Lecture Notes in Computer Science 3895

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

Editorial Board

Oded Goldreich Arnold L. Rosenberg
Alan L. Selman (Eds.)

Theoretical Computer Science

Essays in Memory of Shimon Even

Springer

Volume Editors

Oded Goldreich
Weizmann Institute of Science
Department of Computer Science
Rehovot, Israel
E-mail: oded.goldreich@weizmann.ac.il

Arnold L. Rosenberg
University of Massachusetts Amherst
Department of Computer Science
Amherst, MA 01003, USA
E-mail: rsnbrg@cs.umass.edu

Alan L. Selman
University at Buffalo, The State University of New York
Department of Computer Science and Engineering
Buffalo, NY 14260-2000, USA
E-mail: selman@cse.buffalo.edu

The illustration appearing on the cover of this book is the work of Daniel Rozenberg (DADARA).

Library of Congress Control Number: 2006922002

CR Subject Classification (1998): F.2.2, G.1.2, G.2.2, C.2.4, E.3

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-32880-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-32880-3 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Boller Mediendesign
Printed on acid-free paper SPIN: 11685654 06/3142 5 4 3 2 1 0

Shimon Even (1935–2004)

Preface

On May 1, 2004, the world of theoretical computer science suffered a stunning loss: Shimon Even passed away. Few computer scientists have had as long, sustained, and influential a career as Shimon.

Shimon Even was born in Tel-Aviv in 1935. He received a B.Sc. in Electrical Engineering from the Technion in 1959, an M.A. in Mathematics from the University of Northern Carolina in 1961, and a Ph.D. in Applied Mathematics from Harvard University in 1963. He held positions at the Technion (1964–67 and 1974–2003), Harvard University (1967–69), the Weizmann Institute (1969–74), and the Tel-Aviv Academic College (2003-04). He visited many universities and research institutes, including Bell Laboratories, Boston University, Cornell, Duke, Lucent Technologies, MIT, Paderborn, Stanford, UC-Berkeley, USC and UT-Dallas.

Shimon Even played a major role in establishing computer science education in Israel and led the development of academic programs in two major institutions: the Weizmann Institute and the Technion. In 1969 he established at the Weizmann the first computer science education program in Israel, and led this program for five years. In 1974 he joined the newly formed computer science department at the Technion and shaped its academic development for several decades. These two academic programs turned out to have a lasting impact on the evolution of computer science in Israel.

Shimon Even was a superb teacher, and his courses deeply influenced many of the students attending them. His lectures, at numerous international workshops and schools, inspired a great number of students and researchers. His books, especially his celebrated *Graph Algorithms*, carried his educational message also to computer scientists who were not fortunate enough to meet him in person. As a mentor to aspiring researchers, Shimon was almost without peer, nurturing numerous junior researchers and advising many graduate students, who went on to have their own successful research careers.

Shimon Even was a pioneer in the areas of graph algorithms and cryptography, and his research contributions to these areas influenced the course of their development. Shimon was famous for not confining his interests to a few topics, but choosing rather to work in such diverse areas as switching and automata theory, coding theory, combinatorial algorithms, complexity theory, distributed computing, and circuit layout. In each of these areas, he produced high-quality, innovative research for more than four decades.

Shimon was the purest of pure theoreticians, following his nose toward research problems that were "the right" ones at the moment, not the faddish ones. His standards were impeccable, to the point where he would balk at employing any result whose proof he had not mastered himself. His integrity was unimpeachable: he would go to great lengths to defend any principle he believed in.

Shimon had a great passion for computer science as well as a great passion for truth. He valued simplicity, commitment to science, natural questions and carefully prepared expositions. By merely following his own way, Shimon influenced numerous researchers to adopt his passions and values. We hope that this is reflected in the current volume.

This volume contains research contributions and surveys by former students and close collaborators of Shimon. We are very pleased that Reuven Bar-Yehuda, Yefim Dinitz, Guy Even, Richard Karp, Ami Litman, Yehoshua Perl, Sergio Rajsbaum, Adi Shamir, and Yacov Yacobi agreed to send contributions. In accordance with Shimon's style and principles, the focus of these contributions is on addressing natural problems and being accessible to most researchers in theoretical computer science. The contributions are of three different types, reflecting three main scientific activities of Shimon: original research, technical surveys, and educational essays.

The Contributions

The contributions were written by former students and close collaborators of Shimon. In some cases the contributions are co-authored by researchers who were not fortunate enough to be close to Shimon or even to have met him in person. Below we comment on particular aspects of each contribution that we believe Shimon would have appreciated.

Original Research

Needless to say, everybody likes original research, and Shimon was no exception. We believe that Shimon would have been happy with the attempt to make these research contributions accessible to a wide range of researchers (rather than merely to experts in the area). In order to promote this goal, these contributions were reviewed both by experts and by non-experts.

- P. Fraigniaud, D. Ilcinkas, S. Rajsbaum and S. Tixeuil: *The Reduced Automata Technique for Graph Exploration Space Lower Bounds*. Shimon liked connections between areas, and the areas of graph algorithms and of automata theory were among his favorites.
- O. Goldreich: *Concurrent Zero-Knowledge with Timing, Revisited*. Shimon would have joked at Oded's tendency to write long papers.
- R.M. Karp: *Fair Bandwidth Allocation Without Per-Flow State*. Shimon would have like the fact that the starting point of this work is a practical problem, and that it proceeds by distilling a clear computational problem and resolving it optimally.
- R.M. Karp, T. Nierhoff and T. Tantau: *Optimal Flow Distribution Among Multiple Channels with Unknown Capacities*. This paper has the same flavor as the previous one, and Shimon would have liked it for the very same reason.

- A. Litman: *Parceling the Butterfly and the Batcher Sorting Network*. Shimon would have liked the attempt to present a new complexity measure that better reflects the actual cost of implementations.
- X. Zhou, J. Geller, Y. Perl, and M. Halper: *An Application Intersection Marketing Ontology*. Shimon would have liked the fact that simple insights of graph theory are used for a problem that is very remote from graph theory.
- R.L. Rivest, A. Shamir and Y. Tauman: *How to Leak a Secret: Theory and Applications of Ring Signatures*. Shimon would have like the natural ("daily") problem addressed in this paper as well as the elegant solution provided to it.
- O. Yacobi with Y. Yacobi: *A New Related Message Attack on RSA*. Shimon would have enjoyed seeing a father and son work together.

Technical Surveys

Shimon valued the willingness to take a step back, look at what was done (from a wider perspective), and provide a better perspective on it. We thus believe that he would have been happy to be commemorated by a volume that contains a fair number of surveys.

- R. Bar-Yehuda and D. Rawitz: *A Tale of Two Methods*. Shimon liked stories, and he also liked the techniques surveyed here. Furthermore, he would have been excited to learn that these two techniques are in some sense two sides of the same coin.
- Y. Dinitz: *Dinitz' Algorithm: The Original Version and Even's Version*. Shimon is reported to have tremendously enjoyed Dinitz's lecture that served as a skeleton to this survey.
- C. Glaßer, A.L. Selman, and L. Zhang: *Survey of Disjoint NP-pairs and Relations to Propositional Proof Systems*. This survey focuses on one of the applications of promise problems, which was certainly unexpected in 1984 when Shimon Even, together with Alan Selman and Yacov Yacobi, introduced this notion.
- O. Goldreich: *On Promise Problems*. This survey traces the numerous and diverse applications that the notion of promise problems found in the two decades that have elapsed since the invention of the notion.
- G. Malewicz and A.L. Rosenberg: *A Pebble Game for Internet-Based Computing*. Shimon liked elegant models, and would have been interested to see pebble games used to model an Internet-age problem.

Educational Essays

Shimon liked opinionated discussions and valued independent opinions that challenge traditional conventions. So we are sure he would have enjoyed reading these essays, and we regret that we cannot have his reaction to them.

- G. Even: *On Teaching Fast Adder Designs: Revisiting Ladner & Fischer*. Shimon would have been very proud of this insightful and opinionated exposition of hardware implementations of the most basic computational task.
- O. Goldreich: *On Teaching the Basics of Complexity Theory*. Shimon would have appreciated the attempt to present the basics of complexity theory in a way that appeals to the naive student.
- A.L. Rosenberg: *State*. Shimon would have supported the campaign, launched in this essay, in favor of the Myhill-Nerode Theorem.

December 2005

Oded Goldreich (Weizmann Institute of Science)
Arnold L. Rosenberg (University of Massachusetts Amherst)
Alan L. Selman (University at Buffalo)

Table of Contents

The Reduced Automata Technique for Graph Exploration Space Lower Bounds 1
Pierre Fraigniaud, David Ilcinkas, Sergio Rajsbaum, Sébastien Tixeuil

Concurrent Zero-Knowledge with Timing, Revisited 27
Oded Goldreich

Fair Bandwidth Allocation Without Per-Flow State 88
Richard M. Karp

Optimal Flow Distribution Among Multiple Channels with Unknown Capacities 111
Richard Karp, Till Nierhoff, Till Tantau

Parceling the Butterfly and the Batcher Sorting Network 129
Ami Litman

An Application Intersection Marketing Ontology 143
Xuan Zhou, James Geller, Yehoshua Perl, Michael Halper

How to Leak a Secret: Theory and Applications of Ring Signatures 164
Ronald L. Rivest, Adi Shamir, Yael Tauman

A New Related Message Attack on RSA 187
Oded Yacobi, Yacov Yacobi

A Tale of Two Methods 196
Reuven Bar-Yehuda, Dror Rawitz

Dinitz' Algorithm: The Original Version and Even's Version 218
Yefim Dinitz

Survey of Disjoint NP-pairs and Relations to Propositional Proof Systems 241
Christian Glaßer, Alan L. Selman, Liyu Zhang

On Promise Problems: A Survey 254
Oded Goldreich

A Pebble Game for Internet-Based Computing 291
Grzegorz Malewicz, Arnold L. Rosenberg

On Teaching Fast Adder Designs: Revisiting Ladner & Fischer 313
Guy Even

On Teaching the Basics of Complexity Theory 348
Oded Goldreich

State 375
Arnold L. Rosenberg

Author Index 399