Richard J. Boulton
Paul B. Jackson (Eds.)

LNCS 2152

Theorem Proving in Higher Order Logics

14th International Conference, TPHOLs 2001
Edinburgh, Scotland, UK, September 2001
Proceedings

Springer

Richard J. Boulton Paul B. Jackson (Eds.)

Theorem Proving in Higher Order Logics

14th International Conference, TPHOLs 2001
Edinburgh, Scotland, UK, September 3-6, 2001
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Richard J. Boulton
University of Glasgow, Department of Computing Science
17 Lilybank Gardens, Glasgow G12 8QQ, Scotland, UK
E-mail: boulton@dcs.gla.ac.uk

Paul B. Jackson
University of Edinburgh, Division of Informatics
James Clerk Maxwell Building, King's Buildings
Edinburgh EH9 3JZ, Scotland, UK
E-mail: pbj@dcs.ed.ac.uk

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Theorem proving in higher order logics : 14th international conference ;
proceedings / TPHOLs 2001, Edinburgh, Scotland UK, September 3 - 6, 2001.
Richard J. Boulton ; Paul B. Jackson (ed.). - Berlin ; Heidelberg ; New York ;
Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2152)
ISBN 3-540-42525-X

CR Subject Classification (1998): F.4.1, I.2.3, F.3.1, D.2.4, B.6.3

ISSN 0302-9743
ISBN 3-540-42525-X Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Typesetting: Camera-ready by author, data conversion by Christian Grosche, Hamburg
Printed on acid-free paper SPIN 10845517 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 2152
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

Lecture Notes in Computer Science

For information about Vols. 1–2048
please contact your bookseller or Springer-Verlag

Vol. 1982: S. Näher, D. Wagner (Eds.), Algorithm Engineering. Proceedings, 2000. VIII, 243 pages. 2001.

Vol. 1996: P.L. Lanzi, W. Stolzmann, S.W. Wilson (Eds.), Advances in Learning Classifier Systems. Proceedings, 2000. VIII, 273 pages. 2001. (Subseries LNAI).

Vol. 2049: G. Paliouras, V. Karkaletsis, C.D. Spyropoulos (Eds.), Machine Learning and Its Applications. VIII, 325 pages. 2001. (Subseries LNAI).

Vol. 2060: T. Böhme, H. Unger (Eds.), Innovative Internet Computing Systems. Proceedings, 2001. VIII, 183 pages. 2001.

Vol. 2062: A. Nareyek, Constraint-Based Agents. XIV, 178 pages. 2001. (Subseries LNAI).

Vol. 2064: J. Blanck, V. Brattka, P. Hertling (Eds.), Computability and Complexity in Analysis. Proceedings, 2000. VIII, 395 pages. 2001.

Vol. 2065: H. Balster, B. de Brock, S. Conrad (Eds.), Database Schema Evolution and Meta-Modeling. Proceedings, 2000. X, 245 pages. 2001.

Vol. 2066: O. Gascuel, M.-F. Sagot (Eds.), Computational Biology. Proceedings, 2000. X, 165 pages. 2001.

Vol. 2068: K.R. Dittrich, A. Geppert, M.C. Norrie (Eds.), Advanced Information Systems Engineering. Proceedings, 2001. XII, 484 pages. 2001.

Vol. 2069: C. Peters (Ed.), Cross-Language Information Retrieval and Evaluation. Proceedings, 2000. IX, 389 pages. 2001.

Vol. 2070: L. Monostori, J. Váncza, M. Ali (Eds.), Engineering of Intelligent Systems. Proceedings, 2001. XVIII, 951 pages. 2001. (Subseries LNAI).

Vol. 2071: R. Harper (Ed.), Types in Compilation. Proceedings, 2000. IX, 207 pages. 2001.

Vol. 2072: J. Lindskov Knudsen (Ed.), ECOOP 2001 – Object-Oriented Programming. Proceedings, 2001. XIII, 429 pages. 2001.

Vol. 2073: V.N. Alexandrov, J.J. Dongarra, B.A. Juliano, R.S. Renner, C.J.K. Tan (Eds.), Computational Science – ICCS 2001. Part I. Proceedings, 2001. XXVIII, 1306 pages. 2001.

Vol. 2074: V.N. Alexandrov, J.J. Dongarra, B.A. Juliano, R.S. Renner, C.J.K. Tan (Eds.), Computational Science – ICCS 2001. Part II. Proceedings, 2001. XXVIII, 1076 pages. 2001.

Vol. 2075: J.-M. Colom, M. Koutny (Eds.), Applications and Theory of Petri Nets 2001. Proceedings, 2001. XII, 403 pages. 2001.

Vol. 2076: F. Orejas, P.G. Spirakis, J. van Leeuwen (Eds.), Automata, Languages and Programming. Proceedings, 2001. XIV, 1083 pages. 2001.

Vol. 2077: V. Ambriola (Ed.), Software Process Technology. Proceedings, 2001. VIII, 247 pages. 2001.

Vol. 2078: R. Reed, J. Reed (Eds.), SDL 2001: Meeting UML. Proceedings, 2001. XI, 439 pages. 2001.

Vol. 2079: E. Burke, W. Erben (Eds.), Practice and Theory of Automated Timetabling III. Proceedings, 2001. XII, 359 pages. 2001.

Vol. 2080: D.W. Aha, I. Watson (Eds.), Case-Based Reasoning Research and Development. Proceedings, 2001. XII, 758 pages. 2001. (Subseries LNAI).

Vol. 2081: K. Aardal, B. Gerards (Eds.), Integer Programming and Combinatorial Optimization. Proceedings, 2001. XI, 423 pages. 2001.

Vol. 2082: M.F. Insana, R.M. Leahy (Eds.), Information Processing in Medical Imaging. Proceedings, 2001. XVI, 537 pages. 2001.

Vol. 2083: R. Goré, A. Leitsch, T. Nipkow (Eds.), Automated Reasoning. Proceedings, 2001. XV, 708 pages. 2001. (Subseries LNAI).

Vol. 2084: J. Mira, A. Prieto (Eds.), Connectionist Models of Neurons, Learning Processes, and Artificial Intelligence. Proceedings, 2001. Part I. XXVII, 836 pages. 2001.

Vol. 2085: J. Mira, A. Prieto (Eds.), Bio-Inspired Applications of Connectionism. Proceedings, 2001. Part II. XXVII, 848 pages. 2001.

Vol. 2086: M. Luck, V. Mařík, O. Stěpánková, R. Trappl (Eds.), Multi-Agent Systems and Applications. Proceedings, 2001. X, 437 pages. 2001. (Subseries LNAI).

Vol. 2087: G. Kern-Isberner, Conditionals in Nonmonotonic Reasoning and Belief Revision. X, 190 pages. 2001. (Subseries LNAI).

Vol. 2088: S. Yu, A. Păun (Eds.), Implementation and Application of Automata. Proceedings, 2000. XI, 343 pages. 2001.

Vol. 2089: A. Amir, G.M. Landau (Eds.), Combinatorial Pattern Matching. Proceedings, 2001. VIII, 273 pages. 2001.

Vol. 2090: E. Brinksma, H. Hermanns, J.-P. Katoen (Eds.), Lectures on Formal Methods and Performance Analysis. Proceedings, 2000. VII, 431 pages. 2001.

Vol. 2091: J. Bigun, F. Smeraldi (Eds.), Audio- and Video-Based Biometric Person Authentication. Proceedings, 2001. XIII, 374 pages. 2001.

Vol. 2092: L. Wolf, D. Hutchison, R. Steinmetz (Eds.), Quality of Service – IWQoS 2001. Proceedings, 2001. XII, 435 pages. 2001.

Vol. 2093: P. Lorenz (Ed.), Networking – ICN 2001. Proceedings, 2001. Part I. XXV, 843 pages. 2001.

Vol. 2094: P. Lorenz (Ed.), Networking – ICN 2001. Proceedings, 2001. Part II. XXV, 899 pages. 2001.

Vol. 2095: B. Schiele, G. Sagerer (Eds.), Computer Vision Systems. Proceedings, 2001. X, 313 pages. 2001.

Vol. 2096: J. Kittler, F. Roli (Eds.), Multiple Classifier Systems. Proceedings, 2001. XII, 456 pages. 2001.

Vol. 2097: B. Read (Ed.), Advances in Databases. Proceedings, 2001. X, 219 pages. 2001.

Vol. 2098: J. Akiyama, M. Kano, M. Urabe (Eds.), Discrete and Computational Geometry. Proceedings, 2000. XI, 381 pages. 2001.

Vol. 2099: P. de Groote, G. Morrill, C. Retoré (Eds.), Logical Aspects of Computational Linguistics. Proceedings, 2001. VIII, 311 pages. 2001. (Subseries LNAI).

Vol. 2100: R. Küsters, Non-Standard Inferences in Description Logocs. X, 250 pages. 2001. (Subseries LNAI).

Vol. 2101: S. Quaglini, P. Barahona, S. Andreassen (Eds.), Artificial Intelligence in Medicine. Proceedings, 2001. XIV, 469 pages. 2001. (Subseries LNAI).

Vol. 2102: G. Berry, H. Comon, A. Finkel (Eds.), Computer-Aided Verification. Proceedings, 2001. XIII, 520 pages. 2001.

Vol. 2103: M. Hannebauer, J. Wendler, E. Pagello (Eds.), Balancing Reactivity and Social Deliberation in Multi-Agent Systems. VIII, 237 pages. 2001. (Subseries LNAI).

Vol. 2104: R. Eigenmann, M.J. Voss (Eds.), OpenMP Shared Memory Parallel Programming. Proceedings, 2001. X, 185 pages. 2001.

Vol. 2105: W. Kim, T.-W. Ling, Y-J. Lee, S.-S. Park (Eds.), The Human Society and the Internet. Proceedings, 2001. XVI, 470 pages. 2001.

Vol. 2106: M. Kerckhove (Ed.), Scale-Space and Morphology in Computer Vision. Proceedings, 2001. XI, 435 pages. 2001.

Vol. 2107: F.T. Chong, C. Kozyrakis, M. Oskin (Eds.), Intelligent Memory Systems. Proceedings, 2000. VIII, 193 pages. 2001.

Vol. 2108: J. Wang (Ed.), Computing and Combinatorics. Proceedings, 2001. XIII, 602 pages. 2001.

Vol. 2109: M. Bauer, P.J. Gymtrasiewicz, J. Vassileva (Eds.), User Modelind 2001. Proceedings, 2001. XIII, 318 pages. 2001. (Subseries LNAI).

Vol. 2110: B. Hertzberger, A. Hoekstra, R. Williams (Eds.), High-Performance Computing and Networking. Proceedings, 2001. XVII, 733 pages. 2001.

Vol. 2111: D. Helmbold, B. Williamson (Eds.), Computational Learning Theory. Proceedings, 2001. IX, 631 pages. 2001. (Subseries LNAI).

Vol. 2116: V. Akman, P. Bouquet, R. Thomason, R.A. Young (Eds.), Modeling and Using Context. Proceedings, 2001. XII, 472 pages. 2001. (Subseries LNAI).

Vol. 2117: M. Beynon, C.L. Nehaniv, K. Dautenhahn (Eds.), Cognitive Technology: Instruments of Mind. Proceedings, 2001. XV, 522 pages. 2001. (Subseries LNAI).

Vol. 2118: X.S. Wang, G. Yu, H. Lu (Eds.), Advances in Web-Age Information Management. Proceedings, 2001. XV, 418 pages. 2001.

Vol. 2119: V. Varadharajan, Y. Mu (Eds.), Information Security and Privacy. Proceedings, 2001. XI, 522 pages. 2001.

Vol. 2120: H.S. Delugach, G. Stumme (Eds.), Conceptual Structures: Broadening the Base. Proceedings, 2001. X, 377 pages. 2001. (Subseries LNAI).

Vol. 2121: C.S. Jensen, M. Schneider, B. Seeger, V.J. Tsotras (Eds.), Advances in Spatial and Temporal Databases. Proceedings, 2001. XI, 543 pages. 2001.

Vol. 2123: P. Perner (Ed.), Machine Learning and Data Mining in Pattern Recognition. Proceedings, 2001. XI, 363 pages. 2001. (Subseries LNAI).

Vol. 2124: W. Skarbek (Ed.), Computer Analysis of Images and Patterns. Proceedings, 2001. XV, 743 pages. 2001.

Vol. 2125: F. Dehne, J.-R. Sack, R. Tamassia (Eds.), Algorithms and Data Structures. Proceedings, 2001. XII, 484 pages. 2001.

Vol. 2126: P. Cousot (Ed.), Static Analysis. Proceedings, 2001. XI, 439 pages. 2001.

Vol. 2129: M. Goemans, K. Jansen, J.D.P. Rolim, L. Trevisan (Eds.), Approximation, Randomization, and Combinatorial Optimization. Proceedings, 2001. IX, 297 pages. 2001.

Vol. 2130: G. Dorffner, H. Bischof, K. Hornik (Eds.), Artificial Neural Networks – ICANN 2001. Proceedings, 2001. XXII, 1259 pages. 2001.

Vol. 2132: S.-T. Yuan, M. Yokoo (Eds.), Intelligent Agents. Specification. Modeling, and Application. Proceedings, 2001. X, 237 pages. 2001. (Subseries LNAI).

Vol. 2136: J. Sgall, A. Pultr, P. Kolman (Eds.), Mathematical Foundations of Computer Science 2001. Proceedings, 2001. XII, 716 pages. 2001.

Vol. 2138: R. Freivalds (Ed.), Fundamentals of Computation Theory. Proceedings, 2001. XIII, 542 pages. 2001.

Vol. 2139: J. Kilian (Ed.), Advances in Cryptology – CRYPTO 2001. Proceedings, 2001. XI, 599 pages. 2001.

Vol. 2141: G.S. Brodal, D. Frigioni, A. Marchetti-Spaccamela (Eds.), Algorithm Engineering. Proceedings, 2001. X, 199 pages. 2001.

Vol. 2143: S. Benferhat, P. Besnard (Eds.), Symbolic and Quantitative Approaches to Reasoning with Uncertainty. Proceedings, 2001. XIV, 818 pages. 2001. (Subseries LNAI).

Vol. 2146: J.H. Silverman (Eds.), Cryptography and Lattices. Proceedings, 2001. VII, 219 pages. 2001.

Vol. 2147: G. Brebner, R. Woods (Eds.), Field-Programmable Logic and Applications. Proceedings, 2001. XV, 665 pages. 2001.

Vol. 2149: O. Gascuel, B.M.E. Moret (Eds.), Algorithms in Bioinformatics. Proceedings, 2001. X, 307 pages. 2001.

Vol. 2150: R. Sakellariou, J. Keane, J. Gurd, L. Freeman (Eds.), Euro-Par 2001 Parallel Processing. Proceedings, 2001. XXX, 943 pages. 2001.

Vol. 2152: R.J. Boulton, P.B. Jackson (Eds.), Theorem Proving in Higher Order Logics. Proceedings, 2001. X, 395 pages. 2001.

Vol. 2154: K.G. Larsen, M. Nielsen (Eds.), CONCUR 2001 – Concurrency Theory. Proceedings, 2001. XI, 583 pages. 2001.

Vol. 2161: F. Meyer auf der Heide (Ed.), Algorithms – ESA 2001. Proceedings, 2001. XII, 538 pages. 2001.

Vol. 2164: S. Pierre, R. Glitho (Eds.), Mobile Agents for Telecommunication Applications. Proceedings, 2001. XI, 292 pages. 2001.

Preface

This volume constitutes the proceedings of the *14th International Conference on Theorem Proving in Higher Order Logics* (TPHOLs 2001) held 3–6 September 2001 in Edinburgh, Scotland. TPHOLs covers all aspects of theorem proving in higher order logics, as well as related topics in theorem proving and verification.

TPHOLs 2001 was collocated with the *11th Advanced Research Working Conference on Correct Hardware Design and Verification Methods* (CHARME 2001). This was held 4–7 September 2001 in nearby Livingston, Scotland at the Institute for System Level Integration, and a joint half-day session of talks was arranged for the 5th September in Edinburgh. An excursion to Traquair House and a banquet in the Playfair Library of Old College, University of Edinburgh were also jointly organized. The proceedings of CHARME 2001 have been published as volume 2144 of Springer-Verlag's *Lecture Notes in Computer Science* series, with Tiziana Margaria and Tom Melham as editors.

Each of the 47 papers submitted in the full research category was refereed by at least 3 reviewers who were selected by the Program Committee. Of these submissions, 23 were accepted for presentation at the conference and publication in this volume. In keeping with tradition, TPHOLs 2001 also offered a venue for the presentation of work in progress, where researchers invite discussion by means of a brief preliminary talk and then discuss their work at a poster session. A supplementary proceedings containing associated papers for work in progress was published by the Division of Informatics at the University of Edinburgh.

The organizers are grateful to Bart Jacobs and N. Shankar for agreeing to give invited talks at TPHOLs 2001, and to Steven D. Johnson for agreeing to give an invited talk at the joint session with CHARME 2001. Much of Bart Jacobs's research is on formal methods for object-oriented languages, and he is currently coordinator of a multi-site project funded by the European Union on tool-assisted specification and verification of JavaCard programs. His talk covered his own research and research of this project. A three page abstract on the background to his talk is included in this volume. N. Shankar is one of the principal architects of the popular PVS theorem prover, and has published widely on many theorem-proving related topics. He talked about the kinds of decision procedures that can be deployed in a higher-order-logic setting and the opportunities for interaction between them. We are very pleased to include an accompanying paper in these proceedings. Steven D. Johnson is a prominent figure in the formal methods community. His talk surveyed formalized system design from the perspective of research in interactive reasoning. He contrasted two interactive formalisms: one based on logic and proof, the other based on transformations and equivalence. The latter has been the subject of Johnson's research since the early 1980s. An abstract for this talk is included in these proceedings, and a full accompanying paper can be found in the CHARME 2001 proceedings.

The TPHOLs conference traditionally changes continent each year in order to maximize the chances that researchers all over the world can attend. Starting in 1993, the proceedings of TPHOLs and its predecessor workshops have been published in the following volumes of the Springer-Verlag *Lecture Notes in Computer Science* series:

1993 (Canada)	780	1997 (USA)	1275
1994 (Malta)	859	1998 (Australia)	1479
1995 (USA)	971	1999 (France)	1690
1996 (Finland)	1125	2000 (USA)	1869

The 2001 conference was organized by a team from the Division of Informatics at the University of Edinburgh and the Department of Computing Science at the University of Glasgow.

Financial support came from Intel and Microsoft Research. The University of Glasgow funded publicity and the University of Edinburgh loaned computing equipment. This support is gratefully acknowledged.

June 2001 *Richard J. Boulton, Paul Jackson*

Conference Organization

Richard Boulton	(Conference Chair)
Paul Jackson	(Program Chair)
Louise Dennis	(Local Arrangements Co-chair)
Jacques Fleuriot	(Local Arrangements Co-chair)
Ken Baird	(Local Arrangements & Finances)
Deirdre Burke	(Local Arrangements)
Jennie Douglas	(Local Arrangements)
Gordon Reid	(Computing Support)
Simon Gay	(Publicity Chair)
Tom Melham	(TPHOLs/CHARME Coordinating General Chair)

Program Committee

Mark Aagaard (Waterloo)
David Basin (Freiburg)
Richard Boulton (Glasgow)
Albert Camilleri (Netro)
Victor Carreño (NASA Langley)
Gilles Dowek (INRIA Rocquencourt)
Harald Ganzinger (MPI Saarbrücken)
Ganesh Gopalakrishnan (Utah)
Jim Grundy (Intel)
Elsa Gunter (NJIT)
John Harrison (Intel)
Doug Howe (Carleton)
Bart Jacobs (Nijmegen)
Paul Jackson (Edinburgh)
Sara Kalvala (Warwick)
Michael Kohlhase (CMU & Saarbrücken)
J Moore (Texas, Austin)
Sam Owre (SRI)
Christine Paulin-Mohring (Paris Sud)
Lawrence Paulson (Cambridge)
Frank Pfenning (CMU)
Klaus Schneider (Karlsruhe)
Henny Sipma (Stanford)
Konrad Slind (Cambridge)
Don Syme (Microsoft)
Sofiène Tahar (Concordia)

Invited Speakers

Bart Jacobs (Nijmegen)
Steven D. Johnson (Indiana) (*joint with CHARME 2001*)
N. Shankar (SRI)

Additional Reviewers

Andrew A. Adams
John Cowles
Paul Curzon
Abdelkader Dekdouk
Leonardo Demoura
Ewen Denney
Jonathan Mark Ford
Ruben Gamboa
John Gunnels
Martin Hofmann
Matt Kaufmann
Robert Krug
John Longley
Helen Lowe
Tobias Nipkow
Randy Pollack
Christine Röckl
Harald Ruess
N. Shankar
Jun Sawada
Alan Smaill
Luca Vigano
Burkhart Wolff

CHARME 2001 Organization

Tom Melham	(Conference Chair)
Tiziana Margaria	(Program Chair)
Andrew Ireland	(Local Arrangements Chair)
Steve Beaumont	(Local Arrangements)
Lorraine Fraser	(Local Arrangements)
Simon Gay	(Publicity Chair)

Table of Contents

Invited Talks

Regular Contributions

JavaCard Program Verification

Bart Jacobs

Computing Science Institute, University of Nijmegen
Toernooiveld 1, 6525 ED Nijmegen
bart@cs.kun.nl
http://www.cs.kun.nl/~bart

Abstract. This abstract provides some background information on smart cards, and explains the challenges these cards represent for formal verification of software.

Smart Card Trends

Increasingly, physical keys are being replaced by cryptographic keys, which are typically a thousand bits in size. Modern smart cards are the ideal carriers for such keys, because they have enough computing power to do the necessary en- or de-cryption on-card, so that the secret key never has to leave the card. Smart cards are meant to be tamper-resistant secure tokens, typically bound to individuals via a PIN, possibly in combination with biometric identification.

Modern smart cards contain a standard interface (API) for a mini-operating system which is capable of executing application programs (called *applets*) written in high-level languages. The standard language in this area is JavaCard [Che00], which is a "superset of a subset" of Java: it is a simplified version of Java (no threads, multi-dimensional arrays, floats or doubles) with some special features, like persistent objects and a transaction-commit mechanism. Two further characteristics of modern smart cards are:

- **Multi-application.** One card can hold multiple applets for different applications. These are typically centered around the basic cryptographic functions, in for example banking, telecommunication (GSM or UMTS SIMs), access to buildings or networks, identification, voting, *etc.*) Limited communication can be allowed between applets, *e.g.* for automatically adding loyalty points after certain commercial transactions.
- **Post-issuance Downloading.** In principle, it is possible to add applets to a card after it has been issued. This option gives enormous flexibility, but is disabled for security reasons in all currently operational cards.

Security evaluation and certification are very important in the smart card area, because cards are distributed in large numbers for security critical applications. Correctness should be established both for the card platform, and for applets.

R.J. Boulton and P.B. Jackson (Eds.): TPHOLs 2001, LNCS 2152, pp. 1–3, 2001.

Challenges for Formal Methods

The so-called Common Criteria[1] form a standard for the evaluation of IT security. They are much used for smart cards. The Common Criteria involve seven different levels of evaluation, where the two highest levels (6 and 7) require the explicit use of formal methods. Currently available smart cards are evaluated at levels 4 and 5, but there is a clear pressure to move to higher levels. Therefore the smart card industry is open to the use of formal methods. For the formal verification community smart cards form an ideal target since they are within reach of existing verification tools, because of their limited size.

VerifiCard: Aims

In 2000 a European research consortium called VerifiCard[2] was set up, with support from the European Union's IST programme. Its aim is to apply the existing verification tools (mostly theorem provers, but also model checkers) to establish the correctness of JavaCard-based smart cards. The approach is pragmatic: no new development of semantics of Java(Card) from scratch, but application of available expertise and experience in Europe in tool-assisted formal methods, to see what can be achieved in a concentrated effort in a small, well-defined area. This is a potential killer application for formal methods in software verification, which can cut in two directions: if this succeeds, the success may spread to other areas. But if this fails there may be a serious setback for formal methods in software: it is bad news if these methods cannot deliver for such relatively small systems as smart cards.

VerifiCard: Work

The VerifiCard consortium consists of five academic partners, some of which are well-known in the TPHOLs community: Nijmegen (coordinator; Jacobs, Poll), INRIA (Barthe, Bertot, Jensen, Paulin-Mohring), Munich (Nipkow, Strecker), Hagen (Poetzsch-Heffter), SICS (Dam). Also, the consortium involves two smart card manufacturers: Gemplus and SchlumbergerSema (formerly Bull CP8). The planned work is roughly divided along two lines: source code / byte code, and platform / applets. The work involves for instance formalization of the JavaCard virtual machine and byte code verifier, non-interference properties, and specification and verification of the API and of individual applets. Towards the end of the project the industrial partners will carry out a tool-evaluation, to see which approaches can contribute most to their evaluation needs.

Scientific Work of Nijmegen

The talk will elaborate on the work done at Nijmegen, as part of VerifiCard. This involves verification of JavaCard programs, that are part of the API and applets.

[1] See `http://www.commoncriteria.org`.
[2] See `http://www.verificard.org`.

The correctness properties are specified using the interface specification language JML [LBR99], developed by Gary Leavens *et al.* in Iowa, see *e.g.* [PBJ01]. A Java(Card) program with JML annotation is translated to PVS using the LOOP tool [BJ01]. Actual verification in PVS proceeds via a tailor-made Hoare logic for JML [JP01]. See [BJP01] for a small case study, involving the `AID` class from the JavaCard API. Basically, the verification technology for Java is there, but scaling it up to larger programs is still a real challenge.

References

[BJ01] J. van den Berg and B. Jacobs. The LOOP compiler for Java and JML. In T. Margaria and W. Yi, editors, *Tools and Algorithms for the Construction and Analysis of Software (TACAS)*, number 2031 in Lect. Notes Comp. Sci., pages 299–312. Springer, Berlin, 2001.

[BJP01] J. van den Berg, B. Jacobs, and E. Poll. Formal specification and verification of JavaCard's Application Identifier Class. In I. Attali and Th. Jensen, editors, *Proceedings of the Java Card 2000 Workshop*, Lect. Notes Comp. Sci. Springer, Berlin, 2001.

[Che00] Z. Chen. *Java Card Technology for Smart Cards.* The Java Series. Addison-Wesley, 2000.

[JP01] B. Jacobs and E. Poll. A logic for the Java Modeling Language JML. In H. Hussmann, editor, *Fundamental Approaches to Software Engineering (FASE)*, number 2029 in Lect. Notes Comp. Sci., pages 284–299. Springer, Berlin, 2001.

[LBR99] G.T. Leavens, A.L. Baker, and C. Ruby. JML: A notation for detailed design. In H. Kilov and B. Rumpe, editors, *Behavioral Specifications of Business and Systems*, pages 175–188. Kluwer, 1999.

[PBJ01] E. Poll, J. van den Berg, and B. Jacobs. Formal specification of the JavaCard API in JML: The APDU class. *Comp. Networks Mag.*, 2001. To appear.

View from the Fringe of the Fringe
(Joint with CHARME 2001)

Steven D. Johnson

Computer Science Department
Indiana University, Lindley Hall, Room 215
150 S. Woodlawn, Bloomington, IN 47405-7104, USA

Abstract. Formal analysis remains outside the mainstream of system design practice. Theorem proving is regarded by many to be on the margin of exploratory and applied research activity in this formalized system design. Although it may seem relatively academic, it is vital that this avenue continue to be as vigorously explored as approaches favoring highly automated reasoning. Design derivation, a term for design formalisms based on transformations and equivalence, represents just a small twig on the theorem-proving branch of formal system analysis. A perspective on current trends in is presented from this remote outpost, including a review of the author's work since the early 1980s.
A full accompanying paper can be found in the CHARME 2001 proceedings [1].

References

[1] Steven D. Johnson. View from the fringe of the fringe. In Tiziana Margaria and Tom Melham, editors, *Proceedings of 11th Advanced Research Workshop on Correct Hardware Design and Verification Methods (CHARME 2001)*, volume 2144 of *Lecture Notes in Computer Science*. Springer Verlag, 2001.

R.J. Boulton and P.B. Jackson (Eds.): TPHOLs 2001, LNCS 2152, pp. 4–4, 2001.