**Отзыв научного руководителя**

на выпускную квалификационную работу студента СПбГУ Григорьева Савелия Алексеевича, обучающегося по направлению 01.03.02 (Прикладная математика и информатика)

Тема выпускной квалификационной работы:

“Применение двунаправленного исполнения для вывода индуктивных инвариантов в символьной виртуальной машине KLEE”

Вместе с бурным развитием SAT- и SMT-решателей существенно расширились возможности анализаторов исходного кода программ. Такие техники, как символьное исполнение и ограничиваемая проверка модели, уже сегодня применяются в компаниях с повышенными требованиями к надёжности кода. Одна из ключевых проблем, затрудняющих масштабирование этих подходов --- неограниченный рост пространства поиска в циклическом и рекурсивном коде. Таким образом, долговременным и всегда релевантным направлением исследований в области формальных методов является поиск методов, позволяющих отсекать потенциально бесконечные подпространства поиска.

Одной из ключевых идей в этом направлении является вывод индуктивных инвариантов --- логических утверждений, обобщающих поведение циклического и рекурсивного кода, и позволяющих конечным образом выразить важные свойства бесконечного пространства ветвлений. Область автоматического вывода индуктивных инвариантов сегодня достаточно живая, по ней проводится как минимум три международных академических соревнования, алгоритмы постоянно совершенствуются.

Удивительно, но в мире до сих пор не существует доведённой до конца реализации, конструирующей индуктивные инварианты в процессе символьного исполнения программ (хотя попытки были) --- как правило, работоспособные реализации работают над другими подходами, менее масштабируемыми и успешными на практике. Савелию была поставлена задача попытаться закрыть этот пробел.

Автоматический вывод индуктивных инвариантов в теориях --- крайне трудная проблема как с точки зрения теории, так и на практике. Эта проблема алгоритмически неразрешима даже для разрешимых теорий. На практике использование даже современных мощных алгоритмов конструирования инвариантов, как правило, должно сопровождаться разработкой различных эвристик для обобщения лемм, комбинирования теорий, поддержке сложных программных конструкций и т.д. Резюмируя всё это, Савелий столкнулся с довольно трудным вызовом.

Изначальный план предполагал адаптацию алгоритма IC3/PDR для двунаправленного символьного исполнения с обобщением на основе невыполнимых ядер для битовых векторов. Однако работа над дипломом шла не совсем гладко. В частности, в промежутке с ноября по февраль контактов со студентом не наблюдалось. В феврале работа возобновилась, но изначальный план пришлось существенно изменить.

Если выразить кратко суть итоговых результатов работы, то был получен прототип на основе символьной виртуальной машины KLEE, порождающий леммы в теориях, однако не были проработаны механизм обобщения и распространения этих лемм. Это означает, что реализация способна корректно порождать части

инвариантов, но сходится к неподвижной точке крайне эвристически, лишь в очень "удачных" случаях. Это ясно демонстрируется результатами экспериментов. Другими словами, результаты работы Савелия стоит воспринимать как вполне надёжный фундамент, над которым нужно надстроить опущенную функциональность, чтобы сильно расширить сходимость алгоритма. Есть надежда, что дальнейшая работа группы закроет эту брешь.

Моё общее впечатление такое, что Савелий -- талантливый разработчик, который неудачно спланировал работу и попал в цейтнот. Тем не менее, он показал, что способен выдавать сложный результат в достаточно сжатые сроки и разбираться с достаточно непростыми, передовыми алгоритмами области. Его результаты будут полезны в будущем, несмотря на отклонения от изначального плана. Принимая все факторы во внимание, рекомендую комиссии оценку **"хорошо"**.

Мордвинов Дмитрий Александрович,
к.ф.-м.н., доцент кафедры системного программирования СПбГУ
Дата: 01.06.2023 Подпись: