На правах рукописи

Мордвинов Дмитрий Александрович

АВТОМАТИЧЕСКИЙ ВЫВОД РЕЛЯЦИОННЫХ ИНВАРИАНТОВ ДЛЯ НЕЛИНЕЙНЫХ СИСТЕМ ДИЗЪЮНКТОВ ХОРНА С ОГРАНИЧЕНИЯМИ

Специальность 05.13.11 —
Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Автореферат
диссертации на соискание учёной степени
кандидата физико-математических наук

Новосибирск — 2020

Работа выполнена на кафедре системного программирования федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет».

Научный руководитель: **КОЗНОВ Дмитрий Владимирович,** доктор технических наук, доцент, Санкт-Петербургский государственный университет, профессор кафедры системного программирования

Официальные оппоненты: **ЛОМАЗОВА Ирина Александровна,**
доктор физико-математических наук, профессор,
НИУ ВШЭ,
профессор департамента программной инженерии факультета компьютерных наук НИУ ВШЭ

ШИЛОВ Николай Вячеславович,
кандидат физико-математических наук,
доцент, автономная некоммерческая организация высшего образования «Университет Иннополис»,
старший научный сотрудник лаборатории операционных систем, языков программирования и компиляторов

Ведущая организация: Федеральное государственное бюджетное учреждение науки Институт системного программирования Российской академии наук (ИСП РАН)

Защита состоится 25 марта 2021 г. в 15 часов на заседании диссертационного совета Д 999.082.03 на базе Федерального государственного бюджетного учреждения науки Института систем информатики им. А.П. Ершова Сибирского отделения Российской академии наук (ИСИ СО РАН) по адресу:
630090, г. Новосибирск, проспект академика Лаврентьева, 6, комн. 239.

С диссертацией можно ознакомиться в библиотеке и на сайте ИСИ СО РАН: https://www.iis.nsk.su/files/Dissertaciya_Mordvinova_ot_15.09.2020.pdf

Автореферат разослан _____ декабря 2020 года.

Ученый секретарь
диссертационного совета
Д 999.082.03,
канд. физ.-мат. наук  Мурзин Федор Александрович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. В условиях современного мира, когда компьютеры управляют многочисленными критически важными аспектами жизни человека, доказательство корректности программного кода все больше превращается в необходимость. Объём кода в ядрах операционных систем, драйверах различных устройств, инструментах и библиотеках растет, вопросы его качества становятся всё более насущными. При этом доказательство корректности кода вручную не представляется реалистичным выходом из ситуации, так как требует слишком больших трудозатрат.

В последние 15 лет активное развитие получили подходы, которые привели к появлению SMT-решателей — инструментов эффективного поиска моделей для формул теорий логики первого порядка, используемых для автоматического доказательства теорем. SMT-решатели оказались эффективными для статического анализа кода и автоматического поиска ошибок и используются в таких подходах, как символьное исполнение (Symbolic Execution) и ограниченная проверка моделей (Bounded Model Checking). Они также могут быть использованы для автоматического поиска ошибок и уязвимостей в коде, для генерации тестовых данных для обеспечения высокого уровня покрытия. Однако применение SMT-решателей для формальной верификации программ сталкивается со значительными трудностями.

Большинство современных подходов к верификации, включая вывод индуктивных инвариантов программ, может быть сведено к поиску символьных моделей для систем дизъюнктов Хорна с ограничениями, сформулированными в теориях первого порядка. Это позволяет использовать решатель дизъюнктов Хорна с ограничениями в качестве переиспользуемого ядра верификатора.

Дизъюнкты Хорна с ограничениями позволяют моделировать программы в виде набора логических импликаций. При этом проверка корректности программы сводится к проверке выполнимости дизъюнктов в некоторой теории. Примечательно, что интерпретации, в которых выполняется система дизъюнктов, соответствуют инвариантам моделируемой программы.

В настоящее время существуют высокопроизводительные решатели систем дизъюнктов Хорна (далее — Хорн-решатели), такие как Spacer, Eldarica, Qarmc, HoIce и FreqHorn, использующие SMT-решатели для проверки выполнимости ограничений (в частности, Z3). Были также разработаны эффективные верификаторы, использующие решатели дизъюнктов Хорна для автоматического доказательства утверждений корректности программ на различных языках программирования (SeaHorn, JayHorn, AdaHorn и нек. др.). Эти верификаторы показывают хорошие

результаты на различных соревнованиях (например, SV-COMP), а также на практике.

Система дизъюнктов Хорна с ограничениями называется линейной, если в посылке каждого правила находится не более одного вхождения неинтерпретированного символа; в противном случае система называется нелинейной. Как показывает практика, большинство существующих подходов к решению систем дизъюнктов Хорна с ограничениями эффективны для линейных систем, но плохо справляются с нелинейными системами. В то же время нелинейные системы естественным образом возникают на практике как условия верификации свойств безопасности (т.е. свойств, опровергаемых конечными исполнениями программы), нетривиальных программ с множественными вызовами рекурсивных функций и функций с циклами, а также хорошо подходят для спецификации свойств гипербезопасности программ.

Степень разработанности темы. Исследования по построению эффективных подходов к выводу символьных представлений моделей систем дизъюнктов Хорна активно проводились, начиная с 2000-х годов. Дизъюнкты Хорна с ограничениями стали активно изучаться с появлением логического программирования в ограничениях (Constraint Logic Programming); пионером в этой области является J. Jaffar. Наиболее известными Хорн-решателями являются Spacer (N. Bjorner, A. Gurfinkel, Microsoft Research, США), Eldarica (P. Ruemmer, Швеция), Qarmc (А. Рыбальченко и K. McMillan, США), FreqHorn (Г. Федюкович, США), HoIce (A. Champion, N. Kobayashi, Франция и Япония). Подход PDR к решению систем дизъюнктов Хорна, предложенный A. Bradley, является на сегодняшний день одним из самых эффективных. Он основан на идее *достижимости, направляемой свойством* (Property-Directed Reachability) и реализован в известном Хорн-решателе Spacer. В рамках данного подхода итеративно строится серия *индуктивных усилений* свойства безопасности, что обеспечивает композициональный вывод символьных моделей без раскрутки отношения перехода системы. Как показали результаты соревнований CHC-Comp 2018, этот подход хорошо справляется с построением решений линейных систем, однако на нелинейных системах он работает хуже.

Одна из сложностей решения нелинейных систем дизъюнктов Хорна заключается состоит в том, что часто их символьные модели оказываются непредставимы в теориях первого порядка, используемых Хорн-решателями. При этом у некоторых систем существует теоретико-множественная модель, но не существует символьной модели, представимой в языке ограничений. Эта проблема фундаментальна и связана с компромиссом между разрешимостью и выразительностью теории, используемой Хорн-решателями. Например, арифметика Пресбургера разрешима, но в ней представимы лишь полулинейные отношения, в то время как арифметика Пеано полна для представления моделей систем дизъюнктов Хорна, но неразре-

шима. Поиск эффективного подхода, который мог бы справиться с этими трудностями, при этом наследуя эффективность подхода PDR, остается открытой проблемой.

С 2015 года было сделано несколько попыток построить эффективный поход к решению нелинейных систем дизъюнктов Хорна с ограничениями. Некоторые подходы строят серию линейных приближений нелинейной системы (B. Kafle, J.P. Gallagher); как правило, они не полны и плохо масштабируются. Более удачные попытки были предприняты в 2017-2019 годах на основе обучения с учителем для предугадывания структуры символьных моделей (P. Garg, C. Löding, P. Madhusudan, D. Neider, A. Champion, T. Chiba, N. Kobayashi, R. Sato). Однако они также не справляются с вышеупомянутой проблемой непредставимости моделей системы. Также существуют походы к синтаксической трансформации системы дизъюнктов, упрощающие структуру её моделей (E. De Angelis, F. Fioravanti, A. Pettorossi). Такие подходы частично решают проблему непредставимости моделей, но все их реализации на сегодняшний день раскручивают отношение переходов, и вследствие этого порождают систему экспоненциального размера.

Нелинейный дизъюнкт можно рассматривать как *реляционную спецификацию* корректности, т.е. спецификацию, описывающую *отношение* между входами-выходами нескольких подпрограмм, а не поведение каждой из них по отдельности. Подходы к доказательству таких свойств изучаются в области, называемой *реляционной верификацией* программ.

Один из основных подходов реляционной верификации состоит в сведении к задаче верификации функциональной спецификации одной программы путём построении *программы-произведения* (G. Barthe, J. M. Crespo) с применением различных подходов к выбору отношения переходов этой программы (A. Gurfinkel, R. Sharma, S. Shoham, Y. Vizel). Существуют подходы к реляционной верификации, основанные на синтаксических преобразованиях дизъюнктов Хорна, развиваемые группой исследователей E. De Angelis, F. Fioravanti, A. Pettorossi и M. Proietti. В России и странах бывшего СССР реляционной верификацией занимались, в основном, в контексте проблемы эквивалентности программ. Можно выделить работы следующих исследователей: В.М. Глушкова, В.А. Захарова, А.А. Летичевского, А.А. Ляпунова, Р.И. Подловченко, В.К. Сабельфельда, Ю.И. Янова и других.

Решение задачи по адаптации подходов реляционной верификации с использованием PDR-подхода могло бы существенно повысить работоспособность Хорн-решателей для нелинейных систем.

Целью данной работы является разработка эффективного подхода для решения нелинейных систем дизъюнктов Хорна с ограничениями. Для её реализации были сформулированы следующие задачи.

1. Исследовать проблему представимости моделей систем дизъюнктов Хорна с ограничениями и разработать преобразование нелинейных систем, ослабляющее форму символьных моделей и упрощающее их поиск.
2. Предложить новый вид решений систем дизъюнктов Хорна, который будет представим в языке ограничений для большего множества систем, чем классические символьные модели.
3. Разработать и реализовать алгоритм автоматического построения таких решений систем дизъюнктов Хорна.
4. Провести экспериментальное исследование полученных результатов.

Соответствие диссертации паспорту специальности. Постановка цели и задач исследования соответствует следующим пунктам паспорта специальности 05.13.11: модели, методы и алгоритмы проектирования и анализа программ и программных систем, их эквивалентных преобразований, верификации и тестирования (пункт 1); языки программирования и системы программирования, семантика программ (пункт 2); программные системы символьных вычислений (пункт 5).

Методология и методы исследования. Методология исследования базируется на подходах информатики к формальной верификации программ. В работе используется формализм логики первого порядка с семантикой в стиле Тарского. Программная реализация теоретических результатов выполнена на языке C++ на основе кодовой базы SMT-решателя Z3 и Хорн-решателя SPACER.

Основные положения, выносимые на защиту.

1. Новый подход к синтаксической синхронизации систем дизъюнктов Хорна с ограничениями первого порядка, доказательство его корректности.
2. Алгоритм CHCproduct, реализующий синхронизирующее преобразование дизъюнктов Хорна с ограничениями, доказательство его корректности, завершаемости, анализ сложности.
3. Понятие реляционного сертификата выполнимости и теорема о том, что если у системы существует реляционный сертификат выполнимости, то она выполнима.
4. Алгоритм RelRecMc для автоматического, направляемого свойством, построения реляционных сертификатов выполнимости для систем дизъюнктов Хорна с ограничениями. Доказательство его корректности.
5. Реализация алгоритмов CHCproduct и RelRecMc в SMT-решателе Z3. Экспериментальное исследование данных алгоритмов на различных тестовых примерах, включающих условия верификации свойств безопасности и реляционных проблем верификации свойств гипербезопасности.

Научная новизна результатов, полученных в рамках исследования, заключается в следующем.

- Впервые было введено и формально описано синхронизирующее преобразование дизъюнктов Хорна, а также доказана его корректность.
- Впервые введено понятие реляционного сертификата выполнимости в терминах решения нелинейных систем дизъюнктов Хорна с ограничениями.
- Предложен новый алгоритм автоматического вывода реляционных сертификатов выполнимости RelRecMc, обобщающий известный алгоритм RecMC и улучшающий его поведение на нелинейных системах.

Теоретическая и практическая значимость работы. Диссертационное исследование предлагает новый метод синхронизации нелинейных систем дизъюнктов Хорна с ограничениями, частично решающий проблему непредставимости символьных моделей систем дизъюнктов в языке ограничений.

Практическая значимость работы заключается в создании и реализации алгоритма автоматического вывода реляционных сертификатов выполнимости, который может быть использован для доказательства корректности программного кода относительно произвольных свойств безопасности или гипербезопасности первого порядка, автоматического аннотирования императивных программ в декартовой логике Хоара, для вывода уточняющих типов функциональных программ, доказательства эквивалентности программ и т.д.

Степень достоверности и апробация результатов. Достоверность и обоснованность результатов исследования обеспечивается формальными доказательствами, а также компьютерными экспериментами. Полученные результаты согласуются с результатами, установленными другими авторами.

Основные результаты работы докладывались на следующих научных конференциях и семинарах: внутренний семинар университета Вашингтона (14 декабря 2016 года, Сиэтл, США), конференция LPAR-2017 (7-12 мая 2017, Маун, Ботсвана), внутренний семинар ИСП РАН им. В.П. Иванникова (14 июня 2019, Москва, Россия), конференция ECOOP-2019 (15-19 июля 2019 г., Лондон, Великобритания), открытый семинар PSSV-2019 (1–2 июля 2019, Новосибирск, Россия), конференция FMCAD-2019 (22–25 октября 2019, Сан-Хосе, США), внутренний семинар ИСИ СО РАН (21 ноября 2019, Новосибирск, Россия), внутренний семинар ВШЭ (19 декабря 2019, Москва, Россия).

Публикации по теме диссертации. Основные результаты по теме диссертации изложены в семи печатных работах, зарегистрированных в РИНЦ. Из них две статьи изданы в журналах из “Перечня рецензируе-

мых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук", сформированного согласно требованиям, установленным Министерством образования и науки Российской Федерации. Три статьи опубликованы в издании, входящем в базы цитирования Scopus и Web of Science.

Личный вклад автора в публикациях, выполненных с соавторами, распределён следующим образом. В работе [2] вклад автора заключается в предложении исчисления символьных куч и сведению поиска пространственных инвариантов к решению систем дизъюнктов Хорна с ограничениями; соавторы участвовали в обсуждении идей, постановке экспериментов, разработке алгоритма сведения для произвольных потоков управления. В статье [3] автор предложил формулировку понятия реляционного инварианта как решения нелинейных систем дизъюнктов, разработал и реализовал алгоритм, участвовал в постановке экспериментов; соавторы участвовали в обсуждении основных идей статьи, выполняли обзор предметной области. В работах [6,7] автор представил синхронизирующее преобразования системы дизъюнктов, выполнил доказательство его корректности; соавторы предложили идею синхронизации, ставили эксперименты, участвовали в формализации и улучшении изложения идей статьи. В работах [4,5] вклад автора заключается в доказательстве неразрешимости задачи невыполнимости неэкспансивного фрагмента систем типов; соавторы формализовали задачу, участвовали в улучшении доказательства, а также предложили разрешающую процедуру для полулинейного фрагмента.

Объем и структура работы. Диссертация состоит из введения, четырех глав, заключения и приложения. Полный объем диссертации **169** страниц текста с **12** рисунками и **6** таблицами. Список литературы содержит **149** наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность исследований, выполненных в рамках данной диссертационной работы, приводится краткий обзор научной литературы по изучаемой проблеме, формулируется цель, ставятся задачи работы, излагается научная новизна и практическая значимость представленного исследования.

Первая глава посвящена обзору области исследования. Вводятся синтаксис и семантика систем дизъюнктов Хорна с ограничениями первого порядка. Показано, что проблемы автоматического вывода индуктивных инвариантов императивных программ и уточняющих типов (refinement types) функциональных программ сводятся к поиску моделей систем дизъюнктов Хорна с ограничениями. Приводятся теоретические сведения, характеризующие разрешимость различных теорий и проблемы автомати-

ческого вывода решений систем дизъюнктов. Даётся обзор области реляционной верификации, показывается, что проверка реляционных свойств сводится к решению нелинейных систем дизъюнктов Хорна.

Даётся краткий обзор наиболее успешных методов решения систем дизъюнктов с использованием SMT-решателей: уточнение абстракции по контрпримерам (Counter-Example Guided Abstraction Refinement, CEGAR), применение обучения с учителем для построения символьных решений систем дизъюнктов (подход ICE), синтаческие подходы к синтезу символьных решений (Syntax-Guided Synthesis, SyGuS), а также PDR-подход (Property Directed Reachability).

На основе проделанного обзора делаются следующие выводы.

- Задача автоматического вывода символьных моделей систем дизъюнктов Хорна с ограничениями важна для формальной верификации программ, поскольку к ней сводится большинство проблем доказательства корректности программ на различных языках программирования. При этом нелинейные системы дизъюнктов описывают реляционные спецификации корректности программ.
- PDR-подход в настоящее время является наиболее эффективным к автоматическому решению систем дизъюнктов Хорна.
- Фундаментальным препятствием на пути к решению систем дизъюнктов является непредставимость моделей в языке решателя. В таких ситуациях любой существующий алгоритм автоматического построения символьных моделей не завершается. При этом обогащение языка может сделать проверку выполнимости его формул неразрешимой, что сделает невозможной в общем случае даже автоматическую проверку корректности решений-кандидатов. Для преодоления этой проблемы требуется изменение способа представления решений нелинейных систем дизъюнктов.

Вторая глава посвящена описанию предложенного в диссертации синхронизирующего преобразования систем дизъюнктов Хорна с ограничениями. Синхронизирующее преобразование переписывает входную систему дизъюнктов таким образом, что деревья гиперрезолютивных выводов переписанной системы соответствуют деревьям выводов оригинальной системы со слиянием некоторых путей от корня до листьев. Это преобразование частично решает проблему непредставимости моделей.

Пусть $\mathcal{A}$ — язык первого порядка, называемый *языком ограничений*. Бескванторные формулы языка $\mathcal{A}$ будем называть *ограничениями*. Пусть $\mathcal{R} \stackrel{\text{def}}{=} \{P_1, \ldots, P_n\}$ — множество предикатных символов, не принадлежащих языку $\mathcal{A}$, называемых *неинтерпретированными*. Местность символа P обозначается $ar\,(P)$, $\forall\phi$ обозначает универсальное замыкание формулы ϕ.

Определение 1. *Дизъюнкт Хорна с ограничением в $\mathcal{A}$ над $\mathcal{R}$* является формулой C следующего вида:

$$\phi \wedge R_1(\overline{x}_1) \wedge \ldots \wedge R_m(\overline{x}_m) \to H.$$

При этом H называется *заголовком* дизъюнкта и является либо атомарной формулой $R_0(\overline{x}_0)$, либо $\bot$; $R_i \in \mathcal{R}$ для всех i от 0 до m; ϕ — ограничение; $\overline{x}_i$ — кортежи предметных переменных. Посылка импликации в формуле C называется *телом дизъюнкта*:

$$body(C) \stackrel{\text{def}}{=} \{\phi \wedge R_1(\overline{x}_1) \wedge \cdots \wedge R_m(\overline{x}_m)\} \qquad head(C) \stackrel{\text{def}}{=} H$$

Дизъюнкт называется *линейным*, если $m \leq 1$, иначе он *нелинеен*.

Определение 2. Множество дизъюнктов Хорна с ограничением называется *системой дизъюнктов*. При этом дизъюнкты с заголовком $\bot$ называются *запросами*, дизъюнкты с заголовком $P(\overline{x})$ — *правилами* символа P. Множество правил символа P обозначим $rules(P)$.

Пусть $\mathcal{M}$ — интерпретация языка $\mathcal{A}$. Пусть $\overline{X} = \langle X_1, \ldots, X_n \rangle$ — кортеж отношений на носителе $|\mathcal{M}|$, где $X_i \subseteq |\mathcal{M}|^{ar(P_i)}$. Записью $\left(\mathcal{M}, \overline{X}\right)$ обозначим обогащение $\mathcal{M}\,\{P_1 \mapsto X_1, \ldots, P_n \mapsto X_n\}$.

Определение 3. Система дизъюнктов $\mathcal{S}$ называется *выполнимой* в интерпретации $\mathcal{M}$, если существуют отношения $\overline{X}$, такие что

$$\left(\mathcal{M}, \overline{X}\right) \models \bigwedge_{C \in \mathcal{S}} \forall C$$

В противном случае система называется или *невыполнимой* в $\mathcal{M}$.

Модели системы дизъюнктов также удобно представлять формулами: отношение, интерпретирующее n-местный символ $P \in \mathcal{R}$, естественно представлять формулой языка $\mathcal{A}$ с n свободными переменными. Отображения, сопоставляющие символам формулы, подстановка которых вместо вхождений символов $\mathcal{R}$ в $\mathcal{S}$ выполняется в $\mathcal{M}$, называется *символьной моделью* (или *сертификатом выполнимости*) $\mathcal{S}$.

Пусть $\mathcal{S}$ — система дизъюнктов Хорна с ограничениями. *Графом зависимостей* неинтерпретированных символов назовём ориентированный граф $\langle \mathcal{R}, E \rangle$, где $(P,Q) \in E$ тогда и только тогда, когда символ P появляется в теле некоторого правила символа Q. Символы P, Q называются *рекурсивными*, если P и Q лежат в одной компоненте сильной связности графа зависимостей.

Пусть C — дизъюнкт Хорна с ограничением. Неинтерпретированный атом $R(\overline{x})$ в теле C называется *рекурсивным*, если $C \in rules(P)$, и P и R

рекурсивны. В противном случае, атом называется *нерекурсивным*. Например, атом $P(\overline{x})$ в дизъюнкте $\phi \wedge P(\overline{x}) \to P(\overline{x}')$ рекурсивен, а в дизъюнкте $\phi \wedge P(\overline{x}) \to \bot$ — нерекурсивен.

Множество рекурсивных атомов в теле C обозначим $Rec\,(C)$, множество нерекурсивных атомов — $NRec\,(C)$. Таким образом, тело любого дизъюнкта C с ограничением ϕ можно записать следующим образом:

$$\phi \wedge \bigwedge NRec\,(C) \wedge \bigwedge Rec\,(C)\,.$$

Определение 4. Непустые множества $A_1, \ldots, A_n$ *накрываются* множеством A, если $A \subseteq A_1 \times \cdots \times A_n$, и каждый элемент каждого A_i появляется в позиции i как минимум одного кортежа $x \in A$. Этот факт будем обозначать так: $A \in \lceil A_1, \ldots, A_n \rceil$.

Приведём примеры:

$$\{(1,3,5),(2,4,5)\} \in \lceil \{1,2\},\{3,4\},\{5\} \rceil$$
$$\{(1,3,5),(2,3,5)\} \notin \lceil \{1,2\},\{3,4\},\{5\} \rceil$$

Множество мультимножеств на X, т.е. множество всех отображений X на множество натуральных чисел, обозначим $\mathbb{N}^X$.

Введём счётное множество предикатных символов $\mathcal{R}'$ и биективное отображение $G : \mathbb{N}^{\mathcal{R}} \to \mathcal{R}'$, для которых справедливо $ar\,(G\,(r)) = \sum_{P \in \mathcal{R}} r(P) \cdot ar\,(P)$ для всех $r \in \mathbb{N}^{\mathcal{R}}$.

При этом для удобства будем требовать $\mathcal{R} \subseteq \mathcal{R}'$ и для всех $P \in \mathcal{R}$ $G(\{P \mapsto 1\}) = P$.

Неформально, символы в $\mathcal{R}'$ будут обозначать «слияния» символов их G-прообраза. Будем записывать имена этих символов в виде «произведений» имён соответствующих символов. Например, символ $G(\{P \mapsto 2, Q \mapsto 1\})$ будем называть P^2Q; при этом $ar\left(P^2Q\right) = 2ar\,(P) + ar\,(Q)$.

Пусть $R_1, \ldots, R_m \in \mathcal{R}$, r — мультимножество, соответствующее кортежу $\langle R_1, \ldots, R_m \rangle$ (т.е. мультимножество $\{P \mapsto \#P\}$, где $\#P$ — число вхождений символа P в этот кортеж), $R \stackrel{\text{def}}{=} G(r)$. *Произведением неинтерпретированных атомов* $R_1(\overline{x}_1), \ldots, R_m(\overline{x}_m)$ будем называть следующую формулу:

$$\prod_{i=1}^{m} R_i(\overline{x}_i) \stackrel{\text{def}}{=} R(\overline{x}_1, \ldots, \overline{x}_m).$$

Для любого дизъюнкта C положим следующее:

$$Rec_{/head}\,(C) \stackrel{\text{def}}{=} \begin{cases} Rec\,(C) & \text{если } Rec\,(C) \neq \emptyset, \\ \{head(C)\} & \text{если } Rec\,(C) = \emptyset. \end{cases}$$

Определение 5. Пусть $C_1, \ldots, C_m$ — дизъюнкты, $R_1, \ldots, R_m$ — неинтерпретированные символы (возможно, повторяющиеся) такие, что $C_i \in$

rules(R_i) для всех $i \in \{1,\ldots,m\}$. Дизъюнкт C над $\mathcal{R}'$ называется *произведением* дизъюнктов $C_1,\ldots,C_m$ (обозначается $C = C_1 \times \cdots \times C_m$), если выполнено следующее:

$$
\begin{aligned}
&\mathit{head}(C) = \prod_{i=1}^{m} \mathit{head}(C_i);\\
&\mathit{body}(C) = \phi \wedge \bigwedge \mathit{NRec}\,(C) \wedge \bigwedge \mathit{Rec}\,(C)\,, \qquad \text{где}\\
&\qquad \phi = \bigwedge_{i=1}^{m} \phi_i; \quad \phi_i \text{ — ограничение } C_i;\\
&\qquad \mathit{NRec}\,(C) = \bigcup_{i=1}^{m} \mathit{NRec}\,(C_i)\,;\\
&\qquad A \in \big\lceil \mathit{Rec}_{/\mathit{head}}\,(C_1)\}, \ldots, \mathit{Rec}_{/\mathit{head}}\,(C_m)\}\big\rceil,\\
&\qquad \mathit{Rec}\,(C) = \Big\{ \prod_{i=1}^{m} a_i \;\Big|\; \langle a_1, \ldots a_m\rangle \in A\Big\} \setminus \{\mathit{head}(C)\}. \qquad (1)
\end{aligned}
$$

Например, если $C_1 \equiv \phi_1 \to P(\overline{x})$, $C_2 \equiv \phi_2 \wedge Q(\overline{y}') \to Q(\overline{y})$, то $C_1 \times C_2 \equiv \phi_1 \wedge \phi_2 \wedge PQ(\overline{x},\overline{y}') \to PQ(\overline{x},\overline{y})$.

Каждому символу $R \in \mathcal{R}'$ сопоставим множество правил *rules*(R), сформированных следующим образом. Пусть $G^{-1}(R) = \{P_1 \mapsto k_1,\ldots,P_n \mapsto k_n\}$. Для всех $i \in \{1,\ldots,n\}$ и $j \in \{1,\ldots,k_i\}$ обозначим записью $\mathit{rules}^{(j)}(P_i)$ копию *rules*(P_i) с переименованными переменными таким образом, что переменные в $\mathit{rules}^{(j)}(P_i)$ и $\mathit{rules}^{(j')}(P_{i'})$ различны для $j \neq j'$ или $i \neq i'$. Пусть $k \stackrel{\text{def}}{=} k_1 + \ldots + k_n$. Тогда

$$
\mathit{rules}(R) = \Big\{ C_1 \times \cdots \times C_k \Big| \, \langle C_1,\ldots,C_k\rangle \in \mathit{rules}^{(1)}(P_1) \times \cdots \times \mathit{rules}^{(k_n)}(P_n) \Big\} \qquad (2)
$$

Определение 6. Пусть $\mathcal{S}$ — система дизъюнктов Хорна с ограничениями, и пусть для некоторого $C \in \mathcal{S}$ выполнено следующее:

$$
\begin{aligned}
C &\equiv \phi \wedge \bigwedge \mathit{NRec}\,(C) \wedge \bigwedge \mathit{Rec}\,(C) \to \mathit{head}(C)\\
\mathit{NRec}\,(C) &= \{R_1(\overline{x}_1),\ldots,R_m(\overline{x}_m)\}.
\end{aligned}
$$

Пусть $C \in \mathcal{S}$. *Синхронизацией* C назовём множество дизъюнктов $\mathcal{S}'$ над $\mathcal{R}'$, полученную из $\mathcal{S}$ добавлением новых правил и заменой атомов

Листинг 1: Алгоритм CHCprodуct

Вход : Система дизъюнктов $\mathcal{S}$
Выход : Система дизъюнктов $\mathcal{S}'$
Данные: Очередь дизъюнктов Q

```
1  S' := ∅;
2  Q := {C ∈ S | C — запрос};
3  пока Q ≠ ∅
4      взять C из Q; Q := Q \ {C};
5      ⟨R_1(x̄_1),...,R_m(x̄_m)⟩ := NRec(C);
6      R := G(⟨R_1,...,R_m⟩);
7      (φ ∧ ⋀ Rec(C) ∧ ⋀ NRec(C) → head(C)) := C;
8      C' := (φ ∧ R(x̄_1,...,x̄_m) ∧ Rec(C) → head(C));
9      для всех D ∈ rules(R) добавить D в Q ;
10     S' := S' ∪ {C'};
```

$NRec\,(C)$ в C их произведением:

$$\mathcal{S}' \stackrel{\text{def}}{=} \mathcal{S} \setminus \{C\} \cup \{C'\} \cup \bigcup_{R \in N} rules(R), \text{ где}$$

$$C' \stackrel{\text{def}}{=} \phi \wedge \prod_{i=1}^{m} R_i(\overline{x}_i) \wedge \bigwedge Rec\,(C) \to head(C),$$

N — наименьшее по включению множество символов, содержащее $G(r)$ (где r — мультимножество, соответствующее) $\langle R_1, \ldots, R_m \rangle$ и все символы из $\mathcal{R}'$, входящие в рекурсивные атомы правил символов из N

Листинг 1 представляет псевдокод алгоритма CHCprodуct, который итеративно строит синхронизации дизъюнктов системы. Такое преобразование частично решает проблему непредставимости моделей нелинейных систем. К примеру, следующая система выполнима, но ни одна её модель не представима в линейной целочисленной арифметике (доказательство этого утверждения приведено в диссертации):

$$x{=}0 \wedge z{=}0 \to mul(x,y,z)$$
$$x > 0 \wedge x'{=}x-1 \wedge z{=}z'{+}y \wedge mul(x',y,z') \to mul(x,y,z)$$
$$x{=}x' \wedge y{=}y' \wedge mul(x,y,z) \wedge mul(x',y',z') \to z{=}z'$$

Алгоритм CHCprodуct переписывает данную систему следующим образом (два правила mul^2 с невыполнимым ограничением опущены):

$$x_1{=}0 \wedge z_1{=}0 \wedge x_2{=}0 \wedge z_2{=}0 \to mul^2(x_1{,}y_1{,}z_1{,}x_2{,}y_2{,}z_2)$$
$$x_1 > 0 \wedge x_1' {=} x_1 - 1 \wedge z_1 {=} z_1' {+} y_1 \wedge$$
$$\wedge x_2 > 0 \wedge x_2' {=} x_2 - 1 \wedge z_2 {=} z_2' {+} y_2 \wedge$$
$$\wedge mul^2(x_1'{,}y_1{,}z_1'{,}x_2'{,}y_2{,}z_2') \to mul^2(x_1{,}y_1{,}z_1{,}x_2{,}y_2{,}z_2)$$
$$x{=}x' \wedge y{=}y' \wedge mul^2(x{,}y{,}z{,}x'{,}y'{,}z') \to z{=}z'$$

После переписывания этой системы любой современный Хорн-решатель находит следующее решение: $\{mul^2 \mapsto (x_1 = x_2 \wedge y_1 = y_2 \to z_1 = z_2)\}$.

Важные свойства описанного преобразования формулируются в виде трёх теорем, доказанных в диссертации.

Теорема 1. Алгоритм CHCprodуct всегда завершается.

Теорема 2. Пусть $\mathcal{S}'$ — результат работы алгоритма CHCprodуct на системе дизъюнктов $\mathcal{S}$. Тогда $\mathcal{S}$ выполнима тогда и только тогда, когда выполнима $\mathcal{S}'$.

Теорема 3. Пусть $\mathcal{S}'$ — результат работы алгоритма CHCprodуct на системе дизъюнктов $\mathcal{S}$. Если у $\mathcal{S}$ существует символьная модель, то она существует и у $\mathcal{S}'$.

Как показано выше, обратное утверждение неверно.

Алгоритм CHCprodуct обладает одним существенным недостатком: количество правил в результирующей системе может экспоненциально вырасти по сравнению с количеством правил в изначальной системе (пример такой системы приведён в диссертации). Этим же недостатком обладают все похожие синтаксические преобразования (например, подход, предложенный De Angelis и др.).

В **третьей главе** приводится описание нового класса решений систем дизъюнктов Хорна с ограничениями, называемыми *реляционными сертификатами выполнимости*.

Пусть $\phi(\overline{x})$ и $\psi(\overline{y})$ — формулы со свободными переменными $\overline{x}$ и $\overline{y}$ соответственно. Обозначим через $\phi \overset{+}{\wedge} \psi$ конъюнкцию ϕ и ψ с предварительным переименованием одинаковых свободных переменных операндов:

$$\phi(\overline{x}) \overset{+}{\wedge} \psi(\overline{y}) \overset{\text{def}}{=} (\phi \wedge \psi)\,(\overline{x} \uplus \overline{y})\,.$$

Определение 7. *Реляционная символьная интерпретация* — это частичное отображение $\mathcal{J} : \mathbb{N}^{\mathcal{R}} \to \mathcal{A}$. Обозначим записью $dom(\mathcal{J})$ область её определения. Без потери общности будем считать, что для всех $R \in \mathcal{R}$,

$\{R \mapsto 1\} \in dom(\mathcal{J})$: если это не так, отобразим R в $\top$. Пусть $R_1, \ldots, R_m \in \mathcal{R}$, ϕ — ограничение.

Определим *реляционную подстановку* индуктивно:

$$[\![\phi \wedge R_1(\overline{x}_1) \wedge \ldots \wedge R_m(\overline{x}_m)]\!]_{\mathcal{J}} \stackrel{\text{def}}{=} \phi \ \wedge \bigwedge_{\substack{R_{i_1},\ldots,R_{i_k} \in \{R_1,\ldots,R_m\} \\ \langle R_{i_1},\ldots,R_{i_k}\rangle \in dom(\mathcal{J})}} \mathcal{J}(\langle R_{i_1},\ldots,R_{i_k}\rangle)(\overline{x}_{i_1},\ldots,\overline{x}_{i_k}),$$

$$\left[\!\!\left[\bigwedge_{i=1}^{k} \bigvee_{j=1}^{m_i} F_{i,j} \right]\!\!\right]_{\mathcal{J}} \stackrel{\text{def}}{=} \bigvee_{\substack{1 \le j_1 \le m_1 \\ \ldots \\ 1 \le j_k \le m_k}} [\![F_{1,j_1} \wedge \ldots \wedge F_{k,j_k}]\!]_{\mathcal{J}}\,.$$

При этом $F_{i,j}$ — это конъюнкции ограничений и неинтерпретированных атомов.

Зафиксируем интерпретацию $\mathcal{M}$ языка $\mathcal{A}$.

Определение. Реляционная символьная интерпретация $\mathcal{J}$ является *реляционным сертификатом выполнимости* системы $\mathcal{S}$ с множеством запросов $Q \subseteq \mathcal{S}$, если выполнены следующие свойства:

$$\forall C \in Q,\ \mathcal{M} \models [\![C]\!]_{\mathcal{J}} \qquad \text{(безопасность)}$$

$$\forall A \in dom(\mathcal{J}),\ \mathcal{M} \models [\![\bigwedge_{\substack{R \in \mathcal{R} \\ i \in \{1,\ldots,A(R)\})}}^{+} \bigvee_{C \in rules(R)} body(C)]\!]_{\mathcal{J}} \to \mathcal{J}(A)$$

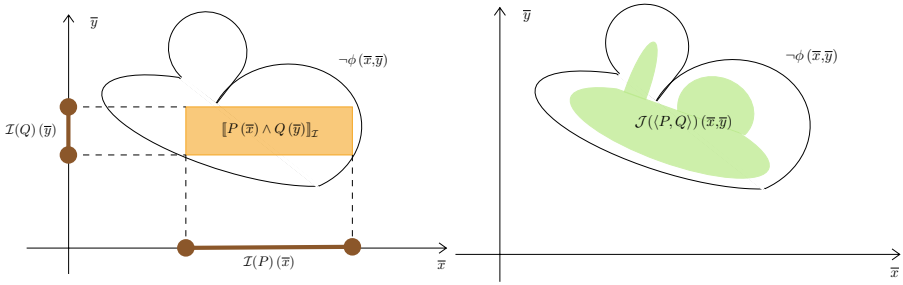
(индуктивность)

В диссертации показано, следующее утверждение о корректности понятия реляционного сертификата выполнимости.

Теорема 4. Если у системы дизъюнктов существует реляционный сертификат выполнимости, то она выполнима.

Неформально говоря, реляционные сертификаты описывают *отношения* над аргументами нескольких символов вместо «резюмирования семантики» каждого символа в отдельности. Поэтому реляционные сертификаты являются более выразительным видом символьных решений нелинейных систем дизъюнктов Хорна по сравнению с «классическими» сертификатами выполнимости (см. рис. 1).

Теорема 5. Если у системы дизъюнктов существует символьная модель, то существует и реляционный сертификат выполнимости.



а) Традиционные сертификаты

б) Реляционные сертификаты

Рис. 1 — Сертификаты выполнимости для проблемы $P(\overline{x}) \wedge Q(\overline{y}) \to \phi(\overline{x},\overline{y})$.

Реляционные сертификаты могут быть получены как «классические» сертификаты выполнимости синхронизированной системы. Например, для примера выше существует реляционный сертификат, интерпретирующий мультимножество $\{mul \mapsto 2\}$ формулой $x_1 = x_2 \wedge y_1 = y_2 \to z_1 = z_2$.

Реляционные сертификаты выполнимости оказываются удобным инструментом, позволяющим решить проблему экспоненциального роста числа правил при преобразовании системы диъзюнктов Хорна. В диссертации приводится способ эффективного вычисления реляционных подстановок, который позволяет избежать вычисления декартового произведения правил за счёт введения дополнительных нульместных предикатных символов.

Таким образом, реляционные сертификаты выполнимости строятся на идее синхронизации систем дизъюнктов Хорна, но является вычислительно эффективным средством проверки корректности утверждений об аргументах различных отношений. Их можно использовать для построения алгоритма автоматического доказательства выполнимости систем дизъюнктов, что и демонстрируется в следующей главе.

В **четвёртой главе** обсуждается алгоритм автоматического вывода реляционных сертификатов выполнимости систем дизъюнктов Хорна. Представлен псевдокод алгоритма RelRecMc и процедуры RelBndSafety. При этом RelRecMc и RelBndSafety обобщают известные PDR-алгоритмы RecMC и BndSafety.

Алгоритм RelRecMc принимает на входе систему дизъюнктов Хорна с ограничениями и в случае останова возвращает ответ `ВЫПОЛНИМА` или `НЕВЫПОЛНИМА`. Если ответ `ВЫПОЛНИМА`, то алгоритм также возвращает реляционный сертификат выполнимости, в случае ответа `НЕВЫПОЛНИМА` возвращается гиперрезолютивное опровержение.

Алгоритм RelRecMc реализует два отображения $\rho : \mathcal{R} \times \mathbb{N} \to \mathcal{A}$ и $\sigma : \mathbb{N}^{\mathcal{R}} \times \mathbb{N} \to \mathcal{A}$. Формулы в образе ρ называются *достижимыми вет-*

вями системы, формулы в образе σ — *реляционными леммами*. Образ ρ используется для построения гиперрезолютивных опровержений системы, в σ размещаются факты, «резюмирующие» систему, которые используются для построения реляционного сертификата выполнимости.

Пусть $P \in \mathcal{R}$. *Семантикой* P глубины b (обозначается $[\![P]\!]^b$) назовём дизъюнкцию формул в корнях всевозможных деревьев гиперрезолютивного вывода P высоты b; для $A \in \mathbb{N}^{\mathcal{R}}$, $[\![A]\!]^b \stackrel{\text{def}}{=} \bigwedge^{+}_{\substack{P \in \mathcal{R} \\ i \in \{1,\ldots,A(P)\})}} [\![P]\!]^b$.

Инвариантом алгоритма являются следующие утверждения:

$$\forall P \in \mathcal{R} \text{ и } b \in \mathbb{N},\ \mathcal{M} \vDash \rho(b,P) \rightarrow [\![P]\!]^b$$
$$\forall A \in \mathbb{N}^{\mathcal{R}} \text{ и } b \in \mathbb{N},\ \mathcal{M} \vDash [\![A]\!]^b \rightarrow \sigma(A,b).$$

Алгоритм $RelRecMc$ увеличивает номер уровня $b \in \mathbb{N}$, начиная с нуля, до тех пор, пока ветви системы ρ не засвидетельствуют контрпример (в таком случае возвращается `НЕВЫПОЛНИМА`), либо реляционные леммы на новом уровне σ не станут индуктивными, т.е. для всех $A \in \mathbb{N}^{\mathcal{R}}$, $\mathcal{M} \vDash [\![A]\!]^b \rightarrow [\![A]\!]^{b-1}$ (тогда возвращается `ВЫПОЛНИМА`). В таком случае множество индуктивных лемм формируют реляционный сертификат выполнимости.

Процедура RelBndSafety, вызванная на уровне b, проверяет, что корни всех деревьев гиперрезолютивного вывода запросов системы глубины b не выполняются в $\mathcal{M}$. В качестве побочного эффекта RelBndSafety усиливает формулы в σ и ослабляет формулы в ρ на уровнях, меньших b.

Процедура RelBndSafety итеративно формулирует и решает *вопросы* $\langle A, \phi, b\rangle$, где $A \in \mathbb{N}^R$, ϕ — ограничение, $b \in \mathbb{N}$. Вопросы помещаются в очередь, которая в начале содержит только вопросы вида $\langle \emptyset, \phi, b\rangle$, где ϕ — ограничения дизъюнктов-запросов системы. На каждый вопрос может быть получен положительный или отрицательный ответ — положительный, если и только если $\mathcal{M} \vDash [\![A]\!]^b \rightarrow \neg\phi$. В случае положительного ответа формулы в образе σ на уровнях, меньших или равных b, усиливаются. В случае отрицательного ответа формулы в образе ρ ослабляются. Если в какой-либо момент оказывается недостаточно сведений о системе для ответа на вопрос, то алгоритм формирует дочерние вопросы на меньших уровнях, которые помещаются в очередь. Алгоритм прекращает работу, как только на все вопросы в очереди получены ответы. При этом, если хотя бы один из корневых вопросов имеет отрицательный ответ, RelBndSafety возвращает `ДОСТИЖИМО`, иначе возвращается `НЕДОСТИЖИМО`.

Процедура RelBndSafety использует *интерполянты Крейга* для обобщения лемм, что ускоряет сходимость лемм к индуктивному инварианту. Также используется *проекции на основе моделей* для элиминации кванторов по экзистенциальным переменным дизъюнктов, что позволяет формулам ветвей системы не разрастаться в размерах с увеличением номера уровня.

Процедура RelBndSafety параметризована оракулом Partition, который разбивает неинтепретированные атомы на мультимножества, для которых будут сформированы дочерние запросы. Partition определяет мультимножества из области определения реляционного сертификата выполнимости. Например, если Partition всегда разбивает неинтерпретированные атомы на группы размера 1, алгоритм будет порождать леммы, интерпретирующие каждый неинтерпретированный символ в отдельности, как и в случае с «классическими» символьными интерпретациями. Для повышения практичности подхода предлагается реализация оракула, *семантически* группирующая атомы. Для этого предлагается вычислять *максимальные индуктивные множества* литералов.

Алгоритм RelRecMc и процедура RelBndSafety имеют следующие свойства, доказанные в диссертации.

Теорема 6. Алгоритм RelRecMc корректен, т.е. если он останавливается для системы $\mathcal{S}$, то она выполнима тогда и только тогда, когда алгоритм вернул `ВЫПОЛНИМА`.

Теорема 7. Процедура RelBndSafety корректна, т.е. для системы $\mathcal{S}$ на уровне b она возвращает `НЕДОСТИЖИМО` тогда и только тогда, когда все корни всех деревьев гиперрезолютивного вывода запросов системы глубины b не выполняются в $\mathcal{M}$.

Теорема 8. Процедура RelBndSafety полна относительно оракула выполнимости в $\mathcal{M}$, т.е. при наличии оракула выполнимости в $\mathcal{M}$ для любой системы $\mathcal{S}$ и уровня $b \in \mathbb{N}$ RelBndSafety останавливается и возвращает `ДОСТИЖИМО`, либо `НЕДОСТИЖИМО`.

Таким образом алгоритм RelRecMc является ко-разрешающей процедурой проблем выполнимости дизъюнктов, т.е. если система невыполнима, то алгоритм гарантированно вернёт `НЕВЫПОЛНИМА`.

Алгоритм RelRecMc идентичен на линейных системах дизъюнктов классическому PDR-алгоритму и *обобщает* его на нелинейные системы: если Partition разбивает атомы в теле дизъюнкта на группы размера 1, то RelRecMc строит «классические» сертификаты выполнимости.

В некоторых случаях, когда «классический» PDR-алгоритм не может вывести сертификат выполнимости нелинейных систем из-за непредставимости моделей в языке ограничений, RelRecMc находит реляционный сертификат выполнимости. Напротив, если PDR-алгоритм завершается и доказывает или опровергает выполнимость системы, то RelRecMc также завершается и выдаёт тот же ответ.

В **пятой главе** представлены детали реализации RelRecMc в ядре решателя SPACER, а также результаты экспериментов. Синхронизирующее преобразование было реализовано как тактика трансформации дизъ-

Кол-во тестов	HoIce	Spacer	RelRecMc
840	808	788	807

Таблица 1 — Количество решённых тестов из тестового набора решателя HoIce

юнктов в популярном SMT-решателе Z3. Реализация была интегрирована в основную ветку Z3.

Алгоритм RelRecMC был реализован в ядре Spacer, современного решателя дизъюнктов Хорна в системе Z3. Было проведено сравнение полученной реализации с Хорн-решателями Spacer (одна из наиболее успешных реализаций PDR-подхода) и HoIce (использует обучение с учителем для генерации инвариантов). Эксперименты были поставлены на двух наборах тестов на компьютере под управлением ОС Arch Linux с процессором Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz.

Первый набор тестов содержал 840 тестовых примеров (проблем), составленных авторами решателя HoIce. Эти тесты включали условия верификации программ на языке OCaml, сгенерированные верификатором MoCHi.

Таймаут для этих тестов составил 30 секунд. Spacer решил 788 из 840 проблем с 50 таймаутами и 2 ошибками времени исполнения. RelRecMC решил 809 проблем с 32 таймаутами. Накладные расходы RelRecMC по времени в сравнении со Spacer оказались незначительными (менее 0.1 секунды на 87% проблем). RelRecMC решил большинство проблем, решённых Spacer. Тем не менее, 10 проблем были решены Spacer, но не RelRecMC; это объясняется несовершенством текущей реализации в RelRecMC процедуры обобщения лемм. HoIce решил 808 проблем с 26 таймаутами и 6 ошибками времени исполнения, при этом и Spacer, и RelRecMC затратили на решённых проблемах меньше времени, чем HoIce .

Второй набор тестов содержал 37 проблем. Сравнение было проведено со Spacer, HoIce и алгоритмом CHCproduct, реализованным как синтаксическое преобразование входной системы дизъюнктов с последующим решением преобразованной системы решателем Spacer.

Схематичное сравнение времени работы решателей показано на рис. 2. Каждая точка на каждом графике представляет пару времён исполнения теста (сек. × сек.) решателем на оси x и другим решателем, на оси y. Если на оси y сразу два решателя, то они различаются разными цветами и формами маркеров на графике: решателю Spacer соответствует круглый маркер, HoIce — треугольный. Превышения временного лимита указаны внутренней пунктирной линией; на внешних пунктирных линиях лежат тесты, на которых решатели завершились с ошибкой времени исполнения.

Кол-во тестов	HoIce	Spacer	CHCProduct	RelRecMc
37	11	11	24	32

Таблица 2 — Количество решённых тестов из реляционного тестового набора

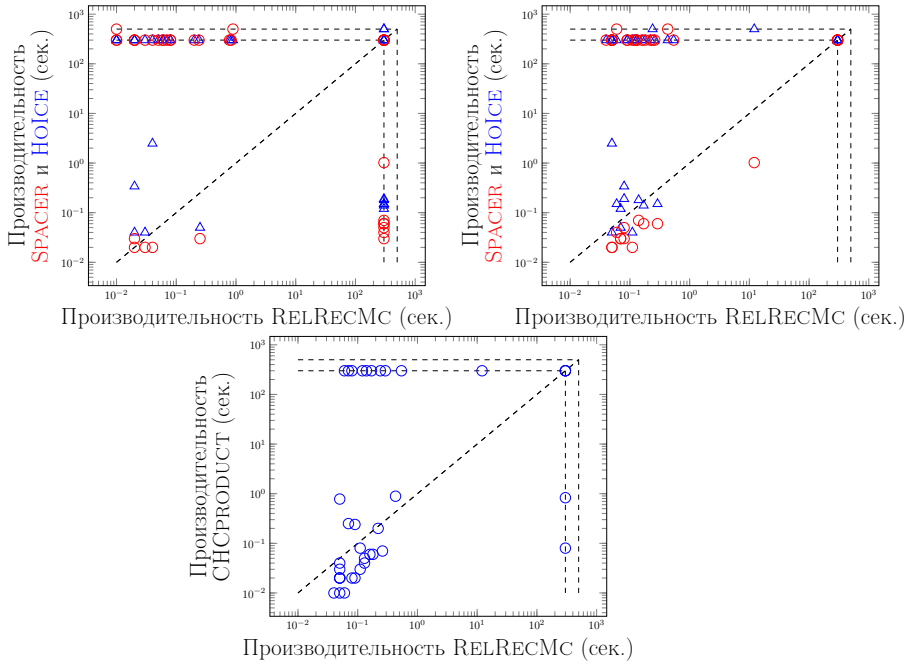


Рис. 2 — Сравнение CHCProduct и RelRecMc с другими решателями

Spacer и HoIce решили только 11 из 37 проблем с 5-минутным таймаутом. Spacer с синтаксической синронизацией решил 24 проблемы, а RelRecMC решил 32 проблемы из 37. Важно, что RelRecMC решил проблемы, с которыми не справился Spacer после явного синтаксического слияния дизъюнктов. Для некоторых невыполнимых проблем большого размера, синтаксическая синхронизация порождает экспоненциальное количество правил, расходуя всё отведённое время, в то время как другие решатели справляются с поиском контрпримера за секунды.

В **заключении** приведены основные результаты работы.

1. Предложено синхронизирующее преобразование систем дизъюнктов Хорна с ограничениями первого порядка. Доказана корректность синхронизирующего преобразования. В частности, показано, что система выполнима тогда и только тогда, когда выполнима

преобразованная, а также что если у системы существует символьная модель, то она существует и у преобразованной.

2. Предложен алгоритм CHCproduct, реализующий синхронизирующее преобразование дизъюнктов Хорна с ограничениями, доказана его корректность, завершаемость, проанализирована сложность.
3. Введено понятие реляционного сертификата выполнимости как решения нелинейных систем дизъюнктов.
4. Предложен алгоритм RelRecMc для автоматического, построения реляционных сертификатов выполнимости для систем дизъюнктов Хорна с ограничениями. Реализация обобщает подход PDR, не меняя его поведения на линейных системах, но позволяя эффективно выводить реляционные сертификаты выполнимости для нелинейных систем вместо «классических» символьных моделей.
5. Алгоритмы CHCproduct и RelRecMc реализованы в известном SMT-решателе Z3. Выполнено экспериментальное исследование данных алгоритмов на различных тестовых наборах, включающих условия верификации свойств безопасности программного обеспечения и проблем реляционной верификации.

В рамках **рекомендации по применению результатов работы** в индустрии и научных исследованиях указывается, что разработанный алгоритм применим для автоматизации рассуждений о системах дизъюнктов над произвольными теориями первого порядка, а также что его реализация выполнена в широко используемом SMT-решателе Z3. Это позволяет модульно реализовать инструменты автоматического доказательства корректности программного кода на любых языках, вывода уточняющих типов произведений функциональных программ, автоматического аннотирования императивных программ в декартовой логике Хоара, а также проверки эквивалентности программ и проверки свойств невмешательства, являющихся важными в области компиляторов и компьютерной безопасности.

Также были определены **перспективы дальнейшей разработки тематики**, основным из которых является разработка подхода к автоматическому определению нетривиальных стратегий синхронизации отношений нелинейных систем дизъюнктов Хорна. Это позволит достичь максимальной гибкости в представлении сертификатов корректности программ за счёт рассмотрения эквивалентных трансформаций изначальной системы. Это особо важно в контексте автоматического доказательства свойств программ, манипулирующих структурами данных с произвольным доступом (например, массивами), позволяя выводить бесквантворные инварианты для программ со сложной логикой обращения к различным областям памяти.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Ниже приведён перечень публикаций, где были представлены основные результаты данной диссертационной работы.

Статьи 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", сформированного согласно требованиям, установленным Министерством образования и науки Российской Федерации

1. Мордвинов, Д.А. Направляемый свойством поиск реляционных инвариантов / Д.А. Мордвинов // Моделирование и анализ информационных систем. — 2019. — Т. 26, №. 4. — С. 550-571.
2. Мордвинов, Д.А. Автоматическое доказательство корректности программ с динамической памятью / Ю.О. Костюков, К.А. Батоев, Д.А. Мордвинов, М.П. Костицын, А.В. Мисонижник // Труды Института системного программирования РАН. — 2019. — Т. 31, №. 5. — С. 37-62.

Статьи в изданиях, входящих в базы цитирования Web of Science и Scopus

3. Mordvinov, D. Property Directed Inference of Relational Invariants. / D. Mordvinov, G. Fedyukovich //Proceedings of the 19th Conference on Formal Methods in Computer-Aided Design (FMCAD 2019). – IEEE. — 2019. — P. 152-160.
4. Mordvinov, D. On Satisfiability of Nominal Subtyping with Variance / A. Misonizhnik, D. Mordvinov // 33rd European Conference on Object-Oriented Programming (ECOOP 2019). — Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik. – 2019. – P. 7:1-7:20.
5. Mordvinov, D. SMT-based Analysis of Constraints on .NET types / A. Misonizhnik, D. Mordvinov // Software Engineering and Information Management. — CEUR. — 2018. — Vol. 2135 — P. 44-52.

Статьи в других изданиях

6. Mordvinov, D. Synchronizing Constrained Horn Clauses / D. Mordvinov, G. Fedyukovich // LPAR-21. 21st International Conference on Logic for Programming, Artificial Intelligence and Reasoning. — 2017. — Vol. 46. — P. 338–355.
7. Mordvinov, D. Verifying Safety of Functional Programs with Rosette/Unbound / D. Mordvinov, G. Fedyukovich [Электронный ресурс]. — URL: https://arxiv.org/abs/1704.04558 (дата обращения: 25.03.2020).

Мордвинов Дмитрий Александрович

АВТОМАТИЧЕСКИЙ ВЫВОД РЕЛЯЦИОННЫХ ИНВАРИАНТОВ ДЛЯ НЕЛИНЕЙНЫХ СИСТЕМ ДИЗЪЮНКТОВ ХОРНА С ОГРАНИЧЕНИЯМИ

Автореф. дис. на соискание ученой степени канд. физ.-мат. наук

Подписано в печать ___.___._____. Заказ № _____
Формат 60×90/16. Усл. печ. л. 1. Тираж 100 экз.
Типография _____