

ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

на выпускную квалификационную работу студента 4 курса
кафедры системного программирования СПбГУ

Никольского Кирилла Андреевича, обучающегося по направлению 010500
(02.03.03)

(математическое обеспечение и администрирование информационных систем)

Тема выпускной квалификационной работы: Формальная верификация окружения
времени выполнения робототехнической системы.

На кафедре системного программирования СПбГУ в течение нескольких лет создается программное обеспечение для робототехнического контроллера ТРИК. Проект в течение трех лет эксплуатируется большим количеством пользователей, при этом время от времени появляются редко воспроизводимые проблемы. Их анализ показал, что все такие проблемы являются следствием сложного взаимодействия большого количества потоков исполнения, однако за довольно большой срок лишь малую часть таких ошибок удалось поправить штатными силами (вследствие редкого их появления). К счастью, в академической среде известны методы борьбы с такими проблемами. Речь идет о формальной верификации программ на моделях (model checking).

Верификация программ на моделях, по сути, представляет собой исчерпывающее тестирование поведения программы, точнее, ее модели. В такой схеме самыми трудными задачами являются построение адекватной и корректной модели системы и формального описания требований к ней, остальное происходит автоматически. Метод проверки модели сегодня актуален как никогда и даже входит промышленные стандарты создания систем, для которых требования безотказности являются критическими (например, в авиастроении).

Перед студентом Никольским К.А. была поставлена задача формальной верификации скриптового окружения времени выполнения, работающего на роботах ТРИК. Для этого необходимо было выбрать наиболее подходящий верификатор, составить корректную и адекватную модель исходной системы, сформулировать требования в терминах темпоральной логики и исследовать все трассы контрпримеров, выданных верификатором.

В ходе работы студентом Никольским К.А. было изучено большое количество материалов (книг, научных статей и онлайн-курсов) на тему формальной верификации (в том числе на иностранном языке), был выполнен обзор существующих подходов и инструментов в области проверки моделей. В результате студентом была смоделирована довольно значительная часть скриптового окружения на контроллере ТРИК (исходный код которой занимает порядка 5 тысяч строк). Качество модели оказалось хорошим, верификатор смог провести исчерпывающий поиск по пространствам состояний (таким образом, студенту удалось избежать т.н. проблемы комбинаторного взрыва). Были сформулированы требования корректности в терминах темпоральной логики линейного времени. В результате было получено множество контрпримеров, часть которых оказалась воспроизводимой на реальной системе.

В процессе работы студент Никольский К.А. активно взаимодействовал с научным руководителем, часто предлагал собственные идеи и вёл самостоятельную работу, почти все результаты были получены в срок. Детальные описания трасс контрпримеров были сообщены штатным разработчикам проекта.

Тем не менее, формальное доказательство корректности системы завершить

не удалось по причине нескольких неразобранных контрпримеров (порядка десяти). Это объясняется тем, что процесс разбора трасс контрпримеров в многопоточной системе является довольно трудоемким, а их количество явилось весьма неожиданным. Таким образом, хоть работа и не завершена, вины студента здесь нет; наиболее сложные задачи (например, построение модели) были успешно решены, работа может быть закончена даже менее квалифицированными людьми.

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

В ходе работы студент получил много опыта и навыков, важных в контексте критических к безопасности систем, показал себя как прекрасный программист, способный самостоятельно разобраться в наукоемких инструментах и подходах и готовый к работе в отрасли. Несмотря на то, что не все ожидаемые результаты были получены, работа, несомненно, заслуживает оценки «отлично».

Терехов Андрей Николаевич,
доктор ф.-м. наук, профессор и зав. каф. системного программирования СПбГУ

Дата: 24 мая 2016г

Подпись: _____