

Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

186

Formal Methods and Software Development



Proceedings of the International Joint Conference
on Theory and Practice of Software Development
(TAPSOFT)

Berlin, March 25–29, 1985

Volume 2:

Colloquium on Software Engineering (CSE)

Edited by Hartmut Ehrig, Christiane Floyd,
Maurice Nivat and James Thatcher



Springer-Verlag
Berlin Heidelberg New York Tokyo

Editorial Board

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

Editors

H. Ehrig

C. Floyd

Technische Universität Berlin

Fachbereich 20, Informatik, SWT FR 5-6

Franklinstr. 28/29, D-1000 Berlin 10, FRG

M. Nivat

L.I.T.P., U.E.R. de Mathématiques

Université de Paris

2, Place Jussieu, F-75251 Paris Cedex, France

J. Thatcher

Math. Department IBM, T.J.W. Research Center

Yorktown Heights, NY 10598, USA

CR Subject Classification (1982): D, D2, F3

ISBN 3-540-15199-0 Springer-Verlag Berlin Heidelberg New York Tokyo

ISBN 0-387-15199-0 Springer-Verlag New York Heidelberg Berlin Tokyo

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically those of translation, reprinting, re-use of illustrations, broadcasting, reproduction by photocopying machine or similar means, and storage in data banks. Under § 54 of the German Copyright Law where copies are made for other than private use, a fee is payable to "Verwertungsgesellschaft Wort", Munich.

© by Springer-Verlag Berlin Heidelberg 1985

Printed in Germany

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.

2145/3140-54321

P R E F A C E

TAPSOFT is an international Joint Conference on Theory and Practice of Software Development. The idea for TAPSOFT originated when it was suggested that the 1985 annual Colloquium on Trees in Algebra and Programming (CAAP) should be held in Berlin. In view of the desired interaction between theory and practice, it was decided to supplement CAAP with a corresponding Colloquium on Software Engineering (CSE), and an advanced seminar connecting both parts. The overall aim of the conference is, to bring together theoretical computer scientists and software engineers (researchers and practitioners) with a view to discussing how formal methods can usefully be applied in software development.

TAPSOFT is being held from March 25-29, 1985 at the Technical University of Berlin. It is organized by the Technical University of Berlin, the Gesellschaft für Informatik, and the European Association for Theoretical Computer Science. The general organizers are Hartmut Ehrig (TU Berlin), Christiane Floyd (TU Berlin), Maurice Nivat (Université de Paris VI) and Jim Thatcher (IBM Research, Yorktown Heights).

TAPSOFT comprises three parts:

- Advanced Seminar on the Role of Semantics in Software Development

The aim of this advanced seminar is to bring together leading experts in the fields of formal semantics and software engineering so as to enable them to present their own work and views on the role of semantics in software development, and to provide a forum for discussions between seminar speakers and all other conference participants.

The seminar consists of invited lecturers and a panel discussion chaired by W. Turski and entitled "Formalism - or else?". Each lecture is followed by a brief response, giving a critical appraisal, and by a general discussion.

The invited speakers are

J. Backus (USA)

M. Broy (Germany)

R.M. Burstall (UK)

A.P. Ershov (USSR)

J.J. Horning (USA)

C.B. Jones (UK)

H.D. Mills (USA)

U. Montanari (Italy)

P. Naur (Denmark)

D.L. Parnas (Canada)

J.C. Reynolds (USA)

D. Scott (USA)

The invited lectures are arranged in three sections:

Concepts of Semantics with a View to Software Development
 The Role of Semantics in Language Design
 The Role of Semantics in the Development of Software Systems

with a considerable overlap between the concerns of the contributions to the different sections.

• Colloquium on Trees in Algebra and Programming (CAAP '85)

The previous Colloquia on Trees in Algebra and Programming were held in France and Italy as autonomous conferences. CAAP '85 is integrated into the TAPSOFT conference.

Following the CAAP tradition, papers accepted for CAAP '85 cover a wide range of topics in theoretical computer science. In line with the theme of the TAPSOFT conference, special emphasis is given in the CAAP '85 program to problems arising in software development.

The selected papers are organized in six sections:

Algorithms and Combinatorics
 Rewriting
 Concurrency
 Graph Grammars and Formal Languages
 Specifications
 Semantics and Data Types.

The program committee for CAAP '85 consists of:

A. Arnold (France)	M.C. Gaudel (France)
G. Ausiello (Italy)	H.-J. Kreowski (Germany)
E. Blum (USA)	B. Mahr (Germany)
W. Brauer (Germany)	U. Montanari (Italy)
R. Cori (France)	M. Nivat (France)
M. Dauchet (France)	G. Plotkin (UK)
H.D. Ehrich (Germany)	G. Rozenberg (Netherlands)
H. Ehrig (Chair, Germany)	E. Wagner (USA)

• Colloquium on Software Engineering (CSE)

CSE focusses on the relevance of formal methods to software development. It tries to answer the following questions:

- Can notions of software engineering be clarified with the help of formal concepts?

- Can concepts of formal semantics be applied in practical software development?
Which supporting tools are needed?
- What experiences have been gained using formal methods and how are they related to the claims of their proponents?
- What alternatives to formal methods can be proposed?

These questions are taken up by researchers presenting concepts together with their realisation, and by practitioners reporting on industrial experience with methodical approaches. This session is supplemented by invited lectures given by experts from leading computer and software companies.

The selected papers are presented in the sections listed below:

Concepts and Methods in Software Development
Tools and Environments
Rigorous Approaches to Programming
Abstract Data Types in Software Development
Views of Concurrency
Industrial Experience

The program committee for CSE consists of:

C. Floyd (Chair, Germany)	P. Löhr (Germany)
C. Haenel (Germany)	P. Naur (Denmark)
P. Henderson (UK)	M. Sintzoff (Belgium)
H.-J. Hoffmann (Germany)	J. Thatcher (USA)
C.B. Jones (UK)	W. Turski (Poland)
G. Kahn (France)	H. Weber (Germany)
W. Koch (Germany)	J. Witt (Germany)
C.H.A. Koster (Netherlands)	

The TAPSOFT conference proceedings are published in advance of the conference in two volumes. The first volume includes the first two sections of invited papers for the Advanced Seminar and the final versions of 19 papers from CAAP '85, selected from a total of 54 papers. One additional selected paper from CAAP '85 was withdrawn by the authors because of an error in the proofs. The second volume includes the third section of invited papers from the Advanced Seminar, the final versions of 20 papers from CSE, selected from a total of 62 papers, together with three invited papers on industrial experience.

We would like to extend our sincere thanks to all program committee members and referees of CAAP '85 and CSE, as well as to the subreferees for CAAP '85 listed below for their care in reviewing and selecting the submitted papers:

E. Astesiano, M. Bellia, G. Berthelot, B. Biebow, M. Bidoit, P. Boehm,
 L. Bonsiepen, L. Bradley, G. Brebner, B. Buchberger, H. Carstensen, C. Choppy,
 H. Cohen, A. Corradini, B. Courcelle, E. Dahlhaus, P. Degano, V. Diekert,
 K. Drosten, J. Engelfriet, W. Fey, P. Flajolet, L. Fribourg, M. Gogolla,
 V. Goltz, U. Grude, J. Gruska, A. Habel, H. Hansen, K.-P. Hasler, D. Haussler,
 C. Kirchner, H. Kirchner, W. Kowalk, K.-J. Lange, G.A. Lanzarone, M. Lightner,
 U. Lipeck, S. Maaß, M. Main, C. Montanero, R. de Nicola, H. Oberquelle,
 R. Orsini, P. Padawitz, F. Parisi-Presicce, J.C. Raoult, M. Simi, F. Simon,
 W. Struckmann, R. Valk, B. Vauquelin, M. Venturini Zilli, G. Violal-Naquet,
 F. Voisin, H. Wagner, E. Welzl, K.-J. Werner, A. Wilharm and K. Winklmann.

We gratefully acknowledge the financial support provided by the following institutions and firms:

Deutsche Forschungsgemeinschaft
 Senator für Wirtschaft und Verkehr, Berlin
 IBM Europe
 Arthur Andersen & Co., Hamburg
 Softlab GmbH, München
 Cray-Research GmbH, München
 Siemens AG, München
 Epsilon GmbH, Berlin

We wish to express our gratitude to the members of the Local Arrangements Committee: Wilfried Koch, Bernd Mahr, Ulrike Niehaus and Christoph Oeters and to all members of the Computer Science Department of the TU Berlin who helped in the organization, in particular: G. Ambach, P. Bacon, H. Barnewitz, M. Bittner, D. Fährdrich, W. Fey, A. Habel, H. Hansen, K.-P. Hasler, K. Kautz, W. Köhler, R. Kutsche, M. Löwe, H. Pribbenow, M. Reisin, K. Schlicht, H. Wagner and K. Wohnhas. Without their help the conference would not have been possible.

Finally, we would like to thank the Springer Verlag, in particular Mrs. I. Mayer for her friendly cooperation in preparing the proceedings.

Berlin, March 1985

Hartmut Ehrig
 Institut für Software
 und Theoretische Informatik
 Technische Universität Berlin

Maurice Nivat
 U.E.R. de Mathématiques
 Université de Paris VI

Christiane Floyd
 Institut für Angewandte
 Informatik
 Technische Universität Berlin

James Thatcher
 IBM T.J.W. Research Center
 Yorktown Heights

CONTENTS OF VOLUME 1

page

INTRODUCTION

H. Ehrig 1

ADVANCED SEMINAR ON THE ROLE OF SEMANTICS IN

SOFTWARE DEVELOPMENT

CONCEPTS OF SEMANTICS WITH A VIEW TO SOFTWARE DEVELOPMENT

M. Broy: 4
Specification and Top Down Design of Distributed Systems
(invited paper)

P. Degano, U. Montanari: 29
Specification Languages for Distributed Systems
(invited paper)

W.L. Scherlis, D.S. Scott: 52
Semantically Based Programming Tools (invited paper)

THE ROLE OF SEMANTICS IN LANGUAGE DESIGN

J. Backus: 60
From Function Level Semantics to Program Transformation
and Optimization (invited paper)

R.M. Burstall: 92
Inductively Defined Functions (invited paper)

J.C. Reynolds: 97
Three Approaches to Type Structure (invited paper)

COLLOQUIUM ON TREES IN ALGEBRA AND PROGRAMMING

ALGORITHMS AND COMBINATORICS

M. Protasi, M. Talamo: 139
On the Maximum Size of Random Trees

B. Chazelle: 145
Fast Searching in a Real Algebraic Manifold with Applications
to Geometric Complexity

P.-L. Curien: 157
Typed Categorical Combinatory Logic

REWRITING	page
D. Kapur, P. Narendran, G. Sivakumar: A Path Ordering for Proving Termination of Term Rewriting Systems	173
D. Kapur, M. Srivas: A Rewrite Rule Based Approach for Synthesizing Abstract Data Types	188
M. Karr: "Delayability" in Proofs of Strong Normalizability in the Typed Lambda Calculus	208
CONCURRENCY	
I. Castellani: Bisimulations and Abstraction Homomorphisms	223
G. Costa: A Metric Characterization of Fair Computations in CCS	239
C. Stirling: A Complete Modal Proof System for a Subset of SCCS	253
GRAPH GRAMMARS AND FORMAL LANGUAGES	
P. Boehm, H.-R. Fonio, A. Habel: Amalgamation of Graph Transformations with Applications to Synchronization	267
U. Lichtblau: Decompilation of Control Structures by Means of Graph Transformations	284
E. Fachini, M. Napoli: Synchronized Bottom - Up Tree Automata and L-Systems	298
SPECIFICATIONS	
D. Sannella, A. Tarlecki: On Observational Equivalence and Algebraic Specification	308
P. Padawitz: Parameter Preserving Data Type Specifications	323
E. Astesiano, G.F. Mascari, G. Reggio, M. Wirsing: On the Parameterized Algebraic Specification of Concurrent Systems	342
SEMANTICS AND DATA TYPES	
E.K. Blum, F. Parisi-Presicce: The Semantics of Shared Submodules Specifications	359
J.A. Makowsky: Why Horn Formulas Matter in Computer Science: Initial Structures and Generic Examples	374

IX

	page
A. Poigné, J. Voss: On the Implementation of Abstract Data Types by Programming Language Constructs	388
C. Choppy, G. Guiho, S. Kaplan: A LISP Compiler for FP Language and its Proof via Algebraic Semantics	403
AUTHOR INDEX	416

CONTENTS OF VOLUME 2

page

INTRODUCTION

C. Floyd:	1
On the Relevance of Formal Methods to Software Development	

ADVANCED SEMINAR ON THE ROLE OF SEMANTICS IN

SOFTWARE DEVELOPMENT

THE ROLE OF SEMANTICS IN THE DEVELOPMENT OF
SOFTWARE SYSTEMS

A.P. Ershov:	
Program Semantics as a Protocol Set (invited paper)	
(paper was not received in time for publication)	
J.J. Horning:	12
Combining Algebraic and Predicative Specifications in Larch	
(invited paper)	
C.B. Jones:	27
The Role of Proof Obligations in Software Design	
(invited paper)	
J. Gannon, R. Hamlet, H. Mills:	42
Functional Semantics of Modules (invited paper)	
P. Naur:	60
Intuition in Software Development (invited paper)	
D.L. Parnas, P.C. Clements:	80
A Rational Design Process: How and Why to Fake It	
(invited paper)	

COLLOQUIUM ON SOFTWARE ENGINEERING

page

CONCEPTS AND METHODS IN SOFTWARE DEVELOPMENT

L. Mathiassen, A. Munk-Madsen: Formalization in Systems Development	101
D.M. Berry, J.M. Wing: Specifying and Prototyping: Some Thoughts on Why They Are Successful	117
L.S. Marshall: A Formal Specification of Line Representations on Graphics Devices	129

TOOLS AND ENVIRONMENTS

G. Snelting: Experiences with the PSG - Programming System Generator	148
N.H. Madhavji, N. Leoutsarakos, D. Vouliouris: Software Construction Using Typed Fragments	163
G. Engels, W. Schäfer: Graph Grammar Engineering: A Method Used for the Development of an Integrated Programming Support Environment	179
D.N. Kimelman: Multidimensional Tree-Structured File Spaces	194

RIGOROUS APPROACHES TO PROGRAMMING

T.S.E. Maibaum, P.A.S. Veloso, M.R. Sadler: A Theory of Abstract Data Types for Program Development: Bridging the Gap?	214
G. Petrone, L. Petrone: Program Development and Documentation by Informal Transformations and Derivations	231

	page
M. Bidoit, C. Choppy:	246
ASSPEGIQUE: An Integrated Environment for Algebraic Specifications	
ABSTRACT DATA TYPES IN SOFTWARE DEVELOPMENT	
L. Bougé, N. Choquet, L. Fribourg, M.C. Gaudel:	261
Application of PROLOG to Test Sets Generation From Algebraic Specifications	
J. Hsiang, M.K. Srivas:	276
A PROLOG Environment for Developing and Reasoning About Data Types	
B. Biebow, J. Hagelstein:	294
Algebraic Specification of Synchronisation and Errors: A Telephonic Example	
VIEWS OF CONCURRENCY	
R. Isle, K.-P. Lühr:	309
Modelling Concurrent Modules	
E.P. Gribomont:	325
Synthesis of Parallel Programs Invariants	
N.G. Leveson, J.L. Stolzy:	339
Analyzing Safety and Fault Tolerance Using Time Petri Nets	
M. Joseph, A. Moitra:	356
Algebraic Specification of a Communication Scheduler	

INDUSTRIAL EXPERIENCE	page
G. Casaglia, F. Pisani: The Integration and Distribution Phase in the Software Life Cycle (invited paper)	371
O. Herzog: Formalized Software Development in an Industrial Environment (invited paper)	385
A. Yonezawa, Y. Matsumoto: Object Oriented Concurrent Programming and Industrial Software Production (invited paper)	395
M.I. Jackson, B.T. Denvir, R.C. Shaw: Experience of Introducing the Vienna Development Method into an Industrial Organisation	410
A. Rushinek, S. Rushinek: EDP System Development Methodology: Auditability and Control	423
K.-H. Alws, I. Glasner-Schapeler: Experiences With Object Oriented Programming	435
AUTHOR INDEX	453