

ОТЗЫВ официального оппонента
о диссертации на соискание ученой степени
кандидата физико-математических наук
Кондратьева Дмитрия Александровича
на тему: «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»

Актуальность избранной темы

Постановка задачи, представленная в работе, объединяет в себе цели развития теории верификации программ и цели совершенствования методов и инструментов верификации, которые смогли бы приблизить техники дедуктивной верификации к практике инженеров-программистов. Автор правильно указывает на три важнейших проблемы, мешающих более широкому применению методов дедуктивной верификации, это: проблемы конструирования инвариантов циклов, проблемы локализации и объяснения ошибок и проблемы автоматизации доказательства условий корректности программ.

Основное содержание работы

Работа состоит из обзорной главы «Методы дедуктивной верификации программ», двух глав, в которых описываются основные результаты, выносимые на защиту, и двух глав, где даются описания опыта применения предложенного комплексного подхода к верификации однопоточных и параллельных программ.

Обзорная глава написана хорошим языком, содержит описание хорошо отобранного материала, на базе которого можно познакомиться с проблемами, которые диссертант рассматривает как основные в своем исследовании, и отправные точки для поиска направлений решения этих проблем. В качестве таких направлений диссертант указывает на сужение

класса рассматриваемых программных систем (программы с финитными итерациями), разработку алгоритмов для автоматизации генерации условий корректности с точностью до отдельных конструкций языка C-light, а также оригинальное решение для упрощения анализа результатов верификации и отладки исходных кодов реализации и артефактов верификации в терминах понятных инженеру-программисту.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

Автор методично рассматривает задачи верификации программных систем в контексте создания программного обеспечения промышленного уровня сложности. Достаточно полно и правильно сформулированы источники проблем, усложняющих внедрение методов верификации в инженерную практику. Рекомендации направлены на:

- некоторое сужение класса программ, написанных на языке Си,
- разработка методов и алгоритмов и реализация инструментальной поддержки автоматизации верификации, которая существенно использует свойства выбранного класса программ,
- развитие инструментов анализа и отладки в процессе верификации, доступных инженеру-программисту, не имеющему глубоких знаний в области верификации.

Интегрально достоверность полученных результатов подкрепляется подробно разобранными сквозными примерами применения предложенных методов и инструментов для верификации однопоточных и параллельных программ.

Новизна полученных результатов

К новым научным результатам относятся:

- метод автоматизации доказательства условий корректности программ с финитными итерациями без использования инвариантов циклов;
- метод локализации ошибок, выявленных во время дедуктивной верификации программ с финитными итерациями без использования инвариантов циклов;
- обобщение опыта применения комплексного подхода к верификации программ в случае однопоточных и параллельных программ.

Замечания


1. Следует признать несбалансированность структуры диссертации. Обзорная глава написана хорошим научным языком и позволяет увидеть общий ландшафт в исследуемой области и особенности предлагаемых направлений исследований. Главы, где излагается основной набор положений, выносимых на защиту, технически насыщены, но не дают обстоятельного изложения общих принципов, на которых основываются предлагаемые методы и техники автоматизации процесса верификации.
2. Предлагаемое сужение подмножества языка, следовало бы исследовать в плане того, какие программы или их фрагменты (например, из известных open source проектов) уже сейчас принадлежат этому подмножеству, и какие можно привести к рамкам этого подмножества при помощи известных техник и инструментов трансляции.
3. Систему ACL2, которая выбрана как основная платформа для развития предлагаемых инструментов автоматизации верификации, можно было бы описать более подробно, иначе читателю приходится знакомиться с ней самостоятельно, а автор даже не подсказывает, где можно найти описание хорошее ACL2. Кроме того, сделав выбор ACL2, следовало бы рассмотреть возможности применения Coq, Frama-C и Isabelle и указать, насколько эти платформы эффективны при реализации методов, предложенных в данной диссертации.
4. Также для рассмотренных в тексте диссертации программ было бы интересно увидеть общие итоговые данные о числе сгенерированных условий верификации, числе автоматически разрешенных условий верификации, времени работы реализованных стратегий и встроенных стратегий системы доказательства теорем ACL2 на сгенерированных условиях верификации. Имело бы смысл сравнить время работы и разрешимость условий верификации с другими целевыми системами доказательства/решателями, например CVC4 или Z3.

Вместе с тем, указанные замечания не умаляют значимости диссертационного исследования.

Диссертация Кондратьева Дмитрий Александровича «Методы комплексного подхода к автоматизации дедуктивной верификации программ с финитными итерациями» является самостоятельной, законченной научно-квалификационной работой, в которой на основании выполненных исследований получено решение актуальной научной проблемы разработки методов верификации важного класса программных систем. Диссертация отвечает требованиям Положения ВАК РФ о порядке присуждения ученых степеней, а ее автор, Кондратьев Дмитрий Александрович, заслуживает присуждения ему ученой степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Официальный оппонент:

заведующий отделом Технологий программирования,
ФГБУН Института системного программирования им. В.П.Иванникова РАН
профессор, доктор физ.-мат. наук,

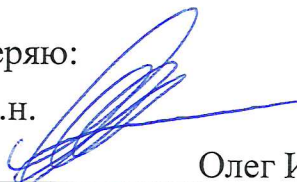


Александр Константинович ПЕТРЕНКО

30 августа 2022 года.

Подпись Петренко А.К. удостоверяю:

Ученый секретарь ИСП РАН, к.т.н.



Олег Ильгисович САМОВАРОВ

30 августа 2022 года



Петренко Александр Константинович, доктор физико-математических наук по специальности 05.13.11 — Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей, профессор, заведующий Отделом технологий программирования Федерального государственного бюджетного учреждения науки Института системного программирования им. В.П. Иванникова Российской академии наук (ИСП РАН),

109004, г. Москва, ул. А. Солженицына, дом 25.

телефон: +7(495) 912-44-25

вебсайт: <https://www.ispras.ru/>

электронная почта: info-isp@ispras.ru

Контактные данные:

телефон: +7(495) 912-56-59 (доб. 404).

электронная почта: petrenko@ispras.ru