

Lecture Notes in Computer Science

967

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Jonathan P. Bowen Michael G. Hinchey (Eds.)

ZUM '95: The Z Formal Specification Notation

9th International Conference of Z Users
Limerick, Ireland, September 7-9, 1995
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Jonathan P. Bowen

Oxford University Computing Laboratory

Wolfson Building, Parks Road, Oxford OX1 3QD, United Kingdom

Michael G. Hinchey

Real-Time Computing Laboratory, New Jersey Institute of Technology

University Heights, Newark, NJ 07102, USA and

Department of Computer Science & Information Systems

University of Limerick, Plassey Technological Park

Castletroy, Limerick, Ireland

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

ZUM <9, 1995, Limerick>:

ZUM '95: the Z formal specification notation : proceedings /
9th International Conference of Z Users, Limerick, Ireland,
September 7 - 9, 1995. J. P. Bowen ; Michael G. Hinchey (ed.).

- Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ;

Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 1995

(Lecture notes in computer science ; Vol. 967)

ISBN 3-540-60271-2

NE: Bowen, Jonathan P. [Hrsg.]; GT

CR Subject Classification (1991): D.2, I.1.3, F.3.1, D.1, G.2

ISBN 3-540-60271-2 Springer-Verlag Berlin Heidelberg New York

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 1995

Printed in Germany

Typesetting: Camera-ready by author

SPIN 10485383 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

For ZUM'95, the 9th in the series, we are pleased to report that we received more than twice as many submissions as any previous Z User Meeting. The past four Z User Meeting proceedings have been published in the Springer-Verlag *Workshops in Computing* series. This year the event has been renamed the *International Conference of Z Users*, being the first in the series to be held outside the United Kingdom, although we are retaining the acronym 'ZUM'. Partly as a result of the change of name, the proceedings is now published in the Springer-Verlag *Lecture Notes in Computer Science* series instead.

The activities associated with the meeting span a whole week. The wide selection of tutorials offered for the three days immediately preceding the main meeting, organized by Norah Power, are intended to provide attendees with the opportunity to gain a grounding in the topics covered. On the day before the meeting, the Z standard committee (under ISO/IEC JTC1/SC22 and ANSI X3J21) is meeting and providing an opportunity for ZUM attendees to learn about the proposed international Z standard during part of the day.

After the 1994 Z User Meeting we held a half-day session on educational issues, organized by Neville Dean. This was very successful, and a similar session is to be held immediately after this meeting, again organized by Neville Dean. The forum gives the opportunity for some more interactive discussion in this important area.

We are fortunate to have an excellent selection of invited speakers at ZUM'95. At the last meeting, we found that inviting speakers from outside the Z community was extremely useful in generating debate and fostering cross-fertilization between different parts of the formal methods community at large. Therefore we have continued this newly-established tradition by inviting David Lorge Parnas (McMaster University, Canada), well known for his work on the certification of the Darlington nuclear reactor software using formal methods, John Rushby (SRI International, USA), originator of the PVS theorem prover based on higher-order logic, and Jeannette Wing (Carnegie Mellon University, USA), one of the developers of the Larch algebraic approach to formal specification and verification. In addition, David Gries (Cornell University, USA) is speaking at the educational issues session and giving the after-dinner speech at the conference dinner.

The meeting is organized by the Z User Group (ZUG), in association with the BCS FACS (Formal Aspects of Computing Science) special interest group. For ZUM'95 we are sponsored by BT, who provided student bursaries and some of the expenses for invited speakers, Forbairt for a donation towards the cost of the meeting, Praxis who maintain and run the Z postal mailing list, and the University of Limerick who have made all of their facilities available to us. In addition, the meeting is supported by the ESPRIT ProCoS-WG Working Group (no. 8694) of 24 European industrial and academic partners with an interest in 'Provably Correct Systems', through the provision of funding for attendance by Working Group members.

Norah Power acted as local organizer, and Gemma Ryan organized the bookings for the meeting at the University of Limerick. We are very grateful to Kevin Ryan and Séamus O'Shea for making the facilities of University of Limerick available to us, and for their invaluable support during the organization of the conference.

During the period since ZUM'94, Trevor King (Praxis, UK) has been an extremely efficient Secretary of the Z User Group. Unfortunately work pressures have meant that he must retire from these duties, but Jonathan Hammond, also of Praxis, has been co-opted as a ZUG committee member in his place. We wish Trevor well in his 'retirement'.

In May 1995, a special issue on Z of the *Information and Software Technology* journal was published. This featured revised versions of selected papers presented at the last ZUM, together with some new material. The aim was to include papers covering a balance of issues concerned with the development and use of Z, together with the more recent B-Method and its associated Abstract Machine Notation (AMN) and B-Toolkit. A copy is being issued to all ZUM'95 attendees as part of the delegate's pack.

With the location at Limerick, we decided to hold a limerick competition on Z and formal methods in general. We offer the following in the hope of inspiring a better selection by the end of the conference:

At the Irish School of VDM
 They do it because of the TDM.
 But if they tried Z
 It would go to their head;
 There seems to be no happy meDM.

For US readers, we offer the following, with a non-deterministic last line:

It's as easy as A - B - C
 But then you get to Z.
 It has to be said
 That those who write Z
 Don't like to say $Z = B$.

Further limericks submitted to the competition are held on-line as part of the World Wide Web (WWW) information on the conference to be found under the following URL (Uniform Resource Locator):

<http://www.comlab.ox.ac.uk/archive/z/zum95.html>

This will be kept up to date before and after the meeting with links to any information relevant to ZUM'95. More general information on Z, the B-Method, and other formal methods, maintained as part of the WWW Virtual Library, are also linked from this page.

We hope that ZUM'95 and this associated proceedings will be of interest and benefit to users of Z, and formal methods in general, both in academia and industry.

Oxford & Cambridge
 May 1995

Jonathan Bowen (Conference Chair)
 Mike Hinchey (Programme Chair)

Programme Committee

Jonathan Bowen, Oxford University, UK (*Conference Chair*)
Stephen Brien, Oxford University, UK
Elsbeth Cusack, BT, UK
Neville Dean, Anglia Polytechnic University, UK
David Garlan, Carnegie Mellon University, USA
Howard Haughton, JP Morgan, UK
Ian Hayes, University of Queensland, Australia
Mike Hinchey, NJIT, USA & Univ. of Limerick, Ireland (*Programme Chair*)
Trevor King, Praxis, UK
Kevin Lano, Imperial College, UK
Norah Power, University of Limerick, Ireland (*Tutorial Chair*)
Gordon Rose, University of Queensland, Australia
Chris Sennett, DRA, UK
David Till, City University, UK
Sam Valentine, University of Brighton, UK
Jim Woodcock, Oxford University, UK
John Wordsworth, IBM UK Laboratories, UK

External Referees

All submitted papers were reviewed by the programme committee and/or a number of external referees. We are very grateful to these people, and apologize in advance for any names omitted from this list:

| | | |
|------------------|--------------------|------------------|
| Rod Abraham | Ralph Becket | Rob Booth |
| David Carrington | Bernie Cohen | Mark Dawson |
| Jill Doakes | Tim Drye | Roger Duke |
| Andy Evans | Stephen Goldsack | Jonathan Hammond |
| Mark Humphrys | Stephen Jarvis | Sara Kalvala |
| Ed Kazmierczak | Peter Kearney | J. McDoowi |
| Brendan Mahony | Rex Matthews | Martin Owen |
| Steven Phillips | Hossein Rafsanjani | Tim Regan |
| Liam Relihan | Gordon Rose | Paul Sanders |
| Lesley Semmens | Graeme Smith | Jo Stanley |
| John Staples | Ben Strulo | Paul Swatman |
| Owen Traynor | Mark Utting | Jim Welsh |
| Clazien Wezeman | Luke Wildman | Jeremy Wilson |
| Pete Young | | |

Sponsors

The 9th International Conference of Z Users greatly benefited from the support and financial assistance of the following:

BT
Forbairt
Praxis
University of Limerick

Tutorial Programme

Ten tutorials were presented on the three days prior to the main sessions (4th – 6th September); they were:

Formal Methods and Conformance with Open Distributed Processing
H. Bowman & J. Derrick (University of Kent, UK)

An Introduction to Object-oriented Formal Methods
K.C. Lano & S. Goldsack (Imperial College, UK)

Engineering of Complex Real-Time Systems
A.D. Stoyenko & P.A. Laplante (New Jersey Institute of Technology, USA)

An Introduction to Z
J. Turner (Staffordshire University, UK)

Building Models in Z: An Active Approach
N. Dean (Anglia Polytechnic University, UK)

The Rôle of Formal Specifications in Software Test
H.-M. Hörcher & J. Peleska (DST Deutsche System-Technik GmbH, Germany)

A Tutorial on Proof in Standard Z
J.C.P. Woodcock, S.M. Brien & A. Martin (Oxford University, UK)

Formal Methods, Requirements and Testing
M. Mac an Airchinnigh (University of Dublin, Ireland)

Using Z to Rigorously Review Structured Specifications
L. Semmens (Leeds Metropolitan University, UK)

Teaching Logic as a Tool
D. Gries (Cornell University, USA)

Contents

Methods

| | |
|--|----|
| Language-Free Mathematical Methods for Software Design (Invited Paper) | |
| <i>D.L. Parnas</i> | 3 |
| A Formal Approach to Software Design: The Clepsydra Methodology | |
| <i>P. Ciaccia, P. Ciancarini & W. Penzo</i> | 5 |
| Refining Database Systems | |
| <i>D. Edmond</i> | 25 |

Applications I

| | |
|--|----|
| Structuring a Z Specification to Provide a Formal Framework for Autonomous Agent Systems | |
| <i>M. Luck & M. d'Inverno</i> | 47 |
| On the Use of Formal Specifications in the Design and Simulation of Artificial Neural Networks | |
| <i>P. Duarte de Lima Machado & S.L. Meira</i> | 63 |
| Structuring Specification in Z to Build a Unifying Framework for Hypertext Systems | |
| <i>M. d'Inverno & M. Priestley</i> | 83 |

Proof

| | |
|--|-----|
| Mechanizing Formal Methods: Opportunities and Challenges (Invited Paper) | |
| <i>J. Rushby</i> | 105 |
| An Algebraic Proof in VDM [†] | |
| <i>A.P. Hughes & A.A. Donnelly</i> | 114 |

Testing

| | |
|---|-----|
| Testing as Abstraction | |
| <i>S. Stepney</i> | 137 |
| Improving Software Tests Using Z Specifications | |
| <i>H.-M. Hörcher</i> | 152 |
| Compilation of Z Specifications into C for Automatic Test Result Evaluation | |
| <i>E. Mikk</i> | 167 |

Language

| | |
|--|-----|
| Equal Rights for Schemas in Z | |
| <i>S.H. Valentine</i> | 183 |
| Structuring Z Specifications: Some Choices | |
| <i>A. MacDonald & D. Carrington</i> | 203 |
| Experiments with the Z Interchange Format and SGML | |
| <i>D.M. Germán & D.D. Cowan</i> | 224 |

Panel Session

The Future of Formal Methods in Industry

J.A. Hall, D.L. Parnas, N. Plat, J. Rushby & C.T. Sennett 237

Object-Orientation

Specifications and Their Use in Defining Subtypes (Invited Paper)

B. Liskov & J.M. Wing 245

How Firing Conditions Help Inheritance

B. Strulo 264

Extending \mathcal{W} for Object-Z

G. Smith 276

Applications II

A Formal Semantics for a Language with Type Extension

P. Bancroft & I. Hayes 299

From Z to Code: A Graphical User Interface for a Radiation Therapy Machine

J. Jacky & J. Unger 315

The French Population Census for 1990

P. Bernard & G. Laffitte 334

Animation

Implementing Z in Isabelle

I. Kraan & P. Baumann 355

The Z-into-Haskell Tool-Kit: An Illustrative Case Study

H.S. Goodman 374

Types and Sets in Gödel and Z

M.M. West 389

Exploring Specifications with Mathematica

C. Reilly 408

Method Integration

Using Z to Rigorously Review a Specification of a Network Management System

*T. Bryant, A. Evans, L. Semmens, R. Milovanovic, S. Stockman,
M. Norris & C. Selley* 423

A Two-Dimensional View of Integrated Formal and Informal Specification Techniques

R.B. France & M.M. Larrondo-Petrie 434

Viewpoints and Objects

H. Bowman, J. Derrick & M. Steen 449

Education Session

Teaching Programming as Engineering

D.L. Parnas 471

A Course on Formal Methods in Software Engineering:

Matching Requirements with Design

P. Ciaccia & P. Ciancarini 482

Hints for Writing Specifications

J.M. Wing 497

Mental Models of Z: I — Sets and Logic

N. Dean 498

Equational Logic: A Great Pedagogical Tool for Teaching a Skill in Logic

D. Gries 508

Z Browser — A Tool for Visualization of Z Specifications

L. Mikušiak, V. Vojtek, J. Hasaralejko & J. Hanzelová 510

Appendices

Select Z Bibliography

J.P. Bowen 527

Comp.specification.z and Z FORUM Frequently Asked Questions

J.P. Bowen 561

Author Index 571