Отзыв научного руководителя

на диссертацию Юрия Олеговича Костюкова

«Автоматический вывод индуктивных инвариантов программ с алгебраическими типами данных»,

представленную на соискание учёной степени кандидата физико-математических наук по специальности 2.3.5. Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей

В последние два десятилетия исследования в области верификации программного обеспечения стали очень актуальны для практического применения – SAT-революция, model checking, символьное исполнение и др. теоретические результаты показали беспрецедентную релевантность практическим нуждам по обеспечению качества больших программных комплексов.

Работа Юрия Олеговича Костюкова посвящена автоматической верификации программ с алгебраическими типами данных на основе индуктивных инвариантов. В последние несколько лет появляется всё больше исследовательских и индустриальных работ, посвящённых этой тематике. Создаются инструменты верификации языков с алгебраическими типами, например, для Rust и Scala. При этом индуктивные инварианты позволяют формально доказать, что суждения верификатора о корректности программы с циклами и рекурсивными функциями верны. Поскольку алгебраические типы имеют рекурсивную структуру, то ключевым ограничением существующих подходов является их неспособность строить индуктивные инварианты, явно выражающие рекурсивный обход алгебраического терма. На практике это

приводит к тому, что соответствующие инструменты не завершаются на большинстве программ с алгебраическими типами. Поэтому актуальной является задача построения таких классов индуктивных инвариантов, которые способны явно задать рекурсивный обход терма, а также вывод инвариантов в таких классах.

В своей диссертационной работе Юрий Олегович предлагает методы автоматического вывода для трёх классов индуктивных инвариантов, построенных на автоматах над деревьями, которые применяются для верификации программ с алгебраическими типами данных и позволяют строить рекурсивные обходы термов.

В диссертационной работе также предложены новые методы автоматического вывода для классов инвариантов, основанные на классических и синхронных автоматах над деревьями. Эти методы выполняют сведение данной задачи к поиску конечных моделей, что является новой технике, благодаря которой реализация предложенных методов позволила решить множество задач, не решаемых существующими подходами. Следует отметить, что появление этой техники является очень важным событием в области вывода инвариантов программ с алгебраическими типами, поскольку классические техники либо тяжело адаптируются к этой задаче, либо не дают ожидаемых практических результатов.

Кроме того, Юрий Олегович предложил новый класс индуктивных инвариантов, основанный на комбинации формул и автоматов над деревьями. Поскольку в этом классе выразимы все инварианты, выразимые в объединяемых подклассах, то с его помощью может быть верифицировано значительное количество реальных программ. Основываясь на этом, была предложена техника комбинации методов вывода инвариантов в подклассах, которая позволяет путём небольших изменений существующих инструментов получить вывод инвариантов

в более широком классе. Эффективность предложенной техники была проверена экспериментально – с её помощью из общепринятого тестового набора было решено существенно больше задач, чем имеющимися на данный момент инструментами. Также пилотная реализация этой техники заняла первое место на известном международном соревновании верификаторов CHC-COMP 2022 (трек алгебраических типов данных).

Наконец, в работе представлено теоретическое сравнение предложенных и существующих классов индуктивных инвариантов – их выразительной силы и доступных операций. Для нужд этого теоретического сравнения были сформулированы и доказаны аналоги лемм о «накачке» для языков логики первого порядка, которые являются новым теоретическим инструментом для доказательства отсутствия у программы индуктивного инварианта в заданном классе. Данное теоретическое сравнение вносит порядок относительно существующих классов индуктивных инвариантов, что позволит проектировать новые, приспособленные к автоматической верификации, классы инвариантов.

Юрия Олегович занимается данной тематикой более пяти лет, ещё со времен обучения в бакалавриате, и является активным членом исследовательской группы по языкам программирования кафедры системного программирования. За это время он показал себя мотивированным исследователем, способным к плодотворным творческим прорывам, а также продемонстрировал уникальную работоспособность. Следует отметить имеющиеся у него редкое сочетание склонности к математическим построениям и прекрасные навыки практической работы (знание многочисленных языков программирования, умение быстро разбираться с различными программными инструментами, создавать эффективные программные реализации). Он способен брать на себя инициативу и очень быстро создавать различные рабочие продукты – от пилотной

программной реализации нового метода до текста диссертации. Он весьма самодостаточен и в то же время легко работает в коллективе.

Хочу также подчеркнуть, что результаты работы опубликованы в ведущих международных конференциях по языкам программирования (PLDI, LPAR) и, таким образом, согласованы с международным научным сообществом. В то же время у автора имеются публикации в ведущих российских журналах по данной тематике — «Труды ИСП РАН», «Вестник ИТМО».

Следует отметить, что диссертационная работа была выполнена автором полностью самостоятельно, полученные результаты обладают несомненной научной новизной, а также имеют важное прикладное значение.

Итак, можно сделать вывод, что представленная диссертация является законченной научно-исследовательской работой и отвечает всем требованиям, предъявляемым к кандидатским диссертациям, в частности, полностью соответствует паспорту специальности 2.3.5. Соответственно, её автор, Юрий Олегович Костюков, заслуживает присуждения ему учёной степени кандидата физико-математических наук по специальности 2.3.5. Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей.

Кознов Дмитрий Владимирович,
доктор технических наук, доцент,
профессор кафедры системного
программирования Санкт-Петербургского
государственного университета

Подпись руки Кознова Д.В.
УДОСТОВЕРЯЮ
Специалист по кадровой работе
«07» 09 2023 г.