

ЗАКЛЮЧЕНИЕ ОБЪЕДИНЕННОГО ДИССЕРТАЦИОННОГО СОВЕТА

Д 999.082.03, созданного на базе

федерального государственного бюджетного учреждения науки Института систем информатики им. А.П. Ершова Сибирского отделения Российской академии наук (ИСИ СО РАН),

федерального государственного бюджетного учреждения науки Института вычислительной математики и математической геофизики Сибирского отделения Российской академии наук (ИВМиМГ СО РАН),

федерального государственного бюджетного учреждения науки Института математики им. С. Л. Соболева Сибирского отделения Российской академии наук (ИМ СО РАН),

по диссертации на соискание ученой степени кандидата наук

аттестационное дело № _____

решение диссертационного совета от 25.03.2021 г. №11

О присуждении Мордвинову Дмитрию Александровичу, гражданину Российской Федерации, ученой степени кандидата физико-математических наук.

Диссертация «Автоматический вывод реляционных инвариантов для нелинейных систем дизъюнктов Хорна с ограничениями» по специальности 05.13.11 - Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей принята к защите 13 ноября 2020 года (протокол заседания № 10) объединенным диссертационным советом 999.082.03, созданным на базе федерального государственного бюджетного учреждения науки Института систем информатики им. А. П. Ершова Сибирского отделения Российской академии наук (ИСИ СО РАН), федерального государственного бюджетного учреждения науки Института вычислительной математики и математической геофизики Сибирского отделения Российской академии наук (ИВМиМГ СО РАН), федерального государственного бюджетного учреждения науки Института математики им. С.Л. Соболева Сибирского отделения Российской академии наук (ИМ СО РАН), находящимся по адресу: 630090, проспект Академика Лаврентьева, дом 6, г. Новосибирск. Совет утвержден приказом Минобрнауки России №793/нк от 24 июня 2016 года.

Соискатель Мордвинов Дмитрий Александрович, 1991 года рождения, в 2016 году окончил аспирантуру федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет», с 2018 г. по настоящее время работает в

федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет» в должности старшего преподавателя.

Диссертация выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет» на кафедре системного программирования.

Научный руководитель – Кознов Дмитрий Владимирович, доктор технических наук, доцент, профессор кафедры системного программирования федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет».

Официальные оппоненты:

- Ломазова Ирина Александровна – доктор физико-математических наук, профессор, федеральное государственное автономное образовательное учреждение высшего образования Национальный исследовательский университет высшей школы экономики, факультет компьютерных наук, департамент программной инженерии, профессор.

- Шилов Николай Вячеславович – кандидат физико-математических наук, доцент, Автономная некоммерческая организация высшего образования «Университет Иннополис», начальник лаборатории программной инженерии, дали положительные отзывы на диссертацию.

Ведущая организация – федеральное государственное бюджетное учреждение науки Институт системного программирования Российской академии наук им. В.П.Иванникова (ИСП РАН), Москва, в своем положительном отзыве, подписанном канд.физ.-мат. наук Куляминым В.В. и утвержденным директором института академиком А.И.Аветисяном, указала, что диссертация Мордвинова Дмитрия Александровича соответствует всем требованиям Положения о присуждении ученых степеней, предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук, а ее автор Мордвинов Дмитрий Александрович заслуживает присуждения ему ученой степени кандидата физико-математических наук по специальности 05.13.11 - Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Соискатель имеет 11 опубликованных работ, в том числе по теме диссертации опубликовано 5 работ, которые в полной мере отражают результаты диссертации, из них в рецензируемых научных журналах опубликовано 2 работы и 3 статьи в изданиях, включенных в международные базы цитирования RSCI, Web of Science и Scopus. В диссертации **отсутствуют недостоверные сведения**, а также неправомерные заимствования. Все результаты успешно прошли апробацию на ряде международных конференций и ведущих научных семинарах. Научные

работы соискателя посвящены исследованию задачи вывода символьных решений систем дизъюнктов Хорна с ограничениями, в рамках которого, во-первых, предложены способы частичного решения проблемы невыразительности языков ограничений для представления символьных решений систем дизъюнктов Хорна с ограничениями, во-вторых, разработаны и применены новые алгоритмы автоматического вывода символьных решений систем дизъюнктов.

Публикации в журналах, рекомендуемых ВАК РФ:

1. Мордвинов, Д.А. Направляемый свойством поиск реляционных инвариантов // Моделирование и анализ информационных систем. — 2019. — Т. 26, №. 4. — С. 550-571.

2. Мордвинов Д.А. Автоматическое доказательство корректности программ с динамической памятью / Ю.О.Костюков, К.А.Батоев, Д.А.Мордвинов, М.П.Костицын, А.В.Мисонижник //Труды Института системного программирования РАН. – 2019.- Т. 31, № 5. – С. 37-62.

Личный вклад автора: предложение исчисления символьных куч и доказательство возможности сведения поиска пространственных инвариантов к решению систем дизъюнктов Хорна с ограничениями; соавторы участвовали в обсуждении идей, постановке экспериментов, разработке алгоритма сведения для произвольных потоков управления.

Публикации в изданиях, индексируемых в SCOPUS и Web of Science:

1. Mordvinov, D. Property Directed Inference of Relational Invariants. / D. Mordvinov, G. Fedyukovich //Proceedings of the 19th Conference on Formal Methods in Computer-Aided Design (FMCAD 2019). – IEEE. — 2019. — P. 152-160.

Личный вклад автора: предложение формулировки понятия реляционного инварианта как решения нелинейных систем дизъюнктов, разработка и реализация алгоритма доказательства корректности, участие в постановке экспериментов; соавторы участвовали в обсуждении основных идей статьи, выполняли обзор предметной области.

2. Mordvinov, D. On Satisfiability of Nominal Subtyping with Variance / A. Misonizhnik, D. Mordvinov // 33rd European Conference on Object-Oriented Programming (ECOOP 2019). — Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik. – 2019. – P. 7:1-7:20.

Личный вклад автора: доказательство неразрешимости задачи невыполнимости неэкспансивного фрагмента систем типов; соавторы формализовали задачу, участвовали в улучшении доказательства, а также предложили разрешающую процедуру для полулинейного фрагмента.

3. Mordvinov, D. Synchronizing Constrained Horn Clauses / D. Mordvinov, G. Fedyukovich // LPAR-21. 21st International Conference on Logic for Programming, Artificial Intelligence and Reasoning. — 2017. — Vol. 46. — P. 338–355.

Личный вклад автора: разработка синхронизирующего преобразования системы дизъюнктов, доказательство корректности этого преобразования; соавторы предложили идею синхронизации, ставили эксперименты, участвовали в формализации и улучшении изложения идей статьи.

На диссертацию и автореферат поступили отзывы двух оппонентов, ведущей организации и четыре отзыва на автореферат диссертации. Все отзывы положительные.

Отзывы на автореферат предоставили: 1) д.ф.-м.н. профессор факультета вычислительной математики и кибернетики Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова» Захаров В.А.; 2) к.ф.-м.н. профессор кафедры математического обеспечения вычислительных систем ФГАОУ «Пермский государственный национальный исследовательский университет» Чуприна С.И.; 3) к.т.н. заведующий лабораторией логических и оптимизационных методов анализа сложных систем Института динамики систем и теории управления им. В.М. Матросова СО РАН Семенов А.А., 4) к.т.н. директор Высшей школы интеллектуальных систем и суперкомпьютерных технологий Санкт-Петербургского политехнического университета имени Петра Великого Ицксон В.М.

В отзывах отмечается актуальность темы исследования, научная новизна, теоретическая и практическая значимость полученных результатов, а также понятность и грамотность научного языка.

Основные замечания: небольшое число описок и стилистических неточностей, не раскрыт вопрос о сложности предложенных алгоритмов, избыточность формализма с мультимножествами. На все замечания в процессе защиты соискатель дал аргументированные ответы.

Выбор официальных оппонентов обосновывается их высоким уровнем компетентности и способностью оценить научную и практическую ценность диссертации. Д.ф.-м.н. Ломазова И.А. и к.ф.-м.н. Шилов Н.В. являются известными специалистами в области формальных методов и верификации программного обеспечения и имеют публикации по теме диссертации в рецензируемых научных журналах.

Выбор ведущей организации обосновывается тем, что ИСП РАН является признанным лидером в области программной инженерии и верификации программного обеспечения. Сотрудники ИСП РАН имеют значительный объём публикаций по тематике диссертации в ведущих научных изданиях и способны определить и аргументировано обосновать научную и практическую ценность диссертационной работы Мордвинова Д.А.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- **разработан** новый алгоритм синхронизации системы дизъюнктов Хорна с ограничениями, а также алгоритм автоматического вывода реляционных сертификатов выполнимости для систем дизъюнктов Хорна с ограничениями;
- **предложено** новое синхронизирующее преобразование систем дизъюнктов Хорна с ограничениями первого порядка;
- **доказана** корректность синхронизирующего преобразования, корректность и завершаемость алгоритма синхронизации систем дизъюнктов и корректность алгоритма вывода реляционных сертификатов выполнимости;
- **введен** новый класс символьных решений систем дизъюнктов Хорна с ограничениями, называемый реляционными сертификатами выполнимости, что позволило находить решения или строить опровержения в случаях, когда существующие методы не могли этого сделать.

Теоретическая значимость исследования обоснована тем, что:

- **доказана** теорема о корректности разработанного синхронизирующего преобразования;
- **использованы** современные подходы информатики к формальной верификации программ, в частности, PDR-подход, что позволило существенно повысить эффективность решателей дизъюнктов Хорна с ограничениями;
- **изложены** доказательства корректности синхронизирующего преобразования, алгоритма вывода реляционных сертификатов выполнимости и алгоритма синхронизации систем дизъюнктов;
- **раскрыта** проблема непредставимости моделей, а также проблема экспоненциального взрыва возможных вариантов при поиске решения/опровержения нелинейных систем дизъюнктов Хорна с ограничениями;
- **изучена** проблема представимости решений систем дизъюнктов Хорна с ограничениями в языках ограничений первого порядка, решена задача экспоненциального увеличения числа правил при преобразованиях таких систем;
- **проведена модернизация** методов решения нелинейных систем дизъюнктов Хорна, что позволило получать хорошие результаты при верификации реальных систем;
- **предложено** синхронизирующее преобразование, решающее проблему представимости решений нелинейных систем дизъюнктов Хорна в случае выразимости инвариантов системы в виде реляционных сертификатов.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

- **разработаны и внедрены** новые алгоритмы автоматического решения систем дизъюнктов Хорна с ограничениями, позволяющие практическое использование

предложенных методов. Разработанные алгоритмы внедрены в известный открытый SMT-решатель Z3, что говорит о признании практической полезности результатов работы научным сообществом, а также позволяет использовать созданные результаты в рамках готовой инфраструктуры;

- **определены** перспективы дальнейшего развития подходов к автоматическому определению нетривиальных стратегий синхронизации отношений нелинейных систем дизъюнктов Хорна в контексте автоматического доказательства свойств программ, манипулирующих структурами данных с произвольным доступом;

- **создан** новый метод проверки выполнимости нелинейных систем дизъюнктов Хорна путём сведения к линейным системам, что позволяет применять методы формальной верификации на основе систем дизъюнктов Хорна к существенно более широкому классу свойств программ;

- **представлены** рекомендации по практическому использованию разработанных алгоритмов для модульной реализации инструментов автоматического доказательства корректности программного кода, вывода уточняющих типов произведений функциональных программ, автоматического аннотирования императивных программ в декартовой логике Хоара, а также проверки эквивалентности программ и проверки свойств невмешательства, являющихся важными в области компиляторов и компьютерной безопасности.

Оценка достоверности результатов исследования выявила:

- для экспериментальных работ - использование сертифицированного и зарегистрированного в Федеральной службе по интеллектуальной собственности программного обеспечения и воспроизводимость результатов исследования для различных задач верификации;

- **теория построена** на последних достижениях в области формальной верификации программ и систем;

- **идея базируется** на анализе, обобщении и развитии передового опыта в области разработки методов формальной верификации;

- **использованы** опубликованные данные по рассматриваемой теме, которые сравнивались с авторскими данными;

- **установлено** качественное улучшение авторских результатов по сравнению с аналогичными результатами, представленными в различных источниках, использованы современные методики сбора и обработки исходной информации.

Личный вклад соискателя заключается в выполнении основного объема теоретических и экспериментальных исследований, изложенных в диссертационной работе, включая постановку исследовательских задач, создание подходов, методов и алгоритмов для их решения, выполнение доказательств утверждений и теорем, реализация предложенных алгоритмов и выполнение экспериментального исследования. Конфликт интересов с соавторами

отсутствует. Все выносимые на защиту результаты получены автором лично. Соискатель лично участвовал во всех научных экспериментах, апробации достигнутых результатов, подготовке научных публикаций по теме работы.

На заседании 25 марта 2021 года диссертационный совет принял решение присудить Мордвинову Д.А. учёную степень кандидата физико-математических наук по специальности 05.13.11 - Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

При проведении открытого голосования диссертационный совет в количестве 16 человек, из них 8 докторов наук по специальности 05.13.11 - Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей, участвовавших в заседании, из 21 человек, входящих в состав совета, проголосовали: за 16, против нет. воздержавшихся – нет.

Председатель диссертационного совета

Д 999.082.03

д-р физ.-мат. наук, профессор



А.Г.Марчук

ВРИО ученого секретаря

диссертационного совета

д-р физ.-мат. наук, профессор

В.Л.Селиванов

25.03.2021