Федеральное государственное автономное образовательное учреждение
высшего образования Университет ИТМО

обновлено: 19 мая 2024 г.

Методы декомпозиции задачи булевой выполнимости для синтеза и верификации моделей автоматных программ

Чухарев Константин

Специальность 2.3.5 (05.13.11)

Математическое и программное обеспечение вычислительных машин,
комплексов и компьютерных сетей

Научный доклад
об основных результатах диссертации
на соискание учёной степени
кандидата технических наук

Научный руководитель:
Семёнов Александр Анатольевич
к.т.н., доцент

Санкт-Петербург, Россия
2024

Общая характеристика работы

Актуальность темы. В современном мире существует множество различных приложений, в которых возникают задачи большой размерности. Особенно это актуально в контексте задач синтеза и верификации дискретных управляющих (ДУ) систем, таких как конечные автоматы и цифровые схемы, которые используются в различных областях, включая робототехнику, электронику, информационную безопасность. Основыми проблемами в области дискретных систем управления являются их синтез и верификация. Синтез ДУ-модели заключается в построении модели системы, которая обладает заданными свойствами. Верификация ДУ-модели заключается в проверке того, что модель удовлетворяет заданной спецификации. Важно отметить, что задачи синтеза и верификации ДУ-моделей являются NP-полными. Это означает, что на сегодняшний день не существует эффективных алгоритмов, способных решать эти задачи за разумное время для всех возможных входных данных. Это приводит к тому, что существующие методы не всегда применимы для решения задач большой размерности. Таким образом, развитие методов и алгоритмов, способных решать подобные задачи более эффективно, остается актуальной и важной задачей в области дискретной математики и компьютерных наук.

Распространённым подходом к *автоматическому* синтезу и верификации является *сведение* к классическим NP-полным задачам, таким как задача выполнимости булевой формулы (Boolean satisfiability problem, SAT), задача максимальной выполнимости (MaxSAT) и задача выполнимости в теориях (Satisfiability Modulo Theory, SMT), с последующим применением так называемых *решателей*, реализующих современные алгоритмы решения этих задач. Данные задачи являются «универсальными», в том смысле что они могут быть использованы для решения широкого класса задач, исключая тем самым необходимость разработки специализированных алгоритмов для каждой конкретной задачи.

Одной из центральных проблем в области синтеза и верификации ДУ-моделей является отсутствие априорных оценок времени работы алгоритмов решения задачи SAT. В рамках данной диссертационной работы предлагаются и развиваются методы и алгоритмы, которые позволяют строить такие оценки. Для этого используются специальные декомпозиционные представления булевых формул. Идеи построения декомпозиций уже выдвигались ранее, но они обладают меньшей точностью. Методы декомпозиции, предложенные в данной работе, учитывают особенности исходной

задачи, которая решается с помощью сведения к SAT, например, особенности задачи синтеза конечно-автоматных моделей или задачи проверки эквивалентности логических схем.

Резюмируя, предложенные в диссертации методы и алгоритмы позволяют повысить эффективность комбинаторных алгоритмов в применении к задачам синтеза и верификации ДУ-моделей. Эти методы могут быть использованы для решения различных задач в области автоматизированного проектирования и управления дискретными системами.

Цель работы. Целью данной работы является повышение эффективности работы полных алгоритмов решения задачи булевой выполнимости (SAT) в применении к задачам синтеза и верификации ДУ-моделей за счет оригинальных методов и техник декомпозиции булевых формул.

Задачи работы. Для достижения поставленной цели были решены следующие научно-технические задачи:

1. Разработаны оригинальные алгоритмы кодирования в SAT задач синтеза конечно-автоматных моделей с заданным поведением и свойствами, отличающиеся от существующих добавлением кодирования структуры охранных условий в виде деревье разбора соответствующих формул.
2. Разработаны оригинальные алгоритмы кодирования в SAT задачи синтеза модульных конечно-автоматных моделей с заданным поведением и свойствами, отличающиеся от существующих автоматизированным модульным разбиением.
3. Разработаны оригинальные алгоритмы кодирования в SAT задачи синтеза булевых схем и булевых формул по заданной таблице истинности, отличающиеся от существующих возможностью использования произвольных элементарных гейтов.
4. Разработаны оригинальные методы оценивания декомпозиционной трудности булевых формул, кодирующих задачи синтеза конечно-автоматных моделей и верификации булевых схем, отличающиеся от существующих учётом особенностей исходной задачи, а также низкой дисперсией времени решения подзадач.
5. С применением разработанных алгоритмов решены трудные примеры задач синтеза ДУ-моделей (как конечно-автоматных моделей, так и логических схем).

6. Разработан новый SAT решатель, использующий вероятностные лазейки для вывода новой информации при работе с трудными булевыми формулами.
7. Разработана программная библиотека для взаимодействия с SAT-решателями через API (программный интерфейс).
8. Проведены масштабные вычислительные эксперименты для подтверждения эффективности всех разработанных методов.

Научная новизна. Новыми являются все основные результаты, полученные в диссертации, в том числе:

1. Новые алгоритмы синтеза конечно-автоматных и модульных конечно-автоматных моделей, основанные на сведении к проблеме булевой выполнимости (SAT).
2. Новые методы оценивания декомпозиционной трудности булевых формул, кодирующих задачи синтеза ДУ-моделей.
3. Оригинальные алгоритмы решения трудных инстансов задачи SAT, использующие объединение нескольких вероятностных лазеек.
4. Решение экстремально трудных задач синтеза ДУ-моделей при помощи разработанных алгоритмов.

Основные положения, выносимые на защиту.

1. Оригинальные алгоритмы кодирования в SAT задачи синтеза конечно-автоматных моделей, отличающиеся от существующих добавлением кодирования структуры охранных условий в виде деревье разбора соответствующих формул.
2. Оригинальные алгоритмы кодирования в SAT задачи синтеза булевых схем и булевых формул по заданной таблице истинности, отличающиеся от существующих возможностью использования произвольных элементарных гейтов.
3. Оригинальные алгоритмы оценивания декомпозиционной трудности булевых формул применительно к задачам верификации логических схем, отличающиеся от существующих учётом особенностей исходной задачи.
4. Программная библиотека[1,2] для взаимодействия с различными SAT-решателями через API (программный интерфейс), отличающаяся от существующих полнотой, гибкостью и удобством.

[1] Для языка Kotlin: `https://github.com/Lipen/kotlin-satlib`

[2] Для языка Rust: `https://github.com/Lipen/sat-nexus`

Теоретическая и практическая значимость. Теоретическая значимость диссертации заключается в разработанных в ней концепциях и алгоритмах решения задач синтеза ДУ-моделей и методах построения оценок трудности таких задач. Практическая значимость диссертации состоит в том, что основные разработанные в ней алгоритмы применимы к индустриальным задачам синтеза и верификации ДУ-моделей, а также в том, что на целом ряде конкретных примеров практическая реализация и апробация разработанных алгоритмов демонстрируют лучшую эффективность в сравнении с известными подходами.

Методы и инструменты исследования. Теоретическая часть работы использует методологию дискретной математики и математической логики, теории вычислительной сложности,а также теорию эволюционных вычислений. Для синтеза конечно-автоматных моделей был использован программный комплекс fbSAT, разработанный в рамках данной диссертации[3]. При построении вычислительных задач из области проверки логической эквивалентности схем использовалась программная система Transalg[4]. Для решения конкретных инстансов задачи SAT использовались различные современные SAT-решатели, находящиеся в открытом доступе, такие как MiniSAT, Glucose, Kissat, CaDiCaL. В вычислительных экспериментах задействовался вычислительный кластер.

Соответствие специальность. Содержание научно-квалификационной работы охватывает такие направления как: синтез и верификация управляющих систем дискретной природы; разработку проблемно-ориентированных комбинаторных алгоритмов, применимых к автоматическому проектированию и верификации ДУ-моделей; разработку алгоритмов декомпозиции сложных экземпляров комбинаторных задач; разработку программных средств для эффективного взаимодействия и SAT-решателями; разработку специализированных SAT-решателей, учитывающих особенности решаемых задач. Программная библиотека, являющаяся одним из основных практических результатов диссертации, обеспечивает эффективное взаимодействие с SAT-решателями через программный интерфейс (API), а также содержит дополнительный функционал для кодирования (сведения) комбинаторных

[3] https://github.com/ctlab/fbSAT

[4] https://gitlab.com/transalg/transalg

задач в SAT. Таким образом, можно утверждать, что работа соответствует паспорту специальности 2.3.5 (05.13.11) в пунктах 1 и 3.

Достоверность результатов проведённых исследований. [TODO]

Апробация работы. Основные результаты диссертации докладывались на следующих конференциях:

- VIII Конгресс молодых ученых, Университет ИТМО, Санкт-Петербург, 2019.
- Конференция СПИСОК-2019, СПбГУ, Санкт-Петербург, 2019.
- IX Конгресс молодых ученых, Университет ИТМО, Санкт-Петербург, 2020.
- Конференция ППС 2021, Университет ИТМО, Санкт-Петербург, 2021.
- X Конгресс молодых ученых, Университет ИТМО, Санкт-Петербург, 2021.
- Воркшоп SAT/SMT Solvers: Theory and Practice, Санкт-Петербург, 2021.
- XI Конгресс молодых ученых, Университет ИТМО, Санкт-Петербург, 2022.

Диссертационная работа была выполнена при поддержке грантов и проектов:

- Грант РФФИ №19-07-01195 А «Разработка методов машинного обучения на основе SAT-решателей для синтеза модульных логических контроллеров киберфизических систем».
- Грант №19-37-51066 Научное наставничество «Разработка методов синтеза конечно-автоматных алгоритмов управления для программируемых логических контроллеров в распределенных киберфизических системах».
- НИР-ФУНД 77051 «Исследование алгоритма тестирования на основе обучения и улучшения его эффективности», 2020-2021.
- НИР-ПРИКЛ 222004 «Алгоритмы решения SAT для логических схем и анализа программ», 2021-2023.
- НИР-ПРИКЛ 223099 «Алгоритмы решения SAT для логических схем и анализа программ», 2023-2024.

Публикации по теме диссертации. Основные результаты по теме диссертации изложены в 9 публикациях. Из них 3 опубликовано в изданиях, индексируемых в базе цитирования Scopus.

Краткое содержание работы

В Главе 1...

В Главе 2...

В Главе 3...

В заключении сформулированы основные результаты научной работы.

Основные выводы и результаты работы

[TODO]

Основные публикации по теме диссертации

1. Automatic State Machine Reconstruction from Legacy PLC Using Data Collection and SAT Solver / D. Chivilikhin, S. Patil, **K. Chukharev**, A. Cordonnier, V. Vyatkin // IEEE Transactions on Industrial Informatics. 2020. Vol. 16, issue 12. P. 7821–7831. (**Q1, Scimago**)
2. SAT-based Counterexample-Guided Inductive Synthesis of Distributed Controllers / **K. Chukharev**, D. Suvorov, D. Chivilikhin // IEEE Access. 2020. Vol. 8. P. 207485–207498. (**Q1, Scimago**)
3. fbSAT: Automatic Inference of Minimal Finite-State Models of Function Blocks Using SAT Solver / **K. Chukharev**, D. Chivilikhin // IEEE Access. 2022. Vol. 10. P. 131592–131610. (**Q1, Scimago**)
4. **Чухарев К.** Применение инкрементальных SAT-решателей для решения NP-трудных задач на примере задачи синтеза минимальных булевых формул // Научно-технический вестник информационных технологий, механики и оптики. 2020. Т. 20, 6(130). С. 841—847. (**ВАК**)
5. **Чухарев К.**, Чивилихин Д. Построение минимальных конечно-автоматных моделей функциональных блоков по обучающим примерам // Сборник тезисов докладов конгресса молодых ученых. Электронное издание. СПб: Университет ИТМО, 2018. URL: http://openbooks.ifmo.ru/ru/file/8061/8061.pdf (дата обр. 17.06.2020).
6. **Чухарев К.** Построение конечно-автоматных моделей функциональных блоков по примерам поведения и темпоральным свойствам // Сборник тезисов докладов

конгресса молодых ученых. Электронное издание. СПб: Университет ИТМО, 2019. URL: https://kmu.itmo.ru/digests/article/1283 (дата обр. 17.06.2020).

7. **Чухарев К.** Автоматический синтез минимальных конечно-автоматных моделей функциональных блоков по примерам поведения и темпоральным свойствам // Материалы 8-й всероссийской научной конференции по проблемам информатики СПИСОК-2019. СПб.: ВВМ, 2019.
8. **Чухарев К.** Синтез конечно-автоматных моделей модульных логических контроллеров по примерам поведения с помощью SAT-решателей // Сборник тезисов докладов конгресса молодых ученых. Электронное издание. СПб: Университет ИТМО, 2020. URL: https://kmu.itmo.ru/digests/article/3555 (дата обр. 17.06.2020).
9. Гречишкина Д., **Чухарев К.** Программный интерфейс для SAT-решателей на основе технологии JNI // Сборник тезисов докладов конгресса молодых ученых. Электронное издание. СПб: Университет ИТМО, 2020. URL: https://kmu.itmo.ru/digests/article/4456 (дата обр. 17.06.2020).