

ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 999.082.03,
СОЗДАННОГО НА БАЗЕ Федерального государственного бюджетного
учреждения науки Института систем информатики им. А.П. Ершова
Сибирского отделения Российской академии наук (ИСИ СО РАН),
Федерального государственного бюджетного учреждения науки Института
вычислительной математики и математической геофизики Сибирского
отделения Российской академии наук (ИВМиМГ СО РАН),
Федерального государственного бюджетного учреждения науки Института
математики им. С.Л. Соболева Сибирского отделения Российской академии
наук (ИМ СО РАН)
ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА
НАУК

аттестационное дело № _____
решение диссертационного совета от 14.09.2022 № 3

О присуждении Кондратьеву Дмитрию Александровичу, гражданину Российской Федерации ученой степени кандидата физико-математических наук.

Диссертация «Методы комплексного подхода к автоматизации дедуктивной верификации программ с финитными итерациями» по специальности 05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей принята к защите 13 июля 2022 года (протокол заседания №2) диссертационным советом Д 999.082.03, созданным на базе Федерального государственного бюджетного учреждения науки Института систем информатики им. А.П. Ершова Сибирского отделения Российской академии наук (ИСИ СО РАН), Федерального государственного бюджетного учреждения науки Института вычислительной математики и математической геофизики Сибирского отделения Российской академии наук (ИВМиМГ СО РАН), Федерального государственного бюджетного учреждения науки Института математики им. С.Л. Соболева Сибирского отделения Российской академии наук (ИМ СО РАН), находящимся по адресу 630090, г. Новосибирск, Проспект Академика Лаврентьева, дом 6. Совет утвержден приказом Минобрнауки России №793/нк от 24 июня 2016 года.

Соискатель Кондратьев Дмитрий Александрович 14 марта 1992 года рождения.

В 2019 году соискатель окончил аспирантуру Федерального государственного бюджетного учреждения науки Института систем

информатики им. А.П. Ершова Сибирского отделения Российской академии наук, работает младшим научным сотрудником в Федеральном государственном бюджетном учреждении науки Институте систем информатики им. А.П. Ершова Сибирского отделения Российской академии наук.

Диссертация выполнена в Лаборатории теоретического программирования Федерального государственного бюджетного учреждения науки Института систем информатики им. А.П. Ершова Сибирского отделения Российской академии наук.

Научный руководитель — кандидат физико-математических наук Промский Алексей Владимирович, Федеральное государственное бюджетное учреждение науки Институт систем информатики им. А.П. Ершова Сибирского отделения Российской академии наук, заместитель директора по научной работе.

Официальные оппоненты:

– Петренко Александр Константинович, доктор физико-математических наук, профессор, Федеральное государственное бюджетное учреждение науки Институт системного программирования им. В.П. Иванникова Российской академии наук, Отдел технологий программирования, заведующий отделом,
– Скопин Игорь Николаевич, кандидат физико-математических наук, старший научный сотрудник, Федеральное государственное бюджетное учреждение науки Институт вычислительной математики и математической геофизики Сибирского отделения Российской академии наук, Лаборатория синтеза параллельных программ, старший научный сотрудник
дали положительные отзывы на диссертацию.

Ведущая организация — Федеральное государственное бюджетное образовательное учреждение высшего образования «Ярославский государственный университет» им. П.Г. Демидова (г. Ярославль), в своем положительном отзыве, подписанном доктором физ.-мат. наук, доцентом, заведующим Кафедрой теоретической информатики Факультета информатики и вычислительной техники Е.В. Кузьминым и утвержденном ректором, доктором хим. наук, профессором А.И. Русаковым, указала, что 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.

Соискатель имеет 46 опубликованных работ, в том числе по теме диссертации опубликовано 38 работ, из них в рецензируемых научных изданиях опубликовано 14 работ. В диссертации отсутствуют недостоверные сведения об опубликованных соискателем работах.

Краткая характеристика научных работ соискателя:

1. Кондратьев Д. А. На пути к автоматической дедуктивной верификации C-программ с Sisal-циклами в системе C-lightVer // Моделирование и анализ информационных систем. – 2021. – Т. 28, № 4. – С. 372-393.

2. Кондратьев Д. А. Расширение системы C-light символическим методом верификации финитных итераций // Вычислительные технологии. – 2017. – Т. 22, Специальный выпуск 1. – С. 44-59.

3. Maryasov I. V., Nepomniaschy V. A., Kondratyev D. A. Invariant Elimination of Definite Iterations over Arrays in C Programs Verification // Modeling and Analysis of Information Systems. – 2017. – Vol. 24, Issue 6. – P. 743-754.

Авторский вклад: алгоритм генерации функций, выражающих результаты итераций с вложенными условными инструкциями над неизменяемыми массивами; стратегия интерактивного доказательства условий корректности; проведение эксперимента.

4. Kasyanov V. N., Kasyanova E. V., Kondratyev D. A. Formal verification of Cloud Sisal programs // Proc. Applied Physics, Simulation and Computing, Rome, Italy, May 23-25, 2020. – Journal of Physics: Conference Series. – 2020. – Vol. 1603. – Article ID: 012020.

Авторский вклад: применение в системе CPPS методов комплексного подхода системы C-lightVer; реализация формальной верификация Cloud Sisal программ с помощью дедуктивной верификации их C-представления в системе C-lightVer; реализация формальной верификации Cloud Sisal программ с использованием аксиоматической семантики языка Cloud Sisal.

5. Kondratyev D. Implementing the Symbolic Method of Verification in the C-Light Project // Lect. Notes Comput. Sci. – Cham, 2018. – Vol. 10742. – P. 227-240.

6. Kondratyev D. A., Maryasov I. V., Nepomniaschy V. A. The Automation of C Program Verification by the Symbolic Method of Loop Invariant Elimination // Automatic Control and Computer Sciences. – 2019. – Vol. 53, Issue 7. – P. 653-662.

Авторский вклад: алгоритм генерации функций, выражающих результаты итераций над изменяемыми массивами; стратегия доказательства условий корректности для программ, постусловием которых является разбор

случаев выхода из цикла; метод генерации операции замены для финитных итераций в системе C-lightVer; эксперимент по верификации программы изменения знака первого отрицательного элемента массива.

7. Kondratyev D., Maryasov I., Nepomniaschy V. Towards Automatic Deductive Verification of C Programs over Linear Arrays // Lect. Notes Comput. Sci. – Cham, 2019. – Vol. 11964. – P. 232-242.

Авторский вклад: стратегия доказательства для программ, спецификации которых содержат функции со свойством конкатенации; стратегия доказательства для финитных итераций с инструкцией break; стратегия доказательства для финитных итераций над изменяемыми массивами; стратегия выбора посылок; эксперимент по автоматической верификации программы сортировки простыми вставками с инвариантом внешнего цикла и без инварианта внутреннего цикла.

8. Kondratyev D. A., Nepomniaschy V. A. Automation of C program deductive verification without using loop invariants // Programming and Computer Software. – 2022. – Vol. 48, Issue 5, – P. 331-346.

Авторский вклад: метод генерации операции замены для вложенных финитных итераций; стратегия доказательства для программ с вложенными циклами; стратеги доказательства для программ с финитными итерациями над массивами; стратегия локализации ошибок, эксперимент по верификации сортировки простыми вставками.

9. Kondratyev D. A., Promsky A. V. Developing a Self Applicable Verification System. Theory and Practices // Automatic Control and Computer Sciences. – 2015. – Vol. 49, Issue 7. – P. 445-452.

Авторский вклад: реализация методов комплексного подхода в системе C-lightVer.

10. Kondratyev D., Promsky A. Correctness of Proof Strategy for the Sisal Program Verification // Proc. 2019 Intern. Multi-Conf. Eng., Comput. and Inf. Sci., Novosibirsk, Russia, October 21-27, 2019. – IEEE, 2019. – P. 641-646.

Авторский вклад: доказательство корректности стратегии усиления условий корректности; эксперимент по автоматической верификации C-представления Sisal программы, проверяющей упорядоченность элементов массива по возрастанию.

11. Kondratyev D., Promsky A. Proof Strategy for Automated Sisal Program Verification // Lect. Notes Comput. Sci. – Cham, 2019. – Vol. 11771. – P. 113-120.

Авторский вклад: стратегия усиления условий корректности; эксперимент по верификации C-представления Sisal программы, проверяющей наличие в массиве не менее заданного числа вхождений ключа.

12. Kondratyev D. A., Promsky A. V. The Complex Approach of the C-lightVer System to the Automated Error Localization in C-Programs // Automatic Control and Computer Sciences. – 2020. – Vol. 54, Issue 7. – P. 728-739.

Авторский вклад: алгоритм генерации функций, выражающих результаты финитных итераций, с семантическими метками для итераций над изменяемыми массивами; алгоритм генерации объяснений недоказанных условий корректности; язык семантических меток; стратегия локализации ошибок; реализация в системе C-lightVer алгоритма генерации объяснений недоказанных условий корректности; эксперимент по локализации ошибок.

13. Kondratyev D. A., Promsky A. V. Towards verification of scientific and engineering programs. The CPPS project // Journal of Computational technologies. – 2020. – Vol. 25, Issue 5. – P. 91-106.

Авторский вклад: аксиоматическая семантика языка Cloud-Sisal-kernel, эксперимента по программы, вычисляющей сумму элементов матрицы.

14. Maryasov I. V., Nepomniaschy V. A., Promsky A. V., Kondratyev D. A. Automatic C Program Verification Based on Mixed Axiomatic Semantics // Automatic Control and Computer Sciences. – 2014. – Vol. 48, Issue 7. – P. 407-414.

Авторский вклад: реализация метода локализации ошибок в системе C-lightVer.

На диссертацию и автореферат поступили положительные отзывы ведущей организации, двух официальных оппонентов и три отзыва на автореферат. Отзывы на автореферат предоставили: 1) к.н., доцент АНО ВО «Университет Иннополис» Наумчев А.В.; 2) к.ф.-м.н., доцент кафедры «Прикладная математика» ФГБОУ ВО «Алтайский государственный технический университет им. И.И. Ползунова» Старолетов С.М.; 3) к.ф.-м.н., доцент, начальник Лаборатории программной инженерии АНО ВО «Университет Иннополис» Шилов Н.В.

В отзывах отмечается актуальность темы исследования, научная новизна, теоретическая и практическая значимость полученных результатов, а также понятность и грамотность научного языка.

Основные критические замечания: незначительная часть предложенных стратегий является не полностью автоматической, а интерактивной; субъективная оценка приемлемости стратегий; сжатость описания основных методов и техник; нет обзора вкладываемости известных open source проектов в предлагаемые языки; сжатый обзор системы ACL2; не приводятся количественные характеристики проведенных экспериментов; нет обоснования выбора термина «комплексный»; не показаны границы применимости метода; неудачный стиль изложения в ряде случаев.

На все замечания в процессе защиты соискатель дал аргументированные ответы.

Выбор официальных оппонентов обосновывается их высоким уровнем компетентности и способностью оценить научную и практическую ценность диссертации. Д.ф.-м.н. Петренко А.К. и к.ф.-м.н. Скопин И.Н. являются известными специалистами в области формальных методов и проверки корректности программ, имеют публикации по теме диссертации в рецензируемых научных журналах. **Выбор ведущей организации** обосновывается тем, что Кафедра теоретической информатики Факультета информатики и вычислительной техники ЯрГУ является одним из центров компетенции в области фундаментальных основ информатики, программной инженерии и верификации программного обеспечения. Сотрудники кафедры имеют значительный объем публикаций по тематике диссертации в ведущих научных изданиях и способны определить и аргументировано обосновать научную и практическую ценность диссертации Кондратьева Д.А.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- **разработаны** метод генерации операции замены для циклов, позволяющий проводить верификацию без инвариантов циклов, набор стратегий автоматического и интерактивного доказательства условий корректности с такой операцией, а также аксиоматическая семантика языка Cloud-Sisal-kernel;
- **предложена** реализация метода локализации ошибок, позволяющая сопоставлять недоказанные условия корректности и исходный код;
- **доказана** корректность ряда стратегий упрощения и доказательства условий корректности и продемонстрирована применимость комплексного метода для ряда примеров, с которыми не справляются известные системы;
- **введены** новые классы семантических меток для метода Денни и Фишера, эффективно выражающие свойства программ с финитными итерациями.

Теоретическая значимость исследования обоснована тем, что:

- **доказаны** теорема о корректности ряда стратегий, а также общая применимость комплексного подхода не только для императивного языка Си, но и для функционального Cloud Sisal;
- **изложены** основы комплексного подхода к верификации программ с финитными итерациями, позволяющего решать задачу в целом, без дробления на слабо связанные модули;
- **раскрыта** зависимость успешного доказательства условий корректности для финитных итераций от ряда характерных условий, что позволило разработать соответствующие стратегии;

- **изучена** проблема объяснения результатов верификации для пользователя, особенно, не являющегося специалистом в логических исчислениях, применяемых при верификации;
- **проведена модернизация** системы C-LightVer, позволяющая вместо классической генерации условий корректности применять на лету теорию метаженерации.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

- **разработаны** модули системы C-LightVer и стратегии для системы ACL2, позволяющие проводить сквозные эксперименты по верификации программ с финитными итерациями и нашедшие применение в ряде проектов РФФИ и РНФ;
- **определены** перспективы перехода от верификации последовательных программ на языке Си к верификации массово параллельных программ на языке Cloud Sisal;
- **создана** модель записи финитных итераций языка Cloud Sisal в синтаксисе языка C-Light, что позволяет воспользоваться готовой системой верификации;
- **представлены** результаты серии экспериментов по верификации программ на языках Си и Cloud Sisal, из которых особый интерес представляют программы из соревнований по верификации, представляющие проблемы для известных систем.

Оценка достоверности результатов исследования выявила:

- **для экспериментальных работ** результаты получены с привлечением сертифицированного и зарегистрированного в Федеральной службе по интеллектуальной собственности модуля метаженерации условий корректности и показана воспроизводимость результатов исследований для двух языков программирования с различающимися парадигмами;
- **теория** построена как на классических принципах дедуктивной верификации программ, так и на последних достижениях в данной области;
- **идея базируется** на анализе теории и практики, на обобщении и развитии передового опыта отечественных и зарубежных коллективов;
- **использованы** опубликованные данные по рассматриваемой тематике, которые сравнивались с авторскими и показали актуальность выбранных решений;
- **установлено** качественное совпадение, а для некоторых случаев преимущество авторских результатов по сравнению с результатами, представленными в независимых источниках по данной тематике.

Личный вклад соискателя состоит в выполнении основного объема теоретических и экспериментальных исследований, представленных в

диссертации, включая выявление имеющихся в данной области проблем, анализ имеющегося опыта, постановку задач, создание методов, алгоритмов и стратегий для их решения, выполнение доказательств, реализацию предложенных алгоритмов и выполнение экспериментов. Конфликт интересов с соавторами не обнаружен. Все выносимые на защиту положения получены автором лично.

На заседании 14 сентября 2022 года диссертационный совет за решение научной задачи, имеющей значение для развития теоретической и прикладной информатики, принял решение присудить Кондратьеву Д.А. ученую степень кандидата физико-математических наук по специальности 05.13.11 — Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

При проведении тайного голосования диссертационный совет в количестве 17 человек, из них 7 докторов наук по научной специальности 05.13.11, участвовавших в заседании, из 21 человека, входящих в состав совета, проголосовали: за — 16, против — 0, воздержался — 1 (член совета, являющийся научным руководителем соискателя).

Председатель
диссертационного совета
д-р физ.-мат. наук, профессор

МАРЧУК Александр Гурьевич

Ученый секретарь
диссертационного совета
канд. физ.-мат. наук

ПРОМСКИЙ Алексей Владимирович

Дата: 14.09.2022