О Т З Ы В

официального оппонента, старшего научного сотрудника
Федерального государственного учреждения
«Федеральный исследовательский центр Институт прикладной
математики им. М.В. Келдыша Российской академии наук»,
к.ф.-м.н. Климова Юрия Андреевича
на диссертацию
Мандрыкина Михаила Усамовича
«Моделирования памяти Си-программ для инструментов
статической верификации на основе SMT-решателей»,
представленную на соискание ученой степени кандидата физико-
математических наук по специальности 05.13.11 — математическое и
программное обеспечение вычислительных машин, комплексов и
компьютерных сетей.

Актуальность темы

Обеспечение надежного функционирования современного программного обеспечения, очевидно, является актуальной и важной задачей. Особенно с учетом распространения всевозможных небольших устройств, например, сетевых роутеров, систем управления и т.п., с одной стороны, от надежного функционирования которых зависит благополучие людей, и, с другой стороны, которые могут подвергаться хакерским атакам и впоследствии использоваться для проведения таких атак. Поэтому обеспечение надежности функционирования операционных систем на устройствах является актуальной задачей.

На многих современных вычислительных устройствах: от небольших устройств, например, сетевых роутеров, до высокопроизводительных серверов, используется операционная система Linux, поэтому необходимо обеспечение надежного функционирования ядра ОС Linux. На каждом из таких устройств присутствует разнообразное аппаратное обеспечение, что приводит к

необходимости создания множества модулей ядра ОС Linux. И необходимо обеспечить их корректное и надежное функционирования.

Для верификации программ разработано множество методов. При этом среди них можно выделить класс методов статической верификации, которые могут доказательно гарантировать отсутствия некоторых классов ошибок. Существуют инструменты статической верификации, отдельные компоненты которых можно модифицировать для усиления работы всего инструмента. Данная работа направлена на разработку и реализацию методов моделирования памяти.

При создании модулей для ядра ОС Linux в основном используется язык Си, обладающий рядом особенностей, которые позволяют достигать высокой эффективности написанного на нем кода. Однако, с другой стороны, именно эти особенности создают проблемы при статической верификации. А именно: адресная арифметика, возможность приведения адреса к числу и обратно, возможность обращения по одному и тому же адресу за объектами разного типа, возможность получения адреса объемлющей структуры, возможность перекрытия массивов. Эти особенности требуют поддержки в инструментах статической верификации, которая не реализована в необходимой мере в существующих инструментах.

В результате автором диссертации были поставлены следующие актуальные задачи:

- Провести анализ существующих методов моделирования памяти Си-программ в инструментах автоматической статической и дедуктивной верификации.
- Выявить требования к моделям памяти, наиболее подходящим для применения в инструментах автоматической статической и дедуктивной верификации, используемых на практике для модулей ядра ОС Linux.
- Разработать модели памяти для практически используемых инструментов автоматической статической и дедуктивной верификации, отвечающих выявленным требованиям.

- Провести теоретическое обоснование корректности и полноты разработанной модели памяти для инструмента дедуктивной верификации.
- Реализовать предложенные модели памяти в используемых на практике инструментах верификации.
- Провести практическое сравнение эффективности разработанных моделей памяти с ранее реализованными моделями, в том числе для выявления направлений дальнейшего развития.

Степень обоснованности научных положений, выводов и рекомендаций

Диссертация Мандрыкина М.У. состоит из введения, четырех глав, заключения, списка литературы, перечня свидетельств о государственной регистрации программ для ЭВМ и приложения.

Во **введении** обосновывается актуальность темы, определяются цели и задачи работы.

В **первой главе** рассматривается актуальной задачи статической верификации Си-программ. Приведен обзор существующих методов и инструментов статический верификации. Описаны особенности языка Си, возникающие при создание моделей памяти Си-программ. Основной частью главы является обзор существующих методов моделирования памяти Си-программ, их анализ и сравнение. Делается вывод, что существующие методы не поддерживают все описанные ранее особенности языка Си.

Во **второй главе** рассмотрены два проекта статической верификации Си-программ с целью практического использования разработанных автором моделей памяти Си-программ в данных проектах.

В **третьей главе** формально описана разработанная автором модель памяти Си-программ для инструмента автоматической статической верификации, использующего предикатные абстракции. В предложенной модели используется комбинация теории неинтерпретируемых функций с теорией линейной целочисленной или вещественной арифметики. В

завершении приведено сравнение разработанной модели с существующими моделями памяти.

В **четвертой главе** представлена разработанная автором модель памяти с поддержкой вложенных структур и массивов для инструмента дедуктивной верификации Си-программ. Описывается формальный язык представления программ и задается его модельная семантика. Доказываются теоремы о корректности и полноте модельной семантики.

Таким образом, диссертация содержит обоснование актуальности темы, формулировку задачи и предлагает решение поставленной задачи. Доказываются теоремы о корректности и полноте корректности предложенных методов. Показано, что предлагаемые методы применимы на практике в современных инструментах верификации программ.

Оценка научной новизны и достоверности

В качестве основных научных результатов, полученных автором работы, можно указать следующие:

- Новая модель памяти на основе теории неинтерпретируемых функций для автоматической статической верификации Си-программ.
- Новая полная модель памяти с поддержкой вложенных структур и массивов, а также объединений и переинтерпретации типов указателей с автоматизированным разделением на непересекающиеся области для дедуктивной верификации Си-программ;
- Формализация низкоуровневой семантики практически значимого подмножества языка Си совместно с формальными доказательствами корректности и полноты модели памяти с поддержкой вложенных структур и массивов для дедуктивной верификации Си-программ.
- Доказательства полноты метода автоматического разделения на непересекающиеся регионы.

Достоверность результатов работы подтверждается теоретическими доказательствами корректности и полноты моделей, а также успешным применением разработанных методов в реальных инструментах верификации

Си-программ: в инструменте автоматической статической верификации CPAchecker и в инструменте дедуктивной верификации Jessie.

Основные результаты диссертации опубликованы в 10-ти печатных работах и доложены в ряде научных конференций и семинаров (в том числе и международных).

Замечания по диссертационной работе

- В работе отсутствуют примеры проверифицированных программ (как с положительным, так и отрицательном результатом). Было бы полезно привести такие примеры в приложении, что наглядно бы показало какого рода ошибки могут отлавливать инструменты статической верификации с разработанными автором моделями памяти.
- В разделе 3.4 для таблицы 3.3 (страница 110) и таблицы 3.5 (странице 112) не приведен анализ причин превышения лимитов времени работы инструмента верификации. Известны ли некоторые возможные направления улучшения модели памяти, позволяющие увеличить число верификационных заданий, которые удается проверить за выделяемый временной интервал?
- В работе эффективность различных моделей памяти сравнивается на специальных тестовых наборах. Было бы полезно привести результаты применения разработанных методов к полному набору модулей для какого-либо устройства, например, для сетевого роутера, и проверифицировать все модули для данного устройства.

Однако, указанные замечания не ставят под сомнение ценность проделанной диссертантом работы, а являются, скорее, пожеланиями по дальнейшему обобщению и углубления полученных результатов.

В тексте диссертации имеются небольшие стилистические погрешности. Например:

- В разделе 1.7 в таблице 1.2 (страница 77) у двух моделей памяти не указано, что они разработаны автором, однако это восстанавливается из текста диссертации.

- Четвертая глава перегружена формальными рассуждениями и формулами, отсутствует неформальное описание основных идей, что затрудняет ее чтение.

В целом отмеченные недостатки не затрагивают сущность исследований, не снижают их качество и не влияют на главные теоретические и практические результаты диссертации.

Заключение

Диссертация Мандрыкина М.У. является законченной научно-квалификационной работой, выполненной автором самостоятельно на высоком научном уровне. В работе представлены решения ряда задач, возникающих при статической верификации сложных программных комплексов. Полученные автором результаты достоверны, выводы и заключения обоснованы.

Автореферат соответствует основному содержанию диссертации.

Диссертационная работа отвечает всем требованиям Положения ВАК о присуждении ученых степеней, а ее автор Мандрыкин Михаил Усамович безусловно заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.11 «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Официальный оппонент,
старший научный сотрудник ИПМ им. М.В. Келдыша РАН, к.ф.-м.н.

24 ноября 2016

Ю. А. Климов

Подпись старшего научного сотрудника Климова Юрия Андреевича заверяю.
Ученый секретарь ИПМ им. М.В. Келдыша РАН

А.И. Маслов