

Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

321

J. Zwiers

Compositionality, Concurrency and Partial Correctness

Proof Theories for Networks of Processes,
and Their Relationship



Springer-Verlag

Berlin Heidelberg New York London Paris Tokyo

Editorial Board

D. Barstow W. Brauer P. Brinch Hansen D. Gries D. Luckham
C. Moler A. Pnueli G. Seegmüller J. Stoer N. Wirth

Author

Job Zwiers
Philips Research Laboratories
P.O. Box 80.000, NL-5600 JA Eindhoven, The Netherlands

CR Subject Classification (1987): F.3.1, D.2.4, D.2.1, D.3.1

ISBN 3-540-50845-7 Springer-Verlag Berlin Heidelberg New York

ISBN 0-387-50845-7 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 other ways, and storage in data banks. Duplication of this publication or parts thereof is only permitted under the provisions of the German Copyright Law of September 9, 1965, in its version of June 24, 1985, and a copyright fee must always be paid. Violations fall under the prosecution act of the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1989

Printed in Germany

Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
2145/3140-543210

ACKNOWLEDGEMENTS

I thank Willem-Paul de Roever for his cooperation and his many constructive comments.

I thank Peter van Emde Boas, Jozef Hooman and Ernst-Rudiger Olderog, for carefully reading the manuscript.

In the person of Dr. Ir. Henk Bosma I thank the management of Philips Research Laboratories for generously allowing me to finish this monograph

And finally I thank my wife Elisabeth for typing the manuscript, and, most of all, for providing me with all the support I needed.

Table of Contents

1	Introduction	1
1.1	Summary and perspective	1
1.2	Compositionality and modularity	9
1.3	Compositional and modular completeness	12
1.4	Specification and construction of processes	20
1.5	Hoare specifications and Invariant specifications	29
1.5.1	An example of adaptation	38
2	The languages DNP and TNP	41
2.1	Introduction	41
2.2	The language TNP	43
2.3	Intuitive explanation of TNP	46
2.4	Parametrization of TNP processes	52
2.5	Translation of DNP into TNP	54
3	The semantics for TNP	55
3.1	Introduction	55
3.2	The domain of observations	58
3.3	Prefix closures	67
3.4	Semantic operations	71
3.5	Process bases	77
3.5.1	Chaotic closures	77
3.6	Parallel composition	83
3.7	Process environments	87
3.8	The definition of the semantics <i>Obs</i>	88
3.9	An alternative representation	93
4	Correctness formulae	99
4.1	Introduction	99
4.2	The syntax of assertions	100
4.3	The meaning of assertions	102
4.4	Assertions in normal form	106
4.5	Validity and proper validity	112
4.6	Mixed terms	119
4.7	Correctness formulae	124
4.8	Substitution in correctness formulae	127
4.9	Predicate transformers	127
4.10	Natural deduction and correctness formulae	135
4.11	Logical rules	136
4.12	Axioms and rules for (in-) equalities	139

4.13	Satisfiability	140
4.14	The relation between SAT and Hoare formulae	141
4.15	Proper correctness formulae	142
5	Proof systems for TNP	147
5.1	Introduction	147
5.2	The SAT proof system	152
5.2.1	Axioms for atomic processes	152
5.2.2	Rules for the TNP constructs	153
5.2.3	Adaptation rules for the SAT system	154
5.3	The Hoare system	155
5.3.1	Axioms for atomic processes	155
5.3.2	Rules for the TNP constructs	156
5.3.3	Adaptation rules for the Hoare system	158
5.3.4	Extra adaptation rules for the Hoare system	159
5.4	The Invariant System	160
5.4.1	Axioms for atomic processes	160
5.4.2	Rules for the TNP constructs	161
5.4.3	Adaptation rules for the Invariant system	162
5.5	Scott's induction rule	164
5.6	The soundness of the SAT system	167
5.7	The soundness of the Hoare system	174
5.7.1	The Hoare-SAT transformation	174
5.8	Soundness of the Invariant system	187
6	Completeness	197
6.1	Introduction	197
6.2	The expressive power of specifications	197
6.3	Characteristic specifications	201
6.4	Expressiveness of characteristic assertions	206
6.5	Characteristic assertions and recursion again	213
6.6	Compositional completeness of the SAT system	215
6.7	Modular completeness	224
7	The Hoare and Invariant systems	227
7.1	The SAT-Hoare transformation	227
7.2	Compositional completeness for the Hoare system	248
7.3	Freeze predicates	249
7.4	Adaptation completeness for the Hoare system	256
7.5	The Invariant system	258
	References	266