

Lecture Notes in Computer Science

735

Edited by G. Goos and J. Hartmanis

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



Dines Bjørner Manfred Broy
Igor V. Pottosin (Eds.)

Formal Methods in Programming and Their Applications

International Conference
Academgorodok, Novosibirsk, Russia
June 28 - July 2, 1993
Proceedings

Springer-Verlag

Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Series Editors

Gerhard Goos
Universität Karlsruhe
Postfach 69 80
Vincenz-Priessnitz-Straße 1
D-76131 Karlsruhe, Germany

Juris Hartmanis
Cornell University
Department of Computer Science
4130 Upson Hall
Ithaca, NY 14853, USA

Volume Editors

Dines Bjørner
United Nations University, International Institute for Software Technology
P. O. Box 3058, Macau

Manfred Broy
Institut für Informatik, Technische Universität München
Postfach 20 24 20, D-80290 München, Germany

Igor V. Pottosin
Institute of Informatics Systems
Av. Acad. Lavrentyev 6, Novosibirsk 630090, Russia

CR Subject Classification (1991): F.3-4, D.2-3, I.1-2

ISBN 3-540-57316-X Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-57316-X 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 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 1993
Printed in Germany

Typesetting: Camera-ready by author
Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
45/3140-543210 - Printed on acid-free paper

Preface

The volume comprises the papers selected for presentation at the international conference "Formal Methods in Programming and Their Applications", held in Akademgorodok (Novosibirsk, Russia), June 28 - July 2, 1993.

The conference was organized by the Institute of Informatics Systems of the Siberian Division of the Russian Academy of Sciences. The Institute is engaged in active research in the field of theoretical programming. The Institute has been an organizer of several international conferences related to programming and formal methods in programming but the latter have been considered together with other problems of programming. The current conference is the first forum organized by the Institute which is entirely dedicated to formal methods.

The main scientific tracks of the conference have been centered around the formal methods of program development and program construction. They include:

- specification, synthesis, transformation and verification of programs;
- parallel and distributed computations;
- semantics and logic of programs;
- theory of compilation and optimization;
- mixed computation, partial evaluation and abstract interpretation.

One of the main goals of the conference has been to promote formal methods in programming and to present and discuss the most interesting approaches to practical programming. A number of papers delivered at the conference are aimed at such a goal.

Scientists from eleven countries have been participants to the conference (Austria, Brazil, Canada, Denmark, England, France, Germany, the Netherlands, Russia, Turkey, and the USA as well as from the Territory of Macau)!

Also in the opinion of the participants the conference has been a success and similar conferences should be held in the future, perhaps, with a greater focus on the application of formal methods and the problems connected with it.

The organizers of the conference express their deep gratitude to the colleagues of Russian and international communities who supported actively the conference by rendering assistance and advice, review and participation.

We would also like to thank the Springer-Verlag for excellent co-operation.

FMP&TA Organization

Programme Committee Co-Chairs:

Dines Bjørner United Nations University
Intl.Inst.f.Softw.Techn., Macau
Manfred Broy Technische Universität München
Institut für Informatik, Munich, Germany
Igor Pottosin Institute of Informatics Systems
Novosibirsk, Russia

Programme Committee:

| | |
|--------------------------------|----------------------------------|
| Jan Barzdin, Riga | Reino Kurki-Suonio, Tampere |
| Mikhail Bulyonkov, Novosibirsk | Alexander Letichevski, Kiev |
| Patrick Cousot, Paris | Gregory Mints, Stanford |
| Pierre Deransart, Rocquencourt | Valery Nepomniaschy, Novosibirsk |
| Yuri Ershov, Novosibirsk | Anil Nerode, Ithaca |
| Yuri Gurevich, Ann Arbor | Amir Pnueli, Rehovot |
| Victor Ivannikov, Moscow | Mikhail Taitslin, Tver |
| Cliff Jones, Manchester | Boris Trachtenbrot, Tel-Aviv |
| Philippe Jorrand, Grenoble | Enn Tyugu, Stockholm |
| Vadim Kotov, Palo Alto | |

Invited Speakers

| | |
|----------------------------|---------------------------|
| ChaoChen Zhou, Macau | Bernhard Möller, Augsburg |
| Patrick Cousot, Paris | Peter Pepper, Berlin |
| Yuri Ershov, Novosibirsk | Mikhail Taitslin, Tver |
| Philippe Jorrand, Grenoble | Martin Wirsing, Munich |

Organizing Committee:

Valery Nepomniaschy, chairman
Victor Sabelfeld, publication of proceedings
Mikhail Bulyonkov, general organization
Alexander Bystrov, treasury
Tatiana Churina, scientific secretary

List of Referees

| | |
|----------------|----------------|
| K.Andrew | B.Möller |
| J.Barzdin | T.Mogensen |
| Yu.Gurevich | V.Nepomniaschy |
| P.Deransart | V.Sazonov |
| Yu.Ershov | V.Sabelfeld |
| N.Jones | N.Shilov |
| C.Jones | M.Taitslin |
| P.Jorrand | E.Tyugu |
| R.Kurki-Suonio | M.Valiev |
| A.Letichovsky | I.Virbitskaite |
| G.Mints | C.Zhou |

TABLE OF CONTENTS

FORMAL SEMANTICS METHODS

| | |
|---|----|
| Theory of Domains and Nearby (Invited Paper) | 1 |
| <i>Yu.L.Ershov</i> | |
| Predicative Programming — A Survey | 8 |
| <i>J.Grundy</i> | |
| A Three-Valued Logic for Refinement | 26 |
| <i>J.Grundy</i> | |
| A Compositional Semantics of Combining Forms for Gamma Programs | 43 |
| <i>D.Sands</i> | |

ALGEBRAIC SPECIFICATION METHODS

| | |
|---|----|
| Algebraic Properties of Loop Invariants | 57 |
| <i>G.Futschek</i> | |
| An Approach to Parameterized First-Order Specifications: Semantics, Correctness, Parameter Passing | 67 |
| <i>W.Reif</i> | |
| Algebraic Modelling of Imperative Languages with Pointers | 81 |
| <i>A.V.Zamulin</i> | |

SEMANTIC PROGRAM ANALYSIS AND ABSTRACT INTERPRETATION

| | |
|---|-----|
| Galois Connection Based Abstract Interpretations for Strictness Analysis (Invited Paper) | 98 |
| <i>P.Cousot, R.Cousot</i> | |
| Efficient Chaotic Iteration Strategies with Widenings | 128 |
| <i>F.Bourdoncle</i> | |
| Semantic Analysis of Interval Congruences | 142 |
| <i>F.Masdupuy</i> | |
| Polymorphic Typing for Call-By-Name Semantics | 156 |
| <i>B.Monsuez</i> | |
| Logic Program Testing Based on Abstract Interpretation | 170 |
| <i>L.Lu, P.Greenfield</i> | |

| | |
|---|-----|
| Analysis of Some Semantic Properties for Programs of the Applicative Language AL | 181 |
| <i>V.Sabelfeld</i> | |

SEMANTICS OF PARALLELISM

| | |
|--|-----|
| Communication as Unification in Process Algebras: Operational Semantics (Invited Paper) | 190 |
| <i>Ph.Jorrand</i> | |
| Functional Development of Massively Parallel Programs (Invited Paper) | 217 |
| <i>P.Pepper, J.Ezner, M.Südholt</i> | |
| Observing Some Properties of Event Structures | 239 |
| <i>I.B.Virbitskaite</i> | |

LOGIC OF PROGRAMS

| | |
|--|-----|
| The Other Linear Logic (Invited Paper) | 251 |
| <i>M.Taitlin, D.Arkhangel'sky</i> | |
| Duration Calculi: An Overview (Invited Paper) | 256 |
| <i>Ch.Zhou</i> | |
| A Unique Formalism for Specifying and Designing Objects in a Parallel Environment | 267 |
| <i>J.P.Bahoun, C.Servieres, C.Seguin</i> | |
| On the Smooth Calculation of Relational Recursive Expressions out of First-Order Non-Constructive Specifications Involving Quantifiers | 281 |
| <i>A.M.Haeberer, G.A.Baum, G.Schmidt</i> | |
| Saturation Replaces Induction for a Miniscope Linear Temporal Logic | 299 |
| <i>R.Pluskevičius</i> | |

SOFTWARE SPECIFICATION AND VERIFICATION

| | |
|--|-----|
| A Formal Approach to Requirements Engineering (Invited Paper) | 312 |
| <i>F.Nickl, M.Wirsing</i> | |
| A Two-Phase Approach to Reverse Engineering Using Formal Methods | 335 |
| <i>G.C.Gannod, B.H.C.Cheng</i> | |

| | |
|--|-----|
| Algebraically Provable Specification of Optimized Compilations | 349 |
| <i>V.Levin</i> | |

| | |
|--|-----|
| Formal Derivation of an Error-Detecting Distributed Data Scheduler Using Changeling | 363 |
| <i>H.Lutfiyya, B.McMillin, A.Su</i> | |

| | |
|--|-----|
| REAL92: A Combined Specification Language for Real-Time Concurrent Systems and Properties | 377 |
| <i>V.Nepomniaschy, N.Shilov</i> | |

TRANSFORMATIONAL DEVELOPMENT AND PROGRAM SYNTHESIS

| | |
|--|--|
| Algebraic Calculation of Graph and Sorting Algorithms (Invited Paper) 394 <i>B.Möller</i> | |
|--|--|

| | |
|---|-----|
| Automatical Synthesis of Programs with Recursions | 414 |
| <i>A.P.Beltiukov</i> | |

| | |
|------------------------|-----|
| Parsing in ISBES | 423 |
| <i>E.A.Boiten</i> | |

| | |
|--------------------|-----|
| AUTHOR INDEX | 434 |
|--------------------|-----|