



Universiteit
Leiden
The Netherlands

Modelling and analysis of real-time coordination patterns

Kemper, S.

Citation

Kemper, S. (2011, December 20). *Modelling and analysis of real-time coordination patterns*. IPA Dissertation Series. BOXPress BV, 2011-24. Retrieved from <https://hdl.handle.net/1887/18260>

Version: Corrected Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/18260>

Note: To cite this publication please use the final published version (if applicable).

Modelling and Analysis of Real-Time Coordination Patterns

Stephanie Kemper

Modelling and Analysis of Real-Time Coordination Patterns

PROEFSCHRIFT

ter verkrijging van

de graad van Doctor aan de Universiteit Leiden

op gezag van Rector Magnificus prof. mr. P.F. van der Heijden,

volgens besluit van het College voor Promoties

te verdedigen op dinsdag 20 december 2011

klokke 11:15 uur

door

Stephanie Kemper

geboren te Bremerhaven, Duitsland, in 1979

Promotiecommissie

Promotoren:	Prof. Dr. F.S. de Boer	Universiteit Leiden
	Prof. Dr. F. Arbab	Universiteit Leiden
Overige Leden:	Prof. C. Baier	Technische Universität Dresden
	Dr. E.P. de Vink	Technische Universiteit Eindhoven
	Prof. Dr. J.N. Kok	Universiteit Leiden
	Prof. Dr. J.J.M.M Rutten	Radboud Universiteit Nijmegen
	Dr. M. Bonsangue	Universiteit Leiden
	Dr. A. Silva	Radboud Universiteit Nijmegen



The work in this thesis has been carried out at the Centrum Wiskunde & Informatica (CWI), and under the auspices of the research school IPA (Institute for Programming research and Algorithmics). The research was partially funded by the Netherlands Organisation for Scientific Research (NWO) under the BRICKS project (Basic Research in Informatics for Creating the Knowledge Society).

Copyright ©2011 by Stephanie Kemper

Cover design by Nils Kemper.

Printed and published by Boxpress BV || Proefschriftmaken.nl

ISBN: 978-90-8891-360-0

IPA Dissertation Series 2011-24

Contents

Contents	i
1 Introduction	1
1.1 Contents and Structure of this Thesis	2
1.2 Origin of Material and Main Contributions	4
2 System Models	7
2.1 Preliminaries	8
2.1.1 Time	8
2.1.2 Data	10
2.2 Timed Automata	11
2.2.1 Syntax of Timed Automata	12
2.2.2 Semantics of Timed Automata	13
2.2.3 Systems of Timed Automata	15
2.2.4 Discussion	16
2.3 Timed Constraint Automata	18
2.3.1 Syntax of Timed Constraint Automata	19
2.3.2 Semantics of Timed Constraint Automata	22
2.3.3 Systems of Timed Constraint Automata	24
2.3.4 Discussion	27
2.4 Timed Network Automata	28
2.4.1 Syntax of Timed Network Automata	29
2.4.2 Semantics of Timed Network Automata	32
2.4.3 Systems of Timed Network Automata	33
2.4.4 Discussion	40
2.5 Conclusion	41
3 SAT-based Verification	43
3.1 Formula Representation	44
3.1.1 Preliminaries	44
3.1.2 Timed Automata	46
3.1.3 Timed Constraint Automata	49

3.1.4	Timed Network Automata	53
3.2	Bounded Model Checking	57
3.2.1	Notations	57
3.2.2	Unfolding for BMC	58
3.2.3	BMC of Properties	59
3.2.4	Completeness of BMC	59
3.2.5	Correctness	61
3.3	Discussion	61
3.3.1	Occurrence of Actions on Transitions of TA	61
3.3.2	Choice of Variable Types	61
3.3.3	Temporal Difference Encoding of Clocks	62
3.3.4	Linear Boolean Encoding of Finite Sets	63
3.3.5	Encoding of Transitions	64
3.4	Conclusion	65
4	Abstraction Refinement	67
4.1	Abstraction by Merging Omission	68
4.2	Concretisation	74
4.3	Interpolation	75
4.3.1	Craig Interpolants	75
4.3.2	Expressiveness of Interpolants	77
4.3.3	Sequential Formula Order for $\varphi(\mathfrak{S})$	79
4.4	Refinement	81
4.4.1	Ruling Out a Counterexample Trace	81
4.4.2	Refining a Previously Abstracted Parameter	82
4.4.3	Refinement Heuristics	83
4.5	Conclusion	85
5	Tool Development and Application to Case Studies	87
5.1	Implementation	88
5.1.1	The Extensible Automata framework in ECT	88
5.1.2	The Timed Constraint Automaton Plugin	91
5.1.3	From TCA to Formulas	92
5.1.4	Abstraction Refinement	95
5.2	Workflow	97
5.2.1	Editing	98
5.2.2	Formula Generation	100
5.2.3	Verification	102
5.3	Case Studies	104
5.3.1	Alternating Bit Protocol	104
5.3.2	Lip-Synchronisation Protocol	108
5.3.3	Advantages of using TCA	120
6	Conclusions	123
6.1	Future Directions	124
A	Proofs	127

A.1 Correctness of Representation	127
A.2 Correctness of Abstraction	136
Abstract	149
Samenvatting	151
Curriculum Vitae	153
Index	155
Bibliography	159

