МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АНГАРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИНСТИТУТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И МАТЕМАТИЧЕСКОЙ ГЕОФИЗИКИ СО РАН

НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ИССЛЕДОВАНИИ СЛОЖНЫХ СТРУКТУР

МАТЕРИАЛЫ ЧЕТЫРНАДЦАТОЙ МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ 19–24 сентября 2022 г.

Томск
Издательский Дом Томского государственного университета
2022

В работе [6] предложен алгоритм исключения переменной из КНФ Цейтина, основанный на исключении входов элементов (или самих элементов) из схемы. Таким образом, становится возможным получение новой КНФ Цейтина, соответствующей функции с исключённой переменной.

В данной работе предлагается совмещение предложенных ранее алгоритмов с целью получения КНФ Цейтина, каждое решение которой представляет собой как минимум одну тестовую пару для обнаружения неисправности задержки пути. Получение нескольких тестовых пар для одного пути целесообразно в случаях, когда необходимо построение тестовых последовательностей с низкой потребляемой мощностью [4], поскольку в этом случае требуется получение интервалов, порождающих тестовые пары. За счёт пересечения интервалов различных путей и задания необходимых значений неопределённым компонентам интервалов возможно получение тестовых последовательностей с минимально возможной потребляемой мощностью для её фрагментов. Кроме того, предложенный подход позволяет осуществлять получение тестовых пар для схем, размер которых не позволяет представить их функции в виде ROBDD-графов ввиду возможности экспоненциального роста числа вершин получаемых графов.

Литература

1. *Lyu Y, Mishra P.* Automated Test Generation for Trojan Detection using Delay-based Side Channel Analysis // DATE '20: Proceedings of the 23rd Conference on Design, Automation and Test in Europe. – San Jose: EDA Consortium, 2020. – P. 1031–1036.
2. *I. Exurville, L. Zussa, J. Rigaud and B. Robisson,* Resilient hardware Trojans detection based on path delay measurements // 2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). – New-York: IEEE, 2015. – P. 151–156.
3. *Matrosova A.Yu., Andreeva V.V., Nikolaeva E.A.* Finding Test Pairs for PDFs in Logic Circuits Based on Using Operations on ROBDDs // Russian Physics Journal. – 2018. – Vol. 61, № 5. – P. 994–999.
4. *Матросова А.Ю., Тычинский В.З., Андреева В.В.* Построение тестовых последовательностей для робастно тестируемых неисправностей задержек путей с низкой потребляемой мощностью с использованием SAT-решателей и ROBDD-графов // Проблемы разработки перспективных микро- и наноэлектронных систем (МЭС). – 2020. – № 2. – С. 43–49.
5. *Цейтин Г. С.* О сложности вывода в исчислении высказываний // Записки научных семинаров ЛОМИ АН СССР. – 1968. – Т. 8. – С. 234–259.
6. *Тычинский В.З.* Метод исключения переменной из КНФ Цейтина // Материалы VIII Международной молодежной научной конференции «Математическое и программное обеспечение информационных, технических и экономических систем» / под ред. И.С. Шмырина. – Томск: Изд-во Том. гос. ун-та, 2021. – С. 223–228.

ЭКСПЕРИМЕНТАЛЬНОЕ СРАВНЕНИЕ МЕТОДОВ ПРОВЕРКИ ЭКВИВАЛЕНТНОСТИ РАСШИРЕННЫХ ПОЛУАВТОМАТОВ

А.В. Лапутенко[1], Е.М. Винарский[2, 3], А.С. Твардовский[1]

[1] Томский государственный университет, Томск, Россия
[2]Высшая школа экономики, Москва, Россия
[3]Институт системного программирования РАН им.В.П.Иванникова, Москва, Россия
laputenko.av@gmail.com, vinevg2015@gmail.com, tvardal@mail.ru

EXPERIMENTAL COMPARISON OF EQUIVALENCE CHECKING METHODS FOR EXTENDED AUTOMATA

A.V. Laputenko[1], E.M. Vinarskii[2, 3], A.S. Tvardovskii[1]

[1]Tomsk State University, Tomsk, Russia
[2]Higher School of Economics, Moscow, Russia
[3]Ivannikov Institute for System Programming of the RAS, Moscow, Russia

Одной из классических задач анализа в теории полуавтоматов является проверка эквивалентности [1]. Формально, конечным полуавтоматом является кортеж $\mathbf{M} = (S, A, h, s_0, F)$, где S – конечное множество состояний с выделенным начальным состоянием s_0 и принимающими состояниями $F \subseteq S$, A – конечный входной алфавит, $h \subseteq S \times A \times S$ – отношение переходов. При моделировании ряда современных систем, модель конечного полуавтомата часто расширяется контекстными переменными, а также связанными с ними предикатами на переходах вида $x \bullet const$, где $\bullet \in \{>, \leq, <, \geq, ==\}$, и функциями обновления $x := const$ и $x := x * const$, где $* \in \{+, -\}$. Таким образом, вводится понятие *расширенного полуавтомата*, переходы которого выполняются лишь при истинности соответствующего предиката, при этом контекстные переменные обновляются в соответствии с функциями обновления. Однако, при расширении модели двумя контекстными переменными данная задача становится алгоритмически неразрешимой [1]. В связи с этим, исследования в данной области направлены на разработку приближённых алгоритмов проверки эквивалентности.

В данной работе были рассмотрены две группы приближённых подходов к проверке эквивалентности расширенных полуавтоматов, основанные на использовании классической абстракции (l-эквивалента),

поведение которой совпадает с таковым для исходного полуавтомата для всех последовательностей длины не больше *l*. Идея подходов первой группы заключается в построении для абстракции расширенного полуавтомата некоторого конечного множества трасс и поиске в нем трассы, принимаемой одним полуавтоматом и не принимаемой другим, эквивалентность которого первому полуавтомату требуется проверить. В качестве множества таких трасс были рассмотрены последовательности, полученные обходом графа переходов классического полуавтомата, а также, все простые пути из начального состояния в любое из финальных состояний. Ко второй группе подходов относится проверка свойств исследуемых автоматов с использованием верификаторов. В логике линейного времени (LTL) формулируется свойство, согласно которому любое из финальных состояний в каждом из полуавтоматов достигается одновременно при выполнении любой входной трассы. В настоящей работе использовался верификатор Spin [2], который позволяет проверять требования, заданные в виде LTL-формул для систем, описанных на языке Promela.

Экспериментальная оценка предложенных подходов проводилась для случайно сгенерированных расширенных полуавтоматов в двух сериях экспериментов. Рассматривались полуавтоматы с числом состояний от 3 до 6, двумя входными символами и двумя целочисленными контекстными переменными. Предикаты и функции обновления задавались в соответствии с данным выше определением, в то время как входящие в них константы ограничивались диапазоном {1..5}. Абстракции расширенных автоматов с n состояниями строились до длины $l = n+1$, т.е. множество допустимых последовательностей длины не больше $n+1$ совпадали для расширенного полуавтомата и его абстракции.

В первой серии экспериментов проверка эквивалентности проводилась для двух случайно сгенерированных полуавтоматов. Во второй серии проверка эквивалентности проводилась для каждого случайно сгенерированного полуавтомата и его изменённой копии, полученной изменением предиката на одном из переходов. В каждой серии из случайно сгенерированных полуавтоматов отбирались те пары, для которых проверка формулы с помощью Spin показала неэквивалентность. В результате, для 758 пар полуавтоматов первой серии экспериментов подход на основе обхода графа переходов позволил определить неэквивалентность в 98.8% случаев; с помощью последовательностей, соответствующих простым путям – в 100%. Для 182 пар полуавтоматов второй серии экспериментов соответствующие результаты составили 36.8% и 44%. Таким образом, согласно проведенным экспериментам, обход графа переходов *l*-эквивалента позволяет эффективно выполнять проверку эквивалентности расширенных полуавтоматов, не прибегая к построению и перебору большого числа других последовательностей, например, всевозможных простых путей в полуавтомате. Дальнейшая работа может быть направлена на оценку предложенного подхода для полуавтоматов с большим числом различных предикатов и функций обновления, а также, рассмотрение других способов построения проверяющих последовательностей.

Литература

1. *Минский М.* Вычисления и автоматы. – М.: Мир, 1971. – 360 с.
2. *Spin* [Электронный ресурс]. – URL: https://spinroot.com/ (дата обращения: 13.07.2022).

ИСПОЛЬЗОВАНИЕ КОНЕЧНО-АВТОМАТНЫХ АБСТРАКЦИЙ ПРИ РЕШЕНИИ ЗАДАЧ АНАЛИЗА И СИНТЕЗА ДЛЯ ВРЕМЕННЫХ АВТОМАТОВ

А.С. Твардовский[1], *Н.В. Евтушенко*[2]

[1] Томский Государственный университет, Томск, Россия
[2]Институт системного программирования РАН, Москва, Россия
tvardal@mail.ru, evtushenko@ispras.ru

SOLVING ANALYSIS AND SYNTHESIS PROBLEMS FOR TIMED FINITE STATE MACHINES BASED ON THEIR FSM ABSTRACTIONS

A.S. Tvardovskii[1], *N.V. Yevtushenko*[2]

[1]Tomsk State University, Tomsk, Russia
[2]Ivannikov Institute for System Programming of the RAS, Moscow, Russia

Исследования в области анализа и синтеза конечных автоматов проводятся с середины прошлого века [1]. Полученные результаты используются при синтезе компонентов программного и аппаратного обеспечения с требуемыми свойствами, при решении задач оптимизации, тестирования и верификации дискретных систем и др. При моделировании современных систем часто приходится учитывать временные аспекты в их поведении, такие, например, как таймауты в телекоммуникационных протоколах. Соответственно, для их исследования вводится понятие временного автомата, который отличается от классического наличием временной переменной и расширений в виде таймаутов и временных ограничений. При решении задач анализа и синтеза временных автоматов достаточно часто строятся конечно-автоматные абстракции, для которых применяются известные