



**Series Editors**

Douglas S. Bridges, *Canterbury University, NZ*

Cristian S. Calude, *University of Auckland, NZ*

**Advisory Editorial Board**

J. Casti, *Sante Fe Institute, USA*

G. J. Chaitin, *IBM Research Center, USA*

E. W. Dijkstra, *University of Texas at Austin, USA*

J. Goguen, *University of California at San Diego, USA*

R. L. Graham, *University of California at San Diego, USA*

J. Hartmanis, *Cornell University, USA*

H. Jürgensen, *University of Western Ontario, Canada*

A. Nerode, *Cornell University, USA*

G. Rozenberg, *Leiden University, The Netherlands*

A. Salomaa, *Turku University, Finland*

C. Ding, T. Helleseeth and H. Niederreiter (Eds)

---

# **Sequences and their Applications**

**Proceedings of SETA '98**



**Springer**

C. Ding  
Department of Computer Science, School of Computing, National University of Singapore,  
Lower Kent Ridge Road, Singapore 119260

T. Helleseeth  
Department of Informatics, University of Bergen, N-5020 Bergen, Norway

H. Niederreiter  
Institute of Information Processing, Austrian Academy of Sciences, Sonnenfelsgasse 19,  
A01010 Vienna, Austria

ISBN 978-1-85233-196-2

British Library Cataloguing in Publication Data

Sequences and their applications : proceedings of SETA '98.

- (Discrete mathematics and theoretical computer science)

1. Sequences (Mathematics) - Congresses 2. Sequences

(Mathematics) - Data processing - Congresses

I. Ding, C. (Cunsheng) II. Helleseeth, Tor III. Niederreiter,

Harald, 1944-

515.2'4

ISBN 978-1-85233-196-2 ISBN 978-1-4471-0551-0 (eBook)

DOI 10.1007/978-1-4471-0551-0

Library of Congress Cataloging-in-Publication Data

A catalog record for this book is available from the Library of Congress

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers.

© Springer-Verlag London 1999

Originally published by Springer-Verlag London Limited in 1999

The use of registered names, trademarks etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant laws and regulations and therefore free for general use.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

Typesetting: Camera ready by contributors

34/3830-543210 Printed on acid-free paper SPIN 10739473

# Preface

This volume contains the refereed proceedings of the International Conference on Sequences and Their Applications which was held at the River View Hotel in Singapore during December 14-17, 1998. The program of this conference was arranged by a committee consisting of Claude Carlet (University of Caen), Agnes Chan (Northeastern University), Cunsheng Ding (National University of Singapore, co-chair), Dieter Gollmann (Microsoft Research), Tor Helleseth (University of Bergen, co-chair), Kyoki Imamura (Kyushu Institute of Technology), Andrew Klapper (University of Kentucky), Vijay Kumar (University of Southern California), Siu Lun Ma (National University of Singapore), Harald Niederreiter (Austrian Academy of Sciences, co-chair), Dilip Sarwate (University of Illinois at Urbana-Champaign), Hans Schotten (Aachen University of Technology), Jeffrey Shallit (University of Waterloo), Neil Sloane (AT&T Shannon Lab), and Aimo Tietäväinen (University of Turku). The local organization was in the hands of Cunsheng Ding, Kwok Yan Lam (chair), Sjauntele Lau, and Sew Kiok Toh, all of the National University of Singapore.

The idea for the conference grew out of the recognition that sequences in discrete structures like the ring of integers, residue class rings of the integers, and finite fields have found many important applications in modern information and communication technologies. Among these applications we mention cryptographic schemes, ranging systems, spread spectrum communication systems, multi-terminal system identification, code-division multiple-access communication systems, global positioning systems, software testing, circuit testing, and computer simulation. There are also connections between sequences in discrete structures and error-correcting codes. In view of these exciting applications of sequences in discrete structures, it seemed worthwhile and timely to have a conference focusing on the properties of such sequences. The excellent response we received to this idea encouraged us to organize the conference, and we hope that these proceedings will be a testimony to the success of the conference.

We are grateful to the members of the Program Committee for screening abstracts and refereeing full papers. We also thank Jean-Paul Allouche, Eric Bach, Simon Blackburn, Anna Frid, Iiro Honkala, Tohru Kohda, Jyrki Lahtonen, Tero Laiho, Halvard Martinsen, Alfred Menezes, David Pointcheval, Ari Renvall, Jean-Pierre Tillich, Jinzhong Xu, and Muxiang Zhang for serving as additional referees. All these colleagues have contributed enormously to the quality of the conference presentations and to guaranteeing high standards of these proceedings.

We appreciate the financial support for the conference received from the Centre for Systems Security of the National University of Singapore and the Lee Foundation. The conference would not have been successful without the essential organizational tasks performed in a skillful manner by Sjauntele Lau and Sew Kiok Toh. We express our gratitude to Springer-Verlag for publishing this

volume, and especially to Ian Shelley and Caroline Ching for the encouragement and support provided so generously. We thank Professor Cristian Calude for his support of publishing this volume in the Springer DMTCS book series.

May 1999

Cunsheng Ding   Tor Helleseeth   Harald Niederreiter

# CONTENTS

## Invited Contributions

The Ubiquitous Prouhet-Thue-Morse Sequence <i>J.-P. Allouche and J. Shallit</i> .....	1
On Ideal Autocorrelation Sequences Arising from Hyperovals <i>A. Chang, S. W. Golomb, G. Gong and P. V. Kumar</i> .....	17
Cyclic Hadamard Difference Sets – Constructions and Applications <i>S. W. Golomb</i> .....	39
Correlation of $m$ -Sequences and Related Topics <i>T. Helleseeth</i> .....	49
Some Computable Complexity Measures for Binary Sequences <i>H. Niederreiter</i> .....	67
Meeting the Welch Bound with Equality <i>D. V. Sarwate</i> .....	79
My Favorite Integer Sequences <i>N. J. A. Sloane</i> .....	103

## Regular Contributions

Complementary Interpolants and a Welch-Berlekamp-Style Algorithm <i>M. A. Armand</i> .....	131
Multiscale Coarse-Graining Invariant Sequences <i>A. Barbé</i> .....	146
Regular Cosets and Upper Bounds on the Linear Complexity of Certain Sequences <i>P. Caballero-Gil</i> .....	161
Hadamard Matrices, Self-Dual Codes over the Integers Modulo 4 and their Gray Images <i>C. Charney</i> .....	171
On Constructing Balanced Correlation Immune Functions <i>T. W. Cusick</i> .....	184

On Bispecial Words and Subword Complexity of D0L Sequences <i>A. Frid and S. V. Avgustinovich</i> .....	191
On the Distribution of the RSA Generator <i>J. B. Friedlander, D. Lieman and I. E. Shparlinski</i> .....	205
Edit Probability Correlation Attack on the Alternating Step Generator <i>J. Dj. Golić and R. Menicocci</i> .....	213
Automaticity of Solutions of Mahler Equations <i>F. von Haeseler and W. Jürgensen</i> .....	228
Correlation Distribution of the Quaternary Kasami Sequences <i>T. Helleseeth, P. V. Kumar, H. M. Martinsen and O. N. Vassbakk</i> .....	240
Multicovering Radii of Reed-Muller Codes and the Existence of Secure Stream Ciphers <i>I. Honkala and A. Klapper</i> .....	254
Inclusion Relations of Boolean Functions Satisfying PC( $l$ ) of Order $k$ <i>T. Iwata and K. Kurosawa</i> .....	263
Notes on $q$ -ary Interleaved Sequences <i>S. Jiang, Z.-D. Dai and G. Gong</i> .....	273
A New Algorithm for the $k$ -Error Linear Complexity of Sequences over $GF(p^m)$ with Period $p^n$ <i>T. Kaida, S. Uehara and K. Imamura</i> .....	284
Sequences of I.I.D. Binary Random Variables Using Chaotic Dynamics <i>T. Kohda</i> .....	297
Explicit Sequence Expansions <i>D. Kohel, S. Ling and C. Xing</i> .....	308
Counting Functions and Expected Values in the Stability Theory of Stream Ciphers <i>H. Niederreiter and H. Paschinger</i> .....	318
On-Line Constraint-Based Pattern Matching on Sequences <i>V. A. Oleshchuk</i> .....	330
On the Randomness of a $[d, k]$ Self-Decimation Stream Key Generator <i>F. Sato and K. Kurosawa</i> .....	343



Sequence Families with Optimum Aperiodic Mean-Square Correlation  
Parameters

*H. D. Schotten* ..... 354

Period and Linear Complexity of Cascaded Clock-Controlled Generators

*C. H. Tan* ..... 371

Feedback with Carry Shift Registers over  $\mathbb{Z}(N)$

*J. Xu and A. Klapper* ..... 379

**Author Index** ..... 393