МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2021 № 52

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

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

Подписной индекс в объединённом каталоге «Пресса России» 38696

УЧРЕДИТЕЛЬ
Томский государственный университет

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

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

Периодичность выхода журнала: 4 номера в год.

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

Подписано к печати 08.06.2021. Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 14,8. Тираж 300 экз.
Заказ № 4684. Цена свободная. Дата выхода в свет 17.06.2021.

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

СОДЕРЖАНИЕ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

Селиверстов А. В. Двоичные решения для больших систем линейных уравнений 5
Roman'kov V. A. Algorithmic theory of solvable groups 16
Kiss R., Nagy G. P. On the nonexistence of certain orthogonal arrays of strength four 65

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Буханов Д. Г., Поляков В. М., Редькина М. А. Обнаружение вредоносного программного обеспечения с использованием искусственной нейронной сети на основе адаптивно-резонансной теории 69
Девянин П. Н., Леонова М. А. Приёмы описания модели управления доступом ОССН Astra Linux Special Edition на формализованном языке метода Event-B для обеспечения её верификации инструментами Rodin и ProB 83

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

Абросимов М. Б., Костин С. В., Лось И. В. О наибольшем числе вершин примитивных однородных графов порядка 2, 3, 4 с экспонентом, равным 2 97
Москин Н. Д. Метрика для сравнения графов с упорядоченными вершинами на основе максимального общего подграфа 105
Мышкис П. А., Таташев А. Г., Яшина М. В. Дискретная замкнутая одночастичная цепочка контуров 114
СВЕДЕНИЯ ОБ АВТОРАХ 126

CONTENTS

THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS

Seliverstov A. V. Binary solutions to large systems of linear equations 5
Roman'kov V. A. Algorithmic theory of solvable groups 16
Kiss R., Nagy G. P. On the nonexistence of certain orthogonal arrays of strength four 65

MATHEMATICAL BACKGROUNDS OF COMPUTER SECURITY

Bukhanov D. G., Polyakov V. M., Redkina M. A. Detection of malware using an artificial neural network based on adaptive resonant theory 69
Devyanin P. N., Leonova M. A. The techniques of formalization of OS Astra Linux Special Edition access control model using Event-B formal method for verification using Rodin and ProB 83

APPLIED GRAPH THEORY

Abrosimov M. B., Kostin S. V., Los I. V. The maximum number of vertices of primitive regular graphs of orders 2, 3, 4 with exponent 2 97
Moskin N. D. Metric for comparing graphs with ordered vertices based on the maximum common subgraph 105
Myshkis P. A., Tatashev A. G., Yashina M. V. Discrete closed one-particle chain of contours 114

BRIEF INFORMATION ABOUT THE AUTHORS 126

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.161

ДВОИЧНЫЕ РЕШЕНИЯ ДЛЯ БОЛЬШИХ СИСТЕМ ЛИНЕЙНЫХ УРАВНЕНИЙ[1]

А. В. Селиверстов

Институт проблем передачи информации им. А. А. Харкевича Российской академии наук, г. Москва, Россия

Понятие генерической вычислительной сложности распространено на обобщённые регистровые машины над упорядоченным полем. В этом случае машина на каждом входе останавливается и почти на каждом входе даёт содержательный ответ, но может отказаться от вычисления посредством явного уведомления об этом, иными словами, существует особое неопределённое состояние остановки. При этом машина не делает ошибок. Предложен генерический алгоритм полиномиального времени для распознавания систем линейных уравнений без какого-либо двоичного решения, когда число уравнений m близко к числу неизвестных n. Более точно — требуется выполнение двух условий. Во-первых, выполнено неравенство $2n \geqslant (n-m+1)(n-m+2)$. Такие системы называются большими, поскольку число уравнений близко к числу неизвестных. Во-вторых, выполнены некоторые предположения общности системы уравнений. Наш подход основан на поиске положительно определённой квадратичной формы среди множества форм, зависящих от параметров. С другой стороны, найден контрпример, показывающий неприменимость этого метода для проверки отсутствия двоичного решения у одного уравнения.

Ключевые слова: *двоичное решение, линейное уравнение, обобщённая регистровая машина, вычислительная сложность.*

DOI 10.17223/20710410/52/1

BINARY SOLUTIONS TO LARGE SYSTEMS OF LINEAR EQUATIONS

A. V. Seliverstov

Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute), Moscow, Russia

E-mail: slvstv@iitp.ru

The concept of generic computational complexity has been extended to generalized register machines over an ordered field. In this case, the machine halts at every input and gives a meaningful answer at almost every input, but it can abandon the calculation using explicit notification, that is, there exists the vague halting state. Note that the machine does not make any error. A generic polynomial time algorithm is

[1]Исследование выполнено при финансовой поддержке РФФИ, проект № 18-29-13037.

proposed to recognize systems of linear equations without any binary solution, when the number of equations m is close to the number of unknowns n. More precisely, two conditions are required. Firstly, the inequality $2n \geqslant (n-m+1)(n-m+2)$ holds. Such systems are called large because the number of equations is close to the number of unknowns. Secondly, some assumptions of generality of the system of equations are fulfilled. Our approach is based on finding a positive definite quadratic form among the set of forms that depend on parameters. On the other hand, a counterexample has been found, whicht shows the inapplicability of this method for checking the absence of any binary solution to one equation.

Keywords: *binary solution, linear equation, generalized register machine, computational complexity.*

Введение

Задача о существовании двоичного решения у системы линейных уравнений с рациональными коэффициентами NP-полная [1, следствие 18.1b, т. 2, с. 397], она сводится за полиномиальное время к задаче о существовании двоичного решения одного линейного уравнения. Иногда получается уравнение с целыми коэффициентами, близкими к нулю [2]. Если линейное уравнение имеет целые коэффициенты, чьи модули достаточно малы, то поиск двоичного решения для этого уравнения быстро выполняется методом динамического программирования [1, 3–5]. В случае отсутствия ограничений на коэффициенты для поиска двоичного решения одного линейного уравнения от n неизвестных предложены детерминированный алгоритм, использующий экспоненциальное время $\mathrm{poly}(n)2^{0{,}5n}$ и экспоненциальную память $\mathrm{poly}(n)2^{0{,}25n}$, а также вероятностный алгоритм, использующий большее время $\mathrm{poly}(n)2^{0{,}86n}$, но полиномиальную память [6, 7]. Гипотеза о высокой вычислительной сложности этой задачи согласуется с оценками степеней многочленов, необходимых для доказательства отсутствия двоичного решения посредством Positivstellensatz [8]. Для близкой задачи Equal-Subset-Sum, которая эквивалентна поиску $(-1, 0, 1)$-решения линейного уравнения, известны детерминированный алгоритм с временем работы $\mathrm{poly}(n)3^{0{,}5n}$, а также вероятностный алгоритм, дающий ответ за время $\mathrm{poly}(n)1{,}7088^n$ с высокой вероятностью [9].

Посредством исключения переменных поиск двоичного решения системы из m линейно независимых линейных уравнений от n неизвестных сводится к параллельной проверке продолжаемости двоичных решений одного линейного уравнения от $(n-m)$ неизвестных до двоичного решения системы уравнений от n неизвестных. Следовательно, исходная задача разрешима за полиномиальное время, когда разность между числом неизвестных и числом линейно независимых уравнений ограничена функцией вида $n - m = O(\log n)$. В этой работе мы рассмотрим случай, когда разность числа неизвестных n и числа уравнений m ограничена сверху сравнительно быстро растущей функцией вида $n - m = O(\sqrt{n})$ и выполнено некоторое предположение общности для системы уравнений. Так улучшены ранее полученные оценки, но предложенный метод в общем случае бесполезен для одного уравнения.

Для многих NP-полных задач также известны эвристические алгоритмы, работающие при дополнительных ограничениях. Например, для задачи 3-SAT о выполнимости 3-КНФ при дополнительном условии, когда число элементарных дизъюнкций в 3-КНФ от n переменных ограничено снизу функцией вида $\mathrm{poly}(\log n)n\sqrt{n}$, существует алгоритм полиномиального времени, который для большой доли случаев (при любом фиксированном значении n) распознаёт невыполнимость 3-КНФ [10, 11].

Более сильный результат известен для задачи NAE-3-SAT. Здесь проверяется существование оценки n булевых переменных, при которой каждая элементарная дизъюнкция в 3-КНФ содержит как истинный, так и ложный литералы. При дополнительном условии, когда число элементарных дизъюнкций в 3-КНФ превышает $\frac{27}{2}n$, существует алгоритм полиномиального времени, который для большой доли случаев (при любом фиксированном значении n), стремящейся к единице с ростом n, распознаёт отсутствие решения [12].

1. Вычислительная модель

Оценивая вычислительную сложность, мы рассматриваем обобщённые регистровые машины над упорядоченным полем $(K, 0, 1, +, -, \times, ()^{-1}, <, =)$, которое вложено в поле вещественных чисел [13]. Над полем вещественных чисел такая модель вычислений известна как BSS-машина [14]. Элементы поля K будем называть числами, но можно рассматривать любые упорядоченные поля. Здесь $x^{-1}x = 1$, когда $x \neq 0$, и дополнительно $0^{-1} = 0$. Каждый регистр содержит число из поля K. Машина имеет также индексные регистры, содержащие неотрицательные целые числа. За один шаг машина либо выполняет операцию над индексными регистрами, либо копирует число из одного регистра в другой, либо записывает в регистр константу 0 или 1, либо вычисляет сумму, разность или произведение двух чисел в регистрах, либо вычисляет обратное число к записанному в регистр, либо выполняет сравнение двух чисел в регистрах. При этом номера используемых регистров хранятся в индексных регистрах, над которыми производятся обычные операции. Время работы полиномиальное, если общее число операций, выполняемых машиной до остановки, ограничено многочленом от числа регистров, занятых входом. В начальный момент времени это число записано в нулевом индексном регистре, а другие индексные регистры содержат нули. Так же определяются недетерминированные обобщённые регистровые машины. Недетерминированный шаг состоит в записи в указанный регистр нового числа из поля K, которое не было вычислено на предыдущих шагах.

Говоря менее формально, рассматривая обобщённые регистровые машины, мы оцениваем арифметическую сложность. С другой стороны, вычисления на обобщённых регистровых машинах тесно связаны с методами алгебраической геометрии над произвольными алгебраическими структурами [15]. Над полем, вычислимым за полиномиальное время, полиномиальная вычислимость на обобщённой регистровой машине не влечёт полиномиально ограниченную битовую сложность [16, 17]. Для этого дополнительно требуется, чтобы на каждом шаге записанные в регистрах числа имели полиномиально ограниченную длину записи. Это ограничение существенно. Например, возведение рационального числа в степень n требует лишь $O(\log n)$ умножений. Однако в общем случае длина двоичной записи результата не ограничена сверху функцией типа $\mathrm{poly}(\log n)$. С другой стороны, трудно указать минимальное число умножений, необходимое для вычисления такого числа оптимальным способом [18].

Для положительного целого числа k фраза «почти все последовательности из k чисел» обозначает «все численные оценки k переменных, на которых как-то фиксированный многочлен положительной степени от k переменных не обращается в нуль» [19]. Многочлен отождествляется с последовательностью числовых коэффициентов, включая нулевые значения, используя фиксированное мономиальное упорядочение. Так же с последовательностями чисел отождествляются системы уравнений и матрицы, чьи элементы упорядочиваются в зависимости от контекста.

Мы рассматриваем машины, которые могут давать неопределённый результат — отказ от вычисления. Но принимая или отвергая вход, машина не ошибается. Рассмотрим обобщённую регистровую машину над упорядоченным полем с тремя состояниями остановки, обозначаемыми через ACCEPT, REJECT и VAGUE. В состоянии ACCEPT машина принимает вход, в состоянии REJECT — отвергает вход, в состоянии VAGUE — отказывается дать содержательный ответ. По аналогии с обычными генерическими вычислениями [20–23] обобщённая регистровая машина называется *генерической*, когда выполнены два условия: 1) машина останавливается на каждом входе и 2) для каждого положительного целого числа k и для почти всех входов, каждый из которых занимает ровно k регистров, машина принимает или отвергает вход, но не останавливается в состоянии VAGUE. Аналогично определяются генерические машины, вычисляющие нетривиальный выход в регистрах. Если машина остановилась в состоянии VAGUE, то записанный в регистрах выход признаётся бессмысленным. Однако для любого k и для почти всех входов, каждый из которых занимает ровно k регистров, машина не приходит в состояние VAGUE.

Над полем вещественных чисел множество входов, на котором генерическая обобщённая регистровая машина останавливается в состоянии VAGUE, имеет меру нуль. Поэтому такие машины служат аналогом обычных генерических алгоритмов.

Часто условием вычислимости служит ограничение на ранг матрицы. В общем случае степень детерминатального многообразия (над полем комплексных чисел) может очень быстро расти при увеличении размера (прямоугольной) матрицы [24]. Однако над линейно упорядоченным полем верхняя граница k на ранг матрицы выражается обращением в нуль суммы квадратов миноров порядка k. Это многочлен степени $2k$ от элементов матрицы.

Для чисел n и $r \leqslant n$ ранг $(r \times n)$-матрицы равен r тогда и только тогда, когда отличен от нуля некоторый многочлен степени $2r$ от элементов матрицы. При этом достаточным условием, которое выполнено для почти всех таких матриц, служит отличие от нуля одного из миноров порядка r, равного многочлену степени r.

Согласно критерию Сильвестра, симметричная матрица положительно определена тогда и только тогда, когда все её угловые миноры Δ_k положительные. Определитель матрицы над полем K вычисляется обобщённой регистровой машиной за полиномиальное время. Для проверки положительной определённости числовой матрицы удобно использовать также LDU-разложение, чья вычислительная сложность имеет тот же порядок, что и для матричного умножения [25].

2. Основные результаты

Для каждого натурального числа n рассмотрим n-мерное аффинное пространство над полем K с фиксированной системой координат. Точка, каждая координата которой равна 0 или 1, называется $(0,1)$-точкой. Поиск бинарного решения системы линейных уравнений эквивалентен поиску $(0,1)$-точки, инцидентной аффинному подпространству. Многочлен второй степени, который равен линейной комбинации многочленов вида $x_k(x_k-1)$, обращается в нуль в каждой $(0,1)$-точке. Гомогенизацией такого многочлена служит линейная комбинация квадратичных форм вида $x_k(x_k-x_0)$, где через x_0 обозначена новая переменная. Такие квадратичные формы служат для сертификации отсутствия двоичных решений.

Аффинное пространство вложено в проективное пространство с однородными координатами $(x_0 : \cdots : x_n)$. При $\alpha \neq 0$ линейная форма αx_0 определяет бесконечно

удалённую гиперплоскость в проективном пространстве. Аффинное пространство соответствует значению $x_0 = 1$.

Теорема 1. Даны натуральные числа n и s, для которых выполнено неравенство $2n \geqslant (s+1)(s+2)$. Для почти каждого набора из $(n-s)$ линейных форм $\ell_j(x_0, \cdots, x_s)$ для индексов $j > s$ найдутся такие значения коэффициентов λ_k, что будет положительно определена квадратичная форма

$$\sum_{k=1}^{s} \lambda_k x_k(x_k - x_0) + \sum_{j=s+1}^{n} \lambda_j \ell_j(\ell_j - x_0)$$

от переменных x_0, …, x_{n-s}. Более того, значения этих коэффициентов вычисляются генерической обобщённой регистровой машиной за полиномиальное время. Эта машина может остановиться в состоянии VAGUE лишь на таком входе, на котором обращается в нуль некоторый многочлен степени не выше $(s+1)(s+2)$ от коэффициентов линейных форм ℓ_j.

Доказательство. Достаточно найти значения λ_1, …, λ_n, при которых выполнено равенство многочленов

$$\sum_{k=1}^{s} \lambda_k x_k(x_k - x_0) + \sum_{j=s+1}^{n} \lambda_j \ell_j(\ell_j - x_0) = \sum_{k=0}^{s} x_k^2.$$

Этот набор значений служит решением неоднородной системы линейных уравнений от n неизвестных $\lambda_1, \ldots, \lambda_n$, в которой число уравнений равно $s+1$. Обозначим через ℓ_{jk} коэффициенты линейной формы $\ell_j = \ell_{j0}x_0 + \ldots + \ell_{js}x_s$. Коэффициенты при мономах x_0^2 определяют для неизвестных λ_1, …, λ_n неоднородное уравнение

$$\sum_{j=s+1}^{n} \ell_{j0}(\ell_{j0} - 1)\lambda_j = 1. \tag{1}$$

Коэффициенты при мономах x_k^2, где $1 \leqslant k \leqslant s$, дают s уравнений

$$\lambda_k + \sum_{j=s+1}^{n} \ell_{jk}^2 \lambda_j = 1. \tag{2}$$

Коэффициенты при мономах $x_k x_0$, где $1 \leqslant k \leqslant s$, дают s уравнений

$$-\lambda_k + \sum_{j=s+1}^{n} \ell_{jk}(2\ell_{j0} - 1)\lambda_j = 0. \tag{3}$$

Коэффициенты при мономах $x_k x_i$, где $1 \leqslant i < k \leqslant s$, дают уравнения

$$\sum_{j=s+1}^{n} \ell_{jk}\ell_{ji}\lambda_j = 0. \tag{4}$$

Обозначим через r число уравнений от неизвестных λ_1, …, λ_n, которое составляет $r = \dfrac{1}{2}(s+1)(s+2) \leqslant n$. Достаточным условием существования решения служит полный ранг матрицы такой системы. Для этого достаточно отличия от нуля одного из миноров Δ_r порядка r этой $(r \times n)$-матрицы, который служит многочленом степени r от элементов матрицы. Элемент матрицы — это (вообще говоря, неоднородный) многочлен степени не выше второй от коэффициентов линейных форм ℓ_j. Следовательно,

минор Δ_r — это многочлен от коэффициентов линейных форм ℓ_j, степень которого не превышает $2r = (s+1)(s+2)$. Для завершения доказательства нужно показать, что этот многочлен не равен нулю тождественно.

Обозначим через $c(i,k)$ номер пары индексов (i,k), $1 \leqslant i \leqslant k \leqslant s$, принимающий значения от 1 до $r-s-1$. Рассмотрим набор линейных форм $\ell_j = \frac{1}{2}x_0 + x_i + x_k$, где при $s+1 \leqslant j \leqslant r-1$ индексы связаны уравнением $j = s + c(i,k)$. При $j = r$ полагаем $\ell_r = \frac{1}{2}x_0$. При $j > r$ полагаем $\ell_j = 0$.

Уравнение (1) принимает вид $-\frac{1}{4}(\lambda_{s+1} + \ldots + \lambda_r) = 1$. Уравнения типа (2) принимают вид $\lambda_k + 4\lambda_j = 1$, где $1 \leqslant k \leqslant s$ и $j = s + c(k,k)$. Уравнения типа (3) принимают вид $-\lambda_k = 0$, где $1 \leqslant k \leqslant s$. Складывая соответствующие уравнения типов (2) и (3), получим уравнения типа $4\lambda_j = 1$, где $1 \leqslant k \leqslant s$ и $j = s + c(k,k)$. Уравнения типа (4) принимают вид $\lambda_j = 0$, где $1 \leqslant i < k \leqslant s$ и $j = s + c(i,k)$.

Итак, при выбранных линейных формах ℓ_j подсистема без уравнения (1) эквивалентна системе уравнений, каждое из которых зависит от одной из переменных λ_1, $\ldots$, λ_{r-1} без повторений. Число этих уравнений равно $r-1$. Следовательно, эта система имеет единственное решение. Также существует единственное значение λ_r, при котором это решение продолжается до решения уравнения (1). При $n > r$ значения λ_{r+1}, $\ldots$, λ_n могут быть любыми. Поэтому соответствующая матрица имеет полный ранг r, а её угловой минор Δ_r отличен от нуля. ■

Замечание 1. Над полем рациональных чисел $\mathbb{Q}$ битовая вычислительная сложность поиска коэффициентов λ_1, $\ldots$, λ_n также полиномиально ограничена, поскольку задача сводится к решению системы линейных уравнений. При этом суммарный размер двоичных записей чисел на промежуточных шагах вычисления ограничен многочленом от длины входа [1, теорема 3.3, т. 1, с. 55]. Более того, так получается генерический алгоритм полиномиального времени в смысле определения из работ [20–23]. Если на вход поступают рациональные числа, чьи длины двоичных записей ограничены сверху многочленом $\mathrm{poly}(n)$, то верхняя оценка доли тех входов, на которых машина останавливается в состоянии VAGUE, получается из леммы Шварца — Зиппеля [26].

Теорема 2. Для любых натуральных чисел n и s, удовлетворяющих неравенству $2n \geqslant (s+1)(s+2)$, и для почти каждого набора $(n-s)$ линейных форм $\ell_j(x_0, \cdots, x_s)$ для индексов $j > s$ генерическая обобщённая регистровая машина за полиномиальное время распознаёт отсутствие какой-либо $(0,1)$-точки, инцидентной аффинному подпространству, заданному системой уравнений $x_j = \ell_j(1, x_1, \cdots, x_s)$ для индексов $j > s$. Более того, эта машина может остановиться в состоянии VAGUE лишь на таком входе, на котором обращается в нуль некоторый многочлен степени не выше $(s+1)(s+2)$ от коэффициентов линейных форм ℓ_j.

Доказательство. Согласно теореме 1, генерическая обобщённая регистровая машина за полиномиальное время вычисляет такие коэффициенты λ_1, $\ldots$, λ_n, что при значении переменной $x_0 = 1$ выполнено равенство

$$\sum_{k=1}^{s} \lambda_k x_k(x_k - 1) + \sum_{j=s+1}^{n} \lambda_j \ell_j(\ell_j - 1) = 1 + \sum_{k=1}^{s} x_k^2.$$

Этот многочлен нигде не обращается в нуль. Однако он должен обращаться в нуль в каждой $(0,1)$-точке, принадлежащей аффинному подпространству, определяемому

системой уравнений $x_j = \ell_j(1, x_1, \ldots, x_s)$ для индексов $j > s$. Следовательно, такой ответ служит подтверждением, что никакая $(0,1)$-точка не принадлежит этому аффинному подпространству. Иначе машина останавливается в состоянии VAGUE. Оценка степени многочлена, обращающегося при этом в нуль, совпадает с оценкой из теоремы 1. ■

Теорема 3. Существует такое число $\varepsilon > 0$, что для любых чисел α и γ из интервала $(1-\varepsilon, 1+\varepsilon)$ и для любых чисел β, λ_1, λ_2 и λ_3 квадратичная форма от трёх переменных x_0, x_1 и x_2, равная

$$\lambda_1 x_1(x_1 - x_0) + \lambda_2 x_2(x_2 - x_0) + \lambda_3 \left(\alpha x_1 + \beta x_2 - \frac{1}{2}\gamma x_0\right)\left(\alpha x_1 + \beta x_2 - \frac{1}{2}\gamma x_0 - x_0\right),$$

не бывает положительно определена.

Доказательство. При $\alpha = \beta = \gamma = 1$ матрица Гессе квадратичной формы равна

$$\begin{pmatrix} \frac{3}{2}\lambda_3 & -\lambda_1 - 2\lambda_3 & -\lambda_2 - 2\lambda_3 \\ -\lambda_1 - 2\lambda_3 & 2\lambda_1 + 2\lambda_3 & 2\lambda_3 \\ -\lambda_2 - 2\lambda_3 & 2\lambda_3 & 2\lambda_2 + 2\lambda_3 \end{pmatrix}.$$

Её угловой минор второго порядка $\Delta_2 = -\lambda_1\lambda_3 - \lambda_1^2 - \lambda_3^2$ не принимает положительных значений. В общем случае

$$\Delta_2 = \lambda_1(\lambda_3\alpha)\left(\frac{\gamma}{\alpha}(\gamma+2) - 2\gamma - 2\right) - \lambda_1^2 - (\lambda_3\alpha)^2.$$

При малых значениях ε выполнены неравенства

$$-2 < \left(\frac{\gamma}{\alpha}(\gamma+2) - 2\gamma - 2\right) < 0.$$

Поэтому угловой минор второго порядка не принимает положительных значений. Следовательно, эта матрица Гессе (и соответствующая квадратичная форма) не бывает положительно определена ни при каких значениях коэффициентов λ_1, λ_2 и λ_3. ■

3. Обсуждение

Теоремы 1 и 3 имеют ясный геометрический смысл над полем вещественных чисел. Однородные координаты в проективном пространстве нигде не обращаются в нуль одновременно. Следовательно, положительно определённая квадратичная форма задаёт в проективном пространстве алгебраическое множество без вещественных точек — мнимый эллипсоид. Если же квадратичная форма не является знакоопределённой, то она обращается в нуль в некоторой вещественной точке проективного пространства. Эта точка может быть бесконечно удалённой, то есть не принадлежать аффинному пространству.

При $n = 3$ и $s = 1$ из теоремы 1 следует, что прямая общего положения в $\mathbb{R}^3$ не пересекает некоторую поверхность второго порядка, проходящую через все $(0,1)$-точки. Это выполнено и для проективного замыкания.

Согласно теореме 3, каждая проективная плоскость в $\mathbb{RP}^3$, заданная уравнением $x_3 = \alpha x_1 + \beta x_2 - \frac{1}{2}\gamma x_0$, где $\alpha \approx 1$ и $\gamma \approx 1$, пересекает в вещественных точках каждую поверхность второго порядка, проходящую через все $(0,1)$-точки аффинного пространства, в котором $x_0 = 1$. Такие плоскости соответствуют непустому открытому

(в аналитической топологии) множеству в пространстве параметров. Следовательно, условие $2n \geqslant (s+1)(s+2)$ в теореме 1 нельзя ослабить при $n = 3$.

Проверяемое генерическим алгоритмом в доказательстве теоремы 1 достаточное условие можно ослабить, если не требовать быстрой вычислимости искомых коэффициентов $\lambda_1, \ldots, \lambda_n$. С другой стороны, если не вычислять, а недетерминированно угадать эти коэффициенты, то за полиномиальное время можно проверить, будет ли полученная квадратичная форма положительно определена. Поэтому меньше отказов от вычисления может обеспечить недетерминированная обобщённая регистровая машина над упорядоченным полем. Однако теорема 3 показывает, что и в этом случае отсутствие решения $\lambda_1, \ldots, \lambda_n$ не означает отсутствия $(0,1)$-точки, принадлежащей данному подпространству.

Детерминированный генерический алгоритм в теореме 2 либо корректно распознаёт отсутствие двоичного решения у большой системы уравнений, либо даёт неопределённый ответ. С другой стороны, двоичное решение можно искать бинарным поиском, проверяя этим алгоритмом отсутствие двоичных решений при оценках некоторых переменных. Например, если при некоторой $(0,1)$-оценке одной из переменных система не имеет двоичного решения, то число неизвестных уменьшается. Однако при неопределённом ответе требуется проверка новых гипотез. Поэтому в худшем случае требуется перебор большого числа гипотез даже для систем, включающих много линейно независимых уравнений. Теорема 2 не позволила также улучшить результаты о выполнимости 3-КНФ. Хотя обе задачи 3-SAT и NAE-3-SAT сводятся к поиску двоичных решений у системы линейных уравнений, в интересных случаях число линейно независимых уравнений оказывается значительно меньше числа переменных.

Алгоритм в теореме 2 нельзя применить для проверки существования двоичного решения у одного линейного уравнения. Теорема 3 подтверждает это при $n = 3$.

Заключение

Понятие генерического алгоритма распространено на обобщённые регистровые машины над упорядоченным полем. Предложен генерический алгоритм полиномиального времени для распознавания систем линейных уравнений без какого-либо двоичного решения, когда число уравнений m и число неизвестных n связаны неравенством $2n \geqslant (n-m+1)(n-m+2)$. Этот алгоритм распознавания служит для обоснования эвристического метода поиска двоичного решения такой системы уравнений. Однако в худшем случае поиск двоичного решения остаётся вычислительно трудной задачей.

ЛИТЕРАТУРА

1. *Схрейвер А.* Теория линейного и целочисленного программирования. В 2-х т.М.: Мир, 1991. 702 с.
2. *Селиверстов А. В.* О двоичных решениях систем уравнений // Прикладная дискретная математика. 2019. № 45. С. 26–32.
3. *Koiliaris K. and Xu C.* Faster pseudopolynomial time algorithms for subset sum // ACM Trans. Comput. Theory. 2019. V. 15. No. 3. Article 40.
4. *Curtis V. V., Sanches C. A. A.* An improved balanced algorithm for the subset-sum problem // European J. Operational Res. 2019. V. 275. P. 460–466.
5. *Mucha M., Węgrzycki K., and Włodarczyk M.* A subquadratic approximation scheme for partition // Proc. Ann. ACM-SIAM Symp. Discrete Algorithms. Philadelphia: SIAM, 2019. P. 70–88.

6. *Schroeppel R. and Shamir A.* A $T = O(2^{n/2})$, $S = O(2^{n/4})$ algorithm for certain NP-complete problems // SIAM J. Computing. 1981. V. 10. No. 3. P. 456–464.
7. *Bansal N., Garg S., Nederlof J., and Vyas N.* Faster space-efficient algorithms for subset sum, k-sum, and related problems // SIAM J. Computing. 2018. V. 47. No. 5. P. 1755–1777.
8. *Grigoriev D.* Complexity of Positivstellensatz proofs for the knapsack // Comput. Complexity. 2001. V. 10. P. 139–154.
9. *Mucha M., Nederlof J., Pawlewicz J., and Węgrzycki K.* Equal-subset-sum faster than the meet-in-the-middle // 27th Ann. Europ. Symp. Algorithms, ESA 2019. Leibniz Intern. Proc. Informatics, LIPIcs. V. 144. Schloss Dagstuhl, Leibniz-Zentrum für Informatik, 2019. Article 73.
10. *Goerdt A. and Lanka A.* Recognizing more random unsatisfiable 3-SAT instances efficiently // Electronic Notes in Discrete Math. 2003. V. 16. P. 21–46.
11. *Brown-Cohen J. and Raghavendra P.* Extended formulation lower bounds for refuting random CSPs // Proc. ACM-SIAM Symp. Discrete Algorithms. Philadelphia: SIAM, 2020. P. 305–324.
12. *Deshpande Y., Montanari A., O'Donnell R., et al.* The threshold for SDP-refutation of random regular NAE-3SAT // Proc. Ann. ACM-SIAM Symp. Discrete Algorithms. Philadelphia: SIAM, 2019. P. 2305–2321.
13. *Neumann E. and Pauly A.* A topological view on algebraic computation models // J. Complexity. 2018. V. 44. P. 1–22.
14. *Blum L., Shub M., and Smale S.* On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines // Bull. American Mathematical Society (N.S.). 1989. V. 21. No. 1. P. 1–46.
15. *Даниярова Э. Ю., Мясников А. Г., Ремесленников В. Н.* Алгебраическая геометрия над алгебраическими системами. IX. Главные универсальные классы и Dis-пределы // Алгебра и логика. 2018. Т. 57. № 6. С. 639–661.
16. *Алаев П. Е., Селиванов В. Л.* Поля алгебраических чисел, вычислимые за полиномиальное время. I // Алгебра и логика. 2019. Т. 58. № 6. С. 673–705.
17. *Алаев П. Е.* Полиномиально вычислимые структуры с конечным числом порождающих // Алгебра и логика. 2020. Т. 59. № 3. С. 385–394.
18. *Коточигов А. М., Сучков А. И.* Метод сокращения перебора в алгоритмах построения минимальных аддитивных цепочек // Компьютерные инструменты в образовании. 2020. № 1. С. 5–18.
19. *Селиверстов А. В.* Симметричные матрицы, элементами которых служат линейные функции // Журн. вычислительной математики и математической физики. 2020. Т. 60. № 1. С. 109–115.
20. *Рыбалов А. Н.* О генерической неразрешимости десятой проблемы Гильберта для полиномиальных деревьев // Прикладная дискретная математика. 2019. № 44. С. 107–112.
21. *Рыбалов А. Н.* О генерической NP-полноте проблемы выполнимости булевых схем // Прикладная дискретная математика. 2020. № 47. С. 101–107.
22. *Рыбалов А. Н.* О генерической сложности проблемы представимости натуральных чисел суммой двух квадратов // Прикладная дискретная математика. 2020. № 48. С. 93–99.
23. *Рыбалов А. Н.* О генерической сложности экзистенциальных теорий // Прикладная дискретная математика. 2020. № 49. С. 120–126.
24. *Harris J. and Tu L. W.* On symmetric and skew-symmetric determinantal varieties // Topology. 1984. V. 23. No. 1. P. 71–84.
25. *Malaschonok G. and Scherbinin A.* Triangular decomposition of matrices in a domain // LNCS. 2015. V. 9301. P. 292–306.

26. *Schwartz J. T.* Fast probabilistic algorithms for verification of polynomial identities // J. ACM. 1980. V. 27. No. 4. P. 701–717.

REFERENCES

1. *Schrijver A.* Theory of linear and integer programming. New York, John Wiley & Sons, 1986.
2. *Seliverstov A. V.* O dvoichnykh resheniyakh sistem uravneniy [On binary solutions to system of equations]. Prikladnaya Diskretnaya Matematika, 2019, no. 45, pp. 26–32. (in Russian)
3. *Koiliaris K. and Xu C.* Faster pseudopolynomial time algorithms for subset sum. ACM Trans. Comput. Theory, 2019, vol. 15, no. 3, article 40.
4. *Curtis V. V. and Sanches C. A. A.* An improved balanced algorithm for the subset-sum problem. European J. Operational Res., 2019, vol. 275, pp. 460–466.
5. *Mucha M., Węgrzycki K., and Włodarczyk M.* A subquadratic approximation scheme for partition. Proc. Ann. ACM-SIAM Symp. Discrete Algorithms, 2019, pp. 70–88.
6. *Schroeppel R. and Shamir A.* A $T = O(2^{n/2})$, $S = O(2^{n/4})$ algorithm for certain NP-complete problems. SIAM J. Computing, 1981, vol. 10, no. 3, pp. 456–464.
7. *Bansal N., Garg S., Nederlof J., and Vyas N.* Faster space-efficient algorithms for subset sum, k-sum, and related problems. SIAM J. Computing, 2018, vol. 47, no. 5, pp. 1755–1777.
8. *Grigoriev D.* Complexity of Positivstellensatz proofs for the knapsack. Comput. Complexity, 2001, vol. 10, pp. 139–154.
9. *Mucha M., Nederlof J., Pawlewicz J., and Węgrzycki K.* Equal-subset-sum faster than the meet-in-the-middle. 27th Ann. European Symp. Algorithms, ESA 2019. Leibniz Intern. Proc. Informatics, LIPIcs, vol. 144, Schloss Dagstuhl, Leibniz-Zentrum für Informatik, 2019. Article 73.
10. *Goerdt A. and Lanka A.* Recognizing more random unsatisfiable 3-SAT instances efficiently. Electronic Notes in Discrete Math., 2003, vol. 16, pp. 21–46.
11. *Brown-Cohen J. and Raghavendra P.* Extended formulation lower bounds for refuting random CSPs. Proc. ACM-SIAM Symp. Discrete Algorithms, 2020, pp. 305–324.
12. *Deshpande Y., Montanari A., O'Donnell R., et al.* The threshold for SDP-refutation of random regular NAE-3SAT. Proc. Ann. ACM-SIAM Symp. Discrete Algorithms, 2019, pp. 2305–2321.
13. *Neumann E. and Pauly A.* A topological view on algebraic computation models. J. Complexity, 2018, vol. 44, pp. 1–22.
14. *Blum L., Shub M., and Smale S.* On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. Bull. American Mathematical Society (N.S.), 1989, vol. 21, no. 1, pp. 1–46.
15. *Daniyarova E. Yu., Myasnikov A. G., and Remeslennikov V. N.* Algebraic geometry over algebraic structures. IX. Principal universal classes and Dis-limits. Algebra and Logic, 2019, vol. 57, no. 6, pp. 414–428.
16. *Alaev P. E. and Selivanov V. L.* Fields of algebraic numbers computable in polynomial time. I. Algebra and Logic, 2020, vol. 58, no. 6, pp. 447–469.
17. *Alaev P. E.* Polynomially computable structures with finitely many generators. Algebra and Logic, 2020, vol. 59, no. 3, pp. 266–272.
18. *Kotochigov A. M. and Suchkov A. I.* Metod sokrashcheniya perebora v algoritmakh postroeniya minimal'nykh additivnykh tsepochek [A method for reducing iteration in algorithms for building minimal additive chains]. Komp'yuternye Instrumenty v Obrazovanii, 2020, no. 1, pp. 5–18. (in Russian).
19. *Seliverstov A. V.* Symmetric matrices whose entries are linear functions. Comput. Math. and Math. Physics, 2020, vol. 60, no. 1, pp. 102–108.

20. *Rybalov A. N.* O genericheskoy nerazreshimosti desyatoy problemy Gil'berta dlya polinomial'nykh derev'ev [On generic undecidability of Hilbert's tenth problem for polynomial trees]. Prikladnaya Diskretnaya Matematika, 2019, no. 44, pp. 107–112. (in Russian).
21. *Rybalov A. N.* O genericheskoy NP-polnote problemy vypolnimosti bulevykh skhem [On generic NP-completeness of the problem of Boolean circuits satisfiability]. Prikladnaya Diskretnaya Matematika, 2020, no. 47, pp. 101–107. (in Russian).
22. *Rybalov A. N.* O genericheskoy slozhnosti problemy predstavimosti natural'nykh chisel summoy dvukh kvadratov [On generic complexity of the problem of representation of natural numbers by sum of two squares]. Prikladnaya Diskretnaya Matematika, 2020, no. 48, pp. 93–99. (in Russian).
23. *Rybalov A. N.* O genericheskoy slozhnosti ekzistentsial'nykh teoriy [On generic complexity of the existential theories]. Prikladnaya Diskretnaya Matematika, 2020, no. 49, pp. 120–126. (in Russian).
24. *Harris J. and Tu L. W.* On symmetric and skew-symmetric determinantal varieties. Topology, 1984, vol. 23, no. 1, pp. 71–84.
25. *Malaschonok G. and Scherbinin A.* Triangular decomposition of matrices in a domain. LNCS, 2015, vol. 9301, pp. 292–306.
26. *Schwartz J. T.* Fast probabilistic algorithms for verification of polynomial identities. J. ACM, 1980, vol. 27, no. 4, pp. 701–717.

UDC 512.54 DOI 10.17223/20710410/52/2

ALGORITHMIC THEORY OF SOLVABLE GROUPS[1]

V. A. Roman'kov

Dostoevsky Omsk State University, Omsk, Russia

E-mail: romankov48@mail.ru

The purpose of this survey is to give some picture of what is known about algorithmic and decision problems in the theory of solvable groups. We will provide a number of references to various results, which are presented without proof. Naturally, the choice of the material reported on reflects the author's interests and many worthy contributions to the field will unfortunately go without mentioning. In addition to achievements in solving classical algorithmic problems, the survey presents results on other issues. Attention is paid to various aspects of modern theory related to the complexity of algorithms, their practical implementation, random choice, asymptotic properties. Results are given on various issues related to mathematical logic and model theory. In particular, a special section of the survey is devoted to elementary and universal theories of solvable groups. Special attention is paid to algorithmic questions regarding rational subsets of groups. Results on algorithmic problems related to homomorphisms, automorphisms, and endomorphisms of groups are presented in sufficient detail.

Keywords: *solvable groups, algorithmic and decision problems, algorithms.*

1. Introduction

Awareness of the algebraic nature of many important concepts of topology and function theory in the 1880s led to the formation of a combinatorial group theory. Groups, already represented in the works of F. Klein, H. Poincare and other mathematicians, gained the right to independence after W. Dick discovered a universal way to define them using generators and defining relations [50]. H. Poincare [198, 199] established the first contacts between combinatorial topology and group theory. He introduced the fundamental groups of manifolds into consideration, while at the same time finitely defined groups of finite simplicial complexes were distinguished as effective objects. E. S. Fedorov [58] discovered a remarkable application of groups to the geometry of crystals. F. Klein proposed in his inaugural lecture in 1872 at the University of Erlangen (Germany) the famous *Erlangen program*, classifying geometries by their basic symmetry groups [106]. This program is an influential synthesis of much of the mathematics of the time.

It turned out that many important topology problems are algorithmic in nature. At the very beginning of the twentieth century, the basic algorithmic problems were formulated for a class of finitely defined groups. The word problem was posed by M. Dehn [42]: Is there an algorithm that, from two arbitrary group words from the generating elements of the group, determines whether they define the same element of the group? H. Tietze [250] developed the Tietze transformations for group presentations, and was the first to pose the group isomorphism problem: Is there an algorithm that finds out, from two arbitrary finite group

[1]Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-11-50063.

assignments by generating elements and defining relations, whether these assignments define isomorphic groups?

From the very beginning, combinatorial group theory was closely intertwined with computability theory. We are currently seeing many new successful interactions between group theory and computer science. Complexity theory and automata theory began to play more important role in the group theory, especially in the algorithmic directions. Questions of random choice and asymptotic properties of groups have acquired significant importance. On the other hand, various mathematical fields such as algebraic cryptography and data compression have led to new questions in group theory.

More than thirty-five years ago, the author, together with V. N. Remeslennikov, published the survey [210], devoted to the algorithmic and model-theoretic questions in group theory. The survey is widespread, its objective was to give a fairly complete description of group-theoretic results of an algorithmic nature in their historical development, as well as to present the methods of model-theoretical research in group theory. These two lines of research are closely interrelated and have a common focus, as they seek to answer one general question: what properties and characteristics of groups can be effectively identified? Some aspects of this research are reflected in [152, 186].

V. N. Remeslennikov

The content of the papers [186, 210] and the monograph [152] is largely due to the significantly increased interest in research in combinatorial group theory at that time. This area was formed in the 60–70s of the twentieth century. Two monographs with the same title "Combinatorial group theory" written by W. Magnus, A. Karrass and D. Solitar [132], and by R. Lyndon and P. Shupp [125] played a significant role in its formation. The title of [132] has a subtitle "Representation of groups in terms of generators and relations". These monographs laid the foundations for combinatorial group theory as one of the most actively developing areas of group theory and mathematics in general in the following decades to our time. Both monographs were translated into Russian and subsequently reprinted several times. W. Magnus et al.'s book focuses on representing groups in terms of generators and defining relations. The authors consider free constructions: free groups and products, free amalgamated products, Higman — Neumann — Neumann (HNN) extensions. The term "combinatorial" itself arose from the frequent and significant use of combinatorial methods. The book touched on algorithmic problems, from the classic Dehn problems to problems that only arose at that time. The value of the book [132] for the further development of the combinatorial group theory is very great. It is a tutorial, a problem source, and a research sample.

The book [125] is clearly an important contribution to the mathematical literature. It contains proof of Whitehead's theorems and related theorems by J. McCool, proof of the Karrass — Solitar theorem on subgroups of free products with one amalgamated subgroup by Nielsen methods and its obvious promise applications. It also contains discussion of cohomology, graph-theoretical connections, discussion of HNN extensions, elegant treatment of one-relator groups, proof of the Higman embedding theorem, connections with logic, the use of van Kampen diagrams and the consideration of small cancellation theory and its applications are very good advances.

The history of combinatorial group theory is described by W. Magnus and B. Chandler in [34]. Results on combinatorial algebra are presented in the monograph by L. A. Bokut and G. P. Kukin [32]. O. Kharlampovich and M. Sapir presented in [103] a survey of results on algorithmic problems in varieties of algebraic systems.

The origins of the theory of solvable (some authors use the term "soluble") groups go back to the first half of the nineteenth century, when Évariste Galois determined a necessary and sufficient condition for a polynomial to be solvable by radicals, thereby solving a problem standing for 350 years. His work laid the foundations for Galois theory and group theory, two major branches of abstract algebra. He realized that the algebraic solution to a polynomial equation is related to the structure of a group of permutations associated with the roots of the polynomial, the Galois group of the polynomial. He found that an equation could be solved in radicals if one can find a series of subgroups of its Galois group, each one normal in its successor with abelian quotient, or its Galois group is solvable.

Évariste Galois

This proved to be a fertile approach, which later mathematicians adapted to many other fields of mathematics besides the theory of equations to which Galois originally applied it. The achievements of Galois theory stimulated intensive study of permutation groups, and indeed in the early stages of its development, group theory was preoccupied almost exclusively with finite groups.

However, under the influence of geometry, topology, and the theory of differential equations, there arose a pressing need to consider infinite groups of transformations. The theory of infinite groups began to develop in the 20s of the twentieth century. Free groups first arose in the study of hyperbolic geometry, as examples of Fuchsian groups (discrete groups acting by isometries on the hyperbolic plane). The algebraic study of free groups was initiated by Jakob Nielsen in 1920s, who gave them their name and established many of their basic properties [179, 180]. Otto Schreier published an algebraic proof of the Nielsen — Schreier theorem in [243]. Max Dehn realized the connection of groups with topology, and obtained the first proof of the Nielsen — Schreier theorem [42]. Kurt Reidemeister included a comprehensive treatment of free groups in [204] and in his book [205], the first monograph on combinatorial group theory and topology. Parametric groups made their appearance in the works of S. Lie [114].

In the 1930s of the twentieth ccentury, Wilhelm Magnus invented the connection between the lower central series of free groups and free Lie algebras (see [133]).

Wilhelm Magnus

From the Preface of [133]: "Magnus has had such a profound influence on combinatorial group theory because many of his ideas, startingly and strikingly simple, have provided not only deep insights into a very difficult subject but also powerful methods for dealing with these difficulties. His ideas have also found application in topology, K-theory, the theory of Lie and associative algebras, computational complexity, and also in logic. The expert in group theory, however, will be astonished to find that this reprinting of Magnus' papers contains a very large amount of very important work on diffraction problems and related topics in analysis. Indeed Magnus is one of the very few mathematicians who has done significant work in two completely different fields. There is a large number of mathematicians who know Magnus for his work in analysis but are totally unaware of his work in group theory. His books, his teaching, his many doctoral students, his effect on the thinking of his colleagues both in private conversation and in seminars have also helped to establish him as a mathematician of the first rank and enriched the mathematical community." — G. Baumslag and B. Chandler.

Intensive research on solvable groups began in the 30s of the twentieth century. This research was initiated by P. Hall, who just completed his great sequence of papers on finite solvable groups [83]. His PhD-student K. A. Hirsch published a sequence of five papers [85 –

89], where he introduced and investigated polycyclic groups. From the very beginning it became clear that the theory of infinite solvable groups needs in some original methods of studying. It turned out later that the methods come from ring theory, matrix group theory and homological algebra. Thus, the theory of infinite solvable groups has a broader connection in algebra.

In 1950s A. I. Mal'cev established the basic theory of solvable matrix groups [141]. He also invented the notion of a rank and investigated solvable groups of finite rank [139]. He showed the undecidability of the elementary theory of finite groups, of free nilpotent groups, of free soluble groups and many others. This Mal'cev's works determined the perspective direction of research for many years.

A. I. Mal'cev is a great mathematician known for his fundamental achievements in algebra and mathematical logic. He is one of the founders of the general theory of algebraic systems and model theory and the founder of the Siberian School of Algebra and Logic.

At the same time, P. Hall made a significant contribution to the development of the theory of soluble groups. Namely, he published a series of papers [78 – 82] on finitely generated solvable and nilpotent groups. In these papers, he proved a number of results that are important in theory and determine further research in this area.

Since that time the solvable group theory became one of the central topics in group theory.

Solvable groups are interesting not only in and of themselves. They are an effective tool for investigating more general objects of group theory. Suffice it to recall the Sylow subgroups, solvable radicals, Borel subgroups and so on. Below we give two examples of the results obtained by passing to solvable factor groups.

The following result was proposed by M. Dehn and proved by his student, W. Magnus, in his doctoral thesis (see [129]). It is well-known as the *freedom theorem* of Magnus or

The *Freiheitssatz*: Let

$$G = \langle x_1, \ldots, x_n : r \rangle$$

be a group presentation given by n generators x_i and a single cyclically reduced relator r. If x_1 appears in r, then the subgroup of G generated by $x_2, \ldots, x_n$ is a free group, freely generated by $x_2, \ldots, x_n$.

Magnus' method of proof of the Freiheitssatz relies on free amalgamation products of groups. This method initiated the use of these products in the study of infinite discrete groups.

N. S. Romanovskii used a different approach in his proving the *generalized freedom theorem* for groups with several relations (solution of the Lyndon problem) [217]: Let the group

$$G = \langle x_1, \ldots, x_n : r_1, \ldots, r_m \rangle$$

have deficiency $d = n - m > 0$. Then there exist a subset of d of the given generators which freely generates a subgroup of G isomorphic to F_d. A similar assertion was also proved for groups defined by generators and relations in varieties of solvable and nilpotent groups and pro-p groups. He essentially used solvable groups as a tool for these proofs.

In [228], the author proved that the automorphism group of the free pro-p group $\tilde{F}_r(p)$ of rank $r \geqslant 2$ is topologically infinitely generated. A similar assertion was also proved for free profinite groups $\tilde{F}_r$ and for free metabelian pro-p groups $M_r(p)$. His methods of proofs are also related to solvable groups.

The modern theory of solvable groups is presented in the monograph [113] by J. C. Lennox and D. J. S. Robinson. See also the author's monograph [239]. The theory of nilpotent groups is presented in the lectures [9] by G. Baumslag and [82] by P. Hall.

The main object of research in the monograph by E. I. Timoshenko [256] — free groups in varieties of solvable groups and their universal theories. In addition, groups of automorphisms and semigroups of endomorphisms of solvable groups are described. A significant part of the results belongs to the author of the monograph.

Algebraic geometry over groups arose in the mid-90s of the twentieth century in the works of B. I. Plotkin [194, 195] on the one hand and in the works of G. Baumslag, V. N. Remeslennikov, A. G. Myasnikov and O. G. Kharlampovich [17, 168, 101, 102] on the other. The current state of algebraic geometry over groups and more generally over algebraic systems is presented in [196, 197], and in [41].

2. Algorithmic problems

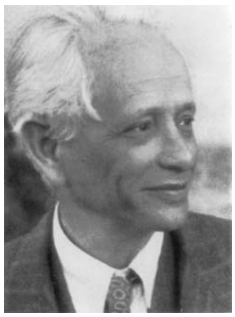
In the very beginning of the twentieth century M. Dehn and H. Titze proposed the following three algorithmic problems:

- The word problem (Dehn [42]): Given a group presentation $G = \langle X : R\rangle$ and words $w(X), u(X)$ in the alphabet X determine if $w(X) =_G u(X)$.
- The conjugacy problem (Dehn [42]): Given a group presentation $G = \langle X : R\rangle$ and words $w(X), u(X)$ in the alphabet X determine if there exists some $g(X)$ such that $g(X)^{-1}w(X)g(X) =_G u(X)$.
- The isomorphism problem (Tietze [250]): Given two group presentations $G = \langle X : R\rangle$ and $H = \langle Y : S\rangle$ determine if they define isomorphic groups.

Subsequently, the following problem began to be added to this list of problems:

- The subgroup membership problem: Given a group presentation $G = \langle X : R\rangle$ and a finite set of words $g(X), w_1(X), \ldots, w_k(X)$ in the alphabet X find out whether or not $g(X) \in \mathrm{gp}(w_1(X), \ldots, w_k(X))$.

The subgroup membership problem is often called the *generalized word problem* or simply *the membership problem* in the literature of combinatorial group theory.



Max Dehn

Until the 1950s of the twentieth century only positive results could be obtained since totally new methods were needed even to state the problem of finding a group with unsoluble word problem with the formal precision. In particular, W. Magnus published in [130] a complete proof of the solution of the word problem for the class of one-relator groups.

The proof of the algorithmic undecidability of the word problem in the class of all finitely defined groups, obtained by Petr Sergeevich Novikov in 1952 is one of the best results in algorithmic group theory and mathematics in general.

Theorem 1 (P. S. Novikov [187, 188]). There exists a finitely presented group G such that the word problem for G is undecidable.

A wonderful example of P. S. Novikov was of fundamental importance for further research on algorithmic issues in group theory. Obviously conjugacy and membership problems are also unsolvable in the class of finitely presented groups.

W. W. Boone gave in [33] an independent proof of Novikov's result. See [267] for some other results on the word problem in groups.

Let us especially note the importance of the work of S. I. Adian [1], in which a number of algorithmic problems are solved. In particular, he showed the undecidability of the isomorphism problem in the class of finitely defined groups. S. I. Adian in some his proofs based on the idea of the following Markov property.

Markov Property: An abstract property $\mathbb{P}$ of finitely presented groups is a *Markov property* if there are two finitely presented groups G^+ and G^- such that

— G^+ has property $\mathbb{P}$;
— G^- cannot be embedded as a subgroup in any finitely presentable group with property $\mathbb{P}$.

Theorem 2 (S. I. Adian [1]). If $\mathbb{P}$ is a Markov property of finitely presented groups, then $\mathbb{P}$ is not recursively recognisable.

Therefore, the following properties of finitely defined groups are not recognized recursively, namely: to be trivial (finite, abelian, nilpotent, solvable, free, torsion-free, or residually finite) group, having a solvable word problem, and so on.

M. O. Rabin [201] proved similar results, which are now called the *Adian — Rabin theorem.*

S. I. Adian and V. G. Durnev [2] presented a detailed survey of results concerning the main decision problems of group theory and semigroup theory. They discuss results on the word problem, isomorphism problem, recognition problems, and other algorithmic questions related to them. The classical theorems of A. A. Markov and E. L. Post, P. S. Novikov, S. I. Adian and M. O. Rabin, G. Higman, W. Magnus, and R. C. Lyndon are given with complete proofs.

Further in the paper, we do not present here other results of algorithmic theory pertaining to classes of groups other than solvable.

For simplicity, we will simplify expressions, speaking not about group representations, but about groups, not about words in the generators of a given representation, but about group elements, etc.

After the obtained negative results on the solvability of algorithmic problems in the class of all finitely defined groups, the interest of researchers was turned to various classes of groups. The methods of assigning groups have expanded. The algorithmic problems themselves became more diverse. Algorithmic problems of the following two types began to be considered:

— *Decision problems*: Given a property $\mathbb{P}$ and an object $\mathcal{O}$, find out whether or not the object $\mathcal{O}$ has the property $\mathbb{P}$.
— *Search problems*: Given the property $\mathbb{P}$ and the information "$\mathcal{O}$ satisfies $\mathbb{P}$", find out at least one specific implementation of $\mathbb{P}$ to $\mathcal{O}$.

For example, if we know that elements w and u are conjugate in the group G, the search problem is to find a conjugating element $g \in G$ such that $g^{-1}wg = u$.

The issues of solvability of search problems are especially important for applications and algorithms used in practice. For theory and practical applications, the complexity of the algorithms is essential. At present, the issues of the complexity of algorithms, in particular — computational complexity, have become of paramount importance. There is a huge amount of research in this area. Some results related to the complexity of algorithms for solvable groups will be touched upon in this review.

Friendly definitions:

— Sol = solvable groups;

— ThAlg(Sol) — Algorithmic theory of Sol = Information about Sol-groups, their elements, subgroups, subsets, structure, etc., that can, in principle at least, be obtained by machine computation, namely Turing machines, automata, computers, and so on.

Relative presentation in the variety $\mathfrak{L}$:

$$G = \langle x_1, \dots, x_n : \{r_\lambda : \lambda \in \Lambda\}; \mathfrak{L}\rangle.$$

That is

$$G = F(X, \mathfrak{L})/ncl\{r_\lambda : \lambda \in \Lambda\},$$

where $F(X, \mathfrak{L})$ is a free group in the variety $\mathfrak{L}$ with basis $X = \{x_1, \dots, x_n\}$, and Λ is finite or, more generally, recursive enumerable set.

Presentation by generators:

$$G = \mathrm{gp}(g_1, \dots, g_n) \leqslant \bar{G},$$

where $\bar{G}$ is some bigger group, for example, $\bar{G} = GL_n(K)$, the general linear (matrix) group over K, or $\bar{G} = \pi_1(S)$, the fundamental group of a topological space S.

Presentation by action:

$$G = Aut(H),$$

where H is some other group (more generally, some structure), or

$$G = \pi_1(S),$$

where S is some topological space.

Classical algorithmic problems:

For a group G:

— *The word problem* (WP): $w = 1$?
— *The conjugacy problem* (CP): $\exists g : g^{-1}wg = u$?
— *The membership problem* (MP): $w \in H \leqslant G$?

For a class of groups $\mathcal{C}$:

— *The isomorphism problem* (IP): $G \simeq H$?

We also highlight the following two problems concerning automorphisms and homomorphisms, which can also be considered classical because of their high importance. The first problem is formulated for an arbitrary group G:

— *The automorphic conjugacy problem* (J. H. C. Whitehead [266]): Is there an algorithm that finds out from two arbitrary group words from the generating elements of the group, do they determine automorphically conjugate elements of the group? In other words, is there an automorphism of a group that takes one of the given elements to another?

The automorphism problem for a free group F_r of rank r was algorithmically solved by J. H. C. Whitehead himself in a classic 1936 paper [266] and his solution came to be known as *Whitehead's algorithm*. This proof was topological.

Subsequently, E. S. Rapaport [202] and later, based on her work, P. J. Higgins and R. C. Lyndon in [84] gave a purely combinatorial and algebraic re-interpretation of Whitehead's algorithm. The exposition of Whitehead's algorithm in the book of R. Lyndon and P. Schupp [125] is based on this combinatorial approach.

In 1946, Emil Post [200] invented the following

The Post correspondence problem (PCP). Given an alphabet Σ, an instance of PCP is a finite set of pairs of strings (g_i, h_i), where $1 \leqslant i \leqslant s$, over Σ. A solution to this instance is a sequence of selections $i_1, i_2, \ldots$ (repetition is possible) such that

$$g_{i_1} g_{i_2} \ldots g_{i_n} = h_{i_1} h_{i_2} \ldots h_{i_n}.$$

Is an effective procedure answering for any instance on the question: Does a solution exist for this instance?

It was also proved in [200] that PCP in the classical setting is unsolvable.

This gives rise to a more general definition often found in the literature, according to which any two homomorphisms α, β with a common domain F and a common codomain G form an instance of the Post correspondence problem, which now asks whether there exists a nonempty word $w \in F$ such that $\alpha(w) = \beta(w)$.

Obviously, PCP can be posed for a free algebraic system F.

PCP(F): For a pair of endomorphisms $\alpha, \beta \in \mathrm{End}(F)$, is there a (nontrivial) element (word) $w \in F$ such that $\alpha(w) = \beta(w)$?

Moreover, PCP can be formulated for any algebraic system A as follows. Let $F(A)$ be a free algebraic system in the variety $\mathrm{Var}(A)$ generated by A, and $\alpha, \beta : F(A) \to A$ be a pair of homomorphisms.

PCP(A): Is there a (nontrivial) element (word) $w \in F(A)$ such that $\alpha(w) = \beta(w)$?

Thus, we can formulate PCP for any group G.

— Let $F(G)$ be a free group in the variety $\mathrm{Var}(G)$ generated by G, and $\alpha, \beta : F(G) \to G$ be a pair of homomorphisms. Is there a nontrivial element $w \in F(G)$ such that $\alpha(w) = \beta(w)$?

In this paper we give a special Section 7 devoted to the Post correspondence problem and its generalizations.

A word $u(x) = u(x_1, \ldots, x_r)$ in certain variables $x = (x_1, \ldots, x_r)$ is called an *identity* in a group G if under substitution of any sequence $g = (g_1, \ldots, g_r)$ of elements of G into $u(x)$ in place of x we obtain the equality $u(g) = 1$. In other words, G satisfies the identity $u(x) \equiv 1$. A quasi-identity is an implication of the form $u_1(x) = 1 \wedge \ldots \wedge u_n(x) = 1 \to u(x) = 1$.

The I-theory (Q-theory) of a class $\mathcal{C}$ of groups is the totality of all identities (quasi-identities) that are true on all the groups in $\mathcal{C}$.

A. I. Mal'cev posed in [108] (Question 2.40 (a)) the following *identity (quasi-identity) problem*: Does there exist a finitely axiomatizable variety of groups whose I-theory (Q-theory) is non-decidable?

Further decision problems:

For a group G:

— *The twisted conjugacy problem* (TCP): For endomorphism $\varphi \in \mathrm{End}(G))$ and elements $g, f \in G$ to decide whether there exists an element $x \in G$ such that $\varphi(x)g = fx$.

— *The bi-twisted conjugacy problem* (BTCP): For endomorphisms $\varphi, \psi \in \mathrm{End}(G))$ and elements $g, f \in G$ to decide whether there exists an element $x \in G$ such that $\varphi(x)g = f\psi(x)$.

— *The generation and presentation problem* (GPP):
Find generators or presentation of a subgroup, centralizer, an automorphism group, etc.

— *The equation problem* (EqP):

$$\exists x_1 \ \ldots \ \exists x_n \big(w(x_1, \ldots, x_n) = 1\big)?$$

— *The endomorphism* (*automorphism*) *problem* (EndoP or AutoP):

$$\exists \varphi \in \mathrm{End}(G)\ (\mathrm{Aut}(G))\big(\varphi(g) = f\big)?$$

For a class $\mathcal{C}$ of groups:

— *The epimorphism problem* (EpiP): $\exists \varphi \in \mathrm{Hom}(G, H)\big(\varphi(G) = H\big)$?

Recall that a group G is called *residually finite* if for each nontrivial element $g \in G$ there exists a finite group K and a homomorphism $\varphi : G \to K$ such that $\varphi(g) \neq 1$. A. I. Mal'cev proved that every finitely presented residually finite group G has the decidable WP [142].

3. Finitely generated nilpotent and polycyclic groups

In his series of papers [78 – 72] P. Hall established a remarkable connection between the theory of polycyclic groups and commutative algebra.

Philip Hall

He noted that, since the class of finitely presented groups is closed under extensions, polycyclic groups are finitely presented. These groups satisfies max, the maximal condition for subgroups, and they admit many other nice properties.

A. I. Mal'cev [142] showed that residual finiteness of some recursive enumerable property $\mathbb{P}$ of a group G implies decidability of $\mathbb{P}$ in G. Subsequently, many proofs of the solvability of algorithmic problems were based on the corresponding finite residuality.

Classical decision problems. Positive solutions:

— M. F. Newman [178]: the conjugacy problem is solvable for any finitely generated nilpotent group.

— S. Blackburn [31]: every finitely generated nilpotent group G is *conjugacy separable*, i.e., residually finite with respect to the conjugacy property. In other words, for every pair $g, f \in G$ of elements that are not conjugate in G there is a homomorphism $\mu : G \to K$ onto finite group K for which $\mu(g), \mu(f)$ are not conjugate in K.

— V. N. Remeslennikov [206] and E. Formanek [59]: every polycyclic group is conjugacy separable. Therefore, the conjugacy problem for any polycyclic group is decidable.

Let $Fin(G)$ denote the set of isomorphism classes of finite quotients of the group G. Two groups G and H are said to *have the same finite quotients* if $Fin(G) = Fin(H)$. Obviously, for a finitely generated abelian group A we have $Fin(A) = \{A\}$. G. A. Noskov proved that $Fin(M) = \{M\}$ for any free metabelian group M [184].

P. F. Pickel constructed infinitely many nonisomorphic finitely presented metabelian groups with the same finite quotients, using modules over a suitably chosen ring [193]. These groups also give an example of infinitely many nonisomorphic split extensions of a fixed finitely presented metabelian group by a fixed finite abelian group, all having the same finite quotients. G. Baumslag proved that there exists non-isomorphic meta-cyclic groups G and H for which $Fin(G) = Fin(H)$ [10].

F. Grunewald and P. Zalesskii introduced in [72] a notion of a *genus* $g(\mathcal{C}, G)$ for a class of groups $\mathcal{C}$ and $G \in \mathcal{C}$. It consists of isomorphism classes of groups from $\mathcal{C}$ having the same profinite completion as G. They showed finiteness results for $g(\mathcal{C}, G)$ for several important families of groups including finitely generated virtually free groups. They also developed formulas for the number of elements in $g(\mathcal{C}, G)$ in various cases. By these they found interesting examples where $g(\mathcal{C}, G)$ contains only one element.

Let G be a finitely generated group. By $\tilde{G}$ we denote the profinite completion of G, G and $\tilde{G}$ have the same finite quotients. The key result to formalize the precise connection

between the collection of finite quotients of G and those of $\tilde{G}$ is the following. Suppose that G and H are finitely generated abstract groups. Then $\tilde{G}$ and $\tilde{H}$ are isomorphic if and only if $Fin(G) = Fin(H)$. This is basically proved in [47]. A. W. Reid [203] introduced the mild difference in the statement by emploing the great result by N. Nikolov and D. Segal [182] to replace topological isomorphism with isomorphism.

Now we list the known positive results on the Isomorphism problem for the classes $\mathcal{N}$ and $\mathcal{P}$ of finitely generated nilpotent and polycyclic groups, respectively:

— P. F. Pickel [192] proved that the genus of every finitely generated nilpotent group N is finite. Consequencly, the isomorphism problem to a fixed finitely generated nilpotent group N is decidable.
— F. Grunewald, P. F. Pickel, and D. Segal [69] established that every $g(\mathcal{PF})$-class of polycyclic-by-finite groups is the union of finitely many isomorphism classes.
— F. Grunewald and D. Segal [70, 71] constructed some rather general algorithms, which can (in theory) be applied in diverse situations. In particular, they gave an algorithm that solves the isomorphism problem for finitely generated nilpotent groups.
— R. A. Sarkisjan [241, 242] independently solved the isomorphism problem for finitely generated nilpotent groups under certain conditions, the validity of which was not known at that time. Later it turned out that the condition is met.

Theorem 3 (D. Segal [244]). There is an algorithm which does the following: given a finitely presented virtually polycyclic group G, given elements $a_1, \ldots, a_n, b_1, \ldots, b_n$ of G, and given finitely generated subgroups $A_1, \ldots, A_m, B_1, \ldots, B_m$ of G, it decides whether there exists an automorphism α of G such that $\alpha(a_i) = b_i$ (and $\alpha(A_i) = B_i$) for $i = 1, \ldots, n$, and $j = 1, \ldots, m$.

As a consequence of this statement, we obtain that the isomorphism problem for the class of virtually polycyclic groups is decidable. Indeed, the solvability of the classical isomorphism problem for virtually polycyclic groups is an immediate consequence of Theorem 3: For any pair of groups A and B we can write down a presentation for $G = A \times B$, and observe that $A \simeq B$ if and only if there exists an automorphism α of G with $\alpha(A) = B$.

The Further decision problems. Positive and negative solutions:

— V. A. Roman'kov [231] proved that TCP is solvable for any polycyclic group. He also proved in [225] that EqP and EndoP are not solvable for free nilpotent groups of class $\geqslant 9$.
— V. N. Remeslennikov [208] established that EpiP is not solvable for the variety $\mathfrak{N}_2$ of nilpotent groups of class $\geqslant 2$.

Theorem 4 (G. Baumslag, F. B. Cannonito, D. J. S. Robinson, and D. Segal [12]).
Let $G = \langle x_1, \ldots, x_n | r_1, \ldots, r_m \rangle$ be a presentation of a polycyclic group. Then there is a uniform algorithm which, when given a finite subset U of G, produces a finite presentation of $\mathrm{gp}(U)$. Hence we can efficiently find a polycyclic presentation of G, the Hirsch number $h(G)$, the Fitting ($\mathrm{Fitt}(G)$) and Frattini ($\mathrm{Fratt}(G)$) subgroups, the center $\mathrm{C}(G)$, decide if G is torsion-free, and so on.

For nilpotent groups, an algorithm to solve the conjugacy problems for subgroups is described in [115].

G. Baumslag, C. F. Miller III, and G. Ostheimer [16] described an algorithm for deciding whether or not a given finitely generated torsion-free nilpotent group is decomposable as the direct product of nontrivial subgroups.

Let O be a binomial ring, i.e., an integral domain containing the ring of integers $\mathbb{Z}$ and containing with every element λ all binomial coefficients

$$\binom{\lambda}{n} = \frac{\lambda(\lambda-1)\cdots(\lambda-n+1)}{n!}, \quad n \in \mathbb{N}.$$

P. Hall [82] itroduced the class of nilpotent O-power groups. M. I. Kargapolov et al. [95] solved in a uniform way various algorithmic problems for O-power groups: word, conjugacy, and membership problems, determination of the O-periodic part, determination of intersection of two O-subgroups, and description of the O-subgroups in terms of generators and defining relations. Note, that in the case $O = \mathbb{Z}$ we have the usual nilpotent groups.

Gilbert Baumslag, an outstanding mathematician and great enthusiast of solvable groups and algorithms.

See other results the O-power groups and its generalizations in [4, 111, 134, 135], etc.

4. Metabelian groups

P. Hall [78] proved that every finitely generated metabelian group G satisfies $max\text{-}n$ (the maximal property for normal subgroups). Therefore, G is finitely defined in the variety $\mathfrak{A}^2$ of all metabelian groups.

The basis of any finitely generated metabelian group G is its commutant G', which can be considered as a module over a finitely generated commutative group ring $\mathbb{Z}[G/G']$. Since this ring is Noetherian, G' as a module is finitely generated. Therefore, there exists a finite description of the commutant G', despite the fact that it is not always finitely generated as a subgroup. The following theorem is of fundamental importance.

Theorem 5 (G. Baumslag, F. B. Cannonito, and D. J. S. Robinson [11]). There is an algorithm that, given a finitely generated metabelian group G by generating elements and defining relations, finds a finite representation of $\mathbb{Z}[G/G']$-module G'.

Corollary 1. This statement has a number of consequences. There is an algorithm, that:

1) finds the center of $\mathrm{C}(G)$ and its finite representation, an algorithm that finds a finite set of elements whose normal closure in the group coincides with the Fitting subgroup $\mathrm{Fitt}(G)$;
2) determines the presence of nontrivial elements of finite order, which determines the order for a given element, determines all possible finite orders of elements of a group;
3) ascertaining the conjugacy of two sets of group elements (using one of Noskov's lemmas);
4) finding the Frattini subgroup $\mathrm{Fratt}(G)$.

On the whole, this allows us to speak of a satisfactory basic algorithmic theory of finitely generated metabelian groups.

W. Magnus invented his famous Magnus embedding, which became a very efficient instrument in the theory of solvable groups.

The Classical decision problems. Positive solutions:

— WP: P. Hall [81] proved that every finitely generated abelian-by-nilpotent group is residually finite. In particular, finitely generated metabelian groups are always residually finite. Since every finitely generated metabelian group G is finitely presented in $\mathfrak{A}^2$, therefore, the word problem is decidable in G.

N. S. Romanovskii

— E. I. Timoshenko presented in [253] a direct algorithm that solves the word problem in an arbitrary finitely generated metabelian group.
— CP: G. A. Noskov [183] proved that the conjugacy problem is decidable in an arbitrary finitely generated metabelian group.
— MP: N. S. Romanovskii [216] proved that the membership problem is decidable in an arbitrary finitely generated metabelian group. In [218], he proved that the membership problem is decidable in an arbitrary abelian-by-nilpotent group.
— M. I. Kargapolov and E. I. Timoshenko [96] proved that in general case a finitely generated metabelian group is not conjugate separable.

5. Solvable groups of arbitrary length

The Classical decision problems. Positive solutions:

— O. Kharlampovich [98]: The WP is decidable in any subvariety of $\mathfrak{N}_2\mathfrak{A}$. (Consequently R. Bieri and R. Strebel [27] proved that every finitely presented group $G \in \mathfrak{N}_2\mathfrak{A}$ is residually finite.)
— C. K. Gupta and N. S. Romanovskii [222]: Any polynilpotent group with a single primitive defining relation has a decidable word problem.

The Classical decision problems. Negative solutions:

V. N. Remeslennikov [207] constructed an example of a group finitely defined in the variety $\mathfrak{A}^5$ with an unsolvable word problem. In addition, a finitely defined in $\mathfrak{A}^4$ group G and a finitely generated subgroup $H \leqslant G$ were given, such that the membership problem with respect to H is unsolvable.

Theorem 6 (O. Kharlampovich [97]). There is a finitely presented solvable group G of class 3 in which WP is undecidable. More exactly, G can be chosen in the centrally-nilpotent of class 2-by-abelian variety $\mathcal{Z}\mathfrak{N}_2\mathfrak{A}$ defined by identity $[[[x_1, x_2], [x_3, x_4]], [x_5, x_6]], y] \equiv 1$ [99]. Thus, WP is unsolvable in the variety $\mathfrak{N}_3\mathfrak{A}$.

Olga Kharlampovich

O. Kharlampovich demonstrated how results of M. Minsky from recursion theory works in constructing counter examples in the solvable group theory.

Subsequently, this was proved in a different way by G. Baumslag, D. Gildenhuys, and R. Strebel [13, 14]. They constructed a finitely presented solvable of class 3 group G and a recursive set of words $w_1, \ldots, w_n, \ldots$ in generators of G such that $w_i^p = 1$ with p a prime and $w_i \in C(G)$ for which there is no algorithm to decide if a given w_i equals the identity in G. This group can also be used to show that the IP is undecidable in the finitely presented solvable groups of class 3.

In [27], R. Bieri and R. Strebel constructed for every finitely generated $\mathbb{Z}Q$-module A, where Q is a finitely generated abelian group of torsion-free rank n, a subset of the unit

sphere $\mathbb{S}^{n-1} \subseteq \mathbb{R}^n$. This subset is equivalent to the set of equivalence classes $[\nu]$ of valuations (homomorphisms) $\nu : Q \to \mathbb{R}^+$. One can attach to every finitely generated Q-module A the set

$$\Sigma_A = \{[\nu] : A \text{ is finitely generated over } Q_\nu\},$$

where $Q_\nu = \{g \in Q : \nu(g) \geqslant 0\}$. In [27], the relations between geometric properties of Σ_A and algebraic properties of A are investigated. In particular, this invariant determines which metabelian groups are finitely presented. For generalizations of concepts and results of the paper [27] see [28, 26].

In [15], an algorithm is presented which decides for a free metabeliab group (or, more generally, for the wreath product of two free abelian groups) whether the intersection of two finitely generated subgroups is finitely generated or trivial. The existence of an algorithm that solves this question for metabelian groups in general is unknown.

Free solvable groups of finite ranks

The Classical decision problems. Positive and negative solutions:

— M. I. Kargapolov and V. N. Remeslennikov [94] proved that the conjugacy problem is solvable for any free solvable group. V. N. Remeslennikov and V. G. Sokolov [211] established that any free solvable group is conjugacy separable.

— U. U. Umirbaev [261] constructed an example of a group G with undecidable word problem which is finitely presented in a variety of solvable groups $\mathfrak{S}_3$ of class $\geqslant 3$. This group G is defined by the relations from the last commutator subgroup of the corresponduing free solvable group. Early S. A. Agalakov [3] proved that there are a finitely generated not finitely separated subgroups in each non-abelian free solvable group of class $d \geqslant 3$.

The identity problem for the class of solvable groups was solved by Yu. G. Kleiman [104, 105].

Theorem 7 (Yu. G. Kleiman [104, 105]). There exists a finitely based variety of groups $\mathfrak{D} \subseteq \mathfrak{A}^7$ in whose free noncyclic groups the equality problem (hence also the identity problem) is unsolvable. Furthermore, it is possible to find a word $v(x)$ such that there exists no algorithm for determining whether or not an arbitrary identity $u(x) \equiv 1$ follows from $v(x) \equiv 1$.

Fox derivatives

For a given positive integer r and for the free group F_r with basis $\{f_1, \ldots, f_r\}$ the *Fox derivatives* are defined as follows.

For $j = 1, \ldots, r$, the (left) Fox derivative associated with f_j is the linear map $D_j : \mathbb{Z}[F_r] \to \mathbb{Z}[F_r]$ satisfying the conditions

$$D_j(f_j) = 1, D_j(f_i) = 0 \text{ for } i \neq j,$$
$$D_j(uv) = D_j(u) + uD_j(v) \text{ for all } u, v \in F_r.$$

Obviously, an element $u \in F_r$ is trivial if and only if $D_i(u) = 0$ for all $i = 1, \ldots, r$. Also note that for an arbitrary element g of F_n and every $j = 1, \ldots, n$, $D_j(g^{-1}) = -g^{-1}D_j(g)$. An introduction to the theory of the Fox derivatives and possible applications of them can be found in [239, 256].

The *trivialization* homomorphism $\varepsilon : \mathbb{Z}[F_r] \to \mathbb{Z}$ is defined on the generators of F_n by $f_i\varepsilon = 1$ for all $i = 1, \ldots, r$ and extended linearly to the group ring $\mathbb{Z}F_n$.

The Fox derivatives appear in another setting as well. Let ΔF_r denote the fundamental ideal of the group ring $\mathbb{Z}[F_r]$. It is a free left $\mathbb{Z}[F_r]$-module with a free basis consisting of

$\{f_1 - 1, \ldots, f_r - 1\}$. This it leads us to the following formula which is called the *main identity* for the Fox derivatives:

$$\sum_{i=1}^{r} D_i(\alpha)(f_i - 1) = \alpha - \alpha\varepsilon,$$

where $\alpha \in \mathbb{Z}F_r$. Conversely, if for any element $f \in F_r$ and $\alpha_i \in \mathbb{Z}[F_r]$ we have equality

$$\sum_{i=1}^{r} \alpha_i(f_i - 1) = f - 1,$$

then $D_i(f) = \alpha_i$ for $i = 1, \ldots, r$.

Let $M_r = F_r/F_r''$ be a free metabelian group of rank r and $A_r = M_r/M_r' \simeq F_r/F_r'$ be a free abelian group of rank r. Further, denote by $\pi : M_r \to A_r$, $\pi' : F_r \to A_r$ and $\pi'' : F_r \to M_r$ the canonical epimorphisms. Let $\{a_1, \ldots, a_r\}$ and $\{x_1, \ldots, x_r\}$ be the bases for A_n and M_n obtained by π' and π''. The maps π, π' and π'' can be extended linearly to $\pi : \mathbb{Z}M_r \to \mathbb{Z}A_r$, $\pi' : \mathbb{Z}F_r \to \mathbb{Z}A_r$ and $\pi'' : \mathbb{Z}F_r \to \mathbb{Z}M_r$. The kernels of π' and π'' are the ideals of $\mathbb{Z}F_r$ generated by the elements $u - 1$ with $u \in F_r'$ and $u \in F_r''$, respectively.

For every $j = 1, \ldots, r$ the free Fox derivative D_j induces a linear map $d_j : \mathbb{Z}M_r \to \mathbb{Z}A_r$. These maps also are called the *free Fox derivatives*.

Magnus embedding

One of the most powerful approaches to study free solvable groups is via the *Magnus embedding*. Originally W. Magnus established in [131] an embedding of a group $\bar{G}$ of type F_r/R' into the group $M(G, T_r) = \begin{pmatrix} G & T_r \\ 0 & 1 \end{pmatrix}$, where $G = F_r/R$ is a finite group, and T_r is a free module over $\mathbb{Z}[F_r]$ with basis $\{t_1, \ldots, t_r\}$. This map is called the *Magnus embedding*. The finiteness restriction on G can be easily eliminated (see [77]). Also the Magnus embedding can be naturally extended to $\bar{G} \to M(G, T)$ where $\bar{G}$ is a group of the type F/R', and $G = F/R$. Here $F = F_{|\Lambda|}$ has a basis $\{f_\lambda | \lambda \in \Lambda\}$ of arbitrary cardinality $|\Lambda|$, and the free module $T = T_{|\Lambda|}$ over $\mathbb{Z}G$ has a basis $\{t_\lambda | \lambda \in \Lambda\}$. In the following usually $\Lambda = \{1, \ldots, r\}$, and $F = F_r$.

A. L. Shmel'kin [246] (see [109]) interpreted the Magnus theorem as an embedding β of the group $\bar{G}$ in the wreath product $W = A_r \mathrm{wr} G$ in the following way.

Let

$$\bar{\beta} : F_r \to W$$

be defined by the map

$$\bar{\beta}(f_i) = a_i \cdot \mu(f_i) \text{ for } i = 1, \ldots, r,$$

where $\mu : F_r \to G$ is the canonical epimorphism, and $\{a_1, \ldots, a_r\}$ is the basis of A_r corresponding to the basis $\{f_1, \ldots, f_r\}$ for F_r.

Then by the Magnus theorem, $\ker(\overline{\beta}) = R'$, hence $\overline{\beta}$ induces an embedding $\beta : \overline{G} \to W$.

Recall that W is isomorphic to $M(G, T_r)$. The embedding β above is defined in this setting by the map

$$\beta(\mu'(f_i)) = \begin{pmatrix} \mu(f_i) & t_i \\ 0 & 1 \end{pmatrix},$$

where $\mu' : F_r \to \overline{G}$ is the canonical epimorphism.

Easy to prove that every matrix $A \in \beta(\overline{G})$ has the form

$$A = \begin{pmatrix} \mu(f) & \sum\limits_{i=1}^{r} \mu(D_i(f))\, t_i \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \bar{\mu}(f') & \sum\limits_{i=1}^{r} d_i(f')\, t_i \\ 0 & 1 \end{pmatrix},$$

where $f' = \mu'(f)$ is arbitrary element of $\overline{G}$, $\overline{\mu} : \overline{G} \to G$ is the canonical epimorphism, and d_i are the induced free Fox derivatives with values in $\mathbb{Z}G$.

It turned out (see [8, 211] for metabelian case and [30]) that the group $\overline{G}$ is *well embedded* in $M(G, T_r)$. Namely, the image of $\overline{G}$ in $M(G, T_r)$ under the Magnus embedding can be described as follows.

A matrix

$$A = \begin{pmatrix} 1 & \sum\limits_{i=1}^{r} \alpha_i t_i \\ 0 & 1 \end{pmatrix} \in M(G, T_r)$$

belongs to the image $\beta(\overline{G})$ if and only if

$$\sum_{i=1}^{r} \alpha_i (\mu(f_i) - 1) = 0.$$

Therefore, a matrix

$$A = \begin{pmatrix} g & \sum\limits_{i=1}^{r} \alpha_i t_i \\ 0 & 1 \end{pmatrix} \in M(G, T_r)$$

belongs to the image $\beta(\overline{G})$ if and only if

$$\sum_{i=1}^{r} \alpha_i (\mu(f_i) - 1) = g - 1.$$

6. Equations

Solvability problem for equations in various classes of groups has been actively researched for many years. First general results on equations in groups appeared in the 1960s in the works of R. Lyndon [122 – 124] and A. I. Mal'cev [144]. In the 1970s G. S. Makanin [137, 138] proved the solvability of the systems equations for free monoids and free groups. In recent years, significant progress has been made in the computational complexity and structure of solution sets.

R. C. Lyndon

For a general survey of the current state of the theory of solvability of equations and systems of equations in groups, see the observing paper by the author [232] and his monograph [239].

The *Diophantine problem* in a group G is the task to determine whether or not a given finite system of equations with constants in G has a solution in G. This problem is decidable if there is an algorithm that given a finite system E of equations with constants in G decides whether or not E has a solution in G.

Equations in nilpotent groups

Denote by $\mathcal{N}$ the class of all nilpotent groups. As above $\mathfrak{N}_c$ denotes the variety of all nilpotent groups of class $\leqslant c$. In particular $\mathfrak{N}_1$ coincides with the class $\mathfrak{A}$ of all abelian groups.

A. I. Mal'cev [140] proved that any equation of the form $x^m = g$ where g is an element of a torsion-free nilpotent group $G \in \mathfrak{N}_c$, $m \in \mathbb{N}$, has a solution in some torsion-free nilpotent group $H \in \mathfrak{N}_c$, $H \geqslant G$. Moreover, there is a divisible torsion-free nilpotent group $\tilde{G} \in \mathfrak{N}_c$, least by inclusion, containing the group G. Such a group $\tilde{G}$ is uniquely defined up to isomorphism and is called the *Mal'cev completion* of G.

Clearly every abelian group embeds into a divisible abelian group.

Since every finitely generated nilpotent group $G \in \mathfrak{N}_c$ embeds into a direct product of a torsion-free nilpotent group G_0 and a finite direct product $\prod\limits_p G_p$ of finite p-groups G_p (p are primes) also of class c, every equation of the form $x^m = g$, as above, has a solution in a some nilpotent overgroup H of G. Indeed, we can embed G_0 in a torsion-free complete nilpotent group H_0 keeping the class c by [140], and embed every p-group G_p into a finite p-group H_p containing a solution of the considering equation. Note that we need only to extend G_p with roots of equations of the form $x^{p^k} = g_p$. Then we set $H = H_0 \times \prod\limits_p H_p$. But in general, H has class greater than c. Therefore, any finitely generated nilpotent group can be embedded into a divisible nilpotent group.

A system of $m = k$ equations is called *unimodular* if the matrix consisting of the sums of exponentials of the unknowns with which they enter the equations, has determinant 1.

A. L. Shmel'kin [247] established that any unimodular system of equations over a nilpotent group G has an unique solution in G.

Theorem 8 (V. A. Roman'kov [225, 226]). The following statements hold:

— Let $N_{r,c}$ be a free nilpotent group of rank $r \geqslant 2$ and class $c \geqslant 9$ with basis $\{x_1, \ldots, x_r\}$. Then there is an algorithm which for every Diophantine equation $D(\zeta_1, \ldots, \zeta_n) = 0$ gives a split equation $g(z_1, \ldots, z_p) = f$ over the group $N_{r,c}$ that has a solution in $N_{r,c}$ if and only if $D(\zeta_1, \ldots, \zeta_n) = 0$ has a solution in integers. An element f can be chosen in the subgroup $\mathrm{gp}(x_1, x_2)$ of $N_{r,c}$.

— Let M_r be the free metabelian group of rank $r \geqslant 2$ with basis $\{x_1, \ldots, x_r\}$. Then there is an algorithm which for every Diophantine equation $D(\zeta_1, \ldots, \zeta_n) = 0$ gives a split equation $g(z_1, \ldots, x_q) = f$ over group M_r that has a solution in M_r if and only if $D(\zeta_1, \ldots, \zeta_n) = 0$ has a solution in integers. An element f can be chosen in subgroup $\mathrm{gp}(x_1, x_2)$ of M_r.

Therefore, the equation problem for any free nilpotent group $N_{r,c}$, $r \geqslant 2$, $c \geqslant 9$, or free metabelian group M_r, $r \geqslant 2$, is algorithmically undecidable.

The method of interpretation of Diophantine equations in free nilpotent and free metabelian groups has been used in a row forthcoming papers. N. N. Repin applied this method for studying the solvability of equations in nilpotent groups.

We record a number results by N. N. Repin on recognizing the solvability of equations in nilpotent groups, see [213, 214]:

— For every finitely generated nilpotent group of class two the problem of recognizing the solvability of one-variable equations is decidable.

— There is a finitely generated nilpotent group of class 3 in which the problem of recognizing the solvability of one-variable equations is undecidable.

— For every free nilpotent group $N_{r,c}$ of rank $r \geqslant 600$ and class $c \geqslant 3$ the problem of recognizing the solvability of equations is udecidable.

— For every free nilpotent group $N_{r,c}$ of rank $r \geqslant 2$ and class $c \geqslant 5 \cdot 10^{10}$ the problem of recognizing the solvability of one-variable equations is undecidable.

In another setting, the interpretation of Diophantine equations was used by Yu. G. Kleiman to prove that the identity problem is undecidable for some relatively free solvable groups (see Theorem 7 above).

Theorem 9 (V. A. Roman'kov [236]). For every Diophantine polynomial $D(\zeta_1, \ldots, \zeta_n)$ there exists a finitely generated nilpotent group G of class 2 with the following property. For every equation of the form $D(\zeta_1, \ldots, \zeta_n) = c$, $c \in \mathbb{Z}$, there is an element $u = u(c) \in G$ such that u is a commutator in G (in other words, the equation $[x, y] = u$ is solvable in G),

if and only if the equation $D(\zeta_1, \ldots, \zeta_n) = c$ is decidable over $\mathbb{Z}$. The group G and each element $u(c)$ can be effectively constructed. By the famous Matijasevich's theorem there is a Diophantine polynomial D for which the equation problem is undecidable for the class of equations of the form $\{D = c : c \in \mathbb{Z}\}$. Therefore, the commutator problem is undecidable for G.

Moreover, G is the first example of a finitely generated nilpotent group with undecidable equation problem for the class of quadratic equations. In [236], a finitely generated nilpotent group H of class 2 is also presented for which the endomorphism problem is undecidable. It also has been proved that the retract problem (i.e., question whether the given finitely generated subgroup is a retract of the whole group) is undecidable for the class of finitely generated 2-step nilpotent groups. On the other hand, there is an algorithm which for a given element $u \in N_{r,2}$ determines whether or not u is a commutator.

A. G. Makanin proved in [136] that every split equation $w(x_1, \ldots, x_k) = g$, $g \in G$, over a finitely generated torsion-free nilpotent group G, where $w(x_1, \ldots, x_k)$ does not belong to the derived subgroup $F(X)'$, i.e., $w(x_1, \ldots, x_k)$ is a *non-commutator* word, is finitely approximable.

In [49], M. Duchin et al. show that there exists an algorithm to decide any single equation in the Heisenberg group. The method works for all nilpotent groups of class 2 with rank-one derived subgroup, which includes the higher Heisenberg groups.

Equations in metabelian case

The metabelian Baumslag — Solitar groups are defined by one-relator presentations $\mathrm{BS}(1,k) = \langle a, b | b^{-1}ab = a^k \rangle$, where $k \in \mathbb{N}$. If $k = 1$, then $\mathrm{BS}(1,1)$ is free abelian of rank 2, so the Diophantine problem in this group is decidable (it reduces to solving finite systems of linear equations over the ring of integers $\mathbb{Z}$).

O. Kharlampovich, L. Lopéz and A. Myasnikov proved in [100]) that the Diophantine problem is decidable in $G = A wr \mathbb{Z}$, where A is a finitely generated abelian group. Equations in the Baumslag — Solitar group $\mathrm{BS}(1,k)$ are also decidable.

I. Lysenok and A. Ushakov [126] proved that the equation problem for spherical quadratic equations in free metabelian groups is solvable and, moreover, NP-complete. E. I. Timoshenko [258] proved the first (solvability) result by using the Magnus embedding.

By the *spherical quadratic equation* over group G with unknowns $X = \{x_1, \ldots, x_t, \ldots\}$ one means an equation of the form

$$\prod_{i=1}^{n} x_i^{-1} c_1 x_i = 1, \quad c_i \in G.$$

V. N. Remeslennikov and N. S. Romanovskii [209] study into algebraic geometry over a non-commutative u-group G, that is, a finitely generated metabelian group whose universal theory is the same as is one for a free metabelian group of rank at least two. They present the construction for a u-product $G_{1,2} = G_1 \circ G_2$ of two u-groups G_1 and G_2, and prove that $G_{1,2}$ is also a u-group and that every u-group, which contains G_1 and G_2 and is generated by these, is a homomorphic image of $G_{1,2}$. They prove that the coordinate group of an affine space G^n is equal to $G \circ M_n$. In [209] irreducible algebraic sets in G are treated for the case where G is a free metabelian group or wreath product of two free abelian groups of finite ranks.

Interpretation of Diophantine equations

The author [225, 226] derived the undecidability of EqP and EndoP in the classes of free nilpotent and free metabelian groups. He based on the famous results by Yu. V. Matijasevich on undecidability of the Diophantine problem [148, 149].

He proved that if $N = N_{r,c}$ is the free nilpotent group of sufficiently large rank r and class $c \geqslant 9$, then for any Diophantine polynomial $D(z_1, \ldots, z_n) \in \mathbb{Z}[z_1, \ldots, z_n]$, we can effectively construct two elements $g, f \in N$ such, that there is an endomorphism $\varphi \in \mathrm{End}(N)$ that $\varphi(g) = f$ if and only if the equation $D(z_1, \ldots, z_n) = c$, where $c \in \mathbb{Z}$, has a solution in $\mathbb{Z}$. Moreover, if such φ exists, we can effectively find it if and only if we can effectively solve the corresponding Diophantine equation. We can also fix the left side of equation $D(z_1, \ldots, z_n) = c$ to obtain non-decidable class of Diophantine equations. Hence, we can fix the element g above to obtain non-decidability of the EqP and EndoP in N. The second element f we choose in a specific cyclic subgroup.

By definition, the *relation matrix* $M(G)$ of the presentation $G = \langle x_1, \ldots, x_n : r_1, \ldots, r_m \rangle$ is an integral $m \times n$ matrix whose ij-th entry is the sum of the exponents of the x_j's that occur in r_i. Recall, that a matrix is said to have *full rank* if its rank equals the largest possible for a matrix of the same dimensions, which is the lesser of the number of rows and columns.

The authors of [64] study metabelian groups G given by a full rank finite presentations $\langle x_1, \ldots, x_n : r_1, \ldots, r_m; \mathfrak{A}^2 \rangle$ in the variety $\mathfrak{A}^2$. They prove that G is a product of a free metabelian subgroup of rank $\max(0, n-m)$ and a virtually abelian normal subgroup, and that if $m \leqslant n-2$, then the Diophantine problem for G is undecidable, while it is decidable if $m \geqslant n$. They also prove that if $m \leqslant n-1$, then, in any direct decomposition of G, all factors, except one, are virtually abelian. Since finite presentations have full rank asymptotically almost surely, metabelian groups finitely presented in the variety of metabelian groups satisfy all the aforementioned properties asymptotically almost surely.

7. Post correspondence problem

Different versions of PCP

There are the bounded versions of PCP. We consider two sorts of a bound: the bound on the solution length n ($\mathrm{BPCP}_{sl}(n)$) and the bound on the size s ($\mathrm{BPCP}_s(s)$).

The following statements are true:

— BPCP_{sl} is NP-complete [62];
— $\mathrm{BPCP}_s(2)$ is decidable [51] (but it remains unknown whether the PCP is solvable for 3–6 pairs of words);
— $\mathrm{BPCP}_s(l)$ for $l \geqslant 7$ is undecidable [150, 151].

Let A be an algebraic system and let $F(A)$ be a free algebraic system in the variety $\mathrm{Var}(A)$ generated by A. For two arbitrary homomorphisms $\varphi, \psi \in \mathrm{Hom}(F(A), A)$ the subset

$$\mathrm{Eq}_A(\varphi, \psi) = \{a \in F(A) : \varphi(a) = \psi(a)\}$$

of $F(A)$ is said to be the *equalizer* of φ and ψ, that is obviously a subsystem of $F(A)$.

The following problem arises: PCP(A): $\mathrm{Eq}_A(\varphi, \psi) \neq 0$?

The Post correspondence and related problems for groups

Further we will talk only about groups.

Let $\bar{G}, G$ be a pair of groups, and let $\varphi, \psi \in \mathrm{Hom}(\bar{G}, G)$ be a pair of homomorphisms. We denote by

$$\mathrm{Eq}_G(\varphi, \psi) = \{g \in \bar{G} : \varphi(g) = \psi(g)\}$$

the equalizer of φ and ψ, that is obviously a subgroup of $\bar{G}$.

Equalization presentation problem (EPP): Let $\mathcal{C}$ be a class of finitely generated groups. We say that EPP is decidable in $\mathcal{C}$ if for any pair of groups $\bar{G}, G \in \mathcal{C}$ and any pair of homomorphisms $\varphi, \psi \in \mathrm{Hom}(\bar{G}, G)$ we can find effectively a presentation of $\mathrm{Eq}_G(\varphi, \psi)$.

A form of presentation depends of $\mathcal{C}$. It should be explicit for $\mathcal{C}$. In particular case, when $\bar{G} = G$, $\varphi, \psi \in \mathrm{End}(G)$, we get EPP for G.

Equalization problem (EP): We say that EP is decidable in the class $\mathcal{C}$ if for any pair of groups $\bar{G}, G \in \mathcal{C}$ and any pair of homomorphisms $\varphi, \psi \in \mathrm{Hom}(\bar{G}, G)$ there is an algorithm that determines non-triviality of $\mathrm{Eq}_G(\varphi, \psi)$.

In particular case, when $\bar{G} = G$, $\varphi, \psi \in \mathrm{End}(G)$, we consider EP for G.

Let we formulate the Post correspondence problem PCP(G) for a group G in the corresponding variety. Namely, when $\bar{G} = F(\mathrm{Var}(G))$ be a relatively free group in the variety $\mathrm{Var}(G)$, generated by G, we get PCP for G.

PCP(G): $\mathrm{Eq}_G(\varphi, \psi) \neq 1$?

Generalized equalization problem (GEP). Also, we say that GEP is decidable in the class $\mathcal{C}$ if for any pair of groups $\bar{G}, G \in \mathcal{C}$, any pair of homomorphisms $\varphi, \psi \in \mathrm{Hom}(\bar{G}, G)$ and given a nontrivial element $v \in G$ we can decide effectively whether there is $g \in \bar{G}$ such that

$$\varphi(g) = v \cdot \psi(g).$$

We consider it as an equation with unknown element $g \in \bar{G}$.

In particular case, when $\bar{G} = G$, $\varphi \in \mathrm{End}(G)$, $\psi = id$, we get TCP for G. If $\psi \in \mathrm{End}(G)$, then we get BTCP for G.

The generalized Post correspondence problem (GPCP)

When $\bar{G} = F(\mathrm{Var}(G))$ is a relatively free group in the variety $\mathrm{Var}(G)$, generated by G, we get GPCP for G.

GPCP(G): Given a finite sequence of instances $(g_1, h_1), \ldots, (g_s, h_s)$ and element f in G, determine if there is a word $w = w(x_1, \ldots, x_s)$ such that

$$w(g_1, \ldots, g_s) = f \cdot w(h_1, \ldots, h_s).$$

This problem admits the following equivalent formulation. Let $F_s(G)$ be a free group of rank s in $\mathrm{Var}(G)$.

GPCP(G): Given a pair $\varphi, \psi \in \mathrm{Hom}(F_s(G), G)$, decide if the solution $w \in F_s(G)$ exists or not of the equation

$$\varphi(w) = f \cdot \psi(w).$$

Now we formulate the hereditary word problem (HWP(G)) in a group G. The following problem is the strongest form of the word problem in G:

HWP(G): Given a finite set $R \cup \{f\}$ of words in generators of G, decide whether or not f is trivial in the quotient $G/ncl(R)$.

GPCP can be decidable only in a group with decidable HWP.

The following results are proved in [162]. Let G be a finitely generated group. Then:

— HWP(G)) P-time reduces to GPCP(G).
— If G contains F_2 then GPCP(G) is undecidable.

In [163] the classical knapsack and subset sum problems to arbitrary groups are introduced. The computational complexity of these new problems were studied. It was shown that these problems, as well as the bounded submonoid membership problem, are P-time decidable in hyperbolic groups and give various examples of finitely presented groups where the subset sum problem is NP-complete.

These problems for a group G are formulated as follows:

— Knapsack problem (KP): Given $g_1, \ldots, g_k, g \in G$, decide if

$$g = \prod_{i=1}^{k} (g_i)^{\mu_i}$$

for some non-negative integers $\mu_1, \ldots, \mu_k$.

— The subset sum problem (SSP): Given $g_1, \ldots, g_k, g \in G$, decide if

$$g = \prod_{i=1}^{k} (g_i)^{\epsilon_i}$$

for some $\epsilon_1, \ldots, \epsilon_k \in \{\pm 1\}$.

— Bounded submonoid membership problem (BSMP): Given $g_1, \ldots, g_k, g \in G$ and $1^m \in \mathbb{N}$ (in unary), decide if g is equal in G to a product of the form $g = \prod_{j=1}^{s} g_j$, where $i_j \in$ $\in \{1, \ldots, k\}$ and $s \leqslant m$.

Let G be a finitely generated virtually nilpotent group. Then SSP(G) and BSMP(G), as well as their search and optimization (with respect to number of factors) variations, are in P [163]. Every polycyclic non-virtually-nilpotent group has NP-complete subset sum problem [181].

In [164], a number of algorithmic problems in groups were introduced and studied, modeled after the classical computational lattice problems. Polynomial time solutions for a nilpotent group have been given to problems such as finding a subgroup element closest to a given group element, or finding the shortest nontrivial subgroup element.

Twisted conjugacy problem

Originally the twisted conjugacy problem was posed as following:

Let G be a group, and $u, w \in G$. Given an endomorphism $\xi \in \mathrm{End}(G)$, one says that u and w are *ξ-twisted conjugated*, denoted by $u \sim_\xi w$, if and only if there exists $g \in G$ such that $u = \xi(g)^{-1} \cdot wg$, or equivalently $\xi(g)\, u = wg$. So it is a question if following equation have a solution g in G:

$$\xi(g)\, u = wg.$$

The question about ξ-twisted conjugacy of given elements $u, w \in G$ can be reduced to case where one of the elements is trivial. To do it we change ξ to $\varphi = \xi \circ \sigma_u$, where $\sigma_u : g \mapsto u^{-1}gu, g \in G$, is an inner automorphism. We get

$$\varphi(g) = vg$$

for $v = u^{-1}w$.

We consider finitely generated metabelian and polycyclic groups. We have the following two equations:

$$\varphi(g) = \psi(g)$$

and

$$\varphi(g) = u\psi(g).$$

Following [11], call a subgroup H of a finitely generated metabelian group M *nearly normal* if the intersection $H \cap M'$ is a normal subgroup of M.

Then

$$H = \mathrm{gp}(h_1, \ldots, h_k, \{v_1, \ldots, v_l\}^{\mathbb{Z}[M/M']}$$

is a finite description of H.

The following results were presented in the talk of the author [234] (see also [233]).

The first assertion shows that the question of the decidability of GEP ($\varphi(g) = f\psi(g)$) under certain assumptions can be transformed into a similar question about the subgroup H of a finite index in G:

— Let G be any group and let $H \leqslant G$ be any subgroup of a finite index in G. Let $\bar{G}$ be a group and $\varphi, \psi \in \mathrm{Hom}(\bar{G}, G)$. Suppose that the membership problem in H is decidable for G. Then, if GEP is decidable for H, it is also decidable for G.

Let us present the main technical results for obtaining solutions of the problems under consideration in the class of all finitely generated metabelian groups:

— Let G be a group and A be its abelian normal subgroup. Let $\bar{G} = \mathrm{gp}(f_1, \ldots, f_n)$ be a finitely generated group and let $\varphi, \psi : \bar{G} \to G$ be a pair of homomorphisms such that $G = \mathrm{gp}(\varphi(\bar{G}), \psi(\bar{G}))$. For every $g \in \bar{G}$ denote $a(g) = \varphi(g)(\psi(g))^{-1}$. In particular, denote $a_i = a(f_i)$, $i = 1, \ldots, n$.

Suppose that the following assumptions are true:

1) for every $g \in \bar{G}$ one has $a(g) \in A$;

2) the derived subgroup G' acts identically on A, i.e., $[G', A] = 1$;

3) $\bar{G}' \leqslant \mathrm{Eq}_G(\varphi, \psi)$, i.e., for every $g \in \bar{G}'$ one has $\varphi(g) = \psi(g)$.

Then

$$\mathrm{Eq}_G(\varphi, \psi) \leqslant \psi^{-1}(\mathrm{C}_G(a_1, \ldots, a_n)),$$

where $\mathrm{C}_G(a_1, \ldots, a_n)$ is the centralizer of the elements $a_1, \ldots, a_n$ in G.

Moreover, for every $g \in \psi^{-1}(\mathrm{C}_G(a_1, \ldots, a_n))$ one has $a(g) \in \zeta_1 G$;

4) hence, if the center $\zeta_1(G)$ of G is trivial, then

$$\mathrm{Eq}_G(\varphi, \psi) = \psi^{-1}(\mathrm{C}_G(a_1, \ldots, a_n)).$$

In general case there is a homomorphism

$$\rho : \psi^{-1}(\mathrm{C}_G(a_1, \ldots, a_n)) \to \zeta_1 G, g \mapsto a(g),$$

and

$$\mathrm{Eq}_G(\varphi, \psi) = \ker(\rho).$$

Let G be a group and A be its abelian normal subgroup. Let $\bar{G}$ be a group and let $\varphi, \psi : \bar{G} \to G$ be a pair of homomorphisms such that $G = \mathrm{gp}(\varphi(\bar{G}), \psi(\bar{G}))$. Let $a(g) = \varphi(g)(\psi(g))^{-1}$. Suppose that the following assumptions are true:

1) for every $g \in \bar{G}$ one has $a(g) \in A$;

2) the derived subgroup G' acts identically on A, i.e., $[G', A] = 1$.

Then

$$a(\bar{G}') = \{a(g) : g \in \bar{G}'\}$$

is a normal subgroup of G.

Moreover, if $\bar{G}'$ is generated as a normal subgroup by a set of elements $\{u_i : i \in I\}$, then $a(\bar{G}')$ is generated as a normal subgroup by the set $\{a(u_i) : i \in I\}$.

Let all the previous notation and assumptions be satisfied. Let $G_1 = G/a(\bar{G})$, and $G \to G_1$ be the standard homomorphism. For simplicity, we do not change the notation for the compositions φ and ψ with this standard homomorphism. Also, we do not change the designation of the images of elements of G in G_1.

Then

$$\mathrm{Eq}_{G_1}(\varphi,\psi) \leqslant \psi^{-1}(\mathrm{C}_{G_1}(a_1,\ldots,a_n)).$$

Moreover, if $\zeta_1 G_1 = 1$, then

$$\mathrm{Eq}_{G_1}(\varphi,\psi) = \psi^{-1}(\mathrm{C}_{G_1}(a_1,\ldots,a_n)).$$

Main results for metabelian and polycyclic groups

Theorem 10. Let M be a finitely generated metabelian group, and let $\bar{M}$ be a finitely generated metabelian group with generating set $\{f_1,\ldots,f_n\}$. Let N be an abelian normal subgroup of M, containing M'.

Then EPP and EP are solvable for any pair of homomorphisms $\varphi,\psi \in \mathrm{Hom}(\bar{M},M)$ satisfying the assumption that, for any $g \in \bar{M}$, $g\varphi(g\psi)^{-1} \in N$. Equalizer $\mathrm{Eq}_M(\varphi,\psi)$ is described as a nearly normal subgroup of M, i.e.,

$$\mathrm{Eq}_M(\varphi,\psi) = \mathrm{gp}\left(h_1,\ldots,h_k,\{v_1,\ldots,v_l\}^{\mathbb{Z}M/N}\right),$$

where $h_1,\ldots,h_k,v_1,\ldots,v_l$ are given by the algorithm.

Corollary 2. Let M be a finitely generated metabelian group, and let $\bar{M} = F(\mathrm{Var}(M))$ be a relatively free metabelian group in the variety $\mathrm{Var}(M)$ generated by M with basis $\{f_1,\ldots,f_n\}$, $n \geqslant 2$.

Then PCP is solvable for any pair of instances $\bar{c} = (c_1,\ldots,c_n)$ and $\bar{d} = (d_1,\ldots,d_n)$ such that for the corresponding homomorphisms $\varphi : f_i \to c_i$ and $\psi : f_i \to d_i$, respectively, one has $a_i = \varphi(f_i)(\psi(f_i))^{-1} \in N$, $i = 1,\ldots,n$.

Theorem 11.

1. Let M be a metabelian polycyclic group, and let $\bar{M}$ be a metabelian polycyclic group with generating set $\{f_1,\ldots,f_n\}$, $n \geqslant 2$. Then EPP and EP are decidable for any pair of homomorphisms φ,ψ of $\bar{M}$ to M.
2. Let M be a metabelian polycyclic group, and let $\bar{M} = F(\mathrm{Var}(M))$ be a relatively free group in the variety $\mathrm{Var}(M)$ generated by M with basis $\{f_1,\ldots,f_n\}$, $n \geqslant 2$. Then PCP_n is decidable for any pair of instances $\bar{c} = (c_1,\ldots,c_n), \bar{d} = (d_1,\ldots,d_n) \in \bar{M}^n$.
3. Let M be a finitely generated metabelian group, and let $\bar{M}$ be a finitely generated metabelian group generated by $f_1,\ldots,f_n$, $n \geqslant 2$. Let N be an abelian normal subgroup of M, that contains M'. Then GEP is solvable for any pair of homomorphisms $\varphi,\psi \in \mathrm{Hom}(\bar{M},M)$ and any element $a \in N$ such that for any $g \in \bar{M}$ one has $\varphi(g)(\psi(g))^{-1} = a(g) \in N$.

Corollary 3.

1. Let M be a finitely generated metabelian group and N a normal abelian subgroup of M containing M'. Let φ,ψ be a pair of endomorphisms in $\mathrm{End}(M)$ such that, for each $g \in M$, $\varphi(g)(\psi(g))^{-1} \in N$. Then the bi-twisted conjugacy problem is solvable for φ,ψ.

   In particular, the bi-twisted conjugacy problem is solvable for any pair of endomorphisms $\varphi,\psi \in \mathrm{End}(M)$, each of which induces an identical map onto M/M'. This generalizes the main result of paper [264], where φ induces an identical map onto M/M' and $\psi = id$.
2. Let M be a finitely generated metabelian group, and let $\bar{M} = F(\mathrm{Var}(M))$ be a relatively free metabelian group in the variety $\mathrm{Var}(M)$ with basis $\{f_1,\ldots,f_n\}$, $n \geqslant 2$. Let N be an abelian normal subgroup of M, that contains M'.

Then GPCP_n is decidable for every pair of instances $\bar{c} = (c_1, \ldots, c_n), \bar{d} = (d_1, \ldots, d_n) \in M^n$ such that for the corresponding to these instances homomorphisms $\varphi, \psi \in \mathrm{Hom}(\bar{M}, M)$ and every element $g \in \bar{M}$ we have $\varphi(g)(\psi(g))^{-1} = a(g) \in N$.

Theorem 12. Let M be a metabelian polycyclic group. Let N be an abelian normal subgroup of M, that contains M'. Let $\bar{M}$ be a metabelian polycyclic group generated by $f_1, \ldots, f_n$, $n \geqslant 2$. Then GEP is decidable for every pair of homomorphisms φ and ψ of $\bar{M}$ to M.

Corollary 4. Let M be a polycyclic metabelian group and N be a normal abelian subgroup of M containing M'. Then the bi-twisted conjugacy problem is solvable for any pair of endomorphisms φ, ψ of M. Thus, the bi-twisted conjugacy problem is solvable for M. This generalize the result [264] where φ is arbitrary endomorphism and $\psi = id$.

Theorem 13. Let M be a metabelian polycyclic group, and let $\bar{M} = F(\mathrm{Var}(M))$ be a relatively free group in $\mathrm{Var}(M)$, $n \geqslant 2$. Then GPCP_n is decidable for any pair of instances $\bar{c} = (c_1, \ldots, c_n), \bar{d} = (d_1, \ldots, d_n) \in \bar{M}^n$.

Theorem 14. All the problems just considered are solvable in the class of polycyclic groups.

8. Elementary and universal theories

The elementary theory $\mathrm{Th}(G)$ of a group G (or a ring, or an arbitrary structure) in a language L is the set of all first-order sentences in L that are true in G.

We restrict ourselves to considering only the group-theoretical case. Usually L is the standard group-theoretic language $\langle \cdot, ^{-1}, =, 1 \rangle$. Sometimes L includes predicates or other than 1 constants. If the group A is elementarily equivalent to the group B, i.e., if $\mathrm{Th}(A) = \mathrm{Th}(B)$, then we write $A \equiv B$.

One of the main results of W. Szmielew [249] is the determination of group theoretic invariants $I(A)$ which characterize abelian groups A up to elementary equivalence. The decidability of the theory of abelian groups follows relatively easily from this result: $A \equiv B \leftrightarrow I(A) = I(B)$. More exactly, $\mathrm{Th}(A)$ is decidable if the sequence of Szmielew invariants of A is computable. Finitely generated abelian groups have decidable elementary theories. This assertion easily carries over to their finite extensions, i.e., almost abelian finitely generated groups. Two finitely generated abelian groups are elementary equivalent if and only if they are isomorphic, that is, $A \equiv B \leftrightarrow A \simeq B$.

A compretiensive survey of the first-order properties of abelian groups is given by P. C. Eklof and E. R. Fisher in [54]. Their principal method is the investigation of saturated abelian groups. They gave a new model-theoretic proof results of Szmielew and obtained new results on the existence of saturated models of complete theories of abelian groups. It turned out that elementarily equivalent saturated abelian groups of the same cardinality are isomorphic.

There are several main results on elementary theories of nilpotent groups. Examples of finitely generated nilpotent groups with undecidable elementary theories were first given by A. I. Mal'cev. In his pioneering paper [146], A. I. Mal'cev showed that the ring R with unity can be defined by first-order formulas in the group $\mathrm{UT}_3(R)$ of unitriangular matrices over R (considered as an abstract group). In particular, the ring of integers $\mathbb{Z}$ is definable in the group $\mathrm{UT}_3(\mathbb{Z})$, which is a free nilpotent of rank 2 and class 2. Yu. L. Ershov [57] proved that the group $\mathrm{UT}_3((Z))$ (hence the ring $\mathbb{Z}$) is definable in any finitely generated nilpotent group G, which is not virtually abelian. Therefore, the elementary theory of G is undecidable (see more general statement of theorem 15 below).

In [143], A. I. Mal'cev proved that the elementary theory of any free solvable group $S_{r,d}$ of rank $r \geqslant 2$ and class $d \geqslant 2$ is undecidable. All members of the derived series are definable in $S_{r,d}$. In [145], he established fundamental results on linear groups. In particular, he proved the following theorem: Let G =GL (or PGL, SL, PSL), let $n, m \geqslant 3$, and let K and L be commutative rings of characteristic zero, then $\mathrm{GL}_m(K) \equiv \mathrm{GL}_n(L)$ if and only if $m = n$ and $K \equiv L$. In the case of GL and PGL the result holds for $n, m \geqslant 2$.

In [108], M. I. Kargapolov posed the following Question 1.26: Does elementary equivalence of two finitely generated nilpotent groups imply that they are isomorphic?

In [268], B. I. Zil'ber constructed an example of two finitely generated nilpotent of class 2 groups that are elementary equivalent but nonisomorphic.

M. I. Kargapolov was the initiator of many studies on solvable groups and algorithms

A. G. Myasnikov in the series of papers [158, 160, 161] studied the elementary theories of bilinear mappings. In particular, he gave a description of abstract isomorphisms of bilinear mappings.

If G is torsion free finitely generated nilpotent group and R is binomial domain, then G^R means the P. Hall R-completion of G.

In the papers [164–166] A. G. Myasnikov and V. N. Remeslennikov proved that the Kargapolov's conjecture holds "essentially" true in the class of nilpotent $\mathbb{Q}$-groups (i.e., divisible torsion-free nilpotent groups). Indeed, it turned out that two such groups G and H are elementarily equivalent if their cores $\tilde{G}$ and $\tilde{H}$ are isomorphic and G and H either simultaneously coincide with their cores or they do not. Here the *core* of G is uniquely defined as a subgroup $\tilde{G} \leqslant G$ such that $\mathrm{C}(\tilde{G}) \leqslant \tilde{G}'$ and $G = \tilde{G} \times G_0$, for some abelian $\mathbb{Q}$-group G_0. Developing this approach, A. G. Myasnikov described in [157, 159] all groups elementarily equivalent to a given finitely generated nilpotent K-group G over an arbitrary field K of characteristic zero.

In a series of papers [22–24] O. V. Belegradek completely characterized groups which are elementarily equivalent to a unitriangular matrix group $\mathrm{UT}_n(\mathbb{Z})$ for $n \geqslant 3$. In particular, he showed in [23, 24] that there are groups elementarily equivalent to $\mathrm{UT}_n(\mathbb{Z})$ which are not isomorphic to any group of the type $\mathrm{UT}_n(R)$ as above (he called them *quasi-unitriangular groups*).

A. G. Myasnikov

The paper [174] gives a complete algebraic description of the groups G that are elementarily equivalent to the P. Hall completion N^R of a given free nilpotent group N of finite rank over an arbitrary binomial domain R. In particular, all groups elementarily equivalent to a free nilpotent group N of finite rank are characterized. F. Oger [189] studied special circumstances under which elementary equivalence of two finitely generated finite-by-nilpotent groups implies isomorphism. Finally, F. Oger showed in [190] that two finitely generated nilpotent groups G and H are elementarily equivalent if and only if they are essentially isomorphic, i.e., $G \times \mathbb{Z} \simeq H \times \mathbb{Z}$. However, the full classification problem for finitely generated nilpotent groups is currently wide open.

A *universal formula* is a formula which can be written $\forall x_1 \ldots \forall x_n \Phi(x_1, \ldots, x_n)$ for some quantifier free formula $\Phi(x_1, \ldots, x_n)$. If it has no free variables, a universal formula is called a *universal sentence*. The universal theory $\mathrm{Th}_\forall(G)$ of a group G is the set of universal sentences satisfied by G. If the group G is universally equivalent to the group H, i.e., if $\mathrm{Th}_\forall(G) = \mathrm{Th}_\forall(H)$, then we write $G \equiv_\forall H$.

Similarly, one can define existential formulae and sentences, and the existential theory $\mathrm{Th}_{\exists}(G)$ of a group G. Note that two groups which have the same universal theory also have the same existential theory since the negation of a universal sentence is equivalent to an existential statement.

It is well known that two nontrivial free abelian groups are universally equivalent. E. I. Timoshenko [252] established that any two free solvable groups $S_{r,d}$ and $S_{q,d}$ of the same length $d \geqslant 1$ and $r, q \geqslant 2$ (in the case $d = 1$, $r, q \geqslant 1$) are universally equivalent ($S_{r,d} \equiv_\forall S_{qd}$). This result has been independently proved in [61]. In [252], E. I. Timoshenko also proved that any two free nilpotent groups $N_{r,c}$ and $N_{q,c}$ where $r \neq q$, of the same class $c \geqslant 2$ are universally equivalent if and only if the following conditions are satisfied: $r, q \geqslant c - 1$ for $c \geqslant 3$; and $r, q \geqslant 2$ for $c = 2$.

E.I. Timoshenko

The first example of a finitely generated nilpotent group G, whose universal theory $\mathrm{Th}_\forall(G)$ is undecidable, was constructed by the author in [227]. This group G is a torsion-free metabelian group of the nilpotency class 4 with 6 generators.

In [251], E. I. Timoshenko considers the problem of preserving elementary and universal equivalence under wreath products. His result is as follows. If the group A is elementarily equivalent to the group B, and K is a finite group, then the wreath product $G = AwrK$ is elementarily equivalent to $H = BwrK$. Universal equivalence is preserved under wreath products, that is $A_1 \equiv_\forall A_2, B_1 \equiv_\forall B_2 \to A_1 wr B_1 \equiv_\forall A_2 wr B_2$, but elementary equivalence (in the general case) is not, that is $A_1 \equiv A_2, B_1 \equiv B_2 \not\to A_1 wr B_1 \equiv A_2 wr B_2$ [251].

In [35], O. Chapuis proved his remarkable result: The elementary theory of any free metabelian group is decidable. An explicit description of this theory is given by him in [36]. He also proved that a noncyclic free metabelian group is universally equivalent to the wreath product of any two nontrivial torsion-free abelian groups.

V. Remeslennikov and R. Stöhr [212] characterizated the finitely generated groups in the quasivariety generated by a noncyclic free metabelian group from three different points of view: In terms of wreath products, in terms of module theoretic properties of their Fitting subgroups, and in terms of quasi-identities.

In [37], O. Chapuis proved that the terms of the derived series of a free solvable group are definable by existential formulae. He used this result to prove that if Hilbert's 10th problem has a negative answer for the field of the rationals, then the universal theory of a noncyclic free solvable group of class $\geqslant 3$ is undecidable. N. S. Romanovskii [221] proved that a free solvable group of derived length at least 4 has an algorithmically undecidable universal theory.

E. I. Timoshenko [257] proved that the universal theory of a free polynilpotent group $\mathfrak{N}_{c_1} \cdots \mathfrak{N}_{c_s}$, $s \geqslant 2$, $c_i \geqslant 1$, for $i = 1, \ldots, s-1$, $c_s \geqslant 2$, is undecidable.

The following result has been proved in [254]. Let $F(\mathfrak{V})$ be a free group of a variety $\mathfrak{V}$, approximable by finite p-groups for an infinite sequeuce of primes p. If the subgroup G of $F(\mathfrak{V})$ generates the same variety as $F(\mathfrak{V})$, then $G \equiv_\forall F(\mathfrak{V})$.

In [112], an algebraic characterization of elementary equivalence for polycyclic-by-finite groups was established. This characterization allowed to give the relations between their elementary equivalence and the elementary equivalence of the factors in their decompositions in direct products of indecomposable groups. In particular, it has been proved that the elementary equivalence of two such groups $G \equiv H$ is equivalent to each of the following properties: (1) $G \times \cdots \times G$ (k times G) for an integer $k \geqslant 1$; (2) $A \times G \equiv B \times H$

for two polycyclic-by-finite groups A, B such that $A \equiv B$. It is not presently known if (1) implies $G \equiv H$ for any groups G, H.

N. S. Romanovskii and E. I. Timoshenko found in [223] conditions for the universal equivalence of the metabelian group G with few relations to the free metabelian group M_r of rank r. They also proved that if an n-generated solvable group G is elementarily equivalent to a free solvable group S_{rd} of rank r and derived length d, then for $d = 2$ or $d > 2$ and $n = r$, the groups G and $S_{r,d}$ are isomorphic. In [260], E. I. Timoshenko studies elementary and universal theories of relatively free solvable groups in a group signature expanded by one predicate distinguishing primitive or annihilating systems of elements. In [259], he proved the following results. Let be the set of all primitive elements of M_2. Then there is a countable set of existential formulas that determines P, however, no finite subset of these formulas does. He also proved that two elements $g, f \in M_2'$ conjugate by some automorphism of M_2 if and only if they satisfy the same existential formulas.

The concept of a rigid (solvable) group was introduced by N. S. Romanovskii about 10 years ago. The rigid group class turned out to be quite interesting and noteworthy. At present, a number of results have been obtained for it, both group-theoretical and model-theoretic. Most of these results were obtained by the discoverer of this class. For these reasons, rigid groups can be called *Romanovskii' groups*. A group G is said to be m-rigid, where m is a natural number, if it has a normal series of the form $G = G_1 > \ldots > > G_m > G_{m+1} = 1$, whose quotients G_i/G_{i+1} are abelian and are torsion free when treated as $\mathbb{Z}[G/G_i]$-modules. Examples of rigid groups are free soluble groups. A. G. Myasnikov and N. S. Romanovskii [169] gave a recursive system of universal axioms distinguishing m-rigid groups in the class of solvable groups of length m. They proved that if G is an arbitrary m-rigid group, and W is an iterated wreath product of m infinite cyclic groups, then the universal theories for these groups satisfy the inclusions $\mathrm{Th}_\forall(W) \subseteq \mathrm{Th}_\forall(\mathrm{G}) \subseteq \subseteq \mathrm{Th}_\forall(\mathrm{S_{r,m}})$, where $r \geqslant 2$. An $\exists$-axiom is given that distinguish among m-rigid groups those that are universally equivalent to W. An arbitrary m-rigid group embeds in a divisible decomposed m-rigid group M, the semidirect product of m abelian groups. A recursive system of axioms distinguishing among M-groups those that are universally equivalent to M. As a consequence, it is stated that the universal theory of M with constants is decidable. By contrast, the universal theory of W with constants is undecidable.

Let $\Gamma = (X, E)$ be a finite simple graph. The right-angled Artin group (in other terminology, a partially commutative group) $G(\Gamma)$, corresponding to Γ, has the specification $\langle X,\, xy = yx\,(x, y) \in E\rangle$. If $\mathfrak{V}$ is a variety of groups, then the partially commutative $\mathfrak{V}$-group, corresponding to Γ, has the specification $\langle X,\, xy = yx\,(x, y) \in E; \mathfrak{V}\rangle$.

The paper [74] proves that two partially commutative metabelian groups have equal elementary theories if and only if their defining graphs are isomorphic, and that every partially commutative metabelian group is embeddable in a finitely generated metabelian group with decidable universal theory. In [224], N. S. Romanovskii and E. I. Timoshenko proved the following statement: Let the variety $\mathfrak{V}$ contain the variety $\mathfrak{N}_2$, and the finitely generated group H is elementarily equivalent to the partially free group $G = F(\Gamma, \mathfrak{V})$, then $G \simeq H$.

In [255], necessary and sufficient conditions are given for two partially commutative metabelian groups defined by trees to be universally equivalent. In [75], further properties of partially commutative metabelian groups and of their universal theories are described. In particular, it is shown that two partially commutative metabelian groups defined by cycles are universally equivalent if and only if the cycles are isomorphic. It is proved also

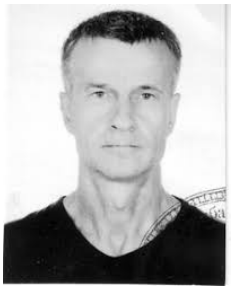
that the metabelian product of two non-trivial free abelian groups is universally equivalent to any free noncyclic metabelian group.

In [155] some necessary and sufficient conditions of the universal equivalence of the nilpotent R-groups of class 2 defined by trees, with R a binomial Euclidean ring are determined. Partially commutative nilpotent metabelian groups are considered in [76]. Universal theories for partially commutative nilpotent metabelian groups are compared: conditions on defining graphs of two partially commutative nilpotent metabelian groups are presented which are sufficient for the two groups to have equal universal theories; conditions on defining graphs of two partially commutative metabelian groups are specified which are sufficient for the two groups to be universally equivalent; a criterion is given that decides whether two partially commutative nilpotent metabelian groups defined by trees are universally equivalent.

A description of solvable groups with solvable elementary theory is known.

Theorem 15 (Yu. L. Ershov [57], N. S. Romanovskii [219], G. A. Noskov [185]).

The elementary theory of a finitely generated solvable group is decidable if and only if the group is virtually abelian.



G. A. Noskov

The corresponding problem has been posed in [95]. Yu. L. Ershov proved this statement [57] in the nilpotent case, N. S. Romanovskii [219] generalized it to the polycyclic case, and finally, G. A. Noskov [185] established the most general statement for the case of a finitely generated solvable group.

9. Rational subsets

The class $\mathrm{Rat}(G)$ of *rational subsets* of a group G is the smallest class that contains all finite subsets of G and that is closed with respect to the following *rational* operations:

— union $= A, B \in \mathrm{Rat}(G) \to A \cup B \in \mathrm{Rat}(G)$;
— product $= A, B \in \mathrm{Rat}(G) \to A \cdot B \in \mathrm{Rat}(G)$;
— taking the monoid generated by a set (Kleeny operation) $= A \in \mathrm{Rat}(G) \to A^* = \{1\} \cup \bigcup\limits_{i=1}^{\infty} A^i$.

This concept generalizes the classical notion of a regular subset of the free monoid Σ.

There is an analogue of Kleene's theorem on the definition of regular subsets of a free monoid by finite automata: a subset R of a group G is rational if and only if R is the output set of a finite automaton over G.

Recall that a finite automaton A over an alphabet σ consists of:

— a finite directed graph with edges labeled by elements of Σ;
— a distinguished initial vertex v_0;
— a set of final vertices $v_1, \ldots, v_t$.

The language $L(A)$ of the automaton consists of all words labeling a path from the initial vertex to a final vertex. A language is called *rational* if it is accepted by some finite automaton.

For definitions and basic properties of rational subsets in groups, see [66, 67, 235].

By well-known theorem of A. Anissimov and A. W. Seifert [5], a subgroup H of G belongs to $\mathrm{Rat}(G)$ if and only if H is finitely generated.

Rational submonoids need not be finitely generated. Rational subsets are not in general closed under complement and intersection.

Rational subset theory has many applications:

— V. Diekert, C. Gutierrez, and C. Hagenah [45] showed solving equations with rational constraints over free groups is PSPACE-complete.
— V. Diekert and M. Lohrey [46] used this to solve equations and decide the positive theory for right-angled Artin groups.
— F. Dahmani and V. Guirardel [40] solved equations over hyperbolic groups with special rational constraints. They gave an algorithm for solving equations and inequations with rational constraints in virtually free groups. This algorithm is based on E. Rip's classification of measured band complexes. Using canonical representatives, they deduced an algorithm for solving equations and inequations in hyperbolic groups (maybe with torsion).
— F. Dahmani and J. Groves [39] used rational subsets in their solution to the isomorphism problem for toral relatively hyperbolic groups.
— The order of g is finite if and only if $g^{-1} \in \{g\}^*$, so decidability of submonoid membership gives decidability of order.

The *rational subset membership problem* for a finitely generated group G is the decision problem, where for a given rational subset A of G and a group element g it is asked whether $g \in A$.

This section presents a survey on known decidability and undecidability results for the rational subset membership problem for groups. The membership problems for finitely generated submonoids and finitely generated subgroups will be discussed as well.

We list some of known results on the rational subset problem.

Positive results:

— (M. Benois [25]). Rational subset membership is decidable for free groups. (The proof uses an automata theoretic analogue of Stallings folding.)
— (C. Eilenberg and M. P. Schutzenberger [53]). Rational subset membership is decidable in abelian groups.
— (Z. Grunschlag [73]). Decidability of rational subset membership is a virtual property. (A property is called *virtual* if its execution for a subgroup of the finite index entails its execution on the entire group.)
— (M. Yu. Nedbai [177]). The decidability of rational subset membership passes through free products.
— (M. Cadilhac, D. Chistikov, and G. Zetzsche [38]). Rational subset membership is decidable for the Baumslag — Solitar groups $\mathrm{BS}(1, q)$ for $q \geqslant 2$.
— (M. Kambites, P. W. Silva, and B. Steinberg [91]). Decidability of rational subset membership is preserved by free products with amalgamation and HNN-extensions with finite edge groups. More generally, if G is a fundamental group of a graph of groups with finite edge groups and for each vertex group the rational set membership problem is solvable, then this problem is also solvable for G.

Let $\mathcal{C}$ be the smallest class of groups containing the trivial group and closed under:

— taking finitely generated subgroups;
— taking finite index overgroups;
— free products with amalgamation and HNN-extensions with finite edge groups;
— direct product with $\mathbb{Z}$.

Theorem 16 (M. Lohrey and B. Steinberg [118]). Every group in the class $\mathcal{C}$ has decidable rational subset membership problem.

There is no need to talk about the solvability of the membership problem for finitely generated submonoids of the group G if the classical problem of the membership for finitely generated subgroups of the group G is unsolvable. Note that direct products do not preserve the solvability of the occurrence problem. It was shown by K. A. Mikhailova [154], that the direct product $F_2 \times F_2$ of two copies of the free group of rank 2 contains a fixed finitely generated subgroup with an undecidable membership problem. In particular, $F_2 \times F_2$ has an undecidable subgroup membership problem. Hence, also the submonoid membership problem and the rational subset membership problem for $F_2 \times F_2$ are undecidable. This result is remarkable since $F_2 \times F_2$ is a very natural group.

The above result of M. Benois cannot be generalized to hyperbolic groups. Indeed, E. Rips [215] proved the existence of hyperbolic torsion-free groups, in particular, groups with small cancellation, on which condition $C'_{1/6}$ is satisfied, and in which the membership problem is unsolvable.

Let $\Gamma = (X, E)$ be a finite simple graph. Recall, that the right-angled Artin group (in other terminology, a partially commutative group) $G(\Gamma)$, corresponding to Γ, has the specification $\langle X,\, xy = yx\,(x, y) \in E\rangle$. It is said that the graph $\Gamma_1 = (X, E)$ contains a *induced graph* Γ_2 if there is a subset of vertices $U \subseteq V$ such that the graph Γ_2 is isomorphic to the graph $(U, E \cap (U \times U))$.

The subgroup membership problem is solvable in any group $G(\Gamma)$ when the graph Γ does not contain an induced cycle C_4 of length 4 [93]. On the other hand, the group $G(C_4)$ contains the direct product $F_2 \times F_2$, therefore, by the above-mentioned theorem of K. A. Mikhailova, there is a finitely generated subgroup in it with unsolvable membership problem.

M. Lohrey and B. Steinberg [118] show that the membership problem in a finitely generated submonoid of a right-angled Artin group is decidable if and only if the independence graph (commutation graph) is a transitive forest, i.e., it does not contain induced subgraphs of type C_4 or P_4, where P_4 denotes a straight line segment consisting of four vertices and three edges. Moreover, in the unsolvable case, one can indicate a fixed finitely generated submonoid of the group $G(\Gamma)$, the membrtship problem for which is unsolvable.

It is shown in [118] that membership in rational subsets of wreath products $HwrV$ with H a finite group and V a virtually free group is decidable. On the other hand, it is shown that there exists a fixed finitely generated submonoid in the wreath product $\mathbb{Z}wr\mathbb{Z}$ with an undecidable membership problem.

The author proved in [237] that any verbal subset $w[G]$ of a finitely generated nilpotent group G with respect to a word w of positive exponent is rational. Examples of verbal subsets of finitely generated metabelian groups that are not rational are given. Recall that the *verbal subset* of a group G is the set of all values of the group word w in this group.

Negative results:

— (V. A. Roman'kov [229]). There exists a number r such that the free nilpotent group $N_{r,2}$ of class 2 generated by r elements has an undecidable rational subset membership problem.
— M. Lohrey and B. Steinberg show in [119]that the free metabelian group M_2 of rank 2 contains a fixed finitely generated submonoid with an undecidable membership problem.

This result is shown via a reduction from the membership problem for finitely generated subsemimodules of free $(\mathbb{Z}\times\mathbb{Z})$-modules of finite rank. This considered problem is shown to be undecidable in by interpreting it as a particular tiling problem of the Euclidean plane that in turn is shown to be undecidable via a direct encoding of a Turing machine.

— M. Lohrey, B. Steinberg, and G. Zetzsche [120] prove that the submonoid membership problem is undecidable for $\mathbb{Z}\mathrm{wr}\mathbb{Z}$.

— U. U. Umirbaev [261] show that the free solvable group $S_{2,3}$ of derived length 3 and rank 2 has an undecidable subgroup membership problem.

— M. Lohrey [117] prove that there are numbers $n, l \geqslant 3$ and a sequence of cyclic subgroups $C_1, \ldots, C_l$ of the unitriangular matrix group $\mathrm{UT}_n(\mathbb{Z})$ over integers such that the membership problem with respect to the product $C_1 \cdots C_l$ is unsolvable.

The submonoid membership problem is the most important fragment of the rational subset problem. The well-known submonoid membership problem for nilpotent groups was recently solved by the author.

Theorem 17 (V. A. Roman'kov [240]). There is a finitely generated submonoid M of a free nilpotent group $N_{r,l}$ of class $l \geqslant 2$ of sufficiently large rank r, the membership problem for which is algorithmically unsolvable.

A. G. Myasnikov and the author [170] established that a verbal subset $w[F_r]$ of a free group F_r of finite rank $r \geqslant 2$ is rational in F_r if and only if $w[F_r] = 1$ or $w[F_r] = F_r$. The last two cases are easily recognized by the form of the word w. This statement is generalized to a wide class of free products of groups.

Rational subsets in nilpotent groups were also studied by G. A. Bazhenova [19]. She proved that the rational subsets of a finitely generated nilpotent group G are a Boolean algebra if and only if G is virtually abelian. Other results on the characterization of finitely generated groups G in which the set of rational subsets $\mathrm{Rat}(G)$ is a Boolean algebra, that is, a family of subsets closed under union, intersection, and complement operations are given in [20, 235, 238].

See [147] for a connection between the submonoid membership problem for a group G and the geometric properties of this group.

It is worth noting that the submonoid membership problem of entering for a free abelian group $A_r \simeq \mathbb{Z}^r$ of rank r is related to the following integer linear programming problem: For a given matrix $A \in \mathrm{M}_{m\times r}$ and vector $b \in \mathbb{Z}^r$ determine whether there exists a solution $x \in \mathbb{N}^m$ of the equation $xA = b$.

In group-theoretic language, this is the submonoid membership problem for the group A_r generated by the rows of the matrix A. It is well known that this version of the integer linear programming problem belongs to the class of NP-complete problems. The submonoid membership problem for an arbitrary group is currently considered as a natural generalization of the problem of integer linear programming. An overview of the related results can be found in [18].

10. Geodesic problems

The computational complexity of the WP in free solvable groups $S_{r,d}$, where $r \geqslant 2$ is the rank and $d \geqslant 2$ is the solvability class of the group, was studied in [171]. Let n be a length of a word (input) $w \in S_{r,d}$.

It is known that the Magnus embedding of $S_{r,d}$ into matrices provides a polynomial time decision algorithm for WP in a fixed group $S_{r,d}$. Unfortunately, the degree of the polynomial grows together with d, so the uniform algorithm is not polynomial in d.

Theorem 18 (A. Myasnikov, V. Roman'kov, A. Ushakov, and A. Vershik [171]).

— The Fox derivatives of elements from $S_{r,d}$ with values in the group ring $\mathbb{Z}S_{r,d-1}$ can be computed in time $O(n^3rd)$.

— The WP has time complexity $O(rn\log_2 n)$ in $S_{r,2}$, and $O(n^3rd)$ in $S_{r,d}$ for $d \geqslant 3$.

In [171], the following algorithmic and decision problems were considered:

— *The Geodesic problem* (GP): Given a word $w \in F(X)$, find a word $u \in F(X)$ which is geodesic in G such that $w =_G u$.

— *The Geodesic length problem* (GLP): Given a word $w \in F(X)$, find $|w|_G$.

— *Bounded geodesic length problem* (BGLP): Given a word $w \in F(X)$ and an integer k, decide if a geodesic representative has length $\leqslant k$.

It has been shown that for free metabelian groups (with standard generating sets) BGLP is NP-complete.

Though GLP seems easier than GP, in practice, to solve GLP one usually solves GP first, and only then computes the geodesic length. It is an interesting question if there exists a group G and a finite set X of generators for G relative to which GP is strictly harder than GLP.

Turing reducibility of the geodesic problems

It has been shown in [171] that a polynomial time solution to any of these problems implies a polynomial time solution to the next, and each implies a polynomial time solution to the word problem for the group.

The algorithmic "hardness" of the problems WP, BGLP, GLP, and GP in a given group G is explained by the following implications: each one is Turing reducible in polynomial time to the next one in the list:

$$WP \preceq_{T,p} BGLP \preceq_{T,p} GLP \preceq_{T,p} GP,$$

and GP is Turing reducible to WP in exponential time:

$$GP \preceq_{T,\exp} WP.$$

M. Elder and A. Rechnitzer [56] established that GP, GLP and BGLP are polynomial time and space reducible to each other.

Complexity of the geodesic problems

Recall the concept of time complexity. Let A be an algorithm with inputs from a set S, $|w|$ is the size of $w \in S$, $TA(w)$ is the number of steps required for A to stop on the input $w \in S$, A is in polynomial time if for some polynomial $p(x)$ means $TA(w) \leqslant p(|w|)$.

If G has polynomial *growth*, i.e., there is a polynomial $p(n)$ such that for each n cardinality of the ball B_n of radius n in the Cayley graph $\Gamma(G, X)$ is at most $p(n)$, then one can easily construct this ball B_n in polynomial time with an oracle for the WP in G. It follows that if a group with polynomial growth has WP decidable in polynomial time, then all the problems above have polynomial time complexity. Observe now, that by famous Gromov's theorem finitely generated groups of polynomial growth are virtually nilpotent. It is also known that the latter have WP decidable in polynomial time (nilpotent finitely generated groups are linear). These two facts together imply that the GP is polynomial time decidable in finitely generated virtually nilpotent groups.

On the other hand, there are many groups of exponential growth where GP is decidable in polynomial time:

— hyperbolic groups — B. A. Epstein et al;

— the Baumslag — Solitar group (metabelian, non polycyclic of exponential growth)

$$BS(1,p) = \langle a, t \mid t^{-1}at = a^p \rangle$$

(M. Elder [55]). An algorithm is presented to convert a word of length n in the standard generators of the solvable Baumslag — Solitar group BS$(1,p)$ into a geodesic word, which runs in linear time and $O(nlogn)$ space on a random access machine.

In general, if WP in G is polynomially decidable, then BGLP is in the class NP, i.e., it is decidable in polynomial time by a non-deterministic Turing machine. In this case GLP is Turing reducible in polynomial time to an NP problem, but we cannot claim the same for GP. Observe, that BGLP is in NP for any finitely generated metabelian group, since they have WP decidable in polynomial time.

It might happen though, that WP in a group G is polynomial time decidable, but BGLP in G is NP-complete.

W. Parry [191] showed that BGLP is NP-complete in the metabelian group $\mathbb{Z}_2 wr(\mathbb{Z}\times\mathbb{Z})$, the wreath product of $\mathbb{Z}_2$ and $\mathbb{Z}\times\mathbb{Z}$.

It was claimed by C. Droms, J. Lewin, and H. Servatius [48] that in $S_{r,d}$ GLP is decidable in polynomial time. Unfortunately, in this particular case their argument is fallacious. It turned out [171], that BGLP for M_r, $r \geqslant 2$, is NP-complete. Therefore, the search problems SGP and SGLP are NP-hard in non-abelian M_r. To see the NP-completeness, the authors of [171] constructed a polynomial reduction of the rectilinear Steiner tree problem to BGLP in M_r.

Free solvable groups of finite ranks

The conjugacy problem for S_r, d reduces via the Magnus embedding to a similar problem for $A_r wr S_{r,d-1}$ in time $O(n^3 rd)$.

The power problem (PP) in a group G:

$$\exists ? n \in \mathbb{Z} : g^n = f.$$

S. Vassileva [263] proved the following statements.

— The power problem in $S_{r,d}$ is decidable in time $O(n^6 rd)$.
— The conjugacy problem has time complexity $O(n^8 rd)$ in $S_{r,d}$.

A. Ushakov [262] designed new deterministic and randomized algorithms for computational problems in free solvable groups. He improved the results of [171, 263], namely, he proved that:

— There exists a quasi-quadratic time $\tilde{O}(n^2)$ deterministic algorithm solving the word problem in $S_{r,d}$.
— There exists a quasi-quadratic time $\tilde{O}(n^2)$ deterministic algorithm solving the power problem in $S_{r,d}$.
— There exists a quasi-quintic time $\tilde{O}(n^5)$ deterministic algorithm solving the conjugacy problem in $S_{r,d}$.

These results can be improved further if we grant our machine an access to a random number generator. But the result in this approach can be incorrect. Fortunately, the probability of an error is under control: for any fixed polynomial p we can adjust some internal parameter in the algorithm to guarantee that the probability of an error converges to 0 as fast as $O(1/p(n))$. In other words, there exists a quasi-linear time $\tilde{O}(n)$ false-biased randomized algorithm solving the word problem in $S_{r,d}$. There also exists a quasi-linear time $\tilde{O}(n)$ unbiased randomized algorithm solving the power problem in $S_{r,d}$.

Moreover, there exists a quasi-quartic time $\tilde{O}(n^4)$ unbiased randomized algorithm solving the conjugacy problem in $S_{r,d}$.

Thus, A. Ushakov [262] proved that the word problem and the power problem can be solved in quasi-linear time and the conjugacy problem can be solved in quasi-quartic time by Monte Carlo type algorithms.

The origins of computation group theory date back to the late nineteenth and early twentieth centuries. Since then, the field has flourished, particularly during the past 30 to 40 years, and today it remains a lively and active branch of mathematics.

The Handbook of Computational Group Theory offers the first complete treatment of all the fundamental methods and algorithms in CGT presented at a level accessible even to advanced undergraduate students. It develops the theory of algorithms in full detail and highlights the connections between the different aspects of CGT and other areas of computer algebra. While acknowledging the importance of the complexity analysis of CGT algorithms, the authors' primary focus is on algorithms that perform well in practice rather than on those with the best theoretical complexity.

Throughout the book, applications of all the key topics and algorithms to areas both within and outside of mathematics demonstrate how CGT fits into the wider world of mathematics and science. The authors include detailed pseudocode for all of the fundamental algorithms, and provide detailed worked examples that bring the theorems and algorithms to life.

We assume that practical algorithms work with random data. In numerous of cases "random" exclude "the worst" case. The Simplex Method is a very good sample of such algorithm.

Hence, the generic set of data when the algorithm works well became a very important notion.

It is known [65] that the Dehn function $\mathrm{D}(G)$ of a finitely presented group G is recursive if and only if G has decidable word problem. Moreover, for every finitely presented group G with Dehn function $\mathrm{D}(G)$ there exists a nondeterministic Turing machine $\mathrm{M}(G)$ which solves the word problem in G with time function equivalent to $\mathrm{D}(n)$. This machine solves the word problem in every finitely generated subgroup of G as well. Therefore if a finitely generated group G is a subgroup of a finitely presented group with polynomial isoperimetric function then the word problem in G is in NP (i.e., it can be solved by a non-deterministic Turing machine with polynomial time function

J. C. Birget, A. Y. Olshanskii, E. Rips, and M. V. Sapir [29] obtained a general result on the connection between the complexity of the Dehn function of a group and the complexity of the word problem. The word problem of a finitely generated group G is in NP if and only if this group is a subgroup of a finitely presented group H with polynomial isoperimetric function. The embedding can be chosen in such a way that G has bounded distortion in H.

There is a natural concept of the averaged Dehn function $\mathrm{D}_{av}(G)$, introduced by M. Gromov [68]. In [110], E. G. Kukina and the author, answering to the question, posed in [68], proved that $\mathrm{D}(A_r)$ is sub-quadratic (remind that $\mathrm{D}(A_r)$ is quadratic). In [230], the author answered to the another question posed in [68] on the average Dehn function of a free nilpotent group. He showed that this function is asymptotically negligible to the Dehn function in this case.

In [92], I. Kapovich, A. G. Myasnikov, V. Shpilrain, and P. Schupp proposed a generic approach to the theory of computability and computational complexity. Within the framework of this approach, the algorithmic problem is considered not on the entire set of inputs, but on a certain subset of almost all inputs. They showed that for a large class

of finitely generated groups the generic time complexity of some classical decision problems from combinatorial group theory, namely the word problem, conjugacy problem and membership problem, are linear. It turns also out that some classical undecidable problems are, in fact, strongly undecidable, i.e., they are undecidable on every strongly generic subset of inputs. A. G. Myasnikov and A. N. Rybalov [172] proved an analog of the Rice theorem for strongly undecidable problems, which provides plenty of examples of strongly undecidable problems. To construct strongly undecidable problems, they introduced a method of generic amplification (an analog of the amplification in complexity theory).

In recent years, interest in the analysis of algorithms from the point of view of complexity theory and practical feasibility has significantly increased. Substitution groups form the most developed part of the computational theory of groups. The basis for this was the corresponding technique for their study, developed by C. Simps back in the 60s of the twentieth century. M. L. Furst, D. Hopcroft, and E. M. Luks [60] showed that the method proposed by Simps works in polynomial time. The time-polynomial theory of linear groups began with a consideration of matrix groups over finite fields. The main problems were the problems of determining the order of a subgroup given by a finite set of generators, and the membership problem for a given group. Even in the case of abelian groups, it is not known how to solve such problems without solving difficult number-theoretic problems, for example, problems of the discrete logarithm and factorization of numbers. The approach to finding a solution using a number-theoretic oracle became natural.

Computing in permutation and in matrix groups

Permutation groups is the most developed subdomain in the Computational Group Theory. Fundamental is a technique first proposed by C. Sims in the 1960's, see monograph [248]. C. Sims introduced many algorithms for working with permutation groups. These were among the first algorithms in CAYLEY and GAP. In 1990s nearly linear algorithms for permutation groups emerged. These are now in GAP and MAGMA. In 2003, Á. Seress published his monograph [245] described the theory behind permutation group algorithms, including developments based on the classification of finite simple groups. He gave rigorous complexity estimates, implementation hints, and advanced exercises. The book fills a significant gap in the symbolic computation literature.

Let $G \leqslant Sym(\Omega)$, where $\Omega = \{\omega_1, \ldots, \omega_n\}$. The tower

$$G = G^{(1)} \geqslant \ldots \geqslant G^{(n+1)} = 1,$$

where $G^{(i)}$ is a pointwise stabilizer of $\{\omega_1, \ldots, \omega_{i-1}\}$, underlines almost all practical algorithms. It was proved in [60] that a variant of Sims' method runs in polynomial time. Now there is the non-substancional polynomial-time library for permutation groups.

Polynomial-time theory of linear groups started with matrix groups over finite fields. Such group is specified by finite list of generators. The two most basic questions are:

— membership in $\mathrm{gp}(U)$;
— the order of the group $\mathrm{gp}(U)$.

Even in the case of abelian groups it is not known how to answer these questions without solving hard number-theoretic problems (factoring and discrete logarithm). So the reasonable question is whether these problems are decidable in randomized polynomial time using number theory oracles.

The first algorithms for computing with finite solvable matrix groups were designed by E. M. Luks [121].

E. M. Luks, L. Babai, R. Beals, Á. Seress et al. study this area for last 25–30 years (see [7]). Let $G \leqslant GL(n, \mathbb{F}_q)$ be a finitely generated matrix group over a finite field $\mathbb{F}_q$.

— One can test in polynomial time whether G is solvable and, if so, whether G is nilpotent.
— If G is solvable, one can also find, for each prime p, the p-part of G. In the nilpotent case it is its (unique) Sylow p-subgroup.
— Also, given a solvable $G \leqslant GL(n, \mathbb{F}_q)$ the following problems can be solved: find $|G|$, decide the MP with respect to G, find a presentation of G via generators and defining relators, find a composition series of G, et cetera.

For polycyclic groups pc-presentation approach was introduced by B. Eick, D. Kahrobaei, G. Ostheimer et al. See [52] for definition and basic properties of pc-presentations. Pc-presentation of a polycyclic group exhibits its polycyclic structure. Pc-presentations allows efficient computations with the groups they define. In particular, the WP is efficiently decidable in a group given by a pc-presentation. GAP package polycyclic is designed for computations with polycyclic groups which are given by a pc-presentations.

Let G be a polycyclic group. Then

$$G \in \mathcal{N}\mathfrak{A}\mathcal{F}.$$

Hence, nilpotent-by-abelian-by finite presentation approach can be applied in this case.

In particular, Bieri — Strebel's invariant is defined for for this type of groups [28].

The solution of BTCP in a finitely generated metabelian group looks more practical than the Noskov's solution in the classical case of the CP. Main feature is that we can reduce the problem changing the group itself. In the polycyclic case we can start with the metabelian image G/G'' and then use induction relative the structure of a polycyclic group as above.

A. Garetta et al. [63] introduce a model of random finitely generated, torsion-free nilpotent groups G of class 2. They prove that for some values of parameters the following holds asymptotically almost surely:

— The ring of integers $\mathbb{Z}$ is definable in G.
— Systems of equations over $\mathbb{Z}$ are reducible to systems over G (and hence they are undecidable).
— The maximal ring of scalars of G is $\mathbb{Z}$.
— G is indecomposable as a direct product of non-abelian factors.

The similar models of random polycyclic groups and random finitely generated nilpotent groups of any nilpotency step, possibly with torsion, were also introduced

For matrix groups over infinite fields, we state the following theorem as the first result.

Theorem 19 (V. M. Kopytov [107]). Let $G \leqslant GL(n, K)$ be a finitely generated matrix group over an algebraic number field K. Then the following problems are decidable:

— determine finiteness of G;
— determine solvability of G;
— MP_{sol} = the membership problem with respect to solvable G.

Most computational problems are known to be decidable for polycyclic matrix groups over number fields.

The WP and MP can be solved [6], many further structural problems have a practical solution.

D. F. Holt, B. Eick, and O'Brien published the monograph "The Handbook of Computational Group Theory" [90] which offers the first complete treatment of all the fundamental methods and algorithms in computational group theory. It develops the theory of algorithms in full detail and highlights the connections between the different aspects of

computational group theory and other areas of computer algebra. The monograph focused on algorithms that perform well in practice rather than on those with the best theoretical complexity.

Some methods are developed for computing with matrix groups defined over a range of infinite domains.

A. Detinko, B. Eick, and D. L. Flannery [43] gave a practical nilpotent testing algorithm for finitely generated matrix groups over an infinite field $\mathbb{F}$.

The main algorithms have been implemented in GAP, for groups over $\mathbb{Q}$.

Let $\mathbb{F} = \bar{\mathbb{Q}}$ be an algebraic number field. By the celebrated Tits's theorem a finitely generated subgroup $G \leqslant GL(n, \bar{\mathbb{Q}})$ either contains a nonabelian free subgroup F or has a solvable subgroup H of finite index (*Tits Alternative*).

R. Beals [21] established the following results:

— There is a polynomial time algorithm for deciding which of two conditions of the Tits's Alternative holds for a given G.

— Let G has a solvable subgroup H of finite index. Then one is able in polynomial time to compute a homomorphism φ such that $\varphi(G)$ is a finite matrix group, and $\ker(\varphi)$ is solvable.

If, in addition, H is nilpotent, then there is efficient method to compute an encoding of elements of G.

Nowadays, it is recognized that there are decision and search variations of algorithmic problems:

— Search word problem (SWP) in G : given $w \in F(X)$, such that $w =_G 1$, find a decomposition $w = \prod_{i=1}^{n} g_i^{-1} r_{i_j} g_i$, where $g_i \in F(X)$, $r_{i_j} \in R^{\pm 1}$.

— Search conjugacy problem (SCP) in G: given two words $u, v \in F(X)$, which define conjugated elements in G, find a conjugator.

— Search membership problem (SMP) in G for a fixed subgroup $H \leqslant G$: given $w \in F(X)$ which belongs to H, find its decomposition as a product of the generators of H.

— Search isomorphism problem (SIP) in a given class $\mathcal{C}$ of presentations: given two presentations in $\mathcal{C}$ of isomorphic groups, find an isomorphism.

In [127], it is proved that the basic algorithmic problems (normal forms, conjugacy of elements, subgroup membership, centralizers, presentation of subgroups, etc.) can be solved by algorithms running in logarithmic space and quasilinear time. Further, if the problems are considered in "compressed" form with each input word provided as a straight-line program, we showed that the problems are solvable in polynomial time. See monograph [116] for the necessary background and detailed exposition of known results on the compressed word problem, emphasizing efficient algorithms for the compressed word problem in various groups.

Basic information about circuit complexity is contained in monograph [265]. This monograph presents a broad and up-to-date view of the computational complexity theory of Boolean circuits. The theory of circuit complexity classes is thoroughly developed.

In [176], the authors pushed the complexity of these problems lower, showing that they may be solved by TC^0 circuits. In [175], it was shown that the conjugacy problem in a wreath product $AwrB$ is uniform-TC^0-Turing-reducible to the conjugacy problem in the factors A and B and the power problem in B. Under certain natural conditions, there is a uniform TC^0 Turing reduction from the power problem in $AwrB$ to the power problems of A and B.

In [128], the authors expand the list of algorithmic problems for nilpotent groups which may be solved in these low complexity conditions to include several fundamental problems concerning subgroups. The following algorithmic problems are solved using TC^0 circuits, or in logspace and quasilinear time, uniformly in the class of nilpotent groups with bounded nilpotency class and rank: subgroup conjugacy, computing the normalizer and isolator of a subgroup, coset intersection, and computing the torsion subgroup. Additionally, if any input words are provided in compressed form as straight-line programs or in Mal'cev coordinates, the algorithms run in quartic time.

A. V. Menshov, A. G. Myasnikov, and A. V. Ushakov [153] study the computational complexity of the fundamental algorithmic problems in finitely generated metabelian groups. They rewrite and streamline some classical algorithms to fit them into the framework of Groebner basis. In many cases this reduction can be done in polynomial time. The algorithmic problems in metabelian groups are classified in terms of logspace and circuit complexities.

Acknowledgments. The reported study was funded by RFBR, project number 20-11-50063.

REFERENCES

1. *Adian S. I.* Nerazreshimost' nekotorykh algoritmicheskikh problem teorii grupp [Unsolvability of some algorithmic problems in the theory of groups]. Tr. Mosk. Mat. Obs., 1957, vol. 6, pp. 231–298. (in Russian)
2. *Adian S. I. and Durnev V. G.* Decision problems for groups and semigroups. Russian Math. Surveys, 2000, vol. 55, no. 2, pp. 207–296.
3. *Agalakov S. A.* Finite separability of groups and Lie algebras. Algebra and Logic, 1983, vol. 22, no. 4, pp. 261–268.
4. *Amaglobeli M. G.* Varieties of exponential MR-groups. Doklady Math., 2020, vol. 101, no. 1, pp. 1–4.
5. *Anissimov A. and Seifert A. W.* Zur algebraischen Charakteristik der durch kontextfreie Sprachen definierten Gruppen. Elektron. Inform. Verarb. Kybern., 1975. vol. 11, pp. 695–702. (in German)
6. *Assman B. and Eick B.* Computing polycyclic presentations for polycyclic rational matrix groups. J. of Symb. Comp., 2005, vol. 40, no. 6, pp. 1269–1284.
7. *Babai L, Beal R., and Seress A.* Polynomial-time theory of matrix groups. Proc. STOC'09, May 31–June 2, 2009, Bethesda, Maryland, pp. 55–64.
8. *Bachmuth S.* Automorphisms of free metabelian groups. Trans. Amer. Math. Soc., 1965, vol. 118, pp. 93–104.
9. *Baumslag G.* Lecture Notes on Nilpotent Groups. C.B.M.S. Regional Conf. Series, 2, Providence, 1971. 73 p.
10. *Baumslag G.* Residually finite groups with the same finite images. Compositio Math., 1974, vol. 29, pp. 249–252.
11. *Baumslag G., Cannonito F. B., and Robinson D. J. S.* The algorithmic theory of finitely generated metabelian groups. Trans. Amer. Math. Soc., 1994, vol. 344, no. 2, pp. 629–648.
12. *Baumslag G., Cannonito F. B., Robinson D. J. S., and Segal D.* The algorithmic theory of polycyclic-by-finite groups. J. Algebra, 1991, vol. 141, pp. 118–149.
13. *Baumslag G., Gildenhuys D., and Strebel R.* Algorithmically insoluble problems about finitely presented solvable groups, Lie and associative algebras. I. J. Pure Appl. Algebra, 1986, vol. 39, pp. 53–94.

14. *Baumslag G., Gildenhuys D., and Strebel R.* Algorithmically insoluble problems about finitely presented solvable groups, Lie and associative algebras. II. J. Algebra, 1985, vol. 97, pp. 278–285.
15. *Baumslag G., Miller C. F. III, and Ostheimer G.* Subgroups of free metabelian groups. Groups Geom. Dyn., 2010, vol. 4, pp. 657–679.
16. *Baumslag G., Miller C. F. III, and Ostheimer G.* Decomposability of finitely generated torsion-free nilpotent groups. Int. J. Algebra and Comput., 2016, vol. 26, no. 8, pp. 1529–1546.
17. *Baumslag G., Myasnikov A. G., and Remeslennikov V. N.* Algebraic geometry over groups. I. J. Algebra, 1999, vol. 219, pp. 16–79.
18. *Bassino F., Kapovich I., Lohrey M., et al.* Complexity and Randomness in Group Theory: GAGTA BOOK 1, Walter de Gruyter GmbH, Berlin, Boston, 2020. 386 p.
19. *Bazhenova G. A.* Rational sets in finitely generated nilpotent groups. Algebra and Logic, 2000, vol. 39, no. 4, pp. 215–223.
20. *Bazhenova G. A.* Closure of one class of groups under free product. Siberian Math. J., 2000, vol. 41, no. 4, pp. 611–613.
21. *Beals R.* Algorithms for matrix groups and the Tits alternative. J. Comput. System Sci., 1999, vol. 58, no. 2, pp. 260–279.
22. *Belegradek O. V.* The Mal'cev correspondence revisited. Proc. Int. Conf. Algebra, Part 1 (Novosibirsk, 1989), pp. 37–59; Contemp. Math., vol. 131, Part 1, Amer. Math. Soc., Providence, RI, 1992.
23. *Belegradek O. V.* The model theory of unitriangular groups. Ann. Pure Appl. Logic, 1994, vol. 68, pp. 225–261.
24. *Belegradek O. V.* Model theory of unitriangular groups. Model Theory and Applications, Amer. Math. Soc. Transl. Ser. 2, 1999, vol. 195, pp. 1–116.
25. *Benois M.* Parties rationnelles du groupe libre. C. R. Acad. Sci., Paris, Ser. A, 1969, vol. 269, pp. 1188–1190. (in French)
26. *Bieri R., Neumann W. D., and Strebel R.* A geometric invariant of discrete groups. Invent. Math., 1987, vol. 90, no. 3, pp. 451–477.
27. *Bieri R. and Strebel R.* Valuations and finitely presented metabelian groups. Proc. London. Math. Soc., 1980, vol. 41, no. 1, pp. 439–464.
28. *Bieri R. and Strebel R.* A geometric invariant for nilpotent-by-abelian-by-finite groups. J. Pure Appl. Algebra, 1982, vol. 25, no. 1, pp. 1–20.
29. *Birget J. C., Olshanskii A. Y., Rips E., and Sapir M. V.* Isoperimetric and isodiametric functions of groups and computational complexity of the word problem. Ann. Math., 2002, vol. 156, no. 2, pp. 467–518.
30. *Birman J. S.* Braids, Links and Mapping Class Groups. Ann. Math. Stud., vol. 82, Princeton, Princeton Univ. Press, 1974. 237 p.
31. *Blackburn S.* Conjugacy in nilpotent groups. Proc. Amer. Math. Soc., 1965, vol. 16, pp. 143–148.
32. *Bokut L. A. and Kukin G. P.* Algorithmic and Combinatorial Algebra. (Math. and its Applications, vol. 255), Netherlands, Springer. 1994. XVI + 384 p.
33. *Boone W. W.* The word problem. Ann. Math., 1959, vol. 70, no. 2, pp. 207–265.
34. *Chandler B. and Magnus W.* The History of Combinatorial Group Theory. A Case Study in the History of Ideas. Studies in the History of Math. and Physical Sciences, N.Y., Springer Verlag, 1982, vol. 9, VIII + 234 p.
35. *Chapuis O.* Universal theory of certain solvable groups and bounded Ore group-rings. J. Algebra, 1995, vol. 176, no. 2, pp. 368–391.

36. *Chapuis O.* ∀-free metabelian groups. J. Symb. Logic, 1997, vol. 62, no. 1, pp. 159–174.
37. *Chapuis O.* On the theories of free solvable groups. J. Pure Appl. Algebra, 1998, vol. 131, no. 1, pp. 13–24.
38. *Cadilhac M., Chistikov D., and Zetzsche G.* Rational subsets of Baumslag — Solitar groups. Proc. ICALP 2020, Leibniz, Dagstuhl Publ., 2020, pp. 116:1–116:16.
39. *Dahmani F. and Groves D.* The isomorphism problem for toral relatively hyperbolic groups. Publications mathématiques de l'IHES, 2008, vol. 107, no. 1, pp. 211–290
40. *Dahmani F. and Guirardel D. V.* Foliations for solving equations in groups: free, virtually free, and hyperbolic groups. J. Topology, 2010, vol. 3, no. 2, pp. 343–404.
41. *Danyarova E. Yu., Myasnikov A. G., and Remeslennikov V. N.* Algebraicheskaya geometriya nad algebraicheskimi sistemami [Algebraic Geometry over Algebraic Systems]. Novosibirsk, Siberian Branch of Russian Academy of Sciences Publ., 2016. 243 p. (in Russian).
42. *Dehn M.* Über unendliche diskontinuierliche Gruppen. Math. Ann., 1911, vol. 71, no. 1, pp. 116–144. (in German)
43. *Detinko A. S., Eick B., and Flanneri D. L.* Computing with matrix groups over infinite fields. London Math. Soc. Lect. Note Ser., 2011, vol. 387, pp. 256–270.
44. *Detinko A. S., Eick B., and Flannery D. L.* Nilmat — Computing with nilpotent matrix groups, A refereed GAP, 2007.
45. *Diekert V., Gutierrez C., and Hagenah C.* The existential theory of equations with rational constraints in free groups is PSPACE-complete. Inform. and Computation, 2005, vol. 202, no. 2, pp. 105–140.
46. *Diekert V. and Lohrey M.* Word equations over graph products. Int. J. Algebra Comput., 2008, vol. 18, no. 3, pp. 493–533.
47. *Dixon J. D., Formanek E. W., Poland J. C. and Ribes L.* Profinite completions and isomorphic finite quotients. J. Pure Appl. Algebra, 1982, vol. 23, no. 3, pp. 227–231.
48. *Droms C., Lewin J., and Servatius H.* The length of elements in free solvable groups. Proc. Amer. Math. Soc., 1993, vol. 119, pp. 27–33.
49. *Duchin M., Liang H., and Shapiro M.* Equations in nilpotent groups. Proc. Amer. Math. Soc., 2015, vol. 143, no. 11, pp. 4723–4731.
50. *Dyck W. von.* Analysis Situs I. Math. Ann., 1888, vol. 32, pp. 457–512.
51. *Ehrenfeucht A., Karhumaki J., and Rozenberg G.* The (generalized) Post correspondence problem with lists consisting of two words is decidable. Theoret. Comput. Sci., 1982, vol. 21, pp. 119–144.
52. *Eick B.* Computing with infinite polycyclic groups. Groups and Computations, III. G. R. Baker, W. D. Neumann, and K. Rubin (eds.), Proc. Int. Conf. at the Ohio State Univ., June 15–19, 1999, Berlin; New York, Walter de Gruyterm, pp. 139–154.
53. *Eilenberg S. and Schutzenberger M. P.* Rational sets in commutative monoids. J. Algebra, 1969, vol. 13, pp. 173–191.
54. *Eklof P. C. and Fischer E. R.* The elementary theory of abelian groups. Ann. Math. Logic, 1972, vol. 4, no. 2, pp. 115–171.
55. *Elder M.* A linear-time algorithm to compute geodesics in solvable Baumslag — Solitar groups. Illinois J. Math., 2010, vol. 54, no. 1, pp. 109–128.
56. *Elder M. and Rechnitzer A.* Some geodesic problems in groups. Groups, Complexity, Cryptology, 2010, vol. 2, pp. 223–229.
57. *Ershov Yu. L.* Ob elementarnykh teoriyakh grupp [Elementary group theories]. Dokl. Akad. Nauk SSSR, 1972, vol. 203, no. 6, pp. 1240–1243. (in Russian)

58. *Fedorov E. S.* Simmetrija pravil'nich system figur [Symmetry of regular systems of figures]. Zap. Imperatorsk. S-Peterburgsk. Mineral. Občestva Verhandl. d. Russisch-Kaiserl. Mineral. Gesellschaft zu St. Petersburg, 1891, vol. 28, pp. 1–146. (in Russian)
59. *Formanek E.* Conjugacy separability in polycyclic groups. J. Algebra, 1976, vol. 42, pp. 1–10.
60. *Furst M. L., Hopcroft J., and Lucks E. M.* Polynomial-time algorithms for permutation groups.. Proc. 21st FOCS, ICEE C.S., 1980, vol. 198, pp. 36–41.
61. *Gaglione J. R. and Spellman D.* The persistence of universal formulae in free algebras. Bull. Austr. Math. Soc., 1987, vol. 36, pp. 11–17.
62. *Garey M. R. and Johnson D. S.* Computers and Intractability: A Guide to the Theory of NP-Completeness. N.Y., W. H. Freeman, 1979. 338 p.
63. *Garreta A., Miasnikov A., and Ovchinnikov D.* Random nilpotent groups, polycyclic presentations, and Diophantine problems. Groups, Complexity, Cryptology, 2017, vol. 9, no. 2, pp. 99–115.
64. *Garreta A., Legarreta L., Miasnikov A., and Ovchinnikov D.* Metabelian groups: Full-rank presentations, randomness and Diophantine problems. J. Group Theory, 2020, accepted for publication.
65. *Gersten S. M.* Dehn functions and l_1-norms for finite presentations. Algorithms and Classification in Combinatorial Group Theory. G. Baumslag and C. F. Miller (eds.), MSRI Publ., vol. 23, Berlin, Springer Verlag, 1992.
66. *Gilman R. H.* Formal languages and infinite groups. Geometric and Computational Perspectives on Infinite Groups, DIMACS, Ser. Discr. Math. Theor. Comput. Sci., Providence, 1996, vol. 25, pp. 27–51.
67. *Gilman R. H.* Formal languages and their application to combinatorial group theory. Groups, Languages, Algorithms, Contemporary Math. Series, Providence, 2005, vol. 378, pp. 1–36.
68. *Gromov M.* Asymptotic invariants of infinite groups. Geometric Group Theory, Cambridge, Cambridge Univ. Press, 1993, pp. 1–295.
69. *Grunewald F., Pickel P. F., and Segal D.*, Polycyclic groups with isomorphic finite quotients. Ann. Math., 1980. vol. 111, pp. 155–195.
70. *Grunewald F. and Segal D.* The solubility of certain decision problems in arithmetic and algebra. Bull. Amer. Math. Soc., 1979, vol. 1, no. 6, pp. 915–918.
71. *Grunewald F. and Segal D.* Some general algorithms. I. Arithmetic groups. II. Nilpotent groups. Ann. Math., 1980, vol. 112, no. 3, pp. 531–583.
72. *Grunewald F. and Zalesskii P.* Genus for groups. J. Algebra, 2011, vol. 326, no. 1, pp. 130–168.
73. *Grunschlag Z.* Algorithms in Geometric Group Theory. PhD. Thesis, University of California at Berkley, 1999. 127 p.
74. *Gupta C. K. and Timoshenko E. I.* Partially commutative metabelian groups: centralizers and elementary equivalence. Algebra and Logic, 2009, vol. 48, no. 3, pp. 173–192.
75. *Gupta C. K. and Timoshenko E. I.* Universal theories for partially commutative metabelian groups. Algebra and Logic, 2011, vol. 50, no. 1, pp. 3–25.
76. *Gupta C. K. and Timoshenko E.,I.* Properties and universal theories for partially commutative nilpotent metabelian groups. Algebra and Logic, 2012, vol. 51, no. 4, pp. 285–305.
77. *Hall M. Jr.* The Theory of Groups. N.Y., Macmillan, 1959. 434 p.
78. *Hall P.* Finiteness conditions for soluble groups. Proc. London Math. Soc., 1954, vol. 4(3), pp. 419–436.
79. *Hall P.* Finite-by-nilpotent groups. Proc. Cambridge Philos. Soc., 1956., vol. 52, pp. 611–616.
80. *Hall P.* Some sufficient conditions for a group to be nilpotent. Illinois J. Math., 1958, vol. 2, pp. 787–801.

81. *Hall P.* On the finiteness of certain soluble groups. Proc. London Math. Soc., 1959, vol. 9(3), pp. 595–622.
82. *Hall P.* The Edmonton Notes on Nilpotent Groups. Queen Mary College Math. Notes. Queen Mary College, London, 1969. 76 p.
83. *Hall P.* The collected Works of Philip Hall. Oxford Science Publications. N.Y., Oxford University Press, 1988. 776 p.
84. *Higgins P. J. and Lyndon R. C.* Equivalence of elements under automorphisms of a free group. J. London Math. Soc., 1974, vol. 8, pp. 254–258.
85. *Hirsch K. A.* On infinite soluble groups, I. Proc. London Math. Soc., 1938, vol. 44(2), pp. 53–60.
86. *Hirsch K. A.* On infinite soluble groups, II. Proc. London Math. Soc., 1938, vol. 44(2), pp. 336–344.
87. *Hirsch K. A.* On infinite soluble groups, III. Proc. London Math. Soc., 1946, vol. 49(2), pp. 184–194.
88. *Hirsch K. A.* On infinite soluble groups, IV. Proc. London Math. Soc., 1952, vol. 27(3), pp. 81–85.
89. *Hirsch K. A.* On infinite soluble groups, V. Proc. London Math. Soc., 1954, vol. 29(3), pp. 250–261.
90. *Holt D. F., Eick B., and O'Brien E. A.* Handbook of Computational Group Theory. Chapman and Hall/CRC, 2020. 536 p.
91. *Kambites M., Silva P. V., and Steinberg B.* On the rational subset problem for groups. J. Algebra, 2007, vol. 309, no. 2, pp. 622–639.
92. *Kapovich I., Myasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks. J. Algebra, 2003, vol. 264, no. 2, pp. 665–694.
93. *Kapovich I., Weidmann R., and Myasnikov A.* Foldings, graphs of groups and the membership problem. Int. J. Algebra and Comput., 2005, vol. 15, no. 1, pp. 95–128.
94. *Kargapolov M. I. and Remeslennikov V. N.* Problema sopryazhennosti dlya svobodnykh razreshimykh grupp [Conjugacy in free solvable groups]. Algebra i Logika, 1966, vol. 5, no. 6, pp. 15–25. (in Russian)
95. *Kargapolov M. I., Remeslennikov V. N., Romanovskii N. S., et al.* Algorithmic problems for o-powered groups. Algebra and Logic, 1969, vol. 8, no. 6, pp. 363–374.
96. *Kargapolov M. I. and Timoshenko E. I.* Some questions in the theory of soluble groups. Lect. Notes in Math., 1974, vol. 372, pp. 389–394.
97. *Kharlampovich O. G.* A finitely presented solvable group with undecidable word problem. Math. USSR-Izvestiya, 1982, vol. 19, no. 1, pp. 151–169.
98. *Kharlampovich O. G.* Equality problem for subvarieties of the variety $\mathfrak{N}_2\mathfrak{A}$. Algebra and Logic, 1987, vol. 26, no. 4, pp. 284–299.
99. *Kharlampovich O. G.* Finitely presented solvable groups and Lie algebras with unsolvable equality problem. Math. Notes, 1989, vol. 46, no. 3, pp. 731–739.
100. *Kharlampovich O., López L., and Myasnikov A.* The Diophantine problem in some metabelian groups. Math. Comp., 2020, vol. 89, pp. 2507–2519.
101. *Kharlampovich O. and Myasnikov A.* Irreducible affine varieties over free groups, I: Irreducibility of quadratic equations and Nullstellensatz. J. Algebra, 1998, vol. 200, no. 2, pp. 472–516.
102. *Kharlampovich O. and Myasnikov A.* Irreducible affine varieties over free groups, II: Systems in triangular quasi-quadratic form and description of residually free groups. J. Algebra, 1998, vol. 200, no. 2, pp. 517–570.

103. *Kharlampovich O. and Sapir M.* Algorithmic problems in varieties, a survey. Int. J. Algebra and Comp., 1995, vol. 12, pp. 379–602.
104. *Kleiman Yu. G.* Tozhdestva i nekotorye algoritmicheskie problemy v gruppakh [Identities and some algorithmic problems in groups]. Dokl. Akad. Nauk SSSR, 1979, vol. 244, no. 4, pp. 814–818. (in Russian)
105. *Kleiman Yu. G.* O tozhdestvakh v gruppakh [On identities in groups]. Tr. Mosk. Mat. Obs., 1982, vol. 44, pp. 62–108. (in Russian)
106. *Klein F.* Vergleichende Betrachtungen über neuere geometrische Forschungen. Math. Ann., 1893, vol. 43, pp. 63–100. (in German)
107. *Kopytov V. M.* Solvability of the problem of occurrence in finitely generated soluble groups of matrices over the field of algebraic numbers. Algebra and Logic, 1968, vol. 7, no. 6, pp. 388–393.
108. Kourovka Notebook. Unsolved problems in group theory. V. D. Mazurov and E. I. Khukhro (eds.), no. 19, Novosibirsk, Sobolev Institute of Math., Russian Academy of Sciences, Siberian Branch, 2018. 246 p.
109. *Krasilnikov A. N. and Shmel'kin A. L.* Primeneniya vlozheniya Magnusa v teorii mnogoobraziy grupp i algebr Li [Applications of the Magnus embedding in the theory of varieties of groups and Lie algebras]. Fundam. Prikl. Mat., 1999, vol. 5, pp. 493–502. (in Russian)
110. *Kukina E. G. and Roman'kov V. A.* Subquadratic growth of the averaged Dehn function for free Abelian groups. Siberian Math. J., 2003. vol. 44, no. 4, pp. 605–610.
111. *Lashkhi A. A. and Bokelavadze T. Z.* Subgroup lattices and the geometry of Hall W-power groups. Doklady Math., 2009. vol. 80, no. 3, pp. 731–734.
112. *Lasserre C. and Oger F.* Direct products and elementary equivalence of polycyclic-by-finite groups. J. Algebra, 2014, vol. 418, pp. 213–226.
113. *Lennox J. C. and Robinson D. J. S.* The Theory of Infinite Soluble Groups. Oxford Math. Monographs. Oxford, Oxford Science Publ., Clarendon Press, 2004. 342 p.
114. *Lie S.* Theorie der Transformationsgruppen I. Leipzig, B. G. Teubner, 1888. 650 p. (in German)
115. *Lo E. H.* Finding intersection and normalizer in finitely generated nilpotent groups. J. Symb. Comput., 1998, vol. 25, pp. 45–59.
116. *Lohrey M.* The Compressed Word Problem for Groups. Berlin, Springer Science & Business Media, 2014. 153 p. (Springer Briefs in Math.).
117. *Lohrey M.* Rational subsets of unitriangular groups. Int. J. Algebra and Comput., 2015, vol. 25, no. 01n02, pp. 113–121.
118. *Lohrey M. and Steinberg B.* The submonoid and rational subset membership problems for graph groups. J. Algebra, 2008, vol. 320, pp. 728–755.
119. *Lohrey M. and Steinberg B.* Tilings and submonoids of metabelian groups. Theory of Comput. Systems, 2011, vol. 48, no. 2, pp. 411–427.
120. *Lohrey M., Steinberg B., and Zetzsche G.* Rational subsets and submonoids of wreath products. Inform. and Comput., 2015, vol. 243, pp. 191–204.
121. *Luks E. M.* Computing in solvable matrix groups. Proc. 33rd IEEE Symp. Foundations of Comput. Sci., 1992, pp. 111–120.
122. *Lyndon R. C.* The equation $a^2b^2 = c^2$ in free groups. Michigan Math. J., 1959, vol. 6, pp. 89–95.
123. *Lyndon R. C.* Equations in free groups. Trans. Amer. Math. Soc., 1960, vol. 96, pp. 445–457.
124. *Lyndon R. C.* Equations in free metabelian groups. Proc. Amer. Math. Soc., 1966, vol. 17, pp. 728–730.

125. *Lyndon R. C. and Shupp P. E.* Combinatorial Group Theory. Berlin; Heidelberg; New York, Springer Verlag, 1977. 339 p.
126. *Lysenok I. and Ushakov A.* Spherical quadratic equations in free metabelian groups. Proc. Amer. Math. Soc., 2016, vol. 144, pp. 1383–1390.
127. *Macdonald J., Myasnikov A., Nikolaev A., and Vassileva S.* Logspace and compressed-word computations in nilpotent groups. arXiv: 1503.03888v1 [math. GR] 12 Mar 2015, pp. 1–38.
128. *Macdonald J., Miasnikov A., and Ovchinnikov D.* Low-complexity computations for nilpotent subgroup problems. Int. J. Algebra and Comput., 2019, vol. 29, no. 4, pp. 639–661.
129. *Magnus W.* Über diskontinuierliche Gruppen mit einer definierenden Relation. (Der Freiheitssatz). J. Reine Angew. Math., 1930, vol. 163, pp. 141–165. (in German)
130. *Magnus W.* Das Identitätsproblem für Gruppen mit einer definierenden Relation. Math. Ann., 1932, vol. 106, no. 1, pp. 295–307. (in German)
131. *Magnus W.* On a theorem of Marshall Hall. Ann. Math., 1939, vol. 40, pp. 764–768.
132. *Magnus W., Karrass A., and Solitar D.* Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations. N.Y., Wiley, 1966. 444 p.
133. *Magnus W.* Collected Papers. G. Baumslag and B. Chandler (eds.) N.Y., Springer Verlag, 1984. 726 p.
134. *Majewicz S.* On classes of exponential A-groups. Comm. in Algebra, 2010, vol. 38, no. 4, pp. 1363–1384.
135. *Majewicz S. and Zyman M.* Power-commutative nilpotent R-powered groups. Groups, Complexity, Cryptology, 2009. vol. 1, no. 2, pp. 297–310.
136. *Makanin A. G.* O finitnoy approksimiruemosti uravneniy v konechno porozhdennykh nil'potentnykh gruppakh [Residual finiteness of equations in finitely generated nilpotent groups]. Vestnik Moskov. Univ. Ser. 1, Mat. Mekh., 1992, no. 1, pp. 48–51. (in Russian).
137. *Makanin G. S.* Equations in a free group. Math. USSR-Izvestia, 1983, vol. 21, no. 3, pp. 483–546.
138. *Makanin G. S.* Decidability of universal and positive theories of a free group. Math. USSR-Izvestia, 1985, vol. 25, no. 1, pp. 75–88.
139. *Mal'cev A. I.* O gruppakh konechnogo ranga [On groups of finite rank]. Mat. Sb. (N.S.), 1948, vol. (64), no. 2, pp. 351–352. (in Russian)
140. *Mal'cev A. I.* Nil'potentnye gruppy bez krucheniya [Nilpotent torsion-free groups]. Izv. Akad. Nauk SSSR, Ser. Mat., 1949, vol. 13, iss. 3, pp. 201–212. (in Russian)
141. *Mal'cev A. I.* O nekotorykh klassakh beskonechnykh razreshimykh grupp [On some classes of infinite soluble groups]. Mat. Sb. (N.S.), 1951, vol. 28(70), no. 3, pp 567–588. (in Russian)
142. *Mal'cev A. I.* Gomomorfizmy na konechnykh gruppakh [Homomorphisms onto finite groups]. Ivanov. Gos. Ped. Inst. Uchen. Zap., 1958, no. 18, pp. 49–60. (in Russian)
143. *Mal'cev A. I.* O svobodnykh razreshimykh gruppakh [On free solvable groups]. Dokl. Akad. Nauk SSSR, 1960, vol. 130, no. 3, pp. 495–498. (in Russian)
144. Mal'cev A. I. Ob uravnenii $zxyx^{-1}y^{-1} = aba^{-1}b^{-1}$ v svobodnoy gruppe [On the equation $zxyx^{-1}y^{-1} = aba^{-1}b^{-1}$ in a free group]. Algebra i Logika. Sem., 1962, vol. 1, no. 5, pp. 45–50. (in Russian)
145. *Mal'cev A. I.* The elementary properties of linear groups. A. I. Mal'cev. The Metamath. of Algebraic Systems. Collected papers: 1936–1967, Studies in Logic and Foundations of Math., vol. 66, Amsterdam, North-Holland Publ. Company, 1971.
146. *Mal'cev A. I.* On a certain correspondencece between rings and groups. A. I. Mal'cev. The Metamath. of Algebraic Systems, Collected papers: 1936–1967, Studies in Logic and Foundations of Math., vol. 66, Amsterdam, North-Holland Publ. Company, 1971.

147. *Margolis S. W., Meakin J. C., and Šunik Z.* Distortion functions and the membership problem for submonoids of groups and monoids. Geometric Methods in Group Theory, Contemporary Math., vol. 372, Amer. Math. Soc., 2005, pp. 109–129.

148. *Matijasevič Yu. V.* Diophantine representation of enumerable predicates. Math. USSR-Izvestiya, 1971, vol. 5, no. 1, pp. 1–28.

149. *Matiyasevich Yu.* Some purely mathematical results inspired by mathematical logic. Proc. Fifth Intern. Congr. Logic, Methodology and Philos. of Sci., London, Ont., 1995, pp. 121–127.

150. *Matiyasevich Yu. and Senizergues G.* Decision problems for semi-Thue systems with a few rules. LNCS, 1996, vol. 96, pp. 523–531.

151. *Matiyasevich Yu. and Senizergues G.* Decision problems for semi-Thue systems with a few rules. Theor. Comput. Sci., 2005, vol. 330, pp. 145–169.

152. *Mel'nikov O. V., Remeslennikov V. N., Roman'kov V. A., et al.* Obshchaya algebra. V. 1 [General Algebra, vol. 1.] Moscow, Nauka Publ., 1990. 591 p. (in Russian)

153. *Menshov A. V., Myasnikov A. G. and Ushakov A. V.* Algorithms for metabelian groups. Vestnik Omskogo Universiteta, 2018, vol. 23, no. 2, pp. 27–34.

154. *Mikhailova K. A.* Problema vkhozhdeniya dlya pryamykh proizvedeniy grupp [The occurrence problem for direct products of groups]. Mat. Sb. (N.S.), 1966, vol. 70(112), no. 2, pp. 241–251. (in Russian)

155. *Mishchenko A. A. and Timoshenko E. I.* Universal equivalence of partially commutative nilpotent groups. Siberian Math. J., 2011, vol. 52, no. 5, pp. 884–891.

156. *Mostowski A.* Computational algorithms for deciding some problems for nilpotent groups. Fund. Math., 1966, vol. 59, no. 2, pp. 137–152.

157. *Myasnikov A. G.* Elementary theories and abstract isomorphisms of finite dimensional algebras and unipotent groups. Dokl. Math., 1988, vol. 36, no. 3,pp. 464–467.

158. *Myasnikov A. G.* Elementary theory of a module over a local ring. Siberian Math. J., 1989, vol. 30, no. 3, pp. 403–412.

159. *Myasnikov A. G.* The structure of models and a criterion for the decidability of complete theories of finite-dimensional algebras. Math. USSR-Izvestia, 1990, vol. 34, no. 2, pp. 389–407.

160. *Myasnikov A. G.* The theory of models of bilinear mappings. Siberian Math. J., 1990, vol. 31, no. 3, pp. 439–451.

161. *Myasnikov A. G.* Definable invariants of bilinear mappings. Siberian Math. J., 1990. vol. 31, no. 1, pp. 89–99.

162. *Myasnikov A., Nikolaev A., and Ushakov A.* The Post correspondence problem in groups. J. Group Theory, 2014, vol. 17, pp. 991–1008.

163. *Myasnikov A., Nikolaev A., and Ushakov A.* Knapsack problems in groups. Math. of Comput., 2015, vol. 84, no. 292, pp. 987–1016.

164. *Myasnikov A., Nikolaev A., and Ushakov A.* Non-commutative lattice problems. J. Group Theory, 2016, vol. 19, no. 3, pp. 455–475.

165. *Myasnikov A. G. and Remeslennikov V. N.* Klassifikatsiya stepennykh nil'potentnykh grupp po elementarnym svoystvam [Classification of nilpotent power groups by their elementary properties]. Trudy Inst. Mat. Sib. Otd. AN SSSR, 1982, vol. 2, pp. 56–87. (in Russian)

166. *Myasnikov A. G. and Remeslennikov V. N.* Definability of the set of Mal'cev bases and elementary theories of finite-dimensional algebras. I. Siberian Math. J., 1982, vol. 23, no. 5, pp. 711–724.

167. *Myasnikov A. G. and Remeslennikov V. N.* Definability of the set of Mal'cev bases and elementary theories of finite-dimensional algebras. II. Siberian Math. J., 1983, vol. 24, no. 2, pp. 231–246.

168. *Myasnikov A. G. and Remeslennikov V. N.* Algebraic geometry over groups, II: Logical foundations. J. Algebra, 2000, vol. 234, pp. 225–276.
169. *Myasnikov A. G. and Romanovskii N. S.* Universal theories for rigid soluble groups. Algebra and Logic, 2012, vol. 50, no. 6, pp. 539–552.
170. *Myasnikov A. and Roman'kov V.* On rationality of verbal subsets in a group. Theory Comput. Syst., 2013, vol. 52, no. 4, pp. 587–598.
171. *Myasnikov A., Roman'kov V., Ushakov A., and Vershik A.* The word and geodesic problems in free solvable groups. Trans. Amer. Math. Soc., 2010, vol. 362, no. 9, pp. 4655–4682.
172. *Myasnikov A. and Rybalov A.* Generic complexity of undecidable problems //J. Symb. Logic. 2008. vol. 73, no. 2, pp. 656–673.
173. *Myasnikov A., Shpilrain V., and Ushakov A.* Non-commutative Cryptography and Complexity of Group-theoretic Problems. Providence, Rhode Island, Amer. Math. Soc., 2011. 385 p. (Math. Surveys and Monographs, vol. 177).
174. *Myasnikov A. G. and Sohrabi M.* Groups elementarily equivalent to a free nilpotent group of finite rank. Ann. Pure Appl. Logic, 2011, vol. 162, no. 11, pp. 916–833.
175. *Myasnikov A., Vassileva S., and Weiss A.* The conjugacy problem in free solvable groups and wreath product of abelian groups is in TC^0. Theory Comput. Syst., 2019, vol. 63, pp. 809–832.
176. *Myasnikov A. and Weiss A.* TC^0 circuits for algorithmic problems in nilpotent groups. 2017. Preprint at arXiv:1702.06616 [math.GR].
177. *Nedbai M. Yu.* Problema vkhozhdeniya v ratsional'noe podmnozhestvo svobodnogo proizvedeniya grupp [The rational subset problem for free products of groups]. Vestnik Omskogo Universiteta, 2000, no. 2, pp. 17–18. (in Russian)
178. *Newman M. F.* On a class of nilpotent groups. Proc. London Math. Soc., 1960, vol. 10(3), pp. 365–375.
179. *Nielsen J.* Om regning med ikke-kommutative faktorer og dens anvendelse i gruppeteorien. Math. Tidsskrift, 1921, vol. B, pp. 77–94. (in Danish)
180. *Nielsen J.* Die isomorphismengruppe ger freien Gruppen. Math. Ann., 1924, vol. 91, pp. 169–209. (in German)
181. *Nikolaev A. and Ushakov A.* Subset sum problem in polycyclic groups. J. Symb. Comput., 2018, vol. 84, pp. 84–94.
182. *Nikolov N. and Segal D.* On finitely generated profinite groups. I. Strong completeness and uniform bounds. Ann. Math., 2007, vol. 65, no. 1, pp. 171–238.
183. *Noskov G. A.* Conjugacy problem in metabelian groups. Math. Notes, 1982, vol. 31, no. 4, pp. 252–258.
184. *Noskov G. A.* O rode svobodnoy metabelevoy gruppy [On the Genus of a Free Metabelian Group]. Preprint no. 84-509, Academy of Sciences USSR, Siberian Branch, Novosibirsk, Comput. Center, 1984, 18 p. (in Russian)
185. *Noskov G. A.* On the elementary theory of a finitely generated almost solvable group. Izv. Akad. Nauk SSSR Ser. Mat., 1984, vol. 47, no. 3, pp. 465–482.
186. *Noskov G. A., Remeslennikov V. N., and Roman'kov V. A.* Infinite groups. J. Soviet Math., 1982, vol. 18, no. 5, pp. 669–735.
187. *Novikov P. S.* On the algorithmic unsolvability of the word problem in group theory //Trudy Mat. Inst. Steklov. 1955. vol. 44, 143 p.
188. *Novikov P. S.* Über einige algorithmische Probléme der Gruppentheorie. Jber. Deutsch. Math. Verein, 1958, vol. 61, pp. 88–92. (in German)
189. *Oger F.* Elementary equivalence and isomorphism of finitely generated nilpotent groups. Comm. Algebra, 1984, vol. 12, pp. 1899–1915.

190. *Oger F.* Cancellation and elementary equivalence of finitely generated finite-by-nilpotent groups. J. London Math. Soc., 1991, vol. 44(2), pp. 173–183.
191. Parry W. Growth series of some wreath products. Trans. Amer. Math. Soc., 1992, vol. 331, pp. 751–759.
192. *Pickel P. F.* Finitely generated nilpotent groups with isomorphic finite quotients. Trans. Amer. Math. Soc., 1971, vol. 160, pp. 327–341.
193. *Pickel P. F.* Metabelian groups with the same finite quotients. Bull. Austral. Math. Soc., 1974, vol. 11, pp. 115–120.
194. *Plotkin B. I.* Varieties of algebras and algebraic varieties. Izrael J. Math., 1996, vol. 96, no. 2, pp. 511–522.
195. *Plotkin B. I.* Varieties of algebras and algebraic varieties. Categories of algebraic varieties. Siberian Adv. Math., 1997, vol. 7, no. 2, pp. 64–97.
196. *Plotkin B. I.* Geometrical equivalence, geometrical similarity, and geometrical compatibility of algebras. J. Math. Sci., 2007, vol. 140, no. 5, pp. 716–728.
197. *Plotkin B.* Seven lectures on algebraic geometry. Groups, Algebras and Identities. E. Plotkin (ed.), Research workshop of the Israel Science Foundation Honoring Boris Plotkin's 90th birthday, March 20–24, 2016. Contemporary Math., 2016, vol. 726, pp. 143–211.
198. *Poincaré H.* Sur l'Analysis situs Comptes Rendus, 1892, vol. 115, pp. 633–636. (in French)
199. *Poincaré H.* Analysis Situs. J. d'Ecole Polytechnique Normale, 1895, vol. 1, pp. 1–121. (in French)
200. *Post E. L.* A variant of a recursively unsolvable problem. Bull. Amer. Math. Soc., 1946, vol. 52, pp. 264–268.
201. *Rabin M. O.* Recursive unsolvability of group theoretic problems. Ann. Math., 1958, vol. 67, no. 1, pp. 172–194.
202. *Rapaport E.* On free groups and their automorphisms. Acta Math., 1958, vol. 99, pp. 139–163.
203. *Reid A. W.* Profinite rigidity. Proc. Int. Cong. Math., Rio de Janeiro, 2018, vol. 1, pp. 1191–1214.
204. *Reidemeister K.* Über unendliche discrete Gruppen. Hamburg Abh., 1926, vol. 3, pp. 33–39. (in German)
205. *Reidemeister K.* Einführung in die kombinatorische Topologie. Braunschweig, 1932, XII + 209 p. (in German). Translated and reprinted by Chelsea, New York, 1952.
206. *Remeslennikov V. N.* Conjugacy separability of groups. Siberian Math. J., 1971, vol. 12, pp. 783–792.
207. *Remeslennikov V. N.* Example of a group finitely generated in the variety $\mathfrak{A}^n, n \geqslant 5$, with the unsolvable word problem. Algebra and Logic, 1973, vol. 12, no. 5, pp. 327–346.
208. *Remeslennikov V. N.* An algorithmic problem for nilpotent groups and rings. Siberian Math. J., 1979, vol. 20, no. 5, pp. 71–74.
209. *Remeslennikov V. N. and Romanovskii N. S. Irreducible algebraic sets in metabelian groups.* Algebra and Logic, 2005, vol. 44, no. 5, pp. 336–347.
210. *Remeslennikov V. N. and Roman'kov V. A.* Model-theoretic and algorithmic questions in group theory. J. Soviet Math., 1985, vol. 31, no. 3, pp. 2887–2939.
211. *Remeslennikov V. N. and Sokolov V. G.* Some properties of a Magnus embedding. Algebra and Logic, 1970, vol. 9, no. 5, pp. 342–349.
212. *Remeslennikov V. N. and Stöhr R.* On the quasivariety generated by a non-cyclic free metabelian group. Alg. Colloq., 2004, vol. 11, no. 2, pp. 191–214.
213. *Repin N. N.* Equations with one unknown in nilpotent groups. Math. Notes, 1983, vol. 34, no. 2, pp. 582–585.

214. *Repin N. N.* The solvability problem for equations in one unknown in nilpotent groups. Math. USSR-Izv., 1985, vol. 48, no. 6, pp. 1295–1313.
215. *Rips E.* Subgroups of small cancellation groups. Bull. London Math. Soc., 1982, vol. 14, no. 1, pp. 45–47.
216. *Romanovskii N. S.* Some algorithmic problems for solvable groups. Algebra and Logic, 1974, vol. 13, no. 1, pp. 13–16.
217. *Romanovskii N. S.* Free subgroups of finitely presented groups. Algebra and Logic, 1977, vol. 16, no. 1, pp. 62–68.
218. *Romanovskii N. S.* The occurrence problem for extensions of abelian groups by nilpotent groups. Siberian Math. J., 1980, vol. 21, pp. 170–174.
219. *Romanovskii N. S.* On the elementary theory of an almost polycyclic group. Math. USSR-Sbornik, 1981, vol. 39, no. 1, pp. 125–132.
220. *Romanovskii N. S.* Algebraic sets in metabelian groups. Algebra and Logic, 2007, vol. 46, no. 4, pp. 503–513.
221. *Romanovskii N. S.* Universal theories for free solvable groups. Algebra and Logic, 2012, vol. 51, no. 3, pp. 259–263.
222. *Romanovskii N. S. and Gupta C. K.* The word problem for polynilpotent groups with a single primitive defining relation. Algebra and Logic, 2006, vol. 45, no. 1, pp. 17–25.
223. *Romanovskii N. S. and Timoshenko E. I.* On some elementary properties of soluble groups of derived length 2. Siberian Math. J., 2003, vol. 44, pp. 350–354.
224. *Romanovskii N. S. and Timoshenko E. I.* Elementary equivalence and direct product decompositions of partially commutative groups of varieties. Siberian Math. J., 2020, vol. 61, no. 3, pp. 538–541.
225. *Roman'kov V. A.* Unsolvability of the endomorphic reducibility problem in free nilpotent groups and in free rings. Algebra and Logic, 1977, vol. 16, no. 4, pp. 310–320.
226. *Roman'kov V. A.* Equations in free metabelian groups. Siberian Math. J., 1979, vol. 20, no. 3, pp. 469–471.
227. *Roman'kov V. A.* Universal theory of nilpotent groups. Math. Notes, 1979, vol. 25, no. 4, pp. 253–258.
228. *Roman'kov V. A.* Infinite generation of automorphism groups of free pro-p groups. Siberian Math. J., 1993, vol. 34, no. 4, pp. 727–732.
229. *Roman'kov V. A.* On the occurence problem for rational subsets of a group. V. Roman'kov (ed.), Int. Conf. on Comb. and Comput. Methods in Math., 1999, pp. 76–81.
230. *Roman'kov V. A.* Asymptotic growth of averaged Dehn function for nilpotent groups. Algebra and Logic, 2007, vol. 46, no. 1, pp. 37–45.
231. *Roman'kov V. A.* The twisted conjugacy problem for endomorphisms of polycyclic groups //J. Group Theory. 2010. vol. 13, no. 3, pp. 355–364.
232. *Roman'kov V. A.* Equations over groups. Groups, Complexity, Cryptology, 2012, vol. 4, no. 2, pp. 191–239.
233. *Roman'kov V. A.* The Post Correspondence Problem in metabelian and polycyclic groups. Proc. Conference "Algebra and Math. Logic: Theory and Applications" (Kazan, June 2–6, 2014), Kazan: Kazan Federal University, 2014, pp. 32–32.
234. *Roman'kov V. A.* The Post Correspondence Problem. `https://www.researchgate.net/publication/269169063_The_Post_Correspondence_Problem_PCP`, 2014.
235. *Roman'kov V. A.* Ratsional'nye podmnozhestva v gruppakh [Rational Subsets in Groups]. Omsk, Omsk State Univrersity, 2014. 176 p. (in Russian)
236. *Roman'kov V. A.* Diophantine questions in the class of finitely generated nilpotent groups. J. Group Theory, 2016, vol. 19, no. 3, pp. 497–516.

237. *Roman'kov V. A.* Rationality of verbal subsets of solvable groups. Algebra and Logic, 2018, vol. 57, no. 1, pp. 39–48.
238. *Roman'kov V. A.* Polycyclic, metabelian, or soluble of type $(\mathrm{FP})_\infty$ groups with Boolean algebra of rational sets and biautomatic soluble groups are virtually abelian. Glasgow Math. J., 2018, vol. 60, no. 1, pp. 209–218.
239. *Roman'kov V. A.* Essays in Group Theory and Cryptology. Solvable Groups. Omsk, Omsk State University Publishing House, 2017. 268 p.
240. *Roman'kov V. A.* Nonsolvability of the submonoid membership problem for the free nilpotent group of class $l \geqslant 2$ of suffitiently large rank. Izv. RAS, Ser. Math., submitted for publication.
241. *Sarkisjan R. A.* Algorithmic questions for linear algebraic groups, I. Math. USSR-Sbornik, 1982, vol. 41, no. 2, pp. 149–189.
242. *Sarkisjan R. A.* Algorithmic questions for linear algebraic groups, II. Math. USSR-Sbornik, 1982, vol. 41, no. 3, pp. 329–359.
243. *Schreier O.* Die Untergruppen der freien Gruppen. Abh. Math. Sem. Univ. Hamburg, 1927, vol. 5, pp. 161–183. (in German)
244. *Segal D.* Decidable properties of polycyclic groups.Proc. London Math. Soc., 1990, vol. 61, pp. 497–528.
245. *Seress Á.* Permutation Group Algorithms, Cambridge Tracts in Math. 152, Cambridge, Cambridge University Press, 2003. 264 p.
246. *Shmel'kin A. L.* Wreath products and varieties of groups. Math. USSR-Izvestia, 1965, vol. 29, pp. 433–434.
247. *Shmel'kin A. L.* O polnykh nil'potentnykh gruppakh [On complete nilpotent groups]. Algebra i Logika. Sem., 1967, vol. 6, no. 2, pp. 111–114. (in Russian)
248. *Sims C. C.* Computation with finitely presented groups, Encyclopedia of Math. and its Applications. Cambridge, Cambridge University Press, 1994, vol. 48. 624 p.
249. *Szmielew W.* Elementary properties of abelian groups. Fund. Math., 1955, vol. 41, pp. 203–271.
250. *Tietze H.* Über die topologischen Invarianten mehrdimensionaler Mannigfaltigkeiten. Monatsh. f. Math. u. Phys., 1908, vol. 19, pp. 1–118. (in German)
251. *Timoshenko E. I.* Preservation of elementary and universal equivalence under the wreath product. Algebra and Logic, 1968, vol. 7, no. 4, pp. 273–276.
252. *Timoshenko E. I.* K voprosu ob elementarnoy ekvivalentnosti grupp [On the question of elementary equivalence of groups]. Algebra, 1972, vol. 1, Irkutsk, Irkutsk State University, pp. 92– 96. (in Russian)
253. *Timoshenko E. I.* Algorithmic problems for metabelian groups. Algebra and Logic, 1973, vol. 12, no. 2, pp. 132–137.
254. *Timoshenko E. I.* Universally equivalent solvable groups. Algebra and Logic, 2000, vol. 39, no. 2, pp. 131–138.
255. *Timoshenko E. I.* Universal equivalence of partially commutative metabelian groups. Algebra and Logic, 2010. vol. 49, no. 2, pp. 177–196.
256. *Timoshenko E. I.* Endomorfizmy i universal'nye teorii razreshimykh grupp [Endomorphisms and universal theories of solvable groups]. Novosibirsk, Novosibirsk State Technical University, 2011. 327 p. (in Russian)
257. *Timoshenko E. I.* Universal theory of a free polynilpotent group. Izv. Math., 2016, vol. 80, no. 3, pp. 623–632.
258. *Timoshenko E. I.* A remark on spherical equations in free metabelian groups. Groups, Complexity, Cryptology, 2017, vol. 9, no. 2, pp. 155–158.

259. *Timoshenko E. I.* O fragmentakh teoriy nekotorykh razreshimykh ili nil'potentnykh grupp [On fragments of theories of some solvable or nilpotent groups]. Vestnik Omskogo universiteta, 2018, vol. 23, no. 2, pp. 47–52. (in Russian)

260. *Timoshenko E. I.* Theories of relatively free solvable groups with extra predicate. Algebra and Logic, 2018, vol. 57, no. 4 pp. 295–308.

261. *Umirbaev U. U.* Occurrence problem for free solvable groups. Algebra and Logic, 1995, vol. 34, no. 2, pp. 112–124.

262. *Ushakov A.* Algorithmic theory of free solvable groups: randomized computations. J. Algebra, 2014, vol. 407, no. 1, pp. 178–200.

263. *Vassileva S.* Polynomial time conjugacy in wreath products and free solvable groups. Groups, Complexity, Cryptology, 2011, vol. 3, no. 1, pp. 105–120.

264. *Ventura E. and Roman'kov V. A.* The twisted conjugacy problem for endomorphisms of metabelian groups. Algebra and Logic, 2009. vol. 48, no. 2, pp. 89–98.

265. *Vollmer H.* Introduction to Circuit Complexity. Berlin, Springer, 1999. 272 p.

266. *Whitehead J. H. C.* On equivalent sets of elements in a free group. Ann. Math., 1936, vol. 37, no. 4, pp. 782–800.

267. Word problems, II. S. I. Adian, W. W. Boone, G. Higman (eds.), Amsterdam; N.Y.; Oxford, North-Holland, 1980 (Studies in Logic and the Foundations of Math., vol. 95). 578 p.

268. *Zil'ber B. I.* An example of two elementarily equivalent but non-isomorphic finitely generated groups. Algebra and Logic, 1971, vol. 10, no. 3, pp. 192–197.

UDC 519.142 DOI 10.17223/20710410/52/3

ON THE NONEXISTENCE OF CERTAIN ORTHOGONAL ARRAYS OF STRENGTH FOUR[1]

R. Kiss*, G. P. Nagy**

*,** *Bolyai Institute, University of Szeged, Szeged, Hungary*
** *Department of Algebra, Budapest University of Technology and Economics, Budapest, Hungary*

E-mail: Kiss.Rebeka@stud.u-szeged.hu, nagyg@math.bme.hu

We show that no orthogonal arrays $OA(16\lambda, 11, 2, 4)$ exist with $\lambda = 6$ and 7. This solves an open problem of the NSUCRYPTO Olympiad 2018. Our result allows to determine the minimum weights of certain higher order correlation-immune Boolean functions.

Keywords: *orthogonal array, NSUCRYPTO.*

Introduction

In the Fifth International Students' Olympiad in Cryptography NSUCRYPTO'2018 [1, 2] the following problem was stated. Given three positive integers n, t, and λ such that $t < n$, we call a $\lambda 2^t \times n$ binary array (i.e., matrix over the two-element field) a $t-(2, n, \lambda)$ orthogonal array if in every subset of t columns of the array, every (binary) t-tuple appears in exactly λ rows; t is called the strength of this orthogonal array. Find a $4-(2, 11, \lambda)$ orthogonal array with minimal value of λ. So far, the best known answer to this question is $\lambda = 8$. Delsarte's Linear Programming Bound [3, Theorem 4.15 and Table 4.19] implies $\lambda \geqslant 6$.

In this short note, we use the terminology of the monograph [3] and we denote a $t-(2, n, \lambda)$ orthogonal array by $OA(2^t\lambda, n, 2, t)$. The integers $N = 2^t\lambda$ and n are called the number of runs and the number of factors of the array. In an orthogonal array, the same row can occur multiple times. The orthogonal array is *simple,* if each row occurs exactly once.

Our solution to the problem is stated in the following theorem.

Theorem 1. No orthogonal arrays $OA(16\lambda, 11, 2, 4)$ exist with $\lambda = 6$ and 7.

A Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is *correlation-immune* of some order $t < n$ (in brief, t-CI) if fixing at most t of the n input variables $x_1, \ldots, x_n$ does not change the output distribution of the function, whatever are the positions chosen for the fixed variables and the values chosen for them. Equivalently, the support of the function must be a simple binary orthogonal array of strength t [4, 5]. The weight of a Boolean function is the size of its support. Low weight t-CI Boolean functions have practical importance in cryptography, since they resist the Siegenthaler attack. Furthermore, t-CI Boolean functions allow reducing the overhead while keeping the same resistance to side channel attacks; see [5] and the references therein.

[1]Support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme, within the SETIT Project 2018-1.2.1-NKP-2018-00004. Partially supported by NKFIH-OTKA Grants 119687, 115288 and SNN 132625.

Theorem 1 allows us to determine the minimum weights of t^{th}-order correlation-immune Boolean functions in n variables,

$$n \in \{11, 12, 13\}, \quad t \in \{4, 5\}.$$

These values were marked as unknown in [4, Table 2] and [5, Table 2].

We would like to thank Claude Carlet (Paris, France and Bergen, Norway) for his detailed comments on the previous version of this paper.

1. Proof of the theorem

Our proof uses the results [6 – 9]. D. A. Bulutoglu and F. Margot [6] used integer linear programming (ILP) methods, while the algorithms [7, 8] are based on the systematic study of the extensions of orthogonal arrays by new columns. Moreover, both approaches must deal with the isomorphism problem of orthogonal arrays.

***Proof of the Theorem* 1.** From [6, Table 1], [7, Table III] and also [9] we can see that no $OA(96, 8, 2, 4)$ and no $OA(112, 7, 2, 4)$ exist. We explain the relevant rows of the two tables. In [6, Table 1] there are 4 columns with the following meanings (see Table 1):

— OA gives the parameters of the classified orthogonal array;
— m' is the number of linearly independent equality constraints of the generated ILP problem;
— $p_{\max}$ is an upper bound on the maximum number of times a run can appear in an $OA(2^t\lambda, n, 2, t)$;
— h is the number of non-isomorphic orthogonal arrays with the given parameters.

Table 1

OA	m'	$p_{\max}$	h
$OA(96, 8, 2, 4)$	163	2	0
$OA(112, 7, 2, 4)$	99	3	0

From this table we can see that if $\lambda = 6$ then no orthogonal array exists with $n = 8$, which implies that no OA exists with $n \geqslant 8$. Similarly if $\lambda = 7$ then no orthogonal array exists with $n = 7$, thus no OA exists with $n \geqslant 7$.

In [7, Table III] (see also Table 2) orthogonal arrays with strength 4 are included, where

— N gives the run-size of the classified orthogonal array;
— the notation 2^a for the factor set means a binary array with a factors;
— $a_{\max}$ is the maximum number a, such that there exists an OA with N runs and a factors;
— the numbers m_a, $a \in \{t + 1, \ldots, a_{\max}\}$, in the last column denote the number of isomorphism classes of arrays with N runs and a factors.

Table 2

N	Factor set	$a_{\max}$	Isomorphism classes
96	2^a	7	$4, 9, 4$
112	2^a	6	$4, 3$

This means that with run-size 96 the maximum number a such that an $OA(96, a, 2, 4)$ exists is 7, and with run-size 112 the maximum number a with an existing $OA(112, a, 2, 4)$ is 6. ■

Remark 1. According to [8], the number of isomorphism classes of binary orthogonal arrays with run-size $N = 128$, factor-size $n = 11$, and strength $t = 4$ is 477. The papers [6, 7]

claim to achieve the above results within a few seconds. Using SageMath [10], the GLPK package [11] and the integer linear programming solver SCIP [12], a straightforward implementation of the formulas of [6] used 51 630 s and 481 s CPU time for the nonexistence of $OA(96, 8, 2, 4)$ and $OA(112, 7, 2, 4)$, respectively.

2. Minimum weight of correlation-immune Boolean functions

Using the notation of [3], we denote by $F(n, 2, t)$ the minimal number of runs N in any $OA(N, n, 2, t)$ for given values n and t. Theorem 1 says that $F(11, 2, 4) \geqslant 128$, and in fact, equality holds. Let $\omega_{n,t}$ denote the minimum weight of t-CI Boolean functions in n variables. Equivalently, $\omega_{n,t}$ is the minimum number of runs in a *simple* orthogonal array with number of factors n and strength t. Hence,

$$F(n, 2, t) \leqslant \omega_{n,t}. \tag{1}$$

Suppose A is an $OA(N, n, s, t)$. As in [3, p. 5], one can construct an $OA(N/s, n-1, s, t-1)$, say A'. Clearly, if A is simple then A' is simple too. This implies

$$\begin{aligned} F(n-1, 2, t-1) &\leqslant \frac{1}{2} F(n, 2, t), \\ \omega_{n-1,t-1} &\leqslant \frac{1}{2} \omega_{n,t}. \end{aligned} \tag{2}$$

We are now able to fill some unknown values of [4, Table 2] and [5, Table 2].

Proposition 1. For the minimum weight of t-CI Boolean functions in n variables, we have

$$\omega_{11,4} = \omega_{12,4} = \omega_{13,4} = \omega_{14,4} = \omega_{15,4} = 128; \tag{3}$$

$$\omega_{11,5} = \omega_{12,5} = \omega_{13,5} = \omega_{14,5} = \omega_{15,5} = \omega_{16,5} = 256. \tag{4}$$

Proof. The Nordstrom — Robinson code and also Sloane gives a simple $OA(256, 16, 2, 5)$, see [1, 13, 14]. Straightforward computation shows that deleting the last 5 columns of it, the resulting orthogonal array is simple. Hence, $\omega_{n,5} \leqslant 256$ for $n \in \{11, \ldots, 16\}$. By (2), $\omega_{n,4} \leqslant 128$ for $n \in \{10, \ldots, 15\}$. Theorem 1 implies $F(n, 2, 4) \geqslant 128$ for $n \geqslant 11$. From (1) and (2) follow (3) and (4). ■

REFERENCES

1. *Gorodilova A., Agievich S., Carlet C., et al.* The Fifth International Students' Olympiad in cryptography — NSUCRYPTO: Problems and their solutions. Cryptologia, 2020, vol. 44, no. 3, pp. 223–256.
2. `www.nsucrypto.nsu.ru/unsolved-problems/` — NSUCRYPTO Unsolved problems, 2020.
3. *Hedayat A. S., Sloane N. J. A., and Stufken J.* Orthogonal Arrays: Theory and Applications. N.Y., Springer Verlag, 1999.
4. *Carlet C. and Chen X.* Constructing low-weight dth-order correlation-immune Boolean functions through the Fourier — Hadamard transform. IEEE Trans. Inform. Theory, 2018, vol. 64, no. 4, pp. 2969–2978.
5. *Carlet C. and Guilley S.* Correlation-immune Boolean functions for easing counter measures to side-channel attacks (Ch. 3). H. Niederreiter, A. Ostafe, D. Panario, A. Winterhof (eds.). Algebraic Curves and Finite Fields Cryptography and Other Applications, Radon Series on Computational and Applied Mathematics, vol. 16, Berlin, De Gruyter, 2014, pp. 41–70.
6. *Bulutoglu D. A. and Margot F.* Classification of orthogonal arrays by integer programming. J. Statistical Planning Inference, 2008, vol. 138, no. 3, pp. 654–666.

7. *Schoen E. D., Eendebak P. T., and Nguyen M. V. M.* Complete enumeration of pure-level and mixed-level orthogonal arrays. J. Combinat. Designs, 2009, vol. 18, no. 2, pp. 123–140.
8. *Schoen E. D., Eendebak P. T., and Nguyen M. V. M.* Correction to: Complete enumeration of pure-level and mixed-level orthogonal arrays. J. Combinat. Designs, 2010, vol. 18, no. 6, pp. 488–488.
9. *Eendebak P.* Complete series of non-isomorphic orthogonal arrays. `www.pietereendebak.nl/oapackage/series.html`. 2020.
10. `www.sagemath.org` — The Sage Developers. SageMath, the Sage Mathematics Software System (Version 9.1), 2020.
11. *Makhorin A.* Gnu linear programming kit. `www.gnu.org/software/glpk/`. 2020.
12. *Gamrath G., Anderson D., Bestuzheva K., et al.* The SCIP Optimization Suite 7.0. `www.optimization-online.org/DB_HTML/2020/03/7705.html`. 2020.
13. *Bierbrauer J.* Nordstrom — Robinson code and A_7-geometry. Finite Fields and Their Appl., 2007, vol. 13, no. 1, pp. 158–170.
14. *Sloane N. J. A.* A Library of Orthogonal Arrays. `www.neilsloane.com/oadir/`. 2020.

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.056.57

ОБНАРУЖЕНИЕ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ НА ОСНОВЕ АДАПТИВНО-РЕЗОНАНСНОЙ ТЕОРИИ[1]

Д. Г. Буханов, В. М. Поляков, М. А. Редькина

Белгородский государственный технологический университет им. В. Г. Шухова, г. Белгород, Россия

Рассматривается процесс выявления вредоносного программного кода антивирусными системами. Для анализа исполняемого кода используется граф потока управления. Предлагается в качестве классификатора применять искусственные нейронные сети на основе адаптивно-резонансной теории с иерархической структурой памяти. Для удобного представления графа потока управления при классификации используется алгоритм `graph2vec`. Проведены эксперименты на модельных примерах, которые показали хорошие результаты точности и скорости определения типа вредоносного программного обеспечения.

Ключевые слова: *вредоносное программное обеспечение, анализ исполняемых файлов, граф потока управления, векторизация, деобфускация, искусственная нейронная сеть на базе адаптивной резонансной теории, кластеризация.*

DOI 10.17223/20710410/52/4

DETECTION OF MALWARE USING AN ARTIFICIAL NEURAL NETWORK BASED ON ADAPTIVE RESONANT THEORY

D. G. Bukhanov, V. M. Polyakov, M. A. Redkina

Belgorod State Technological University named after V. G. Shukhov, Belgorod, Russia

E-mail: db.old.stray@gmail.com, p_v_m@mail.ru, redckina.rit@mail.ru

The process of detecting malicious code by anti-virus systems is considered. The main part of this process is the procedure for analyzing a file or process. Artificial neural networks based on the adaptive-resonance theory are proposed to use as a method of analysis. The `graph2vec` vectorization algorithm is used to represent the analyzed program codes in numerical format. Despite the fact that the use of this vectorization method ignores the semantic relationships between the sequence of executable commands, it allows to reduce the analysis time without significant loss of accuracy. The use of an artificial neural network ART-2m with a hierarchical memory structure made it possible to reduce the classification time for a malicious file. Reducing the

[1]Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ), проект № 13, и гранта РФФИ № 19-29-09056мк.

classification time allows to set more memory levels and increase the similarity parameter, which leads to an improved classification quality. Experiments show that with this approach to detecting malicious software, similar files can be recognized by both size and behavior.

Keywords: *malware, analysis of portable executable files, control flow graph, vectorization, deobfuscation, artificial neural networks based on adaptive resonance theory, clustering.*

Введение

Вредоносное программное обеспечение (ВПО), проникающее в систему пользователя, может задействовать ресурсы атакуемой ЭВМ в своих целях или привести к потере данных и, следовательно, убыткам пользователей и компаний. В [1] представлены результаты исследований убытков от ВПО. От вируса-вымогателя WannaCry компании понесли потери в 1 млрд долл., а среднегодовые убытки от киберугроз обходятся банкам в 18,28 млн долл. С каждым годом стоимость последствий проведения кибератак растёт, к 2018 г. [2] средняя стоимость инцидента для крупной компании выросла на 24 % (с 992 тыс. долл. до 1,23 млн долл.), а для малого и среднего бизнеса — на 38 % (с 88 до 120 тыс. долл.) по сравнению с предыдущим годом. С ростом угроз растёт сложность определения ВПО. Все чаще при распространении ВПО злоумышленники прибегают к методам сокрытия его присутствия либо к методам социальной инженерии [3].

Основным инструментом при выявлении ВПО является специализированное программное обеспечение — антивирус. Ядром любого антивируса является модуль анализа файлов и процессов. Они базируются на сигнатурном и эвристическом методах выявления зловредного программного обеспечения.

Недостатком сигнатурного анализа [4] является невозможность выявления нового и замаскированного программного обеспечения. Разработчики ВПО прибегают к следующим способам маскировки исполняемых кодов:

1) шифрование [5];
2) самомодификация [6];
3) упаковка [7, 8];
4) обфускация кода [9, 10].

Обфускация представляет собой процесс добавления инструкций, не изменяющих функциональность программы, но изменяющих её размеры и увеличивающих сложность понимания анализируемых инструкций. Далее рассмотрен процесс деобфускации с целью упростить процесс обработки исходного кода.

В отличие от сигнатурного анализа, эвристический используется при выявлении неизвестного ранее ВПО. Основным принципом является нахождение отклонения поведения программы от нормального состояния. Перспективным подходом в построении систем определения ВПО является использование в них искусственных нейронных сетей (ИНС) [11].

ИНС принимает на вход числовые векторы данных, для получения которых исполняемый код ВПО можно представить в виде графа потока управления (ГПУ) [12]. Такая структуризация исполняемого кода позволяет сравнивать вершины друг с другом и выявлять среди них уникальные. Для сравнения графовых структур применяется алгоритм graph2vec [13], позволяющий описать граф вектором чисел.

В работе [14] анализируется накопленная во время выполнения ВПО информация, включающая сетевой трафик, инструкции центрального процессора, дампы оперативной памяти. Авторы используют ИНС Кохонена, основным недостатком которой является необходимость знать заранее число кластеров.

В [15] рассматривается последовательность вызова системных API-функций у 500 исполняемых файлов. При классификации полученных данных несколькими классификаторами лучшую точность обнаружения показал наивный байесовский классификатор. Но он не позволяет выявлять новые виды ранее неизвестного ВПО.

В настоящее время существуют различные архитектуры ИНС, общим недостатком которых является необходимость проводить переобучение, возникающее при добавлении нового образа, недостаточная пластичность и невозможность дообучения в режиме функционирования. Этот недостаток преодолён в [16] при разработке ИНС на основе адаптивной резонансной теории (АРТ).

В работе решается проблема выявления ВПО на основе ИНС адаптивно-резонансной теории с иерархической структурой памяти путём выполнения следующих шагов:

1) деобфускация кода;
2) построение ГПУ;
3) векторизация ГПУ;
4) классификация ВПО по ГПУ.

1. Деобфускация кода

Объектами анализа являются запущенный процесс, дамп его памяти, исполняемый файл или PE-файл (Portable Executable, «переносимый исполняемый»), которые дизассемблируются для изучения и дальнейшей обработки. На первом шаге производится деобфускация кода. Методы анализа при деобфускации программного кода бывают: синтаксические, статические, статистические, динамические [17]. В работе используется метод статического анализа: очистка кода происходит без его выполнения с удалением заранее определенных выражений:

1) команды `nop`, предписывающей ничего не делать;
2) парных команд `<push, pop>`, `<inc, dec>`, `<dec, inc>`, операндами которых являются регистры, не используемые в коде, заключенном между данной парой команд;
3) равнозначные инструкции `xor <operand>,<operand>`, `mov <operand>,0`, если среди инструкций, заключенных между этими двумя, `<operand>` не был упомянут;
4) бесполезные инструкции: `or <operand>,<operand>`; `mov <operand>,<operand>`;
5) команды логического сдвига (`shr`, `shl` и т. д.), `add`, `sub`, второй операнд которых равен нулю;
6) не имеющая смысла пара инструкций `xchng <operand1>,<operand2>` и `xchng <operand2>,<operand1>`, если их операнды не были упомянуты между ними, и др.

Рассмотрим пример деобфускации следующего исполняемого кода:

```
1 401000 sub esp,1C
2 401003 inc edx
3 401004 mov eax,ss:[esp+20]
4 401008 mov eax,ds:[eax]
```

```
 5  40100A mov eax,ds:[eax]
 6  40100C cmp eax,C0000091
 7  401012 ja 401060
 8  401018 cmp eax,C000008D
 9  40101E dec edx
10  40101F shr eax,0
11  401022 jae 401079
12  401028 cmp eax,C0000005
13  40102E add edx,0
14  401031 jne 4010F0
15  401037 nop
16  401038 mov ebx,ebx
17  40103A nop
```

После деобфускации в данном примере значимыми останутся только следующие строки кода:

```
 1  401000 sub esp,1C
 2  401004 mov eax,ss:[esp+20]
 3  401008 mov eax,ds:[eax]
 4  40100A mov eax,ds:[eax]
 5  40100C cmp eax,C0000091
 6  401012 ja 401060
 7  401018 cmp eax,C000008D
 8  401022 jae 401079
 9  401028 cmp eax,C0000005
10  401031 jne 4010F0
```

Были удалены следующие команды: попарные операции `401003 inc edx`, `40101E dec edx`, так как в коде, заключенном между ними, регистра `edx` или его составляющих (`dh, dl`) не найдено; `40101F shr eax,0`; `40102E add edx,0`; `401038 mov ebx,ebx`, которые не изменяют значение первого операнда, следовательно, не имеют смысла; `401037 nop`, `40103A nop` — незначащие операции.

2. Построение ГПУ

На следующем шаге выполняется построение ГПУ. Преобразованный код разбивается на базовые блоки, каждому из которых соответствует вершина ГПУ. Базовые блоки формируются при последовательном анализе кода и не содержат в себе команд управления потоком. Таким образом, вершину можно представить набором команд, из которых состоит базовый блок, соответствующий текущей вершине. Передача управления потоком и конец вершины определяются следующими типами команд:

1) безусловные: `jmp`, `call`, где `jmp` — это команда, приводящая лишь в одну вершину, а `call` работает по принципу условных команд передачи управления;
2) условные: `je`, `jz` и другие, подразумевающие переход в вершину по условию, при его невыполнении переход на следующую команду за данной;
3) команды управления циклом: `loop`, `loope`, `loopz` и другие, работающие по принципу команд условной передачи управления.

Проанализируем участок кода, полученный на предыдущем шаге. Среди набора инструкций можно выделить три вершины, заканчивающиеся условными командами передачи управления: `ja 401060`, `jae 401079`, `jne 4010F0`. ГПУ для заданного участка программы представлен на рис. 1, где показано, что вершин, содержащих адреса

`401060`, `401079`, `4010F0`, в коде не встречено, поэтому символами «???» отмечены неизвестные команды, которые скрыты за соответствующими адресами. Следовательно, переход в эти вершины, расположенные вне рассматриваемого кода, можно отметить как переход в недостижимые: -1.

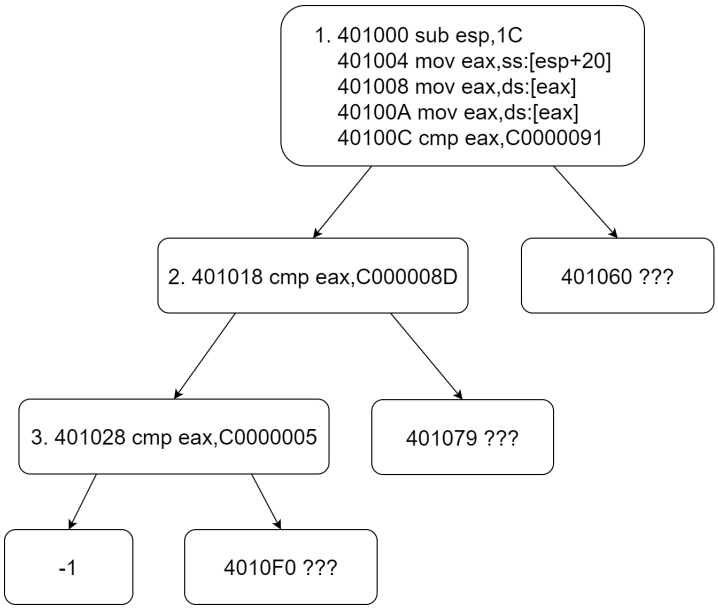


Рис. 1. ГПУ программы

3. Векторизация ГПУ

После выполнения процесса деобфускации кода и составления по нему ГПУ необходимо получить векторное представление графа. Каждую вершину можно описать вектором количеств повторений ассемблерных команд для архитектуры x86-64, из которых она состоит. После сравнения полученных векторов требуется определить уникальные вершины и получить векторное представление ГПУ.

Представим в качестве алфавита команд набор инструкций, используемый в архитектуре x86-64. Для примера алфавит состоит из команд, упомянутых в коде: `sub`, `mov`, `cmp` и др.; W_i — вектор количеств повторений команд, обозначающий i-ю вершину:

$$W_1 = (1, 3, 1), \quad W_2 = W_3 = (0, 0, 1).$$

Уникальных вершин в этом ГПУ $n = 2$. Каждой уникальной вершине присваивается бинарный вектор $VB = (vb_1, \ldots, vb_n)$, одинаковый для повторяющихся вершин; в нём $vb_i = 1$, где i — порядковый номер уникальной вершины, остальные $n - 1$ элементов заполняются нулями. Для нашего примера $VB_1 = (1, 0)$, $VB_2 = VB_3 = (0, 1)$.

Вектор, описывающий данную программу: $V = \sum_{i=1}^{3} VB_i = (1, 2)$. Векторизация ГПУ из примера представлена на рис. 2, где наглядно отображены переходы между вершинами, векторы W_i, V_i, $i = 1, 2, 3$, описывающие соответствующие вершины, а также полученный результирующий вектор V для данной программы.

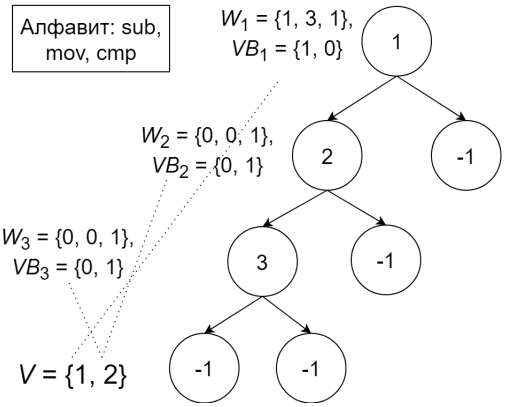


Рис. 2. Векторизация ГПУ

4. Разработка классификатора на основе адаптивно-резонансной теории с иерархической структурой памяти

ИНС на основе АРТ является самоорганизующейся сетью, позволяющей в реальном времени решать задачи кластеризации и распознавания входных образов без учителя. Принцип работы ИНС АРТ основан на нахождении соответствия между восходящим сигналом и ожидаемым нисходящим.

В ИНС АРТ-2 с непрерывными входными сигналами были выявлены недостатки, связанные с низкой скоростью её работы в процессе распознавания образов при большом объёме анализируемых данных. Для решения этой проблемы в работе [18] представлена модификация сети АРТ-2m, имеющая древовидную структуру памяти с рекуррентно изменяющимся параметром сходства для каждого уровня в дереве.

На рис. 3 представлена сеть АРТ-2m, которая состоит из полей F_1, F_2, а также поля сходства G, представленного набором параметров сходства $Riter_i$ для каждого уровня i, где $i = 1, \ldots, max\_level$; max_level — общее количество всех уровней памяти.

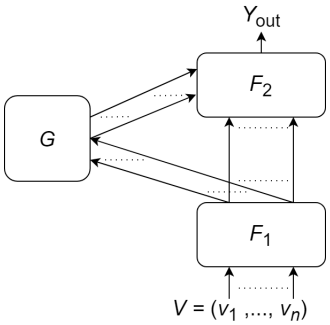


Рис. 3. Схема АРТ-2m

Использование сети с многоуровневой структурой памяти позволяет выполнять поиск активного нейрона быстрее, чем использование классической структуры сети АРТ-2 [16]. Проверка на соответствие происходит только между теми нейронами, которые связаны с нейронами нижележащих уровней. При выявлении ВПО это позволяет уменьшить время идентификации и нахождения зависимостей между уже существующими образами в памяти и поданными на вход.

5. Исследование качества определения ВПО

Проведены эксперименты по моделированию ситуации выявления сходства между ВПО, исходным файлом (ИФ) и ИФ, заражённым этим ВПО. Файлами для экспериментов послужили программа построения ГПУ в качестве ВПО, программа, реализующая принцип работы ART-2m в качестве ИФ, и программа, которая представляет «склейку» ВПО и ИФ, в качестве заражённого ИФ. Данные экспериментов отображены в табл. 1 и 2.

Таблица 1

Исходные данные эксперимента 1

Тип файла	Размер исполняемого кода, кбайт	Общее количество вершин в ГПУ	Количество уникальных вершин
ВПО	202	1596	443
ИФ	160	1256	417
Заражённый файл	363	2851	558

Выходные векторы V_j, описывающие программы, состоят из $n = 558$ элементов и имеют следующий вид:

$$V_1 = (1, 98, 115, 44, 1, \ldots, 0, 0, 0),$$
$$V_2 = (1, 98, 88, 46, 1, \ldots, 1, 1, 0),$$
$$V_3 = (1, 196, 203, 90, 2, 206, \ldots, 1, 0, 1).$$

Начальный параметр сходства $Riter_1 = 0{,}8$. Значение параметров сходства различных уровней определяется следующей рекуррентной зависимостью:

$$Riter_{i+1} = Riter_i + 0{,}7(1 - Riter_i), \quad i = 1, \ldots, max\_level.$$

При $max\_level = 8$ параметры сходства для уровней равны

$$0{,}8,\ 0{,}94,\ 0{,}982,\ 0{,}9946,\ 0{,}99838,\ 0{,}999514,\ 0{,}999854,\ 0{,}999956.$$

Значение параметра сходства $Riter_1 = 0{,}8$ было выбрано эмпирически на основе данных [16]. При значении параметра сходства $\geqslant 0{,}8$ получение новых классов образов происходит с большей вероятностью.

Память представляет набор матриц весовых коэффициентов (z) для каждого уровня иерархии [18]; z-веса для каждого образа вычисляются следующим образом:

1) обучение весов нового нейрона с номером m:

$$z^k_{m\,i} := d \cdot u_i, \quad i = 1, \ldots, n, \quad k = 1, \ldots, max\_level,$$

где u_i — элементы слоя U, входящего в состав поля F_1; k — уровень иерархии;

2) дообучение весов нейрона-победителя с номером $i_{\max}$:

$$z_{i_{\max} i} := z_{i_{\max} i} + d(1 - d)\left(\frac{u_i}{1 - d} - z_{i_{\max} i}\right), \quad i = 1, \ldots, n.$$

В ходе эксперимента для программ получены следующие веса:

1) z-веса ВПО:
   1.1. $z^k_{m\,i}$ = 0,00364339, 0,357052, 0,41899, ..., 0, 0; $k = 1, \ldots, max\_level$, $m = 1$, $i = 1, \ldots, n$;
2) z-веса ИФ:
   2.1. z^k_{mi} = 0,0788018, 0,772257, 0,782974, ..., 0,00456469, 0; $k = 1, \ldots, 4$, $m = 1$, $i = 1, \ldots, n$;
   2.2. z^k_{mi} = 0,00456469, 0,44734, 0,401693, ..., 0,00456469, 0; $k = 5, \ldots$, max_level, $m = 2$, $i = 1, \ldots, n$;
3) z-веса заражённого файла:
   3.1. z^k_{mi} = 0,00925834, 1,11188, 1,13624, ..., 0,004153, 0,00208738; $k = = 1, \ldots, 4$, $m = 1$, $i = 1, \ldots, n$;
   3.2. z^k_{mi} = 0,00540287, 0,734044, 0,805019, ..., 0, 0,00208738; $k = 5$, $m = 1$, $i = 1, \ldots, n$;
   3.3. z^k_{mi} = 0,00208738, 0,409127, 0,423739, ..., 0, 0,00208738; $k = 6, \ldots$, max_level, $m = 3$, $i = 1, \ldots, n$.

На рис. 4 представлена память АРТ-2m сети в виде древовидной структуры. Внутри узлов записаны координаты вершин в декартовой системе. Это позволяет проследить зависимость между объектами исследования: после «заражения» ИФ стал похож на ВПО.

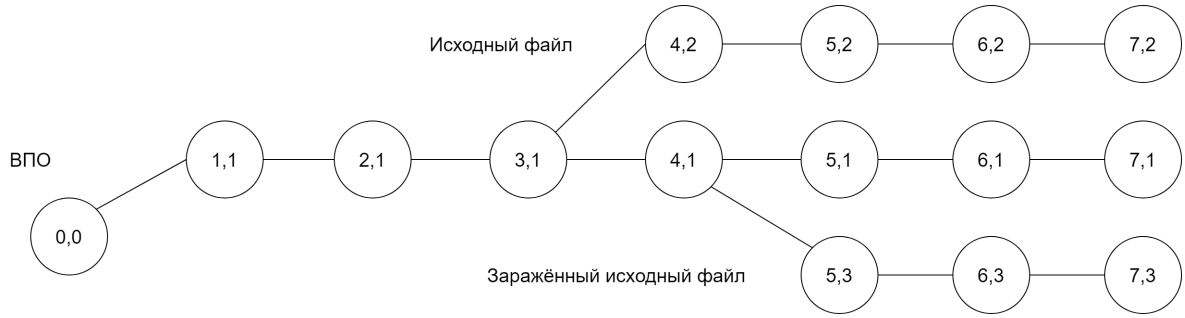


Рис. 4. Структура памяти АРТ-2m (эксперимент 1)

Как видно из рис. 4, заражённый ИФ похож на ВПО с параметром схожести $Riter_5 = 0{,}99838$, а ВПО — на ИФ с $Riter_4 = 0{,}9946$.

В табл. 2 представлены данные для экспериментов, результаты которых изображены на рис. 5–8. Обнаружено, что заражённый файл больше похож на файл, размер которого больше. Полученные графы показывают, что ИФ перестаёт быть похожим на себя. Были использованы четыре типа файлов эквивалентных размеров.

Из рис. 5 видно, что ИФ2 похож на ВПО с параметром схожести $Riter_5 = 0{,}99838$, а Заражённый файл2 — на ИФ2 с $Riter_6 = 0{,}999514$.

Таблица 2

Исходные данные экспериментов 2–5

Эксперимент № п/п	Тип файла	Размер исполняемого кода, кбайт	Общее количество вершин в ГПУ	Количество уникальных вершин	На что больше похож заражённый файл
2	ВПО	202	1596	443	
	ИФ2	204	1693	417	+
	Заражённый файл2	406	3288	506	
3	ВПО	202	1596	443	
	ИФ3	228	1700	427	+
	Заражённый файл3	431	3295	560	
4	ВПО2	204	1693	417	+
	ИФ	160	1256	417	
	Заражённый файл4	365	2948	540	
5	ВПО2	204	1693	417	
	ИФ3	228	1700	427	+
	Заражённый файл5	432	3392	548	

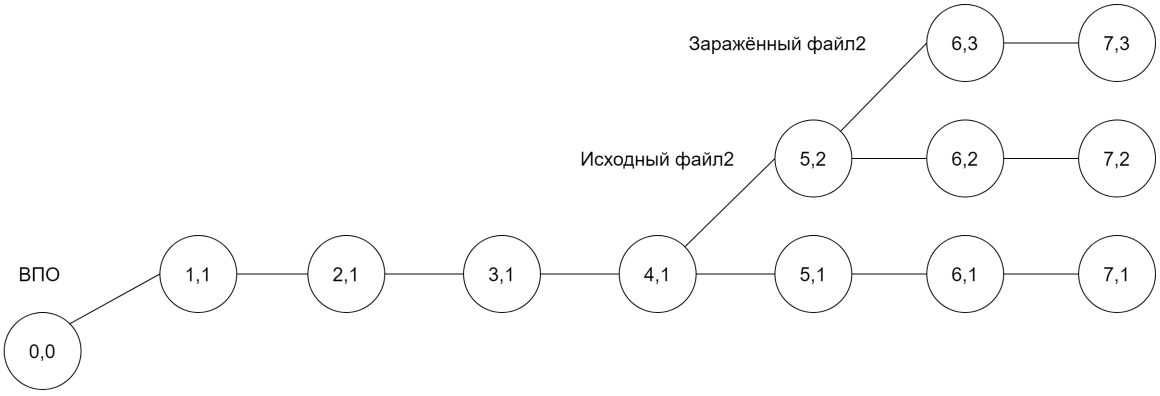


Рис. 5. Результаты эксперимента 2

На рис. 6 показано, что ИФ3 похож на ВПО с параметром схожести $Riter_4 = 0{,}9946$, а Заражённый файл3 — на ИФ3 с $Riter_6 = 0{,}999514$.

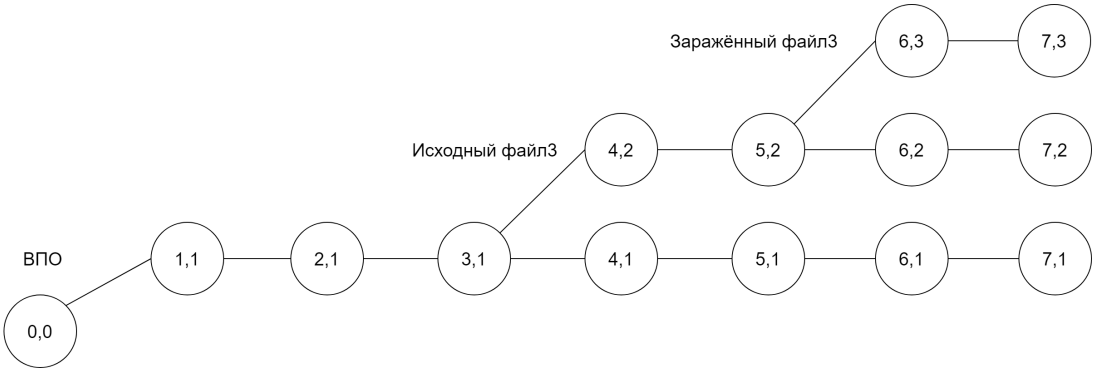


Рис. 6. Результаты эксперимента 3

Из рис. 7 видно, что Заражённый файл4 похож на ВПО2 с параметром схожести $Riter_5 = 0{,}99838$, а ИФ — на ВПО2 с $Riter_4 = 0{,}9946$.

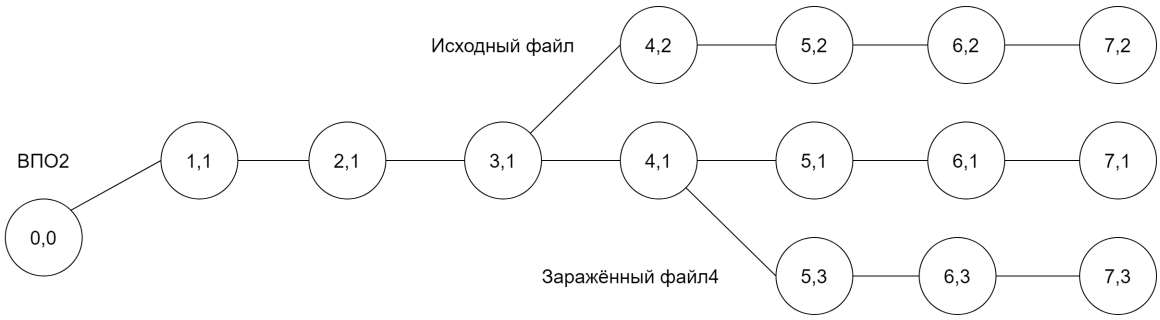


Рис. 7. Результаты эксперимента 4

На рис. 8 показано, что ИФ3 похож на ВПО2 с параметром схожести $Riter_4 = 0{,}9946$, а Зараженный файл5 — на ИФ3 с $Riter_5 = 0{,}99838$.

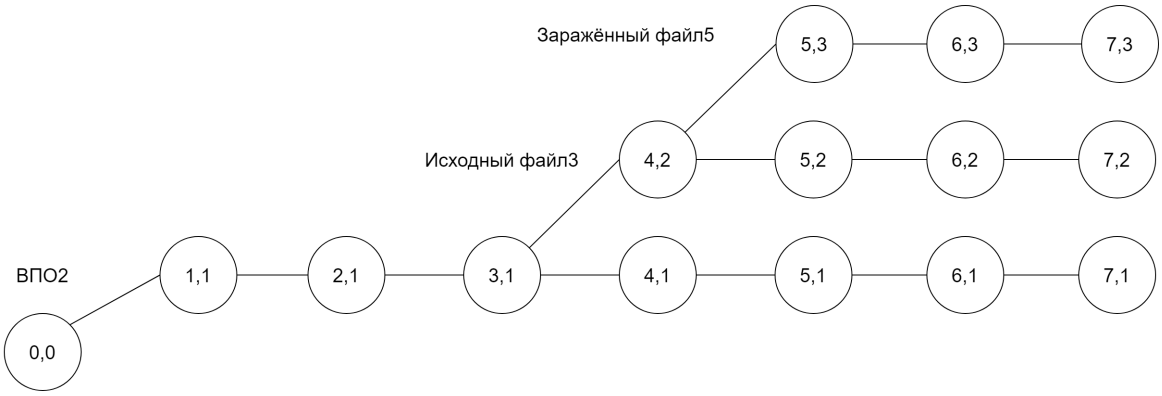


Рис. 8. Результаты эксперимента 5

Результаты экспериментов показывают, что когда размер ИФ превышает размер вредоносного, заражённый файл больше похож на исходный. В этом случае для повышения точности требуется ввести дополнительный уровень памяти. Чем больше уровней, тем выше параметр сходства *Riter* и точность классификации.

Для оценки качества классификации (без учёта фактора размера файла и доли входных данных в конечном файле) проведены дополнительные эксперименты.

6. Исследование качества классификации APT-2m при анализе файлов схожих размеров

В табл. 3 представлены параметры исходных данных эксперимента — приложений и их модификаций (по четыре модификации для каждого приложения).

Первая программа ex_socket_1 выполняет открытие udp socket для всех интерфейсов системы и приём данных. Модификация ex_socket_2, помимо этого, выполняет запись принятых данных в файл, ex_socket_3 — вывод полученных данных на консоль, ex_socket_4 позволяет выбрать файл для записи и записать принятые данные. Вторая программа ex_qe_1 получает от пользователя коэффициенты квадратного уравнения и находит его корни. В качестве модификаций ex_qe_2, ex_qe_3 использованы программы, которые отличаются выводом результата (консоль, файл), а ex_qe_4 содержит ввод значений не через консоль, а через файл.

Таблица 3

Исходные данные эксперимента

Файл	Размер исполняемого кода, кбайт	Общее количество вершин в ГПУ	Количество уникальных вершин
ex_socket_1	86,7	499	192
ex_socket_2	89,7	481	199
ex_socket_3	91,2	489	202
ex_socket_4	89,8	480	205
ex_qe_1	139,2	601	269
ex_qe_2	135,5	616	274
ex_qe_3	135,5	627	278
ex_qe_4	135,9	613	281

Из рис. 9, где представлено дерево памяти классификатора АРТ-2m ГПУ файлов, описанных в табл. 3, видно, что модификации разных программ привели к созданию различных поддеревьев на начальных уровнях. Программы ex_socket_2 и ex_socket_3 схожи по поведению, обе используют потоки для передачи данных, только одна из них использует файловый поток, другая — поток вывода. Результаты проведенного эксперимента показывают, что при схожих размерах файла на качество классификации влияет его содержание. Размеры файлов ex_qe_2 и ex_qe_3 совпадают, но общее количество вершин ГПУ и уникальных вершин различно. Следовательно, размер файла имеет косвенное значение для определения схожести файлов, а основным параметром являются вершины ГПУ.

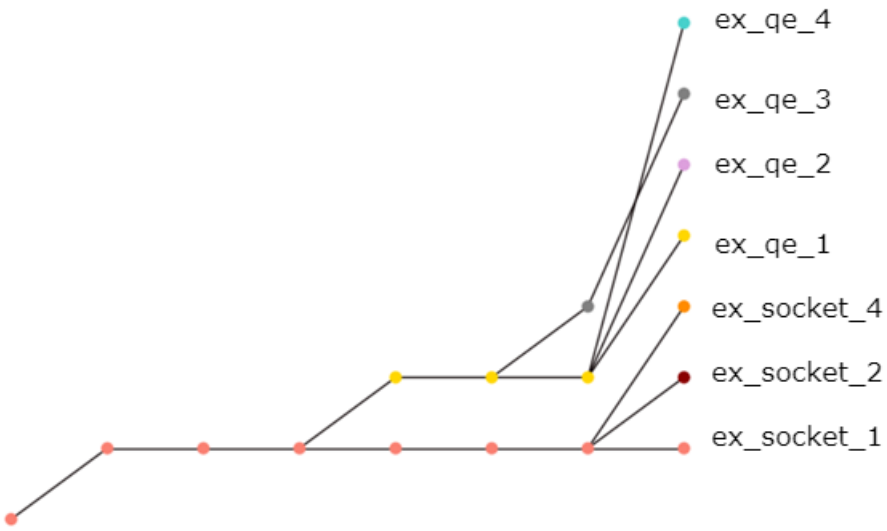


Рис. 9. Дерево памяти классификатора АРТ2-m

7. Исследование временных характеристик при определении ВПО

Анализ времени, затрачиваемого на векторизацию, представлен на рис. 10. Для эксперимента было взято пять файлов размеров 100 кбайт (содержит 4458 инструкций), 200 (9361), 300 (13898), 500 (23446) и 1000 кбайт (46234 инструкций).

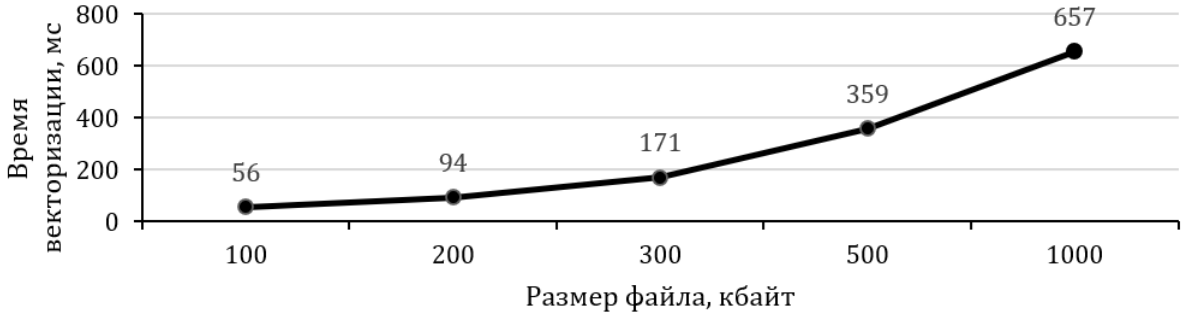


Рис. 10. Время, затрачиваемое на векторизацию файлов различных размеров

Для анализа скорости распознавания образов на вход сети были поданы $m = 100, 500, 1000, 1500, 2000, 2500$ уникальных образов, имеющих 100 входов. В ходе эксперимента использовано 10 образов, номера N_i которых вычисляются по формуле

$$N_1 = \triangle, \quad N_{i+1} = N_i + \triangle, \quad i = 1, \ldots, 9, \quad \triangle = m/10.$$

Среднее время распознавания образа представлено на рис. 11.

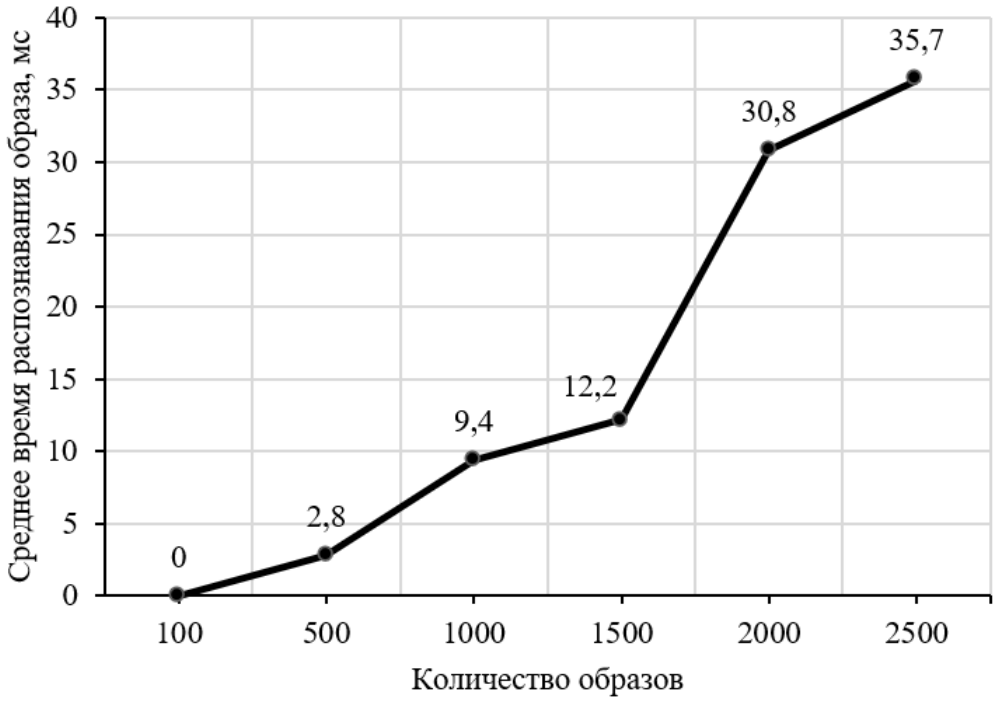


Рис. 11. Среднее время распознавания образа

Графики наглядно демонстрируют быстродействие как модуля программного обеспечения, направленного на векторизацию ГПУ исполняемого кода, так и модуля, реализующего ART-2m. Из результатов видно, что время на анализ и векторизацию исполняемого файла значительно превышает время на классификацию.

Заключение

Проведённые исследования показали, что применение ИНС АРТ-2m для обнаружения ВПО, а также выявления схожести между сохранёнными образами и новыми

даёт высокие результаты: распознавание или добавление нейрона происходит в среднем за 18 мс за счёт древовидной организации памяти. Благодаря использованию ИНС рассмотренной архитектуры можно выявлять схожесть между образами, поданными на вход сети, и затем использовать эти данные для дальнейшего анализа. Получение нового образа происходит в пределах 1 с.

Подход, используемый в векторизации программы, не учитывает семантические связи между вершинами, поэтому для повышения точности предлагается заменить модуль векторизации вершин на векторизацию рёбер ГПУ.

ЛИТЕРАТУРА

1. `https://opendatasecurity.io/how-much-does-a-cyberattack-cost-companies/` — How much does a cyberattack cost companies. 2017.
2. *Salahdine F. and Kaabouch N.* Social Engineering Attacks: A Survey // Future Internet. 2019. V. 11. `https://www.mdpi.com/1999-5903/11/4/89/htm`
3. `https://www.kaspersky.ru/blog/economics-report-2018/20655/` — Во сколько может обойтись потеря данных. 2018.
4. *Харченко С. С., Давыдова Е. М., Тимченко С. В.* Сигнатурный анализ программного кода // Ползуновский вестник. 2012. № 3. С. 60–64.
5. *Babak B. R., Maslin M., and Suhaimi I.* Camouflage in malware: from encryption to metamorphism // Intern. J. Computer Science and Network Security. 2012. V. 12. P. 74–83.
6. *Cai H., Shao Z., and Vaynberg A.* Certified Self-Modifying Code (extended version & coq implementation). Technical Report YALEU/DCS/TR-1379. 2007.
7. *Wei Y., Zheng Z., and Nirwan A.* Revealing packed malware // IEEE Security & Privacy. 2008. V. 6. No. 5. P. 65–69.
8. *Jacob G., Comparetti P. M., Neugschwandtner M., et al.* A static, packer-agnostic filter to detect similar malware samples // LNCS. 2013. V. 7591. P. 102–122.
9. *Linn C. and Debray S.* Obfuscation of executable code to improve resistance to static disassembly // Proc. CCS'03. Washington, USA, 2003. P. 290–299.
10. *Golovkin M.* Systems and methods for detecting obfuscated malware // Patent U.S. 9087195. 2015.
11. *Solomon I. A., Jatain A, and Bajaj S. B.* Neural network based intrusion detection: State of the art // Proc. Intern. Conf. SUSCOM. Amity University Rajasthan, Jaipur-India, February 26–28, 2019.
12. *Bonfante G., Kaczmarek M., and Marion J.* On abstract computer virology from a recursion theoretic perspective // J. Computer Virology. 2009. V. 5. No. 3. P. 263–270.
13. *Narayanan A., Chandramohan M., Chen L., et al.* Subgraph2vec: Learning Distributed Representations of Rooted Sub-graphs from Large Graphs. arXiv: 1606.08928. 2016.
14. *Burnap P., French R., Turner F., and Jones K.* Malware classification using self organising feature maps and machine activity data // Computers & Security. 2018. V. 73. P. 399–410.
15. *Ahmed F., Hameed H., Shafiq M. Z., and Farooq M.* Using spatio-temporal information in API calls with machine learning algorithms for malware detection // Proc. AISec'09. Chicago, Illinois, USA, 2009. P. 55–62.
16. *Carpenter G. A. and Grossberg S.* ART 2: self-organization of stable category recognition codes for analog input patterns // Appl. Opt. 1987. V. 26. No. 23. P. 4919–4930.
17. *Курмангалеев Ш. Ф., Долгорукова К. Ю., Савченко В. В. и др.* О методах деобфускации программ // Труды Института системного программирования РАН. 2013. Т. 24. С. 145–160.

18. *Буханов Д. Г., Поляков В. М.* Сеть адаптивно-резонансной теории с многоуровневой памятью // Научные ведомости БелГУ. 2018. Т. 45. № 4. С. 709–717.

REFERENCES

1. `https://opendatasecurity.io/how-much-does-a-cyberattack-cost-companies/` — How much does a cyberattack cost companies. 2017.
2. *Salahdine F. and Kaabouch N.* Social Engineering Attacks: A Survey. Future Internet, 2019, vol. 11. `https://www.mdpi.com/1999-5903/11/4/89/htm`
3. `https://www.kaspersky.ru/blog/economics-report-2018/20655/.` 2018.
4. *Harchenko S. S., Davydova E. M., and Timchenko S. V.* Signaturnyy analiz programmnogo koda [Signature analysis of program code]. Polzunovskiy Vestnik, 2012, vol. 3, pp. 60–64. (in Russian)
5. *Babak B. R., Maslin M., and Suhaimi I.* Camouflage in malware: from encryption to metamorphism. Intern. J. Computer Science and Network Security, 2012, vol. 12, pp. 74–83.
6. *Cai H., Shao Z., and Vaynberg A.* Certified Self-Modifying Code (extended version & coq implementation). Technical Report YALEU/DCS/TR-1379. 2007.
7. *Wei Y., Zheng Z., and Nirwan A.* Revealing Packed Malware // IEEE Security & Privacy, 2008, vol. 6, no. 5, pp. 65–69.
8. *Jacob G., Comparetti P. M., Neugschwandtner M., et al.* A static, packer-agnostic filter to detect similar malware samples. LNCS, 2013, vol. 7591, pp. 102–122.
9. *Linn C. and Debray S.* Obfuscation of executable code to improve resistance to static disassembly. Proc. CCS'03, Washington, USA, 2003, pp. 290–299.
10. *Golovkin M.* Systems and methods for detecting obfuscated malware. Patent U.S. 9087195. 2015.
11. *Solomon I. A., Jatain A, and Bajaj S. B.* Neural network based intrusion detection: State of the art. Proc. Intern. Conf. SUSCOM, Amity University Rajasthan, Jaipur-India, February 26–28, 2019.
12. *Bonfante G., Kaczmarek M., and Marion J.* On abstract computer virology from a recursion theoretic perspective. J. Computer Virology, 2009, vol. 5, no. 3, pp. 263–270.
13. *Narayanan A., Chandramohan M., Chen L., et al.* Subgraph2vec: Learning Distributed Representations of Rooted Sub-graphs from Large Graphs. arXiv: 1606.08928. 2016.
14. *Burnap P., French R., Turner F., and Jones K.* Malware classification using self organising feature maps and machine activity data. Computers & Security, 2018, vol. 73, pp. 399–410.
15. *Ahmed F., Hameed H., Shafiq M. Z., and Farooq M.* Using spatio-temporal information in API calls with machine learning algorithms for malware detection. Proc. AISec'09, Chicago, Illinois, USA, 2009, pp. 55–62.
16. *Carpenter G. A. and Grossberg S.* ART 2: self-organization of stable category recognition codes for analog input patterns. Appl. Opt., 1987, vol. 26, no. 23, pp. 4919–4930.
17. *Kurmangaleev SH. F., Dolgorukova K. YU., Savchenko V. V., et al.* O metodah deobfuskacii programm [About methods of programs deobfuscation]. Proc. Ivannikov Institute for System Programming of the RAS, 2013, vol. 24, pp. 145–160. (in Russian)
18. *Bukhanov D. G. and Polyakov V. M.* Set' adaptivno-rezonansnoy teorii s mnogourovnevoy pamyat'yu [Adaptive resonance theory network with multilevel memory]. Nauchnye Vedomosti BelSU, 2018, vol. 45, no. 4, pp. 709–717. (in Russian)

УДК 004.056.5, 004.94

ПРИЁМЫ ОПИСАНИЯ МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ ОССН ASTRA LINUX SPECIAL EDITION НА ФОРМАЛИЗОВАННОМ ЯЗЫКЕ МЕТОДА Event-B ДЛЯ ОБЕСПЕЧЕНИЯ ЕЁ ВЕРИФИКАЦИИ ИНСТРУМЕНТАМИ Rodin И ProB

П. Н. Девянин, М. А. Леонова

ООО «РусБИТех-Астра», г. Москва, Россия

Рассматриваются приёмы по доработке описания модели управления доступом отечественной защищённой операционной системы специального назначения Astra Linux Special Edition (МРОСЛ ДП-модели) в формализованной нотации (на формализованном языке метода Event-B), основанные на использовании нескольких глобальных типов, разделении общих тотальных функций на частные тотальные функции и сокращении числа инвариантов и охранных условий событий, предполагающих перебор подмножеств некоторого множества. Результатом их применения стало упрощение автоматизированной дедуктивной верификации модели с применением инструмента Rodin и её адаптация к верификации с использованием инструмента проверки моделей ProB. Данные приёмы могут быть полезны при разработке других моделей управления доступом и их верификации с применением соответствующих инструментов.

Ключевые слова: *модель управления доступом, дедуктивная верификация, Event-B, Rodin, метод проверки моделей, ProB.*

DOI 10.17223/20710410/52/5

THE TECHNIQUES OF FORMALIZATION OF OS ASTRA LINUX SPECIAL EDITION ACCESS CONTROL MODEL USING Event-B FORMAL METHOD FOR VERIFICATION USING Rodin AND ProB

P. N. Devyanin, M. A. Leonova

RusBITech-Astra, Moscow, Russia

E-mail: pdevyanin@astralinux.ru, mleonova@astralinux.ru

The paper presents techniques to specification access control model of OS Astra Linux Special Edition (the MROSL DP-model) in the formalized notation (formalized using the Event-B formal method), that are based on the use of several global types, separation of general total functions into specific total functions, reduction in the number of invariants and guard of events, which iterate over subsets of a certain set. The result of using these techniques was the simplification of automated deductive verification of formalized notation using the Rodin tool and adaptation of the model to verification by model checking formalized notation using the ProB tool. These techniques can be useful in development of the MROSL DP-model, and also in development of other access control models and verification using appropriate tools.

Keywords: *access control model, deductive verification, Event-B, Rodin, model checking, ProB.*

1. Анализ приёмов, использующихся для иерархического представления МРОСЛ ДП-модели и её верификации

Верификация модели управления доступом отечественной защищённой операционной системы специального назначения (ОССН) Astra Linux Special Edition [1, 2] необходима как для применения в основе разработки ОССН научно обоснованных технологий, так и для обеспечения выполнения при сертификации ОССН требований высшего первого уровня доверия согласно утверждённым Приказом ФСТЭК России № 76 от 02.06.2020 «Требованиям по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» [3].

Превысивший пятьсот страниц объём описания модели, называемой мандатной сущностно-ролевой ДП-моделью безопасности управления доступом и информационными потоками в ОС семейства Linux (сокращённо МРОСЛ ДП-моделью) [4, 5], на языке, принятом в математике (в математической нотации), потребовал поиска путей повышения эффективности разработки, проверки корректности и отсутствия ошибок в самой модели. Найденным здесь решением стал перевод описания модели на формализованный язык метода Event-B (в формализованную нотацию) [6] и её автоматизированная дедуктивная верификация с применением инструмента Rodin [7]. При этом элементам, задающим в рамках МРОСЛ ДП-модели состояния системы, в формализованной нотации ставятся в соответствие переменные Event-B, правилам перехода из состояний в состояния — события Event-B, а инварианты на переменные описывают свойства внутренней согласованности элементов МРОСЛ ДП-модели [8]. В результате при помощи инструмента Rodin доказывается, что любой переход из состояния в состояние, заданный событиями Event-B, сохраняет все инварианты состояния, что позволяет убедиться в корректности описания модели и доказать выполнение в её рамках условий безопасности системы.

В то же время, несмотря на достигнутые с момента начала в 2012 г. разработки МРОСЛ ДП-модели результаты по её формированию и внедрению в ОССН, она продолжает развиваться и дорабатываться для, с одной стороны, учёта в модели изменений, вносимых в механизмы защиты ОССН, а с другой — для создания на перспективу условий для включения в ОССН новых механизмов защиты или расширения охватываемых ими компонент ОССН. Например, в модель были добавлены запрещающие роли (т. е. роли, наличие прав доступа у которых не разрешает, а, наоборот, запрещает предоставление субъект-сессиям соответствующих доступов) [9]. Также в неё были включены элементы, позволяющие моделировать управление доступом штатной СУБД PostgreSQL [10].

Таким образом, сложность и постоянное развитие модели обусловило постановку задачи по исследованию и поиску приёмов, направленных, во-первых, на согласованное описания МРОСЛ ДП-модели в математической и формализованной нотациях с целью учёта постоянно вносимых в модель изменений; во-вторых, на сокращение затрачиваемых на её верификацию ресурсов, а именно: упрощение дедуктивной верификации модели с применением поддерживающего язык метода Event-B инструмента Rodin и автоматизированное выявление при этом возможных ошибок или их дублирования; в-третьих, на обеспечение более точного соответствия модели её реализации непосредственно в программном коде ОССН.

Основой для поиска путей согласованного описания МРОСЛ ДП-модели в математической и формализованной нотациях, а также «приближения» этого описания к реализации модели в программном коде ОССН стал переход из её монолитного в иерар-

хическое представление [4, 11]. Для ОССН в иерархическом представлении МРОСЛ ДП-модели имеются четыре уровня (для СУБД PostgreSQL сформированы отдельные аналогичные четыре уровня):

— первый (базовый) — модель системы ролевого (дискреционного) управления доступом;
— второй — модель системы ролевого управления доступом и мандатного контроля целостности;
— третий — модель системы ролевого управления доступом, мандатного контроля целостности и мандатного управления доступом только с информационными потоками по памяти;
— четвёртый — модель системы ролевого управления доступом, мандатного контроля целостности и мандатного управления доступом с информационными потоками по памяти и по времени.

Аналогично при описании модели на формализованном языке метода Event-B используется техника пошагового уточнения (*refinement*) [12], когда вместо создания монолитной спецификации уточнение позволяет разрабатывать серию связанных между собой спецификаций, где каждая последующая спецификация в серии является уточнением предыдущих. Таким образом, в формализованной нотации модель также представляется четырьмя соответствующими описанию в математической нотации уровнями уточнений [8]. При этом сам переход на применение пошагового уточнения стал существенным шагом в развитии технологий и практических приёмов разработки МРОСЛ ДП-модели и её дедуктивной верификации.

Однако накопление опыта описания МРОСЛ ДП-модели в математической и формализованной нотациях, её дедуктивной верификации показало наличие существенных недостатков у использовавшихся для этого подходов [13]. Во-первых, это независимое друг от друга описание элементов модели для различных видов управления доступом, во-вторых, многократное дублирование одинаковых условий их выполнения, не соответствующее реализации проверок этих условий непосредственно в программном коде ОССН, в-третьих, сложность добавления уровней уточнений, моделирующих взаимодействующие с ОССН системы (например, СУБД PostgreSQL).

Для устранения этих недостатков, которые наиболее существенны для формализованной нотации, в [13] предложено логически объединить проверки условий, заданных для мандатных управления доступом, контроля целостности и ролевого управления доступом, улучшить структуру применённых при этом элементов нотации. Кроме того, для повышения качества описания и верификации МРОСЛ ДП-модели в формализованной нотации, расширения спектра применяемых для этого методов и инструментов, моделирования и в перспективе автоматизированного тестирования на соответствие этой модели её реализации непосредственно в программном коде и настройках конфигурации механизма управления доступом ОССН в настоящее время осуществляется верификация модели с использованием инструмента проверки моделей ProB [14].

Как показал опыт, используемые ProB (как и другими инструментами проверки моделей) алгоритмы перебора значений элементов верифицируемой модели и, как следствие, наличие проблемы комбинаторного взрыва в большинстве случаев также требуют доработки описания модели в формализованной нотации. То есть некоторые способы представления МРОСЛ ДП-модели на формализованной языке метода Event-B, успешно использовавшиеся при её дедуктивной верификации инструментом Rodin, оказались непригодными для применения инструмента ProB, так как приводи-

ли к завершению его работы с ошибкой вида `timeout`, вызванной превышением установленного для выполнения переборных алгоритмов интервала времени. При этом в ходе экспериментов по многократному увеличению значения данного интервала времени результат оставался одним и тем же, из чего был сделан вывод, что проблема не в задаваемом интервале, а в том, что инструмент ProB сталкивается по сути с неразрешимой для него задачей.

К приводящим к ошибкам вида `timeout` способам можно отнести использование для большинства элементов модели (субъект-сессий, сущностей, ролей и др.) единого глобального типа. К таким типам в формализованном языке метода Event-B относятся задаваемые в контексте (*context*) несущие множества (*carrier sets*) [6]. При описании элементов модели в контексте или машине (*machine*) с использованием конкретного глобального типа задаются его подмножества, например для областей значений и определения функций. При этом инструментами Rodin и, что особенно важно, ProB каждый элемент модели представляется на основе именно его глобального типа, а не используемых при описании этого элемента подмножеств глобального типа, которые для упрощения дедуктивной верификации авторами было предложено использовать в качестве подтипов [13] (подтипами будем называть подмножества глобального типа, для каждой пары которых они либо не пересекаются, либо один подтип включает другой подтип пары; подтипы позволяют выполнять над ними операции объединения, пересечения, разности, дополнения). Поэтому инструментом ProB перебор значений элементов модели предположительно выполняется на множестве всех возможных значений глобального типа этого элемента. Таким образом, при проверке инструментом ProB выполнения инвариантов (*invariants*) или охранных условий (*guards* или *grd*) событий (*events*) модели на таких множествах значений глобальных типов выполняется перебор элементов областей определения или значения функций, а если при этом использованы подмножества соответствующих областей, то и их перебор.

В результате для устранения ошибки вида `timeout` и верификации МРОСЛ ДП-модели инструментом проверки моделей ProB представление модели на формализованном языке метода Event-B было доработано авторами. Для этого разработаны и апробированы два приёма, основанные на использовании, во-первых, нескольких глобальных типов и частных тотальных функций, во-вторых, на сокращении числа инвариантов и охранных условий, предполагающих перебор подмножеств некоторого множества. Рассмотрим и проанализируем эти приёмы подробнее.

2. Использование нескольких глобальных типов и частных тотальных функций

В МРОСЛ ДП-модели для первого уровня (ролевого управления доступом) [4] в формализованной нотации, описанной в [13], задано четыре глобальных типа:

- $Names$ — множество допустимых имён сущностей, ролей, запрещающих и административных ролей;
- $Accesses$ — множество видов доступа;
- $AccessRights$ — множество видов прав доступа;
- $Union$ — множество, включающее все остальные элементы модели (субъект-сессии, сущности, роли и т. д.).

Для уменьшения мощности множества, на котором ведётся перебор значений элементов, авторами предлагается приём по разделению там, где это возможно, общего глобального типа на несколько глобальных типов. Поскольку над глобальными типами правилами языка метода Event-B не допускаются операции объединения, пересечения,

разности, дополнения (какие-либо дополнительные ограничения на эти множества могут быть заданы аксиомами — *axioms* или *axm*), то в первую очередь требуется проанализировать на предмет возможности внесения изменений, необходимых при разделении общего глобального типа, все компоненты контекстов и машин модели. К их числу относятся: несущие множества, константы (*constants*), аксиомы, переменные (*variables* или *var*), инварианты, события, включая их параметры (*parameters*), охранные условия и действия (*action* или *act*).

В результате анализа принято решение о разделении общего глобального типа *Union*, в который входили подтипы сущностей, ролей, субъект-сессий, учётных записей пользователей, на несколько глобальных типов:

— *EntitiesU* — для сущностей;
— *RolesU* — для ролей, запрещающих и административных ролей;
— *SubjectsU* — для субъект-сессий;
— *UsersU* — для учётных записей пользователей.

При этом задание нескольких глобальных типов не исключает использования их подтипов (см. листинг 1). Это связано с тем, что при применении подтипов есть ряд описанных в [13] преимуществ, в том числе: более ясное моделирование соответствующих элементов модели в формализованной нотации, расширение возможности Rodin по проверке корректности их использования, лучшая структурированность и приспособленность модели к добавлению новых уровней уточнений или модификации существующих.

```
sets
UsersU, SubjectsU, EntitiesU, RolesU, Names, Accesses,
    AccessRights
axioms
UsersUIsFinite: finite(UsersU)
SubjectsUIsFinite: finite(SubjectsU)
EntitiesUIsFinite: finite(EntitiesU)
RolesUIsFinite: finite(RolesU)
NamesIsFinite: finite(Names)
EntitiesUPartition: partition(EntitiesU, ObjectsU,
    ContainersU)
RolesUPartition: partition(RolesU, AdmRolesU, OrdRolesU,
    NRolesU)
```

Листинг 1. Задание глобальных типов с использованием подтипов

Кроме того, в формализованной нотации, представленной в [8], некоторые функции реализовывались несколькими охранными условиями (*grd*) в большинстве событий, включая события получения доступов к сущностям или ролям, изменения прав доступа ролей и ряде других. Такое представление функций обладает рядом недостатков, проанализированных в [13], в том числе: «громоздкость» и трудночитаемость охранных условий, из-за чего в них легко не заметить ошибки; повторение этих «громоздких» условий в нескольких событиях, что может дублировать уже допущенную ошибку или внести новую при редактировании условия для конкретного события; возможное несоответствие охранного условия по сути тому, как аналогичные проверки реализуются в механизме управления доступом ОССН. В связи с этим предложен подход по представлению функций математической нотации в виде тотальных функций (*total function*) в формализованной нотации, состоящих из двух видов инвариантов:

— *инвариант-типа*, задающий области определения и значения функции;
— *инвариант-истинности*, задающий условия истинности функции для элементов её области определения.

Для каждой функции инвариант-типа должен быть один, так как области определения и значения задаются однозначно, а инвариантов-истинности может быть несколько, так как для разных элементов области определения возможны различные условия истинности значения тотальной функции.

Например, в формализованной нотации модели используется $CheckRight$ — тотальная функция наличия прав доступа, параметрами которой являются субъект-сессия, сущность (роль или субъект-сессия) и право доступа, а значением — множество текущих у субъект-сессии ролей, имеющих заданное право доступа к сущности (роли или субъект-сессии).

При использовании в формализованной нотации модели общего глобального типа $Union$ инвариант-типа $CheckRightType$ тотальной функции $CheckRight$, согласно [13], имел вид, представленный в листинге 2.

```
   CheckRightType:
CheckRight ∈ (Subjects ↔ (Entities ∪ Roles ∪ Subjects ↔ AccessRights)) →
ℙ(Roles)
   CheckRightFuncE:
∀ s,e,ar,r · s ∈ Subjects ∧ e ∈ Entities ∧ ar ∈ AccessRights ∧ r ∈ Roles ⇒
(r ∈ CheckRight({s ↦ {e ↦ ar}}) ⇔ r ↦ ReadA ∈ SubjectAdmAccesses(s) ∧
e ↦ ar ∈ RoleRights(r))
   CheckRightFuncR:
∀s,e,ar,r · s ∈ Subjects ∧ e ∈ Roles ∧ ar ∈ AccessRights ∧ r ∈ Roles ⇒
(r ∈ CheckRight({s ↦ {e ↦ ar}}) ⇔ r ↦ ReadA ∈ SubjectAdmAccesses(s) ∧
r ∈ AdmRoles ∧ e ↦ ar ∈ RoleAdmRights(r))
   CheckRightFuncS1:
∀s,e,ar,r · s ∈ Subjects ∧ e ∈ Subjects ∧ ar ∈ AccessRights ∧
r ∈ OrdRoles ∪ AdmRoles ⇒
(r ∈ CheckRight({s ↦ {e ↦ ar}}) ⇔ r ↦ ReadA ∈ SubjectAdmAccesses(s) ∧
ar = Own ∧ r = SubjectOwner(e))
   CheckRightFuncS2:
∀s,e,ar,r · s ∈ Subjects ∧ e ∈ Subjects ∧ ar ∈ AccessRights ∧ r ∈ NRoles ⇒
(r ∈ CheckRight({s ↦ {e ↦ ar}}) ⇔ r ↦ ReadA ∈ SubjectAdmAccesses(s) ∧
ar = Own ∧ r ∈ SubjectNOwners(e))
```

Листинг 2. Инвариант-типа и инварианты-истинности тотальной функции $CheckRight$

Однако при разделении общего глобального типа $Union$ на глобальные типы $EntitiesU$, $RolesU$, $SubjectsU$ и $UsersU$, а следовательно, невозможности объединения их подмножеств, стало необходимым разделение области определения функции $CheckRight$. В итоге задаются следующие три частные тотальные функции (листинг 3):

— $CheckRightE$ — функция наличия прав доступа у субъект-сессии к сущности;
— $CheckRightR$ — функция наличия прав доступа у субъект-сессии к роли;
— $CheckRightS$ — функция наличия прав доступа у субъект-сессии к субъект-сессии.

```
   CheckRightEType:
CheckRightE ∈ Subjects × Entities × AccessRights → ℙ(Roles)
```

```
   CheckRightEFunc:
∀s,e,ar,r · s ∈ Subjects ∧ e ∈ Entities ∧ ar ∈ AccessRights ∧ r ∈ Roles ⇒
(r ∈ CheckRightE(s ↦ e ↦ ar) ⇔ r ↦ ReadA ∈ SubjectAdmAccesses(s) ∧
e ↦ ar ∈ RoleRights(r))
   CheckRightRType:
CheckRightR ∈ Subjects × Roles × AccessRights → ℙ(AdmRoles)
   CheckRightRFunc:
∀s,e,ar,r · s ∈ Subjects ∧ e ∈ Roles ∧ ar ∈ AccessRights ∧ r ∈ AdmRoles ⇒
(r ∈ CheckRightR(s ↦ e ↦ ar) ⇔ r ↦ ReadA ∈ SubjectAdmAccesses(s) ∧
e ↦ ar ∈ RoleAdmRights(r))
   CheckRightSType:
CheckRightS ∈ Subjects × Subjects × {Own} → ℙ(Roles)
   CheckRightSFunc1:
∀s,e,r · s ∈ Subjects ∧ e ∈ Subjects ∧ r ∈ OrdRoles ∪ AdmRoles ⇒
(r ∈ CheckRightS(s ↦ e ↦ Own) ⇔ r ↦ ReadA ∈ SubjectAdmAccesses(s) ∧
r ∈ SubjectOwner(e))
   CheckRightSFunc2:
∀s,e,r · s ∈ Subjects ∧ e ∈ Subjects ∧ r ∈ NRoles ⇒
(r ∈ CheckRightS(s ↦ e ↦ Own) ⇔ r ↦ ReadA ∈ SubjectAdmAccesses(s) ∧
r ∈ SubjectNOwners(e))
```

Листинг 3. Задание частных тотальных функций *CheckRightE*, *CheckRightR* и *CheckRightS*

Приём по разделению общей тотальной функции *CheckRight* на частные необходим не только для корректного их задания при использовании нескольких глобальных типов. Разделение (там, где это возможно) на непересекающиеся множества областей определения и значения функций и задание на них отдельных функций позволяет упростить их переопределения в событиях, где производится перебор значений элементов этих областей.

Например, при переопределении функции *CheckRight* [13] в событии создания субъект-сессией объекта *create_object* (листинг 4) отдельным охранным условием (*grd*25) было необходимо для всех субъект-сессий s, сущностей (кроме создаваемого объекта *object*), ролей, субъект-сессий e и видов прав доступа ar значение новой функции *checkRight* задать его повторением от исходной функции *CheckRight*. При этом при работе инструмента *ProB* необходимо перебрать значения элементов всей области определения ($Entities \cup Roles \cup Subjects$), тогда как изменения вносятся только в множество сущностей *Entities* добавлением в неё нового объекта. При использование трёх функций *CheckRightE*, *CheckRightR* и *CheckRightS* необходимо переопределение только функции *CheckRightE* (листинг 5), а следовательно, сокращается перебор значений элементов.

```
   grd24:
checkRight ∈ (Subjects ↔ ((Entities ∪ {object}) ∪ Roles ∪ Subjects
↔ AccessRights)) → ℙ(Roles)
   grd25:
∀s,e,ar·s∈Subjects ∧ e ∈ Entities ∪ Roles ∪ Subjects ∧ ar ∈ AccessRights
⇒ checkRight({s ↦ {e ↦ ar}}) = CheckRight({s ↦ {e ↦ ar}})
```

```
   grd26:
∀s,ar,r · s ∈ Subjects ∧ ar ∈ AccessRights ∧ r ∈ Roles ∧
r ↦ ReadA ∉ SubjectAdmAccesses(s) ⇒ r ∉ checkRight({s ↦ {object ↦ ar}})
   grd27:
∀s,ar,r · s ∈ Subjects ∧ ar ∈ AccessRights ∧ r ∈ Roles ∧
r ↦ ReadA ∈ SubjectAdmAccesses(s) ⇒
(r ∈ checkRight({s ↦ {object ↦ ar}}) ⇔ object ↦ ar ∈ roleRights(r))
   act8:
CheckRight := checkRight
```

Листинг 4. Переопределение тотальной функции *CheckRight* в событии *create_object*

```
   grd20:
checkRightE ∈ Subjects × (Entities ∪ {object}) × AccessRights → ℙ(Roles)
   grd21:
∀s,e,ar · s ∈ Subjects ∧ e ∈ Entities ∧ ar ∈ AccessRights ⇒
checkRightE(s ↦ e ↦ ar) = CheckRightE(s ↦ e ↦ ar)
   grd22:
∀s,ar,r · s ∈ Subjects ∧ ar ∈ AccessRights ∧ r ∈ Roles ⇒
(r ∈ checkRightE(s ↦ object ↦ ar) ⇔ r ↦ ReadA ∈ SubjectAdmAccesses(s) ∧
object ↦ ar ∈ roleRights(r))
   act7:
CheckRightE := checkRightE
```

Листинг 5. Переопределение частной тотальной функции *CheckRightE* в событии *create_object*

Дополнительным преимуществом использования частных тотальных функций взамен общих является возможность более детального их задания, что также сокращает перебор значений элементов. Сравним, например, инварианты-истинности функций *CheckRight* и *CheckRightS* (см. листинги 2 и 3). Согласно МРОСЛ ДП-модели, субъект-сессия с помощью текущей роли может обладать к другой субъект-сессии только правом доступа владения own_r (*Own*), но, используя общую тотальную функцию *CheckRight*, необходимо также задавать значения функции (пустое множество) и для остальных прав доступа, соответственно ProB при этом будет совершать дополнительный перебор. С применением частных тотальных функций на этапе задания инварианта-типа для *CheckRightS* соответствующее модели ограничение на права доступа субъект-сессии к субъект-сессии накладывается более точно.

3. Сокращение числа инвариантов и охранных условий, предполагающих перебор подмножеств некоторого множества

Ещё один приём, предлагаемый для устранения ошибки вида `timeout` и успешного применения инструмента проверки моделей ProB при верификации МРОСЛ ДП-модели, — сокращение числа инвариантов и охранных условий, предполагающих при использовании ProB перебор подмножеств некоторого множества, путём введения (там, где это возможно) тотальных функций, значениями которых являются данные подмножества. Для таких функций большинство их значений не должно изменяться в событиях, а значит, не потребуется соответствующий перебор подмножеств (например, вместо перебора подмножеств ролей для построения множества ролей, подчинённых

некоторой роли в иерархии, может быть задана функция потомков ролей), иначе использование данных функций может усложнить работу ProB.

Для примера рассмотрим изменение инварианта-истинности булевой функции доступа субъект-сессии к сущностям в контейнерах $ExecuteContainer$, параметрами которой являются субъект-сессия и сущность, а значение по определению является истинным в случае, когда в иерархии сущностей существует путь к заданной в параметрах сущности от некоторой корневой сущности-контейнера и субъект-сессия через её текущие роли имеет право доступа на выполнение $execute_r$ ($Execute$) ко всем сущностям-контейнерам, из которых состоит данный путь, и, наоборот, не имеет запрещающей роли, обладающей правом доступа $execute_r$ ($Execute$) хотя бы к одной сущности-контейнеру этого пути. В формализованной нотации, описанной в [13], данная функция представлена в виде тотальной функции $ExecuteContainer$ (листинг 6).

```
   ExecuteContainerType:
ExecuteContainer ∈ (Subjects ↔ Entities) → BOOL
   ExecuteContainerFunc:
∀s,e · s ∈ Subjects ∧ e ∈ Entities ⇒ (ExecuteContainer({s ↦ e}) = TRUE ⇔
(∃E, c · E ⊆ Containers ∧ Root ∉ E ∧ ((e ∈ dom(EntityNames) ∧
c∈dom(EntityNames(e)) ∧ Parent[E]∪{c} = E∪{Root}) ∨ (E = ∅ ∧ e = Root))
∧ (∀o · o ∈ E ∪ {Root} ⇒ (∃r · r ∈ CheckRight({s ↦ {o ↦ Execute}}) ∧
CheckRight({s ↦ {o ↦ Execute}}) ⊆ OrdRoles ∪ AdmRoles))))
```

Листинг 6. Задание тотальной функции $ExecuteContainer$

В инварианте-истинности функции ($ExecuteContainerFunc$) требуется существование подмножества множества сущностей-контейнеров E, представляющего собой путь к сущности e от некоторой корневой сущности-контейнера $Root$. При верификации модели с использованием ProB в событиях, где происходит переопределение функции $ExecuteContainer$, инструменту необходимо для каждой сущности e найти данное подмножество E путём перебора подмножеств множества глобального типа $Union$.

Данного перебора можно избежать, задав отдельно функцию $CPath$, значением которой для сущности-контейнера c является путь до неё от корневой сущности-контейнера, включая саму сущность-контейнер c (листинг 7).

```
   CPathType:
CPath ∈ Containers → ℙ1(Containers)
   CPath1:
∀c · c ∈ Containers ⇒ (c = Root ∧ CPath(c) = {Root}) ∨
(c ≠ Root ∧ {c,Root} ⊆ CPath(c) ∧ CPath(c) = CPath(Parent(c)) ∪ {c})
   NoCyclesForContainers:
∀c1,c2 · c1 ∈ Containers ∧ c2 ∈ Containers ∧ c2 ∈ CPath(c1) ∧ c1 ≠ c2 ⇒
c1 ∉ CPath(c2)
```

Листинг 7. Задание тотальной функции $CPath$

Эта функция переопределяется только в событиях создания сущности-контейнера $create\_container$ и удаления сущности $delete\_entity$, при этом исключается перебор подмножеств множества глобального типа $EntitiesU$ (функция $CPath$ была задана после разделения общего глобального типа $Union$), так как изменения вносятся однозначно для конкретной сущности-контейнера:

— при создании сущности-контейнера (каталога) *container* в сущности-контейнере (каталоге) *parent*: $CPath(container) = CPath(parent) \cup \{container\}$;
— при удалении сущности-контейнера (каталога) *container* в событии происходит проверка того, что она не содержит в себе других сущностей (каталог является пустым), а значит, *container* принадлежит только множеству $CPath(container)$ и просто исключается из области определения функции.

При использовании функции $CPath$ инвариант-истинности функции $ExecuteContainer$ имеет вид, представленный в листинге 8.

```
   ExecuteContainerFunc:
∀s,e · s ∈ Subjects ∧ e ∈ Entities ⇒ (ExecuteContainer(s ↦ e) = TRUE ⇔
e = Root ∨ (e ≠ Root ∧ (∃c · c ∈ Containers ∧ c ∈ dom(EntityNames(e)) ∧
(∀o·o∈CPath(c) ⇒ CheckRightE(s↦o↦Execute)∈ℙ1(OrdRoles∪AdmRoles)))))
```

Листинг 8. Инвариант-истинности тотальной функций *ExecuteContainer* с использованием тотальной функции $CPath$

При переопределении функции *ExecuteContainer* и нахождении её значения для субъект-сессии s и сущности e вместо перебора подмножеств множества глобального типа $Union$ для нахождения пути до сущности e используется значение функции $CPath(p)$, где p является сущностью-контейнером — родителем сущности e.

4. Апробация предложенных приёмов

Описанные приёмы прошли апробацию при верификации инструментом ProB первого уровня (уровня ролевого управления доступом) МРОСЛ ДП-модели в формализованной нотации. Без использования этих приёмов ошибка вида `timeout` возникала в следующих двух случаях.

Первый случай — при попытке инструментом ProB нахождения множества удовлетворяющих охранным условиям значений параметров для событий, в которых несколько охранных условий (*grd*) предполагали перебор подмножеств некоторого множества (например, в событии создания субъект-сессии *create_subject*) (рис. 1).

Второй случай — при задании уточнённого для инструмента ProB контекста модели (выполнении специального события *SETUP_CONTEXT*, осуществляющего инициализацию начального состояния системы в рамках модели) (рис. 2). Связано это с тем, что для верификации модели с использованием ProB (в отличие от Rodin, для которого необходимо для каждого глобального типа задать только условие его конечности) в контексте требуется явно указать мощность каждого множества глобального типа, что на практике часто является сложной задачей. С одной стороны, мощность каждого такого множества желательно задать достаточной для приближения модели в формализованной нотации к реальной ОССН, а именно: включения в него всех важных с точки зрения безопасности компонент системы. Например, множество сущностей глобального типа *EntitiesU* должно включать корневой каталог файловой системы («/»), каталог, где находятся параметры ОССН («/etc/»), домашний каталог пользователя («/home/») и др. С другой стороны, приходится учитывать накладываемые самим инструментом ProB ограничения по его производительности ввиду того, что при увеличении мощности множеств глобальных типов увеличивается и выполняемый инструментом перебор значений элементов данных множеств, что может привести к комбинаторному взрыву и завершению работы ProB с ошибкой вида `timeout`.

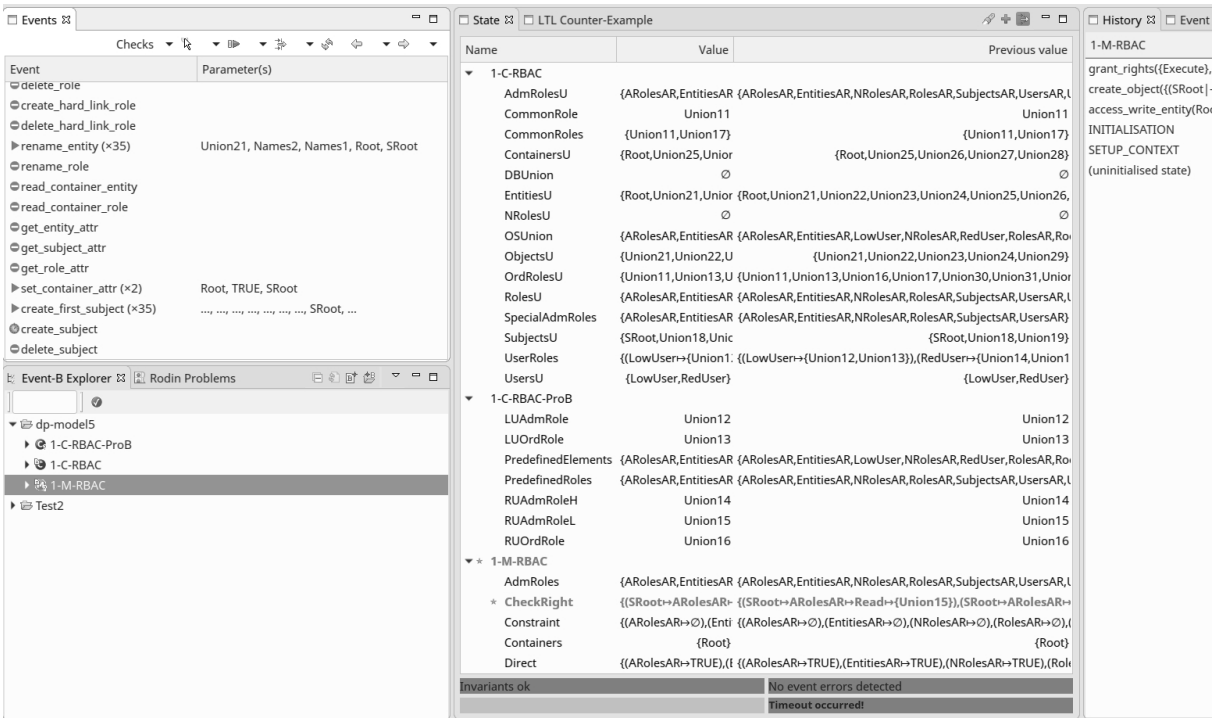


Рис. 1. Ошибка вида `timeout` для события *create_subject*

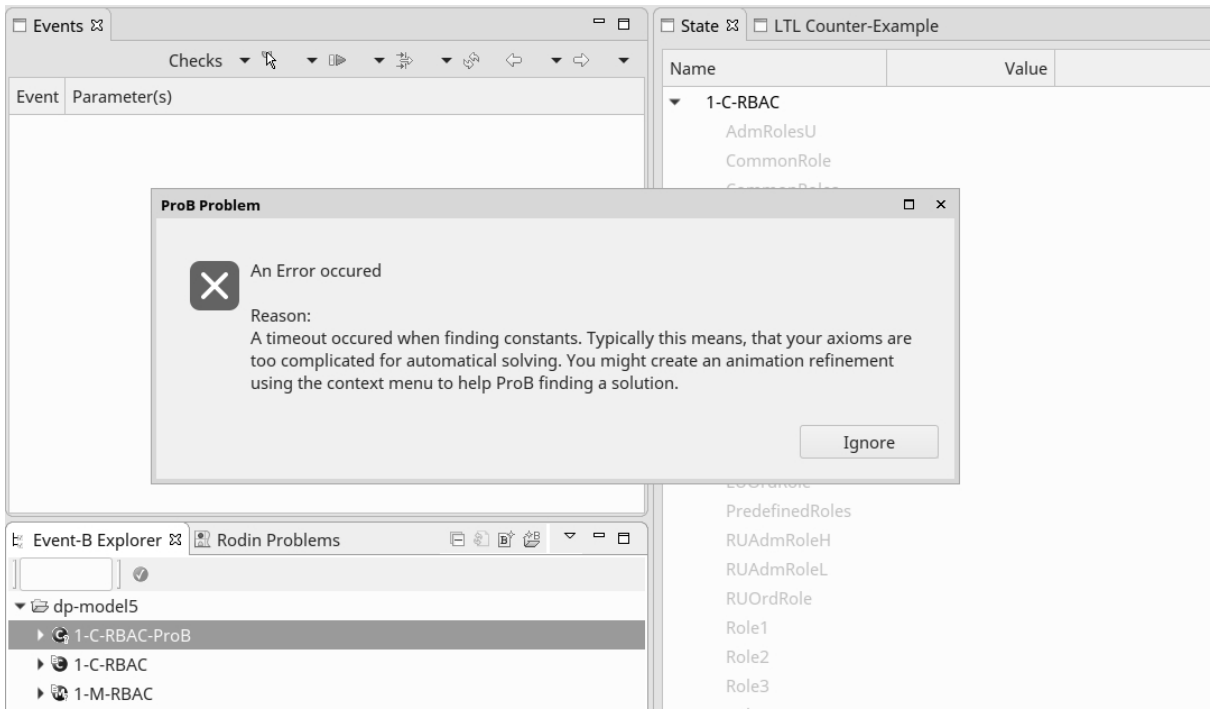


Рис. 2. Ошибка вида `timeout` при выполнении специального события *SETUP_CONTEXT*

В результате использования описанных приёмов в рассмотренных двух случаях была устранена ошибка вида `timeout`. Во-первых, стало возможным выполнить любое событие модели, так как для него алгоритмами инструмента ProB за приемлемое время происходит перебор и нахождение множества значений, удовлетворяющих охранным условиям события (пример результатов выполнения события *create_subject* приведён на рис. 3). Во-вторых, стало успешным выполнение специального события

SETUP_CONTEXT при большем числе элементов верифицируемой модели. Если ранее на развёрнутом авторами стенде данное событие выполнялось без ошибки максимум при 20 элементах в каждом состоянии системы (для $card(Union) = 20$), что очевидно недостаточно для адекватного моделирования основных важных с точки зрения безопасности компонент ОССН, то с использованием предложенных приёмов общее число элементов увеличилось до 68 (для $card(UsersU) = 10$, $card(EntitiesU) = 18$, $card(RolesU) = 30$ и $card(SubjectsU) = 10$).

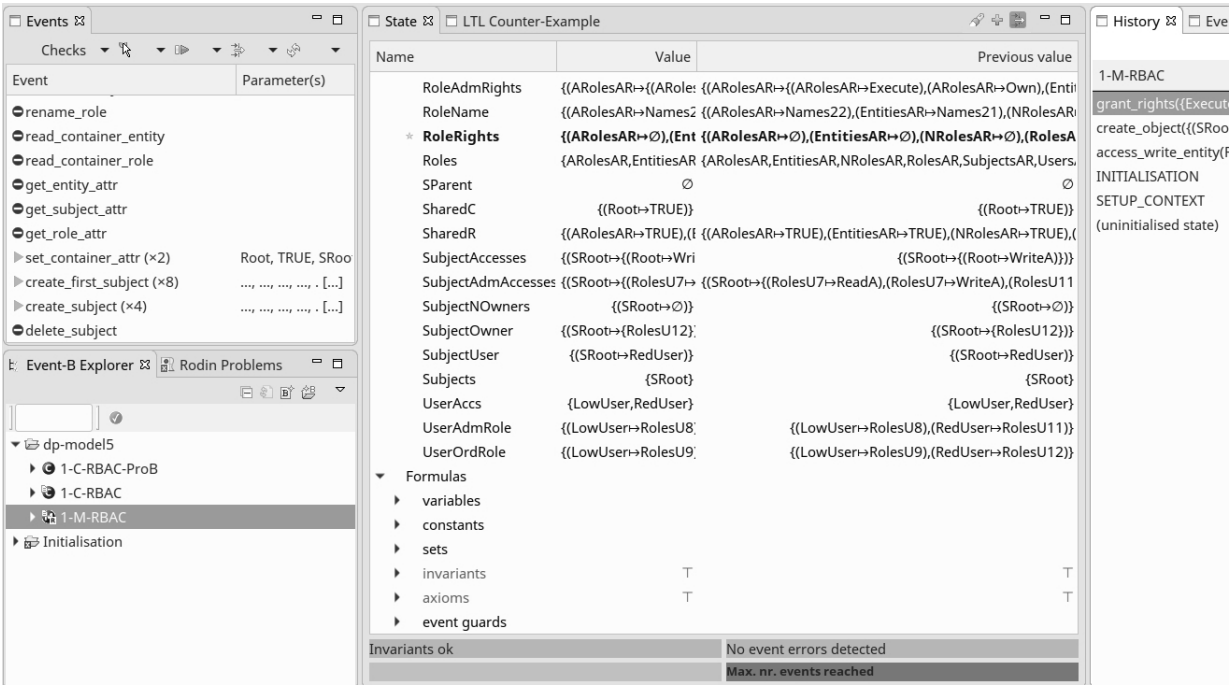


Рис. 3. Возможность выполнения события *create_subject*

Заключение

В настоящей работе на основе опыта использования инструмента проверки моделей ProB для верификации модели управления доступом промышленной ОССН Astra Linux Special Edition (МРОСЛ ДП-модели) в формализованной нотации (на формализованном языке метода Event-B) отмечено, что в большинстве случаев реализованные в ProB алгоритмы перебора значений элементов верифицируемой модели (и, как следствие, наличие проблемы комбинаторного взрыва) требуют доработки описания модели в формализованной нотации. В первую очередь это связано с тем, что некоторые способы представления модели, успешно использовавшиеся при её дедуктивной верификации инструментом Rodin, оказались непригодными для применения инструмента ProB.

Предложенные приёмы по доработке описания МРОСЛ ДП-модели в формализованной нотации, а именно использование нескольких глобальных типов, разделение общих тотальных функций на частные тотальные функции и сокращение числа инвариантов и охранных условий событий, предполагающих перебор подмножеств некоторого множества, создают условия для согласованной верификации описания всех восьми уровней модели инструментом проверки моделей ProB и инструментом дедуктивной верификации Rodin. Эти приёмы также могут быть полезны при разработке

других формальных моделей управления доступом и их верификации с применением соответствующих инструментов.

ЛИТЕРАТУРА

1. `https://astralinux.ru/products/astra-linux-special-edition/` — Операционная система специального назначения Astra Linux Special Edition.
2. *Буренин П. В., Девянин П. Н., Лебеденко Е. В. и др.* Безопасность операционной системы специального назначения Astra Linux Special Edition: учеб. пособие для вузов / под ред. П. Н. Девянина. 3-е изд., перераб. и доп. М.: Горячая линия — Телеком, 2019. 404 с.
3. `https://fstec.ru/component/attachments/download/2832` — Информационное сообщение ФСТЭК России от 15.10.2020 № 240/24/4268.
4. *Девянин П. Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб. пособие для вузов. 3-е изд., перераб. и доп. М.: Горячая линия — Телеком, 2020. 352 с.
5. *Devyanin P. N., Khoroshilov A. V., Kuliamin V. V., et al.* Integrating RBAC, MIC, and MLS in verified hierarchical security model for operating system // Program. Comput. Soft. 2020. V. 46. P. 443–453.
6. *Abrial J.-R.* Modeling in Event-B: System and Software Engineering. Cambridge University Press, 2010.
7. *Abrial J.-R., Butler M., Hallerstede S., et al.* Rodin: An open toolset for modelling and reasoning in Event-B // Intern. J. Software Tools for Technology Transfer. 2010. V. 12. No. 6. P. 447–466.
8. *Девянин П. Н., Ефремов Д. В., Кулямин В. В. и др.* Моделирование и верификация политик безопасности управления доступом в операционных системах. М.: Горячая линия — Телеком, 2019. 214 с.
9. *Девянин П. Н.* Уровень запрещающих ролей иерархического представления МРОСЛ ДП-модели // Прикладная дискретная математика. 2018. № 39. С. 58–71.
10. *Девянин П. Н.* Подходы к моделированию управления доступом в СУБД PostgreSQL в рамках МРОСЛ ДП-модели // Прикладная дискретная математика. Приложение. 2018. № 11. С. 95–98.
11. *Девянин П. Н.* О результатах формирования иерархического представления МРОСЛ ДП-модели // Прикладная дискретная математика. Приложение. 2016. № 9. С. 83–87.
12. *Abrial J.-R. and Hallerstede S.* Refinement, decomposition, and instantiation of discrete models: Application to Event-B // Fundamenta Informaticae. 2007. V. 77. Iss. 1–2. P. 1–28.
13. *Девянин П. Н., Леонова М. А.* Применение подтипов и тотальных функций формального метода Event-B для описания и верификации МРОСЛ ДП-модели // Программная инженерия. 2020. Т. 11. № 4. С. 230–241.
14. *Leuschel M. and Butler M.* ProB: an automated analysis toolset for the B method // Int. J. Softw. Tools Technol. Transf. 2008. No. 10(2). P. 185–203.

REFERENCES

1. `https://astralinux.ru/products/astra-linux-special-edition/` — OS Astra Linux Special Edition, 2020.
2. *Burenin P. V., Devyanin P. N., Lebedenko E. V., et al.* Bezopasnost' operacionnoy sistemy special'nogo naznacheniya Astra Linux Special Edition [Security of Operating System Astra Linux Special Edition]. Moscow, Goryachaya liniya — Telekom, 2019. 404 p. (in Russian)
3. `https://fstec.ru/component/attachments/download/2832` — Information message of FSTEC Russia dated 15.10.2020 no. 240/24/4268.

4. *Devyanin P. N.* Modeli bezopasnosti komp'yuternyh sistem. Upravlenie dostupom i informacionnymi potokami [The Models of Security of Computer Systems: Access Control and Information Flows]. Moscow, Goryachaya liniya — Telekom, 2020. 352 p. (in Russian)
5. *Devyanin P. N., Khoroshilov A. V., Kuliamin V. V., et al.* Integrating RBAC, MIC, and MLS in verified hierarchical security model for operating system. Program. Comput. Soft., 2020, vol. 46, pp. 443–453.
6. *Abrial J.-R.* Modeling in Event-B: System and Software Engineering. Cambridge University Press, 2010.
7. *Abrial J.-R., Butler M., Hallerstede S., et al.* Rodin: An open toolset for modelling and reasoning in Event-B. Intern. J. Software Tools for Technology Transfer, 2010, vol. 12, no. 6, pp. 447–466.
8. *Devyanin P. N., Efremov D. V., Kuliamin V. V., et al.* Modelirovanie i verifikaciya politik bezopasnosti upravleniya dostupom v operacionnyh sistemah [Modeling and Verification Access Control Security Policies on Operating Systems]. Moscow, Goryachaya liniya — Telekom, 2019. 214 p. (in Russian)
9. *Devyanin P. N.* Uroven' zapreschayuschih roley ierarhicheskogo predstavleniya MROSL DP-modeli [The level of negative roles of the hierarchical representation of MROSL DP-model]. Prikladnaya Diskretnaya Matematika, 2018, no. 39, pp. 58–71. (in Russian)
10. *Devyanin P. N.* Podhody k modelirovaniyu upravleniya dostupom v SUBD PostgreSQL v ramkah MROSL DP-modeli [Approaches to formal modeling of access control in PostgreSQL within framework of the MROSL DP-model]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2018, no. 11, pp. 95–98. (in Russian).
11. *Devyanin P. N.* O rezul'tatah formirovaniya ierarhicheskogo predstavleniya MROSL DP-modeli [About results of design hierarchical representation of MROSL DP-model]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2016, no. 9, pp. 83–87. (in Russian)
12. *Abrial J.-R. and Hallerstede S.* Refinement, decomposition, and instantiation of discrete models: Application to Event-B. Fundamenta Informaticae, 2007, vol. 77, iss. 1–2, pp. 1–28.
13. *Devyanin P. N. and Leonova M. A.* Primenenie podtipov i total'nyh funkciy formal'nogo metoda Event-B dlya opisaniya i verifikacii MROSL DP-modeli [Application of subtypes and total functions of Event-B formal method for the formalization and verification of the MROSL DP-model]. Programmnaya Ingeneria, 2020, vol. 11, no. 4, pp. 230–241. (in Russian)
14. *Leuschel M. and Butler M.* ProB: an automated analysis toolset for the B method. Int. J. Softw. Tools Technol. Transf., 2008, no. 10(2), pp. 185–203.

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

УДК 519.17

О НАИБОЛЬШЕМ ЧИСЛЕ ВЕРШИН ПРИМИТИВНЫХ ОДНОРОДНЫХ ГРАФОВ ПОРЯДКА 2, 3, 4 С ЭКСПОНЕНТОМ, РАВНЫМ 2[1]

М. Б. Абросимов*, С. В. Костин**, И. В. Лось*

*Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского, г. Саратов, Россия

**МИРЭА — Российский технологический университет, г. Москва, Россия

В 2015 г. вышло исследование, в котором рассмотрен вопрос о максимальном числе вершин n_k для регулярных графов заданного порядка k с диаметром 2. Авторы получили результаты для однородных графов порядка 2, 3 и 4: $n_2 = 5$, $n_3 = 10$, $n_4 = 15$. В данной работе исследуется аналогичный вопрос о наибольшем числе вершин np_k примитивного однородного графа порядка k с экспонентом, равным 2. Все примитивные однородные графы с экспонентом, равным 2, кроме полного, также имеют диаметр $d = 2$. Получены аналогичные значения для примитивных однородных графов с экспонентом 2: $np_2 = 3$, $np_3 = 4$, $np_4 = 11$.

Ключевые слова: *примитивный граф, примитивная матрица, экспонент, однородный граф.*

DOI 10.17223/20710410/52/6

THE MAXIMUM NUMBER OF VERTICES OF PRIMITIVE REGULAR GRAPHS OF ORDERS 2, 3, 4 WITH EXPONENT 2

M. B. Abrosimov*, S. V. Kostin**, I. V. Los*

*Saratov State University, Saratov, Russia

**MIREA — Russian Technological University, Moscow, Russia

E-mail: mic@rambler.ru, kostinsv77@mail.ru, los.ilia.ru@gmail.com

In 2015, the results were obtained for the maximum number of vertices n_k in regular graphs of a given order k with a diameter 2: $n_2 = 5$, $n_3 = 10$, $n_4 = 15$. In this paper, we investigate a similar question about the largest number of vertices np_k in a primitive regular graph of order k with exponent 2. All primitive regular graphs with exponent 2, except for the complete one, also have diameter $d = 2$. The following values were obtained for primitive regular graphs with exponent 2: $np_2 = 3$, $np_3 = 4$, $np_4 = 11$.

Keywords: *primitive graph, primitive matrix, exponent, regular graph.*

[1]Работа выполнена при поддержке Минобрнауки России в рамках выполнения госзадания (проект № FSRR-2020-0006).

Введение

Понятие примитивности изначально было сформулировано для квадратных матриц в работе [1]. Если рассматривать квадратную матрицу как матрицу смежности графа, то понятие примитивности естественным образом переносится на графы. Напомним необходимые определения. Неотрицательная квадратная матрица A называется *примитивной*, если существует натуральное t, такое, что A^t положительна. Минимальное такое значение t называется *экспонентом* матрицы A [1].

Вершина v достижима из вершины u за $t \geqslant 1$ шагов, если существует последовательность рёбер (маршрут) $\{u, w_1\}, \{w_1, w_2\}, \ldots, \{w_{t-1}, v\}$. Если A — матрица смежности графа $G = (V, \alpha)$, то достижимость вершины v из вершины u за t шагов означает, что на пересечении строки и столбца, соответствующих вершинам u и v соответственно, в матрице A^t стоит 1.

Граф G называется *примитивным*, если существует натуральное t, такое, что между любой парой вершин графа G существует маршрут длины t (иначе говоря, в матрице A^t все элементы равны 1). Минимальное такое значение t называется *экспонентом* графа G и обозначается $\exp(G)$. Примитивные графы представляют большой интерес как с теоретической, так и с практической точек зрения [2–5]. Ряд работ посвящён исследованию экспонентов однородных примитивных матриц [6–8]; рассматриваемые в этих работах матрицы соответствуют орграфам. В данной работе мы будем рассматривать экспоненты неориентированных однородных графов. Напомним, что *однородным* (или *регулярным*) графом порядка k называется простой неориентированный граф, все вершины которого имеют степень k. Множество n-вершинных однородных графов порядка k будем обозначать $R_{n,k}$.

В [8] исследуется вопрос о минимальном числе дуг (рёбер) у орграфов (графов) с экспонентом, равным 2. В частности, для неориентированных графов с экспонентом 2 минимальное число рёбер есть $(3n-3)/2$ для нечётного n и $(3n-2)/2$ для чётного n. В [6] доказано, что однородные ориентированные графы порядка k (степени исхода и захода каждой вершины равны k) с экспонентом, равным 2, существуют при следующих значениях n:

$$k + 1 \leqslant n \leqslant 2k - 1.$$

Если рассматривать каждое ребро неориентированного графа как пару встречных дуг, то однородный неориентированный граф порядка k можно считать однородным ориентированным графом порядка $2k$. Тогда оценка для неориентированных графов принимает вид

$$k + 1 \leqslant n \leqslant 4k - 1.$$

Нижняя оценка достигается для полных графов K_n. Через np_k обозначим максимальное число вершин в примитивном однородном графе порядка k с экспонентом 2. В [9] рассматриваются однородные графы с диаметром 2. Напомним, что *диаметром* $d(G)$ связного графа G называется максимальное из расстояний между всеми парами вершин G. Через n_k авторы [9] обозначили максимальное число вершин в однородном графе порядка k и доказали, что $5(k-1) \leqslant n_k \leqslant k^2 + 1$, а также нашли точное значение n_k для $k = 2, 3, 4$: $n_2 = 5$, $n_3 = 10$, $n_4 = 15$. Очевидно, что $np_k \leqslant n_k$. С учётом оценки из [6] получаем, что

$$k + 1 \leqslant np_k \leqslant 4k - 1.$$

Таким образом, $np_2 \leqslant 7$, $np_3 \leqslant 11$, $np_4 \leqslant 15$. Так как $np_k \leqslant n_k$, то получаем лучшие оценки: $np_2 \leqslant 5$, $np_3 \leqslant 10$. Цель данной работы — получить точные значения.

1. Основные результаты

Очевидно, что любой примитивный граф является связным. Графы с числом вершин $n < 3$ не являются примитивными, поэтому далее рассматриваем графы с числом вершин $n \geqslant 3$. Цикл длины 3 будем называть треугольником. Через $g(G)$ обозначим обхват графа G, то есть наименьшую из длин циклов графа G. Так как в неориентированных графах нет петель, то примитивных графов с экспонентом, равным 1, не существует, то есть $\exp(G) > 1$. Нас будут интересовать однородные графы с $\exp(G) = 2$. Очевидно, что диаметр таких графов $d(G) \leqslant 2$, однако это условие не является достаточным.

Теорема 1. Граф G с числом вершин $n \geqslant 3$ является примитивным с $\exp(G) = 2$ тогда и только тогда, когда $d(G) \leqslant 2$ и каждое ребро графа G входит в треугольник.

Доказательство. Необходимость. Пусть G — примитивный граф с числом вершин $n \geqslant 3$ и $\exp(G) = 2$. Рассмотрим две произвольные различные вершины u, v. Между ними есть путь длины 2, следовательно, эксцентриситет этих вершин не превосходит 2. В силу произвольности выбора вершин получаем, что $d(G) \leqslant 2$. Заметим, что $d(G) = 1$ только для полного графа. Полный n-вершинный граф K_n является однородным порядка $n - 1$ и примитивным с экспонентом $\exp(K_n) = 2$.

Рассмотрим две произвольные смежные вершины u, v. Между ними должен быть путь длины 2, который не может содержать ребро (u, v). Следовательно, есть отличная от u и v вершина w, смежная с u и v. Таким образом, ребро (u, v) входит в треугольник, образованный вершинами u, v и w.

Достаточность. Пусть $d(G) \leqslant 2$ и каждое ребро графа G входит в треугольник. Тогда граф G связный и, очевидно, в нём есть маршрут длины 2 из любой вершины в саму себя. Покажем, что такой маршрут есть и между любыми двумя различными вершинами u и v. Так как $d(G) \leqslant 2$, то $d(u, v) \leqslant 2$. Если вершины u и v несмежны, то между ними нет маршрута длины 1, следовательно, есть маршрут длины 2.

Если вершины u и v смежны, то по условию ребро (u, v) входит в треугольник, следовательно, есть отличная от u и v вершина w, смежная с u и v, получаем маршрут длины 2: uwv. ■

Следствие 1. Пусть G — примитивный граф с $\exp(G) = 2$. Тогда его обхват $g(G) = 3$.

В данной работе исследуем следующий вопрос: какое максимальное число вершин np_k может быть у примитивного однородного графа порядка k с экспонентом $\exp(G) = 2$?

Легко заметить, что любой полный граф K_n при $n > 2$ является примитивным и $\exp(K_n) = 2$. Так как каждое ребро примитивного графа G с $\exp(G) = 2$ входит в треугольник, степень всех вершин графа G не ниже 2. Оказывается, оценку минимальной степени вершин графов с экспонентом, равным 2, можно повысить. В [8] получен следующий результат: для неориентированных графов с экспонентом 2 минимальное число рёбер есть $(3n - 3)/2$ для нечётного n и $(3n - 2)/2$ для чётного n. Очевидно, что полный граф K_3 является регулярным порядка 2 и примитивным с экспонентом 2. С учётом этого получаем

Теорема 2. $np_2 = 3$.

Следствие 2. Среди регулярных графов $R_{n,2}$ только граф K_3 имеет экспонент, равный 2.

С другой стороны, кубические графы (то есть регулярные графы порядка 3) содержат $3n/2$ рёбер и удовлетворяют условию из работы [8]. Однако получен следующий результат:

Теорема 3. $np_3 = 4$.

Доказательство. Очевидно, что полный граф K_4 является регулярным порядка 3 и примитивным с экспонентом 2.

Пусть G — примитивный кубический n-вершинный граф с $\exp(G) = 2$ и $n > 4$. По следствию 2 обхват графа G равен 3. Рассмотрим произвольный треугольник в G: $\{u_1, u_2, u_3\}$. Так как граф G кубический, то вершина u_1, кроме вершин u_2 и u_3, смежна ещё с одной вершиной w. Рассмотрим ребро (u_1, w). По теореме 1 это ребро должно входить в треугольник. Так как кроме w вершина u_1 смежна только с вершинами u_2 и u_3, то w должна быть смежна с одной из них. Если вершина w смежна и с u_2, и с u_3, то получаем граф K_4. Не ограничивая общности, будем считать, что вершина w смежна с u_2, но несмежна с u_3. Следовательно, вершина w смежна ещё с некоторой вершиной v, отличной от u_1, u_2 и u_3. Снова по теореме 1 ребро (w, v) должно входить в некоторый треугольник. Однако вершина w, кроме v, смежна только с u_1 и u_2, а вершина v с ними смежной быть не может, так как вершины u_1 и u_2 имеют степень 3, причём смежны между собой и с вершинами w и u_3. Получили противоречие. ■

Следствие 3. Среди регулярных графов $R_{n,3}$ только граф K_4 имеет экспонент, равный 2.

Далее перейдём к исследованию биквадратных графов, то есть однородных графов $R_{n,4}$ порядка 4.

2. Биквадратные графы

Согласно оценке [6], $np_4 \leqslant 15$. Следующая теорема даёт оценку, худшую для графов с большим k, но лучшую для нашего случая, чем оценка из [6].

Лемма 1. Для однородных графов порядка k справедливо

$$np_k \leqslant k^2 - k + 1 \text{ при чётном } k;$$
$$np_k \leqslant k^2 - k \text{ при нечётном } k.$$

Доказательство. Пусть G — примитивный n-вершинный граф порядка k с $\exp(G) = 2$. Выберем произвольную вершину v и расположим все остальные вершины по расстоянию от вершины v: на нулевом уровне — вершина v, на первом уровне — вершины, смежные с v; все остальные вершины — на втором уровне.

Так как все вершины имеют степень k, вершин на первом уровне будет в точности k. Обозначим их $v_1, \ldots, v_k$. Рассмотрим произвольную из этих вершин, например v_1. По теореме 1 ребро $\{v, v_1\}$ должно входить в треугольник, то есть должна быть вершина w, смежная с v и с v_1. Однако все вершины, смежные с v, расположены на первом уровне, следовательно, w — это одна из вершин $v_2, \ldots, v_k$. Таким образом, каждая из вершин $v_1, \ldots, v_k$ смежна по крайней мере с одной вершиной из этого же списка.

Если k чётно, то у произвольной вершины v_i первого уровня одно ребро идёт к вершине v, ещё одно ребро — к одной из вершин первого уровня, а остальные $k-2$ ребра могут идти к вершинам второго уровня. Тогда на последнем уровне может быть $k(k-2)$ вершин. Всего получаем $np_k \leqslant 1 + k + k(k-2) = k^2 - k + 1$.

Если k нечётно, то, как и в первом случае, можем соединить рёбрами $k-1$ вершину, а оставшаяся вершина будет смежна с одной из уже использованных. Поэтому на

втором уровне может быть $(k-1)(k-2)+(k-3) = k^2-2k-1$ вершин. Всего получаем $np_k \leqslant 1+k+k^2-2k-1 = k^2-k$. ■

Для малых значений k лемма 1 даёт оценки $np_2 \leqslant 3$, $np_3 \leqslant 6$, $np_4 \leqslant 13$, что лучше оценок, полученных по неравенству из работы [6]. Для np_5 лемма 1 даёт оценку 20, а из [6] получается оценка 18. Компьютерный эксперимент показал, что $np_5 = 16$ [10].

Теорема 4. $np_4 = 11$.

Доказательство. По лемме 1 $np_4 \leqslant 13$. Покажем, что при $n = 13$ и 12 не существует примитивного биквадратного графа G с $\exp(G) = 2$. Рассмотрим каждый случай отдельно и попробуем построить граф с нужными свойствами.

С л у ч а й 1: $n = 13$. Предположим, что G — примитивный биквадратный граф с $\exp(G) = 2$. Расположим вершины по уровням, как в доказательстве леммы 1. Для удобства будем делать укладку, начиная с вершины 1, а смежные с ней вершины обозначим 2, 3, 4 и 5 (рис. 1).

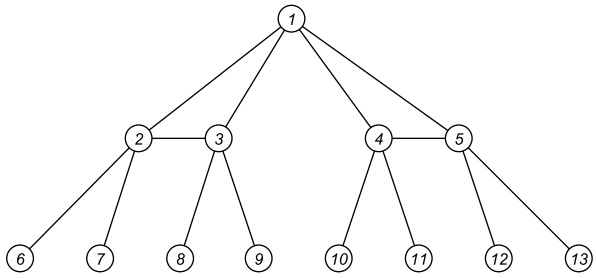


Рис. 1. Укладка вершин 13-вершинного графа

У нас остаётся свобода в добавлении рёбер между вершинами второго уровня. Рассмотрим две смежные вершины из первого и второго уровней, например 2 и 6. По теореме 1 ребро $(2, 6)$ должно входить в треугольник, следовательно, вершины 6 и 7 должны быть смежны. Аналогично, смежными по необходимости будут вершины 8 и 9, 10 и 11, 12 и 13 (рис. 2).

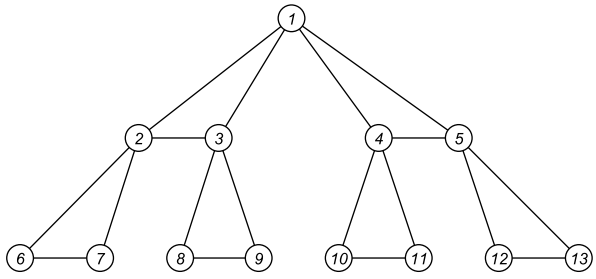


Рис. 2. Укладка вершин 13-вершинного графа (продолжение)

Рассмотрим вершины второго уровня. Так как $\exp(G) = 2$, между несмежными вершинами должны быть маршруты длины 2. Например, от вершины 6 должны существовать маршруты длины 2 до вершин 8, 9, 10, 11, 12 и 13, однако это невозможно, так как осталось только два возможных ребра, инцидентных вершине 6.

С л у ч а й 2: $n = 12$. Предположим, что G — примитивный биквадратный граф с $\exp(G) = 2$. Расположим вершины по уровням, как в предыдущем случае. Мы долж-

ны добавить минимум два ребра между вершинами первого уровня (см. доказательство леммы 1). Заметим, что если добавить более двух рёбер между вершинами первого уровня, то не хватит рёбер для соединения четырёх вершин первого уровня с семью вершинами второго уровня. Поэтому восемь рёбер будут соединять вершины первого и второго уровней, т. е. одна вершина второго уровня должна быть смежна с двумя вершинами первого уровня. Не ограничивая общности, оставим свободным одно ребро у вершины 5 и рассмотрим различные варианты соединения вершины 5 с какой-либо вершиной 6–11 (рис. 3). Заметим, что вершины множеств $\{6, 7, 8, 9\}$ и $\{10, 11\}$ являются подобными, поэтому достаточно рассмотреть соединение ребром вершины 5 с одной из вершин каждого множества. Как и в предыдущем случае, по теореме 1 мы должны добавить рёбра между вершинами 6 и 7, 8 и 9, 10 и 11.

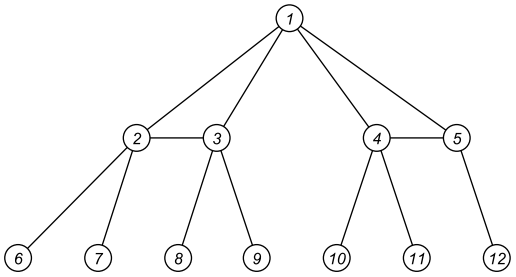


Рис. 3. Укладка вершин 12-вершинного графа

1. Добавим ребро $(5, 9)$. По теореме 1 ребро $(5, 9)$ должно входить в треугольник, следовательно, необходимо добавить и ребро $(9, 12)$. Вершина 9 теперь имеет степень 4 (рис. 4). Так как $\exp(G) = 2$, между несмежными вершинами должны быть маршруты длины 2. Например, от вершины 9 должны быть маршруты длины 2 до вершин 6, 7, 10 и 11. У нас остаётся возможность добавить только два ребра от вершины 8 и два ребра от вершины 12. С учётом теоремы 1, это можно сделать только двумя способами.

1.1. Добавляем рёбра от вершины 8 к вершинам 6 и 7, а от вершины 12 — к вершинам 10 и 11. Но тогда от вершины 5 не будет маршрута длины 2 до вершин 6 и 7.

1.2. Добавляем рёбра от вершины 8 к вершинам 10 и 11, а от вершины 12 — к вершинам 6 и 7. После этого остаётся возможность соединить двумя рёбрами вершины 6 и 7 с вершинами 10 и 11, но это сделать невозможно без нарушения теоремы 1.

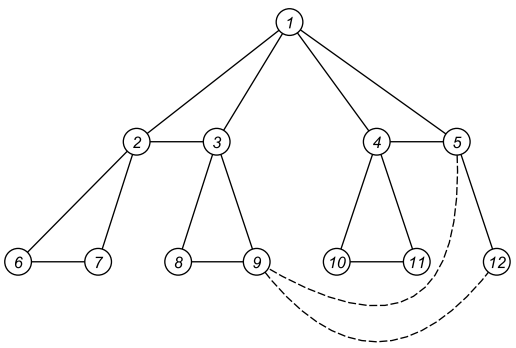


Рис. 4. Укладка 12-вершинного графа, соединяем вершины 5 и 9

2. Добавим ребро $(5, 11)$. По теореме 1 оно должно входить в треугольник, следовательно, необходимо добавить и ребро $(11, 12)$. Вершина 11 теперь имеет степень 4

(рис. 5). Так как $\exp(G) = 2$, между несмежными вершинами должны быть маршруты длины 2. Например, от вершины 5 должны быть маршруты длины 2 до вершин 6, 7, 8 и 9, но у нас остаётся возможность добавить только два ребра от вершины 12, что недостаточно.

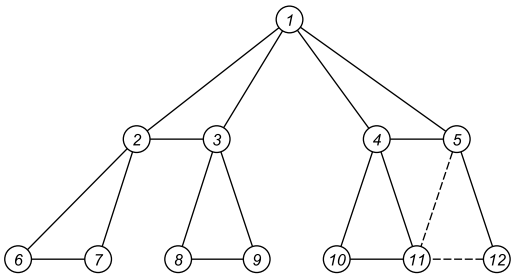
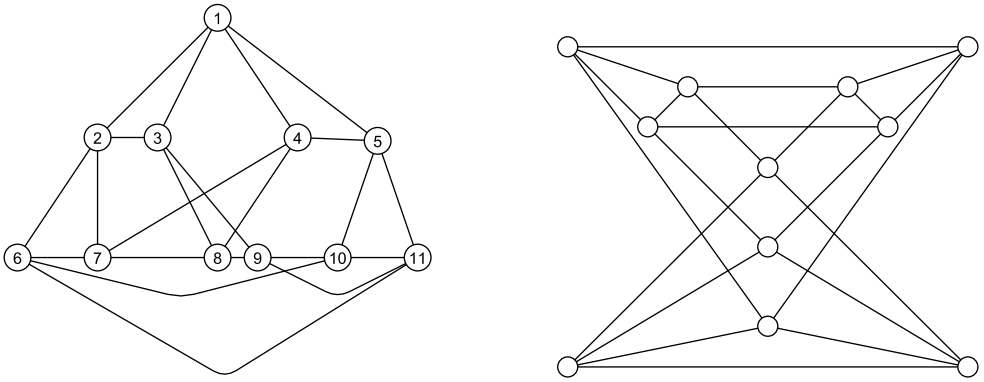


Рис. 5. Укладка 12-вершинного графа, соединяем вершины 5 и 11

Таким образом, доказано, что $np_4 < 12$. На рис. 6 приведён 11-вершинный 4-регулярный граф с экспонентом 2: *а* — изображение в стиле доказательства теоремы; *б* — по работе [11].



а *б*

Рис. 6. 11-Вершинный регулярный граф порядка 4 с $\exp(G) = 2$.

Теорема 4 доказана. ■

Был проведён вычислительный эксперимент, в рамках которого найдены все биквадратные графы с экспонентом 2 [10]. Всего таких графов 10: полный граф K_5, один 6-вершинный граф $O_2 + O_2 + O_2$, два 7-вершинных, два 8-вершинных, три 9-вершинных и один 11-вершинный граф, представленный на рис. 6.

ЛИТЕРАТУРА

1. *Wielandt H.* Unzerlegbare nicht negative Matrizen // Math. Zeitschr. 1950. V. 52. P. 642–648.
2. *Сачков В. Н., Ошкин И. Б.* Экспоненты классов неотрицательных матриц // Дискретная математика. 1993. № 2. С. 150–159.
3. *Салий В. Н.* Минимальные примитивные расширения ориентированных графов // Прикладная дискретная математика. 2008. № 1(1). С. 116–119.
4. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(11). С. 101–112.

5. *Фомичев В. М., Авезова Я. Э.* Точная формула экспонентов перемешивающих орграфов регистровых преобразований // Дискретный анализ и исследование операций. 2020. № 2(27). С. 117–135.
6. *Jin M., Lee S. G., and Seol H. G.* Exponents of r-regular primitive matrices // Inform. Center Math. Sci. 2003. V. 6. No. 2. P. 51–57.
7. *Bueno M. I. and Furtado S.* On the exponent of r-regular primitive matrices // ELA. Electronic J. Linear Algebra. 2008. V. 17. P. 28–47.
8. *Kim B., Song B., and Hwang W.* Nonnegative primitive matrices with exponent 2 // Linear Algebra Appl. 2005. No. 407. P. 162–168.
9. *Hoa V. D. and Do M. T.* k-Regular graph with diameter 2 // Int. J. Adv. Comput. Technol. 2015. V. 4. No. 5. P. 14–19.
10. *Лось И. В., Абросимов М. Б., Костин С. В.* К вопросу о примитивных однородных графах с экспонентом, равным 2 и 3 // Компьютерные науки и информационные технологии. Материалы Междунар. науч. конф. Саратов: Изд. центр «Наука», 2018. С. 251–253.
11. *Костин С. В.* Об использовании задач по теории графов для интеллектуального развития учащихся // Математика в образовании: сб. статей. Вып. 10 / под ред. И. С. Емельяновой. Чебоксары: Изд-во Чуваш. ун-та. 2014. С. 68–74.

REFERENCES

1. *Wielandt H.* Unzerlegbare nicht negative Matrizen. Math. Zeitschr., 1950, vol. 52, pp. 642–648.
2. *Sachkov V. N., Oshkin I. B.* Eksponenty klassov neotritsatel'nykh matrits [Exponents of classes of non-negative matrices]. Diskretnaya Matematika, 1993, no. 2, pp. 150–159. (in Russian)
3. *Salii V. N.* Minimal'nye primitivnye rasshireniya orientirovannykh grafov [Minimal primitive extensions of oriented graphs]. Prikladnaya Diskretnaya Matematika, 2008, no. 1(1), pp. 116–119. (in Russian)
4. *Fomichev V. M.* Otsenki eksponentov primitivnykh grafov [The estimates of exponents for primitive graphs]. Prikladnaya Diskretnaya Matematika, 2011, no. 2(11), pp. 101–112. (in Russian)
5. *Fomichev V. M. and Avezova Ya. E.* The exact formula for the exponents of the mixing digraphs of register transformations. J. Appl. Ind. Math., 2020, no. 14, pp. 308–320.
6. *Jin M., Lee S. G., and Seol H. G.* Exponents of r-regular primitive matrices. Inform. Center Math. Sci., 2003, vol. 6, no. 2, pp. 51–57.
7. *Bueno M. I. and Furtado S.* On the exponent of r-regular primitive matrices. ELA. Electronic J. Linear Algebra, 2008, vol. 17, pp. 28–47.
8. *Kim B., Song B., and Hwang W.* Nonnegative primitive matrices with exponent 2. Linear Algebra Appl., 2005, no. 407, pp. 162–168.
9. *Hoa V. D. and Do M. T.* k-Regular graph with diameter 2. Int. J. Adv. Comput. Technol., 2015, vol. 4, no. 5, pp. 14–19.
10. *Los' I. V., Abrosimov M. B., and Kostin S. V.* K voprosu o primitivnykh odnorodnykh grafakh s eksponentom, ravnym 2 i 3 [On the question of primitive regular graphs with exponent equals to 2 and 3]. Komp'yuternye Nauki i Informatsionnye Tekhnologii. Saratov, Nauka Publ., 2018, pp. 251–253. (in Russian)
11. *Kostin S. V.* Ob ispol'zovanii zadach po teorii grafov dlya intellektual'nogo razvitiya uchashchikhsya [On the use of graph theory problems for the intellectual development of students]. Matematika v Obrazovanii. I. S. Emel'yanova (ed.). Cheboksary, Chuvash University Publ., 2014, pp. 68–74. (in Russian)

УДК 519.17

МЕТРИКА ДЛЯ СРАВНЕНИЯ ГРАФОВ С УПОРЯДОЧЕННЫМИ ВЕРШИНАМИ НА ОСНОВЕ МАКСИМАЛЬНОГО ОБЩЕГО ПОДГРАФА

Н. Д. Москин

Петрозаводский государственный университет, г. Петрозаводск, Россия

Работа посвящена методам сравнения и классификации графов. Данное направление известно под названием «graph matching». Приводится обзор метрик для сравнения графов, основанных на максимальном общем подграфе. Предложена модификация расстояния на основе максимального общего подграфа, которое учитывает упорядоченность вершин. Показано, что эта функция удовлетворяет всем свойствам метрики (неотрицательность, тождественность, симметричность, неравенство треугольника).

Ключевые слова: *граф, сравнение, метрика, максимальный общий подграф, graph matching.*

DOI 10.17223/20710410/52/7

METRIC FOR COMPARING GRAPHS WITH ORDERED VERTICES BASED ON THE MAXIMUM COMMON SUBGRAPH

N. D. Moskin

Petrozavodsk State University, Petrozavodsk, Russia

E-mail: moskin@petrsu.ru

The paper is devoted to the methods of comparison and classification of graphs. This direction is known as graph matching. An overview of metrics for comparing graphs based on a maximum common subgraph is given. A graph $\mathrm{mcs}(G, F)$ is a maximal common subgraph of graphs G and F if it is isomorphic to $G' \subseteq G$ and $F' \subseteq F$ and contains the maximum number of vertices. In some tasks (for example, comparing texts), it is important to take into account one more factor: vertex numbering. A modification of the distance based on the maximum common subgraph is proposed, taking into account this factor (each vertex has its own unique number). We determine a function of graphs G and F as follows: $d(G, F) = 1 - \min\limits_{i=1,\ldots,k}(|\mathrm{mcs}(g_{\min(i,m)}, f_i)|/i)$. Here $|G|$ denotes the number of vertices in G, $|G| = m$, $|F| = k$, $m \leqslant k$; and g_i is the subgraph of G containing vertices with numbers from 1 to i and all edges of G incident to these vertices (the graphs f_i are defined similarly). It is shown that this function satisfies all the properties of the metric (nonnegativity, identity, symmetry, triangle inequality). This metric can be used to solve various problems of image recognition (for example, to establish the authorship of texts).

Keywords: *graph, comparison, metric, maximum common subgraph, graph matching.*

Введение

В настоящее время графы используются в различных областях науки и могут быть построены по разным принципам. Одной из задач, которая возникает при построении подобных моделей, является задача сравнения и классификации [1]. Методы, известные в рамках направления graph matching, нашли своё применение в обработке изображений [2], молекулярной биологии [3], дактилоскопии [4], распознавании почерка [5], исследовании социальных сетей [6], при анализе документов [7] и т. д. На множестве графов задаётся расстояние, которое позволяет оценить, насколько те или иные структуры похожи друг на друга. Как правило, эта функция выражает степень неточностей, которые возникают при нахождении изоморфизма графов или подграфов. При этом в некоторых задачах (например, при сравнении текстов) важно учитывать ещё один фактор: нумерацию вершин.

Одной из таких задач является атрибуция текстов. Например, данная проблема возникает при анализе коллекции текстов из дореволюционных журналов «Время» (1861–1863), «Эпоха» (1864–1865) и еженедельника «Гражданин» (1873–1874). Известно, что Ф. М. Достоевский (вместе со своим братом М. М. Достоевским) редактировал и возглавлял эти журналы, поэтому уже давно ведутся исследования на предмет принадлежности его перу данных произведений. Большое количество этих статей опубликовано анонимно, т. е. либо без подписи, либо под псевдонимами. Впрочем, это относится и к статьям, которые исследователи давно приписывали Достоевскому, более или менее основываясь на документальных данных.

Для решения задачи атрибуции текстов могут быть использованы «графы сильных связей» [8]. Множество вершин подобного графа — это множество грамматических форм, которые встречаются в текстах, а рёбра отражают «сильные связи» между вершинами. Две вершины v_i и v_j связаны ребром, если частота встречаемости пары грамматических классов больше или равна заданному в исследовании пороговому значению α. Далее грамматические формы и соответствующие им вершины могут быть отсортированы в порядке убывания по степени их встречаемости в определённых текстах (или группе текстов). Кроме того, если вершина не имеет инцидентных рёбер в результате отбрасывания «слабых» связей, она рассматривается как изолированная вершина. С точки зрения филологии при распознавании авторского стиля писателя важно не только наличие в корпусе тех или иных грамматических конструкций, но и порядок их встречаемости в текстах.

В п. 1 данной работы описаны несколько известных метрик, основанных на максимальном общем подграфе. В п. 2 предложена модификация расстояния на основе максимального общего подграфа, которая учитывает упорядоченность вершин (т. е. каждой вершине ставится в соответствие её уникальный порядковый номер). Показано, что эта функция удовлетворяет всем свойствам метрики (неотрицательность, тождественность, симметричность, неравенство треугольника).

1. Метрики на множестве графов, основанные на максимальном общем подграфе

Одним из способов сравнения графов является расстояние на основе максимального общего подграфа. Максимальным общим подграфом графов G_1 и G_2 будем называть граф $\mathrm{mcs}(G_1, G_2)$, который изоморфен $G'_1 \subseteq G_1$, $G'_2 \subseteq G_2$ и содержит максимальное число вершин.

Обозначим через $|G|$ число вершин в графе G. Расстояние между непустыми графами G_1 и G_2 можно вычислить следующим образом [9]:

$$d_1(G_1, G_2) = 1 - \frac{|\mathrm{mcs}(G_1, G_2)|}{\max(|G_1|, |G_2|)}. \tag{1}$$

Расстояние $d_1(G_1, G_2)$ принимает значения от 0 до 1 включительно. Если графы изоморфны, то $d_1(G_1, G_2) = 0$. Заметим, что, исходя из определения, максимальный общий подграф $\mathrm{mcs}(G_1, G_2)$ не обязательно уникален.

Вторая функция на основе максимального общего подграфа предложена в [10]:

$$d_2(G_1, G_2) = 1 - \frac{|\mathrm{mcs}(G_1, G_2)|}{|G_1| + |G_2| - |\mathrm{mcs}(G_1, G_2)|}.$$

Значения $d_2(G_1, G_2)$, как и $d_1(G_1, G_2)$, находятся в пределах от 0 до 1. Ещё одно похожее расстояние предложено в [11], но оно не нормализовано для отрезка [0, 1]:

$$d_3(G_1, G_2) = |G_1| + |G_2| - 2|\mathrm{mcs}(G_1, G_2)|.$$

При задании функции на множестве графов желательно, чтобы $d(G_i, G_j)$ удовлетворяла следующим свойствам метрики (для произвольных i, j, k):

1) $d(G_i, G_j) \geqslant 0$ (неотрицательность);
2) $d(G_i, G_j) = 0 \Leftrightarrow G_i = G_j$ (тождественность);
3) $d(G_i, G_j) = d(G_j, G_i)$ (симметричность);
4) $d(G_i, G_j) \leqslant d(G_i, G_k) + d(G_k, G_j)$ (неравенство треугольника).

В [9] показано, что функция (1) удовлетворяет всем свойствам метрики.

2. Метрика на основе максимального общего подграфа для сравнения графов с упорядоченными вершинами

При сравнении графов с упорядоченными вершинами важно учитывать нумерацию вершин. Представим граф с упорядоченными вершинами в виде цепочки порождающих его подграфов $g_1, g_2, g_3, \ldots, g_m$, как показано на рис. 1 (m — число вершин графа G). Здесь граф g_i является подграфом G, который содержит вершины с номерами от 1 до i включительно и все рёбра G, инцидентные этим вершинам. Подграф g_m совпадает с графом G.

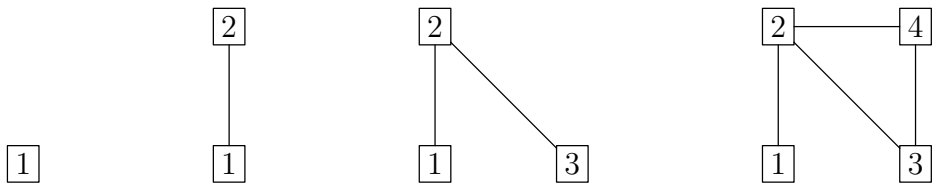


Рис. 1. Цепочка порождающих графов для графа G

Цепочку порождающих графов можно рассматривать как частный случай динамических графов [12]. Динамический граф представляет собой последовательность конечных невзвешенных (не всегда связных) графов $g_1, g_2, g_3, \ldots, g_l, \ldots$, в которой переход к последующему графу g_{l+1} осуществляется применением операции $\varphi(g_l) = g_{l+1}$.

Операция, осуществляющая переход, может быть как простой (удаление/добавление ребра, удаление/добавление вершины), так и сложной (это операция, которую можно описать чередованием простых операций). Последовательность графов, составляющих динамический граф, называют траекторией динамического графа.

Определим функцию на графах G и F следующим образом (пусть для определённости $|G| = m$, $|F| = k$, $m \leqslant k$):

$$d(G, F) = 1 - \min_{i=1,\ldots,k}(|\mathrm{mcs}(g_{\min(i,m)}, f_i)|/i). \tag{2}$$

Теорема 1. Величина d удовлетворяет всем свойствам метрики.

Доказательство.

а) Докажем первое свойство. Так как количество вершин в графах $g_{\min(i,m)}$ и f_i не превосходит i для $i = 1, \ldots, k$, то $|\mathrm{mcs}(g_{\min(i,m)}, f_i)| \leqslant i$, т. е.

$$|\mathrm{mcs}(g_{\min(i,m)}, f_i)|/i \leqslant 1.$$

Следовательно, справедливо неравенство

$$\min_{i=1,\ldots,k}(|\mathrm{mcs}(g_{\min(i,m)}, f_i)|/i) \leqslant 1.$$

Тогда получаем

$$d(G, F) = 1 - \min_{i=1,\ldots,k}(|\mathrm{mcs}(g_{\min(i,m)}, f_i)|/i) \geqslant 0.$$

б) Докажем второе свойство.

$\Rightarrow$ Пусть $d(G, F) = 0$. Тогда по формуле (2)

$$\min_{i=1,\ldots,k}(|\mathrm{mcs}(g_{\min(i,m)}, f_i)|/i) = 1,$$

поэтому для $i = 1, \ldots, k$

$$|\mathrm{mcs}(g_{\min(i,m)}, f_i)|/i \geqslant 1,$$

т. е. $|\mathrm{mcs}(g_{\min(i,m)}, f_i)| \geqslant i$.

С другой стороны, $|\mathrm{mcs}(g_{\min(i,m)}, f_i)| \leqslant i$. Поэтому $|\mathrm{mcs}(g_{\min(i,m)}, f_i)| = i$. При $i \geqslant m$ выполняется равенство $|\mathrm{mcs}(g_m, f_i)| = i$, что возможно только если $i = m$. Следовательно, $|\mathrm{mcs}(g_m, f_m)| = m$, т. е. графы G и F изоморфны.

$\Leftarrow$ Пусть $G = F$. Тогда $m = k$ и $\min(i, m) = i$ для $i = 1, \ldots, k$; $g_i = f_i$ для $i = 1, \ldots, k$, следовательно, максимальный общий подграф имеет i вершин, т. е. $|\mathrm{mcs}(g_i, f_i)| = i$ для $i = 1, \ldots, k$. Отсюда

$$\min_{i=1,\ldots,k}(|\mathrm{mcs}(g_{\min(i,m)}, f_i)|/i) = 1,$$

поэтому $d(G, F) = 0$.

в) Третье свойство справедливо, поскольку $|\mathrm{mcs}(g_{\min(i,m)}, f_i)| = |\mathrm{mcs}(f_i, g_{\min(i,m)})|$ для $i = 1, \ldots, k$.

г) Докажем четвёртое свойство. Пусть H — произвольный граф с t вершинами. Необходимо показать, что $d(G, F) \leqslant d(G, H) + d(H, F)$. Рассмотрим три случая (по

условию $m \leqslant k$, поэтому возможны три варианта расположения t относительно m и k: $t < m \leqslant k$, $m \leqslant t \leqslant k$ и $m \leqslant k < t$).

С л у ч а й 1: $t < m \leqslant k$. Согласно (2), надо доказать, что

$$1 - \min_{i=1,\ldots,k}(|\mathrm{mcs}(g_{\min(i,m)}, f_i)|/i) \leqslant 1 - \min_{i=1,\ldots,m}(|\mathrm{mcs}(g_i, h_{\min(i,t)})|/i) + \\ +1 - \min_{i=1,\ldots,k}(|\mathrm{mcs}(h_{\min(i,t)}, f_i)|/i).$$

Так как графы g_i, f_i, h_i содержат i вершин, т. е. $|g_i| = |f_i| = |h_i| = i$, выполним следующую замену:

$$1 - \min_{i=1,\ldots,k}\left(\frac{|\mathrm{mcs}(g_{\min(i,m)}, f_i)|}{\max(|g_{\min(i,m)}|, |f_i|)}\right) \leqslant 1 - \min_{i=1,\ldots,m}\left(\frac{|\mathrm{mcs}(g_i, h_{\min(i,t)})|}{\max(|g_i|, |h_{\min(i,t)}|)}\right) + \\ +1 - \min_{i=1,\ldots,k}\left(\frac{|\mathrm{mcs}(h_{\min(i,t)}, f_i)|}{\max(|h_{\min(i,t)}|, |f_i|)}\right).$$

Перейдя от поиска минимума к максимуму, получим

$$\max_{i=1,\ldots,k}\left(1 - \frac{|\mathrm{mcs}(g_{\min(i,m)}, f_i)|}{\max(|g_{\min(i,m)}|, |f_i|)}\right) \leqslant \max_{i=1,\ldots,m}\left(1 - \frac{|\mathrm{mcs}(g_i, h_{\min(i,t)})|}{\max(|g_i|, |h_{\min(i,t)}|)}\right) + \\ + \max_{i=1,\ldots,k}\left(1 - \frac{|\mathrm{mcs}(h_{\min(i,t)}, f_i)|}{\max(|h_{\min(i,t)}|, |f_i|)}\right).$$

Согласно формуле (1), перепишем неравенство:

$$\max_{i=1,\ldots,k} d_1(g_{\min(i,m)}, f_i) \leqslant \max_{i=1,\ldots,m} d_1(g_i, h_{\min(i,t)}) + \max_{i=1,\ldots,k} d_1(h_{\min(i,t)}, f_i).$$

1.1. Предположим, что $\max\limits_{i=1,\ldots,k} d_1(g_{\min(i,m)}, f_i)$ достигается при некотором индексе i^*, который находится на интервале $1 \leqslant i^* \leqslant t$, тогда

$$\max_{i=1,\ldots,k} d_1(g_{\min(i,m)}, f_i) = d_1(g_{i^*}, f_{i^*}) \leqslant d_1(g_{i^*}, h_{i^*}) + d_1(h_{i^*}, f_{i^*}) \leqslant \\ \leqslant \max_{i=1,\ldots,t} d_1(g_i, h_i) + \max_{i=1,\ldots,t} d_1(h_i, f_i) \leqslant \max_{i=1,\ldots,m} d_1(g_i, h_{\min(i,t)}) + \max_{i=1,\ldots,k} d_1(h_{\min(i,t)}, f_i).$$

Неравенство выполняется, так как величина d_1 удовлетворяет всем свойствам метрики, а граф h_{i^*} существует при $i^* \leqslant t$.

1.2. Предположим, что $\max\limits_{i=1,\ldots,k} d_1(g_{\min(i,m)}, f_i)$ достигается при некотором индексе i^*, который находится на интервале $t < i^* \leqslant m$, тогда

$$\max_{i=1,\ldots,k} d_1(g_{\min(i,m)}, f_i) = d_1(g_{i^*}, f_{i^*}) \leqslant d_1(g_{i^*}, h_t) + d_1(h_t, f_{i^*}) \leqslant \\ \leqslant \max_{i=t+1,\ldots,m} d_1(g_i, h_t) + \max_{i=t+1,\ldots,m} d_1(h_t, f_i) \leqslant \max_{i=1,\ldots,m} d_1(g_i, h_{\min(i,t)}) + \max_{i=1,\ldots,k} d_1(h_{\min(i,t)}, f_i).$$

Неравенство выполняется, так как величина d_1 удовлетворяет всем свойствам метрики.

1.3. Предположим, что $\max\limits_{i=1,\ldots,k} d_1(g_{\min(i,m)}, f_i)$ достигается при некотором индексе i^*, который находится на интервале $m < i^* \leqslant k$, тогда

$$\max_{i=1,\ldots,k} d_1(g_{\min(i,m)}, f_i) = d_1(g_m, f_{i^*}) \leqslant d_1(g_m, h_t) + d_1(h_t, f_{i^*}) \leqslant d_1(g_m, h_t) + \\ + \max_{i=m+1,\ldots,k} d_1(h_t, f_i) \leqslant \max_{i=1,\ldots,m} d_1(g_i, h_{\min(i,t)}) + \max_{i=1,\ldots,k} d_1(h_{\min(i,t)}, f_i).$$

Неравенство выполняется, так как величина d_1 удовлетворяет всем свойствам метрики.

С л у ч а й 2: $m \leqslant t \leqslant k$. Согласно (2), надо доказать, что

$$1 - \min_{i=1,\dots,k}(|\mathrm{mcs}(g_{\min(i,m)}, f_i)|/i) \leqslant 1 - \min_{i=1,\dots,t}(|\mathrm{mcs}(g_{\min(i,m)}, h_i)|/i) + \\ +1 - \min_{i=1,\dots,k}(|\mathrm{mcs}(h_{\min(i,t)}, f_i)|/i).$$

Так как $|g_i| = |f_i| = |h_i| = i$, выполним следующую замену:

$$1 - \min_{i=1,\dots,k}\left(\frac{|\mathrm{mcs}(g_{\min(i,m)}, f_i)|}{\max(|g_{\min(i,m)}|, |f_i|)}\right) \leqslant 1 - \min_{i=1,\dots,t}\left(\frac{|\mathrm{mcs}(g_{\min(i,m)}, h_i)|}{\max(|g_{\min(i,m)}|, |h_i|)}\right) + \\ +1 - \min_{i=1,\dots,k}\left(\frac{|\mathrm{mcs}(h_{\min(i,t)}, f_i)|}{\max(|h_{\min(i,t)}|, |f_i|)}\right).$$

Перейдя от поиска минимума к максимуму, получим

$$\max_{i=1,\dots,k}\left(1 - \frac{|\mathrm{mcs}(g_{\min(i,m)}, f_i)|}{\max(|g_{\min(i,m)}|, |f_i|)}\right) \leqslant \max_{i=1,\dots,t}\left(1 - \frac{|\mathrm{mcs}(g_{\min(i,m)}, h_i)|}{\max(|g_{\min(i,m)}|, |h_i|)}\right) + \\ + \max_{i=1,\dots,k}\left(1 - \frac{|\mathrm{mcs}(h_{\min(i,t)}, f_i)|}{\max(|h_{\min(i,t)}|, |f_i|)}\right).$$

Согласно формуле (1), перепишем неравенство так:

$$\max_{i=1,\dots,k} d_1(g_{\min(i,m)}, f_i) \leqslant \max_{i=1,\dots,t} d_1(g_{\min(i,m)}, h_i) + \max_{i=1,\dots,k} d_1(h_{\min(i,t)}, f_i).$$

2.1. Предположим, что $\max\limits_{i=1,\dots,k} d_1(g_{\min(i,m)}, f_i)$ достигается при некотором индексе i^*, который находится на интервале $1 \leqslant i^* \leqslant m$, тогда

$$\max_{i=1,\dots,k} d_1(g_{\min(i,m)}, f_i) = d_1(g_{i^*}, f_{i^*}) \leqslant d_1(g_{i^*}, h_{i^*}) + d_1(h_{i^*}, f_{i^*}) \leqslant \max_{i=1,\dots,m} d_1(g_i, h_i) + \\ + \max_{i=1,\dots,m} d_1(h_i, f_i) \leqslant \max_{i=1,\dots,t} d_1(g_{\min(i,m)}, h_i) + \max_{i=1,\dots,k} d_1(h_{\min(i,t)}, f_i).$$

Неравенство выполняется, так как величина d_1 удовлетворяет всем свойствам метрики, а граф h_{i^*} существует при $i^* \leqslant m \leqslant t$.

2.2. Предположим, что $\max\limits_{i=1,\dots,k} d_1(g_{\min(i,m)}, f_i)$ достигается при некотором индексе i^*, который находится на интервале $m < i^* \leqslant t$, тогда

$$\max_{i=1,\dots,k} d_1(g_{\min(i,m)}, f_i) = d_1(g_m, f_{i^*}) \leqslant d_1(g_m, h_{i^*}) + d_1(h_{i^*}, f_{i^*}) \leqslant \\ \leqslant \max_{i=m+1,\dots,t} d_1(g_m, h_i) + \max_{i=m+1,\dots,t} d_1(h_i, f_i) \leqslant \max_{i=1,\dots,t} d_1(g_{\min(i,m)}, h_i) + \max_{i=1,\dots,k} d_1(h_{\min(i,t)}, f_i).$$

Неравенство выполняется, так как величина d_1 удовлетворяет всем свойствам метрики, а граф h_{i^*} существует при $i^* \leqslant t$.

2.3. Предположим, что $\max\limits_{i=1,\dots,k} d_1(g_{\min(i,m)}, f_i)$ достигается при некотором индексе i^*, который находится на интервале $t < i^* \leqslant k$, тогда

$$\max_{i=1,\dots,k} d_1(g_{\min(i,m)}, f_i) = d_1(g_m, f_{i^*}) \leqslant d_1(g_m, h_t) + d_1(h_t, f_{i^*}) \leqslant d_1(g_m, h_t) + \\ + \max_{i=t+1,\dots,k} d_1(h_t, f_i) \leqslant \max_{i=1,\dots,t} d_1(g_{\min(i,m)}, h_i) + \max_{i=1,\dots,k} d_1(h_{\min(i,t)}, f_i).$$

Неравенство выполняется, так как величина d_1 удовлетворяет всем свойствам метрики.

С л у ч а й 3: $m \leqslant k < t$. Согласно (2), надо доказать, что

$$1 - \min_{i=1,\dots,k}(|\mathrm{mcs}(g_{\min(i,m)}, f_i)|/i) \leqslant 1 - \min_{i=1,\dots,t}(|\mathrm{mcs}(g_{\min(i,m)}, h_i)|/i) + \\ +1 - \min_{i=1,\dots,t}(|\mathrm{mcs}(h_i, f_{\min(i,k)})|i).$$

Так как $|g_i| = |f_i| = |h_i| = i$, выполним следующую замену:

$$1 - \min_{i=1,\dots,k}\left(\frac{|\mathrm{mcs}(g_{\min(i,m)}, f_i)|}{\max(|g_{\min(i,m)}|, |f_i|)}\right) \leqslant 1 - \min_{i=1,\dots,t}\left(\frac{|\mathrm{mcs}(g_{\min(i,m)}, h_i)|}{\max(|g_{\min(i,m)}|, |h_i|)}\right) + \\ +1 - \min_{i=1,\dots,t}\left(\frac{|\mathrm{mcs}(h_i, f_{\min(i,k)})|}{\max(|h_i|, |f_{\min(i,k)}|)}\right).$$

Перейдя от поиска минимума к максимуму, получим

$$\max_{i=1,\dots,k}\left(1 - \frac{|\mathrm{mcs}(g_{\min(i,m)}, f_i)|}{\max(|g_{\min(i,m)}|, |f_i|)}\right) \leqslant \max_{i=1,\dots,t}\left(1 - \frac{|\mathrm{mcs}(g_{\min(i,m)}, h_i)|}{\max(|g_{\min(i,m)}|, |h_i|)}\right) + \\ + \max_{i=1,\dots,t}\left(1 - \frac{|\mathrm{mcs}(h_i, f_{\min(i,k)})|}{\max(|h_i|, |f_{\min(i,k)}|)}\right).$$

Согласно формуле (1), перепишем неравенство так:

$$\max_{i=1,\dots,k} d_1(g_{\min(i,m)}, f_i) \leqslant \max_{i=1,\dots,t} d_1(g_{\min(i,m)}, h_i) + \max_{i=1,\dots,t} d_1(h_i, f_{\min(i,k)}).$$

3.1. Предположим, что $\max\limits_{i=1,\dots,k} d_1(g_{\min(i,m)}, f_i)$ достигается при некотором индексе i^*, который находится на интервале $1 \leqslant i^* \leqslant m$, тогда

$$\max_{i=1,\dots,k} d_1(g_{\min(i,m)}, f_i) = d_1(g_{i^*}, f_{i^*}) \leqslant d_1(g_{i^*}, h_{i^*}) + d_1(h_{i^*}, f_{i^*}) \leqslant \max_{i=1,\dots,m} d_1(g_i, h_i) + \\ + \max_{i=1,\dots,m} d_1(h_i, f_i) \leqslant \max_{i=1,\dots,t} d_1(g_{\min(i,m)}, h_i) + \max_{i=1,\dots,t} d_1(h_i, f_{\min(i,k)}).$$

Неравенство выполняется, так как величина d_1 удовлетворяет всем свойствам метрики, а граф h_{i^*} существует при $i^* \leqslant m < t$.

3.2. Предположим, что $\max\limits_{i=1,\dots,k} d_1(g_{\min(i,m)}, f_i)$ достигается при некотором индексе i^*, который находится на интервале $m < i^* \leqslant k$, тогда

$$\max_{i=1,\dots,k} d_1(g_{\min(i,m)}, f_i) = d_1(g_m, f_{i^*}) \leqslant d_1(g_m, h_{i^*}) + d_1(h_{i^*}, f_{i^*}) \leqslant \\ \leqslant \max_{i=m+1,\dots,k} d_1(g_m, h_i) + \max_{i=m+1,\dots,k} d_1(h_i, f_i) \leqslant \max_{i=1,\dots,t} d_1(g_{\min(i,m)}, h_i) + \max_{i=1,\dots,t} d_1(h_i, f_{\min(i,k)}).$$

Неравенство выполняется, так как величина d_1 удовлетворяет всем свойствам метрики, а граф h_{i^*} существует при $i^* \leqslant k < t$.

Таким образом, величина d удовлетворяет всем свойствам метрики. ■

На рис. 2 изображены три графа G_1, G_2, G_3 с разной нумерацией вершин. Расстояния между ними следующие: $d(G_1, G_2) = 1/3$, $d(G_1, G_3) = d(G_2, G_3) = 1/2$. Как видно на рисунке, отличия в первой паре графов возникают на уровне третьего порождающего графа, тогда как в двух остальных парах различия видны уже на втором уровне.

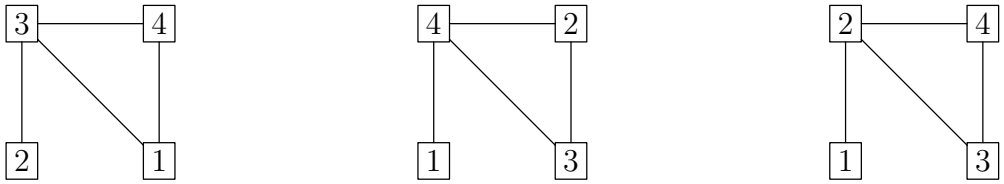


Рис. 2. Графы G_1, G_2, G_3 с различной нумерацией вершин

Заключение

В работе рассмотрена задача сравнения и классификации графов. Предложена функция для сравнения графов, которая основана на максимальном общем подграфе и учитывает упорядоченность вершин. Доказано, что эта величина удовлетворяет всем свойствам метрики. Классические алгоритмы для поиска максимального общего подграфа $\mathrm{mcs}(G_1, G_2)$ для двух графов основаны на алгоритме поиска с возвратом, предложенном МакГрегором, или на поиске максимальной клики, предложенном Леви [13]. Первый ищет все возможные общие подграфы и выбирает среди них максимальный, второй строит специальный граф соответствий и в нём ищет максимальную клику, которая определяет максимальный общий подграф. Заметим, что обе задачи являются NP-полными. Для проведения вычислительных экспериментов был реализован алгоритм первого типа, осуществляющий полный перебор возможных подграфов. При подсчёте расстояний между графами разной размерности, построенными случайным образом, свойства метрики выполняются.

Отметим, что данная метрика может быть использована в различных задачах теории распознавания образов (например, при сравнении текстов и изображений).

ЛИТЕРАТУРА

1. *Conte D., Foggia P., Sansone C., and Vento M.* Thirty years of graph matching in pattern recognition // Int. J. Pattern Recognit. Artif. Intell. 2004. V. 18. No. 3. P. 265–298.
2. *Sharma H., Pawar A., Chourasia C., and Khatri S.* Implementation of face recognition system based on elastic bunch graph matching // Intern. J. Engineering Sciences & Research Technology (IJESRT). 2016. V. 5. No. 3. P. 888–895.
3. *Schirmer S., Ponty Y., and Giegerich R.* Introduction to RNA secondary structure comparison // RNA Sequence, Structure, and Function: Computational and Bioinformatic Methods. Methods in Molecular Biology. Totowa, NJ: Humana Press, 2014. V. 1097. P. 247–273.
4. *Pawar V. and Zaveri M.* K-Means graph database clustering and matching for fingerprint recognition // Intelligent Information Management. 2015. V. 7. No. 4. P. 242–251.
5. *Fischer A., Suen C., Frinken V., et al.* A fast matching algorithm for graph-based handwriting recognition // LNCS. 2013. V. 7877. P. 194–203.
6. *Ogaard K., Roy H., Kase S., et al.* Discovering patterns in social networks with graph matching algorithms // LNCS. 2013. V. 7812. P. 341–349.
7. *Stauffer M., Fischer A., and Riesen K.* Speeding-up graph-based keyword spotting in historical handwritten documents // LNCS. 2017. V. 10310. P. 83–93.
8. *Рогов А. А., Седов А. В., Сидоров Ю. В., Суровцова Т. Г.* Математические методы атрибуции текстов. Петрозаводск: Изд-во ПетрГУ, 2014. 96 с.
9. *Bunke H. and Shearer K.* A graph distance metric based on the maximal common subgraph // Pattern Recognit. Lett. 1998. V. 19. No. 3–4. P. 255–259.

10. *Wallis W., Shoubridge P., Kraetz M., and Ray D.* Graph distances using graph union // Pattern Recognit. Lett. 2001. V. 22. P. 701–704.
11. *Bunke H.* On a relation between graph edit distance and maximum common subgraph // Pattern Recognit. Lett. 1997. V. 18. P. 689–694.
12. *Кочкаров А. А., Сенникова Л. И.* Метрические характеристики динамических графов и их применение // Новые информационные технологии в автоматизированных системах. М.: Московский институт электроники и математики НИУ ВШЭ, 2015. № 18. С. 236–241.
13. *Bunke H., Foggia P., Guidobaldi C., et al.* A comparison of algorithms for maximum common subgraph on randomly connected graphs // LNCS. 2002. V. 2396. P. 123–132.

REFERENCES

1. *Conte D., Foggia P., Sansone C., and Vento M.* Thirty years of graph matching in pattern recognition. Int. J. Pattern Recognit. Artif. Intell., 2004, vol. 18, no. 3, pp. 265–298.
2. *Sharma H., Pawar A., Chourasia C., and Khatri S.* Implementation of face recognition system based on elastic bunch graph matching. Intern. J. Engineering Sciences & Research Technology (IJESRT), 2016, vol. 5, no. 3, pp. 888–895.
3. *Schirmer S., Ponty Y., and Giegerich R.* Introduction to RNA secondary structure comparison. RNA Sequence, Structure, and Function: Computational and Bioinformatic Methods. Methods in molecular biology. Totowa, NJ, Humana Press, 2014, vol. 1097, pp. 247–273.
4. *Pawar V. and Zaveri M.* K-Means graph database clustering and matching for fingerprint recognition. Intelligent Information Management, 2015, vol. 7, no. 4, pp. 242–251.
5. *Fischer A., Suen C., Frinken V., et al.* A fast matching algorithm for graph-based handwriting recognition. LNCS, 2013, vol. 7877, pp. 194–203.
6. *Ogaard K., Roy H., Kase S., et al.* Discovering patterns in social networks with graph matching algorithms. LNCS, 2013, vol. 7812, pp. 341–349.
7. *Stauffer M., Fischer A., and Riesen K.* Speeding-up graph-based keyword spotting in historical handwritten documents. LNCS, 2017, vol. 10310, pp. 83–93.
8. *Rogov A. A., Sedov A. V., Sidorov Y. V., and Surovceva T. G.* Matematicheskie metody atribucii tekstov [Mathematical Methods for text Attribution]. Petrozavodsk, PetrSU Publ., 2014. 96 p. (in Russian)
9. *Bunke H. and Shearer K.* A graph distance metric based on the maximal common subgraph. Pattern Recognit. Lett., 1998, vol. 19, no. 3–4, pp. 255–259.
10. *Wallis W., Shoubridge P., Kraetz M., and Ray D.* Graph distances using graph union. Pattern Recognit. Lett., 2001, vol. 22, pp. 701–704.
11. *Bunke H.* On a relation between graph edit distance and maximum common subgraph. Pattern Recognit. Lett., 1997. vol. 18. pp. 689–694.
12. *Kochkarov A. A. and Sennikova L. I.* Metricheskiye kharakteristiki dinamicheskikh grafov i ikh primeneniye [Metric characteristics of dynamic graphs and their application]. Novyye Informatsionnyye Tekhnologii v Avtomatizirovannykh Sistemakh, 2015, no. 18, pp. 236–241. (in Russian)
13. *Bunke H., Foggia P., Guidobaldi C., et al.* A comparison of algorithms for maximum common subgraph on randomly connected graphs. LNCS, 2002, vol. 2396, pp. 123–132.

УДК 519.7

ДИСКРЕТНАЯ ЗАМКНУТАЯ ОДНОЧАСТИЧНАЯ ЦЕПОЧКА КОНТУРОВ

П. А. Мышкис, А. Г. Таташев, М. В. Яшина

Московский автомобильно-дорожный государственный технический университет (МАДИ), г. Москва, Россия

Рассматривается дискретная динамическая система, называемая замкнутой цепочкой контуров, которая принадлежит классу контурных сетей, введённому А. П. Буслаевым. Замкнутая цепочка содержит N контуров, на каждом из которых имеется $2m$ ячеек и одна частица. Контур имеет общую точку, называемую узлом, с каждым из двух соседних контуров слева и справа. Узлы делят контур на две равные части. В каждый момент $t = 0, 1, 2, \ldots$ частица перемещается на одну ячейку в заданном направлении, если нет задержек. Если две частицы стремятся пересечь один и тот же узел, то возникает задержка. В этом случае перемещается только частица контура, расположенного слева от узла. Вводится величина потенциальной задержки частицы, зависящая от времени и принимающая значения 0 или 1. При $t \geqslant m$ равенство этой величины 1 означает, что время до задержки частицы не превышает m. Сумма потенциальных задержек всех частиц называется потенциалом задержек. Начиная с некоторого момента времени, состояния системы периодически повторяются (предельные циклы). Отношение числа перемещений частицы к периоду цикла называется средней скоростью частицы. Доказаны следующие теоремы: 1) Потенциал задержек является невозрастающей функцией от времени, причём на предельном цикле значение потенциала задержек не изменяется и равно неотрицательному целому числу не больше $2N/3$. 2) Если средняя скорость частиц на предельном цикле меньше 1, то период цикла (возможно, не являющийся наименьшим) равен $(m + 1)N$. 3) Средняя скорость частиц равна $v = 1 - H/((m + 1)N)$, где H — потенциал задержек на предельном цикле. 4) Для любого m существует N, такое, что существует предельный цикл с потенциалом задержек $H > 0$ и, следовательно, со средней скоростью $v < 1$.

Ключевые слова: *динамическая система, контурная сеть, предельный цикл, потенциал задержек.*

DOI 10.17223/20710410/52/8

DISCRETE CLOSED ONE-PARTICLE CHAIN OF CONTOURS

P. A. Myshkis, A. G. Tatashev, M. V. Yashina

Moscow Automobile and Road Construction State Technical University (MADI), Moscow, Russia

E-mail: p.myshkis@yandex.ru, a-tatashev@yandex.ru, mv.yashina@madi.ru

A discrete dynamical system called a closed chain of contours is considered. This system belongs to the class of the contour networks introduced by A. P. Buslaev. The closed chain contains N contours. There are $2m$ cells and a particle at each contour. There are two points on any contour called a node such that each of these points is common for this contour and one of two adjacent contours located on the left

and right. The nodes divide each contour into equal parts. At any time $t = 0, 1, 2, \ldots$ any particle moves onto a cell forward in the prescribed direction. If two particles simultaneously try to cross the same node, then only the particle of the left contour moves. The time function is introduced, that is equal to 0 or 1. This function is called the potential delay of the particle. For $t \geqslant m$, the equality of this function to 1 implies that the time before the delay of the particle is not greater than m. The sum of all particles potential delays is called the potential of delays. From a certain moment, the states of the system are periodically repeated (limit cycles). Suppose the number of transitions of a particle on the limit cycle is equal to $S(T)$ and the period is equal to T. The ratio $S(T)$ to T is called the average velocity of the particle. The following theorem have been proved. 1) The delay potential is a non-increasing function of time, and the delay potential does not change in any limit cycle, and the value of the delay potential is equal to a non-negative integer and does not exceed $2N/3$. 2) If the average velocity of particles is less than 1 for a limit cycle, then the period of the cycle (this period may not be minimal) is equal to $(m + 1)N$. 3) The average velocity of particles is equal to $v = 1 - H/((m + 1)N)$, where H is the potential of delays on the limit cycle. 4) For any m, there exists a value N such that there exists a limit cycle with $H > 0$ and, therefore, $v < 1$.

Keywords: *dynamical system, contour network, limit cycle, potential of delays.*

Введение

В работе рассматривается дискретная динамическая система, относящаяся к классу контурных сетей, появившихся в результате моделирования автотранспортных потоков на сложных улично-дорожных сетях [1, 2] и получивших название сетей Буслаева. Такие контурные сети отражают свойства математических транспортных моделей иметь периодические траектории и конфликтные точки в пересечениях потоков. Благодаря регулярности структуры, исследование динамических систем такого типа позволяет получить содержательные аналитические результаты.

Контурная сеть содержит систему контуров, причём имеются точки, общие для двух или более соседних контуров. Эти общие точки называются узлами. Рассматриваются дискретный и непрерывный варианты контурных сетей. В дискретном варианте каждый контур разбит на ячейки. В любой дискретный момент времени каждая ячейка может быть свободна или в ней находится частица. Рассматриваются дискретные контурные сети с характером движения двух типов. При типе движения, названного индивидуальным, частица на каждом шаге перемещается в направлении движения на одну ячейку, если ячейка впереди свободна, и остаётся на месте, если эта ячейка занята другой частицей. Такое правило движения аналогично правилу движения в исследовавшихся ранее математических моделях трафика, для которых в случае движения по одномерной бесконечной замкнутой решётке были получены аналитические результаты [3, 4]. Транспортная модель с аналогичным типом движения, но осуществляемым на двумерной тороидальной решётке, исследована в [5–8]. Второй тип движения частиц в дискретных кластерных моделях введён в [9] и назван кластерным. При кластерном движении находящиеся в соседних ячейках частицы образуют кластер и эти частицы перемещаются одновременно. Для непрерывных контурных сетей пространство состояний системы и время непрерывны. По контурам непрерывной сети движутся отрезки постоянной длины, которые по аналогии со случаем дискретной системы также называются кластерами. Скорость движения кластера без учёта задержек принимается за единицу. В контурных сетях при прохождении частицами

или кластерами узлов возникают задержки, обусловленные ограничением, в соответствии с которым частицы (кластеры) не могут проходить через узел одновременно. Основной исследуемой характеристикой системы является средняя скорость частиц, представляющая собой среднее расстояние, проходимое частицей в единицу времени. Помимо применения при математическом моделировании трафика, контурные сети могут иметь другие приложения, например они могут использоваться при анализе работы инфокоммуникационных систем.

Одним из типов контурных сетей, для которых получены аналитические результаты, являются замкнутые и открытые цепочки контуров одинаковой длины. В замкнутой цепочке каждый контур соединён узлами с двумя соседними контурами, расположенными слева и справа от данного, причём каждый контур делится узлами на две части равной длины. Открытая цепочка отличается от замкнутой тем, что для крайнего слева и крайнего справа контуров имеется лишь по одному соседнему. Аналитические результаты получены для замкнутых и открытых цепочек, таких, что на каждом контуре имеется лишь один кластер. Поведение открытых цепочек удалось исследовать более полно. В [2] установлено, что для непрерывной открытой цепочки, на каждом контуре которой находится по одному контуру одинаковой для всех кластеров длины, средняя скорость кластера не зависит от начального состояния системы и от того, на каком контуре находится кластер. При длине кластера, не превышающей половины длины контура, начиная с некоторого момента все кластеры движутся без задержек (система попадает в состояние свободного движения, самоорганизация) и, следовательно, скорость кластеров равна 1. При длине кластера больше половины длины контура средняя скорость меньше 1. Найдена формула для значения этой скорости и исследован характер поведения системы на реализующемся предельном цикле, представляющем собой циклическую траекторию в множестве состояний системы.

В [10] рассматривается дискретная открытая цепочка контуров, в которой кластеры различаются по длине. Для случаев, когда длина любого кластера не больше половины длины контура и когда длина любого кластера превышает половину длины контура, получены результаты, аналогичные [2]. В [10] приведены примеры, показывающие, что если имеются как кластеры, длина которых не превышает половину длины контура, так и кластеры длины, большей половины длины контура, то в общем случае средняя скорость кластера может зависеть как от начального состояния системы, так и от номера контура, на котором находится кластер.

В [11–14] исследованы дискретная и непрерывная замкнутые цепочки контуров. В [11] рассмотрена дискретная замкнутая цепочка, на каждом контуре которой имеются две ячейки и одна частица. Доказаны утверждения, подробно описывающие поведение системы, и найден спектр значений средней скорости при различных правилах разрешения конфликта, возникающего в случае, если две частицы соседних контуров пытаются одновременно пересечь общий узел. В частности, для левоприоритетного правила, при котором преимущество всегда предоставляется частице, находящейся на контуре, расположенном слева от узла, спектр скоростей содержит значение 1 и множество значений меньше 1, число которых равно $[N/3]$, где N — число контуров. В [12] исследуется поведение замкнутой цепочки с тремя или двумя контурами. Пусть l — отношение длины кластера к длине контура. Как доказано в [12], при любых значении l и начальном состоянии системы средняя скорость всех кластеров одинакова, при этом для средней скорости v верно следующее: $v = 1$ (самоорганизация), если $l \leqslant 1/6$; $v = 1$ или $4/(3 + 6l)$ в зависимости от начального состояния системы, если $1/6 < l \leqslant 1/2$; $v = 0$ (коллапс, т. е. ни один кластер не перемещается, начиная с некоторого момента),

если $l > 1/2$. При числе контуров, равном двум, поведение системы имеет существенно более простой вид, а именно: система попадает в состояние свободного движения при $l \leqslant 1/2$ и в состояние коллапса при $l > 1/2$. В [13] получены результаты, аналогичные [12], для дискретного варианта замкнутой цепочки с двумя или тремя контурами. В [14] для дискретной замкнутой цепочки, на каждом контуре которой имеются одно и то же чётное число ячеек и одна частица, доказано, что для любого сколь угодно большого числа ячеек на контуре (сколь угодно малой плотности частиц) можно задать число контуров и начальное состояние системы таким образом, что средняя скорость частиц будет меньше 1. В [12] наряду с симметричными цепочками контуров рассмотрены некоторые частные случаи цепочки с несимметричным расположением узлов, т. е. замкнутые и открытые цепочки, в которых узлы делят контур на две неодинаковые по длине части.

В настоящей работе рассматривается дискретная замкнутая цепочка, являющаяся обобщением бинарной замкнутой цепочки с левоприоритетным правилом. На каждом контуре системы имеются чётное число ячеек и одна частица. Располагающиеся на контуре два узла делят контур на части, содержащие одинаковое число ячеек. На каждом такте частица перемещается на ячейку вперёд в направлении движения. Если в некоторый момент времени две частицы находятся перед узлом, то на данном шаге перемещается только частица контура, расположенного слева. Получено необходимое и достаточное условие того, что заданное состояние принадлежит предельному циклу системы. Найдено правило, позволяющее вычислить среднюю скорость частиц, соответствующую этому предельному циклу. Получено правило, которое позволяет вычислить все значения, принадлежащие спектру значений средних скоростей при заданных количествах контуров и ячеек.

В [15] рассматривается динамическая система с дискретным временем и конечным числом состояний, называемая динамической системой ориентаций полного графа. Постановки задач исследования этой системы и относящиеся к ней понятия имеют аналогии с понятиями, возникающими при исследовании контурных сетей. Кроме того, в [15] приводится интерпретация динамической системы с конечным числом состояний в виде полного ориентированного графа. Дискретная контурная сеть является динамической системой с конечным числом состояний, поэтому связанные с этой интерпретацией понятия применимы и к контурным сетям.

1. Описание системы

Пусть система содержит N *контуров,* имеющих номера $i = 0, 1, \ldots, N-1$. На каждом контуре имеются $2m$ *ячеек*, $m \geqslant 1$, и одна *частица.* Частица может перемещаться в дискретные моменты времени $t = 0, 1, 2, \ldots$ Ячейки контура имеют номера $0, 1, \ldots, 2m-1$, они нумеруются в направлении движения частицы (рис. 1).

Будем говорить, что контур i системы находится в состоянии j, если частица находится в ячейке с номером j, $j = 0, 1, \ldots, 2m-1$. Каждый контур имеет два соседних — слева и справа. Для контура i соседним слева является контур $i-1$, справа — $i+1$ (вычитание и сложение по модулю N), $i = 0, 1, \ldots, N-1$. Соседние контуры i, $i+1$ имеют общую точку, называемую узлом $(i, i+1)$ (сложение по модулю N), $i = 0, 1, \ldots, N-1$, причём этот узел располагается между ячейками 0 и 1 на контуре i и между ячейками m и $m+1$ на контуре $i+1$. Если в момент t частица находится в ячейке с номером i, то в момент $t+1$ частица будет находиться в ячейке $i+1$ (сложение по модулю $2m$), если нет задержки в перемещении частицы. Задержки обусловлены невозможностью одновременного прохождения двух частиц через один и тот же общий узел. Если в мо-

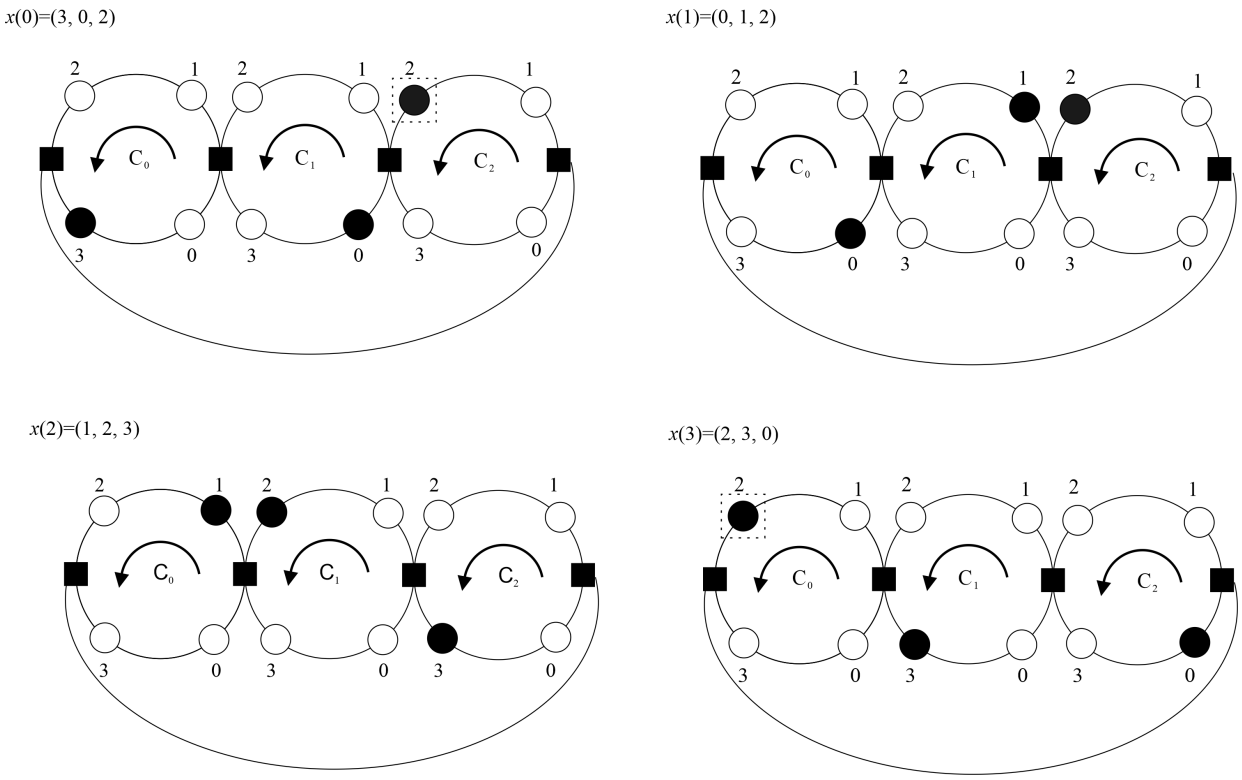


Рис. 1. Замкнутая цепочка при $m = 2$, $N = 3$

мент t частица контура i (*частица* i) находится в ячейке 0, а частица контура $i + 1$ (сложение по модулю N) — в ячейке m, то произойдёт задержка в перемещении частицы $i + 1$, а именно: в момент $t + 1$ частица i будет находиться в 1, а частица $i + 1$ — оставаться в ячейке m, $i = 0, 1, \ldots, N - 1$.

Состояние системы в момент t представляет собой вектор

$$x(t) = (x_0(t), x_1(t), \ldots, x_{N-1}(t)),$$

где $x_i(t)$ — номер ячейки, в которой находится частица i в момент t, $i = 0, 1, \ldots, N - 1$. Начальное состояние $x(0)$ задаётся.

Будем использовать обозначение

$$\Delta_i(t) = x_i(t) - x_{i-1}(t),$$

где вычитание понимается по модулю $2m$, а вычитание в индексе — по модулю N.

Рассматриваемая система относится к классу контурных сетей, называемых *замкнутыми цепочками* контуров. Каждый контур замкнутой цепочки имеет два соседних — слева и справа, в отличие от открытых цепочек, для которых крайний слева и крайний справа контуры имеют только по одному соседнему.

2. Предельные циклы, средняя скорость частиц, состояние свободного движения

Так как система детерминированная и её число состояний конечно, начиная с некоторого момента времени состояния системы периодически повторяются. Пусть T — длительность предельного цикла, т. е. период этого цикла.

Пусть $S_i(t)$ — число перемещений частицы i в интервале времени $(0, t)$. Предел

$$v_i = \lim_{t\to\infty} \frac{S_i(t)}{t}$$

называется средней скоростью частицы i, $i = 0, 1, \ldots, N-1$. Ясно, что этот предел существует и равен отношению числа перемещений частицы i в течение предельного цикла к периоду.

Как доказано в настоящей работе, средняя скорость частицы может зависеть от начального состояния системы, но средние скорости всех частиц одинаковы. Будем обозначать среднюю скорость частиц через v.

Будем говорить, что система находится в момент времени t_0 в состоянии свободного движения, если в любой момент времени $t \geqslant t_0$ все частицы перемещаются. Ясно, что если система попадает в состояние свободного движения, то $v = 1$.

3. Потенциал задержек частиц

Определим функции состояния системы, которые будем называть потенциальной задержкой частицы и потенциалом задержек. Пусть $x = (x_0, x_1, \ldots, x_{N-1})$. Назовём потенциальной задержкой частицы i функцию $h_i(x)$, такую, что $h_i(x) = 0$, если $\Delta_i \neq m$, и $h_i(x) = 1$, если $\Delta_i = m$.

Потенциалом задержек называется функция

$$H(x) = \sum_{i=0}^{N-1} h_i(x).$$

Теорема 1. Для любых t_1, t_2, таких, что $t_1 < t_2$, выполняется неравенство

$$H(x(t_2)) \leqslant H(x(t_1)).$$

Доказательство. Предположим, что момент t_0 — первый момент времени после t_1, такой, что для некоторого i_0 выполняются равенства $h_{i_0}(t_0) = 0$, $h_{i_0}(t_0 + 1) = 1$, т. е. в правой части равенства

$$H(x(t)) = \sum_{i=0}^{N-1} h_i(x(t)) \tag{1}$$

есть слагаемое, которое возрастает при переходе от момента t_0 к моменту $t_0 + 1$. Изменение значения потенциальной задержки частицы i_0 не могло произойти, если обе частицы i_0 и $i_0 - 1$ переместились. Если бы частица i_0 не переместилась, то значение её потенциальной задержки $h_{i_0}(t_0)$ было бы равно 1, что противоречит предположению. Следовательно, не переместилась частица $i_0 - 1$. Но тогда $h_{i_0-1}(t_0) = 1$ и $h_{i_0-1}(t_0 + 1) = 0$. Таким образом, каждому слагаемому в правой части (1), возрастающему на единицу при переходе от момента t_0 к моменту $t_0 + 1$, соответствует убывающее слагаемое с индексом на 1 меньше (вычитание по модулю N). Отсюда следует доказываемое утверждение. ■

Таблица показывает соответствие состояний, разностей Δ_t, потенциалов задержек ($m = 2$, $N = 3$) при начальном состоянии $x(0)$ на рис. 1.

Состояния $x(t) = (x_0(t), x_1(t), x_2(t))$ первых четырёх строк таблицы совпадают с состояниями системы на рис. 1. Видно, что циклический вектор состояния $x(t)$ смещается на одну позицию вправо при увеличении t на $m + 1 = 3$ (см. далее лемму 4) и возвращается к исходному состоянию при увеличении t на $T = (m + 1) N = 9$ — период предельного цикла (см. далее теорему 5).

t	x_0	x_1	x_2	Δ_0	Δ_1	Δ_2	h_0	h_1	h_2	H
0	3	0	2	1	1	2	0	0	1	1
1	0	1	2	2	1	1	1	0	0	1
2	1	2	3	2	1	1	1	0	0	1
3	2	3	0	2	1	1	1	0	0	1
4	2	0	1	1	2	1	0	1	0	1
5	3	1	2	1	2	1	0	1	0	1
6	0	2	3	1	2	1	0	1	0	1
7	1	2	0	1	1	2	0	0	1	1
8	2	3	1	1	1	2	0	0	1	1
$9 = 0$	3	0	2	1	1	2	0	0	1	1

4. Необходимое и достаточное условие пребывания системы в состоянии свободного движения

Теорема 2. Необходимым и достаточным условием того, что система находится в момент времени t в состоянии свободного движения, является равенство $H(x(t)) = 0$.

Доказательство. Задержка частицы i может произойти лишь в случае, если в текущий момент значение потенциальной задержки этой частицы положительно. Но если потенциал задержки в текущий момент равен нулю, то он будет равен нулю и в будущем и, следовательно, задержек не будет. Если потенциал задержек в текущий момент не равен 0, то не позднее чем через время $2m$ произойдёт задержка какой-либо частицы. Таким образом, система не находится в состоянии свободного движения. ■

Теорема 3. Необходимым и достаточным условием того, что состояние системы x принадлежит предельному циклу, которому соответствует скорость частиц, равная 1, является равенство $H(x) = 0$. Период этого предельного цикла равен $2m$.

Доказательство. Если система находится в состоянии свободного движения, то состояние повторяется через $2m$ шагов. Отсюда и из утверждения теоремы 2 получаем утверждение теоремы 3. ■

5. Необходимое и достаточное условие принадлежности состояния предельному циклу со средней скоростью частиц меньше 1

Докажем сначала некоторые леммы.

Лемма 1. Если система не попадает в состояние свободного движения, то происходит бесконечное число задержек каждой частицы.

Доказательство. Предположим, что, начиная с некоторого момента времени t_0, задержки частицы i_0 не происходят. Пусть в некоторый момент t_1 происходит первая после t_0 задержка частицы $i_0 + 1$ (сложение по модулю N). Тогда в момент $t_1 + 1$ потенциальная задержка частицы $i_0 + 1$ будет равна 0. Для того чтобы после момента времени $t_1 + 1$ произошла новая задержка частицы $i_0 + 1$, необходимо, чтобы после этого момента потенциальная задержка частицы i_0+1 снова стала не равной 0. Это возможно лишь в случае, если после момента $t_1 + 1$ произойдёт задержка частицы i_0, что противоречит предположению. Следовательно, после момента t_1 задержек частицы $i_0 + 1$ не происходит. Таким образом, из предположения о конечности числа задержек частицы i_0 следует конечность числа задержек частицы $i_0 + 1$. С помощью индукции получаем, что система попадает в состояние свободного движения, что противоречит условию леммы. ■

Лемма 2. Если в момент времени t_0 система находится в состоянии

$$x(t_0) = (x_0(t_0), x_1(t_0), \ldots, x_{N-1}(t_0)),$$

таком, что для некоторого i_0 выполняются неравенства

$$\Delta_{i_0}(t_0) \neq m - 1; \tag{2}$$

$$\Delta_{i_0}(t_0) \neq m, \tag{3}$$

то существует момент времени $t > t_0$, такой, что в этот момент система попадает в состояние свободного движения или выполняется неравенство $H(x(t)) < H(x(t_0))$.

Доказательство. Если система попадает в состояние свободного движения при некотором $t > t_0$, то $H(x(t)) = 0$ и лемма справедлива. Предположим теперь, что система никогда не попадает в состояние свободного движения. Тогда из леммы 1 следует, что будет бесконечное количество задержек частицы i_0. Возьмём наименьший момент времени $t_1 > t_0$, при котором произойдёт задержка частицы i_0. Но тогда $\Delta_{i_0}(t_1) = m \neq \Delta_{i_0}(t_0)$ и, значит, величина $\Delta_{i_0}(t)$ изменилась при $t_0 \leqslant t < t_1$. У частицы i_0 на этом интервале времени задержек не было, поэтому изменение $\Delta_{i_0}(t)$ вызвано задержками частицы $i_0 - 1$. Возьмём наименьший момент времени $t_2 \in \{t_0, \ldots, t_1\}$, при котором произойдёт задержка частицы $i_0 - 1$. Тогда $h_{i_0-1}(t_2) = 1$, $h_{i_0-1}(t_0 + 1) = 0$ и значение h_{i_0-1} уменьшается. С другой стороны, в силу неравенств (2), (3), обе разности $\Delta_{i_0}(t_2)$ и $\Delta_{i_0}(t_2 + 1) = \Delta_{i_0}(t_2) + 1$ не равны m, поэтому $h_{i_0}(t_2) = h_{i_0}(t_2 + 1) = 0$ и значение h_{i_0} не увеличивается. Из доказательства теоремы 1 следует, что каждому элементу h_i, возрастающему на единицу при переходе от момента t_2 к моменту $t_2 + 1$, соответствует убывающий элемент h_{i-1} (вычитание по модулю N). Следовательно, $H(x(t_2 + 1)) < H(x(t_2)) \leqslant H(x(t_0))$ и для завершения доказательства леммы достаточно взять $t = t_2 + 1$. ■

Лемма 3. Если в момент времени t_0 система находится в состоянии

$$x(t_0) = (x_0(t_0), x_1(t_0), \ldots, x_{N-1}(t_0)),$$

таком, что при некотором i_0 выполняются условия

$$h_{i_0}(t_0) = 1,\ h_{i_0+1}(t_0) = 1, \qquad 1 \leqslant x_{i_0}(t_0) \leqslant m, \tag{4}$$

то для некоторого момента $t > t_0$ выполняется неравенство $H(x(t)) < H(x(t_0))$.

Доказательство. Возьмем наименьший момент времени $t_1 \geqslant t_0$, при котором $x_{i_0}(t_1) = m$. Из (4) следует, что $x_{i_0-1}(t_1) = 0$ и при $t = t_1$ произойдёт задержка частицы i_0. Легко видеть, что обе частицы, расположенные на соседних контурах, при $t \in \{t_0, \ldots, t_1\}$ задержки не имеют, поэтому разности $\Delta_{i_0}(t)$ и $\Delta_{i_0+1}(t)$ изменят свои значения с величины m при $t \leqslant t_1$ до $m - 1$ и $m + 1$ при $t = t_1 + 1$ соответственно. Получаем уменьшение сразу двух соседних элементов: $h_{i_0-1}(t_1 + 1) = 0$, $h_{i_0}(t_1 + 1) = 0$. Используя рассуждения, подобные рассуждениям в лемме 2, получаем требуемое неравенство при $t = t_1 + 1$. ■

Лемма 4. Пусть состояние

$$x(t_0) = (x_0(t_0), x_1(t_0), \ldots, x_{N-1}(t_0))$$

удовлетворяет следующим условиям:

1) значение потенциала задержки $H(x(t_0))$ не равно 0;
2) при любом i выполняется одно из равенств $\Delta_i = m-1$, $\Delta_i = m$;
3) ни для одного i_0 не выполняются одновременно оба условия (3) и (4);
4) не существует значения i_0, такого, что $h_{i_0+1}(t_0) = 1$ и $1 \leqslant x_{i_0}(t_0) \leqslant m-1$.

Тогда за $m+1$ шагов циклический вектор состояния смещается на одну позицию вправо.

Доказательство. Предположим, что выполняются следующие условия:

$$x_{i_0-1}(t_0) = k-m+1,\ x_{i_0} = k,\ x_{i_0+1} = k+m-1$$

(вычитание и сложение по модулю $2m$). Тогда в момент t_0+m+1 частица i_0+1, совершив $m+1$ перемещений, оказывается в ячейке с номером k. Таким образом, $x_{i_0+1}(t_0+m+1) = x_{i_0}(t_0)$.

Пусть выполняются условия

$$x_{i_0-1} = k-m+1,\ x_{i_0} = k,\ x_{i_0+1} = k+m,\ m+1 \leqslant x_0 \leqslant 2m-1$$

(вычитание и сложение по модулю $2m$). Тогда в момент t_0+m+1, совершив m перемещений, частица i_0 оказывается в ячейке с номером k.

Пусть выполняются условия

$$x_{i_0-1} = m+1,\ x_{i_0} = 0,\ x_{i_0+1} = m.$$

Тогда в момент t_0+m+1, совершив $m+1$ перемещений, частица i_0+1 оказывается в ячейке с номером 0.

Пусть выполняются условия

$$x_{i_0-1} = m,\ x_{i_0} = 0,\ x_{i_0+1} = m.$$

Тогда в момент t_0+m+1, совершив m перемещений, частица i_0+1 оказывается в ячейке с номером 0.

Таким образом, учитывая леммы 1 и 2, получаем, что при выполнении условия леммы верны равенства

$$x_{i+1}(t_0+m+1) = x_i(t_0),\ i = 0, 1, \ldots, N-1$$

(сложение в индексе по модулю N). ■

Следствием леммы 4 является следующая

Теорема 4. Состояние системы, удовлетворяющее лемме 4, принадлежит предельному циклу с периодом, являющимся делителем числа $(m+1)N$, и со средней скоростью, меньшей 1.

Лемма 5. Если состояние системы x удовлетворяет условиям 1–3 леммы 4, но не удовлетворяет условию 4 леммы 4, то это состояние не принадлежит предельному циклу.

Доказательство. Как можно убедиться, при выполнении условия леммы 5 система не более чем за m шагов попадает в состояние предельного цикла, удовлетворяющего условию леммы 4, откуда следует утверждение леммы 5. ■

Из теоремы 4 и лемм 2, 3 и 5 получаем следующее утверждение:

Теорема 5. Состояние системы принадлежит предельному циклу со средней скоростью, меньшей 1, в том и только в том случае, если это состояние удовлетворяет условию леммы 4. Период этого предельного цикла является делителем $(m+1)N$.

Таким образом, период предельного цикла не превышает $(m+1)N$ и в общем случае при некоторых начальных состояниях может быть меньше $(m+1)N$.

6. Формула для средней скорости частиц

Лемма 6. Состояниям, принадлежащим одному и тому же предельному циклу, соответствует одно и то же значение потенциала задержек.

Лемма 6 является следствием теоремы 1.

Теорема 6. Пусть H — значение потенциала задержек, соответствующее предельному циклу. Тогда этому предельному циклу соответствует средняя скорость частиц v, вычисляемая по формуле

$$v = 1 - \frac{H}{(m+1)N}. \tag{5}$$

Доказательство. Если $H = 0$, то в соответствии с теоремой 2 имеем $v = 1$. Пусть $H \geqslant 1$. Предположим, что в момент времени t_0 происходит задержка частицы i_0. В этот момент частица i_0 находится в ячейке m, а частица i_0+1, в соответствии с теоремой 5, — в ячейке $2m-1$. В момент t_0+1 (сложение по модулю N) потенциальная задержка частицы i_0 меняет значение 1 на значение 0, а потенциальная задержка частицы i_0+1 — значение 0 на значение 1. В этот момент частица i_0+1 будет находиться в ячейке 0, а частица i_0 по-прежнему в ячейке m. В момент времени t_0+m+1 частица i_0 окажется в ячейке 0, а частица i_0+1 — в ячейке m. Произойдёт задержка частицы i_0+1 и значение 1 потенциальной задержки частицы i_0+1 перейдёт частице i_0+2. Таким образом, на каждых последовательных $m+1$ тактах задерживаются один раз H из N частиц, откуда следует утверждение теоремы 6. ■

7. Спектр скоростей частиц

Для того чтобы при заданных значениях N и m найти множество возможных значений средней скорости при различных начальных состояниях систем, нужно, в соответствии с теоремой 6, найти возможные значения H и для каждого такого значения проверить, существуют ли векторы состояния со значениями H, удовлетворяющими условию леммы 4.

Теорема 7. Необходимым условием существования предельного цикла с потенциалом задержек, равным H, является выполнение следующих соотношений:

$$\begin{gathered} 1 \leqslant H \leqslant \frac{2N}{3}, \\ Nm - N + H = 2m, \end{gathered} \tag{6}$$

где равенство (6) понимается по модулю $2m$.

Доказательство. Из леммы 4 следует, что для существования предельного цикла с потенциалом задержек, равным H, необходимо выполнение условия (5) и равенства

$$Hm + (N-H)(m-1) = 2m$$

по модулю $2m$, равносильного равенству (6). ■

8. Бинарная замкнутая цепочка

Предположим, что $m = 1$. Тогда, применив изложенное в п. 3 правило нахождения значений потенциала задержек, таких, что эти значения соответствуют предельным циклам, имеем $H = 0, 2, 4, \ldots, 2\,[N/3]$. Отсюда, используя формулу (5), в которой полагаем $m = 1$, получаем, что спектр скоростей содержит $[N/3] + 1$ значений $v = 1 - k/N$, $k = 0, 1, \ldots, \left[\frac{N}{3}\right]$, что соответствует результатам работы [11].

Заключение

Проведено исследование дискретной динамической системы, принадлежащей классу контурных сетей Буслаева. Эта система представляет собой замкнутую цепочку контуров, на каждом из которых имеется чётное число ячеек и одна частица.

Найдены предельные циклы системы с соответствующими им значениями средней скорости движения частиц. Найдено правило, позволяющее найти множество возможных значений средней скорости при различных состояниях системы и заданных числе контуров и числе ячеек на контуре. Введено понятие потенциала задержки, которое используется при анализе поведения системы. Потенциал задержек представляет собой невозрастающую во времени функцию состояния системы, которая постоянна на предельном цикле и равна нулю лишь в случае, когда система находится в состоянии свободного движения, т. е. когда на предельном цикле все частицы движутся без задержек.

ЛИТЕРАТУРА

1. *Kozlov V. V., Buslaev A. P., and Tatashev A. G.* On synergy of totally connected flows on chainmails // Proc. Intern. Conf. CMMSE. 2013. V. 3. P. 861–874.
2. *Buslaev A. P. and Tatashev A. G.* Spectra of local cluster flows on open chain of contours // Europ. J. Pure Appl. Math. 2018. V. 11. No. 3. P. 628–641.
3. *Бланк М. Л.* Точный анализ динамических систем, возникающих в моделях транспортных потоков // Успехи математических наук. 2000. Т. 55. № 3(333). С. 167–168.
4. *Belitsky V. and Ferrari P. A.* Invariant measures and convergence properties for cellular automation 184 and related processes // J. Stat. Phys. 2005. V. 118. No. 3/4. P. 589–623.
5. *Biham O., Middleton A. A., and Levine D.* Self-organization and a dynamic transition in traffic-flow models // Phys. Rev. A. 1992. V. 46. No. 10. P. R6124–R6127.
6. *D'Souza R. M.* Coexisting pases and lattice dependence of a cellular automaton model for traffic flow // Phys. Rev. E. 2005. V. 71. No. 6:066112.
7. *Angel O., Horloyd A. E., and Martin J. B.* The jammed phase of the Biham — Middelton — Levine traffic model // Elec. Commun. Probability. 2005. V. 10.
8. *Austin D. and Benjamini I.* For what number of cars must self organization occur in the Biham — Middleton — Levine traffic model from any possible starting configuration? arXiv preprint math/0607759. 2006.
9. *Bugaev A. S., Buslaev A. P., Kozlov V. V., and Yashina M. V.* Distributed problems of monitoring and modern approaches to traffic modeling // 14th Intern. IEEE Conf. ITSC. 2011. P. 477–481.
10. *Buslaev A. P. and Tatashev A. G.* Spectra of local cluster flows on open chain of contours // 7th Intern. Conf. ICCMA. 2019. P. 283–288.
11. *Kozlov V. V., Buslaev A. P., and Tatashev A. G.* Monotonic walks on a necklace and a coloured dynamic vector // Int. J. Comput. Math. 2015. V. 92. No. 9. P. 1910–1920.
12. *Buslaev A. P., Tatashev A. G., and Yashina M. V.* Flows spectrum on closed trio of contours // Europ. J. Pure Appl. Math. 2018. V. 11. No. 1. P. 260–283.

13. *Buslaev A. P., Fomina M. Yu., Tatashev A. G., and Yashina M. V.* On discrete flow networks model spectra: statement, simulation, hypotheses // J. Physics: Conf. Ser. 2018. V. 1053. No. 012034. P. 1–7.
14. *Tatashev A. G. and Yashina M. V.* Spectrum of elementary cellular automata and closed chains of contours // Machines. 2019. V. 7. No. 2. P. 28.
15. *Жаркова А. В.* О количестве недостижимых состояний в конечных динамических системах ориентаций полных графов // Прикладная дискретная математика. Приложение. 2020. № 13. С. 100–103.

REFERENCES

1. *Kozlov V. V., Buslaev A. P., and Tatashev A. G.* On synergy of totally connected flows on chainmails. Proc. Intern. Conf. CMMSE, 2013, vol. 3, pp. 861–874.
2. *Buslaev A. P. and Tatashev A. G.* Spectra of local cluster flows on open chain of contours. European J. Pure Appl. Math., 2018, vol. 11, no. 3, pp. 628–641.
3. *Blank M. L.* Exact analysis of dynamical systems arising in models of traffic flow. Russian Math. Surveys, 2000, vol. 55, no. 3, pp. 562–563.
4. *Belitsky V. and Ferrari P. A.* Invariant measures and convergence properties for cellular automation 184 and related processes. J. Stat. Phys., 2005, vol. 118, no. 3/4, pp. 589–623.
5. *Biham O., Middleton A. A., and Levine D.* Self-organization and a dynamic transition in traffic-flow models. Phys. Rev. A, 1992, vol. 46, no. 10, R6124–R6127.
6. *D'Souza R. M.* Coexisting pases and lattice dependence of a cellular automaton model for traffic flow. Phys. Rev. E, 2005, vol. 71, no. 6, 066112.
7. *Angel O., Horloyd A. E., and Martin J. B.* The jammed phase of the Biham — Middelton — Levine traffic model. Elec. Commun. Probability, 2005, vol. 10.
8. *Austin D. and Benjamini I.* For what number of cars must self organization occur in the Biham — Middleton — Levine traffic model from any possible starting configuration? arXiv preprint math/0607759, 2006.
9. *Bugaev A. S., Buslaev A. P., Kozlov V. V., and Yashina M. V.* Distributed problems of monitoring and modern approaches to traffic modeling. 14th Intern. IEEE Conf. ITSC, 2011, pp. 477–481.
10. *Buslaev A. P. and Tatashev A. G.* Spectra of local cluster flows on open chain of contours. 7th Intern. Conf. ICCMA, 2019, pp. 283–288.
11. *Kozlov V. V., Buslaev A. P., and Tatashev A. G.* Monotonic walks on a necklace and a coloured dynamic vector. Int. J. Comput. Math., 2015, vol. 92, no. 9, pp. 1910–1920.
12. *Buslaev A. P., Tatashev A. G., and Yashina M. V.* Flows spectrum on closed trio of contours. Europ. J. Pure Appl. Math., 2018, vol. 11, no. 1, pp. 260–283.
13. *Buslaev A. P., Fomina M. Yu., Tatashev A. G., and Yashina M. V.* On discrete flow networks model spectra: statement, simulation, hypotheses. J. Physics: Conf. Ser., 2018, vol. 1053, no. 012034, pp. 1–7.
14. *Tatashev A. G. and Yashina M. V.* Spectrum of elementary cellular automata and closed chains of contours. Machines, 2019, vol. 7, no. 2, p. 28.
15. *Zharkova A. V.* O kolichestve nedostizhimykh sostoyaniy v konechnykh dinamicheskikh sistemakh orientatsiy polnykh grafov [On number of inaccessible states in finite dynamic systems of complete graphs orientations]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2020, no. 13, pp. 100–103. (in Russian)

СВЕДЕНИЯ ОБ АВТОРАХ

АБРОСИМОВ Михаил Борисович — доктор физико-математических наук, доцент, зав. кафедрой Саратовского национального исследовательского государственного университета имени Н. Г. Чернышевского, г. Саратов. E-mail: **mic@rambler.ru**

БУХАНОВ Дмитрий Геннадьевич — старший преподаватель кафедры программного обеспечения вычислительной техники и автоматизированных систем Белгородского государственного технологического университета им. В. Г. Шухова, г. Белгород. E-mail: **db.old.stray@gmail.com**

ДЕВЯНИН Петр Николаевич — доктор технических наук, профессор, член-корреспондент Академии криптографии Российской Федерации, научный руководитель ООО «РусБИТех-Астра», г. Москва. E-mail: **pdevyanin@astralinux.ru**

КОСТИН Сергей Вячеславович — старший преподаватель МИРЭА — Российского технологического университета, г. Москва. E-mail: **kostinsv77@mail.ru**

ЛЕОНОВА Мария Александровна — старший научный сотрудник ООО «РусБИТех-Астра», г. Москва. E-mail: **mleonova@astralinux.ru**

ЛОСЬ Илья Викторович — аспирант Саратовского государственного национального исследовательского государственного университета имени Н. Г. Чернышевского, г. Саратов. E-mail: **los.ilia.ru@gmail.com**

МОСКИН Николай Дмитриевич — кандидат технических наук, доцент, доцент кафедры информатики и математического обеспечения Петрозаводского государственного университета, г. Петрозаводск. E-mail: **moskin@petrsu.ru**

МЫШКИС Петр Анатольевич — кандидат физико-математических наук, доцент, доцент Московского автомобильно-дорожного государственного технического университета (МАДИ), г. Москва. E-mail: **p.myshkis@yandex.ru**

ПОЛЯКОВ Владимир Михайлович — кандидат технических наук, доцент, проректор по образовательной деятельности Белгородского государственного технологического университета им. В. Г. Шухова, г. Белгород. E-mail: **p_v_m@mail.ru**

РЕДЬКИНА Маргарита Александровна — студентка кафедры программного обеспечения вычислительной техники и автоматизированных систем Белгородского государственного технологического университета им. В. Г. Шухова, г. Белгород.
E-mail: **redckina.rit@mail.ru**

РОМАНЬКОВ Виталий Анатольевич — доктор физико-математических наук, профессор, заведующий кафедрой Омского государственного университета им. Ф. М. Достоевского, главный научный сотрудник Института математики им. С. Л. Соболева СО РАН (Омский филиал), г. Омск. E-mail: **romankov48@mail.ru**

СЕЛИВЕРСТОВ Александр Владиславович — кандидат физико-математических наук, ведущий научный сотрудник Института проблем передачи информации им. А. А. Харкевича Российской академии наук, г. Москва. E-mail: **slvstv@iitp.ru**

ТАТАШЕВ Александр Геннадьевич — доктор физико-математических наук, доцент, профессор Московского автомобильно-дорожного государственного технического университета (МАДИ), г. Москва. E-mail: **a-tatashev@yandex.ru**

ЯШИНА Марина Викторовна — доктор технических наук, кандидат физико-математических наук, доцент, зав. кафедрой Московского автомобильно-дорожного государственного технического университета (МАДИ), г. Москва.
E-mail: **mv.yashina@madi.ru**

KISS Rebeka — Bolyai Institue, University of Szeged, Szeged.
E-mail: **Kiss.Rebeka@stud.u-szeged.hu**

NAGY Gábor Péter — Bolyai Institue, University of Szeged, Szeged; Department of Algebra, Budapest University of Technology and Economics, Budapest.
E-mail: **nagyg@math.bme.hu**

Журнал «Прикладная дискретная математика» входит в перечень ВАК рецензируемых научных изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание учёной степени кандидата и доктора наук по специальностям 01.01.06 — «Математическая логика, алгебра и теория чисел», 01.01.09 — «Дискретная математика и математическая кибернетика», 05.13.11 — «Математическое и программное обеспечение вычислительных машин,комплексов и компьютерных сетей», 05.13.17 — «Теоретические основы информатики», 05.13.19 — «Методы и системы защиты информации, информационная безопасность», а также в перечень журналов, рекомендованных ФУМО ВО ИБ в качестве учебной литературы по специальности «Компьютерная безопасность».

Журнал индексируется в базах данных Web of Science (Emerging Sources Citation Index (ESCI) и Russian Science Citation Index (RSCI)), Scopus, MathSciNet и Zentralblatt MATH.

Журнал «Прикладная дискретная математика» распространяется по подписке; его подписной индекс 38696 в объединённом каталоге «Пресса России». Полнотекстовые электронные версии вышедших номеров журнала доступны на его сайте journals.tsu.ru/pdm и на Общероссийском математическом портале www.mathnet.ru. На сайте журнала можно найти также правила подготовки рукописей статей для публикации в журнале.

Тематика публикаций журнала:

- *Теоретические основы прикладной дискретной математики*
- *Математические методы криптографии*
- *Математические методы стеганографии*
- *Математические основы компьютерной безопасности*
- *Математические основы надёжности вычислительных и управляющих систем*
- *Прикладная теория кодирования*
- *Прикладная теория автоматов*
- *Прикладная теория графов*
- *Логическое проектирование дискретных автоматов*
- *Математические основы информатики и программирования*
- *Вычислительные методы в дискретной математике*
- *Дискретные модели реальных процессов*
- *Математические основы интеллектуальных систем*
- *Исторические очерки по дискретной математике и её приложениям*