Texts in Theoretical Computer Science
An EATCS Series

Editors: W. Brauer G. Rozenberg A. Salomaa
On behalf of the European Association
for Theoretical Computer Science (EATCS)

Springer-Verlag Berlin Heidelberg GmbH

Klaus Schneider

Verification of Reactive Systems

Formal Methods and Algorithms

With 149 Figures

Springer

Author

Prof. Dr. Klaus Schneider
FB Informatik
AG Reaktive Systeme
Universität Kaiserslautern
67653 Kaiserslautern
Germany

klaus.schneider@informatik.uni-kl.de

Series Editors

Prof. Dr. Wilfried Brauer
Institut für Informatik
Technische Universität München
Arcisstrasse 21, 80333 München, Germany
brauer@informatik.tu-muenchen.de

Prof. Dr. Grzegorz Rozenberg
Leiden Institute of Advanced Computer Science
University of Leiden
Niels Bohrweg 1, 2333 CA Leiden, The Netherlands
rozenber@liacs.nl

Prof. Dr. Arto Salomaa
Data City
Turku Centre for Computer Science
20 500 Turku, Finland
asalomaa@utu.fi

Library of Congress Cataloging-in-Publication Data applied for

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliographie; detailed bibliographic data is available in the Internet at <http://dnd.dd.de>

ACM Computing Classification (1998): F.3.1, D.2.4, F.4.1

ISBN 978-3-642-05555-3 ISBN 978-3-662-10778-2 (eBook)
DOI 10.1007/978-3-662-10778-2

springeronline.com

Originally published by Springer-Verlag Berlin Heidelberg New York in 2004
Softcover reprint of the hardcover 1st edition 2004

Cover Design: KünkelLopka, Heidelberg
Typesetting: Camera-ready by the author
45/3142 – 5 4 3 2 1 0 – Printed on acid-free paper

To Tim, Katja and Kai

Foreword

Computer systems are becoming ubiquitous. Many of the most important and prevalent ones are reactive systems. Reactive systems include microprocessors, computer operating systems, air traffic control systems, as well as on-board avionics and other embedded systems. These systems are characterized technically by their ongoing, ideally infinite behavior; termination is impossible or aberrant behavior, in contrast to classical theories of computation. Reactive systems tend to be characterized in practice by having failure modes that can severely compromise safety, even leading to loss of life. Alternatively, errors can have serious financial repercussions such as expensive recalls. Reactive systems need to be correct before being deployed.

To determine whether such reactive systems do behave correctly, a rich mathematical theory of verification of reactive systems has been developed over the last two decades or so. In contrast to earlier work emphasizing the role of proofs in deductive systems to establish correctness, the alternative suggestion is to take a model-theoretic view. It turns out that this permits the process of reasoning about program correctness to be fully automated in principle and partially automated to a high degree in practice.

It is my pleasure to introduce Klaus Schneider's excellent book *Verification of Reactive Systems: Formal Methods and Algorithms*. This book is the story of reactive systems verification, reflecting Klaus's broad expertise on the subject. It addresses both applications and theory, providing especially strong coverage of basic as well as advanced theory not otherwise available in book form. Key topics include Kripke and related transition structures, temporal logics, automata on infinite strings including Safra's determinization construction, expressiveness and Borel hierarchies of ω-languages, as well as monadic predicate logics. An underlying theme is the use of the vectored μ-calculus to provide an elegant "Theory of Everything". *Verification of Reactive Systems* belongs on the bookshelf of every serious researcher into the topic. It should also serve as a valuable text for graduate students and advanced undergraduates.

April 2003

E. Allen Emerson,
Endowed Professor of Computer Sciences
University of Texas at Austin

Preface

The design of modern information processing systems like digital circuits or protocols is becoming more and more difficult. A large part of the design costs and time (about 70%) is currently spent on methods that try to guarantee the absence of design errors. For this reason, designing systems is now more and more a synonym for verifying systems.

The research into the verification of reactive systems, in particular, into model checking, is one of the most impressive successes of theoretical computer science. Two decades after the publication of the basic papers on the formal foundation, the methods became mature enough for industrial usage. Nowadays, the hardware industry employs hundreds of highly specialized researchers working with formal methods to detect design bugs.

When I entered this field, it was an enormous effort to read hundreds of papers to understand the relationships between the different formal methods that are currently in use. It was surprising to me that there was no book covering all these methods, even the basic ones, although there is such a huge interest in them. For this reason, I decided to write this book to provide newcomers and researchers with a textbook that covers most of the relevant logics, with a particular emphasis on (verification and translation) algorithms.

The book is intended for graduate students as well as for researchers already working in this area. It is self-contained and gives proofs and algorithms for all important constructions. For a less detailed and formal introduction, I want to recommend the book of Clarke, Grumberg, and Peled [111]. Supplemental material on actual tools is found in [38], and further topics on the μ-calculus and infinite games are found in [221].

There are many persons I have to thank for helping me to write this book. In particular, I want to thank Detlef Schmid and the hardware verification group at the University of Karlsruhe, in particular Jorgos Logothetis, Tobias Schüle, and Roberto Ziller. Many discussions with Moshe Vardi moved me to improve the book. Allen Emerson was soon interested in the project and also gave fruitful comments. Moreover, I want to thank Amir Pnueli, Wolfgang Thomas, and Peter Schmitt for comments on early versions of the manuscript. Last, but not least, it should be mentioned that the editors of the EATCS series, in particular, Prof. Brauer, and the team at Springer-Verlag helped me to publish this book.

Kaiserslautern, September 2003 *Klaus Schneider*

Contents