Book Review for AMS Reviews

Review of *Unfoldings: A Partial-Order Approach to Model Checking*
by Javier Esparza and Keijo Heljanko, Springer, 2008.

This monograph introduces researchers interested in concurrency and automatic verification to the *unfolding technique*, which aims at alleviating the state explosion problem that arises when model checking concurrent systems. The authors are leading experts in the field and provide an excellent account of the most important results in unfoldings within a coherent framework, which is accompanied by many examples. Unfoldings are based on true concurrency models and were first adapted to model checking by McMillan in 1992. Since then the unfolding technique has been successfully applied to, e.g., the verification of communication protocols, the analysis of asynchronous logic circuits, and the monitoring of discrete event systems. It has also been adapted to rich modeling formalisms and implemented in sophisticated verification tools.

Given a description of a concurrent system as a product of labeled transition systems, the unfolding technique constructs a special partially ordered graph – a Petri net variant – whose nodes are not the product's reachable states themselves but still contain full information about them. To check the validity of a desired temporal property of the system, only a *finite* prefix of the system's unfolding needs to be explored, which can be exponentially smaller than the unfolding of the system's associated global transition system, depending on the exhibited degree of concurrency. Hence, unfoldings can be viewed as a compact data structure representing a system's computations.

The monograph focuses on the algorithmic ideas behind unfoldings, its highlight being an unfolding-based algorithm for model checking concurrent systems against properties specified as formulas in linear temporal logic (LTL). The book's elegant approach and structure relies on the decomposability of the LTL model checking problem into a repeated executability problem and a livelock problem, for next-state less LTL formulas. Accordingly, the authors discuss unfoldings first for the *executability* problem, then for the *repeated executability* problem, and finally for the *livelock* problem.

In each case, a search procedure is given, consisting of a search strategy and a search scheme. While the strategy can be any order on transition sequences refining the prefix preorder – such as 'shortest history' or 'breadth first' –, specific search schemes are presented depending on the verification problem at hand. Intuitively, a scheme determines when an unfolding can be cut off and is constructed so that the search procedure is correct and complete for all (adequate) strategies. While the generated prefixes of unfoldings are guaranteed to be finite, their sizes depend on the choice of strategy.

The monograph convinces by its clear, systematic approach, an admirable provision of intuition for complex, yet elegant constructions, and the many illuminating examples guiding the reader – despite those often requiring one to turn pages. Experts in unfoldings may have wished that the authors had stuck with established terminology, although any deviation is clearly pointed out. The authors pay much attention to carefully presenting the proofs of their results and especially the completeness proofs for their search schemes, which are well-structured and contain sufficient detail; the occasional typo is easy to identify and correct.

The only substantial criticism is that, although the monograph emphasizes algorithmic aspects of unfoldings, it does not contain a chapter with experimental results that compare unfoldings to related techniques such as partial order reduction; instead, the authors only provide references to tools and experimental studies. Otherwise, the book is self-contained and thus suitable for experts in formal methods and graduate students alike. However, basic knowledge of concurrency models – in particular of Petri nets and Mazurkiewicz traces – and of classic LTL model checking will prove helpful.

Overall, this monograph is a success and highly recommended reading for everyone interested in concurrency and automatic verification.

GERALD LÜTTGEN
Software Technologies Research Group
University of Bamberg
D–96045 Bamberg, Germany
E-mail: gerald.luettgen@swt-bamberg.de