A coordination language for databases

We present a coordination language for the modeling of distributed database applications. The language, baptized Klaim-DB, borrows the concepts of localities and nets of the coordination language Klaim but re-incarnates the tuple spaces of Klaim as databases. It provides high-level abstractions and primitives for the access and manipulation of structured data, with integrity and atomicity considerations. We present the formal semantics of Klaim-DB and develop a type system that avoids potential runtime errors such as certain evaluation errors and mismatches of data format in tables, which are monitored in the semantics. The use of the language is illustrated in a scenario where the sales from different branches of a chain of department stores are aggregated from their local databases. Raising the abstraction level and encapsulating integrity checks in the language primitives have benefited the modeling task considerably.
Coordination is essential for dynamic distributed systems whose components exhibit interactive and autonomous behaviors. Spatially distributed, locally interacting, propagating computational fields are particularly appealing for allowing components to join and leave with little or no overhead. Computational fields are a key ingredient of aggregate programming, a promising software engineering methodology particularly relevant for the Internet of Things. In our approach, space topology is represented by a fixed graph-shaped field, namely a network with attributes on both nodes and arcs, where arcs represent interaction capabilities between nodes. We propose a SMuC calculus where μ-calculus-like modal formulas represent how the values stored in neighbor nodes should be combined to update the present node. Fixpoint operations can be understood globally as recursive definitions, or locally as asynchronous converging propagation processes. We present a distributed implementation of our calculus. The translation is first done mapping SMuC programs into normal form, purely iterative programs and then into distributed programs. Some key results are presented that show convergence of fixpoint computations under fair asynchrony and under reinitialization of nodes. The first result allows nodes to proceed at different speeds, while the second one provides robustness against certain kinds of failure. We illustrate our approach with a case study based on a disaster recovery scenario, implemented in a prototype simulator that we use to evaluate the performance of a recovery strategy.

Asynchronous Distributed Execution of Fixpoint-Based Computational Fields

Coordination is essential for dynamic distributed systems whose components exhibit interactive and autonomous behaviors. Spatially distributed, locally interacting, propagating computational fields are particularly appealing for allowing components to join and leave with little or no overhead. Computational fields are a key ingredient of aggregate programming, a promising software engineering methodology particularly relevant for the Internet of Things. In our approach, space topology is represented by a fixed graph-shaped field, namely a network with attributes on both nodes and arcs, where arcs represent interaction capabilities between nodes. We propose a SMuC calculus where μ-calculus-like modal formulas represent how the values stored in neighbor nodes should be combined to update the present node. Fixpoint operations can be understood globally as recursive definitions, or locally as asynchronous converging propagation processes. We present a distributed implementation of our calculus. The translation is first done mapping SMuC programs into normal form, purely iterative programs and then into distributed programs. Some key results are presented that show convergence of fixpoint computations under fair asynchrony and under reinitialization of nodes. The first result allows nodes to proceed at different speeds, while the second one provides robustness against certain kinds of failure. We illustrate our approach with a case study based on a disaster recovery scenario, implemented in a prototype simulator that we use to evaluate the performance of a recovery strategy.

General information

State: Accepted/In press
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, Università degli Studi di Firenze, University of Pisa
Authors: Lluch Lafuente, A. (Intern), Loreti, M. (Ekstern), Montanari, U. (Ekstern)
Number of pages: 47
Publication date: 2017
Main Research Area: Technical/natural sciences

Publication information

Journal: Logical Methods in Computer Science
ISSN (Print): 1860-5974
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 2
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 2
Scopus rating (2016): CiteScore 1.02 SJR 0.493 SNIP 1.149
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 0.579 SNIP 1.179 CiteScore 1.11
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 0.55 SNIP 1.312 CiteScore 1.06
Automated specification and verification of Web-based applications

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, Consiglio Nazionale delle Ricerche
Authors: ter Beek, M. H. (Ekstern), Lluch Lafuente, A. (Intern)
Pages: 51-51
Publication date: 2017
Main Research Area: Technical/natural sciences

Publication information
Journal: Journal of Logical and Algebraic Methods in Programming
Volume: 87
Ratings:
Web of Science (2018): Indexed yes
Web of Science (2017): Indexed Yes
Scopus rating (2016): CiteScore 0.88 SJR 0.394 SNIP 1.175
Scopus rating (2015): SJR 0.25 SNIP 1.166 CiteScore 0.55
Original language: English
DOIs:
10.1016/j.jlamp.2016.11.004
Publication: Research › Editorial – Annual report year: 2017

Many-to-Many Information Flow Policies
Information flow techniques typically classify information according to suitable security levels and enforce policies that are based on binary relations between individual levels, e.g., stating that information is allowed to flow from one level to another. We argue that some information flow properties of interest naturally require coordination patterns that involve sets of security levels rather than individual levels: some secret information could be safely disclosed to a set of confidential channels of incomparable security levels, with individual leaks considered instead illegal; a group of competing agencies might agree to disclose their secrets, with individual disclosures being undesired, etc. Motivated by this we propose a simple language for expressing information flow policies where the usual admitted flow relation between individual security levels is replaced by a relation between sets of security levels, thus allowing to capture coordinated flows of information. The flow of information is expressed in terms of causal dependencies and the satisfaction of a policy is defined with respect to an event structure that is assumed to capture the causal structure of system computations. We suggest applications to secret exchange protocols, program security and security architectures, and discuss the relation to classic
notions of information flow control.

Microservices: Yesterday, Today, and Tomorrow

Microservices is an architectural style inspired by service-oriented computing that has recently started gaining popularity. Before presenting the current state of the art in the field, this chapter reviews the history of software architecture, the reasons that led to the diffusion of objects and services first, and microservices later. Finally, open problems and future challenges are introduced. This survey primarily addresses newcomers to the discipline, while offering an academic viewpoint on the topic. In addition, we investigate some practical issues and point out a few potential solutions.
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.
A Fixpoint-Based Calculus for Graph-Shaped Computational Fields

Coordination is essential for dynamic distributed systems exhibiting autonomous behaviors. Spatially distributed, locally interacting, propagating computational fields are particularly appealing for allowing components to join and leave with little or no overhead. In our approach, the space topology is represented by a graph-shaped field, namely a network with attributes on both nodes and arcs, where arcs represent interaction capabilities between nodes. We propose a calculus where computation is strictly synchronous and corresponds to sequential computations of fixpoints in the graph-shaped field. Under some conditions, those fixpoints can be computed by synchronised iterations, where in each iteration the attributes of a node is updated based on the attributes of the neighbours in the previous iteration. Basic constructs are reminiscent of the semiring μ-calculus, a semiring-valued generalisation of the modal μ-calculus, which provides a flexible mechanism to specify the neighbourhood range (according to path formulae) and the way attributes should be combined (through semiring operators). Additional control-How constructs allow one to conveniently structure the fixpoint computations. We illustrate our approach with a case study based on a disaster recovery scenario, implemented in a prototype simulator that we use to evaluate the performance of a disaster recovery strategy.
**AVOCLOUDY: a simulator of volunteer clouds**

The increasing demand of computational and storage resources is shifting users toward the adoption of cloud technologies. Cloud computing is based on the vision of computing as utility, where users no more need to buy machines but simply access remote resources made available on-demand by cloud providers. The relationship between users and providers is defined by a service-level agreement, where the non-fulfillment of its terms is regulated by the associated penalty fees. Therefore, it is important that the providers adopt proper monitoring and managing strategies. Despite their reduced application, intelligent agents constitute a feasible technology to add autonomic features to cloud operations. Furthermore, the volunteer computing paradigm—one of the Information and Communications Technology (ICT) trends of the last decade—can be pulled alongside traditional cloud approaches, with the purpose to ‘green’ them. Indeed, the combination of data center and volunteer resources, managed by agents, allows one to obtain a more robust and scalable cloud computing platform. The increased challenges in designing such a complex system can benefit from a simulation-based approach, to test autonomic management solutions before their deployment in the production environment. However, currently available simulators of cloud platforms are not suitable to model and analyze such heterogeneous, large-scale, and highly dynamic systems. We propose the AVOCLOUDY simulator to fill this gap. This paper presents the internal architecture of the simulator, provides implementation details, summarizes several notable applications, and provides experimental results that measure the simulator performance and its accuracy. The latter experiments are based on real-world worldwide distributed computations on top of the PlanetLab platform.

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, University of Parma, IMT Institute for Advanced Studies Lucca
Authors: Sebastio, S. (Ektern), Amoretti, M. (Ektern), Lluch Lafuente, A. (Intern)
Pages: 3-30
Publication date: 2015
Main Research Area: Technical/natural sciences

**Publication information**

Journal: Software: Practice & Experience
Volume: 46
Issue number: 1
ISSN (Print): 0038-0644
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 2
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 2
Web of Science (2016): Indexed yes
Scopus rating (2016): SJR 0.409 SNIP 1.298 CiteScore 1.61
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 0.409 SNIP 1.208 CiteScore 1.41
Web of Science (2015): Indexed yes
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 0.539 SNIP 2.323 CiteScore 2.38
BFI (2013): BFI-level 2
Scopus rating (2013): SJR 0.55 SNIP 1.905 CiteScore 2.22
ISI indexed (2013): ISI indexed yes
BFI (2012): BFI-level 2
Scopus rating (2012): SJR 0.599 SNIP 1.875 CiteScore 2.05
ISI indexed (2012): ISI indexed yes
Web of Science (2012): Indexed yes
BFI (2011): BFI-level 2
Scopus rating (2011): SJR 0.343 SNIP 0.876 CiteScore 1.2
ISI indexed (2011): ISI indexed yes
BFI (2010): BFI-level 2
Scopus rating (2010): SJR 0.338 SNIP 0.961
Web of Science (2010): Indexed yes
BFI (2009): BFI-level 2
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.
This paper presents an approach to specify and check discretionary information flow properties of concurrent systems. The approach is inspired by the success of the interaction-oriented paradigm to concurrent systems (cf. choreographies, behavioural types, protocols,...) in providing behavioural guarantees of global properties such as deadlock-absence. We show how some information flow properties are easier to formalise and check on a global interaction-oriented description of a concurrent system rather than on a local process-oriented description of the components of the system. We use a simple choreography description language adapted from the literature of choreographies and session types. We provide a generic method to instrument the semantics with information flow annotations. Policies are used to specify the admissible flows of information. The main contribution of the paper is a sound type system for statically checking if a system specification ensures an information flow policy. The approach is illustrated with two archetypal examples of distributed and parallel computing systems: a protocol for an identity-secured data providing service and a parallel MapReduce computation.
Klaim-DB: A Modeling Language for Distributed Database Applications
We present the modelling language, Klaim-DB, for distributed database applications. Klaim-DB borrows the distributed nets of the coordination language Klaim but essentially re-incarnates the tuple spaces of Klaim as databases, and provides high-level language abstractions for the access and manipulation of structured data, with integrity and atomicity considerations. We present the formal semantics of KlaimDB and illustrate the use of the language in a scenario where the sales from different branches of a chain of department stores are aggregated from their local databases. It can be seen that raising the abstraction level and encapsulating integrity checks (concerning the schema of tables, etc.) in the language primitives for database operations benefit the modelling task considerably.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, East China Normal University
Authors: Wu, X. (Ekstern), Li, X. (Intern), Lluch Lafuente, A. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 197-212
Publication date: 2015

Host publication information
Title of host publication: Coordination Models and Languages: Proceedings of the 17th IFIP WG 6.1 International Conference (COORDINATION 2015)
Publisher: Springer
Editors: Holvoet, T., Viroli, M.
ISBN (Print): 978-3-319-19281-9
ISBN (Electronic): 978-3-319-19282-6

Series: Lecture Notes in Computer Science
Volume: 9037
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: 17th IFIP WG 6.1 International Conference, COORDINATION 2015, Grenoble, France, 02/06/2015 - 02/06/2015
Electronic versions:
klaim_db.pdf
DOIs:
10.1007/978-3-319-19282-6_13
Source: FindIt
Source-ID: 274873271
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Preface

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, University of Leicester
Authors: Lluch Lafuente, A. (Intern), Tuosto, E. (Ekstern)
Number of pages: 1
Pages: 211
Publication date: 2015
Main Research Area: Technical/natural sciences

Publication information
Journal: Service Oriented Computing and Applications
Volume: 9
Issue number: 3-4
ISSN (Print): 1863-2386
Ratings:
Web of Science (2018): Indexed yes
Proceedings 11th International Workshop on Automated Specification and Verification of Web Systems

These proceedings contain the papers presented at the 11th International Workshop on Automated Specification and Verification of Web Systems (WWV 2015), which was held on 23 June 2015 in Oslo, Norway, as a satellite workshop of the 20th International Symposium on Formal Methods (FM 2015). WWV is a yearly interdisciplinary forum for researchers originating from the following areas: declarative, rule-based programming, formal methods, software engineering and web-based systems. The workshop fosters the cross-fertilisation and advancement of hybrid methods from such areas.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Consiglio Nazionale delle Ricerche
Authors: ter Beek, M. H. (ed.) (Ekstern), Lluch Lafuente, A. (ed.) (Intern)
Publication date: 2015

Publication information
Original language: English
Series: Electronic Proceedings in Theoretical Computer Science
ISSN: 2075-2180
Main Research Area: Technical/natural sciences
DOIs: 10.4204/EPTCS.188
Publication: Research - peer-review › Book – Annual report year: 2015

Proceedings 8th Interaction and Concurrency Experience

This volume contains the proceedings of ICE 2015, the 8th Interaction and Concurrency Experience, which was held in Grenoble, France on the 4th and 5th of June 2015 as a satellite event of DisCoTec 2015. The ICE procedure for paper selection allows PC members to interact, anonymously, with authors. During the review phase, each submitted paper is published on a discussion forum with access restricted to the authors and to all the PC members not declaring a conflict of interest. The PC members post comments and questions to which the authors reply. Each paper was reviewed by three PC members, and altogether 9 papers, including 1 short paper, were accepted for publication (the workshop also featured 4 brief announcements which are not part of this volume). We were proud to host three invited talks, by Leslie Lamport (shared with the FRIDA workshop), Joseph Sifakis and Steve Ross-Talbot. The abstracts of the last two talks are included in this volume together with the regular papers.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Université de Lorraine, IMT Institute for Advanced Studies Lucca, Università di Bologna
Publication date: 2015

Publication information
Original language: English
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.
Replica-Based High-Performance Tuple Space Computing

We present the tuple-based coordination language RepliKlaim, which enriches Klaim with primitives for replica-aware coordination. Our overall goal is to offer suitable solutions to the challenging problems of data distribution and locality in large-scale high performance computing. In particular, RepliKlaim allows the programmer to specify and coordinate the replication of shared data items and the desired consistency properties. The programmer can hence exploit such flexible mechanisms to adapt data distribution and locality to the needs of the application, so to improve performance in terms of concurrency and data access. We investigate issues related to replica consistency, provide an operational semantics that guides the implementation of the language, and discuss the main synchronization mechanisms of our prototypical run-time framework. Finally, we provide a performance analysis, which includes scenarios where replica-based specifications and relaxed consistency provide significant performance gains.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, IMT Institute for Advanced Studies Lucca
Authors: Andric, M. (Ekstern), De Nicola, R. (Ekstern), Lluch Lafuente, A. (Intern)
Pages: 3-18
Publication date: 2015

Host publication information

Title of host publication: Coordination Models and Languages: Proceedings of the 17th IFIP WG 6.1 International Conference (COORDINATION 2015)
Publisher: Springer
Editors: Holvoet, T., Viroli, M.
ISBN (Print): 978-3-319-19281-9
ISBN (Electronic): 978-3-319-19282-6

Series: Lecture Notes in Computer Science
Volume: 9037
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: 17th IFIP WG 6.1 International Conference, COORDINATION 2015, Grenoble, France, 02/06/2015 - 02/06/2015

Electronic versions:
Replica_based_High_Performance_Tuple_Space_Computing.pdf. Embargo ended: 05/06/2016
DOIs:
10.1007/978-3-319-19282-6_1
Source: FindIt
Source-ID: 274873258
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015
Replicating Data for Better Performances in X10
Linguistic primitives for replica-aware coordination offer suitable solutions to the challenging problems of data distribution and locality in large-scale high-performance computing. The data replication mechanisms that had previously been designed to extend Klaim with replicated tuples are now used to experiment with X10, a parallel programming language primarily targeting clusters of multi-core processors linked in a large-scale system via high-performance networks. Our approach aims at allowing the programmer to specify and coordinate the replication of shared data items by taking into account the desired consistency properties. The programmer can hence exploit such flexible mechanisms to adapt data distribution and locality to the needs of the application, in order to improve performance in terms of concurrency and data access. We investigate issues related to replica consistency and provide a performance analysis, which includes scenarios where replica based specifications and relaxed consistency provide significant performance gains.

General information
State: Published
Organisations: Language-Based Technology, Department of Applied Mathematics and Computer Science , IMT Institute for Advanced Studies Lucca
Authors: Andrić, M. (Ekstern), De Nicola, R. (Ekstern), Lluch Lafuente, A. (Intern)
Pages: 236-251
Publication date: 2015

Host publication information
Title of host publication: Semantics, Logics, and Calculi : Essays Dedicated to Hanne Riis Nielson and Flemming Nielson on the Occasion of Their 60th Birthdays
Publisher: Springer
Editors: Probst, C. W., Hansen, R. R., Hankin, C.
ISBN (Print): 978-3-319-27809-4
ISBN (Electronic): 978-3-319-27810-0

Series: Lecture Notes in Computer Science
Volume: 9560
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
DOIs: 10.1007/978-3-319-27810-0_12
Source: FindIt
Source-ID: 2291785454
Publication: Research - peer-review › Book chapter – Annual report year: 2016

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 MultiVeSIA. 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
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
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Autonomic computing, Programming languages, Adaptation policies, Formal methods, Verification

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, Université Libre de Bruxelles, University of Limerick, Ludwig-Maximilians-Universität
Pages: 429-448
Publication date: 2015
A computational field framework for collaborative task execution in volunteer clouds
The increasing diffusion of cloud technologies offers new opportunities for distributed and collaborative computing. Volunteer clouds are a prominent example, where participants join and leave the platform and collaborate by sharing computational resources. The high complexity, dynamism and unpredictability of such scenarios call for decentralized self-* approaches. We present in this paper a framework for the design and evaluation of self-adaptive collaborative task execution strategies in volunteer clouds. As a byproduct, we propose a novel strategy based on the Ant Colony Optimization paradigm, that we validate through simulation-based statistical analysis over Google cluster data.

Can We Efficiently Check Concurrent Programs Under Relaxed Memory Models in Maude?
Relaxed memory models offer suitable abstractions of the actual optimizations offered by multi-core architectures and by compilers of concurrent programming languages. Using such abstractions for verification purposes is challenging in part due to their inherent non-determinism which contributes to the state space explosion. Several techniques have been proposed to mitigate those problems so to make verification under relaxed memory models feasible. We discuss how to adopt some of those techniques in a Maude-based approach to language prototyping, and suggest the use of other techniques that have been shown successful for similar verification purposes.
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.
Proceedings 3rd Workshop on GRAPH Inspection and Traversal Engineering (GRAPHITE 2014)
 These are the proceedings of the Third Workshop on GRAPH Inspection and Traversal Engineering (GRAPHITE 2014), which took place on April 5, 2014 in Grenoble, France, as a satellite event of the 17th European Joint Conferences on Theory and Practice of Software (ETAPS 2014).
 The aim of GRAPHITE is to foster the convergence on research interests from several communities dealing with graph analysis in all its forms in computer science, with a particular attention to software development and analysis. Graphs are used to represent data and processes in many application areas, and they are subjected to various computational algorithms in order to analyze them. Just restricting the attention to the analysis of software, graph analysis algorithms are used, for instance, to verify properties using model checking techniques that explore the system's state space graph or static analysis techniques based on control flow graphs. Further application domains include games, planning, and network analysis. Very often, graph problems and their algorithmic solutions have common characteristics, independent of their application domain. The goal of this event is to gather scientists from different communities, who do research on graph analysis algorithms, such that awareness of each others' work is increased.

General information
 State: Published
 Organisations: Department of Applied Mathematics and Computer Science , Language-Based Technology, Eindhoven University of Technology, University of Bremen
 Publication date: 2014
Proceedings of the 7th Interaction and Concurrency Experience (ICE 2014)
This volume contains the proceedings of ICE 2014, the 7th Interaction and Concurrency Experience, which was held in Berlin, Germany on the 6th of June 2014 as a satellite event of DisCoTec 2014. The ICE procedure for paper selection allows PC members to interact, anonymously, with authors. During the review phase, each submitted paper is published on a Wiki and associated with a discussion forum whose access is restricted to the authors and to all the PC members not declaring a conflict of interests. The PC members post comments and questions that the authors reply to. Each paper was reviewed by three PC members, and altogether 8 papers (including 3 short papers) were accepted for publication. We were proud to host two invited talks, by Pavol Cerny and Kim Larsen, whose abstracts are included in this volume together with the regular papers.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, University of Lisbon, Università di Bologna, Universität Salzburg
Number of pages: 110
Publication date: 2014

Publication information
Original language: English
Main Research Area: Technical/natural sciences
DOIs:
10.4204/EPTCS.159
Publication: Research - peer-review › Book – Annual report year: 2014

Proceedings of the 8th Symposium on Trustworthy Global Computing (TGC 2013)
This book constitutes the thoroughly refereed post-conference proceedings of the 8th International Symposium on Trustworthy Global Computing, TGC 2013, held in Buenos Aires, Argentina, in August 2013. The 15 revised full papers presented together with 3 invited talks were carefully reviewed and selected from 29 submissions. The papers cover a wide range of topics in the area of global computing and safe and reliable computation. They are organized in topical sections on security, π-calculus, information flow, models, specifications and proofs and quantitative analysis.

General information
State: Published
Organisations: University of California, Santa Cruz, IMT Institute for Advanced Studies Lucca
Authors: Abadi, M. (ed.) (Ekstern), Lluch Lafuente, A. (ed.) (Intern)
Number of pages: 331
Publication date: 2014

Publication information
ISBN (Print): 978-3-319-05118-5
ISBN (Electronic): 978-3-319-05119-2
Original language: English
Series: Lecture Notes in Computer Science
Volume: 8358
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Publication: Research - peer-review › Book – Annual report year: 2014

Programming and Verifying Component Ensembles
A simplified version of the kernel language SCEL, that we call SCELlight, is introduced as a formalism for programming and verifying properties of so-called cyber-physical systems consisting of software-intensive ensembles of components, featuring complex intercommunications and interactions with humans and other systems. In order to validate the
amenability of the language for verification purposes, we provide a translation of SCELlight specifications into Promela. We test the feasibility of the approach by formally specifying an application scenario, consisting of a collection of components offering a variety of services meeting different quality levels, and by using SPIN to verify that some desired behaviors are guaranteed.

General information
State: Published
Organisations: IMT Institute for Advanced Studies Lucca, Università degli Studi di Firenze
Authors: De Nicola, R. (Ekstern), Lluch Lafuente, A. (Intern), Loreti, M. (Ekstern), Morichetta, A. (Ekstern), Pugliese, R. (Ekstern), Senni, V. (Ekstern), Tiezzi, F. (Ekstern)
Pages: 69-83
Publication date: 2014

Host publication information
Publisher: Springer
ISBN (Print): 978-3-642-54847-5
ISBN (Electronic): 978-3-642-54848-2

Series: Lecture Notes in Computer Science
Volume: 8415
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: ETAPS Workshop, FPS 2014, Grenoble, France, 06/04/2014
DOIs: 10.1007/978-3-642-54848-2_5
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Reputation-based Cooperation in the Clouds
The popularity of the cloud computing paradigm is opening new opportunities for collaborative computing. In this paper we tackle a fundamental problem in open-ended cloud-based distributed computing platforms, i.e., the quest for potential collaborators. We assume that cloud participants are willing to share their computational resources for shared distributed computing problems, but they are not willing to disclose the details of their resources. Lacking such information, we advocate to rely on reputation scores obtained by evaluating the interactions among participants. More specifically, we propose a methodology to assess, at design time, the impact of different (reputation-based) collaborator selection strategies on the system performance. The evaluation is performed through statistical analysis on a volunteer cloud simulator.

General information
State: Published
Organisations: Istituto per le Applicazioni del Calcolo, Ludwig-Maximilians-Universität, IMT Institute for Advanced Studies Lucca
Authors: Celestini, A. (Ekstern), Lluch Lafuente, A. (Intern), Mayer, P. (Ekstern), Sebastio, S. (Ekstern), Tiezzi, F. (Ekstern)
Pages: 213-220
Publication date: 2014

Host publication information
Title of host publication: Trust Management VIII : 8th IFIP WG 11.11 International Conference, IFIPTM 2014, Singapore, July 7-10, 2014. Proceedings
ISBN (Print): 978-3-662-43812-1
ISBN (Electronic): 978-3-662-43813-8
Main Research Area: Technical/natural sciences
Conference: 8th IFIP WG 11.11 International Conference on Trust Management, Singapore, Singapore, 07/07/2014 - 07/07/2014
DOIs: 10.1007/978-3-662-43813-8_15
Publication: Research › Conference abstract in proceedings – Annual report year: 2014

A Cooperative Approach for Distributed Task Execution in Autonomic Clouds
Virtualization and distributed computing are two key pillars that guarantee scalability of applications deployed in the Cloud. In Autonomous Cooperative Cloud-based Platforms, autonomous computing nodes cooperate to offer a PaaS Cloud for the deployment of user applications. Each node must allocate the necessary resources for applications to be executed with certain QoS guarantees. If the QoS of an application cannot be guaranteed a node has mainly two options: to allocate
more resources (if it is possible) or to rely on the collaboration of other nodes. Making a decision is not trivial since it involves many factors (e.g. the cost of setting up virtual machines, migrating applications, discovering collaborators). In this paper we present a model of such scenarios and experimental results validating the convenience of cooperative strategies over selfish ones, where nodes do not help each other. We describe the architecture of the platform of autonomous clouds and the main features of the model, which has been implemented and evaluated in the DEUS discrete-event simulator. From the experimental evaluation, based on workload data from the Google Cloud Backend, we can conclude that (modulo our assumptions and simplifications) the performance of a volunteer cloud can be compared to that of a Google Cluster.

**General information**

State: Published
Organisations: University of Parma, IMT Institute for Advanced Studies Lucca
Authors: Amoretti, M. (Ekstern), Lluch Lafuente, A. (Intern), Sebastio, S. (Ekstern)
Number of pages: 8
Pages: 274-281
Publication date: 2013
Conference: 21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, Belfast, United Kingdom, 27/02/2013 - 27/02/2013
Main Research Area: Technical/natural sciences

**Publication information**

Journal: Euromicro Conference on Parallel, Distributed and Network-Based Processing. Proceedings
ISSN (Print): 1066-6192
Ratings:
- BFI (2016): BFI-level 1
- BFI (2015): BFI-level 1
- BFI (2014): BFI-level 1
- BFI (2013): BFI-level 1
- ISI indexed (2013): ISI indexed no
- BFI (2012): BFI-level 1
- ISI indexed (2012): ISI indexed no
- BFI (2011): BFI-level 1
- ISI indexed (2011): ISI indexed no
- BFI (2010): BFI-level 1
- BFI (2009): BFI-level 1
- BFI (2008): BFI-level 1
Original language: English
Cloud computing, Discrete event simulation, Quality of service, Distributed computer systems, Autonomous computing, Autonomous systems, Cooperative strategy, Discrete-event simulators, Distributed tasks, Experimental evaluation, Volunteer clouds, Volunteer computing, autonomic clouds, autonomous systems, cloud computing, distributed tasks execution, volunteer computing, COMPUTER, NETWORK VIRTUALIZATION, SERVICES, decision making, discrete event simulation, quality of service, resource allocation, software architecture, software fault tolerance, task analysis, virtual machines, virtualisation, autonomous cloud architecture, autonomous computing node, autonomous cooperative cloud-based platform, cooperative approach, DEUS, discrete event simulator, distributed computing, distributed task execution, Google Cloud Backend, node collaboration, PaaS cloud, QoS, user application deployment, virtualization

DOIs: 10.1109/PDP.2013.47
Source: FindIt
Source-ID: 240684631
Publication: Research - peer-review › Conference article – Annual report year: 2013

**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.

General information
State: Published
Organisations: Università di Pisa, IMT Institute for Advanced Studies Lucca
Authors: Bruni, R. (Ekstern), Corradini, A. (Ekstern), Gadducci, F. (Ekstern), Lluch Lafuente, A. (Intern), Vandin, A. (Intern)
Publication date: 2013

Host publication Information
Title of host publication: Tiny Transactions on Computer Science
Volume: 2
Main Research Area: Technical/natural sciences
Publication: Research - peer-review › Book chapter – Annual report year: 2013

Combining Declarative and Procedural Views in the Specification and Analysis of Product Families

General information
State: Published
Organisations: IMT Institute for Advanced Studies Lucca, Leiden University, University of Pisa
Authors: Ter Beek, M. (Ekstern), Lluch Lafuente, A. (Intern), Petrocchi, M. (Ekstern)
Publication date: 2013
Main Research Area: Technical/natural sciences
Publication: Research - peer-review › Paper – Annual report year: 2013

Constraint design rewriting
Constraint networks are hyper-graphs whose nodes and hyper-edges respectively represent variables and relations between them. The problem to assign values to variables by satisfying all constraints is NP-complete. We propose an algebraic approach to the design and transformation of constraint networks, inspired by Architectural Design Rewriting (ADR). The main idea is to exploit ADR to equip constraint networks with some hierarchical structure and represent them as terms of a suitable algebra, when possible. Constraint network transformations such as constraint propagations are then specified with efficient rewrite rules exploiting the network's structure provided by terms. The approach can be understood as (i) an extension of ADR with constraints, and (ii) an application of ADR to the design of reconfigurable constraint networks. © 2013 Elsevier B.V. All rights reserved.

General information
State: Accepted/In press
Organisations: Università di Pisa, IMT Institute for Advanced Studies Lucca
Authors: Bruni, R. (Ekstern), Lluch Lafuente, A. (Intern), Montanari, U. (Ekstern)
Publication date: 2013
Main Research Area: Technical/natural sciences

Publication information
Journal: Science of Computer Programming
ISSN (Print): 0167-6423
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 2
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 2
Scopus rating (2016): CiteScore 1.36 SJR 0.454 SNIP 1.271
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 0.442 SNIP 1.182 CiteScore 1.18
Web of Science (2015): Indexed yes
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 0.438 SNIP 1.479 CiteScore 1.2
Proceedings of the 6th Interaction and Concurrency Experience (ICE 2013)
This volume contains the proceedings of ICE 2013, the 6th Interaction and Concurrency Experience workshop, which was held in Florence, Italy on the 6th of June 2013 as a satellite event of DisCoTec 2013. The ICE procedure for paper selection allows PC members to interact, anonymously, with authors. During the review phase, each submitted paper is published on a Wiki and associated with a discussion forum whose access is restricted to the authors and to all the PC members not declaring a conflict of interests. The PC members post comments and questions that the authors reply to. Each paper was reviewed by three PC members, and altogether 6 papers were accepted for publication. We were proud to host two invited talks, Davide Sangiorgi and Filippo Bonchi, whose abstracts are included in this volume together with the regular papers. The workshop also featured a brief announcement of an already published paper.

General information
State: Published
Organisations: Universitá di Bologna, Universität Salzburg, IMT Institute for Advanced Studies Lucca, IT University of Copenhagen
Authors: Carbone, M. (ed.) (Ekstern), Lanese, I. (ed.) (Ekstern), Lluch Lafuente, A. (ed.) (Intern), Sokolova, A. (ed.) (Ekstern)
Publication date: 2013

Publication information
Publisher: Open Publishing Association
Original language: English
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.
Evaluating the performance of model transformation styles with Maude

Rule-based programming has been shown to be very successful in many application areas. Two prominent examples are the specification of model transformations in model driven development approaches and the definition of structured operational semantics of formal languages. General rewriting frameworks such as Maude are flexible enough to allow the programmer to adopt and mix various rule styles. The choice between styles can be biased by the programmer's background. For instance, experts in visual formalisms might prefer graph-rewriting styles, while experts in semantics might prefer structurally inductive rules. This paper evaluates the performance of different rule styles on a significant benchmark taken from the literature on model transformation. Depending on the actual transformation being carried out, our results show that different rule styles can offer drastically different performances. We point out the situations from which each rule style benefits to offer a valuable set of hints for choosing one style over the other.
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.

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.

On structured model-driven transformations
Structural aspects play a key role in the model-driven development of software systems. Effective techniques and tools must therefore be based on suitable representation formalisms that facilitate the specification, manipulation and analysis
of the structure of models. Graphical and algebraic approaches have been shown to be very successful for such purposes: 1) graphs offer natural a representation of topological structures, 2) algebras offer a natural representation of compositional structures, 3) both graphs and algebras can be manipulated in a declarative way by means of rule-based techniques, 4) they allow for a layered presentation of models that enables compositional techniques and favours scalability. Most of the existing approaches represent such layering in a plain manner by overlapping the intra- and the inter-layered structure. It has been shown that some layering structures can be conveniently represented by an explicit hierarchical structure enabling then structurally inductive manipulations of the resulting models. Moreover, providing an inductive presentation of the structure facilitates the compositional analysis and verification of models. In this paper we compare and reconcile some recent approaches and synthesise them into an algebraic and graph-based formalism for representing and manipulating models with inductively defined hierarchical structure. Key words: hierarchical graphs; rewriting logic; model transformations

General information
State: Published
Organisations: University of Pisa, IMT Institute for Advanced Studies Lucca
Authors: Bruni, R. (Ekstern), Lluch Lafuente, A. (Intern), Montanari, U. (Ekstern)
Pages: 185-206
Publication date: 2012
Main Research Area: Technical/natural sciences

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.

General information
State: Published
Organisations: University of Illinois, IMT Institute for Advanced Studies Lucca
Authors: Lluch Lafuente, A. (Intern), Meseguer, J. (Ekstern), Vandin, A. (Intern)
Pages: 430-446
Publication date: 2012

Host publication information
Publisher: Springer Berlin Heidelberg
ISBN (Print): 978-3-642-34280-6
ISBN (Electronic): 978-3-642-34281-3
Series: Lecture Notes in Computer Science
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: 14th International Conference on Formal Engineering Methods, Kyoto, Japan, 12/11/2012 - 12/11/2012
DOIs: 10.1007/978-3-642-34281-3_30
Publication: Research - peer-review › Article in proceedings – Annual report year: 2012

A formal support to business and architectural design for service-oriented systems
Architectural Design Rewriting (ADR) is an approach for the design of software architectures developed within Sensoria by reconciling graph transformation and process calculi techniques. The key feature that makes ADR a suitable and
expressive framework is the algebraic handling of structured graphs, which improves the support for specification, analysis and verification of service-oriented architectures and applications. We show how ADR is used as a formal ground for high-level modelling languages and approaches developed within Sensoria.

General information
State: Published
Organisations: Imperial College London, University of Pisa, IMT Institute for Advanced Studies Lucca, University of Leicester
Authors: Bruni, R. (Ekstern), Foster, H. (Ekstern), Lluch Lafuente, A. (Intern), Montanari, U. (Ekstern), Tuosto, E. (Ekstern)
Pages: 133-152
Publication date: 2011

Host publication information
Title of host publication: Rigorous Software Engineering for Service-Oriented Systems : Results of the SENSORIA Project on Software Engineering for Service-Oriented Computing
Publisher: Springer Berlin Heidelberg
ISBN (Print): 978-3-642-20400-5
ISBN (Electronic): 978-3-642-20401-2
Series: Lecture Notes in Computer Science
Volume: 6582
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
DOIs: 10.1007/978-3-642-20401-2_7
Publication: Research - peer-review › Book chapter – Annual report year: 2011

A Lewisian approach to the verification of adaptive systems
Many software artifacts like software architectures or distributed programs are characterized by a high level of dynamism involving changes in their structure or behaviour as a response to external stimuli or as the result of programmed reconfigurations. When reasoning on such adaptive systems one is not only interested in proving properties on their global behaviour like system correctness, but also on the evolution of the single components. For instance, when analysing the well-known stable marriage problem one would like to know whether a solution ensures that “two females never claim to be married with the same male”. To enable automatic reasoning, two main things are needed: models for the software artifacts and logic-based languages for describing their properties. One of the most successful and versatile model for such artifacts are graphs. Regarding the property specification languages, variants of quantified temporal logics have been proposed, which combine the modal operators of temporal logics with monadic second-order logic for graphs. Unfortunately, the semantical models for such logics are not clearly cut, due to the possibility to interleave modal operators and quantifiers in formulae like $\forall x.\Diamond \psi$ where $x$ is quantified in a world but $\psi$ states properties about $x$ in a reachable world or state where it does not necessarily exist or even have the same identity. The issue is denoted in the quantified temporal logic literature as trans-world identity [1, 3]. A typical solution follows the so-called “Kripke semantics” approach: roughly, a set of universal items is chosen, and its elements are used to form each state. This solution is the most widely adopted, and it underlines all the proposals we are aware of Kripke-like solutions do not fit well with the merging, deletion and creation of components, neither allows for an easy inclusion of evolution relations possibly forming cycles: if the value of an open formula is a set of states, how to account e.g. for an element that is first deleted and then added again? This problem is often solved by restricting the class of admissible evolution relations: this forces to reformulate the state transition relation modeling the system evolution, hampering the intuitive meaning of the logic. In [2, 5] we presented an alternative approach, inspired to counterpart theory [4]. The key point of Lewis's proposal is the notion of counterpart, which is a consequence of his refusal to interpret the relation of trans-world sameness as strict identity. In our approach we exploit counterpart relations, i.e. (partial) functions among states, explicitly relating elements of different states. Our solution avoids some limitations of the existing approaches, in particular in what regards the treatment of the possible merging and reuse of components. Moreover, the resulting semantics is a streamlined and intuitively appealing one, yet it is general enough to cover most of the alternatives 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. (Ekstern)
Publication date: 2011
Main Research Area: Technical/natural sciences

Publication information
Journal: Rivista Italiana di Filosofia Analitica Junior
Volume: 2
Issue number: 2
Hierarchical models for service-oriented systems

General information
State: Published
Organisations: University of Pisa, IMT Institute for Advanced Studies Lucca
Authors: Bruni, R. (Ekstern), Corradini, A. (Ekstern), Gadducci, F. (Ekstern), Lluch Lafuente, A. (Intern), Montanari, U. (Ekstern)
Pages: 349-368
Publication date: 2011

Host publication information
Title of host publication: Rigorous Software Engineering for Service-Oriented Systems: Results of the SENSORIA project on Software Engineering for Service-Oriented Computing
Publisher: Springer Berlin Heidelberg
ISBN (Print): 978-3-642-20400-5
ISBN (Electronic): 978-3-642-20401-2
Series: Lecture Notes in Computer Science
Volume: 6582
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
DOIs:
10.1007/978-3-642-20401-2_16
Publication: Research - peer-review » Journal article – Annual report year: 2011

Internet e Web 2.0

General information
State: Published
Organisations: IMT Institute for Advanced Studies Lucca
Authors: Lluch Lafuente, A. (Intern)
Publication date: 2011

Publication information
ISBN (Print): 978-8860083418
Original language: English
Main Research Area: Technical/natural sciences
Publication: Research - peer-review » Book – Annual report year: 2011

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-calculi 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.

General information
State: Published
Organisations: IMT Institute for Advanced Studies Lucca
Authors: Lluch Lafuente, A. (Intern), Vandin, A. (Intern)
A formalisation of Adaptable Pervasive Flows

Adaptable Pervasive Flows is a novel workflow-based paradigm for the design and execution of pervasive applications, where dynamic workflows situated in the real world are able to modify their execution in order to adapt to changes in their environment. In this paper, we study a formalisation of such flows by means of a formal flow language. More precisely, we define APFoL (Adaptable Pervasive Flow Language) and formalise its textual notation by encoding it in Blite, a formalisation of WS-BPEL. The encoding in Blite equips the language with a formal semantics and enables the use of automated verification techniques. We illustrate the approach with an example of a Warehouse Case Study.
A Graph Syntax for Processes and Services
We propose a class of hierarchical graphs equipped with a simple algebraic syntax as a convenient way to describe configurations in languages with inherently hierarchical features such as sessions, fault-handling scopes or transactions. The graph syntax can be seen as an intermediate representation language, that facilitates the encoding of structured specifications and, in particular, of process calculi, since it provides primitives for nesting, name restriction and parallel composition. The syntax is based on an algebraic presentation that faithfully characterises families of hierarchical graphs, meaning that each term of the language uniquely identifies an equivalence class of graphs (modulo graph isomorphism). Proving soundness and completeness of an encoding (i.e. proving that structurally equivalent processes are mapped to isomorphic graphs) is then facilitated and can be done by structural induction. Summing up, the graph syntax facilitates the definition of faithful encodings, yet allowing a precise visual representation. We illustrate our work with an application to a workflow language and a service-oriented calculus.

An Algebra of Hierarchical Graphs
We define an algebraic theory of hierarchical graphs, whose axioms characterise graph isomorphism: two terms are equated exactly when they represent the same graph. Our algebra can be understood as a high-level language for describing graphs with a node-sharing, embedding structure, and it is then well suited for defining graphical representations of software models where nesting and linking are key aspects.
An algebra of hierarchical graphs and its application to structural encoding

We define an algebraic theory of hierarchical graphs, whose axioms characterise graph isomorphism: two terms are equated exactly when they represent the same graph. Our algebra can be understood as a high-level language for describing graphs with a node-sharing, embedding structure, and it is then well suited for defining graphical representations of software models where nesting and linking are key aspects. In particular, we propose the use of our graph formalism as a convenient way to describe configurations in process calculi equipped with inherently hierarchical features such as sessions, locations, transactions, membranes or ambients. The graph syntax can be seen as an intermediate representation language, that facilitates the encodings of algebraic specifications, since it provides primitives for nesting, name restriction and parallel composition. In addition, proving soundness and correctness of an encoding (i.e. proving that structurally equivalent processes are mapped to isomorphic graphs) becomes easier as it can be done by induction over the graph syntax.

Counterpart semantics for a secondorder mu-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.
Exploiting the hierarchical structure of rule-based specifications for decision planning

Rule-based specifications have been very successful as a declarative approach in many domains, due to the handy yet solid foundations offered by rule-based machineries like term and graph rewriting. Realistic problems, however, call for suitable techniques to guarantee scalability. For instance, many domains exhibit a hierarchical structure that can be exploited conveniently. This is particularly evident for composition associations of models. We propose an explicit representation of such structured models and a methodology that exploits it for the description and analysis of model- and rule-based systems. The approach is presented in the framework of rewriting logic and its efficient implementation in the rewrite engine Maude and is illustrated with a case study.

Rewriting nested graphs, through term graphs

We present an algebra for graphs with nesting and restriction features as a handy linear syntax for denoting a class of hierarchical graphs. We discuss how such graphs can be encoded into term graphs, showing that through this translation we can borrow definitions and results from the established theory of term graph rewriting.
A service-oriented UML profile with formal support

We present a UML Profile for the description of service oriented applications. The profile focuses on style-based design and reconfiguration aspects at the architectural level. Moreover, it has formal support in terms of an approach called Architectural Design Rewriting, which enables formal analysis of the UML specifications. We show how our prototypical implementation can be used to analyse and verify properties of a service oriented application.

Hierarchical Design Rewriting with Maude

Architectural Design Rewriting (ADR) is a rule-based approach for the design of dynamic software architectures. The key features that make ADR a suitable and expressive framework are the algebraic presentation and the use of conditional rewrite rules. These features enable, e.g. hierarchical (top-down, bottom-up or composition-based) design and inductively-defined reconfigurations. The contribution of this paper is twofold: we define Hierarchical Design Rewriting (HDR) and present our prototypical tool support. HDR is a flavour of ADR that exploits the concept of hierarchical graph to deal with system specifications combining both symbolic and interpreted parts. Our prototypical implementation is based on Maude and its presentation serves several purposes. First, we show that HDR is not only a well-founded formal approach but also a tool-supported framework for the design and analysis of software architectures. Second, our illustration tailored to a particular algebra of designs and a particular scenario traces a general methodology for the reuse and exploitation of ADR concepts in other scenarios.
On Symbolic Semantics for Namedecorated Contexts

Under several regards, various of the recently proposed computational paradigms are open-ended, i.e. they may comprise components whose behaviour is not or cannot be fully specified. For instance, applications can be distributed across different administration domains that do not fully disclose their internal business processes to each other, or the dynamics of the system may allow reconfigurations and dynamic bindings whose specification is not available at design time. While a large set of mature design and analysis techniques for closed systems have been developed, their lifting to the open case is not always straightforward. Some existing approaches in the process calculi community are based on the need of proving properties for components that may hold in any, or significantly many, execution environments. Dually, frameworks describing the dynamics of systems with unspecified components have also been presented. In this paper we
lay some preliminary ideas on how to extend a symbolic semantics model for open systems in order to deal with name-based calculi. Moreover, we also discuss how the use of a simple type system based on name-decoration for unknown components can improve the expressiveness of the framework. The approach is illustrated on a simple, paradigmatic calculus of web crawlers, which can be understood as a term representation of a simple class of graphs.
Partial-order reduction for general state exploring algorithms

Partial-order reduction is one of the main techniques used to tackle the combinatorial state explosion problem occurring in explicit-state model checking of concurrent systems. The reduction is performed by exploiting the independence of concurrently executed events, which allows portions of the state space to be pruned. An important condition for the soundness of partial-order-based reduction algorithms is a condition that prevents indefinite ignoring of actions when pruning the state space. This condition is commonly known as the cycle proviso. In this paper, we present a new version of this proviso, which is applicable to a general search algorithm skeleton that we refer to as the general state exploring algorithm (GSEA). GSEA maintains a set of open states from which states are iteratively selected for expansion and moved to a closed set of states. Depending on the data structure used to represent the open set, GSEA can be instantiated as a depth-first, a breadth-first, or a directed search algorithm such as Best-First Search or A*. The proviso is characterized by reference to the open and closed set of states of the search algorithm. As a result, it can be computed in an efficient manner during the search based on local information. We implemented partial-order reduction for GSEA based on our proposed proviso in the tool HSF-SPIN, an extension of the explicit-state model checker SPIN for directed model checking. We evaluate the state space reduction achieved by partial-order reduction using the proposed proviso by comparing it on a set of benchmark problems to the use of other provisos. We also compare the use of breadth-first search (BFS) and A*, two algorithms ensuring that counterexamples of minimal length will be found, together with the proviso that we propose. © Springer-Verlag 2008.

General information
State: Published
Organisations: Eindhoven University of Technology, University of Konstanz, University of Pisa
Authors: Bošnacki, D. (Ekstern), Leue, S. (Ekstern), Lluch Lafuente, A. (Intern)
Number of pages: 13
Pages: 39-51
Publication date: 2009
Main Research Area: Technical/natural sciences

Publication information
Journal: International Journal on Software Tools for Technology Transfer
Volume: 11
Issue number: 1
ISSN (Print): 1433-2779
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 1
Scopus rating (2016): SJR 0.574 SNIP 1.642 CiteScore 2.14
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.587 SNIP 1.587 CiteScore 1.59
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.469 SNIP 1.6 CiteScore 1.5
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.585 SNIP 1.884 CiteScore 1.62
ISI indexed (2013): ISI indexed no
Specification and Analysis with Hierarchical Graphs

Ten virtues of structured graphs
This paper extends the invited talk by the first author about the virtues of structured graphs. The motivation behind the talk and this paper relies on our experience on the development of ADR, a formal approach for the design of styleconformant, reconfigurable software systems. ADR is based on hierarchical graphs with interfaces and it has been conceived in the attempt of reconciling software architectures and process calculi by means of graphical methods. We have tried to write an ADR agnostic paper where we raise some drawbacks of flat, unstructured graphs for the design and analysis of software systems and we argue that hierarchical, structured graphs can alleviate such drawbacks.
Architectural Design Rewriting as an Architecture Description Language

Architectural Design Rewriting (ADR) is a declarative rule-based approach for the design of dynamic software architectures. The key features that make ADR a suitable and expressive framework are the algebraic presentation of graph-based structures and the use of conditional rewrite rules. These features enable the modelling of, e.g. hierarchical design, inductively defined reconfigurations and ordinary computation. Here, we promote ADR as an Architectural Description Language.

Graph-Based Design and Analysis of Dynamic Software Architectures

We illustrate two ways to address the specification, modelling and analysis of dynamic software architectures using: i) ordinary typed graph transformation techniques implemented in Alloy; ii) a process algebraic presentation of graph transformation implemented in Maude. The two approaches are compared by showing how different aspects can be tackled, including representation issues, modelling phases, property specification and analysis.

On GS-Monoidal Theories for Graphs with Nesting

We propose a sound and complete axiomatisation of a class of graphs with nesting and either locally or globally restricted nodes. Such graphs allow to represent explicitly and at the right level of abstraction some relevant topological and logical
features of models and systems, including nesting, hierarchies, sharing of resources, and pointers or links. We also
provide an encoding of the proposed algebra into terms of a gs-monoidal theory, and through these into a suitable class of
"wellscoped" term graphs, showing that this encoding is sound and complete with respect to the axioms of the algebra.

**General information**
State: Published
Organisations: Università di Pisa, IMT Institute for Advanced Studies Lucca
Authors: Bruni, R. (Ekstern), Corradini, A. (Ekstern), Gadducci, F. (Ekstern), Lluch Lafuente, A. (Intern), Montanari, U. (Ekstern)
Pages: 59-86
Publication date: 2008

**Host publication information**
Title of host publication: Graph Transformations and Model-Driven Engineering : Essays Dedicated to Manfred Nagl on the
Occasion of his 65th Birthday
Publisher: Springer Berlin Heidelberg
ISBN (Print): 978-3-642-17321-9
ISBN (Electronic): 978-3-642-17322-6

Series: Lecture Notes in Computer Science
Volume: 5765
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
DOIs: 10.1007/978-3-642-17322-6_4
Publication: Research - peer-review › Book chapter – Annual report year: 2008

**Service Oriented Architectural Design**
We propose Architectural Design Rewriting (ADR), an approach to formalise the development and reconfiguration of
software architectures based on term-rewriting. An architectural style consists of a set of architectural elements and
operations called productions which define the well-formed compositions of architectures. Roughly, a term built out of such
ingredients constitutes the proof that a design was constructed according to the style, and the value of the term is the
constructed software architecture. A main advantage of ADR is that it naturally supports style-preserving reconfigurations.
The usefulness of our approach is shown by applying ADR to SRML, an emergent paradigm inspired by the Service
Component Architecture. We model the complex operation that composes several SRML modules in a single one by
means of suitable rewrite rules. Our approach guarantees that the resulting module respects SRML’s metamodel.

**General information**
State: Published
Organisations: University of Pisa, University of Leicester
Authors: Bruni, R. (Ekstern), Lluch Lafuente, A. (Intern), Montanari, U. (Ekstern), Tuosto, E. (Ekstern)
Pages: 186-203
Publication date: 2008

**Host publication information**
Title of host publication: Trustworthy Global Computing : Third Symposium, TGC 2007, Sophia-Antipolis, France,
November 5-6, 2007, Revised Selected Papers
ISBN (Print): 978-3-540-78662-7
ISBN (Electronic): 978-3-540-78663-4

Series: Lecture Notes in Computer Science
Volume: 4912
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: 3rd International Symposium on Trustworthy Global Computing, Sophia-Antipolis, France, 05/11/2007 -
05/11/2007
DOIs: 10.1007/978-3-540-78663-4_14
Publication: Research - peer-review › Article in proceedings – Annual report year: 2008

**Style-Based Architectural Reconfigurations**

**General information**
State: Published
Organisations: University of Pisa, University of Leicester
A Temporal Graph Logic for Abstractions of Graph Rewriting Systems

We extend our approach for verifying properties of graph transformation systems using suitable abstractions. In the original approach properties are specified as formulae of a propositional temporal logic whose atomic predicates are monadic second-order graph formulae. We generalize this aspect by considering more expressive logics, where edge quantifiers and temporal modalities can be interleaved, a feature which allows, e.g., to trace the history of objects in time. This requires the use of graph transition systems, a generalization of transition systems where states and transitions are mapped to graphs and graph morphisms, respectively, and of a corresponding notion of abstraction. After characterizing fragments of the logic which can be safely checked on the approximations, we show how the verification of the logic over graph transformation systems can be reduced to the verification of a logic over suitably defined Petri nets.

A Temporal Graph Logic for Abstractions of Graph Rewriting Systems

We extend our approach for verifying properties of graph transformation systems using suitable abstractions. In the original approach properties are specified as formulae of a propositional temporal logic whose atomic predicates are monadic second-order graph formulae. We generalize this aspect by considering more expressive logics, where edge quantifiers and temporal modalities can be interleaved, a feature which allows, e.g., to trace the history of objects in time. This requires the use of graph transition systems, a generalization of transition systems where states and transitions are mapped to graphs and graph morphisms, respectively, and of a corresponding notion of abstraction. After characterizing fragments of the logic which can be safely checked on the approximations, we show how the verification of the logic over graph transformation systems can be reduced to the verification of a logic over suitably defined Petri nets.

A Temporal Graph Logic for Abstractions of Graph Rewriting Systems

We extend our approach for verifying properties of graph transformation systems using suitable abstractions. In the original approach properties are specified as formulae of a propositional temporal logic whose atomic predicates are monadic second-order graph formulae. We generalize this aspect by considering more expressive logics, where edge quantifiers and temporal modalities can be interleaved, a feature which allows, e.g., to trace the history of objects in time. This requires the use of graph transition systems, a generalization of transition systems where states and transitions are mapped to graphs and graph morphisms, respectively, and of a corresponding notion of abstraction. After characterizing fragments of the logic which can be safely checked on the approximations, we show how the verification of the logic over graph transformation systems can be reduced to the verification of a logic over suitably defined Petri nets.
Graphical Encoding of a Spatial Logic for the pi-calculus

This paper extends our graph-based approach to the verification of spatial properties of π-calculus specifications. The mechanism is based on an encoding for mobile calculi where each process is mapped into a graph (with interfaces) such that the denotation is fully abstract with respect to the usual structural congruence, i.e., two processes are equivalent exactly when the corresponding encodings yield isomorphic graphs. Behavioral and structural properties of π-calculus processes expressed in a spatial logic can then be verified on the graphical encoding of a process rather than on its textual representation. In this paper we introduce a modal logic for graphs and define a translation of spatial formulae such that a process verifies a spatial formula exactly when its graphical representation verifies the translated modal graph formula.

Towards Model Checking Spatial Properties with SPIN

We present an approach for the verification of spatial properties with Spin. We first extend one of Spin’s main property specification mechanisms, i.e., the linear-time temporal logic LTL, with spatial connectives that allow us to restrict the reasoning of the behaviour of a system to some components of the system, only. For instance, one can express whether the system can reach a certain state from which a subset of processes can evolve alone until some property is fulfilled. We give a model checking algorithm for the logic and propose how Spin can be minimally extended to include the algorithm. We also discuss potential improvements to mitigate the exponential complexity introduced by spatial connectives. Finally, we present some experiments that compare our Spin extension with a spatial model checker for the π-calculus.
A Logic for Application Level QoS

Service Oriented Computing (SOC) has been proposed as a paradigm to describe computations of applications on wide area distributed systems. Awareness of Quality of Service (QoS) is emerging as a new exigency in both design and implementation of SOC applications. We do not refer to QoS aspects related to low-level performance and focus on those high-level non-functional features perceived by end-users as application dependent requirements, e.g., the price of a given service, or the payment mode, or else the availability of a resource (e.g., a file in a given format). In this paper we present a logic which includes mechanisms to consider the three main dimensions of systems, namely their structure, behaviour and QoS aspects. The evaluation of a formula is a value of a constraint-semiring and not just a boolean value expressing whether or not the formula holds. This permits to express not only topological and temporal properties but also QoS properties of systems. The logic is interpreted on SHReQ, a formal framework for specifying systems that handles abstract high-level QoS aspects combining Synchronised Hyperedge Replacement with constraint-semirings. © 2006 Elsevier B.V. All rights reserved.
A logic for graphs with QoS

We introduce a simple graph logic that supports specification of Quality of Service (QoS) properties of applications. The idea is that we are not only interested in representing whether two sites are connected, but we want to express the QoS level of the connection. The evaluation of a formula in the graph logic is a value of a suitable algebraic structure, a c-semiring, representing the QoS level of the formula and not just a boolean value expressing whether or not the formula holds. We present some examples and briefly discuss the expressiveness and complexity of our logic. © 2005 Elsevier B.V. All rights reserved.

General information
State: Published
Organisations: Università di Pisa
Authors: Ferrari, G. (Ekstern), Lluch Lafuente, A. (Intern)
Number of pages: 18
Pages: 143-160
Publication date: 2006
Main Research Area: Technical/natural sciences

Publication information
Journal: Electronic Notes in Theoretical Computer Science
Volume: 142
Issue number: SPEC. ISS.
ISSN (Print): 1571-0661
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
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
Graphs are suitable modeling formalisms for software and hardware systems involving aspects such as communication, object orientation, concurrency, mobility and distribution. State spaces of such systems can be represented by graph transition systems, which are basically transition systems whose states and transitions represent graphs and graph morphisms. Heuristic search is a successful Artificial Intelligence technique for solving exploration problems implicitly present in games, planning, and formal verification. Heuristic search exploits information about the problem being solved to guide the exploration process. The main benefits are significant reductions in the search effort and the size of solutions.

We propose the application of heuristic search for the analysis of graph transition systems. We define algorithms and heuristics and present experimental results.
Partial-Order Reduction for General State Exploring Algorithms

An important component of partial-order based reduction algorithms is the condition that prevents action ignoring, commonly known as the cycle proviso. In this paper we give a new version of this proviso that is applicable to a general search algorithm skeleton also known as the General State Expanding Algorithm (GSEA). GSEA maintains a set of open (visited but not expanded) states from which states are iteratively selected for exploration and moved to a closed set of states (visited and expanded). Depending on the open set data structure used, GSEA can be instantiated as depth-first, breadth-first, or a directed search algorithm. The proviso is characterized by reference to the open and closed set of states in GSEA. As a result the proviso can be computed in an efficient manner during the search based on local information. We implemented partial-order reduction for GSEA based on our proposed proviso in the tool HSF-SPIN, which is an extension of the model checker SPIN for directed model checking. We evaluate the state space reduction achieved by partial-order reduction according to the proviso that we propose by comparing it on a set of benchmark problems to other reduction approaches. We also compare the use of breadth-first search and A*, two algorithms ensuring that counterexamples of minimal length will be found, together with the proviso that we propose.

General information
State: Published
Organisations: Eindhoven University of Technology, University of Konstanz, via del Giardino A 58
Authors: Bošnački, D. (Ekstern), Leue, S. (Ekstern), Lluch Lafuente, A. (Intern)
Pages: 271-287
Publication date: 2006

Host publication information
Title of host publication: Model Checking Software : 13th International SPIN Workshop, Vienna, Austria, March 30 - April 1, 2006. Proceedings
Publisher: Springer Berlin Heidelberg
ISBN (Print): 978-3-540-33102-5
ISBN (Electronic): 978-3-540-33103-2

Action Planning for Graph Transition Systems

Graphs are suitable modeling formalisms for software and hardware systems involving aspects such as communication, object orientation, concurrency, mobility and distribution. State spaces of such systems can be represented by graph transition systems, which are basically transition systems whose states and transitions represent graphs and graph morphisms. In this paper, we propose the modeling of graph transition systems in PDDL and the application of heuristic search planning for their analysis. We consider different heuristics and present experimental results.

General information
State: Published
Organisations: University of Dortmund, Università di Pisa
Authors: Edelkamp, S. (Ekstern), Jabbar, S. (Ekstern), Lluch Lafuente, A. (Intern)
Publication date: 2005
Cost-Algebraic Heuristic Search

Heuristic search is used to efficiently solve the single-node shortest path problem in weighted graphs. In practice, however, one is not only interested in finding a short path, but an optimal path, according to a certain cost notion. We propose an algebraic formalism that captures many cost notions, like typical Quality of Service attributes. We thus generalize A*, the popular heuristic search algorithm, for solving optimal-path problem. The paper provides an answer to a fundamental question for AI search, namely to which general notion of cost, heuristic search algorithms can be applied. We proof correctness of the algorithms and provide experimental results that validate the feasibility of the approach.

Graphical encoding of a spatial logic for the pi-calculus

This paper extends our graph-based approach to the verification of spatial properties of pi-calculus specifications. The mechanism is based on an encoding for mobile calculi where each process is mapped into a graph (with interfaces) such that the denotation is fully abstract with respect to the usual structural congruence, i.e., two processes are equivalent exactly when the corresponding encodings yield isomorphic graphs. Behavioral and structural properties of pi-calculus processes expressed in a spatial logic can then be verified on the graphical encoding of a process rather than on its textual representation. In this paper we introduce a modal logic for graphs and define a translation of spatial formulae such that a process verifies a spatial formula exactly when its graphical representation verifies the translated modal graph formula.
Quantitative mu-calculus and CTL defined over constraint semirings

Model checking and temporal logics are boolean. The answer to the model checking question does a system satisfy a property? is either true or false, and properties expressed in temporal logics are defined over boolean propositions. While this classic approach is enough to specify and verify boolean temporal properties, it does not allow to reason about quantitative aspects of systems. Some quantitative extensions of temporal logics has been already proposed, especially in the context of probabilistic systems. They allow to answer questions like with which probability does a system satisfy a property? We present a generalization of two well-known temporal logics: CTL and the mu-calculus. Both extensions are defined over c-semirings, an algebraic structure that captures quantitative aspects like quality of service or soft constraints. Basically, a c-semiring consists of a domain, an additive operation and a multiplicative operation, which satisfy some properties. We present the semantics of the extended logics over transition systems, where a formula is interpreted as a mapping from the set of states to the domain of the c-semiring, and show that the usual connection between CTL and mu-calculus does not hold in general. In addition, we reason about the complexity of computing the logics and illustrate some applications of our framework, including boolean model checking. (c) 2005 Elsevier B.V. All rights reserved.
Quantitative μ-calculus and CTL Based on Constraint Semirings

Model checking and temporal logics are boolean. The answer to the model checking question does a system satisfy a property? is either true or false, and properties expressed in temporal logics are defined over boolean propositions. While this classic approach is enough to specify and verify boolean temporal properties, it does not allow to reason about quantitative aspects of systems. Some quantitative extensions of temporal logics has been already proposed, especially in the context of probabilistic systems. They allow to answer questions like with which probability does a system satisfy a property? We present a generalization of two well-known temporal logics: CTL and the μ-calculus. Both extensions are defined over c-semirings, an algebraic structure that captures many problems and that has been proposed as a general framework for soft constraint satisfaction problems (CSP). Basically, a c-semiring consists of a domain, an additive operation and a multiplicative operation, which satisfy some properties. We present the semantics of the extended logics over transition systems, where a formula is interpreted as a mapping from the set of states to the domain of the c-semiring, and show that the usual connection between CTL and μ-calculus does not hold in general. In addition, we reason about the feasibility of computing the logics and illustrate some applications of our framework, including boolean model checking.

General information
State: Published
Organisations: Università di Pisa
Authors: Montanari, U. (Ekstern), Lluch Lafuente, A. (Intern)
Number of pages: 23
Pages: 37-59
Publication date: 2005
Conference: 2nd Workshop on Quantitative Aspects of Programming Languages, Barcelona, Spain, 27/03/2004 - 27/03/2004
Main Research Area: Technical/natural sciences

Publication information
Journal: Electronic Notes in Theoretical Computer Science
Volume: 112
Issue number: SPEC. ISS.
ISSN (Print): 1571-0661
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
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
Using Linear Temporal Logic for Goal-Oriented Policy Refinement Frameworks

Policy refinement is meant to derive lower-level policies from higher-level ones so that these more specific policies are better suited for use in different execution environments. Although it has been recognized as crucial, it has received relatively little attention. We present a policy refinement framework grounded in goal-elaboration methodologies and reactive systems analysis. Through Linear-Time Model Checking, we obtain system trace executions aimed at fulfilling lower-level goals refined with the KAOS goal-elaboration method. From system executions, we abstract managed entities, conditions and actions to encode the refined policies. We present our framework and provide a refinement scenario applied to the DiffServ QoS Management domain.

Abstraction in Directed Model Checking

Abstraction is one of the most important issues to cope with large and infinite state spaces in model checking and to reduce the verification efforts. The abstract system is smaller than the original one and if the abstract system satisfies a correctness specification, so does the concrete one. However, abstractions may introduce a behavior violating the specification that is not present in the original system.

This paper bypasses this problem by proposing the combination of abstraction with heuristic search to improve error detection. The abstract system is explored in order to create a database that stores the exact distances from abstract states to the set of abstract error states. To check, whether or not the abstract behavior is present in the original system,
Efficient exploration algorithms exploit the database as a guidance.

**General information**
State: Published
Organisations: Universität Dortmund, Università di Pisa
Authors: Edelkamp, S. (Ekstern), Lluch Lafuente, A. (Intern)
Publication date: 2004

**Host publication information**
Title of host publication: Proceedings of the 1st ICAPS Workshop on Connecting Planning Theory with Practice
Main Research Area: Technical/natural sciences
Conference: 1st International Conference on Automated Planning and Scheduling Workshop on Connecting Planning Theory with Practice, Whistler, Canada, 03/06/2004 - 03/06/2004
Publication: Research › Article in proceedings – Annual report year: 2004

**Directed explicit-state model checking in the validation of communication protocols**
The success of model checking is largely based on its ability to efficiently locate errors in software designs. If an error is found, a model checker produces a trail that shows how the error state can be reached, which greatly facilitates debugging. However, while current model checkers find error states efficiently, the counterexamples are often unnecessarily lengthy, which hampers error explanation. This is due to the use of “naive” search algorithms in the state space exploration. In this paper we present approaches to the use of heuristic search algorithms in explicit-state model checking. We present the class of A* directed search algorithms and propose heuristics together with bitstate compression techniques for the search of safety property violations. We achieve great reductions in the length of the error trails, and in some instances render problems analyzable by exploring a much smaller number of states than standard depth-first search. We then suggest an improvement of the nested depth-first search algorithm and show how it can be used together with A* to improve the search for liveness property violations. Our approach to directed explicit-state model checking has been implemented in a tool set called HSF-SPIN. We provide experimental results from the protocol validation domain using HSF-SPIN.

**General information**
State: Published
Organisations: Albert Ludwigs Universität Freiburg
Authors: Edelkamp, S. (Ekstern), Leue, S. (Ekstern), Lluch Lafuente, A. (Intern)
Number of pages: 21
Pages: 247-267
Publication date: 2004
Main Research Area: Technical/natural sciences

**Publication information**
Journal: International Journal on Software Tools for Technology Transfer
Volume: 5
Issue number: 2-3
ISSN (Print): 1433-2779
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 1
Scopus rating (2016): SJR 0.574 SNIP 1.642 CiteScore 2.14
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.587 SNIP 1.587 CiteScore 1.59
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.469 SNIP 1.6 CiteScore 1.5
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.585 SNIP 1.884 CiteScore 1.62
ISI indexed (2013): ISI indexed no
BFI (2012): BFI-level 1
Scopus rating (2012): SJR 0.5 SNIP 1.313 CiteScore 1.28
ISI indexed (2012): ISI indexed no
Partial-order reduction and trail improvement in directed model checking

In this paper we present work on trail improvement and partial-order reduction in the context of directed explicit-state model checking. Directed explicit-state model checking employs directed heuristic search algorithms such as A* or best-first search to improve the error-detection capabilities of explicit-state model checking. We first present the use of directed explicit-state model checking to improve the length of already established error trails. Second, we show that partial-order reduction, which aims at reducing the size of the state space by exploiting the commutativity of concurrent transitions in asynchronous systems, can coexist well with directed explicit-state model checking. Finally, we illustrate how to mitigate the excessive length of error trails produced by partial-order reduction in explicit-state model checking. In this context we also propose a combination of heuristic search and partial-order reduction to improve the length to already provided counterexamples.

**General information**

State: Published
Organisations: Universität Dortmund, Universität Konstanz, Università di Pisa
Authors: Edelkamp, S. (Ekstern), Leue, S. (Ekstern), Lluch Lafuente, A. (Intern)
Number of pages: 25
Pages: 277-301
Publication date: 2004
Main Research Area: Technical/natural sciences

**Publication Information**

Journal: International Journal on Software Tools for Technology Transfer
Volume: 6
Issue number: 4
ISSN (Print): 1433-2779
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 1
Scopus rating (2016): SJR 0.574 SNIP 1.642 CiteScore 2.14
Web of Science (2016): Indexed yes
Symmetry Reduction and Heuristic Search for Error Detection in Model Checking

The state explosion problem is the main limitation of model checking. Symmetries in the system being verified can be exploited in order to avoid this problem by defining an equivalence (symmetry) relation on the states of the system, which induces a semantically equivalent quotient system of smaller size. On the other hand, heuristic search algorithms can be applied to improve the bug finding capabilities of model checking. Such algorithms use heuristic functions to guide the exploration. Bestfirst is used for accelerating the search, while A* guarantees optimal error trails if combined with admissible estimates. We analyze some aspects of combining both approaches, concentrating on the problem of finding the optimal path to the equivalence class of a given error state. Experimental results evaluate our approach.

General information

State: Published
Organisations: Albert Ludwigs Universität Freiburg
Authors: Lluch Lafuente, A. (Intern)
Publication date: 2003

Host publication information

Title of host publication: Proceedings of the 2nd Workshop on Model Checking and Artificial Intelligence
Publisher: AAAI Press
Main Research Area: Technical/natural sciences
Partial Order Reduction in Directed Model Checking

Partial order reduction is a very successful technique for avoiding the state explosion problem that is inherent to explicit state model checking of asynchronous concurrent systems. It exploits the commutativity of concurrently executed transitions in interleaved system runs in order to reduce the size of the explored state space. Directed model checking on the other hand addresses the state explosion problem by using guided search techniques during state space exploration. As a consequence, shorter errors trails are found and less search effort is required than when using standard depth-first or breadth-first search. We analyze how to combine directed model checking with partial order reduction methods and give experimental results on how the combination of both techniques performs.

Directed Explicit Model Checking with HSF-SPIN

We present the explicit state model checker HSF-SPIN which is based on the model checker SPIN and its Promela modeling language. HSF-SPIN incorporates directed search algorithms for checking safety and a large class of LTL-specified liveness properties. We start off from the A* algorithm and define heuristics to accelerate the search into the direction of a specified failure situation. Next we propose an improved nested depth-first search algorithm that exploits the structure of Promela Never-Claims. As a result of both improvements, counterexamples will be shorter and the explored part of the state space will be smaller than with classical approaches, allowing to analyze larger state spaces. We evaluate the impact of the new heuristics and algorithms on a set of protocol models, some of which are real-world industrial protocols.
Protocol Verification with Heuristic Search

We present an approach to reconcile explicit state model checking and heuristic directed search and provide experimental evidence that the model checking problem for concurrent systems, such as communications protocols, can be solved more efficiently, since finding a state violating a property can be understood as a directed search problem. In our work we combine the expressive power and implementation efficiency of the SPIN model checker with the HSF heuristic search workbench, yielding the HSF-SPIN tool that we have implemented. We start off from the A* algorithm and some of its derivatives and define heuristics for various system properties that guide the search so that it finds error states faster. In this paper we focus on safety properties and provide heuristics for invariant and assertion violation and deadlock detection. We provide experimental results for applying HSF-SPIN to two toy protocols and one real world protocol, the CORBA GIOP protocol.

Trail-Directed Model Checking

HSF-SPIN is a Promela model checker based on heuristic search strategies. It utilizes heuristic estimates in order to direct the search for finding software bugs in concurrent systems. As a consequence, HSF-SPIN is able to find shorter trails than blind depth-first search.

This paper contributes an extension to the paradigm of directed model checking to shorten already established unacceptable long error trails. This approach has been implemented in HSF-SPIN. For selected benchmark and industrial communication protocols experimental evidence is given that trail-directed model-checking effectively shortcuts existing witness paths.
BFI (2014): BFI-level 2  
Scopus rating (2014): SJR 0.708 SNIP 1.228 CiteScore 1.08  
Web of Science (2014): Indexed yes  
BFI (2013): BFI-level 2  
Scopus rating (2013): SJR 0.739 SNIP 1.38 CiteScore 1.17  
ISI indexed (2013): ISI indexed yes  
BFI (2012): BFI-level 2  
Scopus rating (2012): SJR 0.844 SNIP 1.288 CiteScore 1.16  
ISI indexed (2012): ISI indexed yes  
Web of Science (2012): Indexed yes  
BFI (2011): BFI-level 2  
Scopus rating (2011): SJR 0.81 SNIP 1.289 CiteScore 1.17  
ISI indexed (2011): ISI indexed yes  
Web of Science (2011): Indexed yes  
BFI (2010): BFI-level 2  
Scopus rating (2010): SJR 0.91 SNIP 1.329  
Web of Science (2010): Indexed yes  
BFI (2009): BFI-level 2  
Scopus rating (2009): SJR 0.948 SNIP 1.475  
BFI (2008): BFI-level 2  
Scopus rating (2008): SJR 1.188 SNIP 1.638  
Web of Science (2008): Indexed yes  
Scopus rating (2007): SJR 0.997 SNIP 1.65  
Scopus rating (2006): SJR 0.911 SNIP 1.49  
Web of Science (2006): Indexed yes  
Scopus rating (2005): SJR 0.821 SNIP 1.486  
Web of Science (2005): Indexed yes  
Scopus rating (2004): SJR 0.804 SNIP 1.366  
Web of Science (2004): Indexed yes  
Scopus rating (2003): SJR 0.936 SNIP 1.523  
Scopus rating (2002): SJR 0.837 SNIP 1.358  
Web of Science (2002): Indexed yes  
Scopus rating (2001): SJR 0.934 SNIP 1.514  
Scopus rating (2000): SJR 0.61 SNIP 1.343  
Scopus rating (1999): SJR 0.519 SNIP 1.166  

Original language: English  
DOI: 10.1016/S1571-0661(04)00261-0  
Publication: Research - peer-review › Conference article – Annual report year: 2001  

Projects:  

**Formal methods for Secure Trust Infrastructures**  
Technical University of Denmark  
Period: 01/12/2016 → 05/01/2018  
Number of participants: 3  
Phd Student:  
Birkedal, Rasmus (Intern)  
Supervisor:  
Lluch Lafuente, Alberto (Intern)  
Main Supervisor:  
Mödersheim, Sebastian Alexander (Intern)  

Financing sources
LiIGHTest foundation

Technical University of Denmark
Period: 01/09/2016 → 06/09/2016
Number of participants: 3
Phd Student:
Bjerregaard, Mathias Ormstrup (Intern)
Supervisor:
Lluch Lafuente, Alberto (Intern)
Main Supervisor:
Mödersheim, Sebastian Alexander (Intern)

Financing sources
Source: Internal funding (public)
Name of research programme: Anden EU-finansiering
Project: PhD

Cognitive and Perceptive Cameras - Compilation system

Technical University of Denmark
Period: 01/10/2013 → 18/01/2017
Number of participants: 6
Phd Student:
Jensen, Nicklas Bo (Intern)
Supervisor:
Karlsson, Sven (Intern)
Main Supervisor:
Probst, Christian W. (Intern)
Examiner:
Lluch Lafuente, Alberto (Intern)
Kessler, Christoph W. (Ekstern)
Sestoft, Peter (Intern)

Financing sources
Source: Internal funding (public)
Name of research programme: 1/3 FUU, 1/3 inst 1/3 Andet

Relations
Publications:
High Performance with Prescriptive Optimization and Debugging
Project: PhD

Stochastic Model Checking of Socio- Technical Models

Technical University of Denmark
Period: 01/07/2013 → 23/11/2016
Number of participants: 6
Phd Student:
Aslanyan, Zaruhi (Intern)
Supervisor:
Probst, Christian W. (Intern)
Main Supervisor:
Nielson, Flemming (Intern)
Examiner:
Lluch Lafuente, Alberto (Intern)
Hansen, René Rydhof (Intern)
Legay, Axel (Ekstern)
Financing sources
Source: Internal funding (public)
Name of research programme: 1/3 FUU, 1/3 inst 1/3 Andet

Relations
Publications:
Formal Analysis of Graphical Security Models
Project: PhD

Modelling Socio-Technical Aspects of Organizational Security
Technical University of Denmark
Period: 15/01/2013 → 20/04/2016
Number of participants: 5
Phd Student:
Ivanova, Marieta Georgieva (Intern)
Main Supervisor:
Probst, Christian W. (Intern)
Examiner:
Lluch Lafuente, Alberto (Intern)
Gollmann, Dieter (Ekstern)
Schürmann, Carsten (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: 1/3 FUU, 1/3 inst 1/3 Andet

Relations
Publications:
Modelling Socio-Technical Aspects of Organisational Security
Project: PhD

Modeling and Verifying eID Protocols (Future ID)
Technical University of Denmark
Period: 15/12/2012 → 24/02/2016
Number of participants: 6
Phd Student:
Almousa, Omar (Intern)
Supervisor:
Nielson, Hanne Riis (Intern)
Main Supervisor:
Mödersheim, Sebastian Alexander (Intern)
Examiner:
Lluch Lafuente, Alberto (Intern)
Brucker, Achim D. (Ekstern)
Sprenger, Christoph (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Anden EU-finansiering
Project: PhD

Portable and Predictable Performance Heterogeneous Embedded Manycores - Upper Level System stack
Technical University of Denmark
Period: 01/10/2012 → 21/01/2016
Number of participants: 6
Phd Student:
Bonnichsen, Lars Frydendal (Intern)
Supervisor:
Karlsson, Sven (Intern)
Main Supervisor:
Probst, Christian W. (Intern)
Examiner:
Lluch Lafuente, Alberto (Intern)
Assmann, Uwe (Ekstern)
Hansen, René Rydhof (Intern)

Financing sources
Source: Internal funding (public)
Name of research programme: 1/3 FUU, 1/3 inst 1/3 Andet

Relations
Publications:
An Adaptive Middleware for Improved Computational Performance
Project: PhD

Cyber-Physical Systems secure communication protocols
Technical University of Denmark
Period: 01/12/2011 → 04/03/2015
Number of participants: 6
Phd Student:
Vigo, Roberto (Intern)
Supervisor:
Nielsen, Hanne Riis (Intern)
Main Supervisor:
Nielsen, Flemming (Intern)
Examiner:
Lluch Lafuente, Alberto (Intern)
Victor, Björn (Ekstern)
Viganò, Luca (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: 1/3 FUU, 1/3 inst 1/3 Andet
Project: PhD