На правах рукописи

Рыбалов Александр Николаевич

ГЕНЕРИЧЕСКИЙ ПОДХОД К АЛГОРИТМИЧЕСКИМ ПРОБЛЕМАМ

01.01.06 – математическая логика,
алгебра и теория чисел

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
доктора физико-математических наук

Омск 2018

Работа выполнена в Федеральном государственном бюджетном учреждении науки Институте математики им. С. Л. Соболева Сибирского отделения Российской академии наук.

Научный консультант:
Ремесленников Владимир Никанорович, доктор физико-математических наук, профессор.

Официальные оппоненты:
Бадаев Серикжан Агыбаевич, доктор физико-математических наук, профессор, Казахский национальный университет им. аль-Фараби, профессор кафедры фундаментальной математики.
Добрица Вячеслав Порфирьевич, доктор физико-математических наук, профессор, Федеральное государственное бюджетное образовательное учреждение высшего образования «Юго-Западный государственный университет», профессор кафедры информационной безопасности.
Фролов Андрей Николаевич, доктор физико-математических наук, доцент, Федеральное государственное автономное образовательное учреждение высшего образования «Казанский (Приволжский) федеральный университет», старший научный сотрудник Института математики и механики им. Н.И.Лобачевского.

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования Новосибирский государственный технический университет.

Защита состоится 24 ноября 2018г. в 11:00 на заседании диссертационного совета Д 003.015.02 при Институте математики им. С.Л. Соболева СО РАН по адресу г. Новосибирск, пр. акад. Коптюга 4.

С диссертацией можно ознакомиться в библиотеке Федерального государственного бюджетного учреждения науки Института математики им. С.Л.Соболева Сибирского отделения Российской академии наук и на сайте http://math.nsc.ru.

Автореферат разослан _ сентября 2018.

Учёный секретарь диссертационного совета
кандидат физ.-мат. наук, доцент, Стукачев А.И.

Актуальность темы. Диссертация посвящена генерическому подходу к вычислимости и вычислительной сложности алгоритмических проблем — новому направлению исследований, возникшему на стыке теории вычислимости, теории сложности вычислений и комбинаторной алгебры.

Генерический подход был предложен в 2003 году И.Каповичем, А.Г.Мясниковым, В.Шпильрайном и П.Шуппом в работе [61]. В рамках этого подхода изучается поведение алгоритмов на множестве «почти всех» входов (это множество называется генерическим), игнорируя поведение алгоритма на остальных входах, на которых алгоритм может работать медленно или вообще не останавливаться. Такой подход имеет приложения в криптографии, где требуется, чтобы алгоритмические проблемы были трудными для «почти всех» входов. Понятие «почти все» формализуется введением асимптотической плотности на множестве входных данных I: для подмножества $S \subseteq I$ определяется последовательность

$$\rho_n(S) = \frac{|S_n|}{|I_n|},\ n = 1, 2, 3, \ldots,$$

где I_n – множество входов размера n, а $S_n = S \cap I_n$ – множество входов из S размера n. *Асимптотической плотностью* S называется предел (если он существует)

$$\rho(S) = \lim_{n\to\infty} \rho_n(S).$$

Множество S называется *генерическим*, если $\rho(S) = 1$, и *сильно генерическим*, если последовательность $\rho_n(S)$ экспоненциально быстро сходится к 1. С точки зрения практики, алгоритмы, решающие быстро проблему на генерическом множестве, так же хороши, как и быстрые алгоритмы для всех входов. Классическим примером такого алгоритма является симплекс-метод: В. Кли и Г. Минти показали [65], что этот алгоритм имеет экспоненциальную сложность в худшем случае, но А. М. Вершик и П. В. Спорышев [22, 23] и, независимо от них, С. Смейл [80] доказали, что он за полиномиальное время решает задачу линейного программирования для большинства входных данных. В теории сложности вычислений поведение алгоритмов на множестве «почти всех» входов традиционно изучается в рамках подхода к сложности в среднем [47, 67, 33, 81], при этом время работы алгоритма усредняется по всему множеству входных данных. В отличие от сложности в среднем, генерический подход является более универсальным, так как может оказаться, что на множестве «плохих» входов даже усредненное время работы алгоритма неполиномиально. В то же время генерический алгоритм просто игнорирует эти входы. Более того, генерический подход применим также и к алгоритмически неразрешимым проблемам. Таким образом, может оказаться, что проблема

трудноразрешима или вообще неразрешима в классическом смысле, но легкоразрешима в генерическом смысле. В работах А. Г. Мясникова, В. Н. Ремесленникова, А. В. Боровика, В. А. Романькова, П. Шуппа, Р. Гилмана, В. Дикерта, М. Камбитеса и др. [61, 34, 35, 40, 41, 46, 52, 60, 62, 71, 72, 73] было доказано, что таким поведением обладают многие алгоритмически неразрешимые проблемы алгебры и теории алгоритмов. Для многих классических NP-полных и трудноразрешимых проблем полиномиальные генерические алгоритмы были предложены в работах П. Эрдеша, Л. Бабаи, Р. Карпа, Ю. Гуревича, С. Шелаха, Э. Х. Гимади, Н. И. Глебова, В. А. Перепелицы и др. [4, 44, 48, 28, 63].

В тоже время, большой интерес как с теоретической точки зрения, так и с точки зрения практических приложений, представляют алгоритмические проблемы, которые остаются неразрешимыми или трудноразрешимыми и в генерическом случае. Например, в современной криптографии интересны такие проблемы, которые, являясь (гипотетически) трудными в классическом смысле, остаются трудными и в генерическом смысле, т.е. для почти всех входов. Это объясняется тем, что при случайной генерации ключей в криптографическом алгоритме происходит генерация входа некоторой трудной алгоритмической проблемы, лежащей в основе алгоритма. Если проблема будет генерически легкоразрешимой, то для почти всех таких входов ее можно будет быстро решить и ключи почти всегда будут нестойкими. Поэтому проблема должна быть генерически трудной.

А. Г. Мясников и Дж. Хэмкинс в [52] доказали, что проблема остановки для машин Тьюринга с лентой, бесконечной в одну сторону, проблема остановки является генерически разрешимой. Там же ими была поставлена следующая проблема.

Проблема 1. *Является ли проблема остановки для машин Тьюринга с лентой, бесконечной в обе стороны, генерически разрешимой?*

В данной диссертации доказывается, что проблема остановки неразрешима на сильно генерических множествах входов. Также доказывается ее генерическая неразрешимость для так называемых нормализованных машин Тьюринга. В программе нормализованной машины Тьюринга из любого нефинального состояния q_i в соответствующих ему правилах в программе возможен переход в состояния q_j, где $j \leq mi + 1$, где m – размер рабочего алфавита. Смысл этого ограничения соответствует процессу экономного написания программы: начиная с первого правила, в каждом очередном новом правиле можно либо переходить в одно из старых состояний, либо в одно новое. Это ограничение никак не уменьшает множество вычислимых функций. Полученные результаты верны для машин с лентой, бесконечной и в одну сторону, и

в обе. Первый результат в частности говорит о том, что генерический алгоритм Мясникова-Хэмкинса нельзя сделать сильно генерическим. Из второго результата следует, что алгоритм Мясникова-Хэмкинса не является генерическим для нормализованных машин. В качестве приложения развитой техники, доказывается генерический аналог теоремы Клини о неподвижной точке [66, 1]. Отметим, что проблема остановки изучалась также и в рамках других подходов Г. Чейтиным, К. Калуде, А. Шенем и др. [31, 36, 37].

Классические примеры конечно определенных полугрупп с алгоритмически неразрешимой проблемой равенства слов были построены А. А. Марковым [10], Э. Постом [75], Г. С. Цейтиным [25], Ю. В. Матиясевичем [11]. Однако, как было показано М. Камбитесом [60], проблема равенства слов в этих полугруппах генерически разрешима за полиномиальное время. Причина этого явления состоит в том, что при интерпретации какой-либо неразрешимой проблемы (например, проблемы остановки для машин Тьюринга) внутри данной конечно определенной полугруппы, привносится много «мусора» в виде вспомогательных порождающих и определяющих соотношений для моделирования вычислений машин Тьюринга, что делает проблему равенства легкоразрешимой для большинства входов. Возникает следующая естественная проблема.

Проблема 2. *Существуют ли конечно определенные полугруппы с генерически неразрешимой проблемой равенства слов?*

В данной диссертации строятся примеры таких полугрупп. Остается открытым вопрос о существовании конечно определенной группы с генерически неразрешимой проблемой равенства слов. Р. Гилман, А. Г. Мясников и Д. Осин [45] построили пример конечно определенной группы с проблемой равенства слов, неразрешимой на сильно генерических подмножествах. Используя неравенство Голода-Шафаревича, А. Г. Мясников и Д. Осин [69] построили конечно порожденную группу с рекурсивным множеством определяющих соотношений, проблема равенства слов в которой генерически неразрешима. А. Г. Мясников и Б. Хуссаинов в [64] построили пример рекурсивно определенной группы с проблемой равенства слов, неразрешимой на множествах ненулевой асимптотической плотности.

В 1970 году Ю. В. Матиясевич, основываясь на работах М. Девиса, Дж. Робинсон и Х. Патнема, доказал [12], что 10-я проблема Гильберта алгоритмически неразрешима, то есть не существует алгоритма, который по любому диофантовому уравнению определяет, разрешимо ли оно в целых числах В дальнейшем, Ю. В. Матиясевич и Дж. Робинсон в [68] показали, что десятая проблема Гильберта неразрешима для диофантовых уравнений с числом неизвестных $m \leq 13$. Д. Джонс в [56] снизил эту границу до 9. Б. Пунен и

Д. Ф. Волох [74] изучили разрешимость «случайных» диофантовых уравнений над рациональными числами для некоторых естественных представлений. А. Г. Мясников и В. А. Романьков [70, 18, 19] показали, что основные функции шифрования многих криптографических систем с открытым ключом, среди которых система RSA и системы, основанные на трудноразрешимости проблемы дискретного логарифма, записываются на языке диофантовых уравнений. Эффективная генерическая разрешимость этих уравнений приводит к взлому соответствующих систем, поэтому важной является следующая проблема.

Проблема 3. *Является ли проблема разрешимости диофантовых уравнений генерически (легко) разрешимой?*

В диссертации эта проблема изучается для двух представлений диофантовых уравнений: с помощью арифметических схем и с помощью систем Сколема [79].

Большой пласт алгоритмических проблем связан с элементарными теориями различных алгебраических систем – см. прекрасный обзор Ю. Л. Ершова, И. А. Лаврова, А. Д. Тайманова и М. А. Тайцлина [6]. Как правило, эти теории либо неразрешимы, либо имеют очень большую вычислительную сложность в худшем случае. М. Рабин и М. Фишер [49] доказали, что любой алгоритм, разрешающий теорию натуральных чисел с операцией сложения (так называемая арифметика Пресбургера), имеет как минимум дважды экспоненциальную сложность от длины формулы. Более точно: для любого алгоритма $\mathcal{A}$, распознающего арифметику Пресбургера, существует формула Φ длины n такая, что алгоритм $\mathcal{A}$ работает на формуле Φ за время, большее 2^{2^n}. К проблемам разрешимости элементарных теорий непосредственно примыкает знаменитая теорема Гёделя о неполноте [51, 3], которая утверждает, что если формальная арифметика непротиворечива, то она неполна, то есть в ней существует недоказуемое и неопровержимое утверждение. Возникает вопрос, а если ограничиться не всеми утверждениями, а «почти всеми», что можно сказать о такой генерической полноте формальной арифметики?

Проблема 4.

1. *Существуют ли неразрешимые элементарные теории, которые являются генерически разрешимыми?*
2. *Будет ли арифметика Пресбургера генерически разрешимой за полиномиальное время?*
3. *Существует ли генерическое множество замкнутых арифметических формул, для любой из которых либо сама формула, либо ее отрицание*

выводимо из аксиом формальной арифметики (при условии ее непротиворечивости)?

В диссертации дается отрицательное решение всех пунктов этой проблемы для естественного представления формул первого порядка с помощью бинарных деревьев. Также в диссертации изучаются вопросы о генерической трудноразрешимости следующих классических алгоритмических проблем: проблема выполнимости булевых формул, проблемы дискретного логарифма, проблемы извлечения корня в группах вычетов, проблемы поиска изоморфизма графов, проблемы распознавания квадратичных вычетов. Для получения всех результатов о генерической неразрешимости и трудноразрешимости был предложен метод генерической амплификации.

В 2012 г. К. Джокуш и П. Шупп [55] начали изучение классической теории вычислимости в рамках генерического подхода. В частности, они ввели понятие грубой вычислимости, когда алгоритм может ошибаться на пренебрежимом множестве входов. Также они изучили связь между генеричностью и такими классическими понятиями теории вычислимости, как иммунность, би-иммунность, гипериммунность и др. Кроме того, ими были введены аналоги тьюринговой сводимости для генерической вычислимости. Эта статья привлекла внимание специалистов по теории вычислимости к генерическому подходу и вызвала большое количество публикаций К. Джокуша, С. Лемпа, Р. Доуни, Д. Диамондстоуна, Д. Хиршфельда, Э. Астора, П. Чолака, Г. Игусы и др. [26, 27, 30, 31, 38, 42, 43, 53, 54, 57, 58], посвященных генерической теории вычислимости. Также в этой статье была поставлена следующая проблема.

Проблема 5. *Какова структура степеней (в том числе, рекурсивно перечислимых) генерической сводимости? В частности, существуют ли минимальные степени, минимальные пары для генерической сводимости?*

В работах П. Чолака и Г. Игусы [38, 57, 58] были изучены проблемы существования минимальных степеней (не обязательно рекурсивно перечислимых) и минимальных пар относительно генерической сводимости и было дано условное решение этой проблемы по модулю некоторого утверждения о структуре степеней генерической сводимости. В данной диссертации вводятся несколько новых типов генерических сводимостей. Изучается структура рекурсивно перечислимых степеней относительно этих сводимостей, в частности, доказывается несуществование минимальных рекурсивно перечислимых генерических степеней.

Важнейшим понятием классической теории сложности вычислений является понятие полиномиальной сводимости алгоритмических проблем. С его

помощью можно сравнивать проблемы по вычислительной сложности и развивать богатую теорию NP-полноты [5]. Л. Левин [67] ввел понятие полиномиальной сводимости и NP-полноты в среднем. Ю. Гуревич [47] построил примеры алгоритмических проблем, которые являются NP-полными в среднем. В данной диссертации вводится полиномиальная генерическая сводимость, определяются генерические классы P и NP, строятся примеры генерически NP-полных проблем.

Т. Бейкер, Дж. Гилл и Р. Соловей в 1975 г. доказали [29], что существуют два оракула A и B такие, что $\mathrm{P}^A = \mathrm{NP}^A$, но $\mathrm{P}^B \neq \mathrm{NP}^B$. Тем самым, они показали, что неравенство $\mathrm{P} \neq \mathrm{NP}$ не может быть доказано с использованием метода диагонализации: если с помощью диагонализации доказано неравенство каких-либо классов алгоритмических проблем $C_1 \neq C_2$, то для любого оракула A неравенство $C_1^A \neq C_2^A$ будет также верно (принцип релятивизации). В связи с этим представляет интерес следующая проблема.

Проблема 6. *Является ли генерический аналог проблемы о равенстве классов вычислительной сложности P и NP «проще» классической проблемы P vs NP? Можно ли использовать диагонализацию для доказательства неравенства генерических аналогов классов P и NP?*

В диссертации доказывается генерический аналог теоремы Бейкера-Гилла-Соловея, который, как и классическая теорема Бейкера-Гилла-Соловея, говорит о том, что «традиционнные» методы теории вычислимости, типа диагонализации, эту проблему не решают.

Основные результаты. На защиту выносятся следующие результаты (ниже в виде ссылок указаны работы, где был опубликован соответствующий результат).

1. Предложен метод генерической амплификации алгоритмических проблем [84]. С его помощью получены следующие результаты:
   (a) Доказана генерическая неразрешимость проблемы остановки для машин Тьюринга [83, 95].
   (b) Доказана генерическая неразрешимость десятой проблемы Гильберта [87, 88, 99].
   (c) Доказана генерическая неразрешимость элементарных теорий, неразрешимых в классическом смысле [84, 86, 92].
   (d) Построен пример полугруппы с генерически неразрешимой проблемой равенства слов [84].

(e) Доказано, что арифметика Пресбургера генерически неразрешима за экспоненциальное время [85].

(f) Доказано, что проблема выполнимости булевых формул генерически неразрешима за полиномиальное время при условии $P \neq NP$ и $P = BPP$ [100].

(g) Доказана генерическая трудноразрешимость проблемы распознавания квадратичных вычетов [90], проблемы дискретного логарифма [93], проблемы извлечения корня в группах вычетов [102], проблемы поиска изоморфизма графов [91], при условии трудноразрешимости этих проблем в худшем случае.

(h) Доказан генерический аналог теоремы Гёделя о неполноте формальной арифметики [89, 97].

(i) Доказан генерический аналог теоремы Клини о неподвижной точке [98].

2. Изучен вопрос о границах применимости метода генерической амплификации: построен пример генерически неразрешимой проблемы, которая не может быть получена с помощью генерической амплификации из неразрешимой в худшем случае проблемы [104]; доказано, что любое рекурсивно перечислимое множество положительной асимптотической плотности может быть получено генерической амплификацией множества натуральных чисел [104]. Доказано существование абсолютно неразрешимых проблем, которые неразрешимы на любом множестве ненулевой асимптотической плотности [84].

3. Предложены генерические аналоги сводимостей алгоритмических проблем: gm-сводимость [105], генерическая клонирующая сводимость [94], генерическая тьюрингова сводимость [104]. Изучена структура рекурсивно перечислимых степеней относительно генерической тьюринговой сводимости: доказано существование полных степеней [104], доказано существование несравнимых степеней (аналог теоремы Мучника-Фридберга) [104], отсутствие минимальных и максимальных неполных степеней [104], доказан генерический аналог классической теоремы Сакса о разложении [104].

4. Предложен генерический аналог полиномиальной сводимости [96]. Доказана генерическая NP-полнота проблемы выполнимости булевых формул [96] и ограниченной проблемы остановки для машин Тьюринга [101].

5. Доказан генерический аналог теоремы Бейкера-Гилла-Соловея о релятивизации проблемы $P \neq NP$ [103].

Научная новизна работы. Все основные результаты диссертации являются новыми.

Методика исследований. В качестве методов исследования использовались методы теории вычислимости, теории сложности вычислений, алгебры, математической логики и теории чисел.

Теоретическая и практическая ценность. Диссертация носит теоретический характер. Ее результаты могут быть использованы в дальнейших исследованиях по теории вычислимости, теории сложности вычислений, при чтении спецкурсов для студентов и аспирантов.

Апробация работы. Результаты диссертации докладывались на Омском алгебраическом семинаре (2006-2018), международных математических конференциях «Мальцевские чтения» (Новосибирск, 2006-2017), международных математических конференциях «Methods of Logic in Mathematics» (Санкт-Петербург, 2006, 2008), международной конференции «Computer Science in Russia» (Екатеринбург, 2007), международной математической конференции «Leonard Euler and Modern Combinatorics» (Санкт-Петербург, 2007), посвященной 300-летию Л. Эйлера, конференции «Стохастические модели в биологии и предельные алгебры» (Омск, 2010), алгебраическом семинаре в Stevens Institute of Technology (Хобокен, США, 2005, 2007, 2011, 2016), конференции «Аппроксимация логических моделей, алгоритмов и задач» (Омск, 2015), конференции SIBECRYPT-15 (Новосибирск, 2015), конференции SIBECRYPT-17 (Красноярск, 2017), международной конференции «Математика в современном мире» (Новосибирск, 2017), на семинаре по дискретной математике лаборатории математической логики Санкт-Петербургского отделения Математического института им. В.А.Стеклова РАН (Санкт-Петербург, 2017), на Колмогоровском семинаре по сложности вычислений и сложности определений кафедры математической логики и теории алгоритмов механико-математического факультета МГУ им. М. В. Ломоносова (Москва, 2017), на международной алгебраической конференции памяти А. Г. Куроша (Москва, 2018), на конференции «Computability in Europe» (Киль, Германия, 2018).

Структура и объём работы. Диссертация изложена на 171 странице, содержит введение, раздел с предварительными сведениями, четыре раздела с полученными результатами, заключение и список литературы. Разделы разбиты на подразделы, список литературы содержит 105 наименований. Нумерация утверждений (теорем, лемм, следствий), сквозная внутри каждого раздела и состоит из двух чисел: первое число — это номер раздела, второе — порядковый номер внутри раздела.

Публикации. Результаты диссертации опубликованы в работах [83]–

[105], входящих в перечень ВАК рецензируемых научных журналов, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученых степеней доктора и кандидата наук. Работа [84] написана в соавторстве с А.Г.Мясниковым. В диссертацию вошли результаты из [84], которые получены автором самостоятельно.

Используемые обозначения.

$\mathbb{N} = \{1, 2, 3, \ldots\}$ – натуральные числа без нуля.

$\omega = \{0, 1, 2, 3, \ldots\}$ – натуральные числа с нулем.

$P(A)$ – множество всех подмножеств множества A.

$|A|$ – мощность конечного множества A.

$|w|$ – длина слова w над конечным алфавитом A.

A^* – множество всех конечных слов конечного алфавита A.

$\overline{A} = I \setminus A$ – дополнение множества $A \subseteq I$.

A_n – множество всех элементов размера n множества A.

$M(x)\downarrow$ – машина M останавливается на входе x.

Содержание работы

В **первом разделе** даются основные определения и факты теории алгоритмов, теории сложности вычислений и теории генерической вычислимости. Для подмножества $S \subseteq I$ определим последовательность

$$\rho_n(S) = \frac{|S_n|}{|I_n|},\ n = 1, 2, 3, \ldots,$$

где I_n – множество входов размера n, а $S_n = S \cap I_n$ – множество входов из S размера n. *Асимптотической плотностью* S назовем предел (если он существует)

$$\rho(S) = \lim_{n\to\infty} \rho_n(S).$$

Множество S называется *генерическим*, если $\rho(S) = 1$, *пренебрежимым*, если $\rho(S) = 0$, *сильно пренебрежимым*, если последовательность $\rho_n(S)$ экспоненциально быстро сходится к 0 и *сильно генерическим*, если его дополнение $\overline{S}$ сильно пренебрежимо. Алгоритм $\mathcal{A} : I \to J \cup \{?\}$ называется *(сильно) генерическим*, если $\mathcal{A}$ останавливается на всех входах из I и множество $\{x \in I : \mathcal{A}(x) =?\}$ (сильно) пренебрежимо. Генерический алгоритм $\mathcal{A}$ вычисляет функцию $f : I \to J$, если для всех $x \in I$ $\mathcal{A}(x) = y \in J \Rightarrow f(x) = y$. Множество $S \subseteq I$ и соответствующая проблема распознавания (S, I)

- *генерически разрешимы*, если существует генерический алгоритм, вычисляющий характеристическую функцию S.

- *сильно генерически разрешимы*, если существует сильно генерический алгоритм, вычисляющий характеристическую функцию S.

Множество $S \subseteq I$ и соответствующая проблема распознавания (S, I)

- *супер неразрешимы*, если S не является генерически разрешимым.
- *сильно неразрешимы*, если S не является сильно генерически разрешимым.

Отметим, что данное определение генерической разрешимости отличается от определения генерической разрешимости используемое К. Джокушем и П. Шуппом в [55], где для распознавания множества A применяются алгоритм $\mathcal{A}$ с генерическим множеством остановки $H_{\mathcal{A}}$: внутри $H_{\mathcal{A}}$ алгоритм корректно вычисляет характеристическую функцию A, а вне $H_{\mathcal{A}}$ алгоритм не останавливается. Это более широкое определение генерической разрешимости – см., например, теорему 2.22 и следствие 2.24 в [55]. В связи с этим, будет отличаться и определение генерической тьюринговой сводимости, которое вводится в четвертом разделе. Однако наше определение представляется более «эффективным», так как в нем генерические алгоритмы всегда останавливаются. Кроме того, все известные примеры конкретных генерических алгоритмов для различных алгоритмических проблем тоже всегда останавливаются. Более того, все результаты диссертации о генерической неразрешимости аналогично могут быть доказаны для определения Джокуша-Шуппа.

Второй раздел посвящен доказательству генерической неразрешимости классических алгоритмически неразрешимых проблем с помощью метода генерической амплификации. Пусть I, J – некоторые множества с определенными на них функциями размера. *Клонирование* множества I в множестве J – это функция $C : I \to P(J)$, из I во множество всех подмножеств $P(J)$ множества J такая, что $\forall x, y \in I$

- либо $C(x) \cap C(y) = \varnothing$,
- либо $C(x) \subseteq C(y)$ или $C(y) \subseteq C(x)$.

Для множества $S \subseteq I$ определим *клон* $C(S)$ как объединение всех клонов элементов из S:

$$C(S) = \bigcup_{x \in S} C(x).$$

Будем называть клонирование C из I в J *эффективным*, если существует всюду определенная вычислимая функция $E : I \times \omega \to J$ такая, что для любого $x \in I$

$$C(x) = \{E(x, 0), E(x, 1), \ldots, \}.$$

Таким образом, с помощью алгоритма E можно эффективно перечислять все элементы каждого клона. Клонирование $C : I \to P(J)$ называется *непренебрежимым* (соответственно, *не сильно пренебрежимым*), если для любого $x \in I$ множество $C(x)$ не является пренебрежимым (соответственно, сильно пренебрежимым) в J. Если $\mathcal{D} = (L, I)$ – проблема распознавания в I, то проблема распознавания $C(\mathcal{D}) = (C(L), J)$ в J называется *клоном* $\mathcal{D}$ в J относительно C.

Теорема 1. *Пусть I, J – множества с функциями размера и $C : I \to P(J)$ – эффективное клонирование. Тогда для любой неразрешимой проблемы распознавания $\mathcal{D} = (L, I)$ в I имеет место следующее:*

1. *Если C – непренебрежимое клонирование, то проблема $C(\mathcal{D})$ супер неразрешима в J.*
2. *Если C – не сильно пренебрежимое клонирование, то проблема $C(\mathcal{D})$ сильно неразрешима в J.*

Далее доказывается генерическая неразрешимость проблемы остановки для машин Тьюринга. Обозначим множество всех машин Тьюринга через $\mathcal{M}$. Машина Тьюринга называется *нормализованной*, если из любого нефинального состояния q_i в соответствующих ему правилах в программе возможен переход в состояния q_j, где $j \leq |A|i + 1$, где A – рабочий алфавит машины. Обозначим множество всех нормализованных машин Тьюринга через $\mathcal{NM}$. Рассмотрим теперь один из вариантов классической проблемы остановки. Зафиксируем рабочий алфавит $A = \{0, 1, \square\}$, где $\square$ – пустой символ. Определим следующее множество

$$HP_{\mathcal{M}} = \{M \in \mathcal{M} : M \text{ останавливается на входе } 0\}.$$

Аналогично определим

$$HP_{\mathcal{NM}} = \{M \in \mathcal{NM} : M \text{ останавливается на входе } 0\}.$$

Проблемы $(HP_{\mathcal{M}}, \mathcal{M})$ и $(HP_{\mathcal{NM}}, \mathcal{NM})$ в классическом смысле являются алгоритмически неразрешимыми.

Теорема 2. *Верно следующее:*

1. *Проблема $(HP_{\mathcal{M}}, \mathcal{M})$ сильно неразрешима.*
2. *Проблема $(HP_{\mathcal{NM}}, \mathcal{NM})$ супер неразрешима.*

Доказывается генерический аналог классической теоремы Клини о неподвижной точке.

Теорема 3. *Имеет место следующее:*

1. *Для любого генерического алгоритма* $\mathcal{A} : \mathcal{NM} \to \mathcal{NM} \cup \{?\}$ *существует такая машина Тьюринга* M, *что* $\mathcal{A}(M) \neq ?$ *и машина* $\mathcal{A}(M)$ *вычисляет ту же функцию, что и* M.

2. *Для любого сильно генерического алгоритма* $\mathcal{A} : \mathcal{M} \to \mathcal{M} \cup \{?\}$ *существует такая машина Тьюринга* M, *что* $\mathcal{A}(M) \neq ?$ *и машина* $\mathcal{A}(M)$ *вычисляет ту же функцию, что и* M.

Строятся примеры полугрупп с генерически неразрешимой проблемой равенства слов. Пусть $\mathfrak{S} = \langle A|R\rangle$ — конечно определенная полугруппа с множеством порождающих $A = \{a_1, \ldots, a_n\}$ и множеством определяющих соотношений $R = \{r_1 = s_1, \ldots, r_k = s_k\}$. Для символа $x \notin A$ положим

$$\mathfrak{S}_x = \langle A, x|R, x = xa_1, \ldots, x = xa_n, x = xx\rangle.$$

Теорема 4. *Если проблема равенства слов в полугруппе* $\mathfrak{S}$ *неразрешима, то проблема равенства слов в полугруппе* $\mathfrak{S}_x$ *супер неразрешима.*

Доказывается генерическая разрешимость десятой проблемы Гильберта для двух способов представления диофантовых уравнений. Будем отождествлять диофантово уравнение $P(x_1, \ldots, x_m) = 0$ с арифметической схемой, представляющей полином P. *Арифметическая схема* от переменных $x_1, \ldots, x_m$ состоит из конечного числа промежуточных переменных $x_{m+1}, \ldots, x_{n+m}$ и присваиваний (одно присваивание для каждой промежуточной переменной) одного из следующих типов:

- $x_i = x_j * x_k$, где $j, k < i$ и $* \in \{+, -, \times\}$,
- $x_i = x_j + 1$, где $j < i$,
- $x_i = x_j - 1$, где $j < i$.

Переменные $x_1, \ldots, x_m$ называются *входными переменными* схемы. Последняя промежуточная переменная x_{m+n} называется *выходной переменной* схемы. Размер схемы – это число присваиваний n. Обозначим через $\mathcal{D}$ множество всех диофантовых уравнений, представленных с помощью арифметических схем. Определим множество

$$SOL(\mathcal{D}) = \{P \in \mathcal{D} : \exists x_1 \in \mathbb{Z} \ldots \exists x_m \in \mathbb{Z}\ P(x_1, \ldots, x_m) = 0\}.$$

Теорема 5. *Проблема* $(SOL(\mathcal{D}), \mathcal{D})$ *сильно неразрешима.*

Система диофантовых уравнений записана в *форме Сколема* [79, 13], если каждое уравнение в ней имеет один из следующих типов:

1. $x_i = x_j x_k$,

2. $x_i = x_j + x_k$,

3. $x_i = 1$.

Будем называть систему в форме Сколема *нормализованной*, если в k-м уравнении системы могут встречаться только переменные x_i, где $i \leq 3k$. Обозначим через $\mathcal{S}$ множество всех нормализованных систем диофантовых уравнений в форме Сколема. Определим множество

$$SOL_{\mathbb{N}}(\mathcal{S}) = \{S \in \mathcal{S} : \text{система } S \text{ разрешима над } \mathbb{N}\}.$$

Здесь множество натуральных чисел $\mathbb{N}$ не содержит 0.

Теорема 6. *Проблема разрешимости диофантовых уравнений в форме Сколема* $(SOL_{\mathbb{N}}(\mathcal{S}), \mathcal{D})$ *генерически разрешима за полиномиальное время.*

Определим теперь множество

$$SOL_{\mathbb{Z}}(\mathcal{S}) = \{S \in \mathcal{S} : \text{система } S \text{ разрешима над } \mathbb{Z}\}.$$

Теорема 7. *Проблема разрешимости нормализованных систем диофантовых уравнений в форме Сколема над множеством целых чисел* $(SOL_{\mathbb{Z}}(\mathcal{S}), \mathcal{D})$ *сильно неразрешима.*

Далее доказывается генерическая неразрешимость элементарных теорий, которые неразрешимы в классическом смысле. Зафиксируем конечную сигнатуру

$$\sigma = \{P_1^{(a_1)}, \ldots, P_k^{(a_k)}, f_1^{(b_1)}, \ldots, f_m^{(b_m)}, c_1, \ldots, c_l\},$$

где P_i предикаты, f_i функции и c_i константы. Положим

$$K = K_\sigma = \max_{i=1,\ldots,k, j=1,\ldots,m} \{a_i, b_j + 1, 2\}.$$

Пусть $\mathfrak{A} = \langle A, \sigma \rangle$ – алгебраическая система сигнатуры σ. Назовем замкнутую формулу Φ сигнатуры σ *простой атомарной* если она имеет следующий вид:

1) $x_j = f_i(x_{i_1}, \ldots, x_{i_s})$,

2) $P_i(x_{i_1}, \ldots, x_{i_r})$,

3) $x_i = c_j$.

Замкнутая формула Φ сигнатуры σ имеет *натуральную пренексную* форму, если она имеет вид:

$$\Phi = Q_1 x_1 \ldots Q_t x_t \varphi,$$

где $Q_i \in \{\forall, \exists\}$ – кванторы, φ бескванторная формула, полученная с помощью конъюнкций, дизъюнкций из простых атомарных формул или их отрицаний. Заметим, что любая замкнутая формула может быть приведена с помощью эквивалентных преобразований к натуральной пренексной форме. При этом размер формулы увеличивается не более чем линейно.

Пусть теперь φ – бескванторная формула, которая является булевой комбинацией простых атомарных формул и их отрицаний. Естественным образом можно сопоставить формуле φ бинарное дерево T_φ, которое представляет конструкцию φ из простых атомарных формул и их отрицаний с помощью конъюнкций и дизъюнкций. Внутренние вершины T_φ помечены символами $\vee$ и $\wedge$, а листья T_φ помечены простыми атомарными или их отрицаниями. Если T_φ имеет n листьев, то не более Kn переменных могут встретиться в T_φ, поэтому в дальнейшем будем полагать, что все переменные T_φ лежат в множестве $x_1, \ldots, x_{Kn}$. Пусть $\Phi = Q_1 x_1 \ldots Q_t x_t \varphi$ – формула в натуральной пренексной форме. *Представление* Φ состоит из бинарного дерева T_φ, которое кодирует бескванторную часть φ, и кванторной приставки $Q_1 x_1 \ldots Q_t x_t$. Если T_φ имеет n листьев, то длина кванторной приставки не более Kn. Под размером $size(\Phi)$ формулы Φ будем понимать число n листьев дерева T_φ. Обозначим через $\mathcal{F}$ множество всех формул в натуральной пренексной форме.

Теорема 8. *Пусть $\mathfrak{A} = \langle A, \sigma \rangle$ – алгебраическая система конечной сигнатуры σ с неразрешимой элементарной теорией $Th(\mathfrak{A})$. Проблема распознавания $(Th(\mathfrak{A}), \mathcal{F})$ является сильно неразрешимой.*

Будем называть формулу $\Phi \in \mathcal{F}$ *нормализованной*, если в дереве T_φ, представляющем бескванторную часть φ формулы Φ, для любой переменной x_i, $i > q$ найдется переменная x_{i-1}, расположенная либо в том же листе дерева, либо в более левом. Другими словами, переменные в листьях дерева T_φ занумерованы слева направо. В представление нормализованной формулы размера n, помимо дерева T_φ и кванторной приставки $Q_1 Q_2 \ldots Q_{Kn}$, будет входить еще перестановка $\pi_\Phi = (i_1, i_2, \ldots, i_{Kn})$ индексов переменных $(1, 2, \ldots, Kn)$, показывающая на какую переменную x_m навешан квантор Q_m. Обозначим через $\mathcal{NF}$ множество всех нормализованных формул сигнатуры σ.

Теорема 9. *Пусть $\mathfrak{A} = \langle A, \sigma \rangle$ – алгебраическая система конечной сигнатуры σ с неразрешимой элементарной теорией $Th(\mathfrak{A})$. Проблема распознавания $(Th(\mathfrak{A}), \mathcal{NF})$ является супер неразрешимой.*

Доказывается генерический аналог теоремы Гёделя о неполноте формальной арифметики.

Теорема 10. *Пусть формальная арифметика непротиворечива. Имеет место следующее:*

1. *Не существует сильно генерического множества арифметических формул $\mathcal{G} \subseteq \mathcal{F}$ такого, что для любой формулы $\Phi \in \mathcal{G}$ либо Φ, либо $\neg\Phi$ выводится из аксиом формальной арифметики.*

2. *Не существует генерического множества арифметических формул $\mathcal{G} \subseteq \mathcal{NF}$ такого, что для любой формулы $\Phi \in \mathcal{G}$ либо Φ, либо $\neg\Phi$ выводится из аксиом формальной арифметики.*

Далее изучаются ограничения метода генерической амплификации. Предполагается, что натуральные числа ω представляются в двоичном виде, а размер натурального числа n есть длина его двоичной записи $[\log_2 n] + 1$.

Теорема 11. *Пусть $A \subseteq \omega$ – простое пренебрежимое множество. Тогда*

1. *Множество A супер неразрешимо.*

2. *Не существует непренебрежимого клонирования $C : \omega \to P(\omega)$ такого, что $A = C(S)$ для некоторого множества $S \subseteq \omega$.*

С другой стороны, любое рекурсивно перечислимое множество натуральных чисел с ненулевой асимптотической плотностью можно всегда получить из множества ω с помощью генерической амплификации.

Теорема 12. *Пусть $A \subseteq \omega$ – любое рекурсивно перечислимое множество с ненулевой асимптотической плотностью. Тогда существует эффективное непренебрежимое клонирование $C : \omega \to P(\omega)$ такое, что $A = C(\omega)$.*

Строится пример абсолютно неразрешимой проблемы. Будем называть множество $A \subseteq \omega$ *абсолютно неразрешимым*, если не существует алгоритма $\mathcal{A} : \omega \to \{0, 1, ?\}$ такого, что

1. $\forall x \in \omega\ \mathcal{A}(x)\downarrow$,

2. множество $\{x \in \omega : \mathcal{A}(x) \neq ?\}$ непренебрежимо,

3. $\mathcal{A}(x) \neq ? \Rightarrow \mathcal{A}(x) = \chi_A(x)$, где $\chi_A(x)$ – характеристическая функция множества A.

Теорема 13. *Пусть $A \subseteq \omega$ – простое пренебрежимое множество. Тогда A абсолютно неразрешимо.*

В **третьем разделе** изучается генерическая сложность некоторых классических алгоритмических проблем. Доказывается генерическая трудноразрешимость арифметики Пресбургера – теории первого порядка алгебраической системы $\mathfrak{N} = \langle \mathbb{N}, \sigma_{PA} \rangle$ с сигнатурой $\sigma_{PA} = \{+, 1\}$.

Теорема 14. *Не существует сильно генерического экспоненциального алгоритма, решающего* $(Th(\mathfrak{N}), \mathcal{F})$.

Далее доказывается генерическая трудноразрешимость проблемы выполнимости булевых формул при условии трудноразрешимости этой проблемы в худшем случае. Пусть φ – булева формула в базисе $\{\vee, \wedge, \neg\}$. Естественным образом можно сопоставить формуле φ бинарное дерево T_φ, которое представляет конструкцию φ из переменных и их отрицаний с помощью конъюнкций и дизъюнкций. Внутренние вершины T_φ помечены символами $\vee$ и $\wedge$, а листья T_φ помечены переменными или их отрицаниями. Обозначим через $\mathcal{BF}$ множество всех булевых формул.

Теорема 15. *Если* $P \neq NP$ *и* $P = BPP$, *то не существует сильно генерического полиномиального алгоритма, решающего проблему выполнимости на множестве* $\mathcal{BF}$.

Далее доказывается генерическая трудноразрешимость классических проблем криптографии: проблемы распознавания квадратичных вычетов, проблемы дискретного логарифма, проблемы извлечения корня в группах вычетов, проблемы поиска изоморфизма графов, при условии трудноразрешимости этих проблем в худшем случае.

Пусть $\mathbb{Z}/(m)$ – мультипликативная группа вычетов по модулю $m \in \mathbb{N}$. *Квадратичным вычетом* в группе $\mathbb{Z}/(m)$ называется любой элемент x, для которого существует $y \in \mathbb{Z}/(m)$ такой, что $x = y^2$. Рассмотрим следующее множество входов:

$$RES = \{(m, x) \in \mathbb{N}^2 : m = pq, \text{ где } p, q - \text{простые числа}, x \in \mathbb{Z}/(m)\}.$$

Под *проблемой распознавания квадратичных вычетов* понимается проблема распознавания (QR, RES), где

$$QR = \{(m, x) \in RES : x - \text{ квадратичный вычет в } \mathbb{Z}/(m)\}.$$

Рассмотрим любую бесконечную последовательность натуральных чисел $\mu = \{m_1, m_2, \ldots\}$ такую, что для любого n имеет место $2^n < m_n < 2^{n+1}$ и m_n – произведение двух различных простых чисел. Будем называть такую последовательность *экспоненциальной*. Теперь определим алгоритмическую проблему $(QR(\mu), RES(\mu))$ как ограничение проблемы распознавания квадратичных вычетов (QR, RES) на следующее множество входных данных:

$$RES(\mu) = \{(m, x) : m \in \mu, x \in \mathbb{Z}/(m)\}.$$

Теорема 16. *Если для проблемы* (QR, RES) *не существует полиномиального вероятностного алгоритма, то существует экспоненциальная последовательность* μ *такая, что проблема* $(QR(\mu), RES(\mu))$ *не является генерически полиномиально разрешимой.*

Проблема дискретного логарифма состоит в вычислении функции $dl : I \to \mathbb{N}$, где I – это множество троек (a, p, g_p) таких, что p – простое число, g_p – фиксированный первообразный элемент в поле $GF(p)$ и $a \in GF(p)$, $a \neq 0$. Сама функция dl определяется следующим образом:

$$dl(a, p, g_p) = x \Leftrightarrow g_p^x = a \in GF(p).$$

Рассмотрим любую бесконечную последовательность простых чисел $\pi = \{p_1, p_2, \ldots, p_n, \ldots\}$, удовлетворяющую условию $2^n \leq p_n < 2^{n+1}$ для любого n. Будем называть такую последовательность *экспоненциальной*. Теперь определим функцию dl_π как ограничение функции dl на множество троек (a, p, g_p) таких, что $p \in \pi$.

Теорема 17. *Если для вычисления функции dl не существует полиномиального вероятностного алгоритма, то существует экспоненциальная последовательность π такая, что для вычисления функции dl_π не существует генерического полиномиального алгоритма.*

Проблема извлечения корня в группах вычетов состоит в вычислении функции $root : I \to \mathbb{N}$, где I – это множество троек (a, e, m) таких, что $m = pq$ и p, q – различные простые числа, $e < m$, $(\varphi(m), e) = 1$ и $a \in \mathbb{Z}/(m)$. Сама функция $root$ определяется следующим образом:

$$root(a, e, m) = x \Leftrightarrow x^e = a \in \mathbb{Z}/(m).$$

Рассмотрим любую бесконечную последовательность пар натуральных чисел $\mu = \{(e_1, m_1), (e_2, m_2), \ldots\}$ такую, что $2^n < m_n < 2^{n+1}$ для любого n, m_n – произведение двух различных простых чисел, для любого $n > 1$, и $e_n < m_n$ и $(\varphi(m_n), e_n) = 1$ для любого n. Будем называть такую последовательность *экспоненциальной*. Теперь определим функцию $root_\mu$ как ограничение функции $root$ на следующее множество входных данных:

$$I = \{(a, e, m) : (e, m) \in \mu, a \in \mathbb{Z}/(m)\}.$$

Теорема 18. *Если для вычисления функции root не существует полиномиального вероятностного алгоритма, то существует экспоненциальная последовательность μ такая, что для вычисления функции $root_\mu$ не существует генерического полиномиального алгоритма.*

Напомним, что два графа G_1 и G_2 называются изоморфными, если существует биекция π между множествами вершин G_1 и G_2 такая, что для любых вершин v, u графа G_1 v и u соединены ребром в G_1 тогда и только тогда, когда $\pi(v)$ и $\pi(u)$ соединены ребром в G_2. Биекция π, осуществляющая

изоморфизм, является перестановкой множества вершин графов G_1, G_2, если вершины обоих графов занумерованы числами $\{1, 2, \ldots, n\}$. Множеством входов для проблемы поиска изоморфизма графов является множество всех пар изоморфных графов. В этой проблеме требуется вычислять следующую функцию.

$$sgi(G_1, G_2) = \text{перестановка, осуществляющая изоморфизм } \pi$$

$$\text{между изоморфными графами } G_1 \text{ и } G_2.$$

Рассмотрим бесконечную последовательность графов $\gamma = \{G_1, G_2, \ldots, G_n, \ldots\}$ такую, что G_n имеет n вершин для любого n. Для каждой последовательности графов γ определим функцию sgi_γ – ограничение функции sgi на множество пар (G, G_n), где $G_n \in \gamma$ и граф G изоморфен графу G_n.

Теорема 19. *Если для вычисления функции sgi не существует полиномиального вероятностного алгоритма, то существует последовательность графов γ такая, что для вычисления функции sgi_γ не существует генерического полиномиального алгоритма.*

В **четвертом разделе** вводятся три типа генерических сводимостей. Изучаются их свойства. Изучается структура рекурсивно перечислимых степеней самой общей — генерической тьюринговой сводимости. В данном разделе будем предполагать, что натуральные числа ω представляются в двоичном виде, а размер натурального числа n есть длина его двоичной записи $[\log_2 n]+1$.

Множество $A \subseteq \omega$ *генерически m-сводится* к $B \subseteq \omega$ (обозначается $A \leq_{gm} B$), если существует вычислимая функция $f : \omega \to \omega$ такая, что

1. $\forall x \in \omega \; x \in A \Leftrightarrow f(x) \in B$,
2. $\forall S \subseteq \omega \; S$ непренебрежимо $\Rightarrow f(S)$ непренебрежимо.

Множество $A \subseteq \omega$ *генерически клонированно сводится* к множеству $B \subseteq \omega$ (обозначается это $A \leq_{gc} B$), если либо $A = B$, либо существует такая всюду определенная вычислимая функция $f : \omega \times \omega \to \omega \cup \{?\}$, что

1. $\forall x \in \omega$ если $f(x, 0) \neq ?$, то $\forall n \in \omega \; f(x, n) \neq ?$.
2. Множество $\{x \in \omega : f(x, 0) = ?\}$ пренебрежимо.
3. $\forall x \in \omega$ если $f(x, 0) \neq ?$, то множество $\{f(x, n) : n \in \omega\}$ непренебрежимо.
4. $\forall x \in \omega$ если $f(x, 0) \neq ?$, то
   - $x \in A \Rightarrow \forall n \in \omega \; f(x, n) \in B$.

- $x \notin A \Rightarrow \forall n \in \omega\ f(x,n) \notin B$.

Пусть A – произвольное множество натуральных чисел. *Генерическим оракулом* множества A называется функция $\varphi_A : \omega \to \{0, 1, ?\}$ такая, что

1. Множество $\{x : \varphi_A(x) =?\}$ пренебрежимо.
2. $\forall x \in \omega\ \varphi_A(x) = 1 \Rightarrow x \in A$.
3. $\forall x \in \omega\ \varphi_A(x) = 0 \Rightarrow x \notin A$.

Множество $A \subseteq \omega$ *генерически сводится по Тьюрингу* к множеству $B \subseteq \omega$, если существует машина M с командами обращения к оракулу такая, что для любого генерического оракула φ_B генерический алгоритм M^{φ_B} вычисляет характеристическую функцию A. Обозначается это $A \leq_{gT} B$.

Теорема 20. *Пусть $A, B \subseteq \omega$.*

1. *Если $A \leq_{gm} B$, то $A \leq_{gT} B$.*
2. *Если $A \leq_{gc} B$, то $A \leq_{gT} B$.*

Будем писать $A \equiv_{gT} B$, если $A \leq_{gT} B$ и $B \leq_{gT} A$. Определим также генерическую тьюрингову степень множества A как

$$d_{gT}(A) = \{B \subseteq \omega : B \equiv_{gT} A\}.$$

Генерическая тьюрингова $\mathbf{a}$ степень рекурсивно перечислима, если содержит хотя бы одно рекурсивно перечислимое множество. Будем писать, что $\mathbf{a} \leq \mathbf{b}$, если существуют $A \in \mathbf{a}$ и $B \in \mathbf{a}$ такие, что $A \leq_{gT} B$. Аналогично определяется отношение $\mathbf{a} < \mathbf{b}$. Все генерически разрешимые множества образуют одну генерическую тьюрингову степень, которая обозначается $\mathbf{0}$. Для любой генерической тьюринговой степени $\mathbf{a}$ имеет место $\mathbf{0} \leq \mathbf{a}$.

Рекурсивно перечислимое множество A будем называть *gT-полным*, если для любого рекурсивно перечислимого B имеет место $B \leq_{gT} A$. Соответствующая степень называется *gT-полной*.

Теорема 21. *Существуют gT-полные генерические рекурсивно перечислимые степени.*

Следующее утверждение является аналогом классической теоремы Мучника-Фридберга о существовании несравнимых относительно тьюринговой сводимости рекурсивно перечислимых степеней.

Теорема 22. *Существуют несравнимые генерические тьюринговы рекурсивно перечислимые степени.*

Будем называть генерическую тьюрингову рекурсивно перечислимую степень $\mathbf{a}$ *максимальной*, если не существует неполной генерической тьюринговой рекурсивно перечислимой степени $\mathbf{b}$ такой, что $\mathbf{a} < \mathbf{b}$.

Теорема 23. *Не существует максимальной генерической рекурсивно перечислимой степени.*

Ненулевая генерическая тьюрингова рекурсивно перечислимая степень $\mathbf{a}$ называется *минимальной*, если не существует такой генерической тьюринговой рекурсивно перечислимой степени $\mathbf{b}$ что $\mathbf{0} < \mathbf{b} < \mathbf{a}$.

Теорема 24. *Не существует минимальной генерической тьюринговой рекурсивно перечислимой степени.*

Доказывается генерический аналог классической теоремы Сакса о разложении.

Теорема 25. *Пусть A – супер неразрешимое рекурсивно перечислимое множество. Тогда $A = B_0 \cup B_1$, где B_0, B_1 – непересекающиеся рекурсивно перечислимые множества такие, что $A \not\leq_{gT} B_0$ и $A \not\leq_{gT} B_1$.*

В **пятом разделе** вводится понятие генерической полиномиальной сводимости алгоритмических проблем. Определяются генерические аналоги классов P и NP. Доказывается генерическая генерическая NP-полнота проблемы выполнимости булевых формул и ограниченной проблемы остановки для машин Тьюринга.

Пусть I, J — некоторые множества входов с определенными на них функциями размера. Множество $A \subseteq I$ *генерически полиномиально сводится* к множеству $B \subseteq J$ (обозначается $A \leq_{GenP} B$), если существуют вероятностный полиномиальный алгоритм $\mathcal{R} : I \times \mathbb{N} \to P(J) \cup \{?, !\}$, полином $p(n)$, полином $q(n)$ степени больше 2 и константа $C > 0$, такие, что

1. для всех $x \in I$ либо $\forall n\, \mathcal{R}(x, n) = \{?\}$, либо для всех $n \geq q(k)$, где $k = size(x)$, выполнены следующие условия:
   (a) $\forall y \in \mathcal{R}(x, n)\ (y \neq !\ \Rightarrow\ size(y) = n)$;
   (b) все элементы в $\mathcal{R}(x, n) \setminus \{!\}$ выдаются алгоритмом $\mathcal{R}$ равновероятно;
   (c) вероятность получить ответ «!» в $\mathcal{R}(x, n)$ не больше 2^{-Ck};
   (d) $\dfrac{|\mathcal{R}(x, n)|}{|J_n|} > \dfrac{1}{(p(n))^k}$;
   (e) $x \in A \Rightarrow \mathcal{R}(x, n) \subseteq B$;
   (f) $x \notin A \Rightarrow \mathcal{R}(x, n) \subseteq J \setminus B$;
2. множество $\{x \in I : \forall n\ (\mathcal{R}(x, n) = ?)\}$ сильно пренебрежимо.

Определим сильно генерический аналог класса NP. Пусть I – множество входов с определенной на нем функцией размера входа. Множество $S \subseteq I$ принадлежит *классу* sgNP, если существует полиномиальное сильно генерическое множество $G \subseteq I$, такое, что $S \cap G \in$ NP. Множество $S \in$ sgNP называется *генерически NP-полным*, если для любого $A \in$ sgNP имеет место $A \leq_{GenP} S$.

Теорема 26. *Проблема выполнимости булевых формул генерически NP-полна.*

Рассмотрим множество $BHP \subseteq \mathcal{M}$ машин Тьюринга M над алфовитом $\{0, 1, \square\}$ таких, что существует $x \in \{0,1\}^*$ такой, что $|x| < size(M)$ и M останавливается на x за $\leq size(M)$ шагов и выдает 1.

Теорема 27. *Множество BHP генерически NP-полное.*

Пусть I – множество входов с определенной на нем функцией размера входа. Множество $S \subseteq I$ принадлежит *классу* genP, если существует полиномиальный генерический алгоритм, вычисляющий характеристическую функцию множества S. Множество $S \subseteq I$ принадлежит *классу* genNP, если существует разрешимое за полиномиальное время генерическое множество $G \subseteq I$ такое, что $S \cap G \in$ NP. Аналогично определяются релятивизованные генерические классы genP и genNP.

Доказывается генерический аналог теоремы Бейкера-Гилла-Соловея о релятивизации проблемы P $\neq$ NP.

Теорема 28. *Существуют такие оракулы A и B, что $genP^A = genNP^A$ и $genP^B \neq genNP^B$.*

Список литературы

[1] М. М. Арсланов. О некоторых обобщениях теоремы о неподвижной точке. Изв. вузов. Матем., 5 (1981), 9–16.

[2] И. В. Ашаев. Основы теории алгоритмов, Омск: Издательство ОмГУ, (2006), 172 с.

[3] Л. Д. Беклемишев. Теоремы Гёделя о неполноте и границы их применимости. I. Успехи математических наук, 65:5(395) (2010), 61–106.

[4] Э. Х. Гимади, Н. И. Глебов, В. А. Перепелица. Алгоритмы с оценками для задач дискретной оптимизации. Проблемы кибернетики, 31 (1975), 35–42.

[5] М. Гэри, Д. Джонсон. Вычислительные машины и труднорешаемые задачи. М.: Мир, (1982), 419 с.

[6] Ю. Л. Ершов, И. А. Лавров, А. Д. Тайманов, М. А. Тайцлин. Элементарные теории. УМН, 20:4(124) (1965), 37–108.

[7] Д. Кнут. Искусство программирования. Изд. Вильямс, (2010), 720 с.

[8] Н. Коблиц. Курс теории чисел и криптографии. Москва: ТВП, (2001), 254 с.

[9] А. И. Мальцев. Алгоритмы и рекурсивные функции. М.: Наука, (1965), 394 с.

[10] А. А. Марков. Невозможность некоторых алгорифмов в теории ассоциативных систем. Доклады АН СССР, 55(7) (1947), 587–590.

[11] Ю. В. Матиясевич. Простые примеры неразрешимых канонических исчислений. Труды МИАН СССР, 93 (1967), 50–88.

[12] Ю. В. Матиясевич Диофантовость перечислимых множеств. Доклады Академии наук СССР, 191 (2) (1970), 279–282.

[13] Ю. В. Матиясевич. Десятая проблема Гильберта. Москва: Наука, (1993), 224 с.

[14] Э. Мендельсон. Введение в математическую логику. Москва: Наука, (1976), 320 с.

[15] А. А. Мучник. Неразрешимость проблемы сводимости теории алгоритмов. Доклады АН СССР, 108 (1956), 194– 197.

[16] Х. Роджерс. Теория рекурсивных функций и эффективная вычислимость. М.:Мир, (1972), 624 с.

[17] В. А. Романьков. Введение в криптографию. 2-е изд., исправ., М. : ФОРУМ, (2012). 240 с.

[18] В. А. Романьков. Диофантова криптография на бесконечных группах. Прикладная дискретная математика, 16 (2012), 15–42.

[19] В. А. Романьков. Алгебраическая криптография, Омск: ОмГУ, (2013), 136 с.

[20] Р. И. Соар. Вычислимо перечислимые множества и степени. Казань: Казанское математическое общество, (2000), 576 с.

[21] Н. К. Верещагин, А. Шень. Лекции по математической логике и теории алгоритмов. Часть 3. Вычислимые функции. М.: МЦНМО, (2012), 160 с.

[22] А.М. Вершик, П.В. Спорышев. Оценки среднего числа шагов симплекс-метода и задачи асимптотической интегральной геометрии. Доклады Академии наук СССР, 271 (5) (1983), 1044–1048.

[23] А. М. Вершик, П. В. Спорышев. Асимптотическая оценка среднего числа шагов параметрического симплекс-метода. Журнал вычислительной математики и математической физики, 26 (6) (1986), 813–826.

[24] М. Вялый, А. Китаев, А. Шень. Классические и квантовые вычисления. М.: МЦНМО, ЧеРо, (1999), 192 с.

[25] Г. С. Цейтин. Ассоциативное исчисление с неразрешимой проблемой эквивалентности. Труды МИАН СССР, 52 (1958), 172–189.

[26] U. Andrews, M. Cai, D. Diamondstone, C. Jockusch, S. Lempp. Asymptotic density, computable traceability, and 1-randomness. Fundamenta Mathematicae, 234 (2016), 41–53.

[27] E. Astor. Asymptotic density, immunity, and randomness. Computability, 4 (2) (2015), 141–158.

[28] L. Babai, P. Erdos, S. Selkow. Random graph isomorphism. SIAM Journal of Computing, 9 (3) (1980), 628–635.

[29] T. Baker, J. Gill, R. Solovay. Relativizations of the P=?NP question. SIAM Journal on Computing, 4 (1975), 431–442.

[30] L. Bienvenu, A. Day, R. Holzl. From bi-immunity to absolute undecidability. Journal of Symbolic Logic, 78 (4) (2013), 1218–1228.

[31] L. Bienvenu, D. Desfontaines, A. Shen. Generic algorithms for halting problem and optimal machines revisited. Logical Methods in Computer Science, 12 (2:1) (2016), 1–29.

[32] M. Blum. How to prove a theorem so no one else can claim it. Proceedings of the International Congress of Mathematicians, Berkeley, CA, (1986), pp. 1444–1451.

[33] A. Bogdanov, L. Trevisan. Average-Case Complexity. Electronic Colloquium on Computational Complexity, Report No. 73 (2006).

[34] A. V. Borovik, A. G. Myasnikov, V. N. Remeslennikov. The conjugacy problem in amalgamated products I: regular elements and black holes. International Journal of Algebra and Compututation, 17 (7) (2007), 1299–1333.

[35] A. V. Borovik, A. G. Myasnikov, V. N. Remeslennikov. Generic complexity of the conjugacy problem in HNN-extensions and algorithmic stratification of Miller's groups. Int. J. Algebra Comput., 17 (963) (2007), 963–997.

[36] C.S. Calude, M.A. Stay. Most programs stop quickly or never halt, Advances in Applied Mathematics, 40 (3) (2008), 295–308.

[37] G. J. Chaitin. A theory of program size formally identical to information theory, Journal of ACM, 22 (1975), 329–340.

[38] P. Cholak, G. Igusa. Bounding a density-1 and quasiminimality in the generic degrees. The Journal of Symbolic Logic, 82 (3) 2017, 931–957.

[39] S. Cook. The complexity of theorem proving procedures. Proceedings of the Third Annual ACM Symposium on Theory of Computing, (1971), 151–158.

[40] V. Diekert, A. G. Myasnikov, A. Weiß. Conjugacy in Baumslag's group, generic case complexity, and division in power circuits. Algorithmica, 4 (76) (2016), 961–988.

[41] V. Diekert, A. G. Myasnikov, A. Weiß. Amenability of Schreier graphs and strongly generic algorithms for the conjugacy problem. Journal of Symbolic Computation, 83 (2017), 147–165.

[42] R.G. Downey, C.G. Jockusch, P.E. Schupp. Asymptotic density and computably enumerable sets. Journal of Mathematical Logic, 13 (2013), 43 pp.

[43] R.G. Downey, C.G. Jockusch, T.H. McNicholl, P.E. Schupp, Asymptotic density and the Ershov Hierarchy, Math. Log. Quarterly, 61 (2015), 189–195.

[44] R. Gilman, A. G. Miasnikov, A. D. Myasnikov, A. Ushakov. Report on generic case complexity. Herald of Omsk University, Special Issue, (2007), 103–110.

[45] R. Gilman, A. G. Miasnikov, D. Osin. Exponentially generic subsets of groups. Illinois J. Math., 1 (54) (2010), 371–388.

[46] R. Gilman, A. G. Miasnikov, V. A. Roman'kov. Random equations in nilpotent groups. Journal of Algebra, 1 (352) (2012), 192–214.

[47] Y. Gurevich. Average case completeness. Journal of Computer and System Sciences, 42 (1991), 346–398.

[48] Y. Gurevich, S. Shelah. Expected computation time for Hamiltonian path problem. SIAM Journal on Computing, 3 (16) (1987), 486–502.

[49] M.J. Fischer, M.O. Rabin. Super-Exponential Complexity of Presburger Arithmetic. Proceedings of the SIAM-AMS Symposium in Applied Mathematics, 7 (1974), 27–41.

[50] R. M. Friedberg. Two recursively enumerable sets of incomparable degrees of unsolvability. Prod. Nat. Acad. Sci. USA, 43 (1957), 236–238.

[51] K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme. I. Monatshefte für Mathematik und Physik, 38 (1931), 173–198.

[52] J. D. Hamkins and A. Miasnikov. The halting problem is decidable on a set of asymptotic probability one. Notre Dame Journal of Formal Logic, 47 (4) (2006), 515–524.

[53] D. Hirschfeldt, C. Jockusch, R. Kuyper, P. Schupp. Coarse reducibility and algorithmic randomness. Journal of Symbolic Logic, 81 (3) (2016), 1028–1046.

[54] D.R. Hirschfeldt, C.G. Jockusch, T. McNicholl, P.E. Schupp. Asymptotic density and the coarse computability bound. Computability, 5 (2016), 13–27.

[55] C. Jockusch, P. Schupp. Generic computability, Turing degrees, and asymptotic density. Journal of the London Mathematical Society, 85 (2) (2012), 472–490.

[56] J. Jones. Undecidable Diophantine equations. Bull. Amer. Math. Soc., 3 (2) (1980), 859–862.

[57] G. Igusa. Nonexistence of minimal pairs for generic computability. Journal Symbolic Logic, Vol. 78 (2013), No. 2, pp. 511–522.

[58] G. Igusa. The generic degrees of density-1 sets, and a characterization of the hyperarithmetic reals. Journal of Symbolic Logic, 80 (4) (2015), 1290–1314.

[59] Impagliazzo R., Wigderson A. P=BPP unless E has Subexponential Circuits: Derandomizing the XOR Lemma. Proceedings of the 29th STOC, (1997), 220–229.

[60] M. Kambites. Generic Complexity of Finitely Presented Monoids and Semigroups. Computational complexity, 20 (1) (2011), 21–50.

[61] I. Kapovich, A. Myasnikov, P. Schupp, V. Shpilrain. Generic-case complexity and decision problems in group theory. Journal of Algebra, 264 (2003), 665–694.

[62] I. Kapovich, P. Schupp. Genericity, the Arzhantseva-Ol'shanskii method and the isomorphism problem for one-relator groups Mathematische Annalen, 331 (2005), 1–19.

[63] R. Karp. The fast approximate solution of hard combinatorial problems. Graph Theory and Computing, (1975), 15–31.

[64] B. Khoussainov, A. Miasnikov. Finitely presented expansions of groups, semigroups, and algebras. Trans. Amer. Math. Soc., 366 (2014), 1455–1474.

[65] V. Klee, G. Minty. How good is the simplex algorithm? Inequalities, III (Proc. Third Sympos., Univ. California, Los Angeles, Calif., 1969; dedicated to the memory of Theodore S. Motzkin), Academic Press, New York, (1972), 159–175.

[66] S.C. Kleene. On Notation for Ordinal Numbers. Journal of Symbolic Logic, 3 (1938), 150–155.

[67] Levin L. Average case complete problems. SIAM Journal on Computing, 15 (1987), 285–286.

[68] Matiyasevich Yu., Robinson J. Reduction of an arbitrary diophantine equation to one in 13 unknowns. Acta Arithmetica, 27 (1975), 521–553.

[69] A. Myasnikov, D. Osin. Algorithmically finite groups. Journal of Pure and Applied Algebra, 215 (2011), 2789–2796.

[70] A. Myasnikov, V. Romankov. Diophantine cryptography in free metabelian groups: Theoretical base. Groups, Complexity, Cryptology, 6 (2) (2014), 103–120.

[71] A. Miasnikov, P. Schupp. Computational complexity and the conjugacy problem. Computability, 4 (6) (2017) 307–318.

[72] A. Myasnikov, V. Shpilrain, A. Ushakov. Non-commutative cryptography and complexity of group-theoretic problems. Mathematical Surveys and Monographs, American Mathematical Society, 177 (2011).

[73] A. Myasnikov, A. Ushakov. Random van Kampen Diagrams and algorithmic problems in groups. Groups Complexity Cryptology, 3 (1) (2011), 121–185.

[74] B. Poonen, J. F. Voloch. Random Diophantine Equations. Arithmetic of higher dimensional algebraic varieties, Progress in Mathematics 226, Birkhäuser (2004), 175–184.

[75] E. L. Post. Recursive unsolvability of a problem of Thue. Journal of Symbolic Logic, 1 (12) (1947), 1–11.

[76] R. Rivest, A. Shamir, L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM, 21 (2) (1978), 120–126.

[77] G. E. Sacks. On the degrees less than $0'$. Annals of mathematics, 77 (2) (1963), 211–231.

[78] G. E. Sacks. The recursively enumerable degrees are dense. Annals of mathematics, 80 (2) (1964), 300–312.

[79] T. Skolem. Diophantische Gleichungen. Berlin: Springer, (1938).

[80] S. Smale. On the average number of steps of the simplex method of linear programming. Mathematical programming, 27 (3) (1983), 241–262.

[81] J. Wang. Average-case intractable NP problems. Advances in Languages, Algorithms, and Complexity, Kluwer Academic Publishers, (1997), 313–378.

[82] W. Woess. Cogrowth of groups and simple random walks. Archive of Mathematics, 41 (1983), 363–370.

Работы автора по теме диссертации, опубликованные в журналах из списка ВАК

[83] A.N.Rybalov. On the strongly generic undecidability of the Halting Problem. Theoretical Computer Science, 377 (2007), 268–270.

[84] A.G.Myasnikov, A.N.Rybalov. Generic complexity of undecidable problems. Journal of Symbolic Logic, 73 (2) (2008), 656–673.

[85] A.N. Rybalov. Generic Complexity of Presburger Arithmetic. Theory of Computing Systems, 46 (1) (2010), 2–8.

[86] А.Н. Рыбалов. Генерическая сложность теорий первого порядка. Сибирские электронные математические известия, 8 (2011), 168–178.

[87] А.Н. Рыбалов. О генерической неразрешимости Десятой проблемы Гильберта. Вестник Омского университета, 4 (2011), 19–22.

[88] A.N. Rybalov. Generic complexity of the Diophantine problem. Groups Complexity Cryptology, 5 (1) (2013), 25–30.

[89] А.Н. Рыбалов. Генерическая неполнота формальной арифметики. Сибирские электронные математические известия, 12 (2015), 185–189.

[90] А.Н. Рыбалов. О генерической сложности проблемы распознавания квадратичных вычетов. Прикладная дискретная математика, 28 (2015), 54–58.

[91] A.N. Rybalov. On the generic complexity of the searching graph isomorphism problem. Groups Complexity Cryptology, 7 (2) (2015), 191–194.

[92] А.Н. Рыбалов. О генерической сложности элементарных теорий. Вестник Омского университета, 4 (2015), 14–17.

[93] А.Н. Рыбалов. О генерической сложности проблемы дискретного логарифма. Прикладная дискретная математика, 33 (2016), 93–97.

[94] А.Н. Рыбалов. Об одном генерическом отношении рекурсивно перечислимых множеств. Алгебра и логика, 55 (5) (2016), 587–596.

[95] A.N. Rybalov. On the Generic undecidability of the Halting Problem for normalized Turing machines. Theory of Computing Systems, 60 (4) (2017), 671–676.

[96] А.Н. Рыбалов. О генерической NP-полноте проблемы выполнимости булевых формул. Прикладная дискретная математика, 36 (2017), 106–112.

[97] А.Н. Рыбалов. Генерическая теорема Гёделя о неполноте. Алгебра и логика, 56 (3) (2017), 348–353.

[98] А.Н. Рыбалов. Генерическая теорема Клини о неподвижной точке. Сибирские электронные математические известия, 14 (2017), 732–736.

[99] А.Н. Рыбалов. О генерической сложности проблемы разрешимости систем диофантовых уравнений в форме Сколема. Прикладная дискретная математика, 37 (2017), 100–106.

[100] A.N. Rybalov. Generic hardness of the Boolean satisfiability problem. Groups Complexity Cryptology, 9(2) (2017), 151–154.

[101] А.Н. Рыбалов. О генерической NP-полноте ограниченной проблемы остановки. Вестник Омского университета, 4 (2017), 22–25.

[102] А.Н. Рыбалов. О генерической сложности проблемы извлечения корня в группах вычетов. Прикладная дискретная математика, 38 (2017), 95–100.

[103] А.Н. Рыбалов. Релятивизованные генерические классы P и NP. Прикладная дискретная математика, 40 (2018), 100–104.

[104] А.Н. Рыбалов. О структуре рекурсивно перечислимых степеней генерической сводимости. Вестник Омского университета, 2 (2018), 35–41.

[105] A. N. Rybalov. A generic m-reducibility. Lecture Notes in Computer Science, 10936 (2018), 359–364.