ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА
на диссертацию Дмитрия Александровича Кондратьева
«Методы комплексного подхода к автоматизации дедуктивной верификации программ с финитными итерациями», представленную на соискание ученой степени кандидата физико-математических наук по научной специальности 05.13.11 — Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Актуальность темы. Диссертация Д.А. Кондратьева относится к одному из традиционных направлений программной инженерии, которое очень важно в прикладном плане и одновременно является весьма трудным для исследований. Несмотря на длительную историю развития формальной верификации программ, она остается неприспособленной к реальным потребностям программистов. О полученных в этой области результатах еще рано говорить, как о сложившейся технологии верификации программ. Для этого необходимо сочетание строгого математического описания семантик языков программирования и смысла программ на этих языках, представления их в виде, пригодном для формирования методов проверки надежности и безопасности, и требование доведения предлагаемых методов до уровня инструментов для массового применения в реальном программировании. Все это характеризует актуальность темы, выбранной Д.А. Кондратьевым для диссертационного исследования. Полученные им результаты оказывают весомый вклад во все три аспекта актуальности: фундаментальный, практический и технологический. Выбор для развиваемого подхода в качестве предмета исследования дедуктивной верификации, очень важной для практического применения, определяет важность обсуждаемой работы и полученных результатов.

Цель диссертационной работы. Автор диссертационной работы определяет цели исследования как разработку методов, обеспечивающих автоматизацию, расширяемость и проблемную ориентированность предлагаемого им похода к формальной верификации программ без использования инвариантов циклов. Для ее достижения были поставлены и решены следующие важные задачи:

1. Разработка метода, позволяющего генерировать условия корректности для программ с финитными итерациями без использования инвариантов циклов.
2. Разработка стратегий, автоматизирующих доказательство условий корректности программ с финитными итерациями, и доказательство корректности этих стратегий.
3. Разработка метода автоматизированной локализации ошибок при дедуктивной верификации программ с финитными итерациями.
4. Разработка аксиоматической семантики языка Cloud Sisal, позволяющей проводить дедуктивную верификацию программ на данном языке без использования инвариантов циклических выражений. Разработка аксиоматической семантики расширения языка C конструкциями языка Sisal, позволяющей применять в системе CPPS методы комплексного подхода системы C-lightVer.
5. Реализация методов комплексного подхода в системе C-lightVer, позволяющая при дедуктивной верификации программ с финитными итерациями, заданных на языках C, Cloud Sisal и на расширении C конструкциями Cloud Sisal, автоматизировать доказательство условий корректности и автоматизировать локализацию ошибок. Проведение экспериментов по автоматизированной верификации программ на данных языках.

Научная значимость и новизна результатов. В качестве элемента несомненной научной новизны на защиту выносится следующее:

1. Впервые предложены стратегии автоматического и интерактивного доказательства условий корректности программ с финитными итерациями без использования инвариантов циклов.
2. Впервые предложены методы локализации ошибок при дедуктивной верификации программ с финитными итерациями без использования инвариантов циклов.

3. Впервые в рамках одной работы исследована применимость подхода к программам на языках с императивной и функциональной парадигмами программирования.

Теоретическая значимость исследования заключается в разработке формальных методов, которые позволяют в случае финитных итераций решить проблемы, обусловленные использованием инвариантов циклов, автоматизации доказательства условий корректности и автоматизации локализации ошибок. При этом корректность ключевых стратегий подхода гарантирована формальным доказательством.

Практическая значимость работы состоит в программной реализации системы верификации C-lightVer применимой для верификации программ на языках C и Cloud Sisal. Эта системы рассматривается в качестве прототипа, предназначенного для постановки и выполнения экспериментов, связанных с предлагаемыми методами, а также для выработки основных требований к верификатору, который планируется в качестве перспективного развития проведенной работы.

Структура диссертационной работы. Диссертация состоит из введения, 5 глав, заключения и библиографии.

Во **Введении** автор обосновывает актуальность диссертационной работы, формулирует ее цель, аргументирует научную новизну, показывает практическую значимость полученных результатов и представляет выносимые на защиту научные положения.

В **первой главе** приводятся классические методы, составляющие основу дедуктивной верификации, и новые методы, используемые в комплексном подходе для решения проблем, возникающих при дедуктивной верификации программ. Также представлена информация о научных результатах автора, полученных в связи с разработкой системы C-lightVer до проведения диссертационного исследования. Информация о них необходима для понимания дальнейшего изложения.

Вторая глава посвящена алгоритмам генерации функций, выражающих результаты различных классов финитных итераций. Использование этих алгоритмов приводит к генерации условий корректности, содержащих применения символической функции замены. В данной главе описаны также стратегии доказательства таких условий.

В **третьей главе** излагается метод автоматизации локализации ошибок, реализованный в системе C-lightVer. Этот метод включает стратегии локализации ошибок и средства генерации текстов о сопоставлении подформул условий корректности с фрагментами верифицируемой программы.

Четвертая глава содержит описание применения развиваемого автором подхода, названного комплексным, к дедуктивной верификации программам на языке C. Рассмотрена модифицированная система C-lightVer. Описаны эксперименты по верификации программ с финитными итерациями на языке C-light. Продемонстрировано использование комплексного подхода для избегания задания инвариантов циклов, автоматизации доказательства и локализации ошибок.

В **пятой главе** описано применение комплексного подхода к программам на языке Cloud Sisal. Рассмотрены два реализованных в качестве модулей системы CPPS способа дедуктивной верификации данных программ. Описана разработанная аксиоматическая семантика языка Cloud-Sisal-kernel, позволяющая проводить дедуктивную верификацию без использования инвариантов циклических выражений. Предложено расширение языка C циклами Cloud Sisal, позволяющее применить в системе CPPS методы комплексного подхода системы C-lightVer. Описан ряд экспериментов.

В **Заключении** приведены выводы о выполненной работе, сформулированы основные результаты и перспективы развития направления исследований. Достоверность полученных результатов обоснована строгой формализацией излагаемых положений, доказательствами корректности, проведенными экспериментами, а также апробацией предоставленных автором докладов на многочисленных конференциях и семинарах.

Таким образом, диссертация Д.А. Кондратьева достаточно полно освещает проведенное исследование и полученные результаты. Она написана хорошим научным

языком, грамотно оформлена и представляет собой полный монографический труд. Автореферат диссертации корректно отражает ее содержание. Выносимые на защиту положения полностью представлены в публикациях автора.

Публикации. Материалы диссертации опубликованы в 38 печатных работах, включая 14 статей в изданиях перечня ВАК, из них 11 публикаций входят в международные базы цитирования Scopus и Web of Science. Было получено свидетельство о государственной регистрации программы для ЭВМ.

Замечания и вопросы. Несомненные достоинства обсуждаемой работы и значимость полученных результатов оставляют хорошее впечатление о диссертационном исследовании Д.А. Кондратьева. Тем не менее, нельзя не отметить ее ряд недостатков:

1. К сожалению, автор слабо обосновал выбор термина *комплексный* для своего подхода. С одной стороны, безусловно, набор методов, алгоритмов и стратегий можно совокупно назвать комплексом. Но для объективности, следовало бы провести сравнение с другими подходами именно по данному показателю, явно продемонстрировав, почему они не являются комплексными. Или, если и они обладают признаками комплексности, то в чем разница с разработкой автора.
2. В работе не хватает построения *системы базовых понятий* предлагаемого подхода, в рамках которой можно было бы дать определения ошибочных программ, типизации и классификации ошибок, локализации ошибок в тексте программы, а также возможных вариантов проверок, из которых строятся процессы верификации программы и др. На этой основе можно было показать границы применимости предлагаемого подхода.
3. Автор часто опускает важную оговорку о характере *ошибок*, на поиск которых ориентирован комплексный подход. Очевидно, что речь идет об ошибках Хоаровского типа, т.е. о несоответствии программы и ее спецификаций. Без указанной оговорки читатель может воспринимать термин ошибка в более широкой трактовке, в результате чего может сложиться необоснованное представление о гораздо больших возможностях подхода.
4. Автор довольно сжато сформулировал понятие *символической верификации финитных итераций*, в основном сделав отсылку на работы В.А. Непомнящего, предложившего его. В результате возникает риск, что неподготовленный читатель, не знакомый с указанными работами, может не понять ряд ключевых моментов, связанных с данным методом.
5. Основная платформа, на которой строится автоматизация верификации описана недостаточно полно: читателю приходится восполнять недостающую информацию из внешних источников.
6. Есть претензии к стилю изложения материала. Так, излюбленный прием автора начинать суждения со слов «Рассмотрим…» часто используется и тогда, когда читатель еще не знает, для чего приводится это рассмотрение. Это затрудняет восприятие информации.

В целом, перечисленные недостатки не являются принципиальными и не умаляют достоинств диссертации. Многое из них следует рассматривать как пожелания для дальнейших работ автора.

Заключение. Резюмируя сказанное выше по поводу работы Д.А. Кондратьева, можно сделать следующий вывод. Диссертационное исследование «Методы комплексного подхода к автоматизации дедуктивной верификации программ с финитными итерациями» является целостной и завершенной научно-исследовательской работой. Автором самостоятельно и на высоком научном уровне получены результаты по целому ряду направлений в теории и практике верификации программ. Новизна, достоверность и обоснованность результатов позволяют характеризовать их как значительное научное достижение в данной области. Работа изложена последовательно, полно и аккуратно.

На основании вышеизложенного считаю, что диссертация Дмитрия Александровича Кондратьева «Методы комплексного подхода к автоматизации дедуктивной верификации

программ с финитными итерациями» соответствует требованиям, предъявляемыми нормативными актами Российской Федерации к диссертациями на соискание степени кандидата наук, а ее автор, Кондратьев Дмитрий Александрович заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.11. — Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Официальный оппонент:
к.ф.-м.н., старший научный сотрудник Лаборатория синтеза параллельных программ Федерального государственного бюджетного учреждения науки Института вычислительной математики и математической геофизики Сибирского отделения Российской академии наук (ИВМиМГ СО РАН)

Игорь Николаевич Скопин

Дата 29.08.2022

Подпись к.ф.-м.н., с.н.с. И.Н. Скопина заверяю
И.о. ученого секретаря ИВМиМГ СО РАН Крайнева Марина Владимировна

Скопин Игорь Николаевич, кандидат физико-математических наук
по специальности 05.13.11 — Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей
старший научный сотрудник Лаборатория синтеза параллельных программ
Федерального государственного бюджетного учреждения науки
Института вычислительной математики и математической геофизики
Сибирского отделения Российской академии наук (ИВМиМГ СО РАН),
630090, г. Новосибирск, проспект Академика Лаврентьева, 6.
телефон: (383) 3308652
вебсайт: www.iis.nsk.su
электронная почта: iis@iis.nsk.su

Контактные данные:
телефон: +7-983-126-26-86
электронная почта: iskopin@gmail.com