ОТЗЫВ

на автореферат диссертации Кондратьева Дмитрия Александровича «Методы комплексного подхода к автоматизации дедуктивной верификации программ с финитными итерациями», представленной на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Задача формальной верификации программ является актуальной не только в теоретической, но и в прикладной плоскости. Сегодня формальная верификация активно применяется при разработке операционных систем (mCertikOS, Hyper-V), компиляторов (CompCert, CakeML), систем управления транспортом (Roissy Shuttle) и других видов систем, к корректности и отказоустойчивости которых предъявляются повышенные требования. Развитие SMT-решателей сделало возможным бурное развитие и прикладное применение подходов к формальной верификации, основанных на дедукции. Большим плюсом таких подходов является возможность задания спецификаций непосредственно в коде программы, что позволяет проводить спецификацию и верификацию кода, уже находящегося в эксплуатации и не подлежащего изменению (в отличие от верификации с помощью интерактивных доказателей, таких как Coq и Isabelle/HOL, когда верификация, в сущности, является сертифицированной трансформацией исполняемой спецификации в целевой язык программирования). Это позволяет утверждать, что дедуктивная верификация более применима к т.н. «гибкой» разработке, являющейся доминирующим в настоящее время подходом к разработке программного обеспечения.

Особенностью дедуктивного подхода, однако, является невозможность прямого вмешательства разработчика в процесс верификации, поскольку текст программы не является доказательством собственной корректности – программа транслируется в промежуточное представление (обычно на языке Boogie), которое, в свою очередь, транслируется в модель для решателя (обычно z3). В результате для каждого элемента спецификации процесс верификации порождает двоичный результат – успех/неудача. В случае неудачи разработчик обречен на поиск источника проблемы методом «пристального взгляда» и подбор правильного решения проблемы методом проб и ошибок. Ситуация усугубляется тем, что источник проблемы не всегда является дефектом реализации. Исполняемый код зачастую является де-факто корректным (исходя из фактического замысла разработчика), а причина неудачи дедуктивной верификации при этом может заключаться в (1) недостаточной строгости инварианта цикла, (2) противоречивости требуемого постусловия, или (3) записи того и другого в форме, которую решатель не поддерживает.

Дмитрий Александрович Кондратьев в своей работе предлагает подходы к решению всех указанных проблем. Наиболее фундаментальным решением, на мой взгляд, является избрание подмножества целевого языка программирования в качестве

промежуточного языка верификации. Как указывает Автор, это, несомненно, упрощает аксиоматизацию операционной семантики языка. Но это также упрощает отладку неудачных попыток верификации, поскольку разработчику не требуется переключение между разными режимами восприятия кода. Автор использует метод семантической разметки для автоматической локализации ошибок в исходном коде на основании исправлений, внесенных в промежуточное представление. На мой взгляд, жизнеспособность этого подхода обеспечивается как раз использованием одного и того же языка программирования для исходных программ и для их промежуточного представления для верификации.

Еще одним крупным результатом работы Дмитрия Александровича я считаю полное исключение необходимости записи инвариантов циклов для целого класса циклов – финитных итераций. Считаю важным расширить использованный подход для применения и к другим классам циклов, таких как обходы связных структур данных. Использование стандартных схем циклов позволяет избежать типовых ошибок ручной записи инвариантов циклов. Автор также предлагает подходы для обнаружения противоречивых постусловий, что позволяет избежать пустой траты времени разработчика на попытки корректно реализовать заведомо невыполнимые требования.

Со своей стороны хотел бы заметить, что предложенные методы следует попытаться перенести на объектно-ориентированную парадигму программирования, в которой центральную роль занимают инварианты классов, а также способность двух переменных указывать на один и тот же объект (что ведет к целому классу проблем).

Учитывая все вышеизложенное, считаю, что диссертация «Методы комплексного подхода к автоматизации дедуктивной верификации программ с финитными итерациями» является законченной научно-исследовательской работой, а ее автор, Дмитрий Александрович Кондратьев, заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Доцент магистерской программы
«Разработка безопасных систем и сетей»
АНО ВО «Университет Иннополис»,
кандидат наук

Наумчев Александр Владимирович

Сведения об организации:
Автономная некоммерческая организация высшего образования «Университет Иннополис»
420500, Российская Федерация,
Республика Татарстан, город Иннополис,
улица Университетская, д. 1
Телефон: +7 (843) 203-92-53
Веб-сайт: https://innopolis.university
E-mail: university@innopolis.ru

Подпись Наумчева А.В. заверяю.
Директор по развитию и кадровой политике
АНО ВО «Университет Иннополис»
Р.Ф. Валиев