Отзыв официального оппонента

доктора физико-математических наук Соколова Валерия Анатольевича
на диссертационную работу Мордань Виталия Олеговича на тему:
«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»

Актуальность

Данная диссертационная работа имеет целью развитие методов статической верификации программного обеспечения, которые позволяют автоматически доказывать выполнение некоторых требований в программах. Подобные методы используются для проверки программного обеспечения с высокими требованиями надежности, ошибки в котором могут приводить к серьезным последствиям.

На практике статическая верификация применима для относительно небольших программ, при этом требует значительного количества вычислительных ресурсов. В существующих методах статической верификации проверка выполнения множества требований не предусмотрена, поскольку в общем случае она приводит к усложнению решаемых задач и к потере результата на практике, поэтому для проверки выполнения нескольких требований каждое из них верифицируется отдельно. Подобное решение является нерациональным и на практике приводит к чрезмерному расходованию вычислительных ресурсов. Помимо этого, существующие методы статической верификации не позволяют выявлять более одного нарушения требования в программах. Именно на решение этих проблемы и нацелена диссертационная работа.

Предложенные в работе методы статической верификации программного обеспечения предназначены для проверки соответствия программ композиции требований с учетом того, что каждое требование может нарушаться более одного раза. Для данных методов указано множество поддерживаемых требований, для которых были сформулированы и доказаны теоремы о сохранении полноты и корректности верификации относительно базового метода. На практике предложенные методы позволили повысить производительность верификации композиции требований в несколько раз.

Структура работы

Диссертация В.О. Мордань состоит из введения, пяти глав, списка литературы и трех приложений.

Во **введении** обоснована актуальность темы диссертационной работы, поставлены ее цели и задачи, сформулированы научная новизна и выносимые на защиту результаты работы.

Первая глава диссертации содержит обзор существующих методов статической верификации программного обеспечения с точки зрения возможности их использования для верификации композиции требований.

Во **второй главе** предложены два новых метода статической верификации – метод обнаружения всех однотипных нарушений и метод условной многоаспектной верификации. Данные методы решают проблемы существующих методов статической верификации, которые возникают при верификации композиции требований. Метод обнаружения всех однотипных нарушений предназначен для выявления большего числа нарушений требования в программах. Метод условной многоаспектной верификации решает проблему экспоненциального роста числа состояний в модели программы, которая является следствием усложнения задач верификации, путем эвристического ограничения времени проверки каждого требования. Указанная эвристика применима только в подходе уточнения абстракции по контрпримерам (CEGAR). Данный метод предназначен для снижения ресурсов на верификацию композиции требований за счет переиспользования промежуточных результатов верификации, которые не ведут к чрезмерному росту числа состояний в модели программы. Для сохранения полноты и корректности верификации в методе условной многоаспектной верификации вводятся ограничения на формализацию проверяемых требований, которые запрещают изменять исходные пути выполнения программы.

В **третьей главе** рассмотрена проблема усложнения непосредственно проверяемого кода, в который перед верификацией добавляются вспомогательные проверки выполнения требований, что увеличивает накладные расходы на верификацию при возрастании числа требований. Для ее решения предлагается метод автоматных спецификаций, который передает модель требования верификатору в его внутреннем представлении, не модифицируя при этом код программы. Для проверки композиции требований данный метод расширяется до метода декомпозиции автоматной спецификации, который разбивает все требования на группы требований для более эффективной верификации и решения проблемы экспоненциального роста числа состояний в модели программы. При выполнении ограничений на формализацию требований доказывается сохранение полноты и корректности в методе декомпозиции автоматной спецификации относительно базового метода. В сравнении с методом условной многоаспектной верификации, который является расширением подхода CEGAR, данный метод может использоваться совместно с произвольными подходами статической верификации, то есть его область применимости значительно шире.

Четвертая глава посвящена реализации методов, предложенных в

диссертационной работе.

В **пятой главе** представлены результаты экспериментов, в которых производилась верификация всех модулей ядра операционной системы Linux. Метод обнаружения всех однотипных нарушений позволил выявить в 1.5 раза больше ошибок, однако для этого потребовалось существенное время на анализ результата. Методы условной многоаспектной верификации и декомпозиции автоматной спецификации сократили время верификации в несколько раз при незначительных потерях результата.

Научная новизна

Научной новизной обладают следующие результаты диссертационной работы:

- Метод статической верификации программного обеспечения для обнаружения всех однотипных нарушений проверяемого требования.
- Метод статической верификации программного обеспечения для проверки выполнения композиции требований (условная многоаспектная верификация).
- Метод статической верификации программного обеспечения, расширяющий возможности представления требований в виде их автоматных спецификаций.
- Метод статической верификации программного обеспечения на основе декомпозиции автоматной спецификации требований на группы требований для совместной верификации внутри группы.
- Сформулированы и доказаны утверждения и теоремы, являющиеся обоснованием корректности предложенных методов.

Практическая значимость

Реализация методов выполнена на основе открытых проектов. Предложенные в данной работе методы могут применяться в других исследовательских проектах для верификации произвольных программ.

Достоверность и обоснованность научных положений и выводов работы

Достоверность результатов работы подтверждается доказательством теорем о сохранении полноты и корректности для предложенных методов и апробацией основных результатов на 7 научных конференциях и семинарах. По теме диссертации автором было опубликовано 5 работ, 3 из которых опубликованы в

изданиях из списка ВАК, и получено 2 свидетельства о государственной регистрации программы для ЭВМ.

Замечания

Наряду с интересными и практически важными результатами, диссертационная работа содержит ряд неточностей и опечаток.

К опечаткам можно, вероятно, отнести следующие погрешности:

- Стр. 17. «… для одной 32-битной переменной без начального значения нужно перебрать 2^32 только начальных состояний, а для рассматриваемой простейшей программы граф достижимости состоял бы из 3*2^32 (почти 13 миллиардов) состояний». Вероятно, имелось в виду, что для программы с тремя 32-битными переменными без начального значения будет (2^32)*(2^32)*(2^32) начальных состояний у соответствующего ей графа достижимости.
- Стр. 34. «данный метод … позволяет во многих случаях как существенно ускорить верификацию, так и разрешить ранее неразрешимые задачи». Несколько вольное отношение к понятию «неразрешимая задача». Возможно, предполагалось «ранее нерешённая задача».
- Стр. 45. Опечатка в имени переменной «modev_var_X». Должно быть «model_var_X».
- Стр. 77. Указывается, что наблюдательный автомат – это недетерминированный конечный автомат. Но при его определении автором используется функция перехода между состояниями, а не отношение перехода. Другими словами, на самом деле в тексте приводится определение детерминированного автомата.

В некоторых определениях и формулировках встречаются неточности.

Так, например, на стр. 50 в пункте "Формализация эквивалентности трасс ошибок" нет чёткого определения эквивалентности двух трасс. Понятие эквивалентности трасс вводится неформально с использованием функции фильтра f(t1,t2), определения которой также не приводится.

На стр. 52 определяется тип фильтрации на основе функции преобразования conversation(t). Две трассы считаются эквивалентными, если результаты применения к ним функции преобразования совпадают. Но в тексте диссертации не поясняется, что является результатом применения функции преобразования conversation(t).

В пункте 2.2.3 весьма поверхностно описывается полуавтоматическая фильтрация трасс ошибок. Остаётся непонятной степень вовлечённости человека и его трудозатраты на полуавтоматическую фильтрацию.

На стр. 87 осталось непонятным, что понимается под "грамотным

распределением ресурсов".

Доказательства ряда утверждений оформлены избыточно. Например, в доказательстве утверждения 1, занимающего всего лишь половину страницы, две трети доказательства приходятся на переформулировку утверждения и подытоживание рассуждений, которые в свою очередь составляют оставшуюся треть текста доказательства (т.е. не более шести строк).

Из работы следует, что большинство (или даже все) из предлагаемых методов и подходов в общем случае неразрешимы, но рамки разрешимости не устанавливаются. В частности, на стр. 51 указывается, что автоматическая фильтрация найденных трасс ошибок не является разрешимой задачей. При этом для упрощения предлагается сравнивать трассы на полную эквивалентность, но понятие полной эквивалентности в работе не определяется. На этой же странице появляется без пояснений и термин «идентичные трассы ошибок».

Исправление отмеченных недостатков, скорее всего, помогло бы улучшить стиль изложения диссертационной работы. Однако, считаю, что эти недостатки не оказывают существенного влияния на значение полученных автором результатов, прошедших практическую апробацию и продемонстрировавших впечатляющие показатели.

Заключение

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

Заведующий кафедрой теоретической
информатики ЯрГУ им. П.Г.Демидова,
доктор физико-математических наук, профессор В.А. Соколов

27 апреля 2017 г.

Подпись доктора физико-математических наук,
профессора В.А. Соколова удостоверяю.
1-й проректор ЯрГУ им. П.Г. Демидова,
доктор физико-математических наук, проф С.А. Кащенко

27 апреля 2017 г.