Enhancing State Space Reduction Techniques for Model Checking

Dragan Bošnački
Bosnacki, Dragan
NUGI 855
Subject headings : model checking / programming; formal methods / software; specifications / software verification
CR Subject Classification (1998) : D.2.4.

The work in this thesis has been carried out under the auspices of the research school IPA (Institute for Programming research and Algorithmics).

IPA dissertation series 2001-14
Printed by University Press Facilities, Eindhoven
ENHANCING STATE SPACE REDUCTION TECHNIQUES FOR MODEL CHECKING

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de Technische Universiteit Eindhoven, op gezag van de Rector Magnificus, prof.dr. R.A. van Santen, voor een commissie aangewezen door het College voor Promoties in het openbaar te verdedigen op woensdag 7 november 2001 om 16.00 uur

door

Dragan Bošnački

geboren te Berovo, Macedonië
Dit proefschrift is goedgekeurd door de promotoren:

prof.dr. J.C.M. Baeten
en
prof.ir. M.P.J. Stevens

Copromotor:

dr. D.R. Dams
Acknowledgments

There are many people and institutions who helped me in various ways during the writing of this thesis. Aware of the inevitable risk of forgetting someone, I will try to list them with some words of gratitude that unfortunately often will be only a pale shadow of what they should have been. For those that I have forgotten to mention – a proverb from my homeland: "May the evil also forget you".

First of all, I would like to thank my copromotor Dennis Dams. I consider myself extremely fortunate that I had during all these years his valuable guidance and friendship. His was always able to help with all my technical questions, as well as to give me the right advise at the right time. Dennis is also a coauthor of several papers whose modified versions became chapters of this thesis.

No less gratitude is reserved for my promotor Jos Baeten. He opened for me the doors of the Western European science by inviting me to a short stay at the Eindhoven University of Technology in the fall of 1996. Since then he has been offering me continuously technical and moral support. He also deserves the credit for creating a nice working atmosphere in the Formal Methods group. Jos is the only boss that I know that regularly goes from door to door in order to gather his group for lunch.

Gerard Holzmann provided for me the opportunity to spend an unforgettable summer 1998 in Bell Laboratories. The experience of walking in the corridor with probably the greatest concentration of computer science celebrities in the world is something I always talk about with pleasure. Thanks go to Gerard also for patiently answering numerous technical questions regarding Spin and model checking in general.

Most of the work on this thesis was done under the auspices of the European Community’s Fourth Framework project Verifying Industrial REactive Systems (VIRES) (Esprit LTR 23498) which I gratefully acknowledge. I would like to also thank all the participants in the project with whom I had the opportunity to discuss my research.

During the Ph.D. studies in Eindhoven I was on leave from the Institute of Informatics, Faculty of Natural Sciences and Mathematics of the St. Cyril and Methodius University in Skopje, Macedonia. I am immensely grateful to my colleagues from the Institute for their understanding and support.

On this occasion I should not forget the technical and financial support by the IPA postgraduate school. The events organized by the school offered an excellent opportunities for learning and enjoyment.

I am grateful to Leszek Holenderski for coauthoring the papers who became basis for two of the chapters in this thesis. We spent a lot of time on interesting discussions, often outside our research. We had different opinions about many issues, but at the end I think that I learned many interesting things from him.
Tanks go to Twan Basten for coauthoring of Chapter 2, numerous discussions on the topic of partial order reduction, and helping me with the Samenvatting in Dutch.

Natalia Sidorova is a coauthor of the paper who is a basis of Chapter 5 of the thesis. I am also grateful to her for the numerous discussions regarding the verification of timed systems.

I would like to thank Mario Stevens for accepting to be my second promotor. Doron Peled and Hans Toetenel kindly accepted to be members of the reading committee and gave valuable insightful comments on the first version of this document, for which I am indebted to them.

I am mostly grateful to Smile Markovski for his support during the years I spent at the Institute of Informatics in Skopje, Macedonia. Many things in theoretical computer science I learned from him. I am also honored that he accepted to be a member of the defense committee for my thesis.

Jan-Friso Groote and Antti Valmari also kindly accepted to be members of the defense committee, for which I honor them.

Many thanks to Tijn Borghuis and Tim Willemsen for their helpful remarks on parts of the manuscript and their friendship.

I am grateful to Peter Hilbers for believing in my potentials as a researcher and his understanding during the finishing of the last chapter of the thesis.

Rob Gerth and Bart Knaack drew my attention to Spin, for which I would like to thank them. Rob also played a significant role in my decision to come to Eindhoven.

Many people from the University helped indirectly with my thesis, for which I give them my warmest thanks: Suzana Andova for her moral support, constructive criticism and helping me not to forget the taste of the Macedonian cuisine; Marcella de Rooij, Victor Bos, Georgi Jojgov and Martijn Oostdijk for being with me during my ups and downs and letting me winning couple of Risk games; Sjouke Mauw for his friendship, valuable advises and always supportive smile; Ana Sokolova, Anne-Meta Overstegen, Ruurd Kuiper, Rob Nederpelt, Nicu Goga, Peter Peters, Roel Bloo, Michael Franssen, Andre Engels, Erik de Vink, Kees Middelburg, Loe Feijs, François Monin, Francien Dechesne, Dmitri Chkliaev, Elize Russell, Michel Reniers, Sergey Tourine, Nino Mushkudiani, Olga Caprotti, Oana Balan, Marcin Grodek, Martin Hill, Desiree Mijers, Jolande Mathijssse, Trees Klaver, and Monique Bechtold for making my days at the University more enjoyable.

The successful finishing of this thesis would not be possible without the good education I received at the St. Cyril and Methodius University in Skopje, Macedonia, during the postgraduate studies at the Institute of Informatics, Faculty of Natural Sciences and Mathematics, and the undergraduate studies at the Faculty of Electrical Engineering.

The last, but by far the greatest gratitude goes to my parents for their endless love, all kinds of unconditional support, and for always believing in me much more than I believed in myself.

Contents

Acknowledgments ........................................................... iii

Contents ........................................................................... v

1 Introduction .............................................................. 1

2 Enhancing Partial-Order Reduction via Process Clustering .... 13

3 Partial Order Reduction in Presence of Rendez-vous
   Communications with Unless Constructs and Weak Fairness .... 31

4 Integrating Real Time into Spin: A Prototype Implementation 55

5 Model Checking SDL with Spin ......................................... 77

6 A Heuristic for Symmetry Reductions with Scalarsets .......... 93

7 Nested Depth First Search Algorithms for Symmetry Reduction
   in Model Checking ...................................................... 123

8 Conclusions .............................................................. 169

9 Samenvatting ............................................................. 173