РЕЦЕНЗИЯ
на выпускную квалификационную работу обучающейся СПбГУ
Черниговской Лидии Александровны
по теме Реализация синхронизирующего решателя дизъюнктов Хорна

Формальная верификация рекурсивных программ – необходимый, но сложный и затратный процесс. Для того, чтобы доказать, что в программе нет ошибок, которые противоречили бы данной спецификации, нужно рассмотреть все возможные варианты входных данных, а в случае наличия в программе рекурсивных функций, количество вызовов которых зависит от входных данных, необходимо рассмотреть все возможные цепочки вызовов. Стандартный подход к этой задаче – это поиск индуктивных инвариантов – таких свойств программ, что 1) каждый инвариант выполняется для состояния программы перед первым вызовом рекурсивной функции, и 2) из выполнимости инварианта для состояния программы перед вызовом N рекурсивной функции следует выполнимость инварианта перед вызовом N+1 этой же рекурсивной функции. Задачей поиска инвариантов занимаются специализированные решатели дизъюнктов Хорна, однако научному сообществу известен факт неразрешимости этой задачи. На практике это препятствие можно пытаться обойти, если предварительно произвести упрощение или трансформацию данной программы.

Работа Черниговской Лидии Александровны посвящена задаче поиска инвариантов для случая, когда в программе последовательно вызываются две или более рекурсивные функции, а формальная спецификация затрагивает входные данные и результаты обеих функций. Такой сценарий часто встречается, например, в задачах реляционной верификации: когда необходимо доказать эквивалентность двух реализаций одного алгоритма или доказать монотонность данной функции. В последнее время в научном сообществе активно развиваются автоматические подходы для поиска утечек информации, которые сводятся к реляционной верификации, и соответственно, могут быть адресованы Хорн-решателям. В этой связи, актуальность ВКР не вызывает сомнений.

ВКР имеет следующую структуру. После плавного введения в курс работы, дается строгое математическое определение систем дизъюнктов Хорна, их выполнимости и инвариантов. Далее описываются современные инструменты решения выполнимости дизъюнктов Хорна. Отдельная глава посвящена алгоритму синхронизации дизъюнктов Хорна, опубликованному в 2017 году, целью которого является трансформация системы дизъюнктов Хорна путем произведения отдельно выбранных дизъюнктов. В основной части ВКР приводятся два варианта улучшения алгоритма, и в последней части работы приводятся их реализация на основе решателя μZ, ссылки на исходный код и описание экспериментов.

Основным научным результатом ВКР является улучшение алгоритма, который в оригинальной трактовке 2017 года имел определенные недоработки. Интуитивно, для двух рекурсивных вызовов, алгоритм определяет, могут ли они быть объединены в один рекурсивный мета-вызов; и если так, то для его верификации достаточно найти не два индивидуальных инварианта, а один (что на практике существенно проще). Однако, алгоритм 2017 года в ряде случаев был не способен использовать часть спецификации для искусственно созданного мета-вызова. Текущая работа предлагает делать тщательный анализ данной спецификации во время трансформации и выводить из нее так называемые синхронизационные леммы – индуктивные свойства искусственно

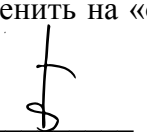
созданного мета-вызова. Часто они оказываются решающими при поиске окончательного индуктивного инварианта.

ВКР предлагает два алгоритма поиска синхронизационных лемм. Первый основан на итеративном ослаблении спецификации с помощью автоматического SMT-решателя (от англ. Satisfiability Modulo Theories – задача выполнимости формул в теориях). Поиск начинается с гипотезы что вся спецификация полностью является синхронизационной леммой. Эта гипотеза кодируется в формулу первого порядка и посылается в SMT-решатель. Неразрешимость формулы говорит о выполнимости гипотезы, и алгоритм завершается. В противном случае, SMT-решатель возвращает модель, по которой алгоритм делает вывод о том, где и как ослабить гипотезу, и переходит на следующую итерацию. Достоинство алгоритма в том, что количество итераций всегда конечно.

Второй алгоритм поиска синхронизационных лемм создает новую систему дизъюнктов Хорна, решением которой является искомая синхронизационная лемма. В этом случае, вся вычислительная нагрузка приходится на Хорн-решатель, который не может гарантировать результат, но рассматривает существенно более широкий диапазон возможных решений чем первый алгоритм. На практике, для одних классов задач более предпочтительно использование первого алгоритма, для других классов задач – второго.

В целом, ВКР оформлена исключительно прилежно. Все главы содержат большое количество примеров. Единственный недостаток – краткость описания экспериментов. Было бы желательно увидеть больше статистических данных: на каких программах какой из алгоритмов работает лучше. Но не зависимо от этого, работу необходимо считать успешной. На ее основе рекомендуется подготовить статью для подачи на международную конференцию ранга ICLP, CP или LPAR.

В итоге, ВКР рекомендовано оценить на «отлично», и ее исполнителю рекомендовано присудить звание бакалавра.

«20» мая 2018 г.  *Федюкович Григорий Геннадьевич*

Подпись *ФИО*