

Table of Contents

Invited Papers

Theories of Programming: Top-Down and Bottom-Up Meeting in the Middle	1
<i>C. A. R. Hoare</i>	
Scientific Decisions which Characterise VDM	28
<i>C. B. Jones</i>	
Mechanized Formal Methods: Where Next?	48
<i>J. Rushby</i>	
Integration, the Price of Success	52
<i>J. Sifakis</i>	
The Role of Formalism in Method	56
<i>M. Jackson</i>	

Integration into the Development Process

Formal Design for Automatic Coding and Testing: The ESSI/SPACES Project	57
<i>E. Conquet and J.-L. Marty</i>	
A Business Process Design Language	76
<i>H. Eertink, W. Janssen, P. O. Luttighuis, W. Teeuw, and C. Vissers</i>	

Software Architecture

Refinement of Pipe-and-Filter Architectures	96
<i>J. Philipps and B. Rumpe</i>	
A Formalization of Software Architecture	116
<i>J. Herbert, B. Dutertre, R. Riemenschneider, and V. Stavridou</i>	

European Association for Theoretical Computer Science (EATCS)

Component and Interface Refinement in Closed-System Specifications	134
<i>R. Kurki-Suonio</i>	
Semantics of First Order Parametric Specifications	155
<i>D. Pavlović</i>	

Model Checking

A Perfecto Verification: Combining Model Checking with Deductive Analysis to Verify Real-Life Software	173
<i>Y. Kesten, A. Klein, A. Pnueli, and G. Raanan</i>	
Error Detection with Directed Symbolic Model Checking	195
<i>F. Reffel and S. Edelkamp</i>	
Formal Modeling and Analysis of Hybrid Systems: A Case Study in Multi-robot Coordination	212
<i>R. Alur, J. Esposito, M. Kim, V. Kumar, and I. Lee</i>	
On-the-Fly Controller Synthesis for Discrete and Dense-Time Systems ...	233
<i>S. Tripakis and K. Altisen</i>	
On-the-Fly Verification of Linear Temporal Logic	253
<i>J.-M. Cowreur</i>	
Symbolic Model Checking with Fewer Fixpoint Computations	272
<i>D. Déharbe and A. M. Moreira</i>	
Formula Based Abstractions of Transition Systems for Real-Time Model Checking	289
<i>R. Barbuti, N. De Francesco, A. Santone, and G. Vaglini</i>	
IF: An Intermediate Representation and Validation Environment for Timed Asynchronous Systems	307
<i>M. Bozga, J.-C. Fernandez, L. Ghirvu, S. Graf, J.-P. Krimm, and L. Mounier</i>	
Automatic Verification of Pointer Data-Structure Systems for All Numbers of Processes	328
<i>F. Wang</i>	

The B Method

The Use of the B Formal Method for the Design and the Validation of the Transaction Mechanism for Smart Card Applications	348
<i>D. Sabatier and P. Lartigue</i>	
Météor: A Successful Application of B in a Large Project	369
<i>P. Behm, P. Benoit, A. Faivre, and J.-M. Meynadier</i>	
Formal Development of Databases in ASSO and B	388
<i>B. Matthews and E. Locuratolo</i>	

Interpreting the B-Method in the Refinement Calculus	411
<i>Y. Rouzaud</i>	
Compositional Symmetric Sharing in B	431
<i>M. Büchi and R. Back</i>	
Structural Embeddings: Mechanization with Method	452
<i>C. Muñoz and J. Rushby</i>	
The Safe Machine: A New Specification Construct for B	472
<i>S. Dunne</i>	
csp2B: A Practical Approach to Combining CSP and B	490
<i>M. Butler</i>	
Test Criteria Definition for B Models	509
<i>S. Behnia and H. Waeselynck</i>	

Composition and Synthesis

Bunches for Object-Oriented, Concurrent, and Real-Time Specification . . .	530
<i>R. F. Paige and E. C. R. Hehner</i>	
Applications of Structural Synthesis of Programs	551
<i>E. Tyugu, M. Matskin, and J. Penjam</i>	
Towards a Compositional Approach to the Design and Verification of Distributed Systems	570
<i>M. Charpentier and K. M. Chandy</i>	

Telecommunications

Formal Modeling in a Commercial Setting: A Case Study	590
<i>A. Wong and M. Chechik</i>	
KVEST: Automated Generation of Test Suites from Formal Specifications	608
<i>I. Burdonov, A. Kossatchev, A. Petrenko, and D. Galter</i>	
Feature Interaction Detection Using Testing and Model-Checking Experience Report	622
<i>L. du Bousquet</i>	
Emma: Developing an Industrial Reachability Analyser for SDL	642
<i>N. Husberg and T. Manner</i>	
Correction Proof of the Standardized Algorithm for ABR Conformance . .	662
<i>J.-F. Monin and F. Klay</i>	

Verifying a Distributed Database Lookup Manager Written in Erlang 682
T. Arts and M. Dam

Security

Secure Interoperation of Secure Distributed Databases 701
F. Gilham, R. A. Riemenschneider, and V. Stavridou

A Formal Security Model for Microprocessor Hardware 718
V. Lotz, V. Kessler, and G. Walter

Abstraction and Testing 738
S. Schneider

Formal Analysis of a Secure Communication Channel: Secure Core-Email
 Protocol 758
D. Zhou and S.-K. Chin

Probabilistic Polynomial-Time Equivalence and Security Analysis 776
P. Lincoln, J. Mitchell, M. Mitchell, and A. Scedrov

A Uniform Approach for the Definition of Security Properties 794
R. Focardi and F. Martinelli

Group Principals and the Formalization of Anonymity 814
P. F. Syverson and S. G. Stubblebine

Object-Orientation

Developing BON as an Industrial-Strength Formal Method 834
R. F. Paige and J. S. Ostroff

On the Expressive Power of OCL 854
L. Mandel and M. V. Cengarle

A Systematic Approach to Transform OMT Diagrams to a B specification 875
E. Meyer and J. Souquières

Testing

Verifying Consistency and Validity of Formal Specifications by Testing . . . 896
S. Liu

A GSM-MAP Protocol Experiment Using Passive Testing 915
M. Tabourier, A. Cavalli, and M. Ionescu

Author Index 935

Table of Contents, Volume II

Foundations of System Specification (IFIP WG 1.3)

From Informal Requirements to COOP: A Concurrent Automata Approach	939
<i>P. Poizat, C. Choppy, and J.-C. Royer</i>	
A Framework for Defining Object-Calculi	963
<i>F. Lang, P. Lescanne, and L. Liquori</i>	

European Theory and Practice of Software (ETAPS)

A Translation of Statecharts to Esterel	983
<i>S. A. Seshia, R. K. Shyamasundar, A. K. Bhattacharjee, and S. D. Dhodapkar</i>	
An Operational Semantics for Timed RAISE	1008
<i>X. Yong and C. George</i>	
Data Abstraction for CSP-OZ	1028
<i>H. Wehrheim</i>	
Systems Development Using Z Generics	1048
<i>F. Polack and S. Stepney</i>	
A Brief Summary of VSPEC	1068
<i>P. Alexander, M. Rangarajan, and P. Baraona</i>	
Enhancing the Pre- and Postcondition Technique for More Expressive Specifications	1087
<i>G. T. Leavens and A. L. Baker</i>	

Program Verification

On Excusable and Inexcusable Failures	1107
<i>M. Müller-Olm and A. Wolf</i>	
Interfacing Program Construction and Verification	1128
<i>R. Verhoeven and R. Backhouse</i>	
Software Verification Based on Linear Programming	1147
<i>S. Dellacherie, S. Devulder, and J.-L. Lambert</i>	

Integration of Notation and Techniques

Sensors and Actuators in TCOZ	1166
<i>B. Mahony and J. S. Dong</i>	
The UniForM Workbench, a Universal Development Environment for Formal Methods	1186
<i>B. Krieg-Brückner, J. Peleska, E.-R. Olderog, and A. Baer</i>	
Integrating Formal Description Techniques	1206
<i>B. Schätz and F. Huber</i>	

Formal Description of Programming Concepts (IFIP WG 2.2)

A More Complete TLA	1226
<i>S. Merz</i>	
Formal Justification of the Rely-Guarantee Paradigm for Shared-Variable Concurrency: A Semantic Approach	1245
<i>F. S. de Boer, U. Hannemann, and W.-P. de Roever</i>	
Relating Z and First-Order Logic	1266
<i>A. Martin</i>	

Open Information Systems

Formal Modeling of the Enterprise JavaBeans™ Component Integration Framework	1281
<i>J. P. Sousa and D. Garlan</i>	
Developing Components in the Presence of Re-entrance	1301
<i>L. Mihajlov, E. Sekerinski, and L. Laibinis</i>	
Communication and Synchronisation Using Interaction Objects	1321
<i>H. B. M. Jonkers</i>	
Modelling Microsoft COM Using π -Calculus	1343
<i>L. M. G. Feijs</i>	

Co-design

Validation of Mixed SIGNAL-ALPHA Real-Time Systems through Affine Calculus on Clock Synchronisation Constraints	1364
<i>I. M. Smarandache, T. Gautier, and P. Le Guernic</i>	

Combining Theorem Proving and Continuous Models in Synchronous Design	1384
<i>S. Nadjm-Tehrani and O. Åkerlund</i>	
ParTS: A Partitioning Transformation System	1400
<i>J. Iyoda, A. Sampaio, and L. Silva</i>	
A Behavioral Model for Co-design	1420
<i>J. He</i>	

Refinement

A Weakest Precondition Semantics for an Object-Oriented Language of Refinement	1439
<i>A. Cavalcanti and D. A. Naumann</i>	
Reasoning About Interactive Systems	1460
<i>R. Back, A. Mikhajlova, and J. von Wright</i>	
Non-atomic Refinement in Z	1477
<i>J. Derrick and E. Boiten</i>	
Refinement Semantics and Loop Rules	1497
<i>E. C. R. Hehner and A. M. Gravell</i>	

Safety

Lessons from the Application of Formal Methods to the Design of a Storm Surge Barrier Control System	1511
<i>M. Chaudron, J. Tretmans, and K. Wijbrans</i>	
The Value of Verification: Positive Experience of Industrial Proof	1527
<i>S. King, J. Hammond, R. Chapman, and A. Pryor</i>	
Formal Development and Verification of a Distributed Railway Control System	1546
<i>A. E. Haxthausen and J. Peleska</i>	
Safety Analysis in Formal Specification	1564
<i>K. Sere and E. Troubitsyna</i>	
Formal Specification and Validation of a Vital Communication Protocol .	1584
<i>A. Cimatti, P. L. Pieraccini, R. Sebastiani, P. Traverso, and A. Villafiorita</i>	
Incremental Design of a Power Transformer Station Controller Using a Controller Synthesis Methodology	1605
<i>H. Marchand and M. Samaan</i>	

OBJ/Cafe OBJ/Maude

Verifying Behavioural Specifications in CafeOBJ Environment	1625
<i>A. Mori and K. Futatsugi</i>	
Component-Based Algebraic Specification and Verification in CafeOBJ . .	1644
<i>R. Diaconescu, K. Futatsugi, and S. Iida</i>	
Using Algebraic Specification Techniques in Development of Object-Oriented Frameworks	1664
<i>S. Nakajima</i>	
Maude as a Formal Meta-tool	1684
<i>M. Clavel, F. Durán, S. Eker, J. Meseguer, and M.-O. Stehr</i>	
Hiding More of Hidden Algebra	1704
<i>J. Goguen and G. Roşu</i>	

**Abstract State Machines (ASM) and Algebraic Methods in Software
Technology (AMAST)**

A Termination Detection Algorithm: Specification and Verification	1720
<i>R. Eschbach</i>	
Logspace Reducibility via Abstract State Machines	1738
<i>E. Grädel and M. Spielmann</i>	
Formal Methods for Extensions to CAS	1758
<i>M. N. Dunstan, T. Kelsey, U. Martin, and S. Linton</i>	
An Algebraic Framework for Higher-Order Modules	1778
<i>R. Jiménez and F. Orejas</i>	

Avionics

Applying Formal Proof Techniques to Avionics Software: A Pragmatic Approach	1798
<i>F. Randimbivololona, J. Souyris, P. Baudin, A. Pacalet, J. Raguideau, and D. Schoen</i>	
Secure Synthesis of Code: A Process Improvement Experiment	1816
<i>P. Garbett, J. P. Parkes, M. Shackleton, and S. Anderson</i>	
Cronos: A Separate Compilation Toolset for Modular Esterel Applications	1836
<i>O. Hainque, L. Pautet, Y. Le Biannic, and É. Nassor</i>	

Works-in-Progress

Tool Support for Production Use of Formal Techniques	1854
<i>J. C. Knight, P. T. Fletcher, and B. R. Hicks</i>	
Modeling Aircraft Mission Computer Task Rates	1855
<i>J. S. Dong, B. P. Mahony, and N. Fulton</i>	
A Study of Collaborative Work: Answers to a Test on Formal Specification in B	1856
<i>H. Habrias, P. Poizat, and J.-Y. Lafaye</i>	
Archived Design Steps in Temporal Logic	1858
<i>P. Kellomäki and T. Mikkonen</i>	
A PVS-Based Approach for Teaching Constructing Correct Iterations . . .	1859
<i>M. Lévy and L. Trilling</i>	
A Minimal Framework for Specification Theory	1861
<i>B. Baumgarten</i>	
A Model of Specification-Based Testing of Interactive Systems	1862
<i>I. MacColl and D. Carrington</i>	
Algebraic Aspects of the Mapping between Abstract Syntax Notation One and CORBA IDL	1863
<i>R. Ocicǎ and D. Ionescu</i>	
Retrenchment	1864
<i>R. Banach and M. Poppleton</i>	
Proof Preservation in Component Generalization	1866
<i>A. M. Moreira</i>	

Industrial Experience

Formal Modelling and Simulation of Train Control Systems Using Petri Nets	1867
<i>M. Meyer zu Hörste and E. Schnieder</i>	
Formal Specification of a Voice Communication System Used in Air Traffic Control	1868
<i>J. Hörl and B. K. Aichernig</i>	
Model-Checking the Architectural Design of a Fail-Safe Communication System for Railway Interlocking Systems	1869
<i>B. Buth and M. Schröner</i>	

Analyzing the Requirements of an Access Control Using VDMTools and PVS	1870
<i>G. Droschl</i>	
Cache Coherence Verification with TLA+	1871
<i>H. Akhiani, D. Doligez, P. Harter, L. Lamport, J. Scheid, M. Tuttle, and Y. Yu</i>	
Author Index	1873