ОТЗЫВ НАУЧНОГО КОНСУЛЬТАНТА
НА ДИССЕРТАЦИОННУЮ РАБОТУ

Рыбалова Александра Николаевича
«Генерический подход к алгоритмическим проблемам»,
представленную на соискание ученой степени
доктора физико-математических наук по специальности
01-01-06 — математическая логика, алгебра и теория чисел.

Диссертация посвящена генерическому подходу к алгоритмическим проблемам – одному из актуальных направлений исследований на стыке теории вычислимости, теории сложности вычислений и алгебры. Данное направление в настоящее время активно развивается, о чем свидетельствует большое количество работ по генерической вычислимости и сложности различных алгоритмических проблем алгебры и других разделов математики (см. библиографию настоящей диссертации).

В рамках генерического подхода алгоритмические проблемы рассматриваются для «почти всех» входов. Понятие «почти все» уточняется введением асимптотической плотности на множестве входных данных. При этом проблема может быть трудноразрешимой или вообще неразрешимой в классическом смысле, но для нее существует эффективный (полиномиальный) генерический алгоритм, который для «почти всех» входов выдает правильный ответ, а для оставшихся редких «плохих» входов выдает ответ «не знаю». Такие алгоритмы, например, были получены в конце 1970-х годов П.Эрдошем, Л. Бабаи и С.Селковым для знаменитой проблемы изоморфизма графов. Другой классический пример – это известный алгоритм симплекс-метод – А.М.Вершик, В.П.Спорышев и, независимо от них, С.Смейл доказали, что для почти всех входов он работает за полиномиальное время. В 1990-х годах в рамках проекта MAGNUS (руководители Г.Баумслаг, В.Н.Ремесленников, А.Г.Мясников) по разработке программного комплекса, реализующего классические алгоритмы комбинаторной теории групп, было экспериментально замечено, что часто трудоемкие и сложные алгоритмы для решения той или иной проблемы комбинаторной теории групп могут быть заменены простыми и эффективными тестами, которые быстро решают проблему для «почти всех» входов. Это привело к введению в 2003 году И.Каповичем, А.Г.Мясниковым, В.Шрильрайном и П.Шуппом генерического подхода. С тех пор в работах А.Г.Мясникова, В.Н.Ремесленникова, В.А.Романькова, А.В.Боровика, П.Шуппа, В.Дикерта, Р.Гилмана и других исследователей были построены эффективные генерические алгоритмы для многих неразрешимых и трудных проблем комбинаторной алгебры. В 2004 году А.Г.Мясников и Дж.Хэмкинс построили генерический алгоритм, решающий проблему остановки для машин Тьюринга с однонаправленной лентой.

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.

В диссертации изучается генерическая вычислимость и сложность различных классических алгоритмических проблем алгебры, математической логики, теории чисел и информатики. В диссертации соискатель решает проблемы, поставленные

А.Г.Мясниковым, Дж.Хэмкинсом, П.Шуппом, К.Джокушем и другими исследователями.

Диссертация состоит из введения, пяти разделов и списка литературы. В первом разделе приводятся необходимые предварительные сведения из теории вычислимости, теории вычислительной сложности и теории генерической вычислимости.

Во втором разделе диссертации А.Н.Рыбаловым получены результаты о генерической неразрешимости следующих классических алгоритмических проблем: проблема остановки для машин Тьюринга, проблема равенства слов в некоторых конечно определенных полугруппах, неразрешимые элементарные теории, десятая проблема Гильберта. Для получения этих результатов был предложен метод генерической амплификации. Этот метод из проблем, неразрешимых или трудноразрешимых в классическом смысле, позволяет получать проблемы, неразрешимые или трудноразрешимые в генерическом случае.Также, с помощью метода генерической амплификации, были доказаны генерические аналоги классических теорем Клини о неподвижной точке и Гёделя о неполноте формальной арифметики.

Третий раздел посвящен доказательству генерической трудноразрешимости следующих классических алгоритмических проблем информатики и криптографии: проблема разрешимости арифметики Пресбургера, проблема выполнимости булевых формул, проблема дискретного логарифма, проблема извлечения корня в группах вычетов, проблема поиска изоморфизма графов, проблема распознавания квадратичных вычетов. Здесь метод генерической амплификации применяется для получения генерически трудноразрешимых проблем из проблем, трудноразрешимых в классическом случае. Большинство полученных результатов о генерической трудноразрешимости опираются на известные недоказанные гипотезы о вычислительной сложности рассматриваемых проблем в худшем случае, типа гипотезы P=/=NP и P=BPP.

В четвертом разделе диссертации вводятся три типа генерических сводимостей: генерическая m-сводимость, клонирующая сводимость и генерическая тьюрингова сводимость подмножеств натуральных чисел. Первые два типа сводимостей являются частными случаями более общей сводимости третьего типа. Изучаются свойства этих сводимостей. Исследуется структура рекурсивно перечислимых степеней относительно генерической тьюринговой сводимости: доказано существование полных множеств, существование несравнимых степеней, несуществование минимальных и максимальных рекурсивно перечислимых генерических степеней. Также получен генерический аналог классической теоремы Сакса о разложении.

В пятом разделе вводится полиномиальная генерическая сводимость алгоритмических проблем, строятся примеры генерически NP-полных проблем, доказаны генерические аналоги классических теоремы Ладнера о существовании NP-неполных проблем в классе NP, не лежащих в классе P, и теоремы Бейкера-Гилла-Соловея о релятивизациях проблемы P vs NP. Последний результат говорит о том, что генерический аналог знаменитой открытой проблемы о равенстве классов вычислительной сложности P и NP не проще классической проблемы P vs NP.

В процессе работы над диссертацией соискателем были развиты методы теории вычислимости и теории сложности вычислений. В частности, им был предложен метод генерической амплификации алгоритмических проблем, который из проблем,

неразрешимых или трудноразрешимых в классическом смысле, позволяет получать проблемы, неразрешимые или трудноразрешимые в генерическом случае.

Все результаты диссертации являются новыми, представляют содержательное научное исследование, снабжены корректными доказательствами, и опубликованы в рецензируемых научных журналах. Результаты диссертации докладывались на многих международных конференциях (как в России так и за рубежом) и на семинарах в ИМ СО РАН (Омский филиал). Результаты диссертации могут использоваться для дальнейших исследований по теории вычислимости и сложности вычислений и при чтении специальных курсов по данной тематике.

Считаю, что представленная диссертация «Генерический подход к алгоритмическим проблемам» соответствует всем критериям, установленным в положении о присуждении ученых степеней, а соискатель – Рыбалов Александр Николаевич – заслуживает присуждения ему ученой степени доктора физико-математических наук по специальности 01.01.06 - математическая логика, алгебра и теория чисел.

Научный консультант
Ремесленников Владимир Никанорович
доктор физико-математических наук,
профессор, заведующий лабораторией
комбинаторных и вычислительных методов алгебры и логики
ФГБУН Институт математики им. С.Л. Соболева
Сибирского отделения Российской академии наук
адрес: 644099, г. Омск, ул. Певцова, 13
телефон: +7 (3812) 972251,
e-mail: remesl@ofim.oscsbras.ru

Ремесленников В.Н.
28.05.2018

Подпись В.Н. Ремесленникова заверяю
Начальник ОК
Шлюшинская Л.А.