1 \pmod 3.$$

Substituting the found p into (1) we obtain s_2, s_3 and N for $d \equiv 0, 1 \pmod 3$ (the version with "+").

C a s e 2. Let p be an odd number. Similarly to case 1, we have the following: the maximum of $N = N(p)$ for a given d is reached when

$$p = 2\lfloor d/3 \rfloor + 1, \quad \text{if} \quad d \equiv 1, 2 \pmod 3.$$

Substituting the found p into (1), we obtain s_2, s_3, and N for $d \equiv 1, 2 \pmod 3$ (the version with "$-$"). ■

3. A series of circulants with generators $s_2 = f(d^2)$

We will now study the case when generators s_2 and s_3 of a graph are polynomials in d of order 2. We have the following result.

Theorem 3. Let $1 \leqslant p < d$ for any integer $d > 1$. Then any circulant graph $C(N; 1, s_2, s_3)$, where

$$\begin{cases} N = -8p^3 + (8d + 4)p^2 + 2d + 1, \\ s_2 = -4p^2 + 4dp + 4p - 2d, \\ s_3 = s_2 + 4d - 4p + 2, \end{cases} \tag{5}$$

has diameter d.

We introduce the concept of a series of graphs of Φ. For any integer $d > 1$, let $p = 1, 2, \ldots, d-1$. Then we have an infinite set (series) Φ of triple loop graphs with diameters $d = 2, 3, \ldots$:

$$\Phi = \bigcup_{(d>1)\wedge(1\leqslant p<d)} C(N; 1, s_2, s_3),$$

where N, s_2 and s_3 are defined by (5).

First, we prove Lemma 2, which gives a general analytical method for obtaining the distance function $D(v)$ for all graphs in Φ. We can restrict our consideration to the values $0 \leqslant v \leqslant \lfloor N/2 \rfloor$, since $D(v) = D(N - v)$ in any circulant graph.

Lemma 2. Let $C(N; 1, s_2, s_3) \in \Phi$ be a triple loop graph and $\delta = 2(d + 1 - p)$. For any vertex v, $0 \leqslant v \leqslant \lfloor N/2 \rfloor$ of the graph C let $i = \lfloor v/s_3 \rfloor$. If $v \leqslant (i+1)s_2$, then

$$D(v) = \begin{cases} i + 2j + \delta - |k|, & \text{if } (0 \leqslant i + 2j \leqslant d - \delta) \text{ and } (-\delta \leqslant k < \delta - 2), \\ & \text{or if } (d - \delta < i + 2j \leqslant d) \text{ and} \\ & (-\delta \leqslant k \leqslant d - \delta - (i + 2j)), \text{ or} \\ & i + 2j - (d - \delta) \leqslant k < \delta - 2, \\ 2d + 1 - (i + 2j + \delta - |k|) & \text{otherwise,} \end{cases} \tag{6}$$

where

$$j = \lfloor (v - is_3)/(s_3 - s_2) \rfloor, \quad k = v - is_3 - j(s_3 - s_2) - \delta. \tag{7}$$

If $v > (i+1)s_2$, then

$$D(v) = \begin{cases} i + \delta - |k|, & \text{if } (0 \leqslant i \leqslant d - \delta) \text{ and } (-\delta < k < \delta - 1), \\ & \text{or if } (d - \delta < i \leqslant d - \delta/2) \text{ and} \\ & (-\delta < k \leqslant d - \delta - i), \text{ or } i - (d - \delta) \leqslant k < \delta - 1, \\ 2d + 1 - (i + \delta - |k|) & \text{otherwise,} \end{cases} \tag{8}$$

where

$$j = \lfloor (v - (i+1)s_2)/(s_3 - s_2) \rfloor, \quad k = v - (i+1)s_2 - j(s_3 - s_2) - \delta + 1. \tag{9}$$

Proof. Consider a graph $C(N; 1, s_2, s_3) \in \Phi$, where $d > 1$ and $p = 1, 2, \ldots, d-1$. For simplicity, we define $\Delta = s_3 - s_2 = 4(d - p) + 2$, $\delta = \Delta/2 + 1$. Hence, $p = \lfloor s_3/\Delta \rfloor$, $N = (2p-1)s_3 + \Delta + 1$, and

$$\delta = 2(d + 1 - p). \tag{10}$$

The representation of vertices of C is shown in Fig. 2, here $q = 2p - 1$, $r = \Delta + 1$. We will divide the vertices $0 \leqslant v \leqslant N/2$ into the following segments:

$$A_i = [is_3, (i+1)s_2], \quad B_i = [(i+1)s_2, (i+1)s_3], \quad 0 \leqslant i < p.$$

Note that $v = \lfloor N/2 \rfloor \in B_{p-1}$. We have $|A_i| = (p - i - 1)\Delta + \Delta/2 + 1$, $|B_i| = (i+1)\Delta$, $D(is_2) = D(is_3) = i$.

Consider two types of vertices in A_i reached from vertices is_3 by $+\Delta$-jumps and from vertices $(i+1)s_2$ by $-\Delta$-jumps:

$$x_{ij} = is_3 + j\Delta = (i + j)s_3 - js_2,$$
$$x'_{ij} = x_{ij} + \delta = (i+1)s_2 - (p - 1 - i - j)\Delta = (p - j)s_2 - (p - 1 - i - j)s_3,$$

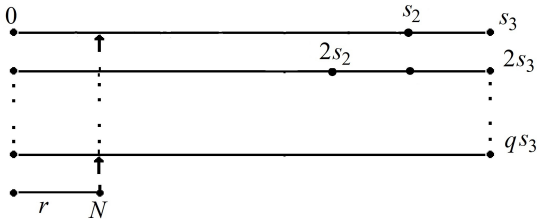


Fig. 2. The representation of vertices of a graph defined by (5)

where $0 \leqslant i < p$, $0 \leqslant j < p - i$. Using (10) and taking into account that there is a path from x'_{ij} to x_{ij} with length $2p - 1 - (i + 2j) + \delta = 2d + 1 - (i + 2j)$, we obtain $D(x_{ij}) = \min\{i + 2j, 2d + 1 - (i + 2j)\}$. Therefore,

$$D(x_{ij}) = \begin{cases} i + 2j, & \text{if } i + 2j \leqslant d, \\ 2d + 1 - (i + 2j), & \text{if } i + 2j > d. \end{cases} \tag{11}$$

Similarly, we have $D(x'_{ij}) = \min\{2d + 1 - i - 2j - \delta, i + 2j + \delta\}$ and

$$D(x'_{ij}) = \begin{cases} i + 2j + \delta, & \text{if } i + 2j \leqslant d - \delta, \\ 2d + 1 - (i + 2j + \delta), & \text{if } i + 2j > d - \delta. \end{cases} \tag{12}$$

Consider the vertices in B_i reached from vertices $(i + 1)s_2$ by $+\Delta$-jumps:

$$y_{ij} = (i + 1)s_2 + j\Delta = (i + 1 - j)s_2 + js_3, \quad 0 \leqslant i < p, \quad 0 \leqslant j \leqslant i + 1.$$

From here we have

$$D(y_{ij}) = i + 1. \tag{13}$$

Note that $B_i = \bigcup\limits_{j=0}^{i} [y_{ij}, y_{ij+1}]$.

Let $0 \leqslant v \leqslant \lfloor N/2 \rfloor$ be a vertex of the graph. Compute $i = \lfloor v/s_3 \rfloor$.

C a s e 1. Let $v \leqslant (i + 1)s_2$, hence $v \in A_i$, $0 \leqslant i < p$. Compute j and k by (7). Having $0 \leqslant j < p - i$, $-\delta \leqslant k < \delta - 2$, and using (10), we obtain $0 \leqslant i + 2j \leqslant 2d - \delta - i$. Taking into account that either $0 \leqslant i + 2j \leqslant d - \delta$, or $d - \delta < i + 2j \leqslant d$, or $d < i + 2j \leqslant 2d - \delta - i$, and using (11) and (12), we obtain (6).

C a s e 2. Let $v > (i + 1)s_2$, hence $v \in B_i$, $0 \leqslant i < p$. Compute j and k by (9).

2a) Let $0 \leqslant i \leqslant d - \delta$. Using (13), we obtain $D(v) = i + \delta - |k|$ when $-\delta < k < \delta - 1$.

2b) Let $i > d - \delta$. In the graph, the movement from N to 0 alone generators $-s_3$ and $-s_2$ decreases the function $D(v)$ for vertices $v \in [y_{ij}, y_{ij+1}]$, $d - \delta < i < p$, $0 \leqslant j \leqslant i$. Consider the vertices m_{ij} lying in the middle of segments $[y_{ij}, y_{ij+1}]$:

$$m_{ij} = y_{ij} + \delta - 1 = (i + 1)s_2 + j\Delta + \delta - 1, \quad d - \delta < i < p, \quad 0 \leqslant j \leqslant i.$$

The movement from N to 0 alone generators $-s_3$ and $-s_2$ gives

$$D(m_{ij}) = 2d + 1 - i - \delta, \tag{14}$$

since $m_{ij} = N - (d + 1 - \delta/2 - j)s_3 - (d - \delta/2 - i + j)s_2$. Taking into account that either $-\delta < k \leqslant d - i - \delta$, or $|k| < i + \delta - d$, or $i + \delta - d \leqslant k < \delta - 1$, and using (13) and (14) and taking the minimum path from 0 to v, we obtain (8). ■

We can now prove Theorem 3.

Proof. Using the formulas (6) and (8), we have the following: the sum of lengths of two possible paths from 0 to v is always equal to $2d+1$ for any vertex v. Therefore, one of the lengths is less than or equal to d. Now it is necessary to show that there is a vertex v of C with $D(v) = d$. Let $v = \lfloor N/2 \rfloor = -4p^3 + (4d+2)p^2 + d$. For even p, there is a path of length d from 0 to v, since $\lfloor N/2 \rfloor = d - p + (p/2)(s_2 + s_3)$. For odd p we have $\lfloor N/2 \rfloor - N = -\lceil N/2 \rceil = d - p - \lfloor p/2 \rfloor s_2 - \lceil p/2 \rceil s_3$ and for v there is also a path of length d from 0. The same result follows from (8). There are no other paths in the graph to v with length less than d. ■

Now, let us consider the optimization problem for Φ: to find a function $p = p(d)$ giving the maximum of $N = N(p)$ for all $d > 1$ among graphs of Φ with diameter $d > 1$.

Theorem 4. Let $d > 1$ be an integer. The maximum order of circulant graphs $C(N; 1, s_2, s_3) \in \Phi$ with diameter d is

$$N = \begin{cases} 32d^3/27 + 16d^2/9 + 2d + 1 & \text{for } d \equiv 0 \pmod 3, \\ 32\lfloor d/3 \rfloor^3 + 48\lfloor d/3 \rfloor^2 + 30\lfloor d/3 \rfloor + 7 & \text{for } d \equiv 1 \pmod 3, \\ 32\lfloor d/3 \rfloor^3 + 80\lfloor d/3 \rfloor^2 + 70\lfloor d/3 \rfloor + 21 & \text{for } d \equiv 2 \pmod 3. \end{cases} \tag{15}$$

The bound is achieved with the following generators:

$$(s_2, s_3) = \begin{cases} (8d^2/9 + 2d/3, 8d^2/9 + 2d + 2) & \text{for } d \equiv 0 \pmod 3, \\ (8\lfloor d/3 \rfloor^2 + 6\lfloor d/3 \rfloor + 2, 8\lfloor d/3 \rfloor^2 + 10\lfloor d/3 \rfloor + 4) & \text{for } d \equiv 1 \pmod 3, \\ (8\lfloor d/3 \rfloor^2 + 10\lfloor d/3 \rfloor + 4, 8\lfloor d/3 \rfloor^2 + 14\lfloor d/3 \rfloor + 6) & \text{for } d \equiv 2 \pmod 3. \end{cases} \tag{16}$$

Proof. Consider a circulant graph $C(N; 1, s_2, s_3) \in \Phi$ with diameter d. The function N is a cubic polynomial in p with the following coefficients: $a = -8$, $b = 8d+4$, $c = 0$. We will find a valued-integer function $p(d)$ such that N defined by (5) has a maximum for any $d > 1$. Take the derivative of $N(p)$ with respect to p: $\dfrac{dN}{dp} = -24p^2 + 2(8d+4)p = 0$. Therefore, N has the maximum when $p = (2d+1)/3$. Since $p(d)$ is a valued-integer function, we take the nearest integer and obtain for any $d \geqslant 1$

$$p(d) = p^* = (2d + d \bmod 3)/3.$$

Substituting p^* into (5), we get that N, s_2 and s_3 are equal to (15) and (16), respectively. ■

The family with $p = d$, namely the graphs $C(4d^2 + 2d + 1; 1, 2d, 2d + 2)$, where $d > 1$, can also be included in Φ since they have diameter d.

4. A series of circulants with generators $s_2 = f(d^3)$

The case of circulant graphs, when all N, s_2 and s_3 are polynomials in d of order 3, was studied in [29].

Theorem 5 [29]. Let $1 \leqslant p < d$ for any integer $d > 1$. Then any circulant graph $C(N; 1, s_2, s_3)$, where

$$\begin{cases} N = 8p^3 - (16d+8)p^2 + (8d^2+8d)p + 2d + 1, \\ s_2 = 4p(d-p)^2 + 2p(d-p) + d - 3p, \\ s_3 = s_2 + 4p, \end{cases} \tag{17}$$

has diameter d.

For any integer $d > 1$, let $p = 1, 2, \ldots, d-1$. Then we obtain an infinite set (series) Ψ of triple loop graphs with diameters $d = 2, 3, \ldots$:

$$\Psi = \bigcup_{(d>1)\wedge(1\leqslant p<d)} C(N; 1, s_2, s_3),$$

where N, s_2 and s_3 are defined by (17). In [29], the optimization problem for Ψ has been also solved.

Theorem 6. Let $d > 1$ be an integer. The maximum order of circulant graphs $C(N; 1, s_2, s_3) \in \Psi$ with diameter d is

$$N = \begin{cases} 32d^3/27 + 16d^2/9 + 2d + 1 & \text{for } d \equiv 0 \pmod 3, \\ 32\lfloor d/3\rfloor^3 + 48\lfloor d/3\rfloor^2 + 22\lfloor d/3\rfloor + 3 & \text{for } d \equiv 1 \pmod 3, \\ 32\lfloor d/3\rfloor^3 + 80\lfloor d/3\rfloor^2 + 70\lfloor d/3\rfloor + 21 & \text{for } d \equiv 2 \pmod 3. \end{cases} \tag{18}$$

The bound is achieved with the following generators:

$$(s_2, s_3) = \begin{cases} (16d^3/27{+}4d^2/9, s_2{+}4d/3) & \text{for } d \equiv 0 \pmod 3, \\ (16d^3/27{+}4d^2/9{-}2d/3{+}17/27, s_2{+}4d/3{-}4/3) & \\ \text{ or} & \\ (16d^3/27{+}4d^2/9{-}4d/3{-}46/27, s_2{+}4d/3{+}8/3) & \text{for } d \equiv 1 \pmod 3, \\ (16d^3/27{+}4d^2/9{-}2d/9{-}29/27, s_2{+}4d/3{+}4/3) & \text{for } d \equiv 2 \pmod 3. \end{cases} \tag{19}$$

For all diameters $d \equiv 0, 2 \pmod 3$ the value of N from (18) is equal to the maximum N from (15), but for $d \equiv 1 \pmod 3$ it is less. Note that for $d \equiv 1 \pmod 3$ there are two sets of generators for N, defined by (18). It is easy to check that for $d \equiv 0, 2 \pmod 3$ the generators (19) are obtained by an equivalent transformation of generators (4), and thus the graphs from Theorems 2 and 6 are isomorphic for these diameters.

Comparing the values of N obtained in Theorems 2, 4, and 6, we come to the conclusion that (15) gives the largest values of N among graphs of sets Γ, Φ and Ψ for all diameters d. This result is in good agreement with the extremal values of N obtained in [9, 28].

5. New families of three-dimensional circulants

If we take any valued-integer functions $p(d)$ such that $1 \leqslant p(d) \leqslant d$ as a parameter p, then we can generate new infinite families of circulant graphs. We have shown examples of new families of circulants constructed by this method for sets Γ, Φ and Ψ (Theorems 2, 4, and 6). These found families are the best ones in the ratio N/d (order/diameter) among all known families of degree 6 circulants. Some examples of constructing other possible families of sets Γ, Φ, and Ψ are presented below.

Example 1. Let $C(N; 1, s_2, s_3) \in \Gamma$, $d > 1$, and

$$p(d) = \begin{cases} 2\lfloor d/3\rfloor - 1 & \text{for } d \equiv 0 \pmod 3, \\ 2(\lfloor d/3\rfloor + 1) & \text{for } d \equiv 1, 2 \pmod 3. \end{cases}$$

Substituting the value of p in (1), we obtain N, s_2 and s_3 for a new infinite family. The resulting N is less than (3) by $4\lfloor d/3\rfloor + 2$ for $d \equiv 0, 2 \pmod 3$ or by $12\lfloor d/3\rfloor + 2$ for $d \equiv 1 \pmod 3$.

Example 2. Let $C(N;1,s_2,s_3)\in\Phi$, $d>1$, and

$$p(d)=\begin{cases}2d/3+1 & \text{for } d\equiv 0 \pmod 3,\\ 2(d-1)/3 & \text{for } d\equiv 1 \pmod 3,\\ (2d-1)/3 & \text{for } d\equiv 2 \pmod 3.\end{cases}$$

Substituting the value of p in (5), we obtain N, s_2, and s_3 for a new infinite family. Resulting N is less than (15) by $8\lfloor d/3\rfloor+4$ for $d\equiv 0,2 \pmod 3$ or by $24\lfloor d/3\rfloor+4$ for $d\equiv 1 \pmod 3$.

With respect to N, the resulting graphs $C(N;1,s_2,s_3)$ in examples 1 and 2 are the nearest to the graphs with the maximum N among all graphs of the sets Γ and Φ, respectively.

For Ψ, the following family was created in [29].

Example 3. Let $C(N;1,s_2,s_3)\in\Psi$, $d>1$, and $p(d)=\lceil d/2\rceil$. Then

$$(N;1,s_2,s_3)=\begin{cases}(d^3+2d^2+2d+1;1,(d^3+d^2-d)/2,(d^3+d^2+3d)/2) & \text{for even } d,\\ (d^3+d^2+d;1,(d^3-3)/2-d,(d^3-3)/2+d+2) & \text{for odd } d.\end{cases}$$

For Ψ, the following function $p(d)$ generates a new family of circulants.

Example 4. Let $C(N;1,s_2,s_3)\in\Psi$, $d>1$, and

$$p(d)=\begin{cases}2\lfloor d/3\rfloor & \text{for } d\equiv 0 \pmod 3,\\ 2\lfloor d/3\rfloor+1 & \text{for } d\equiv 1,2 \pmod 3.\end{cases}$$

Substituting the value of p in (17), we obtain N, s_2, and s_3 for a new infinite family.

As for the ratio N/d, the new families of circulants in examples 1 and 2 are better than families in [5, 6, 8, 22, 26], and the family in example 3 is better than families in [6, 8, 22, 26] and, moreover, in contrast to families from [5, 6, 8, 26], all the obtained families exist for any diameter of the graph.

6. Descriptions of graphs series

Using the system Wolfram Mathematica 10, fragments of circulant families for all sets Γ, Φ, and Ψ with diameters $d=2,\dots,25$ have been implemented (see the Appendix).

Tables 1–3 show part of the descriptions of the obtained circulants $C(N;1,s_2,s_3)$ with diameters d, $2\leqslant d\leqslant 10$: the diameters of graphs d, the values of p, where $1\leqslant p\leqslant d$ for Γ, Φ and $1\leqslant p\leqslant d-1$ for Ψ, the orders of graphs N, and generators s_2 and s_3.

Figures 3–5 show the dependence of the number of vertices N on diameter d, $2\leqslant d\leqslant 25$, and parameter p for the fragments of descriptions for sets Γ, Φ, and Ψ. The values of N of graphs corresponding to the families with the maximum orders for the given diameters are marked in blue in Fig. 3–5. Figure 5 additionally shows the orders of graphs of the family from Example 4 in red. Note that parameter p has a different meaning in figures: $p=\lfloor N/s_3\rfloor$ in Fig. 3, $p=\lfloor s_3/(s_3-s_2)\rfloor$ in Fig. 4, and $p=(s_3-s_2)/4$ in Fig. 5.

Table 1

Descriptions of the graphs of Γ

d	p	N	s_2	s_3	d	p	N	s_2	s_3
2	1	21	3	13	8	1	369	15	241
2	2	19	3	7	8	2	535	15	211
3	1	49	5	31	8	3	647	13	183
3	2	55	5	21	8	4	713	13	157
3	3	47	3	13	8	5	737	11	133
4	1	89	7	57	8	6	727	11	111
4	2	111	7	43	8	7	687	9	91
4	3	111	5	31	8	8	625	9	73
4	4	97	5	21	9	1	469	17	307
5	1	141	9	91	9	2	691	17	273
5	2	187	9	73	9	3	851	15	241
5	3	203	7	57	9	4	957	15	211
5	4	197	7	43	9	5	1013	13	183
5	5	173	5	31	9	6	1027	13	157
6	1	205	11	133	9	7	1003	11	133
6	2	283	11	111	9	8	949	11	111
6	3	323	9	91	9	9	869	9	91
6	4	333	9	73	10	1	581	19	381
6	5	317	7	57	10	2	867	19	343
6	6	283	7	43	10	3	1083	17	307
7	1	281	13	183	10	4	1237	17	273
7	2	399	13	157	10	5	1333	15	241
7	3	471	11	133	10	6	1379	15	211
7	4	505	11	111	10	7	1379	13	183
7	5	505	9	91	10	8	1341	13	157
7	6	479	9	73	10	9	1269	11	133
7	7	431	7	57	10	10	1171	11	111

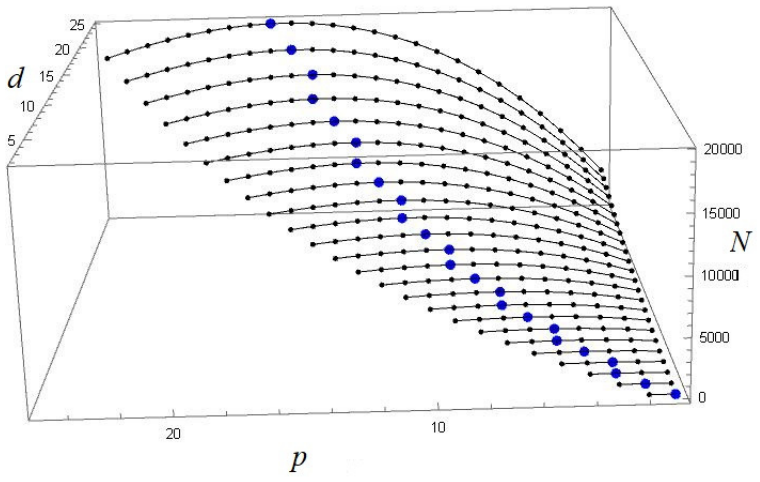


Fig. 3. Number of vertices $N = N(d, p)$ for $C(N; 1, s_2, s_3) \in \Gamma$

Table 2

Descriptions of the graphs of Φ

d	p	N	s_2	s_3	d	p	N	s_2	s_3
2	1	17	4	10	8	1	77	16	46
2	2	21	4	6	8	2	225	40	66
3	1	27	6	16	8	3	413	56	78
3	2	55	10	16	8	4	593	64	82
3	3	43	6	8	8	5	717	64	78
4	1	37	8	22	8	6	737	56	66
4	2	89	16	26	8	7	605	40	46
4	3	117	16	22	8	8	273	16	18
4	4	73	8	10	9	1	87	18	52
5	1	47	10	28	9	2	259	46	76
5	2	123	22	36	9	3	487	66	92
5	3	191	26	36	9	4	723	78	100
5	4	203	22	28	9	5	919	82	100
5	5	111	10	12	9	6	1027	78	92
6	1	57	12	34	9	7	999	66	76
6	2	157	28	46	9	8	787	46	52
6	3	265	36	50	9	9	343	18	20
6	4	333	36	46	10	1	97	20	58
6	5	313	28	34	10	2	293	52	86
6	6	157	12	14	10	3	561	76	106
7	1	67	14	40	10	4	853	92	118
7	2	191	34	56	10	5	1121	100	122
7	3	339	46	64	10	6	1317	100	118
7	4	463	50	64	10	7	1393	92	106
7	5	515	46	56	10	8	1301	76	86
7	6	447	34	40	10	9	993	52	58
7	7	211	14	16	10	10	421	20	22

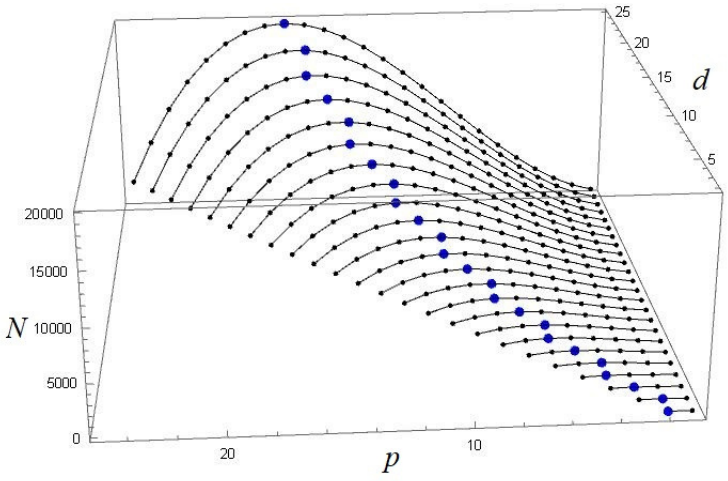


Fig. 4. Number of vertices $N = N(d, p)$ for $C(N; 1, s_2, s_3) \in \Phi$

Table 3

Descriptions of the graphs of Ψ

d	p	N	s_2	s_3	d	p	N	s_2	s_3
3	1	55	20	24	8	3	737	329	341
3	2	39	9	17	8	4	657	284	300
4	1	105	43	47	8	5	497	203	223
4	2	105	38	46	8	6	305	110	134
4	3	57	13	25	8	7	129	29	57
5	1	171	74	78	9	1	595	278	282
5	2	203	83	91	9	2	915	423	431
5	3	155	56	68	9	3	1027	468	480
5	4	75	17	33	9	4	979	437	453
6	1	253	113	117	9	5	819	354	374
6	2	333	144	152	9	6	595	243	267
6	3	301	123	135	9	7	355	128	156
6	4	205	74	90	9	8	147	33	65
6	5	93	21	41	10	1	741	349	353
7	1	351	160	164	10	2	1173	548	556
7	2	495	221	229	10	3	1365	631	643
7	3	495	214	226	10	4	1365	622	638
7	4	399	163	179	10	5	1221	545	565
7	5	255	92	112	10	6	981	424	448
7	6	111	25	49	10	7	693	283	311
8	1	465	215	219	10	8	405	146	178
8	2	689	314	322	10	9	165	37	73

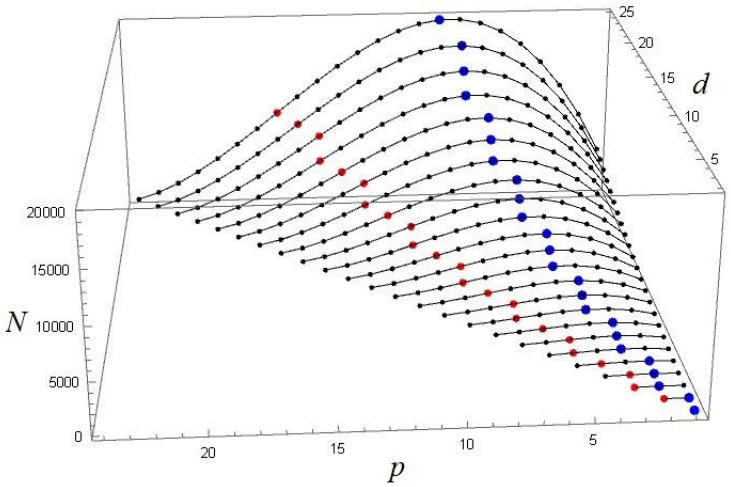


Fig. 5. Number of vertices $N = N(d, p)$ for $C(N; 1, s_2, s_3) \in \Psi$

7. Conclusion

The graphs of three series of the circulants obtained in this paper have not only general topological properties, but also general communicative properties that relate to the organization of routing for these graphs. We do not review in detail the existing routing algorithms for degree 6 circulant graphs. This is a topic for a separate paper. Let's just say that few routing algorithms are known for these graphs and they are not efficient for use in NoCs, therefore analytical routing algorithms that can be developed for graphs of the series obtained are of interest. It should also be noted that the proof of Lemma 2 implies the existence of a general analytical method for calculating the distance function in all graphs

of Φ. This property in turn allowed us to develop a general analytical routing algorithm for all families of Φ. The routing algorithm is described in [18, 30] and implemented in NoC using the example of one of the possible families of Φ as a NoC topology.

Thus, as we could demonstrate on the example of the series Φ of circulans, a general structure of graphs of each found series makes it possible to develop a general analytical method for calculating the distance function and then to obtain the shortest-path vectors for a routing algorithm for all graphs included in the series, changing only the value of the parameter $p(d)$, which defines the form of a considered family of circulants.

The second interesting question is whether there are other series of circulant graphs analytically described and given by two parameters d and $p(d)$ that have the same structural and communication properties? Or is it a common property in the space of analytical descriptions of circulant graphs? Are there other designs of circulant series that contain the largest possible graphs for a given degree and a given diameter? Generalizing this problem, we can say that the question is to discover new regularities in obtaining series of circulant graphs that establish relationships between the analytical connection of the order and generators of a graph and the geometry of the resulting series of graphs.

Acknowledgments

The author thanks O. G. Monakhov for useful discussions.

REFERENCES

1. *Monakhova E. A.* A survey on undirected circulant graphs. Discr. Math. Algorithms Appl., 2012, vol. 4, no. 1, 1250002, 30 p.
2. *Bermond J.-C., Comellas F., and Hsu D. F.* Distributed loop computer networks: a survey. J. Parallel Distrib. Comput., 1995, vol. 24, pp. 2–10.
3. *Feria-Puron R., Pérez-Rosés H., and Ryan J.* Searching for Large Circulant Graphs. arXiv:1503.07357v1 [math.CO], Aug. 11, 2018, 31 p.
4. *Hwang F. K.* A survey on multi-loop networks. Theor. Comput. Sci., 2003, vol. 299, pp. 107–121.
5. *Chen S. and Jia X.-D.* Undirected loop networks. Networks, 1993, no. 23(4), pp. 257–260.
6. *Stojmenović I.* Multiplicative circulant networks. Topological properties and communication algorithms. Discr. Appl. Math., 1997, no. 77, pp. 281–305.
7. *Thomson A. and Zhou S.* Gossiping and routing in undirected triple-loop networks. Networks, 2010, no. 55(4), pp. 341–349.
8. *Wong C. K. and Coppersmith D.* A combinatorial problem related to multimodule memory organizations. J. Assoc. Comput. Mach., 1974, no. 21(3), pp. 392–402.
9. *Monakhova E.* Optimal triple loop networks with given transmission delay: Topological design and routing. Proc. INOC'2003, Evry/Paris, France, 2003, pp. 410–415.
10. *Lewis R. R.* The degree-diameter problem for circulant graphs of degree 8 and 9. Electron. J. Combin., 2014, no. 21(4), article no. P4.50.
11. *Lewis R. R.* The degree-diameter problem for circulant graphs of degrees 10 and 11. Discrete Math., 2018, no. 341, pp. 2553–2566.
12. *Dalfó C., Fiol M. A., Lopéz N., and Ryan J.* An improved Moore bound and some new optimal families of mixed Abelian Cayley graphs. Discr. Math., 2020, vol. 343, no. 10.
13. *Miller M. and Siran J.* Moore graphs and beyond: A survey of the degree/diameter problem. Electron. J. Combin., Dyn. Surv., 2005, no. DS14, 61 p.
14. *Pérez-Rosés H.* Algebraic and computer-based methods in the undirected degree/diameter problem – A brief survey. Electron. J. Graph Theory Appl., 2014, no. 2(2), pp. 166–190.

15. The Degree/Diameter Problem For Circulant Graphs. http://combinatoricswiki.org/wiki/The_Degree_Diameter_Problem_for_Circulant_Graphs.
16. *Monakhova E. A., Romanov A. Yu., and Lezhnev E. V.* Shortest path search algorithm in optimal two-dimensional circulant networks: Implementation for networks-on-chip. IEEE Access, 2020, no. 8, pp. 215010–215019.
17. *Romanov A., Amerikanov A., and Lezhnev E.* Analysis of approaches for synthesis of networks-on-chip by using circulant topologies. J. Physics. Conf. Series, 2018, vol. 1050, no. 1, pp. 1–12.
18. *Monakhova E. A., Monakhov O. G., Romanov A. Yu., and Lezhnev E. V.* Analytical routing algorithm for networks-on-chip with the three-dimensional circulant topology. Proc. MWENT 2020, Moscow, Russia, March 11–13, 2020, pp. 1–6.
19. *Romanov A. Yu. and Starykh V. A.* Routing in triple loop circulants: A case of networks-on-chip. Heliyon, 2020, no. 6(7), pp. 1–7.
20. *Ansari A. Q., Ansari M. R., and Khan M. A.* Modified quadrant-based routing alglrithm for 3D torus network-on-chip architecture. Perspect. Sci., 2016, vol. 8, pp. 718–721.
21. *Joseph J. M., Blochwitz C., Garcia-Ortiz A., and Pionteck T.* Area and power savings via asymmetric organization of buffers in 3D-NoCs for heterogeneous 3D-SoCs. Microprocess. Microsyst., 2017, vol. 48, pp. 36–47.
22. *Yebra J. L. A., Fiol M. A., Morillo P., and Alegre I.* The diameter of undirected graphs associated to plane tessellations. Ars Combinatoria, 1985, no. 20B, pp. 159–171.
23. *Martinez C., Stafford E., Beivide R., and Gabidulin E. M.* Modeling hexagonal constellations with Eisenstein — Jacobi graphs. Problems Inform. Transmission, 2008, no. 44(1), pp. 1–11.
24. *Barrière L., Fàbrega J., Simo E., and Zaragozá M.* Fault-tolerant routings in chordal ring networks. Networks, 2000, no. 36(3), pp. 180–190.
25. *Liestman A. L., Opatrny J., and Zaragozá M.* Network properties of double and triple fixed-step graphs. Int. J. Found. Comp. Sci., 1998, no. 9(1), pp. 57–76.
26. *Jha P. K.* A family of efficient six-regular circulants representable as a Kronecker product. Discr. Appl. Math., 2016, no. 203, pp. 72–84.
27. *Parhami B.* A class of odd-radix chordal ring networks. CS'J J. Comput. Sci. Eng., 2006, vol. 4, no. 2–4, pp. 1–9.
28. *Dougherty R. and Faber V.* The degree-diameter problem for several varieties of Cayley Graphs, 1: The Abelian case. SIAM J. Discr. Math., 2004, no. 17(3), pp. 478–519.
29. *Monakhova E. A.* Parametricheskoe zadanie serii semeystv analiticheski opisyvaemykh tsirkulyantnykh setey stepeni shest' [A set of families of analytically described triple loop networks defined by a parameter]. Prikladnaya Diskretnaya Matematika, 2020, no. 49, pp. 108–119. (in Russian)
30. *Monakhova E. A. and Monakhov O. G.* Dinamicheskij algoritm parnoj marshrutizacii dlya analiticheski zadavaemyh semeystv cirkulyantnyh setey stepeni shest' [A dynamic algorithm of two-terminal routing for analytically described families of circulant networks of degree six]. Proc. XIX Inter. Conf. "Problems of Information in Education, Management, Economics and Technology", Penza, Russia, 2019, pp. 30–37. (in Russian)

СВЕДЕНИЯ ОБ АВТОРАХ

АЛЕКСЕЕВ Евгений Константинович — кандидат физико-математических наук, начальник отдела криптографических исследований ООО «КРИПТО-ПРО», г. Москва. E-mail: **alekseev@cryptopro.ru**

МОНАХОВА Эмилия Анатольевна — кандидат технических наук, доцент, старший научный сотрудник Института вычислительной математики и математической геофизики СО РАН, г. Новосибирск. E-mail: **emilia@rav.sscc.ru**

НИКОЛАЕВ Василий Дмитриевич — заместитель начальника отдела криптографических разработок ООО «КРИПТО-ПРО», г. Москва.
E-mail: **nikolaev@cryptopro.ru**

ОСИПОВА Марина Анатольевна — кандидат физико-математических наук, доцент, доцент кафедры алгебры, геометрии и анализа Дальневосточного федерального университета, научный сотрудник Института прикладной математики ДВО РАН, г. Владивосток. E-mail: **mao1975@list.ru**

СМЫШЛЯЕВ Станислав Витальевич — кандидат физико-математических наук, заместитель генерального директора ООО «КРИПТО-ПРО», г. Москва.
E-mail: **svs@cryptopro.ru**

СОЛОМАТИН Денис Владимирович — кандидат физико-математических наук, доцент, доцент кафедры математики и методики обучения математике Омского государственного педагогического университета, г. Омск.
E-mail: **solomatin_dv@omgpu.ru**

ТРИФОНОВ Дмитрий Игоревич — эксперт технического комитета по стандартизации «Криптографическая защита информации», г. Москва.
E-mail: **d.arlekino@gmail.com**

ФОМИН Денис Бонифлавович — старший преподаватель Национального исследовательского университета «Высшая школа экономики», г. Москва.
E-mail: **dfomin@hse.ru**

ЦИЦИАШВИЛИ Гурами Шалвович — доктор физико-математических наук, профессор, главный научный сотрудник Института прикладной математики ДВО РАН, г. Владивосток. E-mail: **guram@iam.dvo.ru**

GHAZARYAN Aghasi Bagrat — Ph.D., Yerevan State University, Yerevan.
E-mail: **ghazaryan.aghasi@gmail.com**

Журнал «Прикладная дискретная математика» входит в перечень ВАК рецензируемых научных изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание учёной степени кандидата и доктора наук по специальностям 01.01.06 — «Математическая логика, алгебра и теория чисел», 01.01.09 — «Дискретная математика и математическая кибернетика», 05.13.11 — «Математическое и программное обеспечение вычислительных машин,комплексов и компьютерных сетей», 05.13.17 — «Теоретические основы информатики», 05.13.19 — «Методы и системы защиты информации, информационная безопасность», а также в перечень журналов, рекомендованных ФУМО ВО ИБ в качестве учебной литературы по специальности «Компьютерная безопасность».

Журнал индексируется в базах данных Web of Science (Emerging Sources Citation Index (ESCI) и Russian Science Citation Index (RSCI)), Scopus, MathSciNet и Zentralblatt MATH.

Журнал «Прикладная дискретная математика» распространяется по подписке; его подписной индекс 38696 в объединённом каталоге «Пресса России». Полнотекстовые электронные версии вышедших номеров журнала доступны на его сайте journals.tsu.ru/pdm и на Общероссийском математическом портале www.mathnet.ru. На сайте журнала можно найти также правила подготовки рукописей статей для публикации в журнале.

Тематика публикаций журнала:

- *Теоретические основы прикладной дискретной математики*
- *Математические методы криптографии*
- *Математические методы стеганографии*
- *Математические основы компьютерной безопасности*
- *Математические основы надёжности вычислительных и управляющих систем*
- *Прикладная теория кодирования*
- *Прикладная теория автоматов*
- *Прикладная теория графов*
- *Логическое проектирование дискретных автоматов*
- *Математические основы информатики и программирования*
- *Вычислительные методы в дискретной математике*
- *Дискретные модели реальных процессов*
- *Математические основы интеллектуальных систем*
- *Исторические очерки по дискретной математике и её приложениям*