Verifying OCL specifications of UML models : tool support and compositionality

Kyas, M.

Verifying OCL Specifications of UML Models: Tool Support and Compositionality

PROEFSCHRIFT

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van de Rector Magnificus Dr. D. D. Breimer,
hoogleraar in der Faculteit der Wiskunde en
Natuurwetenschappen en die der Geneeskunde,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 4 april 2006
te klokke 14.15 uur

door

Marcel Kyas
geboren te Pinneberg, Duitsland
in 1975

Promotiecommissie

Promotores:	Prof. dr. J.N. Kok
	Prof. dr. W.-P. de Roever *Christian-Albrechts-Universität zu Kiel*
Copromotor:	Dr. F.S. de Boer
Referent:	Prof. dr. Olaf Owe *Universitetet i Oslo*
Overige leden:	Prof. dr. F. Arbab
	Prof. dr. G. Rozenberg
	Prof. dr. S.M. Verduyn Lunel

Part of this work has been financially supported by IST project OMEGA (IST-33522-2001) and NWO/DFG project Mobi-j (RO 1122/9-1, RO 1122/9-2). The work has been carried out at the Christian-Albrechts-Universität zu Kiel, Germany.

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

Bibliografische Informationen der Deutschen Bibliothek:

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über `http://dnb.ddb.de/` abrufbar.

Verifying OCL Specifications of UML Models: Tool Support and Compositionality / Marcel Kyas. – With ref.
Berlin: Lehmanns Media, LOB.de, 2006.
Zugl.: Dissertation, Universiteit Leiden.
Zugl.: IPA Dissertation Series 2006-05.

ISBN: 3-86541-142-8

Printed by docupoint GmbH, Magdeburg, Germany.

Cover photograph "Dog sledging on Svalbard," © 2005 by Martin Steffen. Used with permission.

Preface

Another year is gone;
and I still wear
straw hat and straw sandal.

(Bashō)

This dissertation describes the results of my research at the Chair of Software Technology at the Christian-Albrechts-Universität zu Kiel, which was conducted as part of the Omega project (IST-2001-33522, see also `http://www-omega.imag.fr/`). The aim of Omega was to create a development method in UML (Unified Modelling Language) for embedded and real-time systems built on formal footing. My task was to adapt OCL (Object Constraint Language) to the Omega method. My solution is to extend OCL to a trace-based specification language facilitating compositional reasoning. Especially, I had to solve problems related to object-orientation and object creation.

OCL requires a context in which it is interpreted. This context is provided by other UML diagrams. However, UML is a large language. For this dissertation I have selected class-diagrams and state-machines for providing the context for OCL.

Class diagrams describe the structure of a system. They are well-understood and a very stable part of UML. They were present in the beginning of UML in 1997 and are based on entity-relationship diagrams, introduced in 1976 [24]. Considering this almost thirty year history, class diagrams will probably not change drastically anymore.

State machines provide a notation for describing the behaviour of systems. They evolved from Harel's statecharts [60] and their object-oriented development [61]. According to Hewitt [63], event-driven semantics are the essence of object-oriented computation. Such a semantics is used for state machines and allowed me to avoid all complications of more "modern" object-oriented programming languages.

While I was researching for my dissertation, the UML 2.0 standard has been actively developed. Many promising ideas have been introduced. It was a considerable amount of work to follow these developments and often results became obsolete or invalid. I hope that tracking this moving target contributed to making my results more robust.

Acknowledgements. I thank all people who supported me during the time of researching and writing this thesis.

Bengt Jonsson has been a very insightful reviewer of the Omega project. His opinion

on my deliverables has helped to improve this dissertation. He generously took the time to explain his work and views on trace-based specification and verification of systems.

Willem-Paul de Roever was very attentive of my well-being, sometimes "commanding" me to take a holiday. When I followed his "order" in 2001, I decided to visit Oslo, because at that time my fiancée was studying there. Willem-Paul suggested that I visit Ole-Johan Dahl on this occasion. Instead, I met Olaf Owe who told me that Ole-Johan Dahl was very ill. In spite of me not being invited he took the time to introduce me to his research. I was impressed by his work and suggested that he would present his work in Kiel. Instead he sent Einar Broch Johnsen. This set up the foundation for fruitful collaborations between Oslo, Kiel, and Frank de Boer in Amsterdam. Einar's most memorable contribution was to organise a working meeting on Spitsbergen during February 2005, as displayed on this book's cover.

Frank de Boer proved to be an excellent troubleshooter when we wrote a paper together. He always came up with new ideas whenever a problem arose *and* found the time to discuss them with me.

Martin Steffen's encyclopedic knowledge — not limited to computer science — his attentive observations, and his questions helped me to understand my own ideas better.

I also thank my numerous co-authors: Harald Fecher and Jens Schönborn discussed the subtleties of the semantics of UML; especially Jens worked out the semantics of UML 2.0 state machines, which helped me to understand the version used in the Omega project. Mark van der Zwaag formalised the semantics of Omega state machines in PVS and explained it to me. I based the translation of OCL into PVS on his work. Hillel Kugler and Tamarah Arons were the testers of this translator. Without their feedback, patience, and willingness to work with an evolving tool, many problems with the theory and its implementations would have emerged later, if at all. Jozef Hooman has been a great help in working with PVS and modelling the MARS case study.

Mirco Kuhlmann volunteered to read various drafts of this dissertation. He has pointed out many mistakes and omissions and suggested many improvements.

Our secretaries Sabine Hilge and especially Änne Straßner handled most bureaucratic tasks reliably. Thanks to their effort I was able to focus on research and teaching.

I thank my friends for reminding me of a life with leisure. Especially Jan Engelbach and Ortwin Ebhardt invited me for a chat over lunch or a party whenever the occasion arose.

I thank my parents Heidemarie and Horst for their loving encouragement and support. I shall always remain grateful for their advice.

Finally, my fiancée Ann-Dörte took care of me and most of the daily errants during the final stages in writing this thesis, reminded me to take shorter and longer breaks from work, and was wonderfully supportive and loving. She deserves all the praise for the fact that I remained healthy and sane in this memorable part of my life.

Marcel Kyas
January 26, 2006, Kiel

Contents

List of Tables

List of Figures