Отзыв

члена диссертационного совета **СПбГУ А2.3.5.23.15468 Шалыто Анатолия Абрамовича** 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»

При верификации программного обеспечения важную роль играет задача автоматического вывода индуктивных инвариантов. Эти инварианты специфичны для различных фрагментов программ — циклов, арифметики, работы с массивами и т. д. В настоящее время в функциональных программах активно используются алгебраические типы данных (АТД). Соответственно, для успешной верификации программ с АТД требуются методы, способные автоматически выводить инварианты, учитывающие рекурсивные и синхронные отношения между структурами данных.

Предшествующие исследования в этом направлении были ограничены классическими символьными инвариантами, которые не способны адекватно выражать индуктивные свойства программ, использующих АТД.

В диссертации были получены следующие новые научные результаты.

1. Метод автоматического вывода индуктивных инвариантов, основанных на автоматах над деревьями и позволяющих выражать рекурсивные отношения для значительного числа программ.

2. Метод автоматического вывода индуктивных инвариантов в классе инвариантов, основанных на синхронных автоматах над деревьями.

3. Новый класс индуктивных инвариантов, основанный на булевой комбинации классических инвариантов и автоматов над деревьями, а также метод совместного вывода индуктивных инвариантов этого класса посредством вывода инвариантов в комбинируемых подклассах.

4. Проведена теоретическая классификация существующих и предложенных классов индуктивных инвариантов.

Текст диссертации состоит из введения, шести глав и заключения. Объём диссертации составляет 110 страниц, список литературы содержит 128 наименований.

Основные результаты диссертационного исследования изложены в четырех статьях, две из которых опубликованы в журналах, рекомендованных ВАК, а две — в трудах конференций, индексируемых *Web of Science/Scopus* (в трудах конференции *PLDI*, имеющей ранг A*, и *LPAR*, имеющей ранг A).

Ниже представлен обзор диссертации по главам.

Во введении обоснована актуальность исследования, выполнена постановка задачи, представлены результаты, выносимые на защиту, описана их научная новизна и соответствие паспорту специальности, описана апробация работы и сделан обзор публикаций по теме исследований.

В первой главе выполнен обзор предметной области, а также основных понятий и результатов, необходимых для проведенного исследования. Во второй главе описан метода автоматического вывода индуктивных инвариантов, основанных на автоматах над деревьями. Этот метод расширяет класс выразимости инвариантов, включая рекурсивные отношения, что, в свою очередь, расширяет возможности верификации программ, используемых на практике. Важность данного метода несомненна, поскольку он позволяет эффективно решать задачи, ранее недоступные для автоматизации. Научная новизна метода состоит в использовании конечных моделей как инструментария для поиска индуктивных инвариантов в новом классе, что демонстрирует оригинальность подхода.

В третьей главе представлен метод автоматического вывода индуктивных инвариантов, основанный на синхронности и автоматах над деревьями. Важность предложенного метода состоит в том, что он

разрешает класс задач, достижимых для автоматического вывода, в случаях, когда взаимодействие рекурсии и синхронности привносит дополнительную сложность.

В четвёртой главе описывается новый класс индуктивных инвариантов, который сочетает классические инварианты и автоматы над деревьями. Данный класс сохраняет способность выражать рекурсивные отношения и, одновременно, обладает достаточной эффективностью для автоматизированного вывода индуктивных инвариантов. В главе также описывается метод автоматического вывода индуктивных инвариантов для предложенного класса инвариантов.

В пятой главе представлено теоретическое исследование по сравнению классов индуктивных инвариантов, релевантных для АТД — существующих и предложенных в рамках данного исследования. Исследуется замкнутость этих классов относительно теоретико-множественных операций, разрешимости, выразимости рекурсивных отношений и т. д. Также исследуются отношения этих классов между собой — включение, пересечение и отделимость.

В шестой главе описана программная реализация разработанных методов и результаты экспериментального исследования на стандартном наборе задач *Tons of Inductive Problems*, содержащим задачи с АТД. Экспериментальное исследование показало, что представленные в диссертации методы решают совокупно более, чем в три раза больше задач из тестового набора, чем каждый из существующих методов. Также в этой главе представлено соотнесение предложенных методов и существующих, реализованных в известных Хорн-решателях *Spacer*, *Racer*, *Eldarica*, *VeriCaT*, *HoIce* и *RCHC*.

В заключении приведены результаты диссертационного исследования, а также описаны направления дальнейших исследований по этой тематике.

В целом следует отметить, что диссертация написана хорошим научным языком, математический аппарат используется адекватно и грамотно, работа включает значительное число примеров и пояснений, и встроена в международный научный контекст.

Следует отметить, что теоретической ценностью работы являются предложенные новые методы вывода индуктивных инвариантов для программ с АТД, новый класс индуктивных инвариантов, теоретическое исследование классов индуктивных инвариантов, актуальных для АТД. Следует особо выделить сформулированные и доказанные леммы о «накачке» для ограничений, включая те, которые расширены функцией размера терма. Эти леммы могут быть полезны для проведения фундаментальных исследований в этой области.

Практической ценностью данный работы является программная реализация предложенных методов, а также экспериментальное исследование, демонстрирующее практическую эффективность предложенных теоретических результатов. Также предложенные методы могут быть повторно использованы для разработки практических инструментов доказательства корректности программ с арифметикой, массивами и т. д.

Однако представленная диссертационная работа не свободна от некоторых недостатков.

1. Поскольку в каждой главе предложен некоторый метод, главы целесообразно начинать псевдокодом, схемой алгоритма, а также текстовым описанием всех шагов предлагаемого метода. Например, рисунок 2.1 (стр. 31) мог бы служить такой схемой алгоритма для главы 2, но у него есть существенный недостаток: на нём присутствуют промежуточные объекты, но отсутствуют некоторые конструктивные шаги соответствующего метода.

2. Некоторые встраиваемые в текст объекты (рисунки, листинги, формулы и т. п.) смешиваются друг с другом, разрываются с текстом, который их описывает, что существенно затрудняет чтение. Например, на стр. 52 оказался рисунок автомата, который существенно связан с последним абзацем стр. 51, но при этом под этим рисунком находится ещё и листинг кода.

3. Из-за того, что чаще всего в тексте используются однотипные скобки, некоторые формулы трудно читать, вдобавок, в них оказываются ошибки. Например, в последнем дизъюнкте на стр. 43 содержится лишняя закрывающая скобка.

Вместе с тем эти недостатки не влияют на общую положительную оценку работы.

В заключении 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.

21.02.2024

Доктор технических наук, профессор,
профессор факультета «Информационные технологии и программирования» Университета ИТМО

Анатолий Абрамович Шалыто