ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

на диссертацию Дмитрия Александровича Кондратьева

«Методы комплексного подхода к автоматизации дедуктивной верификации программ с финитными итерациями», представленную на соискание ученой степени кандидата физико-математических наук по научной специальности 05.13.11 — Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Рост производительности компьютеров, происходивший в соответствии законом Мура, в равной степени отразился на сложности и объеме программного обеспечения. Отчасти сама ошеломляющая производительность, плюс снизившийся порог вхождения в профессию программиста, стала причиной, по которой многие разработчики уже не пытаются подходить ответственно к написанию кода, а полностью полагаются на оптимизации и проверки в средствах разработки ПО. Как следствие, обычное тестирование уже просто не способно выявить все потенциальные источники опасности в разросшихся программах. Зачастую пользователи становятся невольными тестировщиками «сырого» ПО, на отладку которого у разработчиков не хватило средств и времени. Но проникновение компьютерных технологий во все сферы жизни человека приводит к тому, что цена пропущенной при тестировании ошибки может стать непомерной.

С другой стороны, практически уже на ранних этапах информатики теоретиками была осознана важность формальных методов проверки корректности программ, позволяющих с математической точностью находить ошибки. Одним из таких методов стала дедуктивная верификация. Но парадокс ситуации в том, что за более чем полвека существования верификация практически так и не вышла за рамки коллективов теоретиков в институтах и университетах. У обычных программистов нет ни времени, ни желания осваивать еще и фундаментальные основы математики и логики, которые нужны для успешного применения верификации. Поэтому основной мотивацией Д.А. Кондратьева к написанию диссертации стало желание сделать верификацию более дружелюбной к программистам.

Важнейший вывод, который сделал Д.А. Кондратьев при планировании диссертации, состоит в том, что данную проблему необходимо решать в комплексе. Зачастую диссертации по теме верификации программ касаются только одного или нескольких этапов этого процесса. Не получая дальнейшего развития и интеграции с другими этапами, многие интересные предложения исследователей так и остаются сугубо теоретическими результатами. И наоборот, Д.А. Кондратьев разработал и воплотил в жизнь набор методик для полного цикла верификации — от автоматического порождения подходящего генератора

условий корректности до объяснения пользователю ложных/недоказанных условий на естественном языке.

Взяв за основу уже известные методы верификации финитных итераций, метагенерации условий корректности, семантической разметки условий, Д.А. Кондратьев творчески доработал и усилил их, получив ряд важных результатов. Особенно следует отметить, что метагенерация условий, предложенная еще в начале 1980-х годов, оказалась незаслуженно предана забвению. Д.А. Кондратьев своей работой вдохнул новую жизнь в этот метод и показал его полезность.

Все результаты, полученные Д.А. Кондратьевым в диссертации, так или иначе способствуют упрощению верификации программ и повышают степень автоматизируемости этого процесса:

1) Разработанные им варианты аксиоматических семантик для финитных итераций в языках C и Cloud Sisal позволяют избавиться от инвариантов циклов, которые всегда были одним из камней преткновения для обычных программистов. При этом класс программ, соответствующий финитным итерациям, не является искусственным и ограниченным. Циклическая обработка массивов, списков, деревьев — это одна из фундаментальных основ программирования.

2) Он показал, что предложенные семантики удовлетворяют ограничениям нормальной формы из метода метагенерации, а значит пользователь может автоматически порождать генератор условий корректности, который, как система вывода, полон и непротиворечив относительно исходной семантики. Важным элементом новизны в работе стало то, что генератор может порождаться вообще на лету.

3) Для ряда интересных случаев, когда автоматические системы доказательства теорем не справляются и требуют интерактивных сессий, им был предложен набор автоматизированных стратегий. Важнейшим результатом при этом стало формальное доказательство корректности некоторых из них.

4) Порождаемые автоматически объяснения для недоказанных или ложных условий корректности позволят программисту легче понять смысл контрпримера и потенциальное место ошибки в программе или в спецификации.

5) Наконец, успешные эксперименты по верификации программ на императивном языке C и на функциональном языке Cloud Sisal продемонстрировали, что предложенные методы не ограничены одной парадигмой и достаточно универсальны.

Все защищаемые результаты являются новыми, достоверными и теоретически обоснованными. Результаты диссертации были представлены в более чем достаточном списке из 38 публикаций, включая 14 статей в изданиях из списка ВАК и 11 в журналах из баз цитирования Web of Science и Scopus. Из публикаций, написанных в соавторстве с коллегами, в диссертации представлены только результаты, полученные автором лично. А квалификация автора как программиста подтверждается свидетельством о государственной регистрации программы для ЭВМ. Также Д.А. Кондратьев представлял свои достижения на многочисленных российских и международных семинарах и конференциях. Отметим, что работы автора оказались востребованными в ряде проектов РФФИ, РНФ и в проекте в интересах компании Huawei, что говорит о достойной оценке со стороны научного сообщества.

В целом, диссертация Д.А. Кондратьева является самостоятельной и законченной научно-исследовательской работой. Тематика и полученные результаты соответствуют паспорту специальности 05.13.11 — Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей. Автор обладает широким математическим кругозором, способен самостоятельно формулировать задачи и решать их. Считаю, что диссертационная работа соответствует требованиям ВАК, предъявляемым к кандидатским диссертациям, а ее автор — Кондратьев Дмитрий Александрович — заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.11.

Научный руководитель
кандидат физ.-мат. наук (специальность 05.13.11),
заместитель директора по научной работе
ФГБУН Института систем информатики
им. А.П. Ершова Сибирского отделения
Российской академии наук Алексей Владимирович ПРОМСКИЙ

promsky@iis.nsk.su, тел. (383) 330-70-68
630090, г. Новосибирск, пр-т ак. Лаврентьева, 6

27.06.2022

Личную подпись А.В. Промского
удостоверяю

мл. сотр. ИСИ СО РАН		Е.Н. Насибулов
(должность)	(подпись)	(ФИО)