УТВЕРЖДАЮ

Директор Федерального государственного бюджетного учреждения науки Институт систем информатики им. А.П. Ершова Сибирского отделения Российской академии наук, д.ф.-м.н.

_____ Пальянов А.Ю.

04 апреля 2022 г.

ОТЗЫВ

ведущей организации на диссертацию

Ушаковой Марии Сергеевны

"Методы и инструментальные средства формальной верификации функционально-потоковых параллельных программ"

по специальности 2.3.5 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей на соискание учёной степени кандидата технических наук

Актуальность дедуктивной верификации программ на языке Пифагор обусловлена необходимостью обеспечить корректность параллельно-потоковых программ, что невозможно полноценно реализовать методом традиционного тестирования. Дедуктивная верификация абсолютно гарантирует корректность программы при правильной спецификации. Но она чрезвычайно сложна и трудоемка; ее проведение требует высокой квалификации. Здесь же трудность верификации усугубляется необходимостью дополнительно рассматривать условия на типы ввиду динамической типизации в языке Пифагор, подобно типизации в языке «Автокод Эльбрус» и известном языке Лисп.

Эффективная реализация языка Пифагор возможна лишь на параллельно-потоковой (асинхронной) архитектуре вычислительных машин. В конце 1980-х годов в рамках проекта «Старт» был разработан прототип компьютера с асинхронной архитектурой. Но работы были остановлены. Лет семь назад появились две статьи Аркадия Климова по асинхронной архитектуре. Были другие работы. Однако до сих пор в мире не появилось компьютеров с асинхронной архитектурой. Александр Легалов со своими учениками уже более 30 лет ведет исследования на базе языка Пифагор в надежде, что такая архитектура появится в будущем. Частично потоковый параллелизм присутствует в функциональном языке Sisal. Однако надежды на высокую эффективность Sisal-программ не оправдались.

Таким образом, язык Пифагор оказался уникальным, не имеющим аналогов. Дедуктивная верификация параллельно-потоковых программ реализована **впервые**. Ранее подобные исследования не встречались.

В первой главе диссертации представлен капитальный обзор современных методов и средств дедуктивной верификации программ на базе более сотни различных публикаций по верификации

программ на разных языках программирования с применением разнообразных инструментов верификации. Более подробно анализируется метод дедуктивной верификации Хоара. Выбор этого метода для верификации параллельно-потоковых программ на языке Пифагор является вполне обоснованным.

Вторая глава посвящена построению формальной семантики языка Пифагор, определяющей точное математическое определение всех конструкций языка и являющейся необходимой для проведения формальной верификации. Семантика конструкция языка Пифагор определена в виде набора троек Хоара. В качестве языка спецификаций определен язык спецификаций системы автоматического доказательства HOL. Данное решение является вполне адекватным для представления предусловий, постусловий и других формул спецификации. На языке HOL представлены теории для целых и вещественных и других типов данных языка Пифагор. Свойства для операций над типами необходимы при доказательстве формул корректности программы. Этапы построения формальной семантики представлены последовательно и детально, в хорошем математическом стиле.

Интересной особенностью данной диссертационной работы является использование унифицированного графического представления ИГР (информационного графа с разметкой) для представления программы на языке Пифагор, спецификаций программы, генерируемых формул корректности и процесса их доказательства.

В третьей главе рассматриваются методы генерации формул корректности для рекурсивных функций, базирующихся на использовании ограничивающей функции, значения которой строго меньше на аргументах рекурсивного вызова. Подробно описываются методы сведения взаимной и косвенной рекурсии к простой одиночной рекурсии.

Четвертая глава описывает разработанный автором инструмент дедуктивной верификации программ на языке Пифагор, реализующий множество разнообразных функций. Инструмент с хорошим графическим интерфейсом работы пользователя на информационном графе программы, возможностями ввода и редактирования, трансляции термов и формул во внутреннее представление, различными преобразованиями графа, автоматизацией генерации формул корректности и процессом проведения доказательства формул корректности с привлечением аксиом и теорем из библиотеки. Реализация такого инструмента требует длительной работы и высокой программисткой квалификации.

Особого внимания заслуживает выбранный **способ реализации** дедуктивной верификации параллельно-потоковых программ на языке Пифагор.

Традиционный способ реализации дедуктивной верификации предполагает ориентацию на некоторую систему автоматического доказательства, логика которой обычно используется в качестве языка спецификаций. Разрабатывается формальная семантика языка программирования. Для основных операторов языка реализуются алгоритмы автоматической генерации формул корректности. Система верификации для конкретного языка автоматически генерирует формулы корректности для входной программы. Сгенерированные формулы корректности оформляются в теорию на языке системы доказательства вместе с описаниями типов, констант и переменных. Сгенерированная теория импортирует теории стандартной библиотеки, определяющей свойства типов и операций языка. На этом система верификации завершает работу. Далее, в системе доказательства автономно проводится доказательство формул корректности.

В диссертационной работе применяется другая схема реализации дедуктивной верификации. Сгенерированная формула корректности тут же доказывается в ручном или автоматическом режиме без записи формулы корректности в теорию. Нужные для доказательства аксиомы и теоремы автоматически находятся в стандартной библиотеке для языка Пифагор. Дерево доказательства развертывается непосредственно в составе графического представления ИГР. Данная схема верификации сложнее стандартной и ранее не встречалась в практике дедуктивной верификации.

Замечания по диссертационной работе

1. Имеются неточности в формулировке второго пункта научной новизны диссертации: «Для доказательства завершения функционально-потоковых параллельных программ впервые предложен метод, использующий ограничивающую функцию, который допускает изменение спецификации программы таким образом, чтобы доказательство частичной корректности одновременно характеризовало и завершение программы». Метод на базе ограничивающей функции (или меры) был предложен еще 1980-х годах, что отмечается и в тексте диссертации. Здесь следовало бы сказать точнее, что данный метод впервые адаптирован для доказательства завершения программ на языке Пифагор. Есть также неточность во второй части предложения. Доказательство завершения программы всегда требует проверки, что аргументы вызова (аппликации) строго меньше в смысле ограничивающей функции, что невозможно свести к доказательству частичной корректности.
2. Аналогичная неточность присутствует в формулировке третьего пункта научной новизны диссертации: «Для функционально-потоковых параллельных программ впервые предложен метод удаления взаимной рекурсии нескольких функций, позволяющий преобразовывать произвольную функцию в функцию с прямой рекурсией …». Метод сведения к прямой рекурсии разработан давно, о чем есть ссылки в тексте диссертации. В данном случае данный метод впервые адаптирован для программ на языке Пифагор, что, тем не менее, является нетривиальным значимым результатом диссертации.
3. Одним из существенных результатов диссертации является верификация в системе автоматического доказательства HOL теорий для типов данных и операций (Приложение В) и условий корректности конструкций программ (Приложение Г). Доказательство корректности используемых при верификации библиотек является важной часть разработки инструмента верификации. Данный факт обнаружен лишь на семинаре в ИСИ СО РАН и никак не представлен в диссертационной работе.
4. В заключительной части диссертационной работы нет описания опыта апробации разработанного автором инструмента верификации на конкретных программах языка Пифагор. Частично такая информации представлена в приложениях Е и Ж.
5. Стр. 22. «Классические языки спецификации … не позволяют описать параллельность выполнения операций. … Это означает, что, во-первых, необходимо разработать правила распараллеливания спецификации» ». В данном фрагменте неточности в рассуждениях. Параллельность операций неявно выразима в логике в виде конъюнкции формул для параллельно исполняемых операций. А сами спецификации никогда не подлежат распараллеливанию.

Рекомендации по использованию результатов и выводов диссертации

Предлагается исследовать возможность реализации полностью автоматической генерации формул корректности параллельно-потоковых программ на языке Пифагор.

Заключение по диссертации.

Сформулированная в диссертации цель исследования достигнута. Основные результаты в полной мере отражены в научных публикациях автора. Автореферат достаточно полно отражает содержание диссертации. Диссертационная работа Ушаковой М.С. является законченным научно-

исследовательским трудом, выполненным автором самостоятельно на хорошем научном уровне. Проделана значительная по объему и сложности работа. Отметим, что разработка методов дедуктивной верификации соответствует уровню PhD в зарубежных диссертациях.

Диссертация соответствует требованиям п.9 "Положения о присуждении учёных степеней" постановления Правительства Российской Федерации от 24.09.2013 г. № 842, а её автор Ушакова Мария Сергеевна достойна присуждения учёной степени кандидата технических наук.

Отзыв обсужден и одобрен на заседании объединенного семинара Института систем информатики им. А.П. Ершова СО РАН и кафедры программирования НГУ «Интеллектуальные системы и системное программирование», протокол заседания № 1 от 17 февраля 2022 г.

Заведующий лабораторией
системного программирования
Федерального государственного
бюджетного учреждения науки
Институт систем информатики
им. А.П. Ершова Сибирского отделения
Российской академии наук
(ИСИ СО РАН),
кандидат технических наук _____ Шелехов Владимир Иванович

04 апреля 2022 г.

Подпись зав. лабораторией ИСИ СО РАН,
к.т.н., Шелехова В. И. заверяю

Личную подпись заверяю
Нач. отдела кадров _____

ОТДЕЛ КАДРОВ

Ученый секретарь ИСИ СО РАН,
к.ф.-м.н. _____ Е.А. Насибулов

04 апреля 2022 г.

Федеральное государственное бюджетное учреждение
науки «Институт систем информатики им. А.П. Ершова
Сибирского отделения Российской академии наук»,
630090, Российская Федерация, г. Новосибирск, проспект
Академика Лаврентьева, 6, (383) 330-86-52,
https://www.iis.nsk.su, E-mail: iis@iis.nsk.su.