ОТЗЫВ

члена диссертационного совета Владимирова Андрея Георгиевича на диссертацию Юрия Олеговича Костюкова на тему «Автоматический вывод индуктивных инвариантов программ с алгебраическими типами данных», представленную на соискание учёной степени кандидата физико-математических наук по специальности 2.3.5. Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей

Программные системы становятся всё более распространенными и всё более сложными, поэтому вопрос об их корректности является чрезвычайно актуальным. В последнее время появилось большое количество формальных методов для верификации и поиска ошибок в программах с большим пространством возможных состояний. Однако основные исследования в этой области посвящены классическим типам данных и уделяют мало внимания новым типам данных из более современных языков программирования, таких как Haskell и Rust, в частности, алгебраическим типам данных (АТД).

Для обеспечения корректности программ, использующих АТД, могут быть использованы методы дедуктивной верификации и вывода уточняющих типов. Однако они требуют предоставления пользователем индуктивных инвариантов программ, формулировка которых является сложной задачей. Таким образом, задача верификации программ с АТД сводится к задаче автоматического вывода индуктивных инвариантов, которая может быть сформулирована как задача проверки выполнимости системы дизъюнктов Хорна с ограничениями.

Диссертация Костюкова Юрия Олеговича нацелена на решение проблемы поиска выразительных представлений для инвариантов функциональных программ с АТД, а также их эффективного вывода. Современные методы проверки выполнимости систем дизъюнктов Хорна с ограничениями для программ с АТД выводят инварианты в крайне ограниченном языке теории АТД, что не позволяет использовать эти методы на практике: вне зависимости от сложности и качества

реализации полученный инструмент будет пропускать все инварианты, не представимые в этом языке. Поэтому заявленную тему можно с уверенностью назвать актуальной как с теоретической, так с и практической точки зрения. В последние годы подобные инструменты всё чаще используются для верификации программ, особенно в области проверки корректности самоисполняемых смарт-контрактов. Соответственно, постоянно создаются новые методы — каждый год появляется значительное количество статей по этой теме на конференциях CAV, POPL, PLDI (конференции A*) и др.

В диссертации предложены три новых метода автоматического вывода индуктивных инвариантов, основанные на автоматах над деревьями. Последние оказываются более эффективным представлением индуктивных инвариантов программ с АТД, чем логика первого порядка, поэтому они уже были изучены ранее. Однако автор диссертации предложил для регулярных и синхронных регулярных инвариантов (основаны на автоматах над деревьями) новые, нестандартные методы вывода, использующие алгоритмы трансформации программ и поиска конечных моделей. Предложенные методы основываются на классической теореме об изоморфизме автоматов над деревьями и конечных моделей.

Кроме того, Ю.О. Костюков предложил новое представление индуктивных инвариантов, основанное на булевой комбинации формул теории АТД и автоматов над деревьями. Также в работе предложен метод вывода инвариантов для нового представления, позволяющий объединить два эффективных метода с целью вывода более сложных инвариантов. Эксперименты показывают, что предложенный метод позволяет доказать корректность существенно бо́льшего числа программ, чем дочерние методы, используемые по отдельности.

Наконец, в диссертации проведено теоретическое сравнение предложенных и существующих представлений индуктивных инвариантов, а также выполнена пилотная программная реализация предложенных методов. Экспериментальное сравнение с существующими инструментами и победа разработанного инструмента на международных соревнованиях верификаторов показывают, что предложенные методы являются перспективной практической разработкой.

Текст диссертации написан четким и ясным профессиональным языком, в соответствии с современными научными стандартами. Полученные результаты опубликованы и изложены на ведущих международных конференциях по данной теме (среди которых стоит выделить конференцию PLDI ранга A* и конференцию LPAR ранга A), а так же в русскоязычных журналах.

На основании вышеизложенного хочу заключить, что работа Костюкова Юрия Олеговича на тему «Автоматический вывод индуктивных инвариантов программ с алгебраическими типами данных» соответствует основным требованиям, установленным Приказом от 19.11.2021 № 11181/1 «О порядке присуждения научных степеней в Санкт-Петербургском государственном университете», а сам соискатель, Костюков Юрий Олегович, заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.5. Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Член диссертационного совета

доктор физико-математических наук,
старший научный сотрудник
Института прикладного анализа и стохастических
процессов им. К. Вейерштрасса
(Германия, г. Берлин), Владимиров Андрей Георгиевич

29 января 2024 года