УТВЕРЖДАЮ
Директор Федерального государственного
бюджетного учреждения науки
Института систем информатики
им. А.П. Ершова
Сибирского отделения
Российской академии наук

д.ф.-м.н. _____ А.Ю. Пальянов

« 27 » июня 2022 г.

ЗАКЛЮЧЕНИЕ

Федерального государственного бюджетного учреждения науки
Института систем информатики им. А.П. Ершова
Сибирского отделения Российской академии наук

Диссертация «Методы комплексного подхода к автоматизации дедуктивной верификации программ с финитными итерациями», представленная на соискание ученой степени кандидата технических наук по специальности 05.13.11 — «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей», выполнена в Федеральном государственном бюджетном учреждении науки Институте систем информатики им. А.П. Ершова Сибирского отделения Российской академии наук (ИСИ СО РАН) в лаборатории теоретического программирования. Научный руководитель — Промский Алексей Владимирович, кандидат физико-математических наук, основное место работы: ИСИ СО РАН; должность: заместитель директора по научной работе.

В 2015 году Кондратьев Дмитрий Александрович с отличием окончил магистратуру Федерального государственного автономного образовательного учреждения высшего образования «Новосибирский национальный исследовательский государственный университет» по направлению подготовки 09.04.01 — «Информатика и вычислительная техника». В 2019 году освоил программу подготовки научно-педагогических кадров в аспирантуре Федерального государственного бюджетного учреждения науки Института систем информатики им. А.П. Ершова Сибирского отделения Российской академии наук по направлению подготовки 09.06.01 — «Информатика и вычислительная техника». В период подготовки диссертации Кондратьев Дмитрий Александрович работал в ИСИ СО РАН в качестве программиста 1 категории и младшего научного сотрудника.

Сведения о сдаче экзаменов по философии, иностранному языку и по специальности 05.13.11 — «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей» содержатся в приложении к диплому об окончании аспирантуры, выданном в 2019 году Федеральным государственным бюджетным учреждением науки Институтом систем информатики им. А.П. Ершова Сибирского отделения Российской академии наук.

Тема диссертации относится к **актуальным** направлениям теоретической и прикладной информатики, входит в круг проблем, решаемых в ИСИ СО РАН.

Предмет исследования — методы комплексного подхода к автоматизации дедуктивной верификации программ без использования инвариантов циклов.

Цель — исследование и разработка методов для задания семантик языков программирования в классе программ над финитными итерациями и для автоматического вывода условий корректности таких программ, разработка стратегий автоматизированного доказательства условий корректности для финитных итераций, разработка способов объяснения недоказанных/ложных условий корректности для пользователя вместе с алгоритмами локализации ошибок в программах и спецификациях.

В работе получены следующие основные результаты:

1. Разработан метод генерации операции замены для циклов, позволяющий генерировать условия корректности для программ с финитными итерациями без использования инвариантов циклов. Метод включает в себя специализированные алгоритмы для случаев изменяемых/неизменяемых массивов и вида вложенности условных конструкций.
2. Разработаны стратегии доказательства условий корректности для программ с финитными итерациями, позволяющие автоматизировать проверку на истинность. Стратегии включают: выбор посылок; разбор случаев для формул с операцией замены; усиление условий корректности; стратегию для программ, спецификации которых содержат функции со свойством конкатенации; стратегии для финитных итераций с инструкцией **break**, для финитных итераций над изменяемыми массивами, для программ с вложенными циклами. Доказана корректность стратегии усиления условий корректности.
3. Предложен метод автоматического сопоставлении конструкций программы и подформул условий корректности для задачи локализации ошибок в программах с финитными итерациями. Метод включает: язык представления семантических меток; семантические метки для функций, выражающих результаты финитных итераций; алгоритм генерации функций, выражающих результаты финитных итераций, с семантическими метками для итераций над изменяемыми массивами; алгоритм генерации объяснений недоказанных условий

корректности, содержащих операцию замены; стратегию проверки ложности недоказанных условий корректности; стратегию поиска циклов с неиспользуемыми присваиваниями элементам массива; стратегию проверки исполнения инструкции **break** на первой итерации цикла.

4. Разработана аксиоматическая семантика языка Cloud-Sisal-kernel, включающая правила вывода для циклических выражений без инвариантов. Предложена аксиоматическая семантика расширения (C-Sisal-kernel) языка C конструкциями языка Sisal. Разработан алгоритм генерации функций, выражающих результат циклических выражений языка Cloud-Sisal-kernel и языка C-Sisal-kernel.
5. Методы комплексного подхода реализованы в системе C-lightVer для задач верификации программ с финитными итерациями на языках C, Cloud Sisal, C-Sisal-kernel. Проведены успешные эксперименты по автоматизированной верификации, в том числе для программ из международных соревнований по верификации.

Содержание диссертации полностью **соответствует** формуле специальности Высшей Аттестационной Комиссии (ВАК) 05.13.11 — «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей» (физико-математические науки) и пунктам 1, 2 и 5 паспорта специальности.

Все выносимые на защиту результаты **достоверны**, теоретически строго обоснованы и подтверждены экспериментами, проведенными в соответствии с общепринятыми стандартами. Научные результаты, в полном объеме отражающие содержание диссертации, **опубликованы** в 38 научных работах, из них: 14 работ в изданиях перечня ВАК, 11 работ в изданиях, индексируемых в Scopus и/или Web of Science. Получено 1 свидетельство о государственной регистрации программ для ЭВМ. Все результаты успешно прошли **апробацию** на ряде российских и международных конференций.

Личный вклад. Положения, выносимые на защиту, описанные в работах с несколькими соавторами, получены лично автором, конфликт интересов отсутствует.

Новизна. Все результаты, выносимые на защиту, являются новыми. Соискателем предложены оригинальные методы для решения трех задач: повышения степени автоматизации доказательства условий корректности программ с финитными итерациями без использования инвариантов циклов; автоматизации локализации ошибок при дедуктивной верификации данного класса программ; повышения универсальности методов верификации с целью применения как к императивным, так и к функциональным языкам программирования. Методологической основой исследования являются методы математической логики и формальных исчислений. Для программной реализации системы использовались методы объектно-ориентированного программирования и API LLVM/Clang.

Теоретическая и практическая значимость состоит в том, в диссертации даны формальные описания методов для комплексного подхода, которые позволяют в случае финитных итераций решить проблемы инвариантов циклов, автоматизации доказательства УК и автоматизации локализации ошибок. На базе предложенных методов реализована новая версия системы C-lightVer. Подход может быть применен к широкому классу языков императивного и функционального программирования, что подтверждается экспериментами с языками C и Cloud Sisal.

Диссертация соответствует требованиям, установленным пунктом 14 Положения о присуждении ученых степеней.

Диссертация «Методы комплексного подхода к автоматизации дедуктивной верификации программ с финитными итерациями» Кондратьева Дмитрия Александровича рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 05.13.11 — «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Заключение принято на заседании объединенного семинара «Интеллектуальные системы и системное программирование» лаборатории искусственного интеллекта Института систем информатики им. А.П. Ершова СО РАН и кафедры программирования НГУ. Присутствовало на заседании 28 человек, в том числе: от лаборатории информационных систем д.ф.-м.н. Марчук А.Г., к.ф.-м.н. Пономарев Д.К., к.ф.-м.н. Городняя Л.В.; от лаборатории искусственного интеллекта: к.т.н. Загорулько Ю.А., к.т.н. Загорулько Г.Б., к.ф.-м.н. Сидорова Е.А.; от лаборатории моделирования сложных систем: к.ф.-м.н. Мигинский Д.С., к.ф.-м.н. Штокало Д.Н., к.ф.-м.н. Батура Т.В.; от лаборатории теории параллельных процессов: д.ф.-м.н. Вирбицкайте И.Б.; от лаборатории теоретического программирования к.ф.-м.н. Промский А.В., к.ф.-м.н. Ануреев И.С., к.ф.-м.н. Гаранина Н.О.; от лаборатории конструирования и оптимизации программ д.ф.-м.н. Касьянов В.Н.; от лаборатории программного обеспечения и сервисной инженерии Университета Иннополис к.ф.-м.н. Шилов Н.В.

Результаты голосования: «за» — 28 человек, «против» — 0 человек, «воздержалось» — 0 человек, протокол № 5 от 24 марта 2022 г.

Председатель заседания
Доктор физико-математических наук,
зав. лабораторией информационных систем А.Г. Марчук

Личную подпись заверяю
Нач. отдела кадров