Ph. Schnoebelen

Tél.: (+33) 147 407 530
Fax : (+33) 147 407 521
E-mail : `phs@lsv.ens-cachan.fr`

Report on "From Infinite State Systems to Translation of LTL to Automata", an Habilitation Thesis submitted by Jan Strejček

The document submitted by Jan Strejček consists of a collection of 11 research papers published between 2001 and 2012, together with a short foreword that summarizes the thesis contents.

Verification of PRS systems. The main contributions reported in this selection of papers are concerned with the verification of abstract infinite-state models related to the PRS hierarchy. This framework, due to R. Mayr, is able to represent, in an abstract and unified way, most of the features by which recursive parallel programs may give rise to infinite-state transition systems. Because it is based on a simple set of term rewrite rules, the PRS framework lets one focus on the essential algorithmic difficulties faced when trying to develop and analyze decision methods. Furthermore, the framework is very expressive and it encompasses many natural, often preexisting, settings like Petri nets or pushdown automata : every restriction on the form of allowed rules leads to a meaningful and challenging subcase of the PRS verification problem.

In this setting, Jan Strejček tackled the verification problem along three dimensions : (1) by considering different fragments in the PRS hierarchy ; (2) by considering a hierarchy of different verification problems ; (3) by characterizing the precise computational complexity of decidable problems.

With his coauthors, Jan Strejček developed a rich, almost complete, picture of

the verification problem for the PRS hierarchy. One can now just look up in this habilitation thesis and find there the solution to almost any verification question for models in the extended PRS hierarchy. This is a fundamental contribution to the theory of verification and is already a remarkable achievement.

This line of research goes beyond simply solving a series of hard open problems. Indeed, it often leads to discovering or highlighting unexpected structure, e.g., when several different PRS fragments behave the same. It also suggests extensions of the initial settings, e.g., when PRS is extended to wPRS —this is first motivated on technical grounds for tackling weak trace equivalence, but it also raises new questions (e.g., when/how do the w_ fragments add expressive power to the PRS hierarchy?) and leads to new insights—, or when the LIO fragment of LTL is identified in the context of PRS model checking and later leads to impressive developments in actual general-purpose LTL model checking (see below).

Applications. The techniques developed by Jan Strejček for his analysis of the PRS hierarchy have found applications in some papers that are closer to actual verification concerns. Some are by other authors, e.g., the refs [46,47] mentioned in the thesis, and some involve Jan Strejček, e.g., in chapters 13 and 15. In these chapters, models from the PRS hierarchy or some of its extensions are used to describe concurrent recursive programs and analyze them. For ADPN, reachability is undecidable and a compromise solution is to compute reachability within a bounded number of phases, here defined as a context switch in the distributed program.

Another unexpected application is the impressively efficient translation from LIO to ALBA —almost linear Büchi automata— that is reported in chapter 9. Here what started as decidability for wPRS model-checking ended up as very efficient algorithms for generating small and simple Büchi automata. The LIO2BA algorithm has been implemented and shown to outperform its rivals in most practical tests, even thought its worst-case complexity is exponentially worse.

Some suggestions. The excellent work reported above has not yet had the impact it deserves. This is understandable since results of a fundamental nature (on the PRS hierarchy) take time to diffuse, and since the LTL to automata translation is still very recent. However Jan Strejček can facilitate or accelerate the diffusion process by some specific actions. Regarding PRS verification, it would be useful to have a survey paper describing in an accessible and synthetic way all the main existing decidability results and techniques, and linking precisely the main levels of the PRS hierarchy with the less abstract formalisms customarily used in software verification. Regarding the Büchi automata generation, a good strategy could be to initiate an active collaboration with one of the groups, e.g., SPOT, that has already invested many man-years in the development of portable and successful tools for Büchi automata generation.

Assessment. The collected papers contain theoretical and applied work of a very high level in a field, algorithmic verification, where the international competition is very active and quite demanding, and where very few researchers contribute significantly on both the theoretical and the applied sides. Furthermore, while Jan Strejček has chosen, and for the sake of thematic unity, to only present his work on PRS verification and translation of LTL to Büchi automata, there are a good

number of additional contributions to the theory of verification which he could have put forward. His works has been published in some of the most visible and selective conferences of the field (TACAS, CONCUR, CSL, ...). He has initiated new collaborations with foreign researchers of the highest calibre, and at the same time his list of coauthors also includes younger graduate students that he is apparently supervising in a productive way. For these reasons, I think[1] that Jan Strejček has amply proved his excellence and maturity, and is fully deserving of the Habilitation diploma for which he is applying.

Ph. Schnoebelen
CNRS & ENS Cachan

---

1. I do not know what are the specific rules and requirements for Habilitation in Czech universities. But I can tell that Jan Strejček would undoubtedly be granted an Habilitation at ENS Cachan where I have been head of the LSV research lab on Formal Methods and Verification.