«УТВЕРЖДАЮ»
Директор Федерального государственного учреждения
«Федеральный исследовательский центр
Институт прикладной математики им. М.В. Келдыша
Российской академии наук»
·корр. РАН, д. ф.-м. н., проф.
А. И. Аптекарев

_____

«___» апреля 2019 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

на диссертационную работу Захарова Ильи Сергеевича
«**Методы декомпозиции систем и моделирования окружения программных модулей для верификации Си-программ**»,
представленную на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 — математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Практическая значимость и актуальность работы

Язык программирования Си широко используется как инструмент программирования операционных систем, систем управления базами данных, веб-серверов, разнообразного программного обеспечения встраиваемых систем, применяемого в индустрии. В то же время из-за сложной низкоуровневой семантики языка программирования Си верификация крупных программных систем, размер которых может достигать миллионов строк кода, представляется трудной и является актуальной уже несколько десятилетий. Разработано множество методов и систем, автоматизирующих верификацию Си-программ ограниченного объема. Однако, по-прежнему стоит задача масштабирования этих методов на большие программы.

Основная проблема, решаемая в диссертационной работе Захарова И. С., — верификация крупных программных систем на языке программирования Си, которые раньше не поддавались автоматизированной верификации, используя существующие базовые инструменты верификации программ путем разбиения большой верифицируемой системы на модули и верификации их по частям. Поскольку вариантов выделения таких модулей много, потребовалось автоматизировать декомпозицию программных систем на отдельные модули и построения моделей их окружения, после чего для них выполняется синтез и решение

верификационных задач. Более того, этот процесс удалось распараллелить, что позволяет использовать для верификации распределенные вычислительные системы. В совокупности предложенные методы нацелены на значительное снижение трудоемкости и времени верификации, что позволяет верифицировать и находить ошибки в больших подсистемах операционной системы Linux, которые раньше не поддавались верификации.

Общая характеристика работы

Диссертационная работа состоит из введения, пяти глав, заключения и библиографии. Общий объем диссертации составляет 157 страниц. Библиография содержит 143 наименования.

В первой главе дается обзор существующих подходов к верификации программ на языке программирования Си и инструментов верификации моделей программ, выявляются ограничения этих инструментов, существенные для верификации больших программных систем, а также формулируются требования к практическим системам верификации, выполняющих проверку разнообразных требований к программным системам.

Вторая глава содержит основные теоретические результаты, а именно описание трех основных методов, предложенных в диссертации: метода автоматизированной декомпозиции Си-программ на модули, метода спецификации моделей окружения на основе композиции систем переходов и метода автоматизированного синтеза моделей окружения для модулей программ на языке Си. Описан процесс автоматизированного синтеза верификационных задач согласно предложенным методам.

Третья глава описывает архитектуру системы верификации, реализующих разработанные методы с использованием многоядерных и распределенных вычислительных систем и преодолевающих ряд серьезных ограничений существующих аналогов.

Четвертая глава посвящена реализации предложенных в диссертации методов в системе верификации Klever, которая позволяет проверять требования к модулям крупных программных систем на языке программирования Си, к которым существующие системы верификации не были применимы.

В пятой главе представлены результаты практического применения системы верификации Klever для верификации драйверов и подсистем ядра операционной системы Linux и апплетов BusyBox, а также анализ полученных результатов и выводы о применимости предложенных методов для верификации различных программ на языке программирования Си.

В заключении сформулированы основные результаты диссертационной работы.

Основные научные результаты и их значимость для науки и практики

Разработанные в диссертационной работе Захарова И. С. метод автоматизированной декомпозиции программ на языке программирования Си на модули, метод спецификации моделей окружения модулей при помощи композиции систем переходов и метод автоматизированного синтеза моделей окружения обладают как теоретической, так и практической значимостью.

Значимость для науки этих результатов заключается в том, что предложенные методы обладают новизной и дополняют существующие методы верификации так, что позволяют масштабировать задачу верификации на большие программные системы, с которыми не справляются имеющиеся ранее системы.

Практическая значимость разработанных Захаровым И. С. методов и реализованных им в системе верификации Klever продемонстрирована в диссертационной работе на верификации драйверов и других компонентов операционной системы Linux, причем обнаружено около сотни ошибок в промышленном программном коде при снижении трудозатрат и времени, необходимых для верификации и повышении уровня точности по сравнению с ближайшими аналогами.

Достоверность основных положений и результатов работы

Достоверность положений диссертационной работы подтверждается качеством теоретического исследования, включающего доказательство ряда лемм и теоремы об изоморфизме множеств путей программы на языке ELZ и ее трансляции в язык LZ, где языки LZ и ELZ были разработаны автором для построения моделей Си-программ, и экспериментальной проверкой предложенных методов, реализованных в системе верификации Klever.

Результаты диссертации апробированы на 14 научных конференциях и семинарах, а также опубликованы в 11 научных статьях, из которых 9 работ опубликованы в изданиях, входящих в перечень рецензируемых научных изданий ВАК при Минобрнауки РФ.

Замечания

Работа Захарова И. С. является развитием систем верификации программ, которые ранее разрабатывались в Институте системного программирования РАН, и решает проблемы масштабирования в случае верификации программных систем значительного объема. Диссертационная работа содержит детальный обзор существенных для данной работы характеристик этих систем.

Однако, при изложении своих результатов автор недостаточно ярко выделяет новизну своей работы по сравнению с работами предшественников. В результате этого читатель может

недооценить степень оригинальности предлагаемых методов автоматизированного выделения и композиции модулей, построения моделей окружения модулей в реализованной соискателем системе верификации Klever и проведения массовой верификации на многоядерных и распределенных вычислительных системах.

При описании метода спецификации моделей окружения для модулей Си-программ автор указал на возможность разной реализации средств задания моделей в рамках предлагаемого метода, но в главе, посвященной системе верификации Klever, как именно реализованы эти средства подробно не рассматривается.

Заключение

Отмеченные недостатки никак не влияют на общую положительную оценку диссертационной работы. Диссертационная работа Захарова И. С. на тему «Методы декомпозиции систем и моделирования окружения программных модулей для верификации Си-программ», является законченной научно-квалификационной работой, содержит новые научные и практические результаты, связанные с решением актуальной задачи повышения надежности разработки программ на языке Си, имеющей большое теоретическое и практическое значение для развития методов верификации программ и их приложений. Название диссертации соответствует основному содержанию диссертации. Автореферат достаточно полно отражает содержание работы.

Диссертационная работа может быть квалифицирована как законченное научное исследование по актуальной тематике и соответствует требованиям, предъявляемым ВАК РФ к работам на соискание степени кандидата физико-математических наук, а ее автор, Захаров Илья Сергеевич, заслуживает присуждения ему ученой степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Отзыв на диссертацию подготовлен на основании заключения структурного подразделения «Отдел программного обеспечения высокопроизводительных вычислительных систем и сетей» Федерального государственного учреждения «Федеральный исследовательский центр Институт прикладной математики им. М.В. Келдыша Российской академии наук» по результатам проведенного обсуждения диссертации на его заседании 27 марта 2019.

Старший научный сотрудник
ФГУ ФИЦ ИПМ им. М.В. Келдыша РАН
кандидат физико-математических наук Ю. А. Климов