ОТЗЫВ НА АВТОРЕФЕРАТ ДИССЕРТАЦИИ
на соискание ученой степени
кандидата физико-математических наук
МОРДВИНОВА Дмитрия Александровича
«Автоматический вывод реляционных инвариантов
для нелинейных систем дизъюнктов Хорна с ограничениями»

Подобно тому, как полвека назад разработка оптимизирующих компиляторов для языков программирования высокого уровня считалась одной из центральных задач системного программирования, столь же значимой в настоящее время является задача разработки автоматических систем верификации программ. Но, в отличие от задач синтаксического анализа и трансляции, которые имеют эффективные методы решения для наиболее востребованных классов формальных языков, задачи проверки семантических свойств программ, как следует из т.н. теоремы Райса, алгоритмически неразрешимы. Выходом из этого положения становится разработка большого арсенала специальных методов, обеспечивающих проверку правильности вычислений для тех или иных классов программ и требований корректности. Эти методы, даже в совокупности, не дают универсального решения задачи верификации программ, но можно рассчитывать, что во многих практически важных «стереотипных» случаях с их помощью удастся полностью автоматизировать проверку и доказательство корректности программ. Успешное выполнение этой масштабной научно-исследовательской программы, инициированной Ч.Э. Хоаром в начале столетия, зависит от успешного решения нескольких ключевых задач, одна из которых – это создание эффективных методов генерации нетривиальных инвариантов программ. Таким образом, тема диссертации является чрезвычайно актуальной и вполне соответствует современным тенденциям развития математических методов системного программирования.

Одна из принципиальных трудностей задачи синтеза инвариантов программ состоит в том, что даже для сравнительно простых программ отношения между данными, вычисляемые в некоторых точках программы, могут быть невыразимы логическими формулами в сигнатуре программы, а расширение сигнатуры приводит к неразрешимой логико-математической теории. Этот эффект был впервые обнаружен почти полвека назад независимо И.А. Ломазовой и Э. М. Кларком. Поэтому методы автоматической генерации инвариантов для верификации программ должны суметь найти проход между Сциллой тривиальных инвариантов, бесполезных для доказательства свойств корректности вычислений, и Харибдой сложных невыразимых отношений, которые непригодны для используемых систем автоматической проверки выполнимости логических формул. Таким образом, задача, решению которой посвящена диссертация Д.А. Мордвинова, является трудной математической задачей, возникшей на стыке нескольких дисциплин – математической логики, алгебры и программирования.

Автореферат показывает, что диссертационная работа Д.А. Мордвинова представляет собой глубокое и хорошо сбалансированное научное исследование. В самом начале работы автор позаботился о создании надежного теоретического основания для своего первоначального замысла. Основная идея состоит в том, чтобы подвергнуть системы хорновских дизъюнктов с ограничениями, описывающих вычисления программ,

равносильным преобразованиям, вводя новые комбинированные переменные-предикаты так, чтобы можно было получить явное формульное решение для этих новых производных предикатов. Теоремы 1-3 второй главы диссертации показывают, что предложенный метод преобразования систем дизъюнктов (автор называет его синхронизацией) может быть осуществлен корректно. Предложенный метод преобразований весьма остроумен. Справедливость утверждений теорем не вызывает сомнений прежде всего потому, что автор предварительно детально разработал хорошо понятный понятийный аппарат для описания метода синхронизаций систем хорновских дизъюнктов.

Как видно из автореферата, в третьей главе диссертации автор развивает идею метода синхронизации и, предлагает новое понятие сертификата выполнимости систем хорновских дизъюнктов с ограничениями. Концепция сертификата выполнимости позволяет доказывать выполнимость некоторых систем хорновских дизъюнктов в заданных теориях даже в тех случаях, когда предикаты, неявно описываемые этими системами, невыразимы в рассматриваемых теориях. Теоремы 4 и 5 подтверждают корректность предложенного подхода. Введенное понятие сертификата выполнимости для систем хорновских дизъюнктов является новым и очень полезным для последующего использования в решении задач проверки выполнимости этих систем.

Результаты, представленные в первых главах диссертации, служат теоретической основой для новых алгоритмов проверки выполнимости систем хорновских дизъюнктов в специальных логико-математических теориях. Эти алгоритмы представлены автором в четвертой главе диссертации. Поскольку ограниченный объем автореферата не позволяет включить в него подробное описание этих алгоритмов, судить о них можно только по описаниям их предназначения и сценариев работы. Это описания вполне убедительны, содержательны и не вызывают сомнений в достоверности утверждений теорем 6-8 о корректности предложенных алгоритмов проверки выполнимости систем дизъюнктов.

В автореферат включены также результаты экспериментального исследования реализаций указанных алгоритмов, которому посвящена пятая глава диссертации. Эти результаты показывают, что реализованные автором алгоритмы проверки выполнимости соответствуют своему назначению и справляются с теми задачами, которые оказались не по силам другим разрешающим системам.

В заключительном разделе подведен итог проведенным исследованиям, коротко сформулированы основные результаты и намечены направления дальнейшей работы в развитии метода синхронизации.

Автореферат диссертации Д.А. Мордвинова демонстрирует многочисленные достоинства работы. Очень хорошо хорошо организован блок определений основных понятий, связанных с задачей проверки выполнимости систем хорновских дизъюнктов и представленный в первой главе диссертации; этих определений вполне достаточно, чтобы понимать и оценивать все утверждения и алгоритмические конструкции, представленные в автореферате. Строго и емко сформулированы новые концепции (синхронизации, сертификата выполнимости), содержательно и доступно для широкого понимания описаны новые методы проверки выполнимости систем дизъюнктов в заданных теориях. Представленные в автореферате результаты свидетельствуют о глубоком и систематическом исследовании основной задачи диссертации, и о большой значимости полученных им результатов. Эти результаты представляют собой новое и значимое научное

достижение в построении разрешающих процедур для проверки выполнимости систем логических формул, возникающих при решении задач верификации программ. Математические методы, описанные в диссертации, представляют несомненный интерес для специалистов в области математической логики, теории вычислений и программирования.

Автореферат не содержит существенных недостатков. Небольшое число описок и стилистических неточностей легко устраняются; они не заслуживают обсуждения, и о них автору было сообщено в частном порядке.

Считаю, что автореферат Д.А. Мордвинова удовлетворяет требованиям, предъявляемым к авторефератам диссертационных работ на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей, а автор работы заслуживает присуждения ему указанной ученой степени.

Профессор факультета вычислительной математики
и кибернетики МГУ имени М. В. Ломоносова,
доктор физико-математических наук

Захаров Владимир
Анатольевич

02.03.2021

Сведения об организации:
Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М.В. Ломоносова»
119991, Москва, Ленинские горы, д. 1
Телефон: (495) 939-10-00
Факс: (495) 939-01-26
Веб-сайт: www.msu.ru
E-mail: info@rector.msu.ru