Contents

Preface ix

List of abbreviations xi

List of common symbols xvii

1 Introduction 1
   1.1 Prologue 1
   1.2 Elements of pseudo random signal processing 2
   1.3 Outline of the book 5

2 Characterization of signals and sequences 7
   2.1 Classification of signals and sequences 7
       2.1.1 Morphological classification 8
       2.1.2 Phenomenological classification 9
       2.1.3 Energy classification 12
       2.1.4 Spectral classification 12
   2.2 Transformations of signals and sequences 13
       2.2.1 Basic transformations 13
   2.3 Correlation measures 16
       2.3.1 Autocorrelation and crosscorrelation functions 17
       2.3.2 Discrete periodic correlation functions 19
       2.3.3 Aperiodic correlation functions 23
       2.3.4 Other properties and relationships 26
       2.3.5 Correlation of binary sequences 34
       2.3.6 Orthogonality 37
   2.4 Power spectral density 39
       2.4.1 Power spectral density of analog signals 39
       2.4.2 Power spectral density of periodic signals 41
       2.4.3 Power spectral density of periodic pulse trains 44
   2.5 Pseudo random signals and sequences 45
       2.5.1 Pseudo randomness criteria 45
       2.5.2 Pseudo randomness and power spectral density 48
       2.5.3 Pseudo randomness and polyphase sequences 49
### 3 Mathematical foundations

3.1 Algebraic structures
- 3.1.1 Binary algebra, semigroup, and monoid
- 3.1.2 Groups, rings, and fields

3.2 Polynomials over finite fields
- 3.2.1 Polynomials and polynomial rings
- 3.2.2 Euclidean algorithm for polynomials
- 3.2.3 Irreducible polynomials
- 3.2.4 Cyclotomic cosets and minimal polynomials
- 3.2.5 Primitive polynomials

### 4 Binary pseudo random sequences

4.1 Classification

4.2 Maximal-length sequences
- 4.2.1 Linear recurring sequences
- 4.2.2 Maximal-length sequences
- 4.2.3 Properties of maximal-length sequences
- 4.2.4 Autocorrelation functions of maximal-length sequences

4.3 Binary sequences with good autocorrelation
- 4.3.1 Difference sets
- 4.3.2 De Bruijn sequences
- 4.3.3 Quadratic residue sequences
- 4.3.4 Other difference set sequences
- 4.3.5 Barker sequences and Williard sequences

4.4 Binary sequences with special crosscorrelation
- 4.4.1 Transorthogonal and orthogonal sequences
- 4.4.2 Gold sequences
- 4.4.3 Gold-like sequences
- 4.4.4 Kasami sequences

### 5 Nonbinary pseudo random sequences

5.1 Classification

5.2 Interference-free window sequences
- 5.2.1 Large-area synchronous codes

5.3 Complex-valued sequences
- 5.3.1 Complex maximal-length sequences
- 5.3.2 Polyphase sequences
- 5.3.3 Quadriphase sequences

5.4 Polyphase sequences with special correlations
- 5.4.1 Equivalent odd and even correlation sequences
- 5.4.2 Oppermann sequences

### 6 Generating pseudo random signals

6.1 Linear autonomous automata
- 6.1.1 Mathematical description
- 6.1.2 Canonical forms
- 6.1.3 State cycles
6.2 Generating maximal-length sequences
6.2.1 Standard circuits for binary maximal-length sequences
6.2.2 Special cases of modulo 2 arithmetic
6.2.3 High-speed sequence generation
6.2.4 Nonbinary sequence generation with binary encoding
6.3 Transformations of maximal-length sequences
6.3.1 Transversal filtering
6.3.2 Histogram transformation through mapping
6.3.3 Generation of phase-shifted maximal-length sequences
6.4 Combinations of maximal-length sequences
6.4.1 Modifications of binary maximal-length sequences
6.4.2 Product sequences
6.4.3 Combination sequences
6.4.4 Concatenated sequences
6.5 Pseudo random signal processing with microprocessors and memory circuits
6.5.1 Realizations with microprocessors
6.5.2 Realizations with memory circuits
6.5.3 Realizations with programmable logic devices
6.5.4 WIND-FLEX
6.5.5 Pseudo random signal generators

7 Applications of pseudo random signal processing
7.1 Spread spectrum communications
7.1.1 Basic concepts
7.1.2 Basic spread spectrum systems
7.1.3 Spread spectrum communication systems
7.1.4 Universal mobile telecommunications system
7.1.5 Bluetooth
7.2 Ranging and navigation systems
7.2.1 Ranging principles
7.2.2 Correlation receivers
7.2.3 Synchronization
7.2.4 Global positioning system
7.2.5 Galileo
7.2.6 Other ranging and navigation systems
7.3 Scrambling
7.3.1 Scrambling functions
7.3.2 Scrambling techniques
7.3.3 Scramblers for wireline systems
7.3.4 Scramblers for wireless systems
7.4 Automatic testing and system verification
7.4.1 Signature analysis
7.4.2 Built-in self-test schemes
7.4.3 Bit error analysis
7.5 Cryptology
7.5.1 Cryptosystems
7.5.2 Generators for stream ciphers
7.5.3 Feedback carry shift registers
CONTENTS

7.5.4 Content scrambling system for digital versatile discs 372
7.5.5 Encryption in radio and television systems 373
7.5.6 Security encryption algorithm A5 of the global system for mobile communication 376
7.6 Other applications 379
7.6.1 Correlation analysis of linear systems 379
7.6.2 Optical fiber systems 381
7.6.3 Angular sensor systems 384
7.6.4 Add-on data transmission in analog television 386

Bibliography 391
Index 403