Signal Design for Good Correlation

For Wireless Communication, Cryptography, and Radar

This book provides a comprehensive, up-to-date description of the methodologies and the application areas, throughout the range of digital communication, in which individual signals and sets of signals with favorable correlation properties play a central role. The necessary mathematical background is presented to explain how these signals are generated and to show how they satisfy the appropriate correlation constraints. All the known methods to obtain balanced binary sequences with two-valued autocorrelation, many of them only recently discovered, are presented in depth.

Important applications include Code Division Multiple Access (CDMA) signals, such as those already in widespread use for cell-phone communication and planned for universal adoption in the various approaches to third-generation (3G) cell-phone use; systems for coded radar and sonar signals; communication signals to minimize mutual interference in multiuser environments; and pseudorandom sequence generation for secure authentication and for stream cipher cryptology.

SOLOMON W. GOLOMB is professor of mathematics and of electrical engineering at the University of Southern California.

GUANG GONG is professor of electrical and computer engineering at the University of Waterloo, Ontario.

Signal Design for Good Correlation

For Wireless Communication, Cryptography, and Radar

SOLOMON W. GOLOMB
University of Southern California

GUANG GONG
University of Waterloo, Ontario

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
40 West 20th Street, New York, NY 10011-4211, USA

www.cambridge.org
Information on this title: www.cambridge.org/9780521821049

First published 2005

Printed in the United States of America

A catalog record for this publication is available from the British Library.

Library of Congress Cataloging in Publication Data

Golomb, Solomon W. (Solomon Wolf)
Signal design for good correlation for wireless communication, cryptography,
and radar / Soloman W. Golomb, Guang Gong.
p. cm.
Includes bibliographical references and index.
ISBN 0-521-82104-5 (hardcover)
1. Signal theory (Telecommunication) 2. Signal processing – Digital techniques.
I. Gong, Guang, 1956– II. Title.
TK5102.92.G65 2005
621.382′23 – dc22 2005002719

ISBN-13 978-0-521-82104-9 hardback
ISBN-10 0-521-82104-5 hardback

Dedicated to Andrew and Erna Viterbi

Contents

Preface

This book is the product of a fruitful collaboration between one of the earliest developers of the theory and applications of binary sequences with favorable correlation properties and one of the currently most active younger contributors to research in this area. Each of us has taught university courses based on this material and benefited from the feedback obtained from the students in those courses. Our goal has been to produce a book that achieves a balance between the theoretical aspects of binary sequences with nearly ideal autocorrelation functions and the applications of these sequences to signal design for communications, radar, cryptography, and so on. This book is intended for use as a reference work for engineers and computer scientists in the applications areas just mentioned, as well as to serve as a textbook for a course in this important area of digital communications. Enough material has been included to enable an instructor to make some choices about what to cover in a one-semester course. However, we have referred the reader to the literature on those occasions when the inclusion of further detail would have resulted in a book of inordinate length.

We plan to maintain a Web site at http://calliope.uwaterloo.ca/∼ggong/book/book.htm for additions, corrections, and the continual updating of the material in this book.

Solomon W. Golomb, Los Angeles, CA, USA
Guang Gong, Waterloo, ON, Canada
August 31, 2004

Acknowledgments

Many people contributed significantly to the development of the material presented in this book. To the best of our ability we have acknowledged these contributions where they occur, as well as in the Bibliography; but inevitably some references have surely gone unattributed, for which we apologize in advance.

Colleagues as well as both current and former doctoral students of the authors have reviewed portions of the text, but we assume full responsibility for any deficiencies which remain.

Among those deserving special thanks for their assistance are Wensong Chu, Zongduo Dai, Tor Helleseth, Katrin Hoeper, Shaoquan Jiang, Khoongming Khoo, P. Vijay Kumar, Charles Lam, Heekwan Lee, Oscar Moreno, Reza Omrani, Susana Sin, Hong-Yeop Song, Douglas Stinson, Herbert Taylor, Lloyd R. Welch, Amr Youssef, and Nam Yul Yu. Our gratitude for help in preparing the manuscript goes to Mayumi Thatcher.

We further acknowledge reliance on articles we have previously published, either together or separately, in such journals as the *IEEE Transactions on Information Theory* and in conference proceedings, including

(a) *Surveys in Combinatorics, 1991*, A. D. Keedwell (Ed.), Cambridge University Press, 1991.
(b) *Difference Sets, Sequences and Their Correlation Properties (Bad Windsheim, 1998)*, A. Pott et al. (Ed.), NATO Adv. Sci. Inst. Ser. C, Math. Phys. Sci., Vol. 542, Kluwer Acad. Publ., Dordrecht, 1999.
(c) *Sequences and Their Applications – Proceedings of SETA'98*, *Discrete Mathematics and Theoretical Computer Science*, T. Helleseth et al. (Ed.), London, Springer-Verlag, 1999.

(d) *Sequences and Their Applications – Proceedings of SETA'01*, *Discrete Mathematics and Theoretical Computer Science*, V. Kumar, T. Helleseth, and K. Yang (Ed.), Berlin, Springer-Verlag, 2001.

Finally, we are grateful to Lauren Cowles of Cambridge University Press for her encouragement and forebearance with this project.

– S.W. Golomb and G. Gong

Historical Introduction

The prehistory of our subject can be backdated to 1202, with the appearance of Leonardo Pisano's *Liber Abaci* (Fibonacci 1202), containing the famous problem about breeding rabbits that leads to the linear recursion $f_{n+1} = f_n + f_{n-1}$ for $n \geq 2$, $f_1 = f_2 = 1$, which yields the Fibonacci sequence. Additional background can be attributed to Euler, Gauss, Kummer, and especially Edouard Lucas (Lucas 1876). For the history proper, the earliest milestones are papers by O. Ore (Ore 1934), R.E.A.C. Paley (Paley 1933), and J. Singer (Singer 1938). Ore started the systematic study of linear recursions over finite fields (including $GF(2)$), Paley inaugurated the search for constructions yielding Hadamard matrices, and Singer discovered the Singer difference sets that are mathematically equivalent to binary maximum length linear shift register sequences (also known as pseudorandom sequences, pseudonoise (PN) sequences, or m-sequences).

It appears that by the early 1950s devices that performed the modulo 2 sum of two positions on a binary delay line were being considered as key generators for stream ciphers in cryptographical applications. The question of what the periodicity of the resulting output sequence would be seemed initially mysterious. This question was explored outside the cryptographic community by researchers at a number of locations in the 1953–1956 time period, resulting in company reports by E. N. Gilbert at Bell Laboratories, by N. Zierler at Lincoln Laboratories, by L. R. Welch at the Jet Propulsion Laboratory, by S. W. Golomb at the Glenn L. Martin Company (now part of Lockheed-Martin), and probably by others as well. These earliest reports independently arrived at the correspondence between binary linear recurrence relations and polynomials over $GF(2)$, with the m-sequences corresponding to primitive irreducible polynomials. Golomb may have been the first to point out the correspondence between binary sequences with 2-level autocorrelation and cyclic (v, k, λ) difference sets (Golomb 1955) and even earlier (Golomb 1954) to recognize that quadratic residue sequences share the 2-level autocorrelation property of the PN-sequences and to formulate the objective of finding all binary sequences with this autocorrelation function (i.e., identifying all the constructions which yield $(4t-1, 2t-1, t-1)$ cyclic difference sets, also called cyclic Hadamard difference sets).

Beyond the Singer difference sets (equivalent to m-sequences) and the quadratic residue sequences (also called Legendre sequences), additional cyclic Hadamard examples were discovered occasionally: the sextic residue sequences of Marshall Hall, Jr. (see Hall 1956), the twin prime sequences of R. G. Stanton and D.A. Sprott (Stanton and Sprott 1958), and the GMW sequences, with generalizations, of B. Gordon, W. H. Mills, and L. R. Welch (Gordon, Mills, and Welch 1962). This was the state of knowledge when L. D. Baumert's book (Baumert 1971) appeared, except that by exhaustive search at $(v, k, \lambda) = (127, 63, 31)$, Baumert had found *six* inequivalent examples, of which only *three* came from known constructions. More unexplained examples turned up when U. Cheng performed the complete search at $(v, k, \lambda) = (255, 127, 63)$ in (Cheng 1983) and still more when R. B. Dreier and K. W. Smith exhaustively searched the case $(v, k, \lambda) = (511, 255, 127)$ in (Dreier and Smith 1991).

As mentioned in Baumert (1971), all known examples of cyclic Hadamard difference sets with parameters (v, k, λ), where $k = 2\lambda - 1$ and $v = 2k - 1$, have v belonging to one of three types: (i) primes of the form $4t - 1$, (ii) products pq where $q = p + 2$ and both p and q are primes, and (iii) numbers of the form $2^n - 1$. This conjecture (that v must be of one of these three types) looks much stronger now than when Golomb suggested it to Baumert around 1960. All known examples of type (ii) come from the Stanton–Sprott construction. All known examples of type (i) that are not also of type (iii), that is, primes of the form $4t - 1$ that are not Mersenne primes, come either from the quadratic residue construction or from Hall's sextic residue constructions when $p = 4a^2 + 27$. The great multiplicity of examples are of type (iii) and are related, in some way or other, to trace mappings from $GF(2^n)$ to $GF(2)$.

By 1955, Golomb had found all examples of type (iii) through $v = 2^5 - 1$. It was from studying their exhaustive list of examples at $v = 2^6 - 1$ that Gordon, Mill, and Welch (1962) discovered the GMW construction. Starting at $2^5 - 1$ in the 1950s, each decade has seen one more value of n, in $2^n - 1$, subjected to a complete search. It will be a challenge to programming skill and ingenuity to perform a complete search of $2^{11} - 1$ before the year 2020.

Golomb's book *Shift Register Sequences* first appeared in 1967, including the old Martin Company report (Golomb 1955) as its Chapter 3 and further developing the theory of both linear and nonlinear shift register sequences, based on Jet Propulsion Laboratory (JPL) reports he had written from 1956 to 1961, as the subsequent chapters. An enlarged second edition of this book appeared in 1982 (see Golomb 1967) and is still in print. The collaboration of the present authors began in 1996, when Dr. Gong began a two-year postdoctoral fellowship at the University of Southern California, visiting Dr. Golomb.

After decades of very slow progress, there was a sudden profusion of newly discovered constructions for cyclic Hadamard difference sets, starting in 1997. When the complete search was carried out at $(v, k, \lambda) = (1023, 511, 255)$ in (Gaal and Golomb 2001), ten inequivalent examples were found, but all belonged to families that by then had been discovered. These families also included all the previously unexplained examples at $v = 127$, $v = 255$, and $v = 511$. The recent paper by J. Dillon and H. Dobbertin (Dillon and Dobertin 2004) summarizes and completes the validation of all the constructions now known for cyclic Hadamard difference sets and lends credence to the belief that the identification of all such constructions (the task proposed in Golomb 1954) is finally complete. It is therefore timely for the present book, which describes all these constructions in reasonable detail, to make its appearance. We also discuss the more general question of constructing $4t \times 4t$ Hadamard matrices, which are conjectured to exist for all positive integers t (the first unknown case is $t = 167$), and the numerous ways in which these matrices are applied, to form advantageous sets of signals for communication and in Hadamard transforms. Our final chapter concerns the application of sequences with favorable autocorrelation properties to problems of radar, sonar, and synchronization. The only previous book describing applications of this type is Hans Dieter Lüke's Korrelationssignale (Lüke 1992), in German, which appeared before the discovery of all the new constructions.

Interest in sequences with favorable correlation properties, and the communication signals based on these sequences, has increased dramatically in recent years. In addition to the radar and sonar applications, there are important cryptographic and security system applications (see, e.g., Beker and Piper 1982) and there is intense interest in the applications to Code Division Multiple Access (CDMA) signals for mobile and wireless communications (see Viterbi 1995). In fact, essentially all the standards for third generation (3G) cellular telephony are based on CDMA, which in turn uses signals with the correlation properties described in the present book. It is interesting to note that many books, including those just cited, by Beker and Piper on secure communications and by Viterbi on CDMA, faithfully reproduce (with appropriate attribution) the derivation of the three randomness properties of pseudorandom sequences from Golomb's original (1955) Martin Company report.

In recent years, special international conferences on sequences (such as the series "Sequences and Their Applications," or SETA) have become frequent. Starting in 1998, the *Transactions on Information Theory* of the IEEE has had an associate editor for sequences.

For all of these reasons, we believe the appearance of our book to be highly useful, relevant, and timely.