Discrete Mathematics and Theoretical Computer Science

Springer-Verlag London Ltd.

C. Ding, T. Helleseth 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. Helleseth
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.Helleseth, 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

Originally published by Springer-Verlag London Limited in 1999

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 Laihonen, 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 Helleseth Harald Niederreiter

CONTENTS

Invited Contributions

Regular Contributions