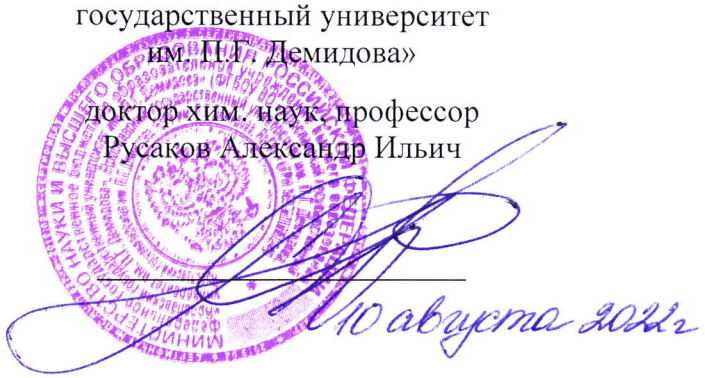
УТВЕРЖДАЮ

Ректор Федерального государственного бюджетного образовательного учреждения высшего образования «Ярославский государственный университет им. П.Г. Демидова»

доктор хим. наук, профессор
Русаков Александр Ильич



10 августа 2022 г

# ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

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 специальности 05.13.11 — Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

**Актуальность темы диссертации.** Важность исследований в области формальной верификации программ обусловлена постоянно возрастающей сложностью программного обеспечения. Как следствие, разработчики тратят на отладку и тестирование программ усилия, сравнимые или превосходящие непосредственно написание исходных текстов. При этом традиционные подходы в виде тестирования или статического анализа зачастую просто не справляются с поиском всех проблем. Но, с другой стороны, хотя дедуктивная верификация способна абсолютно гарантировать корректность программы при правильных спецификациях, она требует высокой научной квалификации. Специалист по верификации должен уметь описывать свойства программ на языке логики, уметь применять средства поддержки доказательства теорем. Наконец, он должен знать, как интерпретировать логические контрпримеры при неудачном доказательстве условий корректности. В результате обычные программисты как применяли тестирование, так и продолжают применять, а верификация была и остается уделом коллективов научных институтов и университетов.

Таким образом, большую актуальность приобретают исследования, способные снизить дополнительную нагрузку на программистов, которые пытаются применять верификацию. Предметом исследований в диссертации Д.А. Кондратьева стал важный класс алгоритмов — финитных итераций над структурами данных — для которого был предложен целый комплекс методов, позволяющих на практике повысить степень автоматизируемости задачи верификации.

**Основные полученные результаты**

1. Разработан метод генерации операции замены для циклов, позволяющий генерировать условия корректности для программ с финитными итерациями без использования инвариантов циклов. Метод включает специализированные алгоритмы для случаев неизменяемых/изменяемых массивов.

2. Разработаны стратегии доказательства условий корректности для программ с финитными итерациями, позволяющие автоматизировать проверку на истинность. Отдельного упоминания заслуживают стратегии для оператора break, который представляет известную проблему для логик Хоаровского типа. Доказана корректность стратегии усиления условий корректности.
3. Предложен метод локализации ошибок, позволяющий автоматизировать сопоставление конструкций программы и подформул условий корректности, а также локализацию ошибок в программах с финитными итерациями. Метод включает: язык представления семантических меток; семантические метки для функций, выражающих результаты финитных итераций; алгоритм генерации объяснений недоказанных условий корректности над финитными итерациями; ряд специальных стратегий.
4. Разработана аксиоматическая семантика языка Cloud-Sisal-kernel, включающая правила вывода для циклических выражений без инвариантов. Предложена аксиоматическая семантика расширения языка C конструкциями языка Sisal (C-Sisal-kernel). Разработан алгоритм генерации функций, выражающих результат циклических выражений языка Cloud-Sisal-kernel и языка C-Sisal-kernel.
5. Реализованы методы комплексного подхода в системе C-lightVer для автоматизированной дедуктивной верификации программ с финитными итерациями на языках C, Cloud-Sisal-kernel и C-Sisal-kernel. Были проведены эксперименты по автоматизированной верификации программ на этих языках, в том числе важные эксперименты по обнаружению и объяснению намеренно внесенных ошибок.

**Личный вклад.** Использование методов Д.А. Кондратьева в системах C-lightVer и CPPS потребовало взаимодействия с другими участниками данных проектов, что отражено в ряде совместных публикаций. Однако все положения, выносимые на защиту, получены Д.А. Кондратьевым лично.

**Новизна.** Верификация программ для класса финитных итераций, ранее известная только по теоретическим моделям, впервые была воплощена в виде полностью автоматического инструментария. Также методы семантической разметки для локализации ошибок и объяснения условий корректности ранее никогда не применялись для программ с финитными итерациями без использования инвариантов циклов. Наконец, важным элементом новизны стали методы, применимые не только к императивным, но и к функциональным языкам программирования.

**Теоретическая значимость.** В диссертации разработаны формальные методы для комплексного подхода, позволяющие в случае финитных итераций решить проблемы инвариантов циклов, автоматизации доказательства условий корректности и автоматизации локализации ошибок. Данный подход может быть применен к широкому классу языков императивного и функционального программирования, позволяющих задавать финитные итерации над структурами данных.

**Практическая значимость.** На практике предложенные теоретические методы были реализованы в прототипе системы верификации C-lightVer. Была продемонстрирована применимость системы для верификации программ на языках, представляющих две парадигмы программирования: язык C, язык Cloud Sisal и язык C-Sisal-kernel. Система оказалась востребована в ряде проектов РФФИ и РНФ. Немаловажным является то, что комплекс методов, затрагивающий все этапы верификации — от специфицирования до доказательства — может найти применение в учебных курсах по формальным основам информатики.

**Обоснованность и достоверность научных выводов, положений и заключений** подтверждается грамотным применением результатов как классических, так и современных исследований в области верификации и математической логики, применением математических способов доказательства, проведением экспериментов. Формальная корректность предложенных стратегий обоснована не только ручным доказательством теорем, но аккуратной работой с автоматическими средствами, такими как ACL2 и SMT-решатели, которые менее подвержены человеческим ошибкам.

Важно отметить, что соискатель в своих экспериментах не ограничился демонстрацией успешной верификации для заведомо корректных троек Хоара, как часто бывает в родственных исследованиях. Проводилась и работа с намеренно внесенными семантическими ошибками.

Дополнительно достоверность результатов подтверждена многочисленными выступлениями на российских и международных семинарах и конференциях.

**Оценка содержания диссертационной работы, ее завершенность в целом, замечания по оформлению**

Диссертация Д.А. Кондратьева представляет собой целостную и содержательную работу, какие-либо противоречия в ней не выявлены. Язык изложения ясный и последовательный. Работа состоит из введения, пяти глав, заключения и списка использованной литературы. Каждая глава заканчивается выводами относительно полученных в ней результатов.

Во **введении** обоснована актуальность диссертационной работы, сформулирована цель и аргументирована научная новизна исследований, показана практическая значимость полученных результатов, представлены выносимые на защиту научные положения. Также введение предлагает очень представительный обзор современных исследований в данной области.

В **первой главе** описаны методы, составляющие основу дедуктивной верификации (логика Хоара, метод слабейшего предусловия), и методы, используемые в комплексном подходе для решения проблем, возникающих при дедуктивной верификации программ (метод метагенерации условий корректности, метод семантической разметки, символический метод верификации финитных итераций). Также рассмотрен задел по системе дедуктивной верификации C-lightVer, созданный до работы над данной диссертацией.

Во **второй главе** описаны алгоритмы генерации рекурсивных функций, выражающих результаты различных классов финитных итераций. Использование таких алгоритмов приводит к генерации условий корректности, содержащих применения функции *rep*. В данной главе описаны также стратегии доказательства таких условий.

В **третьей главе** описан метод автоматизации локализации ошибок, реализованный в системе C-lightVer. Данный метод включает в себя стратегии локализации ошибок и метод генерации текста о сопоставлении подформул условий корректности и фрагментов программы, основанный на специальной семантической разметке правил вывода.

В **четвертой главе** описано применение комплексного подхода к программам на языке С. Рассмотрена созданная в результате модифицированная система C-lightVer. Описаны эксперименты по верификации программ с финитными итерациями на языке C-light. Продемонстрировано использование комплексного подхода для избежания задания инвариантов циклов, автоматизации доказательства условий корректности и автоматизации локализации ошибок.

В **пятой главе** наглядно показано, что методы, предложенные для императивного языка C, могут послужить основой и для функционального языка Cloud Sisal. Рассмотрены два реализованных в качестве модулей CPPS способа дедуктивной верификации: дедуктивная верификация промежуточного представления на языке C и дедуктивная верификация подмножества Cloud Sisal. Описана аксиоматическая семантика языка Cloud-Sisal-kernel для циклических выражений. Также рассмотрено расширение языка C циклами Cloud Sisal, позволяющее применить в системе CPPS методы комплексного подхода системы C-lightVer. Продемонстрированы результаты экспериментов по верификации программ на языках Cloud Sisal, Cloud-Sisal-kernel и C-Sisal-kernel.

В **заключении** приведены выводы из работы, сформулированы основные результаты и перспективы развития направления исследований.

**Замечания:**

1. Отметим, что 2 стратегии доказательства условий корректности исполняются не в автоматическом, а в интерактивном режиме. Тем не менее, это не снижает научную ценность представленного исследования, поскольку 10 описанных стратегий исполняются в полностью автоматическом режиме, а 2 стратегии получают информацию от пользователя в определенной форме, что позволяет упростить верификацию.
2. В таблице 5.1 автор приводит продолжительность сеансов верификации двух программ, на основе которой делает вывод о **приемлемости** предложенной стратегии доказательства. Очевидно, данное утверждение довольно субъективно. Если бы автор привел продолжительности сеансов в других известных системах верификации для тех же примеров, то можно было бы обоснованно говорить об объективной эффективности или неэффективности в сравнении с конкурентами.

**Соответствие автореферата основным положениям диссертации**

Автореферат правильно отражает содержание диссертации.

**Подтверждение опубликованных основных результатов диссертации в научной печати**

Результаты диссертационного исследования были опубликованы в 38 научных работах, включая 14 статей в изданиях из списка ВАК и 11 в журналах из баз цитирования WoS и Scopus.

**Заключение**

Диссертационная работа Д.А. Кондратьева является законченным научным исследованием, выполненным на высоком научном уровне. В работе получены новые и значимые результаты в области формальной семантики языков программирования, методов автоматического доказательства теорем, дедуктивной верификации программного обеспечения.

Полученный автором результаты достоверны, выводы и заключения обоснованы.

Содержание диссертации полностью соответствует формуле научной специальности 05.13.11 — Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей, а также пунктам 1, 2, 5 паспорта специальности.

Диссертационная работа соответствует критериям, установленным Положением о порядке присуждения ученых степеней, 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.

Отзыв на диссертацию обсуждался и был утвержден на заседании кафедры теоретической информатики факультета информатики и вычислительной техники ФГБОУ ВО ЯрГУ, протокол №13 от 10.08.2022 г.

Отзыв составил
доктор физико-математических наук, доцент, заведующий кафедрой теоретической информатики факультета информатики и вычислительной техники Федерального государственного бюджетного образовательного учреждения высшего образования «Ярославского государственного университета им. П.Г. Демидова»

Кузьмин Егор Владимирович 10.08.2022

телефон: +79051306569
e-mail: kuzmin@uniyar.ac.ru

**Федеральное государственное бюджетное образовательное учреждение высшего образования «Ярославский государственный университет им. П.Г. Демидова»**

**Адрес: 150053, г. Ярославль, ул. Советская, д. 14**

**Тел. +7(4852) 797752; E-mail: rectorat@uniyar.ac.ru**

Подпись заверяю:
Начальник управления кадровой политики и социальной работы
В.В. Леванов