Introduction

This book contains survey articles based on some invited lectures of the workshop *Pseudo-Randomness and Finite Fields* (October 15–19, 2018) of the *RICAM Special Semester on Multivariate Algorithms and their Foundations in Number Theory*. This workshop brought together some of the world-wide most prominent researchers in the area of combinatorics and finite fields and their applications.

Combinatorics and finite fields are of great importance in modern applications such as analysis of algorithms, information and communication theory, signal processing and coding theory. This book contains 15 survey articles on topics such as difference sets, polynomials and pseudorandomness. For example, difference sets are intensively studied combinatorial objects with applications such as wireless communication and radar, imaging and quantum information theory. Polynomials appear in check-digit systems and error-correcting codes. Pseudorandom structures guarantee features needed for Monte-Carlo methods or cryptography. Additive combinatorics over finite fields has gained increasing interest in particular because of its applications to computer science and coding theory.

The book presents some new developments and stimulates the interaction between different application areas as well as the continuous quest for new applications.

Chapters 1, 2, 3, 4, 6, 9 and 12 deal with difference sets and related structures. Chapters 3, 4, 5, 7, 8, 12, 13 and 15 survey results on bent functions and permutation polynomials. Chapters 8, 10 and 14 study different concepts of pseudorandomness. Chapters 10, 11 and 13 belong to additive combinatorics and coding theory. All these chapters were reviewed and we wish to thank the anonymous referees for their precious help.

We also like to thank Annette Weihs and Wolfgang Forsthuber for administrative support and all the speakers of the workshops listed below who contributed with excellent talks and made the workshop a great success: Nurdagül Anbar Meidl (Sabancı University Istanbul), Marco Buratti (University of Perugia), Jim Davis (University of Richmond), Daniel Katz (California State University), Gohar Kyureghyan (University of Rostock), Philipp Lampe (University of Kent), Christian Mauduit (Université d'Aix-Marseille), Wilfried Meidl (RICAM Linz), Laszlo Mérai (RICAM Linz), Giacomo Micheli (University of Oxford), Daniel Panario (Carleton University Ottawa), Giorgis Petridis (University of Georgia), Claudio Qureshi (University of Campinas), Joël Rivat (Université d'Aix-Marseille), Oliver Roche-Newton (RICAM Linz), Joachim Rosenthal (Universität Zürich), Misha Rudnev (University of Bristol), András Sárközy (Eötvös Loránd University Budapest), Bernhard Schmidt (Nanyang Technological University Singapore), John Sheekey (University College Dublin), Ilya Shkredov (Steklov Mathematical Institute Moscow), Akhilesh Siddhanti (BITS Pilani KK Birla Goa Campus), Ming Su (Nankai University), Cathy Swaenepoel (Université d'Aix-Marseille), David Thomson (Carleton University Ottawa), Alev Topuzoğlu (Sabancı University Istanbul),

https://doi.org/10.1515/9783110642094-201

Koen van Greevenbroek (University Bonn), Qiang Wang (Carleton University Ottawa), Alfred Wassermann (University of Bayreuth), Qing Xiang (University of Delaware), Oğuz Yayla (Hacettepe University Ankara), Yue Zhou (National University of Defense Technology Changsha), Jens Zumbrägel (Universität Passau).

More details on this special semester can be found on the webpage http://www.ricam.oeaw.ac.at/specsem/specsem2018/.

We also thank the Radon Institute for Computational and Applied Mathematics (RICAM) of the Austrian Academy of Sciences for financial support.

Linz/Paderborn, December 2018

Kai-Uwe Schmidt and Arne Winterhof