Отзыв

члена диссертационного совета Льва Владимировича Уткина на диссертацию Юрия Олеговича Костюкова

«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

Данная диссертационная работа посвящена актуальной проблеме – верификации программного обеспечения (доказательство корректности программ). В последние годы в этой области наметился существенный сдвиг от сугубо теоретических построений к эффективным практическим применениям. При этом важным конструктивным элементом верификации ПО является индуктивный инвариант, наличие которого свидетельствует о корректности соответствующей программы. Автоматический вывод таких инвариантов для различных видов программ является актуальной задачей. Однако тут возникает проблема баланс между выразимостью и разрешимостью языков представления индуктивных инвариантов.

Диссертационное исследование Юрия Олеговича посвящено автоматическому выводу индуктивных инвариантов для функциональных программ с алгебраическими типам данных (АТД) – списков, деревьев и т.д. В работе подробно описал контекст исследования, начиная с исторического развития инструментария верификации и заканчивая современными подходами к статическому анализу программ. Актуальность исследования обоснована растущим использованием АТД в современном программировании и недостаточной разработанностью соответствующих подходов к верификации.

В работе предложен новаторский метод автоматического вывода индуктивных инвариантов, использующий автоматы над деревьями для выражения рекурсивных отношений в программных структурах. Данный метод значительно расширяет возможности анализа реальных программ, учитывая их рекурсивную природу. Отличительной чертой является использование поиска конечных моделей.

Также Юрий Олегович разработал эффективный метод вывода индуктивных инвариантов для класса задач, традиционно считающегося сложным для автоматического анализа – речь идет о синхронных автоматах над деревьями. Предложенный метод позволяет моделировать не только рекурсивные, но и синхронные отношения в программах, тем самым расширяя класс решаемых задач и повышая точность верификации.

Кроме этого, в диссертации введён новый класса индуктивных инвариантов, основаный на булевой комбинации классических инвариантов и автоматов над деревьями, который является значительным теоретическим вкладом диссертации. Для этого класса разработан метод совместного вывода инвариантов, который значительно улучшает эффективность анализа программ с АТД.

Наконец, диссертация включает в себя теоретическое сравнение новых и существующих классов индуктивных инвариантов, подкрепленное формулировкой и доказательством лемм о "накачке" для языков ограничений. Данное исследование, включая леммы о "накачке", является значительным теоретическим вкладом Юрия Олеговича в современную математическую логику.

Следует отметить, что помимо теоретических результатов диссертационная работа включает в себя значимую практическую часть – пилотную реализацию разработанных методов и выполнение экспериментального исследования. Последнее показало, что предложенные автором методы решили в 3,74 раза больше задач из стандартного тестового набора, чем существующие методы.

Результаты диссертации опубликованы в следующих конференциях, ведущих по данной тематике – международной конференции по логическому программированию и автоматизированным рассуждениям (LPAR, A), международной конференции по разработке программного обеспечения (PLDI,

A*). Также имеются необходимое количество публикации в российских журналах из списка ВАК.

Диссертация имеет большое значение для теории и практики формальных методов верификации программ. Предложенные методы могут быть использованы при создании статических анализаторов для языков с алгебраическими типами данных, а также в разработке верификаторов и генераторов тестовых покрытий для таких языков, как Rust, Scala, Solidity, Haskell и OCaml.

В работе имеются следующие недостатки.

1. Иногда при формулировке математических утверждений наблюдается недостаток описаний на русском языке. Например, в лемме 1 главы 2 (стр. 26) читаем: «Тогда <H, X_1, ..., X_k> является ...», и не понятно, идёт ли речь о кортеже множеств, моделей или же расширении модели множествами.
2. Некоторые примеры иногда оказываются плохо читаемыми, поскольку имеется слишком большое количество скобок. Например, в примере 4 (раздел 2.3, стр. 29) имеем терм «S(S(S(S(Z))))». Хорошо было бы использовать скобки разных размеров или применять альтернативный синтаксис, например, «S4(Z)».
3. Некоторые утверждения, относящиеся скорее к выводам, разбросаны по тексту глав. Например, абзац «Использование метода для вывода инвариантов» (с. 29) говорит о невозможности расширенного применения предложенного метода, хотя основное применение метода будет рассмотрено только в следующих за этим абзацем разделах.
4. Некоторые формулы тяжело читать из-за того, что они разрываются переносом строки. Например, в формулировке лемме 4 (раздела 3.1.1, стр. 34) имеем перенос строки после следующего фрагмента: «L ∈».

Указанные недостатки не влияют на положительную оценку работы.

Таким образом, можно сделать вывод о том, что диссертация Ю.О. Костюкова на тему «Автоматический вывод индуктивных инвариантов программ с алгебраическими типами данных» соответствует требованиям, установленным Приказом от 19.11.2021 № 11181/1 «О порядке присуждения

научных степеней в Санкт-Петербургском государственном университете», а сам соискатель Юрий Олегович Костюков заслуживает присуждения ему ученой 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.

Член диссертационного совета,
профессор, доктор технических наук, профессор
Высшей школы технологий искусственного интеллекта
Санкт-Петербургского политехнического университета Петра
Великого (СПбПУ)
Лев Владимирович Уткин