ОТЗЫВ

научного руководителя на диссертацию Дмитрия Александровича Мордвинова **«Автоматический вывод реляционных инвариантов для нелинейных систем дизъюнктов Хорна с ограничениями»**, представленную на соискание учёной степени кандидата физико-математических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Автоматическая проверка надёжности программного обеспечения была и остаётся одной из центральных проблем информатики. К настоящему моменту имеется множество инструментов для автоматизации рассуждений о корректности программ, например, SMT-решатели. Такие инструменты позволяют эффективно проверять выполнимость заданного набора ограничений к ПО, описанных на некотором формальном языке. Однако использование таких инструментов для доказательства корректности программ сопряжено с фундаментальной проблемой (следствие теоремы Гёделя о неполноте арифметики): либо формальный язык невыразителен, т.е. не может позволить описать значимые инварианты программ, либо он неразрешим, т.е. невозможно выполнить формальные рассуждения (доказательства) для утверждений на этом языке.

В диссертации Дмитрия Александровича выдвигается тезис о том, что в ряде важных практических случаев указанную проблему можно решить, автоматически преобразовав программу таким образом, что порождаемые для неё ограничения будут эффективно проверяться SMT-решателями. При этом сценарии поведения программ можно описывать в виде множества логических импликаций, называемых системами дизъюнктов Хорна с ограничениями. В диссертации был предложен подход к синхронизации дизъюнктов Хорна,

который позволяет объединять дизъюнкты, упрощая запросы к SMT-решателю, но не изменяя при этом семантику ограничений. На основе этого подхода был разработан алгоритм преобразования системы дизъюнктов Хорна, что открывает возможность практического использования невыразительных, но разрешимых языков ограничений.

Помимо этого результата Дмитрий Александрович выполнил обобщение недавно появившегося в литературе подхода PDR на предложенный им подход к синхронизации дизъюнктов Хорна. Наконец, в работе выполнена интересная апробация полученных результатов, включающая интеграцию реализованных алгоритмов в известный SMT-решатель Z3 (Microsoft Research). Также выполнено сопоставление полученных результатов с другими решателями дизъюнктов Хорна, показавшее значительные преимущества предложенных решений. Важно подчеркнуть, что интеграция с Z3 является важным фактом международного признания результатов Дмитрия Александровича – данная интеграция выполнена по предложению ведущих мировых специалистов в данной области, которые являются авторами Z3.

Итак, диссертация Дмитрия Александровича выполнена на переднем крае науки и интегрирована в международный научный контекст. Это подтверждено, в частности, его публикацией на ведущих мировых научных форумах и конференциях по этой тематике: 21st International Conference on Logic for Programming, Artificial Intelligence and Reasoning (LPAR-2017), 33rd European Conference on Object-Oriented Programming (ECOOP-2019), 19th Conference on Formal Methods in Computer-Aided Design (FMCAD-2019). Вместе с тем автор представил результаты своего исследования также и в Российском научном сообществе – в ИСП им. В.П. Иванникова (Москва), в МГУ ВМК (Москва) и ВШЭ (Москва), а также в ИСИ СО РАН им. А.П.Ершова (Новосибирск).

Следует отметить, что Дмитрий Александрович является сформировавшимся исследователем и, в общем-то, уже не нуждается в научном руководстве. Напротив, он сам является руководителем успешного студенческого исследовательского коллектива. Отмечу такие его личные качества как увлечённость, жадность до знаний, общительность и обучаемость. Дмитрий Александрович имеет широкий кругозор в своей области, живо интересуется различными смежными областями. Он готов часами рассказывать про свою работу в любой аудитории, обсуждать различные варианты развития своих исследований. Он имеет амбициозные планы. Дмитрий Александрович умеет публично представлять результаты своих исследований и имеет навыки международных научных коммуникаций, а также является желанным гостем во многих университетах и на различных конференциях – как в России, так и за рубежом. Он также инициировал нескольких совместных исследовательских проектов с различными зарубежными университетами.

В процессе подготовки диссертации Дмитрий Алексеевич столкнулся с непростым вызовом – интегрировать западную (статейную) культуру представления результатов и традиционную российскую культуру в области математической логики, существенно ориентированную на написание монографий. С одной стороны, имеем различные подходы к максимально наглядному, доступному изложению сложных результатов (часто – в ущерб формальной строгости). С другой стороны, речь идёт о скрупулёзности доказательной базы, о выверенной терминологии и в целом о математической опрятности. На мой взгляд, Дмитрий Александрович успешно интегрировал в своей работе обе этих культуры, хотя, конечно же, работы в этом направлении в нашей научной школе будут продолжаться – до полного решения данной проблемы ещё далеко.

Итак, следует заключить, что представленную диссертацию можно считать законченной научно-исследовательской работой. Её тематика и

достигнутые научные результаты полностью соответствуют паспорту специальности 05.13.11 «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей». Следует также отметить, что работа соответствует требованиям Положения о порядке присуждения учёных степеней, обладает теоретической и практической ценностью. Следовательно, её автор, Дмитрий Александрович Мордвинов, заслуживает присуждения ему учёной степени кандидата физико-математических наук по специальности 05.13.11.

Доктор технических наук,
профессор кафедры системного
программирования Санкт-петербургского
государственного университета,
докторская диссертация защищена
по специальности 05.13.11,
согласен на обработку персональных данных Д.В.Кознов

16.09.2020

Личную подпись Д.В. Кознова
удостоверяю
зам. начальника
Управления кадров СПбГУ
Суфьянова О.С.
16.09.2020