ОТЗЫВ

члена диссертационного совета Гавриловой Татьяны Альбертовны 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 научной специальности 2.3.5. Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей

Диссертация посвящена решению одной из основных проблем в области формальных методов – автоматическому выводу индуктивных инвариантов для программ. При этом рассматриваются программы, использующих алгебраические типы данных. Эта задача важна, так как алгебраические типы данных активно используются в функциональных языках программирования, а также в языках спецификации самовыполняющихся контрактов. Однако язык ограничений алгебраических типов данных не позволяет выразить индуктивные инварианты для большинства реальных программ, что приводит к тому, что современные Хорн-решатели не могут автоматически доказывать корректность таких программ.

В представленном диссертационном исследовании были получены следующие новые результаты.

1. Предложен эффективный метод автоматического вывода индуктивных инвариантов, основанных на автоматах над деревьями; при этом данные инварианты позволяют выражать рекурсивные отношения в большем количестве реальных программ; метод базируется на поиске конечных моделей.
2. Предложен метод автоматического вывода индуктивных инвариантов, основанный на трансформации программы и поиске конечных моделей, в сложном для автоматического вывода инвариантов классе, основан ном на синхронных автоматах над деревьями; этот класс инвариантов позволяет выражать рекурсивные и синхронные отношения.
3. Предложен класс индуктивных инвариантов, основанный на булевой комбинации классических инвариантов и автоматов над деревьями, который, с одной стороны, позволяет выражать рекурсивные отношения в реальных программах, а, с другой стороны, позволяет эффективно выводить индуктивные инварианты; также предложен эффективный

метод совместного вывода индуктивных инвариантов в этом классе по средством вывода инвариантов в подклассах.

4. Проведено теоретическое сравнение классов индуктивных инвариантов, существующих и предложенных в рамках диссертации; в том числе сформулированы и доказаны леммы о «накачке» для языка ограничений и для языка ограничений расширенного функцией размера терма.

Диссертация состоит из введения, шест глав и заключения, имеет объем 110 страниц, её список литературы содержит 128 наименований. Имеется достаточное количество публикаций по теме диссертации, которые выполнены в ведущих зарубежных издания по тематике, а также в российских журналах из перечня ВАК.

Ниже представлен краткий обзор диссертации по главам.

Во введении объяснена актуальность и степень проработанность данной тематики, дана постановка задачи, перечислены результаты диссертационного исследования, выносимые на защиту, показано их соответствие паспорту специальности 2.3.5 и кратко изложена их научная новизна, объяснена теоретическая и практическая ценность диссертации, сделан обзор публикаций по диссертации.

В **первой главе** дан обзор истории развития верификации программного обеспечения, а также объяснены основные понятия результаты, используемые в исследовании.

Во **второй главе** описан метод автоматического вывода индуктивных инвариантов, основанный на автоматах над деревьями. Этот метод позволяет выражать рекурсивные отношения, характерные для большого количества реальных программ. Главная научная новизна этого метода заключается в использовании процесса поиска конечных моделей, что обеспечивает значительное расширение класса программ, корректность которых может быть автоматически проверена.

В **третьей главе** описан метод автоматического вывода индуктивных инвариантов для класса программ, осложненного наличием синхронных автоматов над деревьями. Этот метод расширяет возможности выражения рекурсивных и синхронных отношений, что является ключевым для анализа и верификации широкого круга программ. Отличительная черта предложенного метода - комбинация трансформации программы с поиском конечных моделей, что представляет собой заметный прогресс в области автоматического вывода индуктивных инвариантов.

В **четвёртой главе** представлен новый класс индуктивных инвариантов, которые объединяют в себе булеву комбинацию классических инвариантов и автоматов над деревьями. Такой подход позволяет не только выражать рекурсивные отношения, но и обеспечивает эффективный вывод индуктивных инвариантов. Помимо нового класса индуктивных инвариантов в этой главе представлен также метод совместного вывода соответствующих инвариантов.

В **пятой главе** выполнено теоретическое сравнение существующих и предложенных в работе классов индуктивных инвариантов. Сформулированы и

доказаны леммы о «накачке» языка ограничений и его расширениями, что позволяет глубже изучить структуру и возможности применения различных классов инвариантов для решения задач верификации.

В **шестой главе** описана пилотная программную реализацию предложенных автоматических методов вывода индуктивных инвариантов на языке программирования F#. Также в этой главе представлено экспериментальное исследование, выполняющее созданных методов с существующими на стандартном тестовом наборе «Tons of Inductive Problems». Показано преимущество предложенных методов: предложенные методы смогли решить в 3,74 раза больше задач, чем наилучший из существующих. Этот факт является существенным аспектом практической значимости результатов диссертации.

Данная диссертационная работа хорошо сфокусирована, само исследование выполнено в тесной связи с международным научным сообществом. Текст диссертации выверен, является грамотным с точки зрения русского языка, а также математически корректен. Каждая глава содержит краткие выводы, что значительно облегчает ознакомление с материалом представленного исследования. Работа содержит большое число примеров с подробными объяснениями, что существенно облегчает прочтение и понимание диссертации.

Однако работа не свободна от ряда недостатков.

1. При описании модификации подхода CEGAR (глава 4) было бы целесообразно представить общую схему подхода: очень трудно собрать всю информацию этой главы единое целое, опираясь только на фрагменты псевдокода. В целом, работу бы украсило б*о*льшее число рисунков, выполненных в роли «принципиальной схемы», главной иллюстрации той или иной идеи.
2. Наблюдается склонность автора к минимализму в формулировках на русском языке, например, на стр. 40 (теорема 11) можно было бы пояснить утвердительную часть теоремы словами.
3. В работе содержатся опечатки, например, на стр. 20 имеется лишняя запятая в следующем фрагменте «путем добавления в сорта Int, операций из арифметики Пресбургера». Кое-где встречаются неудачные англицизмы, например, «бэкенд-решатель» (стр. 86).
4. В выводе синхронных регулярных инвариантов размер формул может расти экспоненциально в зависимости от типа синхронизации, используемой в автомате (глава 3, раздел 3.2.1). Можно ли обойти это ограничение, оставаясь при этом в достаточно выразительном классе инвариантов?

Тем не менее, эти недостатки не влияют на общую 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 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.

19.02.2024

Член диссертационного совета,

Гаврилова Татьяна Альбертовна

Доктор технических наук,
профессор кафедры информационных технологий в менеджменте

Высшая школа менеджмента
Санкт-Петербургский государственный Университет
Волховский пер.3, 199004, СПб,

gavrilova@gsom.spbu.ru
https://gsom.spbu.ru/about-gsom/faculty/gavrilova/