ОТЗЫВ

на автореферат диссертации Мордвинова Дмитрия Александровича «Автоматический вывод реляционных инвариантов для нелинейных систем дизъюнктов Хорна с ограничениями», представленной на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Диссертация Д.А. Мордвинова является исследованием в области логических методов искусственного интеллекта. Объектами исследования являются конструкции, методы и алгоритмы, используемые в современных направлениях логического программирования (ЛП). Более точно, исследуются возможности сочетать формализм дизъюнктов Хорна, широко применяемый в ЛП, с современными подходами к сокращению комбинаторной сложности конечных задач за счет использования т.н. “SMT-подхода” (от Satisfiability Modulo Theories)

Практическая востребованность методов формальной верификации возрастает год от года. На начальном этапе этого пути основным «поставщиком» задач верификации была индустрия проектирования микросхем. Однако за последние 30 лет формальная верификация стала одним из базовых инструментов в таком бурно развивающемся направлении как анализ корректности программ. К классическим вопросам в этой области относится задача порождения инвариантов программ. Инвариант – это некоторое свойство программы, не меняющееся в процессе ее выполнения. Инварианты могут использоваться для подтверждения правильности работы рассматриваемой программы – инварианты циклов дают в этом смысле простые и понятные примеры. Индуктивный инвариант – это инвариант, наличие которого может быть доказано при помощи схемы индукции (опять-таки можно привести в пример циклы). Насколько можно судить из автореферата, проблема построения индуктивных инвариантов программ стала одним из основных мотивирующих факторов для диссертационного исследования Д.А. Мордвинова.

Проблему наличия у программы некоторого инварианта заданного вида можно сформулировать, используя традиционный для логического программирования формализм дизъюнктов Хорна: с их помощью можно представлять проверяемые свойства в виде последовательности логических импликаций. Такой подход является классикой логического программирования (пожалуй, самый известный пример в данном контексте – язык/система вывода «Пролог») и поддерживается многими современными системами формального анализа программ. Если рассматриваемая программа работает с данными некоторой конкретной предметной области, то естественным выглядит при синтезе инвариантов использовать дополнительную информацию из этой предметной области. Это достигается за счет формулировки дополнительных ограничений в языке предметной области (т.н. «язык ограничений»). Соответствующие формулы уже не обязаны быть хорновскими, однако для

проверки выполнимости полученных наборов таких «гибридных» ограничений можно использовать SMT решатели. Неинтерпретированные предикатные мета-символы при этом интерпретируются формулами из языка ограничений (т.н. «символьная интерпретация»).

Как следует из автореферата, в диссертации приводится ряд примеров, когда подход на основе символьной интерпретации не позволяет вывести инварианты ввиду слабой выразительности языка ограничений, притом что использование более выразительного языка приводит к необходимости работать в неразрешимой теории (сказанное хорошо иллюстрируется примером с арифметиками Пресбургера и Пеано). Для выхода из данной ситуации Д.А. Мордвинов предлагает обратиться к т.н. «реляционным интерпретациям». Точнее, вводится понятие реляционной символьной интерпретации, которая подразумевает возможность заменять формулами группы неинтерпретированных символов (для этой цели специально вводится понятие реляционной подстановки). Данная идея, насколько можно судить из автореферата, есть развитие предложенной ранее Д.А. Мордвиновым с соавторами техники синхронизирующих преобразований. Далее в контексте понятия реляционной интерпретации возникает понятие реляционного сертификата выполнимости. Реляционные сертификаты – это, в некотором роде, более слабые версии «обычных» сертификатов выполнимости, однако важно то, что из существования у системы дизъюнктов реляционного сертификата следует выполнимость этой системы (теорема 4 из автореферата). Реляционный сертификат может представлять, например, некоторый инвариант и, таким образом, использоваться для доказательства безопасности программ. Алгоритм вывода реляционных сертификатов выполнимости для систем дизъюнктов Хорна (алгоритм RelRecMC) предложен в 4-й главе диссертации.

В экспериментальной части работы (глава 5) приведены результаты реализации алгоритма RelRecMC в рамках известной программной системы работы с хорновскими дизъюнктами SPACER. Эксперименты демонстрируют, что предложенный алгоритм сопоставим по эффективности либо превосходит известные системы с аналогичным функционалом (SPACER, HOICE).

Замечания по тексту автореферата.

1. Лично мне кажется, что формализм с мультимножествами избыточен, так как некоторые интуитивно ясные моменты выглядят путано. В частности, при анализе ключевого определения реляционной символьной интерпретации (стр. 14) из-за обозначения $\{R \mapsto 1\}$ возникает впечатление, что в этом определении фактически фигурируют обычные множества. Разве нельзя предикаты с одинаковой семантикой обозначить различными символами, используя, например, дополнительные индексы? Из автореферата не ясно, насколько принципиален учет возможности многократного вхождения одного и того же предикатного символа в кортеж.
2. Произвольный предикатный символ обозначается то буквой P, то буквой R. Это происходит неоднократно (стр. 9,10,11,12), что затрудняет

понимание смысла. Символ R вообще имеет несколько различных трактовок: это и предикатный символ, и R = (def)G(r) (стр. 11).

3. Встречаются несогласованные словосочетания: «… систем дизъюнктов Хорна заключается состоит в том, что …» (стр. 4); «реляционные сертификаты выполнимости строятся …, но является …» (стр. 16).

Сделанные замечания не влияют на итоговую положительную оценку работы. Исследование производит сильное впечатление широтой охваченной тематики и уровнем полученных результатов. Очевидно, что эти результаты находятся в тренде современных мировых исследований в логическом программировании.

Основное направление работы – формальная верификация программ. Также в диссертации разработаны техники, повышающие эффективность символьных вычислений (SMT-решателей) применительно к рассматриваемой предметной области. Таким образом, соответствие диссертации Д.А. Мордвинова паспорту специальности 05.13.11 не вызывает сомнений.

Работа прошла хорошую апробацию – ее основные результаты были доложены на рейтинговых международных конференциях, среди которых одна из ведущих в мире конференций по логическому программированию LPAR.

Резюмируя сказанное, считаю, что диссертация «Автоматический вывод реляционных инвариантов для нелинейных систем дизъюнктов Хорна с ограничениями» выполнена на высоком уровне, является законченной научно-исследовательской работой, а ее автор, Дмитрий Александрович Мордвинов заслуживает присвоения ученой степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Заведующий лабораторией логических и
оптимизационных методов анализа сложных систем
Института динамики систем и теории
управления им. В.М. Матросова СО РАН
к.т.н. по специальности 05.13.18
«Математическое моделирование, численные методы
и комплексы программ», доцент А.А. Семёнов

16.12.2020

Семёнов Александр Анатольевич
664033, Иркутск, ул. Лермонтова, 134
Институт динамики систем и теории
управления им. В.М. Матросова СО РАН,
тел. +7 (3952) 45-30-54
e-mail: biclop.rambler@yandex.ru

Подпись заверяю
Нач. отдела делопроизводства
и организационного обеспечения
ИДСТУ СО РАН
Г.Б. Кононенко
16.12.2020