ОТЗЫВ

официального оппонента Муромцева Дмитрия Ильича на диссертацию соискателя Хаберланда Рене на тему «Логический язык программирования как инструмент спецификации и верификации динамической памяти», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Актуальность темы диссертации

Постоянный рост сложности программного обеспечения (ПО), появление новых языков программирования, библиотек и инструментов разработки приводит к усложнению оценки качества работы ПО. Большинство существующих подходов (например, тестирование и профилирование) не дают гарантий корректности выполнения, за исключением методик верификации программного кода. Однако, применение данных методик затрудняется сложностью описаний моделей функционирования ПО. В диссертационном исследовании Хаберланда Рене описывается решение данной проблемы с помощью создания единого языка для спецификации и верификации динамической памяти на базе диалекта Пролога, а также инструментов автоматизации анализа. Подобное решение значительно упрощает процедуру разработки и валидации качества работы ПО, в связи с чем решаемая в диссертации задача является актуальной.

Научная новизна результатов исследования

В ходе проведенных исследований автором получены следующие новые научные результаты:

1. Диалект языка Пролог как инструмент спецификации и верификации динамической памяти, позволяющий в рамках одного формализма описывать желаемое поведение ПО и проверять соответствие для уже разработанного продукта за счет снятия ограничений выразимости.
2. Метод для верификации абстрактных предикатов куч на основе распознавания атрибутной транслирующей грамматики, обеспечивающий верификацию куч на этапе синтаксического анализа их структуры, что позволяет проводить автоматическое сравнение с имеющимся экземпляром памяти.
3. Подход к устранению многозначности описания куч для упрощения их анализа и верификации, позволяющий упростить сравнение куч, а также обеспечивает возможность автоматического доказательства равенства или неравенства куч.

4. Комплекс программных средств для верификации динамической памяти, обеспечивающий гибкую проверку динамической памяти (включая верификацию) для различных входных языков, в том числе и пустого языка.

Обоснованность и достоверность результатов исследования

Обоснованность и достоверность полученных в диссертации результатов обеспечивается подробностью проведенного исследования литературы, включившего в себя важнейшие работы в международных научных изданиях, адекватностью используемых моделей, строгостью математического изложения и доказательств, разработкой прототипа.

Ценность результатов исследования для науки и практики

Основная теоретическая ценность исследования заключается в разработке обобщенной архитектуры верификатора динамической памяти, а также в устранении многозначности описаний куч, благодаря ужесточению операций над кучами и использованию абстрактных предикатов, что позволяет использовать логический язык в качестве инструмента верификации динамической памяти, а также позволяет свести языки спецификации и верификации к одному языку.

Практическая ценность результатов исследования состоит в возможности существенной автоматизации верификации динамической памяти по известному коду программы с помощью диалекта языка Пролог с одновременной спецификацией на этом же диалекте. Помимо этого, разработанное решение обеспечивает возможность настройки используемых теорий о кучах, а также может быть применено для широкого диапазона императивных языков.

Замечания

По диссертационной работе можно отметить отдельные замечания:

1. Недостаточно раскрыты вопросы использования комплекса программных средств (Builder, Shrinker, ProLogika) для проектов, обладающей большой кодовой базой, в частности верификация проектов, опирающихся на сторонние библиотеки.
2. Описание языка OCL приводится дважды в тексте работы (с. 53 и с. 155).
3. При описании расширения «UML/OCL» указателями с ужесточенной моделью не приводится подхода для адаптации существующих решений к требуемому виду.
4. В подразделе “4.4 Представление знаний” не указываются критерии подбора тестовых данных для проведения эксперимента.
5. В разделе 6.8. описана практическая реализация разработанного научного метода. Однако примеры в тексте диссертации носят иллюстративный характер. Было бы интересно проиллюстрировать работу метода на исходных кодах реальных программ.

6. В тексте диссертации содержатся несколько несогласованных предложений (Цель анализа заключается в постановлении критерий доверительных компиляторов), присутствуют незначительные опечатки.

Отмеченные недостатки не снижают общей высокой оценки диссертационного исследования и не изменяют общую положительную оценку работы.

Заключение

Диссертация Хаберланда Рене является законченным научным исследованием. В диссертации решена актуальная научно-техническая задача разработки и реализации единого языка для спецификации и верификации динамической памяти. Достоверность результатов подтверждается корректным использованием математического аппарата, формальными доказательствами, а также апробацией результатов работы на всероссийских и международных конференциях.

Представленная диссертация "Логический язык программирования как инструмент спецификации и верификации динамической памяти" полностью соответствует требованиям пункта п. 9 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24.09.2013 года № 842 (в ред. Постановлений Правительства РФ от 21.04.2016 N 335, от 02.08.2016 N 748, от 29.05.2017 N 650, от 28.08.2017 N 1024), предъявляемым к кандидатским диссертациям, а ее автор, Хаберланд Рене, заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Официальный оппонент,
к.т.н., доцент
доцент
федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»
(Университет ИТМО)
Российская Федерация, 197101, Санкт-Петербург, Кронверкский пр., д. 49
тел.+7 812 232-97-04, mouromtsev@itmo.ru, https://itmo.ru/

Муромцев Дмитрий Ильич

20 марта 2020 г.