

Lecture Notes in Computer Science

1214

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Michel Bidoit Max Dauchet (Eds.)

TAPSOFT '97: Theory and Practice of Software Development

7th International Joint Conference CAAP/FASE
Lille, France, April 14-18, 1997
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Michel Bidoit

ENS Cachan, Laboratoire Spécification et Vérification

F-94235 Cachan Cedex, France

E-mail: Michel.Bidoit@lsv.ens-cachan.fr

Max Dauchet

Université de Lille, LIFL, UFR IEEA

F-59655 Villeneuve d'Ascq Cedex, France

E-mail: dauchet@lifl.fr

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Theory and practice of software development : proceedings /
TAPSOFT '97, 7th International Joint Conference CAAP/FASE
Lille, France, April 14 - 18, 1997. Michel Bidoit ; Max Dauchet
(ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ;
Hong Kong ; London Milan ; Paris ; Santa Clara ; Singapore ;
Tokyo : Springer, 1997

(Lecture notes in computer science ; Vol. 1214)

ISBN 3-540-62781-2

NE: Bidoit, Michel [Hrsg.]; TAPSOFT <7, 1997, Lille>; GT

CR Subject Classification (1991): D.1-3, F.1-4

ISSN 0302-9743

ISBN 3-540-62781-2 Springer-Verlag Berlin Heidelberg New York

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 1997

Printed in Germany

Typesetting: Camera-ready by author

SPIN 10549438 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

TAPSOFT '97 was the Seventh International Joint Conference on the Theory and Practice of Software Development. It took place at the University of Lille I, France, 14-18 April, 1997.

The TAPSOFT series was started in Berlin in 1985, on the initiative of Hartmut Ehrig, Bernard Mahr, and Christiane Floyd (among others). Since then TAPSOFT has been held biennially, in Pisa (1987), Barcelona (1989), Brighton (1991), Orsay (1993), Aarhus (1995), and Lille (1997).

TAPSOFT is traditionally composed of:

- **Invited lectures** by leading researchers;
- **CAAP**: Colloquium on Trees in Algebra and Programming - covering a wide range of topics in theoretical computer science;
- **FASE**: Colloquium on Formal Approaches in Software Engineering - with the emphasis on practical applicability;
- In recognition of the importance of support tools for practical use of formal approaches, TAPSOFT '97 also included two plenary sessions during which **TOOLS** were demonstrated.

TAPSOFT '97 was the last one, and CAAP '97 is the 22nd and last one too. CAAP was born in Lille in 1976, where it stayed for five years. From 1982 to 1996, it moved across Europe: Genova, Lille (again), L'Aquila, Bordeaux, Berlin, Nice, Pisa, Nancy, Barcelona, Copenhagen, Brighton, Rennes, Orsay, Edinburgh, Aarhus, and Linköping.

Life and science evolve, and conferences must evolve too. This is the reason why TAPSOFT and CAAP/ESOP/CC will now give way to a new series of meetings: The European Joint Conferences on Theory and Practice of Software (ETAPS). Starting in Lisbon, Portugal, 1998, this new annual meeting, covering a wide range of topics in software sciences, will take place in Europe each spring. ETAPS will be a loose and open confederation of existing conferences, such as FASE, and new conferences, such as FoSSaCS (the successor of CAAP), and other events.

TAPSOFT Steering Committee:

A. Arnold, P. Degano, H. Ehrig, M.-C. Gaudel, T. Maibaum, U. Montanari,
P.D. Mosses, M. Nivat, F. Orejas.

Invited Lectures

Special Panel Discussion for the final TAPSOFT and CAAP, before the first ETAPS :

Theoretical Computer Science and Software Sciences: the past, the present, and the future. Invited panelists are Corrado Böhm, a pioneer of this area, Hartmut Ehrig, initiator of TAPSOFT, M. Nivat, initiator of CAAP, and Don Sannella, chairman of ETAPS Steering Committee. Corrado Böhm states that Computer Science is just beginning now. Maurice Nivat agrees with this claim, and points out the importance of algorithmics.

Hartmut Ehrig and Bernd Mahr summarize the evolution of the domain under four trends, and Don Sannella explains why maintenance of a link between theory and practice is a key to the future health of both.

Invited Speakers

Egidio Astesiano and Gianna Reggio illustrate the view that formal methods are useful tools within the context of an overall engineering process. The case of the use of formal specification techniques is developed, with the help of some comparative analysis of concrete examples. They outline, as an attempt, a possible decomposition of that activity into components and facets. Adel Bouhoula, Jean-Pierre Jouannaud, and José Meseguer describe part of a long-term effort to increase expressiveness of algebraic specification languages while at the same time having a simple semantic basis on which efficient execution by rewriting and powerful theorem-proving tools can be based.

Tom Maibaum presents a retrospective on the work of his group, and outlines the basic principles of a general theory of specification. Peter D. Mosses points out that a common framework for algebraic specification and development of software is needed. This framework must provide a family of specification languages at different levels: a central, reasonably expressive language, called CASL, is proposed.

Wolfgang Thomas reviews recent results which aim at generalizing finite automata theory from words and trees to labelled partial orders, with an emphasis on logical aspects. Pictures (two-dimensional words) are considered as an important type of labelled partial order. Frits Vaandrager presents a generalization of the classic theory of testing for (finite state) Mealy machines to a setting of timed automata in the style of Alur and Dill.

CAAP '97**Colloquium on Trees in Algebra and Programming***Programme Committee:*

S. Abramsky (UK)	J.-P. Jouannaud (France)
A. Arnold (France)	H. Kirchner (France)
G. Ausiello (Italy)	U. Montanari (Italy & USA)
C. Böhm (Italy)	M. Nielsen (Denmark)
M. Dauchet (France, chair)	M. Nivat (France)
J. Diaz (Spain)	J.-F. Perrot (France)
H. Ehrig (Germany)	J.-C. Raoult (France)
P. Franchi Zannettachi (France)	S. Tison (France).

The Programme Committee was composed of the chairpersons of all the preceding CAAPs. For the final CAAP, we had one of the greatest number of submissions. Out of 77 submitted papers, 30 papers were selected. These have been grouped into sessions on rewriting and automata, automata and time, termination, bisimulations and Pi-calculus, set constraints, complexity, unification and matching, and types.

FASE '97**Colloquium on Formal Approaches in Software Engineering***Programme Committee:*

E. Astesiano (Italy)	P. Klint (The Netherlands)
D. Basin (Germany)	P.D. Mosses (Denmark)
M. Bidoit (France, chair)	F. Orejas (Spain)
E. Brinksma (The Netherlands)	D. Sannella (UK)
L. Cardelli (USA)	A. Finkel (France)
J. Fitzgerald (UK)	B. Steffen (Germany)
P.G. Larsen (Denmark)	M. Wirsing (Germany)
T. Henzinger (USA)	

The aim of this colloquium was to provide a forum for the presentation, comparison, and discussion of different formal approaches to problems of software specification, development, and verification. Out of 79 submitted papers, the Programme Committee selected 23 for presentation at the conference. These are grouped into sessions on specifications, verification, types and their applications, real-time and distributed systems, semantics, static analysis, refinement, and applications of formal methods to software engineering.

TOOLS

The two plenary TOOLS sessions at TAPSOFT '97 provided demonstrations of eight relevant systems altogether. Moreover, there were facilities for further demonstrations of these and other systems in the breaks and during the parallel sessions. It was hoped that this would give the TAPSOFT participants a useful opportunity to assess some of the main tools that are currently available. Plenary TOOLS sessions were first included in the TAPSOFT programme for TAPSOFT '95 and this was felt to be a very useful complement to the CAAP and FASE presentations. The demonstrations are documented by 4-pages summaries, printed at the back of these proceedings.

Acknowledgments

The organizers gratefully acknowledge the following support:

The CAAP and FASE Programme Committee members, who proved that it is possible to hold good electronic meetings.

Prof. Michel Beaudouin-Lafon, who provided invaluable help for the organization of the FASE electronic PC meeting.

The referees, who provided reports on the submitted papers.

Alfred Hofmann at Springer-Verlag, who kindly agreed to publish the proceedings in the Lecture Notes in Computer Science series.

LIFL (Laboratoire d'Informatique Fondamentale de Lille), which hosted TAPSOFT '97.

The following organizations sponsored TAPSOFT '97:

- The European Association for Theoretical Computer Science
- The HCM European Community project CONSOLE
- Le Ministère de l'Education Nationale, de l'Enseignement Supérieur et de la Recherche
- Le Centre National de la Recherche Scientifique
- L'Ecole Nouvelle d'Ingénieurs en Communication
- La Région Nord/Pas-de-Calais
- Le Département du Nord
- La Ville de Lille
- Le Laboratoire Spécification et Vérification, URA 2236 du CNRS, Ecole Normale Supérieure de Cachan
- Le LIFL, URA 369 du CNRS, Université de Lille I.

TAPSOFT '97 Organizing Committee: A.-C. Caron (chair), M. Tommasi (publicity and demos); Y. André, F. Bossut, R. Gilleron, S. Tison.

Referees

L. Aceto
S. Agerholm
H. Alblas
R. Alur
D. Ancona
H.R. Andersen
S. Anderson
J.M. Armstrong
E. Badouel
S. Van Bakel
H. Balsters
F. Barbanera
M. Bauderon
M. Bellia
V. Benzaken
M. Bernardo
D. Bert
Y. Bertot
M. Boreale
A. Bouajjani
L. Bougé
Z. Bouziane
J. Bradfield
T. Brauner
V. Bruyère
O. Burkart
H. Carlsen
D. Caromel
A.C. Caron
A. Carpi
R. Casas
G. Castagna
G.L. Cattani
D. Caucal
G. Cécé
M.V. Cengarle
M. Cerioli
S. Cherubini
C. Choppy
A. Cichon

M. Clerbout
A. Corradini
B. Courcelle
R. Cousot
S. Crespi-Reghizzi
F. D'Amore
P.R. D'Argenio
O. Danvy
Ph. Darondeau
D. de Frutos-Escrig
C. de Sagazan
Ph. de Groote
D. De Schreye
G. De Michelis
R. de Simone
G. Delzanno
S. Demri
J. Despeyroux
M. Dezani
R. Di Cosmo
A. Dicky
L. Dominguez
A. Dovier
G. Dowek
J. Farre
M. Fernandez
L. Ferreira Pires
M. Fiore
M. Fokkinga
P.G. Franciosa
P. Franclosa
L. Fribourg
D. Frigioni
T. Fruehwirth
J. Gabarro
M. Gabbrielli
F. Gadducci
A. Geser
N. Ghani
R. Giaccio
R. Gilleron

E. Giovannetti
S. Gnesi
E. Goubault
B. Gramlich,
M. Grosse-Rhode
S. Guerrini
Y. Gurevich
J. Gustedt
K. H. Rose
R. Harley
K. Havelund
J. Haveman
J.M. Hélary
D. Hofbauer
M. Hofmann
K. Honda
A. Ingólfssdóttir
P. Inverardi
A. Ireland
I. Gnaedig
J. Engelfriet
P. Jackson
D. Janin
K. Jensen
T. Jéron
R. Joan
S. Kahrs
P. Kars
J.-P. Katoen
C. Kenyon
C. Kirchner
H.C.M. Kleijn
J. Knoop
P. Kosiuczenko
M. Koutny
J. Kuper
O. Kupferman
R. Langerak
F. Laroussinie
K.G. Larsen
S. Larsen

- | | | |
|-----------------|-----------------------|--------------------|
| M. Latteux | M. Nesi | C. Russo |
| P. Le Gall | A. Nickelsen | T.C. Ruys |
| U. Lechner | F. Nielson | A. Saeed |
| S. Leonardi | H.R. Nielson | D. Sangiorgi |
| J. Levy | P. Orback | V. Schmitt |
| L.F. Llana-Diaz | P. Padawitz | Ph. Schnoebelen |
| H.H. Lovengreen | J. Padberg | M. Schwartzbach |
| A. Lozano | V. Padovani | D. Seese |
| D. Lugiez | C. Palamidessi | M.J. Serna |
| C. Lüth | J. Palsberg | J. Sifakis |
| J. M. Talbot | P. Pananagden | A. Skou |
| J. M. Couvreur | A. Panconesi | J. Souquières |
| I. Mackie | S.E. Paynter | I. Stark |
| E. Madelaine | R. Péna | L.J. Steggles |
| B. Mahr | H. Petersen | P. Stevens |
| S. Malecki | A. Pietschker | J.M. Talbot |
| L. Mandel | R. Pino Pérez | A. Tarlecki |
| D. Mandrioli | M. Pistore | P.S. Thiagarajan |
| C. Marché | A. Podelski | M. Tommasi |
| T. Margaria | A. Poetzsch-Heffter | J. Tretmans |
| N. Marti-Oliet | C. Prehofer | S. Tripakis |
| B. Martin | L. Priese | J. Underwood |
| C. Martinez | C. Queinnec | G. Utard |
| A. Martini | S. Rajamani | M. van Sinderen |
| S. Matthews | A.P. Ravn | L. Viganò |
| J. Mazoyer | G. Reggio | P. Viry |
| R. McConnell | M. Regnier | F. Voisin |
| P.A. Mellies | H. Reichel | M. von der Beeck |
| M. Mendler | D. Rémy | P.A. Wacrenier |
| D. Méry | A. Restivo | U. Waldmann |
| S. Merz | B. Reus | I. Walukiewicz |
| A. Middeldorp | O. Ridoux | C. Wedler |
| D. Miller | C. Ringeissen | C. Weise |
| E. Moggi | S. Ronchi Della Rocca | G. Winskel |
| B. Monsuez | Y. Roos | U. Wolter |
| A. Monti | K. Rose | S. Yovine |
| P. D. Mosses | F. Rossi | M. Venturini Zilli |
| P. Mukherjee | L. Roversi | E. Zucca |
| M. Mukund | B. Rozoy | J. Zwiers |
| M. Müller-Olm | A. Rubio | |
| N. Mylonakis | M. Rusinowitch | |

Table of Contents

I Invited Lectures	1
Panel	
Theoretical Computer Science and Software Science :	
The Past, the Present and the Future	3
<i>C. Böhm</i>	
Future Trends of TAPSOFT	6
<i>H. Ehrig, B. Mahr</i>	
New Challenges for Theoretical Computer Science.	11
<i>M. Nivat (Paper in French)</i>	
What Does the Future Hold for Theoretical Computer Science?	15
<i>D. Sannella</i>	
Lectures	
Automata Theory on Trees and Partial Orders.	20
<i>W. Thomas</i>	
A Theory of Testing for Timed Automata	39
<i>F. Vaandrager</i>	
Conservative Extensions, Interpretations Between Theories and All That . . .	40
<i>T. Maibaum</i>	
Specification and Proof in Membership Equational Logic	67
<i>A. Bouhoula, J.-P. Jouannaud and J. Meseguer</i>	
Formalism and Method	93
<i>E. Astesiano, G. Reggio</i>	
CoFI: The Common Framework Initiative for Algebraic Specification and Development	115
<i>P. D. Mosses</i>	
II CAAP	139
CAAP-1 : Rewriting and Automata	
Logicity of Conditional Rewrite Systems	141
<i>T. Yamada, J. Avenhaus, C. Loria-Sáenz, A. Middeldorp</i>	
Simulating Forward-Branching Systems with Constructor Systems	153
<i>B. Salinier, R. Strandh</i>	
Reliable Generalized and Context Dependent Commutation Relations	165
<i>I. Biermann, B. Rozoy</i>	

Word-into-Trees Transducers with Bounded Difference	177
<i>Y. Andre, F. Bossut</i>	
CAAP-2 : Automata and Time	
Generalized Quantitative Temporal Reasoning: An Automata-Theoretic Approach	189
<i>E.A. Emerson, R.J. Treffler</i>	
The Railroad Crossing Problem: Towards Semantics of Timed Algorithms and Their Model-Checking in High-Level Languages.	201
<i>D. Beauquier, A. Slissenko</i>	
Model Checking Through Symbolic Reachability Graph	213
<i>J.M. Ilić, K. Ajami</i>	
Optimal Implementation of Wait-Free Binary Relations	225
<i>E. Goubault</i>	
CAAP-3 : Termination	
Relative Undecidability in the Termination Hierarchy of Single Rewrite Rules	237
<i>A. Geser, A. Middeldorp, E. Ohlebusch, H. Zanema</i>	
Termination Proofs Using <i>gpo</i> Ordering Constraints.	249
<i>T. Genet, I. Gnaedig</i>	
Automatically Proving Termination Where Simplification Orderings Fail . . .	261
<i>T. Arts, J. Giesl</i>	
Generating Efficient, Terminating Logic Programs	273
<i>J.C. Martin, A. King</i>	
CAAP-4 : Bisimulations and Pi-calculus	
Modal Characterization of Weak Bisimulation for Higher-Order Processes . . .	285
<i>M. Baldamus, J. Dingel</i>	
Formats of Ordered SOS Rules with Silent Actions	297
<i>I. Ulidowski, I. Phillips</i>	
A Uniform Syntactical Method for Proving Coinduction Principles in Lambda-calculi	309
<i>M. Lenisa</i>	
A Labelled Transition Systems for pi-epsilon-Calculus	321
<i>F. van Breugel</i>	

CAAP-5 : Set Constraints

Set Operations for Recurrent Term Schematizations.	333
<i>A. Amaniss, M. Hermann, D. Lugiez</i>	
Inclusion Constraints over Non-empty Sets of Trees	345
<i>M. Müller, J. Niehren, A. Podelski</i>	
Grid Structures and Undecidable Constraint Theories	357
<i>F. Seynhaeve, M. Tommasi, R. Treinen</i>	

CAAP-6 : Complexity

Predicative Functional Recurrence and Poly-space	369
<i>D. Leivant, J.-Y. Marion</i>	
On the Complexity of Function Pointer May-Alias Analysis.	381
<i>R. Muth, S. Debray</i>	
Maximum Packing for Biconnected Outerplanar Graphs.. . . .	393
<i>T. Kovacs, A. Lingas</i>	
Synchronization of a Line of Identical Processors at a Given Time	405
<i>S. La Torre, M. Napoli, M. Parente</i>	

CAAP-7 : Unification and Matching

An Algorithm for the Solution of Tree Equations	417
<i>S. Mantaci, D. Micciancio</i>	
E-unification by Means of Tree Tuple Synchronized Grammars	429
<i>S. Limet, P. Réty</i>	
Linear Interpolation for the Higher-Order Matching Problem.	441
<i>A. Schubert</i>	

CAAP-8 : Types

A Semantic Framework for Functional Logic Programming with Algebraic Polymorphic Types.	453
<i>P. Arenas-Sánchez, M. Rodríguez-Artalejo</i>	
Subtyping Constraints for Incomplete Objects	465
<i>V. Bono, M. Bugliesi, M. Dezani-Ciancaglini, L. Liquori</i>	
Partializing Stone Spaces Using SFP Domains	478
<i>F. Alessi, P. Baldan, F. Honsell</i>	
Let-Polymorphism and Eager Type Schemes	490
<i>C. Liang</i>	

III FASE	503
FASE-1 : Specifications	
Semantics of Architectural Connectors	505
<i>J.L. Fiadeiro, A. Lopes</i>	
Protective Interface Specifications.	520
<i>G.T. Leavens, J.M. Wing</i>	
Specifying Complex and Structured Systems with Evolving Algebras.	535
<i>W. May</i>	
FASE-2 : Verification	
A Comparison of Modular Verification Techniques.	550
<i>H. R. Andersen, J. Staunstrup, N. Maretti</i>	
A Compositional Proof of a Real-Time Mutual Exclusion Protocol	565
<i>K. J. Kristoffersen, F. Laroussinie, K. G. Larsen, P. Pettersson, W. Yi</i>	
Traces of I/O-Automata in Isabelle/HOLCF.	580
<i>O. Mueller, T. Nipkow</i>	
FASE-3 : Types and Their Applications	
Reactive Types	595
<i>J.-P. Talpin</i>	
A Type-Based Approach to Program Security	607
<i>D. Volpano, G. Smith</i>	
An Applicative Module Calculus	622
<i>J. Courant</i>	
FASE-4 : Real-time and Distributed Systems	
Compositional Specification of Embedded Systems with Statecharts.	637
<i>J. Philips, P. Scholz</i>	
Verification of Message Sequence Charts via Template Matching.	652
<i>V. Levin, D. Peled</i>	
Probabilistic Lossy Channel Systems	667
<i>P. Iyer, M. Narasimha</i>	
FASE-5 : Semantics	
A Logic of Object-Oriented Programs	682
<i>M. Abadi, K. R. M. Leino</i>	

Auxiliary Variables and Recursive Procedures	697
<i>T. Schreiber</i>	
Locality Based Linda: Programming with Explicit Localities	712
<i>R. De Nicola, G. Ferrari, R. Pugliese</i>	
FASE-6 : Static Analysis	
A Syntactic Theory of Dynamic Binding	727
<i>L. Moreau</i>	
A Unified Framework for Binding-Time Analysis	742
<i>P. Thiemann</i>	
A Typed Intermediate Language for Flow-Directed Compilation	757
<i>J. B. Wells, A. Dimock, R. Muller, F. Turbak</i>	
FASE-7 : Refinement	
Action Refinement as an Implementation Relation.	772
<i>A. Rensink, R. Gorrieri</i>	
Behaviour-Refinement of Coalgebraic Specifications with Coinductive Correctness Proofs	787
<i>B. Jacobs</i>	
FASE-8 : Applications of Formal Methods to Software Engineering	
COMPASS: A Comprehensible Assertion Method	803
<i>S. Bonnier, T. Heyer</i>	
Using LOTOS Patterns to Characterize Architectural Styles	818
<i>M. Heisel, N. Lévy</i>	
Automating Formal Specification-Based Testing.	833
<i>M. R. Donat</i>	
IV TOOLS	849
TOOLS - 1	
Typelab: An Environment for Modular Program Development.	851
<i>F.W. von Henke, M. Luther, M. Strecker</i>	
TAS and IsaWin: Generic Interfaces for Transformational Program Development and Theorem Proving	855
<i>Kolyang, C. Lueth, T. Meyer, B. Wolff</i>	
Proving System Correctness with KIV	859
<i>W. Reif, G. Schellhorn, K. Stenzel</i>	

A New Proof-Manager and Graphic Interface for the Larch Prover	863
<i>F. Voisin</i>	
TOOLS - 2	
A Web-Based Animator for Object Specifications in a Persistent Environment.	867
<i>M. Richters, M. Gogolla</i>	
Publishing Formal Specifications in Z Notation on World Wide Web	871
<i>L. Mikušiak, M. Adámy, T. Seidmann</i>	
DOSFOP - A Documentation Tool for the Algebraic Programming	
Language Opal	875
<i>K. Didrich, T. Klein</i>	
AG: A Set of Maple Packages for Symbolic Computing of	
Automata and Semigroups.	879
<i>P. Caron</i>	
Author Index	883