Bernhard Möller Helmut Partsch
Steve Schuman (Eds.)

Formal Program Development

IFIP TC2/WG 2.1 State-of-the-Art Report

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

Bernhard Möller
Institut für Mathematik, Universität Augsburg
Universitätsstr. 2, D-86135 Augsburg, Germany

Helmut Partsch
Fakultät für Informatik, Universität Ulm
Oberer Eselsberg, D-89069 Ulm, Germany

Steve Schuman
Department of Mathematics, University of Surrey
Guildford, Surrey GU2 5XH, United Kingdom

CR Subject Classification (1991): F.3.1, D.2.1, D.2.4, D.2.2, D.1.1, D.2.10, G.2.m, I.1.3, D.2.6

ISBN 3-540-57499-9 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-57499-9 Springer-Verlag New York Berlin Heidelberg

Printed in Germany

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

Preface

Since the late 1960s, much has been done to establish the new field of software engineering. The common objective has been to overcome the well-documented difficulties of software development by adopting the methods, techniques and professional practices of more traditional engineering disciplines. Such efforts have led to significant improvements insofar as project organization and management are concerned, but unfortunately, too many programs produced today still do not behave as expected. However, the last decade has also seen the emergence of a number of approaches wherein software development is viewed as a fully *formal* activity. All of these approaches have *correctness* as their primary focus – that is, their aim is to obtain programs which provably satisfy some given *specification* (a formal statement of the problem to be solved). Thus research in this area necessarily encompasses two principal concerns:

– formal specification of solutions to problems, and
– formal development/calculation of programs from such specifications.

These two topics form the core interests now represented within IFIP Working Group 2.1 on *Algorithmic Languages and Calculi.*

In former times, IFIP Working Group 2.1 was mainly concerned with definition of the *algorithmic languages* ALGOL 60 and ALGOL 68, for which it still has international responsibility. In those days the syntax and semantics of programming languages were at the forefront of computing science research. Since 1975, the Working Group has increasingly focused on *systematic approaches* to programming in its broader sense, and on appropriate *concepts and notations* to support such approaches. Today, the *calculation of programs from specifications* constitutes the central theme of the group's work. This is reflected in its official Aim and Scope, which are as follows:

Aim:
To explore and evaluate new ideas in the field of programming, possibly leading to the design of new languages.

Scope:
1. The study of calculation of programs from specifications.
2. The design of notations for such calculation.

3. The formulation of algorithm theories, using such notations.
4. The investigation of software support for program derivation.
5. Continuing responsibility for ALGOL 60 and ALGOL 68.

For some time the group had felt that its work had reached a state to be presented to a wider audience in the form of in-depth surveys of the various strains of thought. This met well with the emergence of a global activity of IFIP of sponsoring State-of-the-Art Seminars in developing countries. As a result, such a seminar was conceived as to provide access to the foremost front of research on *Formal Program Development.* This book contains background texts for the seminar lectures.

The first actual presentation of the seminar took place in January 1992 near Rio de Janeiro, Brazil. It was hosted by Armando Haeberer from the Pontifica Universidade Católica at Rio de Janeiro and took place in most splendid tropical surroundings on Itacuruçá Island. We are most grateful to Armando for making this seminar possible and for his excellent arrangements. We also express our gratitude to IBM-Brazil, Conselho Naçional de Pesquisa e Disenvolvimiento and Pontifica Universidade Católica at Rio de Janeiro for their generous support. Finally we wish to thank the referees for their detailed evaluations and M. Russling for his help in preparing the manuscript for this volume.

Augsburg, Ulm and Surrey, July 1993

Bernhard Möller, Helmut Partsch, Steve Schuman

Table of Contents