Comparative Evaluation and Improvement of Computational Approaches to Reachability Analysis of Linear Hybrid Systems

Von der Fakultät für Mathematik, Informatik und Naturwissenschaften der RWTH Aachen University zur Erlangung des akademischen Grades einer Doktorin der Ingenieurwissenschaften genehmigte Dissertation

vorgelegt von

Diplom-Informatikerin
Ibtissem Ben Makhlouf
aus
Djerba / Tunesien

Berichter: Universitätsprofessor Dr.-Ing. Stefan Kowalewski
Universitätsprofessor Dr. Goran Frehse

Tag der mündlichen Prüfung: 26. Januar 2016

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über `http://dnb.d-nb.de` abrufbar.

Zugl.: D 82 (Diss. RWTH Aachen University, 2016)

Ibtissem Ben Makhlouf
Lehrstuhl Informatik 11 - Embedded Software
`makhlouf@embedded.rwth-aachen.de`

Aachener Informatik Bericht AIB-2016-2

Herausgeber: Fachgruppe Informatik
RWTH Aachen University
Ahornstr. 55
52074 Aachen
GERMANY

ISSN 0935-3232

Printed in Germany.

ISBN 978-3-8440-4376-1

Shaker Verlag GmbH, Postfach 101818, 52018 Aachen
Telefon: 02407/9596-0, Telefax: 02407/9596-9
Internet: `www.shaker.de`, E-Mail:`info@shaker.de`

Acknowledgments

I would like to express my special appreciation and heartfelt gratitude to my advisor Professor Stefan Kowaleswki, you have been a great mentor for me. I would like to thank you for supporting my research and for allowing me to grow as a research scientist. Your advice on both research as well as on my career has been priceless. Your moral support and understanding of my particular situation has helped me a lot through the course of my thesis. I hope that my work lived up to some of your expectations.

I would also like to thank, Prof. Erika Abraham, Prof. Thomas Seidl, Dr. Goran Frehse for taking their time to serve on my thesis committee. I also want to thank you for letting my defense be an enjoyable moment, and for your brilliant comments and suggestions. Erika and Goran, it has been a great pleasure for me to discuss and exchange thoughts with you.

I would especially like to thank Prof. Lars Grüne, Prof. Matthias Althoff, Dr. André Platzer, Dr. Stefan Matthias Ratschan, Dr. Colas Le Guernic for the precious support. You have always been ready to response quickly to my questions.

This dissertation could not have been completed without the great support that I have received from my students Norman Hansen, Jonathan Gan and Malte Neuss.

Special thanks goes to Prof. Wolfgang Thomas, Helen Bolke-Hermanns and the AlgoSyn group for the financial support and for allowing me to be a member of your group.

Furthermore, I would like to thank my colleagues at the Informatik 11 - Embedded Systems Institute for creating a friendly environment, for the stimulating discussions, for the creative power and the quality of the team dynamics.

I would like to thank my former supervisor Prof. Meriem Jaidane. My work with you has helped to develop my fascination towards research.

I wish to offer my most heartfelt thanks to Dr. Eva M. Navarro-López. I have always been able to turn to you when I needed a listening ear and a dissenting opinion. You have become one of my best friends. We have supported and helped each other through both good times and bad times. Our online discussions in various research directions were a great source of inspiration.

A special thanks to my family. I have an amazing family, unique in many ways. Your support has been unconditional all these years. You have given up many things for me to finally attain this longstanding goal. Thank you Raid, Rim and Rashid for your never ending patience and support.

Words cannot express how grateful I am to my husband Dr. Adel Mhamdi for all the love and support throughout the past few years. Thank you for pushing me to gain more self-confidence and self-belief in dealing with such a difficult topic. You were, in some way, my second advisor. Your knowledge and constant guidance have helped me a long way towards completing this thesis.

Particular thanks to my mother for all of the sacrifices. Your prayer for me was what sustained me thus far. And to my dad. I wish you were here. But you know a great part of you is in me. You taught me that hard work pays off. I feel so very grateful for all your love that I received.

Finally, would like to thank my sister, my brothers and all of my friends who supported me by striving towards my goal.

Ibtissem Ben Makhlouf
Aachen, March 2016

Zusammenfassung

Diese Dissertation befasst sich mit dem Problem der Erreichbarkeitsanalyse, fokussiert auf lineare hybride Systeme. Hybride Systeme sind eine Mischung von kontinuierlichen und diskreten Verhalten. Ein hybrider Automat, bestehend aus einem Graph, in dem die Knoten das kontinuierliche und die Kanten das diskrete Verhalten beschreiben, bietet sich als das passende formale Modell für solche Systeme an. Es besteht aus einen Formalismus, das Differentialgleichungen und logische Ausdrücke im gleichen Rahmen umfasst und damit neue Horizonte für die Forschung und Entwicklung, vor allem in Richtung neuer Methoden und neuer Algorithmen, eröffnet. Trotz des Fortschrittes, der in den letzten Jahren zu verzeichnen war, gibt es vor allem in Hinsicht auf die praktische Anwendung noch viele offene Fragen. Begonnen haben wir diese Arbeit mit der Bewertung einiger Verifikationstools. Speziell für diese Aufgabe wurde eine Reihe von Benchmarks erdacht und zusammengefasst. Die Benchmarks besitzen besondere Eigenschaften in Bezug auf die Prüfung der Effizienz, Anwendbarkeit, Skalierbarkeit und Leistungsfähigkeit dieser Tools. Wir geben einen ausführlichen Überblick über bestehende Methoden zum Berechnen einer Überapproximation der erreichbaren Mengen für lineare zeitinvariante hybride Systeme. Dieser erfasst unterschiedliche Ansätze für die Berechnung einer Überapproximation für die kontinuierliche Dynamik mit und ohne Invarianten sowie auch für die Berechnung der Schnittmenge bei Übergängen. Basierend auf diesen Ergebnissen wurden neue Approximationsmethoden zur Berechnung der erreichbaren Mengen für den kontinuierlichen Teil als auch für den diskreten Teil des hybriden Automaten sowie eine modulare skalierbare Implementierung verschiedene Ansätze vorgeschlagen. Für diese Implementierungen werden zuerst Stützfunktionen und danach Zonotopen verwendet. Für die jeweiligen geometrischen Darstellungen wurde eine Reihe von verschiedenen Ansätzen für den Umgang mit Invarianten, Sprungbedingungen und Transitionen vorgestellt. Zwei Tools sind daraus entstanden. Beide Tools integrieren die oben beschriebenen Methoden und erlauben möglicher Kombinationen. Sie verfügen über eine GUI und ermöglichen eine vom Benutzer konfigurierbare Erreichbarkeitsanalyse. Beide Tools wurden zur Durchführung eines Leistungsvergleiches verschiedener Methoden verwendet. Einen Zusammenhang zwischen diesen Leistungen und die Komplexität der Benchmarks wurde dabei festgestellt. Die Studie mit den vorgeschlagenen Benchmarks führte zu dem Ergebnis, dass der Unterschied zwischen Methoden in Bezug auf die Genauigkeit der Überapproximation und die Rechenzeit unbedeutend ist. Um die Vielfältigkeit der Anwendbarkeit der Erreichbarkeitsanalyse zu veranschaulichen, kam es zum Vorschlag einer vernetzten Fahrzeugkolonne. Zuerst wurde die Analyse verwendet, um sichere und kurze Abständen zwischen Fahrzeugen in einer LMI-geregelten Kolonne zu bestimmen. Nachfolgend wurde eine Erreichbarkeitsanalyse durchgeführt um bei der Entscheidung über den leistungsfähigsten H_2- or H_∞-Regler der gleiche Kolonne zu unterstützen. Sie wurde außerdem eingesetzt um zeitkritische Bedingungen für eine Kreuzung mit einer annähernden Kolonne zu bestimmen und damit den Verkehr innerhalb der Kreuzung sicher zu verwalten.

Abstract

This thesis addresses the problem of reachability analysis with the focus on linear hybrid systems. Hybrid systems are a mixture of continuous and discrete behaviors. The Hybrid automaton consisting of a graph, in which the locations describe the continuous and the transitions the discrete behavior, represents the best formal model for such kind of systems. It provides a formalism integrating differential equations and logic expressions in a same framework, thus opening new horizons in research and development of new methods and novel algorithms. Despite recent progress made in this field in the last years, actual verification methods and available tools have exhibited their shortcomings.

We started this work with the assessment of some verification tools using a suite of benchmarks conceived specially for this task. The benchmarks possess particular characteristics for testing of efficiency, applicability, scalability, capability and performances of these tools.

We offer a theoretical overview of existing methods for computing an overapproximation of reachable sets for linear time invariant hybrid systems. This covers approaches for overapproximating reachable sets of the continuous dynamics with and without invariants as well as methods for solving the problem of guard intersection at transitions. We furthermore propose new overapproximation techniques for treating the continuous part as well as the discrete part of the hybrid automaton. We suggest scalable, modular implementations of these diverse methods allowing thereby possible combinations between them first using support functions and then with zonotopes. The implementations include different approaches for handling invariants, guards and transitions for the above-mentioned set representations. Two toolboxes are the results of this implementation effort. Both tools integrate the methods described above. They offer a GUI and allow for a user-configurable reachability analysis. We use both tools to carry out a performance comparison of different methods. We note thereby that there is a correlation between these performances and the complexity of the tested example. However, we note during this survey using the proposed benchmark suite that the difference in the performance with regards to the tightness of the over-approximation and the computation time is not so crucial for low dimensional systems.

We propose a networked platoon of vehicles to demonstrate different context where reachability analysis can be useful. We first perform a reachability analysis to determine unsafe gaps between the vehicles which are controlled using LMI-formalism. Reachability analysis can be helpful for control design. The choice between controllers on the basis of reachability results has led to controller ensuring the best compromise between safe and small gaps when applying H_2 or H_∞ control design techniques. Reachability can also be used to determine time-critical conditions. As demonstration, we opt for a platoon approaching an intersection.

Contents

1 Introduction **1**

1.1 Motivation and Objectives 3
1.2 Contributions 4
1.3 Outline 5
1.4 Bibliographic Notes 6

2 Assessment and Performance Comparison of Tools **9**

2.1 Introduction 9
2.2 Benchmarks 10
2.3 Description of Tools 11
2.3.1 SpaceEx: The PHAVer and the LGG Scenarios 11
2.3.2 KeYmaera 13
2.3.3 HSolver 14
2.3.4 iSAT 15
2.4 Results 16
2.4.1 SpaceEx 18
2.4.2 KeYmaera 25
2.4.3 HSolver 27
2.4.4 iSAT 28
2.4.5 Performance Evaluation 28
2.5 Conclusion 31

3 Overview of Methods for Computing Reachable Sets of Linear Hybrid Systems **33**

3.1 Introduction 33
3.2 Hybrid Automaton 34
3.3 Run Semantics 35
3.4 Reachable State within a Discrete Mode 36
3.5 Reachable Set of LTI-Systems 38
3.6 Computing an Over-approximation of the Input Contribution 39
3.6.1 Norm-bounded Uncertain Input 40
3.6.2 Bounded Uncertain Input 40
3.6.3 Toward a Tighter Approximation of the Input Contribution . 40
3.6.4 Input Constant within a Time Step 41

3.7 Computing an Over-approximation Ω_0 of $\mathcal{R}_{[0,r]}(X_0)$ 42
3.7.1 Using a Bloating Factor α_r [47] 42
3.7.2 Alternative Approach for Computing a Bloating Factor α_r [73] 43
3.7.3 Toward a Tighter Approximation of the Initial Set [71] 43
3.7.4 Forward and Backward Approximations for Computing an Over-approximation of the Initial Set [44, 96] 44
3.8 Handling Invariants Inside Discrete Modes 44
3.8.1 Handling Invariants as Guards 46
3.8.2 Recursive Scheme with Invariants [71] 46
3.9 Handling Transitions 49
3.10 Conclusion 51

4 Support Function Technique for Computing Reachable Sets 53
4.1 Introduction 53
4.2 Definition and Properties of Support Functions/Support Vectors . . 54
4.3 Computation of the Reachable Set within a Continuous Mode 59
4.3.1 Approximation of the Input Contribution 61
4.3.2 Initial Set Over-approximation Scenarios 62
4.3.3 Impact of the Approximation Method of the Initial Set on the Tightness of the Reachable Set 64
4.4 Collision Detection Between Two Convex Sets 68
4.5 Intersection Computation of Two Convex Sets 69
4.6 Intersection with Hyperplanes or Halfspaces 70
4.6.1 From n to 2 Dimension and the Dichotomous Search 70
4.6.2 The Sandwich Algorithm 74
4.6.3 Optimization Techniques 82
4.7 Handling Invariants with Support Function Techniques 85
4.7.1 Classical Method for Handling Invariants 85
4.7.2 Recursive Scheme Fusing Reachable Sets with Domain/Invariant Conditions 86
4.8 Handling Guards 90
4.9 Simultaneously Handling of Invariants and Guards 90
4.10 Handling Spontaneous Transitions 91
4.11 Handling Time-Triggered Transitions 92
4.12 MATLAB/Simulink Implementation 92
4.13 Experimentation 96
4.14 Conclusion 104

5 Zonotopic Approximation for Computing Reachable Sets 107
5.1 Introduction 107
5.2 Zonotopes 108
5.3 Properties and Geometric Operations of Zonotopes 109
5.4 Zonotope/Hyperplane Intersection 111
5.4.1 Intersection Check Between a Zonotope and a Hyperplane . . 111

5.4.2 From Dimension n to Dimension 2 112
5.4.3 Zonotope/Strip Intersection 122
5.4.4 Zonotope/Hyperplane Intersection using Singular Value Decomposition (SVD) 123
5.4.5 Comparison of Zonotope/Hyperplane Intersection Methods . 124
5.5 Zonotope/Halfspace Intersection 127
5.6 Zonotope/Polyhedron Intersection 128
5.7 Zonotope/Zonotope Intersection 128
5.7.1 Zonotope/Zonotope Collision Detection 129
5.7.2 Intersection of Two Zonotopes using Optimization Techniques 134
5.7.3 Intersection of Two Zonotopes using SVD 135
5.7.4 Comparison of Both Zonotope/Zonotope Intersection Methods 136
5.8 Computing Reachable Sets within Discrete Modes 137
5.9 Handling Invariants 139
5.10 Handling Transitions 139
5.10.1 Taking the First Intersection 140
5.10.2 The Over-approximative Convex Hull Method 141
5.10.3 Pre- and Post-clustering 141
5.10.4 Finding the Min/Max at a Guard Transition 141
5.10.5 Fixpoint-/Time-Triggered Transition 141
5.11 Implementation 142
5.12 Experimental Results and Performance Evaluation 143
5.12.1 Comparison of Intersection Methods 143
5.12.2 Experimental Evaluation at Guard Intersection 145
5.12.3 Handling Invariant 151
5.13 Conclusion 151

6 Reachability Analysis of a Networked Platoon of Trucks 153
6.1 Introduction 153
6.2 Description of a Networked Cooperative Platoon 153
6.2.1 Platoon Model 153
6.3 Information Flow and Interconnection Topology 155
6.4 Control Design 156
6.5 LMI-based Control 157
6.5.1 Hybrid Modeling 158
6.5.2 Safety Verification of the LMI-based Controlled Platoon . . . 159
6.6 H_2/H_∞-based Control 164
6.6.1 Reachability Analysis 172
6.7 Managing Platoons at Intersections 176
6.7.1 The Intersection Infrastructure 177
6.7.2 The Intersection Model 178
6.7.3 Reachability using Zonotopes 178
6.8 Conclusion 183

7 Conclusion **185**

A Appendix A **189**
A.1 Infinity test 189
A.2 The Bouncing Ball Example 189
A.3 The Colliding Masses Benchmark 190
A.4 The Transient in Flower Benchmark 190
A.5 The Two-Tank Benchmark 191
A.6 The Navigation Benchmark 193
A.7 The Heating Benchmark 195
A.8 Cooperative Platoon of Trucks 197
A.8.1 Platoon under full communication (single mode) 198
A.8.2 Platoon under a dropout of communication (2 modes) 198
A.9 A Five Dimensional Linear Switching System (5D LSS) 199

B Appendix B **201**
B.1 Proof of Lemma 1: Norm-bounded uncertain input 201
B.2 Proof of Lemma 3: Toward a tighter approximation of the input contribution 201
B.3 Proof of Lemma 4 203
B.4 Proof of Lemma 3.7.3 204