A practical approach to model checking Duration Calculus using Presburger Arithmetic

This paper investigates the feasibility of reducing a model-checking problem $K \models \phi$ for discrete time Duration Calculus to the decision problem for Presburger Arithmetic. Theoretical results point at severe limitations of this approach: (1) the reduction in Fränzle and Hansen (Int J Softw Inform 3(2–3):171–196, 2009) produces Presburger formulas whose sizes grow exponentially in the chop-depth of $\phi$, where chop is an interval modality originating from Moszkowski (IEEE Comput 18(2):10–19, 1985), and (2) the decision problem for Presburger Arithmetic has a double exponential lower bound and a triple exponential upper bound. The generated Presburger formulas have a rich Boolean structure, many quantifiers and quantifier alternations. Such formulas are simplified using so-called guarded formulas, where a guard provides a context used to simplify the rest of the formula. A normal form for guarded formulas supports global effects of local simplifications. Combined with quantifier-elimination techniques, this normalization gives significant reductions in formula sizes and in the number of quantifiers. As an example, we solve a configuration problem using the SMT-solver Z3 as backend. Benefits and the current limits of the approach are illustrated by a family of examples.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering
Authors: Hansen, M. R. (Intern), Dung, P. A. (Intern), Brekling, A. W. (Intern)
Pages: 251-278
Publication date: 2014
Main Research Area: Technical/natural sciences

Publication information
Journal: Annals of Mathematics and Artificial Intelligence
Volume: 71
Issue number: 1-3
ISSN (Print): 1012-2443
Ratings:
BFI (2018): BFI-level 1
BFI (2017): BFI-level 1
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 1
Scopus rating (2016): SJR 0.441 SNIP 1.069 CiteScore 1.27
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.497 SNIP 0.986 CiteScore 0.93
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.517 SNIP 1.418 CiteScore 1.08
Interval temporal logic, Duration Calculus, Model checking, Presburger Arithmetic

DOIs: 10.1007/s10472-013-9373-7
Source: dtu
Source-ID: u::9981
Publication: Research - peer-review › Journal article – Annual report year: 2013

On Tool Support for Duration Calculus on the Basis of Presburger Arithmetic

Interval Logics are often very expressive logics for which decision and model-checking algorithms are hard or even impossible to achieve, and this also applies for Duration Calculus, which adds the notion of accumulated duration to the Interval Temporal Logic introduced by Moszkowski et al. In this ongoing work, we report on our experiences with implementing the model-checking algorithm in [12], which reduces model checking to checking formulas of Presburger arithmetic. The model-checking algorithm generates Presburger formulas that may have sizes being exponential in the chop depth of the Duration Calculus formulas, so it is not clear whether this is a feasible approach. The decision procedure is partitioned into a frontend with reductions including "cheap", equation-based quantifier eliminations, and a general quantifier-elimination procedure, where we have experimented with an implementation based on Cooper's algorithm and with the SMT solver Z3. The formula reductions are facilitated using a new 'guarded normal form'. Applying the frontend before a general quantifier elimination procedure gave significant improvements for most of the experiments.

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Authors: Hansen, M. R. (Intern), Brekling, A. W. (Intern)
Pages: 115-122
Publication date: 2011

Host publication information
Title of host publication: 2011 Eighteenth International Symposium on Temporal Representation and Reasoning (TIME)
Publisher: IEEE
ISBN (Print): 978-1-4577-1242-5
Analysis for Embedded Systems: Experiments with Priced Timed Automata

Analysis of resource consumption of embedded systems is a major challenge in the industry since the number of components that can be included in a single chip keeps getting bigger. In this paper, we consider simple models of embedded systems and the automated analysis about timing and memory access costs of those models. In order to achieve this, a basic model is built using priced timed automata and some resource consumption scenarios are verified. Even though the experiments are performed on small and basic models, we believe we have taken a basis step in showing that it is promising to use priced timed automata and Uppaal Cora as a model checking tool in reasoning about resource consumption of embedded systems.

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling, Istanbul Technical University
Authors: Ovatman, T. (Ekstern), Brekling, A. W. (Intern), Hansen, M. R. (Intern)
Pages: 81-95
Publication date: 2010
Main Research Area: Technical/natural sciences

Publication information
Journal: Electronic Notes in Theoretical Computer Science
Volume: 238
Issue number: 6
ISSN (Print): 1571-0661
Ratings:
BFI (2018): BFI-level 1
BFI (2017): BFI-level 1
BFI (2016): BFI-level 1
Scopus rating (2016): SJR 0.256 SNIP 0.609 CiteScore 0.66
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.373 SNIP 0.781 CiteScore 0.67
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.382 SNIP 0.771 CiteScore 0.6
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.323 SNIP 0.72 CiteScore 0.55
ISI indexed (2013): ISI indexed no
BFI (2012): BFI-level 1
Scopus rating (2012): SJR 0.386 SNIP 0.608 CiteScore 0.55
ISI indexed (2012): ISI indexed no
BFI (2011): BFI-level 1
Scopus rating (2011): SJR 0.325 SNIP 0.582 CiteScore 0.57
ISI indexed (2011): ISI indexed no
BFI (2010): BFI-level 1
Scopus rating (2010): SJR 0.408 SNIP 0.567
BFI (2009): BFI-level 1
Scopus rating (2009): SJR 0.419 SNIP 0.689
Modelling and Analyses of Embedded Systems Design

We present the MoVES languages: a language with which embedded systems can be specified at a stage in the development process where an application is identified and should be mapped to an execution platform (potentially multicore). We give a formal model for MoVES that captures and gives semantics to the elements of specifications in the MoVES language. We show that even for seemingly simple systems, the complexity of verifying real-time constraints can be overwhelming - but we give an upper limit to the size of the search-space that needs examining. Furthermore, the formal model exposes important scheduling situations that become central in establishing timed-automata models that can be used for analysis of MoVES specifications effectively. Finally we present the MoVES tool, which can conduct automatic verification of interesting properties of MoVES specifications. In several examples, we use the MoVES tool to conduct analysis that identifies timing anomalies. We also conduct design space exploration in an example using the MoVES tool. And we show that it can be used for analysis of systems that, in size, resemble industrially-interesting systems. We find that semantically-based verification is a promising approach for assisting developers of embedded systems. We provide examples of system verifications that, in size and complexity, point in the direction of industrially-interesting systems.

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Authors: Brekling, A. W. (Intern), Hansen, M. R. (Intern), Madsen, J. (Intern)
Publication date: 2010

Publication information
Place of publication: Kgs. Lyngby, Denmark
Publisher: Technical University of Denmark (DTU)
Original language: English
Series: IMM-PHD-2011-236
Main Research Area: Technical/natural sciences
Electronic versions:
phd236_aske-foreloebig.pdf
Source: orbit
Source-ID: 265894
Publication: Research › Ph.D. thesis – Annual report year: 2011

Modelling and Analysis for Embedded Systems

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Authors: Madsen, J. (Intern), Hansen, M. R. (Intern), Brekling, A. W. (Intern)
Number of pages: 766
Pages: 121-145
Publication date: 2010

Host publication information
A modelling and analysis framework for embedded systems

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Authors: Madsen, J. (Intern), Hansen, M. R. (Intern), Brekling, A. W. (Intern)
Publication date: 2009

Host publication information
Title of host publication: Model-Based Design for Embedded Systems
Place of publication: CRC Press
Publisher: Routledge
ISBN (Print): 978-1-4200-6784-2

Series: Computational Analysis, Synthesis, and Design of Dynamic Systems
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 257271
Publication: Research - peer-review › Book chapter – Annual report year: 2009

Analysis of Quantitative Properties of Hardware Specifications

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Authors: Brekling, A. W. (Intern), Madsen, J. (Intern), Hansen, M. R. (Intern)
Pages: 92-94
Publication date: 2009

Host publication information
Title of host publication: 21st Nordic Workshop on Programming Theory (NWPT'09)
Publisher: DTU Informatik, Danmarks Tekniske Universitet
ISBN (Print): 978-87-643-0565-4
Main Research Area: Technical/natural sciences
Workshop: 21st Nordic Workshop on Programming Theory, Lyngby, Denmark, 14/12/2009 - 14/12/2009
Source: orbit
Source-ID: 257294
Publication: Research - peer-review › Article in proceedings – Annual report year: 2009

MoVES - A Framework for Modelling and Verifying Embedded Systems

The MoVES framework is being developed to assist in the early phases of embedded systems design. A system is modelled as an application running on an execution platform. The application is modelled through the individual tasks, and the execution platform is modelled through the processing elements, including the operating systems, and their interconnections. The tasks and processing elements are characterized by their real-time properties. The framework can be used to conduct schedulability analysis and has the potential to reason about different types of resource usage such as memory usage and power consumption. A simple specification language for embedded systems and a verification backend are presented. The framework has a modular, parameterized structure supporting easy extension and adaptation of the specification language as well as of the verification backend. We show, using a number of small examples, how MoVES can be used to model and analyze embedded systems.

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Authors: Brekling, A. W. (Intern), Hansen, M. R. (Intern), Madsen, J. (Intern)
Host publication information
Title of host publication: 2009 International Conference on Microelectronics
Publisher: IEEE
ISBN (Print): 978-1-4244-5815-8
Main Research Area: Technical/natural sciences
Conference: The 21st International Conference on Microelectronics, Marrakesh, Morocco, 01/01/2009
Electronic versions:
Brekling.pdf
DOIs:
10.1109/ICM.2009.5418667

Bibliographical note
Copyright 2009 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for
advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to
reuse any copyrighted component of this work in other works must be obtained from the IEEE.
Source: orbit
Source-ID: 257275
Publication: Research - peer-review › Article in proceedings – Annual report year: 2009

Proceedings of the 21st Nordic Workshop on Programming Theory, NWPT'09, Lyngby, Denmark, 14-16 October 2009

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Authors: Hansen, M. R. (ed.) (Intern), Brekling, A. W. (ed.) (Intern)
Number of pages: 106
Publication date: 2009

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark, DTU Informatics, Building 321
ISBN (Print): 978-87-643-0565-4
Original language: English
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 257585
Publication: Research › Report – Annual report year: 2009

Analysis of costs of embedded systems: experiments with priced timed automata

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling, Istanbul
Technical University
Authors: Ovatman, T. (Ekstern), Brekling, A. W. (Intern), Hansen, M. R. (Intern)
Pages: 1-14
Publication date: 2008

Host publication information
Title of host publication: Formal Foundations of Embedded Software and Component-Based Software Architectures :
FESCA@ETAPS
Publisher: Elsevier
Main Research Area: Technical/natural sciences
Conference: Formal Foundations of Embedded Software and Component-Based Software Architectures, Budapest,
Hungary, 01/01/2008
Source: orbit
Source-ID: 233195
Publication: Research - peer-review › Article in proceedings – Annual report year: 2008

Formal Verification of Design Properties of Hardware Architectures.
Models and formal verification of multiprocessor system-on-chips

In this article we develop a model for applications running on multiprocessor platforms. An application is modelled by task graphs and a multiprocessor system is modelled by a number of processing elements, each capable of executing tasks according to a given scheduling discipline. We present a discrete model of computation for such systems and characterize the size of the computation tree it suffices to consider when checking for schedulability. Analysis of multiprocessor system on chips is a major challenge due to the freedom of interrelated choices concerning the application level, the configuration of the execution platform and the mapping of the application onto this platform. The computational model provides a basis for formal analysis of systems. The model is translated to timed automata and a tool for system verification and simulation has been developed using Uppaal as backend. We present experimental results on rather small systems with high complexity, primarily due to differences between best-case and worst-case execution times. Considering worst-case execution times only, the system becomes deterministic and using a special version of Uppaal, where the no history is saved, we could verify a smart-phone application consisting of 103 tasks executing on 4 processing elements.
MOVES - A tool for Modeling and Verification of Embedded Systems
We demonstrate MOVES, a tool which allows designers of embedded systems to explore possible implementations early in the design process. The demonstration of MOVES will show how designers can explore different designs by changing...
the mapping of tasks on processing elements, the number and/or speed of processing elements, the size of local memories, and the operating systems (scheduling algorithm).

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Ellebæk, J. (Ekstern), Knudsen, K. S. (Ekstern), Brekling, A. W. (Intern), Hansen, M. R. (Intern), Madsen, J. (Intern)
Publication date: 2007

Host publication information
Title of host publication: DATE'07 University Booth
Publisher: EEDA
Main Research Area: Technical/natural sciences
Electronic versions:
MOVES_UBooth.pdf
Source: orbit
Source-ID: 196108
Publication: Research › Article in proceedings – Annual report year: 2007

Semantics and verification of a language for modelling hardware architectures

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Hansen, M. R. (Intern), Madsen, J. (Intern), Brekling, A. W. (Intern)
Pages: 300-319
Publication date: 2007

Host publication information
Title of host publication: Formal Methods and Hybrid Real-Time Systems
Publisher: Springer
Editors: Jones, C. B., Liu, Z., Woodcock, J.
Series: Lecture Notes in Computer Science
Number: 4700
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 208228
Publication: Research - peer-review › Book chapter – Annual report year: 2007

A Timed-Automata Semantics for a System-Level MPSoC model

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Brekling, A. W. (Intern), Hansen, M. R. (Intern), Madsen, J. (Intern)
Publication date: 2006

Host publication information
Title of host publication: Nordic Workshop on Programming Theory
Publisher: Reykjavik University
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 195150
Publication: Research - peer-review › Article in proceedings – Annual report year: 2006

Projects:
Models and Analyses for Embedded Systems Design

Department of Informatics and Mathematical Modeling

Period: 01/04/2007 → 02/02/2011
Number of participants: 6

Phd Student:

Brekling, Aske Wiid (Intern)

Supervisor:

Madsen, Jan (Intern)

Main Supervisor:

Hansen, Michael Reichhardt (Intern)

Examiner:

Sparsø, Jens (Intern)

Ravn, Anders P. (Intern)

Vain, Jüri (Ekstern)

Financing sources

Source: Internal funding (public)

Name of research programme: Forskningsrådsfinansiering

Project: PhD