УТВЕРЖДАЮ
Проректор по научной работе
Университета ИТМО
д.т.н., профессор
_____ В.О. Никифоров
«15» февраля 2024 г.

ОТЗЫВ

ведущей организации на диссертационную работу
Костюкова Юрия Олеговича
«Автоматический вывод индуктивных инвариантов программ
с алгебраическими типами данных», представленную на соискание ученой степени кандидата физико-математических наук по специальности ***2.3.5 – Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей***

Актуальность темы диссертации

Диссертационная работа Костюкова Юрия Олеговича посвящена вопросам автоматического вывода индуктивных инвариантов для программ с алгебраическими типами данных (АТД). Работа относится к области формальных методов и статического анализа, связана с технологиями верификации программ и применения Хорн-решателей. Эти технологии играют ключевую роль в обеспечении корректности программных систем, что становится все более важным с увеличением их сложности и проникновением в различные сферы человеческой деятельности.

Основная проблема, решаемая в диссертации, заключается в невозможности выразить индуктивные инварианты большинства программ, использующих алгебраические типы данных, в языке ограничений. Это приводит к тому, что существующие алгоритмы вывода индуктивных инвариантов не могут построить для таких программ индуктивный инвариант, что затрудняет их автоматическую верификацию. Решение этой проблемы важно для обеспечения корректности программ, использующих алгебраические типы данных, и для развития методов автоматического вывода индуктивных инвариантов.

Таким образом, следует констатировать, что актуальность диссертационной работы Костюкова Ю.О. не вызывает сомнений.

Личный вклад

На основании документов, представленных соискателем, можно сделать вывод, что результаты, выносимые на защиту, получены автором полностью самостоятельно.

Степень обоснованности научных положений, выводов и рекомендаций

Выбор направления исследования основан на тщательном анализе предыдущих работ и проблем в области автоматического вывода индуктивных инвариантов. Это позволило автору диссертации прийти к такой постановке задачи, которая представляет интерес как с теоретической, так и с практической точки зрения. Выводы и рекомендации диссертационной работы достаточно полно и хорошо аргументированы.

В процессе работы диссертантом были использованы методики и подходы, разработанные предшественниками в области автоматического вывода индуктивных инвариантов программ, и предложены новые собственные классы индуктивных инвариантов и методы автоматического вывода индуктивных инвариантов в них. Корректность и полнота предложенных алгоритмов формально доказана средствами математической логики.

Оценка научной новизны и достоверности основных научных положений, выводов и рекомендаций

Результаты, выносимые на защиту, являются новыми и вносят существенный вклад в теорию и практику верификации программ с помощью решения систем дизъюнктов Хорна с ограничениями.

Достоверность полученных результатов обеспечивается формальными доказательствами, а также компьютерными экспериментами на публичных и общепринятых в области тестовых наборах. Полученные в диссертации результаты согласуются с результатами других авторов в области вывода индуктивных инвариантов.

Также важным свидетельством достоверности результатов диссертации являются публикации на ведущих мировых конференциях по языкам программирования и верификации PLDI (A*) и LPAR (A), а также фактом, что комплекс созданных в диссертации методов в 2021 и 2022 годах занял 2 и 1 место на международных соревнованиях CHC-COMP в секции по выводу индуктивных инвариантов для программ с алгебраическими типами данных.

По совокупности выносимых на защиту положений настоящую работу можно квалифицировать как решение важной научной задачи в области математического и программного обеспечения вычислительных систем, комплексов и компьютерных сетей. Следует отметить, что предлагаемые методы автоматического вывода индуктивных инвариантов программ и построенный класс индуктивных

инвариантов вносят весомый вклад в теорию и практику верификации программных продуктов.

Теоретическая и практическая значимость исследования

Теоретическая значимость диссертации заключается в том, что предложенные новые подходы к выводу индуктивных инвариантов программ, фактически, ортогональны существующим, поэтому они могут быть перенесены на программы над другими теориями, например, над теорией массивов, а также могут усилить существующие подходы к выводу индуктивных инвариантов. Также важным теоретическим вкладом является адаптация лемм о «накачке» к языкам первого порядка: эти леммы открывают путь к фундаментальному исследованию проблемы невыразимости индуктивных инвариантов в языках первого порядка и проектированию новых классов индуктивных ин вариантов программ.

Практическая значимость диссертации заключается в том, что предложенные методы могут быть применены при создании статических анализаторов для языков с алгебраическими типами данных (Rust, Scala, Solidity, Haskell и OCaml), а также при разработке верификаторов и генераторов тестовых покрытий для приложений на этих языках. В частности, выполненная пилотная реализация предложенных в диссертации методов может быть использована в качестве «ядра» для статического анализатора языка Rust при помощи фреймворка RustHorn. Таким образом результаты работы рекомендуются к использованию в компаниях по разработке ПО (в частности, в телекоммуникационных компаниях), а также учебных процесса в университете ИТМО и других университетах РФ.

Общая характеристика публикаций автора диссертации

Результаты работ неоднократно докладывались и обсуждались на российских и международных конференциях и семинарах. Основные результаты диссертации опубликованы в 4 научных работах; все они зарегистрированы в РИНЦ. 2 статьи опубликованы в журналах из «Перечня российских рецензируемых научных журналов, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёных степеней доктора и кандидата наук» и 2 статьи в изданиях, входящих в базы цитирования Scopus и Web of Science.

Замечания по диссертационной работе

1. Диссертация имеет логичную структуру и написана понятным языком. Однако, в тексте имеются отдельные опечатки, неудачные формулировки, затрудняющие понимание.
2. При изложении результатов исследования в тексте диссертации избран стиль примеров и пояснений, что очень повышает понятность материала. Однако не хватает структурного, покомпонентного

четкого изложения предложенных методов вывода индуктивных инвариантов (гл. 2 и 3).

3. Леммы о накачке являются важным теоретическим результатом диссертации. Для их более широкого применения теоретиками важен ответ на следующий вопрос: можно ли обобщить эти леммы на различные расширения языка первого порядка алгебраических типов данных – например, арифметикой?

Заключение

Диссертация соответствует критериям, предъявляемым к диссертациям на соискание ученой степени ***кандидата*** наук Приказом от 19.11.2021 № 11181/1 «О порядке присуждения ученых степеней в Санкт-Петербургском государственном университете», а сам соискатель ***Костюков Юрий Олегович*** заслуживает присуждения учёной степени кандидата физико-математических наук по специальности ***2.3.5 – Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей***. Нарушения пунктов 9 и 11 указанного Порядка в диссертации не обнаружены.

Диссертационная работа обсуждалась на заседании диссертационного совета 04.22.00 федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет ИТМО».

Настоящий отзыв рассмотрен и одобрен на заседании указанного диссертационного совета, протокол №1 от «8» февраля 2024 г.

Председатель диссертационного
совета 04.22.00
д.т.н., профессор Бессмертный Игорь Александрович

Сведения о ведущей организации:
Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО» (Университет ИТМО).
Почтовый адрес: 197101, г. Санкт-Петербург, пр-т Кронверкский, д. 49, лит. А
Телефон: (812) 480-00-00
Веб-сайт: https://itmo.ru
Адрес электронной почты: od@itmo.ru