~~One~~ Two Festschrift papers for Bernhard Steffen

Hubert Garavel

Inria Grenoble – LIG

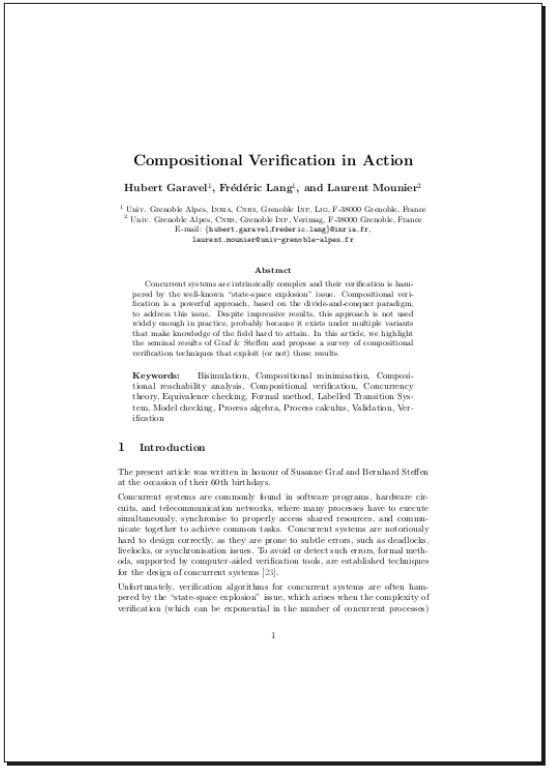
Université Grenoble Alpes

http://convecs.inria.fr

First paper

Compositional Verification in Action

Hubert Garavel, Frédéric Lang, Laurent Mounier



Compositional Verification in Action

Hubert Garavel[1], **Frédéric Lang**[1], **and Laurent Mounier**[2]

[1] Univ. Grenoble Alpes, Inria, Cnrs, Grenoble Inp, Lig, F-38000 Grenoble, France
[2] Univ. Grenoble Alpes, Cnrs, Grenoble Inp, Verimag, F-38000 Grenoble, France
E-mail: {hubert.garavel,frederic.lang}@inria.fr,
laurent.mounier@univ-grenoble-alpes.fr

Abstract

Concurrent systems are intrinsically complex and their verification is hampered by the well-known "state-space explosion" issue. Compositional verification is a powerful approach, based on the divide-and-conquer paradigm, to address this issue. Despite impressive results, this approach is not used widely enough in practice, probably because it exists under multiple variants that make knowledge of the field hard to attain. In this article, we highlight the seminal results of Graf & Steffen and propose a survey of compositional verification techniques that exploit (or not) these results.

Keywords: Bisimulation, Compositional minimisation, Compositional reachability analysis, Compositional verification, Concurrency theory, Equivalence checking, Formal method, Labelled Transition System, Model checking, Process algebra, Process calculus, Validation, Verification

1 Introduction

The present article was written in honour of Susanne Graf and Bernhard Steffen at the occasion of their 60th birthdays.

Concurrent systems are commonly found in software programs, hardware circuits, and telecommunication networks, where many processes have to execute simultaneously, synchronise to properly access shared resources, and communicate together to achieve common tasks. Concurrent systems are notoriously hard to design correctly, as they are prone to subtle errors, such as deadlocks, livelocks, or synchronisation issues. To avoid or detect such errors, formal methods, supported by computer-aided verification tools, are established techniques for the design of concurrent systems [23].

Unfortunately, verification algorithms for concurrent systems are often hampered by the "state-space explosion" issue, which arises when the complexity of verification (which can be exponential in the number of concurrent processes)

- written in honour of Susanne Graf (and Bernhard Steffen)
- 22-page paper in LNCS 11119 (proceedings of FMICS 2018)

First paper's message

- The Graf-Steffen paper at CAV'90 ("Compositional Minimization of Finite State Systems") is a neglected jewel
- Standard compositional minimization works well (25 case studies performed using CADP)
- But it may fail for certain "open" components: hardware buses, network links, shared memories, etc.
- The Graf-Steffen approach solves these issues: behavioural interfaces and semi-composition (8 case studies performed using CADP)

Second paper

Reflections on Bernhard Steffen's Physics of Software Tools

Hubert Garavel and Radu Mateescu

Reflections on Bernhard Steffen's Physics of Software Tools

Hubert Garavel and Radu Mateescu

Univ. Grenoble Alpes, Inria, Cnrs, Lig, F-38000 Grenoble, France
hubert.garavel@inria.fr, radu.mateescu@inria.fr

Abstract. Many software tools have been developed to implement the concepts of formal methods, sometimes with great success, but also with an impressive tool mortality and an apparent dispersion of efforts. There has been little analysis so far of such tool development as a whole, in order to make it more coherent, efficient, and useful to the society. Recently, however, Bernhard Steffen published a paper entitled "The Physics of Software Tools: SWOT Analysis and Vision" that precisely proposes such a global vision. We highlight the key ideas of this paper and review them in light of our own experience in designing and implementing the CADP toolbox for the specification and analysis of concurrent systems.

1 Introduction

The present article was written in honour of Bernhard Steffen and included in a collective Festschrift book offered to him at the occasion of his 60th birthday, in addition to another Festschrift article [18], jointly dedicated to Susanne Graf and Bernhard Steffen.

In a recent position statement entitled *The Physics of Software Tools: SWOT Analysis and Vision* [49], Bernhard Steffen analyzes the current situation of software tools implementing the concepts of formal methods and suggests directions for organizing the development of these tools in a more coherent and efficient way. This analysis is rooted in Bernhard Steffen's double experience in developing software tools (including ETI [50,7], jETI [35], LearnLib [44,42,24] and CINCO [43]) and managing the research community in formal methods (notably with the launch of the TACAS conference[1] of the STTT journal[2], and the RERS challenge[3]). The position statement [49] is written in a lively style, enriched with insightful anecdotes. Despite its seemingly simple form, it puts forward many diverse ideas that freely spring from all parts of the text.

We believe that global debates on the present and future of formal methods are essential, and Bernhard Steffen's position statement is a most welcome contribution in this respect. The present article exposes the key ideas of this position statement in an orderly way, each idea being first illustrated with citations from

[1] http://tacas.info
[2] http://sttt.cs.uni-dortmund.de
[3] http://rers-challenge.org

- written in honour of Bernhard Steffen
- 23-page paper published in LNCS

Second paper's message

- Based on Bernhard Steffen 2017 STTT paper "The Physics of Software Tools: SWOT Analysis and Vision"
- Development of formal tools is not well organized
  - Problems, causes, individual and collective solutions
- Our paper is a response to Bernhard's paper
  - we review and discuss his points
  - we compare them to our own experience (CADP)
- Other tool developers should enter the debate