

Lecture Notes in Computer Science

651

Edited by G. Goos and J. Hartmanis

Advisory Board: W. Brauer D. Gries J. Stoer



Ron Koymans

Specifying Message Passing and Time-Critical Systems with Temporal Logic

Springer-Verlag

Berlin Heidelberg New York

London Paris Tokyo

Hong Kong Barcelona

Budapest

Series Editors

Gerhard Goos
Universität Karlsruhe
Postfach 69 80
Vincenz-Priessnitz-Straße 1
W-7500 Karlsruhe, FRG

Juris Hartmanis
Cornell University
Department of Computer Science
4130 Upson Hall
Ithaca, NY 14853, USA

Autor

Ron Koymans
Philips Research Laboratories, P.O.B. 80 000
NL-5600 JA Eindhoven, The Netherlands

CR Subject Classification (1991): F.3.1, F.4.1, J.7

ISBN 3-540-56283-4 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-56283-4 Springer-Verlag New York Berlin Heidelberg

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1992
Printed in Germany

Typesetting: Camera ready by author/editor
Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
45/3140-543210 - Printed on acid-free paper

List of Figures

2.1	System in its Environment	8
3.1	Schema for Completeness Proof of K	27
5.1	Message Passing System as a Black Box	67
5.2	Unique Identification by Using Counters	76
5.3	Channel with Disconnect	83
5.4	Layered Communication Network	85
5.5	Representation of Layer 1	89
5.6	Representation of Layer 2	93
6.1	Watchdog Timer	122
6.2	Terminal Adaptor	124
6.3	Mixing Synchronous and Asynchronous Input	128

Πάντα χωρεῖ καὶ οὐδὲν μένει (Herakleitos, ±500 B.C.)

Preface

This monograph is an updated and extended version of my Ph.D. thesis [Koy 89]. It is concerned with the application of temporal logic to the areas of message passing and time-critical systems. Apart from the practical use of temporal logic for these two application domains this monograph also incorporates pure fundamental studies on temporal logic. This duality may stem from my education: after studying (mathematical) logic I went on to finish my study in computer science. This is reflected in my main research interest: putting (mathematical) theory into (computer science) practice. Some readers may not be interested in the combination of theory and practice. To those interested mainly in theoretical results I can recommend reading Chapters 3 and 4 and sections 5.1, 5.2, 5.4, 6.1, 6.2 and 6.4. Readers interested more in practical issues could read Chapters 2, 5 and 6, and the following preliminaries from Chapters 3 and 4: section 3.1, section 3.2 till Definition 3.2.24, the definitions of **until** and **since** in section 3.3, section 3.4, section 4.1, section 4.2 till after Proposition 4.2.10, and section 4.4.

Writing my thesis would not have been possible without the help and support of many people. I thank Willem-Paul de Roever and Jan Vytupil for their stimulation and guidance in the last decade. Thanks go to Amir Pnueli who provided numerous suggestions for improvement of my work on many occasions and to Johan van Benthem who had a major influence on Chapter 4. From May 1984 till May 1988 I was involved in the Dutch National Concurrency Project (Dutch acronym LPC) which was supported by the Foundation for Computer Science Research in the Netherlands (SION) with financial aid from the Netherlands Organization for Scientific Research (NWO, formerly ZWO). Jaco de Bakker, Grzegorz Rozenberg and Peter van Emde Boas are thanked for their useful criticisms at several presentations of my work. My former colleagues in the theoretical computer science group of the Eindhoven University of Technology were of great help in many discussions and also contributed in creating a pleasant working atmosphere. Karst has given invaluable assistance through all my studies since my childhood. I am indebted to my parents for their sympathy and encouragement. Special thanks are due to Letty for providing the necessary support.

Eindhoven, May 1992

Ron Koymans

Contents

1	Introduction	1
2	How to Specify	7
3	A Review of Modal and Temporal Logic	13
3.1	Introduction	13
3.2	Classical Modal and Temporal Logic	13
3.3	Temporal Logic with until and since	31
3.4	Temporal Logic in Computer Science	34
4	Polymodal Logics with Inequality	39
4.1	Introduction	39
4.2	Semantics	40
4.3	Proof Theory	52
4.4	Conclusions	61
5	Message Passing Systems	65
5.1	Introduction	65
5.2	What are Message Passing Systems?	66
5.3	How to Specify Message Passing Systems	70
5.4	Inexpressiveness Results	71
5.5	Extensions of Temporal Logic	75
5.6	Specification Examples	77
5.6.1	Example 1: Pure Message Passing Systems	79
5.6.2	Example 2: Channel with Disconnect	82
5.6.3	Example 3: Layered Communication Network	85
	Introduction	85
	Layer 1	87
	Layer 2	88
	Relating Layer 1 and Layer 2	88
	Layer 3 and its Relation to Layer 2	92
5.7	Conclusions	97

6	Time-Critical Systems	99
6.1	Introduction	99
6.2	What are Time-Critical Systems?	101
6.3	How to Specify Time-Critical Systems	103
6.4	Metric Temporal Logic	104
6.5	Specification Examples	118
6.5.1	Example 1: Pure Time-out	121
6.5.2	Example 2: Watchdog Timer	121
6.5.3	Example 3: Wait/delay Statement	123
6.5.4	Example 4: Terminal Adaptor	124
6.5.5	Example 5: Mixing Synchronous and Asynchronous In- put	127
6.5.6	Example 6: Abstract Transmission Medium	131
6.5.7	Example 7: Real-Time Communication Constructs	133
6.5.8	Example 8: Continuously Changing State Variables	136
6.5.9	Example 9: Implementing Reliable Communication	138
6.6	Conclusions	140
7	Summary and Concluding Remarks	143
	Bibliography	151
	Index	162