Отзыв

Официального оппонента на диссертационную работу

Мордвинов Дмитрий Александрович

«Автоматический вывод реляционных инвариантов для нелинейных систем дизъюнктов Хорна с ограничениями», представленную на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 — «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

Актуальность темы. Формальная верификация программ – актуальная научная тема, имеющая фундаментальное, прикладное и технологическое значение. Актуальность фундаментальных исследований по верификации программ обусловлена стремлением понять и математически описать, что такое программы, задаваемые ими вычисления и их смысл. Актуальность прикладных исследований по верификации программ обусловлена необходимостью разработки новых методов повышения надежности (безопасности и защищенности) и работоспособности (функциональности) программ, управляющих критическими системами. Актуальность технологических исследований по верификации программ обусловлена важностью доведения новых методов верификации критически важных программ до уровня технологии и серийного применения в индустрии.

Тематика рассматриваемой диссертационной работы относится к прикладной верификации. Поэтому ее актуальность обусловлена новыми методами верификации, разработанными, обоснованными и экспериментально проверенными в ходе подготовки работы и представленными в тексте.

Цель диссертационной работы. Автор диссертационной работы формулирует целью работы разработку эффективного (на практике) подхода для решения нелинейных систем дизъюнктов Хорна с ограничениями (возникающих при логическом моделировании императивных программ над целыми числами) за счет элиминацию нелинейной рекурсии. Для достижения этой цели автор ставит и решает в работе следующие задачи:

1. Разработать преобразование для нелинейных систем дизъюнктов Хорна с ограничениями упрощающее поиск символьных моделей.

2. Определить класс решений систем дизъюнктов Хорна с ограничениями, который имеет эффективную реализацию и обобщает классы символьных моделей, известные на момент подготовки работы.

3. Провести экспериментальное исследование полученных результатов.

Научная значимость и новизна результатов, выносимых на защиту.

1. Предложен подход к синтаксической синхронизации (линеаризации) систем дизъюнктов Хорна с ограничениями первого порядка, алгоритм CHCproduct, реализующий синхронизирующее преобразования, доказана его корректность b завершаемость.
2. Введено понятие реляционного сертификата выполнимости для систем дизъюнктов Хорна, доказана его корректность (то есть, что он гарантирует выполнимость системы), предложены алгоритмы RelRecMc и RelBndSafety (обобщающие известные алгоритмы для

простых сертификатов выполнимости) для «направляемого свойством» построения (Property Driven Reachability) реляционных сертификатов выполнимости, доказана его корректность и завершаемость (относительно оракула выполнимости).
3. Алгоритмы CHCproduct и RelRecMc реализованы в SMT-решателе Z3 (во взаимодействии с его ядром), проведена и экспериментально подтверждена проверка на тестовых примерах эффективности и корректности реализации.

Структура диссертационной работы.

Работа состоит из Введения, четырех глав и Заключения.

В Первой главе вводятся системы дизъюнктов Хорна с ограничениями, показано значение существования моделей для систем дизъюнктов Хорна с ограничениями, показано, что нелинейные систем естественно возникают при верификации программ, дан обзор области реляционной верификации и методов решения систем с использованием SMT-решателей.

Во Второй главе описанию предложенного в диссертации синхронизирующего преобразования систем дизъюнктов Хорна с ограничениями CHCproduct, доказаны Теоремы о его корректности и завершаемости.

В третьей главе определено понятие реляционных сертификатов выполнимости систем дизъюнктов Хорна с ограничениями, обоснована его корректность, а направляемые свойством алгоритмы построения реляционных сертификатов описаны и обоснованы в четвёртой главе.

Публикации.

По теме представленной диссертационной работы автором опубликовано 7 работ из которых них 2 статьи – в журналах из «Перечня рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук», 3 статьи опубликованы в издании, входящем в базы цитирования Scopus и Web of Science.

Диссертационная работа написана четким научным языком, представляет замкнутый и полный монографический труд, автореферат корректно отражает его содержание, и, кроме того, содержание работы достаточно полно освящено в публикациях автора.

Замечания и вопросы.

1. К сожалению, в работе по верификации представленные алгоритмы не специфицированы должным образом (то есть пред- и постусловиями, инвариантами и вариациями циклов), а доказательства их корректности и завершаемости не используют метод Флойда-Хоара.

2. Фактически, линейные системы Хорна – это итеративные неветвящиеся программы, нелинейные системы – это итеративные ветвящиеся программы. Интересно было бы узнать, что формально известно об этой связи, как задача линеаризации систем дизъюнктов Хорна с ограничениями связана с задачей устранения рекурсии вообще и Datalog'е в частности. (Впрочем, данный вопрос может быть темой для дальнейшего исследования.)

3. Среди публикаций автора есть публикации в изданиях, рекомендованных ВАК, в изданиях, входящих в Scopus и Web of Science, а также в трудах конференций и семинаров, соответствующих по тематике диссертационной работы. Однако, возникает естественный вопрос, пытался ли автор представить свои результате на самом тематическом семинаре по

теме диссертации – Workshop on Horn Clauses for Verification and Synthesis (который в этом году пройдет уже в восьмой раз – см. https://www.sci.unich.it/hcvs21/).

4. К сожалению, в автореферате использована собственная нумерация определений и теорем без ссылки на номера соответствующих определений и (что особенно важно) теорем в тексте диссертационной работы. Этот недостаток затрудняет для читателей автореферата затрудняет поиск соответствующего определения или теоремы в самой работе (если возникнет, например, необходимость познакомиться с доказательством).

Заключение.

Диссертационная работа Д.А. Мордвинова «Автоматический вывод реляционных инвариантов для нелинейных систем дизъюнктов Хорна с ограничениями» является завершенной и целостной научной работой, в которой автором самостоятельно на высоком научном уровне разработаны теоретические основы, методы и алгоритмы решения всех поставленных задач.

Полученные автором результаты достоверны, выводы и заключения обоснованы. Работа базируется на математических доказательствах и компьютерный реализации, она имеет логичную структуру, изложена последовательно и полно, аккуратно оформлена.

Считаю, что диссертационная работа Д.А. Мордвинова «Автоматический вывод реляционных инвариантов для нелинейных систем дизъюнктов Хорна с ограничениями» соответствует требованиям, предъявляемым нормативными актами Российской Федерации к диссертациям на соискание ученой степени кандидата наук, а ее автор Дмитрий Александрович Мордвинов заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.11 — «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Официальный оппонент:
к.ф.-м.н., доцент, начальник Лаборатории программной инженерии Автономной некоммерческой организации высшего образования «Университет Иннополис» (АНО ВО «Университет Иннополис»)

Николай Вячеславович Шилов

Дата 05 марта 2021 г.

Подпись к.ф.-м.н., доцента,
начальника Лаборатории программной инженерии
Н.В. Шилова заверяю
Директор по развитию и кадровой политике
АНО ВО «Университет Иннополис» Радик Фларитович Валиев

Шилов Николай Вячеславович, кандидат физико-математических наук по специальности 05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей, доцент, начальник Лаборатории программной инженерии Автономной некоммерческой организации высшего образования «Университет Иннополис» (АНО ВО «Университет Иннополис»),
420500, г. Иннополис, ул. Университетская, д.1
телефон: +7 843 203-92-53
адрес сайта в сети интернет: https://innopolis.university/
адрес электронной почты: university@innopolis.ru

Контактные данные:
телефон: +7 913 727-04-38
адрес электронной почты: n.shilov@innopolis.ru