

ICFEM 2000

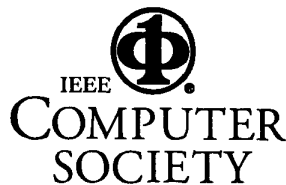
**Third IEEE International Conference on
Formal Engineering Methods**

York, England

4–6 September 2000

Sponsored by
IEEE Computer Society
IEEE Computer Society Technical Committee on Complexity in Computing
University of York

Editors
Shaoying Liu • John A. McDermid • Michael G. Hinchey



Los Alamitos, California

Washington • Brussels • Tokyo

Copyright © 2000 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries may photocopy beyond the limits of US copyright law, for private use of patrons, those articles in this volume that carry a code at the bottom of the first page, provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

Other copying, reprint, or republication requests should be addressed to: IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, P.O. Box 133, Piscataway, NJ 08855-1331.

The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society, or the Institute of Electrical and Electronics Engineers, Inc.

IEEE Computer Society Order Number PR00822
ISBN 0-7695-0822-7
ISBN 0-7695-0824-3 (microfiche)
Library of Congress Number 00-106595

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1 714 821 8380
Fax: + 1 714 821 4641
[http://computer.org/
csbooks@computer.org](http://computer.org/csbooks@computer.org)

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1 732 981 0060
Fax: + 1 732 981 9667
[http://shop.ieee.org/store/
customer-service@ieee.org](http://shop.ieee.org/store/customer-service@ieee.org)

IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81 3 3408 3118
Fax: + 81 3 3408 3553
tokyo.ofc@computer.org

Editorial production by Anne Rawlinson

Cover art production by Alex Torres

Printed in the United States of America by The Printing House

ICFEM 2000

Table of Contents

Message from the General Chair	vii
ICFEM 2000 Committee	ix
Steering Committee	ix
Program Committee.....	xi
■ Invited Speaker	
The Use of Mathematics in Software Engineering.....	1
<i>David Lorge Parnas</i> <i>McMaster University, Canada</i>	
■ Development	
Formal Derivation of Multilayered Hardware/Software Structures	5
<i>T. P. Plaks</i>	
Embedding Formally Proved Code in a Smart Card: Converting B to C.....	15
<i>A. Requet and G. Bossu</i>	
■ Structuring	
Structuring Reactive Systems in B AMN.....	25
<i>K. Lano, K. Androutsopoulos, and P. Kan</i>	
Highly Reliable Component-Based Software Development by Using Algebraic Behavioral Specification.....	35
<i>M. Matsumoto and K. Futatsugi</i>	
Composing Specifications in VSPEC.....	45
<i>A. Venkataraman, M. Rangarajan, and P. Alexander</i>	
■ Algebraic Approaches	
A Unified Algebraic Framework for Specifying Communication Protocols	57
<i>M. Jmaiel</i>	
Formal Treatment of a Family of Fixed-Point Problems on Graphs by CafeOBJ	67
<i>T. Tamai</i>	
■ Invited Speaker	
Legacy Code.....	75
<i>Tony Hoare</i> <i>Microsoft Research, UK</i>	

■ Verification	
SPIN vs. VIS: A Case Study on the Formal Verification of the ATMR Protocol	79
<i>H. Peng, S. Tahar, and F. Khendek</i>	
Mechanical Verification of Transaction Processing Systems	89
<i>D. Chkhaev, J. Hooman, and P. van der Stok</i>	
■ Formal and Informal Notations	
Formal Foundations of Object-Oriented Modeling Notations.....	101
<i>C. Pons and G. Baum</i>	
Using Use Cases in Executable Z.....	111
<i>W. Grieskamp and M. Lepper</i>	
Translating UAN into CSP	121
<i>I. MacColl and D. Carrington</i>	
■ Retrenchment	
Maximally Abstract Retrenchments	133
<i>R. Banach</i>	
Fragmented Retrenchment, Concurrency and Fairness	143
<i>R. Banach and M. Poppleton</i>	
■ Invited Speaker	
Offering Formal Verification Capabilities for Industry Standard Case Tools: Challenges and Results.....	153
<i>Werner Damm</i>	
<i>OFFIS, Germany</i>	
■ Z: Theory and Practice	
Filter Promotion Transformation Strategies for Deriving Efficient Programs from Z Specifications	157
<i>A. E. Abdallah</i>	
ClawZ: Control Laws in Z.....	169
<i>R. Arthan, P. Caseley, C. O'Halloran, and A. Smith</i>	
A Case Study in Partial Specification: Consistency and Refinement for Object-Z	177
<i>C. Taylor, J. Derrick, and E. Boiten</i>	
■ Animation	
An Integrated CSP-Based Tool for the Visualization, Animation and Performance Evaluation of Message Passing Algorithms	189
<i>A. E. Abdallah and M. Green</i>	
An Animatable Operational Semantics of the Verilog Hardware Description Language.....	199
<i>J. P. Bowen, H. Jifeng, and X. Qiwen</i>	
Author Index	209