УТВЕРЖДАЮ:

Директор
Федерального исследовательского центра
«Информатика и управление»
Российской академии наук
(ФИЦ ИУ РАН)

_____ И.А. Соколов

«02» мая 2017 г.

ОТЗЫВ

ведущей организации - Федерального исследовательского центра «Информатика и управление» Российской академии наук (ФИЦ ИУ РАН) на диссертацию Мордань Виталия Олеговича «Методы верификации программ на основе композиции задач достижимости», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Актуальность работы. Диссертационная работа Мордань В. О. относится к области разработки методов и средств верификации программного обеспечения. Существуют формальные методы (например, пошаговое уточнение), при помощи которых может быть получен код программы на языке программирования, доказательно правильно реализующий абстрактную спецификацию требований. Однако, большое количество программного обеспечения (ПО) с требованиями повышенной надежности разрабатывается без использования таких средств. Объемы ПО могут достигать миллионов строк кода, регулярно изменяемых тысячами программистов. Очевидно, что для верификации такого ПО необходимы автоматические методы. Одной из перспективных групп автоматических методов является статическая верификация, когда проверка

исходного кода осуществляется без его выполнения. При этом производится не только поиск встречающихся ошибок, но и доказательство корректности ПО, гарантирующее отсутствие определенных ошибок. Статическая верификация позволяет проверять программы относительно требований, которые сводятся к задачам достижимости исполняемой программой определенного места в коде.

Для проверки выполнения нескольких требований в программе с помощью существующих средств статической верификации для каждого требования подготавливается и решается отдельная задача достижимости. В этом случае промежуточные результаты верификации теряются, поэтому требуемые на верификацию ресурсы в среднем увеличиваются пропорционально числу требований, и для больших программных систем вычислительных ресурсов требуется много.

Конкретной актуальной задачей исследования является разработка методов статической верификации ПО для проверки программ на соответствие композиции требований. Часть требований (или все) объединяются в группу, для них создается и проверяется одна задача достижимости. При этом могут возникнуть новые трудности: во-первых, экспоненциальный рост числа состояний в модели программы за счет усложнения решаемых задач (т.е. в общем случае возможна потеря результата относительно базового метода статической верификации); во-вторых, остановка верификации после нахождения нарушения одного из требований, что ведет к потере результата для остальных требований. Диссертационная работа нацелена на разрешение данных проблем для повышения производительности статической верификации композиции требований без потерь результата.

Структура работы.

Диссертационная работа состоит из введения, пяти глав, списка литературы и трех приложений.

Во введении обосновывается актуальность темы диссертационной работы, ставятся ее цели и задачи и раскрывается ее практическая значимость.

В первой главе приведен обзор существующих методов подготовки и решения задач достижимости в рамках статической верификации. В качестве базового подхода статической верификации рассматривается подход уточнения абстракции по контрпримерам (counterexample-guided abstraction refinement – CEGAR). Помимо этого, рассмотрены различные методы повторного использования информации в статической верификации, в которых решается схожая задача. По результатам обзора делается вывод о том, что существующие методы статической верификации не позволяют эффективно выполнять проверку программы относительно нескольких требований.

Во второй главе описаны методы, нацеленные на разрешение проблем верификации композиции требований. Метод обнаружения всех однотипных нарушений продолжает верификацию после нахождения первого нарушения требования и, следовательно, способен выявлять больше ошибок в программах, нарушающих проверяемое требование. Однако для этого метод требует большего количества ресурсов, нежели базовый метод статической верификации, и проведения ручного анализа результатов с целью выявления причины каждого из найденных нарушений требования.

Метод условной многоаспектной верификации предлагает эвристическое решение проблемы экспоненциального роста числа состояний, имеющее смысл в рамках подхода CEGAR. Основная идея заключается в равномерном распределении ресурсов между проверкой различных требований. Если задача не может быть решена из-за некоторого требования, то соответствующие требованию проверки удаляются и производится верификация без данного требования. Для разработанного метода сформулирована и доказана теорема о сохранении полноты и корректности верификации относительно базового метода.

В третьей главе предлагается расширение метода условной многоаспектной верификации. Для упрощения описания задач достижимости, создаваемых при проверке групп требований, был предложен язык автоматных спецификаций, формализующий требование в виде конечного автомата. Описание автомата передается верификатору независимо от исходного кода программы.

Предложенный язык расширяет известные в литературе описания наблюдательных автоматов возможностью встраивать произвольные конструкции языка программирования во внутреннее представление программы и функцию переходов между состояниями в автомате.

Предложен метод декомпозиции автоматной спецификации, нацеленный на верификацию композиции требований путем разделения их на группы требований. Верификация групп требований является более эффективной, чем последовательная либо совместная верификация всего множества требований. Данный метод является расширением метода условной многоаспектной верификации, то есть он может использоваться на базе произвольных подходов статической верификации. Сформулирована и доказана теорема о сохранении полноты и корректности разработанного метода относительно базового метода статической верификации.

В четвертой главе описывается реализация предложенных методов в рамках открытых проектов Linux Driver Verification Tools (система верификации ядра ОС Linux) и CPAchecker (статический верификатор, реализующий подход CEGAR).

В пятой главе описываются результаты экспериментов. В экспериментах проверялось выполнение требований на корректное использование интерфейсов сердцевины ядра операционной системы Linux в модулях ядра. Методы условной многоаспектной верификации и декомпозиции автоматной спецификации продемонстрировали повышение производительности верификации в 4-5 раз при потерях примерно 1% результата относительно базового метода верификации. Метод обнаружения всех однотипных нарушений позволил выявить в 1.5 раза больше ошибок, однако на ручной анализ результата для выявления причин нарушений требований потребовалось также в 1.5 раза больше времени.

Научная новизна работы заключается в разработке следующих оригинальных методов:

1) Метод статической верификации программного обеспечения для обнаружения всех однотипных нарушений проверяемого требования.

2) Метод статической верификации программного обеспечения для проверки выполнения композиции требований (условная многоаспектная верификация).

3) Метод статической верификации программного обеспечения, расширяющий возможности представления требований в виде их автоматных спецификаций.

4) Метод статической верификации программного обеспечения на основе декомпозиции автоматной спецификации требований на группы требований для совместной верификации внутри группы.

Научной новизной обладают также утверждения и теоремы, обосновывающие корректность разработанных методов.

Значимость результатов исследований заключается в том, что выполненные в работе теоретические исследования расширяют спектр методов статической верификации программ и открывают новые возможности повышения их производительности и качества.

Представляется важным дальнейшее развитие разработанных методов совместно с методами регрессионной верификации, создание новых стратегий разбиения множества требований на группы в методе декомпозиции автоматных спецификаций.

Практическая ценность. Реализация методов статической верификации, предложенных в диссертационной работе, в качестве расширения системы верификации Linux Driver Verification Tools и статического верификатора CPAchecker, позволила повысить производительность верификации в 4-5 раз.

В качестве **рекомендации по использованию результатов диссертации** считаем целесообразным внедрять разработанные инструментальные средства в процессы разработки ПО, к которому предъявляются повышенные требования надежности (операционные системы, встраиваемые системы) в организациях космической, транспортной, медицинской и других отраслей.

Отдельные положения диссертации и разработанные инструментальные средства могут быть использованы в учебном процессе при проведении занятий по дисциплинам, связанным с технологиями верификации программ в высших учебных заведениях.

Обоснованность и достоверность основных научных положений, выводов и результатов, представленных в диссертации, базируется на методах статической верификации программ; утверждениях и теоремах, обосновывающих корректность разработанных методов; результатах экспериментального применения методов на реальных задачах верификации модулей ядра ОС Linux.

Общая характеристика работы. Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования Московский государственный университет имени М.В. Ломоносова и Федеральном государственном бюджетном учреждении науки Институт системного программирования Российской академии наук и состоит из введения, пяти глав, заключения, списка сокращений, списка использованных источников и трех приложений. По структуре и объему замечаний нет. Диссертация аккуратно оформлена, содержание изложено грамотным научным языком. По стилю изложения замечаний нет. Основное содержание диссертационной работы Мордань В. О. опубликовано в 5 печатных работах, из них 3 - в изданиях, рекомендованных ВАК РФ; автором получены 2 свидетельства о государственной регистрации программы для ЭВМ. Материалы диссертации докладывались на 6 международных конференциях и семинарах.

Автореферат правильно отражает основные результаты, полученные в диссертационной работе.

Замечания по работе. По работе Мордань В. О. имеются отдельные замечания.

1) Во введении автору следовало бы более явно выделить область

применения разработанных методов.

2) В п. 2.2.2, 2.2.3 следовало бы сопроводить общие описания функций *conversion, comparison* примерами таких функций и их применения.

3) В п. 2.3.2 следовало бы более подробно объяснить, почему принцип *последнего проверяемого утверждения* является аппроксимацией, и в каких случаях в реальности он нарушается.

4) В формулировках условий утверждений и теорем о корректности разработанных методов следовало бы добавить фразу «без ограничения ресурсов». Хорошо было бы привести доказательство с более высокой степенью формализации (например, в *Утверждении 2* построить по произвольной спецификации инструментирования автоматную спецификацию и, наоборот, индукцией по синтаксису спецификаций).

5) В п. 5.6 на основании экспериментов более корректно было бы говорить о паритете методов инструментирования и автоматных спецификаций.

Заключение. Указанные замечания не снижают значимость теоретических и практических результатов, полученных Мордань В. О. Также эти замечания не снижают положительную оценку диссертационной работы. Диссертация, в соответствии с требованиями «Постановления Правительства Российской Федерации о порядке присуждения ученых степеней» от 24.09.2013 г. № 842 является законченной научно-квалификационной работой, в которой предложены методы и средства решения актуальной научной задачи – *статической верификации программного обеспечения на основе композиции задач достижимости*, и соответствует пункту 1 паспорта специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей». Таким образом, Мордань Виталий Олегович заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Диссертационная работа рассмотрена и рекомендована к защите, отзыв обсужден на семинаре Лаборатории 23 Композиционных методов и средств построения информационных систем ИПИ РАН Федерального исследовательского центра «Информатика и управление» Российской академии наук 19 апреля 2017 г., протокол № 2017-23-01.

Ученый секретарь ФИЦ ИУ РАН,
доктор технических наук

В. Н. Захаров
__ 2017 г.

Заведующий лабораторией ФИЦ ИУ РАН
доктор физико-математических наук, про

Л. А. Калиниченко
__ 2017 г.

Старший научный сотрудник ИПИ ФИЦ ИУ РАН
кандидат технических наук

С. А. Ступников
__ 2017 г.

Наименование организации: Федеральное государственное учреждение Федеральный исследовательский центр "Информатика и управление" Российской академии наук.

Адрес: РФ, 119333, г. Москва, ул. Вавилова, д. 44, корп. 2

E-mail: ipiran@ipiran.ru

Сайт: http://www.frccsc.ru/

Тел.: +7 (499) 135-62-60