Министерство образования и науки Российской Федерации
ФГБОУ ВО «Ивановский государственный университет»

АЛГЕБРА И ТЕОРИЯ АЛГОРИТМОВ

Всероссийская конференция, посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

Иваново, 21 — 24 марта 2018 года

Сборник материалов

Иваново
Издательство «Ивановский государственный университет»
2018

УДК 51
ББК 22.1
А 45

Алгебра и теория алгоритмов [Электронный ресурс] : Всероссийская конференция, посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета : сборник материалов. — Электрон. дан. — Иваново : Иван. гос. ун-т, 2018. — 1 электрон. опт. диск (DVD-ROM) ; 12 см. — Систем. требования: программа чтения файлов в формате PDF 1.4. — ISBN 978-5-7807-1250-3.

В сборнике представлены тезисы докладов участников Всероссийской конференции, посвященной 100-летию факультета математики и компьютерных наук Ивановского государственного университета, прошедшей в ИвГУ 21 — 24 марта 2018 года.

Предназначено ученым, преподавателям, аспирантам и студентам старших курсов, интересующимся данной проблематикой.

Печатается по решению редакционно-издательского совета Ивановского государственного университета

Конференция проведена при финансовой поддержке Российского фонда фундаментальных исследований. Проект № 18-01-20009.

ISBN 978-5-7807-1250-3

СОДЕРЖАНИЕ

Пленарные доклады

Секция 1. Теория групп

Секция 2. Теория колец

Секция 3. Полугруппы и универсальные алгебры

Секция 4. Математическая логика и теория алгоритмов

Секция 5. Прикладная алгебра, дискретная математика и криптография

МАТЕМАТИКА И МАТЕМАТИКИ В ИВАНОВСКОМ ГОСУДАРСТВЕННОМ УНИВЕРСИТЕТЕ: 100-ЛЕТНИЙ ЮБИЛЕЙ

Б. Я. Солон,
декан факультета математики и компьютерных наук

В России первые классические университеты были основаны в XVIII веке. Именовались они императорскими: Императорский Московский университет, Императорский Харьковский университет, Императорский Казанский университет. Сегодня многие из таких учебных заведений находятся на территории других государств: Литвы, Эстонии, Украины, Финляндии и Польши. В России же действуют пять в прошлом императорских университетов — это старейшие учебные заведения страны: **Санкт-Петербургский государственный университет**, **Московский государственный университет**, образованный в 1755 году, **Казанский (Приволжский) федеральный университет**, основанный в 1804 году, **Томский государственный университет**, открытие которого состоялось в 1888 году и **Саратовский государственный университет имени Н. Г. Чернышевского**, учрежденный в 1907 году.

Нашему университету исполняется 100 лет, что вполне сопоставимо с возрастом старейших университетов России. Конечно, в момент образования он не считался университетом — это был учительский институт, который замышлялся как высшее учебное заведение, готовившее учителей для школ, училищ и техникумов. Но и место, где возник наш университет — далеко не столица. Иваново-Вознесенск в начале 20-го века — заштатный город Шуйского уезда Владимирской губернии. Необходимо учитывать также, что до 1914 года в Иваново-Вознесенске не было ни одного высшего учебного заведения и всего две гимназии. Надо сказать, что он сыграл эту роль в полной мере: большинство учителей в Ивановской области, в том числе и по математике, — выпускники нашего университета.

Хотелось бы отметить одну очень важную особенность нашего университета, состоящую в его ярко выраженной классической системе подготовки специалистов. Прежде всего, это относится к факультету математики и компьютерных наук. В момент образования университета было всего два факультета — физико-математический и исторический. Благодаря московским математикам во главе с Н. Н. Лузиным, приехавшим в Иваново-Вознесенск для создания заведений высшего образования, на стадии зарождения был внесен ген фундаментальной математики, который передавался из поколения в поколение преподавателей и профессоров математического факультета. Именно приверженность к классической университетской системе образование дала вектор развития факультета, его известности в математических кругах и позволила его коллективу достичь значительных вершин в научной деятельности.

Итак, усилия организаторов университета 100-летней давности привели к появлению, пусть не сразу, классического университета. Сравнение с другими классическими университетами показывает, что наш университет можно отнести к числу старейших в России. К сожалению, классическое образование не востребовано в настоящее время, но в истории факультета были периоды, когда число студентов превосходило 1000 человек. Будем надеяться, что такие времена вновь настанут, а факультет готов предоставить студентам математические знания так, как это делается в лучших университетах мира.

Вся история факультета тесно переплетена с историей нашего государства и ивановской области. Сам факт образования Ивановской области и Ивановского госуниверситета

был вызван революциями 1917-го года. Энергия первого губернатора — М. В. Фрунзе — позволила сконцентрировать в Иваново-Вознесенске крупные научные силы из Москвы. В те годы Москва голодала, а Иваново-Вознесенск, расположенный в 300 верстах от столицы, был в относительном благополучии. Кроме того, для приглашенных ученых были созданы особые условия. Курсировал между Москвой и Иваново-Вознесенском так называемый «профессорский вагон» — спальный вагон высшего класса, где можно было даже жить продолжительное время. В городе был выделен специальный дом, а впоследствии построен «профессорский дом» на ул. Калинина, где до сих пор живут семьи ивановских профессоров. Приглашенные профессора были обеспечены дополнительными продовольственными пайками, что было в то время самым злободневным на повестке дня.

Конечно, повезло в том, что в Иваново приехали такие крупные математики, как Н. Н. Лузин (академик с 1929 г.), А. Я. Хинчин (член-корреспондент АН СССР с 1939 г.), Д. Е. Меньшов (член-корреспондент АН СССР с 1953 г, А. И. Некрасов (впоследствии академик, заслуженный деятель науки и техники РСФСР). Вместе с Н. Н. Лузиным переехала в Иваново-Вознесенск большая группа молодых московских математиков, в основном его учеников: В. С. Федоров, В. Н. Вениаминов, Н. В. Четверухин, В. Н. Депутатов. Через 4 года многие из них вернулись в Москву, но остался профессор Владимир Семенович Федоров, который сыграл выдающуюся роль в развитии факультета.

Именно он в 1932 году пригласил на работу в качестве ассистента кафедры математики А. И. Мальцева, который в то время работал в Ивановском энергетическом институте, куда был направлен после окончания МГУ в 1931 году. Без отрыва от основной работы в ИГПИ, А. И. Мальцев учился в аспирантуре с 1934 года по 1937 год в НИИМ МГУ. В 1935–36 годы заведующий кафедрой математики В. С. Федоров пригласил на свою кафедру выпускников аспирантуры МГУ Андрея Владимировича Лотоцкого, Ю. В. Руднева и Сергея Васильевича Смирнова, которые, как оказалось, сыграли огромную роль в формировании математической жизни в Иванове.

Важно отметить, что относительно близкое расположение Иванова от Москвы, а также серьезные математические традиции, заложенные предшественниками, способствовали притоку молодых математиков на наш факультет. Кроме того, в истории страны был период, когда лица, подвергшиеся репрессиям, не могли жить в Москве и ряде других городов. Иваново не входило в этот список запрещенных городов, это позволило принять на работу таких известных математиков как профессор Дмитрий Дмитриевич Мордухáй-Болтовскóй, профессор Вадим Арсеньевич Ефремович, профессор Владимир Абрамович Рохлин, профессор Алексей Всеволодович Гладкий (Шуйский филиал). Нескольким нашим преподавателям из-за войны пришлось получать высшее образование и проходить аспирантуру на нашем факультете несмотря на то, что они начинали учиться в других университетах, в том числе в МГУ. Позже они составили славу нашему факультету, это — Анатолий Иванович Черемисин и Евгений Петрович Барановский.

Отмечу еще один забавный факт, напрямую повлиявший на математическую жизнь факультета. Как известно, Иваново — город невест. Из Иванова и была Елена Ивановна, которая в 1957 году участвовала во Всемирном фестивале молодежи и студентов в Москве, и где познакомилась с молодым американцем Мартином Гриндлингером. В 1958 г. в г. Москве он вступил в брак с Еленой Ивановной. В 1959 году переехал в СССР и принял советское гражданство в 1961 году. С 21 декабря 1960 года по 1967 год он работал в Ивановском педагогическом институте сначала ассистентом, затем старшим преподавателем, доцентом кафедры высшей алгебры. С 1 сентября 1965 г. по 1 августа 1966 г. находился на должности старшего научного сотрудника для завершения докторской диссертации по теме «Решение алгоритмических проблем для некоторого класса групп», которую он защитил в ноябре 1966 г. Решением ВАК от 20 мая 1967 г. ему присуждена ученая степень доктора физико-математических наук.

Крупные математики обычно создают свои математические школы, которые становятся центром притяжения молодых людей — студентов, аспирантов, мечтающих посвятить свою жизнь математике. Именно это случилось на нашем факультете.

Благодаря научной и педагогической деятельности академика Анатолия Ивановича Мальцева к 1951 году стала складываться Ивановская алгебраическая школа или просто «Ивановская школа Мальцева». В период с 1950-го по 1960 годы к этой школе следует отнести А. А. Виноградова, А. Т. Гайнова, М. И. Зайцеву, Д. А. Захарова, Л. Я. Куликова, Н. Н. Мягкову (Соколову), В. А. Емеличева, Д. М. Смирнова, А. Д. Тайманова, М. А. Тайцлина, Е. А. Халезова. В этот период были студентами Д. И. Молдаванский, Е. А. Поляков, А. И. Черемисин и И. А. Лавров, они рано начали свою научную деятельность и сложились как математики в алгебраической школе Мальцева. После отъезда А. И. Мальцева и группы математиков в Новосибирск, школа Мальцева не только не перестала существовать, но набрала новые обороты. Яркими лидерами стали Давид Ионович Молдаванский и Евгений Александрович Поляков. Их многочисленные ученики защитили кандидатские диссертации, а Д. Н. Азаров и Б. Я. Солон — докторские диссертации. Созрев в рамках школы Мальцева, работают в США и Израиле Л. М. Шнеерсон, С. Д. Бродский и М. Г. Розинас. В наше время ведущими математиками и лидерами научной школы стали научные внуки и правнуки Мальцева — Е. В. Соколов, Е. К. Логинов.

К 1949–57 годам относится формирование школы равномерной топологии профессора В. А. Ефремовича. В Иванове были написаны его основополагающие работы в этой области, здесь же ему удалось среди студентов найти талантливых учеников, среди которых самым талантливым был А. С. Шварц. Из его учеников этого периода следует упомянуть также москвича Ю. М. Смирнова, ивановцев Е. С. Тихомирова, Р. Н. Федорова. В период 1949 — 1957 годы В. А. Ефремович руководил семинаром по равномерной топологии.

Первые работы Евгения Петровича Барановского, написанные в 1959 — 1960 годах и вышедшие в 1963 году, посвящены именно этой тематике. Однако Евгения Петровича увлекла чисто геометрическая тема о наиболее экономных покрытиях евклидовых пространств равными шарами. В 1966 году Е. П. Барановский сделал доклад на Московском международном конгрессе математиков о наиболее экономном покрытии четырехмерного евклидова пространства равными шарами, причем дал исчерпывающее решение этой трудной проблемы. Выступление Е. П. Барановского получило очень высокую оценку от ведущих специалистов в области геометрии и теории чисел, таких как Г. Коксетер и Г. Дэвенпорт.

Е. П. Барановский воспитал талантливых учеников, среди них Наталья Владимировна Новикова, Евгений Викторович Власов и Павел Геннадиевич Кононенко. Все они защитили кандидатские диссертации, получили и продолжают получать в ней достаточно весомые новые результаты.

В 1957–59 годах профессор Сергей Васильевич Смирнов решил ряд фундаментальных задач о представлении функций многих переменных номографируемыми суперпозициями в классе функций достаточной гладкости. Тогда же С. В. Смирновым и его учениками М. К. Потаповым, Е. Т. Сморкачевым, Г. А. Горевой было получено несколько важных результатов по аппроксимации функций многих переменных при помощи номографируемых суперпозиций. Научные связи этой группы в значительной степени осуществлялись с МГУ и ИВМ АН СССР. Её деятельность долгое время направлялась академиком А. Н. Колмогоровым. Работы С. В. Смирнова и его учеников позволили впоследствии говорить на республиканском уровне о появлении научной номографической школы в Иванове.

В 1970-е годы на факультете была организована серия конференций по номографии. В 1971 году номография была представлена в секции вычислительной математики в составе межвузовской конференции по алгебре, логике и вычислительной математике. Вторично номографы собрались на 1 межвузовском семинаре в 1973 году. Это было признанием заслуг школы ивановских математиков, возглавляемой профессором нашего университета С. В. Смирновым.

Третий раз ведущие номографы страны собрались в г. Иваново с 4 по 6 июня на математическом факультете в аудитории академика А. И. Мальцева, где работал II межвузовский семинар по современным проблемам номографии, организованный Ивановским университетом совместно с отделом номографии Вычислительного центра АН СССР и кафедрой геометрии и топологии МГУ.

В работе семинара были представлены университеты, пединституты, вузы, научно-исследовательские институты и проектные организации 13 городов страны: Москвы, Ленинграда, Минска, Риги, Душанбе, Иванова и др. Преподаватели факультета, кроме прямой работы со студентами, проводили огромное количество организационных, профориентационных, просветительских мероприятий, направленных на повышение уровня математического образования среди школьников и студентов.

В 1959 году по инициативе С. В. Смирнова при Ивановском пединституте была создана одна из первых в стране юношеских математических школ. Многие годы он был ее бессменным руководителем и ведущим преподавателем. Выпускники этой школы, как правило, становились впоследствии самостоятельными работниками в области математики и смежных с ней наук. Сергей Васильевич систематически вел занятия в школах с математическим уклоном, читал лекции для учителей г. Иванова и Ивановской области.

Начиная с 1953 года, ежегодно проводились олимпиады школьников по математике. В разные годы победителями и призерами математических олимпиад становились впоследствии крупные математики, организаторы образования и государственные деятели. В 1962 году на математических олимпиадах блистал Г. Б. Клейнер — будущий член-корр. РАН, известный экономист. Среди призеров городской математической олимпиады в 1974 году был Б. И. Минц — будущий российский предприниматель, общественный деятель и меценат. В начале 70-х годов победителем двух областных и республиканской математических олимпиад был ректор Ивановского университета В. Н. Егоров.

В июле 1968 года на базе спортивного лагеря на Рубском озере впервые была проведена межобластная школа-семинар юных математиков, которой руководил академик А. Н. Колмогоров. Занятия в летней физико-математической школе проходили с 10 июля по 2 августа 1968 года. Все это время А. Н. Колмогоров безвыездно находился в лагере. Каждый день было по 5–6 часов занятий, по субботам — олимпиада, а в воскресенье — разбор задач. Основными лекторами школы были А. Н. Колмогоров и С. В. Смирнов, занятия проводили аспиранты МГУ И. Г. Журбенко, МФТИ В. Вен и В. Куликов, преподаватели ИвГУ Г. В. Пухова и Т. П. Иванова, а также студенты Н. Полякова (ныне Н. С. Корникова), Л. Шнеерсон, Б. Солон, Е. Крюков, А. Сидоров и др.

Факультет математики и компьютерных сегодня — это органичный сплав теоретической математики и ее приложений в различных сферах социальной, образовательной и экономической деятельности. В состав факультета входят три кафедры: алгебры и математической логики, прикладной математики и компьютерных наук, математического анализа и геометрии. Преподавателями факультета проводятся научные исследования по ряду как традиционных, так и относительно новых направлений теоретической и прикладной математики. Факультет поддерживает контакты с ведущими научными центрами страны — Московским, Санкт-Петербургским, Новосибирским и Уральским университетами, Математическим институтом им. В. А. Стеклова РАН, Вычислительным центром РАН, Институтом математики Сибирского отделения РАН. Более 80% преподавателей имеют ученую степень кандидата или доктора наук.

Профессорско-преподавательский состав факультета состоит из высококвалифицированных специалистов в различных областях математики. Блок алгебраических и логических дисциплин ведут доктора ф.-м. наук Д. Н. Азаров, Е. К. Логинов, Б. Я. Солон, а также ряд молодых доцентов Е. А. Туманова, А. В. Розов и др. Блок аналитических дисциплин находится в надежных руках доктора ф.-м. наук А. С. Белова и опытных преподавателей, доцентов Н. Г. Косарев, П. Г. Кононенко, Н. В. Новикова и др. Компьютерные науки представляют доценты Е. В. Соколов, С. И. Хашин, Ю. А. Хашина и др. На факультете работают опытные методисты, руководители педагогической практики — доценты Е. В. Ерёмина, М. А. Артамонов, Т. Я. Сенкевич.

На факультете традиционно проводятся математические конференции, посвященные юбилейным датам крупных математиков, работавших и работающим на нашем факультете. Несколько конференций, посвященных Анатолию Ивановичу Мальцеву, было проведено в 1989 году («Мальцевские чтения, посвященные 80-летию со дня рождения»), в 1999 году,

в 2009 году. Среди участников этих конференций неизменно присутствовали члены семьи Анатолия Ивановича, его коллеги из Новосибирска, крупные математики из различных вузов России.

В 2011 году была проведена научная конференция «Математические чтения, посвященные 100-летию со дня рождения профессора С. В. Смирнова», которая завершила серию конференций «Смирновские чтения», проведенных в 1981 и 1991 годах.

Каждая конференция, кроме научного значения, позволяла осветить новые грани личности Сергея Васильевича, оценить его громадный вклад в организацию и улучшение математического образования в России.

Последняя из этих конференций завершилась изданием юбилейного сборника, в который были включены разнообразные материалы от «Жизненных вех» С. В. Смирнова, до материалов его архива, его историко-математических исследований и поэтического творчества.

С 2 по 5 декабря 2015 года на факультете математики и компьютерных наук проходила международная научная конференция «Алгоритмические проблемы в алгебре и теории вычислимости», посвященная 75-летию д. ф.-м. н., профессора Давида Ионовича Молдаванского, более 50 лет проработавшего на кафедре алгебры нашего университета. Среди участников конференции были ведущие математики из Москвы, Ярославля, Новосибирска и Тулы. В качестве членов оргкомитета в работе конференции приняли участие математики из США А. Ю. Ольшанский, Vanderbilt University, P. E. Schupp, University of Illinois at Urbana–Champaign и Лев Шнеерсон, City University of NY.

Славная история факультета дает надежду на то, что появятся новые математические школы, в которых вырастут новые ученые и педагоги, а факультет достигнет новых вершин в будущем.

Литература

1. *Балдин К. Е.* Ивановский государственный университет, 1918 — 2003: Очерки истории. Иваново: Иван. гос. ун-т, 2004. 588 с., ил.
2. *Безверхний В. Н., Добрынина И. В., Трубицын Ю. Э., Устян А. Е.* М. Д. Гриндлингер — основатель тульской алгебраической школы (К 85-летию профессора) // Чебышевский сборник. 2017. Т. 18, вып. 1. С. 160—166.
3. Владимир Семёнович Фёдоров (К сорокалетию научно-педагогической деятельности) // Успехи математических наук. 1955. Т. 10, № 4. С. 193—196.
4. История факультета математики и компьютерных наук : сайт. URL: http://math.ivanovo.ac.ru/hist/index.html (дата обращения: 13.03.2018).
5. *Колмогоров А. Н., Журбенко И. Г., Пухова Г. В.* Летняя школа на Рубском озере. Из опыта работы летней физико-математической школы. м. : Просвещение, 1971. 160 с.
6. Математик, педагог, поэт: к 100-летию со дня рождения профессора С. В. Смирнова: сб. ст. Иваново: Иван. гос. ун-т, 2011. 128 с.
7. *Молдаванский Д. И.* 40 лет научной логико-алгебраической школе ИвГУ: итоги и перспективы // Вестник Ивановского государственного университета. Сер.: Естественные, общественные науки. 2014. Вып. 2. С. 75—80.

ПЛЕНАРНЫЕ ДОКЛАДЫ

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ALGORITHMIC PROBLEMS FOR GELFAND–DORFMAN–NOVIKOV ALGEBRAS[1]

L. A. Bokut (Guangzhou, China; Novosibirsk, Russia)[2], Yuqun Chen (Guangzhou, China)[3], Zerui Zhang (Guangzhou, China)[4]

Gelfand–Dorfman–Novikov algebras (also known as Novikov algebras) were introduced by Gelfand and Dorfman [4], in connection with Hamiltonian operators in the formal calculus of variations and Balinskii and Novikov [1], in connection with linear Poisson brackets of hydrodynamic type.

We establish Gröbner–Shirshov bases theory for Gelfand–Dorfman–Novikov algebras over a field of characteristic 0. As applications, a PBW type theorem in Shirshov form is given and we provide an algorithm for solving the word problem of Gelfand–Dorfman–Novikov algebras with finite homogeneous relations. We also construct a subalgebra of one generated free Gelfand–Dorfman–Novikov algebra which is not free [2].

In 1997, Xiaoping Xu [5, 6] invented a concept of Novikov–Poisson algebras (we call them Gelfand–Dorfman–Novikov–Poisson (GDN-Poisson) algebras). We construct a linear basis of a free GDN-Poisson algebra. We define a notion of a special GDN-Poisson admissible algebra, based on Xiaoping Xu's definition and an S.I. Gelfand's observation (see [4]). It is a differential algebra with two commutative associative products and some extra identities. We prove that any GDN-Poisson algebra is embeddable into its universal enveloping special GDN-Poisson admissible algebra. Also we prove that any GDN-Poisson algebra with the identity $x \circ (y \cdot z) = (x \circ y) \cdot z + (x \circ z) \cdot y$ is isomorphic to a commutative associative differential algebra [3].

Литература

1. *Balinskii A. A., Novikov S. P.* Poisson brackets of hydrodynamics type. Frobenius algebras and Lie algebras (Russian) // Dokl. Akad. Nauk SSSR. 1985. Vol. 283, № 5. P. 1036—1039.
2. *Bokut L. A., Chen Yuqun, Zhang Zerui.* Gröbner–Shirshov bases method for Gelfand–Dorfman–Novikov algebras // Journal of Algebra and Its Applications. 2017. Vol. 16, № 1. 1750001 (22 pages). https://doi.org/10.1142/S0219498817500013.
3. *Bokut L. A., Chen Yuqun, Zhang Zerui.* On free Gelfand-Dorfman-Novikov-Poisson algebras and a PBW theorem // J. Algebra. 2018. Vol. 500. P. 153—170. http://dx.doi.org/10.1016/j.jalgebra.2016.12.006.
4. *Gelfand I. M., Dorfman I. Ya.* Hamiltonian operators and algebraic structures related to them // Funktsional. Anal. i Prilozhen. 1979. Vol. 13, № 4. P. 13—30.
5. *Xiaoping Xu.* Novikov–Poisson algebras // J. Algebra. 1997. Vol. 190, № 2. P. 253—279. https://doi.org/10.1006/jabr.1996.6911.
6. *Xiaoping Xu.* On simple Novikov algebras and their irreducible modules // J. Algebra. 1996. Vol. 185, № 3. P. 905—934. https://doi.org/10.1006/jabr.1996.0356.

 Получено 06.12.2017. УДК 512.5.

[1]The research was supported by Russian Science Foundation (Project 14-21-00065) and the NNSF of China (11171118, 11571121) and the Program on International Cooperation and Innovation, Department of Education, Guangdong Province (2012gjhz0007).

[2]South China Normal University; Sobolev Institute of Mathematics; Novosibirsk State University.
E-mail: bokut@math.nsc.ru.

[3]South China Normal University.

[4]South China Normal University.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О КОНЕЧНЫХ ГОМОМОРФНЫХ ОБРАЗАХ ГРУПП КОНЕЧНОГО РАНГА

Д. Н. Азаров (Иваново)[1]

Напомним, что группа имеет конечный ранг, если существует число r такое, что любая конечно порожденная подгруппа этой группы порождается не более чем r элементами. Примером группы конечного ранга может служить любая полициклическая группа.

Б. Верфриц в своей статье «Remarks on Azarov's work on soluble groups of finite rank» [3] назвал интересным следующий результат, принадлежащий автору настоящего доклада и опубликованный в работе [1].

Теорема 1. *Если разрешимая группа конечного ранга аппроксимируема конечными π-группами для некоторого конечного множества π простых чисел, то она содержит подгруппу конечного индекса, аппроксимируемую конечными нильпотентными π-группами.*

Удалось существенно усилить эту теорему следующим образом.

Теорема 2. *Пусть π — конечное множество простых чисел. В каждой разрешимой группе конечного ранга существует подгруппа конечного индекса, любой конечный гомоморфный π-образ которой нильпотентен.*

Остается неясным, верна ли эта теорема для произвольных групп конечного ранга, т. е. можно ли в ней отказаться от условия разрешимости. Тем не менее, удалось получить следующий аналог теоремы 2 для конечно порожденных групп конечного ранга.

Теорема 3. *Пусть π — конечное множество простых чисел. В каждой конечно порожденной группе конечного ранга существует подгруппа конечного индекса, любой конечный гомоморфный π-образ которой нильпотентен.*

С другой стороны, имеет место следующая хорошо известная теорема Д. Робинсона.

Теорема 4. *Если полициклическая группа не является нильпотентной, то некоторый ее конечный гомоморфный образ не нильпотентен.*

На самом деле Д. Робинсон доказал это утверждение не только для полициклических групп, но и для некоторых других разрешимых групп конечного ранга (см. [2, п. 5.3.12]).

Вернемся теперь к теоремам 2 и 3. Они показывают, что среди конечных гомоморфных образов групп конечного ранга существует достаточно много нильпотентных групп. Это свидетельствует о значимости упомянутого выше результата Робинсона.

Теоремы 2 и 3 дают следующую информацию о семействе всех конечных гомоморфных π-образов для фиксированной разрешимой (или конечно порожденной) группы конечного ранга, где π — конечное множество простых чисел: в группах этого семейства подгруппы Фиттинга имеют ограниченные индексы. Напомним, что подгруппой Фиттинга данной группы называется ее наибольшая нормальная нильпотентная подгруппа.

Литература

1. *Азаров Д. Н.* Некоторые аппроксимационные свойства разрешимых групп конечного ранга // Чебышевский сборник. 2014. Т. 15, вып. 1. С. 7—18.
2. *Lennox J., Robinson D.* The theory of infinite soluble groups. Oxford : Clarendon press, 2004.
3. *Wehrfritz B. A. F.* Remarks on Azarov's work on soluble groups of finite rank // Boll. Unione Mat. Ital. 2016. Vol. 9. P. 319—322. doi:10.1007/s40574-015-0047-8.

 Получено 09.01.2018. УДК 512.543.

[1]Ивановский государственный университет. E-mail: azarovdn@mail.ru.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ВЫЧИСЛИМОСТЬ НА ДЕЙСТВИТЕЛЬНЫХ ЧИСЛАХ

М. М. Арсланов (Казань)[1]

Действительное число называется вычислимо аппроксимируемым, если оно является пределом вычислимой последовательности рациональных чисел. Сложность аппроксимации таких чисел может быть оценена с помощью скорости сближения к ним вычислимых последовательностей. Главной мерой такой сложности является сводимость по Соловею: α вычисляется проще, чем β, если существует эффективная процедура, которая по рациональной аппроксимации X для β порождает рациональную аппроксимацию Y для α, сходящуюся к α по крайней мере с той же скоростью, что и X к β. В докладе будут рассмотрены эта, а также другие варианты сложности аппроксимации действительных чисел, которые определяются наложением разного рода ограничений на понятие «скорость аппроксимации».

 Получено 25.01.2018. УДК 510.5.

[1]Казанский федеральный университет. E-mail: Marat.Arslanov@kpfu.ru.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ПОЛИНОМИАЛЬНО ПОЛНЫЕ КВАЗИГРУППЫ И ИХ ПРИЛОЖЕНИЯ

В. А. Артамонов (Москва)[1]

Квазигруппой называется множество Q с бинарной операцией умножения xy, причем для любых $a, b \in Q$ уравнения $ax = b$, $ya = b$ имеют единственное решение $x = a\backslash b$, $y = b/a$. Квазигруппы составляют многообразие алгебр с тремя операциями xy, $x\backslash y$, x/y и с тождествами $(xy)/y = x = (x/y)y$, $x\backslash(xy) = y = x(x\backslash y)$.

В работе рассматриваются конечные квазигруппы. Они играют важную роль в построении систем защиты и передачи информации [1, 2, 3]. Для этой цели наиболее применимы полиномиально полные квазигруппы Q, в которых каждая операция получается из основных трех операций путем суперпозиций, присоединения всех констант и операций проекций $p_{in}(x_1, \ldots, x_n) = x_i$, $1 \leqslant i \leqslant n$. Кроме того, важно требовать, чтобы в Q не было бы собственных подквазигрупп.

Квазигруппа Q аффинна (или T-квазигруппа), если в Q существует структура аддитивной абелевой группы $(Q, +)$, причем умножение xy имеет вид $xy = \alpha(x) + \beta(y) + c$, где α, β — автоморфизмы $(Q, +)$, и $c \in Q$.

Известно, что конечная квазигруппа полиномиально полна тогда и только тогда, когда она проста и не аффинна.

Каждая конечная квазигруппа Q порядка n задается своим латинским квадратом (таблицей Кэли) размера n. Он обладает тем свойством, что его строки $\sigma_1, \ldots, \sigma_n$ и столбцы $\tau_1, \ldots, \tau_n$ являются перестановками элементов квазигруппы Q. Обозначим через $G(Q)$ подгруппу в группе S_Q перестановок Q, порождаемую всеми перестановками $\sigma_i\sigma_j^{-1}$, $\tau_i\tau_j^{-1}$, $i, j = 1, \ldots, n$. Показывается, что при изотопии группа $G(Q)$ переходит в сопряженную.

Теорема 1. *Если $G(Q)$ действует дважды транзитивно в Q, то квазигруппа Q полиномиально полна. Свойство дважды транзитивности сохраняется при переходе к изотопу.*

Теорема 2 [4]**.** *Любая конечная квазигруппа порядка не менее 3 изотопна квазигруппе, в которой нет собственных подквазигрупп.*

Пусть заданы две конечные квазигруппы K, Q. Строятся отображения

$$\Phi, \Lambda, \Gamma : K \to S_Q,\ \Psi, \Omega, \Theta : Q \to S_K, \tag{1}$$

и на $K \times Q$ вводится умножение

$$(a, \alpha) * (b, \beta) = \left(\Psi_\alpha\left(\Omega_\alpha(a)\Theta_\alpha(b)\right),\ \Phi_b\left(\Lambda_b(\alpha)\Gamma_b(\beta)\right)\right). \tag{2}$$

Показывается, что получается квазигруппа $K \bowtie Q$.

Теорема 3. *Пусть группы $G(K), G(Q)$ действуют дважды транзитивно на R, Q, причем $|K| < (|Q| - 1)!$, $|Q| < (|K| - 1)!$. Тогда существуют такие отображения из (1), что $G(K \bowtie Q)$ действует дважды транзитивно в $K \times Q$.*

Эта теорема позволяет строить полиномиально полные квазигруппы порядка 8^M для любого M, в частности, полиномиально полные квазигруппы порядка 512. Применяя изотопию из [4], получаем полиномиально полную квазигруппу без собственных подквазигрупп.

 Получено 29.12.2017. УДК 512.573.

[1]Московский государственный университет им. М. В. Ломоносова. E-mail: artamon@mech.math.msu.su.

Литература

1. *Artamonov V. A., Chakrabarti S., Pal S. K.* Characterization of Polynomially Complete Quasigroups based on Latin Squares for Cryptographic Transformations // J. Discrete Applied Mathematics. 2016. Vol. 200. P. 5—17.
2. *Artamonov V. A., Chakrabarti S., Pal S. K.* Characterizations of highly non-associative quasigroups and associative triples // Quasigroups and Related Systems. 2017. Vol. 25. P. 1—19.
3. *Glukhov M. M.* On applications of quasigroups in cryptography // Appl. Discrete Math. 2008. Vol. 2. P. 28—32.
4. *Kepka T.* A note on simple quasigroups // Acta Univ. Carolin. Math. Phys. 1978. Vol. 19, № 2. P. 59—60.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ГРУППА ВИРТУАЛЬНЫХ КОС И ГОМОТОПИЧЕСКИЕ ГРУППЫ 2-МЕРНОЙ СФЕРЫ[1]

В. Г. Бардаков (Новосибирск)[2]

Группа виртуальных кос введена Л. Кауффманом [5] для изучения виртуальных узлов, так же как классическая группа кос B_n была введена для изучения классических узлов. Группа виртуальных кос VB_n, $n \geq 2$, порождается элементами

$$\sigma_1,\ \sigma_2,\ \ldots,\ \sigma_{n-1},\ \rho_1,\ \rho_2,\ \ldots,\ \rho_{n-1},$$

где $\sigma_1,\ \sigma_2,\ \ldots,\ \sigma_{n-1}$ — порождающие группы кос B_n, а элементы $\rho_1,\ \rho_2,\ \ldots,\ \rho_{n-1}$ порождают группу подстановок S_n, т. е. VB_n определяется соотношениями групп B_n и S_n, а также смешанными соотношениями:

$$\sigma_i\rho_j = \rho_j\sigma_i, \quad |i-j| > 1,$$
$$\rho_i\rho_{i+1}\sigma_i = \sigma_{i+1}\rho_i\rho_{i+1}.$$

Существует канонический эпиморфизм $VB_n \to S_n$, ядро которого называется *группой виртуальных крашеных кос* и обозначается символом VP_n. Определим следующие элементы в VP_n:

$$\lambda_{i,i+1} = \rho_i\,\sigma_i^{-1}, \quad \lambda_{i+1,i} = \rho_i\,\lambda_{i,i+1}\,\rho_i = \sigma_i^{-1}\,\rho_i, \quad i = 1, 2, \ldots, n-1,$$
$$\lambda_{ij} = \rho_{j-1}\,\rho_{j-2}\ldots\rho_{i+1}\,\lambda_{i,i+1}\,\rho_{i+1}\ldots\rho_{j-2}\,\rho_{j-1},$$
$$\lambda_{ji} = \rho_{j-1}\,\rho_{j-2}\ldots\rho_{i+1}\,\lambda_{i+1,i}\,\rho_{i+1}\ldots\rho_{j-2}\,\rho_{j-1}, \quad 1 \leq i < j-1 \leq n-1.$$

Известно [1], что VP_n порождается элементами $\lambda_{ij},\ 1 \leq i \neq j \leq n$, и определяется соотношениями:

$$\lambda_{ij}\lambda_{kl} = \lambda_{kl}\lambda_{ij}, \tag{1}$$
$$\lambda_{ki}\lambda_{kj}\lambda_{ij} = \lambda_{ij}\lambda_{kj}\lambda_{ki}, \tag{2}$$

где различные буквы обозначают различные индексы. Группа VP_n разлагается в полупрямое произведение [1]:

$$VP_n = V^*_{n-1} \rtimes VP_{n-1}, \quad n \geq 2, \tag{3}$$

где V^*_{n-1} подгруппа VP_n, $V^*_1 = VP_2 \cong F_2$, VP_1 — тривиальная группа.

Напомним также определение симплициальной группы (см., например, [3]). Последовательность множеств $\mathcal{X} = \{X_n\}_{n\geq 0}$ называется *симплициальным множеством*, если существуют отображения граней:

$$d_i : X_n \longrightarrow X_{n-1} \text{ при } 0 \leq i \leq n$$

и отображения вырождения

$$s_i : X_n \longrightarrow X_{n+1} \text{ при } 0 \leq i \leq n.$$

Эти отображения удовлетворяют симплициальным соотношениям:

(1) $d_id_j = d_{j-1}d_i$ при $i < j$,
(2) $s_is_j = s_{j+1}s_i$ при $i \leq j$,
(3) $d_is_j = s_{j-1}d_i$ при $i < j$,
(4) $d_js_j = id = d_{j+1}s_j$,

 Получено 05.01.2018. УДК 512.7.

[1]Работа выполнена при финансовой поддержке РФФИ, проекты № 16-01-00414, № 18-01-00057.

[2]Институт математики им. С. Л. Соболева СО РАН. E-mail: bardakov@math.nsc.ru.

(5) $d_i s_j = s_j d_{i-1}$ при $i > j+1$.

Симплициальная группа $\mathcal{G} = \{G_n\}_{n\geq 0}$ — это симплициальное множество $\mathcal{G}$, для которого каждое G_n является группой и каждое d_i и s_i является гомоморфизмом. *Комплексом Мура* $N\mathcal{G} = \{N_n\mathcal{G}\}_{n\geq 0}$ симплициальной группы $\mathcal{G}$ называется цепной комплекс $(N\mathcal{G}, d_0)$ с дифференциалом d_0, где

$$N_n\mathcal{G} = \bigcap_{i=1}^{n} \mathrm{Ker}(d_i : G_n \longrightarrow G_{n-1}).$$

Если $\mathcal{G}$ — симплициальная группа, то элемент из

$$\mathrm{B}_n\mathcal{G} = d_0(N_{n+1}\mathcal{G})$$

называется *граничным*, а элемент из

$$\mathrm{Z}_n\mathcal{G} = \mathrm{Ker}(d_0 : N_n\mathcal{G} \longrightarrow N_{n-1}\mathcal{G})$$

называется *циклом*; n-я гомотопическая группа $\pi_n(\mathcal{G})$ определяется равенством

$$\pi_n(\mathcal{G}) = H_n(N\mathcal{G}) = \mathrm{Z}_n\mathcal{G}/\mathrm{B}_n\mathcal{G}.$$

В настоящей работе определяется симплициальная группа

$$VP_* : \cdots \rightleftarrows VP_4 \rightleftarrows VP_3 \rightleftarrows VP_2,$$

где VP_n — группа виртуальных крашеных кос, и доказывается

Предложение. *Симплициальная группа VP_* стягиваема, т. е. $\pi_i(VP_*) = 0$ при всех $i > 0$.*

Также мы определяем симплициальную подгруппу T_* группы VP_* как минимальную симплициальную подгруппу, содержащую порождающие λ_{12} и λ_{21} свободной группы VP_2. Эта группа устроена довольно сложно. В частности, группа T_i не является конечно определенной при $i > 1$, а потому непосредственное вычисление гомотопических групп является довольно сложной задачей. С другой стороны, симплициальная группа

$$\widetilde{T}_* : \cdots \rightleftarrows \mathbb{Z}^3 * \mathbb{Z}^3 \rightleftarrows \mathbb{Z}^2 * \mathbb{Z}^2 \rightleftarrows \mathbb{Z} * \mathbb{Z},$$

является свободным произведением двух симплициальных групп и имеет тот же гомотопический тип, что и пространство петель $\Omega(K(\mathbb{Z},2) \vee K(\mathbb{Z},2))$, где пространство Эйленберга-Маклейна $K(\mathbb{Z},2) = \mathbb{C}P^\infty$. Гомотопический тип пространства $\Omega(K(\mathbb{Z},2) \vee K(\mathbb{Z},2))$ совпадает с гомотопическим типом 2-мерной сферы S^2 в размерностях $i > 1$, т. е.

$$\pi_i(\Omega(K(\mathbb{Z},2) \vee K(\mathbb{Z},2))) = \pi_i(S^2) \text{ при } i > 1 \text{ и } \pi_1(\Omega(K(\mathbb{Z},2) \vee K(\mathbb{Z},2))) = \mathbb{Z} \oplus \mathbb{Z}.$$

Основным результатом работы является

Теорема. *Справедливо равенство $\pi_i(T_*) = \pi_i(\widetilde{T}_*)$ при всех $i > 1$.*

Таким образом, мы получаем возможность описывать гомотопические группы 2-мерной сферы на языке крашеных виртуальных кос.

Для классической группы крашеных кос аналогичные результаты получены Ф. Коэном и Д. Ву [4].

В заключение сформулируем ряд открытых вопросов.

Проблема 1. *Существует ли вложение группы VB_n, $n \geq 3$, в группу автоморфизмов $\mathrm{Aut}(F_m)$ некоторой свободной группы F_m ранга m?*

Проблема 2. *Построить нормальную форму слов в группе VP_n, $n \geq 3$.*

Проблема 3. *Будет ли группа VP_n, $n \geq 4$ аппроксимироваться нильпотентными группами без кручения? При $n = 3$ это так (см. [2]).*

Работа выполнена совместно с Р. Михайловым (Санкт-Петербург) и Д. Ву (Сингапур).

Литература

1. *Bardakov V. G.* The virtual and universal braids // Fund. Math. 2004. Vol. 181. P. 1—18.
2. *Bardakov V. G., Mikhailov R., Vershinin V. V., Wu J.* On the pure virtual braid group PV_3 // Comm. Algebra. 2016. Vol. 44, № 3. P. 1350—1378.
3. *Berrick A. J., Cohen F. R., Wong Y. L., Wu J.* Configurations, braids and homotopy groups // J. Amer. Math. Soc. 2006. Vol. 19, № 2. P. 265—326.
4. *Cohen F. R., Wu J.* Artin's braid groups, free groups, and the loop space of the 2-sphere // Q. J. Math. 2011. Vol. 62. № 4. P. 891—921.
5. *Kauffman L. H.* Virtual knot theory // Eur. J. Comb. 1999. Vol. 20, № 7. P. 663—690.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ЦЕНТРАЛИЗАТОРНАЯ РАЗМЕРНОСТЬ ОБОБЩЕННЫХ ГРУПП БАУМСЛАГА–СОЛИТЕРА[1]

Ф. А. Дудкин (Новосибирск)[2]

Конечно порожденная группа G, которая действует на дереве так, что все вершинные и реберные стабилизаторы — бесконечные циклические группы, называется *обобщенной группой Баумслага–Солитера* (GBS группа). По теореме Басса–Серра всякая GBS группа является фундаментальной группой подходящего графа с метками и может быть получена с помощью последовательных операций взятия свободного произведения с объединением и HNN-расширения из бесконечных циклических групп.

Как заметил Д. Робинсон [3], GBS группы занимают центральные позиции в комбинаторной теории групп благодаря следующим свойствам: нециклические GBS группы — в точности такие конечно порожденные группы когомологической размерности 2, которые имеют соизмеримую бесконечную циклическую группу; GBS группы когерентны.

Пусть $a \in G$ нетривиальный эллиптический элемент (сопряжен с вершинным элементом) GBS группы G. Тогда всякий $g \in G$ удовлетворяет соотношению

$$g^{-1} \cdot a^r \cdot g = a^s$$

в G для подходящих целых чисел r и s, зависящих от g. Отображение

$$\Delta\colon g \to \frac{s}{r}$$

является гомоморфизмом $\Delta\colon G \to \mathbb{Q}^*$, который называется *модулярным гомоморфизмом*. Подробно свойства модулярного гомоморфизма обсуждаются, например, в [1].

Предположим, что в группе G существует строго убывающая цепочка централизаторов $C_1 \supset C_2 \supset \cdots \supset C_d$ длины d, т. е. содержащая ровно d элементов, но не существует такой цепочки длины $d+1$. Тогда *централизаторная размерность группы* G $cdim(G)$ равна d. Если такого числа d не существует, то полагают $cdim(G) = \infty$. Это понятие подробно обсуждается в [2]. Следующие теоремы полностью описывают возможные значения $cdim(G)$ для GBS групп.

Теорема 1. *Пусть G — GBS группа. Централизаторная размерность G конечна тогда и только тогда, когда либо $\Delta(G) \subseteq \{1, -1\}$, либо $G = BS(1, n)$.*

Теорема 2. *Пусть $\mathbb{A}$ редуцированный граф с метками, $\pi_1(\mathbb{A}) = G$. Если $\Delta(G) = \{1\}$, тогда $dim_c(G) \leqslant 2 \cdot |E(A)| + 1$ и $dim_c(G)$ нечётна. Для любого нечётного $3 \leqslant k \leqslant 2 \cdot n + 1$ существует такой редуцированный граф с метками $\mathbb{B}$ с n ребрами, что $dim_c(\pi_1(\mathbb{B})) = k$ и $\Delta(\pi_1(\mathbb{B})) = \{1\}$.*

Теорема 3. *Пусть $\mathbb{A}$ редуцированный граф с метками, $\pi_1(\mathbb{A}) = G$. Если $\Delta(G) = \{1, -1\}$, тогда $dim_c(G) \leqslant 2 \cdot |E(A)| + 3$ и $dim_c(G)$ нечётна. Для любого нечётного $3 \leqslant k \leqslant 2 \cdot n + 3$ существует такой редуцированный граф с метками $\mathbb{B}$ с n ребрами, что $dim_c(\pi_1(\mathbb{B})) = k$ и $\Delta(\pi_1(\mathbb{B})) = \{1, -1\}$.*

 Получено 22.12.2017. УДК 512.54

[1]Исследование выполнено за счет гранта Российского научного фонда, проект № 14-21-00065.

[2]Институт математики им. С. Л. Соболева СО РАН. E-mail: DudkinF@ngs.ru.

Литература

1. *Levitt G.* On the automorphism group of generalized Baumslag–Solitar groups // Geom. Topol. 2007. Vol. 11. P. 473—515.
2. *Myasnikov A., Shumyatsky P.* Discriminating groups and c-dimension // J. Group Theory. 2004. Vol. 7, № 1. P. 135—142.
3. *Robinson D. J. S.* Generalized Baumslag–Solitar groups: a survey of recent progress // In: Groups St Andrews 2013. Cambridge : Cambridge University Press, 2015. (London Mathematical Society Lecture Note Series. Vol. 422.) P. 457—469.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ХАРАКТЕРИЗАЦИИ ЛОКАЛЬНО КОНЕЧНЫХ ПРОСТЫХ ГРУПП В КЛАССЕ ПЕРИОДИЧЕСКИХ ГРУПП[1]

Д. В. Лыткина (Новосибирск)[2], В. Д. Мазуров (Новосибирск)[3]

Определение. Пусть $\mathfrak{M}$ — некоторое множество групп. Группа G *насыщена* группами из $\mathfrak{M}$, если любая конечная подгруппа G содержится в подгруппе, изоморфной некоторому элементу $\mathfrak{M}$.

Пусть L — простая группа лиева типа [8] и X — её лиев тип (т. е. A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4, G_2, ${}^2A_n$, ${}^2B_2$, ${}^2D_n$, ${}^3D_4$, ${}^2E_6$, ${}^2F_4$ или ${}^2G_2$). Из [1, 2, 9, 10, 11] вытекает, что локально конечная группа, насыщенная конечными простыми группами лиева типа X, изоморфна группе $X(P)$ типа X над некоторым локально конечным полем P.

Вопрос о возможности замены здесь условия локальной конечности группы на условие периодичности к настоящему времени решён для типов A_1, A_2, ${}^2A_2$, B_2, ${}^2B_2$, ${}^2G_2$ [3, 4, 5, 6, 7], в частности, для всех груп лиева ранга 1.

Цель настоящего сообщения — анонсировать решение отмеченного вопроса для следующих множеств:

$$\mathfrak{M}_1 = \{C_2(q) = S_4(q) \mid q \text{ — степень простого числа}\},$$
$$\mathfrak{M}_2 = \{G_2(q) \mid q \text{ нечётно}\},$$
$$\mathfrak{M}_3 = \{{}^3D_4(q) \mid q \text{ нечётно}\}.$$

Теорема 1. *Пусть G — периодическая группа, насыщенная группами из $\mathfrak{M}_1$. Тогда G изоморфна $S_4(P)$ для некоторого локально конечного поля P.*

Теорема 2. *Пусть G — периодическая группа, насыщенная группами из множества $\mathfrak{M}_2$. Тогда $G \simeq G_2(P)$ для подходящего локально конечного поля P нечётной характеристики.*

Теорема 3. *Пусть G — периодическая группа, насыщенная группами из множества $\mathfrak{M}_3$. Тогда $G \simeq {}_4(P)$ для подходящего локально конечного поля P нечётной характеристики.*

Литература

1. *Беляев В. В.* Локально конечные группы Шевалле // в сб. Исследования по теории групп. Свердловск : УНЦ АН СССР, 1984. С. 39—50.
2. *Боровик А. В.* Вложения конечных групп Шевалле и периодические линейные группы // Сибирский математический журнал. 1983. Т. 24, № 6. С. 26—35.
3. *Лыткина Д. В., Шлёпкин А. А.* Периодические группы, насыщенные конечными простыми группами типов U_3 и L_3 // Алгебра и логика. 2016. Т. 55, № 4. С. 441—448.
4. *Рубашкин А. Г., Филиппов К. А.* О периодических группах, насыщенных группами $L_2(p^n)$ // Сибирский математический журнал. 2005. Т. 46, № 6. С. 1388—1392.
5. *Филиппов К. А.* Группы, насыщенные конечными неабелевыми простыми группами и их расширениями : дисс. . . . канд. физ.-мат. наук. Красноярск, 2005.
6. *Филиппов К. А.* О периодических группах, насыщенных конечными простыми группами // Сибирский математический журнал. 2012. Т. 53, № 2. С. 430—438.

 Получено 02.12.2017. УДК 512.542.

[1]Работа выполнена за счёт Российского научного фонда, проект № 14-21-00065.

[2]Сибирский государственный университет телекоммуникаций и информатики. E-mail: daria.lytkin@gmail.com.

[3]Институт математики им. С. Л. Соболева СО РАН. E-mail: mazurov@math.nsc.ru.

7. *Шлёпкин А. К.* О некоторых периодических группах, насыщенных конечными простыми группами // Математические труды. 1998. Т. 1, № 1. С. 129—138.
8. *Carter R. W.* Simple groups of Lie type. London : John Wiley & Sons, 1972.
9. *Hartley B., Shute G.* Monomorphisms and direct limits of finite groups of Lie type // The Quaterly Journal of Mathematics. 1984. Vol. 35, № 1. P. 49—71.
10. *Larsen M. J., Pink R.* Finite subgroups of algebraic groups // J. Amer. Math. Soc. 2011. Vol. 24, № 4. P. 1105—1158.
11. *Thomas S.* The classification of the simple periodic linear groups // Arch. Math. 1983. Vol. 41. P. 103—116.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ТЕОРИЯ МОДЕЛЕЙ РАЗРЕШИМЫХ ГРУПП

Н. С. Романовский (Новосибирск)[1]

Группа G называется *m-жёсткой*, если в ней существует нормальный ряд

$$G = G_1 > G_2 > \ldots > G_m > G_{m+1} = 1,$$

факторы которого G_i/G_{i+1} абелевы и, рассматриваемые как (правые) $\mathbb{Z}[G/G_i]$-модули, не имеют модульного кручения. В [4] доказано, что такой ряд, если существует, определяется группой G однозначно и ступень разрешимости группы в точности равна m. Для членов этого (жёсткого) ряда вводятся обозначения $G_i = \rho_i(G)$. Жёсткими (то есть m-жёсткими для соответствующего m) будут свободные разрешимые группы. Жёсткая группа G называется *делимой*, если элементы фактора $\rho_i(G)/\rho_{i+1}(G)$ делятся на ненулевые элементы кольца $\mathbb{Z}[G/\rho_i(G)]$ или, другими словами, $\rho_i(G)/\rho_{i+1}(G)$ является векторным пространством над телом частных $Q(G/\rho_i(G))$ этого кольца. Жёсткая группа G называется *расщепляемой*, если она распадается в последовательное полупрямое произведение $A_1A_2\ldots A_m$ абелевых групп $A_i \cong \rho_i(G)/\rho_{i+1}(G)$, здесь A_i нормализует A_j при $i \leq j$. Делимая расщепляемая жёсткая группа определяется однозначно с точностью до изоморфизма мощностями α_i баз соответствующих векторных пространств A_i, она обозначается через $M(\alpha_1, \ldots, \alpha_m)$. Необходимые конструкции и факты можно найти в [2]. В [3] доказано, что любая делимая жёсткая группа расщепляется, то есть изоморфна какой-то группе $M(\alpha_1, \ldots, \alpha_m)$. Говорят, что одна m-жёсткая группа G вложена в другую H *независимо*, если любая система элементов из $\rho_i(G)/\rho_{i+1}(G)$, линейно независимая над кольцом $\mathbb{Z}[G/\rho_i(G)]$, остается линейно независимой и над кольцом $\mathbb{Z}[H/\rho_i(H)]$. В [2] установлено, что всякая m-жёсткая группа независимо вкладывается в подходящую группу $M(\alpha_1, \ldots, \alpha_m)$.

Зафиксируем счётную делимую m-жёсткую группу M, она конструктивизируема. Обозначим через $\mathfrak{T}_m$ теорию первой ступени класса делимых m-жёстких групп в стандартной сигнатуре теории групп и через $\mathfrak{T}_m(M)$ теорию класса делимых m-жёстких M-групп (содержащих M в качестве фиксированной независимой подгруппы) в сигнатуре, расширенной константами из M. Сформулируем основные результаты, часть из них получена совместно с А. Г. Мясниковым.

Теорема 1. *Теории $\mathfrak{T}_m$ и $\mathfrak{T}_m(M)$ полны и рекурсивно аксиоматизируемы, значит разрешимы и $\mathfrak{T}_m$ совпадает с элементарной теорией любой делимой m-жёсткой группы, а $\mathfrak{T}_m(M)$ — с элементарной теорией с константами из M любой делимой m-жёсткой группы, в которую M независимо вложена.*

Следствие. *Пусть $G \leqslant H$ — модели теории $\mathfrak{T}_m$ или $\mathfrak{T}_m(M)$. Тогда вложение G в H является элементарным в том только том случае, если оно независимо.*

Теорема 2. *Теории $\mathfrak{T}_m$ и $\mathfrak{T}_m(M)$ являются ω-стабильными.*

Отметим, что если группа $M(\alpha_1, \ldots, \alpha_m)$ несчётна, то её мощность совпадает с максимальным α_i. Напомним также [4], что для m-жёсткой группы G определяется размерность $d(G) = (d_1(G), \ldots, d_m(G))$, состоящая из m-ки кардинальных чисел, где $d_i(G)$ обозначает ранг модуля $\rho_i(G)/\rho_{i+1}(G)$, то есть мощность (любой) максимальной линейно независимой над кольцом $\mathbb{Z}[G/\rho_i(G)]$ системы элементов этого модуля. В случае, когда m-жёсткая группа G независимо вложена в m-жёсткую группу H, имеют место неравенства $d_i(G) \leqslant d_i(H)$ для всех индексов, и мы можем говорить о коразмерности H над G, она также представля-

 Получено 04.02.2018. УДК 512.5, 510.6.

[1]Институт математики им. С. Л. Соболева СО РАН. E-mail: rmnvski@gmail.com.

ет из себя m-ку кардинальных чисел. Для делимой m-жёсткой группы $G = M(\alpha_1, \ldots, \alpha_m)$ имеем $d(G) = (\alpha_1, \ldots, \alpha_m)$.

Теорема 3. *Пусть λ — бесконечное кардинальное число.*

1) *Группа $M(\beta_1, \ldots, \beta_m)$ является λ-насыщенной тогда и только тогда, когда $\lambda \leq \beta_i$ для всех индексов.*
2) *Группа $M(\beta_1, \ldots, \beta_m)$ является насыщенной тогда и только тогда, когда $\beta_1 = \ldots = \beta_m$ — бесконечный кардинал.*
3) *Счётная модель теории $\mathfrak{T}_m(M)$ является насыщенной тогда и только тогда, когда ее коразмерность над M равна $(\omega, \ldots, \omega) = \omega^m$.*
4) *Пусть $\lambda > \omega$. Модель мощности λ теории $\mathfrak{T}_m(M)$ является насыщенной тогда и только тогда, когда она имеет вид $M(\lambda, \ldots, \lambda) = M(\lambda^m)$.*

Важную роль в рассматриваемых задачах играет делимая m-жёсткая группа

$$M(\omega, \ldots, \omega) = M(\omega^m),$$

являющаяся счётной насыщенной моделью теории $\mathfrak{T}_m$. Мы утверждаем, что она будет предельной группой системы Fraisse всех конечно порождённых m-жёстких групп. Дадим адаптированные к нашей ситуации определения. Для данной m-жёсткой группы G обозначим через $\mathrm{age}(G)$ множество всех конечно порождённых независимых подгрупп ступени разрешимости m и через $\overline{\mathrm{age}}(G)$ соответствующий класс групп. Пусть также $\mathcal{K}_m$ обозначает класс всех конечно порождённых m-жёстких групп. Мы знаем из [2], что всякая конечно порождённая m-жёсткая группа независимо вкладывается в делимую m-жёсткую группу конечного ранга, а значит и в группу $M(\omega^m)$, поэтому $\overline{\mathrm{age}}(M(\omega^m)) = \mathcal{K}_m$. Назовем m-жёсткую группу G предельной для класса $\mathcal{K}_m$, если она удовлетворяет следующим свойствам:

(i) счётная;
(ii) $\overline{\mathrm{age}}(G) = \mathcal{K}_m$;
(iii) однородность: если $U, V \in \mathrm{age}(G)$ и $\varphi : U \to V$ — изоморфизм, то он расширяется до автоморфизма G.

Теорема 4. *Предельная группа для класса $\mathcal{K}_m$ определяется однозначно и она изоморфна $M(\omega^m)$.*

Мы также изучаем пересечения элементарных подмоделей в моделях теорий $\mathfrak{T}_m$ и $\mathfrak{T}_m(M)$.

Теорема 5.

1) *Пересечение некоторого множества элементарных подмоделей модели теории $\mathfrak{T}_m$ является элементарной подмоделью в том и только том случае, если оно имеет ступень разрешимости m.*
2) *Пересечение любого множества элементарных подмоделей модели теории $\mathfrak{T}_m(M)$ снова является элементарной подмоделью.*

Последняя наша теорема связана с элиминацией кванторов исследуемых теорий.

Теорема 6. *Всякая формула теории $\mathfrak{T}_m$ или теории $\mathfrak{T}_m(M)$ эквивалентна булевой комбинации $\forall\exists$-формул.*

Литература

1. *Мясников А. Г., Романовский Н. С.* Делимые жёсткие группы. Стабильность, насыщенность и элементарные подмодели // Алгебра и логика. 2018. Т. 57, № 1. Принято в печать.
2. *Романовский Н. С.* Делимые жёсткие группы // Алгебра и логика. 2008. Т. 47, № 6. С. 762—776.
3. *Романовский Н. С.* Делимые жёсткие группы. Алгебраическая замкнутость и элементарная теория // Алгебра и логика. 2017. Т. 56, № 5. С. 593—612.
4. *Myasnikov A., Romanovskiy N.* Krull dimension of solvable groups // J. Algebra. 2010. Vol. 324, № 10. P. 2814—2831.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О РАЗРЕШИМОСТИ УРАВНЕНИЙ В РАЗРЕШИМЫХ ГРУППАХ[1]

В. А. Романьков (Омск)[2]

1. Введение

Вопросы разрешимости уравнений в группах и классах групп активно ведутся на протяжении последних 50 лет. Значительный импульс этим исследоваиям был придан А. И. Мальцевым, Р. Линдоном, Б. Нейманом и Г. Баумслагом. Относительно классических результатов в этой области и современном ее состоянии см. обзоры [10, 11, 13], а также монографию [15]. Настоящий доклад посвящен разрешимости уравнений в классах нильпотентных и разрешимых групп.

Напомним, что *уравнением* над группой G от *неизвестных* $x_1, ..., x_n$ называется выражение вида

$$u(x_1, ..., x_n, G) = 1, \tag{1}$$

где левая часть является элементом свободного произведения $G * F_n$ группы G и свободной группы F_n с множеством свободных порождающих (базисом) $\{x_1, ..., x_n\}$. Уравнение однозначно записывается в несократимом виде

$$g_0 x_{i_1}^{\epsilon_1} g_1 x_{i_1}^{\epsilon_1} \cdot ... \cdot g_k x_{i_k}^{\epsilon_k} g_{k+1} = 1, \tag{2}$$

где $g_i \in G, i_j \in \{1, ..., n\}, \epsilon_i = \pm 1, i = 1, ..., k+1$. Участвующие в записи элементы g_i называются *коэффициентами* уравнения. Некоторые из них возможно равны 1, можно считать, что они в несократимой записи не присутствуют. Также считаем, что левая часть циклически несократима в $G * F_n$. В противном случае, выполнив циклическое сокращение, придем к равносильному уравнению меньшей длины. Уравнение вида

$$u(x_1, ..., x_n) = v \tag{3}$$

(равносильное $u(x_1, ..., x_n)v^{-1} = 1$) называется *расщепленным (split)*, если его левая часть не содержит коэффициентов. *Решением* называется любой набор элементов $(f_1, ..., f_n)$ группы G, который при подстановке в уравнение вместо набора $(x_1, ..., x_n)$ неизвестных дает верное равенство. Если решение существует, то говорят, что уравнение *разрешимо* в группе G. В противном случае оно называется *неразрешимым* в G.

Если $\mathcal{C}$ — некоторый класс групп, замкнутый по подгруппам, $G \in \mathcal{C}$, то говорят, что уравнение *разрешимо над группой* G в классе $\mathcal{C}$, если существует группа $H \in \mathcal{C}$, содержащая группу G, в которой данное уравнение имеет решение. Ясно, что уравнение над группой G можно считать уравнением над любой группой, содержащей G. Если речь идет о разрешимости уравнения над группой в классе всех групп, то класс не упоминается, то есть говорится о разрешимости уравнения *над группой*.

Уравнение от одной переменной x называется *регулярным*, если сумма всех показателей степеней, с которыми x входит в запись уравнения, не равна 0, унимодулярным, если эта сумма равна 1.

По теореме Клячко [9] любое унимодулярное уравнение разрешимо над произвольной группой без кручения. Согласно гипотезе Кервера–Лауденбаха любое регулярное уравнение разрешимо над произвольной группой. По гипотезе Левина любое уравнение разрешимо над произвольной группой без кручения. Приведенные гипотезы остаются открытыми.

 Получено 14.01.2018. УДК 512.54.

[1]Работа выполнена при финансовой поддержке РНФ, проект № 16.11.10002.

[2]Омский государственный университет им. Ф. М. Достоевского. E-mail: romankov48@mail.ru.

Через $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$ обозначается коммутатор элементов g_1, g_2 произвольной группы. Он считается простым коммутатором веса 2. Простой коммутатор $[g_1, g_2, ..., g_k]$ веса $k \geq 3$ определяется индуктивно, как $[[g_1, g_2, ..., g_{k-1}], g_k]$.

2. Известные результаты

Приведем несколько давно известных результатов по разрешимости уравнений в классах разрешимых или нильпотентных групп. По теореме А. Л. Шмелькина [8] любое унимодулярное уравнение над нильпотентной группой G имеет единственное решение в самой группе G. В случае эффективного представления конечно порожденной нильпотентной группы G это решение также определяется эффективно. В общем случае не существует алгоритмов, определяющих разрешимость расщепленных уравнений в свободных нильпотентных ступени нильпотентности не меньше 4 и свободных метабелевых группах ранга не меньше 2 [4, 5]. В этих работах использовалась интерпретация диофантовых уравнений. А именно: по любому диофантову уравнению вида $D(z_1, ..., z_n) = a, a \in \mathbb{Z}$, эффективно строилось расщепленное уравнение над рассматриваемой группой, имеющее в этой группе решение тогда и только тогда, когда данное диофантово уравнение имеет решение в целых числах. Согласно знаменитому результату Ю. В. Матиясевича можно зафиксировать многочлен $D(z_1, ..., z_n)$ и рассматривать класс уравнений, меняя правую часть a таким образом, что соответствующая диофантова проблема оказывается алгоритмически неразрешимой. Интерпретация диофантовых уравнений позволяет вывести отсюда алгоритмическую неразрешимость проблемы существования решений у уравнений в рассматриваемых группах.

Метод интерпретации диофантовых уравнений был использован в работах Н. Н. Репина [2, 3], получившего следующие результаты:

- Проблема разрешимости уравнений от одной переменной разрешима в любой конечно порожденной нильпотентной группе ступени нильпотентности $c \leq 2$. Существует конечно порожденная нильпотентная группа ступени нильпотентности 3, в которой эта проблема неразрешима.
- Проблема разрешимости уравнений неразрешима для любой свободной нильпотентной группы ранга $r \geq 600$ ступени нильпотентности $c \geq 3$.
- Проблема разрешимости уравнений от одной переменной неразрешима для любой свободной нильпотентной группы ранга $r \geq 2$ ступени нильпотентности $c \geq 5 \cdot 10^{10}$.

3. Современные исследования

По-прежнему представляют интерес результаты об алгоритмической разрешимости уравнений в группах, в частности, в нильпотентных группах. Сейчас такую проблему принято называть *диофантовой*. В докладе представляются следующие результаты автора.

Теорема 1 [14]. *Существует конечно порожденная нильпотентная группа G ступени 2, для которой неразрешима диофантова проблема для коммутаторных уравнений, то есть расщепленных уравнений вида*

$$[x, y] = u, u \in G. \tag{4}$$

В [14] используется интерпретация диофантовых уравнений. Построение группы и уравнений осуществляется эффективно.

Также в [14] отмечены неразрешимости в классе конечно порожденных нильпотентных групп ступени два проблем *эндоморфной сводимости* (определить, будет ли один из произвольной пары элементов группы эндоморфным образом другого) и *ретракта* (определить, является ли заданная подгруппа ретрактом). Замечено, что диофантова проблема для коммутаторных уравнений разрешима для любой свободной нильпотентной группы ступени $c = 2$.

Элементы g и f группы G называются *скрученно сопряженными* относительно эндоморфизма ϕ, если существует элемент $x \in G$ такой, что $\phi(x)g = fx$, *бинарно скрученно сопряженными* относительно пары эндоморфизмов ϕ, ψ, если существует элемент $x \in G$ та-

кой, что $\phi(x)g = f\psi(x)$. Эти отношения являются эквивалентностями. Соответствующие проблемы называются разрешимыми, если существуют алгоритмы, определяющие эквивалентность для произвольных элементов и эндоморфизмов. Проблемы поиска заключаются в возможности эффективного нахождения x.

Теорема 2.

- [6] *Проблемы сопряженности, скрученной и бинарно скрученной сопряженности, а также соответствующие проблемы поиска разрешимы в классе всех конечно порожденных нильпотентных групп.*
- [12] *Проблема скрученной сопряженности разрешима в любой полициклической группе.*
- [1] *Проблема скрученной сопряженности разрешима в любой конечно порожденной метабелевой группе относительно эндоморфизма тождественного по модулю нормальной подгруппы, содержащей коммутант.*

Теорема 3. *Произвольное расщепленное коммутаторное уравнение вида (3), в котором левая часть $u(x_1, ..., x_n)$ — простой коммутатор, разрешимо над любой конечно порожденной нильпотентной группой в классе конечно порожденных нильпотентных групп.*

Данный результат для внешне коммутаторного простого коммутатора $u(x_1, ..., x_n)$ (то есть простого коммутатора, в котором каждая переменная присутствует один раз) может быть выведен из теоремы Ю. В. Сосновского [16].

Кроме этих результатов в докладе предполагается обсудить результаты о разрешимости регулярных уравнений (в частности из [7]) и некоторые результаты о практической реализации алгоритмов, решающих диофантовы проблемы в классе разрешимых групп и его основных подклассах.

Литература

1. *Вентура Э., Романьков В. А.* Проблема скрученной сопряженности для эндоморфизмов метабелевых групп // Алгебра и логика. 2009. Т. 48, № 2. С. 89—98.
2. *Репин Н. Н.* Уравнения с одной неизвестной в нильпотентных группах // Математические заметки. 1983. Т. 34, № 2. С. 201—206.
3. *Репин Н. Н.* Проблема разрешимости уравнений с одной неизвестной в нильпотентных группах // Известия АН СССР. Серия математическая. 1984. Т. 48, № 6. С. 1295—1313.
4. *Романьков В. А.* О неразрешимости проблемы эндоморфной сводимости в свободных нильпотентных группах и свободных кольцах // Алгебра и логика. 1977. Т. 16, № 4. С. 457—471.
5. *Романьков В. А.* Об уравнениях в свободных метабелевых группах // Сибирский математический журнал. 1979. Т. 20, № 3. С. 671—673.
6. *Романьков В. А.* О разрешимости уравнений с эндоморфизмами в нильпотентных группах // Сибирские электронные математические известия. 2016. Т. 13. С. 716—725.
7. *Романьков В. А.* On solvability of regular equations in the varieties of metabelian groups // Прикладная дискретная математика. 2017. № 36. С. 51—58.
8. *Шмелькин А. Л.* О полных нильпотентных группах // Алгебра и логика. 1967. 2014. Т. 6, № 2. С. 111—114.
9. *Klyachko A. A.* A funny property of sphere and equations over groups // Communications in Algebra. 1993. Vol. 21, № 7. P. 2555—2575.
10. *Noskov G. A., Remeslennikov V. N., Roman'kov V. A.* Infinite Groups // Journal of Mathematical Sciences. 1982. Vol. 18, № 5. P. 669—735.
11. *Remeslennikov V. N., Roman'kov V. A.* Model-theoretic and algorithmic questions of group theory // Journal of Mathematical Sciences. 1985. Vol. 31, № 3. P. 2887—2939.
12. *Roman'kov V.* The twisted conjugacy problem for endomorphisms of polycyclic groups // Journal of Group Theory. 2010. Vol. 13, № 3. P. 355—364.
13. *Roman'kov V.* Equations over groups // Groups, Complexity, Cryptology. 2012. Vol. 4, № 2. P. 191—239.
14. *Roman'kov V. A.* Diophantine questions in the class of finitely generated nilpotent groups // Journal of Group Theory. 2016. Vol. 19, № 3. P. 497—514.
15. *Roman'kov V.* Essays in algebra and cryptology: solvable groups. Омск : Изд-во Омского университета. 2017. 268 с.
16. *Sosnovskiy Y. V.* On the width of verbal subgroups of the groups of triangular matrices over a field of arbitrary characteristic // International Journal of Algebra and Computation. 2016. Vol. 26, № 2. P. 217—222.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

НЕКОТОРЫЕ КАТЕГОРИИ АБЕЛЕВЫХ ГРУПП

А. А. Фомин (Москва)[1]

Рассматриваются две категории абелевых групп. Объектами категории $\mathcal{F}$ являются абелевы группы без кручения конечного ранга с отмеченными базисами. Под базисом здесь понимается любая максимальная линейно независимая система элементов. Объектами категории $\mathcal{D}$ являются смешанные факторно делимые группы с отмеченными базисами. Морфизмами в обеих категориях являются гомоморфизмы групп с целочисленными матрицами относительно отмеченных базисов.

Третья категория $\mathcal{S}$ представляет собой категорию терминов, в которых одновременно описываются объекты категорий $\mathcal{F}$ и $\mathcal{D}$. А именно, объектами категории $\mathcal{S}$ являются конечные последовательности $a_1, \ldots, a_n$ элементов конечно представимых модулей над кольцом полиадических чисел $\widehat{\mathbf{Z}}$. Кольцо полиадических чисел $\widehat{\mathbf{Z}} = \prod\limits_p \widehat{\mathbf{Z}}_p$ — это произведение колец целых p-адических чисел по всем простым числам p. Элементы $a_1, \ldots, a_n$ порождают $\widehat{\mathbf{Z}}$-подмодуль A, который также является конечно представимым $\widehat{\mathbf{Z}}$-модулем. Мы обозначаем $A = \langle a_1, \ldots, a_n \rangle_{\widehat{\mathbf{Z}}}$. Пусть $B = \langle b_1, \ldots, b_k \rangle_{\widehat{\mathbf{Z}}}$ — модуль, соответствующий объекту $b_1, \ldots, b_k$. Морфизмами из объекта $a_1, \ldots, a_n$ в объект $b_1, \ldots, b_k$ являются все возможные пары (φ, M), где $\varphi : A \to B$ — гомоморфизм $\widehat{\mathbf{Z}}$-модулей, а M — целочисленная матрица размера $k \times n$, для которых выполнено матричное равенство

$$(\varphi a_1, \ldots, \varphi a_n) = (b_1, \ldots, b_k)M.$$

Доказывается, что категория $\mathcal{S}$ эквивалентна категории $\mathcal{D}$ и двойственна категории $\mathcal{F}$. Композиция этой эквивалентности и двойственности является двойственностью между категориями $\mathcal{D}$ и $\mathcal{F}$, которую можно рассматривать как модификацию двойственности, полученной в [1].

Литература

1. *Fomin A. A., Wickless W. J.* Quotient divisible Abelian groups // Proc. Amer. Math. Soc. 1998. Vol. 126, № 1. P. 45—52.

 Получено 21.12.2017. УДК 512.541.

[1]Московский педагогический государственный университет. E-mail: alexander.fomin@mail.ru.

Секция 1

ТЕОРИЯ ГРУПП

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

КОНЕЧНЫЕ ГРУППЫ С ЗАДАННЫМИ ХОЛЛОВЫМИ ПОДГРУППАМИ

С. В. Балычев (Гомель, Беларусь)[1], Т. И. Васильева (Гомель, Беларусь)[2]

Все рассматриваемые в данной работе группы конечные. Используются определения и обозначения из [6] и [9].

Пусть π — некоторое множество простых чисел и $\mathfrak{F}$ — класс групп. В соответствии с [6] через $C_\pi\mathfrak{F}$ обозначается класс всех групп, у которых имеется по крайней мере одна π-холлова подгруппа, принадлежащая $\mathfrak{F}$, и любые две π-холловы подгруппы сопряжены.

Если π состоит из одного простого числа p и $\mathfrak{F} = \mathfrak{E}$ — класс всех групп, то по теореме Силова $C_{\{p\}}\mathfrak{E} = \mathfrak{E}$. Однако группа может не иметь π-холловых подгрупп, если в π входит 2 и более простых чисел. Например, в знакопеременной группе A_5 на 5 символах нет $\{2,5\}$-холловых подгрупп, хотя $\{2,5\} \subseteq \pi(A_5)$.

В 1928 году Ф. Холл [10] доказал, что для любого множества простых чисел π во всякой разрешимой группе G существует π-холлова подгруппа, любые две π-холловы подгруппы сопряжены, каждая π-подгруппа содержится в некоторой π-холловой подгруппе из G. Ввиду этого класс $C_\pi\mathfrak{E}$ содержит все разрешимые группы.

Свойства класса групп $C_\pi\mathfrak{F}$ для различных $\mathfrak{F}$ исследовались в работах [4, 5, 7, 8]. В [6, проблема 19] была выдвинута гипотеза: пусть π — некоторое множество простых чисел, $\mathfrak{F}$ — насыщенная формация, тогда $C_\pi\mathfrak{F}$ — насыщенная формация. В [7] для произвольной насыщенной формации $\mathfrak{F}$ был получен критерий насыщенности $C_\pi\mathfrak{F}$ в предположении, что $C_\pi\mathfrak{F}$ — формация. Там же был приведен пример, показывающий, что формация $C_\pi\mathfrak{N}$ в общем случае не является насыщенной. В [4] было доказано, что для любой формации $\mathfrak{F}$ и любого множества простых чисел π класс $C_\pi\mathfrak{F}$ является формацией. В этой же работе были найдены условия, при которых формация $C_\pi\mathfrak{F}$ является p-насыщенной или p-разрешимо насыщенной.

Определение. Пусть t — натуральное число и $\mathfrak{F}$ — класс групп. Обозначим через $\mathrm{H}_t\mathfrak{F}$ следующий класс групп: $\mathrm{H}_t\mathfrak{F} = \cap\, C_{\pi_i}\mathfrak{F}$ по всем $\pi_i \subseteq \mathbb{P}$ таким, что $|\pi_i| = t$.

Ясно, что класс $\mathrm{H}_t\mathfrak{F}$ наследует свойства $C_{\pi_i}\mathfrak{F}$. В то же время $\mathrm{H}_t\mathfrak{F}$ имеет более сильные свойства, чем $C_{\pi_i}\mathfrak{F}$. Например, $\mathrm{H}_2\mathfrak{N} = \mathfrak{N}$ — насыщенная формация, а в [7] показано, что формация $C_{\{3,11\}}\mathfrak{N}$ является композиционной, но не является насыщенной.

В классе всех разрешимых групп получена

Теорема. *Пусть t — натуральное число, $t \geqslant 2$, $\mathfrak{F}$ — наследственная насыщенная формация и F — её максимальный внутренний локальный экран. Тогда $\mathrm{H}_t\mathfrak{F}$ также является наследственной насыщенной формацией и имеет максимальный внутренний локальный экран H такой, что*

$$H(p) = \begin{cases} \mathrm{H}_t F(p),\ H(p) \cap \mathfrak{S}_{p'} = \mathrm{H}_{t-1}(F(p) \cap \mathfrak{S}_{p'}) & \text{для любого } p \in \pi(\mathfrak{F}); \\ \varnothing & \text{для любого } p \in \mathbb{P} \setminus \pi(\mathfrak{F}). \end{cases}$$

Используя эту теорему, найдем $\mathrm{H}_t\mathfrak{F}$ для некоторых конкретных формаций $\mathfrak{F}$.

В [1, 2] был изучен класс $\mathrm{w}\mathfrak{U}$ всех групп, у которых любая силовская подгруппа либо

 Получено 14.12.2017. УДК 512.543.

[1]Гомельский государственный университет им. Франциска Скорины.
E-mail: sergey.baluchev@gmail.com.

[2]Гомельский государственный университет им. Франциска Скорины;
Белорусский государственный университет транспорта. E-mail: tivasilyeva@mail.ru.

совпадает с группой, либо может быть соединена с ней цепью подгрупп с простыми индексами. Отметим, что класс $\mathrm{w}\mathfrak{U}$ образует наследственную насыщенную формацию разрешимых групп [2].

Пример 1. Если $\mathfrak{F} = \mathfrak{U}$ — класс всех сверхразрешимых групп, то $\mathrm{H}_2\mathfrak{U} = \mathrm{w}\mathfrak{U}$.

Подгруппа M группы G называется *модулярной* в G [11], если она является модулярным элементом в решетке всех подгрупп группы, т. е. если выполняются следующие условия:

1) $\langle X, M \cap Z\rangle = \langle X, M\rangle \cap Z$ для всех $X \leq G, Z \leq G$ таких, что $X \leq Z$;

2) $\langle M, Y \cap Z\rangle = \langle M, Y\rangle \cap Z$ для всех $Y \leq G, Z \leq G$ таких, что $M \leq Z$.

Подгруппа H группы G называется *субмодулярной* в G [12], если существует цепь подгрупп $H = H_0 \leq H_1 \leq \cdots \leq H_{s-1} \leq H_s = G$ такая, что H_{i-1} — модулярная подгруппа в H_i для $i = 1, \ldots, s$. Сверхразрешимая группа называется *сильно сверхразрешимой* [3], если в ней любая силовская подгруппа субмодулярна.

В [3] были введены и изучены следующие классы групп: $s\mathfrak{U}$ — класс всех сильно сверхразрешимых групп, $sm\mathfrak{U}$ — класс всех групп с субмодулярными силовскими подгруппами. В частности, эти классы являются наследственными насыщенными формациями, $sm\mathfrak{U}$ — собственный подкласс из $\mathrm{w}\mathfrak{U}$, $\mathfrak{U} \neq s\mathfrak{U}$ и $s\mathfrak{U} \neq sm\mathfrak{U}$.

Пример 2. Если $\mathfrak{F} = sm\mathfrak{U}$, то $\mathrm{H}_2(s\mathfrak{U}) = sm\mathfrak{U}$.

Пример 3. Если $\mathfrak{F} = \mathfrak{NA}$ — класс всех групп с нильпотентным коммутантом, то $\mathfrak{NA} \subset \mathrm{H}_2(\mathfrak{NA}) \subset \mathfrak{NA}$.

Здесь $\mathcal{A}$ — класс всех разрешимых групп с абелевыми силовскими подгруппами, $\mathfrak{N}\mathcal{A}$ — класс всех групп с нильпотентным $\mathcal{A}$-корадикалом.

Отметим, что симметрическая группа S_4 принадлежит $\mathfrak{N}\mathcal{A}$, но $S_4 \notin \mathrm{H}_2(\mathfrak{NA})$. Группа из примера 1 [2] принадлежит $\mathrm{H}_2(\mathfrak{NA})$, но ее коммутант не является нильпотентным. Таким образом, $\mathfrak{NA} \neq \mathrm{H}_2(\mathfrak{NA}) \neq \mathfrak{N}\mathcal{A}$.

Литература

1. *Васильев А. Ф., Васильева Т. И., Тютянов В. Н.* О конечных группах, близких к сверхразрешимым группам // Проблемы физики, математики и техники. 2010. № 2 (3). С. 21—27.
2. *Васильев А. Ф., Васильева Т. И., Тютянов В. Н.* О конечных группах сверхразрешимого типа // Сибирский математический журнал. 2010. Т. 51, № 6. С. 1270—1281.
3. *Васильев В. А.* Конечные группы с субмодулярными силовскими подгруппами // Сибирский математический журнал. 2015. Т. 56, № 6. С. 1277—1288.
4. *Вдовин Е. П., Ревин Д. О., Шеметков Л. А.* Формации конечных C_π-групп // Алгебра и анализ. 2012. Т. 24, № 1. С. 40—52.
5. *Слепова Л. М.* О формациях $E^{\mathfrak{F}}$-групп // Доклады АН БССР. 1977. Т. 21, № 7. С. 587—589.
6. *Шеметков, Л. А.* Формации конечных групп. М. : Наука, 1978. 272 с.
7. *Шеметков Л. А., Васильев А. Ф.* Нелокальные формации конечных групп // Доклады АН Беларуси. 1995. Т. 39, № 4. С. 5—8.
8. *Blessenohl D.* Über Formationen und Halluntergruppen endlicher auflösbarer Gruppen // Math. Z. 1975. Vol. 142, № 3. P. 299—300.
9. *Doerk K., Hawkes T.* Finite soluble groups. Berlin, New York : Walter de Gruyter, 1992. 891 p.
10. *Hall P.* A note on soluble groups // J. London Math. Soc. 1928. Vol. 3. P. 98—105.
11. *Schmidt R.* Subgroup Lattices of Groups. Berlin, New York : Walter de Gruyter, 1994. 572 p.
12. *Zimmermann I.* Submodular Subgroups in Finite Groups // Math. Z. 1989. Vol. 202. P. 545—557.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ПОЧТИ ВПОЛНЕ РАЗЛОЖИМЫЕ ГРУППЫ В КЛАССЕ АБЕЛЕВЫХ ГРУПП БЕЗ КРУЧЕНИЯ: ИСТОЧНИК ИДЕЙ, ПРИЛОЖЕНИЯ[1]

Е. А. Благовещенская (Санкт-Петербург)[2], А. Е. Трифонов (Санкт-Петербург)[3]

Возможность классификации алгебраических структур с точностью до изоморфизма не всегда существует, и тогда оказывается необходимым изобретение новых понятий эквивалентности, более слабых, чем изоморфизм. Это в полной мере относится к теории абелевых групп без кручения, допускающих разложения в прямые суммы неразложимых слагаемых с различными наборами их рангов.

Важными инструментами классификации в данной ситуации наличия неизоморфных прямых разложений оказался так называемый «почти изоморфизм» (обозн. $\cong_{nr}$). Его значимость для абелевых групп без кручения определяется сохранением свойств их разложений в следующем смысле:

Теорема 1 (Д. Арнольд, [5, 12.9 (b), с. 144])**.** *Если X и Y — почти изоморфные абелевы группы без кручения конечного ранга и $X = X_1 \oplus X_2$, то $Y = Y_1 \oplus Y_2$ для некоторых групп $Y_1 \cong_{nr} X_1$, $Y_2 \cong_{nr} X_2$.*

Что касается самого понятия почти изоморфизма, то оно существует в различных эквивалентных формулировках, в том числе:

Определение. Две абелевы группы без кручения конечного ранга G и H *почти изоморфны*, обозн. $G \cong_{nr} H$, если для любого простого p существуют мономорфизмы

$$\Phi_p : G \longrightarrow H, \quad \Psi_p : H \longrightarrow G,$$

для которых группы $G/H\Psi_p$ и $H/G\Phi_p$ конечны, и числа $[G : H\Psi_p]$ и p, а также $[H : G\Phi_p]$ и p, являются взаимно простыми.

Важная роль так называемых почти вполне разложимых групп ([4], [8, 25.2]) определяется присутствием в данном классе всего разнообразия прямых разложений, характерного для абелевых групп без кручения в целом, и определяемого, в первую очередь, наборами рангов неразложимых слагаемых в различных прямых разложениях одного и того же объекта.

Напомним некоторые понятия. Натуральное число n называется *рангом* абелевой группы без кручения X, если оно является мощностью его максимальной линейно независимой системы. Ранг группы X обозначается как $\mathrm{rk}\, X$. Любая прямая сумма групп ранга 1 называется вполне разложимой группой (*cd-группой*).

Acd-группа X (*почти вполне разложимая группа*) — это абелева группа без кручения конечного ранга, содержащая вполне разложимую подгруппу A, так что X/A — конечная группа. Без умаления общности считаем, что A — *регулятор* acd-группы X, то есть её единственным образом специально определенная вполне характеристическая подгруппа (последнее означает, что A содержит образы всех своих элементов при эндоморфизмах X).

 Получено 12.03.2018. УДК 512.541.

[1]Работа выполнена при финансовой поддержке РФФИ, грант 17-01-00849

[2]Петербургский государственный университет путей сообщения Императора Александра I, Санкт-Петербургский политехнический университет Петра Великого. E-mail: blagoveschenskaya@pgups.ru.

[3]Филиал акционерного общества «Концерн радиостроения «Вега» в г. Санкт-Петербурге.
E-mail: algisothal@gmail.com.

Если, к тому же, X/A — циклическая группа, то X называется *crq-группой* (то есть acd-группой с циклическим регуляторным фактором).

Мы говорим, что X является *блочно-жёсткой* группой, если множество $T_{cr}(X)$ представляет собой антицепь, то есть в разложении $A = \bigoplus_{\tau \in T_{cr}(X)} A(\tau)$ в прямую сумму однородных компонент $\mathrm{Hom}(A(\tau), A(\sigma)) = 0$ при $\tau \neq \sigma$. Заметим, что $\mathrm{rk}\, X = \mathrm{rk}\, A$. Локальные почти вполне разложимые группы характеризуются тем, что любые их вполне характеристические подгруппы конечного ранга являются почти вполне разложимыми группами.

Среди важных результатов выделим следующие:

1. Установлено, что аддитивные группы колец эндоморфизмов $\mathrm{End}\, X$ почти изоморфных acd-групп X также являются почти изоморфными acd-группами, при этом группа автоморфизмов кольца $\mathrm{End}\, X$ может рассматриваться как подгруппа группы автоморфизмов кольца $\mathrm{End}\, A$, см. [1].

2. Определено понятие почти изоморфизма для групп без кручения счетного ранга и доказан аналог теоремы Арнольда о прямых разложениях блочно-жестких *локально почти вполне разложимых групп*, в случае *обобщенно циклического регуляторного фактора*, для них построена графическая теория прямых разложений, см. [2, 7].

3. В классах блочно-жестких crq-групп (конечного ранга) и групп счетного ранга с обобщенно циклическим регуляторным фактором доказана их определяемость кольцами эндоморфизмов с точностью до почти изоморфизма (теоремы типа Бэра–Капланского), см. [3].

Специальным графическим методом доказана теорема, открывающая способы оптимального распараллеливания алгоритмов определенного вида, так как ее доказательство базируется на ярусно-параллельных графах (см. [6]):

Теорема 2. *Пусть $n > r \geqslant 2$ — натуральные числа. Существует блочно-жесткая crq-группа X ранга n, разложимая в прямые суммы неразложимых слагаемых рангов r_1, r_2, …, r_s для любых разбиений $n = r_1 + r_2 + \ldots + r_s$, в которых максимальные слагаемые совпадают с числом r.*

Литература

1. *Благовещенская Е. А.* Автоморфизмы колец эндоморфизмов блочно-жестких почти вполне разложимых групп // Фундаментальная и прикладная математика. 2004. Т. 10, № 2. С. 23—50.
2. *Благовещенская Е. А.* Прямые разложения локально почти вполне разложимых групп счетного ранга // Чебышевский сборник. 2005. Т. 6, вып. 4. С. 24—47.
3. *Благовещенская Е. А.* Определяемость абелевых групп без кручения счетного ранга некоторого класса их кольцами эндоморфизмов // Фундаментальная и прикладная математика. 2007. Т. 13, № 1. С. 31—43.
4. *Благовещенская Е. А.* Почти вполне разложимые абелевы группы и их кольца эндоморфизмов. Санкт-Петербург : Изд-во Политехнического ун-та, 2009. 214 с. (Сер.: Математика в политехническом университете.)
5. *Arnold D.* Finite rank torsion free abelian groups and rings. Berlin, Heidelberg, New York : Springer-Verlag, 1982. (Lecture Notes in Mathematics. Vol. 931.)
6. *Blagoveshchenskaya E., Kunetz D.* Direct decomposition theory of torsion-free abelian groups of finite rank: graph method // Lobachevskii Journal of Mathematics. 2018. Vol. 39. № 1. P. 29—34.
7. *Blagoveshchenskaya E., Strüngmann L. H.* Direct decomposition theory under near-isomorphism for a class of infinite rank torsion-free abelian groups // Journal of Group Theory. 2017. Vol. 20, № 2. P. 325—346.
8. *Mader A.* Almost completely decomposable abelian groups. Gordon and Breach Science Publishers : Amsterdam, 1999. (Ser.: Algebra, Logic and Applications. Vol. 13.)

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ПРОИЗВЕДЕНИЯ $K-\mathbb{P}$-СУБНОРМАЛЬНЫХ ПОДГРУПП

П. В. Бычков (Гомель, Беларусь)[1], В. Н. Тютянов (Гомель, Беларусь)[2]

Рассматриваются только конечные группы. Принятые обозначения стандартны. Через $S(G)$ обозначается наибольшая нормальная разрешимая подгруппа группы G. В работе [1] было введено следующее определение.

Определение. Подгруппу H группы G будем называть $K-\mathbb{P}$-субнормальной в G, если существует цепь подгрупп $H = H_0 \subseteq H_1 \subseteq \dots H_{n-1} \subseteq H_n = G$ такая, что либо H_{i-1} нормальна в H_i, либо $|H_i : H_{i-1}|$ есть простое число для любого $i = 1, \dots, n$.

В работе [1] был установлен ряд важных результатов о строении конечных групп, факторизуемых $K-\mathbb{P}$-субнормальными подгруппами. Также ряд важных теорем был доказан в работах [2, 3, 4]. Мы продолжаем данные исследования. Доказана следующая теорема.

Теорема. *Пусть $G = AB$ — конечная группа, где $(|A|, |B|) = 1$ и $|A|$ — нечетное число. Если A и B являются $K-\mathbb{P}$-субнормальными подгруппами группы G, то $A \subseteq S(G)$.*

Литература

1. *Васильев А. Ф., Васильева Т. И., Тютянов В. Н.* О $K-\mathbb{P}$-субнормальных подгруппах конечных групп // Математические заметки. 2014. Т. 95, № 4. С. 517—528.
2. *Васильев А. Ф., Васильева Т. И., Тютянов В. Н.* О произведениях $\mathbb{P}$-субнормальных подгрупп в конечных группах // Сибирский математический журнал. 2012. Т. 53, № 1. С. 59—67.
3. *Тютянов В. Н., Книгина В. Н.* Факторизации конечных групп r-разрешимыми подгруппами с заданными вложениями // Украинский математический журнал. 2014. Т. 66, № 10. С. 1431—1435.
4. *Monakhov V., Kniahina V.* Finite factorised groups witth partially solvable $\mathbb{P}$-subnormal subgroups // Lobachevskii Journal of Mathematics. 2015. Vol. 36, № 4. P. 441—445.

 Получено 24.12.2017. УДК 512.542.

[1]Гомельский государственный университет им. Франциска Скорины. E-mail: pbychkov@tut.by.

[2]Международный университет «МИТСО». E-mail: tyutyanov@front.ru.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

АРИФМЕТИЧЕСКИЕ ГРАФЫ КОНЕЧНЫХ ГРУПП

А. Ф. Васильев (Гомель, Беларусь)[1], В. И. Мурашко (Гомель, Беларусь)[2]

Рассматриваются только конечные группы. В работе используются стандартные терминология и обозначения из теории групп и графов, которые, если необходимо, могут быть найдены в [4, 10, 11]. Напомним, что через $\pi(G)$ обозначается множество всех простых делителей порядка группы G; группой Шмидта называется ненильпотентная группа, все максимальные подгруппы которой нильпотентны; (p, q)-группой Шмидта называется группа Шмидта G, для которой $\pi(G) = \{p, q\}$ и которая имеет нормальную силовскую p-подгруппу; Syl_pG — множество всех силовских p-подгрупп группы G.

В настоящее время имеется значительное число работ, в которых каждой конечной группе ставится в соответствие определенный граф и исследуется связь свойств графа со свойствами группы (см., например, [1, 2, 5, 6, 7, 8, 9, 12, 13, 14]). Это направление восходит к работе [7] А. Кэли 1878 года. Введённый им граф группы, называемый в настоящее время графом Кэли, имеет большое число приложений. Другой яркой иллюстрацией этого направления является проблема П. Эрдеша о графах некоммутативности, решенная Б. Нейманом [13] в 1976 году.

Определение 1. (1) Функцию Γ будем называть арифметической графовой функцией, если она каждой группе G ставит в соответствие граф $\Gamma(G)$ такой, что $V(\Gamma(G))$ — подмножество множества делителей $|G|$ и $\Gamma(1) = \emptyset$. Граф $\Gamma(G)$ назовем арифметическим.

(2) Графом $\Gamma(\mathfrak{X})$ класса групп $\mathfrak{X}$ будем называть $\bigcup\limits_{G\in\mathfrak{X}} \Gamma(G)$.

Примерами арифметических графов являются:

(1) Граф Хоукса $\Gamma_H(G)$ [12]:

$$V(\Gamma_H(G)) = \pi(G) \text{ и } E(\Gamma_H(G)) = \{(p, q) \mid q \in \pi(G/\mathrm{O}_{p',p}(G))\}.$$

(2) Силовский граф $\Gamma_s(G)$ [9]: $V(\Gamma_s(G)) = \pi(G)$ и

$$E(\Gamma_s(G)) = \{(p, q) \mid q \in \pi(N_G(P)/PC_G(P)),\ P \in Syl_pG\}.$$

(3) N-критический граф $\Gamma_{Nc}(G)$: $V(\Gamma_{Nc}(G)) = \pi(G)$ и

$$E(\Gamma_{Nc}(G)) = \{(p, q) \mid G \text{ содержит } (p, q)\text{-подгруппу Шмидта}\}.$$

(4) Граф простых чисел или граф Грюнберга-Кегеля $\Gamma_p(G)$ [2, 14]: $V(\Gamma_p(G)) = \pi(G)$

$$E(\Gamma_p(G)) = \{\{p, q\} \mid G \text{ содержит элемент порядка } pq\}.$$

Следуя работе [1], скажем, что группа G называется распознаваемой по графу простых чисел, если из $\Gamma_p(G) = \Gamma_p(H)$ всегда следует $H \simeq G$ для любой группы H. Как отмечено в работе [1], существует бесконечное множество групп с нетривиальным разрешимым радикалом и одинаковым графом простых чисел. Поэтому, проблема распознавания групп по графу простых чисел представляет интерес только для простых или почти простых групп. Отметим, что граф простых чисел применяется при решении известной проблемы распознавания групп по множеству порядков их элементов, см., например, [3]. В данной работе мы будем рассматривать проблему распознавания групп по графу с точностью до класса групп в смысле следующего определения.

 Получено 25.12.2017. УДК 512.542.

[1]Гомельский государственный университет им. Франциска Скорины. E-mail: formation56@mail.ru.

[2]Гомельский государственный университет им. Франциска Скорины. E-mail: mvimath@yandex.ru.

Определение 2. Пусть Γ — графовая функция и $\mathfrak{X}$ — класс групп. Класс $\mathfrak{X}$ назовем распознаваемым графовой функцией Γ, если из $G_1 \in \mathfrak{X}$ и $\Gamma(G_1) = \Gamma(G_2)$ всегда следует, что $G_2 \in \mathfrak{X}$.

Формации, распознающиеся Γ_H, описывает следующая теорема.

Теорема 1. *Пусть $\mathfrak{F}$ — формация и $\sigma(p) = \{q \,|\, (p,q) \in E(\Gamma_H(\mathfrak{F}))\}$. Формация $\mathfrak{F}$ распознаётся Γ_H тогда и только тогда, когда $\mathfrak{F} = LF(f)$, где $f(p) = \mathfrak{G}_{\sigma(p)}$ для $p \in \pi(\mathfrak{F})$ и $f(p) = \emptyset$ в противном случае.*

Напомним, что формация $\mathfrak{F}$ называется формацией с условием Шеметкова, если всякая минимальная не-$\mathfrak{F}$-группа является либо группой Шмидта, либо группой простого порядка.

Теорема 2. *Формация $\mathfrak{F}$ распознаётся Γ_{Nc} тогда и только тогда, когда $\mathfrak{F}$ — наследственная разрешимо насыщенная формация с условием Шеметкова.*

Следующая теорема устанавливает свойства наследственных формаций $\mathfrak{F}$, распознающихся $\mathfrak{F}_{\Gamma_s}$.

Теорема 3. *Пусть $\mathfrak{F}$ — наследственная формация. Если $\mathfrak{F}$ распознаётся Γ_s, то выполняются следующие утверждения:*
(a) $\Gamma_s(\mathfrak{F})$ — неориентированный граф.
(b) $\mathfrak{F}$ — разрешимо насыщенная формация с условием Шеметкова.

Напомним [8], что локальная формация $\mathfrak{F} = LF(F)$, где $F(p) = \mathfrak{S}_{\pi(F(p))}$ для $p \in \pi(\mathfrak{F})$ и $F(p) = \emptyset$ в противном случае, называется покрывающей формацией разрешимых групп, если $p \in \pi(F(p))$ и $p \in \pi(F(q))$ всегда влечет $q \in \pi(F(p))$ для всех $p, q \in \pi(\mathfrak{F})$. Как было показано в [8], всякая такая формация $\mathfrak{F}$ — наследственная насыщенная формация, содержащая всякую разрешимую группу G, все нормализаторы силовских подгрупп которой принадлежат $\mathfrak{F}$.

Теорема 4. *Пусть $\mathfrak{X}$ — класс групп такой, что $\Gamma_s(\mathfrak{X})$ — неориентированный граф. Тогда:*
(a) $\mathfrak{X}_{\Gamma_s} \cap \mathfrak{S}$ — наследственная формация;
(b) $\mathfrak{X}_{\Gamma_s} \cap \mathfrak{S}$ — покрывающая формация разрешимых групп.

Следствие 1. *Пусть $\mathfrak{F}$ — наследственная формация. Если $\mathfrak{F}$ распознаётся Γ_s, то выполняются следующие утверждения:*
(a) $\Gamma_s(\mathfrak{F})$ неориентирован.
(b) $\mathfrak{F}$ — разрешимо насыщенная формация с условием Шеметкова.
(c) $\mathfrak{F} \cap \mathfrak{S}$ — покрывающая формация в классе разрешимых групп.

Напомним, что группа называется дисперсивной, если найдётся линейный порядок ϕ на $\pi(G)$ такой, что если $\pi(G) = \{p_1, \ldots, p_n\}$, причем $p_i \leq_\phi p_j$ для $i < j$, то G имеет нормальные холловы $\{p_1, \ldots, p_i\}$-подгруппы для всех $i \leq n$. Хоукс [12] показал, что если $\Gamma_H(G)$ не имеет циклов, то группа G дисперсивна.

Теорема 5. *Пусть $\mathfrak{F}$ — класс групп. Если $\pi_1 \subseteq \pi(\mathfrak{F})$, $V(\Gamma_H(\mathfrak{F})) = \pi_1 \cup \pi_2$ и граф $\Gamma_H(\mathfrak{F})$ не имеет ребер, выходящих из π_1 в π_2, то всякая $\mathfrak{F}$-группа имеет нормальную холлову π_1-подгруппу.*

Следствие 2. *Пусть $\mathfrak{F}$ — класс групп, $V(\Gamma_H(\mathfrak{F})) = \pi_1 \cup \pi_2$, где $\pi_1 \cap \pi_2 = \emptyset$ и между π_1 и π_2 нет ребер в $\Gamma_H(\mathfrak{F})$. Тогда всякая группа из $\mathfrak{F}$ — прямое произведение холловых π_1-подгруппы и π_2-подгруппы.*

Теорема 6. *Пусть A, B и C — подгруппы разрешимой группы G, чьи индексы попарно взаимно просты в G. Тогда $\Gamma_H(G) = \Gamma_H(A) \cup \Gamma_H(B) \cup \Gamma_H(C)$.*

Отметим, что условие попарной взаимной простоты индексов не может быть опущено в теореме 6. Рассмотрим симметрическую группу степени 4. Она является произведе-

нием любых двух из следующих подгрупп: силовской 2-подгруппы, знакопеременной группы степени 4 и подгруппы, изоморфной симметрической группе степени 3. Объединение их графов Хоукса равно $\{(2,3),(3,2)\}$. Однако, графом Хоукса симметрической группы степени 4 является $\{(2,3),(3,2),(2,2)\}$.

Следствие 3. *Пусть формация $\mathfrak{F}$ распознаётся Γ_H и группа G содержит три разрешимые $\mathfrak{F}$-подгруппы A, B и C, чьи индексы попарно взаимно просты. Тогда $G \in \mathfrak{F}$.*

Из следствия 3 вытекает известная теорема Кегеля [4, с. 46]:

Следствие 4. *Если группа содержит три нильпотентные подгруппы с попарно взаимнопростыми индексами, то она нильпотентна.*

Следующий результат получен нами путем непосредственного нахождения N-критических графов минимальных простых групп.

Теорема 7. *Пусть G — группа. Если верно хотя бы одно из следующих утверждений, то G разрешима.*

(a) $\Gamma_{Nc}(G)$ не содержит циклов.

(b) Всякий цикл $\Gamma_{Nc}(G)$ не содержит ребра $(2,q)$, для любого $q \in \pi(2^p-1)$ и простого p.

(c) Всякий цикл $\Gamma_{Nc}(G)$ имеет длину, большую 3.

Отметим, что $\Gamma_{Nc}(G) \subseteq \Gamma_H(G)$ для любой группы G. Усилением упомянутой выше теоремы Хоукса является следующая

Теорема 8. *Если $\Gamma_{Nc}(G)$ не имеет циклов, то группа G дисперсивна.*

Литература

1. *Заварницин А. В.* О распознавании конечных групп по графу простых чисел // Алгебра и логика. 2006. Т. 45, № 4. С. 390—408.
2. *Кондратьев А. С.* О компонентах графа простых чисел конечных простых групп // Математический сборник. 1989. Т. 180, № 6. С. 787—797.
3. *Мазуров В. Д.* Распознавание конечных групп по множеству порядков их элементов // Алгебра и логика. 1998. Т. 37, № 6. С. 651—666.
4. *Шеметков Л. А.* Формации конечных групп. М. : Наука, 1978. 272 с.
5. *Ballester-Bolinches A., Cossey J.* Graphs, partitions and classes of groups // Monatsh. Math. 2012. Vol. 166, № 3–4. P. 309—318.
6. *Ballester-Bolinches A., Cossey J., Esteban-Romero R.* Graphs and classes of finite groups // Note Mat. 2013. Vol. 33, № 1. P. 89—94.
7. *Cayley A.* Desiderata and suggestions: No. 2. The Theory of groups: graphical representation // Amer. J. Math. 1878. Vol. 1 (2). P. 174—176.
8. *D'Aniello A., De Vivo C., Giordano G.* Saturated formations closed under Sylow normalizers // Comm. Algebra. 2005. Vol. 33. P. 2801—2805.
9. *D'Aniello A., De Vivo C., Giordano G.* Lattice formations and Sylow normalizers: a conjecture // Atti del Seminario Matematico e Fisico dell Universita di Modena e Reggio Emilia. 2007. № 55. P. 107—112.
10. *Diestel R.* Graph theory. Third edition. Springer-Verlag, 2005. 423 p.
11. *Doerk K., Hawkes T.* Finite soluble groups. Berlin, New York : Walter de Gruyter, 1992. 891 p.
12. *Hawkes T.* On the class of the Sylow tower groups // Math. Z. 1968. № 105. P. 393—398.
13. *Neumann B.* A problem of Paul Erdös on groups // J. Austral. Math. Soc. 1976. № 21. P. 467—472.
14. *Williams J. S.* Prime graph components of finite groups // J. Algebra. 1981. № 69. P. 487—513.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ОПРЕДЕЛЯЕМОСТЬ p-ЛОКАЛЬНЫХ ГРУПП ИХ КОЛЬЦАМИ РАСЩЕПЛЕНИЯ

С. В. Вершина (Москва)[1]

Группа A называется *p-локальной* относительно простого числа p, если она q-делима для всякого простого числа $q \neq p$. Подполе K поля p-адических чисел $\widehat{\mathbb{Q}}_p$ называется *полем расщепления* p-локальной группы без кручения A, если $R \otimes A \cong F \oplus D$, где $R = K \cap \widehat{\mathbb{Z}}_p$, $\widehat{\mathbb{Z}}_p$ — кольцо целых p-адических чисел, F — свободный R-модуль, D — делимый R-модуль. Кольцо R в этом случае называется *кольцом расщепления* для группы A. Если R — кольцо расщепления для группы A и $R \subset R_1$, где R_1 — кольцо, то R_1 также является кольцом расщепления для A. Поэтому кольцом расщепления группы A обычно называют минимальное кольцо расщепления группы A, то есть кольцо, не содержащее собственных колец расщепления группы A.

Каждая p-локальная группа без кручения конечного ранга обладает кольцом расщепления. Будем говорить, что группа A из класса $\mathcal{A}$ *определяется* в классе $\mathcal{A}$ своим кольцом расщепления, если для любой группы B из $\mathcal{A}$ из изоморфизма колец расщеплений групп A и B следует изоморфизм самих групп, $A \cong B$. Проблема определяемости p-локальной группы без кручения своим кольцом расщепления была поставлена в статье [1].

Единственными p-локальными группами без кручения ранга 1 являются аддитивные группы кольца $\mathbb{Z}_p$ и поля рациональных чисел $\mathbb{Q}$, для которых кольцом расщепления является кольцо $\mathbb{Z}_p$ рациональных чисел со знаменателями, не делящимися на простое число p. Неизоморфные группы A и $A \oplus A$ имеют также одно и то же кольцо расщепления. Поэтому естественно рассмотреть класс $\mathcal{A}$ p-локальных групп без кручения, которые являются неразложимыми ранга больше 1.

Теорема 1. *Для группы A класса $\mathcal{A}$ с квадратичным полем расщепления следующие условия эквивалентны:*

(1) *группа A в классе $\mathcal{A}$ определяется с точностью до изоморфизма своим кольцом расщепления;*
(2) *группа A изоморфна аддитивной группе кольца расщепления;*
(3) *кольцо расщепления группы A является E-кольцом.*

Следствие. *Любая неразложимая редуцированная p-локальная группа без кручения с квадратичным полем расщепления определяется с точностью до изоморфизма своим кольцом расщепления в классе неразложимых групп без кручения.*

Теорема 2. *Группа A класса $\mathcal{A}$ с кубическим полем расщепления определяется в классе $\mathcal{A}$ своим кольцом расщепления в том и только том случае, если группа A изоморфна аддитивной группе кольца расщепления.*

Данные теоремы относятся к проблеме, поставленной в статье [1].

Литература

1. *Glaz S., Vinsonhaler C., Wickless W.* Splitting rings for p-local torsion-free groups // Lecture Notes in Pure and Appl. Math. 1995. Vol. 171. P. 223—239.

 Получено 17.12.2017. УДК 512.541.

[1]Московский педагогический государственный университет. E-mail: svetlanavershina@gmail.com.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О ПОДНЯТИИ ЭЛЕМЕНТОВ ГРУППЫ ВЕЙЛЯ ТИПА E_6[1]

А. А. Гальт (Новосибирск)[2], А. М. Старолетов (Новосибирск)[3]

Пусть $\overline{G}$ — простая связная линейная алгебраическая группа над алгебраическим замыканием $\overline{F}_p$ конечного поля простого порядка p, σ — эндоморфизм Стейнберга и $\overline{T}$ — максимальный σ-инвариантный тор группы $\overline{G}$. Хорошо известно, что все максимальные торы сопряжены в $\overline{G}$ и факторгруппа $N_{\overline{G}}(\overline{T})/\overline{T}$ изоморфна группе Вейля W группы $\overline{G}$.

Пусть $w \in W$ и $\pi : N_{\overline{G}}(\overline{T}) \to W$ — канонический эпиморфизм. Следуя [1], будем обозначать порядок элемента g через $o(g)$ и положим

$$\tilde{o}(w) := \min_{g \in \pi^{-1}(w)} o(g).$$

В работе [1] сформулирована проблема о нахождении наименьшего порядка среди прообразов элементов группы Вейля в группе $N_{\overline{G}}(\overline{T})$. Нетрудно понять, что $\tilde{o}(w)$ равен $o(w)$ или $2o(w)$ для любого $w \in W$. Кроме того, если расширение $\overline{T}$ с помощью W расщепляемо, то $\tilde{o}(w) = o(w)$ для всех $w \in W$. Критерий расщепляемости этого расширения был получен независимо в [1] и в серии работ [2, 3, 4, 5]. В работе [1] также найдено значение $\tilde{o}(w)$ для так называемых эллиптических и регулярных элементов группы Вейля. Тем не менее, в общем случае вопрос остается открытым.

Пусть $O^{p'}(\overline{G}_\sigma) \leqslant G \leqslant \overline{G}_\sigma$ — конечная группа лиева типа, $T = \overline{T} \cap G$ — максимальный тор группы G и $N = N_{\overline{G}}(\overline{T}) \cap G$ — его алгебраический нормализатор. Известно, что G-классы σ-неподвижных максимальных торов группы $\overline{G}$ находятся во взаимно однозначном соответствии с классами σ-сопряженности W. Пусть класс сопряженности элемента w соответствует максимальному тору T. Авторами было доказано, что в случае группы лиева типа E_6 всегда найдется элемент $n \in \pi^{-1}(w) \cap N$, такой что $o(n) = o(w)$. В частности, доказана следующая

Теорема. *Пусть $\overline{G}$ — простая алгебраическая группа типа E_6 с группой Вейля W. Тогда для любого $w \in W$ верно $o(\tilde{w}) = o(w)$.*

Литература

1. *Adams J., He X.* Lifting of elements of Weyl groups // Journal of Algebra. 2017. Vol. 485. P. 142—165.
2. *Galt A. A.* On the splitting of the normalizer of a maximal torus in symplectic groups // Izvestiya: Mathematics. 2014. Vol. 78, № 3. P. 443—458.
3. *Galt A. A.* On splitting of the normalizer of a maximal torus in linear groups // Journal of Algebra and its Applications. 2015. Vol. 14, № 7. 1550114 (20 pages).
4. *Galt A. A.* On the splitting of the normalizer of a maximal torus in the exceptional linear algebraic groups // Izvestiya: Mathematics. 2017. Vol. 81, № 2. P. 269—285.
5. *Galt A. A.* On splitting of the normalizer of a maximal torus in orthogonal groups // Journal of Algebra and its Applications. 2017. Vol. 16, № 9. 1750174 (23 pages).

 Получено 26.12.2017. УДК 512.54

[1]Работа выполнена за счет гранта Российского научного фонда, проект № 14-21-00065.

[2]Институт математики им. С. Л. Соболева СО РАН. E-mail: galt@math.nsc.ru.

[3]Институт математики им. С. Л. Соболева СО РАН. E-mail: staroletov@math.nsc.ru.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ДВОЙСТВЕННОСТЬ В АБЕЛЕВЫХ МНОГООБРАЗИЯХ И ФОРМАЛЬНЫХ ГРУППАХ НАД ЛОКАЛЬНЫМИ ПОЛЯМИ

Н. М. Глазунов (Киев, Украина)[1]

Сообщение посвящено памяти Олега Николаевича Введенского (1937 — 1981 гг.). О. Н. Введенский был учеником академика И. Р. Шафаревича [1]. Исследования О. Н. и полученные им результаты связаны с двойственностью в эллиптических кривых (абелевых многообразий размерности 1) и с соответствующими когомологиями Галуа над локальными полями, со спариванием Шафаревича–Тэйта и с другими спариваниями, с локальной и квази-локальной теорией полей классов эллиптических кривых, с теорией коммутативных формальных групп над локальными полями [2, 3, 4, 5, 6, 7].

В предлагаемом сообщении мы планируем во введении дать краткий обзор избранных результатов, полученных О. Н. в направлении двойственности абелевых многообразий и формальных групп. Далее, в последующих разделах, представить над локальными и квази-локальными полями K, над их кольцами целых, и над их полями вычетов k аспекты, связанные (1) с формальной структурой абелевых многообразий, (2) с коммутативными формальными группами, (3) с соответствующими гомоморфизмами, изогениями и (4) с двойственностью. В этих рассмотрениях абелевы схемы и коммутативные формальные групповые схемы определены над локальными и квази-локальными полями, над их кольцами целых, и над их полями вычетов. Предполагается, что характеристика полей вычетов больше 3.

Следуя тематике конференции, мы обращаем внимание на алгорифмические аспекты этих конструкций.

Пусть S есть схема. Абелевой схемой над S называют S-групповую схему $A \to S$, которая собственная, плоская, конечно-представимая и которая имеет гладкие и связные геометрические слои. Известно, что следствием этих свойств является коммутативность абелевой схемы. При $S = Spec\ L$, где L — некоторое поле, получают определения абелева многообразия.

Пусть A — абелево многообразие над полем K с полем вычетов k, A_K — группа точек A, рациональных над K, $\overline{A}$ — многообразие Пикара многообразия A. Для случая алгебраически замкнутого k в [1] доказано, что группа главных однородных пространств над A двойственна фундаментальной группе $\pi_1(\overline{A}_K)$ проалгебраической группы $\overline{A}_K$ (исключая p-компоненты, где $p > 0$ — характеристика k).

Пополнение абелева многообразия как алгебраической группы совпадает с пополнением компоненты единицы алгебраической группы и является коммутативной формальной группой.

Далее рассматриваем только n-мерные аффинные формальные схемы в смысле Гротендика, конструируемые из колец $A = R[[X_1, ..., X_n]] = R[[X]]$ формальных степенных рядов от n переменных над коммутативным кольцом R с единицей. Морфизмы формальных схем (ФС) соответствуют непрерывным гомоморфизмам колец A. В категории ФС существует конечный объект $Spf\ R$ (кольцо R наделено дискретной топологией) и произведения, соответствующие пополненным тензорным произведениям колец A над R. Если $\phi : X \to Spf\ R$ — формальная схема, то формальная групповая схема (ФГС) над R определяется обычным способом заданием трех морфизмов: 1) $\mu : X \times_R X \to X$ (групповой закон), 2) $p : X \to X, p(x) = e$ (единица), 3) $i : X \to X$ (взятие обратного), удовлетворя-

 Получено 19.12.2017. УДК 513.6.

[1]Национальный авиационный университет. E-mail: glanm@yahoo.com.

ющих аксиомам: a) $\mu \circ (\mu \times 1) = \mu \circ (1 \times \mu)$ (ассоциативность), b) $\mu \circ (1, i) = (i, 1) \circ \mu$, c) $\mu \circ (1, p) = (p, 1) \circ \mu = 1$.

Определение 1. Формальным групповым законом от n переменных называется набор $F = (F_i)$ из n формальных степенных рядов $F_i \in R[[X, Y]]$ такой, что (i) $F(X, Y) \equiv X + Y (mod\, deg\, 2)$, (ii) $F(F(X, Y), Z) = F(X, F(Y, Z))$ (ассоциативность).

Групповой закон $F = (F_i)$ называют коммутативным, если выполнена аксиома $F(X, Y) = F(Y, X)$.

Определение 2. Пусть F и G соответственно n и m-мерные групповые законы над R. Набор φ из m формальных степенных рядов без свободных членов от n переменных $T = (T_1, ..., T_n)$ называется R-гомоморфизмом из F в G, если выполнено условие $\varphi \circ F = G \circ \varphi$. (Эта запись обозначает соответствующие подстановки наборов в наборы.) Множество всех R-гомоморфизмом из F в G будем обозначать через $Hom_R(F, G)$. Если $\varphi, \psi \in Hom_R(F, G)$, то можно определить их сумму $\varphi +_H \psi$, положив $(\varphi +_H \psi)(T) = G(\varphi(T), \psi(T))$.

Замечание. Операция $+_H$ задает на множестве $Hom_R(F, G)$ структуру абелевой группы.

Работа [4] продолжает начатое О. Н. Введенским [3] и другими построение аналога локальной и квази-локальной теории полей классов эллиптических кривых и абелевых многообразий. Представим кратко результаты работы [4] и их развитие. Пусть A — эллиптическая кривая одного из следующих 3-х типов, определенная над квази-локальным полем K: I. Инвариант Хассе редукции A отличен от нуля. II. A имеет мультипликативную редукцию. III. Инвариант Хассе редукции A нулевой. Пусть $\overline{F}_L$ проалгебраическая группа, определяемая (по максимальному идеалу кольца целых поля L и по формальной группе F, соответствующей A, или имеющую высоту редукции 3) на $Gal(L/K)$-модуле F_L, $\mathcal{D}_K^* = \bigcap_L N_{L/K}(\pi_1(\overline{F}_L))$ (пересечение по всем конечным расширениям Галуа L/K) — группа универсальных норм формальной группы F, соответствующей A, или формальной группы высоты редукции 3.

Теорема. $\mathcal{D}_K^* = 0$.

Доказательство теоремы основано на прямом вычислении действия норменного гомоморфизма $N_{L/K}$ на фильтрацию $\overline{F}_L$.

Пусть A_K — проалгебраическая группа точек A, рациональных над K, $\pi_1(A_K)$ — фундаментальная группа группы A_K, $\mathcal{D}_K = \bigcap_L N_{L/K}(\pi_1(A_L))$ — подгруппа универсальных норм в $\pi_1(A_K)$.

Следствие 1. $\mathcal{D}_K = 0$.

Следствие 2. *Существует эллиптическая кривая A типа III над квази-локальным полем K такая, что группа когомологий $H^1(Gal(L/K), A)$ бесконечна.*

О. Н. Введенским сформулирован ряд предположений об универсальных нормах и норменных подгруппах коммутативных формальных групп над K. Некоторые из этих предположений доказаны Н. М. Глазуновым и Г. Т. Коноваловым.

Литература

1. *Шафаревич И. Р.* Сочинения. Том 3. Часть 2. Москва, 1996. 637 с.
2. *Введенский О. Н.* Двойственность в эллиптических кривых над локальным полем. II // Известия АН СССР. Серия математическая. 1966. Т. 30, № 4. С. 891—922.
3. *Введенский О. Н.* О локальных "полях классов" эллиптических кривых // Известия АН СССР. Серия математическая. 1973. Т. 37, № 1. С. 20—88.
4. *Введенский О. Н.* О "универсальных нормах" формальных групп, определенных над кольцом локального поля // Известия АН СССР. Серия математическая. 1973. Т. 37, № 4. С. 737—751.
5. *Введенский О. Н.* О квази-локальных "полях классов" эллиптических кривых. I // Известия АН СССР. Серия математическая. 1976. Т. 40, № 5. С. 969—992.
6. *Введенский О. Н.* О спариваниях в эллиптических кривых над глобальными полями // Известия АН СССР. Серия математическая. 1978. Т. 42, № 2. С. 237—260.
7. *Введенский О. Н.* Эффект Артина в абелевых многообразиях. II // Известия АН СССР. Серия математическая. 1981. Т. 45, № 1. С. 23—46.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ПОСЛЕДОВАТЕЛЬНОСТИ КОЛЕЦ ЭНДОМОРФИЗМОВ АБЕЛЕВЫХ ГРУПП

А. В. Гришин (Москва)[1], Е. А. Тимошенко (Томск)[2], А. В. Царев (Москва)[3]

В последней редакции книги Л. Фукса «Абелевы группы», вышедшей в 2015 году [1], сформулирована следующая проблема.

Проблема 18.3. *Для группы A определим последовательность групп (A_n) по следующему правилу: $A_0 = A$ и $A_{n+1} = \operatorname{End} A_n$. На каком шаге может стабилизироваться эта последовательность?*

Напомним следующее важное определение.

Определение [2]**.** Абелева группа A называется E-группой, если она изоморфна своей группе эндоморфизмов, $A \cong \operatorname{End} A$, и ее кольцо эндоморфизмов $\mathsf{E}(A)$ коммутативное.

Получено частичное решение проблемы Фукса, а именно, доказаны следующие утверждения.

Теорема 1. *Пусть A — редуцированная абелева группа, все p-ранги которой конечны. Для последовательности (A_n) следующие условия равносильны:*

1) *$A_{i+1} \cong A_i$ хотя бы для одного i;*
2) *A_i является E-группой хотя бы для одного i;*
3) *$\mathsf{E}(A_i)$ — коммутативное кольцо хотя бы для одного $i \geqslant 1$;*
4) *$A_1 \cong A_2 \cong \ldots \cong A_n \cong \ldots$.*

Теорема 2. *Пусть последовательность (A_n) стабилизируется и содержит хотя бы одну нередуцированную группу. Тогда*

$$A \cong \mathbb{Q} \oplus \mathbb{Z}_m \quad \text{или} \quad A \cong \bigoplus_{p \in P} \mathbb{Z}_{p^{k_p}},$$

где $k_p \in \{\infty, 0, 1, 2, \ldots\}$ и хотя бы одно k_p равно ∞. В первом случае $A_0 \cong A_1$, во втором случае $A_0 \ncong A_1 \cong A_2$.

В заключениие отметим, что для рассмотренных абелевых групп последовательность (A_n) либо никогда не стабилизируется, либо стабилизируется не позднее члена A_1.

Литература

1. *Fuchs L.* Abelian groups. Springer International Publishing, 2015.
2. *Schultz P.* The endomorphism ring of the additive group of a ring // J. Austral. Math. Soc. 1973. Vol. 15, № 1. P. 60—69.

 Получено 19.10.2017. УДК 512.541.

[1]Московский педагогический государственный университет. E-mail: grishinaleksandr@yandex.ru.
[2]Томский государственный университет. E-mail: tea471@mail.tsu.ru.
[3]Московский педагогический государственный университет. E-mail: an-tsarev@yandex.ru.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ОБ ИДЕАЛАХ АССОЦИАТИВНЫХ АЛГЕБР, ПОРОЖДЁННЫХ КОММУТАТОРАМИ

Г. С. Дерябина (Москва)[1], А. Н. Красильников (Brasília, Brazil)[2]

Исследование лиевски нильпотентных ассоциативных алгебр было начато в 1947 году Дженнигсом [22] и с тех пор велось разными авторами с разных точек зрения, см., например, работы [3, 7, 9, 13, 21] и приведенную в них библиографию. Последние 10–15 лет такие алгебры привлекали повышенное внимание. Это было вызвано, с одной стороны, отрицательным решением в 1999 году проблемы Шпехта над полем простой характеристики А. Я. Беловым [2], А. В. Гришиным [5] и В. В. Щиголевым [10] и той ролью, которую алгебра Грассмана и другие лиевски нильпотентные класса 2 ассоциативные алгебры сыграли в этом решении, см. монографию [24], а также, например, работы [1, 6, 11] и приведенную там библиографию. С другой стороны, повышенный интерес к этим алгебрам был вызван появлением в 2007 году пионерской работы Б. Фейгина и Б. Шойхета [20] и последовавшей за ней серией работ П. Этингофа и других авторов, см. обзор [12], а также, например, работы [14, 16, 19, 23] и библиографию в них.

Пусть R — ассоциативное и коммутативное кольцо с единицей; пусть A — ассоциативная R-алгебра с единицей. Напомним, что левонормированный коммутатор $[a_1, a_2, \dots, a_n]$ $(a_i \in A)$ определяется рекурсивно: $[a_1, a_2] = a_1a_2 - a_2a_1$, $[a_1, \dots, a_{n-1}, a_n] = \big[[a_1, \dots, a_{n-1}], a_n\big]$ для любых $n > 2$, $a_i \in A$. Пусть $T^{(n)}(A)$ — двусторонний идеал в A, порождённый всеми коммутаторами $[a_1, \dots, a_n]$, где $a_i \in A$. Алгебра A называется лиевски нильпотентной класса не более $n-1$, если $[a_1, \dots, a_n] = 0$ для всех $a_i \in A$, то есть если $T^{(n)}(A) = 0$.

Пусть A — ассоциативная R-алгебра с единицей, порожденная (как алгебра с единицей) множеством X. Для исследования лиевски нильпотентной факторалгебры $A/T^{(n)}(A)$ важно знать «хорошее» (близкое к минимальному) порождающее множество идеала $T^{(n)}(A)$, которое, в частности, было бы конечным, если конечно множество X. Идеал $T^{(2)}(A)$, очевидно, порождается как двусторонний идеал в A всеми коммутаторами $[x_1, x_2]$ $(x_i \in X)$, которые образуют для него «хорошее» множество порождающих. «Хорошее» множество порождающих идеала $T^{(3)}(A)$ будет состоять из коммутаторов $[x_1, x_2, x_3]$ и элементов $[x_1, x_2][x_3, x_4] + [x_1, x_3][x_2, x_4]$, где $x_i \in X$ для всех i (В. Н. Латышев [8]).

Описание «хорошего» множества порождающих идеала $T^{(4)}(A)$ зависит от того, обратим или нет элемент 3 $(= 1 + 1 + 1)$ в R. Если $1/3 \in R$, то $T^{(4)}(A)$ порождается элементами

$$\begin{aligned} &[x_1, x_2, x_3, x_4] && (x_i \in X),\\ &[x_1, x_2][x_3, x_4, x_5] && (x_i \in X),\\ &\big([x_1, x_2][x_3, x_4] + [x_1, x_3][x_2, x_4]\big)[x_5, x_6] && (x_i \in X). \end{aligned} \tag{1}$$

Это было доказано в 1978 году И. Б. Воличенко [3] и позднее независимо переоткрыто в [4, 19]. Этот результат, вообще говоря, перестаёт быть верным, если $1/3 \notin R$ (например, если $R = \mathbb{Z}$), поскольку тогда, вообще говоря, $[x_1, x_2][x_3, x_4, x_5] \notin T^{(4)}(A)$, см. [25, Theorem 1.1].

Основным результатом нашего сообщения является следующая

 Получено 27.12.2017. УДК 512.552+512.572

[1]Московский государственный технический университет им. Н. Э. Баумана. E-mail: galina_deryabina@mail.ru.

[2]Universidade de Brasília. E-mail: alexei@unb.br.

Теорема 1. *Пусть R — произвольное ассоциативное и коммутативное кольцо с единицей, A — ассоциативная R-алгебра с единицей, порожденная множеством X. Тогда $T^{(4)}(A)$ порождается элементами*

$$[x_1, x_2, x_3, x_4] \qquad (x_i \in X), \tag{2}$$

$$[x_1, x_2][x_3, x_4, x_5] + [x_1, x_3][x_2, x_4, x_5] \qquad (x_i \in X), \tag{3}$$

$$\big([x_1, x_2][x_3, x_4] + [x_1, x_3][x_2, x_4]\big)[x_5, x_6] \qquad (x_i \in X). \tag{4}$$

Отметим,что идеал $T^{(4)}(A)$ содержит элементы $3[x_1, x_2][x_3, x_4, x_5]$ для всех $x_i \in X$ (см. [25, Theorem 1.1]), поэтому, если $1/3 \in R$, то $[x_1, x_2][x_3, x_4, x_5] \in T^{(4)}(A)$ $(x_i \in X)$. Ясно, что в этом случае порождающие идеала $T^{(4)}(A)$ вида (3) могут быть заменены на порождающие вида (1).

Замечание 1. В [17] было доказано, что над любым R идеал $T^{(4)}(A)$ порождается элементами (2)–(4) вместе с элементами

$$[x_1, x_2, x_3][x_4, x_5, x_6] \qquad (x_i \in X) \tag{5}$$

и

$$[x_1, x_2][x_3, x_4, x_5] + [x_1, x_5][x_3, x_4, x_2] \qquad (x_i \in X). \tag{6}$$

В теореме 1 мы доказываем, что элементы вида (5) и (6) лежат в идеале, порожденном элементами вида (2)–(4). Это легко сделать для элементов вида (6) и несколько сложнее — для элементов вида (5).

Замечание 2. В работе [15] было найдено «хорошее» порождающее множество для идеала $T^{(5)}(A)$ алгебры A над любым ассоциативным и коммутативным кольцом с единицей R. Это множество состоит из элементов 8 видов. С другой стороны, в [18] найдены различные «хорошие» порождающие множества идеала $T^{(n)}(A)$ для любого n при условии, что $1/3 \in R$.

Литература

1. *Белов А. Я.* Локальная конечная базируемость и локальная представимость многообразий ассоциативных колец // Известия РАН. Серия математическая. 2010. Т. 74, вып. 1. С. 3—134. DOI: 10.4213/im1122
2. *Белов А. Я.* О нешпехтовых многообразиях // Фундаментальная и прикладная математика. 1999. Т. 5, вып. 1. С. 47—-66.
3. *Воличенко И. Б.* T-идеал, порожденный элементом $[x_1, x_2, x_3, x_4]$. Минск: Ин-т матем. АН БССР. Препринт № 22. 1978. 13 с.
4. *Гордиенко А. С.* Коразмерности коммутатора длины 4 // Успехи математических наук. 2007. Т. 62, вып. 1. С. 191—192. DOI: 10.4213/rm5696
5. *Гришин А. В.* Примеры не конечной базируемости T-пространств и T-идеалов в характеристике 2 // Фундаментальная и прикладная математика. 1999. Т. 5, вып. 1. С. 101—118.
6. *Гришин А. В., Пчелинцев С. В.* Собственные центральные и ядерные многочлены относительно свободных ассоциативных алгебр с тождеством лиевой нильпотентности степени 5 и 6 // Математический сборник. 2016. Т. 207, № 12. С. 54—72. DOI: 10.4213/sm8652
7. *Красильников А. Н.* О полугрупповой и лиевской нильпотентности ассоциативных алгебр // Математические заметки. 1997. Т. 62, вып. 3. С. 510—519. DOI: 10.4213/mzm1634
8. *Латышев В. Н.* О выборе базы в одном T-идеале // Сибирский математический журнал. 1963. Т. 4, № 5. С. 1122—1127.
9. *Латышев В. Н.* О конечной порожденности T-идеала с элементом $[x_1, x_2, x_3, x_4]$ // Сибирский математический журнал. 1965. Т. 6, № 6. С. 1432—1434.
10. *Щиголев В. В.* Примеры бесконечно базируемых T-идеалов // Фундаментальная и прикладная математика. 1999. Т. 5, вып. 1. С. 307—312.
11. *Щиголев В. В.* Примеры бесконечно базируемых T-пространств // Математический сборник. 2000. Т. 191, № 3. С. 143—160. DOI: 10.4213/sm467
12. *Abughazalah N., Etingof P.* On properties of the lower central series of associative algebras // Journal of Algebra and its Applications. 2016. Vol. 15. 1650187 (24 pages). DOI: 10.1142/S0219498816501875
13. *Amberg B., Sysak Ya.* Associative rings whose adjoint semigroup is locally nilpotent // Archiv der Mathematik (Basel). 2001. Vol. 76. P. 426—435.
14. *Bhupatiraju S., Etingof P., Jordan D., Kuszmaul W., Li J.* Lower central series of a free associative algebra over the integers and finite fields // Journal of Algebra. 2012. Vol. 372. P. 251—274. DOI: 10.1016/j.jalgebra.2012.07.052

15. *da Costa E. A., Krasilnikov A.* Relations in universal Lie nilpotent associative algebras of class 4 // To appear in Communications in Algebra. DOI: 10.1080/00927872.2017.1347661
16. *Deryabina G., Krasilnikov A.* Products of commutators in a Lie nilpotent associative algebra // Journal of Algebra. 2017. Vol. 469. P. 84—95. DOI: 10.1016/j.jalgebra.2016.08.031
17. *Deryabina G., Krasilnikov A.* The torsion subgroup of the additive group of a Lie nilpotent associative ring of class 3 // Journal of Algebra. 2015. Vol. 428. P. 230—255. DOI: 10.1016/j.jalgebra.2015.01.009
18. *Dias Jr. C.W.G., Krasilnikov A.* On Lie nilpotent associative algebras // arXiv:1709.05728 [math.RA].
19. *Etingof P., Kim J., Ma X.* On universal Lie nilpotent associative algebras // Journal of Algebra. 2009. Vol. 321. P. 697—703. DOI: 10.1016/j.jalgebra.2008.09.042
20. *Feigin B., Shoikhet B.* On $[A, A]/[A, A, A]$ and on a W_n-action on the consecutive commutators of free associative algebras // Mathematical Research Letters. 2007. Vol. 14. P. 781—795. DOI: 10.4310/MRL.2007.v14.n5.a7
21. *Gupta N., Levin F.* On the Lie ideals of a ring // Journal of Algebra. 1983. Vol. 81. P. 225—231.
22. *Jennings S. A.* On rings whose associated Lie rings are nilpotent // Bulletin of the American Mathematical Society. 1947. Vol. 53. P. 593—597.
23. *Jordan D., Orem H.* An algebro-geometric construction of lower central series of associative algebras // International Mathematics Research Notices. 2015. Vol. 2015. № 15. P. 6330—6352. DOI: 10.1093/imrn/rnu125
24. *Kanel-Belov A., Karasik Ya., Rowen L. H.* Computational Aspects of Polynomial Identities: Volume l, Kemer's Theorems. Boca Raton, London, New York : CRC Press, 2016. 408 p.
25. *Krasilnikov A.* The additive group of a Lie nilpotent associative ring // Journal of Algebra. 2013. Vol. 392. P. 10—22. DOI: 10.1016/j.jalgebra.2013.06.021

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ОБ АЛГОРИТМИЧЕСКИХ ПРОБЛЕМАХ В ОБОБЩЕННЫХ ДРЕВЕСНЫХ СТРУКТУРАХ ГРУПП КОКСТЕРА

И. В. Добрынина (Тула)[1]

1. Введение

Рассмотрим конечно порожденную группу Кокстера, заданную копредставлением

$$G = \langle a_1, \ldots, a_n;\ (a_i a_j)^{m_{ij}}, i, j = \overline{1,n} \rangle,$$

где m_{ij} — элементы симметрической матрицы Кокстера: $m_{ii} = 1$, $m_{ij} \in \mathbb{N} \setminus \{1\} \cup \{\infty\}$, $i, j = \overline{1,n}$, $i \neq j$. В случае $m_{ij} = \infty$ определяющего соотношения между образующими a_i, a_j нет.

Если $m_{ij} > 3$, $i \neq j$, то G называется группой Кокстера экстрабольшого типа. Данный класс групп в 1983 году выделили К. Аппель и П. Шупп [7].

Построим для группы Кокстера G граф Γ такой, что образующим a_i поставим в соответствие вершины графа Γ, а каждому определяющему соотношению $(a_i a_j)^{m_{ij}} = 1$ — ребро, соединяющее a_i и a_j, $i \neq j$. Если при этом получится дерево-граф Γ, то группа G называется группой Кокстера с древесной структурой [5].

Группа Кокстера с древесной структурой может быть представлена как свободное произведение двупорожденных групп Кокстера, объединенных по конечным циклическим подгруппам: от графа Γ группы G перейдем к графу $\overline{\Gamma}$ так, что вершинам графа $\overline{\Gamma}$ поставим в соответствие группы Кокстера на двух образующих

$$G_{ij} = \langle a_i, a_j; a_i^2, a_j^2, (a_i a_j)^{m_{ij}} \rangle,$$

а всякому ребру $\overline{e}$, соединяющему вершины, соответствующие G_{ij} и G_{jk} — циклическую подгруппу $\langle a_j; a_j^2 \rangle$.

В группах Кокстера экстрабольшого типа и группах Кокстера с древесной структурой решены многие алгоритмические проблемы [2].

2. Основные теоремы

Рассмотрим группу Кокстера

$$G = \langle \prod_{s=1}^{t} * G_s; a_{i_m} = a_{j_l}, i \neq j, i, j \in \{\overline{1,t}\} \rangle,$$

представляющую собой древесное произведение групп Кокстера G_s, где G_s либо группа Кокстера с древесной структурой, либо группа Кокстера экстрабольшого типа, запись $a_{i_m} = a_{j_l}$ означает, что объединение групп Кокстера G_i и G_j ведется по циклической подгруппе второго порядка $\langle a_{i_m}; a_{i_m}^2 \rangle$ ($\langle a_{j_l}; a_{j_l}^2 \rangle$), где a_{i_m} — некоторый образующий группы G_i, a_{j_l} — некоторый образующий группы G_j. Такую группу Кокстера G будем называть обобщенной древесной структурой групп Кокстера.

Предложение. *Слово w обобщенной древесной структуры групп Кокстера G имеет конечный порядок тогда и только тогда, когда оно сопряжено с некоторым словом $w' \in G_{ij} = \langle a_i, a_j; (a_i a_j)^{m_{ij}}, a_i^2, a_j^2 \rangle$.*

 Получено 25.12.2017. УДК 519.4.

[1]Тульский государственный педагогический университет им. Л. Н. Толстого.
E-mail: dobrynirina@yandex.ru.

Теорема 1 [1]. *Пусть G — древесное произведение групп*

$$G = \left\langle \prod_{s=1}^{n} * G_s;\ \varphi_{ji}(U_{ij}) = U_{ji} \right\rangle,$$

объединенных по изоморфным подгруппам $U_{ij} < G$ и $U_{ji} < G$ с помощью фиксированного набора конструктивных изоморфизмов φ_{ij}: $\varphi_{ji}(U_{ij}) = U_{ji}$. Тогда, если подгруппы U_{ij} и U_{ji} обладают условием максимальности и в сомножителях разрешимы:

(1) *проблема вхождения;*
(2) *проблема пересечения классов смежности любой конечно порожденной подгруппы $H < G_i$ с подгруппой $U_{ij} < G_i$;*
(3) *существует алгоритм, выписывающий образующие пересечения любой конечно порожденной подгруппы $H < G_i$ с подгруппой $U_{ij} < G_i$,*

то в группе G разрешима проблема вхождения.

Группа Кокстера с древесной структурой, представленная в виде древесного произведения двупорожденных групп Кокстера, объединенных по конечным циклическим подгруппам удовлетворяет условиям данной теоремы. Таким образом, в данном классе групп разрешима проблема вхождения, в частности, проблема вхождения в циклическую подгруппу.

Разрешимость проблемы вхождения в циклическую подгруппу в группах Кокстера экстрабольшого типа следует из работы [6].

Теорема 2. *В обобщенных древесных структурах групп Кокстера разрешима проблема вхождения в циклическую подгруппу.*

Определение 1. Будем говорить, что в группе G разрешима проблема корня, если существует алгоритм, позволяющий для любого $w \in G$ установить, существуют ли $n \in \mathbb{N} \setminus \{1\}$ и $x \in G$ такие, что $x^n = w$.

Следствие. *В обобщенных древесных структурах групп Кокстера разрешима проблема корня.*

Определение 2. Будем говорить, что в группе G разрешима проблема степенной сопряженности слов, если существует алгоритм, позволяющий для любых слов $w, v \in G$ установить, существуют ли ненулевые целые числа n, m такие, что слова w^n, v^m сопряжены в группе G.

Теорема 3. *В обобщенных древесных структурах групп Кокстера разрешима проблема степенной сопряженности слов.*

Решение проблемы степенной сопряженности слов в группах Кокстера экстрабольшого типа получено в [3], в группах Кокстера с древесной структурой — в [4].

Литература

1. *Безверхний В. Н.* Решение проблемы вхождения в некоторых классах групп с одним определяющим соотношением // Алгоритмические проблемы теории групп и полугрупп. Тула: ТГПИ им. Л. Н. Толстого, 1986. С. 3—22.
2. *Безверхний В. Н., Безверхняя Н. Б., Добрынина И. В., Инченко О. В., Устян А. Е.* Об алгоритмических проблемах в группах Кокстера // Чебышевский сборник. 2016. Т. 17, № 4. С. 23—50.
3. *Безверхний В. Н., Добрынина И. В.* Решение проблемы степенной сопряженности слов в группах Кокстера экстрабольшого типа // Дискретная математика. 2008. Т. 20, № 3. С. 101—110.
4. *Безверхний В. Н., Инченко О. В.* Проблема степенной сопряженности слов в группах Кокстера с древесной структурой // Известия Тульского государственного университета. Серия Математика. Механика. Информатика. 2005. Т. 11. С. 63—75.
5. *Инченко О. В.* Проблемы равенства и сопряженности слов в группах Кокстера с древесной структурой // Чебышевский сборник. 2005. Т. 6, № 2. С. 81—90.
6. *Лысенок И. Г.* О некоторых алгоритмических свойствах гиперболических групп // Известия Академии наук СССР. Серия математическая. 1989. Т. 53, № 4. С. 814—832.
7. *Appel K., Schupp P.* Artins groups and infnite Coxter groups // Inventiones Mathematicae. 1983. Vol. 72, № 2. P. 201—220.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О СВОЙСТВАХ МНОЖЕСТВА $K_3(G)$ В НЕКОТОРЫХ КОНЕЧНЫХ ГРУППАХ

А. И. Забарина (Томск)[1], Е. А. Фомина (Томск)[2]

Как известно [2], при доказательстве классификационной теоремы конечных простых групп важную роль сыграло использование свойств централизатора инволюций.

В [3] изучены некоторые свойства конечных групп, каждая инволюция которых перестановочна ровно с двумя элементами группы.

Обратимся к элементам конечных групп, каждый из которых перестановочен ровно с тремя элементами группы.

Пусть G — произвольная конечная группа порядка n, $K_3(G) = \{x \in G \big| |C_G(x)| = 3\}$.

Доказаны следующие утверждения.

Предложение 1. $K_3(G) \neq \varnothing \Rightarrow (n \vdots 3 \wedge n \not\vdots 9)$.

Предложение 2. *$K_3(G)$ является инвариантным подмножеством G.*

Предложение 3. $K_3(G) \neq \varnothing \Rightarrow |K_3(G)| \in \left\{\frac{n}{3}, \frac{2n}{3}\right\}$.

Предложение 4. $|G| \not\vdots 2 \Rightarrow \left(K_3(G) = \varnothing \vee |K_3(G)| = \frac{2n}{3}\right)$.

Предложение 5. $K_3(S_n) \neq \varnothing \Leftrightarrow n \in \{3, 4\}; K_3(A_n) \neq \varnothing \Leftrightarrow n \in \{3, 4, 5\}$.

Предложение 6. $K_3(D_{2n}) = \varnothing$ *для всех* $n > 3$.

Предложение 7. *Пусть G — конечная нильпотентная группа,*

$$|G| = 3^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, k > 1.$$

Тогда $K_3(G) = \varnothing$.

Построен пример семейства разрешимых групп, в каждой из которых множество $K_3(G)$ не пусто.

Согласно предложению 1 во всех спорадических группах, за исключением J_1, множество $K_3(G)$ — пустое.

Предложение 8. *Пусть G — конечная простая группа, в которой $K_3(G) \neq \varnothing$. Тогда все инволюции G образуют один класс сопряжённых элементов.* [1]

Литература

1. *Белоногов В. А., Фомин А. Н.* Матричные представления в теории конечных групп. М. : Наука, 1976. 126 с.
2. *Горенстейн Д.* Конечные простые группы. Введение в их классификацию. М. : Мир, 1985. 352 с.
3. *Забарина А. И., Фомина Е. А., Гусельникова У. А.* О коммутирующих элементах группы // Вестник Томского государственного университета. Математика и механика. 2015. № 6 (38). С. 27—32.

 Получено 16.12.2017. УДК 512.542.

[1]Томский государственный педагогический университет. E-mail: aizabarina@gmail.com.

[2]Томский государственный педагогический университет. E-mail: ef254@mail.ru.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

СПЕЦИАЛЬНЫЕ ИНВАРИАНТНЫЕ ПСЕВДОХАРАКТЕРЫ НА СВОБОДНЫХ ГРУППАХ

Д. З. Каган (Москва)[1]

Данная работа посвящена решению вопроса о существовании нетривиальных псевдохарактеров на свободных группах, инвариантных относительно специального типа эндоморфизмов. В работах Р. И. Григорчука [2, 7] и В. Г. Бардакова [1] сформулированы условия существования нетривиальных псевдохарактеров на свободных произведениях с объединением и HNN-расширениях. В ряде работ также были получены обобщающие результаты о существовании псевдохарактеров и аналогичные результаты о бесконечности ширины вербальных подгрупп на различных свободных групповых конструкциях [3, 4, 5, 6].

В работах Р. И. Григорчука поставлен вопрос о существовании нетривиальных псевдохарактеров на HNN-расширениях в сложных случаях и связанный вопрос об псевдохарактерах свободных групп инвариантных относительно некоторых специальных типов их эндоморфизмов.

Определение 1. *Квазихарактером* на группе G называется вещественная функция f на G, удовлетворяющая следующему условию: существует положительное число ε, такое что $|f(ab) - f(a) - f(b)| \leq \varepsilon$ для любых элементов a, b из G.

Определение 2. *Псевдохарактером* на группе G называется функция f из G в R, удовлетворяющая двум условиям:

1) Функция f является квазихарактером, т. е. $|f(ab) - f(a) - f(b)| \leq \varepsilon$ для некоторого положительного числа ε и для любых элементов a, b группы G.

2) $f(x^n) = nf(x)$ для любого целого n и любых $a, b \in G$. Таким образом, псевдохарактер — это квазихарактер, который является обычным характером на циклических подгруппах.

Теорема. *Пусть* $F_n = < a_0, \ldots, a_{n-1} >$ *— свободная группа ранга* $n > 1$ *и отображение* α *определено преобразованиями порождающих:* $a_0 \to a_1, \ldots, a_{n-2} \to a_{n-1}, a_{n-1} \to W a_i^R W^{-1}$, *где* W *— неединичный элемент* F_n, R *— любое положительное число. Если несократимая запись* W *начинается порождающим* $a_0^{\pm 1}$, *то на свободной группе* F_n *существует нетривиальный псевдохарактер, инвариантный относительно отображения* α.

Литература

1. *Бардаков В. Г.* О ширине вербальных подгрупп некоторых свободных конструкций // Алгебра и логика. 1997. Т. 36, № 5. С. 494—517.
2. *Григорчук Р. И.* Ограниченные когомологии групповых конструкций // Математические заметки. 1996. Т. 59, № 4. С. 546—550.
3. *Добрынина И. В., Безверхний В. Н.* О ширине в некотором классе групп с двумя образующими и одним определяющим соотношением // Труды института математики и механики УрО РАН. 2001. Т. 7, № 2. С. 95—102.
4. *Каган Д. З.* Псевдохарактеры на аномальных произведениях локально индикабельных групп // Фундаментальная и прикладная математика. 2006. Т. 12, № 3. С. 55—64.
5. *Каган Д. З.* Нетривиальные псевдохарактеры на группах с одним определяющим соотношением и нетривиальным центром // Математический сборник. 2017. Т. 208, № 1. С. 80—96.
6. *Файзиев В. А.* Об устойчивости одного функционального уравнения на группах // Успехи математических наук. 1993. Т. 48, № 1. С. 193—194.
7. *Grigorchuk R. I.* Some results an bounded cohomology // In: Combinatorial and Geometric Group Theory. Edinburg 1993. (London Math. Soc. Lecture Notes Ser. Vol. 284.) Cambridge : Cambridge University Press, 1995. P. 111—163.

 Получено 25.12.2017. УДК 512.543.

[1]Российский университет транспорта, Российский университет дружбы народов.
E-mail: dmikagan@gmail.com.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ФАКТОРИЗАЦИИ И ТЕОРЕМЫ ТИПА СИЛОВА[1]

Л. С. Казарин (Ярославль)[2]

Группа $G = AB$ — произведение подгрупп A и B, если любой элемент $g \in G$ может быть представлен в виде $g = ab$. Группы такого вида называются факторизуемыми (подгруппами A и B). Одна из трудностей, встречающихся при исследовании факторизуемых групп, заключается в том, что нормальная подгруппа N факторизуемой группы $G = AB$ далеко не всегда обладает факторизацией. Однако в этом случае всегда имеется подгруппа $X(N)$, получившая название «факторизатор», для которой $X(N) = N(A \cap BN) = N(B \cap AN) = (A \cap BN)(B \cap AN)$, уже произведение трех перестановочных подгрупп. Такого рода группа называется *трифакторизуемой*.

Согласно одному из классических результатов О. Кегеля, конечная группа G, представимая в виде произведения трех попарно перестановочных подгрупп A, B и C с $AB = BC = AC = G$, где A и B нильпотентны (сверхразрешимы), будет нильпотентной (сверхразрешимой), если соответствующим свойством обладает и подгруппа C (см. [3]). Некоторые критерии π-отделимости трифакторизуемой группы для различных множеств простых чисел π были получены Пеннингтон [4]. Имеются различные обобщения результата Кегеля для случая, когда A и B нильпотентны, а C содержится в некоторой насыщенной формации $\mathfrak{F}$, содержащей все конечные нильпотентные группы (см. [1, Theorem 2.5.10]).

Используя классификацию конечных простых групп, Л. С. Казарин [2] доказал, что конечная группа G, представимая в виде $G = AB = AC = BC$, где A, B и C — разрешимые подгруппы, сама разрешима.

Пусть π — некоторое множество простых чисел, а π' — его дополнение во множестве всех простых чисел. Напомним, что π-разложимой называется группа, представимая в виде прямого произведения π-группы и π'-группы. Например, конечная нильпотентная группа будет π-разложимой для любого подмножества π множества простых чисел.

Аналогом подгруппы Силова в конечной группе G является холлова подгруппа. Это такая подгруппа S, что порядок ее делится только на простые числа из множества π, а индекс $|G : S|$ взаимно прост с каждым числом из π. В серии работ автор и его коллеги доказали, что произведение $G = AB$ двух π-разложимых подгрупп A и B имеет холлову π-подгруппу $A_\pi B_\pi$, где A_π и B_π — холловы π-подгруппы групп A и B, соответственно, при условии, что π является подмножеством нечетных простых чисел.

Если π — произвольное множество простых чисел, то группа G называется D_π-группой, если она имеет холлову π-подгруппу, все холловы π-подгруппы сопряжены в G и каждая π-подгруппа группы G содержится в некоторой холловой π-подгруппе группы G. То есть для G и множества π справедлив полный аналог теоремы Силова.

Совместно с А. Мартинес-Пастор и М. Д. Перес-Рамос автор получил следующую теорему

Теорема 1. *Пусть π — произвольное множество нечетных простых чисел. Если конечная группа $G = AB = AC = BC$ — произведение π-разложимых подгрупп A и B, а C является D_π-группой, то G также является D_π-группой.*

Заметим, что теорема Кегеля-Виланда о разрешимости произведения двух конечных нильпотентных групп является следствием упомянутой выше теоремы.

 Получено 14.01.2018. УДК 512.543.

[1]Работа выполнена при финансовой поддержке Ярославского гос.университета, проект ВИП № 008

[2]Ярославский государственный университет им. П. Г. Демидова. E-mail: lsk46@mail.ru.

В качестве непосредственного следствия теоремы 1 получаем

Теорема 2. *Пусть π — произвольное множество простых чисел. Если конечная группа $G = AB = AC = BC$ — произведение π-разложимых подгрупп A и B и C, то G также является π-разложимой группой.*

Литература

1. *Amberg B., Franciosi F., de Giovanni F.* Products of Groups. Oxford : Clarendon Press, 1992.
2. *Kazarin L. S.* Factorizations of finite groups by soluble subgroups // Ukr. Mat. J. 1991. Vol. 43, № 7. P. 883—886.
3. *Kegel O. H.* Zur Struktur mehrfach faktorisierter endlicher Gruppen // Math. Z. 1965. Vol. 87. P. 42—48.
4. *Pennington E.* Trifactorizable groups // Bull. Austral. Math. Soc. 1973. Vol. 8. P. 461—469.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

К ПРОБЛЕМЕ АЙЗЕКСА И ГОНГА О НОРМАЛИЗАТОРНОМ СВОЙСТВЕ КОРАДИКАЛОВ СУБНОРМАЛЬНЫХ ПОДГРУПП КОНЕЧНОЙ ГРУППЫ

С. Ф. Каморников (Гомель, Беларусь)[1]

В данной работе рассматриваются только конечные группы.

Пусть $\mathfrak{F}$ — непустая формация, т.е. класс групп, замкнутый относительно взятия гомоморфных образов и конечных подпрямых произведений. Тогда подгруппа $G^{\mathfrak{F}}$ группы G, равная пересечению всех тех нормальных подгрупп N из G, для которых $G/N \in \mathfrak{F}$, называется $\mathfrak{F}$-корадикалом группы G.

В [3] Гонг и Айзекс, исследуя свойства корадикалов конечных групп, показали, что если подгруппа M группы G нормализует нильпотентный (соответственно разрешимый) корадикал каждой несубнормальной подгруппы группы G, то M нормализует нильпотентный (соответственно разрешимый) корадикал любой подгруппы группы G. В [3] Гонг и Айзекс предположили, что если некоторая подгруппа группы нормализует сверхразрешимый корадикал каждой несубнормальной подгруппы этой группы, то она нормализует сверхразрешимый корадикал любой ее подгруппы.

В [1] получен положительный ответ на сформулированный вопрос. Более того, здесь показано, что аналогичное утверждение имеет место для любой наследственной насыщенной формации, имеющей полную характеристику.

Теорема. *Пусть $\mathfrak{F}$ — наследственная насыщенная формация, содержащая все нильпотентные группы. Если подгруппа M группы G нормализует $\mathfrak{F}$-корадикал $H^{\mathfrak{F}}$ каждой несубнормальной подгруппы H группы G, то M нормализует $\mathfrak{F}$-корадикал любой подгруппы группы G.*

Следствие. *Пусть $\mathfrak{F}$ — наследственная насыщенная формация, содержащая все нильпотентные группы. Если $\mathfrak{F}$-корадикал $H^{\mathfrak{F}}$ каждой несубнормальной подгруппы H группы G нормален в G, то $\mathfrak{F}$-корадикал любой подгруппы группы G нормален в G.*

Группа G из заключения следствия устроена достаточно просто. В частности, она имеет нильпотентный $\mathfrak{F}$-корадикал. Точное ее строение приводится в данной работе.

В теории классов групп предложенная Виландтом идея субнормальности как транзитивного замыкания нормальности нашла воплощение в понятиях $\mathfrak{F}$-субнормальная подгруппа и $\mathfrak{F}$-субнормальная в смысле Кегеля подгруппа.

Концепция $\mathfrak{F}$-субнормальной подгруппы предложена Картером и Хоуксом [2]. Пусть $\mathfrak{F}$ — непустой класс групп. Подгруппа H группы G называется $\mathfrak{F}$-субнормальной, если либо $H = G$, либо существует максимальная цепь подгрупп

$$H = H_0 \subset H_1 \subset \ldots \subset H_n = G$$

такая, что $H_i/Core_{H_i}(H_{i-1}) \in \mathfrak{F}$ для всех $i = 1, 2, \ldots, n$ (множество всех $\mathfrak{F}$-субнормальных подгрупп группы G обозначается $sn_{\mathfrak{F}}(G)$).

Простая проверка показывает, что, если $\mathfrak{N}$ — класс всех нильпотентных групп, то любая $\mathfrak{N}$-субнормальная подгруппа группы G является субнормальной. Более того, для разрешимой группы G справедливо равенство $sn_{\mathfrak{N}}(G) = sn(G)$.

 Получено 18.12.2017. УДК 512.542.

[1]Гомельский государственный университет им. Франциска Скорины. E-mail: sfkamornikov@mail.ru.

Другое понятие $\mathfrak{F}$-субнормальности, развивающее идею субнормальности, предложено Кегелем [4]. Если $\mathfrak{F}$ — непустой класс групп, то подгруппа H группы G называется $\mathfrak{F}$-субнормальной в смысле Кегеля, если существует цепь подгрупп

$$H = H_0 \subseteq H_1 \subseteq ... \subseteq H_n = G$$

такая, что либо подгруппа H_{i-1} нормальна в H_i, либо $H_i/Core_{H_i}(H_{i-1}) \in \mathfrak{F}$ для всех $i = 1$, $2, \ldots, n$ (множество всех K-$\mathfrak{F}$-субнормальных подгрупп группы G обозначается $sn_{K-\mathfrak{F}}(G)$).

Проверка показывает, что для любой группы G справедливо равенство $sn_{K-\mathfrak{N}}(G) = sn(G)$. В связи с этим по аналогии с приведенной теоремой для наследственной насыщенной формации $\mathfrak{F}$, содержащей все нильпотентные группы, возникает предположение, что если $\mathfrak{F}$-корадикал $H^{\mathfrak{F}}$ каждой не $\mathfrak{F}$-субнормальной (или каждой не $\mathfrak{F}$-субнормальной в смысле Кегеля) подгруппы H группы G нормален в G, то $\mathfrak{F}$-корадикал любой подгруппы группы G нормален в G. Однако это не так. Соответствующие примеры приводятся в данной работе.

Литература

1. *Ballester-Bolinches A., Kamornikov S. F., Meng H.* Normalisers of residuals of finite groups // Arch. Math. 2017. Vol. 109, № 4. P. 305—310.
2. *Carter R., Hawkes T.* The $\mathfrak{F}$-normalizers of a finite soluble group // J. Algebra. 1967. Vol. 5, № 2. P. 175—202.
3. *Gong L., Isaacs I. M.* Normalizers of nilpotent residuals // Arch. Math. 2017. Vol. 108, № 1. P. 1—7.
4. *Kegel O. H.* Untergruppenverbande endlicher Gruppen, die den Subnormalteilerverband echt enthalten // Arch. Math. 1978. Vol. 30, № 3. P. 225—228.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ВЕРБАЛЬНО ЗАМКНУТЫЕ ПОДГРУППЫ

А. А. Клячко (Москва)[1]

Теорема Мясникова–Романькова (2014) говорит, что

подгруппа H свободной конечно порождённой группы G является ретрактом тогда и только тогда, когда всякое уравнение вида $v(x, y, \dots) = h$ (где $h \in H$ и v — слово от $x^{\pm 1}$, $y^{\pm 1}$, $\dots$), имеющее решение в G, имеет решение в H.

В докладе будет рассказано о недавних результатах Андрея Мажуги, а также докладчика и Вероники Мирошниченко, обобщающих это утверждение. Например, оказалось, что аналог теоремы Мясникова–Романькова выполняется для любой свободной подгруппы H *любой* конечно порождённой группы G.

 Получено 14.02.2018. УДК 512.543

[1]Московский государственный университет им. М. В. Ломоносова. E-mail: klyachko@math.msu.su.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ДЛИНА РАСЩЕПЛЕНИЯ АБЕЛЕВЫХ MT-ГРУПП

Е. И. Компанцева (Москва)[1]

Длиной расщепления $l(G)$ абелевой группы G называется наименьшее натуральное число n такое, что группа $\bigotimes^n G = G \otimes \cdots \otimes G$ (n экземпляров) расщепляется. Если группа $\bigotimes^n G$ не расщепляется ни при каком натуральном n, то $l(G) = \infty$. Понятие длины расщепления абелевой группы было введено в [2].

В настоящей работе расматриваются вопросы, связанные с длиной расщепления MT-групп. Абелева группа G называется MT-группой, если любое умножение на периодической части $T(G)$ группы G однозначно продолжается до умножения на группе G. Умножением на абелевой группе G называется гомоморфизм $\mu : G \otimes G \to G$. Проблема описания MT-групп сформулирована в [4, стр. 34, проблема 38].

Все рассматриваемые группы — абелевы, и слово “группа” в дальнейшем означает “абелева группа”. Будем использовать следующие обозначения: $\mathbb{N}, \mathbb{N}_0$ — множества натуральных и целых неотрицательных чисел соответственно; если G — группа, то $T_p(G)$ — p-примарная компонента G, $\Lambda(G)$ — множество простых чисел p, для которых $T_p(G) \neq 0$; $h_p(g)$ — p-высота элемента $g \in G$.

Пусть G — группа, d — действвительное число, p — простое число. Согласно [5], элемент $g \in G$ удовлетворяет условию $(*)$ для d и p, если существует неубывающая неограниченная функция $f : \mathbb{N}_0 \to \mathbb{N}_0$ такая, что $h_p(p^i g) > d(i + f(i))$ для любого $i \in \mathbb{N}_0$. В [5] показано, что $l(G) \leq n$ тогда и только тогда, когда для любого $g \in G$ существует $k \in \mathbb{N}$ такое, что kg удовлетворяет условию $(*)$ для $\frac{n}{n-1}$ и любого $p \in \Lambda(G)$.

В [3] для группы G определены подмножества $G^{(n)}$ ($n \in \mathbb{N}$, $n \geq 2$) и G^* следующим образом: $G^{(n)} = \{g \in G \mid (\exists k \in \mathbb{N})\ kg$ удовлетворяет условию $(*)$ для $\frac{n}{n-1}$ и любого $p \in \Lambda(G)\}$, $G^* = \bigcup\limits_{n \geq 2} G^{(n)}$. Применяя это определение к $n = 1$, получим $G^{(1)} = \{g \in G \mid (\exists k \in \mathbb{N})$ $h_p(kg) = \infty$ при любом $p \in \Lambda(G)\}$. Если MT-группа не содержит ненулевой $\Lambda(G)$ — делимой подгруппы без кручения, то $G^{(1)}$ совпадает с $T(G)$. Показано, что G^* и $G^{(n)}$ — сервантные вполне характеристические подгруппы группы G; G/G^* и $G/G^{(n)}$ — группы без кручения при любом $n \in \mathbb{N}$. При этом $T(G) \leq G^{(1)} \leq G^{(2)} \leq \cdots$. Кроме того, $l(G) \leq n$ тогда и только тогда, когда $G = G^{(n)}$.

В [1] доказано, что если G — MT-группа и факторгруппа $G/T(G)$ не более чем счетна, то $l(G) \leq 3$. В настоящей работе этот результат из [5] обобщен следующим образом.

Теорема 1. *Если G — MT-группа и $G/G^{(n)}$ не более чем счетна ($n \in \mathbb{N}$), то*

$$G = G^{(2n+1)}.$$

Теорема 2. *Если G — MT-группа, то либо группа G/G^* несчетна, либо $G = G^*$.*

Результат теоремы 1 нельзя улучшить в том смысле, что для любого $n \in \mathbb{N}$ существует MT-группа G, для которой $G/G^{(n)}$ счетна и $G = G^{(2n+1)} \neq G^{(2n)}$.

 Получено 26.12.2017. УДК 512.541.

[1]Московский педагогический государственный университет;
Финансовый университет при Правительстве РФ. E-mail: kompantseva@yandex.ru.

Литература

1. *Москаленко А. И.* О длине расщепления абелевой группы // Математические заметки. 1978. Т. 24, № 6. С. 749—762.
2. *Irwin J. M., Khabbaz S. A., Rayna G.* Role of tensor product in splitting of abelian groups // J. Algebra. 1970. Vol. 14. P. 423—-442.
3. *Kompantseva E. I.* Absolute nil-ideals of an abelian group // J. Math. Sci. 2014. Vol. 197. P. 625—634.
4. Topics in abelian groups. Chicago, Ill. : Scott, Foresman, 1963.
5. *Toubassi E. H., Lawver D. A.* Height-slope and splitting length of abelian groups // Publs. Math. 1973. Vol. 20. P. 63—71.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ПОДГРУППА АВТОТОПИЗМОВ ПОЛУПОЛЕВОЙ ПЛОСКОСТИ, ИЗОМОРФНАЯ ЗНАКОПЕРЕМЕННОЙ ГРУППЕ A_5[1]

О. В. Кравцова (Красноярск)[2], Б. К. Дураков (Красноярск)[3]

Проективная плоскость называется полуполевой, если ее координатизирующее множество является полуполем (semifield). В частности, конечная проективная плоскость координатизируется полем тогда и только тогда, когда она дезаргова.

Известна гипотеза [4, с. 178] о разрешимости полной группы коллинеаций (автоморфизмов) всякой полуполевой недезарговой плоскости конечного порядка (см. также [1, вопрос 11.76, 1990 г.]). К настоящему моменту эта гипотеза подтверждена лишь для некоторых классов полуполевых плоскостей ([2], [3] и др.). Как доказано в [4] (с. 174), гипотеза о разрешимости полной группы автоморфизмов для недезарговой полуполевой плоскости редуцируется к разрешимости группы автотопизмов. Далее, если группа автотопизмов имеет нечетный порядок, то она разрешима по теореме Фейта–Томпсона. Поэтому при обсуждении вопроса о разрешимости следует рассматривать лишь полуполевые плоскости, допускающие автотопизмы порядка 2.

В предположении неразрешимости полной группы коллинеаций простые композиционные факторы должны быть изоморфны известным простым группам. Непосредственный перебор всех вариантов из списка простых неабелевых групп приводит к очень большому количеству исследований. Предлагается проверить существование подгруппы полной группы коллинеаций, изоморфной знакопеременной группе A_5 (подгруппе значительного количества простых неабелевых групп).

В случае нечетного порядка p^n ($p > 2$ простое) построено матричное представление регулярного множества полуполевой плоскости, допускающей подгруппу автотопизмов, изоморфную знакопеременной группе A_5. Выделена серия плоскостей, не допускающих A_5.

Теорема. *Полуполевая плоскость порядка p^n, где $p > 2$ — простое число и $p - 1$ является квадратом, не допускает подгруппы автотопизмов, изоморфной знакопеременной группе A_5.*

В случае четного порядка 2^n получен ряд технических результатов.

Литература

1. *Мазуров В. Д., Хухро Е. И.* Нерешенные вопросы теории групп. Коуровская тетрадь. Издание 16-е, дополненное, включающее архив решенных задач. Новосибирск, 2006.
2. *Подуфалов Н. Д., Дураков Б. К., Кравцова О. В., Дураков Е. Б.* О полуполевых плоскостях порядка 16^2 // Сибирский математический журнал. 1996. Т. 37, № 3. С. 616—623.
3. *Huang H., Johnson N. L.* 8 semifield planes of order 8^2 // Discrete Math. 1990. Vol. 80, № 1. P. 69—79.
4. *Hughes D. R., Piper F. C.* Projective planes. New York, Heldeberg, Berlin : Springer-Verlag, 1973.

 Получено 27.12.2017. УДК 519.145.

[1]Работа выполнена при финансовой поддержке РФФИ, проект № 16-01-00707.

[2]Сибирский федеральный университет. E-mail: ol71@bk.ru.

[3]Сибирский федеральный университет. E-mail: bkdurakov@gmail.com.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О ФИНИТНОЙ ОТДЕЛИМОСТИ ПОДГРУПП В РАСЩЕПЛЯЕМЫХ РАСШИРЕНИЯХ

А. А. Кряжева (Иваново)[1]

Расщепляемые расширения и их аппроксимационные свойства рассматривались в работах Мальцева А. И. [9] и Азарова Д. Н. [1—5]. В данном докладе рассматривается вопрос финитной отделимости подгрупп в расщепляемых расширениях.

Определение 1. Группа G называется расщепляемым расширением группы A с помощью группы B, если группа A является нормальной подгруппой группы G, B — подгруппа группы G, $G = AB$ и $A \cap B = 1$.

Определение 2. Подгруппа H группы G называется финитно отделимой [9], если для каждого элемента g группы G, не принадлежащего подгруппе H, существует гомоморфизм группы G на некоторую конечную группу, при котором образ элемента g не принадлежит образу подгруппы H.

Хорошо известна следующая теорема Аленби и Грегораса [10].

Теорема 1. *Пусть G — расщепляемое расширение конечно порожденной группы A с помощью группы B.*

1. *Если в группах A и B все подгруппы (все циклические подгруппы) финитно отделимы, то и в группе G все подгруппы (все циклические подгруппы) финитно отделимы.*
2. *Если в группе A все подгруппы финитно отделимы, а в группе B все конечно порожденные подгруппы финитно отделимы, то в группе G все конечно порожденные подгруппы финитно отделимы.*

Хорошо известно и легко проверяется, что прямое произведение двух свободных групп ранга 2 содержит неотделимую конечно порожденную подгруппу [10], поэтому пункт 2 нельзя сформулировать по аналогии с пунктом 1. Легко заметить, что первый пункт теоремы Аленби и Грегораса можно обратить, но второй пункт в таком виде обратить нельзя. Нам удалось получить необходимое и достаточное условие, при котором в группе G все конечно порожденные подгруппы финитно отделимы, а также обобщить теорему Аленби и Грегораса. Мы ослабляем условие конечной порожденности, накладываемое в этой теореме на базовую группу A, до следующего условия: для любого натурального числа n число всех подгрупп группы A индекса n конечно (см., напр., [7, с. 250]). Наш основной результат формулируется следующим образом.

Теорема 2. *Пусть G — расщепляемое расширение группы A с помощью группы B, и группа A удовлетворяет следующему условию: для любого натурального числа n число всех подгрупп группы A индекса n конечно. И пусть Ω — класс групп, замкнутый относительно факторизации и подгрупп конечного индекса. Тогда следующие два условия равносильны.*

1. *В группе G все Ω-подгруппы финитно отделимы.*
2. *В группах A и B все Ω-подгруппы финито отделимы, и сверх того, в группе A финитно отделимы все подгруппы, высекаемые в A Ω-подгруппами группы G.*

 Получено 10.01.2018. УДК 512.543.

[1]Ивановский государственный университет. E-mail: Stasia.07.10@mail.ru.

Так как класс всех конечно порожденных групп замкнут относительно подгрупп конечного индекса, то из теоремы 2 вытекает следующее утверждение.

Следствие 1. *Пусть G — расщепляемое расширение группы A с помощью группы B, и для любого натурального числа n число всех подгрупп группы A индекса n конечно. В группе G все конечно порожденные подгруппы финитно отделимы тогда и только тогда, когда в группах A и B все конечно порожденные подгруппы финитно отделимы, и в группе A финитно отделимы все подгруппы, высекаемые в A конечно порожденными подгруппами группы G. В частности, если в группе A все подгруппы финитно отделимы, а в группе B все конечно порожденные подгруппы финитно отделимы, то в группе G все конечно порожденные подгруппы финитно отделимы.*

Заметим, что пункт 2 теоремы Аленби и Грегораса является частным случаем следствия 1.

Сформулируем теперь еще один результат работы, который получается из теоремы 2 при более жестких ограничениях на класс Ω.

Теорема 3. *Пусть G — расщепляемое расширение группы A с помощью группы B, и группа A удовлетворяет условию: для любого натурального числа n число всех подгрупп группы A индекса n конечно. И пусть Ω — класс групп, замкнутый относительно факторизации и подгрупп. Тогда следующие два утверждения равносильны.*

1. *В группе G все Ω-подгруппы финитно отделимы.*
2. *В группах A и B все Ω-подгруппы финитно отделимы.*

Заметим, что теорема 3 может быть легко установлена с помощью теоремы 2. В самом деле, если Ω — класс групп, замкнутый относительно подгрупп, то п. 2 теоремы 2 равносилен п. 2 теоремы 3.

Так как классы всех групп, всех циклических групп, всех абелевых групп замкнуты относительно подгрупп и факторизации, то из теоремы 3 вытекает следующее утверждение.

Следствие 2. *Пусть G — расщепляемое расширение группы A с помощью группы B, и для любого натурального числа n число всех подгрупп группы A индекса n конечно. Тогда справедливы следующие утверждения.*

1. *В группе G все подгруппы финитно отделимы тогда и только тогда, когда в группах A и B все подгруппы финитно отделимы.*
2. *В группе G все циклические подгруппы финитно отделимы тогда и только тогда, когда в группах A и B все циклические подгруппы финитно отделимы.*
3. *В группе G все абелевы подгруппы финитно отделимы тогда и только тогда, когда в группах A и B все абелевы подгруппы финитно отделимы.*

Заметим, что следствие 2 является обобщением пункта 1 теоремы Аленби и Грегораса.

Еще одно обобщение теоремы Аленби и Грегораса получено Д. Н. Азаровым. В работе [6] он ослабил в этой теореме условие конечной порожденности группы A до требования конечности ее общего ранга (термин введен А. И. Мальцевым в работе [8]). Этот результат перекрывается теоремами 2 и 3, поскольку группа конечного общего ранга может содержать только конечное число подгрупп данного конечного индекса [1].

Литература

1. *Азаров Д. Н.* О группах конечного общего ранга // Вестник Ивановского государственного университета. Сер.: Биология, Химия, Физика, Математика. 2004. Вып. 3. С. 100—103.
2. *Азаров Д. Н., Чуракова Е. И.* Об аппроксимируемости конечными p-группами некоторых расщепляемых расширений // Вестник Ивановского государственного университета. Сер.: Естественные, общественные науки. 2009. Вып. 2. С. 68—71.
3. *Азаров Д. Н.* О почти аппроксимируемости конечными p-группами // Чебышевский сборник. 2010. Т. 11, вып. 3. С. 11—21.
4. *Азаров Д. Н.* Аппроксимационные свойства групп автоморфизмов и расщепляемых расширений // Известия вузов. Математика. 2015. № 8. С. 3—13.

5. *Азаров Д. Н.* Некоторые аппроксимационные свойства полициклических групп и расщепляемых расширений // Владикавказский математический журнал. 2015. Т. 17, № 4. С. 3—10.
6. *Азаров Д. Н.* О финитно аппроксимируемых группах конечного общего ранга // Математические заметки. 2017. Т. 101, № 3. С. 323—329.
7. *Курош А. Г.* Теория групп. М. : Наука, 1967.
8. *Мальцев А. И.* О группах конечного ранга // Математический сборник. 1948. Т. 22, № 2. С. 351—352.
9. *Мальцев А. И.* О гомоморфизмах на конечные группы // Ученые записки Ивановского государственного педагогического института. 1958. Т. 18, № 5. С. 49—60.
10. *Allenby R., Gregorac R.* On locally extended residually finite groups // Lecture Notes Math. 1973. Vol. 319. P. 9—17.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

НЕОБХОДИМЫЕ УСЛОВИЯ НИЛЬПОТЕНТНОЙ АППРОКСИМИРУЕМОСТИ ФУНДАМЕНТАЛЬНОЙ ГРУППЫ ГРАФА ГРУПП[1]

А. Е. Куваев (Иваново)[2]

Пусть Γ — некоторый ориентированный граф и $\bar{\Gamma}$ — неориентированный граф, который получается из Γ путём удаления ориентации рёбер. Будем говорить, что граф Γ *связен*, если связным является граф $\bar{\Gamma}$ (т. е. любые две вершины последнего соединяет как минимум один путь). Точно так же будем считать граф Γ *ациклическим*, если этим свойством обладает граф $\bar{\Gamma}$. Если e — ребро графа Γ, то через $e(1)$ и $e(-1)$ будем обозначать вершины графа Γ, являющиеся соответственно началом и концом ребра e.

Пусть $G = (V, E)$ — произвольный непустой связный ориентированный граф с множеством вершин V и совокупностью рёбер E (число вершин и рёбер не обязано быть конечным, допускаются кратные рёбра и петли). Сопоставив каждой вершине $v \in V$ некоторую группу F_v, каждому ребру $e \in E$ — группу H_e и вложения $\varphi_{+e}\colon H_e \to F_{e(1)}$, $\varphi_{-e}\colon H_e \to F_{e(-1)}$, получим *граф групп* $\mathcal{G}$, соответствующий графу G.

Пусть $T = (V, E_T)$ — некоторое максимальное поддерево графа G (т. е. связный ациклический подграф графа G, содержащий все его вершины). *Фундаментальной группой графа групп* $\mathcal{G}$ называется группа

$$F = \langle *F_v,\ t_f;\ H_e\varphi_{+e} = H_e\varphi_{-e},\ t_f^{-1}(H_f\varphi_{+f})t_f = H_f\varphi_{-f}\ (v \in V,\ e \in E_T,\ f \in E \setminus E_T)\rangle, \quad (1)$$

образующими которой являются образующие групп F_v $(v \in V)$ и буквы t_f $(f \in E \setminus E_T)$, а определяющими соотношениями — соотношения групп F_v, а также всевозможные соотношения вида

$$h\varphi_{+e} = h\varphi_{-e} \quad (e \in E_T,\ h \in H_e),$$
$$t_f^{-1}(h\varphi_{+f})t_f = h\varphi_{-f} \quad (f \in E \setminus E_T,\ h \in H_f).$$

Можно показать (см., напр., [5, глава 1, предложение 20]), что фундаментальная группа графа $\mathcal{G}$ не зависит от выбора дерева T.

Группу X будем называть *локально удовлетворяющей нетривиальному тождеству*, если каждая конечно порождённая подгруппа группы X удовлетворяет некоторому нетривиальному тождеству (не обязательно одному и тому же для всех подгрупп). Будем говорить, что группа X *локально аппроксимируется нильпотентными группами*, если любая её конечно порождённая подгруппа нильпотентно аппроксимируема. Напомним, что подгруппа Y группы X называется *p'-изолированной* в этой группе для некоторого простого числа p, если для каждого простого числа $q \neq p$ и для каждого элемента $x \in X$ из включения $x^q \in Y$ следует, что $x \in Y$. Основным результатом данной работы является

Теорема 1. *Пусть F — фундаментальная группа графа групп вида (1), каждая группа F_v $(v \in V)$ локально удовлетворяет нетривиальному тождеству и для любых $e \in E$, $\varepsilon = \pm 1$ подгруппа $H_e\varphi_{\varepsilon e}$ содержится в группе $F_{e(\varepsilon)}$ собственным образом. Если группа F локально аппроксимируется нильпотентными группами и для всякого ребра $e \in E_T$ хотя бы один из индексов $[F_{e(1)} : H_e\varphi_{+e}]$, $[F_{e(-1)} : H_e\varphi_{-e}]$ больше двух, то существует простое число p такое, что для каждого ребра $e \in E$ и для каждого числа $\varepsilon = \pm 1$ подгруппа $H_e\varphi_{\varepsilon e}$ p'-изолирована в группе $F_{e(\varepsilon)}$.*

 Получено 15.01.2018. УДК 512.543.

[1]Работа поддержана грантом Ивановского государственного университета.

[2]Ивановский государственный университет. E-mail: alexander@kuvaev.me.

Если граф G содержит всего одну вершину v и по крайней мере одно ребро, то группа F имеет представление

$$F = \langle F_v,\ t_f;\ t_f^{-1}(H_f\varphi_{+f})t_f = H_f\varphi_{-f}\ (f \in E)\rangle \tag{2}$$

и называется *HNN-расширением группы F_v с семейством проходных букв* $\{t_f \mid f \in E\}$.

Непосредственно из теоремы 1 вытекает приводимая далее теорема 2, обобщающая основные результаты работ [2] и [6].

Теорема 2. *Пусть F — HNN-расширение вида (2), группа F_v локально удовлетворяет нетривиальному тождеству и для любых $f \in E$, $\varepsilon = \pm 1$ подгруппа $H_f\varphi_{\varepsilon f}$ содержится в группе F_v собственным образом. Если группа F локально аппроксимируется нильпотентными группами, то существует простое число p такое, что для каждого ребра $f \in E$ и числа $\varepsilon = \pm 1$ подгруппа $H_f\varphi_{\varepsilon f}$ p'-изолирована в группе F_v.*

Если граф G является деревом, то группа F имеет представление

$$F = \langle *F_v;\ H_e\varphi_{+e} = H_e\varphi_{-e}\ (v \in V,\ e \in E)\rangle, \tag{3}$$

и называется *древесным произведением групп F_v $(v \in V)$ с объединёнными подгруппами $H_{\varepsilon e}$ $(e \in E,\ \varepsilon = \pm 1)$*. Пусть в дополнение к этому для любых двух рёбер $e, f \in E$ и для любых чисел $\varepsilon, \delta \in \{1, -1\}$ из равенства $e(\varepsilon) = f(\delta)$ вытекает, что $H_e\varphi_{\varepsilon e} = H_f\varphi_{\delta f}$. Тогда в группе F все подгруппы $H_e\varphi_{\varepsilon e}$ $(e \in E,\ \varepsilon = \pm 1)$ оказываются совпадающими и потому группу F называют *свободным произведением семейства групп $\{F_v \mid v \in V\}$ с одной объединённой подгруппой*.

Следующая теорема является обобщением основного результата статьи [1]. Отметим, что, в отличие от теоремы 1, в ней уже нет дополнительного ограничения на индексы, которые объединённая подгруппа имеет в свободных множителях.

Теорема 3. *Пусть F — свободное произведение семейства групп $\{F_v \mid v \in V\}$ с одной объединённой подгруппой H, все группы F_v локально удовлетворяют нетривиальному тождеству и отличны от H. Если группа F локально аппроксимируется нильпотентными группами, то существует простое число p такое, что подгруппа H p'-изолирована в группе F_v при любом $v \in V$.*

Приведенные теоремы в сочетании с полученным в [3, 4] описанием изоляторов подгрупп в нильпотентных и нильпотентно аппроксимируемых группах определенного вида, а также многочисленными результатами об аппроксимируемости свободных конструкций групп конечными p-группами могут послужить основой для отыскания критериев нильпотентной аппроксимируемости некоторых обобщенных свободных произведений и HNN-расширений нильпотентных и нильпотентно аппроксимируемых групп.

Литература

1. *Азаров Д. Н., Иванова Е. А.* К вопросу о нильпотентной аппроксимируемости свободного произведения с объединением локально нильпотентных групп // Научные труды Ивановского государственного университета. Математика. 1999. Вып. 2. С. 5—7.
2. *Савельичева Н. С., Соколов Е. В.* Одно необходимое условие нильпотентной аппроксимируемости HNN-расширения нильпотентной группы // Вестник Ивановского государственного университета. Сер.: Естественные, общественные науки. 2015. Вып. 1. С. 64—68.
3. *Соколов Е. В.* Об отделимости подгрупп нильпотентных групп в классе конечных π-групп // Сибирский математический журнал. 2014. Т. 55, № 6. С. 1381—1390.
4. *Соколов Е. В.* Об отделимости подгрупп нильпотентно аппроксимируемых групп в классе конечных π-групп // Сибирский математический журнал. 2017. Т. 58, № 1. С. 219—229.
5. *Serre J.-P.* Trees. Berlin : Springer–Verlag, 1980. 142 p.
6. *Sokolov E. V.* A necessary condition for the residual nilpotence of HNN-extensions // Lobachevskii Journal of Mathematics. 2018. Vol. 39, № 2. P. 281—285.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ОБ ОДНОЙ НОВОЙ НОТАЦИИ В ТЕОРИИ КВАЗИГРУПП

И. П. Мишутушкин (Москва)[1]

В теории квазигрупп, в дополнение к основной операции $A(x,y)$, добавляют производные операции $A^{-1}(x,y)$ — правого и ${}^{-1}A(x,y)$ — левого обращения [1]. Это дополнение послужило основой предлагаемого обобщения, в котором добавленные операции, в иной нотации, выступают в роли основных операций, распространяемых на все множество группоидов над общим конечным носителем. Такой подход оказался продуктивным для изучения свойств группоидов и, в частности, квазигрупп.

1. Кэлиан

Пусть множество A конечно, $|A| = n$, $G(A) = \{f \mid f : A^2 \to A\}$ множество бинарных операций на A. Элементы $G(A)$ будем называть группоидами.

Определение 1. *Универсальную алгебру*

$$C(A) =< G(A);\ \lambda,\ \rho,\ \tau,\ e_\lambda,\ e_\rho > \tag{1}$$

типа <2,2,1,0,0>, операции которой определены равенствами

$$(\forall f\,\forall g\,\forall x\,\forall y\,(f \in G(A),\ g \in G(A),\ x \in A,\ y \in A)):$$

$$f\lambda g(x,y) \underset{def}{=} g(f(x,y),y), \tag{2}$$

$$f\rho g(x,y) \underset{def}{=} f(x,\ g(x,y)), \tag{3}$$

$$f^\tau(x,y) \underset{def}{=} f(y,x), \tag{4}$$

$$\varepsilon_\lambda(x,y) \underset{def}{=} x, \tag{5}$$

$$\varepsilon_\rho(x,y) \underset{def}{=} y, \tag{6}$$

назовем кэлианом над множеством A.

Операции (2), (3) будем называть, соответственно, левым и правым, или λ- и ρ- умножением. Операцию, определенную равенством (4), назовем транспонированием. Группоиды (5), (6) назовем левой и правой или, соответственно, λ- и ρ- единицами.

На конечных группоидах введенные операции легко реализуются алгоритмически. Название алгебры обусловлено распространенным представлением конечных группоидов таблицами Кэли.

Определение 2. *Группоид $f^\lambda \in G(A)$, для которого $f\lambda f^\lambda = \varepsilon_\lambda$, назовем λ- (или лево-) обратным к f.*

Определение 3. *Группоид $f^\rho \in G(A)$, для которого $f^\rho\rho f = \varepsilon_\rho$, назовем ρ- (или право-) обратным к f.*

Определение 4. *Группоид $\alpha_\lambda(x,y)$, для которого $\forall y(y \in A) : \alpha_\lambda(x,y) = x\alpha$, назовем λ-подстановочным α группоидом.*

Определение 5. *Группоид $\alpha_\rho(x,y)$, для которого $\forall x(x \in A) : \alpha_\rho(x,y) = y\alpha$, назовем ρ-подстановочным α группоидом.*

 Получено 20.12.2017. УДК 512.5.

[1]ЗАО «АСТ». E-mail: lachika@bk.ru.

Обозначим: $G_\lambda(A)$ множество λ-обратимых группоидов, $G_\rho(A)$ множество ρ-обратимых группоидов, $\lambda(A)$, $\rho(A)$ множества λ и ρ подстановочных группоидов, $P =< P(A); \cdot >$ симметрическую полугруппу и $S =< S(A); \cdot >$ симметрическую группу подстановок элементов множества A, P^n, S^n — степени их прямых произведений.

Теорема 1. *Справедливы утверждения:*

(a) $< G(A); \lambda >$ *изоморфно* P^n,
(b) $< G(A); \rho >$ *антиизоморфно* P^n,
(c) $< G_\lambda(A); \lambda >$ *изоморфно* S^n,
(d) $< G_\rho(A); \rho >$ *антиизоморфно* S^n,
(e) $< \lambda(A); \lambda >$ *изоморфно* S,
(f) $< \rho(A); \rho >$ *антиизоморфно* S.

Следующие предложения отражают свойства операций кэлиана.

Теорема 2. $\forall f \forall g \forall u \forall v (f \in G(A), g \in G(A), u \in G(A), v \in G(A))$ *справедливы тождества* (7)–(12)*:*

(связи левого и правого умножений)

$$(f\lambda g)^\tau = g^\tau \rho f^\tau, \tag{7}$$

(двойного действия)

$$(f^\sigma)^\sigma = f, \quad \sigma \in \{\lambda, \rho, \tau\}, \tag{8}$$

(связи нейтральных элементов)

$$(\varepsilon_\lambda)^\tau = \varepsilon_\rho, \tag{9}$$

(поглощения)

$$\varepsilon_\lambda \rho f = \varepsilon_\lambda, \quad f\lambda\varepsilon_\rho = \varepsilon_\rho, \tag{10}$$

(парных сочетаний)

$$f^{\lambda\tau} = f^{\tau\rho} = f^{\rho\lambda}, \quad f^{\rho\tau} = f^{\tau\lambda} = f^{\lambda\rho}, \tag{11}$$

(дистрибутивности)

$$f\lambda g(u, v) = g(f\lambda u, f\lambda v), \quad f(u, v)\rho g = f(u\rho g, v\rho g). \tag{12}$$

Теорема 3. *Справедливы утверждения:*

(a) λ*-обратимый группоид есть группоид с правым сокращением,*
(b) ρ*-обратимый группоид есть группоид с левым сокращением.*

Кэлиан и его операции позволяют по-иному представить известные и обнаруживать новые свойства группоидов. Подтверждением этому является

Теорема 4 (о суперпозиции квазигрупп). $\forall f \forall u \forall v (f \in G(A), u \in Q(A), v \in Q(A)$, *где* $Q(A) = G_\lambda(A) \cap G_\rho(A)$ *— множество квазигрупп над* A*, справедливо:*

$$f(u, v) = u\lambda(f\rho(u^\lambda \lambda v)) = ((u\rho v^\rho)\lambda f)\rho v. \tag{13}$$

То есть, результат указанной суперпозиции в рамках кэлиана вычислим. Ниже приведены другие примеры продуктивного использования кэлиана и его операций.

2. Парастрофы

Пусть $\Pi = \{\varepsilon, \tau, \lambda, \rho\}$, и $f\psi$ — результат воздействия на квазигруппу $f \in Q(A)$ преобразования $\psi \in \Pi$, где ε — пустое преобразование: $f\varepsilon = f$. Группоид $P =< \Pi; \circ >$, операция которого задает последовательное выполнение пары преобразований из P, и для элементов которого, в соответствии с (8), (11), выполняется:

(a) $\sigma \circ \sigma = \sigma, \quad \sigma \in \Pi$,
(b) $\lambda \circ \tau = \tau \circ \rho = \rho \circ \lambda$,
(c) $\rho \circ \tau = \tau \circ \lambda = \lambda \circ \rho$,

изоморфен симметрической группе S_3. Каждая орбита действия P на $Q(A)$ объединяет семейство квазигрупп, образующих парастрофу.

3. Ортогональность

Квазигруппы f, g ортогональны, если множество пар $\{(f(x,y), g(x,y))|(x,y) \in A^2\}$ совпадает с декартовым квадратом множества A.

Теорема 5. *Для существования квазигруппы, ортогональной к $f \in Q(A)$, необходимо и достаточно, чтобы нашлась такая квазигруппа g, что*

$$f^{\lambda} \ \lambda \ g \ \in Q(A) \ \& \ g \ \rho \ f^{\rho} \ \in Q(A). \tag{14}$$

4. Бициклы

Определение 6. *Бициклом конечного группоида $< A; f >$ с правым сокращением называется последовательность элементов $a_0 = a, a_1 = b, a_2, ...,$ в которой $a_{t+2} = f(a_t, a_{t+1})$, $t = 0, 1, ...$*

Всякий группоид с правым сокращением представим бициклическим разложением — набором непересекающихся бициклов. Более подробные сведения о бициклах и их практическом использовании содержатся в [3].

Теорема 6. *Бицикл B группоида f с правым сокращением имеет вид*

$$B = (\varepsilon_{\lambda}, \varepsilon_{\rho}, f, f\lambda f^{\tau}, \cdots, a_m, \cdots), \tag{15}$$

где $a_{m+2} = f \ \lambda \ (a_m \ \rho \ f^{\tau})$.

Таким образом, бицикл, содержащий выбранный элемент в фиксированной позиции таблицы Кэли группоида f, можно получить, последовательно выписывая элементы той же позиции таблиц Кэли группоидов (15).

5. $C(A)$-многообразия

Пусть F — множество функциональных символов, X — множество обозначений переменных. Тождество $T = T(F, X)$ — правильно построенная формула (ППФ) с использованием F, X, задающая предикат типа равенства. Число различных переменных, используемых в записи тождества, назовем его рангом.

Кэлиан-тождеством назовем ППФ $T = T(S, \Phi)$, задающую предикат типа равенства, с использованием множества функциональных символов $S = \{\varepsilon_{\lambda}, \varepsilon_{\rho}, \tau, \lambda, \rho, \alpha_{\lambda}, \alpha_{\rho}\}$ и множества Φ символов переменных, в роли которых, при означивании, выступают элементы $G(A)$.

Определение 7. *Кэлиан- или $C(A)$-многообразием назовем множество $M(A)$ группоидов из $G(A)$, удовлетворяющих системе тождеств $T_1, \cdots, T_t$, истинных при любом означивании символов F элементами $M(A)$ и символов X элементами A.*

Теорема 7. *Система тождеств $T_i(F, X)$, ранги которых не превышают двух, любого $C(A)$-многообразия может быть заменена системой тождеств $T'_i(S, \Phi)$.*

Например, $C(A)$-многообразие идемпотентных группоидов задается $T(S, \Phi)$-тождеством $\varepsilon_{\rho} \ \lambda \ f = \varepsilon_{\rho}$.

Система $T(S, \Phi)$-тождеств $f = f^{\tau}$, $f = f^{\rho}$ задает $C(A)$-многообразие тотально-симметрических квазигрупп.

Литература

1. *Белоусов В. Д.* Основы теории квазигрупп и луп. М. : Мир, 1967.
2. *Мальцев А. И.* Алгебраические системы. М. : Наука, 1970.
3. *Мишутушкин И. П.* Об одной комбинаторной классификации конечных квазигрупп // Мальцевские чтения. Тезисы докладов международной научной конференции. Новосибирск, 21–25 мая 2016 г. Новосибирск : НГУ, 2016. С. 191.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ОБ ОДНОМ СЕМЕЙСТВЕ ГРУПП, ОПРЕДЕЛЯЕМЫХ ЕДИНСТВЕННЫМ СООТНОШЕНИЕМ[1]

Д. И. Молдаванский (Иваново)[2]

В данном сообщении приводится обзор известных результатов о свойствах групп вида

$$G(l,m;k)=\langle a,t;\ t^{-1}a^{-k}ta^{l}t^{-1}a^{k}t=a^{m}\rangle,$$

где l,m,k — произвольные целые числа, отличные от нуля, и формулируются некоторые вопросы, ответов на которые пока нет.

Поскольку группы $G(l,m;k)$, $G(l,m;-k)$, $G(-l,-m;k)$ и $G(m,l;k)$ попарно изоморфны, без потери общности можно считать, что $k>0$ и $|l|\geqslant m>0$; эти условия всюду ниже будут предполагаться выполненными. Заметим также, что применение очевидного преобразования Тице к представлению группы $G(l,m;k)$ показывает, что эта группа является HNN-расширением группы

$$H(l,m)=\langle a,b;\ b^{-1}a^{l}b=a^{m}\rangle,$$

принадлежащей семейству групп Баумслага–Солитэра [7], и это обстоятельство является существенным при работе с группами вида $G(l,m;k)$.

Началом систематического изучения групп этого семейства следует, по-видимому, считать работу А. М. Бруннера [8]. Впрочем, еще в 1969 году Г. Баумслаг [6] показал, что все конечные гомоморфные образы группы $G(2,1;1)$ являются циклическими группами, и тем самым привел пример группы с одним определяющим соотношением, не аппроксимируемой конечными группами и не входящей в упомянутое выше семейство групп Баумслага–Солитэра.

Исследования А. М. Бруннера были продолжены в работе [2] и ряде других, причем рассматривались как структурные свойства групп этого семейства, так и их аппроксимационные свойства.

В статье [2] при условии выполнимости неравенства $|l|>m$ были найдены порождающие и определяющие соотношения группы $\mathrm{Aut}(G)$ автоморфизмов группы $G=G(l,m;k)$; в статье [8] это было сделано в случаях, когда $m=1$ или m не делит l. Описания полученных представлений групп $\mathrm{Aut}\,(G)$ являются довольно громоздкими и требуют введения ряда обозначений. Здесь отметим лишь, что следствием этих результатов является утверждение о том, что группа $\mathrm{Aut}(G)$ является конечно порожденной в точности тогда, когда $m\nmid l$, причем если группа $\mathrm{Aut}(G)$ конечно порождена, то она является конечно определенной. О строении группы $\mathrm{Aut}(G)$ в случае $|l|=m$ ничего не известно.

Описание нехопфовых групп, принадлежащих рассматриваемому семейству, формулируется следующим образом:

Теорема 1 [2, теорема 3]**.** *Группа $G(l,m;k)$ не является хопфовой тогда и только тогда, когда $|l|>m>1$, число m является делителем чисел l и k и числа m и l/m взаимно просты.*

В статье [8] доказана (в теореме 3.4) достаточность этих условий.

Условия, при которых группы этого семейства изоморфны, рассматривались в работе [1]. А именно, в ней доказана

 Получено 15.01.2018. УДК 512.543.

[1]Работа выполнена при финансовой поддержке Минобрнауки России, проект № 1.8695.2017/8.9.

[2]Ивановский государственный университет. E-mail: moldav@mail.ru.

Теорема 2. *Справедливы следующие утверждения:*

(1) *Если группы* $G_1 = G(l_1, m_1; k_1)$ *и* $G_2 = G(l_2, m_2; k_2)$ *гомоморфно отображаются друг на друга и выполнено хотя бы одно из неравенств* $|l_1| > m_1$ *и* $|l_2| > m_2$, *то* $l_1 = l_2$ *и* $m_1 = m_2$.

(2) *Если* $|l| > m$, *то группы* $G_1 = G(l, m; k_1)$ *и* $G_2 = G(l, m; k_2)$ *изоморфны тогда и только тогда, когда выполнено одно из следующих условий:*

(2.1) $k_1 = k_2$;

(2.2) $m > 1$, *числа* k_1 *и* k_2 *делятся на наибольший общий делитель чисел* l *и* m *и* $k_1/k_2 = \pm(l/m)^p$ *для некоторого целого числа* $p \neq 0$;

(2.3) $m = 1$ *и частное* k_1/k_2 *является* l*-числом.*

(3) *Группы* $G_1 = G(l, m; k_1)$ *и* $G_2 = G(l, m; k_2)$ *гомоморфно отображаются друг на друга и не изоморфны тогда и только тогда, когда* $|l| > m > 1$ *и число* m *является делителем каждого из чисел* l, k_1 *и* k_2, *причем число* $s = l/m$ *взаимно просто с* m *и частное* k_1/k_2 *является* s*-числом, не совпадающим ни с какой степенью (с целочисленным показателем) числа* $\pm s$.

Утверждение пункта (3) теоремы 2 дает отрицательный ответ на сформулированный в [5] вопрос 3.33, будут ли изоморфны две группы, каждая из которых задается одним определяющим соотношением и является гомоморфным образом другой? Например, группы $G(18, 2; 2)$ и $G(18, 2; 6)$ не изоморфны и гомоморфно отображаются друг на друга.

Вопрос об условиях изоморфизма групп $G(l_1, m_1; k_1)$ и $G(l_2, m_2; k_2)$ в случае, когда $|l_1| = m_1$ и $|l_2| = m_2$, до сих пор остается открытым.

Переходя к изложению результатов, относящихся к аппроксимационным свойствам групп $G(l, m; k)$, приведем, прежде всего, критерий финитной аппроксимируемости таких групп (необходимость условия отмечена без доказательства в работе [8]).

Теорема 3 [2, теорема 1]**.** *Группа* $G(l, m; k)$ *является финитно аппроксимируемой тогда и только тогда, когда* $|l| = m$.

Оказалось, что финитно аппроксимируемые группы $G(l, m; k)$ обладают и другими аппроксимационными свойствами:

Теорема 4 [9, теорема 6.8]**.** *Следующие утверждения о группе* $G(l, m; k)$ *попарно равносильны:*

(1) $|l| = m$;

(2) *группа* $G(l, m; k)$ *финитно аппроксимируема относительно сопряженности;*

(3) *в группе* $G(l, m; k)$ *все циклические подгруппы финитно отделимы.*

Известно (см. [4, следствие 2]), что при $|l| = m$ в группе $H(l, m)$ все конечно порожденные подгруппы финитно отделимы. Естественно возникает вопрос о справедливости аналогичного утверждения для групп $G(l, m; k)$. Ответ на него неизвестен.

Критерий аппроксимируемости конечными p-группами групп рассматриваемого семейства доставляет

Теорема 5 [3, теорема 4]**.** *Группа* $G(l, m; k)$ *аппроксимируема конечными* p*-группами тогда и только тогда, когда* $|l| = m = p^r$ *и* $k = p^s$ *для некоторых целых чисел* $r \geqslant 0$ *и* $s \geqslant 0$, *причем если* $l = -m$, *то* $p = 2$ *и* $s \leqslant r$.

В случае, когда $l = m$, имеет место следующее обобщение утверждения теоремы 5.

Теорема 6. *Для любого множества* π *простых чисел группа* $G(m, m; k)$ *аппроксимируема конечными* π*-группами тогда и только тогда, когда* m *и* k *являются* π*-числами.*

В случае, когда $l = -m$, соответствующий критерий получить не удалось. Пока можно утверждать лишь, что если группа $G(-m, m; k)$ аппроксимируема конечными π-группами, то m и k являются π-числами и множество π содержит число 2.

Литература

1. *Борщев А. В., Молдаванский Д. И.* Об изоморфизме некоторых групп с одним определяющим соотношением // Математические заметки. 2006. Т. 79, № 1 С. 34—44.
2. *Кавуцкий М. А., Молдаванский Д. И.* Об одном классе групп с одним определяющим соотношением // Алгебраические и дискретные системы. Межвузовский сборник научных трудов. Иваново, 1988. С. 35—48.
3. *Молдаванский Д. И.* Аппроксимируемость конечными p-группами HNN-расширений // Вестник Ивановского государственного университета. Сер.: Биология, Химия, Физика, Математика. 2000. Вып. 3. С. 129—140.
4. *Молдаванский Д. И., Ускова А. А.* О финитной отделимости подгрупп обобщенных свободных произведений групп // Чебышевский сборник. 2013. Т. 14, вып. 3 (47). 2013. С. 92—98.
5. Нерешенные вопросы теории групп. Коуровская тетрадь. Изд. 18-е. Новосибирск, 2014.
6. *Baumslag G.* A noncyclic one-relator group all of whose finite quotients are cyclic // J. Austral. Math. Soc. 1969. Vol. 10, № 3—4. P. 497—498.
7. *Baumslag G., Solitar D.* Some two-generator one-relator non-Hopfian groups // Bull. Amer. Math. Soc. 1962. Vol. 68. P. 199—201.
8. *Brunner A. M.* On a class of one-relator groups // Can. J. Math. 1980. Vol. 50. P. 414—420.
9. *Kim G., Tang C. Y.* A criterion for the conjugacy separability of certain HNN extensions of groups // Journal of Algebra. 1999. Vol. 222. P. 574—594.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ГИПЕРЦЕНТРАЛЬНЫЕ И ФАКТОРИЗАЦИОННЫЕ СВОЙСТВА КОНЕЧНЫХ ГРУПП

В. И. Мурашко (Гомель, Беларусь)[1], А. Ф. Васильев (Гомель, Беларусь)[2]

Рассматриваются только конечные группы. Используются определения и обозначения из [9] и [15]. Одним из содержательных направлений теории групп является изучение структуры группы, представимой в произведение своих подгрупп, в зависимости от свойств сомножителей. К первым результатам данного направления относится знаменитая теорема Бернсайда о разрешимости бипримарных групп.

Во многих работах изучались формации групп, замкнутые относительно взятия произведений определённого типа подгрупп (произвольных [1], нормальных (субнормальных) [13], абнормальных и контранормальных [20] и т. д.). В последние годы активно проводятся исследования формаций, замкнутых относительно произведений обобщенно субнормальных подгрупп. Формации, замкнутые относительно произведений $\mathfrak{F}$-субнормальных подгрупп, изучались в работах [2, 6, 8] и др. Важную роль в этих исследованиях играют формации с условием Шеметкова, т. е. формации $\mathfrak{F}$, у которых всякая минимальная не $\mathfrak{F}$-группа является либо группой Шмидта, либо циклической группой простого порядка.

В 1938 Фиттинг [16] показал, что произведение двух нормальных нильпотентных подгрупп нильпотентно. Это означает, что во всякой группе существует единственная максимальная нормальная нильпотентная подгруппа $\mathrm{F}(G)$, называемая подгруппой Фиттинга. Данная подгруппа оказывает большое влияние на строение конечной разрешимой группы. В связи с этим в работе [5] авторами было введено следующее определение.

Определение 1. Подгруппа H группы G называется $\mathrm{F}(G)$-субнормальной, если H субнормальна в $H\mathrm{F}(G)$.

Пример 1. Очевидно, что всякая субнормальная подгруппа является $\mathrm{F}(G)$-субнормальной. Обратное утверждение неверно. Пусть $G \simeq S_4$ — симметрическая группа степени 4 и H — силовская 2-подгруппа G. Тогда H — максимальная подгруппа G и H не субнормальна в G. Заметим, что $\mathrm{F}(G) \subseteq H$. Таким образом, H — несубнормальная $\mathrm{F}(G)$-субнормальная подгруппа G.

Определение 2. Пусть $\mathfrak{F}$ и $\mathfrak{X}$ — классы разрешимых групп. Класс групп $\mathfrak{F}$ назовем $\mathrm{F}(G)$-радикальным в $\mathfrak{X}$, если $\mathfrak{F}$ содержит всякую $\mathfrak{X}$-группу $G = AB$, где A и B — $\mathrm{F}(G)$-субнормальные $\mathfrak{F}$-подгруппы G.

Определение 3. Класс групп $\mathfrak{X}$ называется S_{ch}-замкнутым, если $\mathfrak{X}$ вместе со всякой группой G содержит все её подгруппы Шмидта.

Теорема 1. *Пусть $\mathfrak{F}$ — S_{ch}-замкнутая насыщенная формация разрешимых групп и $\pi = \pi(\mathfrak{F})$. Следующие утверждения эквивалентны:*

(1) *$\mathfrak{F}$ $\mathrm{F}(G)$-радикальна в $\mathfrak{S}$;*

(2) *$\mathfrak{F}$ является наследственной формацией и существует разбиение $\sigma = \{\pi_i | i \in I\}$ множества простых чисел π на непересекающиеся подмножества такое, что $\mathfrak{F} = \underset{i\in I}{\times} \mathfrak{S}_{\pi_i}$.*

Следствие 1 [5]. *Пусть группа $G = AB$ — произведение нильпотентных $\mathrm{F}(G)$-субнормальных подгрупп. Тогда G нильпотентна.*

© Мурашко В. И., Васильев А. Ф., 2018. Получено 25.12.2017. УДК 512.542.

[1]Гомельский государственный университет им. Франциска Скорины. E-mail: mvimath@yandex.ru.

[2]Гомельский государственный университет им. Франциска Скорины. E-mail: formation56@mail.ru.

Следствие 2. *Пусть группа $G = AB$ — произведение нильпотентных подгрупп. Если $\mathrm{F}(G) \leq A \cap B$, то G нильпотентна.*

Следствие 3. *Пусть π — множество простых чисел и разрешимая группа $G = AB$ — произведение π-разложимых $\mathrm{F}(G)$-субнормальных подгрупп. Тогда G π-разложима.*

Замечание. Отметим, что класс групп $\underset{i\in I}{\times} \mathfrak{S}_{\pi_i} = (G \in \mathfrak{S} | G = O_{\pi_{i_1}}(G) \times \cdots \times O_{\pi_{i_n}}(G))$ является решеточной формацией. Напомним, что формация $\mathfrak{F}$ называется решеточной, если пересечение и порождение $\mathfrak{F}$-субнормальных подгрупп всегда является $\mathfrak{F}$-субнормальной подгруппой. Эти формации были изучены в [2].

Напомним [10, с. 127–128], что главный фактор H/K группы G называется $\mathfrak{F}$-*центральным*, если $H/K \rtimes G/C_G(H/K) \in \mathfrak{F}$. $\mathfrak{F}$-*гиперцентром* группы G называется наибольшая нормальная подгруппа G, все G-главные факторы ниже которой $\mathfrak{F}$-центральны в G. Обозначается $\mathrm{Z}_{\mathfrak{F}}(G)$. В частности, если $\mathfrak{F}$ — класс всех нильпотентных групп, то $\mathrm{Z}_{\mathfrak{F}}(G) = \mathrm{Z}_{\infty}(G)$ — гиперцентр группы G.

Теорема 2. *Пусть $\sigma = \{\pi_i | i \in I\}$ — разбиение множества простых чисел π на непересекающиеся подмножества, $\mathfrak{F} = \underset{i\in I}{\times} \mathfrak{S}_{\pi_i}$ и разрешимая группа $G = AB$, где A и B — $\mathfrak{F}$-подгруппы G. Тогда $(A \cap B)_G \leq \mathrm{Z}_{\mathfrak{F}}(G)$.*

Существуют примеры [21, с. 8] несверхразрешимых групп, являющихся произведением своих нормальных (субнормальных) сверхразрешимых подгрупп. С другой стороны, Бэр в [11] показал, что если группа G является произведением своих двух нормальных сверхразрешимых подгрупп и ее коммутант G' нильпотентен, то G сверхразрешима. В работе [3] было показано, что всякая насыщенная наследственная формация радикальна в классе всех групп с нильпотентным коммутантом.

Теорема 3. *Пусть $\mathfrak{X}$ — наследственная насыщенная формация разрешимых групп. Тогда следующие утверждения эквивалентны:*

(1) *Любая наследственная насыщенная формация $\mathfrak{F}$ $\mathrm{F}(G)$-радикальна в $\mathfrak{X}$.*

(2) *Всякая группа из $\mathfrak{X}$ имеет нильпотентный коммутант.*

Интересная информация о группах, факторизуемых своими $\mathrm{F}(G)$-субнормальными сверхразрешимыми подгруппами была получена в работе [4].

По известной теореме Дёрка [14] группа сверхразрешима, если она содержит четыре сверхразрешимые подгруппы с попарно взаимно простыми индексами. Этот результат был обобщен Крамером [19] на случай произвольной насыщенной формации метанильпотентных групп.

Теорема 4. *Пусть $\mathfrak{F}$ — насыщенная формация метанильпотентных групп. Тогда $\mathfrak{F}$ содержит всякую группу G, имеющую три $\mathrm{F}(G)$-субнормальные $\mathfrak{F}$-подгруппы попарно взаимно простых индексов в G.*

Следствие 4. *Пусть группа G, содержит три $\mathrm{F}(G)$-субнормальные подгруппы с нильпотентным коммутантом и попарно взаимно простыми индексами в G. Тогда коммутант G нильпотентен.*

Следствие 5. *Пусть группа G, содержит три $\mathrm{F}(G)$-субнормальные метанильпотентные подгруппы с попарно взаимно простыми индексами в G. Тогда группа G метанильпотентна.*

В работе [17] Флаверс и Вэкефилд исследовали группы с тремя сверхразрешимыми подгруппами попарно взаимно простых индексов. В частности, если такая группа имеет нильпотентный коммутант, то она сверхразрешима. Нахождению условий, при которых группа, имеющая три сверхразрешимые подгруппы с попарно взаимно простыми индексами, сверхразрешима, посвящена работа [12] Баллестера-Болинше и Эсквэйро. Отметим, что в двух приведенных выше работах рассматривались только индуктивные условия, т. е. условия, сохраняющиеся при переходе к подгруппам и факторгруппам. Легко проверить, что

свойство $\mathrm{F}(G)$-субнормальности в общем случае не переносится на подгруппы и на факторгруппы.

Следствие 6. *Пусть группа G, содержит три $\mathrm{F}(G)$-субнормальные сверхразрешимые подгруппы с попарно взаимно простыми индексами в G. Тогда группа G сверхразрешима.*

Фрисен [18] заметил, что если группа G есть произведение своих двух нормальных (субнормальных) сверхразрешимых подгрупп, имеющих взаимно простые индексы в ней, то она сверхразрешима. Однако, следующий пример показывает, что в теореме Фрисена условие субнормальности нельзя заменить на $\mathrm{F}(G)$-субнормальность.

Пример 2. Пусть G — группа, изоморфная симметрической группе степени 3. Тогда существует точный неприводимый G-модуль V над полем $\mathbb{F}_7$. Пусть T — полупрямое произведение V и G. Рассмотрим $A = VG_3$ и $B = VG_2$, где G_p — силовская p-подгруппа G и $p \in \{2, 3\}$. Так как $7 \equiv 1 \pmod{p}$ для $p \in \{2, 3\}$, то нетрудно видеть, что A и B сверхразрешимы. Так как V — точный неприводимый G-модуль, то $\mathrm{F}(T) = \mathrm{F}_7(T) = V$. Таким образом, A и B — $\mathrm{F}(T)$-субнормальные подгруппы T. Заметим, что $T = AB$, но $T/\mathrm{F}_7(T)$ не является абелевой группой. Поэтому, группа T несверхразрешима.

Аналогом теоремы 2 является следующая

Теорема 5. *Пусть $\mathfrak{F}$ — насыщенная формация метанильпотентных групп и группа G имеет три $\mathfrak{F}$-подгруппы A, B и C попарно взаимно простых индексов в G. Тогда $(A \cap B \cap C)_G \leq \mathrm{Z}_{\mathfrak{F}}(G)$.*

Литература

1. *Амберг Б., Казарин Л. С., Хефлинг Б.* Конечные группы с кратными факторизациями // Фундаментальная и прикладная математика. 1998. Т. 4, № 4. С. 1251—1263.
2. *Васильев А. Ф., Каморников С. Ф., Семенчук В. Н.* О решетках подгрупп конечных групп // Бесконечные группы и примыкающие алгебраические системы / Институт математики Академии наук Украины; редкол.: Н. С. Черников [и др.] Киев, 1993. С. 27—54.
3. *Васильев А. Ф., Симоненко Д. Н.* Относительно радикальные локальные формации // Известия Гомельского государственного университета имени Ф. Скорины. 2006. Т. 38, № 5. С. 19—25.
4. *Монахов В. С., Чирик И. К.* Конечные группы, факторизуемые субнормальными сверхразрешимыми подгруппами // Проблемы физики, математики и техники. 2016. № 3 (28). С. 40—46.
5. *Мурашко В. И., Васильев А. Ф.* О произведениях частично субнормальных подгрупп конечных групп // Веснік Віцебскага дзяржаўнага ўніверсітэта. 2012. Т. 70, № 4. С. 24—27.
6. *Семенчук В. Н.* Разрешимые $\mathfrak{F}$-радикальные формации // Математические заметки. 1996. Т. 59, № 2. С. 261—266.
7. *Семенчук В. Н.* Об одном классе наследственных насыщенных сверхрадикальных формаций // Сибирский математический журнал. 2014. Т. 55, № 1. С. 97—108.
8. *Семенчук В. Н., Шеметков Л. А.* Сверхрадикальные формации // Доклады НАН Беларуси. 2000. Т. 44, № 5. С. 24—26.
9. *Шеметков Л. А.* Формации конечных групп. М. : Наука, 1978. 272 с.
10. *Шеметков Л. А., Скиба А. Н.* Формации алгебраических систем. М. : Наука, 1989. 256 с.
11. *Baer R.* Classes of finite groups and their properties // Illinois J. Math. 1957. Vol. 1. P. 318—326.
12. *Ballester-Bolinches A., Ezquerro L. M.* Triple factorization and supersolubility of finite groups // Proc. of the Edinburg Math. Soc. 2016. Vol. 59, № 2. P. 301—309.
13. *Bryce R. A., Cossey J.* Fitting formations of finite soluble groups // Math. Z. 1972. Vol. 127, № 4. P. 217—223.
14. *Doerk K.* Minimal nicht überauflösbare, endliche Gruppen // Math. Z. 1966. Vol. 91, № 3. P. 198—205.
15. *Doerk K., Hawkes T.* Finite soluble groups. Berlin, New York : Walter de Gruyter, 1992. 891 p.
16. *Fitting H.* Beiträge zur Theorie der endlichen Gruppen // Jahresber. Deutsch. Math.-Verein. 1938. Vol. 48. P. 77—141.
17. *Flowers N., Wakefiels T. P.* On a group with three supersoluble subgroups of pairwise relatively prime indices // Arch. Math. 2010. Vol. 95. P. 309—315.
18. *Friesen D. K.* Products of normal supersolvable subgroups // Proc. Amer. Math. Soc. 1971. Vol. 30, № 1. P. 41—48.
19. *Kramer O. U.* Endliche Gruppen mit Untergruppen mit paarweise teilerfremden Indizes // Math. Z. 1974. Vol. 138, № 1. P. 63—68.
20. *Vasil'ev A. F.* On products of nonnormal subgroups of finite groups // Acta Applicandae Mathematicae. 2005. Vol. 85, № 1. P. 305—311.
21. *Weinstein M.* Between nilpotent and soluble. Passaic : Polygonal Publishing House, 1982. 231 p.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

КОЛЬЦА НА ФАКТОРНО ДЕЛИМЫХ АБЕЛЕВЫХ ГРУППАХ РАНГА 1

Чанг Тхи Куинь Нгуен (Москва)[1]

Кольцом на абелевой группе G называется кольцо, аддитивная группа которого совпадает с G. Если на абелевой группе G любое кольцо является коммутативным и ассоциативным, то G называется $SACR$-группой. Проблема изучения $SACR$-групп сформулирована в [1].

Настоящая работа посвящена изучению колец на факторно делимых абелевых группах. Абелева группа G называется факторно делимой, если она не содержит ненулевых делимых периодических подгрупп, но содержит свободную подгруппу F конечного ранга, такую что G/F — делимая периодическая группа. Факторно делимые абелевы группы без кручения были введены в [2]. В [3] понятие факторно делимой группы было обобщено на смешанные абелевые группы, там же показано, что категория факторно делимых групп с квазигомоморфизмами в качестве морфизмов двойственна категории абелевых групп без кручения конечного ранга с квазигомоморфизмами в качестве морфизмов. При изучении групп без кручения конечного ранга важную роль играют группы ранга 1. Учитывая, что двойственность У. Уиклесса — А. А. Фомина сохраняет ранг без кручения, изучение смешанных факторно делимых групп также должно основываться на исследовании смешанных факторно делимых групп ранга 1.

Теорема. *Любая факторно делимая абелева группа ранга 1 является $SACR$-группой.*

Литература

1. *Andruszkiewicz R. R., Woronowicz M.* On additive groups of associative and commutative rings // J. Quaest. Math. 2017. Vol. 40, № 4. P. 527—537.
2. *Beaumont R., Pierce R.* Torsion free rings // Illinois J. Math. 1961. № 5. P. 61—98.
3. *Fomin A. A., Wickless W.* Quotient divisible abelian groups // Proc. Amer. Math. Soc. 1998. Vol. 126, № 1. P. 45—52.

 Получено 23.12.2017. УДК 512.541.

[1]Московский педагогический государственный университет. E-mail: trangnguyen.ru@gmail.com.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

АППРОКСИМИРУЕМОСТЬ КОРНЕВЫМИ КЛАССАМИ HNN-РАСШИРЕНИЙ С ЦЕНТРАЛЬНЫМИ ЦИКЛИЧЕСКИМИ СВЯЗАННЫМИ ПОДГРУППАМИ[1]

Е. В. Соколов (Иваново)[2], Е. А. Туманова (Иваново)[3]

Напомним, что согласно [10] класс групп $\mathcal{R}$ называется корневым, если он замкнут относительно взятия подгрупп и прямых произведений конечного числа сомножителей, а также удовлетворяет условию Грюнберга: для любой группы X и для любой субнормальной последовательности $Z \leqslant Y \leqslant X$ с факторами из класса $\mathcal{R}$ найдется нормальная подгруппа T группы X, лежащая в Z и такая, что $X/T \in \mathcal{R}$. Данным определением удобно пользоваться при исследовании аппроксимируемости корневыми классами, однако оно не позволяет легко разграничить корневые и некорневые классы групп. Равносильные определения, упрощающие данную задачу, были получены в [13]. Подробнее о свойствах корневых классов и аппроксимируемости ими см. в [9].

До последнего времени имелось, по-видимому, лишь четыре статьи, в которых изучалась аппроксимируемость HNN-расширений произвольным нетривиальным (т. е. содержащим хотя бы одну неединичную группу) корневым классом групп $\mathcal{R}$. В [14] получено одно общее достаточное условие $\mathcal{R}$-аппроксимируемости HNN-расширения G и критерий $\mathcal{R}$-аппроксимируемости группы G при условии, что ее связанные подгруппы совпадают, а связывающий их изоморфизм является тождественным отображением. В [7] также рассматривается случай совпадающих связанных подгрупп, но уже без ограничений на связывающий изоморфизм. В [1] указано достаточное условие $\mathcal{R}$-аппроксимируемости HNN-расширения с центральными тривиально пересекающимися связанными подгруппами; здесь на класс $\mathcal{R}$ накладывается дополнительное требование замкнутости относительно взятия фактор-групп. Наконец, в [4] доказаны первые утверждения об аппроксимируемости HNN-расширений корневыми классами относительно сопряженности.

В данной работе исследуется вопрос об аппроксимируемости HNN-расширения, связанные подгруппы которого являются циклическими и лежат в центре базовой группы. Далее будем считать, что $\mathcal{R}$ — нетривиальный корневой класс групп, замкнутый относительно взятия фактор-групп; B — некоторая $\mathcal{R}$-аппроксимируемая группа; H и K — изоморфные циклические подгруппы группы B, лежащие в ее центре; $\varphi\colon H \to K$ — изоморфизм и G — HNN-расширение группы B с подгруппами H и K, связанными при помощи изоморфизма φ.

Если подгруппы H и K конечны и $L = H \cap K$, то поскольку в конечной циклической группе есть только одна подгруппа заданного порядка, имеет место равенство $L\varphi = L$. Таким образом, ограничение изоморфизма φ на подгруппу L является ее автоморфизмом. Порожденную им циклическую подгруппу группы $\operatorname{Aut} L$ обозначим через Φ.

Теорема 1. [6] *Пусть подгруппы H и K конечны, L и Φ определены, как и выше. Группа G $\mathcal{R}$-аппроксимируема тогда и только тогда, когда $\Phi \in \mathcal{R}$. В частности, если класс $\mathcal{R}$ содержит хотя бы одну непериодическую группу, то группа G $\mathcal{R}$-аппроксимируема.*

Непосредственно из теоремы 1 вытекает

 Получено 17.12.2017. УДК 512.543.

[1]Работа поддержана грантом Ивановского государственного университета. Договор № 141 от 01.01.2016.

[2]Ивановский государственный университет. E-mail: ev-sokolov@yandex.ru.

[3]Ивановский государственный университет. E-mail: helenfog@bk.ru.

Следствие 1. *Пусть подгруппы H и K конечны. Если группа B аппроксимируется разрешимыми группами (конечными разрешимыми группами), то и группа G аппроксимируется разрешимыми группами (соответственно конечными разрешимыми группами).*

Если B — бесконечная циклическая группа, критерий $\mathcal{R}$-аппроксимируемости HNN-расширения G известен [8]. Следующие три теоремы полностью решают вопрос об $\mathcal{R}$-аппроксимируемости группы G в случае, когда группа B не является циклической, а подгруппы H и K бесконечны.

Теорема 2. [6] *Пусть подгруппы H и K бесконечны. Если существует гомоморфизм группы B на группу из класса $\mathcal{R}$, инъективный на подгруппах H и K, то группа G $\mathcal{R}$-аппроксимируема.*

Теорема 3. [6] *Пусть подгруппы H и K бесконечны, $H \cap K \neq 1$ и не существует гомоморфизма группы B на группу из класса $\mathcal{R}$, инъективного на подгруппах H и K. Группа G $\mathcal{R}$-аппроксимируема тогда и только тогда, когда факторгруппы B/H и B/K $\mathcal{R}$-аппроксимируемы, $[H : H \cap K] = [K : H \cap K]$ и класс $\mathcal{R}$ содержит группу порядка 2, если только подгруппа $H \cap K$ не лежит в центре группы G.*

Теорема 4. [6] *Пусть подгруппы H и K бесконечны, $H \cap K = 1$ и не существует гомоморфизма группы B на группу из класса $\mathcal{R}$, инъективного на подгруппах H и K. Пусть также*

$$\Omega = \{N \trianglelefteq B \mid B/N \in \mathcal{R} \wedge \exists n \in \mathbb{Z}^+ \ N \cap HK = (HK)^n\}.$$

Группа G $\mathcal{R}$-аппроксимируема тогда и только тогда, когда подгруппы H и K отделимы семейством Ω, т. е.

$$\bigcap_{N\in\Omega} HN = H \quad \text{и} \quad \bigcap_{N\in\Omega} KN = K.$$

Описание семейства Ω и ответ на вопрос, отделимы ли им подгруппы H и K, для конкретных класса $\mathcal{R}$ и группы B могут оказаться непростой задачей. Потребовав в дополнение к предположениям теоремы 4, чтобы факторгруппа B/HK аппроксимировалась классом $\mathcal{R}$, удается доказать критерий $\mathcal{R}$-аппроксимируемости группы G (теорема 5), условия которого проверить легче. Однако, существуют примеры, показывающие, что $\mathcal{R}$-аппроксимируемость факторгруппы B/HK, вообще говоря, не является необходимым условием $\mathcal{R}$-аппроксимируемости группы G. Поэтому теорема 5 не может служить полной заменой теоремы 4.

Теорема 5. [6] *Пусть подгруппы H и K бесконечны, $H \cap K = 1$ и не существует гомоморфизма группы B на группу из класса $\mathcal{R}$, инъективного на подгруппах H и K. Если факторгруппа B/HK $\mathcal{R}$-аппроксимируема, то группа G $\mathcal{R}$-аппроксимируема тогда и только тогда, когда для каждого $m \geqslant 1$ найдется такое $n > m$, что факторгруппа $B/(HK)^n$ $\mathcal{R}$-аппроксимируема.*

Пусть π — непустое множество простых чисел. Абелеву группу будем называть π-ограниченной, если в каждой ее факторгруппе все компоненты периодической части, соответствующие числам из множества π, конечны. Нильпотентную (разрешимую) группу назовем π-ограниченной, если она обладает конечным центральным (соответственно субнормальным) рядом с π-ограниченными абелевыми факторами. Можно показать [3], что произвольный центральный (субнормальный) ряд π-ограниченной нильпотентной (соответственно разрешимой) группы имеет π-ограниченные абелевы факторы. В частности, нильпотентная группа π-ограничена тогда и только тогда, когда она является π-ограниченной разрешимой.

Отметим, что если π совпадает с множеством всех простых чисел, то π-ограниченная разрешимая группа оказывается ограниченной разрешимой в смысле А. И. Мальцева [2]. Очевидно также, что полициклические и конечно порожденные нильпотентные группы являются соответственно π-ограниченными разрешимыми и π-ограниченными нильпотентными при любом выборе множества π. Приводимые далее утверждения получаются из теорем 2—5 с использованием результатов работ [3, 5].

Следствие 2. *Пусть подгруппы H и K бесконечны. Если группа B является разрешимой $\mathcal{R}$-группой или аппроксимируется разрешимыми $\mathcal{R}$-группами без кручения, то группа G аппроксимируется разрешимыми $\mathcal{R}$-группами. Если группа B является ограниченной разрешимой $\mathcal{R}$-группой, то группа G аппроксимируется классом конечных разрешимых $\mathcal{R}$-групп тогда и только тогда, когда*

а) *фактор-группы $H/H \cap K$ и $K/H \cap K$ имеют одинаковые порядки;*

б) *класс $\mathcal{R}$ содержит группу порядка 2, если только подгруппа $H \cap K$ не лежит в центре группы G.*

Следствие 3. *Пусть подгруппы H и K бесконечны, класс $\mathcal{R}$ состоит лишь из периодических групп, $\pi(\mathcal{R})$ — множество всех простых делителей порядков элементов групп из класса $\mathcal{R}$, группа B является $\pi(\mathcal{R})$-ограниченной нильпотентной или аппроксимируется $\pi(\mathcal{R})$-ограниченными нильпотентными группами без кручения. Тогда приведенные далее утверждения равносильны.*

1. *Группа G аппроксимируется классом $\mathcal{R}$.*
2. *Группа G аппроксимируется классом конечных $\mathcal{R}$-групп.*
3. *Группа G аппроксимируется классом конечных разрешимых $\pi(\mathcal{R})$-групп.*
4. *Выполняются следующие условия:*
   а) *периодические части групп B, B/H и B/K являются $\pi(\mathcal{R})$-группами;*
   б) *фактор-группы $H/H \cap K$ и $K/H \cap K$ имеют одинаковые порядки;*
   в) *$2 \in \pi(\mathcal{R})$, если только подгруппа $H \cap K$ не лежит в центре группы G.*

Полученные результаты дополняют работу [1], а также ряд утверждений о финитной аппроксимируемости HNN-расширений с циклическими связанными подгруппами из [11, 12, 15].

Литература

1. *Гольцов Д. В.* Аппроксимируемость HNN-расширения с центральными связанными подгруппами корневым классом групп // Математические заметки. 2015. Т. 97, № 5. С. 665—669.
2. *Мальцев А. И.* О гомоморфизмах на конечные группы // Ученые записки Ивановского государственного педагогического института. 1958. Т. 18. С. 49—60.
3. *Соколов Е. В.* Об отделимости подгрупп нильпотентных групп в классе конечных π-групп // Сибирский математический журнал. 2014. Т. 55, № 6. С. 1381—1390.
4. *Соколов Е. В.* Об аппроксимируемости относительно сопряженности некоторых свободных конструкций групп корневыми классами конечных групп // Математические заметки. 2015. Т. 97, № 5. С. 767—780.
5. *Соколов Е. В.* Об отделимости подгрупп нильпотентно аппроксимируемых групп в классе конечных π-групп // Сибирский математический журнал. 2017. Т. 58, № 1. С. 219—229.
6. *Соколов Е. В., Туманова Е. А.* Аппроксимируемость корневыми классами HNN-расширений с центральными циклическими связанными подгруппами // Математические заметки. 2017. Т. 102, № 4. С. 597—612.
7. *Туманова Е. А.* Об аппроксимируемости корневыми классами HNN-расширений групп // Моделирование и анализ информационных систем. 2014. Т. 21, № 4. С. 148—180.
8. *Туманова Е. А.* Об аппроксимируемости корневыми классами групп Баумслага–Солитэра // Сибирский математический журнал. 2017. Т. 58, № 3. С. 700—709.
9. *Туманова Е. А.* Об аппроксимируемости корневыми классами некоторых древесных произведений с объединенными ретрактами // Алгебра и теория алгоритмов : Всероссийская конференция, посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета : сборник докладов. Иваново: Иван. гос. ун-т, 2018. С. 77—79.
10. *Gruenberg K. W.* Residual properties of infinite soluble groups // Proc. London Math. Soc. Ser. 3. 1957. Vol. 7. P. 29—62.
11. *Kim G., Tang C. Y.* Cyclic subgroup separability of HNN-extensions with cyclic associated subgroups // Can. Math. Bull. 1999. Vol. 42, № 3. P. 335—343.
12. *Rosenberger G., Sasse S. L.* Residual properties of HNN-extensions with cyclic associated subgroups // Algebra Colloq. 1996. Vol. 3, № 1. P. 91—96.
13. *Sokolov E. V.* A characterization of root classes of groups // Comm. Algebra. 2015. Vol. 43. P. 856—860.
14. *Tieudjo D.* On root-class residuality of some free constructions // JP J. Algebra, Number Theory and Appl. 2010. Vol. 18, № 2. P. 125—143.
15. *Wong K. B., Wong P. C.* Residual finiteness, subgroup separability and conjugacy separability of certain HNN extensions // Math. Slovaca. 2012. Vol. 62, № 5. P. 875—884.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ОБ АППРОКСИМИРУЕМОСТИ КОРНЕВЫМИ КЛАССАМИ НЕКОТОРЫХ ДРЕВЕСНЫХ ПРОИЗВЕДЕНИЙ С ОБЪЕДИНЕННЫМИ РЕТРАКТАМИ

Е. А. Туманова (Иваново)[1]

Напомним, что группа X называется *аппроксимируемой классом групп* $\mathcal{K}$ ($\mathcal{K}$-*аппроксимируемой*), если для каждого неединичного элемента $x \in X$ существует гомоморфизм группы X на некоторую группу из класса $\mathcal{K}$ ($\mathcal{K}$-группу), переводящий x в отличный от 1 элемент. В литературе чаще всего рассматривается свойство финитной аппроксимируемости (т. е. аппроксимируемости классом всех конечных групп), поскольку для конечно определенной группы, обладающей этим свойством, разрешима проблема тождества слов [8]. Изучается также аппроксимируемость конечными p-группами (где p — некоторое простое число), конечными π-группами (где π — непустое множество простых чисел), разрешимыми, нильпотентными и рядом других классов групп.

Поскольку при доказательстве аппроксимируемости одной и той же группы различными классами зачастую применяется схожая аргументация, естественным образом возникает желание провести возможно бóльшую часть рассуждений однократно, используя общие для всех этих классов свойства. Одним из первых данную идею реализовал К. Грюнберг [19], предложивший понятие корневого класса групп. Согласно [19] класс групп $\mathcal{K}$ называется *корневым*, если выполняются следующие три условия.

1. *Наследственность:* если группа X принадлежит классу $\mathcal{K}$ и Y — подгруппа группы X, то группа Y также принадлежит классу $\mathcal{K}$.
2. *Замкнутость относительно взятия прямых произведений конечного числа сомножителей:* прямое произведение любого конечного числа групп из класса $\mathcal{K}$ принадлежит классу $\mathcal{K}$.
3. *Условие Грюнберга:* если $1 \leqslant Z \leqslant Y \leqslant X$ — субнормальный ряд группы X такой, что фактор-группы X/Y и Y/Z принадлежат классу $\mathcal{K}$, то в группе X существует нормальная подгруппа T такая, что $T \subseteq Z$ и фактор-группа X/T принадлежит классу $\mathcal{K}$.

Нетрудно показать, что в этом определении второе условие вытекает из третьего и, таким образом, является излишним. Однако, остающееся без изменения условие Грюнберга не позволяет легко разграничить корневые и некорневые классы групп. Сделать это становится возможным благодаря работе [21], в которой доказано, что для произвольного наследственного класса групп $\mathcal{K}$ равносильны приводимые далее утверждения.

1. Класс $\mathcal{K}$ удовлетворяет условию Грюнберга (и, следовательно, является корневым).
2. Класс $\mathcal{K}$ замкнут относительно взятия декартовых сплетений.
3. Класс $\mathcal{K}$ замкнут относительно взятия расширений и вместе с любыми двумя группами X, Y содержит декартово произведение $\prod_{y \in Y} X_y$, где X_y — изоморфная копия группы X для каждого $y \in Y$.

Отсюда легко следует, что класс, состоящий лишь из конечных групп, является корневым тогда и только тогда, когда он замкнут относительно взятия подгрупп и расширений (этот факт был независимо установлен в [7]), и что пересечение любых двух корневых классов — снова корневой класс групп [21]. Нетрудно видеть также, что корневыми оказываются, например, классы всех разрешимых групп, конечных групп, периодических

 Получено 17.12.2017. УДК 512.543.

[1]Ивановский государственный университет. E-mail: helenfog@bk.ru.

π-групп ограниченного периода (напомним, что периодическая группа называется *π-группой* для некоторого множества простых чисел π, если все простые делители порядков ее элементов содержатся в π), класс всех групп без кручения. Класс всех нильпотентных групп не замкнут относительно взятия расширений и потому корневым не является.

В [1] было установлено, что каждая свободная группа аппроксимируется любым нетривиальным (т. е. содержащим хотя бы одну неединичную группу) корневым классом. В сочетании с результатами из [19] это утверждение позволило полностью решить вопрос об аппроксимируемости произвольным нетривиальным корневым классом (обычного) свободного произведения групп, а также послужило основой для исследований аппроксимируемости корневыми классами других свободных конструкций групп. За последние годы в указанном направлении было получено достаточно много результатов (см. [1—6, 9—16, 21, 22]). В настоящей работе также рассматривается вопрос об аппроксимируемости корневыми классами свободных конструкций групп, а именно свободного произведения двух групп с объединенной подгруппой и его обобщения — древесного произведения конечного семейства групп.

Напомним, что группа X представляет собой *расщепляемое расширение* группы Z при помощи группы Y, если Y — подгруппа группы X, Z — нормальная подгруппа группы X, $X = YZ$ и $Y \cap Z = 1$. О подгруппе Y в этом случае говорят, что она является *ретрактом* группы X, а естественный гомоморфизм группы X на фактор-группу X/Z называют *ретрактирующим*. Иначе говоря, подгруппа Y служит ретрактом X, если существует гомоморфизм группы X на группу Y, действующий на подгруппе Y тождественно.

Дж. Болер и Б. Эванс [18] установили, что свободное произведение двух финитно аппроксимируемых групп с объединенными ретрактами является финитно аппроксимируемой группой. Аналог данного утвржения для свойства аппроксимируемости классом всех конечных p-групп был доказан П. А. Бобровским и Е. В. Соколовым в [17]. Обобщением обоих этих утверждений служит

Теорема 1. [2] *Пусть $\mathcal{K}$ — нетривиальный корневой класс групп, G — свободное произведение некоторых групп A и B с подгруппами $H \leqslant A$ и $K \leqslant B$, объединенными относительно изоморфизма $\varphi\colon H \to K$. Если группы A и B $\mathcal{K}$-аппроксимируемы, подгруппа H является ретрактом группы A и подгруппа K является ретрактом группы B, то группа G $\mathcal{K}$-аппроксимируема.*

Теорема 1 была обобщена автором сразу в нескольких направлениях. В [13] доказано, что аналогичное утверждение имеет место для свободного произведения произвольного семейства групп с одной объединенной подгруппой. В [10] получены достаточные условия аппроксимируемости произвольным нетривиальным корневым классом обобщенного свободного произведения двух групп, в котором только одна из объединенных подгрупп является ретрактом соответствующего свободного множителя. В настоящей работе найдено еще одно обобщение теоремы 1, на этот раз на случай древесного произведения конечного семейства групп.

Напомним (см. [20]), что если T — некоторое неориентированное дерево (т. е. связный ациклический граф) с множеством вершин V и множеством ребер E, каждой вершине $v \in V$ сопоставлена группа G_v, а каждому ребру $\{u, v\} \in E$ — подгруппы $H_{uv} \leqslant G_u$, $H_{vu} \leqslant G_v$ и изоморфизмы $\varphi_{uv}\colon H_{uv} \to H_{vu}$, $\varphi_{vu}\colon H_{vu} \to H_{uv}$ такие, что $\varphi_{uv} = \varphi_{vu}^{-1}$, то *древесным произведением групп G_v ($v \in V$) с подгруппами H_{uv} ($\{u, v\} \in E$), объединенными относительно изоморфизмов φ_{uv} ($\{u, v\} \in E$)*, называется группа G, образующими которой являются образующие всех групп G_v ($v \in V$), а определяющими соотношениями — определяющие соотношения групп G_v ($v \in V$) и всевозможные соотношения вида $h = h\varphi_{uv}$ ($\{u, v\} \in E$, $h \in H_{uv}$). Имеет место

Теорема 2. *Пусть $\mathcal{K}$ — нетривиальный корневой класс групп, T — конечное неориентированное дерево с множеством вершин V и множеством ребер E, G — древесное произведение групп G_v ($v \in V$) с подгруппами H_{uv} ($\{u, v\} \in E$), объединенными относительно изоморфизмов φ_{uv} ($\{u, v\} \in E$). Если все группы G_v ($v \in V$) $\mathcal{K}$-аппроксимируемы и для каждого ребра $\{u, v\} \in E$ подгруппа H_{uv} является ретрактом группы G_u, а подгруппа H_{vu} — ретрактом группы G_v, то группа G $\mathcal{K}$-аппроксимируема.*

В действительности установлено, что если T — конечное неориентированное дерево с множеством вершин V и G — древесное произведение групп G_v ($v \in V$), то для каждой вершины $v \in V$ произвольный гомоморфизм группы G_v на некоторую группу X может быть продолжен до гомоморфизма всей группы G на X. В частности, всякий ретракт группы G_v является ретрактом группы G и потому теорема 2 получается из теоремы 1 индукцией по числу вершин в дереве T.

Литература

1. *Азаров Д. Н., Тъеджо Д.* Об аппроксимируемости свободного произведения групп с объединенной подгруппой корневым классом групп // Научные труды Ивановского государственного университета. Математика. 2002. Вып. 5. С. 6—10.
2. *Азаров Д. Н., Туманова Е. А.* Об аппроксимируемости обобщенных свободных произведений групп корневыми классами // Научные труды Ивановского государственного университета. Математика. 2008. Вып. 6. С. 29—42.
3. *Гольцов Д. В.* О почти аппроксимируемости корневыми классами обобщенных свободных произведений и HNN-расширений групп // Чебышевский сборник. 2013. Т. 14, вып. 3. С. 34—41.
4. *Гольцов Д. В.* Об аппроксимируемости корневыми классами свободных произведений групп // Вестник Ивановского государственного университета. Сер.: Естественные, общественные науки. 2014. Вып. 2. С. 87—90.
5. *Гольцов Д. В.* Аппроксимируемость HNN-расширения с центральными связанными подгруппами корневым классом групп // Математические заметки. 2015. Т. 97, № 5. С. 665—669.
6. *Гольцов Д. В.* Аппроксимируемость фундаментальной группы конечного графа групп корневым классом групп // Чебышевский сборник. 2016. Т. 17, вып. 3. С. 64—71.
7. *Гольцов Д. В., Яцкин Н. И.* Классы групп и подгрупповые топологии // Вестник Ивановского государственного университета. Сер.: Естественные, общественные науки. 2011. Вып. 2. С. 115—128.
8. *Мальцев А. И.* О гомоморфизмах на конечные группы // Ученые записки Ивановского государственного педагогического института. 1958. Т. 18. С. 49—60.
9. *Соколов Е. В.* Об аппроксимируемости относительно сопряженности некоторых свободных конструкций групп корневыми классами конечных групп // Математические заметки. 2015. Т. 97, № 5. С. 767—780.
10. *Соколов Е. В., Туманова Е. А.* Достаточные условия аппроксимируемости некоторых обобщенных свободных произведений корневыми классами групп // Сибирский математический журнал. 2016. Т. 57, № 1. С. 171—185.
11. *Соколов Е. В., Туманова Е. А.* Аппроксимируемость корневыми классами HNN-расширений с центральными циклическими связанными подгруппами // Математические заметки. 2017. Т. 102, № 4. С. 597—612.
12. *Туманова Е. А.* Некоторые условия аппроксимируемости корневыми классами групп обобщенных свободных произведений с нормальной объединенной подгруппой // Чебышевский сборник. 2013. Т. 14, вып. 3. С. 140—147.
13. *Туманова Е. А.* Об аппроксимируемости обобщенных свободных произведений корневыми классами групп // Моделирование и анализ информационных систем. 2013. Т. 20, № 1. С. 133—137.
14. *Туманова Е. А.* Об аппроксимируемости корневыми классами HNN-расширений групп // Моделирование и анализ информационных систем. 2014. Т. 21, № 4. С. 148—180.
15. *Туманова Е. А.* Об аппроксимируемости корневыми классами групп обобщенных свободных произведений с нормальным объединением // Известия вузов. Математика. 2015. № 10. С. 27—44.
16. *Туманова Е. А.* Об аппроксимируемости корневыми классами групп Баумслага–Солитэра // Сибирский математический журнал. 2017. Т. 58, № 3. С. 700—709.
17. *Bobrovskii P. A., Sokolov E. V.* The cyclic subgroup separability of certain generalized free products of two groups // Algebra Colloq. 2010. Vol. 17, № 4. P. 577—582.
18. *Boler J, Evans B.* The free product of residually finite groups amalgamated along retracts is residually finite // Proc. Amer. Math. Soc. 1973. Vol. 37, № 1. P. 50—52.
19. *Gruenberg K. W.* Residual properties of infinite soluble groups // Proc. London Math. Soc. Ser. 3. 1957. Vol. 7. P. 29—62.
20. *Karras A., Solitar D.* Subgroups of HNN groups and groups with one defining relations // Canadian J. Math. 1971. Vol. 23. P. 627—543.
21. *Sokolov E. V.* A characterization of root classes of groups // Comm. Algebra. 2015. Vol. 43. P. 856—860.
22. *Tieudjo D.* On root-class residuality of some free constructions // JP J. Algebra, Number Theory and Appl. 2010. Vol. 18, № 2. P. 125—143.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

КОНЕЧНЫЕ ГРУППЫ, ПРЕДСТАВИМЫЕ В ВИДЕ ПРОИЗВЕДЕНИЯ $\mathbb{P}$-СУБНОРМАЛЬНЫХ ПРОСТЫХ НЕАБЕЛЕВЫХ ГРУПП

В. Н. Тютянов (Гомель, Беларусь)[1]

Рассматриваются только конечные группы. В работе [4] Л. С. Казарин определил все неабелевы композиционные факторы конечной группы G, которая обладает рядом подгрупп $1 = X_0 \subset X_1 \subset \ldots \subset X_n = G$, где $|X_i : X_{i-1}|$ — простое число для всех $i = 1, \ldots, n$. Данная цепь начинается с единичной подгруппы X_0. Поэтому в [1] введено следующее естественное определение.

Определение. Подгруппа H группы G называется $\mathbb{P}$-субнормальной в G (обозначается $H\mathbb{P} - snG$), если либо $H = G$, либо существует цепь подгрупп $H = H_0 \subset H_1 \subset \ldots \subset H_{n-1} \subset H_n = G$ такая, что $|H_i : H_{i-1}|$ — простое число для всех $i = 1, \ldots n$.

Данное определение оказалось весьма полезным и неоднократно расширялось [3, 5]. Группам с системами подгрупп указаных выше типов посвящено достаточно много работ. В частности, в ряде из них изучалось строение факторизуемых групп с сомножителями данного вида [2, 5, 6]. Доказан следующий результат.

Теорема. *Пусть $G = AB$ — конечная группа, где A и B являются простыми неабелевыми группами, $\mathbb{P}$-субнормальными в группе G. Тогда $G = A \times B$.*

Литература

1. *Васильев А. Ф., Васильева Т. И., Тютянов В Н.* О конечных группах сверхразрешимого типа // Сибирский математический журнал. 2010. Т. 51, № 6. С. 1270—1281.
2. *Васильев А. Ф., Васильева Т. И., Тютянов В Н.* О произведениях $\mathbb{P}$-субнормальных подгрупп в конечных группах // Сибирский математический журнал. 2012. Т. 53, № 1. С. 59—67.
3. *Васильев А. Ф., Васильева Т. И., Тютянов В Н.* О К-$\mathbb{P}$-субнормальных подгруппах конечных групп // Математические заметки. 2014. Т. 95, № 4. С. 517—528.
4. *Казарин Л. С.* О группах с факторизацией // Доклады АН СССР. 1981. Т. 256, № 1. С. 26—29.
5. *Тютянов В. Н., Книгина В. Н.* Факторизации конечных групп r-разрешимыми подгруппами с заданными вложениями // Украинский математический журнал. 2014. Т. 66, № 10. С. 1431—1435.
6. *Monakhov V., Kniahina V.* Finite factorised groups with partially solvable $\mathbb{P}$-subnormal subgroups // Lobachevskii Journal of Mathematics. 2015. Vol. 36, № 4. P. 441—445.

 Получено 21.12.2017. УДК 512.542.

[1]Международный университет «МИТСО». E-mail: tyutyanov@front.ru.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ОБ АКСИОМАТИЧЕСКОМ РАНГЕ КЛАССА ЛЕВИ КВАЗИМНОГООБРАЗИЯ, ПОРОЖДЁННОГО КОНЕЧНОЙ P-ГРУППОЙ

С. А. Шахова (Барнаул)[1]

Для произвольного класса групп M обозначим через $L(M)$ класс всех групп G, в которых нормальное замыкание $(a)^G$ каждого элемента $a \in G$ принадлежит M. Класс $L(M)$ называется классом Леви, порождённым классом групп M.

А. И. Будкин установил в [1], что если M – квазимногообразие, то $L(M)$ также является квазимногообразием. Изучению классов Леви квазимногообразий нильпотентных групп посвящены работы [2—7]. В частности, в работе [7] возникли классы Леви квазимногообразий, порождённых конечными группами, заданные бесконечными системами квазитождеств.

Совокупность квазитождеств, задающих квазимногообразие, называется базисом этого квазимногообразия. Говорят, что квазимногообразие имеет бесконечный аксиоматический ранг, если его нельзя задать базисом от конечного числа переменных.

Зафиксируем простое число p, $p \neq 2$, и обозначим через F_2 свободную в многообразии нильпотентных ступени ≤ 2 групп экспоненты p группу ранга 2, а через $F_2 \wr G$ прямое сплетение группы F_2 с группой G. Доказана следующая теорема.

Теорема. *Для произвольной конечной p-группы G класс Леви $L(qF_2 \wr G)$ имеет бесконечный аксиоматический ранг.*

Литература

1. *Будкин А. И.* Квазимногообразия Леви // Сибирский математический журнал. 1999. Т. 40, № 2. С. 266—270.
2. *Будкин А. И.* О классах Леви, порождённых нильпотентными группами // Алгебра и логика. 2000. Т. 39, № 6. С. 635—647.
3. *Будкин А. И., Таранина Л. В.* О квазимногообразиях Леви, порождённых нильпотентными группами // Сибирский математический журнал. 2000. Т. 41, № 2. С. 270—277.
4. *Лодейщикова В. В.* О квазимногообразиях Леви, порождённых нильпотентными группами // Известия Алтайского государственного университета. 2009. Т. 61, № 1. С. 26—29.
5. *Лодейщикова В. В.* Об одном квазимногообразии Леви экспоненты 8 // Известия Алтайского государственного университета. 2010. Т. 65, № 1/2. С. 42—45.
6. *Лодейщикова В. В.* О классах Леви, порождённых нильпотентными группами // Сибирский математический журнал. 2010. Т. 51, № 6. С. 1359—1366.
7. *Лодейщикова В. В.* О квазимногообразиях Леви экспоненты p^s // Алгебра и логика. 2011. Т. 50, № 1. С. 26—41.

 Получено 31.10.2017. УДК 512.54

[1]Алтайский государственный университет. E-mail: sashakhova@gmail.com.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

РЕШЕТКА ВЫПУКЛЫХ НАПРАВЛЕННЫХ ПОДГРУПП В ЧАСТИЧНО УПОРЯДОЧЕННЫХ ГРУППАХ

Е. Е. Ширшова (Москва)[1]

Пусть $G = < G, \cdot >$ — частично упорядоченная группа, e — единица группы G, $G^+ = \{g \in G |\ e \leq g\}$.

Определение 1. G называется *направленной группой*, если для любых $a, b \in G$ существует $c \in G$ для которого $a, b \leq c$.

Класс направленных групп включает в себя многие известные классы частично упорядоченных групп, например, решеточно упорядоченные группы и линейно упорядоченные группы.

Определение 2. Подгруппа M группы G называется *выпуклой*, если из $a \leq g \leq b$ следует $g \in M$ для всех $a, b \in M$ и $g \in G$.

Изучение свойств множества выпуклых подгрупп оказывается необходимым при решении многих задач теории частично упорядоченных групп.

Определение 3. Выпуклая направленная подгруппа M частично упорядоченной группы G называется *значением элемента* $g \in G$ *(регулярной подгруппой)*, если M является максимальной среди выпуклых направленных подгрупп группы G, не содержащих элемент g.

Определение 4. Элементы a и b из G^+ частично упорядоченной группы G называются *почти ортогональными*, если из неравенств $g \leq a, b$ следует верность неравенств $g^n \leq a, b$ для всех элементов $g \in G$ и всех целых чисел $n > 0$.

Частично упорядоченная группа G называется $\mathcal{AO}$*-группой*, если любой элемент $g \in G$ представим в виде $g = ab^{-1}$ для некоторых почти ортогональных элементов a и b группы G.

Определение 5. Говорят, что выпуклая направленная подгруппа M частично упорядоченной группы G *неразложима в пересечение*, если для любых выпуклых направленных подгрупп N_i группы G из равенства $M = \cap_{i \in I} N_i$ следует существование индекса $j \in I$, для которого $M = N_j$.

Теорема. *Пусть G — $\mathcal{AO}$-группа, M — выпуклая направленная подгруппа группы G. Тогда M является регулярной подгруппой в том и только в том случае, когда M неразложима в пересечение.*

 Получено 24.12.2017. УДК 512.545.

[1]Московский педагогический государственный университет. E-mail: shirshova.elena@gmail.com.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ГРУППЫ АВТОМОРФИЗМОВ КОМПАКТНЫХ КОМПЛЕКСНЫХ ПОВЕРХНОСТЕЙ

К. А. Шрамов (Москва)[1]

Группы автоморфизмов алгебраических многообразий могут быть устроены довольно сложно. В частности, многие из них имеют нетривиальную непрерывную и дискретную части (как, например, группы автоморфизмов абелевых многообразий, например, произведений эллиптических кривых). Можно ожидать, что такие группы проще было бы изучать на уровне их конечных подгрупп. Во многом это верно, но во многих случаях даже конечных групп, действующих на данном алгебраическом многообразии, оказывается бесконечно много. Это верно уже для случая группы автоморфизмов проективного пространства $\mathbb{P}^n$, то есть группы $\mathrm{PGL}_{n+1}(\Bbbk)$, где $\Bbbk$ — базовое поле. Поэтому было бы интересно найти какое-нибудь ограничивающее свойство, которому удовлетворяют все конечные группы, действующие на данном алгебраическом многообразии, не прибегая к полной классификации таких групп. Более того, было бы интересно иметь возможность измерять каким-либо образом "сложность" многообразия в терминах максимальной "сложности" действующих на нем конечных групп. Очевидно, что порядок конечных групп автоморфизмов в качестве такой меры сложности не подходит, так как во многих случаях он не ограничен. Один из возможных ответов о том, в чем можно было бы мерить "сложность", дает следующая классическая теорема К. Жордана. Здесь и далее $\Bbbk$ обозначает поле нулевой характеристики.

Теорема 1 (см. например [2, Theorem 36.13])**.** *Для каждого N существует такая константа $J = J(N)$, что в каждой конечной подгруппе G группы $\mathrm{PGL}_N(\Bbbk)$ найдется нормальная абелева подгруппа индекса не больше J.*

Если для некоторой группы Γ выполнено утверждение теоремы 1, то говорят (см. [4, Definition 2.1]), что группа Γ *жорданова*, или *обладает свойством Жордана*. Это свойство можно рассматривать как ограниченность сложности конечных подгрупп в Γ, а минимальную константу J из теоремы 1 можно считать мерой этой сложности.

Оказывается, что свойство Жордана выполнено в очень многих ситуациях, на первый взгляд довольно далеких от описанной в теореме 1.

Теорема 2 [3]**.** *Пусть X — проективное многообразие над $\Bbbk$. Тогда группа автоморфизмов X жорданова.*

В свете теоремы 2 крайне интересным представляется вопрос о том, на автоморфизмы каких многообразий ее можно распространить. В частности, известно, что аналогичное утверждение верно для автоморфизмов квазипроективных поверхностей (см. [1]).

Отметим, что для групп *бирациональных* автоморфизмов, которые как правило устроены более сложно, чем группы обычных автоморфизмов, свойство Жордана имеет место не всегда (см. [9]), однако оно выполняется для многих важных классов многообразий (см. [5, 6, 8]).

В случае, когда поле $\Bbbk$ является полем комплексных чисел $\mathbb{C}$, неособые алгебраические являются частным случаем комплексных (голоморфных) многообразий. Поэтому было бы интересно выяснить, выполнено ли свойство Жордана для групп автоморфизмов многообразий из этого более широкого класса. На данный момент по этому поводу мало что известно, однако в размерности 2 имеется удовлетворительный ответ, обобщающий двумерный случай теоремы 2.

 Получено 15.01.2018. УДК 512.763.

[1]Математический институт им. В. А. Стеклова РАН и НИУ ВШЭ. E-mail: costya.shramov@gmail.com.

Теорема 3 [7]. *Пусть X — компактное комплексное многообразие размерности* 2. *Тогда группа автоморфизмов X жорданова.*

Литература

1. *Bandman T., Zarhin Yu.* Jordan groups and algebraic surfaces // Transform. Groups. 2015. Vol. 20, № 2. P. 327—334.
2. *Curtis Ch., Reiner I.* Representation theory of finite groups and associative algebras. Pure and Applied Mathematics, Vol. XI. Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.
3. *Meng Sh., Zhang D.-Q.* Jordan property for non-linear algebraic groups and projective varieties // arXiv:1507.02230 [math.AG].
4. *Popov V.* On the Makar-Limanov, Derksen invariants, and finite automorphism groups of algebraic varieties // Peter Russell's Festschrift, Proceedings of the conference on Affine Algebraic Geometry held in Professor Russell's honour, 1–5 June 2009, McGill Univ., Montreal., volume 54 of Centre de Recherches Mathématiques CRM Proc. and Lect. Notes, pages 289—311, 2011.
5. *Prokhorov Yu, Shramov. C.* Jordan property for groups of birational selfmaps // Compositio Math. 2014. Vol. 150, № 12. P. 2054—2072.
6. *Prokhorov Yu, Shramov C.* Jordan property for Cremona groups // Amer. J. Math. 2016. Vol. 138, № 2. P. 403—418.
7. *Prokhorov Yu, Shramov C.* Automorphism groups of compact complex surfaces // arXiv:1708.03566 [math.AG].
8. *Serre J.-P.* Le groupe de Cremona et ses sous-groupes finis. Séminaire Bourbaki, Nov. 2008, 61ème année. № 1000. 2008—2009.
9. *Zarhin Yu.* Theta groups and products of abelian and rational varieties // Proc. Edinburgh Math. Soc. 2014. Vol. 57, № 1. P. 299—304.

Секция 2

ТЕОРИЯ КОЛЕЦ

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ГРАДУИРОВАННЫЕ ФРОБЕНИУСОВЫ АЛГЕБРЫ[1]

И. Н. Балаба (Тула)[2]

Фробениусовы алгебры являются одним из важных классов алгебр, изучаемых в теории представлений конечномерных алгебр. Впервые они появились в работе Ф. Г. Фробениуса, потом активно изучались Накаямой, Брауэром, Несбитт, Икедой, Кашем и другими. Основные результаты о фробениусовых алгебрах можно найти в [3, глава 9].

В последние десятилетия отмечается значительный интерес к алгебраическим объектам, снабженным градуировкой. Градуированным фробениусовым алгебрам посвящены работы [4, 5], а в [2] были описаны градуированные квазифробениусовы кольца.

Пусть далее G — мультипликативная группа с единицей e, k — поле и $A\bigoplus_{g\in G}A_g$ — G-градуированная алгебра, т. е. k-алгебра, являющаяся прямой суммой подпространств A_g, таких что $A_gA_h\subseteq A_{gh}$ для любых $g,\ h\in G$.

Для подмножества S в A через $l(S)$ и $r(S)$ обозначим соответственно левый и правый аннуляторы множества S, т. е.

$$l(S)=\{a\in A\mid aS=0\},\qquad R(s)=\{a\in A\mid Sa=0\}.$$

Если множество S является градуированным, т. е. вместе с каждым своим элементом содержит и все его однородные компоненты, то $l(S)$ и $r(S)$ являются соответственно левым и правым градуированными идеалами алгебры A

Левому модулю ${}_AA$ как векторному пространству над полем k можно сопоставить дуальное векторное пространство $A^*=\mathrm{Hom}_k(A,k)$, являющееся правым A-модулем, если положить $(\varphi a)(x)=\varphi(ax)$ для всех $\varphi\in A^*,\ a,x\in A$.

Если алгебра A конечномерна, то A^* является правым градуированным A-модулем со следующей градуировкой

$$A^*_g=\{f\in A^*\mid f(A_h)=0\ \ \textit{для всех}\ h\neq g^{-1}\}\ \ (g\in G).$$

Определение 1. Конечномерная G-градуированная k-алгебра A называется *gr-фробениусовой*, если левые градуированные A-модули ${}_AA$ и $(A_A)^*$ изоморфны.

Ясно, что если градуированная алгебра A является gr-фробениусовой, то A является фробениусовой k-алгеброй. Обратное, вообще говоря, неверно.

Теорема 1. *Пусть $A\bigoplus_{g\in G}A_g$ — конечномерная G-градуированная k-алгебра. Тогда следующие утверждения равносильны:*

1. *Алгебра A — gr-фробениусова.*
2. *Существует невырожденная билинейная форма $f:A\times A\to k$, удовлетворяющая условию ассоциативности:*

$$f(ab,c)=f(a,bc)\ \textit{для всех}\ a,b,c\in A,$$

   такая что $f(a_g,a_h)=0$ для всех $a_g\in A_g,\ a_h\in A_h$, для которых $g\neq h^{-1}$.
3. *Существует линейная функция $\lambda\in A^*$, такая, что $\lambda(a_g)=0,\ a\in A_g,\ g\neq e$, ядро которой не содержит ненулевых градуированных правых и левых идеалов алгебры A.*

© Балаба И. Н., 2018. Получено 11.03.2018. УДК 512.552.

[1]Работа выполнена при финансовой поддержке РФФИ, проект № 16-41-710194.

[2]Тульский государственный педагогический университет им. Л. Н. Толстого. E-mail: ibalaba@mail.ru.

4. *Для всех правых R и всех левых L градуированных идеалов алгебры A выполняются следующие соотношения:*

$$l(r(L)) = L, \qquad \dim_k r(L) + \dim_k L = \dim_k A;$$
$$r(l(R)) = R, \qquad \dim_k l(R) + \dim_k R = \dim_k A.$$

Эквивалентность условий 1 — 3 была доказана в [4].

Определение 2. Градуированная алгебра называется *gr-полупростой*, если A является прямой суммой минимальных левых градуированных идеалов.

Описание gr-полупростых градуированных колец и их гомологическая классификация даны в [1].

Следствие [4, следствие 4.5]**.** *Градуированная gr-полупростая алгебра является gr-фробениусовой*

Пусть A — gr-фробениусова алгебра и $f : A \times A \to k$ — невырожденная ассоциативная билинейная форма, определенная в теореме 1.

Пусть $a_1, a_2, ..., a_n$ — базис k-алгебры A, состоящий из однородных элементов. Так как $\dim_k A = \dim_k A^*$ и градуированные модули A и A^* изоморфны, то существуют такие однородные элементы $b_1, b_2, ..., b_n \in A$, что $f(a_i, b_j) = \delta_{ij}$, $1 \leq i, j \leq n$. Эти однородные базисы называются *дуальными базисами* относительно формы f.

Теорема 2. *Пусть A — gr-фробениусова алгебра над полем k, $a_1, a_2, ..., a_n$ и $b_1, b_2, ..., b_n$ — дуальные друг к другу базисы алгебры A. Тогда для левого градуированного A-модуля M следующие утверждения равносильны:*

1) *модуль M — gr-проективен;*
2) *модуль M — gr-инъективен;*
3) *существует такое k-линейное преобразование ψ градуированного модуля M, что $\psi(M_g) \subseteq M_g$, $g \in G$ и*

$$\sum_{i=1}^{n} b_i \psi a_i = \mathrm{Id}_M.$$

Литература

1. *Балаба И. Н., Краснова Е. Н.* Полупростые градуированные кольца // Известия Саратовского университета. Новая серия. Сер.: Математика. Механика. Информатика. 2013. Т. 13, вып. 4, ч. 2. С. 23—28.
2. *Краснова Е. Н.* Градуированные квазифробениусовы кольца // Алгебра и теория чисел: современные проблемы и приложения: материалы XII Международной конференции, посвященной восьмидесятилетию профессора В. Н. Латышева, Тула, 21–25 апреля 2014 г. Тула: Изд-во Тул. гос. пед. ун-та им. Л. Н. Толстого, 2014. С. 168—171.
3. *Кэртис Ч., Райнер И.* Теория представлений конечных групп и ассоциативных алгебр. М. : Наука, 1969. 668 с.
4. *Dăscălescu S., Năstăsescu C., Năstăsescu L.* Frobenius algebras of corepresentations: gradings // arXiv:1307.7304 [math.QA] URL: https://arxiv.org/abs/1307.7304 (дата обращения 20.12.2017)
5. *Wakamatsu T.* On graded Frobenius algebras // J. Algebra. 2003. Vol. 267. P. 377—395.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

АНАЛОГ КРИТЕРИЯ ПРОСТОТЫ МИЛЛЕРА В ФАКТОРИАЛЬНОМ КОЛЬЦЕ ЦЕЛЫХ АЛГЕБРАИЧЕСКИХ ЭЛЕМЕНТОВ РАСШИРЕНИЯ ГАЛУА ПОЛЯ $\mathbb{Q}$ СТЕПЕНИ НЕ ВЫШЕ 3

М. М. Васьковский (Минск, Беларусь)[1], Н. П. Прохоров (Минск, Беларусь)[2]

1. Введение

В 1976 году Гарри Миллером [8] был предложен критерий и построен полиномиальный алгоритм тестирования чисел на простоту в предположении верности обобщённой гипотезы Римана. Позже его результат был улучшен Эриком Бахом [5]. В 1980 году Михаэль Рабин [9] на основе критерия Миллера предложил полиномиальный вероятностный алгоритм тестирования чисел на простоту, который в настоящее время является самым эффективным вероятностным безусловным алгоритмом тестирования на простоту, который позволяет определять с вероятностью близкой к 1 при достаточном числе итераций, является ли число простым. Данные результаты представляют большой интерес как с теоретической точки зрения, так и с практической: при создании некоторых криптосистем (например RSA) требуются эффективные алгоритмы проверки чисел на простоту.

Данная работа посвящена доказательству аналога критерия Миллера в факториальных кольцах целых элементов расширений Галуа поля $\mathbb{Q}$ степени не выше 3, а также построению на его основе вероятностных и детерминированных алгоритмов тестирования на простоту и их анализа. Данный вопрос интересен как с точки алгебраической и алгоритмической теории чисел, так и с точки зрения криптографии: данные задачи возникают при создании аналогов RSA криптосистемы в факториальных кольцах элементов расширений поля $\mathbb{Q}$.

Определение 1. Числовое поле K, такое что $\mathbb{Q} \subset K$ и K является конечномерным векторным пространством над полем $\mathbb{Q}$, будем называть конечным расширением поля $\mathbb{Q}$. Размерность K, как векторного пространства над полем $\mathbb{Q}$, будем называть степенью расширения.

Определение 2. Конечное расширение K поля $\mathbb{Q}$ будем называть расширением Галуа, если оно нормально и сепарабельно.

Определение 3. Рассмотрим множество целых элементов поля K. Данное множество образует область целостности относительно стандартных операций сложения и умножения. Обозначим данное множество через $\mathcal{O}_K$.

Далее будем рассматривать факториальные $\mathcal{O}_K$.

Обозначим через $\mathrm{Nm}(\cdot)$ норму элемента в K. Также обозначим через $\mathcal{O}_K^\times$ множество обратимых элементов кольца $\mathcal{O}_K$. Пусть $\mathcal{P}_{1,K}$ – множество простых элементов $\mathcal{O}_K$ с чётной нормой.

 Получено 25.12.2017. УДК 511.623.

[1]Белорусский государственный университет. E-mail: vaskovskii@bsu.by.

[2]Белорусский государственный университет. E-mail: nprohorovminsk@mail.ru.

2. Аналог критерия Миллера

Теорема 1. *Пусть $N \in \mathcal{O}_K \setminus \mathcal{O}_K^\times$ — элемент свободный от простых делителей $p \in \mathcal{P}_{1,K}$. Тогда следующие утверждения эквивалентны*

(1) *N простой элемент;*
(2) *$\forall a, (a, N) = 1, a^u \not\equiv 1 \pmod N : \exists k \in \{0, \dots, t-1\}$, такое что $a^{2^k u} \equiv -1 \pmod N$, где $\mathrm{Nm}(N) - 1 = 2^t u, (u, 2) = 1$.*

3. Аналог теста Миллера-Рабина

Определение 4. Целым базисом [2] будем называть такой базис в векторном пространстве K над полем $\mathbb{Q}$, что любой элемент в $\mathcal{O}_K$ представим в виде линейной комбинации базисных векторов с целыми коэффициентами и наоборот – любая комбинация базисных векторов с целыми коэффициентами является элементами $\mathcal{O}_K$.

Далее будем считать, что нам известен целый базис $\{e_1, \dots, e_n\}$ поля K.

Пусть $a \in \mathcal{O}_K$ и $a = \alpha_1 e_1 + \dots + \alpha_n e_n$, тогда под абсолютным значением a будем понимать натуральную величину $|a|_\infty = \max\limits_{i \in \overline{1,n}} |\alpha_i|$.

Алгоритм 1. *Пусть $N \in \mathcal{O}_K \setminus \mathcal{O}_K^\times$ — элемент, свободный от простых делителей $p \in \mathcal{P}_{1,K}$. Мы хотим определить является ли элемент N простым в $\mathcal{O}_K$.*

(1) *Вычислить $\mathrm{Nm}(N)$ и определить числа $u, t \in \mathbb{N}$, $(u, 2) = 1$, такие что $\mathrm{Nm}(N) - 1 = 2^t u$.*
(2) *Выбрать произвольное $a \in \mathcal{O}_K$. Если $a \equiv 0 \pmod N$, то ответ — 'неизвестно', иначе перейти к следующему шагу алгоритма.*
(3) *Вычислить вычет $r_0 \equiv a^u \pmod N$. Если $r_0 = 1$, то ответ — 'неизвестно', иначе положить $k = 0$ и перейти к следующему шагу алгоритма.*
(4) *Если $k < t$ и $r_k = -1$, то ответ — 'неизвестно'. Если $k < t$ и $r_k \neq -1$, то увеличить k на 1, вычислить $r_{k+1} \equiv r_k^2 \pmod N$ и повторить шаг 4. Если $k = t$, то ответ — 'N не является простым'.*

Если был получен ответ 'неизвестно', то мы можем повторить итерацию данного алгоритма (шаги 2 — 5) с другим значением a.

Теорема 2. *Алгоритм 1 имеет сложность равную $O(\log^3 |N|_\infty)$ бинарных операций.*

Обозначим через $\mathcal{O}_{K,N}^\times$ — мультипликативную группу кольца вычетов по модулю N, а через $\mathcal{S}_N$ множество таких $a \in \mathcal{O}_{K,N}^\times$, что Алгоритм 1 даёт ответ 'неизвестно'.

Теорема 3. *Пусть $N \in \mathcal{O}_K \setminus \mathcal{O}_K^\times$ не является простым в $\mathcal{O}_K$, N свободно от простых делителей $p \in \mathcal{P}_{1,K}$. Тогда выполнено неравенство $|\mathcal{S}_N| \leq |\mathcal{O}_{K,N}^\times|/2$.*

Замечание 1. Если элемент $N \in \mathcal{O}_K \setminus \mathcal{O}_K^\times$ не является простым в $\mathcal{O}_K$ и является свободным от делителей $p \in \mathcal{P}_{1,K}$, то, согласно Теореме 3, Алгоритм 1 позволяет доказать, что N не является простым с вероятностью $\mathbb{P} \geq 1 - 2^{-M}$, где M — это число итераций Алгоритма 1.

4. Аналог критерия Миллера-Рабина в предположении ERH

Определение 5. Под Расширенной Гипотезой Римана (ERH) будем понимать следующую гипотезу: нули любой Hecke L — функции на множестве $0 < \mathrm{Re}\, z < 1$ комплексной плоскости лежат на прямой $\mathrm{Re}\, z = 1/2$ [5].

Теорема 4. *Предположим, что ERH выполняется. Пусть $N \in \mathcal{O}_K \setminus \mathcal{O}_K^\times$ — элемент, свободный от простых делителей $p \in \mathcal{P}_{1,K}$. Тогда следующие утверждения эквиваленты:*

(1) *N является простым числом.*
(2) *$\forall a$, $(a, N) = 1, \mathrm{Nm}(a) \leq 12 \log^2 (\Delta_K \mathrm{Nm}(N))$, $a^u \not\equiv 1 \pmod N : \exists k \in \{0, \dots, t-1\}$, такое что $a^{2^k u} \equiv -1 \pmod N$, где $\mathrm{Nm}(N) - 1 = 2^t u$, $(u, 2) = 1$.*

Замечание 2. На основе теоремы 4 может быть предложен детерминированный алгоритм тестирования на простоту в кольце $\mathcal{O}_K$, имеющий сложность $O(\log^3 |N|_\infty \log^2 \mathrm{Nm}(N))$.

Литература

1. *Васьковский М., Кондратёнок Н., Прохоров Н.* Аналог теста Соловея–Штрассена в квадратичных Евклидовых кольцах // Доклады Национальной академии наук Беларуси. 2017. Т. 61. № 5. С. 28—32.
2. *Гекке Э.* Лекции по теории алгебраических чисел. Государственное издательство технико-теоретической литературы. Москва, 1940.
3. *Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В.* Введение в теоретико-числовые методы криптографии. Санкт-Петербург : Лань, 2011.
4. *Чеботарёв Н. Г.* Основы Теории Галуа. Объединённое научно-техническое издание НКТП СССР, 1937.
5. *Bach E.* Explicit bounds for primality testing and related problems // Mathematics of Computation. 1990. P. 355—380.
6. *Kranakis E.* Primality and Cryptography. Teubner, 1986
7. *Koblitz N.* Course in Number Theory and Cryptography. New York : Springer-Verlag, 1994.
8. *Miller G.* Riemann's Hypothesis and Tests for Primality // Journal of Computer and System Sciences. 1976. Vol. 13, № 3. P. 300—317.
9. *Rabin M. O.* Probabilistic Algorithm for Testing Primality // Journal of number theory. 1980. Vol. 12. P. 128—130.
10. *Vaskouski M., Kondratyonok N., Prochorov N.* Primes in quadratic unique factorization domains // Journal of Number Theory. Vol. 168. P. 101—116.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О КОНГРУЭНЦИЯХ НА ПОЛУКОЛЬЦАХ НЕПРЕРЫВНЫХ ЧАСТИЧНЫХ ФУНКЦИЙ[1]

Е. М. Вечтомов (Киров)[2], Е. Н. Лубягина (Киров)[3]

В настоящей заметке исследуются конгруэнции на полукольцах непрерывных частичных числовых функций на топологических пространствах.

Данная тема относится к функциональной алгебре — одному из направлений современной математики (см. [8, Введение]). Отметим, что основы классической теории колец $C(X)$ непрерывных действительнозначных функций на топологических пространствах X даны в монографии Гиллмана и Джерисона [11]. На базе теории колец $C(X)$ выросла теория полуколец непрерывных числовых функций, которой посвящена двухтомная монография [8, 9] и обзорная статья [10]. Систематическое исследование полуколец непрерывных частичных функций мы начали в работах [2, 3, 4, 5, 6, 7, 12].

Введем используемые понятий и обозначения.

Полукольцом называется алгебраическая структура $\langle S;+,\cdot\rangle$ с коммутативно-ассоциативной операцией сложения $+$ и ассоциативной операцией умножения $\cdot$, которая дистрибутивна относительно сложения с обеих сторон. Если на полукольце задана топология, относительно которой полукольцевые операции непрерывны, то получаем *топологическое полукольцо*.

Заметим, что для полуколец определения подполукольца, идеала, конгруэнциии и т. п. носят общеалгебраический характер.

Пусть X — топологическое пространство, S — топологическое полукольцо и $C(X,S)$ — полукольцо всех непрерывных S-значных функций на пространстве X с поточечно определенными операциями сложения и умножения функций. Обозначим через

$$CP(X,S)=\cup\{C(Y,S):Y\subseteq X\}$$

полукольцо всевозможных непрерывных частичных S-значных функций на X с поточечно заданными операциями сложения и умножения частичных функций f и g на их общей области определения $D(f)\cap D(g)$[4]:

$(f+g)(x)=f(x)+g(x)$ и $(fg)(x)=f(x)\cdot g(x)$ для всех $x\in D(f)\cap D(g)=D(f+g)=D(fg)$.

Полукольцо $C(X,S)$ является подполукольцом полукольца $CP(X,S)$. Будем считать, что $C(\varnothing,S)=\{\varnothing\}$; при этом $\varnothing$ служит *поглощающим элементом* полукольца $CP(X,S)$.

Если топологическое полукольцо S имеет единицу 1, то функция-константа 1 будет единицей полуколец $C(X,S)$ и $CP(X,S)$, а если S имеет нуль 0, то функция-константа 0 будет нулем полукольца $C(X,S)$, но не является нулем полукольца $CP(X,S)$.

Среди числовых топологических полуколец S особое место занимают топологическое поле $\mathbf{R}$ всех действительных чисел (с обычной топологией), полуполе с нулем $\mathbf{R}^+$ неотрицательных действительных чисел и полуполе $\mathbf{P}$ положительных действительных чисел.

Положим

$$C(X)=C(X,\mathbf{R}) \text{ и } CP(X)=CP(X,\mathbf{R}),$$

то есть полукольцо $CP(X)$ всех непрерывных частичных $\mathbf{R}$-значных функций на топологи-

 Получено 20.12.2017. УДК 512.55.

[1]Работа выполнена в рамках государственного задания Минобрнауки РФ «Полукольца и их связи», проект № 1.5879.2017/8.9

[2]Вятский государственный университет. E-mail: vecht@mail.ru.

[3]Вятский государственный университет. E-mail: shishkina.en@mail.ru.

[4]Через $D(h)$ обозначается область определения частичной функции h.

ческом пространстве X является дизъюнктным объединением коммутативных колец $C(Y)$ с нулем и единицей по различным подпространствам Y пространства X, включая одноэлементное кольцо $C(\varnothing) = \{\varnothing\}$.

Обозначим через ρ_D конгруэнцию на полукольце $CP(X, S)$, отождествляющую частичные функции с одинаковой областью определения:

$$f \rho_D g \Leftrightarrow D(f) = D(g) \text{ для любых } f, g \in CP(X, S).$$

Конгруэнцию ρ на полукольце $CP(X, S)$ назовем *D-конгруэнцией*, если $\rho_D \subseteq \rho$. Относительно отношения включения $\subseteq$ множество $\mathrm{Con}CP(X, S)$ всевозможных конгруэнций на полукольце $CP(X, S)$ образует полную решетку, при этом множество всех D-конгруэнцией будет ее (полной) подрешеткой.

Предложение 5 статьи [7] фактически дает две следующие теоремы:

Теорема 1. *Для всякой конгруэнции ρ на полукольце $CP(X)$ над произвольным топологическим пространством X эквивалентны следующие утверждения:*

1) *ρ — максимальная конгруэнция;*
2) *ρ — максимальная конгруэнция среди D-конгруэнций;*
3) *ρ — двухклассовая конгруэнция.*

Теорема 2. *Любая собственная конгруэнция на полукольце $CP(X)$ содержится в некоторой максимальной конгруэнции.*

Заметим, что *минимальные конгруэнции* на полукольце $CP(X)$, то есть атомы решетки конгруэнций $\mathrm{Con}CP(X)$, суть конгруэнции $\rho_x, x \in X$, имеющие единственный неодноэлементный класс $CP(\{x\}) = C(\{x\}) \cup \{\varnothing\}$. Ясно, что $C(\{x\}) \equiv \mathbf{R}$.

Из предложения 6 статьи [7] вытекает, что модулярность (дистрибутивность) решетки $\mathrm{Con}CP(X)$ равносильна одноэлементности топологического пространства X.

Напомним, что топологическое пространство с замкнутыми одноточечными множествами называется T_1-*пространством*. Говорят, что проивольное T_1-пространство X *определяется* производной *алгебраической системой* $S(X)$, если для любого T_1-пространства Y изоморфность алгебраических систем $S(X)$ и $S(Y)$ равносильна гомеоморфности пространств X и Y.

В работе [7] получена определяемость T_1-пространств X решеткой идеалов полуколец $CP(X)$, а в статье [6] установлена определяемость T_1-пространств X решеткой подалгебр полуколец $CP(X)$. Из этого следует определяемость любого T_1-пространства X самим полукольцом $CP(X)$. Отметим, что имеет место определяемость T_1-пространств X даже мультипликативной полугруппой полуколец $CP(X)$ [1].

Сформулируем новый результат:

Теорема 3. *Каждое T_1-пространство X определяется решеткой всех конгруэнций полукольца $CP(X)$.*

Заметим, что T_1-пространства X не обязаны определяться решеткой D-конгруэнций полуколец $CP(X)$.

Задача 1. Исследовать алгебраические свойства решеток $\mathrm{Con}CP(X)$.

Задача 2. Верна ли теорема 3 для полуколец $CP(X, \mathbf{R}^+)$ и $CP(X, \mathbf{P})$?

Литература

1. *Вечтомов Е. М.* О полугруппах непрерывных частичных функций на топологических пространствах // Успехи математических наук. 1990. Т. 45, вып. 4. С. 143—144.
2. *Вечтомов Е. М., Лубягина Е. Н.* О полукольцах частичных функций // Вестник Сыктывкарского университета. Серия 1: Математика. Механика. Информатика. 2014. Вып. 19. С. 3—11
3. *Вечтомов Е. М., Лубягина Е. Н.* Полукольца частичных функций // Материалы XIII Международной конференции «Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения». Тула: ТГПУ, 2015. С. 148—150.

4. *Вечтомов Е. М., Лубягина Е. Н.* О категории полуколец непрерывных частичных числовых функций // Материалы международной конференции по алгебре, анализу и геометрии, посвященной юбилеям выдающихся профессоров Казанского университета, математиков Петра Алексеевича (1895—1944) и Александра Петровича (1926—1998) Широковых. Казань : Казанский университет; Изд-во Академии наук РТ, 2016. С. 128—129.
5. *Вечтомов Е. М., Лубягина Е. Н.* О подалгебрах в полукольцах непрерывных частичных действительнозначных функций // Advanced science. Киров : ВятГУ, 2017. № 2.
6. *Вечтомов Е. М., Лубягина Е. Н.* Определяемость T_1-пространств решеткой подалгебр полуколец непрерывных частичных действительнозначных функций на них // Вестник Сыктывкарского университета. Серия 1: Математика. Механика. Информатика. 2017. Вып. 1 (22). С. 21—28.
7. *Вечтомов Е. М., Лубягина Е. Н.* Полукольца непрерывных частичных действительнозначных функций // CEUR-WS.org_Vol-1894. Proceedings of the 48th International Youth School-Conference «Modern Problems in Mathematics and its Applications» Yekaterinburg, Russia, February 5–11, 2017. P. 20—29.
8. *Вечтомов Е. М., Лубягина Е. Н., Сидоров В. В., Чупраков Д. В.* Элементы функциональной алгебры: монография. В 2 т. Т. 1 / под ред. Е. М. Вечтомова. Киров : ООО «Издательство «Радуга-ПРЕСС», 2016. 384 с.
9. *Вечтомов Е. М., Лубягина Е. Н., Сидоров В. В., Чупраков Д. В.* Элементы функциональной алгебры: монография. В 2 т. Т. 2 / под ред. Е. М. Вечтомова. Киров: ООО «Издательство «Радуга-ПРЕСС», 2016. 316 с.
10. *Вечтомов Е. М., Михалев А. В., Сидоров В. В.* Полукольца непрерывных функций // Фундаментальная и прикладная математика. 2016. Т. 21, вып. 2. С. 53—131.
11. *Gillman L., Jerison M.* Rings of continuous functions. Princeton, 1960. 300 p.
12. *Vechtomov E. M., Lubyagina E. N.* On the lattice of ideals of semirings of continuous partial real-valued functions // Proceedings of the 4th Conference of Mathematical Society of Moldova. Chisinau, Republic of Moldova, 2017. P. 169—172.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ВЕЩЕСТВЕННО ЗАМКНУТЫЕ РАСШИРЕНИЯ ПОЛЕЙ ОГРАНИЧЕННЫХ ФОРМАЛЬНЫХ СТЕПЕННЫХ РЯДОВ С СИММЕТРИЧНЫМИ СЕЧЕНИЯМИ

Н. Ю. Галанова (Томск)[1]

Каждое неархимедово вещественно замкнутое поле вкладывается с сохранением порядка в некоторое поле формальных степенных рядов с делимой группой архимедовых классов. Поэтому представляет интерес изучение подполей поля формальных степенных рядов, построенного по делимой линейно упорядоченной группе. Исторический обзор результатов и их доказательства по этой и близким темам рассматривается в [3]. Изучением данного и подобных ему вопросов занимались в последнее время разные авторы, используя свои классификации сечений [2, 4, 5].

Пусть G — линейно упорядоченная делимая абелева группа, β — регулярный кардинал, $\aleph_0 < \beta < \beta^+ = cf(G) = |G|$, $\mathbf{R}[[G,\beta]]$ — поле ограниченных формальных степенных рядов $x = \sum\limits_{g\in G} r_g g$, где $r_g \in \mathbf{R}$, $supp(x) = \{g \in G | r_g \neq 0\}$ — вполне антиупорядоченное подмножество группы G, $|supp(x)| < \beta$.

Так как $\beta^+ = cf(G)$, найдётся $\Gamma = \{g_\gamma\}_{\gamma\in\beta^+}$ — подмножество группы G такое, что отображение $\gamma \mapsto g_\gamma$ задаёт инверсное подобие кардинала β^+ и множества Γ. Зададим ряд: $x_{\beta^+} = \sum\limits_{g\in\Gamma} 1g$, $x_{\beta^+} \in \mathbf{R}[[G]]\backslash\mathbf{R}[[G,\beta^+]]$. Для каждого γ, $\beta \leq \gamma < \beta^+$, обозначим через $x_\gamma = \sum\limits_{g_\delta\in\Gamma,\delta>\gamma} 1g_\delta$ усечение [4] ряда x_{β^+}.

Сечение (A,B) упорядоченного поля F называется симметричным (по Пестову), если для каждого $a \in A$ существует такое $a_1 \in A$, что $(a_1 + (a_1 - a)) \in B$ и для каждого $b \in B$ существует такое $b_1 \in B$, что $(b_1 - (b - b_1)) \in A$ [2].

В [1] вводится конструкция вещественно замкнутого поля H с симметричными (по Пестову) сечениями конфинальности β^+. Применяя эту конструкцию к вещественному замыканию $\overline{\mathbf{R}[[G,\beta]](x_\beta)}$ простого трансцендентного расширения поля ограниченных формальных степенных рядов, можно доказать

Теорема 1. *$H = \bigcup\limits_{\beta\leq\gamma<\beta^+} \overline{\mathbf{R}[[G,\beta]](x_\gamma)}$ — объединение вещественных замыканий простых трансцендентных расширений поля $\mathbf{R}[[G,\beta]]$. Причём каждое поле из объединения упорядоченно изоморфно полю $\overline{\mathbf{R}[[G,\beta]](x_\beta^+)}$.*

Теорема 2. *1) Если для некоторого γ_0 , $\beta \leq \gamma_0 < \beta^+$ все усечения ряда x_{β^+} принадлежат полю $\overline{\mathbf{R}[[G,\beta]](x_{\gamma_0})}$, то $H = \overline{\mathbf{R}[[G,\beta]](x_{\gamma_0})}$ и каждое поле $\overline{\mathbf{R}[[G,\beta]](x_\gamma)}$, где $\beta \leq \gamma \leq \beta^+$ имеет симметричное сечение конфинальности β^+.*

2) Если $H = \overline{\mathbf{R}[[G,\beta]](x_{\gamma_0})}$ для некоторого γ_0 , $\beta \leq \gamma_0 < \beta^+$, то H упорядоченно изоморфно $\overline{\mathbf{R}[[G,\beta]](x_\beta)}$. В этом случае поля H и $\mathbf{R}[[G,\beta^+]]$ упорядоченно изоморфны тогда и только тогда, когда $\mathbf{R}[[G,\beta^+]]$ упорядоченно изоморфно своему подполю $\overline{\mathbf{R}[[G,\beta]](x_\beta)}$.

3) $\overline{H(x_{\beta^+})} \supseteq \overline{\mathbf{R}[[G,\beta]](x_{\beta^+})}$.

4) Поля H и $\overline{H(x_{\beta^+})}$ замкнуты относительно усечений.

 Получено 21.12.2017. УДК 512.623.23

[1]Томский государственный университет. E-mail: galanova@math.tsu.ru.

Если поля H и $\mathbf{R}[[\mathbf{G}, \beta^+]]$ не изоморфны (упорядоченно), то существует вещественно замкнутое поле с симметричными сечениями разной конфинальности. Пока существование такого поля — это вопрос открытый.

Литература

1. *Галанова Н. Ю.* Линейно упорядоченные поля с симметричными сечениями. // Вестник Томского государственного университета. Математика и механика. 2017. № 46. С. 14—20.
2. *Галанова Н. Ю., Пестов Г. Г.* Симметрия сечений в полях формальных степенных рядов // Алгебра и логика. 2008. Т. 47, № 2. С. 174—185.
3. *Dales H. J., Woodin H.* Super real fields. Oxford : Clarenden Press, 1996.
4. *Kuhlmann F.-V., Kuhlmann S., Marshall M., Zekavat. M.* Embedding ordered fields in formal power series fields // Journal of Pure and Applied Algebra. 2002. Vol. 169, Issue 1. P. 71—90.
5. *Shelah S.* Quite Complete Real Closed fields // Israel Journal of Mathematics. 2004. Vol. 142. P. 261—272.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О ПРОЕКТИВНОМ ОБРАЗЕ РАДИКАЛА КОНЕЧНОГО КОЛЬЦА

С. С. Коробков (Екатеринбург)[1]

1. Введение

Рассматриваются ассоциативные кольца. Проектированием (иначе, решёточным изоморфизмом) кольца R на кольцо R^φ называется изоморфизм φ решётки всех подколец $L(R)$ кольца R на решётку всех подколец $L(R^\varphi)$ кольца R^φ. При этом кольцо R^φ называется проективным образом кольца R, а само R — проективным прообразом кольца R^φ. При изучении проектирований колец решаются следующие задачи:

1) выяснить, какие алгебраические свойства колец сохраняются при проектированиях;

2) найти кольца, изоморфные своим проективным образам.

В процессе решения указанных задач возникает вопрос о проективном образе радикала Джекобсона $\operatorname{Rad} R$ кольца R. Прежде всего, это объясняется важным значением радикала Джекобсона для строения кольца. Кроме того, в случае выполнимости равенства

$$(\operatorname{Rad} R)^\varphi = \operatorname{Rad} R^\varphi \tag{1}$$

имеется возможность перехода к индуцируемому решёточному изоморфизму $\overline{\varphi}$ между факторкольцами $\overline{R} = R/\operatorname{Rad} R$ и $\overline{R^\varphi} = R^\varphi/\operatorname{Rad} R^\varphi$. Такой переход позволяет получить существенно больше информации о проективном образе R^φ. Существуют примеры, показывающие, что равенство (1) выполняется не для всех колец. Целью работы является определение тех колец, для которых равенство (1) выполняется.

Прежде, чем переходить к изложению основных результатов, заметим, что изучение решёточных изоморфизмов конечных колец сводится к изучению проективных образов конечных колец, имеющих примарные аддитивные группы (так называемых p-колец (p — простое число)). Действительно, любое конечное кольцо R разложимо в прямую сумму своих p_i-подколец R_i: $R = R_1 \oplus \cdots \oplus R_n$, взятую по различным простым числам p_i. Ясно, что $L(R) \cong L(R_1) \times \cdots \times L(R_n)$, а значит $L(R^\varphi) \cong L(R_1^\varphi) \times \cdots \times L(R_n^\varphi)$.

Уточним используемые в работе обозначения: $R = S \oplus T$ — аддитивная прямая сумма колец S и T; $\langle a_1, a_2, \ldots, a_n\rangle$ — кольцо, порождённое элементами $a_1, a_2, \ldots, a_n$; $o(r)$ — аддитивный порядок элемента r; $\operatorname{ind} r$ — индекс нильпотентности элемента r; буквы k, l, m, n, h, q с индексами и без индексов обозначают натуральные числа, причём p и q — простые числа, строчные греческие буквы, кроме буквы φ, обозначают целые числа.

2. Проектирования простых и полупростых конечных колец

Рассмотрим случай, когда $\operatorname{Rad} R = \{0\}$. Если R — простое кольцо, то либо R — конечное поле, либо R — кольцо квадратных матриц, рассматриваемых над конечным полем.

Определим 4 кольца:

$R_1 = GF(p^{q^n})$, $n \in \mathbb{N} \cup \{0\}$;

$R_2 = GF(p^{p_1 p_2})$, $p_1 \neq p_2$;

$R_3 = GF(p^q) \oplus GF(p)$;

$R_4 = GF(p) \oplus GF(p)$.

Из результатов работ [3, 6] вытекает

Теорема 1. *Пусть конечное простое кольцо R не изоморфно кольцам R_1 и R_2. Пусть φ — проектирование кольца R на кольцо R^φ. Тогда R^φ — простое кольцо.*

 Получено 18.12.2017. УДК 512.552.

[1]Уральский государственный педагогический университет. E-mail: ser1948@gmail.com.

Для полупростых колец доказана следующая теорема:

Теорема 2. *Пусть конечное полупростое p-кольцо R не изоморфно кольцам R_3 и R_4. Пусть φ — решёточный изоморфизм кольца R на кольцо R^φ. Тогда R^φ — полупростое кольцо.*

Замечание 1. Для колец R_1 — R_4 существуют проектирования φ, для которых равенство (1) не выполняется.

3. Проектирования нильпотентных конечных колец

Рассмотрим случай, когда $\operatorname{Rad} R = R$. Решёточные изоморфизмы нильпотентных p-колец изучались в работе [1].

Определим 6 конечных нильпотентных p-колец:

$R_5 = \langle r \rangle$, где $r^3 = 0$, $r^2 \neq 0$, $pr = 0$;

$R_6 = \langle r \rangle$, где $o(r) = p^n$ $(n \in \mathbb{N})$, $r^2 = pr^k$ $(k = \overline{1,n})$;

$R_7 = \langle r_1 \rangle \oplus \langle r_2 \rangle$, где $r_i r_j = 0$ $(i,j = 1,2)$, $2r_1 = 2r_2 = 0$;

R_8 — нильпотентное кольцо, отличное от колец R_6 и R_7, и в котором каждая аддитивная подгруппа является подкольцом (такие кольца описаны в работе [7]);

$R_9 = S_0 \oplus \langle a_1 \rangle$, где S_0 — кольцо с нулевым умножением характеристики p или $S_0 = \{0\}$, $\operatorname{ind} a_1 = 3$, $pa_1 = 0$, $a_i a_j = \alpha_{ij} a_1^2$ $(i,j = 0,1)$, $\alpha_{01} + \alpha_{10} \equiv 0 \pmod p$;

$R_{10} = R_9 \oplus \langle a_2 \rangle$, $p = 2$, $\operatorname{ind} a_2 = 3$, $2a_2 = 0$, $a_2^2 \neq a_1^2$, $a_0 a_2 = a_2 a_0 = \alpha a_2^2$, $a_1 a_2 = a_2 a_1 = \beta a_1^2 + \gamma a_2^2$.

Следующая теорема является следствием из [1, теорема 1].

Теорема 3. *Пусть конечное нильпотентное p-кольцо R не изоморфно кольцам R_5 — R_{10}. Пусть φ — проектирование кольца R на кольцо R^φ. Тогда R^φ — нильпотентное p-кольцо.*

Замечание 2. Для колец R_5 — R_{10} существуют проектирования φ, для которых равенство (1) не выполняется.

4. Проектирования конечных колец с собственным радикалом

Пусть $\operatorname{Rad} R$ — собственное подкольцо в R. Рассмотрим сначала случай, когда $\operatorname{Rad} R$ является прямым слагаемым в R. Определим кольца $R_{i,j}$ следующим образом:

$$R_{i,j} = R_i \oplus R_j, \text{ где } i = \overline{1,4} \text{ и } j = \overline{5,7}.$$

Согласно теореме 1 [2] решётки подколец колец $R_{i,j}$ разложимы в прямое произведение решёток подколец $L(R_i)$ и $L(R_j)$ для $i = \overline{1,4}$ и $j = \overline{5,7}$. Имеет место

Теорема 4. *Пусть конечное p-кольцо R разложимо в прямую сумму полупростого кольца S и нильпотентного кольца N. Предположим, что R не изоморфно ни одному из колец $R_{i,j}$, где $i = \overline{1,4}$ и $j = \overline{5,7}$. Тогда для любого решёточного изоморфизма φ кольца R на кольцо R^φ выполняется равенство (1).*

Замечание 3. Для колец $R_{i,j}$, где $i = \overline{1,4}$ и $j = \overline{5,7}$, существуют проектирования φ, для которых равенство (1) не выполняется.

Согласно [8, теорема XIX.5] любое конечное p-кольцо R с единицей содержит подкольцо S, удовлетворяющее условиям:

$$R = S \oplus N, \tag{2}$$

где $\operatorname{Rad} S = pS$, N — (S,S)-бимодуль из $\operatorname{Rad} R$, $R/\operatorname{Rad} R \cong S/pS$ и S разложимо в прямую сумму матричных колец, рассматриваемых над кольцами Галуа. Следовательно, изучение решёточных изоморфизмов конечных колец связано с изучением проективных образов колец Галуа $GR(p^k, m)$ и матричных колец над ними. Проектирования колец Галуа изучались в работе [4]. Согласно [4, свойство 10] равенство (1) выполняется для любого проектирования φ кольца Галуа $R = GR(p^k, m)$ при $k \geqslant 2$, $m \geqslant 2$. Этот факт, а также следующие две теоремы полностью решают вопрос о выполнимости равенства (1) для случая, когда (S,S)-бимодуль N равен нулю.

Теорема 5. *Пусть $R = M_n(K)$, где $K = GR(p^k, m)$, $n > 1$, $k \geqslant 1$, $m \geqslant 1$. Пусть φ — проектирование кольца R на кольцо R^φ. Тогда $(Rad\, R)^\varphi = Rad\, R^\varphi$.*

Теорема 6. *Пусть конечное кольцо R разложимо в прямую сумму колец: $R = R_1 \oplus \cdots \oplus R_l$, где $l > 1$, $R_i \cong M_{n_i}(K_i)$, $n_i \geqslant 1$, $K_i \cong GR(p^{k_i}, m_i)$ $(i = \overline{1,l})$. Предположим, что в случае, когда $l = 2$, кольцо R не изоморфно кольцам R_3 и R_4. Пусть φ — решёточный изоморфизм кольца R на кольцо R^φ. Тогда $(Rad\, R)^\varphi = Rad\, R^\varphi$.*

Замечание 4. Пусть $R_{11} = \langle e \rangle$, где $e^2 = e$, $o(e) = p^k$. Очевидно, что решётка $L(R_{11})$ — конечная цепь и потому кольцо R_{11} решёточно изоморфно кольцам R_1, R_5, R_6. Отсюда следует, что для R_{11} равенство (1) выполнимо не всегда.

Перейдём к случаю, когда $N \neq \{0\}$. В этом случае решётка подколец $L(R)$ не является цепью. Определим 4 конечных p-кольца с собственным радикалом Джекобсона:

$R_{12} = \langle e, r \rangle$, $e^2 = e$, $o(e) = p^2$, $o(r) = p$, $er = re = r$, $r^2 = \gamma pe$, причем либо $\gamma = 1$, либо γ не является квадратом в $GF(p)$, $p \neq 2$;

$R_{13} = \langle e, r \rangle$, $e^2 = e$, $o(e) = 2^2$, $r^2 = 0$, $o(r) = 2$, $er = re = r$;

$R_{14} = \langle e, r \rangle$, $e^2 = e$, $o(e) = 2^2$, $r^2 = 0$, $o(r) = 2$, $er = re = 0$;

$R_{15} = \langle e \rangle + N_0$, где $e^2 = e$, $o(e) = p^k$, $o(r) = p$, $er = r$ и $re = 0$ (или $er = 0$ и $re = r$) для любого $r \in N_0$, N_0 — ненулевое кольцо с нулевым умножением.

Замечание 5. Для колец R_{12} — R_{15} равенство (1) выполнимо не всегда, так как $L(R_{12}) \cong L(R_2)$, $L(R_{13}) \cong L(R_3)$, $L(R_{14}) \cong L(R_3)$, а кольцо R_{15} решёточно изоморфно кольцу с нулевым умножением.

Теорема 7. *Пусть конечное p-кольцо R не изоморфно кольцам R_{11} — R_{15} и пусть $Rad\, R$ — собственное подкольцо в R. Пусть φ — решёточный изоморфизм кольца R на кольцо R^φ. Тогда $Rad\, R^\varphi$ — собственное подкольцо в R.*

Для конечных коммутативных колец с единицей доказана

Теорема 8. *Пусть конечное коммутативное кольцо R с единицей разложимо в прямую сумму колец T_i $(i = \overline{1,k})$, удовлетворяющих условиям: $T_i = S_i + N_i$, $S_i \cong GR(p^{n_i}, m_i)$, $n_i > 1$, $m_i > 1$, N_i — ненулевой нильпотентный идеал T_i, единица e_i кольца S_i является единицей в T_i $(i = \overline{1,k})$. Пусть φ — решёточный изоморфизм кольца R на кольцо R^φ. Тогда $(Rad\, R)^\varphi = Rad\, R^\varphi$.*

Этот результат обобщает аналогичное утверждение для проектирований конечных однопорождённых колец, рассмотренных в работе [5].

Литература

1. *Коробков С. С.* Проектирования периодических нильколец // Известия вузов. Математика. 1980. № 7. С. 30—38.
2. *Коробков С. С.* Периодические кольца с разложимыми в прямое произведение решётками подколец // Исследование алгебраических систем по свойствам их подсистем. Уральский государственный педагогический университет, 1998. С. 48—59.
3. *Коробков С. С.* Решёточные изоморфизмы конечных колец без нильпотентных элементов // Известия Уральского государственного университета. Математика и механика. 2002. № 22. Вып. 4. С. 81—93.
4. *Коробков С. С.* Проектирования колец Галуа // Алгебра и логика. 2015. Т. 54, № 1. С. 16—33.
5. *Коробков С. С.* Проектирования конечных однопорождённых колец с единицей // Алгебра и логика. 2016. Т. 55, № 2. С. 192—218.
6. *Коробков С. С.* Решёточная определяемость некоторых матричных колец // Математический сборник. 2017. Т. 208, № 1. С. 97—110.
7. *Хмельницкий И. Л.* Кольца, в которых всякая аддитивная подгруппа является подкольцом // Алгебра и математический анализ. Свердловский государственный педагогический институт. 1974. Т. 21. С. 118—138.
8. *McDonald B. R.* Finite rings with identity. New York : Marcel Dekker Incorporated, 1974.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ИЗОТОПЫ АЛГЕБР МИХЕЕВА И ХЕНЦЕЛЯ

А. А. Крылов (Москва)[1]

Понятие изотопа было введено Албертом в 1942 году [7]. Им же было доказано, что при унитальной изотопии сохраняются идеалы, в частности, изотоп простой алгебры является простой алгеброй, если обе алгебры унитальны.

Если A — алгебра с единицей и c — её обратимый элемент, то на пространстве A определим новое умножение $x\cdot_c y = (xc)y$. Новая алгебра $A^{(c)} = (A; +, \cdot_c)$ называется *c-изотопом* алгебры A. Изотоп $A^{(c)}$ называется *центральным*, если элемент c лежит в коммутативном центре, т. е. $[c, A] = 0$.

Алгебра A называется первичной, если для любых её ненулевых идеалов I_1, I_2 произведение I_1I_2 отлично от нуля.

Алгебра A называется *правоальтернативной*, если для любых элементов a и b из A справедливо равенство: $(ab)b = ab^2$.

Пусть H — свободная строго $(-1, 1)$-алгебра с единицей 1 от свободных порождающих a, b. Строение этой алгебры было описано в [8], поэтому H называется *алгеброй Хенцеля*. Пусть M — алгебра Михеева с базисом e, g, h и ненулевыми произведениями базисных элементов: $e^2 = e$, $ge = g$, $g^2 = h$ [4]. *Унитальной алгеброй Михеева* M_0 называется алгебра, полученная внешним присоединением единицы 1 к алгебре M.

Известно [1], что всякий c-гомотоп $M_0^{(c)}$ алгебры Михеева является $(-1, 1)$-алгеброй. Легко понять, что в алгебре Михеева M_0 обратимыми являются элементы вида $\alpha(1 + \beta e + \gamma g + \delta h)$, где $\alpha \neq 0, \beta \neq -1 \in$.

12-мерной алгеброй Михеева M_{12} называется алгебра с таблицей умножения, в которой указаны только ненулевые произведения:

(1) $e_1e_2 = e_5$,
(2) $e_2e_1 = -e_5$, $e_2e_3 = e_8$, $e_2e_5 = e_9$, $e_2e_6 = e_{11}$, $e_2e_{12} = e_{10}$,
(3) $e_3e_2 = e_8$, $e_3e_4 = e_7$, $e_3e_5 = e_{12}$, $e_3e_6 = e_1$, $e_3e_9 = e_{10}$, $e_3e_{11} = e_5$,
(4) $e_4e_5 = e_6$, $e_4e_9 = -e_{11}$, $e_4e_{10} = e_5$, $e_4e_{11} = -e_8$, $e_4e_{12} = e_1$,
(5) $e_5e_2 = -e_9$, $e_5e_3 = -e_{12}$, $e_5e_4 = -e_9$, $e_5e_7 = -e_1$, $e_5e_8 = -e_{10}$,
(6) $e_6e_2 = -e_{11}$, $e_6e_3 = e_1$, $e_6e_8 = e_5$, $e_6e_{11} = e_{10}$,
(7) $e_7e_5 = e_1$, $e_7e_9 = e_5$,
(8) $e_8e_5 = e_{10}$, $e_8e_6 = -e_5$,
(9) $e_9e_4 = e_{11}$, $e_9e_7 = -e_5$,
(10) $e_{10}e_4 = -e_5$,
(11) $e_{11}e_3 = -e_5$.

Получены следующие результаты:

Теорема 1. *Пусть A — первичная унитальная правоальтернативная алгебра и A^* — её главный изотоп. Тогда в каждом из следующих случаев алгебра A^* некоммутативна:*

(а) A — первичная альтернативная алгебра, не являющаяся 2-энгелевой;

(б) A — первичная неассоциативная $(-1, 1)$-алгебра характеристики $\neq 2, 3$;

(в) $A = F \cdot 1 + M_{12}$ — алгебра, полученная внешним присоединением единицы к первичной 12-мерной правоальтернативной алгебре Михеева.

Доказательство теоремы 1 существенно использует [5] и [6].

 Получено 23.10.2017. УДК 512.554

[1]Московский городской педагогический университет. E-mail: oncetoblack@list.ru.

Теорема 2. *Для каждого обратимого элемента $c = \alpha 1 + \beta e + \gamma g + \delta h$ унитальной алгебры Михеева M_0 существует λ-параметрическое семейство изоморфизмов алгебры Михеева в её c-изотоп $\phi : M_0 \to M_0^{(c)}$, каждый из которых задается равенствами:*

$$1^\phi = c^{-1},\ e^\phi = (\alpha+\beta)^{-1}e,\ g^\phi = \lambda g,\ h = \lambda^2(\alpha+\beta)h,\ \text{где } \alpha, \alpha+\beta, \gamma \neq 0.$$

В частности, все изотопы имеют одинаковые идеалы тождеств.

Теорема 3. *Центральные изотопы алгебры Хенцеля изоморфны между собой.*

В доказательстве теоремы 2 существенно используется [8].

Литература

1. *Дедловская М. Е.* Гомотопы $(-1,1)$-алгебр от двух порождающих // Математические заметки. 1996. Т. 59, вып. 4. С. 551—557.
2. *Жевлаков К. А., Слинько А. М., Шестаков И. П., Ширшов А. И.* Кольца, близкие к ассоциативным. М. : Наука, 1978.
3. *Михеев И. М.* О первичных правоальтернативных кольцах с идемпотентом // Математические заметки. 1980. Т. 27, вып. 2. С. 185—191.
4. *Пчелинцев С. В.* О многообразии, порожденном свободной алгеброй типа $(-1,1)$ с двумя порождающими // Сибирский математический журнал. 1981. Т. 22, № 3. С. 162—178.
5. *Пчелинцев С. В.* Первичные альтернативные алгебры, близкие к коммутативным // Известия РАН. Серия математическая. 2004. Т. 68, вып. 1. С. 183—206.
6. *Пчелинцев С. В.* Изотопы первичных $(-1,1)$-алгебр и йордановых алгебр // Алгебра и логика. 2010. Т. 49, № 3. С. 388—423.
7. *Albert A. A.* Non–associative algebras // Ann. Math. 1942. Vol. 43. P. 685—707.
8. *Hentzel I. R.* Nil semi-simple $(-1,1)$-rings // J. Algebra. 1972. Vol. 22, № 3. P. 442—450.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О ПОЧТИ НИЛЬПОТЕНТНЫХ МНОГООБРАЗИЯХ ЛИНЕЙНЫХ АЛГЕБР С ЦЕЛЫМИ ЭКСПОНЕНТАМИ

Н. П. Панов (Ульяновск)[1]

1. Введение

Многообразием алгебр называют класс $\mathbf{V}$ всех алгебр над полем (линейных алгебр), удовлетворяющих некоторому набору тождественных соотношений. Многообразие алгебр почти нильпотентно, если оно не является нильпотентным, но любое его собственное подмногообразие нильпотентно. Если характеристика основного поля Φ равна нулю, то любое тождество эквивалентно некоторой системе полилинейных тождеств, и в абсолютно свободной алгебре $\Phi\{X\}$ с множеством образующих $X = \{x_1, x_2, \ldots\}$ идеал тождеств $Id(\mathbf{V})$ многообразия $\mathbf{V}$ полностью определяется полилинейными тождествами, а именно последовательностью пространств $\{P_n \cap Id(\mathbf{V})\}_{n\geq 1}$, в которой $P_n \subset \Phi\{X\}$ — пространство полилинейных многочленов степени n от образующих $x_1, x_2, \ldots x_n$. Последовательность размерностей $\{c_n(\mathbf{V})\}_{n\geq 1}$, $c_n(\mathbf{V}) = \dim P_n/(P_n \cap Id(\mathbf{V}))$, является одной из основных числовых характеристик многообразия $\mathbf{V}$. Говорят, что её асимптотическое поведение определяет рост многообразия. Если многообразие имеет экспоненциальный рост и существует предел $\lim_{n\to\infty} \sqrt[n]{c_n(\mathbf{V})} = \alpha$, то число α называют экспонентой многообразия $\mathbf{V}$. Если $\mathbf{V}$ нильпотентно, то найдется такое натуральное n_0, что $c_n(\mathbf{V}) = 0$ для всех $n \geq n_0$, и наоборот. Пространство полилинейных элементов $P_n(\mathbf{V})$, $n \geq 1$, рассматривают как вполне приводимый ΦS_n-модуль с характером $\chi_n(\mathbf{V})$, который равен сумме характеров χ_λ с кратностями $m_\lambda(\mathbf{V})$, λ — разбиение числа n, $\lambda \vdash n$, S_n — симметрическая группа.

В работе [3] в классе алгебр над полем нулевой характеристики, удовлетворяющих тождеству $x(yz) \equiv 0$, определено почти нильпотентное многообразие $var(A)$ экспоненты два. С целью изучения многообразия $var(A)$ авторы рассматривали как вполне приводимые ΦS_n-модули пространства полилинейных элементов с фиксированной образующей на первой позиции. Обозначим их через $L_n(var(A))$, соответствующие им кратности обозначим $m^L_\lambda(var(A))$, $\lambda \vdash n$.

В работе [1] определены многообразия $var(A_m)$, $m = 3, 4, \ldots$, в каждом из которых выполняются тождества

$$x(yz) \equiv 0, \tag{1}$$

$$\sum_{\sigma\in S_{m+1}} (-1)^\sigma x_0 X_{\sigma(1)} \ldots X_{\sigma(2)} \ldots X_{\sigma(m+1)} \equiv 0, \tag{2}$$

$$x_0 X^3 \equiv 0, \tag{3}$$

$$x_0 X^2 Z_1 \ldots Z_s Y^2 \equiv 0, \tag{4}$$

где остаток от деления s на m не равен $m-2$, и заглавными буквами обозначены операторы правого умножения на свободные образующие, $x_0X^3 = ((x_0x)x)x$. Известно, что каждое многообразие $var(A_m)$, $m = 3, 4, \ldots$, имеет экспоненту m [1] и является почти нильпотентным [2].

 Получено 17.12.2017. УДК 512.55.

[1]Ульяновский государственный университет. E-mail: nppanov@yandex.ru.

2. Основные результаты

Отметим, что $var(A) = var(A_2)$, и обозначим через $\mathbf{N_m}$, $m = 3, 4, \ldots$, многообразие, определяемое тождествами (1)—(4), $var(A_m) \subseteq \mathbf{N_m}$. Перечислим основные результаты.

Теорема 1. *Многообразие $var(A_m)$ и заданное системой тождеств (1)—(4) многообразие $\mathbf{N_m}$ совпадают, $var(A_m) = \mathbf{N_m}$, $m = 2, 3, \ldots$.*

Суммируем, в том числе приведенные в работе [3], утверждения о кратностях $m_\lambda^L(\mathbf{N_m})$, $m = 2, 3, \ldots$, в следующей теореме.

Теорема 2. *Кратности $m_\lambda^L(\mathbf{N_m})$, $m = 2, 3, \ldots$, определяются следующим образом:*

(1) *если $\lambda = (1^k)$, $1 \leq k \leq m$, то $m_\lambda^L(\mathbf{N_m}) = 1$;*
(2) *если $\lambda = \big((\mathfrak{s}+1)^k, \mathfrak{s}^{m-k}\big)$, $\mathfrak{s} \geq 1$, $1 \leq k \leq m$, то $m_\lambda^L(\mathbf{N_m}) = m$;*
(3) *если $\lambda = \big((\mathfrak{s}+2)^{k_1}, (\mathfrak{s}+1)^{k_2}, \mathfrak{s}^{m-k_1-k_2}\big)$, $\mathfrak{s} \geq 0$, $k_1 \geq 1$, $k_2 \geq 0$, $k_1 + k_2 \leq m-1$, то $m_\lambda^L(\mathbf{N_m}) = k_2 + 1$;*
(4) *$m_\lambda^L(\mathbf{N_m}) = 0$ для всех остальных λ.*

Теорема 3. *Все ненулевые кратности $m_\lambda(\mathbf{N_m})$, $m \geq 2$, определяются следующим образом:*

(1) *если удалением одной клетки из диаграммы λ может быть получена единственная диаграмма μ, для которой $m_\mu^L(\mathbf{N_m}) > 0$, то $m_\lambda(\mathbf{N_m}) = m_\mu^L(\mathbf{N_m})$;*
(2) *если удалением одной клетки из диаграммы λ могут быть получены две различные диаграммы μ_1, μ_2, для которых $m_{\mu_1}^L(\mathbf{N_m}), m_{\mu_2}^L(\mathbf{N_m}) > 0$, то $m_\lambda(\mathbf{N_m}) = m_{\mu_1}^L(\mathbf{N_m}) + m_{\mu_2}^L(\mathbf{N_m})$.*

Литература

1. *Мищенко С. П., Шулежко О. В.* Почти нильпотентные многообразия любой целой экспоненты // Вестник Московского университета. Серия 1: Математика. Механика. 2015. Т. 70, № 2. С. 53—57.
2. *Панов Н. П.* О почти нильпотентных многообразиях с целой экспонентой // Известия Саратовского университета. Новая серия. Сер.: Математика. Механика. Информатика. 2017. Т. 17, № 3. С. 331—343.
3. *Mishchenko S., Valenti A.* An almost nilpotent variety of exponent 2 // Israel Journal of Mathematics. 2014. Vol. 199, № 1. P. 241—257.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ИЗОТОПЫ ПОЧТИ ПРОСТЫХ АЛГЕБР

С. В. Пчелинцев (Москва)[1]

В 1942 г. А. А. Алберт [6] ввел понятие изотопа и начал их изучать. Рассматривая вполне унитальный случай (исходная алгебра и её изотоп унитальны), он доказал, что при вполне унитальной изотопии сохраняются идеалы. Кроме того, если исходная алгебра унитальна и ассоциативна, то изотопия является изоморфизмом.

В работе Р. Х. Брака [7] приведены основные результаты, полученные на тот момент времени. Следуя Р. Х. Браку, конечномерная алгебра называется *изотопно простой*, если всякий её изотоп является простой алгеброй. Известно, что а) всякая конечномерная унитальная простая алгебра изотопно проста; б) над алгебраически замкнутым полем не существует 2-мерных изотопно простых алгебр, но для любого $n \geq 3$ существует простая коммутативная унитальная n-мерная алгебра, значит, изотопно простая алгебра. Примером неунитальной изотопно простой алгебры является простая 3-мерная алгебра Ли sl_2 бесследных матриц. В [7] приведены и другие интересные результаты, например, теорема о наличии в подходящем изотопе конечномерной алгебры композиционного ряда, факторы которого являются изотопно простыми алгебрами. Эта теорема Брака является основным мотивом к изучению изотопно простых алгебр.

В 1952 г. А. И. Мальцев [3] ввел «производные операции» и указал вложение любой конечномерной (неассоциативной) алгебры в «производную алгебру» от полной матричной алгебры. Ему же принадлежит теорема о вложении произвольной алгебры в изотоп подходящей унитальной ассоциативной алгебры.

Частные случаи изотопов, так называемые c-изотопы, оказались полезны при изучении первичных вырожденных альтернативных, йордановых и $(-1, 1)$ алгебр [4, 5].

В [1] был анонсирован ряд результатов о структуре изотопно простых 3-мерных алгебр в классах антикоммутативных и коммутативных алгебр с базисом из ниль-элементов порядка 2. Кроме того, там же приведены некоторые результаты об изотопах «круговых» алгебр $C_n^{\pm}$ при $n \geq 4$. В частности, оказалось, что круговые алгебры изотопно просты; изотоп антикоммутативной алгебры C_4^- может быть коммутативен; изотоп коммутативной алгебры C_4^+ может быть антикоммутативен. Вопрос об изотопности алгебр C_4^- и C_4^+ открыт.

Данная работа посвящена изучению изотопов простых алгебр произвольной размерности и их применениям. Получены следующие результаты.

Теорема 1. *Всякая конечномерная алгебра вложима в конечномерную простую алгебру.*

Этот результат подсказан теоремой Мальцева о производных операциях, а её доказательство основано на использовании подходящего изотопа.

Алгебра A называется *почти простой*, если для каждого собственного идеала $I \lhd A$ факторы I и A/I бесконечномерны. Конечномерная почти простая алгебра является простой. Изотоп алгебры с делением является алгеброй с делением. Однако, изотоп простой алгебры может содержать тривиальные идеалы (см. теорему 4).

Теорема 2. *Изотоп почти простой унитальной алгебры является почти простой алгеброй. В частности, конечномерная унитальная простая алгебра является изотопно простой алгеброй.*

 Получено 17.12.2017. УДК 512.554.

[1]Финансовый университет при Правительстве РФ. E-mail: pchelinzev@mail.ru.

Известно, что всякая простая 3-мерная антикоммутативная алгебра изотопна алгебре sl_2 [1], значит, является изотопно простой. Далее, известна теорема Шафера [8] об изотопах алгебры Кэли–Диксона $C = C(F)$ над полем F: *всякий унитальный изотоп алгебры C изоморфен C*. По теореме Кузьмина [2] центральная простая нелиева конечномерная алгебра Мальцева изоморфна алгебре C_7, совпадающей с фактор-алгеброй $C^-/F \cdot 1$.

Теорема 3. *Простая алгебра Мальцева C_7 изотопно проста. В частности, C_7 не является изотопом никакой алгебры Ли. Если изотоп C_7 является алгеброй Мальцева, то он изоморфен C_7.*

Пусть $A = J(V, f) = \Phi \cdot 1 + V$ — йорданова алгебра невырожденной симметрической билинейной формы f на V, причем пространство V имеет счетный ортонормированный базис e_i, $i = \pm 1, \pm 2, ...$

Теорема 4. *Изотоп алгебры $J(V, f)$ может содержать ненулевой идеал с нулевым умножением.*

Теорема 5. *Пусть F_∞ — алгебра с набором базисных элементов e_{ij}, $i, j \geq 1$ и умножением: $e_{ij} \cdot e_{kl} = \delta_{jk} e_{il}$, где δ_{jk} — символ Кронекера. Тогда изотоп алгебры F_∞ является почти простой алгеброй.*

Литература

1. *Крылов А. А., Пчелинцев С. В.* Изотопно простые алгебры с ниль-базисом // Мальцевские чтения, 2017 : тезисы докладов Международной научной конференции, Новосибирск, 20–24 ноября 2017 г. Новосибирск : НГУ, 2017. С. 121.
2. *Кузьмин Е. Н.* Структура и представления конечномерных алгебр Мальцева // Исследования по теории колец и алгебр. Новосибирск : Наука. Сибирское Отделение, 1989. (Труды Академии наук СССР (Сибирское отделение). Институт математики. Вып. 16).
3. *Мальцев А. И.* Об одном представлении неассоциативных колец // Успехи математических наук. 1952. Т. 7, № 1. С. 181—185.
4. *Пчелинцев С. В.* Изотопы первичных $(-1, 1)$-алгебр и йордановых алгебр // Алгебра и логика. 2010. Т. 49, № 3. С. 388—423.
5. *Пчелинцев С. В.* Изотопы альтернативного монстра и алгебры Скосырского // Сибирский математический журнал. 2016. Т. 57, № 4. С. 850—865.
6. *Albert A. A.* Non-associative algebras // Ann. Math. 1942. Vol. 43. P. 685—707.
7. *Bruck R. H.* Some results in the theory of linear non-associative algebras // Trans. Amer. Math. Soc. 1944. Vol. 56. P. 141—199.
8. *Schafer R. D.* Alternative algebras over an arbiyrary filds // Bull. Amer. Math. Soc. 1943. Vol. 49. P. 549—555.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О ПУЧКАХ ПОЛУКОЛЕЦ $C^\infty(X)$

Н. В. Шалагинова (Киров)[1]

1. Введение

Теория полуколец непрерывных функций сравнительно новое направление функциональной алгебры, активное развитие которого началось с 90-х гг. прошлого века. К исследованию колец и полуколец непрерывных функций может быть применен пучковый подход. Для колец это было сделано в [4], для полуколец — в [3]. Главная роль при исследовании отводится пучку ростков непрерывных (неотрицательных) функций. Его слои использовались как при изучении самих полуколец функций, так и при изучении топологических пространств. Применим данный подход для изучения полуколец непрерывных функций со значениями в полукольце $(0,\ \infty]$.

Напомним, что *полукольцом* называется алгебраическая система $\langle S, +, \cdot\rangle$, в которой $\langle S, +\rangle$ — коммутативная полугруппа, $\langle S, \cdot\rangle$ — полугруппа, выполняются законы дистрибутивности операции умножения $\cdot$ относительно сложения $+$. Полукольцо с коммутативной операцией умножения называется *коммутативным*; с нейтральным элементом по умножению — полукольцом с единицей 1. Элемент $a \in S$ называется *аддитивно* (*мультипликативно*) *поглощающим*, если $a + s = s + a = a$ ($as = sa = a$) для любого $s \in S$; поглощающим, если он одновременно аддитивно и мультипликативно поглощающий.

Отношение эквивалентности на полукольце S называется *конгруэнцией*, если оно согласовано с полукольцевыми операциями. Семейство конгруэнций (ρ_x) полукольца S, индексированное точками топологического пространства X, называется *открытым*, если для любых $a, b \in S$ множество $\{x \in X\colon a\rho_x b\}$ открыто в X.

Непустое подмножество I полукольца S называется *идеалом*, если $x+y, sx, xs \in I$ для любых $x, y \in I$ и $s \in S$. Идеал I, отличный от полукольца S, называется: *простым*, если для любых $a, b \in S$ принадлежность $ab \in I$ влечет $a \in I$ или $b \in I$; *биидеалом*, если $a+b \in I$ для любых $a \in I$ и $b \in S$.

Тройка $\mathbf{P} = (P, \pi, X)$ называется *пучком полуколец*, если выполняются следующие условия:

(1) P и X — топологические пространства;
(2) $\pi\colon P \to X$ — локальный гомеоморфизм;
(3) для каждой точки $x \in X$ множество $P_x = \pi^{-1}(x)$ является полукольцом;
(4) полукольцевые операции непрерывны;
(5) отображения $\hat{0}$ и $\hat{1}$, ставящие каждой точке $x \in X$ соответственно нуль 0 и единицу 1 полукольца P_x (если они существуют), непрерывны.

Имеем $P = \dot{\bigcup}_{x\in X} P_x$.

Полукольцо P_x называется *слоем* пучка в точке x при проекции π. Пространства P и X называются *накрывающим* и *базисным* соответственно. Пусть Y — открытое множество в X. *Сечением* (локальным) пучка $\mathbf{P}$ над Y называется такое непрерывное отображение $\sigma\colon Y \to P$, что $\pi \circ \sigma$ — тождественное отображение множества Y. Сечение, определенное над всем пространством X, называется *глобальным*. Множество $\Gamma(\mathbf{P}) = \Gamma(P, X)$ всех глобальных сечений пучка $\mathbf{P}$ полуколец над X с поточечно определенными операциями является полукольцом.

 Получено 25.12.2017. УДК 512.556.

[1]Вятский государственный университет. E-mail: korshunnv@mail.ru.

Функциональным представлением полукольца S называется полукольцевой гомоморфизм $\alpha\colon S \to \Gamma(P, X)$ полукольца S в полукольцо $\Gamma(P, X)$ глобальных сечений некоторого пучка $\mathbf{P}$ полуколец над топологическим пространством X.

Предпучком $\boldsymbol{P}$ полуколец на X называется функция, сопоставляющая каждому открытому множеству $U \subseteq X$ полукольцо $P(U)$ и каждой паре открытых множеств $U \subseteq V$ — гомоморфизм $r_U^Y\colon P(V) \to P(U)$, называемый *ограничением*, такой что $r_U^U = 1$ и $r_U^V \circ r_V^W = r_U^W$, где $U \subseteq V \subseteq W$.

Для произвольного пучка $\mathbf{P}$ множество $\Gamma(U)$ всех его локальных сечений над $U \subseteq X$ с гомоморфизмами ограничений $r_U^V\colon \Gamma(V) \to \Gamma(U)$, $r_U^V(s) = s|_U$ для любого $s \in \Gamma(V)$, образует предпучок над X, называемый каноническим предпучком пучка $\mathbf{P}$.

Пусть $\boldsymbol{P}$ — предпучок над X и $x \in X$. Введем отношение ρ_x на множестве сечений над открытыми окрестностями точки x. Если $s \in \boldsymbol{P}(U)$, $t \in \boldsymbol{P}(V)$, $x \in U \cap V$, то

$$s\rho_x t \Leftrightarrow r_W^U(s) = r_W^V(t) \Leftrightarrow s|_W = t|_W$$

для некоторой окрестности W точки x. Очевидно, что ρ_x — отношение эквивалентности.

Пусть P_x — множество всех классов эквивалентности по отношению ρ_x. Обозначим $P = \dot{\bigcup}_{x\in X} P_x$. Отображение $\pi\colon P \to X$ определяется формулой $\pi(s) = x$, если $s \in P_x$. Для любого $s \in \boldsymbol{P}(U)$ элемент $s_x \in \boldsymbol{P}$ переводит сечение s в точку x. Положим

$$s_U = \{s_x\colon x \in U\} \subseteq P.$$

Для открытых множеств $U \subseteq X$ подмножества s_U образуют базу топологии на P. Имеем (P, π, X) — пучок ростков предпучка $\boldsymbol{P}$ над X.

Для $s \in \boldsymbol{P}(U)$ отображение $x \to s_x, x \in U$, является локальным сечением пучка P над U. Рассмотрим естественное отображение $\Phi_U\colon \boldsymbol{P}(U) \to P(U)$.

Отображение Φ_U инъективно тогда и только тогда, когда выполняется условие:

P1. Пусть $s,\ t \in \boldsymbol{P}(U)$ и существует такое открытое покрытие $\{U_\alpha\}$ множества U, что $r_{U_\alpha}^U(s) = r_{U_\alpha}^U(t)$ для всех α. Тогда $s = t$.

Пусть Φ_V инъективно для любого открытого подмножества $V \subseteq U$. Тогда Φ_U сюръективно и, значит, биективно тогда и только тогда, когда выполняется условие:

P2. Пусть $\{U_\alpha\}, \alpha \in I$ — открытое покрытие множества U, элементы $s_\alpha \in \boldsymbol{P}(U_\alpha)$ удовлетворяют условию

$$r_{U_\alpha\cap U_\beta}^{U_\alpha}(s_\alpha) = r_{U_\alpha\cap U_\beta}^{U_\beta}(s_\beta)$$

для всех $\alpha, \beta \in I$. Тогда существует такой элемент $s \in P(U)$, что $r_{U_\alpha}^U(s) = s_\alpha$ для всех α.

Предпучок $\boldsymbol{P}(U)$ над X, удовлетворяющий условиям P1 и P2, называется *пучком* над X. Таким образом, имеем два эквивалентных определения пучка полуколец над X.

Топологическое пространство называется *тихоновским*, если оно гомеоморфно подпространству некоторой тихоновской степени $\mathbf{R}$.

2. Пучки полуколец $C^\infty(X)$

Множество $(0,\ \infty]$ является полукольцом без нуля с единицей и поглощающим элементом ∞. Обозначим $C^\infty(X) = C(X, (0,\ \infty])$ полукольцо всех непрерывных $(0,\ \infty]$-значных функций с поточечно определенными операциями сложения и умножения функций [1]. Для каждой функции $f \in C^\infty(X)$ определим H-*множество*:

$$\mathrm{H}(f) = f^{-1}(\infty)$$

Зафиксируем точку $x \in X$ и рассмотрим конгруэнцию $\sim_x$ на $C^\infty(X)$: для любых функций $f, g \in C^\infty(X)$

$$f \sim_x g \Leftrightarrow f = g \text{ на некоторой окрестности } U \text{ точки } x.$$

Множество вида

$$M_x = \{f \in C^\infty(X)\colon f(x) = \infty\}$$

для $x \in X$ является простым биидеалом. Если $fg \in M_x$, то очевидно одна из функций f или g должна принадлежать идеалу и если $f \in M_x$, то $f + g \in M_x$ для любой функции $g \in C^\infty(X)$.

Конгруэнция ρ_{M_x} по идеалу M_x определяется следующим образом: для любых функций $f, g \in C^\infty(X)$

$$f \rho_{M_x} g \Leftrightarrow \exists h \in C^\infty(X)\colon h(x) < \infty \text{ и } fh = gh.$$

Предложение 1. *Для полукольца $C^\infty(X)$ верны следующие утверждения:*

(1) *семейство конгруэнций $\sim_x$ является открытым;*
(2) *семейство конгруэнций ρ_{M_x} является открытым.*

Аналогично случаю полуколец $C^+(X)$[2] рассмотрим три пучка для полуколец $C^\infty(X)$.

Пучок θ_X полуколец $C^\infty(X)/\sim_x$ над X и соответствующее факторное представление $\alpha_1\colon C^\infty(X) \to \Gamma(\theta_X)$, индуцированные открытым семейством конгруэнций $(\sim_x)_{x\in X}$. Представление α_1 является изоморфным представлением полукольца $C^\infty(X)$ в пучке θ_X полуколец $C^\infty(X)/\sim_x$.

Пучок ε_X полуколец $C^\infty(X)/\rho_{M_x}$ над X, порожденный открытым семейством конгруэнций $(\rho_{M_x})_{x\in X}$. Соответствующее факторное представление $\alpha_2\colon C^\infty(X) \to \Gamma(\varepsilon_X)$, индуцированное этим же семейством конгруэнций, также является изоморфным представлением полукольца $C^\infty(X)$ в пучке ϵ_X полуколец $C^\infty(X)/\rho_{M_x}$.

Пучок ϕ_X полуколец ростков непрерывных $(0,\infty]$-значных функций над X определяется как предпучок полуколец $C^\infty(A)$ по всем открытым подмножествам A пространства X с гомоморфизмами ограничения. Элементами слоя пучка ϕ_X служат ростки непрерывных функций, каждый из которых представляет собой класс всевозможных непрерывных $(0,\infty]$-значных функций, определенных на окрестностях точки x и равных на подходящих «малых» окрестностях X. При этом полукольцо $C^\infty(X)$ канонически отождествляется с подполукольцом глобальных сечений пучка ϕ_X полукольца $\Gamma(\phi_X)$.

Изоморфное представление α_3, заданное с помощью отображения $\widehat{}\colon C^\infty(X) \to \Gamma(\phi_X)$, полукольца $C^\infty(X)$ в пучке ϕ_X. Для полукольца $C^\infty(X)$ верно

Предложение 2. *Имеют место следующие утверждения:*

(1) *Каждое из функциональных представлений α_1, α_2, α_3 полукольца $C^\infty(X)$ является изоморфным представлением.*
(2) *Если X — тихоновское пространство, то пучки θ_X, ε_X и ϕ_X совпадают.*

Обозначим через $C^\infty(X)_x$, $x \in X$ фактор-полукольцо $C^\infty(X)/\sim_x$. В случае пучка θ_X полукольцо $C^\infty(X)_x$ является слоем. В случае пучка ϕ_X полукольцо $C^\infty(X)_x$, $x \in X$ будет полукольцом ростков непрерывных $(0,\infty]$-значных функций, определенных на окрестностях точки x и равных на подходящих «малых» окрестностях X. Для тихоновского пространства X полукольцо $C^\infty(X)_x$ является слоем для всех трех пучков.

В терминах полуколец $C^\infty(X)$ уточним определение P-точки: если x — P-точка, то для любой функции $f \in C^\infty(X)$ из $x \in \mathrm{H}(f)$ следует $x \in \mathrm{H}^\circ(f)$.

Предложение 3. *Для любой точки $x \in X$ эквивалентны следующие утверждения:*

(1) *x — P-точка;*
(2) *$C^\infty(X)_x \cong (0,\infty]$;*
(3) *$C^\infty(X)_x$ — регулярное полукольцо.*

Литература

1. *Вечтомов Е. М., Шалагинова Н. В.* Полукольца непрерывных $(0, \infty]$-значных функций // Фундаментальная и прикладная математика. 2015. Т. 20, № 6. С. 43—64.
2. *Шалагинова Н. В.* Три пучка для полуколец непрерывных функций // Лобачевские чтения-2010: Материалы IX Всероссийской молодежной научной школы-конференции. Казань : КФУ, 2010. Т. 40. С. 367—372.
3. *Шалагинова Н. В.* О полукольцах ростков непрерывных неотрицательных функций // Научно-технический вестник Поволжья. 2011. № 3. С. 40—43.
4. *Vechtomov E. M.* Rings of continuous functions with values in topologicals division ring // J. Math. Sci. 1996. Vol. 78, № 6. P. 702—753.

Секция 3

ПОЛУГРУППЫ И УНИВЕРСАЛЬНЫЕ АЛГЕБРЫ

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О СВОЙСТВАХ ПОЛУГРУПП МНОГОЗНАЧНЫХ ПРЕОБРАЗОВАНИЙ, СОХРАНЯЮЩИХ ЗАДАННОЕ БИНАРНОЕ ОТНОШЕНИЕ

Г. Г. Артамонов (Москва)[1], В. А. Ярошевич (Москва)[2]

Все преобразования заданного множества X можно разделить на полные $T(X)$, частичные $P(X)$ и многозначные $B(X)$. Очевидно, что $T(X) \subset P(X) \subset B(X)$. Чем шире класс преобразований, тем больше свободы в выборе определения того, что некоторое преобразование α сохраняет заданное на X бинарное отношение σ. Обозначим подполугруппы полугрупп $T(X)$, $P(X)$ и $B(X)$, сохраняющие в некотором смысле заданное на X отношение σ, через $T_\sigma(X)$, $P_\sigma(X)$ и $B_\sigma(X)$ соответственно. В большей степени изучена $T_\sigma(X)$ [1, 3, 4], есть отдельные результаты для $P_\sigma(X)$ и $B_\sigma(X)$ [2, 5]. Далее предложены три определения $B_\sigma(X)$ и рассмотрены свойства соответствующих $B_\sigma(X)$.

Определение 1. Бинарное отношение $\alpha \in B(X)$ *согласуется* с σ, если $\sigma\alpha \subseteq \alpha\sigma$.

Множество соответствующих бинарных отношений α обозначим через $B_\sigma(X)$

Теорема 1. *Для цепи X такой, что $|X| \geq 2$, полугруппа $B_\sigma(X)$ не является регулярной.*

В [2] было показано, что при $|X| \geq 3$ полугруппа $B(X)$ нерегулярна.

Теорема 2. *Для любого отношения эквивалентности σ, заданного на множестве X таком,что $|X| \geq 3$, полугруппа $B_\sigma(X)$ является нерегулярной.*

Определение 2. Будем говорить, что элемент $\alpha \in B(X)$ *сохраняет σ в широком смысле*, если

$$\forall x, y \in X\ (x, y) \in \sigma \Rightarrow (\exists u \in x\alpha\ \exists v \in y\alpha : (u, v) \in \sigma).$$

Обозначим множество бинарных отношений, сохраняющих бинарное отношение σ в широком смысле, через $B'_\sigma(X)$. Нетрудно установить, что $B'_\sigma(X)$ — полугруппа.

Для случая, когда $|X| \leq 2$ непосредственной проверкой легко получается, что полугруппа $B'_\sigma(X)$ регулярна.

Теорема 3. *Пусть X — множество с заданным бинарным отношением σ и $|X| \geq 3$. Тогда полугруппа бинарных отношений $B'_\sigma(X)$ нерегулярна.*

Определение 3. Будем говорить, что элемент $\alpha \in B(X)$ *сохраняет σ в узком смысле*, если

$$\forall x, y \in X\ \forall u, v \in X\ (u \in x\alpha\ \&\ v \in y\alpha\ \&\ (x, y) \in \sigma) \Rightarrow (u, v) \in \sigma.$$

Обозначим множество бинарных отношений, сохраняющих бинарное отношение σ в узком смысле, через $B''_\sigma(X)$. Нетрудно установить, что $B''_\sigma(X)$ — полугруппа.

В работе [5] показано, что в случае, если X — частично упорядоченное множество, полугруппа $P_\leq(X)$ регулярна в том и только в том случае, если X — антицепь или цепь. Несложно проверить, что при $|X| \leqslant 2$ полугруппа $B''_\sigma(X)$ регулярна.

Теорема 4. *Пусть X — множество такое, что $|X| \geq 3$, а σ — заданное на X отношение эквивалентности. Полугруппа $B''_\sigma(X)$ регулярна в том и только в том случае, когда σ — отношение равенства на множестве X.*

 Получено 15.01.2018. УДК 512.534.5.

[1]Национальный исследовательский университет «МИЭТ». E-mail: glebarta@mail.ru.

[2]Национальный исследовательский университет «МИЭТ». E-mail: v-yaroshevich@ya.ru.

Литература

1. *Айзенштат А. Я.* Регулярные полугурппы эндоморфизмов упорядоченных множеств // Ученые записки Ленинградского государственного педагогического института им. А. И. Герцена. 1968. Т. 387. С. 3—11.
2. *Зарецкий К. А.* Полугруппа бинарных отношений // Математический сборник. 1963. Т. 61 (103), № 3. С. 291—305.
3. *Ким В. И., Кожухов И. Б.* Условия регулярности полугруппы изотонных преобразований счетных цепей // Фундаментальная и прикладная математика. 2006. Т. 12, № 8. С. 97—104.
4. *Ким В. И., Кожухов И. Б., Ярошевич В. А.* Слабо регулярные полугруппы изотонных преобразований // Фундаментальная и прикладная математика. 2012. Т. 17, № 4. С. 145—165.
5. *Ярошевич В. А.* Полугруппы частичных изотонных преобразований. Москва : МИЭТ, 2009.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О КВАЗИПОЛУРЕШЁТКАХ БИНАРНЫХ ОТНОШЕНИЙ

Д. А. Бредихин (Саратов)[1]

1. Введение

Множество бинарных отношений Φ, замкнутое относительно некоторой совокупности Ω операций над ними, образует алгебру (Φ, Ω), называемую *алгеброй отношений*. Основы алгебраического подхода к изучению алгебр отношений были заложены Тарским [16]. В настоящее время теория алгебр отношений является существенной составной частью алгебраической логики, имеющей многочисленные приложения в теоретической кибернетике.

Класс алгебр, изоморфных алгебрам отношений с операциями из Ω, обозначим $R\{\Omega\}$. Операции над отношениями могут быть заданы с помощью формул исчисления предикатов первого порядка. Такие операции называются *логическими*. Классы алгебр отношений $R\{\Omega\}$ с логическими операциями являются элементарно аксиоматизируемыми [14]. При изучении различных классов алгебр отношений естественным образом возникают следующие проблемы.

1. *Найти систему элементарных аксиом для класса* $R\{\Omega\}$.
2. *Выяснить, является ли этот класс квазимногообразием.*
3. *Выяснить, является ли этот класс многообразием.*
4. *Найти базис тождеств многообразия, порождённого этим классом.*

Тарским был рассмотрен класс $R\{\circ, {}^{-1}, \cup, \cap, {}^{-}, \emptyset, \Delta, U \times U\}$, где $\circ$ и ${}^{-1}$ — операции умножения и обращения отношений; $\cup, \cap, {}^{-}$ — булевы операции; $\emptyset$ — пустое множество, Δ — тождественное отношение, $U \times U$ — универсальное отношение. Им было доказано, что указанный класс не является квазимногообразием, а квазимногообразие, порождённое этим классом, образует многообразие. В дальнейшем Линдоном [12] был найден бесконечный базис тождеством для этого многообразия, а Манком [13] было доказано, что указанное многообразие не является конечно базируемым.

Как правило, операции алгебр отношения могут быть выражены через операции алгебры отношений Тарского. Такие алгебры отношений называются обобщёнными подредуктами алгебр отношений Тарского [10]. Исследованию перечисленных выше проблем для различных классов подредуктов алгебр отношения Тарского посвящены работы многочисленных авторов. Так, Йонсоном [11] был рассмотрен класс $R\{\circ, {}^{-1}, \cap, \Delta\}$, играющий важную роль в теории решёток. Им было доказано, что указанный класс образует квазимногообразие, найден его базис квазитождеств, а также поставлена проблема 4 для этого класса, отрицательное решение которой было получено в [5]. С обзором некоторых результатов в этом направлении можно ознакомиться в [10, 14, 15].

Операция над отношениями называется *диофантовой* [1, 2] (в другой терминологии *примитивно-позитивной* [6]), если она может быть задана с помощью формулы, которая в своей префиксной нормальной форме содержит лишь операции конъюнкции и кванторы существования. К числу диофантовых относятся все операции упомянутой выше алгебры отношений Йонсона. Предметом нашего рассмотрения будут классы алгебр отношений с одной дифантовой бинарной операцией, то есть *группоиды отношений*. Подробную мотивацию подобного рода исследований, а также ряд результаты в этом направлении можно найти в работах автора [3, 4, 7, 8, 9].

 Получено 19.11.2017. УДК 501.01.

[1]Саратовский государственный университет им. Н. Г. Чернышевского. E-mail: bredikhin@mail.ru.

2. Формулировка основных результатов

Под группоидом мы понимаем алгебру $(A, \cdot)$ с одной бинарной операцией. Со всяким тождеством $\alpha = \beta$ группоида, где α и β — группоидные термы, можно ассоциировать два новых тождества: $u(\alpha) = u(\beta)$ и $(\alpha)u = (\beta)u$. Назовём группоид *квазиидемпотентным*, если он удовлетворяет тождествам $ux^2 = ux$ и $x^2u = xu$; *квазикоммутативным*, если он удовлетворяет тождествам $u(xy) = u(yx)$ и $(xy)u = (yx)u$; *квазиассоциативным*, если он удовлетворяет тождествам $u((xy)z) = u(x(yz))$ и $u((xy)z) = u(x(yz))$. Всякий квазиидемпотентный, квазикоммутативный и квазиассоциативный группоид назовём *квазиполурешеткой*.

Сосредоточим внимание на следующей бинарной диофантовой операции $*$ над отношениями $\rho, \sigma \subseteq U \times U$, определяемой формулой $\rho * \sigma = \{(v, w) \in U \times U : (v, v) \in \rho \wedge (w, w) \in \sigma\}$. Заметим, что эта операция выразима через операции алгебры отношения Тарского следующим образом $\rho * \sigma = (\rho \cap \Delta) \circ (U \times U) \circ (\sigma \cap \Delta)$, то есть группоид $(\Phi, *)$ является обобщенным подредуктом алгебры отношений Тарского.

Теорема 1. *Группоид $(A, \cdot)$ принадлежит многообразию, порожденному классом $R\{*\}$ тогда и только тогда, когда он является квазиполурёшеткой.*

Теорема 2. *Класс $R\{*\}$ не является ни квазимногообразием, ни многообразием. Квазиполурешетка $(A, \cdot)$ принадлежит классу $R\{*\}$ тогда и только тогда, когда он удовлетворяет следующим аксиомам:*

$$xy = zu \Rightarrow yx = uz,$$
$$xy = uv \Rightarrow (x^2 = z^2 \vee (xy)t = t(xy)),$$
$$(xy)t = t(xy) = xy \Rightarrow (xu = ux = x \vee yv = vy = y).$$

Литература

1. *Бредихин Д. А.* О квазитождествах алгебр отношений с диофантовами операциями // Сибирский математический журнал. 1997. Т. 38. С. 29—41.
2. *Бредихин Д. А.* Об алгебрах отношений с диофантовыми операциями // Доклады Российской Академии Наук. 1998. Т. 360. С. 594—595.
3. *Бредихин Д. А.* О многообразии группоидов бинарных отношений // Известия Саратовского университета. Новая серия. Сер.: Математика. Механика. Информатика. 2013. Т. 13, вып. 1, ч. 1. С. 93—98.
4. *Бредихин Д. А.* О многообразии группоидов отношений с диофантовыми операциями // Известия Саратовского университета. Новая серия. Сер.: Математика. Механика. Информатика. 2013. Т. 13, вып. 4, ч. 2. С. 28—34.
5. *Andreka H., Bredikhin D. A.* The equational theory of union-free algebras of relations // Algebra Univers. 1994. Vol. 33. P. 516—532.
6. *Böner P., Pöschel F. R.* Clones of operations on binary relations // Contributions to general algebras. 1991. Vol. 7. P. 50—70.
7. *Bredikhin D. A.* On relation algebras with general superpositions // Colloq. Math. Soc. J. Bolyai. 1994. Vol. 54. P. 11—124.
8. *Bredikhin D. A.* On varieties of groupoids of relations with operation of binary cylindrification // Algebra Universalis. 2015. Vol. 73. P. 43—52.
9. *Bredikhin D. A.* Varietes of groupoids associated with involuted restrictive bisemigroups of binary relations // Semigroup Forum. 1992. Vol. 44. P. 87—92.
10. *Hodkinson D., Mikulas S.* Axiomatizability of reducts of algebra of relations // Algebra Universalis. 2000. Vol. 43. P. 127—156.
11. *Jónsson B.* Representation of modular lattices and of relation algebras // Trans. Amer. Math. Soc. 1959. Vol. 92. P. 449—464.
12. *Lyndon R. C.* The representation of relation algebras, II // Ann. Math. 1956. Vol. 63. P. 294—307.
13. *Monk D. M.* On representable relation algebras // Michigan Math. J. 1964. Vol. 11. P. 207—210.
14. *Schein B. M.* Relation algebras and function semigroups // Semigroup Forum. 1970. Vol. 1. P. 1—62.
15. *Schein B. M.* Reprezantation of subreducts of Tarski relation algebras Algebraic Logic. North-Holland Publishing Company, 1991. P. 621—635.
16. *Tarski A.* On the calculus of relations // J. Symbolic Logic. 1941. Vol. 4. P. 73—89.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

КОНЕЧНЫЕ ЦИКЛИЧЕСКИЕ ПОЛУКОЛЬЦА БЕЗ ЕДИНИЦЫ[1]

Е. М. Вечтомов (Киров)[2], И. В. Орлова (Киров)[3]

Задача изучения конечных полуколец с циклическим умножением поставлена в работе [2]. Дадим необходимые определения.

Определение 1. *Полукольцом* называется алгебраическая структура $\langle S, +, \cdot\rangle$ с ассоциативными бинарными операциями сложения $+$ и умножения $\cdot$, такими, что умножение дистрибутивно относительно сложения с обеих сторон.

Определение 2. Полукольцо с коммутативным умножением и единицей называется *полуполем*, если каждый его элемент обратим.

Определение 3. Полукольцо S будем называть *циклическим*, если его мультипликативная полугруппа $\langle S, \cdot\rangle$, является циклической (моногенной), то есть порождается *образующим* элементом $a \in S$:

$$S = (a) = \{a^m : m \in \mathbb{N}\} \quad \text{или} \quad S = \{a^m : m \in \mathbb{N} \cup \{0\}\}.$$

В первом случае получаем циклическое полукольцо $S = \{a, a^2, \ldots\}$ без единицы или (циклическое) полуполе, а во втором случае имеем циклическое полукольцо $S = \{a^0, a, a^2, \ldots\}$ с единицей $1 = a^0$.

Циклические полукольца с коммутативным сложением и с единицей начали исследоваться в [2]. Произвольные циклические полукольца с 1 рассматривались в [3]. Циклические полукольца с некоммутативныv сложением и 1 изучались в [5, 6]. Статья [1] посвящена циклическим полукольцам с коммутативным сложением и 1. В пленарном докладе [4] дан обзор развития теории циклических полуколец.

Строение бесконечных циклических полуколец, циклических полуполей, циклических полуколец с нильпотентным образующим известно [2, 5], поэтому будем рассматривать только конечные циклические полукольца без нуля, не являющиеся полуполями.

Любая конечная циклическая полугруппа (a), не являющаяся группой, имеет вид [8]:

$$S = \{a, \ldots, a^k, a^{k+1}, a^{k+2}, \ldots, a^{k+n}\} \quad \text{при} \quad k, n \in \mathbb{N} \quad \text{и} \quad a^{k+n+1} = a^{k+1}, \tag{1}$$

или

$$T = \{1, a, \ldots, a^k, a^{k+1}, \ldots, a^{k+n-1}\} \quad \text{при} \quad k, n \in \mathbb{N} \quad \text{и} \quad a^{k+n} = a^k. \tag{2}$$

Задавая на мультипликативных полугруппах (1) и (2) различные полукольцевые операции сложения, мы получим все конечные циклические полукольца. Биекция $a^m \leftrightarrow a^{m-1}$, $m \in \mathbb{N}$, между множествами (1) и (2) позволяет переносить операцию сложения с (1) на (2), и наоборот. Заметим, что получаемые циклические полукольца S и T имеют изоморфные циклы — циклические полуполя $\{a^{k+1}, a^{k+2}, \ldots, a^{k+n}\}$ и $\{a^k, a^{k+1}, \ldots, a^{k+n-1}\}$, соответственно.

Теорема 1. *Между классом всех конечных циклических полуколец без единицы* (1) *и классом всевозможных конечных циклических полуколец с единицей* (2) *существует естественное взаимно однозначное соответствие.*

 Получено 20.12.2017. УДК 512.55.

[1]Работа выполнена в рамках государственного задания Минобрнауки РФ «Полукольца и их связи», проект № 1.5879.2017/8.9.

[2]Вятский государственный университет. E-mail: vecht@mail.ru.

[3]Вятский государственный университет. E-mail: lubyagina@yandex.ru.

Пример 1. Приведем таблицы Кэли аддитивных полугрупп циклического полукольца $T = \{1, a, a^2\}$, $a^3 = a^2$, и соответствующего полукольца $S = \{a, a^2, a^3\}$, $a^4 = a^3$.

$+$	1	a	a^2
1	a	a^2	a^2
a	a^2	a^2	a^2
a^2	a^2	a^2	a^2

T

$+$	a	a^2	a^3
a	a^2	a^3	a^3
a^2	a^3	a^3	a^3
a^3	a^3	a^3	a^3

S

Таким образом, изучение конечных циклических полуколец без единицы сводится к рассмотрению конечных циклических полуколец с единицей, которые во многом нами уже исследованы [1, 3, 4, 5, 6].

Следствие 1. *Любая конечная циклическая полугруппа без единицы* (1) *допускает структуру циклического полукольца, как с идемпотентным сложением* ($a + a = a$)*, так и с неидемпотентным сложением* ($a + a \neq a$).

Следствие 2. *Идеалы и конгруэнции конечных циклических полуколец без единицы устроены точно так же, как и в конечных циклических полукольцах с единицей.* См. [7].

Связь между конечными циклическими полукольцами с единицей и без единицы может быть установлена и другим способом. Если из конечного циклического полукольца T с единицей (2) убрать 1, то получим циклическое полукольцо $\{a, \dots, a^k, a^{k+1}, \dots, a^{k+n-1}\}$ без единицы в случае $k \neq 1$ (при $k = 1$ получаем циклическое полуполе со своей единицей a^n).

Следующий способ присоединения 1 к циклическому полукольцу

$$\{a, a^2, \dots, a^k, \dots, a^{k+n-1}\}$$

назовем *каноническим*. Если $a + a^{r+1} = a^{s+1}$, $r, s \in \mathbb{N}_0$, то

$$1 + a^r := \begin{cases} a^s, \text{ если } s + 1 \neq k, \\ a^{k+n-1}, \text{ если } s + 1 = k. \end{cases} \tag{3}$$

Аналогично определим суммы $a^r + 1$, $r \in \mathbb{N}_0$.

В примерах 2 и 3 для удобства будем указывать не степени образующего элемента a, а показатели его степеней.

Пример 2. Каноническим присоединением единицы к полукольцу $S = \{a, a^2, \dots, a^6\}$, $a^7 = a^6$, получим структуру T, не являющуюся полукольцом, поскольку $a^6 = (a + 1) + 1 \neq a + (1 + 1) = a^5$.

$+$	1	2	3	4	5	6
1	4	4	5	6	6	6
2	5	5	5	6	6	6
3	6	6	6	6	6	6
4	6	6	6	6	6	6
5	6	6	6	6	6	6
6	6	6	6	6	6	6

S

$+$	0	1	2	3	4	5	6
0	3	3	4	6	6	6	6
1	4	4	4	5	6	6	6
2	6	5	5	5	6	6	6
3	6	6	6	6	6	6	6
4	6	6	6	6	6	6	6
5	6	6	6	6	6	6	6
6	6	6	6	6	6	6	6

T

Этот пример показывает, что канонический способ присоединения 1 не всегда приводит к структуре полукольца.

Следующий пример доказывает, что *из неизоморфных конечных циклических полуколец с единицей — отбрасыванием единицы — можно получить одно и то же циклическое полукольцо без единицы.*

Пример 3. Рассмотрим таблицы Кэли всех попарно неизоморфных циклических полуколец с одинаковой мультипликативной полугруппой $\{1, a, a^2, a^3\}$, $a^4 = a^3$.

+	0	1	2	3
0	0	0	0	0
1	1	1	1	1
2	2	2	2	2
3	3	3	3	3

T_1

+	0	1	2	3
0	0	0	1	2	3
1	0	1	2	3
2	0	1	2	3
3	0	1	2	3

T_2

+	0	1	2	3
0	0	1	2	3
1	1	1	2	3
2	2	2	2	3
3	3	3	3	3

T_3

+	0	1	2	3
0	0	3	2	3
1	3	1	3	3
2	2	3	2	3
3	3	3	3	3

T_4

+	0	1	2	3
0	0	3	3	3
1	3	1	3	3
2	3	3	2	3
3	3	3	3	3

T_5

+	0	1	2	3
0	2	2	3	3
1	2	**3**	**3**	**3**
2	3	**3**	**3**	**3**
3	3	**3**	**3**	**3**

T_6

+	0	1	2	3
0	2	3	3	3
1	3	3	3	3
2	3	3	3	3
3	3	3	3	3

T_7

+	0	1	2	3
0	3	2	3	3
1	2	3	3	3
2	3	3	3	3
3	3	3	3	3

T_8

+	0	1	2	3
0	3	3	3	3
1	3	3	3	3
2	3	3	3	3
3	3	3	3	3

T_9

+	0	1	2	3
0	2	2	3	3
1	3	3	3	3
2	3	3	3	3
3	3	3	3	3

T_{10}

+	0	1	2	3
0	2	3	3	3
1	2	3	3	3
2	3	3	3	3
3	3	3	3	3

T_{11}

+	0	1	2	3
0	3	2	3	3
1	3	3	3	3
2	3	3	3	3
3	3	3	3	3

T_{12}

+	0	1	2	3
0	3	3	3	3
1	2	3	3	3
2	3	3	3	3
3	3	3	3	3

T_{13}

Из каждого идемпотентного полукольца T_4 — T_5 отбрасыванием 1 получаем одно и то же циклическое полукольцо. Из каждого неидемпотентного полукольца T_6 — T_{13} отбрасыванием 1 получаем одно и то же циклическое полукольцо с константным сложением. Каноническим присоединением 1 к этому трехэлементному полукольцу получается неидемпотентное циклическое полукольцо T_9, имеющее коммутативное (константное) сложение.

Полукольцо S из примера 1 не может быть получено ни из какого из полуколец T_1 — T_{13} из примера 3 отбрасыванием 1. Таким образом, *не всякое конечное циклическое полукольцо без единицы может быть получено из конечного циклического полукольца с единицей отбрасыванием* 1.

Сформулируем задачу для дальнейшего исследования.

Задача. Выяснить условия, при которых данное конечное циклическое полукольцо без единицы можно получить из некоторого конечного циклического полукольца с единицей 1 отбрасыванием 1.

Литература

1. *Бестужев А. С., Вечтомов Е. М.* Циклические полукольца с коммутативным сложением // Вестник Сыктывкарского университета. Серия 1: Математика. Механика. Информатика. 2015. Вып. 1 (20). С. 8—39.
2. *Вечтомов Е. М.* Введение в полукольца. Киров : Издательство Вятского государственного педагогического университета. 2000. 44 с.
3. *Вечтомов Е. М., Бестужев А. С., Лубягина И. В.* Полукольца с циклическим умножением // Алгебра и математическая логика: Материалы международной конференции, посвященной 100-летию со дня рождения профессора В. В. Морозова, и молодежной школы-конференции «Современные проблемы алгебры и математической логики». Казань : КФУ, 2011. С. 51—52.
4. *Вечтомов Е. М., Бестужев А. С., Орлова И. В.* Строение циклических полуколец // IX Всероссийская научная конференция «Математическое моделирование развивающейся экономики, экологии и технологий», ЭКОМОД – 2016. Киров : Издательство Вятского государственного университета, 2016. С. 21—30.
5. *Вечтомов Е. М., Лубягина И. В.* Циклические полукольца с идемпотентным некоммутативным сложением // Фундаментальная и прикладная математика. 2012. Т. 17, вып. 1. С. 33—52.
6. *Вечтомов Е. М., Орлова И. В.* Циклические полукольца с неидемпотентным некоммутативным сложением // Фундаментальная и прикладная математика. 2015. Т. 20, вып. 6. С. 17—41.
7. *Вечтомов Е. М., Орлова И. В.* Идеалы и конгруэнции циклических полуколец // Вестник Сыктывкарского университета. Серия 1: Математика. Механика. Информатика. 2017. Вып. 1 (22). С. 29—40.
8. *Скорняков Л. А.* Элементы алгебры. 2-е изд. М. : Наука, 1986. 240 с.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О МЕРЕ ВКЛЮЧЕНИЯ ЦЕНТРА В АЛГЕБРУ $F^{(l)}$

А. В. Гришин (Москва)[1]

Настоящая заметка продолжает исследования, начатые в [3].

Пусть $V = V_1 \bigoplus \ldots \bigoplus V_i \bigoplus \ldots$ — бесконечная прямая сумма конечномерных векторных пространств, причем $\dim V_{i+1} > \dim V_i > 0$, $i = 1, \ldots, n, \ldots$. Любое однородное подпространство в V, имеющее вид $U = U_1 \bigoplus \ldots \bigoplus U_i \bigoplus \ldots$, где $0 \neq U_i \subset V_i$, назовем *градуированным*. Пусть $W = W_1 \bigoplus \ldots \bigoplus W_i \bigoplus \ldots$ — другое градуированное подпространство и $W_i \subset U_i$. Назовем *мерой включения* W *в* U предел (если он существует)

$$\mu(W, U) = \lim_{n\to\infty} \dim W_n / \dim U_n.$$

Мерой включения фактор-пространства U/W в пространство V назовем разность $\mu(U, V) - \mu(W, V)$. Ясно, что мера включения фактор-пространства может быть равна нулю даже, если это фактор-пространство бесконечномерно.

Пусть $V = M(F)$ — *полилинейная часть* относительно свободной счетнопорожденной ассоциативной алгебры $F = k\langle x_1, \ldots, x_i, \ldots\rangle$ некоторого многообразия над бесконечным полем k характеристики $\neq 2, 3$, т. е. $V = \bigoplus_{n=1}^{\infty} F_n$, где F_n — подпространство в F полилинейных многочленов степени n от переменных $x_1, \ldots, x_n$. Рассмотрим градуированные подпространства $D_m = \bigoplus_{n=1}^{\infty}\big([F, F]^m \cap F_n\big)$ и $M\big(Z(F)\big) = \bigoplus_{n=1}^{\infty} Z_n$, где $[F, F]$ — T-пространство порожденное коммутатором $[x_1, x_2]$, $Z(F)$ — центр алгебры F, а $Z_n = Z(F) \cap F_n$.

Всюду ниже $F = F^{(l)}$ — относительно свободная алгебра многообразия, заданного длинным коммутатором $[x_1, \ldots, x_l]$, $\{[x_1, \ldots, x_l]\}^T$ — T-пространство, порожденное длинным коммутатором, а $\big([x_1, \ldots, x_l]\big)^T$ — соответствующий T-идеал. Для любого T-пространства U обозначим через $M(U)$ его полилинейную часть, т. е. $M(U) = \bigoplus_{n=1}^{\infty} U_n$, где $U_n = U \cap F_n$.

Нас будет интересовать мера включения центра в алгебру $F^{(l)}$ при $l = 3, 4, 5$.

Описание центра относительно свободной алгебры или хотя бы частичное его нахождение это всегда весьма интересная и нетривиальная задача. Для алгебры F общих матриц она рассматривалась в [6–9]. Для алгебры $F = F^{(l)}$ при $3 \leq l \leq 6$ центр изучался в [1, 2, 4, 5]. В [1, 2] дано полное описание центра $Z(F)$ при $l = 3$ и 4 с помощью $[F, F]$ и $[F, F]^2$. В [4, 5] начато исследование центра алгебры $F^{(l)}$ при $l \geq 5$.

Теорема 1. *Если* $F = F^{(3)}$, *то* $\mu\big(D_m, M(F)\big) = \mu\Big(M\big(Z(F)\big), M(F)\Big) = 1/2$. *Если* $F = F^{(4)}$ *и* k *— поле нулевой характеристики, то* $\mu\big(D_m, M(F)\big) = \mu\Big(M\big(Z(F)\big), M(F)\Big) = 1/2$.

Нулевая характеристика в случае $l = 4$ нужна в доказательстве, так как для оценки размерностей используются диаграммы Юнга. Весьма вероятно, что данный факт имеет место и при более широких предположениях.

Можно показать, что T-идеал $([x_1, x_2, x_3])^T$ лежит в центре алгебры $F^{(4)}$ и имеет место

Теорема 2. $\mu\Big(M\big(([x_1, x_2, x_3])^T\big), M\big(F^{(4)}\big)\Big) = 0$.

Для алгебры $F^{(5)}$ в [4] доказано, что центр находится между $\{[x_1, x_2, x_3, x_4]\}^T$ и $([x_1, x_2, x_3, x_4])^T$. Вне T-пространства $\{[x_1, x_2, x_3, x_4]\}^T$ находятся некоторые интересные центральные многочлены. Такие, например, как многочлен Холла $[[x_1, x_2]^2, x_3]$ и некоторые следствия из него. Есть ли что-то еще? Вопрос пока открыт.

 Получено 07.12.2017. УДК 512.5.

[1]Московский педагогический государственный университет. E-mail: grishinaleksandr@yandex.ru.

Теорема 3. *Если k — поле нулевой характеристики и $F = F^{(5)}$, то*

$$\mu\Big(M\big(\{[x_1, x_2, x_3, x_4]\}^T\big), M(F)\Big) = 1/2,$$
$$\mu\Big(M\big(Z(F)\big), M(F)\Big) = 1/2,$$
$$\mu\Big(M\big(([x_1, x_2, x_3, x_4])^T\big), M(F)\Big) = 1.$$

Теорема 3 показывает, что мера включения фактор-пространства

$$Z\big(F^{(5)}\big)/\{[x_1, x_2, x_3, x_4]\}^T$$

в пространство $M(F^{(5)})$ равна нулю, т. е. в асимптотическом смысле основная часть центра алгебры $F^{(5)}$ — это T-пространство $\{[x_1, x_2, x_3, x_4]\}^T$.

На основании полученных результатов можно высказать следующую гипотезу.

Для любого нечетного $l = 2m+1$, если $F = F^{(l)}$ и k — поле нулевой характеристики, то

$$\mu\Big(M\big(Z(F)\big), M(F)\Big) = \mu\Big(M\big(\{[x_1, \ldots, x_{2m}]\}^T\big), M(F)\Big) = 1/2,$$

т. е. мера включения фактор-пространства $M\big(Z(F)\big)/M\big(\{[x_1, \ldots, x_{2m}]\}^T\big)$ в пространство $M(F)$ равна нулю и в асимптотическом смысле центр алгебры $F^{(l)}$ описывается, как T-пространство $\{[x_1, \ldots, x_{2m}]\}^T$.

Литература

1. *Гришин А. В.* О строении центра относительно свободной алгебры Грассмана // Успехи математических наук. 2010. Т. 65, № 4. С. 191—192.
2. *Гришин А. В.* О центре относительно свободной лиевски нильпотентной алгебры индекса 4 // Математические заметки. 2012. Т. 91, № 1. С. 42—45.
3. *Гришин А. В.* О мере включения градуированных подпространств // Международная конференция «Мальцевские чтения». Тезисы докладов (электронная версия). Новосибирск, 2017. С. 111.
4. *Гришин А. В., Пчелинцев С. В.* О центрах относительно свободных ассоциативных алгебр с тождеством лиевой нильпотентности // Математический сборник. 2015. Т. 206, № 11. С. 113—130.
5. *Гришин А. В., Пчелинцев С. В.* Собственные центральные и ядерные многочлены относительно свободных алгебр с тождеством лиевой нильпотентности степени 5 и 6 // Математический сборник. 2016. Т. 207, № 12. С. 3—21.
6. *Марков В. Т.* О размерности некоммутативных аффинных алгебр // Известия АН СССР. Серия математическая. 1973. Т. 37, № 2. С. 284—288.
7. *Размыслов Ю. П.* Об одной проблеме Капланского // Известия АН СССР. Серия математическая. 1973. Т. 37, № 3. С. 483—501.
8. *Formanek E.* Central polynomials for matrix rings // J. Algebra. 1972. Vol. 23. P. 129—133.
9. *Okhitin S. V.* Central polynomials of an algebra of second-order matrices // Moscow Univ. Math. Bull. 1988. Vol. 43, № 4. P. 49—51.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

БАЗИСЫ ТОЖДЕСТВ И КВАЗИТОЖДЕСТВ УНАРНЫХ АЛГЕБР

В. К. Карташов (Волгоград)[1], А. В. Карташова (Волгоград)[2]

Проблема существования базисов тождеств и квазитождеств унарных алгебр привлекает внимание многих специалистов по универсальной алгебре.

Г. Биркгоф [6] доказал, что всякая конечная унарная алгебра конечного типа имеет конечный базис тождеств. А. И. Мальцевым было показано [5, с. 352], что любое многообразие унаров, т. е. алгебр с одной операцией, однобазируемо.

Позднее в [10] было доказано, что любое многообразие коммутативных унарных алгебр, т. е. алгебр, у которых любые две операции коммутируют, имеет конечный базис тождеств. Из доказательства этой теоремы вытекает

Следствие. *Для любого целого положительного числа n существует многообразие коммутативных унарных алгебр, независимый базис которого состоит из n тождеств.*

В работах [3, 4] доказано, что любой конечный унар имеет конечный базис квазитождеств, а любой конечнопорожденный унар — независимый базис квазитождеств. При этом установлено существование континуума многообразий унаров, которые не имеют независимого базиса квазитождеств.

И. П. Бесценный [1] приводит необходимые и достаточные условия существования конечного базиса для трехэлементной унарной алгебры конечного типа. Позднее В. А. Горбуновым [2] был приведен пример трехэлементной унарной алгебры, не имеющей независимого базиса квазитождеств. Некоторые условия отсутствия конечного базиса квазитождеств для конечных алгебр указаны в [7, 9]. В [8] рассматриваются унарные алгебры специального типа с нулем, найден критерий существования конечного базиса квазитождеств для таких алгебр.

В [3] показано, что всякая конечная алгебра многообразия коммутативных унарных алгебр с двумя унарными операциями f и g, определенного тождествами $fg(x) = gf(x) = x$, имеет конечный базис квазитождеств.

Обобщением этого результата является

Теорема. *Всякая конечная алгебра многообразия унарных алгебр с двумя унарными операциями f и g, определенного тождеством $fg(x) = x$, имеет конечный базис квазитождеств.*

Литература

1. *Бесценный И. П.* Квазитождества конечных унарных алгебр // Алгебра и логика. 1989. Т. 28, № 5. С. 493—512.
2. *Горбунов В. А.* Покрытия в решетках квазимногообразий и независимая аксиоматизируемость // Алгебра и логика. 1977. Т. 16, № 5. С. 507—548.
3. *Карташов В. К.* Квазимногообразия унаров // Математические заметки. 1980. Т. 27, № 1. С. 7—20.
4. *Карташов В. К.* Квазимногообразия унаров с конечным числом циклов // Алгебра и логика. 1980. Т. 19, № 2. С. 173—193.
5. *Мальцев А. И.* Алгебраические системы. М. : Наука, 1970. 392 с.
6. *Birkhoff G.* On the structure of abstract algebras // Proc. Camb. Philos. Soc. 1935. Vol. 31 (part 4). P. 432—454.

 Получено 25.12.2017. УДК 512.572.

[1]Волгоградский государственный социально-педагогический университет.
E-mail: kartashovvk@yandex.ru.
[2]Волгоградский государственный социально-педагогический университет.
E-mail: kartashovaan@yandex.ru.

7. *Casperson D., Hyndman J.* Primitive positive formulas preventing a finite basis of quasi-equations // Internat. J. Algebra Comput. 2009. Vol. 19, № 7. P. 925—935.
8. *Casperson D., Hyndman J., Mason J., Nation J. B., Schaan B.* Existence of finite bases for quasi-equations of unary algebras with 0 // Internat. J. Algebra Comput. 2015. Vol. 25, № 6. P. 927—950.
9. *Hyndman J.* Positive primitive formulas preventing enough algebraic operations // Algebra Universalis. 2004. Vol. 52, № 2, 3. P. 303—312.
10. *Kartashov V. K.* On the finite axiomatizability of varieties of commutative unary algebras // J. Math. Sci. 2010. Vol. 164, № 1. P. 56—59.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ПОЛИГОНЫ С ТОЖДЕСТВАМИ В РЕШЁТКЕ КОНГРУЭНЦИЙ

И. Б. Кожухов (Москва)[1], А. М. Пряничников (Москва)[2]

Решётка конгруэнций $\mathrm{Con}A$ универсальной алгебры A является важной характеристикой этой алгебры. Наименьшим элементом этой решётки является отношение равенства $\Delta_A = \{(a,a)|a \in A\}$, а наибольшим — универсальное отношение $\nabla_A = A \times A$. Одним из направлений общей алгебры является изучение универсальных алгебр с теми или иными условиями на конгруэнции. Например, условие тривиальности решётки конгруэнций ($\mathrm{Con}A = \{\Delta_A, \nabla_A\}$) определяет простые алгебры (простые группы, кольца, конгруэнц-простые полугруппы и т. д.), условие максимальности или минимальности — соответственно нётеровы и артиновы алгебры. В работе [2] исследовался класс алгебр, противоположный классу простых алгебр, а именно, алгебры, у которых всякое отношение эквивалентности является конгруэнцией (т. е. $\mathrm{Con}A = \mathrm{Eq}A$, где $\mathrm{Eq}A$ — решётка отношений эквивалентности на множестве A). Большое количество работ посвящено подпрямо неразложимым алгебрам, т. е. таким алгебрам A, что либо $|A| = 1$, либо решётка $\mathrm{Con}A$ содержит наименьший, отличный от Δ_A элемент.

Универсальные алгебры, у которых решётка конгруэнций модулярна, или дистрибутивна, или является цепью, тоже привлекали большое внимание специалистов. Можно отметить работы по дистрибутивным и цепным кольцам и модулям, полигонам над полугруппами с дистрибутивной или модулярной решёткой конгруэнций [3, 4]. Интересно отметить, что, хотя полигон над полугруппой — аналог модуля над кольцом, но решётка конгруэнций модуля (т. е. решётка подмодулей) всегда модулярна, а решётка конгруэнций полигона модулярна далеко не всегда.

Дистрибутивные и модулярные решётки образуют многообразия, задаваемые соответственно тождеством $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$ и тождеством $(x \vee y) \wedge (x \vee z) = x \vee (z \wedge (x \vee y))$. Цепи образуют класс решёток, не являющийся многообразием, но обладающий некоторыми свойствами многообразий.

В связи с вышесказанным, кажется естественным изучение универсальных алгебр, у которых решётка конгруэнций удовлетворяет какому-либо нетривиальному решёточному тождеству.

Напомним, что *полигоном над полугруппой* называется множество X, на котором действует полугруппа S, т. е. определено отображение $X \times S \to X,\ (x,s) \mapsto xs$, удовлетворяющее условию $x(st) = (xs)t$ при всех $x \in X,\ s,t \in S$ (см. [5]). Над полугруппой с нулём естественно рассматривать полигоны с нулём, удовлетворяющие условию $0s = x0 = 0$ при всех $x \in X, s \in S$.

Символом $\mathcal{M}^0(G, I, \Lambda, P)$ мы обозначаем регулярную рисовскую матричную полугруппу над группой с нулём $G \cup \{0\}$ с сэндвич матрицей P; регулярность означает, что в каждой строке и в каждом столбце матрицы P есть ненулевые элементы (см. [1, гл. 3]). Согласно хорошо известной теореме Сушкевича-Риса, регулярные рисовские матричные полугруппы — это в точности вполне 0-простые полугруппы.

Цель данной работы состоит в доказательстве следующих утверждений:

Теорема 1. *Пусть X — полигон над конечной полугруппой. Тогда решётка конгруэнций $\mathrm{Con}X$ удовлетворяет какому-либо нетривиальному решёточному тождеству в том и только том случае, если X конечен.*

 Получено 15.01.2018. УДК 512.5

[1]Национальный исследовательский университет «МИЭТ». E-mail: kozhuhov_i_b@mail.ru.

[2]Национальный исследовательский университет «МИЭТ». E-mail: genary@yandex.ru.

Теорема 2. *Пусть $S = \mathcal{M}^0(G, I, \Lambda, P)$ — вполне 0-простая полугруппа и $|G| < \infty$, $|I| < \infty$. Тогда для любого полигона X с нулём над S выполняется следующее: решётка конгруэнций $ConX$ удовлетворяет какому-либо нетривиальному решёточному тождеству в том и только том случае, если X конечен.*

Теорема 3. *Существует вполне 0-простая полугруппа $S = \mathcal{M}^0(G, I, \Lambda, P)$ и бесконечный полигон X с нулём над S такие, что решётка $ConX$ двухэлементна (а значит, удовлетворяет нетривиальному решёточному тождеству).*

Литература

1. *Клиффорд А., Престон Г.* Алгебраическая теория полугрупп. М. : Мир, 1964.
2. *Кожухов И. Б., Решетников А. В.* Алгебры, у которых все отношения эквивалентности являются конгруэнциями // Фундаментальная и прикладная математика. 2010. Т. 16, вып. 3. С. 161—192.
3. *Птахов Д. О., Степанова А. А.* Решётки конгруэнций полигонов // Дальневосточный математический журнал. 2013. Т. 13, № 1. С. 107—115.
4. *Халиуллина А. Р.* Условия модулярности решётки конгруэнций полигонов над полугруппой правых или левых нулей // Дальневосточный математический журнал. 2015. Т. 15, № 1. С. 102—120.
5. *Mikhalev A., Kilp M., Knauer U.* Monoids, acts and categories. Berlin : Walter de Gruyter, 2000.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О СВОЙСТВАХ КОНГРУЭНЦИЙ АЛГЕБР В НЕКОТОРЫХ КЛАССАХ АЛГЕБР С ОПЕРАТОРОМ

А. Н. Лата (Москва)[1]

1. Введение

Алгеброй с операторами называется алгебра с выделенной системой унарных операций, действующих как эндоморфизмы для остальных основных операций. Данные алгебры изучались в работах [7, 8].

Унаром с мальцевской операцией [3] называется алгебра $\langle A, d, f\rangle$ с унарной операцией f и тернарной операцией d, на которой истинны тождества Мальцева $d(x,y,y) = d(y,y,x) = x$ и тождество перестановочности $f(d(x,y,z)) = d(f(x), f(y), f(z))$.

В [3] показано, что на любом унаре $\langle A, f\rangle$ можно задать тернарную операцию p так, что алгебра $\langle A, p, f\rangle$ становится унаром с мальцевской операцией, а унарная операция — ее эндоморфизмом. Эта алгебра определяется следующим образом.

Пусть $\langle A, f\rangle$ — произвольный унар и $x, y \in A$. Для любого элемента x унара $\langle A, f\rangle$ через $f^n(x)$ обозначается результат n-кратного применения операции f к элементу x; при этом $f^0(x) = x$. Положим $M_{x,y} = \{n \in \mathbb{N} \cup \{0\} \mid f^n(x) = f^n(y)\}$, и $k(x,y) = \min\ M_{x,y}$, если $M_{x,y} \neq \emptyset$ и $k(x,y) = \infty$, если $M_{x,y} = \emptyset$. Положим далее

$$p(x,y,z) \stackrel{def}{=} \begin{cases} z, & \text{если } k(x,y) \leqslant k(y,z); \\ x, & \text{если } k(x,y) > k(y,z). \end{cases} \tag{1}$$

С помощью конструкции, предложенной В. К. Карташовым в [3], В. Л. Усольцевым в [5] на произвольном унаре была определена тернарная операция $s(x,y,z)$, называемая симметрической, удовлетворяющая тождествам $s(x,y,y) = s(y,y,x) = s(y,x,y) = x$ и также перестановочная с унарной.

$$s(x,y,z) \stackrel{def}{=} \begin{cases} z, & \text{если } k(x,y) < k(y,z); \\ y, & \text{если } k(x,y) = k(y,z); \\ x, & \text{если } k(x,y) > k(y,z). \end{cases} \tag{2}$$

Алгебры $\langle A, s, f\rangle$ образуют еще один подкласс класса унаров с мальцевской операцией.

В [6] аналогичным образом на произвольном унаре были определены тернарная операция $w(x,y,z)$ и операция большинства $m(x,y,z)$, перестановочные с унарной.

$$w(x,y,z) \stackrel{def}{=} \begin{cases} z, & \text{если } k(x,y) > k(y,z); \\ y, & \text{если } k(x,y) = k(y,z); \\ x, & \text{если } k(x,y) < k(y,z). \end{cases} \tag{3}$$

$$m(x,y,z) \stackrel{def}{=} \begin{cases} z, & \text{если } k(x,y) \geqslant k(y,z); \\ x, & \text{если } k(x,y) < k(y,z). \end{cases} \tag{4}$$

 Получено 11.12.2017. УДК 512.579.

[1]Московский государственный университет им. М. В. Ломоносова. E-mail: alex.lata@yandex.ru.

2. Необходимые определения

Через Con$A$ обозначается решетка конгруэнций алгебры A. Класс конгруэнции θ, порожденный элементом x, будем обозначать через $[x]\theta$.

Элемент $p \neq 0$ решетки L с нулем 0 называется *атомом*, если для любого $x \in L$ неравенство $0 \leqslant x \leqslant p$ влечет $x = 0$ или $x = p$. Двойственным образом определяется *коатом* решетки.

Другие определения и утверждения теории решеток можно найти в [1, 2].

Основные определения и обозначения, связанные с унарами, приведены в [4].

Универсальная алгебра A *конгруэнц–когерентна*, если любая подалгебра в A, содержащая класс произвольной конгруэнции в A, является объединением классов этой конгруэнции.

Универсальная алгебра A, имеющая нульарную операцию 0, называется *слабо когерентной*, если для любой подалгебры B алгебры A и любой конгруэнции θ алгебры A условие $[0]\theta \subseteq B$ влечет $[x]\theta \subseteq B$ для любого $x \in B$.

Универсальная алгебра A, имеющая нульарную операцию 0, называется *локально когерентной*, если для любой подалгебры B алгебры A и любой конгруэнции θ алгебры A из того, что $[x]\theta \subseteq B$ для некоторого $x \in B$, следует $[0]\theta \subseteq B$.

3. Основные результаты

Теорема 1. *Пусть $\langle A, d, f\rangle$ — алгебра с оператором f, где $d(x_1, x_2, x_3)$ — операция, определенная по одному из правил (2)–(4). Решетка* Con$\langle A, d, f\rangle$ *не имеет коатомов тогда и только тогда, когда унар $\langle A, f\rangle$ связен, содержит одноэлементный подунар и имеет бесконечную глубину. В других случаях* Con$\langle A, d, f\rangle$ *имеет единственный коатом.*

Теорема 2. *Пусть $\langle A, d, f\rangle$ — алгебра с оператором f, где $d(x_1, x_2, x_3)$ — операция, определенная по одному из правил (2)–(4). Следующие утверждения эквивалентны:*

1) Con$\langle A, d, f\rangle$ *— решетка с дополнениями (решетка с единственными дополнениями, булева решетка);*
2) Con$\langle A, d, f\rangle$ *— решетка с относительными дополнениями (обобщенная булева решетка);*
3) *алгебра $\langle A, d, f\rangle$ конгруэнц-проста;*
4) *либо операция f инъективна, либо унар $\langle A, f\rangle$ содержит такой элемент a, что $f(x) = a$ для любого $x \in A$.*

Следствие. *Любая нетривиальная конгруэнция алгебры $\langle A, d, f\rangle$ не имеет дополнения.*

Предложение 1. *Пусть $\langle A, d, f\rangle$ — алгебра с оператором f, где $d(x_1, x_2, x_3)$ — операция, определенная по одному из правил (2)–(4). Решетка* Con$\langle A, d, f\rangle$ *является решеткой с копсевдодополнениями.*

Предложение 2. *Пусть $\langle A, d, f\rangle$ — алгебра с оператором f, где $d(x_1, x_2, x_3)$ — операция, определенная по одному из правил (1)–(4). Решетка* Con$\langle A, d, f\rangle$ *является дуально стоуновой решеткой.*

Предложение 3. *Пусть $\langle A, d, f\rangle$ — алгебра с оператором f, где $d(x_1, x_2, x_3)$ — операция, определенная по одному из правил (1)–(4). Решетка* Con$\langle A, d, f\rangle$ *стоунова решетка тогда и только тогда, когда она является решеткой с единственным атомом. Другими словами, алгебра $\langle A, d, f\rangle$ подпрямо неразложима.*

Предложение 4 [4]**.** *Пусть $\langle A, \Omega\rangle$ — произвольная алгебра с оператором $f \in \Omega$. Если $\langle A, f\rangle \cong C_n^0$, или $\langle A, f\rangle \cong C_n^0 + C_m^0$, или $\langle A, f\rangle \cong C_1^t$, где $n, m \in \mathbb{N}$ и $t \in \mathbb{N} \cup \{\infty\}$, то алгебра $\langle A, \Omega\rangle$ является конгруэнц–когерентной*

Теорема 3 [4]**.** *Унар $\langle A, f\rangle$ является конгруэнц–когерентным тогда и только тогда, когда $\langle A, f\rangle$ — один из унаров следующего вида:*

1) C_n^0, $n \in \mathbb{N}$;

2) $C_n^0 + C_m^0$ *для некоторых* $n, m \in \mathbb{N}$;
3) C_1^t, $t \in \mathbb{N} \cup \{\infty\}$.

Теорема 4 [4]. *Пусть* $\langle A, d, f\rangle$ *— алгебра с оператором* f*, где* $d(x_1, x_2, x_3)$ *— операция, определенная по одному из правил* (1)–(4)*. Алгебра* $\langle A, d, f\rangle$ *является конгруэнц–когерентной тогда и только тогда, когда выполняется одно из следующих условий:*

1) *операция* f *на* A *является инъективной;*
2) *унар* $\langle A, f\rangle$ *содержит такой элемент* a*, что* $f(x) = a$ *для любого* $x \in A$*, где* $|A| \geqslant 3$*;*
3) *унар* $\langle A, f\rangle$ *изоморфен* C_1^t *для некоторого* $t \in \mathbb{N} \cup \{\infty\}$.

Теорема 5 [4]. *Пусть* $\langle A, d, f, 0\rangle$ *— алгебра с оператором* f*, где* $d(x_1, x_2, x_3)$ *— операция, определенная по одному из правил* (1)–(4)*, и нульарной операцией* 0*, для которой* $f(0) = 0$*. Алгебра* $\langle A, d, f, 0\rangle$ *является слабо когерентной тогда и только тогда, когда унар* $\langle A, f\rangle$ *является одним из следующих:*

1) *произвольный унар с инъективной операцией;*
2) *связный унар, который не содержит узловых элементов, за исключением, может быть, элемента* 0*;*
3) *сумма унара из пункта 2 и произвольного унара с инъективной операцией.*

Теорема 6 [4]. *Пусть* $\langle A, d, f, 0\rangle$ *— алгебра с оператором* f*, где* $d(x_1, x_2, x_3)$ *— операция, определенная по одному из правил* (1)–(4)*, и нульарной операцией* 0*, для которой* $f(0) = 0$*. Алгебра* $\langle A, d, f, 0\rangle$ *является локально когерентной тогда и только тогда, когда унар* $\langle A, f\rangle$ *является одним из следующих:*

1) *произвольный унар, содержащий одноэлементную компоненту, порожденную* 0*, или одноэлементный унар;*
2) *унар, в котором для всех* $x \in A$ *выполняется* $f(x) = 0$*, где* $|A| \geqslant 3$*;*
3) *унар* $C_1^t, t \in \mathbb{N} \cup \{\infty\}$*;*
4) *связный унар конечной глубины* $t(A)$*, в котором существует единственный узловой элемент* $a \neq 0$*, глубина которого равна* $t(A) - 1$*, и других узловых элементов нет.*

Литература

1. *Артамонов В. А.* [и др.] Общая алгебра. Т. 2. Под общей ред. Л. А. Скорнякова. М. : Наука, 1991. 480 с.
2. *Гретцер Г.* Общая теория решеток. М. : Мир, 1982. 456 с.
3. *Карташов В К.* Об унарах с мальцевской операцией // Универсальная алгебра и ее приложения: Тезисы сообщений участников международного семинара, посвященного памяти профессора Московского государственного университета Л. А. Скорнякова. Волгоград : Перемена, 1999. С. 31—32.
4. *Лата А. Н.* О конгруэнц–когерентных алгебрах Риса и алгебрах с оператором // Чебышевский сборник. 2017. Т. 18, вып. 2. С. 154—172.
5. *Усольцев В. Л.* Свободные алгебры многообразия унаров с мальцевской операцией p, заданного тождеством $p(x, y, x) = y$ // Чебышевский сборник. 2011. Т. 12, вып. 2. С. 127—134.
6. *Усольцев В. Л.* О строго простых тернарных алгебрах с операторами // Чебышевский сборник. 2013. Т. 14, вып. 4. С. 196—204.
7. *Hyndman J., Nation J. B., Nishida J.* Congruence Lattices of Semilattices with Operators // Studia Logica. 2016. Vol. 104, issue 2. P. 305—316.
8. *Johnsson B.* A survey of Boolean algebras with operators // Algebras and Orders, NATO ASI Series. 1993. Vol. 389. P. 239—286.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О Q-УНИВЕРСАЛЬНОСТИ РЕШЕТОК ПОДПОЛУГРУПП ДЛЯ НЕКОТОРЫХ Q-УНИВЕРСАЛЬНЫХ КЛАССОВ[1]

С. М. Луцак (Петропавловск, Казахстан)[2], М. В. Швидефски (Новосибирск)[3]

Авторами изучается сложность строения решетки $\mathrm{Sub}(\mathcal{T}_{\mathbf{K}})$ подполугрупп полугруппы элементарных теорий класса $\mathbf{K} \subseteq \mathbf{K}(\sigma)$ алгебраических систем сигнатуры σ.

Пусть класс $\mathbf{K} \subseteq \mathbf{K}(\sigma)$ замкнут относительно декартовых произведений. Для алгебраических систем $\mathcal{A}, \mathcal{B} \in \mathbf{K}$ полагаем $\mathrm{Th}(\mathcal{A}) * \mathrm{Th}(\mathcal{B}) = \mathrm{Th}(\mathcal{A} \times \mathcal{B})$. Алгебра $\mathcal{T}_{\mathbf{K}} = \langle \{\mathrm{Th}(\mathcal{A}) \mid \mathcal{A} \in \mathbf{K}\}, * \rangle$ является коммутативной полугруппой с единицей. Эту полугруппу мы называем *полугруппой элементарных теорий класса* $\mathbf{K}$.

Теорема 1. *Пусть* $\mathbf{K}$ *является одним из следующих классов систем:*

1. *Многообразие всех унаров;*
2. *Квазимногообразие всех [ориентированных] графов;*
3. *Многообразие всех [точечных] абелевых групп;*
4. *Многообразие всех коммутативных колец с единицей;*
5. *Многообразие MV-алгебр;*
6. *Многообразие модулярных решеток;*
7. *Многообразие дифференциальных группоидов.*

Тогда решетка $\mathrm{Sub}(\mathcal{T}_{\mathbf{K}})$ *содержит подрешетку, изоморфную решетке идеалов свободной решетки счетного ранга, и является Q-универсальной.*

Теорема 1 дает пример квазимногообразия (а именно, многообразие аблевых групп), не являющегося Q-универсальным, для которого решетка подполугрупп элементарных теорий, тем не менее, Q-универсальна. Вопрос о Q-универсальности многообразия модулярных решеток является открытым. Все остальные классы, перечисленые в этой теореме, являются Q-универсальными.

 Получено 25.12.2017. УДК 512.56, 512.57.

[1]Работа выполнена при финансовой поддержке Совета по грантам президента РФ по государственной поддержке ведущих научных школ, проект НШ-6848.2016.1.

[2]Северо-Казахстанский государственный университет им. М. Козыбаева. E-mail: sveta_lutsak@mail.ru.

[3]Институт математики им. С. Л. Соболева СО РАН. E-mail: semenova@math.nsc.ru.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ОБ ЭКСТРЕМАЛЬНЫХ СВОЙСТВАХ ИДЕМПОТЕНТОВ УПОРЯДОЧЕННЫХ МОНОИДОВ

В. Б. Поплавский (Саратов)[1]

1. Вторичные идемпотенты моноида

Пусть $\mathbf{X}$ — частично упорядоченный моноид, т. е. полугруппа с единицей 1, на которой задан стабильный относительно умножения частичный порядок $\leq$.

Определение 1. Пусть существует наибольшее решение уравнения $xa = a$ для некоторого $a \in \mathbf{X}$, тогда обозначим его через a^R. Если существует наименьшее решение уравнения $xa = a$, то обозначим его через a_R. Соответственно, если для уравнения $ax = a$ существует наибольшее решение, то обозначим его через a^L, и если среди решений уравнения $ax = a$ существует наименьшее, то обозначим его через a_L.

Теорема 1. *Если a^R, a_R, a^L, a_L существуют, то они являются идемпотентами моноида $\mathbf{X}$.*

Доказательство. Из определения 1 следует, что $1 \leq a^R$. Умножая последнее неравенство на a^R, получаем $a^R \leq a^R a^R$.

С другой стороны, $(a^R a^R)a = a^R(a^R a) = a$ и, следовательно, из определения 1 следует, что $(a^R a^R) \leq a^R$. Получаем равенство $a^R = a^R a^R$.

Аналогичным образом можно доказать равенство $a^L = a^L a^L$, а учитывая, что $a_R \leq 1$ и $a_L \leq 1$, можно показать и идемпотентность элементов a_R и a_L. □

Теорема 2. *Если a^R, a_R, a^L, a_L существуют, то выполняются следующие равенства:*

$$(a^R)^R = (a^R)^L = a^R,$$
$$(a^L)^L = (a^L)^R = a^L,$$
$$(a_L)_L = (a_L)_R = a_L,$$
$$(a_R)_R = (a_R)_L = a_R.$$

Доказательство. Из неравенства $1 \leq a^R$ получаем

$$(a^R)^R \leq (a^R)^R a^R = a^R, \quad (a^R)^L \leq a^R (a^R)^L = a^R.$$

Это позволяет записать $(a^R)^R \leq a^R$, $(a^R)^L \leq a^R$.

С другой стороны, сравнивая равенства $a^R a^R = a^R$, $(a^R)^R a^R = a^R$, $a^R (a^R)^L = a^R$ и учитывая максимальность элементов $(a^R)^R$, $(a^R)^L$, имеем $a^R \leq (a^R)^R$, $a^R \leq (a^R)^L$, что доказывает равенство $(a^R)^R = (a^R)^L = a^R$.

Остальные равенства доказываются аналогично. □

Теорема 3. *Пусть e — идемпотент моноида $\mathbf{X}$. Тогда следующие условия равносильны:*

$$1 \leq e \iff e = e^R \iff e = e^L;$$
$$e \leq 1 \iff e = e_R \iff e = e_L.$$

 Получено 22.12.2017. УДК 512.53.

[1]Саратовский государственный университет им. Н. Г. Чернышевского. E-mail: poplavskivb@mail.ru.

Доказательство. Пусть $1 \leq e = ee$. Тогда существует решение уравнения $xe = e$. Из неравенства $1 \leq e = xe$ получаем $x \leq xe = xxe = e$, т.е. e является наибольшим решением уравнения $e = xe$. Следовательно e^R существует и $e = e^R$. Таким же способом можно показать, что $e = e^L$.

Если выполняется равенство $e = e^R$, то из неравенства $1 \leq e^R$ получаем $1 \leq e$.

Аналогично доказывается эквивалентность $e \leq 1 \iff e = e_R \iff e = e_L$. □

Определение 2. Идемпотент e назовем *вторичным идемпотентом,* порожденным заданным на моноиде порядком $\leq$, если он сравним с единицей моноида $\mathbf{X}$, т. е. $e \leq 1$ или $1 \leq e$.

Идемпотент назовем *первичным* в противном случае, т. е. если он не сравним с единицей заданным на моноиде частичным порядком $\leq$.

Таким образом, если идемпотент e — вторичный, то выполняется либо $e = e^R = e^L$, либо $e = e_R = e_L$. В случае $e = e^R = e^L$ идемпотент e назовем *вторичным идемпотентом максимального типа*, в случае $e = e_R = e_L$ идемпотент e назовем *вторичным идемпотентом минимального типа.*

Из теорем 1 и 2 получаем, что, если существуют элементы a^R, a_R, a^L, a_L для некоторого $a \in \mathbf{X}$, то они являются вторичными идемпотентами. Будем называть их соответственно *R-вторичными идемпотентами максимального, минимального типа или L-вторичными идемпотентами максимального, минимального типа, порожденными элементом* a. Будем в этом случае также говорить, что элемент a *обладает вторичным идемпотентом (или порождает вторичный идемпотент) соответствующего типа.*

Множества всех идемпотентов, первичных идемпотентов, вторичных идемпотентов максимального и минимального типов будем обозначать символами E, E_0, $E^\uparrow$ и $E_\downarrow$ соответственно. Заметим, что $E_0 \cap E^\uparrow = \emptyset$, $E_0 \cap E_\downarrow = \emptyset$, $E^\uparrow \cap E_\downarrow = \{1\}$, что следует из теоремы 3, и $E = E_0 \cup E^\uparrow \cup E_\downarrow$.

2. Естественный порядок на множестве идемпотентов и его продолжение

Теорема 4. *Пусть* $\mathbf{X}$ *— моноид и* $\leq$ *— некоторый стабильный частичный порядок на нем. Тогда выполняются следующие эквивалентности, если все входящие в них вторичные идемпотенты существуют:*

$$a^R \leq b^R \leftrightarrow a^R \cdot b = b \leftrightarrow a^R \cdot b^R = b^R \cdot a^R = b^R;$$
$$a^L \leq b^L \leftrightarrow b \cdot a^L = b \leftrightarrow a^L \cdot b^L = b^L \cdot a^L = b^L;$$
$$a^L \leq b^R \leftrightarrow a^L \cdot b = b \leftrightarrow a^L \cdot b^R = b^R \cdot a^L = b^R;$$
$$a^R \leq b^L \leftrightarrow b \cdot a^R = b \leftrightarrow a^R \cdot b^L = b^L \cdot a^R = b^L;$$
$$a_R \leq b_R \leftrightarrow b_R \cdot a = a \leftrightarrow a_R \cdot b_R = b_R \cdot a_R = a_R;$$
$$a_L \leq b_L \leftrightarrow a \cdot b_L = a \leftrightarrow a_L \cdot b_L = b_L \cdot a_L = a_L;$$
$$a_L \leq b_R \leftrightarrow a \cdot b_R = a \leftrightarrow a_L \cdot b_R = b_R \cdot a_L = a_L;$$
$$a_R \leq b_L \leftrightarrow b_L \cdot a = a \leftrightarrow a_R \cdot b_L = b_L \cdot a_R = a_R.$$

Доказательство.

$$a^R \leq b^R \to 1 \leq a^R \leq b^R \to b \leq a^R \cdot b \leq b^R \cdot b = b \to a^R \cdot b = b.$$

Тогда по определению R-вторичного идемпотента получаем $a^R \cdot b = b \to a^R \leq b^R$. Поэтому

$$a^R \leq b^R \leftrightarrow a^R \cdot b = b.$$

Далее,

$$a^R \leq b^R \to 1 \leq a^R \leq b^R \to b^R \leq a^R \cdot b^R \leq b^R \cdot b^R = b^R \to a^R \cdot b^R = b^R.$$

Тогда по определению R-вторичного идемпотента и формулы из теоремы 2 получаем

$$a^R \cdot b^R = b^R \to a^R \leq (b^R)^R = b^R.$$

С другой стороны,

$$a^R \le b^R \to 1 \le a^R \le b^R \to b^R \le b^R \cdot a^R \le b^R b^R = b^R \to b^R \cdot a^R = b^R.$$

Поэтому

$$a^R \le b^R \leftrightarrow a^R \cdot b^R = b^R \cdot a^R = b^R.$$

Остальные эквивалентности проверяются аналогично. □

Множество идемпотентов E любой полугруппы $\mathbf{X}$ всегда можно частично упорядочить, вводя так называемый *естественный порядок* $\preceq$, определяемый для элементов $a, b \in E$ следующим образом: $a \preceq b \Leftrightarrow a = a \cdot b = b \cdot a$ (см. [1, 3] и [2, §7.1]).

Следующее утверждение сразу следует из теоремы 4.

Теорема 5. *Какой бы стабильный порядок $\le$ ни был на моноиде $\mathbf{X}$, всегда выполняется равенство $\le = \preceq$ на множестве вторичных идемпотентов минимального типа $E_\downarrow \subseteq \mathbf{X}$, и равенство $\le = \succeq$ на множестве вторичных идемпотентов максимального типа $E^\uparrow$, где $\preceq$ — естественный порядок на множестве идемпотентов $E \subseteq \mathbf{X}$, а частичный порядок $\succeq = \preceq^{-1}$ является обратным для естественного порядка $\preceq$.*

Теорема 6. *Если естественный частичный порядок на множестве идемпотентов $E \subseteq \mathbf{X}$ можно продолжить до стабильного частичного порядка на всем моноиде $\mathbf{X}$, то множество вторичных идемпотентов минимального типа относительно этого частичного порядка состоит из всех идемпотентов моноида $E_\downarrow = E$, а множество вторичных идемпотентов максимального типа состоит из одного элемента: $E^\uparrow = \{1\}$.*

Доказательство. Из определения естественного частичного порядка на множестве идемпотентов $a \preceq b \Leftrightarrow a = a \cdot b = b \cdot a$ следует, что все идемпотенты моноида меньше либо равны единице моноида. □

Приведем пример нетривиального строения множества идемпотентов. Рассмотрим множество всех бинарных отношений $B(X)$ на множестве X ($|X| \ge 3$), которое определяется как множество всевозможных подмножеств декартова квадрата $X \times X$ с частичным порядком включения $\subseteq$. На множестве $B(X)$ определена естественным образом структура моноида с операцией умножения бинарных отношений и единицей $\Delta = \{(x, x) | x \in X\}$. Заметим, что частичный порядок включения $\subseteq$ стабилен относительно умножения бинарных отношений. Для этого частично упорядоченного моноида $(B(X), \subseteq)$ вторичными идемпотентами минимального типа являются все бинарные отношения ρ, для которых выполняется $\rho \subseteq \Delta$, например, $\rho = \{(x, x), (y, y)\}$ для любых $x, y \in X$. Очевидно также, что множество первичных идемпотентов E_0 непусто. Например,

$$\{(x, x), (x, y), (y, y), (y, x)\} \in E_0 \subset B(X).$$

Множество вторичных идемпотентов максимального типа $E^\uparrow$ содержит также элементы, отличные от Δ. Например, $\Delta \cup \{(x, y), (y, x)\} \in E^\uparrow \subset B(X)$.

Таким образом, частичный порядок $\subseteq$, определенный на моноиде $B(X)$ всех бинарных отношений на множестве X, не является продолжением естественного порядка $\preceq$, определенного на множестве всех его идемпотентов $E \subset B(X)$, хотя и совпадает с ним на множестве вторичных идемпотентов минимального типа $E_\downarrow \subset E \subset B(X)$.

Литература

1. *Вагнер В. В.* Обобщенные группы // ДАН СССР. 1952. № 84. С. 1119—1122.
2. *Клиффорд А., Престон Г.* Алгебраическая теория полугрупп. В 2 т. М. : Мир, 1972. Т. 2. 422 с.
3. *Mitsch H.* A Natural Partial Order for Semigroups // Proceedings of the Amer. Math. Society. 1986. Vol. 97, № 3. P. 384—388.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О ФОРМАЦИЯХ УНАРОВ

А. Л. Расстригин (Волгоград)[1]

1. Введение

Класс алгебраических систем называется *формацией*, если он замкнут относительно взятия гомоморфных образов и конечных подпрямых произведений. Формации получили широкое распространение в теории конечных групп [2, 3]. Также разными авторами изучались формации и некоторых других типов алгебраических систем. Общие моменты, касающиеся формаций произвольных алгебраических систем, описаны в [4].

Совокупность формаций, которой вместе с любыми двумя ее формациями принадлежит их пересечение и наименьшая формация, содержащая две данные, образует решетку относительно включения классов. Например, множество всех формаций конечных алгебраических систем некоторого типа или класс всех формаций, являющихся подформациями данной формации, относительно включения образуют решетки. Свойства и строение различных решеток формаций можно найти в [2, 4, 6].

Напомним, что алгебру с одной единственной унарной операцией f называют *унаром*. В работах [1, 5] описана решетка формаций конечных унаров, в [7] сформулированы свойства решеток формаций не более чем счетных унаров.

В настоящей работе найдено необходимое и достаточное условие для того, чтобы решетка подформаций произвольной формации унаров являлась цепью.

2. Результаты

Циклом называют унар, порождаемый любым своим элементом. Унар называется *связным*, если пересечение любых двух его однопорожденных подалгебр непусто. Если унары A_i, $i \in I$, и унар C таковы, что $C = \bigcup_{i\in I} A_i$ и $A_i \cap A_j = \varnothing$ для любых различных $i, j \in I$, то C называется *прямой суммой* унаров A_i, $i \in I$.

Пусть $\mathfrak{F}$ — формация унаров и через $L_F(\mathfrak{F})$ обозначена решетка всех подформаций формации $\mathfrak{F}$.

Теорема. *Решетка $L_F(\mathfrak{F})$ является цепью тогда и только тогда, когда $\mathfrak{F}$ является формацией одного из следующих видов:*

(1) *формация конечных связных унаров, содержащих одноэлементный цикл;*
(2) *формация конечных прямых сумм циклов, длины которых — степени фиксированного для $\mathfrak{F}$ простого числа;*
(3) *подкласс многообразия $f(x) = f(y)$;*
(4) *подкласс многообразия $f(x) = x$.*

Литература

1. *Расстригин А. Л.* Формации конечных унаров // Чебышевский сборник. 2011. Т. 12, вып. 2. С. 102—109.
2. *Скиба А. Н.* Алгебра формаций. Минск : Беларуская навука, 1997.
3. *Шеметков Л. А.* Формации конечных групп. М. : Наука, 1978.
4. *Шеметков Л. А., Скиба А. Н.* Формации алгебраических систем. М. : Наука, 1989.
5. *Jakubíková-Studenovská D., Pócs J.* Formations of finite monounary algebras // Algebra universalis. 2012. Vol. 68, № 3—4. P. 249—255.
6. *Lihová J., Pócs J.* On formations of lattices // Acta Universitatis Matthiae Belii, series Mathematics. 2009. № 15. P. 63—72.
7. *Rasstrigin, A. L.* On lattices of formations of monounary algebras with finitely many cycles // Lobachevskii Journal of Mathematics. 2015. Vol. 36, № 4. P. 419—425.

 Получено 25.12.2017. УДК 512.577.

[1]Волгоградский государственный социально-педагогический университет. E-mail: rasal@fizmat.vspu.ru.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О РИСОВСКИ ПРОСТЫХ АЛГЕБРАХ В КЛАССЕ ТЕРНАРНЫХ АЛГЕБР С ОДНИМ ОПЕРАТОРОМ

В. Л. Усольцев (Волгоград)[1]

В современной универсальной алгебре значительное внимание уделяется изучению взаимосвязей между подалгебрами и конгруэнциями (см., например, [7]). Одна из таких взаимосвязей отражена в понятии рисовски простой алгебры, определяющемся с помощью конгруэнций Риса. В [10] понятие конгруэнции Риса, первоначально введенное для полугрупп, обобщается на произвольные универсальные алгебры. Возникающие при этом определения конгруэнции и подалгебры Риса, приведенные ниже, даны в формулировках работы [6].

Любая конгруэнция алгебры A, представляющаяся как объединение B^2 и отношения равенства $\triangle$ на A для некоторой подалгебры B алгебры A, называется конгруэнцией Риса. Подалгебра B алгебры A называется подалгеброй Риса, если объединение множества B^2 и отношения равенства на A есть конгруэнция алгебры A.

Обозначим через $SubA$ решетку подалгебр универсальной алгебры A, а через $ConA$ — решетку ее конгруэнций. Положим $\emptyset \in SubA$. При этом условии совокупность всех конгруэнций Риса алгебры A образует полную решетку Con_RA относительно включения, нулем и единицей которой являются тривиальные конгруэнции $\bigtriangledown = A^2 \cup \triangle$ и $\triangle = \emptyset^2 \cup \triangle$. Это позволяет ставить для Con_RA задачи, аналогичные тем, которые возникают при изучении решетки $ConA$. В частности, к задачам такого рода относится описание алгебр из заданного класса, решетка конгруэнций Риса которых является двухэлементной цепью. Такие алгебры называются рисовски простыми [5]. Другими словами, неодноэлементная алгебра A рисовски проста, если любая ее конгруэнция Риса является тривиальной.

В настоящей работе изучаются рисовски простые алгебры в некоторых подклассах класса тернарных алгебр с одним оператором. Алгеброй с операторами (см., например, [2, §13]) называется универсальная алгебра $\langle A, \Omega\rangle$ сигнатуры $\Omega = \Omega_1 \cup \Omega_2$, где Ω_1 произвольна и непуста, а Ω_2 состоит из унарных операций, перестановочных с любой операцией из Ω_1, то есть, действующих как эндоморфизмы относительно операций из Ω_1. Унарные операции из Ω_2 называются операторами, а операции из Ω_1 — основными операциями алгебры $\langle A, \Omega\rangle$.

Алгебра с операторами называется тернарной, если она имеет единственную основную операцию, которая является тернарной. Среди тернарных операций особое внимание в алгебре уделяется операциям, перечисленным ниже (см., например, [9]).

Тернарная операция $d(x, y, z)$ называется операцией меньшинства, если для нее выполняются тождества $d(y, y, x) = d(x, y, y) = d(y, x, y) = x$, и операцией большинства, если она удовлетворяет тождествам $d(x, x, y) = d(x, y, x) = d(y, x, x) = x$.

Операцией Пиксли называется тернарная операция $d(x, y, z)$, удовлетворяющая тождествам Пиксли $d(y, y, x) = d(x, y, y) = d(x, y, x) = x$ [8].

Пусть $\langle A, f\rangle$ — произвольный унар, то есть алгебра с одной унарной операцией f. Для любого элемента $z \in A$ через $f^n(z)$ обозначается результат n-кратного применения операции f к элементу z; также положим $f^0(z) = z$.

В [1] показано, что на любом унаре $\langle A, f\rangle$ можно так задать операцию Пиксли $p(x, y, z)$, что алгебра $\langle A, p, f\rangle$ становится алгеброй с оператором f. Эта операция определяется следующим образом. Пусть $x, y \in A$. Положим $M_{x,y} = \{n \in \mathrm{N} \cup \{0\} \mid f^n(x) = f^n(y)\}$, а также

 Получено 23.12.2017. УДК 512.579.

[1]Волгоградский государственный социально-педагогический университет. E-mail: usl2004@mail.ru.

$k(x,y) = \min\ M_{x,y}$, если $M_{x,y} \neq \emptyset$ и $k(x,y) = \infty$, если $M_{x,y} = \emptyset$. Положим далее

$$p(x,y,z) \stackrel{def}{=} \begin{cases} z, & \text{если } k(x,y) \leqslant k(y,z) \\ x, & \text{если } k(x,y) > k(y,z). \end{cases} \tag{1}$$

В [3], на основе подхода, предложенного в [1], на произвольном унаре $\langle A, f\rangle$ задается операция меньшинства $s(x,y,z)$, перестановочная с операцией f:

$$s(x,y,z) \stackrel{def}{=} \begin{cases} z, & \text{если } k(x,y) < k(y,z); \\ y, & \text{если } k(x,y) = k(y,z); \\ x, & \text{если } k(x,y) > k(y,z). \end{cases} \tag{2}$$

Аналогичным способом в [4] на произвольном унаре $\langle A, f\rangle$ задается операция большинства $m(x,y,z)$, перестановочная с f:

$$m(x,y,z) \stackrel{def}{=} \begin{cases} z, & \text{если } k(x,y) \geqslant k(y,z); \\ x, & \text{если } k(x,y) < k(y,z). \end{cases} \tag{3}$$

Через C_h^t, где $h \geqslant 1$, $t \geqslant 0$, обозначается унар $\langle A, f\rangle$ с порождающим элементом a, заданный определяющим соотношением $f^t(a) = f^{t+h}(a)$. Элемент a унара называется периодическим, если $f^t(a) = f^{t+h}(a)$ для некоторых $t \geqslant 0$ и $h \geqslant 1$, и непериодическим в противном случае. Через $T(A)$ и $D(A)$ обозначаются, соответственно, множества периодических и непериодических элементов унара A. Унар $\langle A, f\rangle$ называется периодическим, если $A = T(A)$, и унаром без кручения, если $A = D(A)$. Унар $\langle A, f\rangle$ называется связным, если для любых $x, y \in A$ выполняется условие $f^n(x) = f^m(y)$ для некоторых $n, m \geqslant 0$, и несвязным в противном случае. Подалгебра унара называется подунаром. Максимальный по включению связный подунар унара A называется компонентой связности унара A.

Теорема. *Пусть $\langle A, d, f\rangle$ — тернарная алгебра с оператором f, где $d(x,y,z)$ — операция, определенная по одному из правил (1) — (3). Алгебра $\langle A, d, f\rangle$ является рисовски простой тогда и только тогда, когда выполнено одно из следующих условий:*

1. *$\langle A, f\rangle$ — связный унар без кручения;*
2. *$\langle A, f\rangle$ — связный унар, содержащий подунар, изоморфный C_n^0 для некоторого числа $n > 1$;*
3. *$\langle A, f\rangle$ — унар, содержащий такой элемент a, что $f(x) = a$ для любого $x \in A$;*
4. *$\langle A, f\rangle$ — несвязный унар, каждая компонента связности которого является либо унаром без кручения, либо одноэлементным унаром, либо унаром, содержащим подунар, изоморфный C_n^0 для некоторого $n > 1$.*

Литература

1. *Карташов В. К.* Об унарах с мальцевской операцией // Универсальная алгебра и ее приложения: Тезисы докладов международного семинара, посвященного памяти проф. МГУ Л. А. Скорнякова. Волгоград, 1999. С. 31—32.
2. *Курош А. Г.* Общая алгебра. Лекции 1969-1970 учебного года. М. : Наука, 1974. 160 с.
3. *Усольцев В. Л.* Свободные алгебры многообразия унаров с мальцевской операцией p, заданного тождеством $p(x,y,x) = y$ // Чебышевский сборник. 2011. Т. 12, вып. 2. С. 127—134.
4. *Усольцев В. Л.* О строго простых тернарных алгебрах с операторами // Чебышевский сборник. 2013. Т. 14, вып. 4. С. 196—204.
5. *Усольцев В. Л.* Алгебры Риса и конгруэнц-алгебры Риса в одном классе алгебр с оператором и основной операцией почти единогласия // Чебышевский сборник. 2016. Т. 17, вып. 4. С. 157—166.
6. *Chajda I.* Rees ideal algebras // Math. Bohem. 1997. Vol. 122, № 2. P. 125—130.
7. *Chajda I., Eigenthaler G., Langer H.* Congruence classes in universal algebra. Vienna : Heldermann-Verl., 2003. 192 p.
8. *Pixley A. F.* Distributivity and permutability of congruence relations in equational classes of algebras // Proc. Amer. Math. Soc. 1963. Vol. 14, № 1. P. 105—109.
9. *Szendrei A.* Clones in universal algebra. Montréal : Les presses de l'Université de Montréal, 1986. 166 p.
10. *Tichy R. F.* The Rees congruences in universal algebras // Publ. Inst. Math. (Beograd). 1981. Vol. 29. P. 229—239.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ЭНДОМОРФИЗМЫ БЕСКОНЕЧНЫХ ПОЛУЦИКЛИЧЕСКИХ n-ГРУПП

Н. А. Щучкин (Волгоград)[1]

1. Введение

В 60-е и 70-е годы прошлого века в теории универсальных алгебр активно изучались абелевы алгебры (см. [4, стр. 87]). Одним из основных направлений в теории общей алгебры является описание всех абелевых алгебр в многообразиях классических алгебр и изучение этих алгебр. Так, например, в многообразии групп абелевыми алгебрами будут в точности абелевы группы. Дальше мы вспомним процесс обобщения понятия группы, т. е. рассмотрим определение n-группы для $n \geq 2$, а затем опишем в точности все абелевы алгебры в многообразии n-групп (это было сделано в теореме 3 из [7]).

На непустом множестве G рассмотрим n-арную операцию f, где $n \geq 2$. Алгебру $\langle G, f\rangle$ называют n-группоидом. При действии n-арной операции f для сокращения записи используют стандартные обозначения

$$f(x_1, \ldots, x_k, x_{k+1}, \ldots, x_{k+s}, x_{k+s+1}, \ldots, x_n) = f(x_1^k, \overset{(s)}{x}, x_{k+s+1}^n),$$

где $x_{k+1} = \ldots = x_{k+s} = x$ (x_i^j — пустой символ при $i > j$, также $\overset{(0)}{x}$ — пустой символ).

Если в n-группоиде $\langle G, f\rangle$ выполняется закон ассоциативности

$$\begin{gathered} f(f(x_1, x_2, \ldots, x_{n-1}, x_n), x_{n+1}, \ldots, x_{2n-1}) = \\ = f(x_1, f(x_2, \ldots, x_{n-1}, x_n, x_{n+1}), \ldots, x_{2n-1}) = \ldots \\ \ldots = f(x_1, x_2, \ldots, x_{n-1}, f(x_n, x_{n+1}, \ldots, x_{2n-1})), \end{gathered}$$

то его называют n-полугруппой.

Если в n-полугруппе $\langle G, f\rangle$ для любых элементов $x_0, x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ ($i = 1, \ldots, n$) существует и притом единственный элемент z такой, что

$$f(x_1^{i-1}, z, x_{i+1}^n) = x_0,$$

то ее называют n-группой. При $n = 2$ имеем хорошо знакомое нам определение группы, поэтому можно сказать, что определение n-группы является обобщением определения группы. Более подробную информацию о теории n-групп можно найти в работах [1, 2, 5].

Нас интересуют полуабелевы n-группы. Если в n-группе верно тождество

$$f(x_1, x_2^{n-1}, x_n) = f(x_n, x_2^{n-1}, x_1),$$

то ее называют полуабелевой. Следующая теорема описывает в точности все абелевы алгебры в многообразии n-групп для $n \geq 3$.

Теорема 1 [7, теорема 3]**.** *Любая n-группа для $n \geq 3$ является полуабелевой тогда и только тогда, когда она является абелевой универсальной алгеброй.*

Если в n-группе верны тождества

$$f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

для любой подстановки $\sigma \in S_n$, то ее называют абелевой. Ясно, что любая абелева n-группа является полуабелевой, обратно неверно.

 Получено 24.12.2017. УДК 512.548.

[1]Волгоградский государственный социально-педагогический университет.
E-mail: nikolaj_shchuchkin@mail.ru.

2. Предварительные сведения

Имеется тесная связь между группами и n-группами. Отметим частный случай основных результатов работ [3, 9] для полуабелевых n-групп. На любой полуабелевой n-группе $\langle G, f\rangle$ для фиксированного элемента c можно определить сложение по правилу

$$a + b = f(a, \overset{(n-3)}{c}, \bar{c}, b).$$

Получим абелеву группу G с этим сложением, причем элемент c будет нулем в этой группе. Далее, для отображения $\varphi(x) = f(c, x, \overset{(n-3)}{c}, \bar{c})$, которое является автоморфизмом группы G, и элемента $d = f(\overset{(n)}{c})$ верны равенства

$$\varphi(d) = d, \quad \varphi^{n-1}(x) = x \quad \text{для любого элемента } x \in G, \tag{1}$$

$$f(a_1, \ldots, a_n) = a_1 + \varphi(a_2) + \ldots + \varphi^{n-2}(a_{n-1}) + a_n + d \tag{2}$$

для любых элементов $a_1, \ldots, a_n \in G$. Группу G в этом случае называют ретрактом n-группы $\langle G, f\rangle$ и обозначают $ret_c\langle G, f\rangle$. Известно, что любые два ретракта одной и той же n-группы изоморфны (см. [3, 9]).

Верно и обратно: в любой аддитивной абелевой группе G для выбранных автоморфизма φ и элемента d с условиями (1) задается полуабелева n-группа $\langle G, f\rangle$, где f действует по правилу (2). В этом случае n-группу $\langle G, f\rangle$ называют (φ, d)-определенной на группе G и обозначают $der_{\varphi,d}G$. Известно (см., например, [8]), что для абелевых n-групп и только для них автоморфизм φ, построенный выше, является тождественным.

Обобщением классических алгебр являются также следующие обобщения определения почтикольца и кольца (алгебру $\langle A, +, \circ\rangle$ называют почтикольцом, если $\langle A, +\rangle$ — группа (не обязательно абелева), $\langle A, \circ\rangle$ — полугруппа и выполнен правый закон дистрибутивности (см., например, [4, с. 96]). Алгебру $\langle A, g, \circ\rangle$ с n-арной операцией g и бинарной операцией $\circ$ называют $(n, 2)$-почтикольцом ($(n, 2)$-кольцом) (см., например, [7]), если $\langle A, g\rangle$ является n-группой (абелевой n-группой), $\langle A, \circ\rangle$ является полугруппой и выполнен правый закон дистрибутивности

$$g(x_1^n) \circ y = g(x_1 \circ y, \ldots, x_n \circ y) \tag{3}$$

(оба закона дистрибутивности: $y \circ g(x_1^n) = g(y \circ x_1, \ldots, y \circ x_n)$ и (3)).

Теорема 2 [7, следствия 9 и 10]. *Множество E всех эндоморфизмов полуабелевой (абелевой) n-группы $\langle G, f, \rangle$ является $(n, 2)$-почтикольцом ($(n, 2)$-кольцом) $\langle E, g, \circ\rangle$ с единицей, где n-арная операция g действует по правилу*

$$g(\alpha_1, \ldots, \alpha_n)(x) = f(\alpha_1(x), \ldots, \alpha_n(x)) \ (x \in G),$$

и $\circ$ — композиция эндоморфизмов.

Как и в теории абелевых групп, одной из основных проблем для полуабелевых n-групп является нахождение $(n, 2)$-почтиколец, которые были бы изоморфны $(n, 2)$-почтикольцам эндоморфизмов некоторых полуабелевых n-групп. В данной работе такие $(n, 2)$-почтикольца найдены для бесконечных полуциклических n-групп.

У изоморфных полуабелевых (абелевых) n-групп $(n, 2)$-почтикольца ($(n, 2)$-кольца) эндоморфизмов изоморфны. Проверяется непосредственно.

Если ретракт полуабелевой n-группы является циклической группой, то эту n-группу называют полуциклической. Рассмотрим аддитивную группу целых чисел Z, в которой всего два автоморфизма: тождественный 1_Z и φ, где $\varphi(z) = -z$ для любого целого числа z. Строим абелеву n-группу $\langle Z, f_1\rangle = der_{1_Z,l}Z$, где l — любое целое число, она является примером бесконечной абелевой полуциклической n-группы. Операция f_1 действует по правилу: $f_1(z_1, \ldots, z_n) = z_1 + \ldots + z_n + l$. Для нетождественного автоморфизма φ бесконечной циклической группы Z равенство $\varphi^{n-1}(x) = x$ для любого целого числа x верно только при нечетных n, причем элемент d может быть только нулем. Тогда на бесконечной циклической группе Z можно задать полуциклическую n-группу $\langle Z, f_2\rangle = der_{\varphi,0}Z$ для $n = 2k + 1$, $k \in N$, с n-арной операцией $f_2(z_1, \ldots, z_n) = z_1 - z_2 + \ldots + z_{2k-1} - z_{2k} + z_{2k+1}$.

Любая бесконечная полуциклическая n-группа изоморфна n-группе $\langle Z, f_1\rangle = der_{1_Z,l}Z$,

где $0 \le l \le [\frac{n-1}{2}]$, либо n-группе $\langle Z, f_2\rangle = der_{\varphi,0}Z$ для нечетных n (см. [6]). В первом случае будем говорить, что такая n-группа имеет тип $(\infty, 1, l)$, а во втором случае — имеет тип $(\infty, -1, 0)$.

Если n-группа порождается одним элементом a, то ее называют (как и в группах) циклической с порождающим элементом a. Примером бесконечной циклической n-группы служит n-группа $\langle Z, f_1\rangle = der_{1_Z,1}Z$ с порождающим элементом 0. Любая другая бесконечная циклическая n-группа изоморфна этой n-группе (см., например, [6]).

3. Результаты

В следующей теореме найдено $(n,2)$-кольцо, которое изоморфно $(n,2)$-кольцу эндоморфизмов бесконечной абелевой полуциклической n-группы $\langle Z, f_1\rangle = der_{1_Z,l}Z$, где $0 \le l \le [\frac{n-1}{2}]$.

Теорема 3. *Пусть $\langle E, g, \circ\rangle$ — $(n,2)$-кольцо эндоморфизмов бесконечной абелевой полуциклической n-группы $\langle Z, f_1\rangle = der_{1_Z,l}Z$, где $0 \le l \le [\frac{n-1}{2}]$. В Z выделим множество $P = \{m \mid ml \equiv l \pmod{n-1}\}$ и на этом множестве определим n-арную операцию h по правилу $h(m_1^n) = m_1 + \ldots + m_n$. Тогда алгебра $\langle P, h, \cdot\rangle$, где $\cdot$ — умножение целых чисел, будет $(n,2)$-кольцом, которое изоморфно $\langle E, g, \circ\rangle$.*

Следствие 1. *Пусть $\langle E, g, \circ\rangle$ — $(n,2)$-кольцо эндоморфизмов полуциклической n-группы типа $(\infty, 1, l)$. Тогда $(n,2)$-кольцо $\langle P, h, \cdot\rangle$, построенное в теореме, будет изоморфно $\langle E, g, \circ\rangle$.*

Следствие 2. *Пусть $\langle E, g, \circ\rangle$ — $(n,2)$-кольцо эндоморфизмов бесконечной циклической n-группы. Тогда $(n,2)$-кольцо $\langle P, h, \cdot\rangle$, построенное в теореме при $l = 1$, будет изоморфно $\langle E, g, \circ\rangle$.*

В следующей теореме найдено $(n,2)$-почтикольцо, изоморфное $(n,2)$-почтикольцу эндоморфизмов бесконечной полуциклической n-группы $\langle Z, f_2\rangle = der_{\varphi,0}Z$, где n — нечетное натуральное число и $\varphi(z) = -z$ для любого целого числа z.

Теорема 4. *Пусть $\langle E, g, \circ\rangle$ — $(n,2)$-почтикольцо эндоморфизмов бесконечной полуциклической n-группы $\langle Z, f_2\rangle = der_{\varphi,0}Z$, где n — нечетное натуральное число и $\varphi(z) = -z$ для любого целого числа z. Выбираем n-группу $\langle Z \times Z, h\rangle = \langle Z, f_2\rangle \times \langle Z, f_2\rangle$ и на множестве $Z \times Z$ определим бинарную операцию $\diamond$ по правилу*

$$(m_1, u_1) \diamond (m_2, u_2) = (m_1 m_2, m_1 u_2 + u_1).$$

Тогда $\langle Z \times Z, h, \diamond\rangle$ будет $(n,2)$-почтикольцом, которое изоморфно $\langle E, g, \circ\rangle$.

Следствие 3. *Пусть $\langle E, g, \circ\rangle$ — $(n,2)$-почтикольцо эндоморфизмов полуциклической n-группы типа $(\infty, -1, 0)$. Тогда $(n,2)$-почтикольцо $\langle Z \times Z, h, \diamond\rangle$, построенное в теореме, будет изоморфно $\langle E, g, \circ\rangle$.*

Литература

1. *Гальмак А. М.* n-Арные группы. Часть 1. Гомель : Гомельский государственный университет им. Ф. Скорины, 2003. 195 с.
2. *Гальмак А. М.* n-Арные группы. Часть 2. Минск : Издательский центр БГУ, 2007. 323 с.
3. *Глускин Л. М.* Позиционные оперативы // Математический сборник. 1965. Т. 68 (110), № 3. С. 444—472.
4. *Курош А. Г.* Общая алгебра. Лекции 1969-1970 уч. года. М. : Наука, 1974. 160 с.
5. *Русаков С. А.* Алгебраические n-арные системы. Минск : Навука і техніка, 1992. 263 с.
6. *Щучкин Н. А.* Полуциклические n-арные группы // Известия Гомельского государственного университета им. Ф. Скорины. 2009. Т. 3, № 54. С. 186—194.
7. *Glazek K., Gleichgewicht B.* Abelian n-groups // Proc. Congr. Math. Soc. J. Bolyai Esztergom (Hungaru). 1977. Vol 29. P. 321—329.
8. *Glazek K., Michalski J., Sierocki I.* On evaluation of some polyadic groups // Contributions to General Algebra. 1985. Vol. 3. P. 157—171.
9. *Hosszu M.* On the explicit form of n-group operations // Publ. Math. 1963. Vol. 10. P. 88—92.

Секция 4

МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

НЕКОТОРЫЕ МЕТОДЫ СИМВОЛЬНОГО АНАЛИЗА ОДНОСЧЕТЧИКОВЫХ СЕТЕЙ ПЕТРИ[1]

В. А. Башкин (Ярославль)[2]

1. Введение

Односчетчиковые сети, известные также как одномерные системы векторного сложения с состояниями (1-dim Vector Addition Systems with States — VASS), эквивалентны сетям Петри с одной неограниченной позицией, а также магазинным автоматам с односимвольным стековым алфавитом. Ограничение количества счетчиков делает их менее выразительными, чем обыкновенные сети Петри. С другой стороны, многие алгоритмические проблемы становятся разрешимыми, и в результате сама модель оказывается более удобной для различных специфических задач моделирования и анализа систем.

В работе [1] мы использовали теоретико-числовой метод, основанный на числах Фробениуса, для изучения периодичности значений счетчика односчетчиковой сети. Было доказано, что бесконечное множество достижимых значений счетчика полностью описывается конечным числом арифметических прогрессий с общей разностью.

В работе [2] был представлен метод приближения наибольшей бисимуляции в односчетчиковой сети, основанный на использовании однопериодической символьной арифметики и понятия расслоенной бисимуляции.

В работах [3, 4] введено и исследовано сужение класса односчетчиковых сетей — положительные односчетчиковые контуры. Показано, что в контуре бесконечная часть множества достижимости описывается арифметической прогрессией; получены оценки параметров этой прогрессии через структурные свойства диаграммы переходов. Показано, что для любой односчетчиковой сети существует эквивалентная (в смысле достижимости) правильно сформированная сеть, которая может быть эффективно построена из соответствующего дерева контуров.

В данной работе приводятся результаты, лежащие в основе методов символьных вычислений над одномерными полулинейными множествами, используемых для анализа односчетчиковых сетей Петри.

2. Однопериодические базисы

Для удобства введём новое обозначение одномерных линейных множеств (линейных множеств натуральных чисел). Пусть $m \subseteq Nat$ линейно, тогда для некоторого $l \in \mathbf{Z}_+$ выполняется $m = Lin\{v, \{w_1, \ldots, w_l\}\} =_{\text{def}} \{v + n_1 w_1 + \ldots + n_l w_l \mid n_1, \ldots, n_l \in Nat\}$, где $v, w_1, \ldots, w_l \in Nat$ фиксированы.

Линейное множество $m \subseteq Nat$ назовём *ограниченно неполным,* если $m = m' \setminus m''$, где m' — линейное, а m'' — конечное множество. Если $m' = Lin\{v, \{w_1, \ldots, w_l\}\}$ и $w \in Nat$ — наибольший элемент m'', то обозначим m как $DLin\{v, w + 1, \{w_1, \ldots, w_l\}\}$. Отметим, что выражение $DLin\{v, w, E\}$ не является точным описанием m — это приближение сверху.

Рассмотрим решение задачи Фробениуса о размене монет, называемое также числами Фробениуса. Требуется найти число, являющееся крупнейшей денежной суммой, не набираемой монетами указанных номиналов. Например, крупнейшая сумма, которая не может быть получена, используя только монеты в 3 и 5 единиц, составляет 7. Задачу для двух переменных (двух номиналов монет) решил Сильвестр в [8]:

 Получено 14.01.2018. УДК 519.71.

[1]Работа выполнена при финансовой поддержке РФФИ, проект № 17-07-00823.

[2]Ярославский государственный университет им. П. Г. Демидова. E-mail: v_bashkin@mail.ru.

Факт. *Для любых взаимно простых натуральных a и b и натурального c, такого что $c \geq (a-1)(b-1)$, диофантово уравнение $ax+by=c$ имеет натуральное решение; при этом уравнение $ax+by=c-1$ не имеет натурального решения.*

Обобщение для произвольного числа переменных (номиналов монет) до сих пор не имеет точного решения. Насколько нам известно, наилучшим приближением сверху является квадрат наибольшего номинала [5, 6]. Использование чисел Фробениуса позволяет доказать, что линейное множество с двумя периодами представимо как ограниченно неполное множество с одним периодом:

Лемма 1. *Пусть $m = Lin\{v, \{w_1, w_2\}\}$, $p = НОД(w_1, w_2)$ и $b = v + p(\frac{w_1}{p} - 1)(\frac{w_2}{p} - 1)$. Тогда $m = DLin\{v, b, \{p\}\}$.*

Будем говорить, что множество m распадается на "неполную" (в некотором смысле хаотичную) "голову" $m_0 \subseteq \{b - kp \mid k \in \{1, 2, \ldots, (\frac{w_1}{p} - 1)(\frac{w_2}{p} - 1)\}\}$ и простой бесконечный периодический "хвост" $m_\infty = \{b + kp \mid k \in Nat\}$.

Итак, любое двухпериодическое линейное множество является подмножеством некоего однопериодического множества, причем мы можем найти точную верхнюю границу "неполной" части. Лемма 1 может быть обобщена на случай s периодов:

Лемма 2. *Пусть $Lin\{v, \{w_1, \ldots, w_s\}\}$, $p = НОД(w_1, \ldots, w_s)$, $c = max\{w_1, \ldots, w_s\}^2$ и $b = v + \frac{c}{p}$. Тогда $m = DLin\{v, b, \{p\}\}$.*

Рассмотрим полулинейное множество над Nat. Оно также обладает единственным "периодом", однако в данном случае это уже не интервал, а вектор. Обозначим $\triangleleft$ и $\triangleright$ — операции сдвига множеств целых неотрицательных чисел соответственно влево и вправо на натуральное число (например, $\{1, 3, 12\} \triangleleft 5 = \{-4, -2, 7\}$).

Лемма 3. *Для любых ограниченно неполных линейных множеств с одним периодом $m' = DLin\{v', b', \{p'\}\}$ и $m'' = DLin\{v'', b'', \{p''\}\}$ полулинейное множество $m = m' \cup m''$ распадается на конечное множество и конечное семейство линейных множеств с одинаковым периодом. Обозначив $p = НОК(p', p'')$ и $b = max\{b', b''\}$, получим, что существует* характеристическое множество $\Psi \subseteq \{b, b+1, b+2, \ldots, b+(p-1)\}$, *такое, что*

$$m = m_0 \cup m_\infty, \quad \text{где} \quad m_0 \subseteq \bigcup_{k=1}^{[\frac{b}{p}]} \big(\Psi \triangleleft kp\big), \; m_\infty = \bigcup_{k=0}^{\infty} \big(\Psi \triangleright kp\big). \tag{1}$$

Дальнейшее обобщение Леммы 3 на произвольное число линейных множеств с произвольным числом периодов:

Теорема 1. *Любое полулинейное множество $m \subseteq Nat$ распадается на конечное множество и конечное семейство линейных множеств с одинаковым периодом: для некоторых $p, b \in Nat$, существует представление m в форме (1).*

Замечание. Пусть все линейные подмножества находятся в однопериодической форме. Тогда наименьшее b не превышает наибольшего базового элемента всех линейных подмножеств m, а наименьшее p равно наименьшему общему кратному всех их периодов. В частности, если все эти периоды попарно взаимно просты, то наименьшее b в точности равно наибольшему базовому элементу всех линейных подмножеств.

Теорема 2. *Пусть $m \subseteq Nat$ — полулинейное множество, представленное в форме (1), $x, y \in Nat$. Пусть $\{A^{(i)}\}$ — последовательность полулинейных множеств, такая что $A^{(0)} = m$, $A^{(i+1)} = (A^{(i)} \triangleleft x) \triangleright y$. Тогда существует $j \leq max\{[\frac{b}{|x-y|}], НОК(p, |x-y|)\} + 1$, такое, что* $\bigcup_{i=1}^{\infty} A^{(i)} = \bigcup_{i=1}^{j} A^{(i)}$.

Теорема раскрывает важное свойство одномерных полулинейных множеств: конечно определенная аддитивная последовательность стабилизируется за конечное число шагов. Это свойство стабилизации было доказано как лемма в [7], но только для сложения (сдвига вправо) и без каких-либо оценок требуемого количества шагов.

Рассмотрим двоичный вектор v длины p, такой что $v[i] = 0$ для $b + i \notin \Psi$ и $v[i] = 1$ для $b + i \in \Psi$. Теорема 1 утверждает, что этот вектор является "битовой маской" для периодического "закрашивания" натурального ряда справа от числа b. Таким образом, мы можем использовать в качестве конечного символьного представления произвольного полулинейного одномерного множества m его *однопериодический базис* (m_0, b, p, v), состоящий из

- конечного *базового множества* m_0,
- *базового элемента* b,
- *длины периода* p,
- *вектора периода* v.

Определение. Базис $Z = (m_0, b, p, v)$ полулинейного множества $m \subseteq Nat$ называется *минимальным*, если для любого базиса $Z' = (m'_0, b', p', v')$ множества m выполняется $p < p'$ или $(p = p'$ и $b \le b')$.

Теорема 3. *Для любого одномерного полулинейного множества $m \subseteq Nat$ минимальный базис $Base(m)$ существует и единственен.*

Произвольный базис (m_0, b, p, v) полулинейного множества $m \subseteq Nat$ может быть преобразован в минимальный базис $Base(m)$ за полиномиальное время относительно $b * p$.

Множество, определяемое базисом Z, обозначим как $Set(Z)$. Обозначим процедуру минимизации базиса (m_0, b, p, v) как $Mmz(m_0, b, p, v)$. Для двоичных векторов $v, v' \in \{0, 1\}^p$ через $NOT(v)$, $AND(v, v')$ и $OR(v, v')$ обозначим покомпонентное умножение, сложение и отрицание: $AND(v, v')[i] =_{\text{def}} min\{v[i], v'[i]\}$, $OR(v, v')[i] =_{\text{def}} max\{v[i], v'[i]\}$, $NOT(v)[i] =_{\text{def}} (1 - v[i])$. Через v^k обозначим конкатенацию k векторов v.

Теоретико-множественные операции и отношения могут эффективно вычисляться не над множествами, а непосредственно над их одноперiодическими базисами:

Теорема 4. *Пусть $m, m' \subseteq Nat$ — полулинейные, $Base(m) = (m_0, b, p, v)$, $Base(m') = (m'_0, b', p', v')$, $y \in Nat$. Обозначим $K = max\{b, b'\}$ и $L = HOK(p, p')$. Пусть $K = b + ip = b' + jp'$ для некоторых $i, j \in Nat$. Тогда:*

(1) $Base(Nat) = (\varnothing, 0, 1, (1))$;

(2) $Base(m \cup m') = Mmz\big(\{x \in m \cup m' \mid x < K\}, K, L, OR(v^{\frac{L}{p}}, (v')^{\frac{L}{p'}})\big)$;

(3) $Base(m \cap m') = Mmz\big(\{x \in m \cap m' \mid x < K\}, K, L, AND(v^{\frac{L}{p}}, (v')^{\frac{L}{p'}})\big)$;

(4) $Base(m \setminus m') = Mmz\big(\{x \in m \setminus m' \mid x < K\}, K, L, AND(v^{\frac{L}{p}}, NOT((v')^{\frac{L}{p'}}))\big)$;

(5) $m \subseteq m' \iff AND(v^{\frac{L}{p}}, (v')^{\frac{L}{p'}}) = v^{\frac{L}{p}} \ \wedge \ \forall x \in m \ (x < K \Rightarrow x \in m')$;

(6) $Base(m \triangleright y) = Mmz(\{x + y \mid x \in m_0\}, b + y, p, v)$;

(7) $Base(m \triangleleft y) = Mmz(\{x - y \mid x \in m, x < B, x \ge y\}, B, p, v)$, *где* $B = min_{k \in Nat}\{b + kp - y \mid b + kp - y \ge 0\}$.

Заметим, что ограничение $K = b + ip = b' + jp'$ носит технический характер — оно позволяет записать формулы в более краткой форме. Приведенные операции эффективны, то есть выполняются за полиномиальное время относительно размеров входных базисов.

Литература

1. *Башкин В. А.* Верификация на основе моделей с одним неограниченным счетчиком // Информационные системы и технологии. 2010. № 4 (60). С. 5—12.
2. *Башкин В. А.* Построение приближений бисимуляции в односчетчиковых сетях // Моделирование и анализ информационных систем. 2011. Т. 18, № 4. С. 34—44.
3. *Башкин В. А.* Об эффективном моделировании неограниченного ресурса при помощи односчетчиковых контуров // Моделирование и анализ информационных систем. 2013. Т. 20, № 2. С. 139—156.
4. *Bashkin V. A.* One-counter Circuits // Concurrency, Specification and Programming. CSP 2012 Workshop Proceedings. Vol. 1. Berlin, Germany : Humboldt-Universitat zu Berlin, 2012. P. 25—36.
5. *Brauer A.* On a Problem of Partitions // American Journal of Mathematics. 1942. Vol. 64, № 1. P. 299—312.
6. *Erdös P., Graham R. L.* On a linear diophantine problem of Frobenius // Acta Arithm. 1972. Vol. 21. P. 399—408.
7. *Hopcroft J., Pansiot J.-J.* On the reachability problem for 5-dimensional vector addition systems // Theor. Comp. Science. 1979. Vol. 8, № 2. P. 135—159.
8. *Sylvester J. J.* Question 7382 // Mathematical Questions with their Solutions, Educ. Times. 1884. Vol. 41. P. 21.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

НЕКОТОРЫЕ СВОЙСТВА ИНТУИЦИОНИСТСКОЙ ТЕОРИИ МНОЖЕСТВ ЦЕРМЕЛО–ФРЕНКЕЛЯ С ДОПОЛНИТЕЛЬНЫМ ПРПИНЦИПОМ DCS[1]

А. Г. Владимиров (Москва)[2]

Рассматривается теория множеств Цермело–Френкеля с подлежащей интуиционистской логикой (для краткости будем называть ее интуиционистской теорией множеств Цермело–Френкеля) в двусортном языке (где сорт 0 — для чисел, а сорт 1 — для множеств) со схемой $Collection$ в качестве схемы аксиом подстановки (теория $ZFI2C$). Язык теории $ZFI2C$ содержит константу 0, функциональные символы для всех примитивно рекурсивных функций, а также двухместные предикатные символы $=^0$ для равенства чисел, $=^1$ для равенства множеств, $\in^0$ для принадлежности числа множеству и $\in^1$ для принадлежности множества множеству.

Аксиомы теории $ZFI2C$ содержат все обычные аксиомы и правила Гейтингова исчисления предикатов HPC, все обычные аксиомы и правила Гейтинговой арифметики HA, а также все обычные аксиомы Цермело–Френкеля, включая схему $Collection$ в качестве схемы аксиом подстановки, схема $\in^1$-индукции как схемы регулярности, а также обычных аксиом пары, суммы, степени, выделения и аксиомы бесконечности в виде $\exists x \forall a (a \in x)$.

Напомним дополнительные интуиционистские принципы, которые мы здесь будем рассматривать.

0. Принцип DCS (Double Complement of Sets)

Этот принцип необходим, если мы хотим, чтобы интуиционистская теория множеств Цермело–Френкеля содержала классическую теорию в смысле Геделева негативного перевода, переводящего $\in^0$ в $\in^0$ и $\in^1$ в $\in^1$ Он утверждает, что для каждого множества существует множество всех его не-не-элементов.

Формально принцип DCS записывается следующим образом:

$$\forall x \exists y [\forall z (z \in y \equiv \neg\neg(z \in x)) \wedge \forall a (a \in y \equiv \neg\neg(a \in x)].$$

1. Сильный тезис Черча утверждает, что если для любого a найдется такое b, что выполняется условие $\varphi(a;b)$, то существует общерекурсивная функция с номером e, которая по каждому числу a находит требуемое число b. При этом происходит выбор одного из таких b. Этот принцип отражает конструктивное понимание кванторов по числам. Фактически он утверждает, что любая определимая в теории $\mathbb{ZFI}2C$ арифметическая функция вычислима, так как в CT формула $\varphi(a;b)$ может быть любой формулой языка теории $\mathbb{ZFI}2C$, возможно, с параметрами по множествам.

2. Слабый тезис Черча $CT!$ отличается от сильного только единственностью в посылке:

$$\forall a \exists! b \varphi(a;b) \to \exists e \forall a \exists b [\{e\}(a) = b. \wedge \varphi(a;b)].$$

Здесь, как обычно, $\forall a \exists! b \varphi(a;b)$ означает “для каждого a существует единственное b, такое, что $\varphi(a;b)$”.

Понятно, что CT влечет $CT!$ даже в HPC. Обратное неверно.

 Получено 15.01.2018. УДК 510.649

[1]Работа выполнена при финансовой поддержке гранта РФФИ “Теоретико-модельные и алгоритмические проблемы в модальных и алгебраических логиках”, проект № 16-01-00615.

[2]Московский государственный университет им. М. В. Ломоносова. E-mail: moskvich7707@mail.ru.

3. Тезис Черча в форме nCT имеет вид:

$$[\forall a[\neg\psi(a) \to \exists b\varphi(a;b)] \to \exists c\forall a[\neg\psi(a) \to \exists b(\{e\}(a) = b. \wedge \varphi(a;b))].$$

Во всех трех схемах $\varphi(a;b)$ — произвольная формула языка теории $\mathbb{ZFI}2C$. В схеме nCT $\psi(a)$ — произвольная почти негативная арифметическая формула.

4. Расширенный тезис Черча ECT имеет вид:

$$\forall a[\psi(a) \to \exists b\varphi(a;b)] \to \exists c\forall a[\psi(a) \to \exists b(\{c\}(a) = b. \wedge \varphi(a;b))].$$

Здесь $\varphi(a;b)$ — произвольная формула языка теории $\mathbb{ZFI}2C$, а $\psi(a)$ — произвольная почти негативная арифметическая формула.

Как и в арифметике, здесь легко доказать, что $ECT \to nCT \to CT \to CT!$. Обратное неверно.

5. Принцип конструктивного подбора M (сильный принцип Маркова):

$$\forall a(\varphi(a) \vee \neg\varphi(a)) \wedge \neg\neg\exists a\varphi(a) \to \exists a\varphi(a).$$

6. Слабый принцип конструктивного подбора M^- (слабый принцип Маркова):

$$\neg\neg\exists a\varphi(a) \to \exists a\varphi(a).$$

Здесь $\varphi(a)$ — бескванторная арифметическая формула.

Приведем аргумент в пользу приемлемости сильного принципа Маркова: допустим, что мы можем для некоторой формулы $\varphi(a)$ для каждого натурального числа n проверить, что именно истинно, $\varphi(n)$ или $\neg\varphi(n)$, и пусть еще доказано (неформально), что $\neg\neg\exists a\varphi(a)$. Тогда последовательно проверяем, верно ли $\varphi(0)$, затем $\varphi(1)$ и т. д. Рано или поздно мы найдем такое n, что истинно $\varphi(n)$, так как иначе было бы $\neg\exists a\varphi(a)$, вопреки второй посылке принципа. Конечно, сильный принцип Маркова влечет слабый. Обратное неверно. Отметим еще, что слабый принцип Маркова невыводим в нашей теории $\mathbb{ZFI}2C + DCS$.

7. Принцип униформизации:

$$\forall x\exists a\varphi(x;a) \to \exists a\forall x\varphi(x;a).$$

8. Принцип UZ:

$$\forall x(\varphi(x) \vee \psi(x)) \to \forall x\varphi(x) \vee \forall x\psi(x).$$

Доказаны некоторые свойства частичной консервативности интуиционистской теории множеств Цермело–Френкеля с принципом двойного дополнения (DCS) относительно некоторого класса арифметических формул (класса всех так называемых AEN-формул). А именно, пусть T — любая из теорий $ZFI2C$ и $ZFI2C + DCS$, ECT — это расширенный тезис Черча, M — сильный принцип Маркова, а M^- — слабый принцип Маркова. Тогда выполняется:

Теорема 1. *Пусть T — любая из теорий $ZFI2C$ и $ZFI2C + DCS$.*

(1) *Теория $T + ECT$ консервативна над T относительно класса AEN-формул.*
(2) *Теория $T + ECT + M$ консервативна над $T + M^-$ относительно класса AEN-формул.*

Теорема 2. *К теории T можно добавить принципы UP и UZ с сохранением всех утверждений теоремы 1.*

Кроме того, доказаны следующие свойства частичной консервативности:

Теорема 3.

(1) *$T + ECT + M$ консервативна над $T + M^-$ относительно класса всех негативных арифметических формул.*
(2) *Классическая теория $ZF2$ консервативна над $ZFI2C$ относительно класса всех негативных арифметических формул.*

В доказательстве используется формализованный вариант Клини-реализуемости для теории множеств Цермело–Френкеля.

С другой стороны, доказаны следующие свойства эффективности.

Пусть снова T — это $\mathbb{ZFI}2C$ или $\mathbb{ZFI}2C + DCS$. Тогда:

Теорема 4. *Теория T обладает сдедующими свойствами эффективности:*

(1) *Свойство дизъюнктивности: если $T \vdash (\psi \vee \vartheta)$, то $T \vdash \psi$ или $T \vdash \vartheta$.*
(2) *Нумерическая экзистенциальность (EP_ω): если $T \vdash \exists a \psi(a)$, то найдется (эффективно по выводу формулы $\exists a \psi(a)$) такое натуральное n, что $T \vdash \psi(n)$.*
(3) *Допустимость правила Черча (CR): если $T \vdash \forall a \exists b \psi(a; b)$, то найдется (эффективно по выводу формулы $\forall a \exists b \psi(a; b)$) такое натуральное e, что $T \vdash \forall a \psi(a; \{e\}(a))$.*
(4) *Допустимость правила Маркова (MR): если $T \vdash \forall a(\varphi \vee \neg\varphi)$ и $T \vdash \neg\neg\exists a \psi(a)$, то $T \vdash \neg\neg\exists a \psi(a)$.*
(5) *Допустимость правила униформизации (UR):*
если $T \vdash \forall x \exists a \psi(x; a)$, то $T \vdash \exists a \forall x \psi(x; a)$.
(6) *Допустимость правила UZR:*
если $T \vdash \forall x(\varphi(x) \vee \psi(x))$, то $T \vdash \forall x \varphi(x)$, или $T \vdash \forall x \psi(x)$.

Во всех случаях все входящие в них формулы могут содержать параметры по множествам (но не по числам). Выводы заключений получаются эффективно по выводу посылок.

Теорема 5. *Пусть T — это $\mathbb{ZFI}2C$ или $\mathbb{ZFI}2C + DCS$. Тогда к теории T можно добавить любую комбинацию принципов M, M^-, ECT (а также любой из остальных вариантов тезиса Черча: nCT, CT $CT!$), UP и UZ с сохранением всех утверждений 1–6 теоремы 4.*

Отметим еще, что из свойства дизъюнктивности теории $\mathbb{ZFI}2C + DCS + M$ и из того, что она включена в классическую $\mathbb{ZF}2C = \mathbb{ZFI}2C + LEM$, на которую, как легко видеть, распростаняются классические результаты Геделя и Коэна о независимости континуум-гипотезы CH, получаем:

Теорема 6. *В теории $\mathbb{ZFI}2C + DCS + M$ не выводится $CH \vee \neg CH$.*

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О ПОИСКЕ ВЫВОДА ДЛЯ БЕСКОНЕЧНОЗНАЧНОЙ ЛОГИКИ ЛУКАСЕВИЧА ПЕРВОГО ПОРЯДКА

А. С. Герасимов (Санкт-Петербург)[1]

1. Введение

Математические нечёткие логики служат для формализации приближённых рассуждений. К важнейшим из таких логик относятся бесконечнозначная логика Лукасевича первого порядка Ł∀ и рациональная логика Павелки первого порядка RPL∀, расширяющая Ł∀ истинностными константами (см. [3, 5]).

Развивая методы поиска вывода для Ł∀ и RPL∀, в [1] мы устранили все структурные правила из введённого в [2] гиперсеквенциального исчисления GŁ∀ для Ł∀ и получили кумулятивное и некумулятивное гиперсеквенциальные исчисления G^1Ł∀ и G^2Ł∀ для RPL∀, в которых выводимо любое GŁ∀-выводимое и любое предварённое GŁ∀-выводимое предложение соответственно. Кроме того, в [1] мы разработали семейство алгоритмов, каждый из которых строит некоторый вывод любого предварённого G^2Ł∀-выводимого предложения в табличном варианте исчисления G^2Ł∀. В [4] мы анонсировали гиперсеквенциальное исчисление G^3Ł∀ для RPL∀, в котором выводимо любое G^1Ł∀-выводимое предложение, а также сообщили о семействе алгоритмов, строящих некоторый вывод любого G^3Ł∀-выводимого предложения в табличном варианте исчисления G^3Ł∀.

В данных тезисах мы более подробно излагаем основные идеи из [4] и одновременно представляем модификацию G^3_eŁ∀ исчисления G^3Ł∀, в которой можно строить более короткие выводы, чем в G^3Ł∀, благодаря расширению понятия аксиомы.

Атомарными формулами логик Ł∀ и RPL∀ являются предикатные символы с термами-аргументами и истинностные константы: $\bar{0}$ в Ł∀, а в RPL∀ — константы $\bar{r}$ для всех рациональных чисел $r \in [0,1]$. *Формулы* логик Ł∀ и RPL∀ строятся обычным образом из атомарных формул с помощью *логических символов*: бинарной связки $\to$ и кванторов $\forall, \exists$.

Понятие *интерпретации* отличается от одноимённого понятия классической логики лишь тем, что предикатному символу сопоставляется предикат, действующий в отрезок $[0,1]$ вещественных чисел. *Истинностное значение* $|C|_{M,\nu}$ RPL∀*-формулы* C при интерпретации M (с носителем $\mathcal{D}$) и оценке ν (предметных переменных) определяется следующим образом:

(1) $|\bar{r}|_{M,\nu} = r$;

(2) $|P(t_1,\ldots,t_n)|_{M,\nu} = P^M(|t_1|_{M,\nu},\ldots,|t_n|_{M,\nu})$, где P^M — предикат, сопоставленный n-местному предикатному символу P в M, $|t_i|_{M,\nu}$ — значение терма t_i при M,ν;

(3) $|A \to B|_{M,\nu} = \min(1 - |A|_{M,\nu} + |B|_{M,\nu},\ 1)$;

(4) $|\forall x A|_{M,\nu} = \inf_{d\in\mathcal{D}} |A|_{M,\nu[x\mapsto d]}$, где $\nu[x \mapsto d]$ — оценка, которая может отличаться от ν лишь в x, $\nu[x \mapsto d](x) = d$;

(5) $|\exists x A|_{M,\nu} = \sup_{d\in\mathcal{D}} |A|_{M,\nu[x\mapsto d]}$.

RPL∀-формула C называется *общезначимой* (обозначение: $\vDash C$), если $|C|_{M,\nu} = 1$ при любых интерпретации M и оценке ν.

2. Гиперсеквенциальное исчисление G^3_eŁ∀

Введём два счётно-бесконечных непересекающихся множества новых слов, такие слова будем называть *полупропозициональными переменными типа* 0 и *типа* 1 соответственно.

Секвенция (записывается как $\Gamma \Rightarrow \Delta$) — это упорядоченная пара конечных мульти-

 Получено 25.12.2017. УДК 510.644+510.662.

[1]E-mail: alexander.s.gerasimov@ya.ru.

множеств Γ и Δ, состоящих из RPL$\forall$-формул и полупропозициональных переменных. *Гиперсеквенция* $(\Gamma_1 \Rightarrow \Delta_1 \,|\, \ldots \,|\, \Gamma_n \Rightarrow \Delta_n)$ — это конечное мультимножество секвенций.

Для придания гиперсеквенциям семантического смысла определим *hs-интерпретацию* как интерпретацию, которая дополнительно сопоставляет каждой полупропозициональной переменной типа 0 (соответственно типа 1) любое вещественное число из $[0, +\infty)$ (соответственно $(-\infty, 1]$). Гиперсеквенция $\mathcal{H}$ называется *общезначимой*, если для любых hs-интерпретации M и оценки ν в $\mathcal{H}$ найдётся такая секвенция $\Gamma \Rightarrow \Delta$, что $\sum_{A\in\Gamma}(|A|_{M,\nu} - 1) \leqslant \leqslant \sum_{B\in\Delta}(|B|_{M,\nu} - 1)$, где суммирование проводится с учётом кратностей элементов мультимножеств и $\sum_{A\in\varnothing}(\ldots) = 0$.

С любой гиперсеквенцией $\mathcal{H}$ ассоциируем систему линейных неравенств $\mathcal{S}_{\mathcal{H}}$, которая строится таким образом:

(1) каждому не являющемуся истинностной константой члену F какой-либо секвенции из $\mathcal{H}$ сопоставим уникальную вещественнозначную переменную X_F;

(2) для каждой секвенции $\Gamma \Rightarrow \Delta$ из $\mathcal{H}$ включим в $\mathcal{S}_{\mathcal{H}}$ неравенство $\sum_{F\in\Gamma}(X_F - 1) > > \sum_{F\in\Delta}(X_F - 1)$, где $X_{\bar{r}} = r$;

(3) для каждой переменной X_F включим в $\mathcal{S}_{\mathcal{H}}$ неравенства $0 \leqslant X_F \leqslant 1$, если F — это RPL$\forall$-формула; или неравенство $0 \leqslant X_F$ (соответственно $X_F \leqslant 1$), если F — полупропозициональная переменная типа 0 (соответственно типа 1).

Гиперсеквенцию $\mathcal{H}$ назовём *аксиомой исчисления* $\mathrm{G}^3_{\mathrm{e}}\text{Ł}\forall$, если система $\mathcal{S}_{\mathcal{H}}$ несовместна. (Гиперсеквенция $\mathcal{H}$ называется *аксиомой исчисления* $\mathrm{G}^3\text{Ł}\forall$, если гиперсеквенция, содержащая в точности все секвенции из $\mathcal{H}$ без логических символов, общезначима. Отметим, что $\mathcal{H}$ является аксиомой исчисления $\mathrm{G}^3\text{Ł}\forall$, если и только если несовместна система, которая строится так же, как $\mathcal{S}_{\mathcal{H}}$, но лишь по секвенциям без логических символов.)

Правила вывода исчисления $\mathrm{G}^3_{\mathrm{e}}\text{Ł}\forall$ (и $\mathrm{G}^3\text{Ł}\forall$):

$$\frac{\mathcal{H} \,|\, \Gamma, \mathfrak{p}_1 \Rightarrow \Delta \,|\, B \Rightarrow \mathfrak{p}_1, A}{\mathcal{H} \,|\, \Gamma, A \to B \Rightarrow \Delta}\ (\to\Rightarrow)^3, \qquad \frac{\mathcal{H} \,|\, \Gamma \Rightarrow \Delta; \quad \mathcal{H} \,|\, \Gamma, A \Rightarrow B, \Delta}{\mathcal{H} \,|\, \Gamma \Rightarrow A \to B, \Delta}\ (\Rightarrow\to)^3,$$

$$\frac{\mathcal{H} \,|\, \Gamma, \mathfrak{p}_1 \Rightarrow \Delta \,|\, \forall x A \Rightarrow \mathfrak{p}_1 \,|\, [A]^x_t \Rightarrow \mathfrak{p}_1}{\mathcal{H} \,|\, \Gamma, \forall x A \Rightarrow \Delta}\ (\forall\Rightarrow)^3, \qquad \frac{\mathcal{H} \,|\, \Gamma \Rightarrow [A]^x_a, \Delta}{\mathcal{H} \,|\, \Gamma \Rightarrow \forall x A, \Delta}\ (\Rightarrow\forall)^3,$$

$$\frac{\mathcal{H} \,|\, \Gamma \Rightarrow \mathfrak{p}_0, \Delta \,|\, \mathfrak{p}_0 \Rightarrow \exists x A \,|\, \mathfrak{p}_0 \Rightarrow [A]^x_t}{\mathcal{H} \,|\, \Gamma \Rightarrow \exists x A, \Delta}\ (\Rightarrow\exists)^3, \qquad \frac{\mathcal{H} \,|\, \Gamma, [A]^x_a \Rightarrow \Delta}{\mathcal{H} \,|\, \Gamma, \exists x A \Rightarrow \Delta}\ (\exists\Rightarrow)^3,$$

где $[A]^x_t$ — результат подстановки терма t вместо всех свободных вхождений предметной переменной x в формулу A; t — замкнутый терм; a — предметная константа, не входящая в заключение ни $(\Rightarrow\forall)^3$, ни $(\exists\Rightarrow)^3$; $\mathfrak{p}_i$ — полупропозициональная переменная типа i $(i = 0, 1)$, не входящая в заключение правила, в посылке которого она явно фигурирует.

Под *выводом* для RPL$\forall$-формулы A (в $\mathrm{G}^3_{\mathrm{e}}\text{Ł}\forall$ или $\mathrm{G}^3\text{Ł}\forall$) понимается вывод гиперсеквенции $\Rightarrow A$ в соответствующем исчислении.

Особенностью исчислений $\mathrm{G}^3_{\mathrm{e}}\text{Ł}\forall$ и $\mathrm{G}^3\text{Ł}\forall$, отличающей их от других известных гиперсеквенциальных исчислений для Ł$\forall$ (т. е. GŁ$\forall$, $\mathrm{G}^1\text{Ł}\forall$ и $\mathrm{G}^2\text{Ł}\forall$), является отсутствие структурных правил и при этом бесповторность всех логических правил. Последнее означает, что ни в какой посылке этих правил нет повторений обозначений мультимножеств.

Бесповторные правила $(\to\Rightarrow)^3$, $(\forall\Rightarrow)^3$ и $(\Rightarrow\exists)^3$ можно получить с помощью нестандартных вариантов правила плотности (ср. [6, раздел 4.5]). Например, заключение правила $(\Rightarrow\exists)^3$ получается из его посылки путём применения правила (a), непосредственно отражающего семантику квантора $\exists$, и последующего применения нестандартного варианта (b) правила плотности:

$$\text{(a)}\ \frac{\mathcal{H} \,|\, \Gamma \Rightarrow \exists x A, \Delta \,|\, \Gamma \Rightarrow [A]^x_t, \Delta}{\mathcal{H} \,|\, \Gamma \Rightarrow \exists x A, \Delta}, \qquad \text{(b)}\ \frac{\mathcal{H} \,|\, \Gamma \Rightarrow \mathfrak{p}_0, \Delta \,|\, \mathfrak{p}_0 \Rightarrow C}{\mathcal{H} \,|\, \Gamma \Rightarrow C, \Delta},$$

где C — это RPL$\forall$-формула, а остальные обозначения и условия аналогичны указанным при формулировке правил вывода исчисления $\mathrm{G}^3_{\mathrm{e}}\text{Ł}\forall$.

Теорема 1. *Для любого* RPL$\forall$*-предложения* A*:* (1) *если* $\vdash_{\mathrm{G}^3_{\mathrm{e}}\text{Ł}\forall} A$*, то* $\vDash A$*;* (2) $\vdash_{\mathrm{G}^1\text{Ł}\forall} A$ *тогда и только тогда, когда* $\vdash_{\mathrm{G}^3\text{Ł}\forall} A$*;* (3) *если* $\vdash_{\mathrm{G}^3\text{Ł}\forall} A$*, то* $\vdash_{\mathrm{G}^3_{\mathrm{e}}\text{Ł}\forall} A$.

3. Табличное исчисление $\mathrm{T}^3_\mathrm{e}\text{Ł}\forall$ и поиск вывода

Ввиду ограниченности объёма тезисов мы весьма кратко изложим табличный вариант $\mathrm{T}^3_\mathrm{e}\text{Ł}\forall$ исчисления $\mathrm{G}^3_\mathrm{e}\text{Ł}\forall$ и алгоритмы поиска $\mathrm{T}^3_\mathrm{e}\text{Ł}\forall$-вывода; более точные формулировки можно дать на основе следующих аналогично [1, § 4].

$\mathrm{T}^3_\mathrm{e}\text{Ł}\forall$-*таблица* для RPL$\forall$-предложения A — это конечное упорядоченное корневое дерево, в котором каждый узел помечен гиперсеквенцией и которое строится, начиная с дерева из одной гиперсеквенции $\Rightarrow A$, по правилам:

(1) $(\to\Rightarrow)^3$ и $(\Rightarrow\to)^3$ из $\mathrm{G}^3_\mathrm{e}\text{Ł}\forall$;

(2) $$\frac{\mathcal{H}\,|\,\Gamma, \mathfrak{p}_1 \Rightarrow \Delta\,|\,\forall xA \Rightarrow \mathfrak{p}_1\,|\,[A]^x_v \Rightarrow \mathfrak{p}_1}{\mathcal{H}\,|\,\Gamma, \forall xA \Rightarrow \Delta}\ (\forall\Rightarrow)^3_\mathrm{T}, \qquad \frac{\mathcal{H}\,|\,\Gamma \Rightarrow [A]^x_{f(v_1,\ldots,v_n)}, \Delta}{\mathcal{H}\,|\,\Gamma \Rightarrow \forall xA, \Delta}\ (\Rightarrow\forall)^3_\mathrm{T},$$

$$\frac{\mathcal{H}\,|\,\Gamma \Rightarrow \mathfrak{p}_0, \Delta\,|\,\mathfrak{p}_0 \Rightarrow \exists xA\,|\,\mathfrak{p}_0 \Rightarrow [A]^x_v}{\mathcal{H}\,|\,\Gamma \Rightarrow \exists xA, \Delta}\ (\Rightarrow\exists)^3_\mathrm{T}, \qquad \frac{\mathcal{H}\,|\,\Gamma, [A]^x_{f(v_1,\ldots,v_n)} \Rightarrow \Delta}{\mathcal{H}\,|\,\Gamma, \exists xA \Rightarrow \Delta}\ (\exists\Rightarrow)^3_\mathrm{T},$$

где v — новая для текущей таблицы предметная переменная, называемая *метапеременной*; f — новый для текущей таблицы функциональный символ, $v_1, \ldots, v_n$ — все (попарно различные) метапеременные, входящие в $\Gamma \Rightarrow \forall xA, \Delta$ для $(\Rightarrow\forall)^3_\mathrm{T}$ (соответственно $\Gamma, \exists xA \Rightarrow \Delta$ для $(\exists\Rightarrow)^3_\mathrm{T}$); остальные обозначения и условия такие же, как в формулировке $\mathrm{G}^3_\mathrm{e}\text{Ł}\forall$;

(3) если T является $\mathrm{T}^3_\mathrm{e}\text{Ł}\forall$-таблицей для A и подстановка σ свободна для каждой формулы в T, то $T\sigma$ является $\mathrm{T}^3_\mathrm{e}\text{Ł}\forall$-таблицей для A (*правило подстановки*).

$\mathrm{T}^3_\mathrm{e}\text{Ł}\forall$-таблица для RPL$\forall$-предложения A называется *закрытой*, или $\mathrm{T}^3_\mathrm{e}\text{Ł}\forall$-*выводом* для A, если все её листовые гиперсеквенции являются аксиомами исчисления $\mathrm{G}^3_\mathrm{e}\text{Ł}\forall$. Также мы говорим, что $\mathrm{T}^3_\mathrm{e}\text{Ł}\forall$-таблица *закрываема*, если некоторое применение правила подстановки превращает её в закрытую.

Теорема 2. *Для любого* RPL$\forall$-*предложения* A: (1) *если* $\vdash_{\mathrm{T}^3_\mathrm{e}\text{Ł}\forall} A$, *то* $\vDash A$; (2) *если* $\vdash_{\mathrm{G}^3_\mathrm{e}\text{Ł}\forall} A$, *то* $\vdash_{\mathrm{T}^3_\mathrm{e}\text{Ł}\forall} A$.

При поиске вывода в $\mathrm{T}^3_\mathrm{e}\text{Ł}\forall$ используем вспомогательный алгоритм — *тактику*, указывающую по $\mathrm{T}^3_\mathrm{e}\text{Ł}\forall$-таблице вхождение в неё формулы (в качестве члена секвенции), к которому должно быть применено некоторое правило исчисления $\mathrm{T}^3_\mathrm{e}\text{Ł}\forall$.

При данной тактике алгоритм поиска $\mathrm{T}^3_\mathrm{e}\text{Ł}\forall$-вывода может работать по такой схеме: применять правила к текущей таблице в соответствии с выбором тактики, пока текущая таблица не станет закрываемой. Алгоритм проверки закрываемости $\mathrm{T}^3_\mathrm{e}\text{Ł}\forall$-таблицы подобен описанному в [1, раздел 4.2], но включает в себя унификацию, вообще говоря, неатомарных RPL$\forall$-формул.

Тактика называется *справедливой*, если для любого RPL$\forall$-предложения A в (возможно, бесконечном) дереве, построенном, исходя из $\Rightarrow A$, в соответствии с этой тактикой, верно следующее: для любой ветви $\mathcal{B}$ и любого находящегося на $\mathcal{B}$ вхождения $\mathcal{F}$ неатомарной формулы в качестве члена секвенции применяется правило к некоторому предку $\mathcal{F}$ на $\mathcal{B}$.

Теорема 3. *Любой алгоритм, работающий по приведённой выше схеме и использующий справедливую тактику, строит некоторый* $\mathrm{T}^3_\mathrm{e}\text{Ł}\forall$-*вывод для любого* $\mathrm{G}^3\text{Ł}\forall$-*выводимого предложения.*

Литература

1. *Герасимов А. С.* Бесконечнозначная логика Лукасевича первого порядка: гиперсеквенциальные исчисления без структурных правил и поиск вывода предварённых предложений // Математические труды. 2017. Т. 20, № 2. С. 3—34.
2. *Baaz M., Metcalfe G.* Herbrand's theorem, skolemization and proof systems for first-order Łukasiewicz logic // J. Log. Comput. 2010. Vol. 20, № 1. P. 35—54.
3. *Cintula P., Hájek P., Noguera C. (eds.)* Handbook of mathematical fuzzy logic. London : College Publications, 2011. 928 p.
4. *Gerasimov A. S.* Proof search for non-prenex sentences of rational first-order Pavelka logic // International Conference "Mal'tsev Meeting 2016": Collection of Abstracts. Novosibirsk, 2016. P. 220.
5. *Hájek P.* Metamathematics of fuzzy logic. Dordrecht : Kluwer Academic Publishers, 1998. 299 p.
6. *Metcalfe G., Olivetti N., Gabbay D. M.* Proof theory for fuzzy logics. Dordrecht : Springer, 2009. 276 p.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ИСПОЛЬЗОВАНИЕ ИТЕРАТИВНЫХ ОПЕРАТОРОВ В КЛАССИЧЕСКИХ ЛОГИЧЕСКИХ ТЕОРИЯХ

С. М. Дудаков (Тверь)[1]

1. Введение

Языки математической логики находят широкое применение в качестве языков запросов к базам данных. Так, «классический» SQL является типичной стилизацией языка логики предикатов. Такая традиция восходит к Кодду [9], но возможности этих языков ограничены [6, 8], например, транзитивное замыкание графа невыразимо.

Эта ограниченность преодолевается несколькими путями. Один из них — использование не только отношений базы данных, но и отношений (операций) предметной области, что соответствует вложению конечной алгебраической системы в бесконечный универсум и использованию в формулах логики как отношений этой системы, так и универсума [4, 7].

Другой метод — выход за пределы логики первого порядка, например, использование итеративных операторов. Современные рекурсивные SQL-запросы в точности соответствуют операторам инфляционной фиксированной точки IFP [11].

Таким образом, современный SQL соответствует IFP-логике, когда база данных вложена в универсум. Это сочетание часто позволяет моделировать работу произвольного алгоритма, что приводит к неразрешимости, то есть невозможности в общем случае получить результат за конечное время. Например, общеизвестно, что простой функции следования и бинарных IFP-операторов достаточно, чтобы построить моделирующую формулу.

Здесь мы приводим обзор полученных нами за последнее время результатов о применении IFP-оператора для бесконечных универсумов. Также мы показываем связь конечности IFP-операторов с разрешимостью IFP-теории.

2. Определения

Мы используем обычные определения логики первого порядка FO (см., например, [13]). Строка $\phi(\bar{x})$ означает, что формула ϕ не содержит никаких свободных переменных, кроме, может быть, $\bar{x}$. Тогда $\phi(\bar{y})$ — результат замены $\bar{x}$ на $\bar{y}$. Если $\mathfrak{A}$ — алгебраическая система и $\bar{a} \in \mathfrak{A}$, то $\phi(\bar{a})$ — значение ϕ, когда значения $\bar{x}$ равны $\bar{a}$. Мы рассматриваем обогащение FO-логики оператором инфляционной фиксированной точки IFP.

Определение (см. [11])**.** Формула IFP-логики строится по правилам FO-логики и с помощью IFP-оператора: если $\phi(\bar{x}, \bar{y})$ — формула, содержащая несигнатурный предикатный символ Q, то $\mathrm{IFP}_{Q(\bar{y})}(\phi)$ — тоже формула исходной сигнатуры со свободными переменными $\bar{x}$ и $\bar{y}$. Здесь местность Q равна длине набора $\bar{y}$, это — местность IFP-оператора.

Пусть $\mathfrak{A}$ — это алгебраическая система, $\bar{a} \in \mathfrak{A}$ — значение переменных $\bar{x}$. *Инфляционной фиксированной точкой* $\mathrm{IFP}^{\bar{a}}_{Q(\bar{y})}(\phi)$ называется множество $Q^{\bar{a}}_*$ построенное так:

$$Q^{\bar{a}}_0 = \varnothing; \quad Q^{\bar{a}}_{i+1} = Q^{\bar{a}}_i \cup \{\bar{b} \in \mathfrak{A} : (\mathfrak{A}, Q^{\bar{a}}_i) \models \phi(\bar{a}, \bar{b})\}; \quad Q^{\bar{a}}_* = \bigcup_{i \in \omega} Q^{\bar{a}}_i.$$

Считаем формулу $\mathrm{IFP}_{Q(\bar{y})}(\phi)(\bar{a}, \bar{b})$ истинной, если $\bar{b} \in Q^{\bar{a}}_*$, и ложной, если $\bar{b} \notin Q^{\bar{a}}_*$.

Если $Q^{\bar{a}}_{i+1} = Q^{\bar{a}}_i$ для некоторого i, то будем говорить, что оператор $\mathrm{IFP}^{\bar{a}}_{Q(\bar{y})}(\phi)$ *сходится за i шагов*. Если $\mathrm{IFP}^{\bar{a}}_{Q(\bar{y})}(\phi)$ сходится за конечное число шагов для любого $\bar{a}$, то опе-

 Получено 24.12.2017. УДК 510.6.

[1]Тверской государственный университет. E-mail: sergeydudakov@yandex.ru.

ратор $\mathrm{IFP}_{Q(\bar{y})}(\phi)$ назовём *конечным*. Алгебраическая система $\mathfrak{A}$ является IFP-*безопасной*, если любой IFP-оператор в ней является конечным.

Таким образом, безопасность алгебраической системы $\mathfrak{A}$ означает, что значение любого IFP-оператора вычисляется за конечное количество шагов. С практической точки зрения это делает невозможным «зацикливание» при выполнении запросов.

3. Безопасность и другие свойства

Исходя из правил построения формул IFP-логики, легко видеть, что IFP-операторы могут быть вложенными. Первое, что мы отметим — вложенность IFP-операторов на безопасность не влияет.

Теорема 1 (см. [1]). *Система $\mathfrak{A}$ будет* IFP-*безопасной тогда и только тогда, когда конечен любой оператор вида $\mathrm{IFP}_{Q(\bar{y})}(\phi)$ для любой* FO-*формулы ϕ.*

Следующее свойство показывает, что для безопасности системы количество шагов сходимости не должно зависеть от значений свободных переменных.

Теорема 2 (см. [1]). *Чтобы алгебраическая система $\mathfrak{A}$ была* IFP-*безопасной, необходимо и достаточно, чтобы для любой* FO-*формулы $\phi(\bar{x}, \bar{y})$ оператор вида $\mathrm{IFP}^{\bar{a}}_{Q(\bar{y})}(\phi)$ сходился за ограниченное число шагов, не зависящее от $\bar{a}$.*

Следующий критерий несколько напоминает по формулировке теорему Рыль-Нардзевского (см. [13]) о счётной категоричности. Это даёт возможность связать свойства безопасности и счётной категоричности в некоторых случаях.

Теорема 3 (см. [10]). *Пусть система $\mathfrak{A}$ имеет конечную сигнатуру. Чтобы $\mathfrak{A}$ не была* IFP-*безопасной, необходимо и достаточно существование множества* FO-*формул X, удовлетворяющего следующим условиям:*

(1) *формулы из X не содержат сложных термов (аргументами предиката или функции могут быть только переменные),*
(2) *в X существует бесконечно много попарно неэквивалентных в $\mathfrak{A}$ формул,*
(3) *существует константа K и каждая формула из X содержит не более K переменных (свободных или связанных, без учета кратности).*

Значит, IFP-безопасность определяется исключительно свойствами первого порядка.

Следствие 1. *Элементарно эквивалентные системы являются или не являются* IFP-*безопасными одновременно.*

Следствие 2. IFP-*безопасность является свойством полных теорий.*

Если есть возможность ограничить количество связанных переменных в формулах, то можно получить ещё одно утверждение.

Теорема 4 (см. [10]). *Пусть для теории T существует константа k такая, что любая* FO-*формула ϕ с n свободными переменными эквивалентна в T некоторой* FO-*формуле с $n+k$ переменными (свободными или связанными). Тогда любое полное расширение $T' \supseteq T$ является* IFP-*безопасным тогда и только тогда, когда T' счётно категорично.*

Таким свойством обладают, например, теории линейных порядков (см. [12]).

Следствие 3. *Полная теория линейного порядка* IFP-*безопасна тогда и только тогда, когда она счётно категорична.*

Категоричность не является необходимым условием IFP-безопасности в общем случае.

Теорема 5 (см. [2]). *Существует полная теория T конечной сигнатуры,* IFP-*безопасная, но не счётно категоричная.*

Построенная в доказательстве теория не является конечно аксиоматизируемой. Для конечно аксиоматизируемых теорий удалось доказать такой результат.

Теорема 6 (см. [3]). *Пусть теория T полна, конечно аксиоматизируема, сильно минимальна и имеет бесконечную модель. Тогда теория T не является* IFP-*безопасной.*

4. Алгоритмические проблемы

IFP-безопасность тесно связана с разрешимостью соответствующих проблем.

Теорема 7 (см. [5]). *Если в системе* $\mathfrak{A}$ *на бесконечном множестве определима функция следования, то* IFP*-теория* $\mathfrak{A}$ *неразрешима даже для унарных* IFP*-операторов.*

Применяя этот результат, мы можем доказать следующую теорему.

Теорема 8. *Если полная теория* T *не является* IFP*-безопасной, то* IFP*-теория моделей* T *неразрешима.*

Доказательство (схема). Рассмотрим IFP-оператор $\psi = \mathrm{IFP}^{\bar{a}}_{Q(\bar{y})}(\phi)$ для формулы $\phi(\bar{x}, \bar{y})$, который не сходится за конечное число шагов. Строим формулу $\theta(\bar{x}, \bar{y}_1, \bar{y}_2)$, означающую, что $\bar{y}_1$ попал в ψ раньше $\bar{y}_2$:

$$\theta = \mathrm{IFP}_{P(\bar{y}_1,\bar{y}_2)}(P'(\bar{y}_1) \wedge \phi'(\bar{x}, \bar{y}_2) \wedge \neg P'(\bar{y}_2)).$$

Здесь $P'(\bar{y})$ — это формула $(\exists \bar{y}')(P(\bar{y}, \bar{y}') \vee P(\bar{y}', \bar{y}))$, а ϕ' — результат замены в ϕ всех подформул вида $Q(\bar{z})$ на соответствующие $P'(\bar{z})$.

Тогда $\theta(\bar{a}, \bar{y}_1, \bar{y}_2)$ определяет некоторый тотальный предпорядок $<$, который продуцирует дискретный линейный порядок на классах эквивалентности ($\bar{b}_1 \equiv \bar{b}_2$, если $\bar{b}_1 \leq \bar{b}_2 \leq \bar{b}_1$). Это, в свою очередь, даёт возможность определить функцию следования на классах эквивалентности, что, согласно предыдущей теореме, ведёт к неразрешимости IFP-теории.

5. Заключение

Было бы интересно получить ответы на следующие вопросы:

- Можно ли ослабить в теореме 6 условие сильной минимальности до стабильности или несчётной категоричности?
- Является ли счётная категоричность необходимым условием IFP-безопасности для конечно аксиоматизируемых теорий?
- Как связана между собой конечность IFP-операторов разной местности?

Литература

1. *Дудаков С. М.* О безопасности рекурсивных запросов // Вестник ТвГУ. Серия: Прикладная математика. 2012. № 4. С. 71—80.
2. *Дудаков С. М.* О безопасности IFP-операторов и рекурсивных запросов // Вестник ТвГУ. Серия: Прикладная математика. 2013. № 2. С. 5—13.
3. *Дудаков С. М.* Сильная минимальность и IFP-безопасность // Вестник ТвГУ. Серия: Прикладная математика. 2015. № 3. С. 25—32.
4. *Дудаков С. М., Тайцлин М. А.* Трансляционные результаты для языков запросов в теории баз данных // Успехи математических наук. 2006. Т. 61, № 2 (368). С. 2—65.
5. *Золотов А. С.* Элиминация итеративных операторов в некоторых теориях первого порядка : дис. ... канд. физ.-мат. наук : 01.01.06, защищена 25.05.17, утв. 24.10.17. Тверь, 2017. 150 с.
6. *Aho A. V., Ullman J. D.* Universality of data retrieval languages // Proc. of 6th Symp. on Principles of Programming Languages. 1979. P. 110—120.
7. *Benedikt M., Dong G., Libkin L., Wong L.* Relational expressive power of constraint query languages // Proc. 15th ACM Symp. on Principles of Database Systems. 1996. P. 5—16.
8. *Chandra A., Harel D.* Computable queries for relational databases // Journal of Computer and System Sciences. 1980. Vol. 21, № 2. P. 156—178.
9. *Codd E. F.* Relational completeness of data base sublanguages // Database Systems (ed. Rustin R.). Prentice-Hall, 1972. P. 33—64.
10. *Dudakov S. M.* On inflationary fix-point operators safety // Lobachevskii J. Math. 2015. Vol. 36, № 4. P. 328—331.
11. *Gurevich Y., Shelah S.* Fixed-point extensions of first-order logic // Annals of Pure and Applied Logic. 1986. № 32, P. 265—280.
12. *Immerman N., Kozen D.* Definability with bounded number of bound variables // Information and Computation. 1989. Vol. 83, № 2. P. 121—139.
13. *Marker D.* Model theory: an introduction. New York : Springer-Verlag, 2002. 346 p.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

РЕГИСТРОВЫЕ МАШИНЫ СО СЧЁТЧИКАМИ

И. В. Савицкий (Москва)[1]

1. Введение

В теории алгоритмов определено большое количество различных абстрактных вычислительных устройств. Один из используемых в них способов организации информации — хранение данных в счётчиках, каждый из которых может содержать натуральное число и за один такт может быть либо изменён (увеличен или уменьшен) на константу, либо (в некоторых случаях) сброшен в нуль. Таким образом память устроена и у регистровых машин со счётчиками (RC-машин). Отличительные особенности данного типа устройств заключаются в следующем.

Во-первых, RC-машины не могут свободно оперировать конечной внутренней памятью: в случае перехода в другое состояние машина уже не сможет вернуться в предыдущее.

Во-вторых, RC-машины не могут свободно менять свои счётчики. В процессе вычисления счётчики машины меняются независимо от программы, представляя собой цифры номера текущего такта в системе счисления с достаточно большим значением основания. Машина может лишь следить за изменением счётчиков и в нужные моменты сохранять значение одного из них в специальный рабочий регистр.

В-третьих, для вычисления на RC-машине требуется задать функцию ёмкости счётчиков, определяющую максимальное число, которое может содержать каждый счётчик на данном входе. Но результат вычисления RC-машины не должен зависеть от выбора функции ёмкости счётчиков, если только она достаточно велика.

2. Определения и результаты

Регистровая машина $\mathcal{M}$ со счётчиками состоит из входных регистров $x_1, \ldots, x_n$, счётчиков $t_1, \ldots, t_m$, регистров r и 0 и набора программ $P_1, \ldots, P_s$.

Вычисление на RC-машине $\mathcal{M}$ на входе $\tilde{x}^n$ со значением ёмкости счётчиков t производится следующим образом. Входные регистры содержат значения входа, а нулевой регистр — число 0. В начальный момент счётчики и регистр r содержат 0, и активна программа P_1. На каждом такте активная программа в зависимости от соотношений $=, <, >$ между всеми парами регистров и счётчиков детерминировано выбирает регистр или счётчик, значение которого заносится в r, или любую программу (кроме P_1), которая будет активирована на следующем такте (при этом в любом вычислении каждая программа может быть активирована не более одного раза). Затем счётчики меняются по принципу прибавления единицы к числу

$$t_1 + t_2 \cdot t + \ldots + t_{m-1} \cdot t^{m-2} + t_m \cdot t^{m-1}$$

в позиционной системе счисления с основанием t, после чего происходит переход к следующему такту. Вычисление заканчивается через t^m тактов. Результат вычисления $\mathcal{M}(\tilde{x}^n;\ t)$ содержится в r. Считаем, что $\mathcal{M}(\tilde{x}^n;\ 0) = 0$.

Пусть $T(\tilde{x}^n)$ — частичная функция натурального аргумента. Функция $f(\tilde{x}^n)$ вычислима на RC-машине $\mathcal{M}$ с ёмкостью счётчиков $T(\tilde{x}^n)$, если $f(\tilde{x}^n) = \mathcal{M}(\tilde{x}^n;\ T(\tilde{x}^n))$ (не определена в точках неопределённости $T(\tilde{x}^n)$). Частичная функция $f(\tilde{x}^n)$ строго вычислима на RC-машине $\mathcal{M}$ с ёмкостью счётчиков $T(\tilde{x}^n)$, если она вычислима на машине $\mathcal{M}$ с любой ём-

 Получено 24.12.2017. УДК 519.712.

[1]Московский государственный университет им. М. В. Ломоносова. E-mail: savvvig@gmail.com.

костью счётчиков $T'(\tilde{x}^n)$, имеющей ту же область определения, что и $T(\tilde{x}^n)$, и такой, что $T'(\tilde{x}^n) \geqslant T(\tilde{x}^n)$ на области определения.

В [2] с помощью RC-машин были промоделированы вычисления на машинах SRM (введены в [1]). Это позволяет доказать следующее утверждение.

Теорема 1. *Любая вычислимая функция строго вычислима на некоторой RC-машине с подходящей вычислимой функцией ёмкости счётчиков.*

В отличие от RC-машин, машины SRM могут управлять изменением счётчиков, но сравнивать счётчики они могут только на равенство и неравенство, не различая, какой из счётчиков больше, а какой меньше. Тем не менее, при моделировании машин SRM в [2] возможность RC-машин сравнивать счётчики на больше/меньше существенно использовалась. Интересно выяснить, насколько ограничиваются вычислительные возможности RC-машин, если запретить в них сравнения на больше/меньше.

Будем называть RC-машинами без неравенств RC-машины, программы которых проверяют значения регистров и счётчиков только на равенство или неравенство, не различая, какое из значений больше, а какое меньше.

Теорема 2. *Для любой RC-машины $\mathcal{M}_0$ с n входными регистрами и m счётчиками существует RC-машина без неравенств $\mathcal{M}$, такая что для любых значений входных регистров $\tilde{x}^n$ верно*

$$\mathcal{M}(\tilde{x}^n;\ i) = 0,\ i = \overline{0, m+n+2}$$
$$\mathcal{M}(\tilde{x}^n;\ k+m+n+2) = \mathcal{M}_0(\tilde{x}^n;\ k),\ k = \overline{1, \infty}.$$

Следствие 1. *Для любой RC-машины $\mathcal{M}_0$, строго вычисляющей функцию $f(\tilde{x}^n)$ с ёмкостью счётчиков $T(\tilde{x}^n)$, существует RC-машина без неравенств $\mathcal{M}$ и константа C, такие что $\mathcal{M}$ строго вычисляет функцию $f(\tilde{x}^n)$ с ёмкостью счётчиков $T(\tilde{x}^n) + C$.*

Следствие 2. *Любая вычислимая функция строго вычислима на некоторой RC-машине без неравенств с подходящей вычислимой функцией ёмкости счётчиков.*

Литература

1. *Бельтюков А. П.* Машинное описание и иерархия начальных классов Гжегорчика // Записки научных семинаров Ленинградского отделения Математического института им. В. А. Стеклова АН СССР. 1979. Т. 88. С. 30—46.
2. *Савицкий И. В.* Вычисления на регистровых машинах со счетчиками // Дискретная математика. 2017. Т. 29, № 1. С. 95—113.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ОБ ОТНОСИТЕЛЬНО ЭЛЕМЕНТАРНОЙ ОПРЕДЕЛИМОСТИ КЛАССА ГИПЕРГРАФОВ В КЛАССЕ ПОЛУГРУПП

Е. В. Хворостухина (Саратов)[1]

1. Введение

В настоящей раработе решается задача об относительно элементарной определимости класса гиперграфов в классе полугрупп. Согласно [3] гиперграфом является система вида $H = (X, L)$, где X — непустое множество и L — семейство произвольных подмножеств множества X. Элементы множества X называются вершинами и элементы множества L называются ребрами гиперграфа.

Гиперграф $H = (X, L)$ называется эффективным, если любая его вершина принадлежит некоторому его ребру. Для натурального числа p гиперграф H будем называть гиперграфом с p-определимыми ребрами, если в каждом ребре этого гиперграфа найдется по крайней мере $p + 1$ вершина и, с другой стороны, любые p вершин этого гиперграфа принадлежат не более, чем одному его ребру. Например, проективные плоскости и аффинные плоскости с числом точек более четырех являются эффективными гиперграфами с 2-определимыми ребрами. Эндоморфизмом гиперграфа $H = (X, L)$ называется такое преобразование φ множества X, что $(\forall l \in L)(\exists l' \in L)(\varphi(l) \subset l')$.

Исследуемый в данной работе класс эффективных гиперграфов с p-определимыми ребрами аксиоматизируется следующими формулами:

$$\Gamma_1 = (\forall A)(\exists a)(A \in a);$$

$$\Gamma_2 = (\forall a)(\exists A_1, A_2, ..., A_{p+1}) \left(\bigwedge_{i,j=1, i\neq j}^{p+1} A_i \neq A_j \wedge \bigwedge_{i=1}^{p+1} A_i \in a_i \right) \wedge$$

$$\wedge (\forall A_1, ..., A_p) \left(\bigwedge_{i,j=1, i\neq j}^{p} A_i \neq A_j \Longrightarrow (\forall a, b) \Big(\bigwedge_{i=1}^{p} (A_i \in a \wedge A_i \in b) \Longrightarrow a = b \Big) \right).$$

Так, истинность формулы Γ_1 на гиперграфе H означает, что всякая вершина такого гиперграфа содержится в некотором его ребре, т. е. гиперграфы, на которых истинна эта формула, являются эффективными. Истинность формулы Γ_2 на гиперграфе H означает, что всякое ребро этого гиперграфа содержит по меньшей мере $(p + 1)$ различную вершину и любые p различные вершины могут одновременно содержаться только в одном его ребре, т. е. гиперграфы, на которых истинна эта формула, являются гиперграфами с p-определимыми ребрами.

Пусть $\mathbf{Kn}$ — класс алгебраических систем сигнатуры Ω_0, $\mathbf{K_0}$ — класс алгебраических систем сигнатуры Ω_1. Будем говорить [1], что класс $\mathbf{Kn}$ относительно элементарно определим в классе $\mathbf{K_0}$, если существуют такие формулы $C(x)$, $I(\bar{x}; \bar{y})$ сигнатуры Ω_1 (здесь и далее $\bar{x} = (x_1, \ldots, x_p)$, $\bar{y} = (y_1, \ldots, y_p)$), что для любой алгебраической системы $A_0 \in \mathbf{Kn}$ найдется алгебраическая система $A_1 \in \mathbf{K_0}$, удовлетворяющая следующим условиям:

1) множество $\bar{C} = \{x \in A_1 : C(x)\}$ не пусто;

 Получено 25.12.2017. УДК 519.7.

[1]Саратовский государственный технический университет им. Ю. А. Гагарина.
E-mail: khvorostukhina85@gmail.com.

2) формула $I(\bar{x};\bar{y})$ задает отношение эквивалентности $\bar{I}$ на алгебраической системе $\overline{A_0}$ сигнатуры Ω_0, основное множество которой есть $\bar{C}$, а сигнатурные предикаты и операции определяются формулами сигнатуры Ω_1;
3) алгебраическая система $\overline{A_0}/\bar{I}$ изоморфна A_0.

2. Результат

С помощью результатов работы [2] было доказано, что класс всех эффективных гиперграфов с p-определимыми ребрами относительно элементарно определим в классе всех полугрупп. Рассмотрим следующие формулы языка элементарной теории полугрупп:

$$C(x) = (\forall y)(y \cdot x = x);$$

$$DC(x_1,...,x_p;y_1,...,y_p) = \left(\Big(\bigwedge_{i=1}^{p+1}(C(x_i)\wedge C(y_i))\Big)\wedge(\exists z)\Big(\bigwedge_{i=1}^{p+1} x_i\cdot z = y_i\Big)\right);$$

$$RC(x_1,...,x_p) = \left(\bigwedge_{i=1}^{p+1} C(x_i)\wedge(\forall y_1,...,y_{p+1})\Big(\bigwedge_{i=1}^{p+1} C(y_i)\wedge \bigwedge_{i,j=1,i\neq j}^{p+1} y_i\neq y_j \Longrightarrow \right.$$

$$\left.\Longrightarrow DC(y_1,...,y_p;x_1,...,x_p)\Big)\right);$$

$$L(\bar{x}) = \bigwedge_{i=1}^{p} C(x_i)\ \wedge \bigwedge_{i,j=1,i\neq j}^{p} x_i\neq x_j\ \wedge\ (\exists x)RC(x_1,\ldots,x_p,x);$$

$$\mathrm{Eqv}(\bar{x};\bar{y}) = L(\bar{x})\ \wedge\ L(\bar{y})\ \wedge \bigwedge_{i=1}^{p} RC(x_1,\ldots,x_p,y_i);$$

$$\mathrm{Ins}(x;\bar{x}) = C(x)\ \wedge\ L(\bar{x})\ \wedge\ RC(x_1,\ldots,x_p,x)$$

(здесь и далее $\bar{y}^i = (y^i_1,\ldots,y^i_p)$).

Теорема. *Любой эффективный гиперграф с p-определимыми ребрами $H = (X, L)$ и его полугруппа эндоморфизмов $S = \mathrm{End}H$ удовлетворяют следующим условиям:*

1) *множества $\overline{X} = \{x \in S : C(x)\}$ и $\overline{L} = \{\bar{x} \in S^p : L(\bar{x})\}$ не пусты;*
2) *формула $\mathrm{Eqv}(\bar{x};\bar{y})$ задает отношение эквивалентности $\overline{\mathrm{Eqv}}$ на $\overline{L}$;*
3) *формула $\mathrm{Ins}(x;\bar{y})$ задает такое бинарное отношение $\overline{\mathrm{Ins}}$ между элементами множеств $\overline{X}$ и $\overline{L}$, что $(x,\bar{x}) \in \overline{\mathrm{Ins}}\ \wedge\ \bar{x} \equiv \bar{y}(\overline{\mathrm{Eqv}}) \quad\Longrightarrow\quad (x,\bar{y}) \in \overline{\mathrm{Ins}}$;*
4) *гиперграф $H = (X, L, \in)$ изоморфен двухсортной алгебраической системе $\overline{H} = (\ \overline{X},\ \overline{L}/\overline{\mathrm{Eqv}},\ \overline{\mu}\ )$ с бинарным отношением $\overline{\mu} \subset \overline{X} \times \overline{L}/\overline{\mathrm{Eqv}}$, которое для $x \in \overline{X}$, $Y \in \overline{L}/\overline{\mathrm{Eqv}}$ определяется по формуле: $(x, Y) \in \overline{\mu} \quad\Longleftrightarrow\quad (x,\bar{x}) \in \overline{\mathrm{Ins}}$, при любых $\bar{x} \in Y$;*
5) *для любой формулы Ψ языка $\mathbf{L_H}$ эффективно строится такая формула $\tilde{\overline{\Psi}}$ языка $\mathbf{L_S}$, что Ψ в том и только том случае истинна на гиперграфе H, если формула $\overline{\tilde{\Psi}}$ истинна на полугруппе эндоморфизмов $\mathrm{End}H$, т. е. выполняется условие: $H \models \Psi \quad\Longleftrightarrow\quad \mathrm{End}H \models \overline{\tilde{\Psi}}$.*

Построенная в теореме относительно-элементарная интерпретация класса эффективных гиперграфов с p-определимыми ребрами в классе полугрупп дает возможность проанализировать взаимосвязь важных проблем алгоритмической разрешимости элементарных теорий классов таких гиперграфов и элементарных теорий полугрупп.

Литература

1. *Ершов Ю. Л.* Проблемы разрешимости и конструктивные модели. М. : Наука, 1980. 320 с.
2. *Хворостухина Е. В.* О конкретной характеризации универсальных гиперграфических автоматов // Фундаментальная и прикладная математика. 2008. Т. 14, № 7. С. 395—407.
3. *Bretto A.* Hypergraph theory. An Introduction. Cham. Springer. 2013. 133 p. DOI: 10.1007/978-3-319-00080-0.

Секция 5

ПРИКЛАДНАЯ АЛГЕБРА, ДИСКРЕТНАЯ МАТЕМАТИКА И КРИПТОГРАФИЯ

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

НОВОЕ ТЕНЗОРНОЕ ПРОИЗВЕДЕНИЕ МАТРИЦ И БЫСТРЫЕ АЛГОРИТМЫ

М. С. Беспалов (Владимир)[1]

1. Введение

В качестве синонима термина *тензорное произведение матриц* рассматривалось *кронекерово произведение матриц* $A \otimes B$, которое определяется в виде блочной матрицы с блоками $a_{kj}B$. Основным математическим объектом, исследуемым и применяемым в дискретном гармоническом анализе и в теории цифровой обработки информации, служат операторы дискретных преобразований в виде дискретного преобразования Фурье (ДПФ), дискретного преобразования Уолша (ДПУ) и дискретного преобразования Крестенсона (ДПК).

В качестве матрицы ДПФ порядка p возьмем матрицу декодирования

$$F_p = (\omega^{kj})_{k,j=0}^{p-1}. \quad \text{где } \omega = \omega_p = e^{\frac{2\pi i}{p}}.$$

Частный случай при $p = 2$ выделим и обозначим особо

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Матрица ДПУ в нумерации Адамара (известная как матрица Адамара–Сильвестра) есть ее кроненкерова степень

$$H_n = H^{n\otimes}.$$

Аналогично определяется матрица ДПК-Кронекера: $F_p^{n\otimes}$.

Революционный шаг в цифровой обработке информации связан с появлением быстрого алгоритма Кули–Тьюки [3] реализации ДПФ, который является небольшим видоизменением алгоритма Гуда [4] реализации ДПУ-Адамара. В статье [4] предложены два эквивалентных по числу операций быстрых алгоритма факторизации матрицы кронекеровой степени. Как основной из них в [4] подается следующий результат.

Теорема 1. *Для квадратной матрицы A (порядка m) существует слабозаполненная матрица Z такая, что*

$$A^{n\otimes} = Z^{n\cdot}.$$

В [4] указан вид элементов Z.

Обобщение свойства кронекеровой степени —

$$(A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D)$$

составляет следующий второй алгоритм Гуда.

Следствие. *Возможна следующая факторизация кронекеровой степени квадратной матрицы A:*

$$A^{n\otimes} = S_1 \cdot S_2 \cdot S_3 \cdot \ldots \cdot S_n, \tag{1}$$

где $S_k = E^{(k-1)\otimes} \otimes A \otimes E^{(n-k)\otimes}$, E — единичная матрица одного порядка с A, а сомножители S_k можно переставлять в любом порядке.

 Получено 13.11.2017. УДК 519.61.

[1]Владимирский государственный университет им. А. Г. и Н. Г. Столетовых. E-mail: bespalov@vlsu.ru.

Матричная форма алгоритма Кули–Тьюки порядка $N = 2^n$:

$$F_N = (S_1 T_1) \cdot (S_2 T_2) \cdot \ldots \cdot (S_{n-1} T_{n-1}) \cdot S_n \cdot L, \tag{2}$$

с теми же S_k, где в качестве A берем H, L — матрица реверсной перстановки, о которой ниже, T_k — диагональные матрицы: на диагонале T_{n-1} многократно повторяется набор $1, 1, 1, i$, на диагонале T_{n-2} повторяется набор $1, 1, 1, 1, 1, u, u^2, u^3$, где $u = \frac{1+i}{\sqrt{2}}$, и так далее.

2. Новое тензорное произведение матриц

В пособии [1] введено новое тензорное произведение матриц.

Определение. Назовем b-произведением матриц A и B следующую блочную матрицу

$$A \oslash B = \begin{pmatrix} A^0 \cdot B_0 & A^1 \cdot B_0 & \cdots & A^{m-1} \cdot B_0 \\ A^0 \cdot B_1 & A^1 \cdot B_1 & \cdots & A^{m-1} \cdot B_1 \\ \vdots & \vdots & \ddots & \vdots \\ A^0 \cdot B_{k-1} & A^1 \cdot B_{k-1} & \cdots & A^{m-1} \cdot B_{k-1} \end{pmatrix},$$

где той же буквой, что и матрица, с нижним индексом обозначается соответствующая строка, а с верхним индексом обозначается соответствующий столбец.

В теории ортогональных рядов основной нумерацией системы функций Уолша служит нумерация Пэли. Нумерация Адамара применима только к конечному набору функций Уолша и невозможна для всей системы в целом. Поэтому и для ДПУ основной нумерацией будем считать нумерацию Пэли. В [1] доказана

Теорема 2. *Матрица ДПУ-Пэли есть b-степень H:* $W_n = H^{n\oslash}$.

Известно, что строки (столбцы) матриц H_n и W_n связаны через реверсную перестановку с матрицей L: $W_n = LH_n = H_nL$.

Теорема 3. *Матрица реверсной перстановки есть b-степень единичной матрицы:* $L = E^{n\oslash}$.

Теорема 4. *Непосредственный быстрый алгоритм для ДПУ-Пэли:*

$$H^{n\oslash} = S_1 \cdot S_2 \cdot S_3 \cdot \ldots \cdot S_n, \tag{3}$$

где $S_k = E^{(k-1)\otimes} \otimes (H \oslash E^{(n-k)\otimes})$, E *— единичная матрица второго порядка.*

Теорема 5. *Возможные виды матрицы Z в теореме 1, где указан порядок единичных матриц:*

$$Z = A \oslash E_{m^{n-1}}, \qquad Z = (A \otimes E_{m^{n-1}}) \cdot (E_m \oslash E_{m^{n-1}}),$$
$$Z = E_{m^{n-1}} \oslash A, \qquad Z = (E_{m^{n-1}} \oslash E_m) \cdot (A \otimes E_{m^{n-1}}).$$

Перечисление и доказательства (в случае b-произведения) свойств кронекерова и b-произведения матриц приведены в статье [2].

Литература

1. *Беспалов М. С.* Математические методы в информатике и вычислительной технике. В 2-х ч. Ч. 2. Введение в прикладной гармонический анализ. Владимир : ВлГУ, 2007. 244 с.
2. *Беспалов М. С.* О свойствах тензорного произведения матриц // Журнал вычислительной математики и математической физики. 2014. Т. 54, № 4. С. 547—561.
3. *Cooley J. W., Tukey J. W.* An algorithm for the machine calculation of complex Fourier series // Math. Comput. 1965. Vol. 19, № 90. P. 297—301.
4. *Good I. J.* The interaction algorithm and practical Fourier analysis // J. Royal Stat. Soc., Ser. B. 1958. Vol. 20. P. 361—372.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ПОСТРОЕНИЕ ЦВЕТНЫХ МНОЖЕСТВ ОГРАНИЧЕННОГО ОСТАТКА НА ОСНОВЕ ВЫТЯГИВАНИЯ ЕДИНИЧНОГО КВАДРАТА[1]

Д. А. Блинов (Владимир)[2], А. А. Осипова (Владимир)[3]

Авторы рассматривают пример построения двумерного случая множества, для которого остаточный член асимптотической функции $r_k(i) = iS_k + \delta_k(i)$ ограничен константой, не зависящей от количества точек, а также находят точные границы отклонений. Такие множества, известные как BR-множества (множества ограниченного остатка), были впервые введены немецким математиком Э. Гекке в 1921 году [5]. В работе [5] основной упор был сделан на аналитические функции и распределение чисел по модулю 1, и в качестве примера BR-множества в одномерном случае был приведен интервал $X \subset [0,1)$ длины $0 < |b + a\alpha| < 1$, где $\alpha \neq 0$ и $a,b \in \mathbb{Z}$.

Изучение одномерных множеств ограниченного остатка получило научный интерес и развитие спустя, без малого, 50 лет, ввиду того, что все больше математиков приходило к выводу о важности создания и изучения систем, как неких целостных, организованных объектов, в которых связи между элементами более значимы, чем их связи с элементами других систем.

Так, полное описание одномерных BR-множеств было приведено Х. Кестеном в 1966 году в работе [6]. Первый пример двумерного случая BR-множества был получен в 1954 году. Р. Сюзом [7]. Это было семейство параметрических параллелограммов, для которых выполняется оценка $\delta(i) = O(1)$.

Другой подход к построению двумерных множеств ограниченного остатка в 1984 и 1992 годах соответственно обнаружили Ж. Рози [8] и С. Ференси [4]. Они связали свойство быть BR-множеством со свойствами проекции некоторой площадки в сечении Пуанкаре на себя или на другую площадку вдоль траекторий системы.

В 2012 г. А. А. Абросимовой в работе [1] были построены двумерные трехпараметрические множества ограниченного остатка на основе развертки тора, для них были найдены точные оценки остаточных членов. Позднее А. А. Абросимова (Осипова) получила и другие результаты в этой области и распространила метод параметрических многогранников на случай других размерностей. В совместной работе авторов 2013 г. найдена оптимизация границ отклонений для построенных ранее двумерных множеств [2].

Систематический подход к построению выпуклых многомерных множеств ограниченного остатка был предложен В. Г. Журавлевым в [3], причем, методы, используемые в работе [3] позволяют исследовать и невыпуклый случай.

Рассмотрим методику построения двумерных множеств ограниченного остатка на основе вытягивания единичного квадрата. Построим гексагональную развертку тора $\mathbb{T}$, преобразовав ортонормированный базис

$$\begin{cases} e_1 = (1,0) \\ e_2 = (0,1) \end{cases} \text{ в } \begin{cases} l_1 = e_1 + b = (1 + b_1, b_2) \\ l_2 = e_2 + b = (b_1, 1 + b_2) \end{cases},$$

и зададим выпуклый шестиугольник T с попарно равными и параллельными противопо-

 Получено 21.12.2017. УДК 511.3.

[1]Работа выполнена при финансовой поддержке РФФИ, проект № 16-31-00055-мол-а.

[2]ООО «Спел ЛАБС». E-mail: demetrois@yandex.ru.

[3]Владимирский филиал Российского университета кооперации. E-mail: albina.a.osipova@yandex.ru.

ложными сторонами, с вершинами: $(0,0), (0,1), (b_1,1+b_2), (1+b_1,1+b_2), (1+b_1,b_2), (1,0)$ (рис. 1). Таким образом проведено вытягивание единичного квадрата.

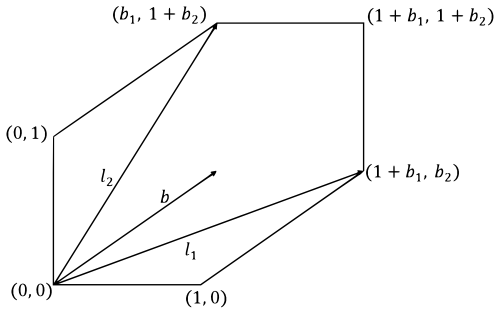

Рис. 1. Вытягивание единичного квадрата

Пусть решётка $\mathbb{Z}$, действует на T как параллельный перенос, тогда шестиугольником T можно замостить плоскость R, а значит T будет являться подмножеством пространства $\mathbb{Z}$, которое в свою очередь будет содержать в точности по одной точке из каждого образа отдельных точек T, другими словами, шестиугольник будет являться фундаментальной областью для квадратной решетки $\mathbb{Z}$ и его можно рассматривать как развертку тора $\mathbb{T}$.

Для нахождения разбиения развертки на множества ограниченного остатка введем параметр $t : 0 < t \leq 1$, отложим вектор $\beta = bt$ от вершин шестиугольника с координатами $(b_1,1+b_2), (1+b_1,1+b_2), (1+b_1,b_2)$ и соединим концы отложенных векторов (рис. 2)

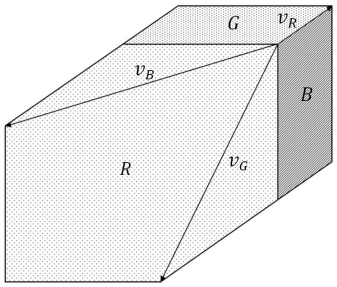

Рис. 2. Векторы перекладывания

В результате получим разбиение области T на три фигуры с заданным для визуальной наглядности своим цветом: T_R — красный, T_G — зеленый, T_B — синий. Площади полученных фигур будут соответственно равны: $S_R = 1 + b_1 + b_2 - b_1 t - b_2 t$, $S_G = b_2 t$, $S_B = b_1 t$.

Очевидно, фигура T будет являться перекладывающейся разверткой тора, с векторами перекладывания $\upsilon_R = \beta$, $\upsilon_G = \beta - b_2$, $\upsilon_B = \beta - b_1$ (рис. 2). Для каждой области T_k, где $k = R, G, B$ можем задать считающие функции $r_k(i) = iS_k + \delta_k(i)$, определяющие количество точек в каждой из областей.

Для дальнейших расчетов введем также вектор-функцию, определяющую положение любой точки на торе — суммарное векторное отклонение $\delta(i) = r_R(i)\upsilon_R + r_G(i)\upsilon_G + r_B(i)\upsilon_B$

Решетка $\mathbb{Z}$ — полная. Для ее базиса (l_1, l_2) зададим двойственный базис (l_1^*, l_2^*) относительно скалярного произведения в качестве неособой билинейной формы на $\mathbb{Z}$, и получим соотношение

$$\begin{cases} l_1 l_1^* = 1 \\ l_1 l_2^* = 0 \\ l_2 l_1^* = 0 \\ l_1 l_2^* = 1 \end{cases}$$

Из этого соотношения находим координаты векторов двойственного базиса

$$l_{1x}^* = \frac{1+b_2}{1+b_1+b_2}, \quad l_{1y}^* = -\frac{b_1}{1+b_1+b_2},$$

$$l^*_{2x} = \frac{b_2}{1+b_1+b_2}, \quad l^*_{2y} = -\frac{1+b_1}{1+b_1+b_2},$$
$$l^*_{0x} = -\frac{2b_2+1}{1+b_1+b_2}, \quad l^*_{0y} = \frac{2b_1+1}{1+b_1+b_2}.$$

Используя полученные координаты, получаем равенства:

$$\delta(i)l^*_1 = -\delta_B(i), \quad \delta(i)l^*_2 = -\delta_G(i), \quad \delta(i)l^*_0 = -\delta_R(i).$$

Отсюда следует, что границы отклонений могут быть определены, как проекции суммарного векторного отклонения $\delta(i)$ на векторы базиса l^*. Для определения границ отклонений, в виду того, что T является компактным множеством, достаточно проверить проекции координат его вершин на направления векторов l^*. Получим следующее множество значений (таблица 1):

координаты x_n		$-x_n l^*_1$	$-x_n l^*_2$	$-x_n l^*_0$
1	$(0,0)$	0	0	0
2	$(0,1)$	$\frac{1+b_1}{1+b_1+b_2}$	$\frac{1+b_1}{1+b_1+b_2}$	$-\frac{2b_1+1}{1+b_1+b_2}$
3	$(b_1, 1+b_2)$	0	1	-1
4	$(1+b_1, 1+b_2)$	$-\frac{1+b_2}{1+b_1+b_2}$	$\frac{1+b_1}{1+b_1+b_2}$	$-\frac{b_1-b_2}{1+b_1+b_2}$
5	$(1+b_1, b_2)$	-1	0	1
6	$(1,0)$	$-\frac{1+b_2}{1+b_1+b_2}$	$-\frac{b_2}{1+b_1+b_2}$	$\frac{2b_2+1}{1+b_1+b_2}$

Таблица 1. Проекции суммарного векторного отклонения $\delta(i)$ на векторы базиса l^*

Выбрав наибольшее и наименьшее значение из соответствующего столбца таблицы 1, приняв во внимание, что $b_1, b_2 > 0$, получим следующие границы отклонений:

$$-1 \le \delta_1(i) \le \frac{b_1}{1+b_1+b_2}, \quad -\frac{b_2}{1+b_1+b_2} \le \delta_2(i) \le 1,$$
$$-1 \le \delta_0(i) \le \frac{2b_2+1}{1+b_1+b_2}, \text{ для } b_1 \le b_2,$$
$$-\frac{2b_1+1}{1+b_1+b_2} \le \delta_0(i) \le \frac{2b_2+1}{1+b_1+b_2}, \text{ для } b_1 > b_2.$$

Рассмотренный в работе подход, разработанный на основе метода вытягивания многомерного куба (метод Журавлева), позволяет доказать обобщение теоремы Гекке на двумерный случай и получить точные оценки остаточных членов для двумерных множеств ограниченного остатка.

Литература

1. *Абросимова А. А.* Средние значения отклонений для распределения точек на торе // Научные ведомости Белгородского государственного университета. Сер.: Математика. Физика. 2012. № 5 (124). Вып. 26. С. 5—11.
2. *Абросимова А. А., Блинов Д. А.* Границы отклонений для BR-множеств // Дифференциальные уравнения и их приложения: сборник материалов Международной конференции, Белгород, 26—31 мая 2013 г. Белгород : ИПК НИУ «БелГУ», 2013. С. 8—9.
3. *Журавлев В. Г.* Многогранники ограниченного остатка // Современные проблемы математики. 2012. Вып. 16. С. 82—102.
4. *Ferenczi S.* Bounded remainder sets // Acta Arithmetica. 1992. Vol. 61. P. 319—326.
5. *Hecke E.* Eber Analytische Funktionen und die Verteilung van Zahlen mod Eins // Math. Sem. Hamburg Univ. 1921. Vol. 5. P. 54—76.
6. *Kesten H.* On a conjecture of Erdos and Szusz related to uniform distribution mod 1 // Acta. Arithmetica. 1966. Vol. 12. P. 193—212.
7. *Szusz R.* Uber die Verteilung der Vielfachen einer komplexen Zahl nach dem Modul des Einheitsquadrats // Acta Math. Acad. Sci. Hungar. 1954. № 5. P. 35—39
8. *Rauzy G.* Nombres algébriques et substitutions // Bull. Soc. Math. France. 1982. № 110. P. 147—178.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

АЛГОРИТМ ДИНАМИЧЕСКОЙ СЕГМЕНТАЦИИ ПАРЫ ПОСЛЕДОВАТЕЛЬНЫХ КАДРОВ

С. Е. Ваганов (Иваново)[1]

Пусть f и g — последовательные кадры видео, представляющие собой пару матриц размера $m \times n$, элементы которых определяют яркости (или цвета) точек изображения.

В случае статической сегментации, сегментом принято называть связный набор точек изображения, схожих по некоторому признаку (например: цвет или яркость). В динамической сегментации, в качестве сегментов мы принимаем множества точек, имеющие схожее межкадровое движение.

Межкадровое движение может быть описано преобразованием $T(x, y)$, представляющим собой отображение непустого множества точек с кадра f на кадр g. Примеры:

$$T(x, y) = (x + a_0,\ y + a_1) \tag{1}$$

$$T(x, y) = (a_0 \cdot x + a_1 \cdot y + a_2,\ a_3 \cdot x + a_4 \cdot y + a_5), \tag{2}$$

где x, y — координаты точки на изображении, а $a_i \in R$ — весовые коэффициенты. Формула (1) определяет преобразование сдвига точки на вещественный вектор, а (2) — аффинное преобразование.

Пусть S — сегмент (множество целочисленных координат точек некоторой области первого кадра), тогда качеством S будем называть величину среднеквадратичного отклонения:

$$Q_s(S, T) = \sqrt{\frac{1}{|S|} \cdot \sum_{u_i \in S} (f(u_i) - g(T(u_i)))^2}, \tag{3}$$

где $|S|$ — количество точек сегмента, а T — отображение, определяющее геометрическое преобразование S с кадра f на кадр g.

Коэффициенты преобразований вида (1) и (2) вычисляются для сегмента S, посредством минимизации (3).

Пусть N — общее число сегментов, тогда качеством сегментации Q будем называть следующую величину:

$$Q = \sqrt{\frac{1}{m \cdot n} \cdot \sum_{i=0}^{N-1} |S_i| \cdot Q_s(S_i, T_i)^2} \tag{4}$$

Основным результатом работы является реализация разработанного алгоритма динамической сегментации пары кадров, а также проведение сравнительного анализа качества сегментации для случаев поиска сдвигов и аффинных межкадровых преобразований для сегментов.

Разработанный алгоритм включает в себя следующие шаги:

1. Разбиение кадра f на прямоугольные сегменты S_i.
2. Нахождение межкадровых геометрических преобразований [1] с кадра f на кадр g для всех S_i.
3. Склейка соседних сегментов с учетом стоимости объединения и близости геометрических преобразований.
4. Уточнение границ сегментов. Выполняет следующие функции:
   а) производит перенос граничной точки S_i к S_j, в случае уменьшения шума;

 Получено 15.01.2018. УДК 519.67.

[1]Ивановский государственный университет. E-mail: pro100-pioner@mail.ru.

б) распределяет сегменты с размером $< MinSize$ между соседями;
в) модифицирует форму сегментов.

5. Вычисление качества сегментации.
6. Если склейка сегментов не осуществлялась и модуль разности величин текущего качества от предыдущего $< \varepsilon$, то завершаем работу алгоритма, иначе перейти к шагу 2 (в дальнейшем $\varepsilon = 0.005$).

Все проверочные изображения [2] имели размер 320×240 точек. Исходные пары кадров были размыты фильтром Гаусса с размером ядра 3×3. Минимальный размер сегмента $MinSize = 50$.

Ниже приведены таблицы, в которых представлены оценки качества работы алгоритма для случаев поиска сдвигов (1) и аффинных преобразований (2).

Таблица 1. Поиск сдвигов

Кадр	**Q**	**NS**	**I**
00.bmp	2.477	3	2
0000.bmp	2.722	2	5
0000000.bmp	4.327	14	12
0109.bmp	5.222	18	14
0300.bmp	8.695	18	12
0402.bmp	11.247	13	6
0500.bmp	5.803	69	16
0503.bmp	4.087	3	3
0600.bmp	4.533	7	12
0604.bmp	6.970	6	10
0616.bmp	5.567	5	5
0617.bmp	3.658	13	8
0618.bmp	6.826	12	3
0619.bmp	4.331	41	13
0620.bmp	4.366	8	6
0621.bmp	5.102	11	18
mult0.bmp	4.392	7	10
00037.bmp	7.428	76	20
Среднее	**5.431**	**18.111**	**9.722**

Таблица 2. Поиск аффинных преобразований

Кадр	**Q**	**NS**	**I**
00.bmp	1.624	2	2
0000.bmp	1.552	2	2
0000000.bmp	2.115	50	8
0109.bmp	2.561	5	3
0300.bmp	3.711	18	10
0402.bmp	3.545	19	11
0500.bmp	3.623	84	36
0503.bmp	1.883	13	6
0600.bmp	3.062	8	8
0604.bmp	3.750	30	23
0616.bmp	4.785	14	45
0617.bmp	2.306	24	14
0618.bmp	3.490	40	17
0619.bmp	2.239	72	13
0620.bmp	2.725	38	6
0621.bmp	3.202	50	15
mult0.bmp	2.431	36	15
00037.bmp	5.562	154	34
Среднее	**3.009**	**36.611**	**14.889**

Здесь, Q — качество сегментации, NS — количество сегментов, а I — число итераций алгоритма (повторений пунктов 2–6).

Метод, использующий поиск (2) в качестве функции межкадрового геометрического преобразования, показал лучшее качество по сравнению с алгоритмом, использующим поиск сдвигов (1).

Разработанный алгоритм может быть использован для решения многих задач, в том числе: поиск и отслеживание объектов в видеопотоке, отделение подвижных объектов от фона, нахождение границ объектов и кодирование видео.

Литература

1. *Ваганов С. Е., Хашин С. И.* Сравнение эффективности различных версий метода Лукаса–Канаде// Вестник Ивановского государственного университета. Сер.: Естественные, общественные науки. 2017. Вып. 2. С. 63—70.
2. Набор тестовых кадров для оценки работы алгоритма динамической сегментации. Электронный ресурс. URL: http://math.ivanovo.ac.ru/dalgebra/Khashin/bmp_ex2/index.html (дата обращения: 19.01.2018).
3. *Хашин С. И.* Динамическая сегментация последовательности кадров // Машинное обучение и анализ данных. 2013. Т. 1, № 6. С. 787—795.
4. *Baker S., Gross R., Matthews I.* Matthews Lucas-Kanade 20 Years On: A Unifying Framework // Int. J. of Computer Vision. 2002. Vol. 56. P. 111—122.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ПОСТРОЕНИЕ И АНАЛИЗ АНАЛОГА RSA-КРИПТОСИСТЕМЫ В ЧИСЛОВЫХ ПОЛЯХ

М. М. Васьковский (Минск, Беларусь)[1], Н. В. Кондратёнок (Минск, Беларусь)[2]

Введение

В августе 1977 года Ривестом, Шамиром и Адлеманом впервые была предложена криптосистема RSA. Полное описание новой криптосистемы было опубликовано в журнале "Communications of the ACM" в феврале 1978 года [9]. Алгоритм был основан на различии в том, насколько легко находить большие простые числа и насколько сложно раскладывать на множители произведение двух больших простых чисел.

Впоследствии было сделано немало обобщений этой криптосистемы. Известны ее модификации для многочленов и Гауссовых чисел. В работе [10] был предложен аналог RSA-криптосистемы в квадратичных кольцах. Целью данной работы является обобщение ранее полученных результатов для RSA-криптосистемы на произвольное конечное расширение поля $\mathbb{Q}$.

Определение 1. Пусть K — произвольное конечное расширение $\mathbb{Q}$. Рассмотрим $\mathcal{O}_K$ — поле целых алгебраических чисел K. В работе рассматриваются K, для которых $\mathcal{O}_K$ является факториальным кольцом. Обозначим через $\mathrm{Nm}(\cdot)$ норму элемента в K.

Определение 2. Будем говорить, что $a|b$, если $a/b = ab^{-1} \in \mathcal{O}_K$. Введем отношение эквивалентности, как сравнение по модулю элемента $N \in \mathcal{O}_K$: будем говорить, что $a \equiv b \pmod N$, если $N \mid a - b$. Наибольший общий делитель введем, используя факториальность кольца аналогично кольцу целых чисел. Будем писать, что $(z_1, z_2) = 1$, если НОД равен обратимому элементу.

Определение 3. Пусть $O_{K,N}$ — множество классов вычетов по модулю N, то есть множество различных классов элементов попарно сравнимых друг с другом, можно показать, что данное множество образует кольцо. Обозначим через $O^{\times}_{K,N}$ — мультипликативную группу этого кольца. Известно, что в ней содержатся только те классы, элементы которых взаимнопросты с N. Обозначим $\alpha_K(N) = |O_{K,N}|$ и $\varphi_K(N) = |O^{\times}_{K,N}|$.

Определение 4. Будем говорить, $p \in \mathcal{O}_K$ является простым, если для любого его делителя $q \in \mathcal{O}_K$ либо q, либо p/q являются обратимыми. Составными элементами будем называть элементы, для которых это не выполнено.

Обозначим через $|\alpha|_\infty = \max\limits_{i \in \overline{1,n}} c_i$ абсолютное значение элемента $\alpha \in \mathcal{O}_K$, где c_i — коэффициенты разложения α в целый базис.

Предложение 1. *Для любого $N \in \mathcal{O}_K \setminus \mathcal{O}^{\times}_K$ выполнено*

$$\varphi_K(N) = \prod_{i=1}^{k} (\mathrm{Nm}(p_i))^{q_i - 1}(\mathrm{Nm}(p_i) - 1),$$

где $N = \prod_{i=1}^{k} p_i^{q_i}$, p_i — различные простые элементы $\mathcal{O}_K$, $q_i \in \mathbb{N}$.

 Получено 25.12.2017. УДК 003.26

[1]Белорусский государственный университет. E-mail: vaskovskii_m@mail.ru.
[2]Белорусский государственный университет. E-mail: nkondr2006@rambler.ru.

Предложение 2. *Пусть* $N \in \mathcal{O}_K \setminus \mathcal{O}_K^\times$, *тогда для любого* $m \in \mathcal{O}_K$, $(m, N) = 1$, *выполнено* $m^{\varphi_K(N)} \equiv 1 \pmod{N}$.

1. Арифметические операции в числовых полях

Выберем и зафиксируем целый базис $\{e_1, \ldots, e_n\}$. Будем полагать, что элемент задается своим разложением по целому базису $\{e_1, \ldots, e_n\}$. Пусть $a = \sum_{i=1}^n a_i e_i$, $b = \sum_{i=1}^n b_i e_i$ и $|a|_\infty \leq N$, $|b|_\infty \leq N$.

Предложение 3. *Сумма имеет вид* $a+b = \sum_{i=1}^n (a_i+b_i)e_i$ *и вычисляется за* $O(\log N)$ *двоичных операций.*

Предложение 4. *Наибольший общий делитель* (a, b) *может быть вычислен за полиномиальное относительно битовой длины* N *время с помощью алгоритма приведенного в* [12].

Предложение 5. *Норма* $\mathrm{Nm}(a)$ *может быть вычислена за* $O(\log^2 N)$ *бинарных операций.*

Определение 5. Сопряженным к a элементом назовем такой элемент a', что

$$a' = \frac{\mathrm{Nm}(a)}{a} \in \mathcal{O}_K.$$

Предложение 6. *Сопряженный элемент* a' *можно вычислить за* $O(\log^2 N)$ *бинарных операций.*

Предложение 7. *Существует универсальная постоянная* M, *зависящая лишь от поля* K *и его инвариантов (например, дискриминант, степень расширения) такая, что для любых элементов* $a, b \in \mathcal{O}_K$, $b \neq 0$, $|a|_\infty \leq N$, $|b|_\infty \leq N$ *можно найти такой элемент* $z \in \mathcal{O}_K$, *что* $a \equiv z \pmod{b}$, $|z|_\infty \leq M = |b|_\infty$, *затратив* $O(\log^2 N)$ *двоичных операций.*

2. Аналог RSA-криптосистемы в числовых полях

Следующий алгоритм был предложен в работе [10].

Алгоритм аналога RSA-криптосистемы. Абонент A выбирает два больших простых элемента $p_A, q_A \in \mathcal{O}_K$, $(p_A, q_A) = 1$, и вычисляет $\varphi_K(N_A)$, где $N_A = p_A q_A$. Далее A выбирает случайное целое положительное число $e_A \in [1, \varphi_K(N_A)]$ такое, что $(e_A, \varphi_K(N_A)) = 1$, и находит целое положительное d_A такое, что $e_A d_A \equiv 1 \pmod{\varphi_K(N_A)}$, используя расширенный алгоритм Евклида. Пара (N_A, e_A) это публичный ключ A, пара (N_A, d_A) секретный ключ A. Тогда $f_A : \mathcal{O}_{K,N_A} \to \mathcal{O}_{K,N_A}$, $f_A(x) \equiv x^{e_A} \pmod{N_A}$, это функция шифрования A, а функция $f_A^{-1} : \mathcal{O}_{K,N_A} \to \mathcal{O}_{K,N_A}$, $f_A^{-1}(x) \equiv x^{d_A} \pmod{N_A}$ нужна для дешифровки. Любая такая тройка (N_A, e_A, d_A) называется параметрами RSA-криптосистемы. Предложение 2 гарантирует корректность работы RSA-криптосистемы в $\mathcal{O}_K$.

Теорема 1. *Пусть* $\mathcal{O}_K$ — *кольцо с единственной факторизацией,* (N, e, d) *параметры RSA-криптосистемы в* $\mathcal{O}_K$. *Если* d *известно, то* N *можно эффективно разложить на множители с вероятностью не менее* $\frac{1}{2}$ *за полиномиальное относительно* $\log |N|_\theta$ *количество арифметических операций в* $\mathcal{O}_K$.

Теорема 2. *Пусть* (N, e, d), $N = pq$, *параметры RSA-криптосистемы в кольце* $\mathcal{O}_K$. *Причем выполнено* $\mathrm{Nm}(q) < \mathrm{Nm}(p) < \alpha^2 \mathrm{Nm}(q)$, *где* $\alpha > 1$. *Если* $d < \frac{1}{\sqrt{2\alpha+2}} (\mathrm{Nm}(N))^{1/4}$, *то* d *можно эффективно вычислить за полиномиальное относительно* $\log \mathrm{Nm}(N)$ *число бинарных операций.*

Теорема 3. *Пусть* $\mathcal{O}_K$ *кольцо с единственной факторизацией,* (N, e, d, p, q) *параметры RSA-криптосистемы в* $\mathcal{O}_K$, *где* $\mathrm{Nm}(p)$ *и* $\mathrm{Nm}(q)$ *имеют одинаковую битовую длину. Пусть* $ed \leq (\mathrm{Nm}(N))^2$, $\mathrm{Nm}(N) \geq 107$. *Если* d *известно, то существует полиномиальный алгоритм (относительно* $\log |N|_\theta$), *который позволяет найти* $\mathrm{Nm}(p)$ *и* $\mathrm{Nm}(q)$.

Теорема 4. *Пусть $N = pq$ — модуль RSA-криптосистемы в конечном расширении $\mathcal{O}_K$. Предположим, что существуют различные простые числа r, s и положительные целые числа k, l такие, что $\varphi_K(p) = rk$, $\varphi_K(q) = sl$, и числа $r-1$, $s-1$ имеют различные простые делители r_1, s_1 соответственно. Пусть y и e — независимые равномерно распределенные случайные величины со значениями в $\mathcal{O}_{K,N}^{\times}$ и $\mathbb{Z}_{\varphi_K(N)}^{*}$ соответственно. Тогда выполняется неравенство $\mathbb{P}(m_{e,y} \geq r_1 s_1) \geq (1 - r^{-1})(1 - s^{-1})(1 - r_1^{-1})(1 - s_1^{-1})$, где $m_{e,y}$ это наименьшее натуральное число такое, что $y^{e^{m_{e,y}}} \equiv y (mod\ N)$.*

Замечание 1. Для обеспечения безопасности RSA-криптосистемы в конечном расширении $\mathcal{O}_K$ против атаки повторного шифрования необходимо брать такие простые элементы p, $q \in \mathcal{O}_K$, что существуют большие различные простые делители r, s чисел $\varphi_K(p)$, $\varphi_K(q)$ и большие различные простые делители r_1, s_1 чисел $r-1$, $s-1$.

Замечание 2. Сравним основные характеристики RSA-криптосистемы в $\mathcal{O}_K$ и $\mathbb{Z}$. Пусть (N_1, e_1, d_1), $N_1 = p_1 q_1$ — параметры криптосистемы в $\mathcal{O}_K$, а $N_2, e_2, d_2)$, $N_2 = p_2 q_2$ — параметры криптосистемы в $\mathbb{Z}$, причем $\mathrm{Nm}(p_1) \leq n$, $\mathrm{Nm}(q_i) \leq n$, $i = \overline{1,2}$, $n \in \mathbb{N}$.

- Генерация ключей. Для генерации ключей необходимо найти два больших простых элемента в $\mathcal{O}_K$. Известно, что в квадратичных кольцах это можно сделать эффективно [10].
- Скорость работы. Сложность шифровки и расшифровки сообщений можно оценить $O(\log^2 n \log n)$. Следует использовать быстрое умножение и бинарное возведение в степень. Такая сложность получается в обоих криптосистемах.
- Сложность взлома. Понятно, что разложить на множители в $\mathcal{O}_K$ не легче, чем в $\mathbb{Z}$.

Литература

1. *Coppersmith D.* Small solutions to polynomial equations, and low exponent RSA vulnerabilities // J. Cryptology. 1997. Vol. 10. P. 233—260.
2. *Coron J. S., May A.* Deterministic polynomial-time equivalence of computing the rsa secret key and factoring // J. Cryptology. 2007. Vol. 20. P. 39—50.
3. *Elkamchouchi H., Elshenawy K., Shaban K.* Extended RSA Cryptosystem and Digital Signature Schemes in the Domain of Gaussian Integers // Proceedings of the 8th International conference on communication systems. 2002. P. 91—95.
4. *El-Kassar A. N., Haraty R. A., Awad Y. A.* Modified RSA in the Domains of Gaussian Integers and Polynomials over Finite Fields // Proceedings of the ISCA 18th International conference on computer applications in industry and engineering. 2005. P. 298—303.
5. *Gekke E.* Lectures on the Theory of Algebraic Numbers. GITTL, 1940.
6. *Glukhov M. M., Kruglov I. A., Pichkur A. B., Cheremushkin A. V.* Introduction to Number Theoretical Methods in Cryptography. Saint-Petersburg : Lan', 2011.
7. *Koblitz N.* Course in Number Theory and Cryptography. New York : Springer-Verlag, 1994.
8. *Li B.* Generalizations of RSA Public Key Cryptosystem // IACR, Cryptology ePrint Arc. 2005.
9. *Rivest R. L., Shamir A., Adleman L.* A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. 1978. Vol. 21. P. 120—126.
10. *Vaskouski M., Kondratyonok N., Prochorov N.* Primes in quadratic unique factorization domains // Journal of number theory. 2016. Vol. 168. P. 101—116.
11. *Wiener M. J.* Cryptanalysis of short RSA secret exponents // IEEE Trans. Inform. Theory. 1990. Vol. 36. P. 553—558.
12. *Wikstrom D.* On the l-Ary GCD-Algorithm in Rings of Integers // Automata, Languages and Programming: 32nd International Colloquium, ICALP 2005, Lisbon, Portugal, July 11–15, 2005. Proceedings. Berlin, Heidelberg : Springer, 2005. P. 1189—1201.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

СЛОЖНОСТЬ ПРОВЕРКИ ПОЛИНОМИАЛЬНОЙ ПОЛНОТЫ КВАЗИГРУПП

А. В. Галатенко (Москва)[1], А. Е. Панкратьев (Москва)[2]

1. Введение

В связи с появлением около 40 лет назад понятия криптографии с открытым ключом резко возрос интерес исследователей к труднорешаемым задачам в таких областях математики как теория чисел, комбинаторика и алгебра. В частности, активно изучается возможность использования различных алгебраических структур, в том числе некоммутативных и неассоциативных, при проектировании систем шифрования. Наиболее широким классом неассоциативных алгебраических структур является класс квазигрупп. Табличное задание квазигруппы представляет собой латинский квадрат, шифрование по которому (так называемое табличное гаммирование) обладает свойством "совершенной секретности," отмеченным еще К. Шенноном [12]. В последнее время появилось много подходов к использованию квазигрупп при решении различных задач криптографии [2], в том числе при разработке систем поточного шифрования [10, 11, 13].

Особое внимание при изучении квазигрупп в контексте криптографических приложений уделяется полиномиально (функционально) полным квазигруппам. Это обусловлено тем, что задача распознавания разрешимости системы уравнений в функционально полной алгебре NP-полна [8]. В данном направлении значительные результаты были получены В. А. Артамоновым с соавторами [3, 4, 5]. Также следует отметить работы [1] и [6], в которых показано, что проверка свойства полиномиальной полноты квазигруппы простого порядка может быть осуществлена за полиномиальное (относительно порядка квазигруппы) время. Естественным обобщением этого результата является его распространение на квазигруппы произвольного порядка.

2. Основные понятия и постановка задачи

Определение 1. Квазигруппой называется множество Q, на котором определена бинарная операция f_Q (или просто f, если из контекста ясно, о какой квазигруппе идет речь) такая, что для любых элементов $a, b \in Q$ уравнения $f(a, x) = b$ и $f(y, a) = b$ однозначно разрешимы в Q. Часто квазигрупповая операция называется умножением и обозначается символом $*$.

Широко распространено табличное задание квазигрупповой операции: для множества элементов $\{q_1, \ldots, q_m\}$, составляющих квазигруппу Q, выписывается квадратная таблица размера $m \times m$ с окаймляющими строкой и столбцом.

Для фиксированного (конечного) множества A обозначим через $\mathcal{O}_n(A)$ совокупность всех n-арных операций на A ($n \geqslant 0$) и пусть $\mathcal{O}(A) = \bigcup\limits_n \mathcal{O}_n(A)$. В данной работе под множеством A везде понимается множество элементов квазигруппы, поэтому мы будем использовать упрощенную запись $\mathcal{O}_n$ и $\mathcal{O}$.

На произвольном подмножестве $F \subseteq \mathcal{O}(A)$ естественным образом вводятся операции суперпозиции и замыкания. Обозначим замыкание множества F через $[F]$.

 Получено 27.12.2017. УДК 512.548.7, 519.716.2

[1]Московский государственный университет им. М. В. Ломоносова. E-mail: agalat@msu.ru.

[2]Московский государственный университет им. М. В. Ломоносова. E-mail: apankrat@intsys.msu.ru.

Определение 2. Квазигруппа Q называется полиномиально (или функционально) полной, если $[\{f_Q\} \cup \mathcal{O}_0] = \mathcal{O}$.

Свойство полиномиальной полноты можно выразить в терминах свойств простоты и неаффинности.

Определение 3. Квазигруппа называется простой, если она не имеет нетривиальных конгруэнций. Иными словами, квазигрупповая операция не сохраняет никакое нетривиальное отношение эквивалентности на элементах квазигруппы.

Определение 4. Квазигруппа $(Q, *)$ называется аффинной, если на множестве Q можно ввести структуру $(Q, +)$ абелевой группы, относительно которой квазигрупповая операция принимает вид $x * y = \alpha(x) + \beta(y) + c$, где α, β — некоторые автоморфизмы абелевой группы и $c \in Q$.

Теорема 1 [7]. *Квазигруппа является полиномиально полной тогда и только тогда, когда она проста и не аффинна.*

Можно показать, что необходимым условием простоты аффинной над абелевой группой $(Q, +)$ квазигруппы примарного порядка является то, что группа $(Q, +)$ является элементарной абелевой [5].

В настоящей работе исследуется сложность проверки полиномиальной полноты квазигруппы произвольного порядка. При оценке сложности под элементарными операциями понимаются сравнение и перестановка элементов, а также арифметические операции в используемых алгебраических структурах. При переходе к операциям над числами фиксированного размера оценка сложности остается полиномиальной.

3. Результаты

Проверку свойств простоты и неаффинности, дающих в совокупности критерий полиномиальной полноты квазигруппы, можно осуществить по отдельности независимо друг от друга.

Теорема 2. *Сложность проверки простоты квазигруппы порядка n оценивается сверху величиной $O(n^4)$.*

Идея доказательства состоит в том, чтобы вычислить транзитивное замыкание для каждого отношения вида $\rho(a, b)$, где элемент a фиксирован, а b — произвольный элемент множества $Q \setminus \{a\}$.

Удивительным образом, проверка простоты квазигруппы оказывается сложнее проверки ее аффинности.

Теорема 3. *Сложность проверки аффинности квазигруппы порядка n оценивается сверху величиной $O(n^3)$.*

Идея доказательства состоит в том, чтобы в предположении аффинности квазигруппы попытаться восстановить представление квазигрупповой операции согласно определению 4. Соответствующая групповая операция может быть восстановлена с квадратичной сложностью при помощи составления новой матрицы, строки которой имеют вид $\sigma_i \sigma_1^{-1}$, где σ_i обозначает i-ю строку таблицы, задающей исходную квазигруппу. Заметим, что в силу результата [9, Лемма 5.2.4.2]) нейтральный элемент группы можно выбрать произвольным образом. Ассоциативность и коммутативность групповой операции проверяются со сложностью $O(n^3)$.

Искомые автоморфизмы $\alpha(\cdot)$ и $\beta(\cdot)$ задаются столбцом и строкой исходной таблицы, начинающимися с нейтрального элемента. Проверка того, что данные перестановки действительно задают групповые автоморфизмы, может быть осуществлена с квадратичной сложностью.

Наконец, последним этапом является проверка выполнения равенства $x * y = \alpha(x) + \beta(y) + c$ для всех пар элементов Q. Нетрудно видеть, что сложность такой проверки также оценивается сверху квадратично относительно мощности множества Q.

Если квазигруппа является аффинной, то искомое представление будет построено. Обратно, выполнение равенства $x * y = \alpha(x) + \beta(y) + c$ для всех пар элементов Q влечет аффинность квазигруппы.

Из теорем 2 и 3 непосредственно следует основной результат настоящей работы.

Теорема 4. *Сложность проверки полиномиальной полноты квазигруппы порядка n оценивается сверху полиномом от n.*

Литература

1. *Галатенко А. В., Панкратьев А. Е., Родин С. Б.* О полиномиально полных квазигруппах простого порядка // Интеллектуальные системы. Теория и приложения. 2016. Т. 20, вып 3. С. 194—198.
2. *Глухов М. М.* О применениях квазигрупп в криптографии // Прикладная дискретная математика. 2008. № 2. С. 28—32.
3. *Artamonov V. A., Chakrabarti S., Gangopadhyay S., Pal S. K.* On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts // Quasigroups and Related Systems. 2013. Vol. 21, № 2. P. 117—130.
4. *Artamonov V. A., Chakrabarti S., Pal S. K.* Characterization of Polynomially Complete Quasigroups based on Latin Squares for Cryptographic Transformations // Discrete Applied Mathematics. 2016. Vol. 200. P. 5—17.
5. *Artamonov V. A., Chakrabarti S., Pal S. K.* Characterizations of highly non-associative quasigroups and associative triples // Quasigroups and Related Systems. 2017. Vol. 25, № 1. P. 1—19.
6. *Galatenko A. V., Pankratiev A. E., Rodin S. B.* Polynomially complete quasigroups of prime orders // International conference Mal'tsev Meeting, November 21–25, 2016. Collection of Abstracts. Novosibirsk, 2016. P. 48.
7. *Hagemann J., Herrmann C.* Arithmetical locally equational classes and representation of partial functions // Universal Algebra, Esztergom (Hungary), 1982. Vol. 29. Colloq. Math. Soc. Janos Bolyai. P. 345—360.
8. *Horváth G., Nehaniv C. L., Szabó Cs.* An assertion concerning functionally complete algebras and NP-completeness // Theoretical Computer Science. 2008. Vol. 407, № 1–3. P. 591—595.
9. *Lau D.* Function algebras on finite sets: a basic course on many-valued logic and clone theory. Springer, 2006.
10. *Markovski S., Gligoroski D., Bakeva V.* Quasigroup String Processing: Part 1 // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci. 1999. Vol. XX, № 1–2. P. 13—28.
11. *Markovski S., Kusacatov V.* Quasigroup String Processing: Part 2 // Proc. of Maked. Academ. of Sci. and Arts for Math. and Tech. Sci. 2000. Vol. XXI, № 1–2. P. 15—32.
12. *Shannon C.* Communication theory of secrecy systems // Bell System Techn. J. 1949. Vol. 28, № 4. P. 656—715.
13. *Shcherbacov V.* Quasigroup based crypto-algorithms // arXiv:1201.3016 [math.GR]. URL: https://arxiv.org/abs/1201.3016 (дата обращения: 20.10.2017).

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ЧИСЛА МОЦКИНА И НЕКОТОРЫЕ КОМБИНАТОРНЫЕ ТОЖДЕСТВА, СВЯЗАННЫЕ С НИМИ

Т. П. Гой (Ивано-Франковск, Украина)[1]

1. Введение

Число Моцкина M_n для данного натурального числа n — это количество возможных вариантов соединения n различных точек на окружности непересекающимися хордами (хорды могут выходить не из каждой точки).

Числа Моцкина имеют и другие комбинаторные интерпретации. Например, число M_n является количеством положительных целых последовательностей длины $n-1$, в которых начальный и конечный элемент равны 1 или 2, а разность между любыми двумя последовательными элементами равна -1, 0 или 1. Число M_n также можно интерпретировать как число путей-маршрутов длины n, которые выходят из начальной точки с координатами $(0,0)$ и заканчиваются в точке $(n,0)$, не опускаясь ниже нулевого уровня.

В [7] указано четырнадцать различных применений чисел Моцкина в комбинаторике, теории чисел и геометрии (см. также, например, [3, 4, 5, 6, 15, 16, 18]).

Числа Моцкина $\{M_n\}_{n\geqslant 0}$ образуют последовательность A001006 из Он-лайн энциклопедии целочисленных последовательностей [19]:

$$1, 1, 2, 4, 9, 21, 51, 127, 323, 835, 2188, 5798, 15511, 41835, 113634, 310572, \ldots$$

Числа Моцкина удовлетворяют рекуррентным соотношениям

$$M_n = M_{n-1} + \sum_{i=0}^{n-2} M_i M_{n-2-i}, \quad M_n = \frac{2n+1}{n+2} M_{n-1} + \frac{3n-3}{n+2} M_{n-2}, \quad n \geqslant 2,$$

где $M_0 = M_1 = 1$, и могут быть выражены по формуле

$$M_n = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n}{2i} C_i, \qquad n \geqslant 0,$$

где $\binom{p}{q} = \frac{p!}{q!(p-q)!}$ — биномиальный коэффициент, $C_n = \frac{1}{n+1}\binom{2n}{n}$ — число Каталана (последовательность A000108 в [19]), $\lfloor s \rfloor$ — наибольшее целое, меньшее или равное s.

2. Матрица и определитель Теплица–Хессенберга

Нижней *матрицей Теплица–Хессенберга* n-го порядка называется матрица вида

$$A_n \equiv A_n(a_0; a_1, \ldots, a_n) = \begin{pmatrix} a_1 & a_0 & 0 & \cdots & 0 & 0 \\ a_2 & a_1 & a_0 & \cdots & 0 & 0 \\ a_3 & a_2 & a_1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \ddots & \cdots & \cdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_1 & a_0 \\ a_n & a_{n-1} & a_{n-2} & \cdots & a_2 & a_1 \end{pmatrix}, \tag{1}$$

где $a_0 \neq 0$ и $a_k \neq 0$ хотя бы для одного индекса k.

 Получено 25.12.2017. УДК 511.176.

[1]Прикарпатский национальный университет им. Василия Стефаника. E-mail: tarasgoy@yahoo.com.

Определитель $\det(A_n)$ матрицы A_n из (1) (*определитель Теплица–Хессенберга*) можно выразить через его элементы по *формуле Труди* [17]

$$\det(A_n) = \sum_{\widetilde{s}=n} (-a_0)^{n-|s|} \binom{|s|}{s_1, \ldots, s_n} a_1^{s_1} a_2^{s_2} \cdots a_n^{s_n}, \tag{2}$$

где $\binom{|s|}{s_1,\ldots,s_n} = \frac{(s_1+s_2+\cdots+s_n)!}{s_1!s_2!\cdots s_n!}$ — мультиномиальный коэффициент, $\widetilde{s} = s_1 + 2s_2 + \cdots + ns_n$, $|s| = s_1 + s_2 + \cdots + s_n$ и, кроме того, $s_i \geqslant 0$.

3. Определители Теплица–Хессенберга, элементами которых являются числа Моцкина

Рассмотрим некоторые последовательности определителей Теплица–Хессенберга специального вида, элементами которых являются числа M_n.

Для удобства далее будем обозначать

$$D_{\pm}(a_1, a_2, \ldots, a_n) = \det(A_n(\pm 1; a_1, a_2, \ldots, a_n)).$$

Теорема 1. *Пусть $n \geqslant 1$, кроме указанных случаев. Тогда*

$$\begin{aligned}
D_+(M_0, M_1, \ldots, M_{n-1}) &= \sum_{i=1}^{n} (-1)^{i-1} \binom{n-1}{i-1} C_{i-1} \\
&= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \binom{n-1}{i-1} \binom{2i-2}{i-1}, \\
D_-(M_0, M_1, \ldots, M_{n-1}) &= \sum_{i=1}^{n} (-1)^{n+i} \binom{n-1}{i-1} \binom{2i-1}{i}, \\
D_+(M_1, M_2, \ldots, M_n) &= \sum_{i=1}^{n} (-1)^{i-1} \binom{n-2}{n-i} C_{i-1} \\
&= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \binom{n-2}{n-i} \binom{2i-2}{i-1}, \\
D_+(M_1, M_2, \ldots, M_n) &= (-1)^{n-1} M_{n-2}, \qquad n \geqslant 2, \\
D_+(M_2, M_3, \ldots, M_{n+1}) &= \frac{(-1)^{n-1}}{n} \sum_{i=1}^{\lfloor (n+1)/2 \rfloor} \binom{n}{i-1} \binom{n-i-1}{i-2}, \qquad n \geqslant 2.
\end{aligned}$$

Используя формулу (2) для определителей Теплица–Хессенберга из теоремы 1, после несложных преобразований получаем следующие тождества с мультиномиальными коэффициентами для чисел Моцкина M_i.

Теорема 2. *Пусть $n \geqslant 1$, кроме указанного случая. Тогда*

$$\sum_{\widetilde{s}=n} (-1)^{|s|+1} \binom{|s|}{s_1, \ldots s_n} M_0^{s_1} M_1^{s_2} \cdots M_{n-1}^{s_n} = \sum_{i=1}^{n} \frac{(-1)^{n+i}}{i} \binom{n-1}{i-1} \binom{2i-2}{i-1}, \tag{3}$$

$$\sum_{\widetilde{s}=n} \binom{|s|}{s_1, \ldots s_n} M_0^{s_1} M_1^{s_2} \cdots M_{n-1}^{s_n} = \sum_{i=1}^{n} (-1)^{n+i-1} \binom{n-1}{i-1} \binom{2i-1}{i}, \tag{4}$$

$$\sum_{\widetilde{s}=n} (-1)^{|s|+1} \binom{|s|}{s_1, \ldots s_n} M_1^{s_1} M_2^{s_2} \cdots M_n^{s_n} = M_{n-2}, \tag{5}$$

$$\sum_{\widetilde{s}=n} (-1)^{|s|+1} \binom{|s|}{s_1, \ldots s_n} M_2^{s_1} M_3^{s_2} \cdots M_{n+1}^{s_n} = \frac{1}{n} \sum_{i=1}^{\lfloor (n+1)/2 \rfloor} \binom{n}{i-1} \binom{n-i-1}{i-2}, \qquad n \geq 2, \tag{6}$$

где суммирование производится по всем целым числам $s_j \geqslant 0$, для которых $\widetilde{s} = n$.

Следствие. *Из формул* (3), (4), (5) *и* (6) *при* $n = 3, 4, 5, 6$ *соответственно получаем:*

$$M_0^3 - 2M_0M_1 + M_2 = 1,$$
$$M_0^4 + 3M_0^2M_1 + 2M_0M_2 + M_1^2 + M_3 = 13,$$
$$M_1^5 - 4M_1^3M_2 + 3M_1^2M_3 + 3M_1M_2^2 - 2M_1M_4 - 2M_2M_3 + M_5 = M_3 = 4,$$
$$M_2^6 - 5M_2^4M_3 + 4M_2^3M_4 + 6M_2^2M_3^2 - 3M_2^2M_5 - 6M_2M_3M_4 + 2M_3M_5$$
$$+ 2M_2M_6 - M_3^3 + M_4^2 - M_7 = 6.$$

Замечание. Формулы, аналогичные формулам из теоремы 2, для чисел Фибоначчи, Люка, Пелля, Якобсталя, Якобсталя–Люка, Каталана, Падована, трибоначчи получены нами в [1, 2, 8, 9, 10, 11, 12, 13, 14].

Литература

1. *Гой Т. П.* Определители матриц Теплица-Хессенберга и числа Люка // Математика и естественные науки. Теория и практика : Межвуз. сб. науч. трудов. Ярославль : Издат. дом ЯГТУ, 2016. Вып. 11. С. 32—36.
2. *Гой Т. П.* Про нові формули для чисел Фібоначчі // Информатика и системные науки (ICH–2017) : Материалы VIII Всеукраинской научно-технической конференции, Полтава, 16–18 марта 2017 г. Полтава : ПУЭТ, 2017. С. 51—54.
3. *Aigner M.* Motzkin numbers // Europ. J. Combin. 1998. Vol. 19. P. 663—675.
4. *Artioli M., Dattoli G., Licciardi S., Pagnutti S.* Motzkin numbers: an operational point of view // arXiv: 1703.07262. URL: https://arxiv.org/pdf/1703.07262 (дата обращения: 24.12.2017).
5. *Barcucci E., Del Lungo A., Pergola E., Pinzani R.* From Motzkin to Catalan permutations // Discr. Math. 2000. Vol. 217. P. 33—49.
6. *Baril J.–L.* Classical sequences revisited with permutations avoiding dotted pattern // Electron. J. Combin. 2011. Vol. 18. Article #P178.
7. *Donaghey R., Shapiro L.W.* Motzkin numbers // J. Combin. Theory Ser. A. 1977. Vol. 23. № 3. P. 291—301.
8. *Goy T.* New Fibonacci and Lucas identities using Toeplitz–Hessenberg permanents // Mathematical, Physical Sciences and Engineering Applications: Abstracts of the 6th Abu Dhabi University Annual International Conference, Abu Dhabi, December 19–21, 2017. Abu Dhabi University, 2017. URL: http://at.yorku.ca/cgi-bin/abstract/cbow-15 (дата обращения: 24.12.2017).
9. *Goy T.* On new Catalan identities using Toeplitz–Hessenberg matrices // 11th International Algebraic Conference in Ukraine dedicated to the 75th anniversary of V. V. Kirichenko : Book of absrtacts, Kyiv, July 3–7, 2017. Kyiv : Institute of Mathematics, 2017. P. 49.
10. *Goy T.* On Jacobsthal and Jacobsthal–Lucas identities with multinomial coefficients // Актуальные проблемы чистой и прикладной математики : Тезисы докладов Международной конференции, посвященной 100-летию со дня рождения академика Тайманова А. Д., Алматы, 22–25 августа 2017 г. Алматы : Институт математики и математического моделирования, 2017. С. 61—64.
11. *Goy T.* On Pell identities with multinomial coefficients // Numbers, Forms and Geometry : Proceedings of the International Conference, Sochi, 21–26 August, 2017. Khabarovsk : Institute of Applied Mathematics, Khabarovsk Division, 2017. P. 23—24.
12. *Goy T.* Some combinatorial identities for two-periodic Fibonacci sequence // Фундаментальные и прикладные проблемы математики и информатики : Материалы XII Международной конференции, Махачкала, 19–22 сентября 2017 г. Махачкала : ДГУ, 2017. С. 107—109.
13. *Goy T.* Some identities for Padovan numbers via the determinants of Toeplitz–Hessenberg matrices // Pure and Applied Mathematics (ICJMS-2017): Book of abstracts of the 30th International Conference of the Jangjeon Mathematical Society, Bab-Ezzouar, Algeria, 12–15 July, 2017. Bab-Ezzouar : Faculty of Mathematics, USTHB, 2017. P. 242—244.
14. *Goy T.* Some tribonacci identities using Toeplitz–Hessenberg determinants // 18th International Scientific Mykhailo Kravchuk Conference: Conference Proceedings, Kyiv–Lutsk, October 7–10, 2017. Kyiv : NTUU "КРІ", 2017. Vol. 1. P. 159—161.
15. *Lengyel T.* On divisibility properties of some differences of Motzkin numbers // Ann. Math. Inform. 2013. Vol. 41. P. 121—136.
16. *Mansour T., Schork M., Sun Y.* Motzkin numbers of higher rank: generating function and explicit expression // J. Integer Seq. 2007. Vol. 10. Article 07.7.4.
17. *Merca M.* A note on the determinant of a Toeplitz–Hessenberg matrix // Spec. Matrices. 2013. Vol. 1. P. 10—16.
18. *Oste R., Van der Jeugt J.* Motzkin paths, Motzkin polynomials and recurrence relations // Electron. J. Combin. 2015. Vol. 22. Article #P2.8.
19. *Sloane N.J.A.* The On-Line Encyclopedia of Integer Sequences. URL: https://oeis.org.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ЛИНЕЙНЫЕ ОТОБРАЖЕНИЯ, СОХРАНЯЮЩИЕ СКРАМБЛИНГ-ИНДЕКС[1]

А. Э. Гутерман (Москва)[2], А. М. Максаев (Москва)[3]

Определение. Скрамблинг-индексом ориентированного графа G с множеством вершин $V(G)$ называется такое наименьшее положительное целое число k, если оно существует, что для любых вершин $a, b \in V(G)$ найдется такая вершина $v \in V(G)$, что в графе G имеются ориентированные пути из a в v и из b в v длины ровно k. Если такого положительного числа k не нашлось, то говорят, что скрамблинг-индекс G равняется 0.

Получена полная характеризация линейных отображений графов (соответственно, матриц над бинарным булевым или другим антинегативным полукольцом без делителей 0), сохраняющих скрамблинг-индекс.

 Получено 06.01.2017. УДК 512.643.

[1]Работа выполнена при частичной финансовой поддержке гранта РФФИ 17-01-00895.

[2]Московский государственный университет им. М. В. Ломоносова. E-mail: guterman@list.ru.

[3]Московский государственный университет им. М. В. Ломоносова.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О НЕКОТОРЫХ АДДИТИВНЫХ ТЕОРЕТИКО–ЧИСЛОВЫХ ЗАДАЧАХ

Н. А. Зинченко (Белгород)[1], Н. Н. Мотькина (Белгород)[2]

Простые числа интересовали ученых с древнейших времен. Они были известны древним египтянам и вавилонянам, отличавшимися своим искусством вычислений [1].

В теории чисел важную роль играют аддитивные задачи с простыми числами. Пусть $k \geq 2$ и $n \geq 1$ — числа. Рассмотрим уравнение

$$p_1^n + p_2^n + \cdots + p_k^n = N \tag{1}$$

в простых числах $p_1,\ p_2, \ldots, p_k$.

Ряд классических проблем теории чисел сводится к вопросу о числе решений уравнения (1). Например, если $n = 1$, а $k = 2$, или 3, то (1) — уравнение Гольдбаха; если $n \geq 3$, то (1) — уравнение Варинга–Гольдбаха.

Уравнение Гольдбаха при $k = 3$ относят к тернарным задачам. А представление натурального числа в виде суммы двух простых чисел — к бинарным.

В 1937 г. И. М. Виноградов полностью решил тернарную проблему Гольдбаха [6]. Утверждение бинарной проблемы Гольдбаха остается до сих пор недоказанным.

Настоящий доклад посвящен некоторым бинарным аддитивным задачам теории чисел.

В 1938 г. Н. Г. Чудаков [8] доказал следующую теорему.

Теорема 1. *Пусть $K(X)$ равно числу тех четных чисел между 6 и X, которые не могут быть представлены как сумма двух нечетных простых. Тогда*

$$K(X) \leq C_D \frac{X}{\log^D X}, \quad 6 \leq X < \infty,$$

где D — произвольное фиксированное положительное число, C_D — положительная константа, зависящая только от D.

Пусть η — алгебраическое число степени n, a и b — произвольные фиксированные действительные числа из отрезка $[0, 1]$. Тогда верна теорема [4].

Теорема 2. *Пусть $K(X)$ — число тех четных чисел между 6 и X, которые не могут быть представлены как сумма двух нечетных простых специального вида*

$$a < \{\eta p_i\} < b, \quad i = 1, 2.$$

Тогда при любом фиксированном $D > 0$

$$K(X) = O(X \log^{-D} X), \quad 6 \leq X < \infty.$$

В докладе будет представлено краткое изложение доказательства теоремы 2.

К бинарным аддитивным задачам относят и проблему делителей Титчмарша, состоящую в выводе асимптотической формулы для числа решений уравнения

$$p - 1 = xy, \qquad p \leq n.$$

Она была решена Ю. В. Линником при помощи дисперсионного метода [7].

 Получено 17.12.2017. УДК 511.34.

[1]Белгородский государственный национальный исследовательский университет.
E-mail: zinchenko@bsu.edu.ru.

[2]Белгородский государственный национальный исследовательский университет.
E-mail: motkina@bsu.edu.ru.

После опубликования И. М. Виноградовым [2] асимптотической формулы для числа простых чисел, не превосходящих x и лежащих в промежутках специального вида, которые получили название «коротких», или «виноградовских», стали рассматриваться аддитивные задачи с простыми числами из таких промежутков. Методом Виноградова были решены некоторые тернарные аддитивные задачи, например, в работе [3]. Однако, бинарные аддитивные задачи с простыми числами из коротких промежутков, в том числе и проблему Титчмарша, пока решить не удается. Можно рассмотреть проблему делителей Титчмарша с полупростыми числами p_1p_2, на которые наложены ограничения [5].

Число решений уравнения

$$p_1p_2 - xy = 1, \tag{2}$$

где $p_1p_2 \le n$, обозначим через $T(n)$. Уравнение (2) решается в переменных x, y, p_1 и p_2, где x и y — числа натуральные. Простые числа p_1 и p_2 удовлетворяют также дополнительным условиям:

$$p_1 > e^{\sqrt{\log n}}, \quad p_2 > e^{\sqrt{\log n}},$$
$$\{(1/2)(p_1p_2)^{1/c}\} < 1/2.$$

Теорема 3. *Пусть c — произвольное число из полуинтервала $(1, 2]$, p_1, p_2 — простые числа,*

$$T(n) = \sum_{\substack{p_1p_2 \le n \\ p_1 > e^{\sqrt{\log n}},\ p_2 > e^{\sqrt{\log n}}}} \tau(p_1p_2 - 1),$$

$$T_1(n) = \sum_{\substack{p_1p_2 \le n \\ p_1 > e^{\sqrt{\log n}},\ p_2 > e^{\sqrt{\log n}} \\ \{(1/2)(p_1p_2)^{1/c}\} < 1/2}} \tau(p_1p_2 - 1).$$

Тогда справедливо равенство:

$$T_1(n) = \frac{1}{2}T(n) + O(n \log\log\log n), \tag{3}$$

где

$$T(n) \sim c_0 n \log\log n$$

и

$$c_0 = \sum_{r=1}^{\infty} \frac{\mu^2(r)}{r\varphi(r)}.$$

С помощью идей и методов, использованных при доказательстве теоремы 3, можно решать и другие бинарные аддитивные задачи с полупростыми числами специального вида из «виноградовских» промежутков.

Литература

1. *Бухштаб А. А.* Теория чисел. М. : Просвещение, 1966. 384 с.
2. *Виноградов И. М.* Некоторое общее свойство распределения простых чисел // Математический сборник. 1940. № 7. С. 365—372.
3. *Гриценко С. А.* Три аддитивные задачи // Известия РАН. Серия математическая. 1992. Т. 56, № 6. С. 1198—1216.
4. *Гриценко С. А., Мотькина Н. Н.* О теореме Чудакова в простых числах специального вида // Чебышевский сборник. 2011. Т. 12, вып. 4. С. 75—84.
5. *Зинченко Н. А.* Бинарная аддитивная задача с полупростыми числами специального вида // Чебышевский сборник. 2005. Т. 6, вып. 2. С. 145—162.
6. *Карацуба А. А.* Основы аналитической теории чисел. М. : Наука, 1983. 240 с.
7. *Линник Ю. В.* Дисперсионный метод в бинарных аддитивных задачах. Л. : Изд-во ЛГУ, 1961. 208 с.
8. *Чудаков Н Г.* О плотности совокупности четных чисел, непредставимых как сумма двух нечетных простых // Известия АН СССР. Серия математическая. 1938. № 1. С. 25—40.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

РАСПРЕДЕЛЕНИЕ ВЕКТОРОВ С АЛГЕБРАИЧЕСКИМИ СОПРЯЖЕННЫМИ КООРДИНАТАМИ В ОБЛАСТЯХ МАЛОЙ МЕРЫ ЛЕБЕГА

Э. И. Ковалевская (Минск, Беларусь)[1]

Цель тезиса — познакомить участников конференции с одним из направлений исследований, проводимых представителями школы теории чисел НАН Беларуси. Эту школу начал формировать профессор В. Г. Спринджук в 70-е годы прошедшего столетия. В настоящее время ее возглавляет профессор В. И. Берник. Здесь подготовлено более 30 кандидатов и 2 доктора физ.-мат. наук.

Задача подсчета целых, рациональных и алгебраических точек или векторов в данных областях — классическая задача теории чисел. С ее решением связаны и другие задачи. Например, проблема круга или задачи метрической теории диофантовых приближений, изучающей точки экстремальных многообразий. В последние 10 лет получено продвижение в решении задач о числе точек с рациональными или действительными алгебраическими сопряженными координатами вблизи некоторых гладких кривых и поверхностей $\Gamma \subset \mathbb{R}^n$, $n \geq 3$. В списке литературы (см. [1—7]) указаны только несколько публикаций по этой тематике. Более полный список можно найти в самих работах. Там же представлены и методики исследований.

Приведем результат из [7], который является распространением результата [2] в пространство $\mathbb{R}^4$. Различие состоит в том, что в [7] мы исследуем определенное диофантово неравенство, связанное с малыми значениями целочисленных многочленов степени 4, а в [2] — аналогичное неравенство для целочисленных многочленов степени 3. Общий случай задачи в настоящее время еще не решен.

Пусть

$$P = P(t) = a_n t^n + \cdots + a_1 t + a_0 \in \mathbb{Z}[t],\ n \geq 4,\ a_n \neq 0,\ t \in \mathbb{R}.$$

Пусть высота $H(P)$ многочлена P, $H(P) = \max(|a_n|, \ldots, |a_0|)$, *возрастает*, но степень n — *фиксирована*. Пусть $\alpha_1, \alpha_2, \ldots, \alpha_n$ — корни многочлена $P(t)$, т. е. они являются *алгебраическими сопряженными числами*, и пусть $\mu_i > 0$ $(i = \overline{1,4})$ — фиксированные числа. Рассмотрим параллелепипед

$$\mathcal{T} = \prod_{i=1}^{4} I_i = \prod_{i=1}^{4} [a_i, b_i] \subset [-1/2, 1/2]^4,$$

где длина $|I_i| = b_i - a_i = Q^{-\mu_i}$, при $Q > Q_0 > 0$ и его подмножество

$$\mathcal{M} = \{\overline{x} = (x_1, x_2, x_3, x_4) \in \mathcal{T} : |x_i - x_j| < 0,001,\ i \neq j\}.$$

Положим $\mathcal{T}_1 = \mathcal{T} \backslash \mathcal{M}$. Введем класс многочленов

$$\mathcal{P}_n(Q) = \{P : |a_n| \asymp H(P), H(P) \leq Q\}.$$

Обозначим через $\mathcal{A}_n(\mathcal{T}_1, Q)$ множество векторов

$$\overline{\alpha} = (\alpha_i, \alpha_j, \alpha_k, \alpha_l),\ 1 \leq i < j < k < l \leq n,$$

 Получено 14.11.2017. УДК 511.36.

[1]Белорусский государственный аграрный технический университет. E-mail: ekovalevsk@mail.ru.

составленных из корней многочлена P, $P \in \mathcal{P}_n(Q)$, таких, что $\overline{\alpha} \in \mathcal{T}_1$, т. е. мы рассматриваем четверки *различных действительных* корней многочлена P. Доказана

Теорема 1. *Если* $0 < \mu_i < 1/4$ $(i = \overline{1,4})$, *то*

$$\sharp\mathcal{A}_n(\mathcal{T}_1, Q) \gg Q^{n+1-\mu_1-\mu_2-\mu_3-\mu_4},$$

где $X \gg Y$ *означает, что* $X > c(n)Y$ *при некоторой абсолютной константе* $c(n) > 0$, *зависящей от* n.

Здесь мы применяем вариант метода *существенных* и *несущественных* областей, как в [2]. Доказательство теоремы основано на построении специальных целочисленных многочленов P с условиями:

1) величины $|P(x_i)|$, $i = \overline{1,4}$, малы при $\overline{x} = (x_1, x_2, x_3, x_4) \in B \subset \mathcal{T}_1$ и *мера Лебега* $(B) \geq \frac{1}{2}$ *меры Лебега* $(\mathcal{T}_1)$,
2) $|P'(x_i)| \asymp H(P) = Q$ в точках $\overline{x} \in B$.

Из теоремы 1 следует основной результат.

Теорема 2. *Пусть функция* $u = f(x, y, z)$ *непрерывна в параллелепипеде*

$$\mathcal{K} = \prod_{i-1}^{3} K_i \subset [-1/2, 1/2]^3.$$

Положим

$$\mathcal{J}(Q, \lambda) = \{(x, y, z, u) : x \in K_1,\ y \in K_2,\ z \in K_3,\ |u - f(x, y, z)| < Q^{-\lambda},\ 0 < \lambda < 1/4\}.$$

Тогда существует, по крайней мере, $c_1(n)Q^{n+1-\lambda}$ *векторов* $\overline{\alpha}$ *из* $\mathcal{A}_n(\mathcal{T}_1, Q)$ *таких, что* $\overline{\alpha} \in \mathcal{J}(Q, \lambda)$, *где* $c_1(n) > 0$ — *некоторая абсолютная константа, зависящая от* n.

Отметим, что метод существенных и несущественных областей был разработан В. Спринджуком в 1964–1965 гг. Затем этот метод развивали и совершенствовали В. Берник, В. Бересневич, Д. Бодягин, М. Додсон, Д. Диккинсон, С. Велани и другие представители школ теории чисел НАН Беларуси и университета г. Йорк (Англия).

Литература

1. *Берник В. И., Гётце Ф., Гусакова А. Г.*. Распределение алгебраических чисел и точек с алгебраическими сопряженными координатами в областях малой меры // Препринт. Ин-т математики НАН Беларуси. 2016. № 1 (578). Мн., 2016. 56 с.
2. *Ковалевская Э. И., Рыкова О. В.* Развитие метода существенных и несущественных областей для подсчета векторов с действительными алгебраическими координатами вблизи гладких поверхностей // Чебышевский сборник. 2013. Т. 14, вып. 4. С. 119—126.
3. *Beresnevich V., Dickinson D., Velani S.* Diophantine approximation on planar curves and the distribution of rational points. With an Appendix II by Vaughan R. C. // Ann. of Math. (2). 2007. Vol. 166, № 2. P. 367—426.
4. *Beresnevich V.* Rational points near manifolds and metric Diophantine approximation // Ann. of Math. 2012. Vol. 175. P. 187—235.
5. *Bernik V., Götze F.* A new connection between metric theory of Diophantine approximations and distribution of algebraic numbers // Contemp. Math. 2015. Vol. 631. P. 33—45.
6. *Kaliada D., Götze F., Kukso O.* The asymptotic number of integral cubic polynomials with bounded heights and discriminants // Lithuanian Math. J. 2014. Vol. 54, № 2. P. 150—165.
7. *Kavaleuskaya E.* The lower value for the number of algebraic vectors in $\mathbb{R}^4$ near smooth manifolds // Abstract of talks. ALaNT 4 – 11th Polish, Slovak and Czech conference on Number Theory and 18th colloquiumfest on Algebra and Logic. Telč, Czech Republic, June 13—17, 2016. P. 14—15.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

РАСПРЕДЕЛЕНИЕ НУЛЕЙ НЕВЫРОЖДЕННЫХ ФУНКЦИЙ НА КОРОТКИХ ОТРЕЗКАХ

И. М. Морозова (Минск, Беларусь)[1], О. Н. Кемеш (Минск, Беларусь)[2]

В последние годы были найдены связи между метрической теорией диофантовых приближений с распределением действительных алгебраических и целых алгебраических чисел на коротких интервалах действительной прямой [1, 4, 5, 6, 7]. Пусть на I заданы непрерывно-дифференцируемые функции $f_1(x), f_2(x), \ldots, f_n(x)$ такие, что вроскиан $W(x)$ их производных

$$W(x) = \begin{vmatrix} f_1'(x) & f_2'(x) & \ldots & f_n'(x) \\ f_1''(x) & f_2''(x) & \ldots & f_n''(x) \\ \vdots & \vdots & \vdots & \vdots \\ f_1^{(n)}(x) & f_2^{(n)}(x) & \ldots & f_n^{(n)}(x) \end{vmatrix}$$

для почти всех x (в смысле меры Лебега) отличен от нуля на I. Такие функции $f_1(x)$, $f_2(x), \ldots, f_n(x)$ будем называть невырожденными на I.

Составим функцию

$$F_n(x) = a_n f_n(x) + \ldots + a_1 f_1(x) + a_0.$$

Введем обозначения: $n = \deg F_n(x)$, $H = H(F_n) = \max|a_j|$, $0 \le j \le n$.

Функции $F_n(x)$ обладают многими свойствами полиномов. Например, количество нулей $F_n(x)$ на I не превосходит cn, где c — *const*.

В работах [1, 2, 3] относительно функций $F_n(x)$ установлено следующее.

Обозначим через $\psi(t)$ положительную монотонно убывающую функцию аргумента $t > 0$, а через $\mathfrak{I}_n(\psi)$ множество $x \in I$, для которых неравенство

$$|F_n(x)| < H^{-n+1}\psi(H) \tag{1}$$

имеет бесконечное число решений в функциях $F_n(x)$.

Тогда

$$\mu\mathfrak{I}_n(\psi) = \begin{cases} 0, & \text{если } \sum\limits_{H=1}^{\infty} \psi(H) < \infty, \\ \mu I, & \text{если } \sum\limits_{H=1}^{\infty} \psi(H) = \infty. \end{cases} \tag{2}$$

Доказано, что $\mu(H^{-v}) = 0$ при $v > 1$ для произвольного n при невырожденных функциях $f_j(x)$, $1 \le j \le n$. В работах [2] и [7] первое и второе равенства (2) были доказаны для произвольной функции $\psi(t)$.

В настоящей работе доказана следующая теорема.

Рассмотрим невырожденные функции $\bar{f} = (f_1(x), f_2(x), \ldots, f_n(x))$ и для целочисленного вектора $\vec{a} = (a_0, a_1, \ldots, a_n)$ составим функцию

$$F_n(x) = a_n f_n(x) + a_{n-1} f_{n-1}(x) + \ldots + a_1 f_1(x) + a_0.$$

Введем замену переменной: $f_1(x) = t$, $f_j(t) = f_j(f_1^{-1}(t))$, $2 \le j \le n$ и перейдем к набору невырожденных функций аргумента t, $f_j(t)$, $2 \le j \le n$. Далее, чтобы не менять

 Получено 03.11.2017. УДК 512.542.

[1]Белорусский государственный аграрный технический университет. E-mail: inna.morozova@tut.by.

[2]Белорусский государственный аграрный технический университет.

обозначений, будем считать, что на интервале J задан набор невырожденных функций $x, f_2(x), \ldots, f_n(x)$ и

$$F_n(x) = a_n f_n(x) + a_{n-1} f_{n-1}(x) + \ldots + a_1 x + a_0 \tag{3}$$
$$\max(|f_j(x)|, x) < c.$$

Введем класс функций при натуральном Q:

$$L_\mathfrak{Z}(Q, \bar{f}) = \{F_n(x) : H(F_n) \le Q\}.$$

Обозначим $l_i = \max\limits_{x \in J} |f_i(x)|$, $l = \max\limits_{1 \le i \le n} l_i$.

Теорема. *На любом интервале I, $\mu I = Q^{-\gamma}$, $0 \le j < 1$ количество нулей функций $F_n(x) \in L_\mathfrak{Z}(Q, \bar{f})$ не превосходит $cnl2^{n+3}Q^{n+1}\mu I$.*

Доказательство теоремы. Разложим функции $F_j(x)$ на интервале J в ряд Тейлора в нуле α_{1j} функции $F_j(x)$, лежащем в J.

$$F_j(x) = F(\alpha_{1j}) + F'(\alpha_{1j})(x - \alpha_{1j}) + \frac{1}{2}F''(\varsigma_{ij})(x - \alpha_{1j})^2, \text{ где } \varsigma_j \in (x; \alpha_{1j}).$$

Так как $F(\alpha_{1j}) = 0$, $|x - \alpha_{1j}| \le \mu J = Q^{-\gamma}$, $|F''(\varsigma_j)| < cnQ$, $|F'(\alpha_{1j})(x - \alpha_{1j})| < nlQ^{1-\gamma}$, то при достаточно большом Q имеем для всех $x \in J$ оценку

$$|F_j(x)| < 2nlQ^{1-\gamma}. \tag{4}$$

Введем вектор $\vec{b} = (a_n, \ldots, a_1)$, состоящий из коэффициентов функции $F_j(x)$, и множество функций $F_j(x)$ с одним и тем же вектором $\vec{b}$ обозначим $F(\vec{b})$. При достаточно большом Q верно неравенство

$$\#F(\vec{b}) = (2Q + 1)^n < 2^{n+1}Q^n,$$

где $\#$ — количество элементов конечного множества.

Занумеруем функции $F_j(x)$, $j = 0, 1, \ldots, 2cnl2^{n+2}Q^{n+1}\mu I$, нули которых лежат на интервале J.

Образуем новые функции $R_j(x) = F_j(x) - F_0(x) = d_j$, которые являются различными целыми числами и $\max|d_j| > 2nlQ^{1-\gamma}$, что противоречит (4). Полученное противоречие доказывает теорему. □

Литература

1. *Beresnevich V.* On approximation of real numbers by real algebraic numbers // Acta Arith. 1999. Vol. 90, № 8. P. 97—112.
2. *Beresnevich V.* A Groshew type theorem for convergence on manifolds // Acta Math. Hungar. 2002. Vol. 94, № 1–2. P. 99—130.
3. *Beresnevich V., Bernik V.* On a metrical theorem of W. Schmidt // Acta Arith. 1996. Vol. 75. P. 219—233.
4. *Bernik V.* On the exact order of approximation of zero by the values of integer-valued polynomials // Acta Arith. 1989. Vol. 53, № 1. P. 17—27.
5. *Bernik V., Getze F.* Distribution of real algebraic numbers of arbitrary degree in short intervals // Izv. Math. RAN. 2015. Vol. 79, № 1. P. 28—39.
6. *Bernik V., Gusakova A., Gotze F.* On points with algebraically conjugate coordinates close to smooth curves // Moscow Journal of Combinatorics and Number Theory. 2016. Vol. 6, iss. 2–3. P. 56—101.
7. *Bernik V., Kleinbock D., Margulis G.* Khintchine-type theorems on manifolds the convergence case for standard and multiplicative versions // Internet. Math. Res. Notices. 2001. P. 453—486.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ПАРАМЕТРИЧЕСКИЕ BR-МНОЖЕСТВА И ПЕРЕКЛАДЫВАЮЩИЕСЯ ПОЛИМИНО[1]

А. А. Осипова (Владимир)[2]

В работе автора 2011 г. [1] впервые был рассмотрен метод построения двумерных множеств ограниченного остатка на основе параметрических разбиений гексагональной торической развертки. Опишем суть метода.

Развертка $T(c)$ двумерного тора $\mathbb{T}$ задается параметром $c = (c_1, c_2)$ из пространства параметров $A = \{c = (c_1, c_2) \in \mathbb{R}^2; c_1, c_2 \geq 0, c_1 + c_2 \leq 1\}$ и является выпуклым шестиугольником, координаты вершин которого $(0,0)$, $(1-c_1, -c_2)$, $(1,0)$, $(1-c_1, 1-c_2)$, $(0,1)$, $(-c_1, 1-c_2)$.

Для построения множеств ограниченного остатка на основе развертки тора необходимо разбить ее на $D+1$ перекладывающуюся область. Перекладывание полученных областей должно вновь давать исходную развертку.

В двумерном случае такое разбиение можно получить, отложив вектор $-\alpha = (-\alpha_1, -\alpha_2)$ от вершин шестиугольника $T(c)$ с координатами $(1,0)$, $(1-c_1, 1-c_2)$, $(0,1)$ и соединив концы отложенных векторов. Здесь вектор $-\alpha = tc$, а параметр $0 < t \leq 1$. Разбиение происходит на три перекладывающиеся области $T_k, k = 0, 1, 2$. Перекладывание областей T_k соответствует сдвигу тора $\mathbb{T}$ на вектор α [3]. Области $T_k, k = 0, 1, 2$ являются множествами ограниченного остатка, для них были получены следующие результаты [3].

Теорема 1. *Пусть дан сдвиг тора на вектор α, и α — иррациональный, т. е. числа $\alpha_1, \alpha_2, 1$ линейно независимы над $\mathbb{Z}$, пусть тор $\mathbb{T}$ разбит на области $\mathbb{T}_k : \mathbb{T} = \mathbb{T}_0 \sqcup \mathbb{T}_1 \sqcup \mathbb{T}_2$, а его развертка $T(c)$ задана параметром $c = (c_1, c_2) \in A$. Тогда для отклонений выполняются точные неравенства:*

$$0 \leq \delta_0(i) \leq 2 - \sigma(c); \quad -1 \leq \delta_1(i) \leq c_1; \quad -1 \leq \delta_2(i) \leq c_2,$$

где $\sigma(c) = c_1 + c_2$.

В работах автора [2—8] были расширены результаты работы [1] и изучены свойства, построенных множеств, в частности найдены средние значения отклонений и доказаны теоремы об оптимизации границ отклонений.

Модифицируем рассмотренный алгоритм для построения трансляционных полимино.

Определение 1. Полимино — это фигура, составленная из квадратов, каждый из которых имеет, по крайней мере, одну сторону, общую с другим входящим в неё же квадратом.

Наибольший интерес для приложений представляют трансляционные полимино, т. е. разбивающие всю плоскость с применением только параллельных переносов, и методы их построения.

Определение 2. Назовем полимино P перекладывающимся, если задано его разбиение на более мелкие полимино $P_1, P_2, \ldots, P_k$, такое, что их перекладывание вновь дает исходную фигуру.

 Получено 13.12.2017. УДК 511.34.

[1]Работа выполнена при финансовой поддержке РФФИ, проект № 16-31-00055-мол_а.

[2]Владимирский филиал Российского университета кооперации. E-mail: albina.a.osipova@yandex.ru.

Рассмотрим алгоритм построения перекладывающихся полимино. Пусть на плоскости имеется квадратная сетка S, базис которой (e_1, e_2), $e_1 = e_2 = e$. Построим на ней параллелограмм K, стороны которого задаются векторами $n_1 = (n_{11}e_1, n_{12}e_2)$, $n_2 = (n_{21}e_1, n_{22}e_2)$, тогда координаты вершин параллелограмма опишем следующим образом:

$$K_1 = (x_0, y_0),$$
$$K_2 = (x_0 + n_{11}, y_0 + n_{12}),$$
$$K_3 = (x_0 + n_{21}, y_0 + n_{22}),$$
$$K_4 = (x_0 + n_{11} + n_{21}, y_0 + n_{12} + n_{22}),$$

где $n_{11}, n_{12}, n_{21}, n_{22} \in \mathbb{N}$, $x_0, y_0 \in \mathbb{Z}$. Проведем в параллелограмме K диагональ K_2K_3. Внутри треугольника $K_1K_2K_3$ построим «звезду» C. Метод «звезды» впервые был предложен научным руководителем автора В. Г. Журавлевым в 2000 г. и позднее опубликован в работе [9]. Для этого выберем произвольную точку C_0 с целыми координатами и соединим ее с вершинами треугольника $K_1K_2K_3$ лучами r, b, g соответственно. Договоримся, что любой луч на плоскости может проходить только по границе сетки S, начинаться и заканчиваться только в вершинах сетки S.

Построим полимино на основе «звезды» C. Отложим от вершин K_2, K_3, K_4 параллелограмма K луч r, и соединим концы отложенных лучей и вершину квадрата K_1 лучами b и g. Получим полимино P, образованное тремя парами лучей r, b, g, разбитое «звездой» C на три более мелких полимино R, B, G. При этом, количество клеток сетки S, образующих исходное полимино P, будет равно значению определителя

$$\begin{vmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{vmatrix}.$$

Для перекладывания фигур и получения исходного полимино P, сдвинем полимино R на вектор r, полимино B — на вектор b, полимино G — на вектор g.

Для получения корректного результата с помощью рассмотренного алгоритма необходимо учесть следующее: лучи r, b, g «звезды» C и их части не должны накладываться и пересекаться, а также не должно совпадать их направление; часть луча «звезды» может совпадать с частью луча полимино, но пересечения также не допустимы.

Теорема 2. *Описанный выше алгоритм порождает трансляционные перекладывающееся полимино P с векторами трансляции параллелограмма K. Малые полимино R, B, G также являются трансляционными, со своими векторами трансляции.*

Доказательство теоремы основывается на использовании первой части критерия Конвея, являющегося достаточным условием трансляционности фигуры. Граница исходного полимино P образована тремя парами попарно параллельных и равных отрезков r, b, g, что удовлетворяет критерию Конвея, таким образом, полимино P является трансляционным. Границу каждого из перекладывающихся полимино R, B, G так же можно разделить на шесть попарно совпадающих отрезков, следовательно полимино R, B, G — трансляционные полимино.

Для нахождения полиминных разбиений в данном подходе используются точки-связки на границе полимино, являющиеся центрами «звезды» C, на основе которой построены полимино, а также точки, в которых сходятся несколько концов лучей. Совмещая эти точки, получаем разбиение.

Более того, рассмотренным методом могут быть построены полиминные разбиения, состоящие из любых двух полимино из трех. В этом случае базис решетки трансляции образуют два вектора, один из которых принадлежит решетке трансляции для исходного полимино P, а второй — решетке трансляции одного из малых полимино, входящих в пару.

Таким образом, рассмотренный метод позволяет не только строить трансляционные полимино P с заданным числом клеток и их разбиения плоскости, но и трансляционные разбиения плоскости на три полимино R, B, G, и трансляционные разбиения плоскости на порожденные полимино R, B, G в отдельности, а также трансляционные разбиения состоящие из пар полимино RB, RG, BG.

Трансляционные полимино широко применяются при моделировании дискретных структур. Так в кристаллографии на основе полимино строятся модели молекулярных кристаллов, в инженерных задачах полимино используются для нахождения оптимального расположения фигур заданной формы.

Литература

1. *Абросимова А. А.* Множества ограниченного остатка на двумерном торе // Чебышевский сборник. 2011. Т. 12, вып. 4. С. 15—23.
2. *Абросимова А. А.* Произведение торических разверток и построение множеств ограниченного остатка // Ученые записки Орловского государственного университета. Сер.: Естественные, технические и медицинские науки. 2012. № 6, ч. 2. С. 30—37.
3. *Абросимова А. А.* Средние значения отклонений для распределения точек на торе // Научные ведомости БелГУ. Сер.: Математика. Физика. 2012. № 5 (124). Вып. 26. С. 5—11.
4. *Абросимова А. А.* Фрактальные множества ограниченного остатка // Математическое моделирование фрактальных процессов, родственные проблемы анализа и информатики: Материалы Второй Международной конференции молодых ученых. Нальчик : ООО «Редакция журнала Эльбрус». 2012. С. 18—21.
5. *Абросимова А. А.* Границы отклонений для трехмерных множеств ограниченного остатка // Научные ведомости БелГУ. Сер.: Математика. Физика. 2013. № 19 (162). Вып. 32. С. 5—21.
6. *Абросимова А. А.* BR-множества // Чебышевский сборник. 2015. Т. 16, вып. 2. С. 8—22.
7. *Абросимова А. А., Блинов Д. А.* Оптимизация границ отклонений для двумерных множеств ограниченного остатка // Научные ведомости БелГУ. Сер.: Математика. Физика. 2013. № 26 (169). Вып. 33. С. 5—13.
8. *Абросимова А. А., Блинов Д. А., Полякова Т. В.* Оптимизация границ отклонений для множеств ограниченного остатка на двумерном торе // Чебышевский сборник. 2013. Т. 14, вып. 1. С. 9—17.
9. *Журавлев В. Г., Осипова А. А.* Полимино с симметриями: учебное пособие для самостоятельной работы по математике. Автономная некоммерческая образовательная организация высшего образования Центросоюза Российской Федерации «Российский университет кооперации», Владимирский филиал. Владимир : ООО «Аркаим», 2016. 48 с.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О НЕКОТОРЫХ ВЕЩЕСТВЕННЫХ КУБИЧЕСКИХ ГИПЕРПОВЕРХНОСТЯХ

А. В. Селиверстов (Москва)[1]

1. Введение

Рассмотрим n-мерное вещественное проективное пространство с фиксированной системой однородных координат $(x_0 : \cdots : x_n)$. Гиперплоскость $x_0 = 0$ будем называть бесконечно удалённой. Точки с координатами ± 1 отождествим с вершинами фиксированного n-мерного куба, называемого ± 1-кубом. Этот куб вложен в аффинное пространство $x_0 = 1$. Множество вершин ± 1-куба служит множеством всех вершин его грани, если некоторые из координат фиксированы, а остальные принимают любое из двух значений ± 1. В частности, гранями служат вершины и рёбра куба. Грани коразмерности один называются фасетами. Обозначим через $h = \alpha_0 + \alpha_1 x_1 + \cdots + \alpha_{n-1} x_{n-1} + x_n$ линейную функцию, все коэффициенты которой отличны от нуля. Аффинная гиперплоскость $h = 0$ инцидентна некоторой вершине ± 1-куба тогда и только тогда, когда существует особая точка у $(n-1)$-мерной проективной гиперповерхности, которая определена кубической формой $g = \alpha_0 x_0^3 + \cdots + \alpha_{n-1} x_{n-1}^3 - (\alpha_0 x_0 + \cdots + \alpha_{n-1} x_{n-1})^3$. Если же таких вершин нет и все коэффициенты $\alpha_i \neq 0$, то эта гиперповерхность гладкая [11]. Число компонент связности вещественной проективной гиперповерхности $g = 0$ зависит от взаимного расположения гиперплоскости $h = 0$ и вершин ± 1-куба. Поскольку общая комплексная проективная кубическая поверхность определяется суммой кубов пяти линейных форм (Sylvester's pentahedral theorem), полученные результаты могут быть использованы для моделирования поверхностей [6, 7, 9]. Но типичный ранг кубической формы быстро растёт при увеличении числа переменных [12]. С другой стороны, получены новые результаты о комбинаторной задаче, близкой к задаче о рюкзаке [2].

Вещественная проективная кубическая гиперповерхность состоит либо из одной, либо из двух компонент связности. У гладкой гиперповерхности одна компонента связности неориентируемая. Если компонент связности две, то одна из них ориентируемая, а другая неориентируемая и гомеоморфная гиперплоскости. Существует вероятностный алгоритм проверки связности гладкого и ограниченного вещественного алгебраического множества, время работы которого экспоненциально зависит от размерности [10].

Известно несколько методов определения числа компонент гладкой кубической кривой на вещественной проективной плоскости. Линейной заменой координат кубическую форму от трёх переменных, определяющую эту кривую, можно привести к виду $f(y_0, y_1) - y_0 y_2^2$. Если дискриминант Δ многочлена третьей степени $f(1, y_1)$ положительный, то кривая связная. Если отрицательный, то существует ориентируемая компонента [4]. Другой метод основан на приведении кубической формы к виду $y_0^3 + y_1^3 + y_2^3 - 3\lambda y_0 y_1 y_2$. Если $\lambda > 1$, то кривая содержит ориентируемую компоненту; если $\lambda < 1$, то кривая связная [5]. Третий метод основан на представлении кубической формы от трёх переменных в виде определителя эрмитовой матрицы третьего порядка, элементами которой служат линейные формы [8]. Проективные инварианты для объединения овала и прямой, в частном случае совпадающие с приводимой кубической кривой, рассмотрены в работе [1].

Для символьных вычислений использован облачный сервис MathPartner [3]. Визуализация кривых и поверхностей выполнялась программой Surfer; уравнения кривых определяют цилиндрические поверхности (https://imaginary.org/de/program/surfer).

 Получено 20.12.2017. УДК 514.144.

[1]Институт проблем передачи информации им. А. А. Харкевича РАН. E-mail: slvstv@iitp.ru.

2. Результаты

Теорема 1. *Если аффинная гиперплоскость $h = 0$, которая не инцидентна никакой вершине и не параллельна никакому ребру ± 1-куба, отделяет одну вершину от остальных вершин ± 1-куба, то вещественная проективная гиперповерхность $g = 0$ состоит из двух компонент связности. Если гиперплоскость $h = 0$ не пересекает ± 1-куб, то вещественная проективная гиперповерхность $g = 0$ гомеоморфна гиперплоскости.*

Доказательство. Если две аффинные гиперплоскости одинаково расположены относительно вершин ± 1-куба, то соответствующие вещественные проективные гиперповерхности имеют равное число компонент связности.

Рассмотрим ε-окрестность точки $\mathbf{1}$, все координаты которой равны 1, и многочлен $\delta - n + x_1^3 + \cdots + x_{n-1}^3 - (\delta - n + x_1 + \cdots + x_{n-1})^3$, где вещественный параметр δ удовлетворяет неравенству $|\delta| < \varepsilon$. В ε-окрестности точки $\mathbf{1}$ этот многочлен равен

$$\delta + 3\sum_{i=1}^{n-1}(x_i - 1)^2 + 3\left(\sum_{i=1}^{n-1}(x_i - 1)\right)^2 + O(\varepsilon^3).$$

При $\delta = 0$ точка $\mathbf{1}$ служит единственной особой точкой гиперповерхности $g = 0$. В этом случае точка $\mathbf{1}$ служит изолированной вещественной точкой гиперповерхности. При $\delta < 0$ около точки $\mathbf{1}$ появляется гладкая ориентируемая компонента связности. При $\delta > 0$ этой компоненты нет. Таким образом, если аффинная гиперплоскость отделяет одну вершину ± 1-куба от остальных, то соответствующая вещественная проективная гиперповерхность состоит из двух компонент связности. Если же гиперплоскость не пересекает ± 1-куб, то соответствующая вещественная проективная гиперповерхность связная.

Рассмотрим гиперповерхность, состоящую из двух компонент связности (при $\delta < 0$). Фиксируем точку U внутри области, ограниченной ориентируемой компонентой, и некоторую гиперплоскость $\mathcal{Y}$, не содержащую точку U. Прямая, проходящая через U, пересекает неориентируемую компоненту в одной точке V. Отображение, которое сопоставляет такой точке V точку пересечения прямой UV с $\mathcal{Y}$, служит гомеоморфизмом. При увеличении параметра δ неориентируемая компонента меняется непрерывно. Следовательно, она остаётся гомеоморфной гиперплоскости при $\delta > 0$. □

Замечание 1. Проективное преобразование объемлющего пространства, переставляющее вершины куба, не меняет число компонент связности гиперповерхности. Если гиперплоскость $h = 0$ отделяет все вершины некоторой грани, кроме одной из них, то вещественная проективная гиперповерхность $g = 0$ содержит ориентируемую компоненту.

Пример 1. Если аффинная гиперплоскость $h = 0$ разделяет две противоположные фасеты ± 1-куба, то вещественная проективная гиперповерхность $g = 0$ связная. Соответствующее проективное преобразование поворачивает бесконечно удалённую гиперплоскость так, чтобы в исходном аффинном пространстве она прошла посередине между этими фасетами. Если же $h = 0$ не пересекает одну из фасет и отделяет от противоположной фасеты ровно одну вершину, то вещественная проективная гиперповерхность $g = 0$ содержит ориентируемую компоненту.

Теорема 2. *Если аффинная плоскость $h = 0$ не инцидентна никакой вершине и не параллельна никакому ребру трёхмерного ± 1-куба, то она отделяет нечётное число вершин тогда и только тогда, когда вещественная проективная кубическая кривая $g = 0$ состоит из двух компонент связности.*

Пример 2. Рассмотрим форму $\alpha_0 x_0^3 + x_1^3 + x_2^3 - (\alpha_0 x_0 + x_1 + x_2)^3$, которая определяет проективную плоскую кривую и соответствует сечению трёхмерного ± 1-куба плоскостью, ортогональной диагонали. Сделаем линейную замену переменных $y_0 = (x_1 + x_2)/2$, $y_1 = \alpha_0 x_0$ и $y_2 = (x_1 - x_2)/2$. Тогда при $\alpha_0 \neq 0$ и $y_0 = 1$ аффинная кривая задана уравнением $6\alpha_0^2 y_2^2 = (\alpha_0^2 - 1)y_1^3 + 6\alpha_0^2 y_1^2 + 12\alpha_0^2 y_1 + 6\alpha_0^2$. Дискриминант многочлена в правой части равен $\Delta = -108\alpha_0^4(\alpha_0^4 - 10\alpha_0^2 + 9)$. Если выполнены неравенства $1 < |\alpha_0| < 3$, то $\Delta > 0$ и кривая состоит из двух компонент связности. Тогда аффинная плоскость $\alpha_0 + x_1 + x_2 + x_3 = 0$

отделяет одну вершину ± 1-куба от остальных. При $\Delta < 0$ кривая связная. Если $0 < \alpha_0 < 1$, то аффинная плоскость отделяет четыре вершины ± 1-куба от четырёх других. Если $\alpha_0 > 3$, то аффинная плоскость не пересекает ± 1-куб.

Замечание 2. Для $n = 4$ нечётность числа отделяемых вершин ± 1-куба не эквивалентна существованию ориентируемой компоненты у проективной поверхности $g = 0$.

Пример 3. Пусть $h = -\alpha + \frac{1}{2}x_1 + \frac{1}{2}x_2 + 3x_3 + x_4$. При $1 < \alpha < 2$ аффинная гиперплоскость $h = 0$ отделяет семь вершин ± 1-куба, проективная гиперповерхность $g = 0$ содержит ориентируемую компоненту. Однако при $\alpha = 3$ аффинная гиперплоскость $h = 0$ отделяет пять вершин ± 1-куба, а проективная гиперповерхность $g = 0$ связная.

Пример 4. Рассмотрим форму $x_0^3 + \cdots + x_{2m+1}^3 - (x_0 + \cdots + x_{2m+1})^3$, которая определяет $2m$-мерную проективную гиперповерхность $\mathcal{X}$. При $m = 1$ это диагональная поверхность Клёбша. На этой гиперповерхности лежат m-мерные линейные подпространства. Одно из них задано системой из $m + 1$ уравнения $x_0 = -x_1, \ldots, x_{2m} = -x_{2m+1}$. Другие получаются перестановками индексов. Поскольку на $\mathcal{X}$ лежат два скрещивающихся m-мерных линейных подпространства $\mathcal{Y}$ и $\mathcal{Z}$, эта гиперповерхность $\mathcal{X}$ рациональная над полем вещественных чисел. Сопоставляя двум точкам $V \in \mathcal{Y}$ и $W \in \mathcal{Z}$ третью точку пересечения проходящей через них прямой VW с гиперповерхностью $\mathcal{X}$, получим бирациональное отображение $\mathcal{Y} \times \mathcal{Z} \dashrightarrow \mathcal{X}$. Поскольку произведение линейных пространств $\mathcal{Y} \times \mathcal{Z}$ рационально, такова же и гиперповерхность $\mathcal{X}$. Если $\mathcal{X}$, $\mathcal{Y}$ и $\mathcal{Z}$ определены над полем вещественных чисел, то $\mathcal{X}$ рационально над полем вещественных чисел. С другой стороны, если вещественная гиперповерхность $\mathcal{X}$ состоит из двух компонент связности, то на ней не могут лежать два вещественных скрещивающихся линейных подпространства размерности m каждая. Оба эти подпространства должны лежать на неориентируемой компоненте. Тогда общая прямая, пересекающая эти два подпространства, пересекает ориентируемую компоненту в чётном числе точек. Но бирациональное отображение должно быть взаимно однозначным в общей точке. Следовательно, ориентирумой компоненты нет. Этот случай соответствует разбиению множества вершин $(2m + 2)$-мерного ± 1-куба на два множества, каждое из которых содержит чётное число вершин.

Литература

1. *Балицкий А. М., Савчик А. В., Гафаров Р. Ф., Коноваленко И. А.* О проективно инвариантных точках овала с выделенной внешней прямой // Проблемы передачи информации. 2017. Т. 53, № 3. С. 84—89.
2. *Дурнев В. Г., Зеткина О. В., Зеткина А. И., Мурин Д. М.* О coNP-полноте задачи «Инъективный рюкзак» // Прикладная дискретная математика. 2016. № 3 (33). С. 85—92.
3. *Малашонок Г. И.* Система компьютерной алгебры MathPartner // Программирование. 2017. № 2. С. 63—71.
4. *Прасолов В. В., Соловьев Ю. П.* Эллиптические функции и алгебраические уравнения. М. : Факториал, 1997. 288 с.
5. *Селиверстов А. В.* Кубические формы без мономов от двух переменных // Вестник Удмуртского университета. Математика. Механика. Компьютерные науки. 2015. Т. 25, № 1. С. 71—77.
6. *Хейфец А. Л.* Коники как сечения квадрик плоскостью (обобщенная теорема Данделена) // Геометрия и графика. 2017. Т. 5, № 2. С. 45—58.
7. *González-Sánchez J., Polo-Blanco I.* Construction algorithms for rational cubic surfaces // Journal of Symbolic Computation. 2017. Vol. 79. P. 309—326.
8. *Plaumann D., Sinn R., Speyer D. E., Vinzant C.* Computing Hermitian determinantal representations of hyperbolic curves // International Journal of Algebra and Computation. 2015. Vol. 25, № 8. P. 1327—1336.
9. *Polo-Blanco I., Top J.* A remark on parameterizing nonsingular cubic surfaces // Computer Aided Geometric Design. 2009. Vol. 26, № 8. P. 842—849.
10. *Safey El Din M., Schost É.* A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets // Journal of the ACM. 2017. Vol. 63, № 6. Article 48. 37 p.
11. *Seliverstov A. V.* On cubic hypersurfaces with involutions // International Conference Polynomial Computer Algebra'2016, Russian Academy of Sciences, St. Petersburg Department of Steklov Mathematical Institute, Euler International Mathematical Institute / Ed. by N. N. Vassiliev. Санкт-Петербург : Издательство ВВМ, 2016. С. 74—77. URL: http://elibrary.ru/item.asp?id=26437524
12. *Torrance D. A.* Generic forms of low Chow rank // Journal of Algebra and Its Applications. 2017. Vol. 16, № 3. Article 1750047. 10 p.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ОБ ОПТИМИЗАЦИИ УМНОЖЕНИЯ ТОЧКИ НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

К. М. Туленбаев (Алматы, Казахстан)[1], Ұ. Э. Оспанова (Алматы, Казахстан)[2]

Эллиптическая криптография — раздел криптографии, который изучает асимметричные криптосистемы, основанные на эллиптических кривых над конечными полями. Основное преимущество эллиптической криптографии заключается в том, что на сегодняшний день не известно существование субэкспоненциальных алгоритмов решения задачи дискретного логарифмирования. Использование эллиптических кривых для создания криптосистем было независимо предложено Нилом Коблицем (*англ.*) и Виктором Миллером (*англ.*) в 1985 году.

Особый интерес к криптографии эллиптических кривых обусловлен теми преимуществами, которые дает её применение в беспроводных коммуникациях — высокое быстродействие и небольшая длина ключа [1]. Асимметричная криптография основана на сложности решения некоторых математических задач. Ранние криптосистемы с открытым ключом, такие как алгоритм RSA, криптостойки благодаря тому, что сложно разложить составное число на простые множители. При использовании алгоритмов на эллиптических кривых полагается, что не существует субэкспоненциальных алгоритмов для решения задачи дискретного логарифмирования в группах их точек.

Арифметические операции с точками на эллиптической кривой не эквивалентны этим арифметическим операциям с их координатами. Точки эллиптической кривой над конечным полем представляют собой группу. Умножение сводится к многократным удвоению и суммированию [2].

Например, $G+G \neq 2G$ (это разные операции), $2G+2^{115G} = 2^{115G}+2G$ (суммирование коммутативно);

$2G = 2 \cdot G$; $4G = 2 \cdot 2G$; $8G = 2 \cdot 4G$; $16 \cdot G = 2 \cdot 8G$, и т. д. (для двух одинаковых точек — только операция удвоения);

$25 \cdot G$; $25 = 11001$ (in binary); $25 = 1 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 = 1 + 8 + 16$; $25G = 16G + 8G + G = 1 \cdot (2^4)G + 2 \cdot (2^3)G + 1 \cdot G$ (операция суммирования);

$24G/3G = 24G \cdot (3G^{-1} \bmod P)$; $5G - 3G = 5G + (3G^{-1} \bmod P)$; где $3G^{-1} \bmod P$ — modular multiplicative inverse.

Пусть E — эллиптическая кривая, определенная над конечным полем F_q, и O — точка на бесконечности [3]. Рассмотрим эндоморфизм $\varphi : E \to E$, удовлетворяющий условию $\varphi(O) = O$. Мы находим представление $kG = k_1G + k_2\varphi(G)$, что позволяет улучшить алгоритм дешифровки.

Литература

1. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. М. : МЦНМО, 2003.
2. *Koblitz N.* CM-curves with good cryptographic properties // In: Feigenbaum J. (eds). Advances in Cryptology – CRYPTO '91. CRYPTO 1991. Lecture Notes in Computer Science. Vol. 576. Berlin, Heidelberg : Springer, 1992. P. 279—287.
3. *Gallant R. P., Lambert R. J., Vanstone S. A.* Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms // In: Kilian J. (eds). Advances in Cryptology – CRYPTO 2001. CRYPTO 2001. Lecture Notes in Computer Science. Vol. 2139. Berlin, Heidelberg : Springer, 2001. P. 190—200.

 Получено 14.01.2018. УДК 512.542.

[1]Университет им. Сулеймана Демиреля. E-mail: tulen75@hotmail.com.
[2]Институт математики и математического моделирования МОН РК. E-mail: ulzhan.ospanova.93@mail.ru.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

НАДЕЖНОСТЬ МЕТОДА ФРОБЕНИУСА ПРОВЕРКИ ЧИСЕЛ НА ПРОСТОТУ[1]

С. И. Хашин (Иваново)[2]

1. Введение

Чаще всего проверку чисел на простоту выполняют с помощью методов, основанных на малой теореме Ферма: методы Миллера–Рабина, Соловея–Штрассена. Надежность этих методов недостаточна. Например, в [12] найдены 24- и 25-значные числа, проходящие 12 и 13 тестов Миллера–Рабина. В дополнение к этому часто используется метод Лукаса [4]. Это радикально усиливает надежность проверки, но математическое исследование совместного использования различных методов затруднительно.

Метод Фробениуса основан на автоморфизме Фробениуса поля $GF(p^2)$ для простого p. Он известен уже довольно давно ([5, 6, 8, 9] etc.). В работе ([6, 11]) приводится даже некоторое его усиление. Но до сегодняшнего дня не известен ни один контрпример даже к его простейшей версии. Правда, в книге [5, стр. 146] утверждается, что число $5777 = 53 * 109$ будет псевдопростым по Фробениусу при $c = 5$. Легко проверить, что это не так, по всей видимости, в этом месте книги термин «псевдопростые по Фробениусу» используется в несколько другом смысле.

Кроме того, в работе [6] доказана оценка сверху вероятности ошибки метода ($\approx 1/1300$). Это намного меньше оценки для метода Миллера–Рабина ($1/4$), но всё равно вероятность ошибки выглядит весьма значительной.

Всё это вместе взятое привело к тому, что метод Фробениуса оказался сильно недооценён. На самом деле на сегодняшний день нет ни одного контрпримера к этому методу и есть основания полагать, что их не существует вовсе.

Тест Фробениуса сводится к проверке некоторого равенства в квадратичном расширении кольца вычетов. Равенство норм соответствующих элементов эквивалентно тесту Ферма, а равенство иррациональных частей — тесту Люка. То есть тест Фробениуса является естественным объединением этих двух тестов.

Трудоёмкость теста Фробениуса в два раза больше трудоёмкости методов Ферма или Миллера–Рабина, то есть равна трудоёмкости двух таких проверок.

2. Основные результаты

Определение 1. Пусть n — нечетное натуральное число, не являющееся полным квадратом. Его индексом Фробениуса $Ind_F(n)$ будем называть наименьшее среди чисел $-1, 2, 3, 4, 5, 6, \ldots$ такое, что символ Якоби $jacobi(c/n) = -1$.

Из мультипликативности символа Якоби следует, что если индекс Фробениуса положителен, то он прост.

Определение 2. Пусть n — нечетное натуральное число, не являющееся полным квадратом и пусть c – его индекс Фробениуса, $c = Ind_F(n)$. Если $c \leq 2$, то положим $z = 2 + \sqrt{c}$, иначе $z = 1 + \sqrt{c}$.

Назовем число n простым по Фробениусу если

$$z^n \equiv \overline{n} \mod n.$$

 Получено 12.01.2018. УДК 513.64.

[1]Работа выполнена при финансовой поддержке Министерства образования и науки РФ, проект № 1201456563.

[2]Ивановский государственный университет. E-mail: khash2@mail.ru.

Пример 1. Пусть $n = 19$. Тогда $c = -1$, $z = 2 + i$,

$$z^n = -3565918 + 2521451i \equiv 2 - i \mod n.$$

Пример 2. Пусть $n = 33$. Тогда $c = -1$, $z = 2 + i$,

$$z^n \equiv 2 + 22i \mod n \neq \overline{z}.$$

Пример 3. Пусть $n = 17$. Тогда $c = 3$, $z = 1 + \sqrt{3}$,

$$z^n = 13160704 + 7598336\sqrt{3} \equiv 1 - \sqrt{3} \mod n.$$

Нас интересуют случаи, когда этот метод ошибается.

Определение 3. Составное нечетное натуральное число n, не являющееся полным квадратом, назовем псевдопростым по Фробениусу (Frobenius pseudoprime, FPP), если оно просто по Фробениусу.

Гипотеза. Псевдопростых по Фробениусу чисел не существует!

Другими словами, тест Фробениуса никогда не ошибается.

Теорема 1. *Не существует чисел, меньших* 2^{64}*, псевдопростых по Фробениусу.*

Теорема 2. *Число, псевдопростое по Фробениусу, обязательно имеет простой делитель, больший* 478 831*.*

3. Выводы

- Метод Фробениуса — один из наиболее эффективных методов проверки простоты числа.
- Его трудоёмкость в два раза выше, чем у методов, основанных на теореме Ферма.
- Во сколько раз увеличивается надёжность, оценить не удается, так как нет ни одного примера, когда метод ошибается.
- Развитие методов, описанных в настоящей работе, может позволить поднять «безопасную» границу, например, до 2^{80}.
- Другой тип вычислительных экспериментов может позволить доказывать утверждения типа: «не существует FPP, представимых в виде произведения любого количества простых чисел, меньших N_0».

Литература

1. *Хашин С. И.* Кратные множители псевдопростых чисел // Вестник Ивановского государственного университета. Сер.: Естественные, общественные науки. 2013. Вып. 2. С. 102—107.
2. *Хашин С. И.* Натуральные числа с большим индексом Фробениуса // Вестник Ивановского государственного университета. Сер.: Естественные, общественные науки. 2015. Вып. 2. С. 75—78.
3. *Хашин С. И., Хашина Ю. А.* Свойства чисел, псевдопростых по Фробениусу // Вестник Ивановского государственного университета. Сер.: Естественные, общественные науки. 2014. Вып. 2. С. 104—108.
4. *Baillie R., Samuel S., Wagstaff Jr.* Lucas Pseudoprimes // Mathematics of Computation. Vol. 35, № 152. P. 1391—1417. DOI: 10.1090/S0025-5718-1980-0583518-6.
5. *Crandall R. E., Pomerance C.* Prime Numbers: A Computational Perspective (Second Edition). Springer-Verlag, 2005. 597 p.
6. *Damgard I. B., Frandsen G. S.* An Extended Quadratic Frobenius Primality Test with Average- and Worst-Case Error Estimate // Journal of Cryptology. 2006. Vol. 19, № 4. P. 489—520, DOI: 10.1007/s00145-006-0332-x
7. *Feitsma J.* Tables of pseudoprimes and related data. URL: http://www.cecm.sfu.ca/Pseudoprimes/index-2-to-64.html (дата обращения: 2017-10-01).
8. *Grantham J.* Frobenius pseudoprimes // Math. of Computation. Vol. 70, № 234. P. 873—891.
9. *Khashin S. I.* Counterexamples for Frobenius primality test // arXiv:1307.7920 [math.NT].
10. *Ribenboim P.* My numbers, my friends: popular lectures on number theory. 2nd ed. New York : Springer, 2000. 392 p. ISBN-10:0387989110.
11. *Seysen M.* A Simplified Quadratic Frobenius Primality Test // Cryptology ePrint Archive, 2005/462. URL: http://eprint.iacr.org/2005/462.pdf.
12. *Sorenson J., Webster J.* Strong Pseudoprimes to Twelve Prime Bases // arXiv:1509.00864 [math.NT].

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ПРЕДСТАВЛЕНИЕ БИКВАДРАТИЧНОЙ ФУНКЦИИ В ВИДЕ СУММЫ-РАЗНОСТИ КВАДРАТОВ

Ю. А. Хашина (Иваново)[1]

При решении некоторых задач компьютерной графики используются биквадратичные функции, то есть многочлены от двух переменных, квадратичные по каждой из них:

$$F = a_{22}x^2y^2 + 2a_{21}x^2y + 2a_{12}xy^2 + a_{20}x^2 + 2a_{11}xy + a_{02}y^2 + 2a_{10}x + 2a_{01}y + a_{00}$$

За последние годы был получен ряд результатов, касающихся биквадратичных функций [1, 2, 3, 4, 5, 6].

Биквадратичные функции часто возникают как суммы квадратов билинейных функций. Если биквадратичная функция может быть представлена в виде суммы нескольких полных квадратов билинейных, то с точностью до постоянного слагаемого ее можно представить в виде суммы не более трех таких слагаемых и неотрицательной константы [6].

Возникает вопрос о существовании подобного представления для произвольной биквадратичной функции.

Любая биквадратичная функция может быть представлена в виде суммы-разности квадратов билинейных функций, поскольку каждый ее моном может быть записан в таком виде. Желательно найти минимальное представление биквадратичной функции в виде суммы-разности квадратов билинейных функций.

Доказано:

(1) каждая биквадратичная функция с точностью до постоянного слагаемого может быть представлена в виде суммы-разности не более четырех квадратов;

(2) это представление минимально в том смысле, что существуют биквадратичные функции, не представимые с точностью до постоянного слагаемого виде суммы-разности меньшего числа квадратов билинейных функций.

Эти результаты могут быть использованы в работах по сжатию видео.

Литература

1. *Ерохина А. В.* Экстремумы биквадратичных функций: Дипломная работа. Иваново, 2015. 48 с.
2. *Кадочникова А. В.* Условия неотрицательности биквадратичной функции: Магистерская диссертация. Иваново, 2017. 33 с.
3. *Конопелько Е. А.* Минимум биквадратичной функции двух переменных: Магистерская диссертация. Иваново, 2006. 26 с.
4. *Косоурова Ю. А.* Достаточные условия отсутствия минимумов биквадратичной функции на единичном квадрате: Дипломная работа. Иваново, 2010. 32 с.
5. *Митрофанова М. К.* Каноническая форма биквадратного многочлена: Дипломная работа. Иваново, 2005. 100 с.
6. *Хашина Ю. А.* Биквадратичные функции и их представление в виде суммы квадратов // Вестник Ивановского государственного университета. Сер.: Естественные, общественные науки. 2017. Вып. 2. С. 36—42.

 Получено 14.01.2018. УДК 513.64.

[1]Ивановский государственный университет. E-mail: khashina_julia@mail.ru.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ОБ АНТИПОДАЛЬНЫХ ДИСТАНЦИОННО РЕГУЛЯРНЫХ ГРАФАХ ДИАМЕТРА ТРИ С ПРИМИТИВНОЙ ПОЧТИ ПРОСТОЙ АНТИПОДАЛЬНОЙ ГРУППОЙ[1]

Л. Ю. Циовкина (Екатеринбург)[2]

Пусть Γ — антиподальный дистанционно регулярный граф и $G \leq \mathrm{Aut}(\Gamma)$. Группу подстановок, индуцированную группой G на множестве антиподальных классов графа Γ, будем называть *антиподальной группой* графа Γ (относительно G).

В настоящей работе мы рассматриваем класс $\mathcal{C}$ антиподальных дистанционно регулярных графов диаметра 3, удовлетворяющих следующему свойству: полная группа автоморфизмов графа содержит подгруппу G такую, что G транзитивна на множестве его вершин и его антиподальная группа относительно G является примитивной и почти простой. Описание графов из $\mathcal{C}$ с транзитивными на дугах группами автоморфизмов завершено в [1]. Эти графы образуют весьма богатый класс, который помимо семейств дистанционно-транзитивных графов содержит еще четыре бесконечных семейства графов. В частности, каждый такой граф имеет 2-транзитивную антиподальную группу. Естественно возникает вопрос, насколько шире класс графов $\mathcal{C}$. То, что он действительно шире, подтверждается примерами двух графов Клина-Пеша с массивами пересечений $\{35, 24, 1; 1, 12, 35\}$ и $\{44, 24, 1; 1, 12, 44\}$, которые связаны с исключительным 3-накрытием группы A_6.

В работе найдены допустимые массивы пересечений графов из $\mathcal{C}$ и получены ограничения на группы автоморфизмов таких графов в следующих дополнительных предположениях: (1) ранг ассоциированной почти простой примитивной антиподальной группы графа не превосходит 5 и (2) число антиподальных классов графа не больше 2500.

Литература

1. *Махнев А. А., Падучих Д. В., Циовкина Л. Ю.* Реберно симметричные дистанционно регулярные накрытия полных графов: почти простой случай // Алгебра и логика, принято к печати.
2. *Brouwer A. E., Cohen A. M., Neumaier A.* Distance-regular graphs. Berlin etc. : Springer-Verlag, 1989.

 Получено 26.12.2017. УДК 519.17+512.54.

[1]Работа выполнена при финансовой поддержке РНФ, проект № 14-11 00061 П.

[2]Институт математики и механики им. Н. Н. Красовского УрО РАН. E-mail: l.tsiovkina@gmail.com.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

СВОЙСТВА ДИАГРАММ ХАССЕ ДОПУСТИМЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В. В. Швыров (Луганск, Украина)[1]

1. Введение

Допустимые последовательности возникают при изучении рядов Купиша полуцепных колец (см. [1]). Такие последовательности определяют много структурных свойств кольца, интересные результаты можно найти в работе [3].

Последовательности заданной длины n могут быть построены, если задан первый элемент последовательности c_1. Случаи, когда $c_1 \in \{1, 2, 3\}$, были рассмотрены в работе [4]. Количество всех допустимых последовательностей длины n, с начальным элементом k, будем обозначать $T(n, k)$.

Следуя работе [1], напомним определение допустимой последовательности.

Определение 1. Пусть A — полуцепное кольцо, $e_1, \ldots, e_n$ — множество базисных примитивных идемпотентов, $J = J(A)$ — радикал Джекобсона кольца A. Последовательность неразложимых проективных модулей $Ae_1, \ldots, Ae_n$ называется *рядом Купиша* кольца A. Если $Je_1 \neq 0$ и $c_i = c(Ae_i)$, где c_i — длина соответствующего модуля, тогда

$$Je_i \equiv Ae_{i-1}/J^{e_i-1}e_{i-1} \ (i = 2, \ldots, n),$$
$$Je_1 \equiv Ae_n/J^{e_1-1}e_n.$$

Откуда, имеем

$$2 \leq c_i \leq c_{i-1} + 1, i = 2, \ldots, n, \ c_1 \leq c_n + 1. \tag{1}$$

Любая последовательность, которая удовлетворяет таким неравенствам, называется *допустимой последовательностью*.

2. Комбинаторные свойства допустимых последовательностей

Обозначим через $T(n, k)$ — количество допустимых последовательностей длины n, таких что $c_1 = k$.

Предложения 1, 2 и 3 определяют комбинаторные свойства чисел $T_{n,k}$ (см. [4]).

Предложение 1. $T(n, 1) = C_{n-1}$.

Предложение 2. $T(n, 2) = C_n$.

Предложение 3. $T(n, 3) = C_{n+1} - C_n$.

Множество допустимых последовательностей, при заданных n и k, может быть естественным образом упорядочено при помощи следующего бинарного отношения.

Определение 2. Положим

$$S_{T(n,k)} = \{\alpha_1, \ldots, \alpha_{T(n,k)}\}$$

— множество всех допустимых последовательностей длины n, таких что $\alpha_i = a_{i,1}, \ldots, a_{i,n}$,

 Получено 25.12.2017. УДК 512.55.

[1]Луганский национальный университет им. Тараса Шевченко. E-mail: slsh@i.ua.

и $a_{i,1} = k$, для любого $i = 1, \ldots, T(n,k)$. Определим сумму допустимой последовательности α_i, как

$$S_{\alpha_i} = \sum_{j=1}^{n} a_{i,j}.$$

Положим, что $\alpha_i <_S \alpha_j$, если $S_{\alpha_i} < S_{\alpha_j}$, и последовательности α_i отличается от последовательности α_j только одним элементом $a_{i,x} \neq a_{j,x}$, $x \in 1, \ldots, n$.

Множество $(S_{T(n,k)}, <_S)$ является частично упорядоченным множеством. И мы можем построить диаграмму Хассе этого множества по отношению $<_S$.

Пример 1. Пусть $T(n,k) = T(4,1)$. По предложению 1, $T(4,1) = C_3 = 5$, следовательно, $S_{T(4,1)} = \{\alpha_1, \ldots, \alpha_5\}$, $\alpha_1 = (1,2,3,4)$, $\alpha_2 = (1,2,3,3)$, $\alpha_3 = (1,2,2,3)$, $\alpha_4 = (1,2,3,2)$, $\alpha_5 = (1,2,2,2)$. Соответственно, $S_{\alpha_1} = 10$, $S_{\alpha_2} = 9$, $S_{\alpha_3} = 8$, $S_{\alpha_4} = 8$, $S_{\alpha_5} = 7$.

Диаграмма Хассе множества (см. [2]) $(S_{T(4,1)}, <_S)$ будет иметь вид

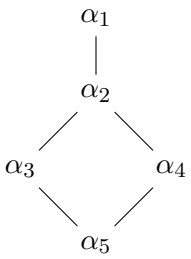

Рис. 1. Диграмма Хассе множества $S_{T(4,1)}$.

Пример 2. Положим, $T(n,k) = T(4,2)$. По предложению 2, $T(4,2) = C_4 = 14$, отсюда, $S_{T(4,2)} = \{\alpha_1, \ldots, \alpha_{14}\}$, $\alpha_1 = (2,3,4,5)$, $\alpha_2 = (2,3,4,4)$, $\alpha_3 = (2,3,3,4)$, $\alpha_4 = (2,3,4,3)$, $\alpha_5 = (2,2,3,4)$, $\alpha_6 = (2,3,3,3)$, $\alpha_7 = (2,3,4,2)$, $\alpha_8 = (2,2,3,3)$, $\alpha_9 = (2,3,2,3)$, $\alpha_{10} = (2,3,3,2)$, $\alpha_{11} = (2,2,2,3)$, $\alpha_{12} = (2,2,3,2)$, $\alpha_6 = (2,3,3,3)$, $\alpha_{13} = (2,3,2,2)$, $\alpha_{14} = (2,2,2,2)$.

Соответственно, $S_{\alpha_1} = 14$, $S_{\alpha_2} = 13$, $S_{\alpha_3} = S_{\alpha_4} = 12$, $S_{\alpha_5} = S_{\alpha_6} = S_{\alpha_7} = 11$, $S_{\alpha_8} = S_{\alpha_9} = S_{\alpha_{10}} = 10$, $S_{\alpha_{11}} = S_{\alpha_{12}} = S_{\alpha_{13}} = 9$, $S_{\alpha_{14}} = 8$.

Диаграмма Хассе множества $(S_{T(4,2)}, <_S)$ будет иметь вид

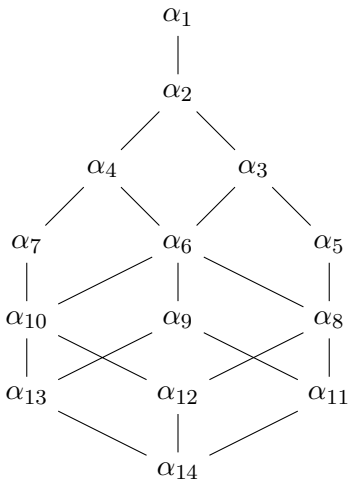

Рис. 2. Диаграмма Хассе множества $S_{T(4,2)}$.

Литература

1. *Anderson F. W., Fuller K. R.* Rings and Categories of modules. 2nd ed. Springer-Verlag, 1992. 385 p.
2. *Bondarenko V. M., Gubareni N. M., Dokuchaev M. A., Kirichenko V. V., Khibina M. A.* Representations of primitive posets. (Russian) // Fundam. Prikl. Mat. 2008. Vol. 14, № 6. P. 41—74; translation in J. Math. Sci. (N. Y.). 2010. Vol. 164, № 1. P. 26—48.
3. *Puninski G.* Serial Rings. Dordrecht, Boston, London : Kluwer Academic Publishers, 2001. 236 p.
4. *Shvyrov V. V.* On the number of admissible sequences for indecomposable serial rings with Noetherian diagonal // Bulletin of Taras Shevchenko National University of Kyiv. Ser. Physics & Math. 2014. № 1. P. 34—40.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

ФРАКТАЛЫ РОЗИ, ОБОБЩЕННОЕ КРУГОВОЕ УМНОЖЕНИЕ И УРАВНЕНИЯ В КОЛЬЦАХ[1]

А. В. Шутов (Владимир)[2]

Пусть $\{F_n\}$ — последовательность Фибоначчи, задаваемая соотношением $F_n = F_{n-1} + F_{n-2}$ и начальными условиями $F_1 = F_2 = 1$. Любое натуральное число N имеет жадное разложение по последовательности $\{F_n\}$. Данное разложение имеет вид

$$N = \sum \varepsilon_n(N) F_n,$$

где $\varepsilon_n(N)$ принимает значение 0 или 1, причем $\varepsilon_n(N)\varepsilon_{n+1}(N) = 0$. Матиясеич [4] ввел понятие кругового умножения Фибоначчи

$$N \circ M = \sum_k \sum_l \varepsilon_k(N)\varepsilon_l(M) F_{k+l}.$$

Введенная операция очевидно коммутативна. Также легко проверить, что она не является дистрибутивной относительно сложения. Кнут доказал, что данная операция является ассоциативной [7]. Альтернативное доказательство ассоциативности было получено в [5].

Обобщенные круговые умножения определяются следующим образом. Пусть $\{T_n\}$ — последовательность, определяемая рекуррентным соотношением

$$T_n = a_1 T_{n-1} + \ldots + a_{k-1} T_{n-k+1} + T_{n-k} \tag{1}$$

с целыми a_i, $1 \le i \le k-1$. При подходящем выборе начальных условий каждое натуральное число N допускает однозначное жадное разложение по последовательности (1):

$$N = \sum_{n=0}^{t(N)} \varepsilon_n(N) T_n, \tag{2}$$

в котором значения $\varepsilon_n(N)$ ограничены константой, зависящей только от вида рекуррентного соотношения (1). Жадность разложения (2) означает, что для любого k, $1 \le k \le t(N)$ выполняется неравенство

$$N - \sum_{n=k}^{t(N)} \varepsilon_n(N) T_n < T_k.$$

Обобщенное круговое умножение $\circ_z$ при этом определяется равенством

$$N \circ M = \sum_{k=0}^{t(N)} \sum_{l=0}^{t(M)} \varepsilon_k(N)\varepsilon_l(M) T_{k+l+z}.$$

Данное умножение вообще говоря уже не ассоциативно, но оказывается ассоциативным при фиксированной последовательности $\{T_n\}$ и достаточно больших z [6, 8]. Задача нахождения минимального z, при котором умножение $\circ_z$ ассоциативно, в настоящее время не решена.

Предположим, что коэффициенты a_i линейного рекуррентного соотношения (1) удовлетворяют неравенствам

$$a_1 \ge \ldots \ge a_{k-1} \ge 1.$$

В этом случае характеристическое уравнение

$$\lambda^k = a_1 \lambda^{k-1} + \ldots + a_{k-1}\lambda + 1 \tag{3}$$

 Получено 21.11.2017. УДК 511.

[1]Работа выполнена при финансовой поддержке РНФ, проект № 14-11-00433.

[2]Математический институт им. В. А. Стеклова РАН. E-mail: a1981@mail.ru.

имеет один вещественный корень, больший единицы и $k-1$ корней, по модулю меньших единицы. Пусть r и $2s$ — число вещественных и комплексных корней характеристического уравнения (ясно, что $r+2s=k$). Обозначим эти корни $\beta_1,\dots,\beta_r,\beta_{r+1},\overline{\beta_{r+1}},\dots,\beta_{r+s},\overline{\beta_{r+s}}$, причем $\beta_1>1$. Определим отображение $\Phi:\mathbb{N}\to\mathbb{Z}[\beta_2]\oplus\ldots\oplus\mathbb{Z}[\beta_{r+s}]$ равенством

$$\Phi(N)=\left(\sum_{n=0}^{t(N)}\varepsilon_n(N)\beta_2^{n+z},\dots,\sum_{n=0}^{t(N)}\varepsilon_n(N)\beta_{r+s}^{n+z}\right).$$

Множество

$$\mathcal{R}_z=\overline{\Phi(\mathbb{N})}$$

представляет собой замкнутое ограниченное множество на плоскости, называемое фракталом Рози. Более того, приведенные выше неравенства на коэффициенты a_i гарантируют, что $\mathcal{R}_z$ является фундаментальной областью некоторой решетки L_z.

Теорема 1. *Справедливы равенства*

$$\Phi(N+M)\equiv\Phi(N)+\Phi(M)\pmod{L_z},$$
$$\Phi(N\circ_z M)\equiv\Phi(N)\Phi(M)\pmod{L_z}.$$

Аналог отображения Φ впервые был построен Журавлевым в случае, когда $\{T_n\}$ является классической последовательностью Фибоначчи и $z=-1$ [1], который рассматривал аналоги классических диофантовых уравнений первой и второй степени, в которых обычное умножение заменяется круговым умножением Фибоначчи (см. также [2, 3]). Теорема 1 также позволяет получать результаты об уравнениях над множеством натуральных чисел с операциями $(\circ_z,+)$ на основе результатов об уравнениях в кольце $R=\mathbb{Z}[\beta_2]\oplus\ldots\oplus\mathbb{Z}[\beta_{r+s}]$ с дополнительными ограничениями в виде неравенств, накладываемыми на решения. Метод позволяет доказывать существование решений таких уравнений, а также получать нижние оценки, а в некоторых случаях и асимптотические формулы для числа решений. Отметим, что кольцо R не имеет делителей нуля ровно в двух случаях: 1) характеристистическое уравнение (3) имеет степень 2 и оба его корня — вещественные; 2) характеристистическое уравнение (3) имеет степень 3, причем оно имеет один действительный и два комплексных корня.

Введенное отображение Φ также позволяет получать результаты, связанные с ассоциативностью и дистрибутивностью обобщенных круговых умножений. Приведем два примера.

Пусть для $x=(x_2,\dots,x_{r+s})\in R=\mathbb{Z}[\beta_2]\oplus\ldots\oplus\mathbb{Z}[\beta_{r+s}]$ $||x||=\max\limits_{2\le i\le r+s}|x_i|$, где $|x_i|$ означает модуль действительного или комплексного числа.

Теорема 2. *Операция $\circ_z$ ассоциатина тогда и только тогда, когда для любого $x\in\mathcal{R}_z$ выполняется неравенство $||x||\le 1$.*

Теорема 3. *Для любого z существует подмножество $\mathbb{N}_z\subseteq\mathbb{N}$ положительной плотности, такое что для любых $N_1,N_2,N_3\in\mathbb{N}_z$ выполняются равенства*

$$(N_1\circ_z N_2)\circ_z N_3=N_1\circ_z(N_2\circ_z N_3),$$
$$(N_1+N_2)\circ_z N_3=N_1\circ_z N_3+N_2\circ_z N_3.$$

Отметим, что ассоциативность обобщенных круговых умножений $\circ_z$ при достаточно больших z является очевидным следствием теоремы 2 и определения фрактала Рози $\mathcal{R}_z$.

Для классического кругового умножения Фибоначчи справедлива явная формула

$$N\circ M=NM+[(N+1)\tau]M+[(M+1)\tau]N,$$

где $[\cdot]$ — целая часть числа и $\tau=\frac{\sqrt{5}-1}{2}$ [4]. Аналогичная формула для умножения Фибоначчи и $z=-1$ получена в [1]. Использование фракталов Рози позволяет получить общие формулы для кругового умножения для произвольных последовательностей $\{T_n\}$ и произвольных z.

Из общей теории фракталов Рози [9] вытекает, что существует каноническое разбиение

$$\mathcal{R}_z = \mathcal{R}_z(1) \sqcup \ldots \sqcup \mathcal{R}_z(k)$$

фрактала Рози $\mathcal{R}_z$ на k непересекающихся областей. Данное разбиение определяет перекладывание областей S, которое оказывается изоморфно сдвигу k-мерного тора на некоторый иррациональный вектор. Пусть

$$r_l(N) = \sharp\{i : 1 \le i \le N : S^i(0) \in \mathcal{R}_z(l)\}.$$

Теорема 4. *Справедливо равенство*

$$N \circ_z M = NM + \sum_{i=2}^{k} \sum_{j=2}^{k} c_{ij} r_i(N) r_j(M)$$

с целыми c_{ij}, зависящими от последовательности $\{T_n\}$ и числа z.

Литература

1. *Журавлев В. Г.* Суммы квадратов над $\circ$-кольцом Фибоначчи // Записки научных семинаров ПОМИ. 2006. Т. 337. С. 165—190.
2. *Журавлев В. Г.* Одномерные квазирешетки Фибоначчи и их приложения к диофантовым уравнениям и алгоритму Евклида // Алгебра и анализ. 2007. Т. 12, вып. 3. С. 151—182.
3. *Журавлев В. Г.* Уравнение Пелля над $\circ$-кольцом Фибоначчи // Записки научных семинаров ПОМИ. 2007. Т. 350. С. 139—159.
4. *Матиясевич Ю. В.* Связь систем уравнений в словах и длинах с 10-й проблемой Гильберта // Записки научных семинаров ЛОМИ. 1968. Т. 8. С. 132—144.
5. *Arnoux P.* Some remarks about Fibonacci multiplication // Appl. Math. Lett. 1989. Vol. 2, № 4. P. 319—320.
6. *Grabner P. J., Pethõ A., Tichy R. F., Woeginger G. J.* Associativity of recurrence multiplication // Appl. Math. Lett. 1994. Vol. 7, № 4. P. 85—90.
7. *Knuth D.* Fibonacci Multiplication // Appl. Math. Lett. 1988. Vol. 1, № 2. P. 3—6.
8. *Messaoudi A.* Tribonacci Multiplication // Appl. Math. Lett. 2002. Vol. 15, № 8. P. 981—985.
9. *Pytheas Fogg N.* Substitutions in dynamics, arithmetics and combinatorics. Berlin : Springer, 2001. 404 p.

Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

О ДОСТАТОЧНЫХ УСЛОВИЯХ КОНЕЧНОЙ ПОРОЖДЕННОСТИ АППРОКСИМАЦИОННЫХ АЛГЕБР КОНЕЧНЫХ ВЕРОЯТНОСТНЫХ РАСПРЕДЕЛЕНИЙ[1]

А. Д. Яшунский (Москва)[2]

1. Введение

В математической кибернетике достаточно давно рассматриваются задачи о получении случайных величин с требуемыми распределениям путем применения детерминированных (не случайных) функций к независимым случайным величинам, распределения которых принадлежат некоторому заданному множеству. Также рассматривается задача аппроксимации случайных величин: получение случайной величины, распределение которой сколь угодно близко к требуемому распределению. По-видимому, наиболее ранние результаты для такой постановки получены в работе Р. Л. Схиртладзе [1]. Относительно недавно задача была «переоткрыта» в работе Х. Жоу, П. Ло и Дж. Брака [5], где были независимо получены результаты работы [1], а также некоторые результаты из [2].

Указанные задачи можно достаточно естественно сформулировать в терминах порождения некоторых алгебр с заданной сигнатурой (подробнее см. определения ниже).

В работах [1, 2, 5] рассматриваются бернуллиевские случайные величины (т. е. величины, принимающие только два значения). Основным результатом в этом случае оказывается возможность сколь угодно точно приблизить произвольную случайную величину при любом невырожденном распределении заданных случайных величин, используя при этом достаточно простую систему операций.

При рассмотрении случайных величин с произвольным конечным множеством значений построение подобных алгебраических систем, позволяющих произвольные аппроксимации, оказывается уже нетривиальным. В данной работе рассматриваются некоторые достаточные условия, при которых возможна аппроксимация произвольного распределения.

2. Основные определения

Пусть X — случайная величина со значениями в множестве $E_k = \{0, 1, \dots, k-1\}$. Тогда ее распределение есть вектор $\mathbf{p} = (p_0, \dots, p_{k-1})$, компоненты которого удовлетворяют условиям $\sum p_i = 1$ и $p_i \geqslant 0, i = 0, \dots, k-1$. Такие вектора, называемые *стохастическими*, образуют в $\mathbb{R}^k$ симплекс, который будем обозначать $\mathbf{S}^{(k)}$. *Носителем* вектора $\mathbf{p} \in \mathbf{S}^{(k)}$ будем называть множество $N(\mathbf{p}) = \{i \in E_k \mid p_i > 0\}$.

Пусть B — некоторое множество операций на E_k, тогда $\langle E_k, B\rangle$ — некоторая конечная алгебра. Если $f(x_1, \dots, x_n) \in B$ — n-арная операция и $X_1, \dots, X_n$ — независимые в совокупности случайные величины со значениями в E_k, с распределениями $\mathbf{p}^1, \dots, \mathbf{p}^n \in \mathbf{S}^{(k)}$ соответственно, то $f(X_1, \dots, X_n)$ есть также случайная величина со значениями в E_k и для ее распределения $\mathbf{q} = (q_0, \dots, q_{k-1}) \in \mathbf{S}^{(k)}$ выполнено

$$q_i = \sum_{\substack{(\sigma_1,\dots,\sigma_n):\\ f(\sigma_1,\dots,\sigma_n)=i}} p^1_{\sigma_1} \cdots p^n_{\sigma_n}.$$

Таким образом, каждая n-арная операция $f \in B$ индуцирует полилинейное отображение

 Получено 23.12.2017. УДК 519.7, 512.57.

[1]Работа выполнена при финансовой поддержке Программы Президиума РАН № 01 «Фундаментальная математика и ее приложения» (грант PRAS–18–01).

[2]Институт прикладной математики им. М. В. Келдыша РАН. E-mail: yashunsky@keldysh.ru.

$\hat{f} : (\mathbf{S}^{(k)})^n \to \mathbf{S}^{(k)}$. Обозначим $\hat{B} = \{\hat{f} \mid f \in B\}$, тогда $\langle \mathbf{S}^{(k)}, \hat{B}\rangle$ есть *алгебра вероятностных распределений, индуцированная алгеброй* $\langle E_k, B\rangle$.

Пусть $\langle H, \hat{B}\rangle$ — подалгебра алгебры $\langle \mathbf{S}^{(k)}, \hat{B}\rangle$. Если множество H содержит все свои предельные точки, то $\langle H, \hat{B}\rangle$ будем называть *аппроксимационной алгеброй*.

Для произвольного $G \subseteq \mathbf{S}^{(k)}$ положим $W_B(G) = \cap H$, где пересечение берется по всем таким H, что $G \subseteq H$ и $\langle H, \hat{B}\rangle$ — аппроксимационная алгебра. Очевидно, что $\langle W_B(G), \hat{B}\rangle$ — также подалгебра в $\langle \mathbf{S}^{(k)}, \hat{B}\rangle$; будем называть ее *аппроксимационной алгеброй, порожденной множеством* G.

В случае, когда множество G состоит из единственного элемента $\mathbf{p}$, будем опускать фигурные скобки, записывая просто $W_B(\mathbf{p})$.

3. Результаты

Будем говорить, что терм над сигнатурой B является *бесповторным*, если каждая переменная встречается в нем не более одного раза. Сигнатуру, состоящую из всевозможных функций, определяемых бесповторными термами над B, будем обозначать $[B]_0$. Несложно доказать следующее утверждение.

Лемма 1. *Для любого* $G \subseteq \mathbf{S}^{(k)}$ *и любой сигнатуры* B *выполнено* $W_B(G) = W_{[B]_0}(G)$.

Аппроксимационные алгебры, индуцированные гомоморфными алгебрами, связаны между собой. Эта связь описывается следующим почти очевидным утверждением.

Лемма 2 (о гомоморфизме, [4])**.** *Пусть* φ *— гомоморфизм алгебры* $\langle E_k, B\rangle$ *в алгебру* $\langle E_r, B'\rangle$. *Определим* $\hat{\varphi}(\mathbf{p}) : \mathbf{S}^{(k)} \to \mathbf{S}^{(r)}$, *положив* $(\hat{\varphi}(\mathbf{p}))_j = \sum\limits_{i:\varphi(i)=j} p_i$. *Тогда имеет место равенство* $\{\hat{\varphi}(\mathbf{q}) \mid \mathbf{q} \in W_B(\mathbf{p})\} = W_{B'}(\hat{\varphi}(\mathbf{p}))$.

Основным результатом данной работы является следующая теорема, дающая достаточные условия для выполнения равенства $W_B(\mathbf{p}) = \mathbf{S}^{(k)}$. С учетом леммы 1 она формулируется в виде условий на множество функций $[B]_0$.

Теорема. *Пусть алгебра* $\langle E_k, B\rangle$ *такова, что* $[B]_0$ *содержит:*

1) 0*-арные функции* $0, 1, \ldots, k-1$;
2) *квазигрупповую на* E_k *бинарную операцию* $+$;
3) *бинарную операцию* $\times$, *такую что для любого* $i \in E_k$ *выполнено* $0 \times i = 0$, *кроме того,* $1 \times 0 = 0$, $1 \times 1 = 1$, *и* $|\{1 \times i \mid i \in E_k\}| = k$;
4) *функцию* $f(x)$, *принимающую ровно два значения:* 0 *и* 1.

Тогда для любого такого $\mathbf{p}$, *что* $N(\mathbf{p}) = E_k$, *выполнено* $W_B(\mathbf{p}) = \mathbf{S}^{(k)}$.

Доказательство. Покажем сначала, что в условиях теоремы $[B]_0$ содержит такую функцию $g(x)$, что $g(0) = 1$, $g(1) = 0$. Поскольку функция $f(x) \in [B]_0$ принимает значение 1, а операция $+ \in [B]_0$ является квазигрупповой, найдется такое $a \in E_k$, что $f(a+0) = 1$. Кроме того, поскольку f также принимает значение 0, найдется такое $b \in E_k$, что $f(a+b) = 0$. Поскольку $1 \times i$ принимает все возможные k значений, найдется такое $c \in E_k$, что $1 \times c = b$. Положим $g(x) = f(a + (x \times c))$. Тогда $g \in [B]_0$, и в силу выбора $a, c \in E_k$, а также свойств операции $\times$ выполнено $g(0) = 1$, $g(1) = 0$.

Тогда алгебра $\langle \{0,1\}; \times, g\rangle$ изоморфна алгебре $\langle \{0,1\}; \&, \neg\rangle$. Заметим, что $N(\hat{f}(\mathbf{p})) = \{0,1\}$. Положим $\mathbf{g} = ((\hat{f}(\mathbf{p}))_0, (\hat{f}(\mathbf{p}))_1) \in \mathbf{S}^{(1)}$. Тогда, используя лемму о гомоморфизме и равенство $W_{\{\&,\neg\}}(\mathbf{g}) = \mathbf{S}^{(1)}$ при $N(\mathbf{g}) = \{0,1\}$ (см. [2, 3]), получаем:

$$G = \{\mathbf{q} \mid N(\mathbf{q}) = \{0,1\}\} = W_{\{\times, g\}}(\hat{f}(\mathbf{p})) \subseteq W_{\{\times, g, f\}}(\mathbf{p}) \subseteq W_B(\mathbf{p}).$$

Для всех распределений из $\mathbf{q} \in \mathbf{S}^{(k)}$ покажем индукцией по $|A|$, $A = N(\mathbf{q})$, что $\mathbf{q} \in W_B(\mathbf{p})$. В силу $0, 1, \ldots, k-1 \in B$ в случае $|A| = 1$ утверждение верно.

Рассмотрим теперь распределения с носителем A, $|A| > 1$ и пусть для всех таких $\mathbf{t}$, что $|N(\mathbf{t})| < |A|$ выполнено $\mathbf{t} \in W_B(\mathbf{p})$.

Пусть $i \in A$, тогда существует такое $i' \in E_k$, что $i = i' + 0$. Положим

$$A' = \{j \mid i' + (1 \times j) \in A \setminus \{i\}\} \subset E_k.$$

Тогда из условия $|\{1 \times j \mid j \in E_k\}| = k$ вытекает $|A'| = |A| - 1$. В силу предположения индукции $H = \{\mathbf{t} \mid N(\mathbf{t}) = A'\}$ лежит в $W_B(\mathbf{p})$.

Пусть $\hat{\times}$ — операция на распределениях, индуцированная $\times$, а $\hat{+}$ — операция, индуцированная $+$. Рассмотрим множество $I = \{\mathbf{q}\hat{\times}\mathbf{t} \mid \mathbf{q} \in G, \mathbf{t} \in H\} \subseteq W_B(\mathbf{p})$. Несложно убедиться, что I состоит в точности из всех распределений с носителем $\{0\} \cup \{1 \times j \mid j \in A'\}$.

Пусть для распределения $\mathbf{e}$ выполнено $N(\mathbf{e}) = i'$, тогда по условию теоремы $\mathbf{e} \in W_B(\mathbf{p})$. Рассмотрим множество распределений $J = \{\mathbf{e}\hat{+}\mathbf{s} \mid \mathbf{s} \in I\} \subseteq W_B(\mathbf{p})$. В силу определения множества A' и равенства $i' + 0 = i$ множество J содержит всевозможные распределения с носителем A. Шаг индукции завершает доказательство. □

Доказанная теорема позволяет легко установить равенство $W_B(\mathbf{p}) = \mathbf{S}^{(k)}$ для некоторых алгебраических систем. В частности, имеют место следствия.

Следствие 1. *Пусть k — степень простого числа и $B = \{0, \ldots, k-1, +, \times, x^2, \ldots, x^{k-1}\}$, где сложение и умножение осуществляются* (mod k). *Тогда для любого такого $p \in \mathbf{S}^{(k)}$, что $N(\mathbf{p}) = E_k$, выполнено $W_B(\mathbf{p}) = \mathbf{S}^{(k)}$.*

Следствие 2. *Пусть k — степень простого числа и B — множество многочленов* (mod k). *Тогда для любого такого $p \in \mathbf{S}^{(k)}$, что $N(\mathbf{p}) = E_k$, выполнено $W_B(\mathbf{p}) = \mathbf{S}^{(k)}$.*

Следствие 3. *Пусть k — степень простого числа и B — множество многочленов над конечным полем порядка k. Тогда для любого такого $p \in \mathbf{S}^{(k)}$, что $N(\mathbf{p}) = E_k$, выполнено $W_B(\mathbf{p}) = \mathbf{S}^{(k)}$.*

Литература

1. *Схиртладзе Р. Л.* О методе построения булевой случайной величины с заданным распределением вероятностей // Дискретный анализ: сборник научных трудов. Новосибирск : Институт математики СО АН СССР. 1966. Вып. 7. С. 71—80.
2. *Яшунский А. Д.* О преобразованиях вероятности бесповторными булевыми формулами // Материалы XVI Международной школы-семинара «Синтез и сложность управляющих систем», Санкт-Петербург, 26—30 июня 2006 г. М. : Изд-во механико-математического факультета МГУ, 2006. С. 150—155.
3. *Яшунский А. Д.* Преобразования бернуллиевских распределений булевыми функциями из замкнутых классов // Препринты ИПМ им. М. В. Келдыша. 2016. № 38. 23 с. doi:10.20948/prepr-2016-38 URL: http://library.keldysh.ru/preprint.asp?id=2016-38 (дата обращения: 15.12.2017).
4. *Яшунский А. Д.* Конечные системы операций для аппроксимации дискретных вероятностных распределений // Препринты ИПМ им. М. В. Келдыша. 2017. № 10. 7 с. doi:10.20948/prepr-2017-10 URL: http://library.keldysh.ru/preprint.asp?id=2017-10 (дата обращения: 15.12.2017).
5. *Zhou H., Loh P., Bruck J.* The synthesis and analysis of stochastic switching circuits // arXiv:1209.0715 [cs.IT]. URL: https://arxiv.org/abs/1209.0715v1 (дата обращения: 15.12.2017).