Lecture Notes in Computer Science **10160**

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison
Lancaster University, Lancaster, UK
Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA
Josef Kittler
University of Surrey, Guildford, UK
Jon M. Kleinberg
Cornell University, Ithaca, NY, USA
Friedemann Mattern
ETH Zurich, Zurich, Switzerland
John C. Mitchell
Stanford University, Stanford, CA, USA
Moni Naor
Weizmann Institute of Science, Rehovot, Israel
C. Pandu Rangan
Indian Institute of Technology, Madras, India
Bernhard Steffen
TU Dortmund University, Dortmund, Germany
Demetri Terzopoulos
University of California, Los Angeles, CA, USA
Doug Tygar
University of California, Berkeley, CA, USA
Gerhard Weikum
Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at http://www.springer.com/series/7408

Thomas Gibson-Robinson · Philippa Hopcroft
Ranko Lazić (Eds.)

Concurrency, Security, and Puzzles

Essays Dedicated to Andrew William Roscoe on the Occasion of His 60th Birthday

Springer

Editors
Thomas Gibson-Robinson
University of Oxford
Oxford
UK

Philippa Hopcroft
University of Oxford
Oxford
UK

Ranko Lazić
University of Warwick
Coventry
UK

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-51045-3 ISBN 978-3-319-51046-0 (eBook)
DOI 10.1007/978-3-319-51046-0

Library of Congress Control Number: 2016960194

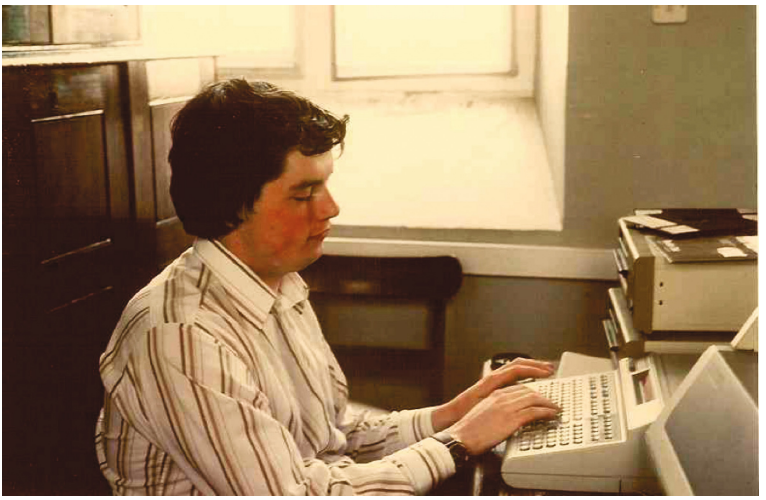
LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer International Publishing AG 2017
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Cover illustration: Self-portrait of the honoree.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland



Bill Roscoe working in University College, Oxford in 1979.
Taken by Coby Roscoe.

Preface

This volume contains papers written in honour of A.W. Roscoe, better known as Bill Roscoe, on the occasion of his 60th birthday. Bill was born in Dundee and went on to read Mathematics at University College, Oxford (Univ) in 1975, achieving the top first. Bill's main tutors at Oxford were Michael Collins and Gordon Screaton, both of whom have had huge influences on his life and career. Remarkably, Bill has never left Univ, and is currently a Senior Research Fellow at the college, having previously been a College Lecturer and a Tutorial Fellow.

After completing his undergraduate degree, Bill completed a DPhil at Oxford under the supervision of Professor Sir Tony Hoare. Bill's thesis was on the mathematical foundations of Communicating Sequential Processes (CSP), a topic to which he has become synonymous and that has come to dominate his research career. His early work on CSP in the 1980s, together with Steve Brookes and others, focused on formally defining the mathematical foundations of CSP, and resulted in the development of the form of CSP used today. More widely, Bill has made huge contributions to the understanding of concurrency, as demonstrated by the fact that his first textbook on the subject, *The Theory and Practice of Concurrency*, has over 2,000 citations. He is undoubtably one of the leading figures worldwide in the area of process algebras. Bill's research interests are not only confined to Computer Science; he also published a number of papers on topology, leading to an Erdös number of 2.

Bill has been the driving force behind the development of FDR, the CSP refinement checker, since its inception in the early 1990s. This also involved the setting up of the first company that he was involved in, Formal Systems (Europe) Limited. Bill is not only the most ardent user of FDR but has also made considerable contributions to the ideas behind FDR; most notably in determining how to efficiently perform refinement checking, and to FDR's compression functions. He has also built various tools to translate other languages into CSP for analysis using FDR, including one for analysing simple imperative programs, and another for analysing Statecharts.

Bill's passion for theory is matched with an equal desire to see his research make an impact in practice by solving industrial challenges. One of Bill's (many) remarkable qualities is his ability to deal with the details of analysing a horrendously combinatorially complex system in his head, even while performing at a board. He became known by some of his industrial partners as the "Professor of Difficult Sums", as he is the go-to person for fiendish challenges! Bill has enjoyed numerous fruitful collaborations with industry partners and government agencies throughout his career; for example, with Draper, Inmos, U.S. Office of Naval Research, and QinetiQ (and its previous versions). One of his early collaborations with Inmos on the verification of the floating-point unit on the T800 transputer, led to a Queen's Award in 1990. These collaborations have proven to be a stimulating influence on Bill's research over the

years, as is demonstrated to this day by his exciting research projects, which combine theory and practice in order to tackle the escalating costs of software development.

Bill is known for his love of solving puzzles using CSP and FDR. One of Bill's first papers was on this topic, and involved solving the so-called trains problem, where trains have to be moved to the correct sheds over a predetermined configuration of tracks. He later wrote a practical to accompany the undergraduate course in Concurrency at Oxford that required students to solve this problem, which is still in use today. He is particularly proud of the fact that FDR managed to find a shorter solution than previously known to a variant of the puzzle. Bill's passion for solving puzzles using CSP and FDR extends over many well-known examples and has become so well-established that they are now used as standard benchmarks for FDR. Indeed, he evaluates all of his new hardware on the basis of how quickly it can master his standard peg solitaire script!

In the mid-1990s Bill became involved in using CSP to analyse the security properties of systems. He first worked on analysing security protocols using CSP and FDR, along with Gavin Lowe amongst others. This work led to FDR becoming widely used as a protocol analysis tool, and also led to many advances in FDR particularly enhancing its scalability. He also worked on information flow, and developed one of the few definitions of non-interference that deals adequately with refinement. Lately, Bill has worked on human-interactive security protocols that allow secure networks to be established using non-fakable information that can be exchanged between humans. This technology has industrial applications such as mobile payments, medical data exchange, and telephony.

Bill's research record is matched by an astonishing track record of leadership and administration within the University of Oxford. Bill took over as Head of the Computer Laboratory at Oxford in 2003, and over a ten-year period led the department to nearly triple in size. His ambitions for the department were perhaps best illustrated in 2011, when he oversaw the change in name of the department, from the Computer Laboratory to the Department of Computer Science. This change in name clearly signalled to the world that the department was now intent on being a world-leading department of computer science — a status that has subsequently been confirmed by many third-party rankings. (Just before we went to press, the *Times Higher Education* published its first ever ranking of worldwide computer science departments, placing Oxford third in the world overall, and first in the UK.) In terms of scale and breadth of research interests, the present Department of Computer Science bears very little resemblance to the Computer Laboratory that Bill joined nearly 40 years ago; but in terms of quality, as these rankings clearly testify, the Department remains world class.

Bill has also been involved in the administration of Univ since he was appointed a tutorial fellow in 1983. Notably, he was appointed as a tutorial fellow in Computer Science two years prior to the degree launching! Bill therefore taught Mathematics for the first two years of his fellowship, which was a major contributor to the cohesion between Computer Science and Mathematics at Univ, something that continues to this day.

No account of Bill would be complete without the mention of his wife Coby, whom he met during his student days at Univ. Their story began in college over a computer and an accounting system in need of some software. The rest is history, filled with amazing stories of their travels around the world together.

November 2016

Thomas Gibson-Robinson
Philippa Hopcroft
Ranko Lazić

Bill Roscoe, on His 60th Birthday

Tony Hoare

Microsoft Research, Cambridge, UK

Happy Birthday, Bill! And many happy returns of the day! And not just of today. I wish you also many returns of the earlier happy days that you and I have spent together as friends and colleagues. For the benefit of our more recent mutual friends and colleagues assembled here, may I recall with gratitude and pleasure some of your notable earlier contributions to the development of Computer Science at Oxford?

In 1978, Bill was awarded the Junior Mathematical Prize for top marks in the Final Examination of his Bachelor's degree at Oxford. Nevertheless, he bravely registered as a Doctoral student in the Programming Research group (PRG), which was then populated by just two academics (Joe Stoy and myself) and two programmers (Malcolm Harper and Andrew Newman). Together with a fellow student Steve Brookes, he embarked on a search for a formal semantics for Communicating Sequential Processes (CSP). This was a new theoretical concurrent programming language which I had designed and published before arrival at Oxford. Indeed, the formalisation of its semantics was a strong part of my motive for moving to Oxford.

An early assignment that I gave to Bill and Steve was to formalise the algebraic laws which governed reasoning about programs expressed in CSP. The next week they came back to ask a question: What were the laws that I wanted? I had no idea how to answer that question. So I threw it straight back at them, as their next assignment, to tell me what laws I should be wanting. To do that we started on an investigation into a mathematical model (then known as a denotational semantics) which the laws would have to satisfy.

On the basis of this model, Bill and Steve proved a highly elegant collection of algebraic laws, entirely to my satisfaction. Bill also formalised and proved the correctness of an abstract implementation of the language, using Gordon Plotkin's notion of a Structural Operational Semantics. The proof of the consistency of a model with its algebraic laws and its operational implementations has been the inspiration for my own life's work on Unifying Theories of Programming right up to the present day.

On graduation in 1982, Bill obtained an IBM Research Fellowship of the Royal Society, and continued work of the CSP model and its applications. At the same time he pursued his previous interest in Topology. In 1983, he accepted the offer of a University Lectureship in Computation at the PRG. He immediately established a close collaboration with David May, the Chief Designer of the Inmos Transputer and its assembly language occam. He led a joint project to check the design of the Inmos floating point unit for their transputer chip, whose architecture was explicitly based on CSP.

This project won, jointly for Inmos and the PRG, the Queen's Award for Technological Achievement, 1990. The award was an enormous boost for the PRG, as a counterbalance to its established reputation as one of the most theoretical Computer Science Departments in the UK. Further boosts were Bill's success between 1985 and

1994 in winning research grants totalling around $1.5 million in research grants from US sources, and about £0.25 million from UK sources.

I am delighted to exploit this occasion to acknowledge in public my deep personal gratitude for all Bill's help to me personally in fulfilling my duties and achieving my aims for the development of Computer Science at Oxford. And on a more personal level, he was the organiser of my own 60th birthday party, and my retirement symposium in 1999, and another symposium organised jointly with Cliff Jones and Ken Wood for my 75th birthday in Cambridge. He edited the proceedings of the two symposia, and they were presented to me as festschrifts.

Let me conclude by turning again to the earlier days. When Bill's external examiner Peter Cameron received a copy of Bill's Doctoral Thesis, he phoned me with the rueful comment that it contained sufficient material to fill three successful theses of the more normal kind. I was able to console him that he needed to examine only one of them, and he could select whichever one he wished.

Now it is my rueful comment that Bill's lifetime achievement would be enough to fill three normal lifetimes; and in this address, I have selected only on the early years of just one of them. They have given me a lot to thank him for. During this symposium, I greatly look forward to hearing more up-to-date accounts of the many facets of his later achievement.

A Tribute to Bill Roscoe, on the Occasion of His 60th Birthday

Stephen Brookes

Department of Computer Science, Carnegie Mellon University, Pittsburgh, USA

I first met Bill Roscoe as an undergrad at University College in 1975. We were both studying Mathematics, and began to gravitate towards Logic and Computer Science in our second and third years. Later we became graduate students together, and we have known each other as friends and colleagues for over 40 years.

At Univ Bill came across initially as a rather shy and enigmatic Scotsman, but we became friends soon, despite his insistence on introducing me to the Poetic Gems of William McGonagall, oft cited as the "worst poet in the world" and (like Bill) hailing from Dundee. Bill has a warm sense of humor (I have lived in the USA long enough that my spell checker no longer corrects back to UK spelling) and I'm sure he agrees with the general assessment of McGonagall's (lack of) talent. Bill also turns out to have a highly competitive (not to say vicious) approach to croquet, which we discovered on the lawns of Logic Lane and Stavertonia. He is also an excellent chef, although he does tend to use every pot and pan in the kitchen.

Academically, it soon became clear that Bill was a star: in 1978 he achieved the top all-round university-wide score in Finals. We both stayed on for graduate studies at the Programming Research Group, where we got started with Tony Hoare, who was looking for a mathematical semantics for CSP. Looking back, I would characterize those years at the PRG as an incredibly satisfying and formative period for both of us. Under Tony's gentle guidance, we began to find our own feet as researchers. This was a time marked by failures and divergences, as we tried out ideas, learned what worked and what did not. Our dissertations emerged from this collaborative effort, culminating in our first journal paper ("A Theory of Communicating Sequential Processes", known to us as HBR, published in J. ACM, July 1984). This work also led ultimately to the foundations of the FDR model checker, which Bill and his team developed into a highly effective tool with many practical applications. We also travelled together to attend our first international conference, (ICALP, Noordwijkerhout, July 1980). Building on our Ph.D. foundations, Bill and I organized a research conference (Seminar on Concurrency, July 1984), together with Glynn Winskel. The failures/divergences model, CSP, and FDR form a lifelong thread connecting us, even as our own research paths diverged into many new directions. It is always rewarding to look back on past achievements and reflect. It is especially pleasing to recall many happy days of working with Bill (and Tony), and to realize that those early days were when we found our own voices and learned to explore and experiment.

As grad students we both enjoyed a couple of years as Lecturers at Univ. In the following years, I moved abroad and Bill travelled briefly across the High to St. Edmund Hall, then back to Univ. Bill came to Florida for my wedding (to Lynn) in 1984, and

Lynn and I came back to Oxford a few years later, when Bill and Coby got married. We have remained fast friends and colleagues. Bill has had an outstanding career and he continues to shine as a researcher, author, advisor, and even administrator. His many graduate students have gone on to establish themselves in academia and industry. He can look back proudly on his own achievements and those of his advisees.

Bill never ceases to remind me that I am older than he is (albeit by less than a month), and that my own hair became grey faster than his. So it is appropriate for me to welcome Bill to the over-60's generation, even though he'll always be a couple of weeks behind me. I look forward to many more years of research, and may more years of friendship. I end with the following paraphrase in echo of McGonagall:

This is Bill's first 60th Birthday year,

And will be the only one, I rather fear:

Therefore, sound drums and trumpets with cheer,

Until the echoes are heard o'er land, sea, email and Twitter.

Herding Cats, Oxford Style

Michael Wooldridge

Department of Computer Science, University of Oxford, Oxford, UK

Managing academics, so the saying goes, is like trying to herd cats. Academic departments, by and large, are not like closely managed small businesses, but more like a collection of cottage industries, each only dimly aware that they are part of a larger activity (the university). It often comes as a complete surprise to outsiders, who imagine that as employees of a university will naturally owe their allegiance to their employer, but the nature of academic life is such that many academics feel their primary allegiance is not to their university, but to their discipline (maths, physics, computer science, and so on). And as if this situation were not strange enough, at Oxford, we have colleges thrown in the mix as well. Academic freedom means that we feel entirely comfortable saying "no" to those who, technically speaking, are our bosses. For good measure, we often like to point out the foolishness of their ways in detail, perhaps in the hope that they will not bother us again. Those benighted souls who agree to be the head of an academic department are burdened with responsibility by the bucketload, but precious little actual power to effect change. Little wonder that many academic heads retreat to their offices, keep their heads down, and try to get through their sentence creating as little fuss as possible.

I have been a member of the UK academic community for more than a quarter of a century. I have spent a great deal of time over that period studying the dynamics of UK computer science departments. Over that period, there has been a lot of change. Some small departments have grown big; some weak departments have grown strong; and some formerly strong departments have plummeted in quality. Naturally, I am curious about what drives the successes, and what factors lead to the failures.

The recipe seems to be relatively simple, but surprisingly difficult to get right. It certainly isn't corporate management techniques that drives academic excellence. Key performance indicators, extensive documentary paper trails, strategic planning away days, and all the rest of it certainly has its place, but you can diligently do all that stuff and more, and still remain resolutely mediocre. There is plenty of evidence of that, not just in the UK academic sector, but in universities across the world.

So what is it, that drives success? Colleagues who have read so far will no doubt be pleased to hear my firm rejection of the culture of managerialism, but they may be less pleased to hear what I am about to say next. Success stories in academia, as elsewhere, don't happen by accident. Wherever I see success, I see evidence of *leadership*.

Leadership and management, of course, are *not* the same thing; academic leadership is hard to define. But it certainly involves having a clear and realistic vision of where you are going; a balanced understanding of your weaknesses, and those areas that you can realistically make progress; the ability to make your case, and have difficult conversations with those who don't get the point; a clear understanding of

academic excellence, and a willingness to support it; and above all, a determination to keep hold of what universities are really all about: research and teaching.

Which brings me to Oxford, and to Bill Roscoe.

It is approaching 15 years since Bill took over as Head of Department of Computer Science at the University of Oxford. He certainly did not take over a weak department: there was excellence aplenty. But, I think it is fair to say, the department at that time was relatively small, and narrowly focussed. Bill took on the challenge of transforming the department in terms of its scale and breadth of activity. Transformative change is not an easy thing to accomplish, even under the best of circumstances. But the nature of Oxford as a collegiate university makes it tremendously difficult to effect transformative change quickly. Decisions at Oxford usually require broad consensus from large and diverse constituencies, and computer science as a relatively new subject has relatively little presence in the colleges and ancient decision-making bodies of the university.

Bill's achievements as Head of Department are, therefore, genuinely remarkable. Oxford's computer science department has grown at a phenomenal rate, and now counts nearly 75 academics in its roster of full-time academic staff. In 2003, the department graduated just three DPhil students; this year we will graduate nearly 50. In the academic year 2014–2015, the department generated more research grant income than in the entire period 2001–2008; we have grown from a pool of about 20 post-doctoral researchers to nearly 150 currently. On every meaningful metric that I can think of, the department has surged ahead.

As an outsider, I watched Oxford's growth with interest, and was deeply impressed. I wanted to join the party, and was fortunate enough, in 2012, to be able to join the fun. This change did not happen by accident. It was not handed to us on a plate. It was not easy. It was not simple. It did not happen overnight. It was the result of a committed, decade-long process, under which the department had determined, focussed leadership, driven to build and improve. It was a tiring, and I daresay at times dispiriting business. It would have been very easy to walk away. But the results, I believe, speak for themselves. Bill was not the father of the Department of Computer Science, but he is, I believe, the father of the department as it stands today – and the department is, I honestly believe, the most exciting place in Europe to be a computer scientist right now. Those of us in the department, and the University of Oxford itself, owe Bill a tremendous debt. The department is clearly a labour of love for Bill; and even ignoring all Bill's other work as a researcher and entrepreneur, it would be a fitting legacy for a career.

Contents