

Decidability of Parameterized Verification

Synthesis Lectures on Distributed Computing Theory

Editor

Jennifer Welch, *Texas A&M University*

Nancy Lynch, *Massachusetts Institute of Technology*

Synthesis Lectures on Distributed Computing Theory is edited by Jennifer Welch of Texas A&M University and Nancy Lynch of the Massachusetts Institute of Technology. The series publishes 50- to 150-page publications on topics pertaining to distributed computing theory. The scope largely follows the purview of premier information and computer science conferences, such as ACM PODC, DISC, SPAA, OPODIS, CONCUR, DialM-POMC, ICDCS, SODA, Sirocco, SSS, and related conferences. Potential topics include, but not are limited to: distributed algorithms and lower bounds, algorithm design methods, formal modeling and verification of distributed algorithms, and concurrent data structures.

[Decidability of Parameterized Verification](#)

Roderick Bloem, Swen Jacobs, Ayrat Khalimov, Igor Konnov, Sasha Rubin, Helmut Veith, and Josef Widder

2015

[Impossibility Results for Distributed Computing](#)

Hagit Attiya and Faith Ellen

2014

[Distributed Graph Coloring: Fundamentals and Recent Developments](#)

Leonid Barenboim and Michael Elkin

2013

[Distributed Computing by Oblivious Mobile Robots](#)

Paola Flocchini, Giuseppe Prencipe, and Nicola Santoro

2012

[Quorum Systems: With Applications to Storage and Consensus](#)

Marko Vukolic

2012

[Link Reversal Algorithms](#)

Jennifer L. Welch and Jennifer E. Walter

2011

Cooperative Task-Oriented Computing: Algorithms and Complexity

Chryssis Georgiou and Alexander A. Shvartsman

2011

New Models for Population Protocols

Othon Michail, Ioannis Chatzigiannakis, and Paul G. Spirakis

2011

The Theory of Timed I/O Automata, Second Edition

Dilsun K. Kaynar, Nancy Lynch, Roberto Segala, and Frits Vaandrager

2010

Principles of Transactional Memory

Rachid Guerraoui and Michal Kapalka

2010

Fault-tolerant Agreement in Synchronous Message-passing Systems

Michel Raynal

2010

Communication and Agreement Abstractions for Fault-Tolerant Asynchronous Distributed Systems

Michel Raynal

2010

The Mobile Agent Rendezvous Problem in the Ring

Evangelos Kranakis, Danny Krizanc, and Euripides Markou

2010

© Springer Nature Switzerland AG 2022

Reprint of original edition © Morgan & Claypool 2015

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopy, recording, or any other except for brief quotations in printed reviews, without the prior permission of the publisher.

Decidability of Parameterized Verification

Roderick Bloem, Swen Jacobs, Ayrat Khalimov, Igor Konnov, Sasha Rubin, Helmut Veith, and Josef Widder

ISBN: 978-3-031-00883-2 paperback

ISBN: 978-3-031-02011-7 ebook

DOI 10.1007/S00658ED1V01Y201508DCT013

A Publication in the Springer series

SYNTHESIS LECTURES ON DISTRIBUTED COMPUTING

THEORY

Lecture #13

Series Editors: Jennifer Welch, *Texas A&M University*

Nancy Lynch, *Massachusetts Institute of Technology*

Series ISSN

Print 2155-1626 Electronic 2155-1634

Decidability of Parameterized Verification

Roderick Bloem and Ayrat Khalimov

Graz University of Technology, Austria

Swen Jacobs

Graz University of Technology, Austria

Saarland University, Saarbrücken, Germany

Igor Konnov, Helmut Veith, and Josef Widder

Vienna University of Technology, Austria

Sasha Rubin

University of Naples “Federico II”, Italy

SYNTHESIS LECTURES ON DISTRIBUTED COMPUTING THEORY #13

ABSTRACT

While the classic model checking problem is to decide whether a finite system satisfies a specification, the goal of parameterized model checking is to decide, given finite systems $\mathbf{M}(n)$ parameterized by $n \in \mathbb{N}$, whether, for all $n \in \mathbb{N}$, the system $\mathbf{M}(n)$ satisfies a specification. In this book we consider the important case of $\mathbf{M}(n)$ being a concurrent system, where the number of replicated processes depends on the parameter n but each process is independent of n . Examples are cache coherence protocols, networks of finite-state agents, and systems that solve mutual exclusion or scheduling problems. Further examples are abstractions of systems, where the processes of the original systems actually depend on the parameter.

The literature in this area has studied a wealth of computational models based on a variety of synchronization and communication primitives, including token passing, broadcast, and guarded transitions. Often, different terminology is used in the literature, and results are based on implicit assumptions. In this book, we introduce a computational model that unites the central synchronization and communication primitives of many models, and unveils hidden assumptions from the literature. We survey existing decidability and undecidability results, and give a systematic view of the basic problems in this exciting research area.

KEYWORDS

parametrized model checking, concurrent systems, distributed systems, formal verification, model checking, decidability, cutoffs

Contents

	Acknowledgments	xi
1	Introduction	1
1.1	Motivation	2
1.2	Who Should Read This Book?	4
1.3	Organization of the Book	4
2	System Model and Specification Languages	5
2.1	Preliminary Terminology and Definitions	5
2.2	System Model	6
2.2.1	Some Standard Synchronization Primitives	9
2.2.2	Runs and Deadlocks	12
2.3	Parameterized Family of Uniform Concurrent Systems	13
2.4	Parameterized Specifications	13
2.4.1	Indexed Temporal Logics	14
2.4.2	Action-based Specifications	18
2.4.3	Specifications in the Literature	18
2.5	Model Checking Problems for Concurrent Systems	19
2.5.1	Computability Assumptions	20
3	Standard Proof Machinery	23
3.1	Techniques to Prove Undecidability of PMCP	23
3.2	How to Prove Decidability of the PMCP	24
3.2.1	Well-structured Transition Systems	25
3.2.2	Vector Addition Systems with States (and Petri Nets)	27
3.2.3	Decompositions and Cutoffs	28
4	Token-passing Systems	31
4.1	System Model	32
4.1.1	Direction-aware Parameterized Systems	32
4.1.2	Token-passing Systems	34
4.2	Results for Direction-unaware Token-passing Systems	37

4.2.1	Decidability for Simple Token-passing in Uni-directional Rings	38
4.2.2	Decidability for Simple Token-passing in Graphs	40
4.2.3	Undecidability Results for Multi-valued Tokens	42
4.3	Results for Direction-aware Token-passing Systems	44
4.3.1	Cutoffs for Change-bounded Tokens in Bi-directional Rings	44
4.3.2	Undecidability for Direction-aware TPSs	45
4.4	Discussion	46
4.4.1	Variations of the Model	48
5	Rendezvous and Broadcast	51
5.1	System Model	51
5.2	Decidability Results	55
5.2.1	Counter Representation	55
5.2.2	Decidability for All Three Primitives	58
5.2.3	Decidability for Pairwise Rendezvous	58
5.3	Undecidability Results	59
5.3.1	Undecidability for Broadcast	59
5.3.2	Undecidability for Asynchronous Rendezvous	62
5.4	Discussion	62
5.4.1	Variations of the Model	64
6	Guarded Protocols	65
6.1	Motivating Example	65
6.2	System Model	69
6.2.1	Classes of Guarded Protocols	73
6.2.2	Specifications	74
6.3	Undecidability: Boolean and Conjunctive Guards	76
6.4	Decidability: Init-Conjunctive and Disjunctive Guards	81
6.4.1	Preliminaries	82
6.4.2	Proof Schemas	84
6.4.3	Init-conjunctive Guards	86
6.4.4	Disjunctive Guards	89
6.5	Disjunctive Guards vs. Rendezvous	96
6.6	Variations on the Model: Guards and Synchronization Primitives	99
6.7	Discussion	100

7	Ad Hoc Networks	103
7.1	Running Example	103
7.2	System Model	104
7.3	PMC Problems for Ad Hoc Networks	105
7.4	Parameterized Connectivity Graphs $\mathbf{BP_k}$, $\mathbf{BPC_k}$, $\mathbf{BD_k}$, \mathbf{C} , \mathbf{All}	107
7.5	Results for (Non-lossy) AHNs	108
7.5.1	Undecidability Results for (Non-lossy) AHNs	108
7.5.2	Decidability Results for (Non-lossy) AHNs	116
7.6	Decidability Results for Lossy Ad Hoc Networks	123
7.7	Discussion	127
7.7.1	Variations of the Model	128
8	Related Work	129
8.1	Abstraction Techniques	129
8.2	Regular Model Checking	131
8.3	Symbolic Techniques	132
8.4	Dynamic Cutoff Detection	134
8.5	Network Invariants	135
8.6	Invisible Invariants	137
8.7	Other Aspiring Approaches	137
9	Parameterized Model Checking Tools	139
10	Conclusions	143
	Bibliography	145
	Authors' Biographies	157

Acknowledgments

We are grateful to Paul Attie, Giorgio Delzanno, Sayan Mitra, and Kedar Namjoshi for carefully reading an earlier draft of this manuscript, and providing detailed and constructive comments.

Supported by the Austrian National Research Network RiSE (S11403, S11405, S11406) and project PRAVDA (P27722) of the Austrian Science Fund (FWF), by the Vienna Science and Technology Fund (WWTF) through grant PROSEED, by the German Research Foundation (DFG) through SFB/TR 14 AVACS and project ASDPS (JA 2357/2-1), and by the Istituto Nazionale di Alta Matematica through INdAM-COFUND-2012, FP7-PEOPLE-2012-COFUND (Proj. ID 600198).

Roderick Bloem, Swen Jacobs, Ayrat Khalimov, Igor Konnov, Sasha Rubin, Helmut Veith, and Josef Widder
August 2015