УДК 512.54

ОБ АЛГОРИТМИЧЕСКИХ ПРОБЛЕМАХ ТЕОРИИ ГРУПП

В. А. Романьков
Омский государственный университет им. Ф. М. Достоевского, г. Омск, Россия

Информация о статье
Дата поступления
28.02.2017

Дата принятия в печать
04.04.2017

Дата онлайн-размещения
15.07.2017

Ключевые слова
Алгоритмическая проблема, уравнение, сложность

Финансирование
Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 16-01-00577

Аннотация. Дается обзор направлений исследования и результатов алгоритмического характера, освещенных в обзорной статье «Теоретико-модельные и алгоритмические вопросы теории групп» В.А. Романькова и В. Н. Ремесленникова, вышедшей в серии «Итоги науки и техники» в 1983 г. (Москва: ВИНИТИ), оценка этой статьи на основе последующих исследований. Приводится ряд результатов по решению алгоритмических проблем, полученных за последние годы. Показываются изменения в направлении алгоритмических исследований в теории групп.

ON ALGORITHMIC PROBLEMS IN GROUP THEORY

V. A. Roman'kov
Dostoevsky Omsk State University, Omsk, Russia

Article info
Received
28.02.1017

Accepted
04.04.2017

Available online
15.07.2017

Keywords
Algorithmic problem, equation, complexity

Acknowledgements
The reported study was funded by RFBR according to the research project № 16-01-00577

Abstract. We give a survey of research directions and results of algorithmic nature, that was presented in the survey "Model-theoretic and algorithmic questions in group theory" by the V. A. Roman'kov and V. N. Remeslennikov that appeared in the series "Itogi nauki i techniki" in 1983 (Moscow: VINITI). We estimate this survey basing on the further investigations. A number of results concerning algorithmic problems are given, that have been obtained during last years. We demonstrate changes in direction of algorithmic research in group theory.

Введение

Осознание алгебраической природы многих важных понятий топологии и теории функций привело в 80-е гг. XIX столетия к формированию комбинаторной теории групп. Группы, уже фигурировавшие в работах Ф. Клейна, А. Пуанкаре и других математиков, обрели право на самостоятельность после открытия В. фон Диком в 1882 г. универсального способа их определения через порождающие элементы и определяющие соотношения. В 1892 г. Пу-

ISSN 1812-3996

анкаре ввел в рассмотрение фундаментальные группы многообразий, в то же время выделились как эффективные объекты конечно определенные группы конечных симплициальных комплексов. Оказалось, что многие важные задачи топологии имеют алгоритмический характер. В самом начале XX столетия были сформулированы основные алгоритмические проблемы для класса конечно определенных групп:

Проблема равенства (Ден, 1910 г.). *Существует ли алгоритм, выясняющий по двум произвольным групповым словам от порождающих элементов группы, определяют ли они один и тот же элемент группы?*

Проблема изоморфизма (Титце, 1908 г.). *Существует ли алгоритм, выясняющий по двум произвольным конечным заданиям групп через порождающие элементы и определяющие соотношения, определяют ли эти задания изоморфные группы?*

Отметим некоторые другие алгоритмические проблемы:

Проблема сопряженности (Ден). *Существует ли алгоритм, выясняющий по двум произвольным групповым словам от порождающих элементов группы, определяют ли они сопряженные между собой элементы группы?*

Проблема вхождения (Нильсен, Магнус). *Существует ли алгоритм, выясняющий по групповому слову g и конечному набору групповых слов $h_1, \dots, h_n$ от порождающих элементов группы, входит ли элемент, заданный g, в подгруппу, порожденную элементами, заданными $h_1, \dots, h_n$?*

Проблема автоморфной сопряженности (Уайтхед). *Существует ли алгоритм, выясняющий по двум произвольным групповым словам от порождающих элементов группы, определяют ли они автоморфно сопряженные между собой элементы группы?*

Другими словами, существует ли автоморфизм группы, переводящий один из заданных элементов в другой?

Тридцать четыре года назад автор настоящей публикации совместно с В. Н. Ремесленниковым опубликовал обзорную статью [1], посвященную алгоритмическим и теоретико-модельным вопросам теории групп. Статья получила широкое распространение, в издательстве «Шпрингер» вышла переводная версия на английском языке. Целью обзора было дать достаточно полное описание теоретико-групповых результатов алгоритмического характера в их историческом развитии, а также представить методы теоретико-модельных исследований в теории групп. Эти два направления исследований имеют тесную взаимосвязь и общую ориентацию, поскольку стремятся ответить на один вопрос общего характера: какие свойства и характеристики групп эффективно определимы? Ряд аспектов такого исследования был отражен в работах [2] и [3].

Содержание обзоров [1] и [2] во многом объясняется значительно возросшим в то время интересом к исследованиям в комбинаторной теории групп. Эта область окончательно сформировалась в 60–70-е гг. XX столетия. Значительную роль в ее становлении сыграли ставшие впоследствии классическими монографии В. Магнуса, А. Карраса и Д. Солитера [4] и Р. Линдона и П. Шуппа [5] под одинаковым названием «Комбинаторная теория групп» (в названии монографии Магнуса, Карраса и Солитера еще добавлено: «Представление групп в терминах образующих и соотношений»). В этих монографиях были заложены основы комбинаторной теории групп как одной из самых активно развивающихся областей теории групп и математики в целом в последующие десятилетия, вплоть до нашего времени. Обе монографии были переведены на русский язык и впоследствии не раз переиздавались. Книга Магнуса [4] сконцентрирована на представлениях групп в терминах порождающих элементов и определяющих соотношений. В ней рассматривались свободные конструкции: свободные группы и произведения, свободные произведения с объединением, HNN-расширения. Сам термин «комбинаторная» возник из-за частого и существенного использования комбинаторных методов. В монографии были затронуты алгоритмические проблемы, начиная с классических проблем Дена и заканчивая проблемами, тогда только появившимися. Значение этой книги для дальнейшего развития комбинаторной теории групп очень велико. Это и учебник, и источник проблем, и образец исследования.

В монографии Линдона и Шуппа [5] основное место заняли геометрические методы исследования. Наряду с рассмотрением свободных конструкций групп им посвящена значительная часть книги. Теория малых сокращений впервые получила в этой книге достаточно полное описание. Также были затронуты многочисленные алгоритмические проблемы и вопросы, связанные с разрешимостью уравнений в группах.

Оценивая роль обзора [1] с позиций настоящего времени, следует заметить, что он до сих пор не утратил своей актуальности. С одной стороны, в

ISSN 1812-3996

нем были представлены и оценены предшествовавшие результаты в их историческом развитии, с другой – в обзоре был поставлен ряд важных, с точки зрения авторов, проблем, часть из которых нашла решения, а часть осталась открытой до сих пор. Полезно также проследить (хотя бы в общих чертах), как менялась направленность исследований в данной области в последующие годы. Что появилось нового в постановке задач и подходах к их решению. Именно этому посвящен настоящий, достаточно краткий для такой темы обзор, в котором только намечаются контуры более фундаментального исследования. Обзор не претендует на исчерпывающую полноту представления результатов. В основном внимание автора сконцентрировано на важных, с его точки зрения, направлениях. Приведена сравнительно небольшая часть результатов алгоритмического характера. Выбор объясняется интересами автора.

1. Решенные и нерешенные проблемы

Конечно определенные группы

Основные алгоритмические проблемы для класса всех конечно определенных групп к моменту выхода обзора [1] были решены отрицательно. В обзоре был выделен выдающийся результат работы П.С. Новикова, который в 1952 г. установил, что существуют конечно определенные группы с неразрешимой проблемой равенства, и таким образом открыл новый этап развития теории. Отмечены другие результаты Новикова, а также результаты С.И. Адяна, в том числе его теорема о неразрешимости проблемы изоморфизма. Приведена теорема Адяна о нераспознаваемости Марковских свойств, к получению которой независимо пришел М. Рабин (сейчас обычно говорят о теореме Адяна – Рабина). Приведены результаты В. Буна, Д. Бриттона, Д. Коллинза и др. В основном они фиксируют различные неразрешимые алгоритмические проблемы. Блок представленных в обзоре разрешимых проблем связан в основном с условиями малого сокращения (см. далее).

В обзорной статье [1] также рассматриваются характеризации групп с разрешимой проблемой равенства и вопросы сложности алгоритмов, формулируемой на языке рекурсивных функций. Знаменательно, что уже в этом обзоре была сформулирована проблема построения реальных алгоритмов (Проблема 3), имеющая в наше время первостепенное значение (см. следующий раздел).

Из проблем, не решенных до сих пор, отметим проблему о минимальном числе соотношений в конечно определенной группе с неразрешимой проблемой равенства (Проблема 1) и проблему изоморфизма для групп с одним соотношением (Проблема 5). Напомним, что известный алгоритм Магнуса решает проблему равенства в группе с одним соотношением. Известны примеры конечно определенных групп с неразрешимой проблемой равенства, заданных двенадцатью соотношениями (примеры Борисова). Но это все было уже известно до написания обзора [1], принципиально новых результатов в данном направлении не появилось. В момент выхода были также известны частичные результаты о разрешимости проблемы изоморфизма для групп с одним соотношением и тривиальным центром (Пиетровски) и для двупорожденных групп с одним соотношением и нетривиальным кручением (Прайд). Позднее З. Села [6] решил проблему изоморфизма для гиперболических групп без кручения, непредставимых как нетривиальные свободные произведения с объединением или HNN-расширения над тривиальной или бесконечной циклической подгруппой. В то же время неизвестно, какие из групп с одним соотношением являются гиперболическими.

Группы с малым сокращением

В 1912 г. при решении проблем равенства и сопряженности в группах поверхностей М. Ден показал, что при перемножении сопряженных к определяющим словам происходит «не так много» сокращений порождающих элементов самих определяющих слов. Изучение соответствующих вопросов теории конечно определенных групп с этой точки зрения привело к тому, что впоследствии было названо «теорией малых сокращений» и было подробно описано в монографии Линдона и Шуппа [5]. Обзоры [1] и [2] осветили целый ряд результатов алгоритмического характера в этой теории, полученных В. А. Тартаковским, М. Гриндлингером, Р. Линдоном, П. Шуппом, И. Рипсом, а также ряд важных результатов, полученных А. Ю. Ольшанским, показавшим продуктивность проведения построений с помощью диаграмм Ван Кампена, возрождение которых связано с именем Линдона. С одной стороны, это значительно расширило область групп с малым сокращением, позволило получить важнейшие результаты, с другой – послужило фундаментом дальнейшего развития геометрической теории групп уже с введением гиперболических и автоматных групп, о чем пойдет речь в следующем разделе.

ISSN 1812-3996

Разрешимые группы

В обзоре [1] особое внимание уделено алгоритмической теории разрешимых групп.

Отмечена теорема О. Харлампович [7] о существовании конечно определенной разрешимой группы ступени три с неразрешимой проблемой равенства. До этого В. Н. Ремесленниковым [8] был построен пример группы конечно определенной в многообразии всех разрешимых групп ступени не выше пяти с неразрешимой проблемой равенства. Приведены следствия этих результатов о неразрешимости проблем вхождения и изоморфизма. Позднее появились статьи [9–10], содержащие бесконечную серию примеров конечно определенных разрешимых групп с неразрешимой проблемой равенства, построенных методом, отличающимся от метода Харлампович. В этих статьях приведен ряд следствий о неразрешимости других алгоритмических проблем в классе конечно определенных разрешимых групп. Блок алгоритмических проблем для разрешимых групп с положительными решениями был представлен для конечно порожденных метабелевых групп работами Е. И. Тимошенко (проблема равенства), Н. С. Романовского (проблема вхождения) и Г. А. Носкова (проблема сопряженности), в классе центрально-метабелевых групп – теоремой Романовского (проблема вхождения).

Полициклические (в частности, конечно порожденные нильпотентные) группы

В классе разрешимых групп в обзоре [1] выделен подкласс полициклических групп, включающий в себя конечно порожденные нильпотентные группы, подчеркнута важность изучения его алгоритмической теории. Приведены результаты Ф. Грюневальда, Д. Сегала [11–12] и Р.А. Саркисяна [13], из которых, в частности, следует разрешимость проблемы изоморфизма в классе конечно порожденных нильпотентных групп (в обзоре [2] проблема изоморфизма названа «основной нерешенной проблемой для нильпотентных групп»). В статье [1] была сформулирована проблема изоморфизма для полициклических групп (Проблема 6). Впоследствии Д. Сегал доказал, что эта проблема положительно решается даже в более широком классе почти полициклических групп (т. е. групп, допускающих полициклические подгруппы конечного индекса).

Ф. Холл установил замечательную связь между теорией полициклических групп и коммутативной алгеброй. Это позволило ему и другим исследователям получить целый ряд свойств полициклических групп. Оказалось, что каждая полициклическая группа конечно определена, удовлетворяет условию максимальности для подгрупп, допускает точное представление матрицами над кольцом целых чисел, содержит подгруппу конечного индекса, являющуюся абелевым расширением нильпотентной группы и т. д. Следующая теорема суммирует часть результатов статьи [14], посвященной описанию разрешимости алгоритмических проблем в полициклических группах.

Теорема (Baumslag, Cannonito, Robinson, Segal [14]). Пусть $G = \langle x_1, \dots, x_n \mid r_1, \dots, r_m \rangle$ – представление полициклической группы. Существует алгоритм, определяющий по любому конечному подмножеству U группы G конечное представление подгруппы $\mathrm{gr}(U)$, порожденной этим подмножеством.

Следовательно, эффективно вычислимы полициклическое представление группы G, ранг Плоткина – Хирша $h(G)$, подгруппы Фиттинга $\mathrm{Fitt}(G)$ и Фраттини $\mathrm{Fratt}(G)$, центр $C(G)$, эффективно определимо наличие кручения в G и т.п.

Ряд результатов алгоритмического характера для полициклических групп отражен в работе [15].

Конечно порожденные метабелевы группы

Ф. Холл в 1954 г. доказал, что любая конечно порожденная метабелева группа G удовлетворяет условию максимальности для нормальных подгрупп. Следовательно, G конечно определена в многообразии всех метабелевых групп. Выше уже отмечались результаты Е. И. Тимошенко, Н. С. Романовского и Г. А. Носкова о разрешимости в классе конечно порожденных метабелевых групп проблем равенства, вхождения и сопряженности, соответственно.

Основанием любой конечно порожденной метабелевой группы G служит ее коммутант G', который может рассматриваться как модуль над конечно порожденным коммутативным групповым кольцом $\mathbb{Z}[G/G']$. Так как это кольцо нетерово, G' как модуль конечно порожден. Поэтому существует конечное описание коммутанта G', несмотря на то, что он не всегда конечно порожден как подгруппа. Фундаментальное значение имеет следующая теорема.

Теорема (Baumslag, Cannonito, Robinson [16]). Существует алгоритм, который по заданию конечно порожденной метабелевой группы порождающими элементами и определяющими соотношениями находит конечное представление $\mathbb{Z}[G/G']$-модуля G'.

Из этого утверждения выводится целый ряд следствий: существует алгоритм, находящий центр

ISSN 1812-3996

C(*G*) и его конечное представление; алгоритм, находящий конечное множество элементов, нормальное замыкание которого в группе совпадает с подгруппой Фиттинга Fitt(G); алгоритм, определяющий наличие нетривиальных элементов конечного порядка, определяющий для данного элемента его конечный порядок; алгоритм, нумерующий все возможные конечные порядки элементов группы; алгоритм, выясняющий сопряженность двух наборов элементов группы (с использованием одной из лемм Носкова); алгоритм, находящий подгруппу Фраттини Fratt(G), и еще ряд алгоритмов.

В целом это позволяет говорить об удовлетворительной базовой алгоритмической теории конечно порожденных метабелевых групп.

Еще в конце 30-х гг. XX столетия В. Магнус ввел в рассмотрение вложение групп вида F/R' в матричные группы размера (2×2), получившее название *вложение Магнуса*. В обзоре [1] вложению Магнуса уделено особое внимание. Это вложение зарекомендовало себя как исключительно эффективный инструмент в теории разрешимых групп. С его использованием получено множество результатов, в том числе алгоритмического характера. См., например, монографию [17]. Заметим, что проблема изоморфизма для конечно порожденных метабелевых групп (Проблема 7 из статьи [1]) остается открытой.

Проблемы подстановки

В обзоре [1] отдельный параграф посвящен проблемам подстановки. В нем собраны сведения о результатах алгоритмического характера, так или иначе связанных со схемой подстановки элементов группы вместо переменных в групповые слова. Сюда относятся проблемы о разрешимости уравнений в группах, проблемы тождества, автоморфной и эндоморфной сводимости и т. п. Была выделена теорема Г.С. Маканина о разрешимости уравнений в свободной группе. Было уделено внимание результатам автора по разрешимости проблемы эндоморфной сводимости и бескоэффициентных уравнений в разрешимых группах. Термин *бескоэффициентное* уравнение идет от Линдона, сейчас чаще такие уравнения называют *расщепляемыми.* Они имеют вид $w(x_1, \dots, x_n) = g$, где левая часть – групповое слово от неизвестных, не включающее в запись элементов группы *G*, над которой уравнение рассматривается, $g \in G$. Было дано описание предложенного автором метода интерпретации диофантовых уравнений в свободных нильпотентных группах. Метод показывает, как по произвольному диофантову уравнению построить групповое уравнение, разрешимое в свободной нильпотентной группе ступени не меньше девяти (впоследствии эта оценка снижена до четырех) в том и только том случае, если исходное уравнение разрешимо в целых числах. Отсюда и из неразрешимости диофантовой проблемы следует неразрешимость расщепляемых уравнений в свободных нециклических нильпотентных группах ступени не меньше девяти (снижено до четырех) и проблемы эндоморфной сводимости в тех же группах достаточно большого ранга [18]. Аналогичные результаты справедливы для свободных метабелевых групп и свободных разрешимых групп большей ступени разрешимости [19]. В дальнейшем метод интерпретации диофантовых уравнений неоднократно применялся при доказательствах алгоритмической неразрешимости. С его использованием Н.Н. Репин в работе [20] доказал неразрешимость уравнений от одной переменной в некоторой конечно порожденной нильпотентной группе ступени три (в конечно порожденных нильпотентных группах ступени два такие уравнения разрешимы), Ю.Г. Клейман решил несколько известных проблем, в частности доказав неразрешимость проблемы тождества в некотором конечно базируемом разрешимом ступени семь многообразии групп [21]. Подробнее об этих и других результатах см. в работе [22].

Элементарные теории

Одними из главных достижений по разрешимости элементарных теорий групп и элементарной эквивалентности является решение двух проблем Тарского (в работе [1] они записаны в виде Гипотезы 23 о разрешимости элементарной теории свободной группы и Вопроса 14 об элементарной эквивалентности свободных неабелевых групп соответственно). Доказательство разрешимости элементарной теории произвольной свободной группы дано А. Мясниковым и О. Харлампович [23–25]. Элементарная эквивалентность свободных неабелевых групп установлена А. Мясниковым и О. Харлампович [25] и независимо З. Села [26].

2. Новые аспекты исследований

Конечно определенные группы

Так как была доказана алгоритмическая неразрешимость основных алгоритмических проблем для класса всех конечно определенных групп, алгоритмическая теория групп уже с 80-х гг. XX столетия сосредотачивается на рассмотрении алгоритмических проблем как для основных классов групп – разреши-

ISSN 1812-3996

мых, в частности нильпотентных и полициклических, периодических, линейных, так и для некоторых других классов. Результатов по всем конечно определенным группам, полученных с этого времени, немного. Приведем для примера один из основных результатов, представленных в работе [27], относительно свойства, не являющегося Марковским.

Теорема (Bridson, Wilton [27]). Проблема существования алгоритма, определяющего по конечно определенной группе наличие в ней собственной подгруппы конечного индекса, алгоритмически неразрешима.

В работе [27] также получен ряд интересных результатов об алгоритмической неразрешимости, в том числе для проконечных и гиперболических групп. Например, доказано, что по данному конечному представлению гиперболической группы *G* без кручения и по данному $d > 2$ в общем случае нельзя построить алгоритм, отвечающий на вопрос: порождается ли (топологически) проконечное пополнение группы *G* множеством мощности меньше, чем *d*?

Геометрическая теория групп

Геометрическая теория групп обязана своим зарождением точке зрения, согласно которой алгебраические объекты, например группы, могут с успехом рассматриваться как геометрические и изучаться с помощью геометрической техники. М. Громов в работе [28] открыл замечательную теорию класса групп, названных им *гиперболическими группами.* И. Г. Лысенок и независимо М. Шапиро доказали, что гиперболические группы могут быть охарактеризованы следующим образом.

Группа *G* гиперболическая тогда и только тогда, когда она имеет конечное представление $G = \langle x_1, \dots, x_n \mid r_1, \dots, r_m \rangle$ со следующим свойством: если *v* – редуцированное слово от порождающих элементов, задающее единичный элемент группы *G*, то *v* содержит общее подслово с некоторым определяющим словом, длина которого превышает половину длины этого определяющего слова. Это означает, что проблема равенства в гиперболических группах решается алгоритмом Дена. Так как класс гиперболических групп совпадает с некоторым подклассом групп с малыми сокращениями, то можно считать, что последующие интенсивные исследования свойств (в том числе алгоритмических) гиперболических групп продолжают соответствующие исследования класса групп с малым сокращением. Однако следует отметить, что современная геометрическая теория групп существенно расширила сферу своего изучения, многообразие методов исследования, области приложений. Данный, достаточно общий подход успешно работает в топологии малых размерностей, теории многообразий, алгебраической топологии, комплексной динамике, римановой геометрии, теории представлений, алгебре и логике и, конечно, комбинаторной теории групп.

Класс гиперболических групп содержится в более широком классе автоматных групп, введенном в работе [29] Д. Б. А. Эпстином и др. О разрешимости некоторых алгоритмических проблем в геометрической теории групп см. публикации [30–31]. Отметим один из полученных результатов.

Теорема (Бирже, Ольшанский, Рипс, Сапир [32]). Конечно порожденная группа *G* имеет проблему равенства, принадлежащую классу NP, тогда и только тогда, когда она может быть вложена в качестве подгруппы в конечно определенную группу с полиномиальной функцией Дена (более того, можно выбрать вложение, при котором эта подгруппа имеет ограниченную дисторцию).

Разрешимые группы

Определенный интерес вызвали проблемы, включающие в себя эндоморфизмы.

Проблема скрученной сопряженности: относительно произвольного фиксированного эндоморфизма φ группы *G* для произвольной пары элементов $g, f \in G$ определить, существует ли элемент $x \in G$ такой, что $\varphi(x)g = fx$.

Проблема бинарно скрученной сопряженности: относительно произвольной фиксированной пары эндоморфизмов φ, ψ группы *G* для произвольной пары элементов $g, f \in G$ определить, существует ли элемент $x \in G$ такой, что $\varphi(x)g = f\psi(x)$.

Алгоритмическая разрешимость проблемы скрученной сопряженности для произвольного эндоморфизма полициклической группы установлена автором настоящей статьи в работе [33].

Аналогичный результат для конечно порожденной метабелевой группы с ограничением на вид эндоморфизма представлен автором совместно с Э. Вентурой в статье [34]. Ограничение снято в работе [35].

В статье [36] показано, как по диофантову многочлену D построить конечно порожденную нильпотентную группу *G* ступени два и по любому целому числу *a* записать в явном виде элемент $w(a) \in G$, являющийся коммутатором в группе *G* тогда и только тогда, когда уравнение $D = a$ разрешимо в целых числах. В виду указанных построений из алгоритми-

ISSN 1812-3996

ческой неразрешимости диофантовых уравнений следует неразрешимость в *G* проблемы коммутатора, а значит, и проблемы разрешимости произвольного квадратичного уравнения.

Из положительных результатов отметим теорему И. Лысенка и А. Ушакова [37], по которой *диофантова проблема* (проблема разрешимости уравнений) для *сферических квадратичных* уравнений, имеющих вид $x_1 g_1 x_1^{-1} \ldots x_k g_k x_k^{-1} = 1$, где x_i – неизвестные, g_i – элементы группы, в свободных метабелевых группах разрешима, более того – NP-полна.

Теория сложности и реальные алгоритмы

Последние годы значительно усилился интерес к анализу алгоритмов с точки зрения теории сложности и практической реализуемости. Группы подстановок составляют наиболее развитую часть *вычислительной теории групп*. Основой для этого послужила соответствующая техника их изучения, развитая Ч. Симпсом еще в 60-е гг. XX столетия. М. Л. Фурст, Д. Хопкрофт и И. М. Люкс (см.: [38]) показали, что предложенный Симпсом метод работает за полиномиальное время. Полиномиальная по времени теория линейных групп началась с рассмотрения матричных групп над конечными полями. В качестве основных выступали проблемы определения порядка подгруппы, заданной конечным множеством порождающих, и проблема вхождения в таким образом заданную подгруппу. Даже в случае абелевых групп неизвестно, как решать подобные проблемы без решения трудных теоретико-числовых проблем, например проблем дискретного логарифма и разложения чисел на множители. Естественным стал подход к нахождению решения с использованием теоретико-числового оракула.

Суммируем некоторые результаты о матричных группах, полученные за последние 25–30 лет усилиями ряда авторов, таких как Люкс, Бабаи, Билс, Сересс и др. (см.: [39]). Пусть *G* – конечно порожденная матричная группа над конечным полем. Тогда за полиномиальное время выясняется разрешимость группы *G*, если она разрешима, то проверяется ее нильпотентность и для любого простого *p* находится силовская p-подгруппа, в случае разрешимости *G* решаются следующие проблемы: находится порядок $|G|$, решается проблема вхождения в *G*, находится представление *G* через порождающие элементы и определяющие соотношения, находится композиционный ряд группы *G* и т. д.

В работе [40] дается практически реализуемое решение ряда алгоритмических проблем для класса конечно порожденных нильпотентных групп. Вычисляются нормальные формы элементов относительно баз Мальцева, решаются проблемы вхождения и сопряженности, строятся конечные представления подгрупп, построения ведутся в логарифмическом пространстве за квазилинейное время. Версии проблем, использующие компрессию слов, решаются за полиномиальное время. Детальное представление о компрессии и некоторые известные результаты алгоритмического характера с ее использованием можно найти в публикации [41].

В статье [42] рассматриваются алгоритмические вопросы теории групп, моделирующие классические вычислительные вопросы теории решеток. Например, в случае конечно порожденной нильпотентной группы за полиномиальное время находится элемент подгруппы ближайший к данному элементу группы, изучается вычислительная сложность этого и некоторых других алгоритмов. Также представлен алгоритм, вычисляющий за полиномиальное время геодезические в данных порождающих элементах подгруппы свободной группы.

В исследовании [43] обобщается классическая проблема соответствия Поста (**PCP**) и ее неоднородная версия (**NPCP**), которые теперь ставятся для некоммутативных групп. Изучается вычислительная сложность этих проблем. Показано, что **PCP** тесно связана с проблемой эквалайзера, в то время как **NPCP** имеет прямое отношение к проблеме бинарно скрученной сопряженности. Более того, одна из наиболее сильных форм проблемы равенства (наследственная проблема равенства, при которой проблема равенства разрешима для всех факторов группы) сводится к **NPCP**.

В статье [44] изучается теоретико-групповой аналог задачи о рюкзаке. Работа [45] посвящена теоретико-групповому аналогу классической проблемы суммы подмножеств. Показано, что она полиномиально разрешима в любой конечно порожденной почти нильпотентной группе. В то же время для любой полициклической не почти нильпотентной группы эта проблема принадлежит классу NP-полных проблем.

В работе [46] исследуется вычислительная сложность проблемы равенства для свободных разрешимых групп $S_{r,d}$, где $r > 1$ – ранг группы, $d > 1$ – ступень разрешимости. Известно, что вложение Магнуса этой группы в матричную группу позволяет получить полиномиальный по времени алгоритм, решающий в ней проблему равенства. К сожалению, степень полиномиальности растет вместе с ростом

ISSN 1812-3996

d, поэтому в целом для класса свободных разрешимых групп этот алгоритм не полиномиален. Показывается, как проблему равенства можно решить для группы $S_{r,2}$ алгоритмом сложности O(*rn* log(*n*)), для группы $S_{r,d}$ при *d* > *2* – алгоритмом сложности O(n^3rd). Тем не менее оказалось, что близкая к проблеме равенства проблема вычисления геодезической длины элемента является NP-полной уже для группы вида $S_{r,2}$, *r* > *1*. Уточнения результатов работы [46] и некоторые новые результаты, связанные с вычислением геодезических в группах, приведены в статье [47]. См. также: [48–49].

Монография [50] посвящена алгоритмам и их сложности в криптографии. Обращается внимание на *усредненную* и *генерическую* сложность. Относительно усредненных характеристик групп см., например, публикации [51–52], где представлены решения двух проблем М. Громова. Генерический подход к алгоритмическим проблемам был предложен в 2003 г. А. Мясниковым, И. Каповичем, П. Шуппом и В. Шпильрайном [51]. В рамках этого подхода алгоритмическая проблема рассматривается не для всего множества входов (сложность в худшем случае), а для множества «почти всех» входов. Термин «почти все входы» уточняется при помощи введения естественной меры на множестве входных данных. Такой подход к сложности имеет практическое значение в случаях, когда входные данные выбираются случайно.

Вопросы генерической сложности рассматривались в ряде статей А. Г. Мясникова и А. Н. Рыбалова (см., например: [52]). Решения двух проблем М. Громова об усредненных функциях Дена даны в работах [53; 54].

СПИСОК ЛИТЕРАТУРЫ

1. *Ремесленников В. Н., Романьков В. А.* Теоретико-модельные и алгоритмические вопросы теории групп // Итоги науки и техн. Сер. Алгебра. Топол. Геом. 1983. Т. 21. С. 3–79. Переводная версия: Model-theoretic and algorithmic questions in group theory // J. Sov. Math. 1985. Vol. 31, № 3. P. 2887–2939.

2. *Носков Г. А., Ремесленников В. Н., Романьков В. А.* Бесконечные группы // Итоги науки и техн. Сер. Алгебра. Топол. Геом. 1979. Т. 17. С. 65–157. Переводная версия: *Noskov G. A., Remeslennikov V. N., Roman'kov V. A.* Infinite groups // J. Sov. Math. 1982. Vol. 18, № 5. P. 669–735.

3. *Мельников О. В., Ремесленников В. Н., Романьков В. А., Скорняков Л. А., Шестаков И. П.* Общая алгебра. Т. 1. М. : Наука : Физматлит., 1990. 591 с. (Сер. «Справочная математическая библиотека»).

4. *Magnus W., Karrass A., Solitar D.* Combinatorial Group Theory: Presentations of groups in terms of generators and relations. N. Y. : Wiley, 1966. 444 p.; *Магнус В., Каррас А., Солитэр Д.* Комбинаторная теория групп. Представление групп в терминах образующих и соотношений : пер. с англ. / под ред. М. Д. Гриндлингера. М.: Наука, 1974. 455 с.

5. *Lyndon R. C., Shupp P. E.* Combinatorial group theory. Berlin ; Heidelberg ; N. Y. : Springer-Verlag, 1977. 339 p.; *Линдон Р., Шупп П.* Комбинаторная теория групп : пер. с англ. / под ред. В. Н. Ремесленникова и В. А. Романькова. М.: Мир, 1980. 447 с.

6. *Sela Z.* The isomorphism problem for hyperbolic groups // Ann. of Math. 1995. Vol. 141, № 2. P. 217–283.

7. *Харлампович О. Г.* Конечно определенная разрешимая группа с неразрешимой проблемой равенства // Изв. АН СССР. Сер. мат. 1981. Т. 45, № 4. С. 854–873.

8. *Ремесленников В. Н.* Пример группы, конечно определенной в многообразии A5, с неразрешимой проблемой равенства // Алгебра и логика. 1973. Т. 12, № 5. С. 577–602.

9. *Baumslag G., Gildenhuys D., Strebel R.* Algorithmically insoluble problems about finitely presented solvable groups, Lie and associative algebras. I // J. Pure and Applied Algebra. 1986. Vol. 39. P. 53–94.

10. *Baumslag G., Gildenhuys D., Strebel R.* Algorithmically insoluble problems about finitely presented solvable groups, Lie and associative algebras. II // J. Algebra. 1985. Vol. 142, № 1. P. 118–149.

11. *Grunewald F., Segal D.* The solubility of certain decision problems in arithmetic and algebra // Bull. (New Ser.) Amer. Math. Soc. 1989. Vol. 1, № 6. P. 915–918.

12. *Grunewald F., Segal D.* Some general algorithms. I. Arithmetic groups. II. Nilpotent groups // Ann. Math. 1980. Vol. 112, № 3. P. 531–583.

13. *Саркисян Р. А.* Алгоритмические вопросы для линейных алгебраических групп. I, II // Математический сборник. 1980. Т. 113, № 2, 3. С. 179–216, 400–436.

14. *Baumslag G., Cannonito F., Robinson D. J. S., Segal D.* The algorithmic theory of polycyclic-by-finite groups // J. Algebra. 1991. Vol. 142, № 1. P. 118–149.

15. *Segal D.* Decidable properties of polycyclic groups // Proc. London Math. Soc. Ser. 3. 1990. Vol. 61, № 3. P. 497–528.

16. *Baumslag G., Cannonito F., Robinson D. J. S.* The algorithmic theory of finitely generated metabelian groups // Trans. Amer. Math. Soc. 1994. Vol. 344, № 2. P. 629–648.

17. *Тимошенко Е. И.* Эндоморфизмы и универсальные теории разрешимых групп. Новосибирск : НГТУ, 2011. 327 с. (Сер. «Монографии НГТУ»).

18. *Романьков В. А.* О неразрешимости проблемы эндоморфной сводимости в свободных нильпотентных группах и в свободных кольцах // Алгебра и логика. 1977. Т. 16, № 4. С. 457–471.

19. *Романьков В. А.* Об уравнениях в свободных метабелевых группах // Сиб. мат. журн. 1979. Т. 20, № 3. С. 671–673.

20. *Репин Н. Н.* Проблема разрешимости уравнений с одной неизвестной в нильпотентных группах // Изв. АН СССР. Сер. мат. 1984. Т. 48. С. 1295–1313.

21. *Клейман Ю. Г.* О тождествах в группах // Тр. Моск. мат. о-ва. 1982. Т. 44. С. 62–108.

22. *Roman'kov V. A.* Equations over groups // Groups, Complexity, Cryptology. 2012. Vol. 4, № 2. P. 191–239.

23. *Kharlampovich O., Myasnikov A.* Irreducible affine varieties over a free group. I. Irreducibility of quadratic equations and Nullstellensatz // J. Algebra. 1998. Vol. 200. P. 472–516.

24. *Kharlampovich O., Myasnikov A.* Irreducible affine varieties over a free group. II. Irreducibility of quadratic equations and Nullstellensatz // J. Algebra. 1998. Vol. 200. P. 517–570.

25. *Kharlampovich O., Myasnikov A.* Elementary theory of free non-abelian groups // J. Algebra. 2006. Vol. 302. P. 451–652.

26. *Sela Z.* Diophantine geometry over groups. VI. The elementary theory of a free group // GAFA. 2006. Vol. 16. P. 707–730.

27. *Bridson M. R., Wilton H.* The triviality problem for profinite completions // Invent. Math. 2015. Vol. 202. P. 839-874.

28. *Gromov M.* Hyperbolic groups // Essays in group theory / ed. by S. Gersten; MSRI Publications. N. Y. : Springer-Verlag, 1987. P. 75–264.

29. *Epstein D. B. A., Paterson M. S., Cannon J. W., Holt D. F., Levy S. V., Thurston W. P.* Word processing in groups. Abingdon : Taylor & Francis, 1992. 332 p.

30. Algorithmic problems in groups and semigroups / editors: J.-C. Birget, S. Margolis, J. Meakin, M. V. Sapir. N. Y. : Springer-Science+Business Media, LLC, 2012. 309 p. (Trends in Mathematics).

31. *Brady N., Riley T., Short H.* The Geometry of the Word Problem for Finitely Generated Groups. Basel ; Boston ; Berlin : Birkhauser Verlag, 2007. 206 p. (Advanced Courses in Mathematics, CRM, Barselona).

32. *Birget J.-C., Olshanskii A. Y., Rips E., Sapir M. V.* Isoperimetric and isodiametric functions of groups and computational complexity of the word problem // Ann. of Math. (Ser. 2). 2002. Vol. 156, № 2. P. 467–518.

33. *Roman'kov V.* The twisted conjugacy problem for endomorphisms of polycyclic groups // J. Group Theory. 2010. Vol. 13. P. 355–364.

34. *Вентура Э., Романьков В. А.* Проблема скрученной сопряженности для эндоморфизмов метабелевых групп // Алгебра и логика. 2009. Т. 48, № 2. С. 157–173.

35. *Романьков В. А.* О разрешимости уравнений с эндоморфизмами в нильпотентных группах // Сиб. электрон. мат. изв. 2016. Т. 13. С. 716–725.

36. *Roman'kov V. A.* Diophantine questions in the class of finitely generated nilpotent groups // J. Group Theory. 2016. Vol. 19. P. 497–514.

37. *Lysenok I., Ushakov A.* Spherical quadratic equations in free metabelian groups // Proc. Amer. Math. Soc. 2016. Vol. 144. P. 1383–1390.

38. *Furst M. L., Hopcroft J., Lucks E. M.* Polynomial-time algorithms for permutation groups // Proc. 21st IEEE Symp. on Foundations of Comp. Sci. [S. l.], 1980. P. 36–41.

39. *Babai L., Beals R., Seress A.* Polynomial-time theory of matrix groups // Proc. 41st ACM Symp. On Theory of Comp. (STOC 2009) (May 31 – June 2, 2009). N. Y., 2009. P. 55–64.

40. *Macdonald J., Myasnikov A., Nikolaev A., Vassileva S.* Logspace and compressed-word computations in nilpotent groups // arXiv: 1503.03888v1 [math. GR] 12 Mar 2015. P. 1–38.

41. *Lohrey M.* The Compressed Word Problem for Groups. Berlin : Springer Science & Business Media, 2014. 153 p. (Springer briefs in mathematics).

42. *Myasnikov A., Nikolaev A., Ushakov A.* Non-commutative lattice problems // J. Group Theory. 2016. Vol. 19, № 3. P. 455–475.

43. *Myasnikov A., Nikolaev A., Ushakov A.* The Post correspondence problem in groups // J. Group Theory. 2014. Vol. 17. P. 991–1008.

44. *Myasnikov A., Nikolaev A., Ushakov A.* Knapsack problems in groups // Mathematics of Computation. 2015. Vol. 84. P. 987–1016.

45. *Nikolaev A., Ushakov A.* Subset sum problem in polycyclic groups // J. Symbolic Computation (в печати).

46. *Myasnikov A., Roman'kov V., Ushakov A., Vershik A.* The word and geodesic problems in free solvable groups // Trans. Amer. Math. Soc. 2010. Vol. 362, № 9. P. 4655–4682.

47. *Elder M., Rechnitzer A.* Some geodesic problems in groups // Groups, Complexity, Cryptology. 2010. Vol. 2. P. 223–229.

48. *Ushakov A.* Algorithmic theory of free solvable groups: randomized computations // J. Algebra. 2014. Vol. 407. P. 178–200.

49. *Vassileva S.* Polynomial time conjugacy in wreath products and free solvable groups // Groups, Complexity, Cryptology. 2011. Vol. 3, № 1. P. 105–120.

50. *Myasnikov A., Shpilrain V., Ushakov A.* Non-commutative cryptography and complexity of group-theoretic problems. Providence : Amer. Math. Soc., 2011. 385 p. (Math. Surveys and Monographs, vol. 177).

51. *Kapovich I., Myasnikov A., Schupp P., Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks // J. Algebra. 264 (2003). Vol. 264, № 2. P. 665–694.

52. *Myasnikov A., Rybalov A.* Generic complexity of undecidable problems // J. Symbolic Logic. 2008. Vol. 73, № 2. P. 656–673.

53. *Кукина Е. Г., Романьков В. А.* Субквадратичность усредненной функции Дена для свободных абелевых групп // Сиб. мат. журн. 2003. Т. 44, № 4. С. 772–778.

54. *Романьков В. А.* Об асимптотическом росте усредненной функции Дена для нильпотентных групп // Алгебра и логика. 2007. Т. 46, № 1. С. 60–74.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Романьков Виталий Анатольевич – доктор физико-математических наук, профессор, заведующий кафедрой компьютерной математики и программирования, *Омский государственный университет им. Ф.М. Достоевского,* 644077, Россия, г. Омск, пр. Мира, 55а; e-mail: romankov48@mail.ru.

INFORMATION ABOUT THE AUTHOR

Roman'kov Vitalii Anatolievich – Doctor of Physical and Mathematical Sciences, Professor, Head of the Chair of Computing Mathematics and Programming, *Dostoevsky Omsk State University,* 55a, pr. Mira, Omsk, 644077, Russia; e-mail: romankov48@mail.ru.

ДЛЯ ЦИТИРОВАНИЯ

Романьков В. А. Об алгоритмических проблемах в теории групп // Вестн. Ом. ун-та. 2017. № 2 (84). С. 18–27.

FOR CITATIONS

Roman'kov V. A. On algorithmic problems in group theory. *Vestnik Omskogo universiteta = Herald of Omsk University*, 2017, no. 2(84), pp. 18–27. (in Russian).