Lecture Notes in Computer Science 4086

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

Guang Gong Tor Helleseth
Hong-Yeop Song Kyeongcheol Yang (Eds.)

Sequences and Their Applications – SETA 2006

4th International Conference
Beijing, China, September 24-28, 2006
Proceedings

Springer

Volume Editors

Guang Gong
University of Waterloo
Department of Electrical and Computer Engineering
200 University Avenue West, Waterloo, ON, N2L 3G1, Canada
E-mail: ggong@calliope.uwaterloo.ca

Tor Helleseth
University of Bergen
Department of Informatics
Thormohlensgate 55, 5020 Bergen, Norway
E-mail: tor.helleseth@ii.uib.no

Hong-Yeop Song
Center for Information Technology of Yonsei University
School of Electrical and Electronics Engineering
Seoul,120-749, Korea
E-mail: hy.song@coding.yonsei.ac.kr

Kyeongcheol Yang
Pohang University of Science and Technology (POSTECH)
Dept. of Electronic and Electrical Engineering
Pohang, Gyungbuk 790-784, Korea
E-mail: kcyang@postech.ac.kr

Library of Congress Control Number: 2006932045

CR Subject Classification (1998): E.4, F.2, I.1, E.3, F.1, G.1

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

ISSN 0302-9743
ISBN-10 3-540-44523-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-44523-4 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11863854 06/3142 5 4 3 2 1 0

Preface

This volume contains the refereed proceedings of the Fourth International Conference on Sequences and Their Applications (SETA 2006), held in Beijing, China during September 24–28, 2006. The previous three conferences SETA '98, SETA 2001, and SETA 2004 were held in Singapore, Bergen, and Seoul, respectively. The SETA conferences are motivated by the numerous applications of sequences in modern communication systems. These applications include pseudorandom sequences in spread spectrum, code-division-multiple-access, stream ciphers in cryptography, and several connections to coding theory and boolean functions.

The Technical Program Committee of SETA 2006 refereed 70 submitted papers. This represented more submissions than to any of the previous SETA conferences. The committee therefore had the challenging task of selecting 32 papers to be presented at the conference in addition to 4 invited papers.

The Co-chairs of the Technical Program Committee for SETA 2006, were Guang Gong (University of Waterloo) and Tor Helleseth (University of Bergen), with Hong-Yeop Song (Yonsei University, Korea) and Kyeongcheol Yang (Pohang University of Science and Technology, Korea) as the co-editors for these proceedings.

The editors wish to thank the other members of the Technical Program Committee: Anne Canteaut (INRIA, France), Claude Carlet (INRIA and University of Paris 8, France), Habong Chung, (Hongik University, Korea), Zongduo Dai (University of Science and Technology of China, Beijing, China), Cunsheng Ding (Hong Kong University of Science and Technology, Hong Kong), Pingzhi Fan (Southwest Jiaotong University, China), Dengguo Feng (Chinese Academy of Sciences, China), Solomon W. Golomb (University of Southern California, USA), Kyoki Imamura (Kyushu Institute of Technology, Japan), Jonathan Jedwab (Simon Fraser University, Canada), Thomas Johansson (University of Lund, Sweden), Andrew Klapper (University of Kentucky, USA), P. Vijay Kumar (University of Southern California, USA), Wai Ho Mow (Hong Kong University of Science and Technology, Hong Kong), Harald Niederreiter (National University of Singapore, Singapore), Jong-Seon No (Seoul National University, Korea), Matthew G. Parker (University of Bergen, Norway), Kenneth G. Paterson (Royal Holloway, University of London, UK), Alexander Pott (Otto-von-Guericke-University Magdeburg, Germany), Hans Schotten (Qualcomm Germany, Nuremberg, Germany), Parampalli Udaya (University of Melbourne, Australia), and Amr Youssef (Concordia University, Canada) for providing clear, insightful, and prompt reviews of the submitted papers.

The editors are also grateful to Serdar Boztas, Jin-Ho Chung, Deepak Kumar Dalai, Frédéric Didier, Gary Greenfield, Yun-Kyoung Han, Tom Høholdt, Alexander Kholosha, Margreta Kuijper, Gohar Kyureghyan, Cedric Lauradoux, Subhamoy Maitra, Joe Rushanan, Frank Ruskey, Igor Semaev, Jean-Pierre

Tillich, and Nam Yul Yu for their help and assistance in the reviewing of papers for SETA 2006. A special thanks goes to Sondre Rønjom for handling all the submissions and the web-review software during the review process.

In addition to the contributed papers, there are four invited papers. These papers provide a historical overview as well as new developments in important areas of the design and analysis of sequences. The invited contribution by Solomon Golomb presents a retro-perspective of some selected results on sequences. The invited paper by Harald Niederreiter includes an updated overview and some recent important results on the complexity of multisequences. Vijay Kumar provides an overview and new results on optical orthogonal codes. This topic is motivated by applying code division multiple access (CDMA) techniques in optical networks. Zongduo Dai presents an overview of multi-continued fraction algorithms and their applications to sequences.

We wish to thank Pingzhi Fan and Dengguo Feng for their support as General Co-chairs of SETA 2006, and Chuan-Kun Wu for local arrangements and updating the web site of SETA '06. We also thank Yi Qin for her support as secretary of SETA 2006, and Shi Zhang for her support as treasurer of SETA 2006. Last but not least, we thank all the authors of the papers for their help and collaboration in preparing this volume. Finally, we would like to thank the National Science Foundation of China (NSFC) and the Chinese Academy of Sciences (CAS) for their financial support.

September 2006

Guang Gong
Tor Helleseth
Hong-Yeop Song
Kyeongcheol Yang

Organization

SETA 2006

September 24-28, 2006, Beijing, China

General Co-chairs

Pingzhi Fan, Southwest Jiaotong University, China
Dengguo Feng, Chinese Academy of Sciences, China

Program Co-chairs

Guang Gong, University of Waterloo, Canada
Tor Helleseth, University of Bergen, Norway

Local Arrangements

Chuan-Kun Wu, Chinese Academy of Sciences, China

Secretary and Registration

Yi Qin, Chinese Academy of Sciences, China

Treasurer

Shi Zhang, Chinese Academy of Sciences, China

Proceedings Co-editors

Guang Gong, University of Waterloo, Canada
Tor Helleseth, University of Bergen, Norway
Hong-Yeop Song, Yonsei University, Korea
Kyeongcheol Yang, Pohang Univ. of Science and Technology, Korea

Technical Program Committee for SETA 2006

Program Co-chairs

Guang Gong ..... University of Waterloo, Canada
Tor Helleseth ..... University of Bergen, Norway

Program Committee

Anne Canteaut ..... INRIA, France
Claude Carlet ..... INRIA and University of Paris 8, France
Habong Chung ..... Hongik University, Korea
Zongduo Dai ..... University of Science and Technology of China, China
Cunsheng Ding ..... Hong Kong University of Science and Technology, China
Pingzhi Fan ..... Southwest Jiaotong University, China
Dengguo Feng ..... Chinese Academy of Sciences, China
Solomon W. Golomb ..... University of Southern California, USA
Kyoki Imamura ..... Kyushu Institute of Technology, Japan
Jonathan Jedwab ..... Simon Fraser University, Canada
Thomas Johansson ..... University of Lund, Sweden
Andrew Klapper ..... University of Kentucky, USA
P. Vijay Kumar ..... University of Southern California, USA
Wai Ho Mow ..... Hong Kong University of Science and Technology, China
Harald Niederreiter ..... National University of Singapore, Singapore
Jong-Seon No ..... Seoul National University, Korea
Matthew G. Parker ..... University of Bergen, Norway
Kenneth G. Paterson ..... Royal Holloway, University of London, UK
Alexander Pott ..... Otto-von-Guericke University Magdeburg, Germany
Hans Schotten ..... Qualcomm Germany, Germany
Hong-Yeop Song ..... Yonsei University, Korea
Parampalli Udaya ..... University of Melbourne, Australia
Kyeongcheol Yang ..... Pohang University of Science and Technology, Korea
Amr Youssef ..... Concordia University, Canada

Table of Contents

Invited Papers

Linear Complexity of Sequences

Correlation of Sequences

Stream Ciphers and Transforms

Topics in Complexities of Sequences

Linear/Nonlinear Feedback Shift Register Sequences

Multi-sequence Synthesis

Filtering Sequences and Pseudorandom Sequence Generators

Sequences and Combinatorics

FCSR Sequences

Aperiodic Correlation and Applications

Boolean Functions