Отзыв официального оппонента

Волконского Владимира Юрьевича на диссертационную работу
Мордань Виталия Олеговича
«Методы верификации программ на основе композиции задач достижимости»,
представленную к защите на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

Задача автоматической проверки корректности программ является крайне важной. С одной стороны, существует большое количество программных систем с требованиями повышенной надежности, ошибки в которых могут привести к различным негативным последствиям. С другой стороны, подобные программные системы постоянно развиваются, в процессе чего неизбежно могут добавляться новые ошибки. Традиционные методы тестирования, базирующиеся на выборочных проверках, не способны гарантировать корректность программ. Для доказательства отсутствия ошибок в программах в настоящее время развиваются различные *методы верификации*. Одним из перспективных направлений для автоматической проверки программ является *статическая верификация* программного обеспечения, значительное усовершенствование которой представлено в диссертационной работе Мордань В.О., что подтверждает ее *актуальность*.

Ограничения существующих алгоритмов статической верификации ведут к нерациональному использованию ресурсов, что существенно затрудняет их использование на практике. Во-первых, в них отсутствует возможность проверять *выполнение нескольких свойств* в программе, вследствие чего проверка выполнения свойств производится по отдельности, а промежуточные результаты верификации теряются. Верификация объединенного свойства не решает всех проблем, так как возможна потеря результата из-за усложнения решаемой задачи. Во-вторых, подходы статической верификации *останавливаются после нахождения первой ошибки*, т. е. они не способны находить несколько однотипных ошибок, что на практике также приводит к увеличению требуемых ресурсов на верификацию для исправления всех подобных ошибок. Хотя статическая верификация требует значительных вычислительных ресурсов даже для проверки одного свойства и выявления только одного его нарушения, предложенный в работе метод статической верификации *композиции требований*, каждое из которых может *нарушаться более одного раза*, подтверждают *научную новизну* работы.

Диссертация состоит из введения, пяти глав и заключения. Список литературы содержит 77 наименований.

Во **введении** формулируется цель работы, ставятся задачи, обосновывается актуальность и раскрывается научная новизна.

В **первой главе** анализируются существующие методы статической верификации. Рассмотрен весь процесс верификации, который включает в себя генерацию верификационных задач (задач достижимости) и их решение. Кроме того, рассмотрены методы, решающие задачу использования ранее полученных результатов верификации, которые показывают нетривиальность поставленной задачи. На основе проведенного обзора делается вывод, что существующие методы не предназначены для решения поставленной цели работы – проверки программы на соответствие композиции требований.

Во **второй главе** рассматриваются *новые методы*, предложенные в диссертационной работе, нацеленные на снятие ограничений используемого базового метода, который проверяет только одно требование и останавливается после первого нарушения. Для решения проблемы остановки статической верификации после нахождения первой ошибки предложен *метод обнаружения всех однотипных нарушений.* Я рассматриваю этот метод как крайне важный результат работы, т.к. он позволяет выявлять за одно применение больше ошибок при сопоставимых затратах ресурсов, хотя даже после автоматической фильтрации «наведенных» трасс ошибок требует дополнительного ручного анализа. Для возможности верификации *композиции требований* предложен *метод условной многоаспектной верификации*, распределяющий вычислительные ресурсы между проверкой различных требований поровну при верификации их композиции. Для этого принимается упрощение, которое верно для подхода уточнения абстракции по контрпримерам. Метод способен повысить эффективность верификации за счет того, что промежуточные результаты верификации не будут теряться, кроме того, ресурсы на проверку каждого требования ограничиваются, как и в базовом методе. В работе также показана возможность совместного использования предложенных методов для нахождения всех однотипных нарушений нескольких проверяемых требований.

В **третьей главе** указываются проблемы предложенных в предыдущей главе методов – усложнение исходного кода при генерации верификационных задач и ограничение области применимости подходом уточнения абстракции по контрпримерам. Для решения первой проблемы предлагается *новый метод* описания проверяемых требований с помощью конечных автоматов, которые не добавляются непосредственно в проверяемый код, – *метод автоматных спецификаций.* На основе автоматных спецификаций был предложен метод декомпозиции автоматной спецификации, предназначенный для построения такого разбиения проверяемых требований на группы, верификация которого будет более эффективной. *Метод декомпозиции автоматных спецификаций* может использоваться совместно с произвольным подходом статической верификации для проверки выполнения композиции требований в программах.

В **четвертой главе** описывается практическая часть работы. Предложенные методы статической верификации были реализованы в инструменте CPAchecker, а новые методы генерации верификационных задач были добавлены в систему верификации Linux Driver Verification Tools, которая предназначена для верификации модулей ядра операционной системы Linux.

В **пятой главе** приводится экспериментальная оценка предложенных методов на основе использования системы Linux Driver Verification Tools. Методы, предназначенные для обнаружения всех однотипных нарушений, позволили находить примерно в 1.5 раза больше ошибок в проверяемом коде, нежели базовый метод, при этом для анализа результата требовались сопоставимые с базовым методом ресурсы. Методы, предназначенные для верификации композиции требований (условная многоаспектная верификация и декомпозиция автоматной спецификации), продемонстрировали сопоставимые результаты, сократив при этом время верификации более чем в 4 раза. Таким образом, эксперименты подтверждают высокую эффективность предложенных в диссертационной работе методов.

В заключении приводятся основные результаты диссертационной работы, которые выносятся на защиту:

- Методы статической верификации программного обеспечения, основанные на инструментировании исходного кода и предназначенные для обнаружения всех однотипных нарушений и проверки выполнения композиции требований с помощью условной многоаспектной верификации.
- Методы статической верификации программного обеспечения, с использованием формализации требований в виде автоматных спецификаций и декомпозиции автоматной спецификации на группы требований для совместной верификации.
- Теорема о полноте и корректности предложенных методов для требований, удовлетворяющих ограничениям инструментирования исходного кода программы.

Практическая значимость диссертации заключается в том, что все предложенные в работе методы были реализованы на основе открытых проектов, после чего применены для верификации большого объема реального кода. Проведенные эксперименты демонстрируют существенное повышение производительности всего процесса верификации при проверке выполнения композиции требований в программах. Для предложенных методов *сформулированы и доказаны утверждения и теоремы о сохранении полноты и корректности*, что подтверждает *достоверность и обоснованность результатов работы*. Основные результаты работы были опубликованы, и прошли апробацию на научных конференциях и семинарах.

По диссертационной работе имеются следующие замечания:

- Применение предложенных методов ограничивается границами модулей, к сожалению, четко не определенными в работе
- Ресурсные ограничения методов статической верификации приводят к потере некоторых потенциальных ошибок, но в работе недостаточно внимания уделено определению оптимального размера ресурсов
- Выбор стратегии релевантности как основной в методе декомпозиции автоматной спецификации не свободен от недостатков, приводящих к снижению его эффективности при большом числе релевантных требований

В целом указанные замечания не влияют на положительную оценку работы.

Автореферат полно и правильно отражает содержание диссертационной работы.

Диссертационная работа соответствует всем требованиям ВАК РФ, предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук, а ее автор, Мордань Виталий Олегович, заслуживает присуждения ему ученой степени по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Кандидат технических наук, старший научный сотрудник, начальник отделения «Системы программирования» публичного акционерного общества «ИНЭУМ им. И.С. Брука» В.Ю. Волконский

Подпись кандидата технически
Волконского В.Ю. заверяю, зам. ген
директора ПАО «ИНЭУМ им. И.С. Б В.И. Перекатов

«5» мая 2017 г.