РЕЦЕНЗИЯ

на выпускную квалификационную работу студента 4 курса
кафедры системного программирования СПбГУ
Костюкова Юрия Олеговича, обучающегося по направлению 231000 (09.03.04)
(программная инженерия)

Тема выпускной квалификационной работы:
Композициональная верификация программ с динамической памятью
на основе дизъюнктов Хорна

Целью данной выпускной квалификационной работы является разработка формального подхода для проведения композициональной верификации программ с динамической памятью в инфраструктуре .NET. Ожидаемая модель обладает свойством точности, что позволяет избежать потери информации об анализируемой функции при кодировании в формализм, что, однако, не защищает от ложных срабатываний при попытке разрешить полученные ограничения с помощью различного вида решателей формул высшего порядка.

Данная работа является частью многообещающего проекта V# по композициональной верификации программ на .NET. Данный проект в случае его успешного завершения должен упростить надежную и безопасную разработку программ на .NET.

В данной работе ставились задачи разработки формализма, доказательства его корректности, интеграции его в проект V# и апробации на входных программах.

В главе 2 вводятся основные понятия, которых оказывается всего два: композициональность и аппроксимация состояний программ. Изложение очень краткое, но при этом позволяет подготовленному читателю уловить суть. Вызывает некоторое сожаление, что данная глава будет трудна для читателя без необходимых знаний.

В третьей главе описывается состояние данной предметной области, а именно разновидности Хорн и SMT решателей и текущие работы по моделированию памяти. Данная глава написана очень хорошо и должна быть понятна как искушенному читателю, так и новичку.

Четвертая глава является сердцем данной работы. Она написана достаточно подробно, по мере чтения не было замечено никаких вольных рассуждений, т.е. Автор проявил себя формалистом в положительном понимании этого слова.

В пятой главе кратко изложена архитектура проекта V#.

По мере чтения возникли следующие вопросы и мысли

1. В четвертой главе автор заявляет о *частичной* механизации доказательств в системе Coq. На сколько она частичная, присутствуют ли какие-то существенные сложности для проведения полной механизации?

2. При тестировании устанавливался таймаут в 30 секунд и ни один тест не превысил его. Бэкенд для вывода refinement типов настолько хорош или Вы не включали такие тесты?

Работа производит впечатление, что автор разобрался с устройством современных языков с динамической памятью. Апробация подхода показывает хорошие результаты, настолько хорошие, что даже подозрительно. Однако, предложенный теоретический подход выглядит как шаг вперед в развитии теории верификации, и заслуживает оценки "отлично". Надеюсь, что смогу прочитать через два года продолжение этой работы, уже в виде магистерской диссертации.

Косарев Дмитрий Сергеевич,
программист ООО "Интеллиджей Лабс"

Дата: 01 июня 2019 г

Подпись: _____