Andrea Vandin - DTU Orbit (11/06/2018)

Andrea Vandin

Organisations

Assistant Professor, Department of Applied Mathematics and Computer Science
28/06/2017 → present
anvan@dtu.dk
VIP

Formal Methods
01/09/2017 → present
VIP

Publications:

Replicated Computations Results (RCR) report for “A holistic approach for collaborative workload execution in volunteer clouds”

“A Holistic Approach for Collaborative Workload Execution in Volunteer Clouds” [3] proposes a novel approach to task scheduling in volunteer clouds. Volunteer clouds are decentralized cloud systems based on collaborative task execution, where clients voluntarily share their own unused computational resources. By using simulation-based statistical analysis techniques—in particular, statistical model checking—the authors show that their approach can outperform existing distributed task scheduling algorithms in the case of computation-intensive workloads. The analysis considered a realistic workload benchmark provided by Google. This replicated computations results report focuses on the prototypical tool implementation used in the article to perform such analysis. The software was straightforward to install and use, and a representative part of the experimental results from the article could be reproduced in reasonable time using a standard laptop.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods
Authors: Vandin, A. (Intern)
Number of pages: 3
Publication date: 2018
Main Research Area: Technical/natural sciences

Publication information
Journal: ACM Transactions on Modeling and Computer Simulation
Volume: 28
Issue number: 2
Article number: 15
ISSN (Print): 1049-3301
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Scopus rating (2017): SNIP 1.151 SJR 0.46
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 1.27 SJR 0.434 SNIP 0.831
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.369 SNIP 0.839 CiteScore 1.41
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.501 SNIP 1.994 CiteScore 1.46
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.579 SNIP 1.253 CiteScore 1.62
ISI indexed (2013): ISI indexed yes
BFI (2012): BFI-level 1
Scopus rating (2012): SJR 0.49 SNIP 1.407 CiteScore 1.12
ISI indexed (2012): ISI indexed yes
Language-based abstractions for dynamical systems

Ordinary differential equations (ODEs) are the primary means to modelling dynamical systems in many natural and engineering sciences. The number of equations required to describe a system with high heterogeneity limits our capability of effectively performing analyses. This has motivated a large body of research, across many disciplines, into abstraction techniques that provide smaller ODE systems while preserving the original dynamics in some appropriate sense. In this paper we give an overview of a recently proposed computer-science perspective to this problem, where ODE reduction is recast to finding an appropriate equivalence relation over ODE variables, akin to classical models of computation based on labelled transition systems.
**EGAC: A genetic algorithm to compare chemical reaction networks**

Discovering relations between chemical reaction networks (CRNs) is a relevant problem in computational systems biology for model reduction, to explain if a given system can be seen as an abstraction of another one; and for model comparison, useful to establish an evolutionary path from simpler networks to more complex ones. This is also related to foundational issues in computer science regarding program equivalence, in light of the established interpretation of a CRN as a kernel programming language for concurrency. Criteria for deciding if two CRNs can be formally related have been recently developed, but these require that a candidate mapping be provided. Automatically finding candidate mappings is very hard in general since the search space essentially consists of all possible partitions of a set. In this paper we tackle this problem by developing a genetic algorithm for a class of CRNs called influence networks, which can be used to model a variety of biological systems including cell-cycle switches and gene networks. An extensive numerical evaluation shows that our approach can successfully establish relations between influence networks from the literature which cannot be found by exact algorithms due to their large computational requirements.

**BProVe: A formal verification framework for business process models**

Business Process Modelling has acquired increasing relevance in software development. Available notations, such as BPMN, permit to describe activities of complex organisations. On the one hand, this shortens the communication gap between domain experts and IT specialists. On the other hand, this permits to clarify the characteristics of software systems introduced to provide automatic support for such activities. Nevertheless, the lack of formal semantics hinders the automatic verification of relevant properties. This paper presents a novel verification framework for BPMN 2.0, called BProVe. It is based on an operational semantics, implemented using MAUDE, devised to make the verification general and effective. A complete tool chain, based on the Eclipse modelling environment, allows for rigorous modelling and analysis of Business Processes. The approach has been validated using more than one thousand models available on a publicly accessible repository. Besides showing the performance of BProVe, this validation demonstrates its practical benefits in identifying correctness issues in real models.
BProVe: Tool support for business process verification

This demo introduces BProVe, a tool supporting automated verification of Business Process models. BProVe analysis is based on a formal operational semantics defined for the BPMN 2.0 modelling language, and is provided as a freely accessible service that uses open standard formats as input data. Furthermore a plug-in for the Eclipse platform has been developed making available a tool chain supporting users in modelling and visualising, in a friendly manner, the results of the verification. Finally we have conducted a validation through more than one thousand models, showing the effectiveness of our verification tool in practice. (Demo video: https://youtu.be/iF5OM7vKtDA)
ERODE: A tool for the evaluation and reduction of ordinary differential equations

We present ERODE, a multi-platform tool for the solution and exact reduction of systems of ordinary differential equations (ODEs). ERODE supports two recently introduced, complementary, equivalence relations over ODE variables: forward differential equivalence yields a self-consistent aggregate system where each ODE gives the cumulative dynamics of the sum of the original variables in the respective equivalence class. Backward differential equivalence identifies variables that have identical solutions whenever starting from the same initial conditions. As back-end ERODE uses the well-known Z3 SMT solver to compute the largest equivalence that refines a given initial partition of ODE variables. In the special case of ODEs with polynomial derivatives of degree at most two (covering affine systems and elementary chemical reaction networks), it implements a more efficient partition-refinement algorithm in the style of Paige and Tarjan. ERODE comes with a rich development environment based on the Eclipse plug-in framework offering: (i) seamless project management; (ii) a fully-featured text editor; and (iii) importing-exporting capabilities.

Maximal aggregation of polynomial dynamical systems

Ordinary differential equations (ODEs) with polynomial derivatives are a fundamental tool for understanding the dynamics of systems across many branches of science, but our ability to gain mechanistic insight and effectively conduct numerical evaluations is critically hindered when dealing with large models. Here we propose an aggregation technique that rests on two notions of equivalence relating ODE variables whenever they have the same solution (backward criterion) or if a self-consistent system can be written for describing the evolution of sums of variables in the same equivalence class (forward criterion). A key feature of our proposal is to encode a polynomial ODE system into a finitary structure akin to a formal chemical reaction network. This enables the development of a discrete algorithm to efficiently compute the largest equivalence, building on approaches rooted in computer science to minimize basic models of computation through iterative partition refinements. The physical interpretability of the aggregation is shown on polynomial ODE systems for biochemical reaction networks, gene regulatory networks, and evolutionary game theory.
<table>
<thead>
<tr>
<th>Year</th>
<th>BFI</th>
<th>Scopus rating</th>
<th>Web of Science</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>Level 2</td>
<td>SNIP 2.626 SJR 6.092</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2017</td>
<td>Level 2</td>
<td>SJR 6.576 SNIP 2.642</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2016</td>
<td>Level 2</td>
<td>CiteScore 8.56</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2015</td>
<td>Level 2</td>
<td>SJR 6.814 SNIP 2.691 CiteScore 8.84</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2014</td>
<td>Level 2</td>
<td>SJR 6.898 SNIP 2.734 CiteScore 8.86</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2013</td>
<td>Level 2</td>
<td>SJR 7.073 SNIP 2.738 CiteScore 9.5</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2012</td>
<td>Level 2</td>
<td>SJR 6.868 SNIP 2.697 CiteScore 9.49</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2011</td>
<td>Level 2</td>
<td>SJR 6.864 SNIP 2.646 CiteScore 9.31</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2010</td>
<td>Level 2</td>
<td>SJR 6.898 SNIP 2.545</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2009</td>
<td>Level 2</td>
<td>SJR 7.025 SNIP 2.556</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2008</td>
<td>Level 2</td>
<td>SJR 7.034 SNIP 2.449</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2007</td>
<td>Level 2</td>
<td>SJR 6.867 SNIP 2.453</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2006</td>
<td>Level 2</td>
<td>SJR 6.849 SNIP 2.45</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2005</td>
<td>Level 2</td>
<td>SJR 6.94 SNIP 2.555</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2004</td>
<td>Level 2</td>
<td>SJR 7.197 SNIP 2.629</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2003</td>
<td>Level 2</td>
<td>SJR 7.129 SNIP 2.515</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2002</td>
<td>Level 2</td>
<td>SJR 6.913 SNIP 2.503</td>
<td>Indexed yes</td>
</tr>
<tr>
<td>2001</td>
<td>Level 2</td>
<td>SJR 7.189 SNIP 2.47</td>
<td>Indexed yes</td>
</tr>
</tbody>
</table>
Syntactic Markovian Bisimulation for Chemical Reaction Networks

In chemical reaction networks (CRNs) with stochastic semantics based on continuous-time Markov chains (CTMCs), the typically large populations of species cause combinatorially large state spaces. This makes the analysis very difficult in practice and represents the major bottleneck for the applicability of minimization techniques based, for instance, on lumpability. In this paper we present syntactic Markovian bisimulation (SMB), a notion of bisimulation developed in the Larsen-Skou style of probabilistic bisimulation, defined over the structure of a CRN rather than over its underlying CTMC. SMB identifies a lumpable partition of the CTMC state space a priori, in the sense that it is an equivalence relation over species implying that two CTMC states are lumpable when they are invariant with respect to the total population of species within the same equivalence class. We develop an efficient partition-refinement algorithm which computes the largest SMB of a CRN in polynomial time in the number of species and reactions. We also provide an algorithm for obtaining a quotient network from an SMB that induces the lumped CTMC directly, thus avoiding the generation of the state space of the original CRN altogether. In practice, we show that SMB allows significant reductions in a number of models from the literature. Finally, we study SMB with respect to the deterministic semantics of CRNs based on ordinary differential equations (ODEs), where each equation gives the time-course evolution of the concentration of a species. SMB implies forward CRN bisimulation, a recently developed behavioral notion of equivalence for the ODE semantics, in an analogous sense: it yields a smaller ODE system that keeps track of the sums of the solutions for equivalent species.
Comparing Chemical Reaction Networks: A Categorical and Algorithmic Perspective

We study chemical reaction networks (CRNs) as a kernel language for concurrency models with semantics based on ordinary differential equations. We investigate the problem of comparing two CRNs, i.e., to decide whether the trajectories of a source CRN can be matched by a target CRN under an appropriate choice of initial conditions. Using a categorical framework, we extend and relate model-comparison approaches based on structural (syntactic) and on dynamical (semantic) properties of a CRN, proving their equivalence. Then, we provide an algorithm to compare CRNs, running linearly in time with respect to the cardinality of all possible comparisons. Finally, we apply our results to biological models from the literature.

Symbolic computation of differential equivalences

Ordinary differential equations (ODEs) are widespread in many natural sciences including chemistry, ecology, and systems biology, and in disciplines such as control theory and electrical engineering. Building on the celebrated molecules-As-processes paradigm, they have become increasingly popular in computer science, with highlevel languages and formal methods such as Petri nets, process algebra, and rule-based systems that are interpreted as ODEs. We consider the problem of comparing and minimizing ODEs automatically. Influenced by traditional approaches in the theory of programming, we propose differential equivalence relations. We study them for a basic intermediate language, for which we have decidability results, that can be targeted by a class of highlevel specifications. An ODE implicitly represents an
uncountable state space, hence reasoning techniques cannot be borrowed from established domains such as probabilistic programs with finite-state Markov chain semantics. We provide novel symbolic procedures to check an equivalence and compute the largest one via partition refinement algorithms that use satisfiability modulo theories. We illustrate the generality of our framework by showing that differential equivalences include (i) well-known notions for the minimization of continuous-time Markov chains (lumpability), (ii) bisimulations for chemical reaction networks recently proposed by Cardelli et al., and (iii) behavioral relations for process algebra with ODE semantics. With a prototype implementation we are able to detect equivalences in biochemical models from the literature that cannot be reduced using competing automatic techniques.

A tool-chain for statistical spatio-temporal model checking of bike sharing systems
Prominent examples of collective systems are often encountered when analysing smart cities and smart transportation systems. We propose a novel modelling and analysis approach combining statistical model checking, spatio-temporal
logics, and simulation. The proposed methodology is applied to modelling and statistical analysis of user behaviour in bike sharing systems. We present a tool-chain that integrates the statistical analysis toolkit MultiVeStA, the spatio-temporal model checker topochecker, and a bike sharing systems simulator based on Markov renewal processes. The obtained tool allows one to estimate, up to a user-specified precision, the likelihood of specific spatio-temporal formulas, such as the formation of clusters of full stations and their temporal evolution.

General information
State: Published
Organisations: CNR, IMT Institute for Advanced Studies Lucca
Authors: Ciancia, V. (Ekstern), Latella, D. (Ekstern), Massink, M. (Ekstern), Paškauskas, R. (Ekstern), Vandin, A. (Intern)
Number of pages: 17
Pages: 657-673
Publication date: 2016

Host publication information
Title of host publication: Leveraging Applications of Formal Methods, Verification and Validation : Foundational Techniques - 7th International Symposium, ISoLA 2016, Proceedings
Volume: 9952 LNCS
Publisher: Springer Verlag
ISBN (Print): 9783319471655

Series: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)
Volume: 9952 LNCS
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: 7th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation, ISoLA 2016, Imperial, Corfu, Greece, 10/10/2016 - 10/10/2016
Collective adaptive systems, MultiVeStA, Spatio-temporal model checking, Statistical model checking
DOIs:
10.1007/978-3-319-47166-2_46
Source: Scopus
Source-ID: 84993950068
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Efficient syntax-Driven lumping of differential equations
We present an algorithm to compute exact aggregations of a class of systems of ordinary differential equations (ODEs). Our approach consists in an extension of Paige and Tarjan’s seminal solution to the coarsest refinement problem by encoding an ODE system into a suitable discrete-state representation. In particular, we consider a simple extension of the syntax of elementary chemical reaction networks because (i) it can express ODEs with derivatives given by polynomials of degree at most two, which are relevant in many applications in natural sciences and engineering; and (ii) we can build on two recently introduced bisimulations, which yield two complementary notions of ODE lumping. Our algorithm computes the largest bisimulations in O(r·s·log s) time, where r is the number of monomials and s is the number of variables in the ODEs. Numerical experiments on real-world models from biochemistry, electrical engineering, and structural mechanics show that our prototype is able to handle ODEs with millions of variables and monomials, providing significant model reductions.

General information
State: Published
Organisations: Microsoft USA, University of Oxford, IMT Institute for Advanced Studies Lucca
Authors: Cardelli, L. (Ekstern), Tribastone, M. (Ekstern), Tschaikowski, M. (Ekstern), Vandin, A. (Intern)
Number of pages: 19
Pages: 93-111
Publication date: 2016

Host publication information
Title of host publication: Tools and Algorithms for the Construction and Analysis of Systems - 22nd International Conference, TACAS 2016 and Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2016, Proceedings
Volume: 9636
Publisher: Springer Verlag
ISBN (Print): 9783662496732

Series: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)
Volume: 9636
Quantitative abstractions for collective adaptive systems

Collective adaptive systems (CAS) consist of a large number of possibly heterogeneous entities evolving according to local interactions that may operate across multiple scales in time and space. The adaptation to changes in the environment, as well as the highly dispersed decision-making process, often leads to emergent behaviour that cannot be understood by simply analysing the objectives, properties, and dynamics of the individual entities in isolation. As with most complex systems, modelling is a phase of crucial importance for the design of new CAS or the understanding of existing ones. Elsewhere in this volume the typical workflow of formal modelling, analysis, and evaluation of a CAS has been illustrated in detail. In this chapter we treat the problem of efficiently analysing large-scale CAS for quantitative properties. We review algorithms to automatically reduce the dimensionality of a CAS model preserving modeller-defined state variables, with focus on descriptions based on systems of ordinary differential equations. We illustrate the theory in a tutorial fashion, with running examples and a number of more substantial case studies ranging from crowd dynamics, epidemiology and biological systems.

General information
State: Published
Organisations: IMT Institute for Advanced Studies Lucca
Authors: Vandin, A. (Intern), Tribastone, M. (Ekstern)
Number of pages: 31
Pages: 202-232
Publication date: 2016

Host publication information
Volume: 9700
Publisher: Springer Verlag
ISBN (Print): 9783319340951
Series: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)
Volume: 9700
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
DOIs:
10.1007/978-3-319-34096-8_7
Source: Scopus
Source-ID: 8497896735
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Statistical Model Checking for Product Lines

We report on the suitability of statistical model checking for the analysis of quantitative properties of product line models by an extended treatment of earlier work by the authors. The type of analysis that can be performed includes the likelihood of specific product behaviour, the expected average cost of products (in terms of the attributes of the products’ features) and the probability of features to be (un)installed at runtime. The product lines must be modelled in QFLan, which extends the probabilistic feature-oriented language PFLan with novel quantitative constraints among features and on behaviour and with advanced feature installation options. QFLan is a rich process-algebraic specification language whose operational behaviour interacts with a store of constraints, neatly separating product configuration from product behaviour. The resulting probabilistic configurations and probabilistic behaviour converge in a discrete-time Markov chain semantics, enabling the analysis of quantitative properties. Technically, a Maude implementation of QFLan, integrated with Microsoft’s SMT constraint solver Z3, is combined with the distributed statistical model checker MultiVeStA, developed by one of the authors. We illustrate the feasibility of our framework by applying it to a case study of a product line of bikes.
Forward and backward bisimulations for chemical reaction networks

We present two quantitative behavioral equivalences over species of a chemical reaction network (CRN) with semantics based on ordinary differential equations. Forward CRN bisimulation identifies a partition where each equivalence class represents the exact sum of the concentrations of the species belonging to that class. Backward CRN bisimulation relates species that have identical solutions at all time points when starting from the same initial conditions. Both notions can be checked using only CRN syntactical information, i.e., by inspection of the set of reactions. We provide a unified algorithm that computes the coarsest refinement up to our bisimulations in polynomial time. Further, we give algorithms to compute quotient CRNs induced by a bisimulation. As an application, we find significant reductions in a number of models of biological processes from the literature. In two cases we allow the analysis of benchmark models which would be otherwise intractable due to their memory requirements.
A white box perspective on behavioural adaptation

We present a white-box conceptual framework for adaptation developed in the context of the EU Project ASCENS coordinated by Martin Wirsing. We called it CoDA, for Control Data Adaptation, since it is based on the notion of control data. CoDA promotes a neat separation between application and adaptation logic through a clear identification of the set of data that is relevant for the latter. The framework provides an original perspective from which we survey a representative set of approaches to adaptation, ranging from programming languages and paradigms to computational models and architectural solutions.
Differential bisimulation for a Markovian process algebra

Formal languages with semantics based on ordinary differential equations (ODEs) have emerged as a useful tool to reason about large-scale distributed systems. We present differential bisimulation, a behavioral equivalence developed as the ODE counterpart of bisimulations for languages with probabilistic or stochastic semantics. We study it in the context of a Markovian process algebra. Similarly to Markovian bisimulations yielding an aggregated Markov process in the sense of the theory of lumpability, differential bisimulation yields a partition of the ODEs underlying a process algebra term, whereby the sum of the ODE solutions of the same partition block is equal to the solution of a single (lumped) ODE. Differential bisimulation is defined in terms of two symmetries that can be verified only using syntactic checks. This enables the adaptation to a continuous-state semantics of proof techniques and algorithms for finite, discrete-state, labeled transition systems. For instance, we readily obtain a result of compositionality, and provide an efficient partition-refinement algorithm to compute the coarsest ODE aggregation of a model according to differential bisimulation.

Quantitative Analysis of Probabilistic Models of Software Product Lines with Statistical Model Checking

We investigate the suitability of statistical model checking techniques for analysing quantitative properties of software product line models with probabilistic aspects. For this purpose, we enrich the feature-oriented language FLAN with action rates, which specify the likelihood of exhibiting particular behaviour or of installing features at a specific moment or in a specific order. The enriched language (called PFLAN) allows us to specify models of software product lines with probabilistic configurations and behaviour, e.g. by considering a PFLAN semantics based on discrete-time Markov chains. The Maude implementation of PFLAN is combined with the distributed statistical model checker MultiVeStA to perform quantitative analyses of a simple product line case study. The presented analyses include the likelihood of certain behaviour of interest (e.g. product malfunctioning) and the expected average cost of products.
Reconciling White-Box and Black-Box Perspectives on Behavioral Self-adaptation

This paper proposes to reconcile two perspectives on behavioral adaptation commonly taken at different stages of the engineering of autonomic computing systems. Requirements engineering activities often take a black-box perspective: A system is considered to be adaptive with respect to an environment whenever the system is able to satisfy its goals irrespectively of the environment perturbations. Modeling and programming engineering activities often take a white-box perspective: A system is equipped with suitable adaptation mechanisms and its behavior is classified as adaptive depending on whether the adaptation mechanisms are enacted or not. The proposed approach reconciles black- and white-box perspectives by proposing several notions of coherence between the adaptivity as observed by the two perspectives: These notions provide useful criteria for the system developer to assess and possibly modify the adaptation requirements, models and programs of an autonomic system.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, University of Pisa, Ludwig-Maximilians-Universität, University of Southampton
Authors: Bruni, R. (Ekstern), Corradini, A. (Ekstern), Gadducci, F. (Ekstern), Hözl, M. (Ekstern), Lluch Lafuente, A. (Intern), Vandin, A. (Intern), Wirsing, M. (Ekstern)
Pages: 163-184
Publication date: 2015

Reconciling White-Box and Black-Box Perspectives on Behavioral Self-Adaptation

This paper proposes to reconcile two perspectives on behavioral adaptation commonly taken at different stages of the engineering of autonomic computing systems. Requirements engineering activities often take a black-box perspective: A system is considered to be adaptive with respect to an environment whenever the system is able to satisfy its goals irrespectively of the environment perturbations. Modeling and programming engineering activities often take a white-box perspective: A system is equipped with suitable adaptation mechanisms and its behavior is classified as adaptive depending on whether the adaptation mechanisms are enacted or not. The proposed approach reconciles black- and white-box perspectives by proposing several notions of coherence between the adaptivity as observed by the two perspectives: These notions provide useful criteria for the system developer to assess and possibly modify the adaptation requirements, models and programs of an autonomic system.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, University of Pisa, Ludwig-Maximilians-Universität, University of Southampton
Authors: Bruni, R. (Ekstern), Corradini, A. (Ekstern), Gadducci, F. (Ekstern), Hözl, M. (Ekstern), Lluch Lafuente, A. (Intern), Vandin, A. (Intern), Wirsing, M. (Ekstern)
Pages: 163-184
Publication date: 2015

Reconciling White-Box and Black-Box Perspectives on Behavioral Self-adaptation

This paper proposes to reconcile two perspectives on behavioral adaptation commonly taken at different stages of the engineering of autonomic computing systems. Requirements engineering activities often take a black-box perspective: A system is considered to be adaptive with respect to an environment whenever the system is able to satisfy its goals irrespectively of the environment perturbations. Modeling and programming engineering activities often take a white-box perspective: A system is equipped with suitable adaptation mechanisms and its behavior is classified as adaptive depending on whether the adaptation mechanisms are enacted or not. The proposed approach reconciles black- and white-box perspectives by proposing several notions of coherence between the adaptivity as observed by the two perspectives: These notions provide useful criteria for the system developer to assess and possibly modify the adaptation requirements, models and programs of an autonomic system.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, University of Pisa, Ludwig-Maximilians-Universität, University of Southampton
Authors: Bruni, R. (Ekstern), Corradini, A. (Ekstern), Gadducci, F. (Ekstern), Hözl, M. (Ekstern), Lluch Lafuente, A. (Intern), Vandin, A. (Intern), Wirsing, M. (Ekstern)
Pages: 163-184
Publication date: 2015

Reconciling White-Box and Black-Box Perspectives on Behavioral Self-adaptation

This paper proposes to reconcile two perspectives on behavioral adaptation commonly taken at different stages of the engineering of autonomic computing systems. Requirements engineering activities often take a black-box perspective: A system is considered to be adaptive with respect to an environment whenever the system is able to satisfy its goals irrespectively of the environment perturbations. Modeling and programming engineering activities often take a white-box perspective: A system is equipped with suitable adaptation mechanisms and its behavior is classified as adaptive depending on whether the adaptation mechanisms are enacted or not. The proposed approach reconciles black- and white-box perspectives by proposing several notions of coherence between the adaptivity as observed by the two perspectives: These notions provide useful criteria for the system developer to assess and possibly modify the adaptation requirements, models and programs of an autonomic system.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, University of Pisa, Ludwig-Maximilians-Universität, University of Southampton
Authors: Bruni, R. (Ekstern), Corradini, A. (Ekstern), Gadducci, F. (Ekstern), Hözl, M. (Ekstern), Lluch Lafuente, A. (Intern), Vandin, A. (Intern), Wirsing, M. (Ekstern)
Pages: 163-184
Publication date: 2015
Statistical analysis of probabilistic models of software product lines with quantitative constraints

We investigate the suitability of statistical model checking for the analysis of probabilistic models of software product lines with complex quantitative constraints and advanced feature installation options. Such models are specified in the feature-oriented language QFLan, a rich process algebra whose operational behaviour interacts with a store of constraints, neatly separating product configuration from product behaviour. The resulting probabilistic configurations and behaviour converge seamlessly in a semantics based on DTMCs, thus enabling quantitative analyses ranging from the likelihood of certain behaviour to the expected average cost of products. This is supported by a Maude implementation of QFLan, integrated with the SMT solver Z3 and the distributed statistical model checker MultiVeSTa. Our approach is illustrated with a bikes product line case study.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Consiglio Nazionale delle Ricerche, French National Institute for Computer Science and Applied Mathematics, University of Southampton
Authors: Beek, M. T. (Ekstern), Legay, A. (Ekstern), Lluch Lafuente, A. (Intern), Vandin, A. (Intern)
Pages: 11-15
Publication date: 2015

Host publication information
Title of host publication: Proceedings of the 19th International Conference on Software Product Line (SPLC ’15)
Publisher: Association for Computing Machinery
ISBN (Print): 978-1-4503-3613-0
BFI conference series: Software Product Lines (5000253)
Main Research Area: Technical/natural sciences
Conference: 19th International Conference on Software Product Line (SPLC ’15), Nashville, United States, 20/07/2015 - 20/07/2015
Electronic versions:
DOIs: 10.1145/2791060.2791087
Source: PublicationPreSubmission
Source-ID: 118084625
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

The SCEL Language: Design, Implementation, Verification

SCEL (Service Component Ensemble Language) is a new language specifically designed to rigorously model and program autonomic components and their interaction, while supporting formal reasoning on their behaviors. SCEL brings together various programming abstractions that allow one to directly represent aggregations, behaviors and knowledge according to specific policies. It also naturally supports programming interaction, self-awareness, context-awareness, and adaptation. The solid semantic grounds of the language is exploited for developing logics, tools and methodologies for formal reasoning on system behavior to establish qualitative and quantitative properties of both the individual components and the overall systems.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, IMT Institute for Advanced Studies Lucca, Consiglio Nazionale delle Ricerche, Università degli Studi di Firenze, University of Southampton
Authors: Rocco De Nicola, R. X. (Ekstern), Latella, D. (Ekstern), Lluch Lafuente, A. (Intern), Loreti, M. (Ekstern), Margheri, A. M. (Ekstern), Massink, M. (Ekstern), Morichetta, A. (Ekstern), Pugliese, R. (Ekstern), Tiezzi, F. (Ekstern), Vandin, A. (Intern)
Pages: 3-71
Publication date: 2015

Host publication information
Title of host publication: Software Engineering for Collective Autonomic Systems : The ASCENS Approach
Publisher: Springer
ISBN (Print): 978-3-319-16309-3
ISBN (Electronic): 978-3-319-16310-9
Series: Lecture Notes in Computer Science
Volume: 8998
Tools for Ensemble Design and Runtime

The ASCENS project deals with designing systems as ensembles of adaptive components. Among the outputs of the ASCENS project are multiple tools that address particular issues in designing the ensembles, ranging from support for early stage formal modeling to runtime environment for executing and monitoring ensemble implementations. The goal of this chapter is to provide a compact description of the individual tools, which is supplemented by additional downloadable material on the project website.

General information
State: Published
Organisations: Fraunhofer Gesellschaft, VERIMAG Laboratory, Charles University, IMT Institute for Advanced Studies Lucca, Università degli Studi di Firenze, University of Pisa, Universite Libre de Bruxelles, University of Limerick, Ludwig-Maximilians-Universität
Pages: 429-448
Publication date: 2015

Host publication information
Title of host publication: Software Engineering for Collective Autonomic Systems : The ASCENS Approach
Publisher: Springer
ISBN (Print): 978-3-319-16309-3
ISBN (Electronic): 978-3-319-16310-9
Chapter: Chapter III.5

Series: Lecture Notes in Computer Science
Volume: 8998
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Tools, Software development, Adaptive systems, Autonomic systems
DOIs:
10.1007/978-3-319-16310-9_1
Source-ID: 118084655
Publication: Research - peer-review › Book chapter – Annual report year: 2015

Distributed statistical analysis of complex systems modeled through a chemical metaphor

The chemical-inspired programming approach is an emerging paradigm for defining the behavior of densely distributed and context-aware devices (e.g., in ecosystems of displays tailored to crowd steering, or to obtain profile-based coordinated visualization). Typically, the evolution of such systems cannot be easily predicted, thus making of paramount importance the availability of techniques and tools supporting prior-to-deployment analysis. Exact analysis techniques do not scale well when the complexity of systems grows: as a consequence, approximated techniques based on simulation assumed a relevant role. This work presents a new simulation-based distributed analysis tool addressing the statistical analysis of such a kind of systems. The tool has been obtained by chaining two existing tools: MultiVeSta and Alchemist. The former is a recently proposed lightweight tool which allows to enrich existing discrete event simulators with automated and distributed statistical analysis capabilities, while the latter is an efficient simulator for chemical-inspired computational systems. The tool is validated against a crowd steering scenario, and insights on the performance are provided by discussing how the analysis tasks scale on a multi-core architecture.

General information
State: Published
Organisations: University of Bologna, IMT Institute for Advanced Studies Lucca, University of Southampton
Authors: Pianini, D. (Ekstern), Sebastio, S. (Ekstern), Vandin, A. (Intern)
An analysis pathway for the quantitative evaluation of public transport systems

We consider the problem of evaluating quantitative service-level agreements in public services such as transportation systems. We describe the integration of quantitative analysis tools for data fitting, model generation, simulation, and statistical model-checking, creating an analysis pathway leading from system measurement data to verification results. We apply our pathway to the problem of determining whether public bus systems are delivering an appropriate quality of service as required by regulators. We exercise the pathway on service data obtained from Lothian Buses about the arrival and departure times of their buses on key bus routes through the city of Edinburgh. Although we include only that example in the present paper, our methods are sufficiently general to apply to other transport systems and other cities.

Modelling and analyzing adaptive self-assembly strategies with Maude

Building adaptive systems with predictable emergent behavior is a difficult task and it is becoming a critical need. The research community has accepted the challenge by introducing approaches of various nature: from software architectures to programming paradigms and analysis techniques. Our white-box conceptual approach to adaptive systems based on the notion of control data promotes a clear distinction between the application and the adaptation logic. In this paper we propose a concrete instance of our approach based on (i) a neat identification of control data; (ii) a hierarchical architecture that provides the basic structure to separate the adaptation and application logics; (iii) computational reflection as the main mechanism to realize the adaptation logic; (iv) probabilistic rule-based specifications and quantitative
verification techniques to specify and analyze the adaptation logic. We show that our solution can be naturally realized in Maude, a Rewriting Logic based framework, and illustrate our approach by specifying, validating and analyzing a prominent example of adaptive systems: robot swarms equipped with self-assembly strategies. © 2013 Elsevier B.V. All rights reserved.

General information
State: Published
Organisations: IMT Institute for Advanced Studies Lucca, Università di Pisa, University of Southampton
Authors: Vandin, A. (Intern), Bruni, R. (Ekstern), Gadducci, F. (Ekstern), Corradini, A. (Ekstern), Lluch Lafuente, A. (Intern)
Pages: 75-94
Publication date: 2014
Main Research Area: Technical/natural sciences

Publication information
Journal: Science of Computer Programming
Volume: 99
ISSN (Print): 0167-6423
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 2
Scopus rating (2017): SNIP 1.041 SJR 0.3
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 2
Scopus rating (2016): CiteScore 1.36 SJR 0.459 SNIP 1.219
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 0.444 SNIP 1.039 CiteScore 1.18
Web of Science (2015): Indexed yes
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 0.506 SNIP 1.337 CiteScore 1.2
Web of Science (2014): Indexed yes
BFI (2013): BFI-level 2
Scopus rating (2013): SJR 0.562 SNIP 1.385 CiteScore 1.3
ISI indexed (2013): ISI indexed yes
Web of Science (2013): Indexed yes
BFI (2012): BFI-level 2
Scopus rating (2012): SJR 0.602 SNIP 1.683 CiteScore 1.66
ISI indexed (2012): ISI indexed yes
BFI (2011): BFI-level 2
Scopus rating (2011): SJR 0.653 SNIP 1.871 CiteScore 1.81
ISI indexed (2011): ISI indexed yes
BFI (2010): BFI-level 2
Scopus rating (2010): SJR 1.076 SNIP 2.391
Web of Science (2010): Indexed yes
BFI (2009): BFI-level 2
Scopus rating (2009): SJR 0.793 SNIP 1.797
BFI (2008): BFI-level 2
Scopus rating (2008): SJR 0.929 SNIP 1.869
Scopus rating (2007): SJR 0.692 SNIP 1.788
Scopus rating (2006): SJR 0.546 SNIP 1.387
Scopus rating (2005): SJR 0.585 SNIP 1.327
Web of Science (2005): Indexed yes
Scopus rating (2004): SJR 0.597 SNIP 1.821
Scopus rating (2003): SJR 0.707 SNIP 1.757
Web of Science (2003): Indexed yes
Scopus rating (2002): SJR 0.852 SNIP 1.474
Reasoning (on) service component ensembles in rewriting logic

Programming autonomic systems with massive number of heterogeneous components poses a number of challenges to language designers and software engineers and requires the integration of computational tools and reasoning tools. We present a general methodology to enrich SCEL, a recently introduced language for programming systems with massive numbers of components, with reasoning capabilities that are guaranteed by external reasoners. We show how the methodology can be instantiated by considering the Maude implementation of SCEL and a specific reasoner, Pirlo, implemented in Maude as well. Moreover we show how the actual integration can benefit from the existing analytical tools of the Maude framework. In particular, we demonstrate our approach by considering a simple scenario consisting of a group of robots moving in an arena aiming at minimising the number of collisions.
Adaptation is a Game

Software systems operating in unpredictable environments must be self-adaptive. Unfortunately, there is no agreed foundational model for adaptation. Already in 1963 Lofti Zadeh claimed that “it is very difficult—perhaps impossible—to find a way of characterizing in concrete terms the large variety of ways in which adaptive behavior can be realized”. His pessimism was due to the inherent difficulty of subsuming both the external manifestations of adaptive systems (black-box adaptation) and the internal mechanisms that realize adaptation (white-box adaptation) in a coherent view.

Generally speaking, a program is considered to be adaptive if it modifies its own behavior in response to changes in its operating environment. According to the traditional view, a program is made of control (i.e. algorithms) and data. A change in the behavior implies a change in the data. The identification of suitable control data leads to an unambiguous definition of adaptation: the run-time modification of such data [1].

The above view can be elegantly formalized in variants of game models for open systems such as Interface Automata [3] enriched with formal counterparts of control data [2]. We argue that such formalization may help to reconcile black- and white-box approaches to adaptation, and may enable the use of Interface Automata both as a component-based design framework and as a verification framework for adaptive systems. For instance, model checking techniques for game models can be used to decide to which extent a system is able to adapt in order to satisfy its requirements despite of changes in the environment.

MultiVeStA: Statistical model checking for discrete event simulators

The modeling, analysis and performance evaluation of large-scale systems are difficult tasks. An approach typically followed by engineers consists in performing simulations of systems models to obtain statistical estimations of quantitative...
properties. Similarly, a technique used by computer scientists working on quantitative analysis is Statistical Model Checking (SMC), where rigorous mathematical languages (e.g., logics) are used to express properties, which are automatically estimated again simulating the model at hand. These property specification languages provide a formal, compact and elegant way to express properties without hard-coding them in the model definition. This paper presents Multi Ve St A, a statistical analysis tool which can be easily integrated with discrete event simulators, enriching them with efficient distributed statistical analysis and SMC capabilities.

A Conceptual Framework for Adaptation

In this position paper we present a conceptual vision of adaptation, a key feature of autonomic systems. We put some stress on the role of control data and argue how some of the programming paradigms and models used for adaptive systems match with our conceptual framework.

Adaptable Transition Systems

We present an essential model of adaptable transition systems inspired by white-box approaches to adaptation and based on foundational models of component based systems. The key feature of adaptable transition systems are control propositions, imposing a clear separation between ordinary, functional behaviours and adaptive ones. We instantiate our approach on interface automata yielding adaptable interface automata, but it may be instantiated on other foundational
models of component-based systems as well. We discuss how control propositions can be exploited in the specification and analysis of adaptive systems, focusing on various notions proposed in the literature, like adaptability, control loops, and control synthesis.

Counterpart Semantics for a Second-Order mu-Calculus

Quantified mu-calculi combine the fix-point and modal operators of temporal logics with (existential and universal) quantifiers, and they allow for reasoning about the possible behaviour of individual components within a software system. In this paper we introduce a novel approach to the semantics of such calculi: we consider a sort of labeled transition systems called counterpart models as semantic domain, where states are algebras and transitions are defined by counterpart relations (a family of partial homomorphisms) between states. Then, formulae are interpreted over sets of state assignments (families of partial substitutions, associating formula variables to state components). Our proposal allows us to model and reason about the creation and deletion of components, as well as the merging of components. Moreover, it avoids the limitations of existing approaches, usually enforcing restrictions of the transition relation: the resulting semantics is a streamlined and intuitively appealing one, yet it is general enough to cover most of the alternative proposals we are aware of. The paper is rounded up with some considerations about expressiveness and decidability aspects.
Exploiting over- and underapproximations for infinite-state counterpart models

Software systems with dynamic topology are often infinite-state. Paradigmatic examples are those modeled as graph transformation systems (GTSs) with rewrite rules that allow an unbounded creation of items. For such systems, verification can become intractable, thus calling for the development of approximation techniques that may ease the verification at the cost of losing in preciseness and completeness. Both over- and under-approximations have been considered in the literature, respectively offering more and less behaviors than the original system. At the same time, properties of the system may be either preserved or reflected by a given approximation. In this paper we propose a general notion of approximation that captures some of the existing approaches for GTSs. Formulae are specified by a generic quantified modal logic that generalizes many specification logics adopted in the literature for GTSs. We also propose a type system to denote part of the formulae as either reflected or preserved, together with a technique that exploits under- and over-approximations to reason about typed as well as untyped formulae.

General information

State: Published
Organisations: University of Pisa, IMT Institute for Advanced Studies Lucca
Authors: Gadducci, F. (Ekstern), Lluch Lafuente, A. (Intern), Vandin, A. (Intern)
Pages: 51-65
Publication date: 2012
Modelling and analyzing adaptive self-assembling strategies with Maude

Building adaptive systems with predictable emergent behavior is a challenging task and it is becoming a critical need. The research community has accepted the challenge by introducing approaches of various nature: from software architectures, to programming paradigms, to analysis techniques. We recently proposed a conceptual framework for adaptation centered around the role of control data. In this paper we show that it can be naturally realized in a reflective logical language like Maude by using the Reflective Russian Dolls model. Moreover, we exploit this model to specify and analyse a prominent example of adaptive system: robot swarms equipped with obstacle-avoidance self-assembly strategies. The analysis exploits the statistical model checker PVesta.

Specification and verification of modal properties for structured systems

System specification formalisms should come with suitable property specification languages and effective verification tools. We sketch a framework for the verification of quantified temporal properties of systems with dynamically evolving structure. We consider visual specification formalisms like graph transformation systems (GTS) where program states are modelled as graphs, and the program behaviour is specified by graph transformation rules. The state space of a GTS can be represented as a graph transition system (GTrS), i.e. a transition system with states and transitions labelled, respectively, with a graph, and with a partial morphism representing the evolution of state components. Unfortunately, GTrSs are prohibitively large or infinite even for simple systems, making verification intractable and hence calling for appropriate abstraction techniques.
State Space c-Reductions of Concurrent Systems in Rewriting Logic
We present c-reductions, a simple, flexible and very general state space reduction technique that exploits an equivalence relation on states that is a bisimulation. Reduction is achieved by a canonizer function, which maps each state into a not necessarily unique canonical representative of its equivalence class. The approach contains symmetry reduction and name reuse and name abstraction as special cases, and exploits the expressiveness of rewriting logic and its realization in Maude to automate c-reductions and to seamlessly integrate model checking and the discharging of correctness proof obligations. The performance of the approach has been validated over a set of representative case studies.

Towards a Maude Tool for Model Checking Temporal Graph Properties
We present our prototypical tool for the verification of graph transformation systems. The major novelty of our tool is that it provides a model checker for temporal graph properties based on counterpart semantics for quantified μ-calculi. Our tool can be considered as an instantiation of our approach to counterpart semantics which allows for a neat handling of creation, deletion and merging in systems with dynamic structure. Our implementation is based on the object-based machinery of Maude, which provides the basics to deal with attributed graphs. Graph transformation systems are specified with term rewrite rules. The model checker evaluates logical formulae of second-order modal μ-calculus in the automatically generated Counterpart Model (a sort of unfolded graph transition system) of the graph transformation system under study. The result of evaluating a formula is a set of assignments for each state, associating node variables to actual nodes.
Counterpart semantics for a second-order μ-calculus

We propose a novel approach to the semantics of quantified μ-calculi, considering models where states are algebras; the evolution relation is given by a counterpart relation (a family of partial homomorphisms), allowing for the creation, deletion, and merging of components; and formulas are interpreted over sets of state assignments (families of substitutions, associating formula variables to state components). Our proposal avoids the limitations of existing approaches, usually enforcing restrictions of the evolution relation: the resulting semantics is a streamlined and intuitively appealing one, yet it is general enough to cover most of the alternative proposals we are aware of.

General information
State: Published
Organisations: University of Pisa, IMT Institute for Advanced Studies Lucca
Authors: Gadducci, F. (Ekstern), Lluch Lafuente, A. (Intern), Vandin, A. (Intern)
Pages: 282-297
Publication date: 2010