Отзыв
официального оппонента на диссертационную работу
Мордвинова Дмитрия Александровича
«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. Надёжность программного обеспечения является одной из центральных тем исследований в программной инженерии. Один из главных прорывов в этой области состоялся три десятилетия назад – появление символьной верификации программ. Суть этого подхода заключается в том, что для представления множества состояний программы используются формулы некоторой логики, а для проверки пустоты множества состояний — разрешающие процедуры проверки выполнимости формул этой логики. Это позволяет верификатору манипулировать большим, иногда бесконечным, множеством состояний программы, что важно для масштабирования всей процедуры на промышленные программные системы.

Инструменты, используемые для символьной верификации программ, быстро эволюционируют. Можно заметить важную тенденцию повышения порядка используемой логики. Три десятилетия назад большинство методов символьной верификации основывалось на логике высказываний (т.н. логике нулевого порядка) с использованием бинарных решающих диаграмм и SAT-решателей в качестве вспомогательных инструментов. Полтора десятилетия назад, вместе с развитием SMT-решателей, применяющих большой арсенал разрешающих процедур различных теорий, стала применяться логика первого порядка. А в последние пять лет стали популярны решатели дизъюнктов Хорна с ограничениями, автоматизирующие проверку выполнимости в рамках фрагмента логики второго порядка.

Решатели дизъюнктов Хорна с ограничениями получают на вход формулы определённого вида с логическими переменными и выдают на выходе интерпретации этих переменных в виде формул некоторого языка первого порядка. При этом может возникнуть следующий интересный эффект, известный ещё со времён появления логики Хоара: входная формула выполнима, но выразительной силы языка недостаточно, чтобы представить хотя бы одну интерпретацию, выполняющую формулу. В таком случае, как правило, работа решателя не завершается, поскольку алгоритм зацикливается, бесконечно уточняя ответ. Полностью решить эту проблему невозможно в силу теоремы Райса, но тем не менее поиски частных решений для ограниченного круга практических задач чрезвычайно актуальны.

Эта проблема актуальна и для верификации на основе нелинейных систем дизъюнктов Хорна. Таким образом, диссертационное исследование проведено на переднем крае современной науки и на актуальную тему.

Целью диссертационной работы является разработка эффективного подхода для решения нелинейных систем дизъюнктов Хорна с ограничениями на основе подходов реляционной верификации.

Новизна исследований и разработок. В качестве научных результатов, обладающих несомненной научной новизной, на защиту выносится следующее.

1. Метод синхронизации систем дизъюнктов Хорна с ограничениями первого порядка. Предложенный метод преобразует систему таким образом, что деревья гиперрезолютивных выводов соответствуют деревьям выводов оригинальной системы со слиянием некоторых путей. Это преобразование частично решает проблему непредставимости моделей.

2. Алгоритм CHCproduct, реализующий синхронизирующее преобразование дизъюнктов Хорна с ограничениями, доказательство корректности и завершаемости алгоритма, анализ его сложности.
3. Новое понятие реляционного сертификата выполнимости; доказательство теоремы о том, что если у системы существует реляционный сертификат выполнимости, то она выполнима.
4. Алгоритм RelRecMc для автоматического построения реляционных сертификатов выполнимости для систем дизъюнктов Хорна с ограничениями; доказательство корректности алгоритма.
5. Реализация алгоритмов CHCproduct и RelRecMc в SMT-решателе Z3; экспериментальное исследование алгоритмов на различных тестовых примерах, включающих условия верификации свойств безопасности и реляционных проблем верификации свойств гипербезопасности.

Диссертация состоит из введения, пяти глав, заключения, а также списка литературы из 149 наименований.

Во **введении** обоснована актуальность темы диссертации, сформулированы цели и задачи исследования, перечислены методы исследования, указаны область, объект и предмет исследования, сформулирована научная новизна, выделены основные результаты, которые выносятся на защиту, отмечаются практическая и теоретическая ценность полученных результатов, приводится информация об апробации работы на международных конференциях.

В **первой главе** проводится обзор области исследования. Вводятся системы дизъюнктов Хорна, приводятся теоретические сведения, характеризующие разрешимость различных теорий и проблемы автоматического вывода решений систем дизъюнктов. Даётся обзор современного состояния в области реляционной верификации, и, в частности, метода PDR.

Во **второй главе** вводится метод синхронизации (преобразования) нелинейной системы дизъюнктов Хорна с ограничениями первого порядка. Показано, что этот метод сохраняет свойство выполнимости/невыполнимости систем. Доказана корректность метода, установлена его алгоритмическая сложность, выполнено семантическое исследование метода с применением семантики неподвижной точки системы дизъюнктов. Предложенный метод синхронизации дизъюнктов является новым и интересным. Глава заканчивается демонстрацией его основной проблемы – вычислительной неэффективности. Решению этой проблемы посвящены следующие две главы.

В **третьей главе** приводится описание нового класса решений систем дизъюнктов Хорна с ограничениями, называемыми реляционными сертификатами выполнимости. Реляционные сертификаты выполнимости основаны на идее синхронизации систем дизъюнктов Хорна. Они служат эффективным средством проверки корректности утверждений об аргументах различных отношений.

В **четвертой главе** реляционные сертификаты выполнимости используются для построения алгоритма RelRecMc, обобщающего известный PDR-алгоритм RecMC на случай нелинейных систем. Доказывается корректность нового алгоритма.

В **пятой главе** описаны реализация разработанных алгоритмов, а также некоторые детали их встраивания в известный верификатор Z3. Также приведены результаты экспериментов, в ходе которых предложенный алгоритм показывает лучшие результаты, чем известные аналоги – алгоритмы Spacer и HoIce.

В **заключении** автор приводит основные результаты работы, рекомендации по их применению и описывает перспективы дальнейших исследований по тематике работы. Достоверность полученных в работе результатов не вызывает сомнений. Результаты, полученные автором диссертации, являются новыми. В диссертации используется современный математический аппарат, предлагаемые методы и алгоритмы реализованы и апробированы на практике.

Выполненные в диссертации исследования показывают, что их автор является высококвалифицированным специалистом в области формальных методов и верификации, что позволило ему предложить принципиально новый подход к верификации программного обеспечения на основе нелинейных систем дизъюнктов Хорна. В то же время, им продемонстрировано понимание особенностей прикладных задач, а также умение строить адекватные формальные модели и разрабатывать эффективные вычислительные алгоритмы.

Следует также отметить, что диссертация грамотно оформлена и написана хорошим научным языком.

Автореферат отражает основные положения диссертационной работы, материалы исчерпывающе освещены в публикациях автора.

Публикации. По теме представленной диссертации автор опубликовал 7 печатных работах, в том числе 2 научных статьи в рецензируемых журналах, рекомендованных ВАК для публикаций материалов кандидатской диссертации, а также 3 статьи, входящие в базы цитирования Scopus и Web of Science.

Замечания. В качестве замечаний к работе отметим следующее.

1. Одной из существенных частей алгоритма RelBndSafety (Листинг 4, стр. 120) является процедура Partition (строка 25, листинг 4). В диссертации утверждается, что эта процедура может быть реализована различными способами, однако ни один из них не приведён в тексте. Таким образом не ясно, влияют ли различные реализации процедуры Partition на эффективность алгоритма RelBndSafety, и какой способ выбран в итоговой версии RelBndSafety.
2. Эксперименты (глава 5, раздел 5.2) можно было лучше структурировать, например, с использованием GQM-метода. При чтении описания экспериментов не сразу становится понятным, что именно подвергается экспериментальной проверке, какому классу принадлежат оцениваемые объекты, какие вопросы ставятся для проверки, почему baseline выбран именно таким способом. Это затрудняем чтение, хотя к качеству экспериментов замечаний нет.
3. В автореферате и тексте диссертации имеется небольшое число опечаток.

Указанные недостатки, однако, не являются принципиальными и не умаляют достоинств диссертации.

Заключение. Диссертация Мордвинова Д.А. «Автоматический вывод реляционных инвариантов для нелинейных систем дизъюнктов Хорна с ограничениями» является завершенной научной работой, в которой автором самостоятельно, на высоком научном уровне, разработал теоретические основы, методы и алгоритмы решения для всех поставленных задач. В работе приведены результаты, которые позволят квалифицировать их как значительное научное достижение в области формальных методов и верификации программного обеспечения. Полученные автором результаты достоверны, выводы и заключения обоснованы. Работа написана грамотно и аккуратно оформлена. По каждой главе и работе в целом сделаны четкие, исчерпывающие выводы.

В целом, на основании вышеизложенного можно сделать заключение, что диссертация Мордвинова Д.А. «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 автор работы, Мордвинов Дмитрий Александрович, достоин присуждения ученой степени

кандидата физико-математических наук по специальности 05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Официальный оппонент:

д.ф.-м. н., профессор, профессор департамента программной инженерии
факультета компьютерных наук Федерального государственного
автономного образовательного учреждения высшего образования «Национальный
исследовательский университет «Высшая школа экономики» (НИУ ВШЭ)

Ирина Александровна Ломазова

Подпись заверяю
СПЕЦИАЛИСТ
ПО КАДРОВОМУ ДЕЛОПРОИЗВОДСТВУ
ОТДЕЛА КАДРОВОГО АДМИНИСТРИРОВАНИЯ
УПРАВЛЕНИЯ ПЕРСОНАЛА
ТИМОХИНА М.С.

Дата 26.02.2021

Подпись д.ф.-м.н., профессора И.А. Ломазовой заверяю

Ломазова Ирина Александровна, доктор физико-математических наук по специальности
05.13.17 – Теоретические основы информатики, профессор, профессор департамента программной
инженерии факультета компьютерных наук Федерального государственного
автономного образовательного учреждения высшего образования «Национальный
исследовательский университет «Высшая школа экономики» (НИУ ВШЭ)
101000, г. Москва, ул. Мясницкая, д. 20.
телефон: (+7 495) 771-32-32
факс: + 7 495 628-79-31
адрес электронной почты: hse@hse.ru
веб-сайт: https://www.hse.ru/

Контактные данные:
телефон: (+7-903) 246-29-95
адрес электронной почты: ilomazova@hse.ru