

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, 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, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Solomon W. Golomb Guang Gong
Tor Helleseeth Hong-Yeop Song (Eds.)

Sequences, Subsequences, and Consequences

International Workshop, SSC 2007
Los Angeles, CA, USA, May 31 - June 2, 2007
Revised Invited Papers

Volume Editors

Solomon W. Golomb

University of Southern California, Department of EE-Systems

Los Angeles, CA 90089-2565, USA

E-mail: sgolomb@usc.edu

Guang Gong

University of Waterloo, Department of Electrical and Computer Engineering

200 University Avenue West, Waterloo, ON N2L 3G1, Canada

E-mail: g.gong@calliope.uwaterloo.ca

Tor Helleseth

University of Bergen, Selmer Center, Department of Informatics

Thormohlensgate 55, 5020 Bergen, Norway

E-mail: tor.helleseth@ii.uib.no

Hong-Yeop Song

Yonsei University, School of Electrical and Electronic Engineering

134 Sinchon-dong Seodaemun-gu, Seoul, 120-749, Korea

E-mail: hysong@yonsei.ac.kr

Library of Congress Control Number: 2007941501

CR Subject Classification (1998): E.3-4, G.2, F.2.2, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-540-77403-3 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-77403-7 Springer 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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 12208166 06/3180 5 4 3 2 1 0

Dedicated to
Professor Solomon W. Golomb
on his 75th Birthday

Preface

These are the proceedings of the Workshop on Sequences, Subsequences, and Consequences that was held at the University of Southern California (USC), May 31 - June 2, 2007. There were three one-hour Keynote lectures, 16 invited talks of up to 45 minutes each, and 1 “contributed” paper.

The theory of sequences from discrete symbol alphabets has found practical applications in many areas of coded communications and in cryptography, including: signal patterns for use in radar and sonar; spectral spreading sequences for CDMA wireless telephony; key streams for direct sequence stream-cipher cryptography; and a variety of forward-error-correcting codes.

The workshop was designed to bring leading researchers on “sequences” from around the world to present their latest results, interchange information with one another, and especially to inform the larger audience of interested participants, including faculty, researchers, scholars, and students from numerous institutions, as well as the readers of these proceedings, about recent developments in this important field.

There were invited speakers from Canada, China, Germany, India, Israel, Norway, Puerto Rico, and South Korea, in addition to those from the USA. Support for the workshop was generously provided by the Office of the Dean of the Viterbi School of Engineering, by the Center for Communications Research (CCR-La Jolla), and by the United States National Science Foundation (NSF). This support is hereby gratefully acknowledged.

As the principal organizers of the workshop and its technical program, we wish to thank the speakers, all the participants, and the above-mentioned organizations that provided funding. Our special thanks go to Milly Montenegro, Gerrielyn Ramos, and Mayumi Thrasher at USC for all the arrangements before, during, and after the workshop, and for their considerable help, along with Xinxin Fan and Honggang Hu at the University of Waterloo (Canada) and Young-Joon Kim at Yonsei University (South Korea), in preparing, typing, and formatting many of the manuscripts.

September 2007

Solomon W. Golomb
Guang Gong
Tor Helleseth
Hong-Yeop Song

Organization

Technical Program Committee for SSC 2007

Principal Organizers

Solomon Golomb	University of Southern California, USA
Guang Gong	University of Waterloo, Canada
Tor Helleseth	University of Bergen, Norway
Hong-Yeop Song	Yonsei University, Korea

Program Committee

Tuvi Etzion	Technion IIT, Israel
Solomon W. Golomb	University of Southern California, USA
Guang Gong	University of Waterloo, Canada
Alfred W. Hales	CCR-La Jolla, USA
Tor Helleseth	University of Bergen, Norway
Alexander Kholosha	University of Bergen, Norway
Andrew Klapper	University of Kentucky, USA
P. Vijay Kumar	University of Southern California, USA, and IISc Bangalore
Robert McEliece	California Institute of Technology, USA
Lothrop Mittenenthal	Teledyne, USA
Oscar Moreno	University of Puerto Rico, Puerto Rico
Alexander Pott	Otto von Guericke University Magdeburg, Germany
Hong-Yeop Song	Yonsei University, Korea
Xiaohu Tang	Southwest Jiao Tong University, China
Herbert Taylor	South Pasadena, USA
Andrew J. Viterbi	Viterbi Group, LLC, USA
Steven Wang	University of Carleton, Canada
Lloyd R. Welch	University of Southern California, USA
Nam Yul Yu	University of Waterloo, Canada

Sponsoring Institutions

University of Southern California, CCR-La Jolla, NSF

Table of Contents

Periodic Binary Sequences: Solved and Unsolved Problems (Invited Keynote Lecture).....	1
<i>Solomon W. Golomb</i>	
On Boolean Functions Which Are Bent and Negabent	9
<i>Matthew G. Parker and Alexander Pott</i>	
Strongly Primitive Elements.....	24
<i>Daniel Goldstein and Alfred W. Hales</i>	
The Perfect Binary Sequence of Period 4 for Low Periodic and Aperiodic Autocorrelations.....	37
<i>Nam Yul Yu and Guang Gong</i>	
On the Dual of Monomial Quadratic p -ary Bent Functions	50
<i>Tor Helleseth and Alexander Kholosha</i>	
A New Family of Gold-Like Sequences	62
<i>Xiaohu Tang, Tor Helleseth, Lei Hu, and Wenfeng Jiang</i>	
Sequencings and Directed Graphs with Applications to Cryptography...	70
<i>Lothrop Mittenenthal</i>	
Double Periodic Arrays with Optimal Correlation for Applications in Watermarking	82
<i>Oscar Moreno and José Ortiz-Ubarri</i>	
Sequences for Phase-Encoded Optical CDMA (Invited Keynote Lecture).....	95
<i>Reza Omrani, Pankaj Bhambhani, and P. Vijay Kumar</i>	
Packing Centrosymmetric Patterns of n Nonattacking Queens on an $n \times n$ Board.....	106
<i>Herbert Taylor</i>	
Cyclotomic Mapping Permutation Polynomials over Finite Fields	119
<i>Qiang Wang</i>	
Single-Track Gray Codes and Sequences	129
<i>Tuvi Etzion</i>	
The Asymptotic Behavior of π -Adic Complexity with $\pi^2 = -2$	134
<i>Andrew Klapper</i>	
Shannon Capacity Limits of Wireless Networks	147
<i>Andrew Viterbi</i>	

Some Mysterious Sequences Associated with LDPC Codes	153
<i>Robert J. McEliece and Sarah L. Sweatlock</i>	
Remarks on a Sequence of Minimal Niven Numbers	162
<i>H. Fredricksen, E.J. Ionascu, F. Luca, and P. Stănică</i>	
The Linear Vector Space Spanned by the Nonlinear Filter Generator (Invited Keynote Lecture)	169
<i>Sondre Rønjom and Tor Helleseeth</i>	
Existence of Modular Sonar Sequences of Twin-Prime Product Length	184
<i>Sung-Jun Yoon and Hong-Yeop Song</i>	
Randomness and Representation of Span n Sequences	192
<i>Guang Gong</i>	
On Attacks on Filtering Generators Using Linear Subspace Structures	204
<i>Sondre Rønjom, Guang Gong, and Tor Helleseeth</i>	
Author Index	219