ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

на выпускную квалификационную работу студента 4 курса
кафедры системного программирования СПбГУ
Батоева Константина Алановича, обучающегося по направлению 010500
(02.03.03)
(математическое обеспечение и администрирование информационных
систем)

Тема выпускной квалификационной работы:
Композициональное символьное исполнение CIL-кода

Символьное исполнение — популярная техника анализа программ, используемая для генерации тестового покрытия и формальной верификации. Проект V# пытается решить одну из фундаментальных проблем символьного исполнения -- комбинаторный взрыв путей исполнения программы -- путем абстракции от циклических и рекурсивных участков программы и автоматическим выводом индуктивных инвариантов для таких участков. Одной из нерешенных задач оставалась проблема символьного исполнения байткода .NET в условиях наличия так называемых *рекурсивных состояний*, позволяющих отказаться от общепринятой в классическом символьном исполнении раскрутки отношения перехода программы. Главной теоретической трудностью задачи было отсутствие подходов к *композициональному* анализу *произвольных* графов потока управления.

Студенту Батоеву К.А. была поставлена задача реализации интерпретатора промежуточного языка CIL платформы .NET для осуществления композиционального символьного исполнения без раскрутки отношения перехода программы в контексте проекта V#.

В ходе работы студентом Батоевым К.А. были изучены работы, описывающие различные алгоритмы символьного исполнения, формальная документация языка CIL. В рамках данной работы был предложен и теоретически обоснован алгоритм композиционального символьного исполнения без раскрутки циклов. Теоретическая часть работы выполнена с хорошей степенью формальности и аккуратности, все утверждения были оформлены в виде теорем и доказаны в отчете.

Предложенная схема была воплощена в проекте V#. Был написан парсер и большая часть интерпретатора CIL-кода, поддержано исполнение большинства инструкций языка CIL. К минусам стоит отнести то, что работа по реализации интерпретатора оказалась незаконченной: не была реализована схема обработки исключений и соответствующие ей инструкции. Это связано

не с теоретическими трудностями, а с недостатком времени: суммарное количество написанного кода составило порядка 4 тысяч строк кода, что является весьма солидным объемом для языка F#. Весь написанный код был протестирован на наборе программ общим объемом порядка десяти тысяч инструкций.

В процессе работы студент Батоев К.А. практически ежедневно взаимодействовал с научным руководителем и другими членами исследовательской группы проекта V#, делал доклады на внутренних семинарах группы, вёл самостоятельную исследовательскую работу. Все результаты были получены в срок.

Проверка ВКР на предмет наличия/отсутствия неправомерных заимствований показала, что работа неправомерных заимствований не содержит.

Константин Аланович проявил себя хорошим программистом и исследователем, готовым к работе как в индустрии, так и в научно-исследовательской области. Без сомнений, работа заслуживает оценки **«отлично»**.

Мордвинов Дмитрий Александрович,
Старший преподаватель кафедры системного программирования

Дата: 05 июня 2019 г.

Подпись: