Review of the book

"Signal Design for Good Correlation For Wireless Communication, Cryptography, and Radar"

by SOLOMON W. GOLOMB and GUANG GONG

Cambridge University Press 2005

ISBN: 0-521-82104-5, 978-0-521-82104-9

Meltem Sönmez Turan
National Institute of Standards and Technology

September 2014

1 Summary of the review

This is the review of the first edition of the book *Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar*. The book is written by two well-known researchers with significant contributions to the theory and applications of binary sequences. In 2013, Golomb had received the National Medal of Science for his advances in mathematics and communication.
This book is very technical and offers a comprehensive coverage of signal design for various applications. It is suitable for engineers, computer scientists and graduate students working in the area of signal design for communication, radar and cryptography.

2 Summary of the book

The book is organized into 12 chapters.

- **Chapter 1: General Properties of Correlation.** The first chapter of the book introduces the correlation measure, with different definitions such as continuous correlation, binary correlation and complex correlation depending on the domain of the functions. The chapter also defines autocorrelation and crosscorrelation. This chapter provides definitions, without going too much into detail. No examples or exercises are provided for the chapter.

- **Chapter 2: Applications of Correlation to the Communication of Information.** The chapter starts with discussing maximum likelihood detectors and coherent versus incoherent detection. It also provides definitions of Hadamard and cyclic Hadamard matrices.

- **Chapter 3: Finite Fields.** The chapter includes a brief overview of finite fields, starting with the definitions of groups and rings. Finite fields have wide range of applications in information theory, combinatorics, coding theory, and modern cryptography. A good understanding of finite fields is essential, especially for cryptographic algorithms that utilize finite fields, such as Diffie-Hellman key exchange, elliptic curve public-key cryptography, and the Digital Signature standard. The chapter presents description and properties of some of the fields that are widely used in cryptography. The chapter also provides examples, exercises and an example Maple program, along with a list of primitive polynomials for reference.

- **Chapter 4: Feedback shift registers.** Feedback shift registers are commonly used in synchronous stream ciphers and random number generators in cryptography. The focus of the chapter is on feedback shift registers with linear feedback polynomials; such registers are called Linear Feedback Shift Registers (LFSRs). The chapter gives different definitions and representations (matrix

and trace) of LFSRs and discusses the periodicity properties of the LFSR sequences, by providing the relations between periodicity and the minimal polynomials of the registers. The chapter provides decomposition of LFSR sequences, when the feedback is a product of distinct irreducible polynomials over F_q. Nonlinear feedback shift registers which are more popular in recent stream cipher designs are not discussed. Part of the content is also available in Golombs *Shift Register Sequences* book, first published in 1967.

- **Chapter 5: Randomness Measurements and m-Sequences.** This chapter presents Golomb's three randomness postulates for binary sequences; regarding frequency of ones and zeroes, number of runs, and autocorrelation. These postulates are also extended to non-binary sequences. The chapter provides a proof that shows m-sequences (outputs of primitive LFSRs) satisfy these randomness postulates. Part of the content of this chapter is also available in Golomb's *Shift Register Sequences* book. The chapter ends by Golomb's conjecture from 1980, claiming that binary sequences that satisfy both ideal n-tuple distribution and two-level autocorrelation are m-sequences.
- **Chapter 6: Transforms of sequences and functions.** The chapter deals with Fourier, Hadamard and convolution transforms that are important in signal processing. The chapter provides fundamental tools for designing sequences with special properties, and two-level autocorrelation.
- **Chapter 7: Cyclic Difference Sets and Binary Sequences with Two-level Autocorrelation.** The chapter introduces cyclic difference sets which are important combinatorial tools and provides the relationship between cyclic difference sets and binary sequences with 2-level autocorrelation.
- **Chapter 8-9: Cyclic Hadamard Sequences, Part I and II.** Cyclic Hadamard sequences have ideal autocorrelation properties. Chapter 8 and 9 are devoted to the construction of these sequences. Early construction methods (before 1997) include a method using m-sequences, a method based on a number theoretic approach, and a construction associated with intermediate subfields. Chapter 8 investigates general constructions of two-level autocorrelation sequences over F_q with subfield decompositions. The chapter also discusses the randomness, linear span, shift-distinct property and implementation of the output sequences. Chapter 9 is devoted to the progress in new constructions (including constructions with multiple trace terms, hyper-oval constructions and Kasami power construction), since 1997.
- **Chapter 10: Signal Sets with Low Crosscorrelation.** The chapter considers sequences with low crosscorrelation, which have important applications in CDMA communications. The chapter first introduces basic concepts and properties for crosscorrelation of sequences, signal sets, and one-to-one correspondences among sequences, polynomial functions and Boolean functions. Next, the chapter presents three classical constructions, namely the Gold-pair construction, the Kasami set construction and the bent function signal set construction.
- **Chapter 11: Correlation of Boolean Functions.** Construction of cryptographically strong Boolean functions are related to constructing sequences with good correlation, due to the existence of one-to-one correspondences between sequences, polynomial functions and Boolean functions. Chapter 11 deals with some of the cryptographic properties of Boolean functions such as correlation immunity, nonlinearity, and resiliency.
- **Chapter 12: Applications of Radar, Sonar, Synchronization and CDMA.** The last chapter of the book focuses on applications. The chapter talks about different types of signals and correlations and introduces Barker and Generalized Barker sequences, optimal rulers. The chapter also includes some related open questions.

3 What is the book like (style)?

This is a technical book, with over four hundred pages. The content is given in 12 chapters. The chapters provide examples, exercises, open questions, and historical discussions on the results. The book can benefit from structural improvements, for example introduction and organization are missing in some of the chapters.

4 Would you recommend this book?

The book will be a useful reference for expert readers, engineers and computer scientists working in the area of signal design for communication, radar and cryptography. It is also suitable to be used as a textbook for graduate course in the area. Researchers working on symmetric key cryptography, especially designing and analyzing synchronous stream ciphers and random number generators based on feedback shift registers will be interested in Chapters 4, 5 and 11.

5 Errata

The following typos can be added to the online errata sheet.

- on Page 423, "A. Bekin" should be "A. Bekir".
- on Page 219, "Section 1" should be "Section 8.1".

The reviewer is a researcher at National Institute of Standards and Technology, working on symmetric key cryptography.