

Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

69

F. L. Bauer, E. W. Dijkstra,
S. L. Gerhart, D. Gries, M. Griffiths,
J. V. Guttag, J. J. Horning, S. S. Owicki,
C. Pair, H. Partsch, P. Pepper,
M. Wirsing, H. Wössner

Program Construction

International Summer School

Edited by F. L. Bauer and M. Broy



Springer-Verlag
Berlin Heidelberg New York 1979

Editorial Board

P. Brinch Hansen D. Gries C. Moler G. Seegmüller
J. Stoer N. Wirth

Editors

Prof. Dr. Dr. h. c. Friedrich L. Bauer
Dipl.-Math. Manfred Broy
Institut für Informatik
der Technischen Universität München
Arcisstraße 21
D-8000 München 2

AMS Subject Classifications (1970): 68-02, 68A05

CR Subject Classifications (1974): 4.12, 4.20, 4.22, 4.30, 4.31, 4.32, 4.34
5.24

ISBN 3-540-09251-X Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-09251-X Springer-Verlag New York Heidelberg Berlin

Library of Congress Cataloging in Publication Data. Main entry under title: Program construction, International Summer School. (Lecture notes in computer science ; 69) "Sponsored by the NATO Scientific Affairs Division." Bibliography: p. Includes index. 1. Electronic digital computers--Programming--Addresses, essays, lectures. I. Bauer, Friedrich Ludwig, 1924- II. Broy, M., 1949- III. North Atlantic Treaty Organization. Division of Scientific Affairs. IV. Series. QA76.6.P75117 001.6'42 79-13704

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically those of translation, reprinting, re-use of illustrations, broadcasting, reproduction by photocopying machine or similar means, and storage in data banks. Under § 54 of the German Copyright Law where copies are made for other than private use, a fee is payable to the publisher, the amount of the fee to be determined by agreement with the publisher.

© by Springer-Verlag Berlin Heidelberg 1979
Printed in Germany

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.
2141/3140-54321

P R E F A C E

In a series of Summer Schools at Marktoberdorf, problems of programming methods and techniques have been dealt with. This fifth undertaking has the general theme of Program Construction. Constructing reliable software at calculable risks is the main concern of Software Engineering. Verification methods have drastically influenced the scene. Only correct programs can be verified, however. Analytic verification techniques have been developed recently into a method of joint construction of program and proof. This more synthetic approach in full consequence leads to general methods for Program Development by Successive Transformations. Both techniques have relative merits in particular situations; a general comparison seems to be difficult, although the transformation approach may be more promising. Moreover, each one method may be viewed as a border case of the other one.

More important than this technical competition is the general observation made at this Summer School as well as at the previous ones: Any reasonable effort in programming needs human thinking more than anything else. The Thinking Programmer knows about the Interplay between Invention and Formal Techniques. Mastering complexity is his aim, and while he needs powerful tools to achieve this, his best assets are the wisdom of knowing his limits.

F. L. Bauer

The International Summer School took place from July 26 to August 6, 1978, in Marktoberdorf. This Summer School was organized under the auspices of the Technical University Munich, and was sponsored by the NATO Scientific Affairs Division under the 1978 Advanced Study Institutes Programme. Partial support for this conference was provided by the European Research Office, the National Science Foundation and the Bund der Freunde der Technischen Universität München.

CONTENTS

I. The Thinking Programmer

Summary (E. W. Dijkstra)	1
E.W. Dijkstra	
A More Formal Treatment of a Less Simple Example	2
Stationary Behaviour of Some Ternary Networks	21
Finding the Correctness Proof of a Concurrent Program	24
On the Interplay between Mathematics and Programming	35
A Theorem about Odd Powers of Odd Integers	47
In Honour of Fibonacci	49
On the Foolishness of "Natural Language Programming"	51
Program Inversion	54
D. Gries	
The Schorr-Waite Graph Marking Algorithm	58
Eliminating the Chaff	70

II. Program Verification

Summary (D. Gries)	75
D. Gries	
Current Ideas in Programming Methodology	77
Basic Axiomatic Definitions	94
The Multiple Assignment Statement	100
Is Sometimes Ever Better Than Always?	113
J. J. Horning	
A Case Study in Language Design: Euclid	125
R.L. London, J.V. Guttag, J.J. Horning, B.W. Lampson, J.G. Mitchell, G.J. Popek	
Proof Rules for the Programming Language Euclid	133
J. J. Horning	
Verification of Euclid Programs	164
S. Owicki	
Specifications and Proofs for Abstract Data Types in Concurrent Programs	174
Specification and Verification of a Network Mail System	198

III. Program Development by Transformation

Summary (F. L. Bauer)		235
F. L. Bauer	Program Development by Stepwise Transformations - The Project CIP. Appendix: Programming Languages under Educational and under Professional Aspects	237
F.L. Bauer, M. Broy, H. Partsch, P. Pepper, H. Wössner	Systematics of Transformation Rules	273
H. Wössner, P. Pepper, H. Partsch, F.L. Bauer	Special Transformation Techniques	290
P. Pepper	A Study on Transformational Semantics	322
F. L. Bauer	Detailization and Lazy Evaluation, Infinite Objects and Pointer Representation	406
H. Partsch, M. Broy	Examples for Change of Types and Object Structures	421
M. Griffiths	Development of the Schorr-Waite Algorithm	464
S. Gerhart	A Derivation Oriented Proof of the Schorr-Waite Marking Algorithm	472

IV. Special Language Considerations and Formal Tools

Summary (J. J. Horning)		493
J. J. Horning	Programming Languages for Reliable Computing Systems	494
M. Griffiths	Programming Methodology and Language Implications	531
F.L. Bauer, M. Broy, R. Gnatz, W. Hesse, B. Krieg-Brückner, H. Partsch, P. Pepper, H. Wössner	Towards a Wide Spectrum Language to Support Program Specification and Program Development	543

VII

M. Broy, R. Gnatz, M. Wirsing	Semantics of Nondeterministic and Noncontinuous Constructs	553
J. V. Guttag	Notes on Type Abstraction	593
C. Pair	Some Theoretical Aspects of Program Construction	617