ОТЗЫВ

председателя диссертационного совета

на диссертацию Юрия Олеговича Костюкова на тему

«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 исследования. Верификация функциональных программ крайне актуальна в таких областях как авионика, криптография и финансовые технологии. Функциональные языки программирования обладают рядом свойств, которые облегчают процесс формальной верификации. Среди них — неизменяемость данных, «чистота» функций и алгебраические типы данных (АТД). АТД позволяют строить сложные типы из более простых с помощью операций «произведения» (как правило, это кортежи или записи) и «суммы» (часто в виде вариантов или объединений), что добавляет выразительность системе типов соответствующего языка программирования и позволяет компилятору осуществлять дополнительные проверки, уменьшая вероятность ошибок во время выполнения. АТД активно используются в таких языках как Haskell, OCaml, F#, Scala и др. В этих языках типы данных могут быть определены пользователем таким образом, чтобы точно описывают предметную область, и программы могут быть проверены на соответствие этим типам. Именно поэтому основная цель диссертации — исследование и разработка методов автоматической верификации программ с АТД — является крайне востребованной.

Верификация — это прежде всего процесс доказательства корректности программы средствами математической логики, основанный на формальных спецификациях и автоматическом доказательстве теорем. По этой причине верификация наследует проблемы математической логики, одна из которых — проблема выразительности логических систем. При верификации эта проблема возникает как проблема выразительности абстракций, используемых при автоматизации верификации. Такая автоматизация требуется, чтобы верификация была практически применима, т.е. чтобы необходимость вручную доказывать корректность программ была сведена к минимуму.

Особенно остро проблема выразительности логической системы стоит в контексте верификации, основанной на выводе индуктивных инвариантов программ. Используемые здесь методы теоретически ограничены выразительностью языка, в котором они представляют индуктивные инварианты. Различные по выразительности языки представления индуктивных инвариантов — классы инвариантов, — а также методы автоматического вывода индуктивных инвариантов в этих классах представлены и изучены в диссертации Юрия Олеговича.

Содержание работы. Диссертационная работа написана на 110 страницах в версии на русском языке, состоит из введения, шести глав, заключения, списка литературы из 128 наименований. *Первая глава* посвящена представлению предметной области, в ней автор аккуратно описывает литературу и текущее состояние проблемы выразимости индуктивных

инвариантов, а также описывает системы дизъюнктов Хорна и дает основные определения. Во *второй главе* приводится новый метод автоматического вывода индуктивных инвариантов систем над алгебраическими типами данных при помощи инструментов автоматического доказательства теорем. В *третьей главе* рассмотрен класс синхронных регулярных инвариантов, и в *четвертой главе* предложен и описан метод вывода комбинированных инвариантов. *Пятая глава* посвящена теоретическому сопоставлению существующих и предложенных автором классов индуктивных инвариантов для программ с алгебраическими типами данных. Программная реализация предложенных методов описывается в *шестой главе*, где также проводится подробное сравнение Хорн-решателей и обсуждаются результаты их работы на тестовом наборе данных.

Научная новизна и значимость результатов. В рамках комплексного исследования описанной проблематики каждое положение, вынесенное на защиту, имеет большую значимость. К основным новым научным результатам Юрия Олеговича, полученным в данном диссертационном исследовании, можно отнести следующее.

1. Предложен новый метод автоматического вывода инвариантов, выразимых автоматами над деревьями. Несмотря на то, что автоматы над деревьями широко применяются в верификации, они редко применяются в качестве основы для языка индуктивных инвариантов. Предложенный метод строит модель для условий верификации программы с АТД в свободной семантике. В работе показано, как по этой свободной модели можно получить модель исходной программы в семантике АТД.

2. Предложен новый метод вывода инвариантов, выразимых синхронными автоматами над деревьями, которые обобщают обычные автоматы. Этот метод строит по программе формулу логики первого порядка в свободной теории, описывающей автомат, выражающий индуктивный инвариант исходной программы.

3. Предложен новый класс комбинированных инвариантов, выразимых в расширении теории алгебраических типов предикатами принадлежности произвольному множеству термов. В работе также предложен метод вывода инвариантов, выразимых в данном языке. Этот метод позволяет верифицировать уникальные системы, когда множества в предикатах принадлежности не выражаются в языке первого порядка.

4. Проведено теоретическое сравнение всех рассмотренных в работе языков для выражения индуктивных инвариантов. Важным вкладом этого теоретического сравнения является разделение классов множеств, выразимых рассмотренными языками. Для него были сформулированы леммы о накачке для языков первого порядка, которые позволяют доказывать невыразимость заданного множества в таких языках.

5. Реализованы все предложенные методы и проведено экспериментальное сравнение с существующими инструментами. Экспериментальное исследование позволяет

понять, какие из предложенных методов и языков для выражения инвариантов лучше ведут себя на практике.

Степень обоснованности научных положений. Достоверность полученных научных результатов обусловлена строгим доказательством всех сформулированных математических утверждений. Результаты, представленные в диссертационной работе Ю.О. Костюкова, были доложены на многих российских и международных конференциях высокого уровня. Основные результаты диссертации опубликованы в четырех печатных изданиях, в том числе, две публикации из них – в научных изданиях, рекомендованных ВАК, и две – в трудах высокорейтинговых конференций, которые проиндексированы в наукометрической базе Scopus. Содержание диссертации соответствует специальности 2.3.5. Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей.

Замечания и вопросы к диссертационной работе. Работа производит положительное впечатление, она имеет четкую структуру. Предметная область аккуратно описана в работе, даются необходимые ссылки на известные результаты. Предложенные автором методы реализованы в виде программного продукта и их работа, также как и работа существующих методов продемонстрирована на тестовом наборе данных. Результаты этой работы подробно проанализированы и сравнение этих методов с описанием преимуществ предложенных Ю.О. Костюковым методов приведено в главе 6. В работе имеется достаточное число примеров, что существенно облегчает чтение диссертации.

К работе имеется ряд следующих вопросов.

1. Предложенный метод автоматического вывода инвариантов, выразимых автоматами над деревьями, выполняет определённые, весьма специфичные, манипуляции над моделями, в связи с чем возникает вопрос: будет ли этот метод эффективно работать, если в исходной программе содержатся также и другие, неалгебраические типы данных?

2. Почему для программной реализации был выбран язык F#? Упрощает ли функциональное программирование реализацию предложенных методов?

3. В таблице 6.1 при сравнении Хорн-решателей одним из критериев является то, возвращает ли решатель инвариант. В каких случаях возвращением инварианта можно пренебречь и имеют ли методы, не возвращающие инварианты, общее преимущество перед методами, их возвращающими?

Указанные вопросы не носят принципиальный характер и не влияют на общее крайне положительное впечатление от работы. Переходя к оценке диссертации в целом, мне хотелось бы отметить аккуратность автора в описании математических постановок задач и их решений. Преимуществом работы является то, что автор добавил в работу множество примеров, иллюстрирующих теоретические результаты. Подчеркну уникальность работы и полученных автором результатов для данной научной области. Результаты исследования реализованы в виде программного продукта. Замечу, что работа имеет как весомую теоретическую, так и практическую значимость.

Заключение. Диссертация Юрия Олеговича Костюкова 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 ученых степеней в Санкт-Петербургском государственном университете», соискатель Юрий Олегович Костюков заслуживает присуждения 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 установлены.

Председатель диссертационного совета,
доктор физико-математических наук, доцент,
профессор Кафедры математической теории игр
и статистических решений,
Санкт-Петербургский государственный университет

Е.М. Парилина
21.02.2024