

K. Deergha Rao

Channel Coding Techniques for Wireless Communications

EXTRA
MATERIALS
springerlink.com

 Springer

Channel Coding Techniques for Wireless Communications

K. Deergha Rao

Channel Coding Techniques for Wireless Communications



Springer

K. Deergha Rao
Research and Training Unit
for Navigational Electronics,
College of Engineering
Osmania University
Hyderabad, Telangana
India

ISBN 978-81-322-2291-0 ISBN 978-81-322-2292-7 (eBook)
DOI 10.1007/978-81-322-2292-7

Library of Congress Control Number: 2015930820

Springer New Delhi Heidelberg New York Dordrecht London
© Springer India 2015

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

Springer (India) Pvt. Ltd. is part of Springer Science+Business Media (www.springer.com)

Consulting Editor

M.N.S. Swamy, Concordia University

मातृभ्यो नमः
पितृभ्यो नमः
गुरुभ्यो नमः

To
*My parents Boddu and Dalamma,
My beloved wife Sarojini,
and My mentor Prof. M.N.S. Swamy*

Preface

The life of people has changed tremendously in view of the rapid growth of mobile and wireless communication. Channel coding is the heart of digital communication and data storage. The traditional block codes and conventional codes are commonly used in digital communications. To approach the theoretical limit for Shannon's channel capacity, the length of a linear block code or constant lengths of convolutional codes have to be increased, which in turn makes the decoder complexity to become high and may render it physically unrealizable. The powerful turbo and LDPC codes approach the theoretical limit for Shannon's channel capacity with feasible complexity for decoding. MIMO communications is a multiple antenna technology which is an effective way for high speed or high reliability communications. The MIMO can be implemented by space-time coding. However, a single book which can serve as a textbook for Bachelor and Master students on this topic is lacking in the market.

In this book, many illustrative examples are included in each chapter for easy understanding of the coding techniques. An attractive feature of this book is the inclusion of MATLAB-based examples with codes to encourage readers to implement on their personal computers and become confident of the fundamentals and gain more insight into coding theory. In addition to the problems that require analytical solutions, MATLAB exercises are introduced to the reader at the end of each chapter.

The book is divided into 11 chapters. Chapter 1 introduces the basic elements of a digital communication system, statistical models for wireless channels, capacity of a fading channel, Shannon's noisy channel coding theorem and the basic idea of coding gain. Chapter 2 gives an overview of the performance analysis of different modulation techniques, and also deals with the performance of different diversity combining techniques in a multi-channel receiver. Chapter 3 introduces Galois fields and polynomials over Galois fields. Chapter 4 covers linear block codes including RS codes because of their popularity in burst error correction in wireless networks. Chapter 5 discusses the design of a convolutional encoder and Viterbi decoding algorithm for the decoding of convolutional codes, as well as the performance analysis of convolutional codes over AWGN and Rayleigh fading

channels. In this chapter, punctured convolutional codes are also discussed. Chapter 6 provides a treatment of the design of turbo codes, BCJR algorithm for iterative decoding of turbo codes, and performance analysis of turbo codes. Chapter 7 focuses on the design and analysis of Trellis-coded modulation schemes using both the conventional and turbo codes. Chapter 8 describes the design of low parity check codes (LDPC), decoding algorithms and performance analysis of LDPC codes. The erasure correcting codes like Luby transform (LT) codes and Raptor codes are described in Chap. 9. Chapter 10 provides an in-depth study of multiple-input multiple-output (MIMO) systems in which multiple antennas are used both at the transmitter and at the receiver. The design of space-time codes and implementations of MIMO systems are discussed in Chap. 11.

Salient features of this book are as follows:

- Provides comprehensive exposure to all aspects of coding theory for wireless channels with clarity and in an easy way to understand
- Provides an understanding of the fundamentals, design, implementation and applications of coding for wireless channels
- Presents illustration of coding techniques and concepts with several fully worked numerical examples
- Provides complete design examples and implementation
- Includes PC-based MATLAB *m*-files for the illustrative examples are included in the book.

The motivation in writing this book is to include modern topics of increasing importance such as turbo codes, LDPC codes and space-time coding in detail, in addition to the traditional RS codes and convolutional codes, and also to provide a comprehensive exposition of all aspects of coding for wireless channels. The text is integrated with MATLAB-based programs to enhance the understanding of the underlying theories of the subject. These MATLAB codes are free to download from the book's page on [Springer.com](#).

This book is written at a level suitable for undergraduate and master students in electronics and communication engineering, electrical and computer engineering, computer science, and applied physics as well as for self-study by researchers, practicing engineers and scientists. Depending on the chapters chosen, this text can be used for teaching a one or two semester course on coding for wireless channels. The prerequisite knowledge of the readers in principles of digital communication is expected.

K. Deergha Rao

Contents

1	Introduction	1
1.1	Digital Communication System.	1
1.2	Wireless Communication Channels	1
1.2.1	Binary Erasure Channel (BEC)	1
1.2.2	Binary Symmetric Channel (BSC)	2
1.2.3	Additive White Gaussian Noise Channel	3
1.2.4	Gilbert–Elliott Channel	3
1.2.5	Fading Channel	4
1.2.6	Fading.	5
1.3	Statistical Models for Fading Channels	6
1.3.1	Probability Density Function of Rician Fading Channel	6
1.3.2	Probability Density Function of Rayleigh Fading Channel	6
1.3.3	Probability Density Function of Nakagami Fading Channel	7
1.4	Channel Capacity	8
1.4.1	Channel Capacity of Binary Erasure Channel	9
1.4.2	Channel Capacity of Binary Symmetric Channel.	9
1.4.3	Capacity of AWGN Channel	9
1.4.4	Channel Capacity of Gilbert–Elliott Channels.	11
1.4.5	Ergodic Capacity of Fading Channels	11
1.4.6	Outage Probability of a Fading Channel	13
1.4.7	Outage Capacity of Fading Channels.	14
1.4.8	Capacity of Fading Channels with CSI at the Transmitter and Receiver	15
1.5	Channel Coding for Improving the Performance of Communication System	16
1.5.1	Shannon’s Noisy Channel Coding Theorem	16
1.5.2	Channel Coding Principle	16
1.5.3	Channel Coding Gain	16

1.6	Some Application Examples of Channel Coding	17
1.6.1	Error Correction Coding in GSM	17
1.6.2	Error Correction Coding in W-CDMA	18
1.6.3	Digital Video Broadcasting Channel Coding	18
1.6.4	Error Correction Coding in GPS L5 Signal	19
	References	20
2	Performance of Digital Communication Over Fading Channels	21
2.1	BER Performance of Different Modulation Schemes in AWGN, Rayleigh, and Rician Fading Channels	21
2.1.1	BER of BPSK Modulation in AWGN Channel	22
2.1.2	BER of BPSK Modulation in Rayleigh Fading Channel	22
2.1.3	BER of BPSK Modulation in Rician Fading Channel	23
2.1.4	BER Performance of BFSK in AWGN, Rayleigh, and Rician Fading Channels	24
2.1.5	Comparison of BER Performance of BPSK, QPSK, and 16-QAM in AWGN and Rayleigh Fading Channels	26
2.2	Wireless Communication Techniques	28
2.2.1	DS-CDMA	28
2.2.2	FH-CDMA	32
2.2.3	OFDM	35
2.2.4	MC-CDMA	36
2.3	Diversity Reception	38
2.3.1	Receive Diversity with N Receive Antennas in AWGN	40
2.4	Diversity Combining Techniques	40
2.4.1	Selection Diversity	41
2.4.2	Equal Gain Combining (EGC)	42
2.4.3	Maximum Ratio Combining (MRC)	42
2.5	Problems	47
2.6	MATLAB Exercises	48
	References	48
3	Galois Field Theory	49
3.1	Set	49
3.2	Group	49
3.3	Field	50
3.4	Vector Spaces	51
3.5	Elementary Properties of Galois Fields	52
3.6	Galois Field Arithmetic	52

3.6.1	Addition and Subtraction of Polynomials	52
3.6.2	Multiplication of Polynomials	53
3.6.3	Multiplication of Polynomials Using MATLAB	53
3.6.4	Division of Polynomials	54
3.6.5	Division of Polynomials Using MATLAB	55
3.7	Polynomials Over Galois Fields	55
3.7.1	Irreducible Polynomial.	56
3.7.2	Primitive Polynomials	56
3.7.3	Checking of Polynomials for Primitiveness Using MATLAB.	56
3.7.4	Generation of Primitive Polynomials Using MATLAB.	57
3.8	Construction of Galois Field $GF(2^m)$ from $GF(2)$	58
3.8.1	Construction of $GF(2^m)$, Using MATLAB	63
3.9	Minimal Polynomials and Conjugacy Classes of $GF(2^m)$	65
3.9.1	Minimal Polynomials	65
3.9.2	Conjugates of GF Elements	65
3.9.3	Properties of Minimal Polynomial.	66
3.9.4	Construction of Minimal Polynomials	67
3.9.5	Construction of Conjugacy Classes Using MATLAB.	69
3.9.6	Construction of Minimal Polynomials Using MATLAB.	69
3.10	Problems	70
4	Linear Block Codes	73
4.1	Block Codes	73
4.2	Linear Block Codes	75
4.2.1	Linear Block Code Properties.	75
4.2.2	Generator and Parity Check Matrices.	76
4.2.3	Weight Distribution of Linear Block Codes	78
4.2.4	Hamming Codes.	79
4.2.5	Syndrome Table Decoding.	81
4.3	Cyclic Codes	83
4.3.1	The Basic Properties of Cyclic Codes	83
4.3.2	Encoding Algorithm for an (n, k) Cyclic Codes	84
4.3.3	Encoder for Cyclic Codes Using Shift Registers	87
4.3.4	Shift Register Encoders for Cyclic Codes.	89
4.3.5	Cyclic Redundancy Check Codes	90
4.4	BCH Codes	91
4.4.1	BCH Code Design	91
4.4.2	Berlekamp's Algorithm for Binary BCH Codes Decoding	96

4.4.3	Chien Search Algorithm	97
4.5	Reed–Solomon Codes	101
4.5.1	Reed–Solomon Encoder.	102
4.5.2	Decoding of Reed–Solomon Codes	105
4.5.3	Binary Erasure Decoding	114
4.5.4	Non-binary Erasure Decoding.	115
4.6	Performance Analysis of RS Codes.	118
4.6.1	BER Performance of RS Codes for BPSK Modulation in AWGN and Rayleigh Fading Channels.	118
4.6.2	BER Performance of RS Codes for Non-coherent BFSK Modulation in AWGN and Rayleigh Fading Channels.	122
4.7	Problems	124
4.8	MATLAB Exercises	125
	References.	126
5	Convolutional Codes	127
5.1	Structure of Non-systematic Convolutional Encoder	127
5.1.1	Impulse Response of Convolutional Codes.	129
5.1.2	Constraint Length	131
5.1.3	Convolutional Encoding Using MATLAB	131
5.2	Structure of Systematic Convolutional Encoder	132
5.3	The Structural Properties of Convolutional Codes	132
5.3.1	State Diagram	132
5.3.2	Catastrophic Convolutional Codes.	133
5.3.3	Transfer Function of a Convolutional Encoder	134
5.3.4	Distance Properties of Convolutional Codes	139
5.3.5	Trellis Diagram	139
5.4	Punctured Convolutional Codes	143
5.5	The Viterbi Decoding Algorithm.	145
5.5.1	Hard-decision Decoding.	147
5.5.2	Soft-decision Decoding	147
5.6	Performance Analysis of Convolutional Codes	151
5.6.1	Binary Symmetric Channel	151
5.6.2	AWGN Channel	153
5.6.3	Rayleigh Fading Channel.	155
5.7	Problems	157
5.8	MATLAB Exercises	159
	References.	159

6 Turbo Codes	161
6.1 Non-recursive and Recursive Systematic Convolutional Encoders	161
6.1.1 Recursive Systematic Convolutional (RSC) Encoder	161
6.2 Turbo Encoder	163
6.2.1 Different Types of Interleavers	164
6.2.2 Turbo Coding Illustration	165
6.2.3 Turbo Coding Using MATLAB	168
6.3 Turbo Decoder	176
6.3.1 The BCJR Algorithm	178
6.3.2 Turbo Decoding Illustration	182
6.3.3 Convergence Behavior of the Turbo Codes	192
6.3.4 EXIT Analysis of Turbo Codes	192
6.4 Performance Analysis of the Turbo Codes	195
6.4.1 Upper Bound for the Turbo Codes in AWGN Channel	195
6.4.2 Upper Bound for Turbo Codes in Rayleigh Fading Channel	197
6.4.3 Effect of Free Distance on the Performance of the Turbo Codes	200
6.4.4 Effect of Number of Iterations on the Performance of the Turbo Codes	203
6.4.5 Effect of Puncturing on the Performance of the Turbo Codes	204
6.5 Problems	205
6.6 MATLAB Exercises	206
References	206
7 Bandwidth Efficient Coded Modulation	209
7.1 Set Partitioning	210
7.2 Design of the TCM Scheme	211
7.3 Decoding TCM	217
7.4 TCM Performance Analysis	219
7.4.1 Asymptotic Coding Gain	219
7.4.2 Bit Error Rate	219
7.4.3 Simulation of the BER Performance of a 8-State 8-PSK TCM in the AWGN and Rayleigh Fading Channels Using MATLAB	230
7.5 Turbo Trellis Coded Modulation (TTCM)	232
7.5.1 TTCTM Encoder	232
7.5.2 TTCTM Decoder	234

7.5.3	Simulation of the BER Performance of the 8-State 8-PSK TTCM in AWGN and Rayleigh Fading Channels	234
7.6	Bit-interleaved Coded Modulation	237
7.6.1	BICM Encoder	238
7.6.2	BICM Decoder	239
7.7	Bit-interleaved Coded Modulation Using Iterative Decoding	239
7.7.1	BICM-ID Encoder and Decoder	240
7.7.2	Simulation of the BER Performance of 8-State 8-PSK BICM and BICM-ID in AWGN and Rayleigh Fading Channels	242
7.8	Problems	244
Appendix A	245
References	250
8	Low Density Parity Check Codes	251
8.1	LDPC Code Properties	251
8.2	Construction of Parity Check Matrix H	252
8.2.1	Gallager Method for Random Construction of H for Regular Codes	252
8.2.2	Algebraic Construction of H for Regular Codes	253
8.2.3	Random Construction of H for Irregular Codes	254
8.3	Representation of Parity Check Matrix Using Tanner Graphs	255
8.3.1	Cycles of Tanner Graph	256
8.3.2	Detection and Removal of Girth 4 of a Parity Check Matrix	257
8.4	LDPC Encoding	260
8.4.1	Preprocessing Method	260
8.5	Efficient Encoding of LDPC Codes	266
8.5.1	Efficient Encoding of LDPC Codes Using MATLAB	269
8.6	LDPC Decoding	270
8.6.1	LDPC Decoding on Binary Erasure Channel Using Message-Passing Algorithm	271
8.6.2	LDPC Decoding on Binary Erasure Channel Using MATLAB	274
8.6.3	Bit-Flipping Decoding Algorithm	275
8.6.4	Bit-Flipping Decoding Using MATLAB	278
8.7	Sum–Product Decoding	280
8.7.1	Log Domain Sum–Product Algorithm (SPA)	284
8.7.2	The Min-Sum Algorithm	285
8.7.3	Sum–Product and Min-Sum Algorithms for Decoding of Rate 1/2 LDPC Codes Using MATLAB	289

8.8	EXIT Analysis of LDPC Codes	291
8.8.1	Degree Distribution.	291
8.8.2	Ensemble Decoding Thresholds	293
8.8.3	EXIT Charts for Irregular LDPC Codes in Binary Input AWGN Channels	294
8.9	Performance Analysis of LDPC Codes	296
8.9.1	Performance Comparison of Sum–Product and Min-Sum Algorithms for Decoding of Regular LDPC Codes in AWGN Channel	296
8.9.2	BER Performance Comparison of Regular and Irregular LDPC Codes in AWGN Channel.	296
8.9.3	Effect of Block Length on the BER Performance of LDPC Codes in AWGN Channel	297
8.9.4	Error Floor Comparison of Irregular LDPC Codes of Different Degree Distribution in AWGN Channel	298
8.10	Problems	300
8.11	MATLAB Exercises	302
	References.	302
9	LT and Raptor Codes.	305
9.1	LT Codes Design	305
9.1.1	LT Degree Distributions	306
9.1.2	Important Properties of the Robust Soliton Distribution	308
9.1.3	LT Encoder	308
9.1.4	Tanner Graph of LT Codes	310
9.1.5	LT Decoding with Hard Decision	310
9.1.6	Hard-Decision LT Decoding Using MATLAB	312
9.1.7	BER Performance of LT Decoding over BEC Using MATLAB	314
9.2	Systematic LT Codes	315
9.2.1	Systematic LT Codes Decoding	316
9.2.2	BER Performance Analysis of Systematic LT Codes Using MATLAB	316
9.3	Raptor Codes	322
9.4	Problems	323
9.5	MATLAB Exercises	323
	References.	323
10	MIMO System	325
10.1	What Is MIMO?	325
10.2	MIMO Channel Model	326
10.2.1	The Frequency Flat MIMO Channel	326

10.2.2	The Frequency-Selective MIMO Channel	327
10.2.3	MIMO-OFDM System	327
10.3	Channel Estimation	328
10.3.1	LS Channel Estimation	329
10.3.2	DFT-Based Channel Estimation	330
10.3.3	MIMO-OFDM Channel Estimation	330
10.3.4	Channel Estimation Using MATLAB	331
10.4	MIMO Channel Decomposition	333
10.5	MIMO Channel Capacity	335
10.5.1	Capacity of Deterministic MIMO Channel When CSI Is Known to the Transmitter	335
10.5.2	Deterministic MIMO Channel Capacity When CSI Is Unknown at the Transmitter	337
10.5.3	Random MIMO Channel Capacity	338
10.6	MIMO Channel Equalization	348
10.6.1	Zero Forcing (ZF) Equalization	350
10.6.2	Minimum Mean Square Error (MMSE) Equalization	350
10.6.3	Maximum Likelihood Equalization	350
10.7	Problems	351
10.8	MATLAB Exercises	353
	References	353
11	Space–Time Coding	355
11.1	Space–Time-Coded MIMO System	355
11.2	Space–Time Block Code (STBC)	356
11.2.1	Rate Limit	357
11.2.2	Orthogonality	357
11.2.3	Diversity Criterion	357
11.2.4	Performance Criteria	358
11.2.5	Decoding STBCs	359
11.3	Alamouti Code	359
11.3.1	2-Transmit, 1-Receive Alamouti STBC Coding	360
11.3.2	2-Transmit, 2-Receive Alamouti STBC Coding	361
11.3.3	Theoretical BER Performance of BPSK Alamouti Codes Using MATLAB	363
11.4	Higher-Order STBCs	364
11.4.1	3-Transmit, 4-Receive STBC Coding	365
11.4.2	Simulation of BER Performance of STBCs Using MATLAB	369
11.5	Space–Time Trellis Coding	372
11.5.1	Space–Time Trellis Encoder	373
11.5.2	Simulation of BER Performance of 4-State QPSK STTC Using MATLAB	381

11.6	MIMO-OFDM Implementation	387
11.6.1	Space-Time-Coded OFDM	389
11.6.2	Space-Frequency-Coded OFDM	390
11.6.3	Space-Time-Frequency-Coded OFDM	390
11.7	Problems	392
11.8	MATLAB Exercises	393
	References	393

About the Author

K. Deergha Rao is director and professor in the Navigational Electronics Research and Training Unit (NERTU), University College of Engineering, Osmania University, Hyderabad, India. Earlier, he was a postdoctoral fellow and part-time professor at the Department of Electronics and Communication Engineering, Concordia University, Montreal, Canada. He has executed several research projects for premium Indian organizations such as Defence Research and Development Organization (DRDO), Hindustan Aeronautical Limited (HAL) and Bharat Electronics Limited (BEL). His teaching areas are digital signal processing, digital image processing, coding theory for wireless channels and MIMO wireless communications, whereas his research interests include GPS signal processing, wireless channel coding, blind equalization, robust multiuser detection, OFDM UWB signal processing, MIMO SFBC OFDM, image processing, cryptosystems and VLSI signal processing. Professor Rao has presented papers at IEEE international conferences several times in the U.S.A., Switzerland and Russia. He has more than 100 publications to his credit, including more than 60 publications in IEEE journals and conference proceedings. He is a senior member of IEEE and has served as chairman of communications and signal processing societies joint chapter of IEEE Hyderabad section. He is currently a member of the IEEE SPS chapters committee. He was awarded 2013 IETE K.S. Krishnan Memorial Award for the best system-oriented paper. He has served as Communications Track Chair for IEEE INDICON 2011 held at Hyderabad. He is an editorial board member of the International Journal of Sustainable Aviation (Inderscience Publishers, U.K.). He has coauthored a book, Digital Signal Processing (Jaico Publishing House, India).

Chapter 1

Introduction

In this chapter, a digital communication system with coding is first described. Second, various wireless communication channels, their probability density functions, and capacities are discussed. Further, Shannon's noisy channel coding theorem, channel coding principle, and channel coding gain are explained. Finally, some application examples of channel coding are included.

1.1 Digital Communication System

A communication system is a means of conveying information from one user to another user. The digital communication system is one in which the data are transmitted in digital form. A digital communication system schematic diagram is shown in Fig. 1.1. The source coding is used to remove redundancy from source information for efficient transmission. The transmitted signal power and channel bandwidth are the key parameters in the design of digital communication system. Using these parameters, the signal energy per bit (E_b) to noise power spectral density (N_0) ratio is determined. This ratio is unique in determining the probability of bit error, often referred to as bit error rate (BER). In practice, for a fixed E_b/N_0 , acceptable BER is possible with channel coding. This can be achieved by adding additional digits to the transmitted information stream. These additional digits do not have any new information, but they make it possible for the receiver to detect and correct errors thereby reducing the overall probability of error.

1.2 Wireless Communication Channels

1.2.1 Binary Erasure Channel (BEC)

Erasure is a special type of error with known location. The BEC transmits one of the two binary bits 0 and 1. However, an erasure 'e' is produced when the receiver receives an unreliable bit. The BEC channel output consists of 0, 1, and e as shown

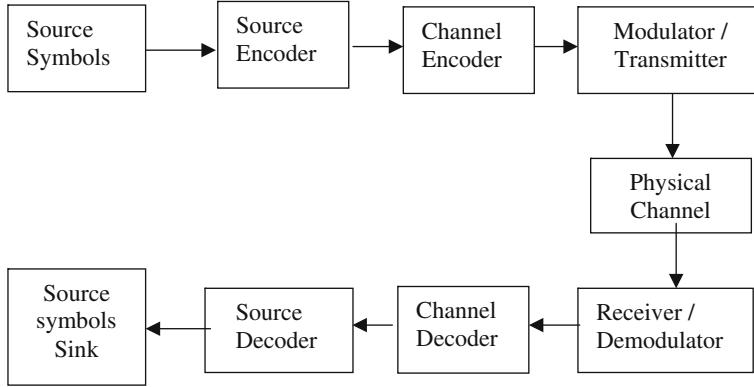


Fig. 1.1 Digital communication system with coding

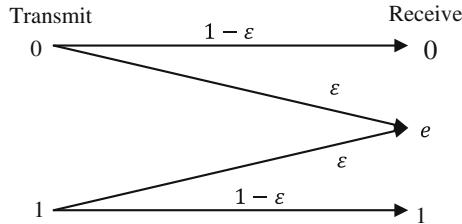


Fig. 1.2 Binary erasure channel

in Fig. 1.2. The BEC erases a bit with probability ε , called the erasure probability of the channel. Thus, the channel transition probabilities for the BEC are

$$\left. \begin{aligned} P(y = 0|x = 0) &= 1 - \varepsilon, \\ P(y = e|x = 0) &= \varepsilon, \\ P(y = 1|x = 0) &= 0, \\ P(y = 0|x = 1) &= 0, \\ P(y = e|x = 1) &= \varepsilon, \\ P(y = 1|x = 1) &= 1 - \varepsilon. \end{aligned} \right\} \quad (1.1)$$

1.2.2 Binary Symmetric Channel (BSC)

The BSC is discrete memoryless channel that has binary symbols both in the input and output. It is symmetric because the probability for receiving 0 when 1 is transmitted is same as the probability for receiving 1 when 0 is transmitted. This

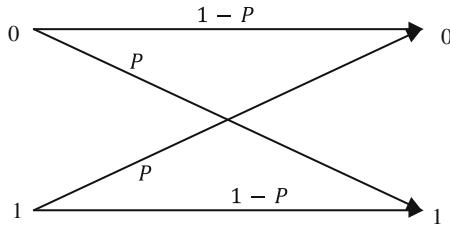


Fig. 1.3 Binary symmetric channel

probability is called the crossover probability of the channel denoted by P as shown in Fig. 1.3. The probability for no error, i.e., receiving the same as transmitted, is $1 - P$. Hence, the channel transition probabilities for the BSC are

$$\left. \begin{array}{l} P(y = 0|x = 0) = 1 - P, \\ P(y = 0|x = 1) = P, \\ P(y = 1|x = 0) = P, \\ P(y = 1|x = 1) = 1 - P, \end{array} \right\} \quad (1.2)$$

1.2.3 Additive White Gaussian Noise Channel

In an AWGN channel, the signal is degraded by white noise η which has a constant spectral density and a Gaussian distribution of amplitude. The Gaussian distribution has a probability density function (pdf) given by

$$P_{df}(\eta) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{\eta^2}{2\sigma^2}\right) \quad (1.3)$$

where σ^2 is the variance of a Gaussian random process.

1.2.4 Gilbert–Elliott Channel

For bursty wireless channels, the Gilbert–Elliott (GE) channel [1, 2] is one of the simplest and practical models. The GE channel is a discrete-time stationary model as shown in Fig. 1.4 with two states: one bad state or burst state ‘2’ wherein a BSC resides with high error probabilities ($1 - P_2$) and the other state is a good state ‘1’ wherein a BSC resides with low error probabilities ($1 - P_1$).

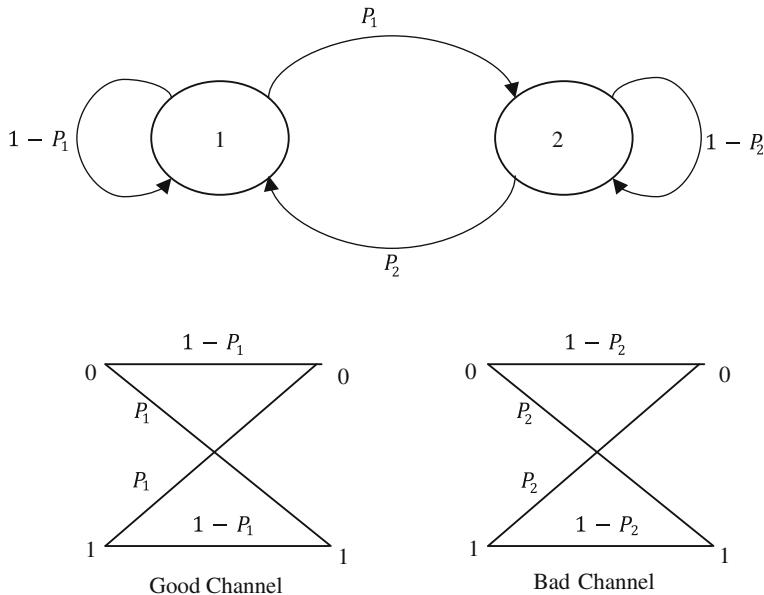


Fig. 1.4 A two-state channel

Another common GE example is that the BEC resides in a bad state with ε close to unity and assigns erasures to all of the bits transmitted during the high-error-rate (bad) state.

1.2.5 Fading Channel

In the radio channel, the received power is affected by the attenuations due to the combinations of the following effects:

1. *The Path loss:* It is the signal attenuation. The power received by the receiving antenna decreases when the distance between transmitter and receiver increases. The power attenuation is proportional to $(\text{distance})^\alpha$, where α values range from 2 to 4. When the distance varies with time, the path loss also varies.
2. *The Shadowing loss:* It is due to the absorption of the radiated signal by scattering structure. It is derived from a random variable with lognormal distribution.
3. *The Fading loss:* The combination of multipath propagation and the Doppler frequency shift produces the random fluctuations in the received power which gives the fading losses.

1.2.6 Fading

Fading gives the variations of the received power along with the time. It is due to the combination of multipath propagation and the Doppler frequency shift which gives the time-varying attenuations and delays that may degrade the communication system performance. The received signal is a distorted version of the transmitted signal which is a sum of the signal components from the various paths with different delays due to multipath and motion.

Let T_s be the duration of a transmitted signal and B_x be the signal bandwidth. The fading channel can be classified based on coherence time and coherence bandwidth of the channel. The coherence time and coherence bandwidth of a channel are defined as follows:

Doppler spread: The significant changes in the channel occur in a time T_c whose order of magnitude is the inverse of the maximum Doppler shift B_D among the various paths, called the *Doppler spread* of the channel.

The coherence time of the channel T_c is

$$T_c \triangleq \frac{1}{B_D} \quad (1.4)$$

Delay spread: The maximum among the path delay differences, a significant change occurs when the frequency change exceeds the inverse of T_D , called the *delay spread* of the channel.

The coherence bandwidth of the channel B_c is as follows:

$$B_c \triangleq \frac{1}{T_D} \quad (1.5)$$

The classification fading channels is shown in Fig. 1.5.

The fast fading causes short burst errors which are easy to correct. The slow fading will affect many successive symbols leading to long burst errors. Due to energy absorption and scattering in physical channel propagation media, the transmitted signal is attenuated and becomes noisy. The attenuation will vary in mobile communications based on the vehicle speed, surrounding trees, buildings, mountains, and

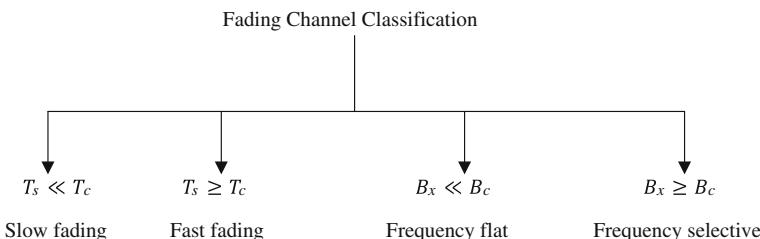


Fig. 1.5 Classification of fading channels

terrain. Based on the receiver location, moving receiver signals interfere with one another and take several different paths. As such, the wireless channels are called multipath fading channels. Hence, the additive white Gaussian noise (AWGN) assumption for wireless channels is not realistic. Thus, the amplitudes in wireless channel are often modeled using Rayleigh or Rician probability density function.

The most common fading channel models are as follows:

1. Flat independent fading channel
2. Block fading channel

In flat independent fading channel, the attenuation remains constant for one symbol period and varies from symbol to symbol. Whereas in block fading channel, the attenuation is constant over a block of symbols and varies from block to block.

1.3 Statistical Models for Fading Channels

1.3.1 Probability Density Function of Rician Fading Channel

When the received signal is made up of multiple reflective rays plus a significant line of sight (non-faded) component, the received envelope amplitude has a Rician probability density function (PDF) as given in Eq. (1.6), and the fading is referred to as Rician fading.

$$P_{df}(x) = \begin{cases} \frac{x}{\sigma^2} \exp\left(-\frac{(x^2 + A^2)}{2\sigma^2}\right) I_0\left(\frac{xA}{\sigma^2}\right) & \text{for } x \geq 0, A \geq 0 \\ 0 & \text{otherwise} \end{cases} \quad (1.6)$$

where x is the amplitude of the received faded signal, I_0 is the zero order modified Bessel function of the first kind, and A denotes the peak magnitude of the non-faded signal component called the specular component. The Rician PDF for different values of sigma and $A = 1$ is shown in Fig. 1.6.

1.3.2 Probability Density Function of Rayleigh Fading Channel

Rayleigh fading occurs when there are multiple indirect paths between the transmitter and the receiver and no direct non-fading or line of sight (LOS) path. It represents the worst case scenario for the transmission channel. Rayleigh fading assumes that a received multipath signal consists of a large number of reflected waves with independent and identically distributed phase and amplitude. The envelope of the received carrier signal is Rayleigh distributed in wireless communications [3].

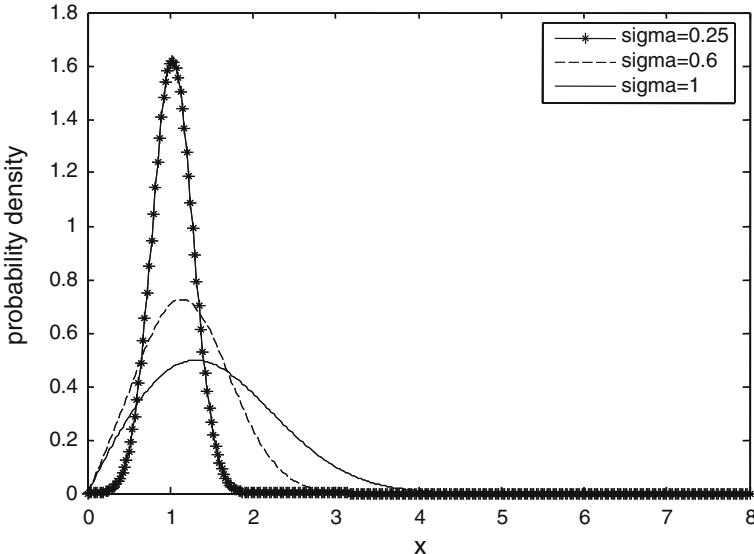


Fig. 1.6 Probability density of Rician fading channel

As the magnitude of the specular component approaches zero, the Rician PDF approaches a Rayleigh PDF expressed as follows:

$$\begin{aligned} P_{df}(x) &= \frac{x}{\sigma^2} \exp\left(-\frac{x^2}{2\sigma^2}\right) && \text{for } x \geq 0 \\ &= 0 && \text{otherwise} \end{aligned} \quad (1.7)$$

The Rayleigh PDF for different values of sigma is shown in Fig. 1.7.

Additive white Gaussian noise and Rician channels provide fairly good performance corresponding to an open country environment, while Rayleigh channel, which best describes the urban environment fading, provides relatively worse performance.

1.3.3 Probability Density Function of Nakagami Fading Channel

The Nakagami model is another very popular empirical fading model [4]

$$P_{df}(r) = \frac{2}{\Gamma(m)} \left(\frac{m}{2\sigma^2}\right)^m r^{2m-1} e^{-\frac{mr^2}{2\sigma^2}} \quad (1.8)$$

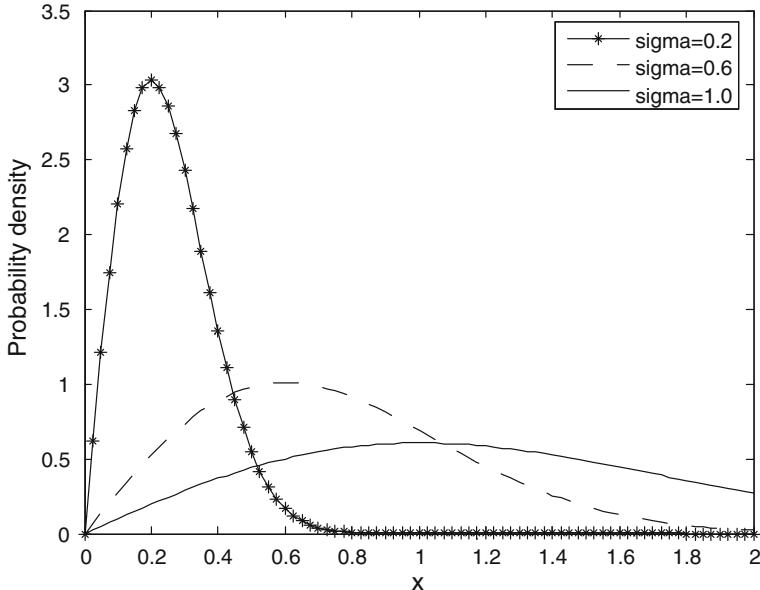


Fig. 1.7 Probability density of Rayleigh fading channel

where $\sigma^2 = \frac{1}{2}E[r^2]$, $\Gamma(\cdot)$ is the gamma function, $m \geq \frac{1}{2}$ is the fading figure.

The received instantaneous power r^2 satisfies a gamma distribution. The phase of the signal is uniformly distributed in $[0, 2\pi]$. The Nakagami distribution is a general model obtained from experimental data fitting, and its shape is very similar to that of the Rice distribution. The shape parameter ‘m’ measures the severity of fading.

When

$m = 1$, it is Rayleigh fading.

$m \rightarrow \infty$, it is AWGN channel; that is, there is no fading.

$m > 1$, it is close to Rician fading.

However, due to lack of the physical basis, the Nakagami distribution is not as popular as the Rician and Rayleigh fading models in mobile communications. Many other fading channel models are discussed in Kuhn [5].

1.4 Channel Capacity

Channel capacity can be defined as the maximum rate at which the information can be transmitted over a reliable channel.

$$\text{Spectral or Bandwidth Efficiency} = \frac{\text{Transmission rate}}{\text{Channel Band width}} = \frac{R_s \mathcal{H}}{B} \text{ bits/s/Hz}$$
(1.9)

where R_s is the symbol rate, and \mathcal{H} is the entropy.

The channel capacity is also known as Shannon's capacity can be defined as the average mutual information for a channel with energy constraint.

1.4.1 Channel Capacity of Binary Erasure Channel

The channel capacity of BEC is

$$C_{\text{BEC}} = 1 - e$$
(1.10)

e is the probability of a bit erasure, which is represented by the symbol e .

1.4.2 Channel Capacity of Binary Symmetric Channel

The Channel capacity of BSC is as follows:

$$C_{\text{BSC}} = 1 - \mathcal{H}(P)$$
(1.11)

$\mathcal{H}(P)$ is the binary entropy function given by Ryan and Lin [6]

$$\mathcal{H}(P) = -P \log_2(P) - (1 - P) \log_2(1 - P)$$
(1.12)

P is the probability of a bit error.

1.4.3 Capacity of AWGN Channel

An AWGN channel can be expressed by the following input–output relationship

$$y = x + \eta$$
(1.13)

where x is the transmitted source signal, y denotes the output of the channel, and η is a real Gaussian process with zero mean, variance $\sigma_\eta^2 = E[\eta^2]$, and two sided power spectral density $\frac{N_0}{2}$. The mutual information $I(x; y)$ with constraint on the energy of the input signal can be expressed as follows:

$$I(x, y) = \mathcal{H}(y) - \mathcal{H}(\eta) \quad (1.14)$$

where $\mathcal{H}(y)$ is the entropy of the channel output, and $\mathcal{H}(\eta)$ is the entropy of the AWGN. Since $\sigma_y^2 = \sigma_x^2 + \sigma_\eta^2$, the entropy $\mathcal{H}(y)$ is bounded by $\frac{1}{2}\log_2 \pi e(\sigma_x^2 + \sigma_\eta^2)$ and thus

$$\begin{aligned} I(x, y) &\leq \frac{1}{2}\log_2 \pi e(\sigma_x^2 + \sigma_\eta^2) - \frac{1}{2}\log_2 \pi e\sigma_\eta^2 \\ &= \frac{1}{2}\log_2(1 + \frac{\sigma_x^2}{\sigma_\eta^2}) \end{aligned} \quad (1.15)$$

The mutual information $I(x, y)$ is maximum when the input x is a real Gaussian process with zero mean and variance σ_x^2 . The capacity of the channel is the maximum information that can be transmitted from x to y by varying the PDF P_{df} of the transmit signal x . The signal-to-noise ratio (SNR) is defined by

$$\text{SNR} \triangleq \frac{\sigma_x^2}{\sigma_\eta^2} \quad (1.16)$$

Thus, the capacity of an AWGN channel is given by

$$\mathbf{C} = \frac{1}{2}\log_2(1 + \text{SNR}) \text{ bits/s/Hz} \quad (1.17)$$

Since $\sigma_x^2 = BE_s$ and $\sigma_\eta^2 = BN_0$, Eq. (1.17) can be rewritten as follows:

$$\mathbf{C} = \frac{1}{2}\log_2\left(1 + 2\frac{E_s}{N_0}\right) \text{ bits/s/Hz} \quad (1.18)$$

where B is the bandwidth, E_s denotes the symbol energy, and N_0 represents the noise spectral density.

If x and η are independent complex Gaussian processes, the channel capacity can be expressed as follows:

$$\mathbf{C} = \log_2(1 + \text{SNR}) \text{ bits/s/Hz} \quad (1.19)$$

Since $\sigma_x^2 = BE_s$ and $\sigma_\eta^2 = BN_0$ for complex Gaussian process, Eq. (1.19) can be rewritten as follows:

$$\mathbf{C} = \log_2\left(1 + \frac{E_s}{N_0}\right) \text{ bits/s/Hz} \quad (1.20)$$

Example 1.1 What is the capacity of a channel with an SNR of 20 dB.

Solution $\mathbf{C} = \log_2(1 + 20) = 6.65$ bits/s/Hz.

The capacity is increasing as a log function of the SNR, which is a slow increase. Clearly, increasing the capacity by any significant factor takes an enormous amount of power.

1.4.4 Channel Capacity of Gilbert–Elliott Channels

The channel capacity of GE Channel is given by Ryan and Lin [6]

$$\mathbf{C}_{\text{GE}} = \sum_{s=1}^S P_s \mathbf{C}_s \quad (1.21)$$

where P_s is the probability of being state in s state, and \mathbf{C}_s is the capacity of the channel in s state.

1.4.5 Ergodic Capacity of Fading Channels

A slow flat fading channel with AWGN can be expressed by the following input–output relationship

$$y = hx + \eta \quad (1.22)$$

where x is the transmitted source signal, y denotes the output of the channel, η is the AWGN, and h is a Gaussian random variable with Rician or Rayleigh PDF.

The fading channel model given in Eq. (1.22) can be seen as a Gaussian channel with attenuation h . If h is assumed to be an ergodic process, the capacity of the fading channel is the Ergodic capacity computed by the following expression

$$\mathbf{C} = E[\log_2(1 + h^2 \text{SNR})] \text{ bits/s/Hz} \quad (1.23)$$

where the expectation $E[\cdot]$ is with respect to random variable h . If $E[h^2] = 1$, Eq. (1.23) is always less than AWGN channel capacity since $E[f(X)] \leq f(E[X])$ according to Jensen inequality. If h has Rayleigh PDF, computation of Eq. (1.24) yields [5]

$$\mathbf{C} = \log_2 e \cdot \exp\left(\frac{1}{\text{SNR}}\right) \cdot \text{expint}\left(\frac{1}{\text{SNR}}\right) \text{ bits/s/Hz} \quad (1.24)$$

where

$$\text{expint } (x) \triangleq \int_x^{\infty} \frac{e^t}{t} dt$$

which is the capacity of the independent Rayleigh fading channel with no constraint on the constellation of the input signal. The following MATLAB program is written and used to compute the AWGN channel capacity in AWGN and the ergodic capacity of a Rayleigh fading channel.

Program 1.1: MATLAB program to compute capacity of AWGN channel and ergodic capacity of Rayleigh fading channel with channel state information (CSI).

```
% capacity of AWGN channel and ergodic capacity of Rayleigh fading
%channel state information (CSI).
clear all
close all
SNRdB = [-10:0.1:30];
SNRlin = 10.^ (SNRdB/10);
C_AWGN = log2 (1 + SNRlin); % AWGN
C_Rayleigh = log2(exp(1)) * exp (1 ./ SNRlin) .* expint( 1 ./ SNRlin); %%
Rayleigh
plot(SNRdB, C_AWGN, '-.', SNRdB, C_Rayleigh, '--');
xlabel('SNR(dB)'), ylabel('{\it Capacity} (bit/s/Hz)');
legend('AWGN', 'Rayleigh fading');
```

The SNR versus capacity plot obtained from the above MATLAB program is shown in Fig. 1.8. From Fig. 1.8, it can be observed that there is a much lower performance difference between the capacities of AWGN and Rayleigh channels. This is highly indicative that the coding of fading channels will yield considerable coding gain for large SNR.

Example 1.2 For large SNR's, verify that the SNR required to obtain the same ergodic capacity for the AWGN channel and the independent Rayleigh fading channel differs by 2.5 dB.

Solution AWGN channel capacity is given by $C = \log_2(1 + \text{SNR})$ bits/s/Hz.

For large SNRs, the above equation can be approximated as follows:

$$C = \log_2(\text{SNR}) \text{ bits/s/Hz}$$

The ergodic capacity in Rayleigh fading channel is given by

$$C = \log_2 e \cdot \exp\left(\frac{1}{\text{SNR}}\right) \cdot \text{expint}\left(\frac{1}{\text{SNR}}\right)$$

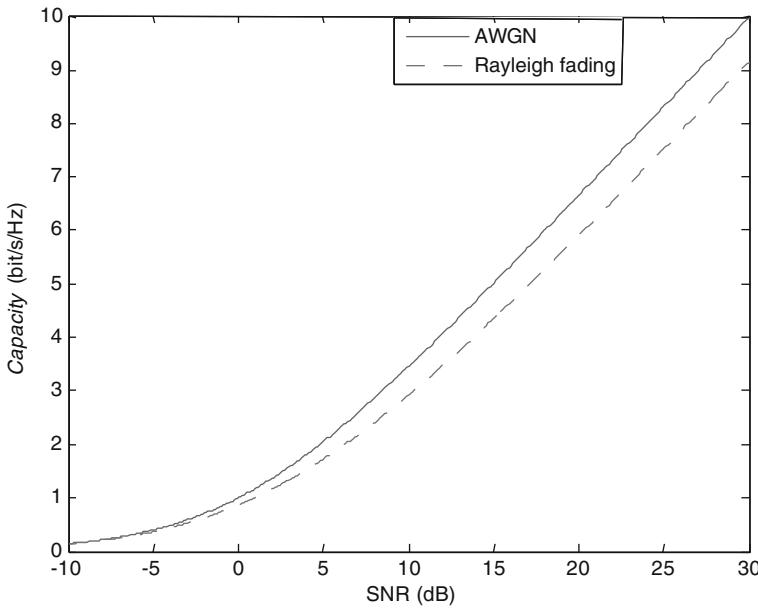


Fig. 1.8 Capacity of AWGN channel and ergodic capacity of independent Rayleigh fading channel

For large SNRs, the above equation can be rewritten as follows:

$$C_{\text{Rayleigh}} = \log_2(\text{SNR}) - 0.8327$$

Since the capacity of an AWGN channel for large SNRs can be approximated as $\log_2(\text{SNR})$, the above relation can be rewritten as follows:

$$C_{\text{Rayleigh}} = C_{\text{AWGN}} - 0.8327$$

Thus, the capacity for AWGN channel and the Rayleigh fading channel differs by 0.8327. The difference in dB can be expressed as follows:

$$10 \log_{10}(2^{0.8327}) = 2.5 \text{ dB}$$

1.4.6 Outage Probability of a Fading Channel

A mobile user will experience rapid changes in SNR as fading channels lead to an oscillating SNR at different locations. As such, the channel can be characterized by an average SNR and BER can be computed by using this. If BER is below a

threshold, then it is not the primary concern for many applications. A more meaningful measure is outage probability, which is the percentage of time that an acceptable quality of communication is not available.

The outage probability of a fading channel is the probability with which the information outage occurs when the transmission rate exceeds the capacity.

The outage probability for a Rayleigh fading channel with the same SNR as that of AWGN is given by Du and Swamy [3]

$$P_{\text{out}} = 1 - \exp\left(\frac{1 - 2^{C_{\text{out}}}}{\text{SNR}}\right) \quad (1.25)$$

1.4.7 Outage Capacity of Fading Channels

The outage capacity of a fading channel is the maximum rate supported by the channel for a given outage probability of the channel. The C_{out} can be expressed as follows:

$$C_{\text{out}} = \log_2(1 - \text{SNR} \log(1 - P_{\text{out}})) \quad (1.26)$$

The following MATLAB program is written and used to compute outage capacity of Rayleigh fading channels for different outage probabilities.

Program 1.2: MATLAB program to compute outage capacities of the Rayleigh fading channel

```
% outage capacities of Rayleigh fading channel
clear all
close all
SNRdB = [-10:0.1:30];
SNRlin = 10.^{(SNRdB/10)};
C_AWGN = log2(1 + SNRlin);% AWGN
C_Rayleigh = log2(exp(1)) * exp(1./ SNRlin) .* expint(1./ SNRlin);%
Rayleigh
P_out = 25e-2;
C_out_25 = log2(1 - SNRlin * log(1-P_out));
P_out = 68e-2;
C_out_68 = log2(1 - SNRlin * log(1-P_out));
plot(SNRdB, C_AWGN, '-', SNRdB, C_Rayleigh, '--', SNRdB,
C_out_68, '.', SNRdB, C_out_25, ':');
xlabel('E_s/N_0 (dB)'), ylabel('C_{out} (bit/s/Hz)');
legend('AWGN', 'Rayleigh fading', 'C_{out} 25%', 'C_{out} 68%', 'C_{out} 46%', 'C_{out} 64%');
```

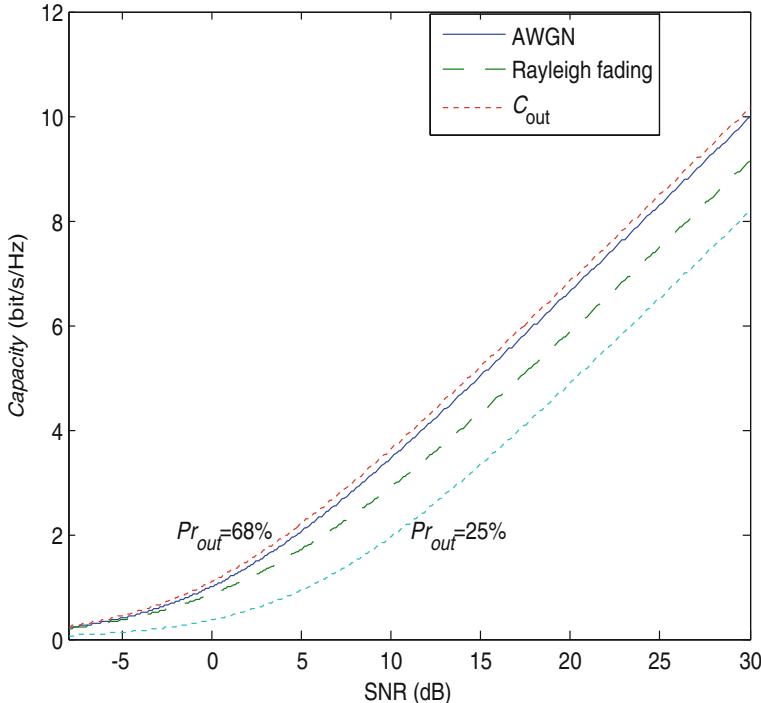


Fig. 1.9 Outage capacities of Rayleigh fading channel

The outage capacity of Rayleigh fading channel for different outage probabilities obtained from the above program is shown in Fig. 1.9.

It is observed from Fig. 1.6 that at $p_{\text{out}} = 68\%$, C_{out} is greater than the capacity of AWGN channel.

1.4.8 Capacity of Fading Channels with CSI at the Transmitter and Receiver

The ergodic capacity of a Rayleigh fading channel with channel state information (CSI) at the transmitter and receiver is given by Goldsmith [7]

$$\mathbf{C} = \int_{\gamma_0}^{\infty} B \log_2 \left(\frac{\gamma}{\gamma_0} \right) P_{\text{df}}(\gamma) d\gamma \text{ bits/s/Hz} \quad (1.27)$$

where γ is the signal-to-noise ratio (SNR), γ_0 is the cutoff SNR, $P_{\text{df}}(\gamma)$ is the PDF of γ due to the fading channel.

1.5 Channel Coding for Improving the Performance of Communication System

1.5.1 Shannon's Noisy Channel Coding Theorem

Any channel affected by noise possesses a specific ‘channel capacity’ C , a rate of conveying information that can never be exceeded without error, but in principle, an error-correcting code always exists such that information can be transmitted at rates less than C with an arbitrarily low BER.

1.5.2 Channel Coding Principle

The channel coding principle is to add redundancy to minimize error rate as illustrated in Fig. 1.10.

1.5.3 Channel Coding Gain

The BER is the probability that a binary digit transmitted from the source received erroneously by the user. For required BER, the difference between the powers required for without and with coding is called the coding gain. A typical plot of BER versus E_b/N_0 (bit energy to noise spectral density ratio) with and without channel coding is shown in Fig. 1.11. It can be seen that coding can arrive at the same value of the BER at lower E_b/N_0 than without coding. Thus, the channel coding yields coding gain which is usually measured in dB. Also, the coding gain usually increases with a decrease in BER.

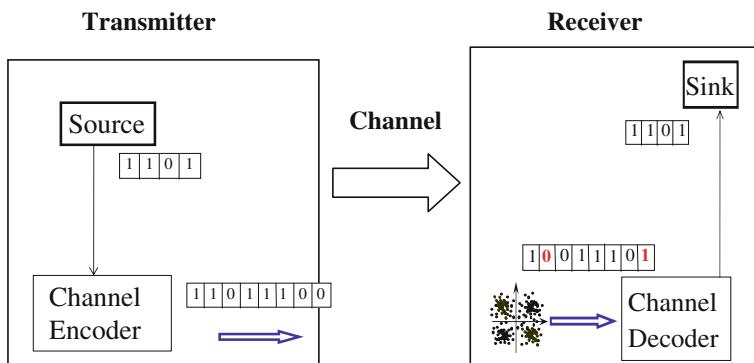


Fig. 1.10 Illustration of channel coding principle

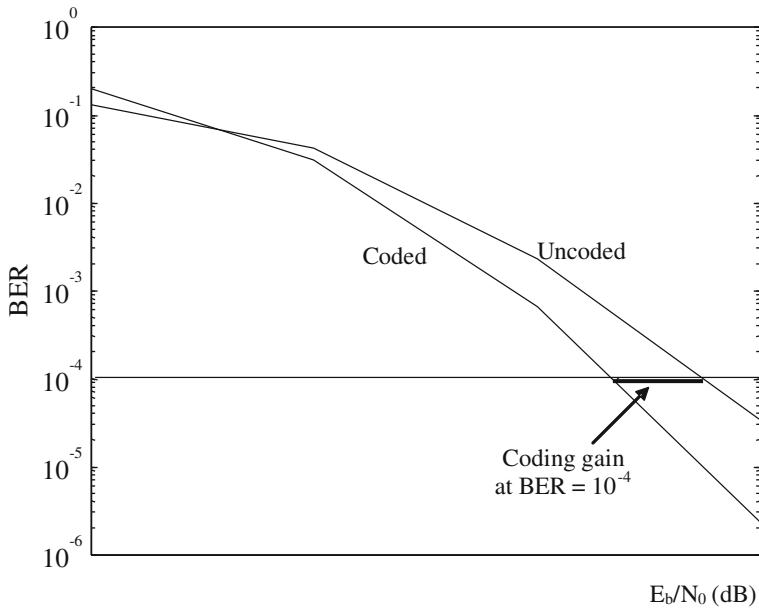


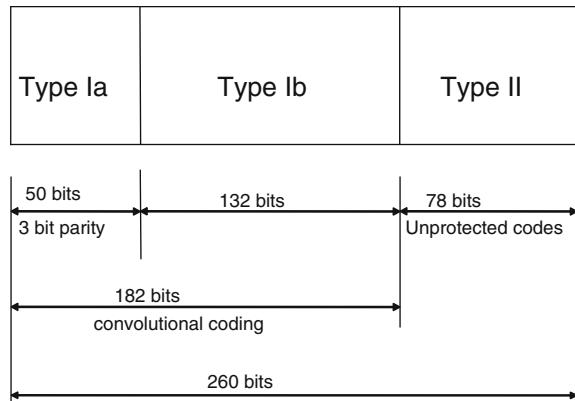
Fig. 1.11 Illustration of coding gain

1.6 Some Application Examples of Channel Coding

1.6.1 Error Correction Coding in GSM

Each speech sample of 20 ms duration is encoded by RPE-LPC as 260 bits with total bit rate of 13 kbps. The 260 bits are classified into three types based on their sensitiveness as shown in Fig. 1.12.

Fig. 1.12 Classification of speech sample 3 in GSM



The 50 bits in Type Ia are the most sensitive to bit errors, the next 132 bits in Type Ib are moderately sensitive to bit errors, and the other 78 bits in Type II do not need any protection. The Type Ia bits are encoded using a cyclic encoder. The Type Ib bits and the encoded Type Ia bits are encoded using convolutional encoder. The Type II bits are finally added to the convolution encoder output bits.

1.6.2 Error Correction Coding in W-CDMA

The W-CDMA standard has defined two error correction coding schemes as shown in Fig. 1.13 for different quality of services. The W-CDMA standard uses convolutional encoding for voice and MPEG4 applications and uses turbo encoding for data applications with longer time delays. The convolutional encoding gives a BER of up to 10^{-3} , and turbo encoding yields a BER of up to 10^{-6} with computational complexity. In Fig. 1.13:

CRC = cyclic redundancy check

DAC = digital-to-analog convertor

NCO = numerically controlled oscillator

OVSF = orthogonal variable spreading factor

RRC = root raised cosine

1.6.3 Digital Video Broadcasting Channel Coding

Convolutional codes concatenated with a Reed-Solomon (RS) code are adopted as physical layer FEC codes in digital video broadcast terrestrial/handheld (DVB-T/H).

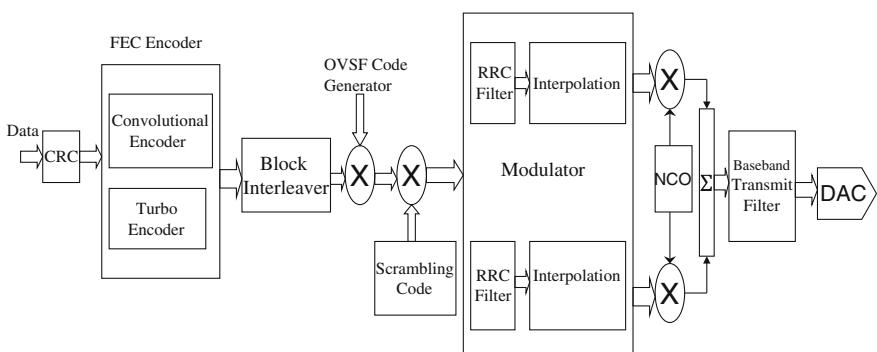


Fig. 1.13 Error correction coding in W-CDMA

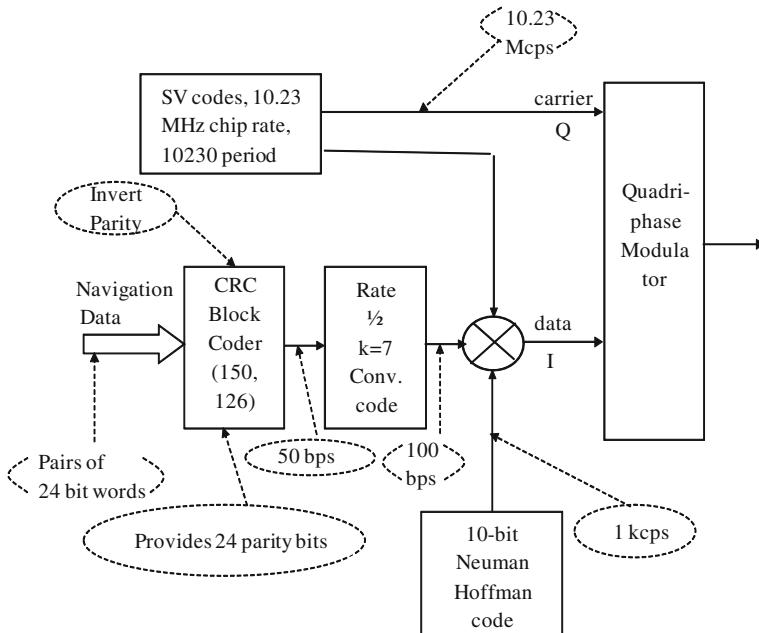


Fig. 1.14 Error correction coding in GPS L5 signal (copy right: 1999 ION)

Turbo codes are used in digital video broadcast satellite services to handhelds/terrestrial (DVB-SH). Low-density parity-check (LDPC) codes concatenated with a Bose-Chaudhuri-Hochquenghem (BCH) code are adopted as physical layer FEC in digital video broadcast second generation satellite (DVB-S2) and digital video broadcast second generation terrestrial (DVB-T2).

1.6.4 Error Correction Coding in GPS L5 Signal

A block diagram of the simplified GPS satellite L5 signal generator [8] is shown in Fig. 1.14. The navigation data is coded in a CRC block coder with a long block of 150 bits or 3 s at 50 bps and provides a 24-bit parity check word for low probability of undetected error. This bit stream is then rate $\frac{1}{2}$ coded using a $K = 7$ convolutional coder for error correction with a soft decision Viterbi decoder in the receiver. This FEC decoding provides approximately 5 dB of coding gain.

References

1. Gilbert, E.N.: Capacity of a burst noise channel. *Bell Syst. Tech. J.* **39**, 1253–1266 (1960)
2. Elliott, E.O.: Estimates for error rates for codes on burst noise channels. *Bell Syst. Tech. J.* **42**, 1977–1997 (1963)
3. Du, K.L., Swamy, M.N.S.: *Wireless Communications: Communication Systems from RF Subsystems to 4G Enabling Technologies*, University Press, Cambridge (2010)
4. Nakagami, M.: The m-distribution: a general formula of intensity distribution of rapid fading. In: Hoffman, W.C. (ed.), *Statistical Methods in Radio Wave Propagation*. Oxford Pergamon Press, pp. 3–36 (1960)
5. Kuhn, V.: *Wireless Communications Over MIMO Channels: Applications to CDMA and Multiple Antenna Systems*. Wiley, Chichester (2006)
6. Ryan, W.E., Lin, S.: *Channel Codes Classical and Modern*. Cambridge University Press, New York (2009)
7. Goldsmith, A.: *Wireless Communications*. Cambridge University Press, Cambridge (2005)
8. Spilker, J.J., Van Dierendonck, A.J.: Proposed New Civil GPS Signal at 1176.45 MHz. In: ION GPS'99, 4–17 Sept. 1999. Nashville, TN

Chapter 2

Performance of Digital Communication Over Fading Channels

In this chapter, bit error rate (BER) performance of some of digital modulation schemes and different wireless communication techniques is evaluated in additive white Gaussian noise (AWGN) and fading channels. Further, the BER performance of different diversity techniques such as selective diversity, EGC, and MRC is also evaluated in Rayleigh fading channel.

2.1 BER Performance of Different Modulation Schemes in AWGN, Rayleigh, and Rician Fading Channels

In this section, the effect of fading is evaluated on different modulation schemes. The bit error probability P_b often referred to as BER is a better performance measure to evaluate a modulation scheme. The BER performance of any digital modulation scheme in a slow flat fading channel can be evaluated by the following integral

$$P_b = \int_0^{\infty} P_{b,\text{AWGN}}(\gamma) P_{df}(\gamma) d\gamma \quad (2.1)$$

where $P_{b,\text{AWGN}}(\gamma)$ is the probability of error of a particular modulation scheme in AWGN channel at a specific signal-to-noise ratio $\gamma = h^2 \frac{E_b}{N_0}$. Here, the random variable h is the channel gain, $\frac{E_b}{N_0}$ is the ratio of bit energy to noise power density in a non-fading AWGN channel, the random variable h^2 represents the instantaneous power of the fading channel, and $P_{df}(\gamma)$ is the probability density function of γ due to the fading channel.

Electronic supplementary material The online version of this chapter (doi:[10.1007/978-81-322-2292-7_2](https://doi.org/10.1007/978-81-322-2292-7_2)) contains supplementary material, which is available to authorized users.

2.1.1 BER of BPSK Modulation in AWGN Channel

It is known that the BER for M-PSK in AWGN channel is given by [1]

$$\text{BER}_{\text{M-PSK}} = \frac{2}{\max(\log_2 M, 2)} \sum_{k=1}^{\max(M/4, 1)} Q\left(\sqrt{\frac{2E_b \log_2 M}{N_0}} \sin \frac{(2k-1)\pi}{M}\right) \quad (2.2)$$

For coherent detection of BPSK, Eq. (2.2) with $M = 2$ reduces to

$$\text{BER}_{\text{BPSK}} = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \quad (2.3)$$

where

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{y^2}{2}\right) dy$$

Equation (2.3) can be rewritten as

$$\text{BER}_{\text{BPSK, AWGN}} = \frac{1}{2} \operatorname{erfc}\left(\sqrt{\frac{E_b}{N_0}}\right) \quad (2.4)$$

where erfc is the complementary error function and $\frac{E_b}{N_0}$ is the bit energy-to-noise ratio. The erfc can be related to the Q function as

$$Q(x) = \frac{1}{2} \operatorname{erfc}\left(\frac{x}{\sqrt{2}}\right) \quad (2.5)$$

For large $\frac{E_b}{N_0}$ and $M > 4$, the BER expression can be simplified as

$$\text{BER}_{\text{M-PSK}} = \frac{2}{\log_2 M} Q\left(\sqrt{\frac{2E_b \log_2 M}{N_0}} \sin \frac{\pi}{M}\right) \quad (2.6)$$

2.1.2 BER of BPSK Modulation in Rayleigh Fading Channel

For Rayleigh fading channels, h is Rayleigh distributed, h^2 has chi-square distribution with two degrees of freedom. Hence,

$$P_{df}(\gamma) = \frac{1}{\bar{\gamma}} \exp\left(-\frac{\gamma}{\bar{\gamma}}\right) \quad (2.7)$$

where $\bar{\gamma} = \frac{E_b}{N_0} E[h^2]$ is the average signal-to-noise ratio. For $E[h^2] = 1$, $\bar{\gamma}$ corresponds to the average $\frac{E_b}{N_0}$ for the fading channel.

By using Eqs. (2.1) and (2.3), the BER for a slowly Rayleigh fading channel with BPSK modulation can be expressed as [2, 3]

$$\text{BER}_{\text{BPSK, Rayleigh}} = \frac{1}{2} \left(1 - \sqrt{\frac{\bar{\gamma}}{1 + \bar{\gamma}}} \right) \quad (2.8)$$

For $E[h^2] = 1$, Eq. (2.8) can be rewritten as

$$\text{BER}_{\text{BPSK, Rayleigh}} = \frac{1}{2} \left(1 - \sqrt{\frac{\frac{E_b}{N_0}}{1 + \frac{E_b}{N_0}}} \right) \quad (2.9)$$

2.1.3 BER of BPSK Modulation in Rician Fading Channel

The error probability estimates for linear BPSK signaling in Rician fading channels are well documented in [4] and is given as

$$P_{b, \text{Rician}} = Q_1(a, b) - \frac{1}{2} \left[1 + \sqrt{\frac{d}{d+1}} \right] \exp\left(-\frac{a^2 + b^2}{2}\right) I_0(ab) \quad (2.10)$$

where

$$a = \left[\sqrt{\frac{K_r^2 [1 + 2d - 2\sqrt{d(d+1)}]}{2(d+1)}} \right], \quad b = \left[\sqrt{\frac{K_r^2 [1 + 2d + 2\sqrt{d(d+1)}]}{2(d+1)}} \right]$$

$$K_r = \frac{\alpha^2}{2\sigma^2}, \quad d = \sigma^2 \frac{E_b}{N_0}.$$

The parameter K_r is the Rician factor. The $Q_1(a, b)$ is the Marcum Q function defined [2] as

$$Q_1(a, b) = \exp\left(-\frac{a^2 + b^2}{2}\right) \sum_{l=0}^{\infty} \left(\frac{a}{b}\right)^l I_0(ab), \quad b \geq a > 0 \quad (2.11)$$

$$Q_1(a, b) = Q(b - a), \quad b \gg 1 \text{ and } b \gg b - a$$

The following MATLAB program is used to illustrate the BER performance of BPSK in AWGN, Rayleigh, and Rician fading channels.

Program 2.1 Program for computing the BER for BPSK modulation in AWGN, Rayleigh, and Rician fading channels

```
clear all;
clc;
M=2;K=5;DIVORDER= 1;
EbNo = 0:5:35;
BER_Ray = BERFADING(EbNo, 'psk', M, DIVORDER);
BER_Rician = BERFADING(EbNo, 'psk', 2, 1, K);
BER = BERAWGN(EbNo, 'psk', M,'nondiff');
semilogy(EbNo,BER,'o-');
hold on
semilogy(EbNo,BER_Ray,'*-');
semilogy(EbNo,BER_Rician,'+-');grid on
legend('AWGN channel','Rayleighchannel','Rician channel');%, 'Rayleigh-Simulation');
xlabel('Eb/No, dB');
ylabel('Bit Error Rate');
axis([ 0 35 1e-5 1 ])
```

The BER performance resulted from the above MATLAB program for BPSK in the AWGN, Rayleigh, and Rician ($K = 5$) channels is depicted in Fig. 2.1.

From Fig. 2.1, for instance, we can see that to obtain a BER of 10^{-4} , using BPSK, an AWGN channel requires $\frac{E_b}{N_0}$ of 8.35 dB, Rician channel requires $\frac{E_b}{N_0}$ of 20.5 dB, and a Rayleigh channel requires $\frac{E_b}{N_0}$ of 34 dB. It is clearly indicative of the large performance difference between AWGN channel and fading channels.

2.1.4 BER Performance of BFSK in AWGN, Rayleigh, and Rician Fading Channels

In BPSK, the receiver provides coherent phase reference to demodulate the received signal, whereas the certain applications use non-coherent formats avoiding a phase reference. This type of non-coherent format is known as binary frequency-shift keying (BFSK).

The BER for non-coherent BFSK in slow flat fading Rician channel is expressed as [3]

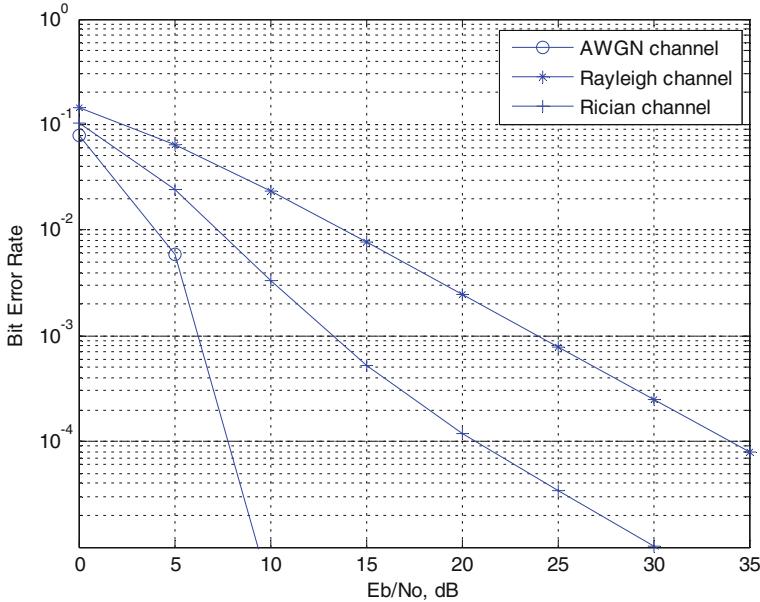


Fig. 2.1 BER performance of BPSK in AWGN, Rayleigh, and Rician fading channels

$$P_{b,\text{BFSK(Ric)}} = \frac{1 + K_r}{2 + 2K_r + \bar{\gamma}} \exp\left(-\frac{K_r \bar{\gamma}}{2 + 2K_r + \bar{\gamma}}\right) \quad (2.12)$$

where K_r is the power ratio between the LOS path and non-LOS paths in the Rician fading channel.

Substituting $K_r = \infty$ in Eq. (2.8), the BER in AWGN channel for non-coherent BFSK can be expressed as

$$P_{b,\text{AWGN}} = \frac{1}{2} \exp\left(-\frac{E_b}{2N_0}\right) \quad (2.13)$$

whereas substitution of $K_r = 0$ leads to the following BER expression for slow flat Rayleigh fading channels using non-coherent BFSK modulation

$$P_{b,\text{BFSK(Ray)}} = \frac{1}{2 + \bar{\gamma}} \quad (2.14)$$

The following MATLAB program is used to illustrate the BER performance of non-coherent BFSK modulation in AWGN, Rayleigh, and Rician fading channels.

Program 2.2 Program for computing the BER for BFSK modulation in AWGN, Rayleigh and Rician fading channels

```

clear all;
clc;
Eb_N0_dB = [0:5:35];
K=5;
EbN0Lin = 10.^Eb_N0_dB/10;
theoryBerAWGN = 0.5*exp(-0.5*EbN0Lin); % theoretical ber
for i=1:8
    theoryBer(i) = 1/(EbN0Lin(i)+2);
    theoryberric(i)=((1+K)/(EbN0Lin(i)+2+2*K))*exp(-
    K*EbN0Lin(i)/(EbN0Lin(i)+2+2*K));
end
semilogy(Eb_N0_dB,theoryBerAWGN,'o','LineWidth',2);
hold on
semilogy(Eb_N0_dB,theoryBer,'-*','LineWidth',2);
semilogy(Eb_N0_dB,theoryberric,'+', 'LineWidth',2);
axis([0 35 10^-6 0.5])
grid on
legend('AWGN channel','Rayleighchannel','Rician channel');%, 'Rayleigh-
Simulation');
xlabel('Eb/No, dB');
ylabel('Bit Error Rate');

```

The BER performance resulted from the MATLAB program 2.2 for non-coherent BFSK in the AWGN, Rayleigh, and Rician ($K = 5$) channels is depicted in Fig. 2.2.

2.1.5 Comparison of BER Performance of BPSK, QPSK, and 16-QAM in AWGN and Rayleigh Fading Channels

The BER of gray-coded M-QAM in AWGN channel can be more accurately computed by [5]

$$\text{BER}_{\text{16QAM, AWGN}} \approx \frac{4}{\log_2 M} \left(1 - \frac{1}{\sqrt{M}} \right) \sum_{i=1}^{\frac{\sqrt{M}}{2}} Q\left(\sqrt{\frac{3 \log_2 M E_b}{(M-1) N_0}} \right) \quad (2.15)$$

In Rayleigh fading, the average BER for M-QAM is given by [6]

$$\text{BER}_{\text{MQAM, AWGN}} \approx \frac{2}{\log_2 M} \left(1 - \frac{1}{\sqrt{M}} \right) \sum_{i=1}^{\frac{\sqrt{M}}{2}} \left(1 - \sqrt{\frac{1.5(2i-1)^2 \bar{\gamma} \log_2 M}{M-1 + 1.5(2i-1)^2 \bar{\gamma} \log_2 M}} \right) \quad (2.16)$$

The following MATLAB program 2.3 is used to compute theoretic BER performance of 4-QAM, 8-QAM, and 16-QAM modulations in AWGN and Rayleigh fading channels.

Program 2.3 Program for computing theoretic BER for 4-QAM, 8-QAM and 16-QAM modulations in AWGN and Rayleigh fading channels

```

clear all;
Eb_N0_dB = [0:35]; % multiple Eb/N0 values
EbN0Lin = 10.^Eb_N0_dB/10;
M=4;
BER_4QAM_AWGN = 0.5* erfc( sqrt( EbN0Lin ) );
BER_4QAM_Rayleigh = 0.5.*(1-1*(1+1./EbN0Lin).^( -0.5));
M=8;
BER_8QAM_AWGN = 4/log2(M) * (1-1/sqrt(M))*( 0.5*erfc( sqrt( 3/2* log2(M) *EbN0Lin / (M-1) ) ) + ... 0.5 * erfc( 3* sqrt( 3/2* log2(M) *EbN0Lin / (M-1) ) ) );
BER_8QAM_Rayleigh = (2/log2(M)) * ( 1 - 1/sqrt(M) )*((1- 1*(1+7./(4.5*EbN0Lin)).^( -0.5))+... (1-1*(1+7./(40.5*EbN0Lin)).^( -0.5)));
M=16;
BER_16QAM_AWGN = 4/log2(M) * ( 1 - 1/sqrt(M) ) * ( 0.5 * erfc( sqrt( 3/2* log2(M) *EbN0Lin / (M-1) ) ) + ...0.5 * erfc( 3* sqrt( 3/2* log2(M) *EbN0Lin / (M-1) ) ) );
BER_16QAM_Rayleigh = 2/log2(M) * ( 1 - 1/sqrt(M) )*((1- 1*(1+15./(6*EbN0Lin)).^( -0.5))+... (1-1*(1+15./(54*EbN0Lin)).^( -0.5)));
close all
Figure
semilogy(Eb_N0_dB,BER_16QAM_Rayleigh,'-*','LineWidth',2);
hold on
semilogy(Eb_N0_dB,BER_8QAM_Rayleigh ,'-','LineWidth',2);
semilogy(Eb_N0_dB,BER_4QAM_Rayleigh ,'-x','LineWidth',2);
semilogy(Eb_N0_dB,BER_16QAM_AWGN,'--','LineWidth',2);
semilogy(Eb_N0_dB,BER_8QAM_AWGN,'-v','LineWidth',2);
semilogy(Eb_N0_dB,BER_4QAM_AWGN ,'-d','LineWidth',2);
axis([0 35 10^-8 1])
grid on
legend('16-QAM Rayleigh','8-QAM Rayleigh','4-QAM Rayleigh','16QAM AWGN','8QAM AWGN','4-QAM AWGN');
xlabel('Eb/No, dB');
ylabel('BER');

```

The BER performance obtained from the above program is depicted in Fig. 2.3.

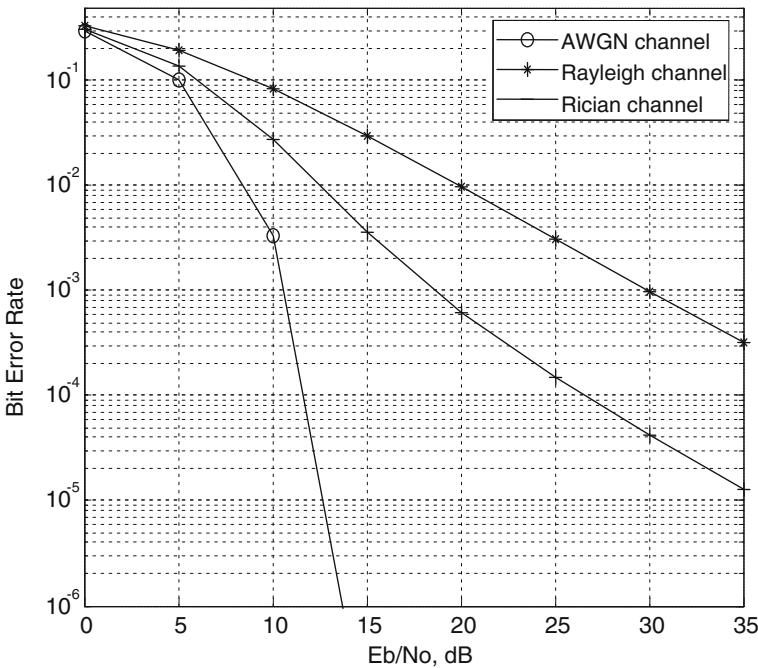


Fig. 2.2 BER performance of BFSK in AWGN, Rayleigh, and Rician fading channels

2.2 Wireless Communication Techniques

The most known wireless communication techniques are:

- Direct sequence code division multiple access (DS-CDMA)
- Frequency hopping CDMA (FH-CDMA)
- Orthogonal frequency division multiplexing (OFDM)
- Multicarrier CDMA (MC-CDMA)

2.2.1 DS-CDMA

In code division multiple access (CDMA) systems, the narrow band message signal is multiplied by a very high bandwidth signal, which has a high chip rate, i.e., it accommodates more number of bits in a single bit of message signal. The signal with a high chip rate is called as spreading signal. All users in the CDMA system use the same carrier frequency and transmit simultaneously. The spreading signal or pseudo-noise code must be random so that no other user could be recognized.

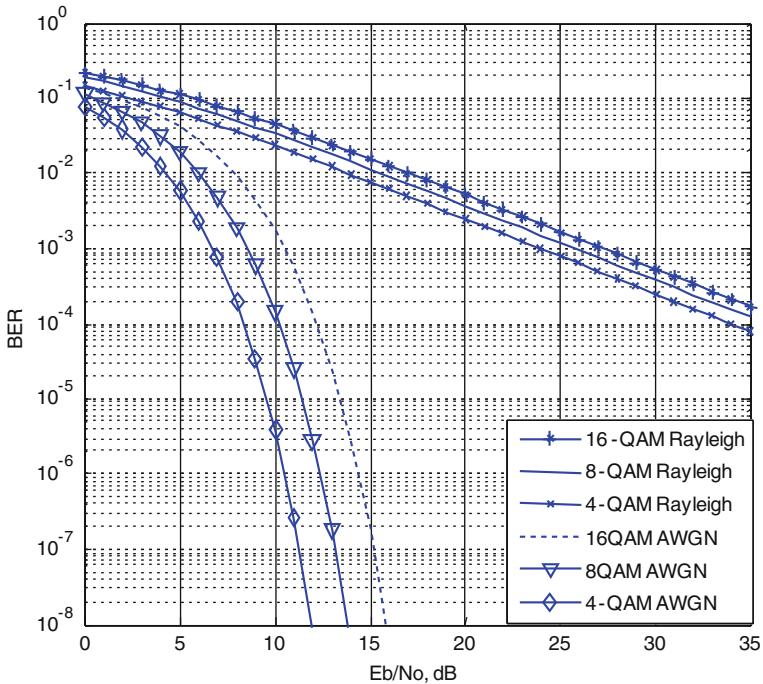


Fig. 2.3 BER performances of 4-QAM, 8-QAM, and 16-QAM in AWGN and Rayleigh fading channels

The intended receiver works with same PN code which is used by the corresponding transmitter, and time correlation operation detects the specific desired codeword only and all other code words appear as noise. Each user operates independently with no knowledge of the other users.

The near-far problem occurs due to the sharing of the same channel by many mobile users. At the base station, the demodulator is captured by the strongest received mobile signal raising the noise floor for the weaker signals and decreasing the probability of weak signal reception. In most of the CDMA applications, power control is used to combat the near-far problem. In a cellular system, each base station provides power control to assure same signal level to the base station receiver from each mobile within the coverage area of the base station and solves the overpowering to the base station receiver by a nearby user drowning out the signals of faraway users.

In CDMA, the actual data are mixed with the output of a PN coder to perform the scrambling process. The scrambled data obtained after scrambling process are then modulated using BPSK or QPSK modulator as shown in Fig. 2.4. The BPSK or QPSK modulated data are then transmitted.

2.2.1.1 BER Performance of DS-CDMA in AWGN and Rayleigh Fading Channels

Let us consider a single cell with K users with each user having a PN sequence length N chips per message symbol. The received signal will consist of the sum of the desired user, $K - 1$ undesired users transmitted signals and additive noise. Approximating the total multiple access interference caused by the $K - 1$ users as a Gaussian random variable, the BER for DS-CDMA in AWGN channel is given [3] by

$$P_{b, \text{CDMA (AWGN)}} = Q\left(\frac{1}{\sqrt{\frac{K-1}{3N} + \frac{N_0}{2E_b}}}\right) \quad (2.17)$$

The BER for DS-CDMA in Rayleigh fading channel can be expressed [7] as

$$P_{b, \text{CDMA(Ray)}} = \frac{1}{2} \left(1 - \frac{1}{\sqrt{1 + \frac{N_0}{2E_b\sigma^2} + \frac{K-1}{3N}}} \right) \quad (2.18)$$

where σ^2 is the variance of the Rayleigh fading random variable.

The following MATLAB program is used to compute theoretic BER of DS-CDMA in AWGN and Rayleigh fading channels.

Program 2.4 Program to compute BER performance of DS-CDMA in AWGN, and Rayleigh fading channels

```
clearall;clc;close all;
Eb_N0_dB=10;
EbN0Lin = 10.^((Eb_N0_dB/10));
N=31;
for k=3:30
    xx(k)=1/sqrt(((k-1)/(3*N))+0.5*1/(EbN0Lin));
    xxf(k)=sqrt(1+((k-1)/N)+0.5*1/(EbN0Lin));
    beredma(k)=0.5*erfc(xx(k)/sqrt(2));
    bercdmaf(k)=0.5-0.5/xxf(k);
end
semilogy(3:30,beredma(3:30),'-*')
hold on
semilogy(3:30,bercdmaf(3:30),'-+')
legend('AWGN channel','Rayleigh channel');
xlabel('Number of users');
ylabel('Bit Error Rate');
```

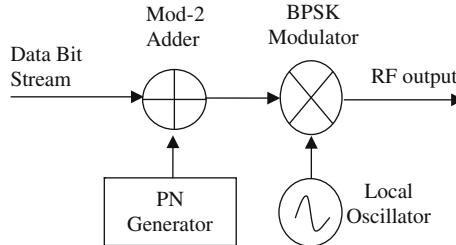


Fig. 2.4 Scrambler system using BPSK modulation

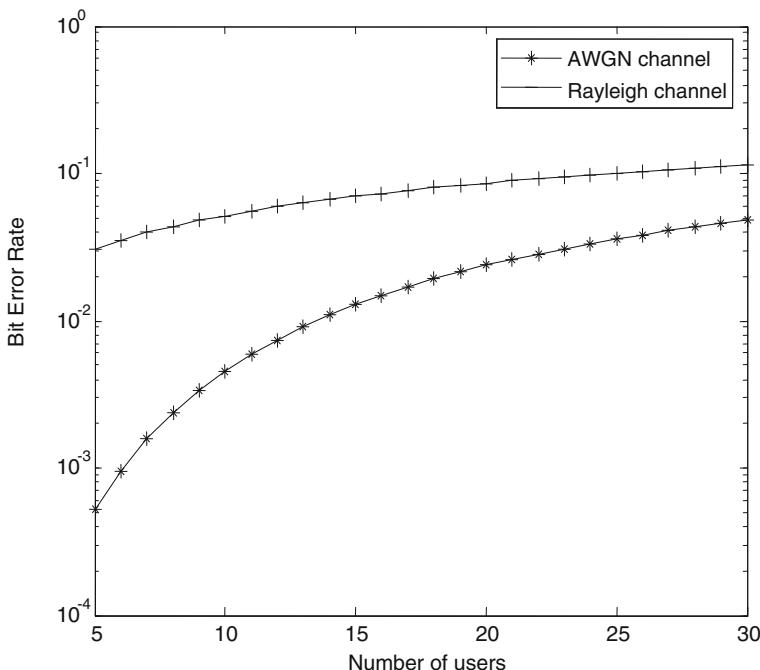


Fig. 2.5 BER performance of DS-CDMA in AWGN and Rayleigh fading channels for $N = 31$, $\sigma^2 = 1$, and $\frac{E_b}{N_0} = 10 \text{ dB}$

The BER performance from the above program for DS-CDMA in the AWGN and Rayleigh channels for $N = 31$, $\sigma^2 = 1$, and $\frac{E_b}{N_0} = 20 \text{ dB}$ is depicted in Fig. 2.5.

From Fig. 2.5, it is observed that the BER performance of DS-CDMA is better in AWGN channel as compared to Rayleigh fading channel. Further, with an increased number of users, the BER performance decreases in both the channels.

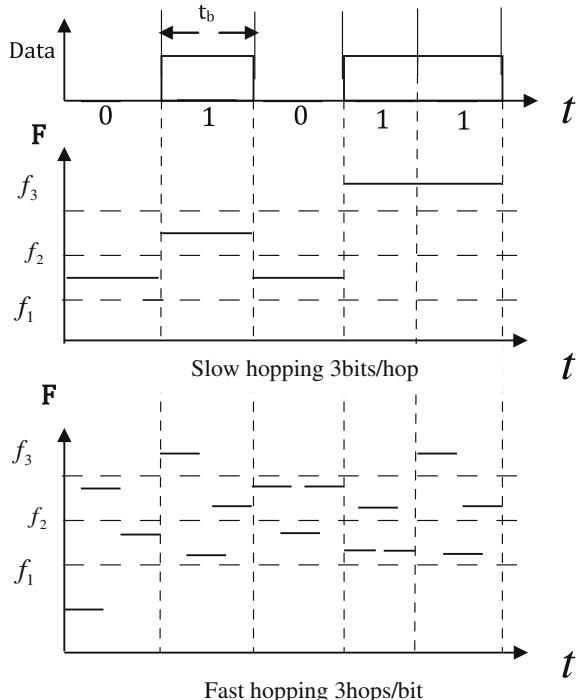
2.2.2 FH-CDMA

In FH-CDMA, each data bit is divided over a number of frequency-hop channels (carrier frequencies). At each frequency-hop channel, a complete PN sequence of length N is combined with the data signal. Applying fast frequency hopping (FFH) requires a wider bandwidth than slow frequency hopping (SFH). The difference between the traditional slow and FFH schemes can be visualized as shown in Fig. 2.6. A slow hopped system has one or more information symbols per hop or slot. It is suitable for high-capacity wireless communications. A fast hopped system has the hopping rate greater than the data rate. During one information symbol, the system transmits over many bands with short duration. It is more prevalent in military communications.

In FH-CDMA, modulation by some kind of the phase-shift keying is quite susceptible to channel distortions due to several frequency hops in each data bit. Hence, an FSK modulation scheme is to be chosen for FH-CDMA.

- Hop set* It is the number of different frequencies used by the system.
- Dwell time* It is defined as the length of time that the system spent on one frequency for transmission.
- Hop rate* It is the rate at which the system changes from one frequency to another.

Fig. 2.6 Slow and fast hopping



2.2.2.1 BER Expression for Synchronous SFH-CDMA

Consider a SFH-CDMA channel with K active users and q (frequency) slots. The hit probability is the probability that a number of interfering users are transmitting on the same frequency-hop channel as the reference user. This probability will be referred to as $P_h(K)$ where K is the total number of active users.

The probability of hitting from a given user is given by [8]

$$P = \frac{1}{q} \left(1 + \frac{1}{N_b} \right) \quad (2.19)$$

where N_b is the number of bits per hop and q stands for the number of hops. The primary interest for our analysis is the probability P_h of one or more hits from the $K - 1$ users is given by

$$P_h = 1 - (1 - P)^{K-1} \quad (2.20)$$

By substituting “ P ” value from Eq. (2.19) in Eq. (2.20), we get the probability of hit from $K - 1$ users as

$$P_h(K) = 1 - \left(1 - \frac{1}{q} \left(1 + \frac{1}{N_b} \right) \right)^{K-1} \quad (2.21)$$

If it is assumed that all users hop their carrier frequencies synchronously, the probability of hits is given by

$$P_h = 1 - \left(1 - \frac{1}{q} \right)^{K-1} \quad (2.22)$$

For large q ,

$$P_h(K) = 1 - \left(1 - \frac{1}{q} \right)^{K-1} \approx \frac{K-1}{q} \quad (2.23)$$

The probability of bit error for synchronous MFSK SFH-CDMA when the K number of active users is present in the system can be found by [9]

$$P_{\text{SFH}}(K) = \sum_{k=1}^K \binom{K-1}{k} P_h^k (1 - P_h)^{K-1-k} P_{\text{MFSK}}(K) \quad (2.24)$$

where $P_{\text{MFSK}}(K)$ denotes the probability of error when the reference user is hit by all other active users. Equation (2.24) is the upper bound of the bit error probability of the SFH-CDMA system. The $P_{\text{MFSK}}(K)$ for the AWGN and flat fading channels can be expressed as [10]

$$P_{\text{MFSK}}(K) = \begin{cases} \sum_{i=1}^{M-1} \frac{(-1)^{i+1}}{i+1} \binom{M-1}{i} \exp\left(-\frac{\frac{E_b}{N_0}}{i+1}\right) \text{AWGN} \\ \sum_{i=1}^{M-1} \frac{(-1)^{i+1}}{1+i+\frac{E_b}{N_0}} \binom{M-1}{i} \quad \text{Rayleigh fading} \end{cases} \quad (2.25)$$

The following MATLAB program computes theoretic BER of SFH-CDMA in AWGN and Rayleigh fading channels.

Program 2.5 Program to compute BER performance of SFH-CDMA in AWGN, and Rayleigh fading channels

```
clearall;clc;
snr1=10;Eb_N0_dB=10;
EbN0Lin = 10.^ (Eb_N0_dB/10);
q=32;
pe=0.5*exp(-(EbN0Lin /2));
for K=3:30
ph=(K-1)/q;
pe1=0;
for k=1:(K-1)
    pe1=pe1+nchoosek(K-1,k)*(ph)^k*(1-ph)^(K-1-k);
end
pesfh(K)=pe1*pe;
end
disp(pesfh);
semilogy(3:30,pesfh(3:30),'-*');
hold on;
pe=1/(2+EbN0Lin );
for K=3:30
ph=(K-1)/q;
pe1=0;
for k=1:(K-1)
    pe1=pe1+nchoosek(K-1,k)*(ph)^k*(1-ph)^(K-1-k);
end
pesfhr(K)=pe1*pe;
end
disp(pesfhr);
semilogy(3:30,pesfhr(3:30),'-+');
hold on;
legend('AWGN','Rayleigh');
xlabel('Number of users');
ylabel('Bit Error Rate');
```

The BER performance from the above program for SFH-CDMA in the AWGN and Rayleigh channels with $q = 32$ and $M = 2$ (BFSK) at $\frac{E_b}{N_0} = 10 \text{ dB}$ is depicted in Fig. 2.7.

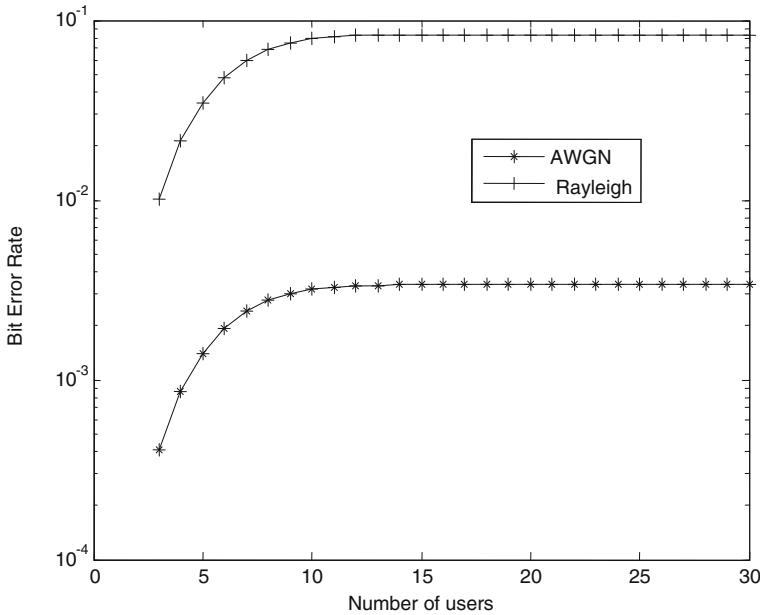


Fig. 2.7 BER performance of SFH-CDMA in AWGN and Rayleigh fading channels with $q = 32$ and $M = 2$ (BFSK) at $\frac{E_b}{N_0} = 10 \text{ dB}$

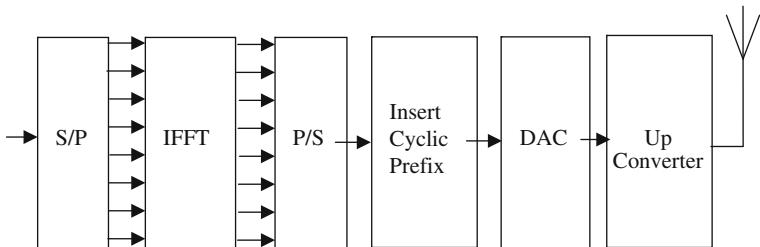


Fig. 2.8 Schematic block diagram of OFDM transmitter

2.2.3 OFDM

The block diagram of OFDM transmitter is shown in Fig. 2.8. In OFDM, the input data are serial-to-parallel converted (the S/P block). Then, the inverse fast Fourier transform (IFFT) is performed on the N parallel outputs of the S/P block to create an OFDM symbol.

The complex numbers in the output of the IFFT block are parallel-to-serial converted (P/S). Then, the cyclic prefix is inserted in order to combat the

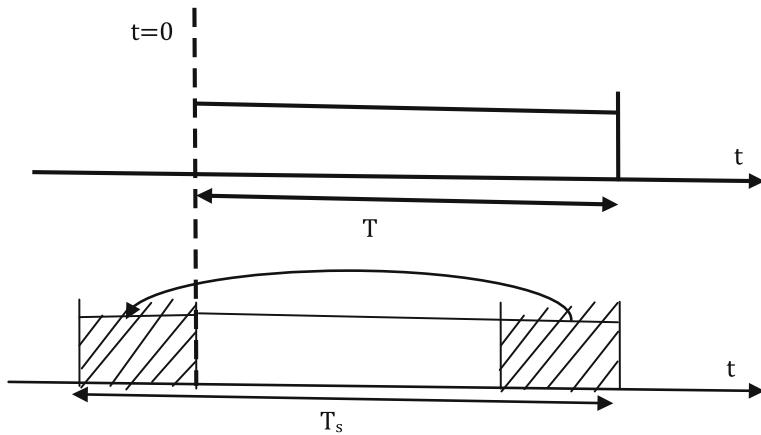


Fig. 2.9 Inserting cyclic prefix

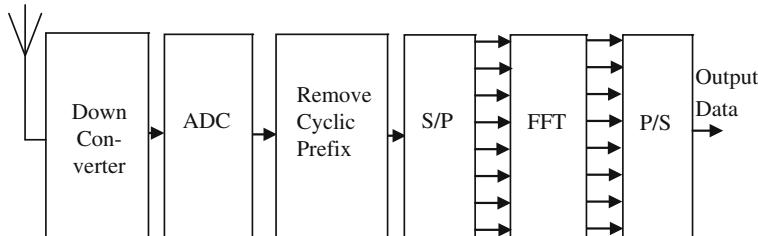


Fig. 2.10 Schematic block diagram of OFDM receiver

intersymbol interference (ISI) and intercarrier interference (ICI) caused by the multipath channel. To create the cyclic prefix, the complex vector of length at the end of the symbol duration T is copied and appended to the front of the signal block as shown in Fig. 2.9. The schematic block diagram of the OFDM receiver is shown in Fig. 2.10. It is the exact inverse of the transmitter shown in Fig. 2.8.

2.2.4 MC-CDMA

MC-CDMA is a combination of OFDM and CDMA having the benefits of both OFDM and CDMA. In MC-CDMA, frequency diversity is achieved by modulating symbols on many subcarriers instead of modulating on one carrier like in CDMA.

In MC-CDMA, the same symbol is transmitted through many subcarriers in parallel, whereas in OFDM, different symbols are transmitted on different subcarriers. The block diagram of the MC-CDMA system transmitter is shown in Fig. 2.11. The block diagram of the MC-CDMA system receiver is shown in Fig. 2.12. In the

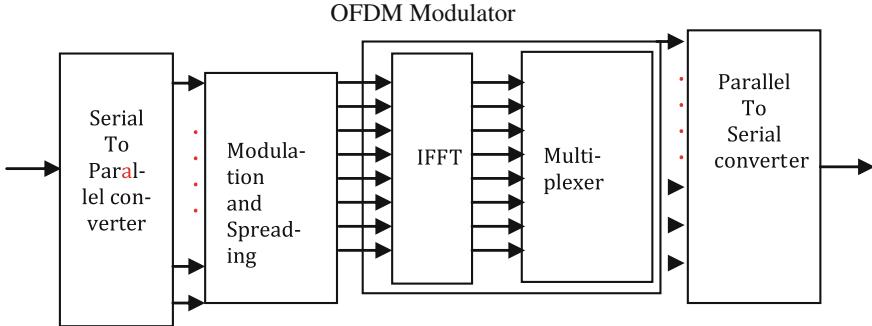


Fig. 2.11 Block diagram of MC-CDMA transmitter

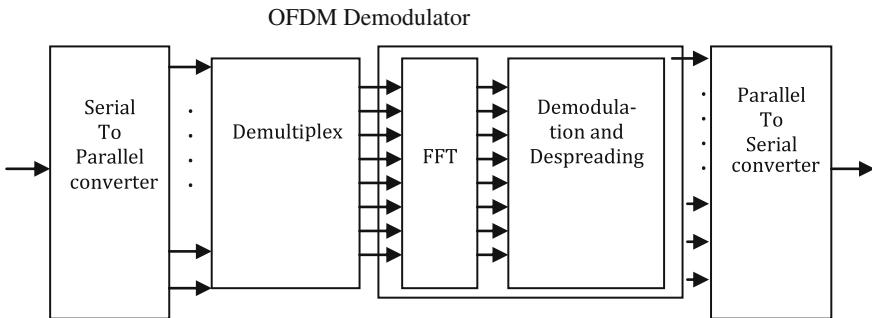


Fig. 2.12 Block diagram of MC-CDMA receiver

receiver, the cyclic prefix is removed and FFT is performed to obtain the signals in the frequency domain.

2.2.4.1 BER Expression for Synchronous MC-CDMA

Assuming a synchronous MC-CDMA system with K users, N subcarriers, and binary phase-shift keying (BPSK) modulation, the BER for MC-CDMA in slowly varying Rayleigh fading channel can be calculated using the residue method by [11]

$$P_{\text{MC-CDMA, Rayleigh}}(K) = \frac{(2c)^{N_c}}{[(N_c - 1)!]^2} \sum_{k=0}^{N_c-1} \binom{N_c - 1}{k} (N_c - 1 - k)! (c + d)^{-(N_c - k)} (2d)^{-(N_c + k)} \quad (2.26)$$

where k stands for the number of users, N_c denotes the number of subcarriers, and the parameters c and d are defined by

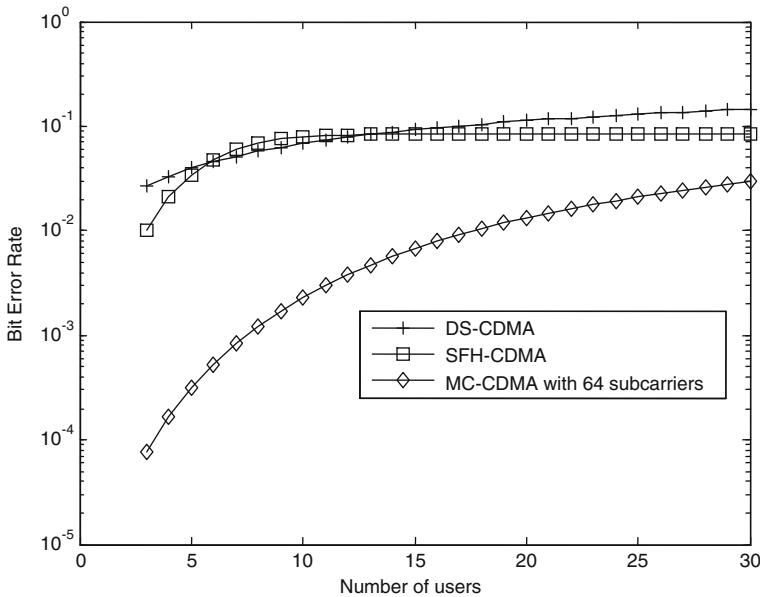


Fig. 2.13 BER performance of DS-CDMA, SFH-CDMA, and MC-CDMA in Rayleigh fading channels at $\frac{E_b}{N_0} = 10 \text{ dB}$

$$\frac{1}{2c} = \frac{N_c}{4E_b/N_0} + \frac{k+1}{4}, \quad d = \sqrt{c^2 + 2c} \quad (2.27)$$

A theoretical BER performance comparison of DS-CDMA, SFH-CDMA, and MC-CDMA in Rayleigh fading channels at $\frac{E_b}{N_0} = 10 \text{ dB}$ is shown in Fig. 2.13.

From Fig. 2.13, it is observed that MC-CDM outperforms both the DS-CDMA and SFH-CDMA.

2.3 Diversity Reception

Two channels with different frequencies, polarizations, or physical locations experience fading independently of each other. By combining two or more such channels, fading can be reduced. This is called diversity.

On a fading channel, the SNR at the receiver is a random variable, the idea is to transmit the same signal through r separate fading channels. These are chosen so as to provide the receiver with r independent (or close-to-independent) replicas of the same signal, giving rise to independent SNRs. If r is large enough, then at any time instant, there is a high probability that at least one of the signals received from the

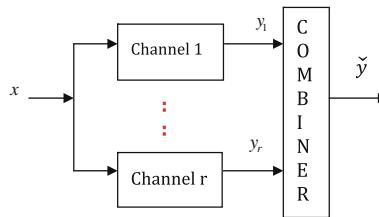


Fig. 2.14 Diversity and combining

r “diversity branches” is not affected by a deep fade and hence that its SNR is above a critical threshold. By suitably combining the received signals, the fading effect will be mitigated (Fig. 2.14).

Many techniques have been advocated for generating the independent channels on which the diversity principle is based, and several methods are known for combining the signals y_1, \dots, y_r obtained at their outputs into a single channel \hat{y} . Among the categorized techniques, the most important ones are as follows:

1. Space diversity
2. Polarization diversity
3. Frequency diversity
4. Time diversity
5. Cooperative diversity

Space diversity: To obtain sufficient correlation, the spacing between the r separate antennas should be wide with respect to their coherent distance while receiving the signal. It does not require any extra spectrum occupancy and can be easily implemented.

Polarization diversity: Over a wireless channel, multipath components polarized either horizontally or vertically have different propagation. Diversity is provided when the receiving signal uses two different polarized antennas. In another way, two cross-polarized antennas with no spacing between them also provide diversity. Cross-polarized are preferred since they are able to double the antenna numbers using half the spacing being used for co-polarized antennas. Polarized diversity can achieve more gain than space diversity alone in reasonable scattering areas, and hence, it is deployed in more and more BSs.

Frequency diversity: In order to obtain frequency diversity, the same signal over different carrier frequencies should be sent whose separation must be larger than the coherence bandwidth of the channel.

Time diversity: This is obtained by transmitting the same signal in different time slots separated by a longer interval than the coherence time of the channel.

Cooperative diversity: This is obtained by sharing of resources by users or nodes in a wireless network and transmits cooperatively. The users or nodes act like an antenna array and provide diversity. This type of diversity can be achieved by combining the signals transmitted from the direct and relay links.

2.3.1 Receive Diversity with N Receive Antennas in AWGN

The received signal on the i th antenna can be expressed as

$$y_i = h_i x + \eta_i \quad (2.28)$$

where

y_i is the symbol received on the i th receive antenna,

h_i is the channel gain on the i th receive antenna,

x is the input symbol transmitted, and

η_i is the noise on the i th receive antenna.

The received signal can be written in matrix form as

$$\mathbf{y} = \mathbf{h}\mathbf{x} + \mathbf{n}$$

where

$\mathbf{y} = [y_1 y_2 \dots y_N]^T$ is the received symbol from all the receive antenna,

$\mathbf{h} = [h_1 h_2 \dots h_N]^T$ is the channel on all the receive antenna,

\mathbf{x} is the transmitted symbol, and

$\mathbf{n} = [\eta_1 \eta_2 \dots \eta_N]^T$ is the AWGN on all the receive antenna.

Effective $\frac{E_b}{N_0}$ with N receive antennas is N times $\frac{E_b}{N_0}$ for single antenna. Thus, the effective $\frac{E_b}{N_0}$ for N antennas in AWGN can be expressed as

$$\left[\frac{E_b}{N_0} \right]_{\text{eff},N} = \frac{NE_b}{N_0} \quad (2.29)$$

So the BER for N receive antennas is given by

$$P_b = \frac{1}{2} \operatorname{erfc} \left(\sqrt{\frac{NE_b}{N_0}} \right) \quad (2.30)$$

2.4 Diversity Combining Techniques

The three main combining techniques that can be used in conjunction with any of the diversity schemes are as follows:

1. Selection combining
2. Equal gain combining (EGC)
3. Maximal ratio combining

2.4.1 Selection Diversity

In this combiner, the receiver selects the antenna with the highest received signal power and ignores observations from the other antennas.

2.4.1.1 Expression for BER with Selection Diversity

Consider N independent Rayleigh fading channels, each channel being a diversity branch. It is assumed that each branch has the same average signal-to-noise ratio

$$\bar{\gamma} = \frac{E_b}{N_0} E[h^2] \quad (2.31)$$

The outage probability is the probability that the bit energy-to-noise ratio falls below a threshold (γ). The probability of outage on i th receive antenna can be expressed by

$$P_{\text{out},\gamma_i} = P[\gamma_i < \gamma] = \int_0^\gamma \frac{1}{\bar{\gamma}} e^{-\frac{\gamma_i}{\bar{\gamma}}} d\gamma_i = 1 - e^{-\frac{\gamma_i}{\bar{\gamma}}} \quad (2.32)$$

The joint probability is the product of the individual probabilities if the channel on each antenna is assumed to be independent; thus, the joint probability with N receiving antennas becomes

$$\begin{aligned} P_{\text{out}} &= P[\gamma_1 < \gamma] P[\gamma_2 < \gamma] \cdots P[\gamma_N < \gamma] \\ &= \left[1 - e^{-\frac{\gamma_i}{\bar{\gamma}}} \right]^N \end{aligned} \quad (2.33)$$

where $\gamma_1, \gamma_2, \dots, \gamma_N$ are the instantaneous bit energy-to-noise ratios of the 1st, 2nd, and so on till the n th receive antenna.

Equation (2.33) is in fact the cumulative distribution function (CDF) of γ . Then, the probability density function (PDF) is given by the derivate of the CDF as

$$P(\gamma) = \frac{dP_{\text{out}}}{d\gamma} = \frac{N}{\bar{\gamma}} e^{-\frac{\gamma}{\bar{\gamma}}} \left[1 - e^{-\frac{\gamma}{\bar{\gamma}}} \right]^{N-1} \quad (2.34)$$

Substituting Eq. (2.34) in Eq. (2.1), BER for selective diversity can be expressed by

$$\text{BER}_{\text{SEL}} = \int_0^\infty \frac{1}{2} \operatorname{erfc}(\sqrt{\gamma}) \frac{N}{\bar{\gamma}} e^{-\frac{\gamma}{\bar{\gamma}}} \left[1 - e^{-\frac{\gamma}{\bar{\gamma}}} \right]^{N-1} d\gamma \quad (2.35)$$

Assuming $\alpha^2 = 1$, the above expression can be rewritten as [12]

$$\text{BER}_{\text{SEL}} = \frac{1}{2} \sum_{k=0}^N (-1)^k \binom{N}{k} \left(1 + \frac{k}{\left(\frac{E_b}{N_0}\right)} \right)^{-\frac{1}{2}} \quad (2.36)$$

2.4.2 Equal Gain Combining (EGC)

In EGC, equalization is performed on the i th receive antenna at the receiver by dividing the received symbol y_i by the a priori known phase of channel h_i . $|h_i|e^{j\theta_i}$ represents the channel h_i in polar form. The decoded symbol is obtained by

$$\hat{y} = \sum_i \frac{y_i}{e^{j\theta_i}} = \sum_i \frac{|h_i|e^{j\theta_i}x + \eta_i}{e^{j\theta_i}} = \sum_i |h_i|x + \tilde{\eta}_i \quad (2.37)$$

where

\hat{y} is the sum of the phase compensated channel from all the receiving antennas and

$\tilde{\eta}_i = \frac{\eta_i}{e^{j\theta_i}}$ is the additive noise scaled by the phase of the channel coefficient.

2.4.2.1 Expression for BER with Equal Gain Combining

The BER with EGC with two receive antennas can be expressed with BPSK and BFSK modulations as [13]

$$\text{BER}_{\text{EGC,BPSK}} = \frac{1}{2} \left[1 - \frac{\sqrt{E_b/N_0(E_b/N_0 + 2)}}{E_b/N_0 + 1} \right] \quad (2.38)$$

$$\text{BER}_{\text{EGC,BFSK}} = \frac{1}{2} \left[1 - \frac{\sqrt{E_b/N_0(E_b/N_0 + 4)}}{E_b/N_0 + 2} \right] \quad (2.39)$$

2.4.3 Maximum Ratio Combining (MRC)

2.4.3.1 Expression for BER with Maximal Ratio Combining (MRC)

For channel h_i , the instantaneous bit energy-to-noise ratio at i th receive antenna is given by

$$\gamma_i = \frac{|h_i|^2 E_b}{N_0}, \quad (2.40)$$

If h_i is a Rayleigh distributed random variable, then h_i^2 is a chi-squared random variable with two degrees of freedom. Hence, the p_{df} of γ_i can be expressed as

$$P_{df}(\gamma_i) = \frac{1}{(E_b/N_0)} e^{\frac{-\gamma_i}{(E_b/N_0)}} \quad (2.41)$$

Since the effective bit energy-to-noise ratio γ is the sum of N such random variables, the p_{df} of γ is a chi-square random variable with $2N$ degrees of freedom. Thus, the p_{df} of γ is given by

$$P_{df}(\gamma) = \frac{1}{(N-1)!(E_b/N_0)^N} \gamma^{N-1} e^{\frac{-\gamma}{(E_b/N_0)}} , \quad \gamma \geq 0 \quad (2.42)$$

Substituting Eq. (2.42) in Eq. (2.1), BER for maximal ratio combining can be expressed by

$$\begin{aligned} \text{BER}_{\text{MRC}} &= \int_0^\infty \frac{1}{2} \operatorname{erfc}(\sqrt{\gamma}) P_{df}(\gamma) d\gamma \\ &= \int_0^\infty \frac{1}{2} \operatorname{erfc}(\sqrt{\gamma}) \frac{1}{(N-1)!(E_b/N_0)^N} \gamma^{N-1} e^{\frac{-\gamma}{(E_b/N_0)}} d\gamma \end{aligned} \quad (2.43)$$

The above expression can be rewritten [12] as

$$\text{BER}_{\text{MRC}} = P^N \sum_{k=0}^{N-1} \binom{N-1+k}{k} (1-P)^k \quad (2.44)$$

where

$$P = \frac{1}{2} - \frac{1}{2} \left(1 + \frac{1}{E_b/N_0} \right)^{-1/2}$$

The following MATLAB program computes the theoretic BER for BPSK modulation in Rayleigh fading channels with selective diversity, EGC, and MRC.

Program 2.6 Program for computing the theoretic BER for BPSK modulation in a Rayleigh fading channel with selection diversity, EGC and MRC

```

clear all;
Eb_N0_dB = [0:20]; % multiple Eb/N0 values
EbNOLin = 10.^Eb_N0_dB/10;
theoryBer_nRx1 = 0.5.*(1-1*(1+1./EbNOLin).^(0.5));
theoryBer_sel_nRx2 = 0.5.*(1-2*(1+1./EbNOLin).^(0.5)) + (1+2./EbNOLin).^(0.5);
theoryBer_EG_nRx2 = 0.5*(1- sqrt(EbNOLin.* (EbNOLin+2))./(EbNOLin+1));
p = 1/2 - 1/2*(1+1./EbNOLin).^(1/2);
theoryBer_MRC_nRx2 = p.^2.* (1+2*(1-p));
semilogy(Eb_N0_dB, theoryBer_nRx1,'*','LineWidth',2);
hold on
semilogy(Eb_N0_dB, theoryBer_sel_nRx2,'-','LineWidth',2);
semilogy(Eb_N0_dB, theoryBer_EG_nRx2,'-+','LineWidth',2);
semilogy(Eb_N0_dB, theoryBer_MRC_nRx2,'--','LineWidth',2);
axis([0 20 10^-5 0.5])
gridon
legend('Rayleigh','selection(nRx=2)', 'EGC(nRx=2)', 'MRC(nRx=2)');
xlabel('Eb/No, dB');
ylabel('BER');

```

The BER performance from the above program with two receive antennas is shown in Fig. 2.15. From Fig. 2.15, it is observed that the BER with MRC is better than selective diversity and EGC and outperforms the single antenna case.

Example 2.1 What is the BER for $E_b/N_0 = 8 \text{ dB}$ at the receiver output in an AWGN channel if coherently demodulated BPSK modulation is used and if no error control coding is used.

Solution For BPSK modulation in AWGN channel, BER is given by

$$\text{BER}_{\text{BPSK, AWGN}} = \frac{1}{2} \operatorname{erfc}\left(\sqrt{\frac{E_b}{N_0}}\right)$$

$$\frac{E_b}{N_0} = 10^{(8/10)} = 6.3096$$

Thus,

$$\text{BER}_{\text{BPSK, AWGN}} = \frac{1}{2} \operatorname{erfc}\left(\sqrt{6.3096}\right) = 0.0001909.$$

Example 2.2 Using the system in the problem1, compute the coding gain that will be necessary if the BER is to be improved to 10^{-6} .

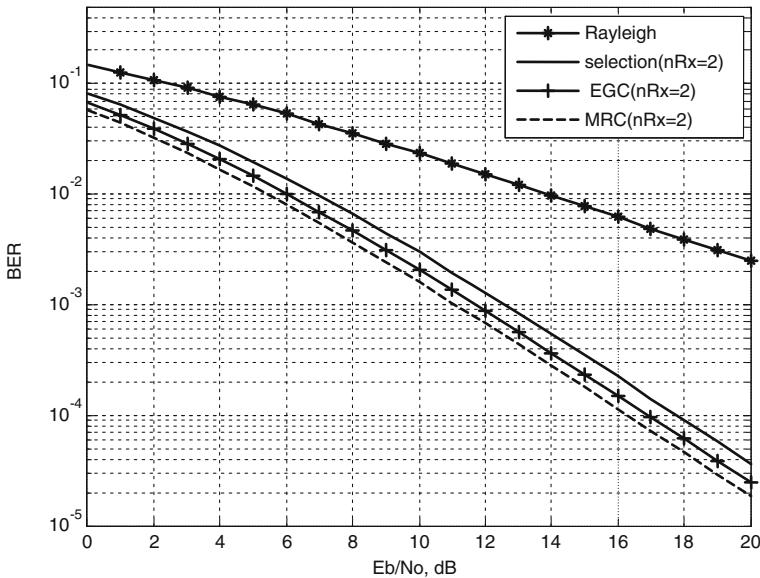


Fig. 2.15 Theoretic BER for BPSK modulation in a Rayleigh fading channel with selection diversity, EGC, and MRC

Solution Here,

$$0.000001 = \frac{1}{2} \operatorname{erfc}\left(\sqrt{\frac{E_b}{N_0}}\right)$$

$$\sqrt{\frac{E_b}{N_0}} = \operatorname{erfcinv}(0.000002) = 3.3612$$

$$\frac{E_b}{N_0} = (3.3612)^2 = 11.29; \frac{E_b}{N_0} (\text{dB}) = 10 \log_{10}(11.29) = 10.5269$$

Hence, necessary coding gain = $10.5269 - 8.0 = 2.5269$ dB.

Example 2.3 Determine the coding gain required to maintain a BER of 10^{-4} when the received Eb/No is fixed, and the modulation format is changed from BPSK to BFSK.

Solution For BPSK in AWGN channel,

$$0.0001 = \frac{1}{2} \operatorname{erfc} \left(\sqrt{\frac{E_b}{N_0}} \right)$$

$$\sqrt{\frac{E_b}{N_0}} = \operatorname{erfcinv}(0.0002) = 2.2697$$

$$\frac{E_b}{N_0} = (2.2697)^2 = 6.9155; \frac{E_b}{N_0} (\text{dB}) = 10 \log_{10}(6.9155) = 8.3982$$

For BFSK in AWGN channel:

$$\text{BER}_{\text{BFSK, AWGN}} = 0.0001 = \frac{1}{2} \exp \left(-\frac{E_b}{2N_0} \right)$$

$$\frac{E_b}{N_0} = -2 \ln(0.0002) = 17.0344; \frac{E_b}{N_0} (\text{dB}) = 10 \log_{10}(17.0344) = 12.3133$$

Hence, necessary coding gain = $12.3133 - 8.3982 = 3.9151$ dB.

Example 2.4 Determine the coding gain required to maintain a BER of 10^{-3} when the received Eb/No remains fixed and the modulation format is changed from BPSK to 8-PSK in AWGN channel.

Solution For BPSK in AWGN channel,

$$0.001 = \frac{1}{2} \operatorname{erfc} \left(\sqrt{\frac{E_b}{N_0}} \right)$$

$$\sqrt{\frac{E_b}{N_0}} = \operatorname{erfcinv}(0.002) = 2.1851$$

$$\frac{E_b}{N_0} = (2.1851)^2 = 4.7748; \frac{E_b}{N_0} (\text{dB}) = 10 \log_{10}(4.7748) = 6.7895$$

From Eq. (2.6), for 8-PSK in AWGN channel,

$$\text{BER}_{8\text{-PSK}} = \frac{2}{3} Q \left(\sin \left(\frac{\pi}{8} \right) \sqrt{\frac{6E_b}{N_0}} \right)$$

$$0.001 = \frac{2}{3} Q \left(\sin \left(\frac{\pi}{8} \right) \sqrt{\frac{6E_b}{N_0}} \right) = \frac{2}{3} Q \left(0.3827 \sqrt{\frac{6E_b}{N_0}} \right)$$

Since,

$$Q(x) = \frac{1}{2} \operatorname{erfc}\left(\frac{x}{\sqrt{2}}\right)$$

$$\frac{0.003}{2} = \frac{1}{2} \operatorname{erfc}\left(\frac{0.3827}{\sqrt{2}} \sqrt{\frac{6E_b}{N_0}}\right)$$

$$0.003 = \operatorname{erfc}\left(0.6629 \sqrt{\frac{6E_b}{N_0}}\right)$$

$$\sqrt{\frac{E_b}{N_0}} = \frac{1}{0.6629} \operatorname{erfcinv}(0.003) = \frac{2.0985}{0.6629} = 3.1656$$

$$\frac{E_b}{N_0} = (3.1656)^2 = 10.0210; \frac{E_b}{N_0} (\text{dB}) = 10 \log_{10}(10.0210) = 10.0091$$

Hence, necessary coding gain = $10.0091 - 6.7895 = 3.2196$ dB.

2.5 Problems

- An AWGN channel requires $\frac{E_b}{N_0} = 9.6$ dB to achieve BER of 10^{-5} using BPSK modulation. Determine the coding gain required to achieve BER of 10^{-5} in a Rayleigh fading channel using BPSK.
- Using the system in Problem 1, determine the coding gain required to maintain a BER of 10^{-5} in Rayleigh fading channel when the modulation format is changed from BPSK to BFSK.
- Determine the necessary $\frac{E_b}{N_0}$ for a Rayleigh fading channel with an average BER of 10^{-5} in order to detect (i) BPSK and (ii) BFSK.
- Determine the necessary $\frac{E_b}{N_0}$ in order to detect BFSK with an average BER of 10^{-4} for a Rician fading channel with Rician factor of 5 dB.
- Determine the probability of error as a function of $\frac{E_b}{N_0}$ for 4-QAM. Plot $\frac{E_b}{N_0}$ vs probability of error and compare the results with BPSK and non-coherent BFSK on the same plot.
- Obtain an approximations to the outage capacity in a Rayleigh fading channel: (i) at low SNRs and (ii) at high SNRs.
- Obtain an approximation to the outage probability for the parallel channel with M Rayleigh branches.
- Assume three-branch MRC diversity in a Rayleigh fading channel. For an average SNR of 20 dB, determine the outage probability that the SNR is below 10 dB.

2.6 MATLAB Exercises

1. Write a MATLAB program to simulate the BER versus number of users performance of SFH-CDMA in AWGN and Rayleigh fading channels at different $\frac{E_b}{N_0}$.
2. Write a MATLAB program to simulate the performance of OFDM in AWGN and Rayleigh fading channels.
3. Write a MATLAB program to simulate the BER versus number of users performance of MC-CDMA in AWGN and Rayleigh fading channels for different number of subcarriers at different $\frac{E_b}{N_0}$.
4. Write a MATLAB program to simulate the performance of selection diversity, equal gain combiner, and maximum ratio combiner and compare the performance with the theoretical results.

References

1. Lu, J., Lataief, K.B., Chuang, J.C.I., Liou, M.L.: M-PSK and M-QAM BER computation using single space concepts. *IEEE Trans. Commun.* **47**, 181–184 (1999)
2. Proakis, J.G.: *Digital Communications*, 3rd edn. McGraw-Hill, New York (1995)
3. Rappaport, T.S.: *Wireless Communications: Principles and Practice*. IEEE Press, Piscataway (1996)
4. Lindsey, W.C.: Error probabilities for Rician fading multichannel reception of binary and n-ary Signals. *IEEE Trans. Inf. Theory* **IT-10**(4), 333–350 (1964)
5. Lu, J., Lataief, K.B., Chuang, J.C.-I., Liou, M.L.: M-PSK and M-QAM BER computation using a signal-space concepts. *IEEE Trans. Commun.* **47**(2), 181–184 (1999)
6. Simon, M.K., Alouini, M.-S.: *Digital Communication Over Fading Channels: A Unified Approach to Performance Analysis*. Wiley, New York (2000)
7. Cheng, J., Beaulieu, N.C.: Accurate DS-CDMA bit-error probability calculation in Rayleigh fading. *IEEE Trans. Wireless Commun.* **1**(1), 3 (2002)
8. Geraniotis, E.A., Parsley, M.B.: Error probabilities for slow-frequency-hopped spread-spectrum multiple-access communications over fading channels. *IEEE Trans. Commun.* **Com-30**(5), 996 (1982)
9. yang, L.L., Hanzo, L.: Overlapping M-ary frequency shift keying spread-spectrum multiple-access systems using random signature sequences. *IEEE Trans. Veh. Technol.* **48**(6), 1984 (1999)
10. Goh, J.G., Maric, S.V.: The capacities of frequency-hopped code-division multiple-access channels. *IEEE Trans. Inf. Theory* **44**(3), 1204–1211 (1998)
11. Shi, Q., Latva-Aho, M.: Exact bit error rate calculations for synchronous MC-CDMA over a Rayleigh fading channel. *IEEE Commun. Lett.* **6**(7), 276–278 (2002)
12. Barry, J.R., Lee, E.A., Messerschmitt, D.G.: *Digital Communication*. Kluwer Academic Publishers, Massachusetts (2004)
13. Zhang, Q.T.: Probability of error for equal-gain combiners over rayleigh channels: some closed- form solutions. *IEEE Trans. Commun.* **45**(3), 270–273 (1997)

Chapter 3

Galois Field Theory

A small portion of linear algebra and combinatorics are used in the development of Hamming codes, the first generation error control codes. The design of error control codes such as BCH codes and Reed Solomon codes relies on the structures of Galois fields and polynomials over Galois fields. This chapter presents briefly algebraic tools for understanding of Galois field theory used in error-correcting codes design.

3.1 Set

A set is defined as an arbitrary collection of objects or elements. The presence of an element X in the set S is denoted by $X \in S$, and if X is certainly not in S , it is denoted by $X \notin S$. An empty set contains zero elements. A set Y is called a subset of a set X if and only if every element Y is in X . Y is a subset of X and is often denoted by $Y \subset X$ which reads “ Y is containing in X .”

Consider two sets, S_1 and S_2 , the new set $S_1 \cup S_2$ is called the union of S_1 and S_2 having the elements in either S_1 or S_2 , or both. Another set $S_1 \cap S_2$ is called the intersection of S_1 and S_2 having the common elements in S_1 and S_2 . If the intersection of two sets is empty, they are said to be disjoint.

3.2 Group

A group is a set on which a binary multiplication operation “ \cdot ” is defined such that the following requirements satisfied

1. For any elements a and b in G , $a \cdot b$ is an element in G
2. For any elements a , b , and c in G , the following associative law

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

3. There is an element e in \mathbf{G} such that for every a in \mathbf{G}

$$a \cdot e = e \cdot a = a \text{ (identity)}$$

4. For any elements a in \mathbf{G} , there is an element a^{-1} in \mathbf{G} such that

$$a \cdot a^{-1} = a^{-1} \cdot a = e \text{ (inverse)}$$

3.3 Field

If the addition and multiplication operations are defined on a set of objects F , then F is said to be a field if and only if

1. F forms a commutative group under addition
2. F forms a commutative group under multiplication
3. Addition and multiplications are distributive.

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

The elements $F = \{1, 2, 3, \dots, p - 1\}$ forms a commutative group of order $(p - 1)$ under modulo p multiplication if and only if p is a prime integer.

All elements of a field form an additive commutative group, whereas all the nonzero elements of a field form a multiplicative commutative group. It is very useful to construct the finite fields. A Galois field that is particularly interesting to the coding theory is a field of finite order.

A Galois field of order q is usually denoted by $\text{GF}(q)$. The simplest of the Galois fields is $\text{GF}(2)$. $\text{GF}(2)$ can be represented by the two-element set $\{0, 1\}$ under standard binary addition and multiplication. The modulo 2 addition and multiplication are shown in Table 3.1.

Galois fields of size p , p a prime, can be constructed by modulo addition and multiplication. If these two operations are allowed to distribute, then a field is formed. The integers $\{0, 1, 2, \dots, p - 1\}$, form the field $\text{GF}(p)$ under modulo p addition and multiplication. The field $\text{GF}(3)$ has the elements $\{0, 1, 2\}$. Finite fields $\text{GF}(q)$ do not exist for all values of q . The value of q must be equal to p^m ,

Table 3.1 Addition and multiplication for $\text{GF}(2)$

Modulo 2 addition			Modulo 2 multiplication		
+	0	1	.	0	1
0	0	1	0	0	0
1	1	0	1	0	1

Table 3.2 Addition and multiplication for GF(7)

Modulo 7 addition							Modulo 7 multiplication								
+	0	1	2	3	4	5	6	.	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6	0	0	0	0	0	0	0	0
1	1	2	3	4	5	6	0	1	0	1	2	3	4	5	6
2	2	3	4	5	6	0	1	2	0	2	4	6	1	3	5
3	3	4	5	6	0	1	2	3	0	3	6	2	5	1	4
4	4	5	6	0	1	2	3	4	0	4	1	5	2	6	3
5	5	6	0	1	2	3	4	5	0	5	3	1	6	4	2
6	6	0	1	2	3	4	5	6	0	6	5	4	3	2	1

where p is a prime positive integer and m is a positive integer. The finite fields of order p^m can be constructed as vector spaces over the prime order field $\text{GF}(p)$.

Example 3.1 Construct addition and multiplication tables over $\text{GF}(7)$.

Solution Here, p equals to 7; therefore, the elements of the GF are $(0, 1, 2, 3, 4, 5, 6)$. The addition and multiplication over $\text{GF}(7)$ will be modulo 7 as shown in Table 3.2.

3.4 Vector Spaces

Let V be a set of vector elements on which a binary addition operation is defined. Let F be a field with scalar elements, and a scalar multiplication operation is defined between the elements of V and the scalar elements of F . V forms a vector space over F if the following properties are satisfied.

Vector spaces

1. V is a commutative group under addition operation on V
2. For any element $a \in F$ and any element $v \in V$, $a \cdot v \in V$
3. For any elements $a, b \in F$ and any element $v \in V$, the following associativity law is satisfied

$$(a \cdot b) \cdot v = a \cdot (b \cdot v) \quad (3.1)$$

4. For any elements $a, b \in F$ and any elements $u, v \in V$, the following distributive law is satisfied

$$a \cdot (u + v) = a \cdot u + a \cdot v \quad (3.2)$$

$$(a + b) \cdot v = a \cdot v + b \cdot v \quad (3.3)$$

5. If 1 is the unit element in F , for any element $v \in V$, $1 \cdot v = v$.

In the case of vector spaces over the scalar field GF(2), V is a collection of binary n-tuples such that if $v_1, v_2 \in V$, then $v_1 + v_2 \in V$, where $+$ stands for component-wise exclusive-or operation. If $v_1 = v_2$, $0 \in V$.

Theorem 3.1 *Let v_1, v_2, \dots, v_k is a set of vectors in a vector space V over a finite field F with dimension k scalars, there is a unique representation of every vector v in V is*

$$v = a_1 v_1 + a_2 v_2 + \cdots + a_k v_k \quad (3.4)$$

3.5 Elementary Properties of Galois Fields

1. Let α be an element in $GF(q)$. The order of α is the smallest positive integer n such that $\alpha^n = 1$.
2. The order q of a Galois field $GF(q)$ must be a power of a prime.
3. Every $GF(q)$ has at least one element α of order $(q - 1)$, which is called a primitive element and that exists in a $GF(q)$ such that $\alpha^{(q-1)} = 1$.
4. All nonzero elements in $GF(q)$ are represented by the $(q - 1)$ consecutive powers of a primitive element α .
5. Let α be a nonzero element in a Galois field $GF(q)$ and n be the order of α , then n divides $q - 1$.

3.6 Galois Field Arithmetic

Finite field arithmetic is different from standard integer arithmetic. In finite field arithmetic, all operations performed on limited number of elements and resulted in an element within the same field.

3.6.1 Addition and Subtraction of Polynomials

In standard integer arithmetic, addition and subtraction of polynomials are performed by adding or subtracting together, whereas in finite field, addition and subtraction are accomplished using the XOR operator and they are identical.

Example 3.2 Add the polynomials $(x^6 + x^4 + x + 1)$ and $(x^7 + x^6 + x^3 + x)$ in $GF(2)$.

Table 3.3 Computation of polynomials in normal algebra and Galois field

p_1	p_2	$p_1 + p_2$ (normal algebra)	$p_1 + p_2$ (GF)
$x^3 + x^2 + x + 1$	$x^3 + x^2$	$2x^3 + 2x^2 + x + 1$	$x + 1$
$x^4 + x^3 + x^2$	$x^5 + x^2$	$x^5 + x^4 + x^3 + 2x^2$	$x^5 + x^4 + x^3$
$x^2 + 1$	$x^3 + 1$	$x^3 + x^2 + 2$	$x^3 + x^2$

Solution

$$(x^6 + x^4 + x + 1) + (x^7 + x^6 + x^3 + x) = x^7 + x^4 + x^3 + 1.$$

The normal algebraic sum and the modulo 2 finite field sum of a few polynomials are tabulated in Table 3.3.

3.6.2 Multiplication of Polynomials

Multiplication of polynomials in Galois field is same as integer arithmetic, but the addition performed after multiplication is similar to Galois field.

Example 3.3 Multiply the polynomials $(x^6 + x^4 + x + 1)$ and $(x^7 + x^6 + x^3 + x)$.

Solution

$$\begin{aligned} & (x^6 + x^4 + x + 1)(x^7 + x^6 + x^3 + x) \\ &= x^{13} + x^{12} + x^9 + x^7 + x^{11} + x^{10} + x^7 + x^5 + x^8 + x^7 + x^4 \\ &\quad + x^2 + x^7 + x^6 + x^3 + x \\ &= x^{13} + x^{12} + x^9 + x^{11} + x^{10} + x^5 + x^8 + x^4 + x^2 + x^6 + x^3 + x \\ &= x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x \end{aligned}$$

3.6.3 Multiplication of Polynomials Using MATLAB

The following MATLAB command computes the multiplication of polynomial p_1 and polynomial p_2 in GF(2).

$$p_3 = \text{gfconv}(p_1, p_2)$$

The degree of the resulting GF(2) polynomial p_3 equals the sum of degree of the polynomial p_1 and degree of the polynomial p_2 . For example, the following

commands result in the multiplication of the polynomials $1 + x + x^3$ and $1 + x + x^2 + x^4$.

$$\begin{aligned} p_1 &= [1 \ 1 \ 0 \ 1] \% 1 + x + x^3 \\ p_2 &= [1 \ 1 \ 1 \ 0 \ 1] \% 1 + x + x^2 + x^4 \\ p_3 &= \text{gfconv}(p_1, p_2); \% (1 + x + x^3) \cdot (1 + x + x^2 + x^4) \end{aligned}$$

The output p_3 for the above commands is

$$p_3 = [1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1] \% 1 + x^7$$

3.6.4 Division of Polynomials

Suppose that $a(x)$ and $b(x) \neq 0$ are polynomials over GF(2). There are unique pair of polynomial called the quotient and remainder, $q(x)$ and $r(x)$ over GF(2), such that

$$a(x) = q(x) b(x) + r(x) \quad (3.5)$$

Example 3.4 Divide $f_1(x) = 1 + x^2 + x^3 + x^5$ by $f_2(x) = 1 + x^3 + x^4$.

Solution

$$\begin{array}{r} 1 + x \text{(quotient)} \\ 1 + x^3 + x^4) \overline{1 + x^2 + x^3 + x^5} \\ \underline{1 \quad \quad \quad + x^3 + x^4} \\ \quad \quad \quad x^2 + x^4 + x^5 \\ \quad \quad \quad \underline{x + x^4 + x^5} \\ \text{remainder: } \underline{x + x^2} \end{array}$$

It can easily be verified that

$$1 + x^2 + x^3 + x^5 = (1 + x^3 + x^4)(1 + x) + (x + x^2).$$

If the remainder $r(x)$ is zero, $a(x)$ is divisible by $b(x)$ and $b(x)$ is a factor of $a(x)$.

Example 3.5 Check whether $f_1(x) = (x^2 + x + 1)$ is a factor of $f_2(x) = x^5 + x^4 + 1$.

Solution

$$\begin{array}{r}
 x^3 + x + 1 \text{(quotient)} \\
 x^2 + x + 1) \overline{x^5 + x^4 + 1} \\
 \underline{x^5 + x^4 + \quad x^3} \\
 \underline{x^3 + 1} \\
 x^3 + x^2 + x \\
 \underline{x^2 + x + 1} \\
 x^2 + x + 1 \\
 \hline
 \text{remainder : 0}
 \end{array}$$

The remainder is zero, and hence, $f_2(x)$ is divisible by $f_1(x)$, and $f_1(x)$ is a factor of $f_2(x)$.

3.6.5 Division of Polynomials Using MATLAB

The following MATLAB command computes the quotient q and remainder r of the division of polynomial p_2 by polynomial p_1 in p_1 GF(2).

$$[q, r] = \text{gfdeconv}(p_2, p_1)$$

For example, the following commands divide polynomial $1 + x^7$ by polynomial $1 + x + x^3$

$$\begin{aligned}
 p_1 &= [1 \quad 1 \quad 0 \quad 1] \% 1 + x + x^3 \\
 p_2 &= [1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1] \% 1 + x^7 \\
 [q, r] &= \text{gfdeconv}(p_2, p_1); \% 1 + x^7 / 1 + x + x^3
 \end{aligned}$$

The output q and r for the above commands are

$$\begin{aligned}
 q &= [1 \quad 1 \quad 0 \quad 1] \% 1 + x + x^2 + x^4 \\
 r &= 0.
 \end{aligned}$$

3.7 Polynomials Over Galois Fields

A polynomial over $\text{GF}(q)$ is of the following form

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \tag{3.6}$$

of degree n (with $a_n \neq 0$) and with coefficients $\{a_i\}$ in the finite field $\text{GF}(q)$.

3.7.1 Irreducible Polynomial

A polynomial $p(x)$ is said to be irreducible in $\text{GF}(q)$, if $p(x)$ has no divisor polynomials in $\text{GF}(q)$ of degree less than m but greater than zero.

Examples

1. $x^3 + x^2 + 1$ is irreducible in $\text{GF}(2)$ as it is not factorable having degree of less than 3.
2. $x^4 + x^2 + 1$ is not irreducible in $\text{GF}(2)$, since the polynomial is divisible by the polynomial $x^2 + x + 1$ with coefficients in $\text{GF}(2)$ and with degree of 2 less than 4.
3. $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\text{GF}(2)$ as it is not factorable having factors of degree less than 4.
4. $x^5 + x^4 + 1$ is not irreducible in $\text{GF}(2)$ since the polynomial is divisible by polynomials of degree less than 5.

3.7.2 Primitive Polynomials

An irreducible polynomial $p(x) \in \text{GF}(2)$ of degree m is said to be primitive if the smallest positive integer n for which $p(x)$ divides $x^n - 1$ is $n = 2^m - 1$.

The roots $\{\alpha_j\}$ of an m th degree primitive polynomial $p(x) \in \text{GF}(2)$ have order $2^m - 1$. All primitive polynomials are irreducible polynomials, but all irreducible polynomials are not primitive.

Examples

1. $x^2 + x + 1$ is primitive. The smallest polynomial of the form $x^n - 1$ for which it is a divisor is $x^3 - 1$ ($3 = 2^2 - 1$).
2. $x^3 + x^2 + 1$ is primitive. The smallest polynomial of the form $x^n - 1$ for which it is a divisor is $x^7 - 1$ ($7 = 2^3 - 1$).
3. $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ is not primitive since it is not irreducible. It can be factorized as product of the polynomials $x^3 + x^2 + 1$ and $x^3 + x + 1$.

3.7.3 Checking of Polynomials for Primitiveness Using MATLAB

The following MATLAB command can be used to check whether the degree- m $\text{GF}(2)$ polynomial p is primitive.

`ck = gfprimck(p);`

The output ck is as follows:

ck = -1 p is not an irreducible polynomial

ck = 0 p is irreducible but not a primitive polynomial

ck = 1 p is a primitive polynomial.

For example, the following MATLAB commands determine whether the polynomial $p(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ is primitive or not

```
p = [1 1 1 1 1 1] % 1 + x + x^3 + x^3 + x^4 + x^5 + x^6
```

```
ck = gfprimck(p);
```

The output ck for the above commands is -1 indicating that the polynomial is not irreducible and hence not primitive.

3.7.4 Generation of Primitive Polynomials Using MATLAB

Primitive polynomials of degree m can be generated using the following MATLAB command `primpoly` as follows:

```
p = primpoly(m, 'all')
```

For example, the primitive polynomials generated using the above m file for $m = 3, 4, 5$, and 6 are tabulated in Table 3.4.

Table 3.4 Primitive polynomials for $m = 3, 4, 5$, and 6

m	Primitive polynomial $p(x)$
3	$p(x) = x^3 + x + 1$
	$p(x) = x^3 + x^2 + 1$
4	$p(x) = x^4 + x + 1$
	$p(x) = x^4 + x^3 + 1$
5	$p(x) = x^5 + x^2 + 1$
	$p(x) = x^5 + x^3 + 1$
	$p(x) = x^5 + x^3 + x^2 + x + 1$
	$p(x) = x^5 + x^4 + x^2 + x + 1$
	$p(x) = x^5 + x^4 + x^3 + x + 1$
	$p(x) = x^5 + x^4 + x^3 + x^2 + 1$
6	$p(x) = x^6 + x + 1$
	$p(x) = x^6 + x^4 + x^3 + x + 1$
	$p(x) = x^6 + x^5 + 1$
	$p(x) = x^6 + x^5 + x^2 + x + 1$
	$p(x) = x^6 + x^5 + x^3 + x^2 + 1$
	$p(x) = x^6 + x^5 + x^4 + x + 1$

3.8 Construction of Galois Field $GF(2^m)$ from $GF(2)$

The 2^m elements of $GF(2^m)$ can be written as $\{0, 1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{2^m-2}\}$. All the nonzero elements of $GF(2^m)$ are generated by the powers of the primitive element α that satisfies the condition $\alpha^{2^m-1} = 1$.

The polynomial representation of the elements of $GF(2^m)$ is given by the remainder of x^n upon division by the polynomial $p(x)$ which is primitive in $GF(2)$.

$$\alpha^n = \text{Remainder}\{x^n/p(x)\} \quad (3.7)$$

Example 3.6 Construct $GF(8)$ as a vector space over $GF(2)$.

Solution Let us consider the construction of $GF(8)$ based on the polynomial $p(x) = x^3 + x + 1$ which is primitive in $GF(2)$. Let α be a root of $p(x)$. This implies that $\alpha^3 + \alpha + 1 = 0$ or equivalently $\alpha^3 = \alpha + 1$. The distinct powers of α must have $(2^3 - 1)$ distinct nonzero polynomial representations of α of degree 2 or less with the coefficients from $GF(2)$. The set $\{1, \alpha, \alpha^2\}$ is used as a basis for the vector space representation of $GF(8)$.

Since every field must contain zero and one element, we have

$$0 = 0$$

$$\alpha^0 = 1$$

Since the reminders of x and x^2 upon division by the primitive polynomial $p(x) = x^3 + x + 1$ are themselves, the other two possible assignments are as follows:

$$\alpha^1 = x$$

$$\alpha^2 = x^2$$

However, the polynomial representation of x^3 can be derived by the following polynomial division:

$$\begin{array}{r} 1 \\ \hline x^3 + x + 1) \overline{x^3} \\ \underline{x^3 + x + 1} \\ -(x + 1) \end{array}$$

The remainder is $-(x + 1)$. Hence, $\alpha^3 = \alpha + 1$

For x^4

$$\begin{array}{r} x \\ \hline x^3 + x + 1) \overline{x^4} \\ x^4 + x^2 + x \\ \hline -(x^2 + x) \end{array}$$

The remainder is $-(x^2 + x)$. Hence, $\alpha^4 = x^2 + \alpha$

For x^5

$$\begin{array}{r} x^2 + 1 \\ \hline x^3 + x + 1) \overline{x^5} \\ x^5 + x^3 + x^2 \\ \hline -x^3 - x^2 \\ x^3 + x + 1 \\ \hline -(x^2 + x + 1) \end{array}$$

The remainder is $-(x^2 + x + 1)$. Hence, $\alpha^5 = x^2 + \alpha + 1$. Similarly, x^6 and x^7 follow the same procedure to get the polynomial representations. All the above values are tabulated in the following Table 3.5.

Example 3.7 Construct GF(16) as a vector space over GF(2).

Solution Let us consider the construction of GF(16) based on the polynomial $p(x) = x^4 + x + 1$ which is primitive in GF(2). We know that

$$0 = 0$$

$$\alpha^0 = 1$$

Table 3.5 Representation of elements of GF(8)

Zero and powers of α	Polynomial representation	Vector space over GF(2) $1\alpha\alpha^2$
0	0	0 0 0
α^0	1	1 0 0
α^1	α	0 1 0
α^2	α^2	0 0 1
α^3	$1 + \alpha$	1 1 0
α^4	$\alpha + \alpha^2$	0 1 1
α^5	$1 + \alpha + \alpha^2$	1 1 1
α^6	$1 + \alpha^2$	1 0 1
α^7	1	1 0 0

Since the reminders of x , x^2 , and x^3 upon division by the primitive polynomial $p(x) = x^4 + x + 1$ are themselves, the other three possible assignments are as follows:

$$\alpha^1 = x$$

$$\alpha^2 = x^2$$

$$\alpha^3 = x^3$$

However, the polynomial representation of x^4 can be derived by the following polynomial division:

$$\begin{array}{r} \underline{1} \\ x^4 + x + 1) \underline{x^4} \\ \underline{x^4 + x + 1} \\ -(x + 1) \end{array}$$

The remainder is $-(x + 1)$. Hence, $\alpha^4 = \alpha + 1$.

Similarly, for the values from x^5 to x^{15} , follow the same procedure to get the polynomial representations. The above values are tabulated in the following Table 3.6.

Table 3.6 Representation of elements of GF(16)

Zero and powers of α	Polynomials over GF(2)	Vector space over GF(2) $1\alpha\alpha^2\alpha^3$
0	0	0 0 0 0
α^0	1	1 0 0 0
α^1	α	0 1 0 0
α^2	α^2	0 0 1 0
α^3	α^3	0 0 0 1
α^4	$1 + \alpha$	1 1 0 0
α^5	$\alpha + \alpha^2$	0 1 1 0
α^6	$\alpha^2 + \alpha^3$	0 0 1 1
α^7	$1 + \alpha + \alpha^3$	1 1 0 1
α^8	$1 + \alpha^2$	1 0 1 0
α^9	$\alpha + \alpha^3$	0 1 0 1
α^{10}	$1 + \alpha + \alpha^2$	1 1 1 0
α^{11}	$\alpha + \alpha^2 + \alpha^3$	0 1 1 1
α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	1 1 1 1
α^{13}	$1 + \alpha^2 + \alpha^3$	1 0 1 1
α^{14}	$1 + \alpha^3$	1 0 0 1
α^{15}	1	1 0 0 0

Example 3.8 Construct $GF(32)$ as a vector space over $GF(2)$.

Solution Let us consider the construction of $GF(32)$ based on the polynomial $p(x) = x^5 + x^2 + 1$ which is primitive in $GF(2)$.

We know that

$$\begin{aligned}0 &= 0 \\x^0 &= 1\end{aligned}$$

Since the reminders of x , x^2 , x^3 , and x^4 upon division by the primitive polynomial $p(x) = x^5 + x^2 + 1$ are themselves, the other four possible assignments are as follows:

$$\begin{aligned}\alpha^1 &= x \\ \alpha^2 &= x^2 \\ \alpha^3 &= x^3 \\ \alpha^4 &= x^4\end{aligned}$$

However, the polynomial representation of x^5 can be derived by the following polynomial division:

$$\begin{array}{r} & \frac{1}{x^5 + x^2 + 1) \overline{x^5}} \\ & \underline{x^5 + x^2 + 1} \\ & -(x^2 + 1)\end{array}$$

The remainder is $-(x^2 + 1)$. Hence, $\alpha^5 = \alpha^2 + 1$.

Similarly, for the values from α^6 to α^{31} , follow the same procedure to get the polynomial representations. All the above values are tabulated in the following Table 3.7.

Example 3.9 Construct $GF(64)$ as a vector space over $GF(2)$.

Solution Let us consider the construction of $GF(64)$ based on the polynomial $p(x) = x^6 + x + 1$ which is primitive in $GF(2)$.

We know that

$$\begin{aligned}0 &= 0 \\x^0 &= 1\end{aligned}$$

Table 3.7 Representation of elements of GF(32)

Zero and powers of α	Polynomials over GF(2)	Vector space over GF(2) 1 $\alpha \alpha^2 \alpha^3 \alpha^4$
0	0	0 0 0 0 0
α^0	1	1 0 0 0 0
α^1	α	0 1 0 0 0
α^2	α^2	0 0 1 0 0
α^3	α^3	0 0 0 1 0
α^4	α^4	0 0 0 0 1
α^5	$1 + \alpha^2$	1 0 1 0 0
α^6	$\alpha + \alpha^3$	0 1 0 1 0
α^7	$\alpha^2 + \alpha^4$	0 0 1 0 1
α^8	$1 + \alpha^2 + \alpha^3$	1 0 1 1 0
α^9	$\alpha + \alpha^3 + \alpha^4$	0 1 0 1 1
α^{10}	$1 + \alpha^4$	1 0 0 0 1
α^{11}	$1 + \alpha + \alpha^2$	1 1 1 0 0
α^{12}	$\alpha + \alpha^2 + \alpha^3$	0 1 1 1 0
α^{13}	$\alpha^2 + \alpha^3 + \alpha^4$	0 0 1 1 1
α^{14}	$1 + \alpha^2 + \alpha^3 + \alpha^4$	1 0 1 1 1
α^{15}	$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$	1 1 1 1 1
α^{16}	$1 + \alpha + \alpha^3 + \alpha^4$	1 1 0 1 1
α^{17}	$1 + \alpha + \alpha^4$	1 1 0 0 1
α^{18}	$1 + \alpha$	1 1 0 0 0
α^{19}	$\alpha + \alpha^2$	0 1 1 0 0
α^{20}	$\alpha^2 + \alpha^3$	0 0 1 1 0
α^{21}	$\alpha^3 + \alpha^4$	0 0 0 1 1
α^{22}	$1 + \alpha^2 + \alpha^4$	1 0 1 0 1
α^{23}	$1 + \alpha + \alpha^2 + \alpha^3$	1 1 1 1 0
α^{24}	$\alpha + \alpha^2 + \alpha^3 + \alpha^4$	0 1 1 1 1
α^{25}	$1 + \alpha^3 + \alpha^4$	1 0 0 1 1
α^{26}	$1 + \alpha + \alpha^2 + \alpha^4$	1 1 1 0 1
α^{27}	$1 + \alpha + \alpha^3$	1 1 0 1 0
α^{28}	$\alpha + \alpha^2 + \alpha^4$	0 1 1 0 1
α^{29}	$1 + \alpha^3$	1 0 0 1 0
α^{30}	$\alpha + \alpha^4$	0 1 0 0 1
α^{31}	1	1 0 0 0 0

Since the reminders of x, x^2, x^3, x^4 and x^5 upon division by the primitive polynomial $p(x) = x^6 + x + 1$ are themselves, the other five possible assignments are as follows:

$$\alpha^1 = x$$

$$\alpha^2 = x^2$$

$$\alpha^3 = x^3$$

$$\alpha^4 = x^4$$

$$\alpha^5 = x^5$$

However, the polynomial representation of x^6 can be derived by the following polynomial division:

$$\begin{array}{r} \underline{1} \\ x^6 + x + 1) \underline{x^6} \\ \underline{x^6 + x + 1} \\ -(x + 1) \end{array}$$

The remainder is $-(x + 1)$. Hence, $\alpha^6 = \alpha + 1$.

Similarly, for the values from x^7 to x^{63} , follow the same procedure to get the polynomial representations. All the above values are tabulated in the following Table 3.8.

3.8.1 Construction of GF(2^m), Using MATLAB

To construct GF(2^m), the following MATLAB function can be used

```
field = gftuple([-1:2^m-2]', m, 2);
```

For example, the GF(8) generated using the above m file for $m = 3$ is as follows:

```
field =
```

0	0	0
1	0	0
0	1	0
0	0	1
1	1	0
0	1	1
1	1	1
1	0	1

Table 3.8 Representation of elements of GF(64)

Zero and powers of α	Polynomials over GF(2)	Vector space over GF(2) $1\alpha\alpha^2\alpha^3\alpha^4\alpha^5$
0	1	0 0 0 0 0 0
α^0	1	1 0 0 0 0 0
α^1	α	0 1 0 0 0 0
α^2	α^2	0 0 1 0 0 0
α^3	α^3	0 0 0 1 0 0
α^4	α^4	0 0 0 0 1 0
α^5	α^5	0 0 0 0 0 1
α^6	$1 + \alpha$	1 1 0 0 0 0
α^7	$\alpha + \alpha^2$	0 1 1 0 0 0
α^8	$\alpha^2 + \alpha^3$	0 0 1 1 0 0
α^9	$\alpha^3 + \alpha^4$	0 0 0 1 1 0
α^{10}	$\alpha^4 + \alpha^5$	0 0 0 0 1 1
α^{11}	$1 + \alpha + \alpha^5$	1 1 0 0 0 1
α^{12}	$1 + \alpha^2$	1 0 1 0 0 0
α^{13}	$\alpha + \alpha^3$	0 1 0 1 0 0
α^{14}	$\alpha^2 + \alpha^4$	0 0 1 0 1 0
α^{15}	$\alpha^3 + \alpha^5$	0 0 0 1 0 1
α^{16}	$1 + \alpha + \alpha^4$	1 1 0 0 1 0
α^{17}	$\alpha + \alpha^2 + \alpha^5$	0 1 1 0 0 1
α^{18}	$1 + \alpha + \alpha^2 + \alpha^3$	1 1 1 1 0 0
α^{19}	$\alpha + \alpha^2 + \alpha^3 + \alpha^4$	0 1 1 1 1 0
α^{20}	$\alpha^2 + \alpha^3 + \alpha^4 + \alpha^5$	0 0 1 1 1 1
α^{21}	$1 + \alpha + \alpha^3 + \alpha^4 + \alpha^5$	1 1 0 1 1 1
α^{22}	$1 + \alpha^2 + \alpha^4 + \alpha^5$	1 0 1 0 1 1
α^{23}	$1 + \alpha^3 + \alpha^5$	1 0 0 1 0 1
α^{24}	$1 + \alpha^4$	1 0 0 0 1 0
α^{25}	$\alpha + \alpha^5$	0 1 0 0 0 1
α^{26}	$1 + \alpha + \alpha^5$	1 1 1 0 0 0
α^{27}	$\alpha + \alpha^2 + \alpha^3$	0 1 1 1 0 0
α^{28}	$\alpha^2 + \alpha^3 + \alpha^4$	0 0 1 1 1 0
α^{29}	$\alpha^3 + \alpha^4 + \alpha^5$	0 0 0 1 1 1
α^{30}	$1 + \alpha + \alpha^4 + \alpha^5$	1 1 0 0 1 1
α^{31}	$1 + \alpha^2 + \alpha^5 +$	1 0 1 0 0 1
α^{32}	$1 + \alpha^3$	1 0 0 1 0 0
α^{33}	$\alpha + \alpha^4$	0 1 0 0 1 0
α^{34}	$\alpha^2 + \alpha^5$	0 0 1 0 0 1
α^{35}	$1 + \alpha + \alpha^3$	1 1 0 1 0 0
α^{36}	$\alpha + \alpha^2 + \alpha^4$	0 1 1 0 1 0
α^{37}	$\alpha^2 + \alpha^3 + \alpha^5$	0 0 1 1 0 1
α^{38}	$1 + \alpha + \alpha^3 + \alpha^4$	1 1 0 1 1 0
α^{39}	$\alpha + \alpha^2 + \alpha^4 + \alpha^5$	0 1 1 0 1 1

(continued)

Table 3.8 (continued)

Zero and powers of α	Polynomials over GF(2)	Vector space over GF(2) 1 $\alpha\alpha^2\alpha^3\alpha^4\alpha^5$
α^{40}	$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^5$	1 1 1 1 0 1
α^{41}	$1 + \alpha^2 + \alpha^3 + \alpha^4$	1 0 1 1 1 0
α^{42}	$\alpha + \alpha^3 + \alpha^4 + \alpha^5$	0 1 0 1 1 1
α^{43}	$1 + \alpha + \alpha^2 + \alpha^4 + \alpha^5$	1 1 1 0 1 1
α^{44}	$1 + \alpha^2 + \alpha^3 + \alpha^5$	1 0 1 1 0 1
α^{45}	$1 + \alpha^3 + \alpha^4$	1 0 0 1 1 0
α^{46}	$\alpha + \alpha^4 + \alpha^5$	0 1 0 0 1 1
α^{47}	$1 + \alpha + \alpha^2 + \alpha^5$	1 1 1 0 0 1
α^{48}	$1 + \alpha^2 + \alpha^3$	1 0 1 1 0 0
α^{49}	$\alpha + \alpha^3 + \alpha^4$	0 1 0 1 1 0
α^{50}	$\alpha^2 + \alpha^4 + \alpha^5$	0 0 1 0 1 1
α^{51}	$1 + \alpha + \alpha^3 + \alpha^5$	1 1 0 1 0 1
α^{52}	$1 + \alpha^2 + \alpha^4$	1 0 1 0 1 0
α^{53}	$\alpha + \alpha^3 + \alpha^5$	0 1 0 1 0 1
α^{54}	$1 + \alpha + \alpha^2 + \alpha^4$	1 1 1 0 1 0
α^{55}	$\alpha + \alpha^2 + \alpha^3 + \alpha^5$	0 1 1 1 0 1
α^{56}	$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$	1 1 1 1 1 0
α^{57}	$\alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5$	0 1 1 1 1 1
α^{58}	$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5$	1 1 1 1 1 1
α^{59}	$1 + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5$	1 0 1 1 1 1
α^{60}	$1 + \alpha^3 + \alpha^4 + \alpha^5$	1 0 0 1 1 1
α^{61}	$1 + \alpha^4 + \alpha^5$	1 0 0 0 1 1
α^{62}	$1 + \alpha^5$	1 0 0 0 0 1
α^{63}	1	1 0 0 0 0 0

3.9 Minimal Polynomials and Conjugacy Classes of GF(2^m)

3.9.1 Minimal Polynomials

Definition 3.1 Suppose that α is an element in GF(2^m). The unique minimal polynomial of α with respect to GF(2) is a polynomial $\phi(x)$ of minimum degree such that $\phi(\alpha) = 0$.

3.9.2 Conjugates of GF Elements

Let α be an element in the Galois field GF(2^m). The conjugates of α with respect to the subfield GF(q) are the elements $\alpha, \alpha^2, \alpha^{2^2}, \alpha^{2^3}, \dots$

The conjugates of α with respect to $GF(q)$ form a set called the conjugacy class of α with respect to $GF(q)$.

Theorem 3.2 (Conjugacy Class) *The conjugacy class of $\alpha \in GF(2^m)$ with respect to $GF(2)$ contains all the elements of the form α^{2^i} for $0 \leq i \leq l - 1$ where l is the smallest positive integer such that $\alpha^{2^l} = \alpha$.*

3.9.3 Properties of Minimal Polynomial

Theorem 3.3 *The minimal polynomial of an element of α of $GF(2^m)$ is an irreducible polynomial.*

Proof Suppose the minimal polynomial, $\phi(x)$, is not irreducible. Then, $\phi(x)$ can be expressed as a product of two other polynomials

$$\phi(x) = \phi_1(x)\phi_2(x)$$

As $\phi(\alpha) = \phi_1(\alpha)\phi_2(\alpha) = 0$, either $\phi_1(\alpha) = 0$ or $\phi_2(\alpha) = 0$.

It is contradictory with the minimality of the degree $\phi(x)$. \square

Theorem 3.4 *Let $f(x)$ be a polynomial over $GF(2)$ and $\phi(x)$ be the minimal polynomial of an element α in $GF(2^m)$. If α is a root of $f(x)$, then $f(x)$ is divisible by $\phi(x)$.*

Proof The division of $f(x)$ by $\phi(x)$ gives

$$f(x) = \phi(x)q(x) + r(x)$$

Since α is a root of $f(x)$, $f(\alpha) = 0$ and $\phi(\alpha) = 0$, it follows that $r(\alpha) = 0$. As the degree of $r(x)$ is less than that of $\phi(x)$, $r(\alpha) = 0$ only when $r(x) = 0$. Hence, $f(x) = \phi(x)q(x)$; therefore, $f(x)$ is divisible by $\phi(x)$. \square

Theorem 3.5 *The nonzero elements of $GF(2^m)$ form all the roots of $x^{2^m-1} - 1$*

Proof Let α be a nonzero elements in the field $GF(2^m)$. Then, it follows that $\alpha^{2^m-1} = 1$, or $\alpha^{2^m-1} + 1 = 0$. This implies that α is a root of the polynomial $x^{2^m-1} + 1$. Hence, every nonzero element of $GF(2^m)$ is a root of $x^{2^m-1} + 1$. Since the degree of $x^{2^m-1} + 1$ is $2^m - 1$, the $2^m - 1$ nonzero elements of $GF(2^m)$ form all the roots of $x^{2^m-1} + 1$. \square

Theorem 3.6 *Let α be an element in the Galois field $F(2^m)$. Then, all its conjugates $\alpha, \alpha^2, \dots, \alpha^{2^{l-1}}$ have the same minimal polynomial.*

A direct consequence of Theorem 3.5 is that $x^{2^m-1} - 1$ is equal to the product of the distinct minimal polynomials of the nonzero elements of $GF(2^m)$.

Theorem 3.7 Suppose that $\phi(x)$ be the minimal polynomial of an element α of $GF(2^m)$ and l be the smallest positive integer such that $\alpha^{2^l} = \alpha$, and then, $\phi(x)$ of degree m or less is given by

$$\phi(x) = \prod_{i=0}^{l-1} (x - \alpha^{2^i}) \quad (3.8)$$

3.9.4 Construction of Minimal Polynomials

The stepwise procedure for the construction of the Galois field is as follows

Step 1: Generate the Galois field $GF(2^m)$ based on the primitive polynomial corresponding to m .

Step 2: Find the groups of the conjugate roots.

Step 3: The construction of minimal polynomial of each elements is by using Eq. (3.8).

Using the above procedure, the following examples illustrate the construction of the minimal polynomial for $GF(8)$, $GF(16)$, and $GF(32)$ with respect to $GF(2)$.

Example 3.10 Determine the minimal polynomials of the elements of $GF(8)$ with respect to $GF(2)$.

Solution The eight elements in $GF(8)$ are arranged in conjugacy classes and their minimal polynomials computed as follows

Conjugacy class	Associated minimal polynomial
$\{0\}$	$\phi^*(x) = x$
$\{1\}$	$\phi_0(x) = x + 1$
$\{\alpha, \alpha^2, \alpha^4\}$	$\phi_1(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4) = x^3 + x + 1$
$\{\alpha^3, \alpha^6, \alpha^5\}$	$\phi_3(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^5) = x^3 + x^2 + 1$

From the Theorem 3.5, it is known that the minimal polynomials of the nonzero elements in the field $GF(8)$ provide the complete factorization of $x^7 - 1$. Hence, $x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$.

Example 3.11 Determine the minimal polynomials of the elements of $GF(16)$ with respect to $GF(2)$.

Solution The 16 elements in $\text{GF}(2^4)$ are arranged in conjugacy classes and their associated minimal polynomials computed as follows:

Conjugacy class	Associated minimal polynomial
$\{0\}$	$\phi^*(x) = x$
$\{1\}$	$\phi_0(x) = x + 1$
$\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$	$\begin{aligned}\phi_1(x) &= (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8) \\ &= x^4 + x + 1\end{aligned}$
$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$	$\begin{aligned}\phi_3(x) &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) \\ &= x^4 + x^3 + x^2 + x + 1\end{aligned}$
$\{\alpha^5, \alpha^{10}\}$	$\phi_5(x) = (x - \alpha^5)(x - \alpha^{10}) = x^2 + x + 1$
$\{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$	$\begin{aligned}\phi_9(x) &= (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{13})(x - \alpha^{11}) \\ &= x^4 + x^3 + 1\end{aligned}$

As a consequence of the Theorem 3.5, the following factorization holds good for $\text{GF}(16)$

$$x^{15} - 1 = (x + 1)(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x^4 + x^3 + 1)$$

Example 3.12 Determine the minimal polynomials of the elements of $\text{GF}(32)$ with respect to $\text{GF}(2)$.

Solution The 32 elements in $\text{GF}(32)$ are arranged in conjugacy classes and their minimal polynomials computed as follows:

Conjugacy class	Associated minimal polynomial
$\{0\}$	$\phi^*(x) = x$
$\{1\}$	$\phi_0(x) = x + 1$
$\{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}\}$	$\begin{aligned}\phi_1(x) &= (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16}) \\ &= x^5 + x^2 + 1\end{aligned}$
$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17}\}$	$\begin{aligned}\phi_3(x) &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24})(x - \alpha^{17}) \\ &= x^5 + x^4 + x^3 + x^2 + 1\end{aligned}$
$\{\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^9, \alpha^{18}\}$	$\begin{aligned}\phi_5(x) &= (x - \alpha^5)(x - \alpha^{10})(x - \alpha^{20})(x - \alpha^9)(x - \alpha^{18}) \\ &= x^5 + x^4 + x^2 + x + 1\end{aligned}$
$\{\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{25}, \alpha^{19}\}$	$\begin{aligned}\phi_9(x) &= (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{28})(x - \alpha^{25})(x - \alpha^{19}) \\ &= x^5 + x^3 + x^2 + x + 1\end{aligned}$

(continued)

(continued)

Conjugacy class	Associated minimal polynomial
$\{\alpha^{11}, \alpha^{22}, \alpha^{13}, \alpha^{26}, \alpha^{21}\}$	$\begin{aligned}\phi_{11}(x) &= (x - \alpha^{11})(x - \alpha^{22})(x - \alpha^{13})(x - \alpha^{26})(x - \alpha^{21}) \\ &= x^5 + x^4 + x^3 + x + 1\end{aligned}$
$\{\alpha^{15}, \alpha^{30}, \alpha^{29}, \alpha^{27}, \alpha^{23}\}$	$\begin{aligned}\phi_{15}(x) &= (x - \alpha^{15})(x - \alpha^{30})(x - \alpha^{29})(x - \alpha^{27})(x - \alpha^{23}) \\ &= x^5 + x^3 + 1\end{aligned}$

According to the Theorem 3.5, the following factorization is valid for GF(32)

$$\begin{aligned}x^{31} - 1 &= (x + 1)(x^5 + x^2 + 1)(x^5 + x^4 + x^3 + x^2 + 1)(x^5 + x^4 + x^2 + x + 1) \\ &\quad (x^5 + x^3 + x^2 + x + 1)(x^5 + x^4 + x^3 + x + 1)(x^5 + x^3 + 1)\end{aligned}$$

3.9.5 Construction of Conjugacy Classes Using MATLAB

```
cst = cosets(m)
```

The MATLAB command can be used to find the conjugacy classes for the nonzero elements in GF(8).

For example, for $m = 3$, the conjugacy classes are generated using the above MATLAB command that is given as follows

```
c = cosets(3);
c{1}'
c{2}'
c{3}'
```

$c\{1\}'$ displays the conjugacy class $\{\alpha^0\}$ which indicates the nonzero element 1 that represents α^0 .

$c\{2\}'$ displays the conjugacy class $\{\alpha^2, \alpha^4, \alpha^6\}$ which indicates the nonzero elements 2, 4, and 6 that represent α , α^2 and $\alpha^2 + \alpha$, respectively.

$c\{3\}'$ displays the conjugacy class $\{\alpha^3, \alpha^5, \alpha^7\}$ which indicates the nonzero elements 3, 5, and 7 that represent $\alpha + 1$, $\alpha^2 + \alpha + 1$ and 1, respectively.

3.9.6 Construction of Minimal Polynomials Using MATLAB

The conjugacy classes of the elements of GF(2^m) and associated minimal polynomials can be constructed using the MATLAB commands `cosets` and `minpol`. For example, for GF(2^4), the following MATLAB program constructs the minimal polynomial of the conjugacy class in which α^7 is an element.

```

clear all;
clc;
m=4;
c = cosets(m); % computes conjugacy classes for GF(16)
c{5}'; % conjugacy class in which  $\alpha^7$  is an element
A=gf([c{5}'],m);
pol=minpol(A')% displays coefficients of the minimal
polynomial in descending order
The output of the above program is as follows

```

Primitive polynomial(s) =

$$x^4 + x^1 + 1$$

pol = GF(2) array.

Array elements =

1	1	0	0	1
1	1	0	0	1
1	1	0	0	1
1	1	0	0	1

From the output, array elements indicate the coefficients of the minimal polynomials in the descending order for four elements in the conjugacy class. Hence, the minimal polynomial for the conjugacy class which α^7 is an element is given by $\phi(x) = x^4 + x^3 + 1$.

3.10 Problems

1. Construct modulo- 5 addition and multiplication tables for GF(5).
2. Divide the polynomial $f(x) = 1 + x + x^4 + x^5 + x^6$ by the polynomial $g(x) = 1 + x + x^3$ in GF(2).
3. Find whether each of the following polynomial is irreducible in GF (2).
 - (a) $p(x) = x^2 + x + 1$
 - (b) $p(x) = x^{11} + x^2 + 1$
 - (c) $p(x) = x^{21} + x^2 + 1$
4. Find whether each of the following polynomial is primitive in GF (2).
 - (a) $p(x) = x^4 + x^3 + x^2 + x + 1$
 - (b) $p(x) = x^8 + x^4 + x^3 + x^2 + 1$
 - (c) $p(x) = x^{12} + x^6 + x^4 + x + 1$

5. Construct GF(128) as a vector space over GF(2).
6. When the 64 elements in GF(2^6) are arranged in conjugacy classes and their associated minimal polynomials. Find the minimal polynomial of the conjugacy class in which α^7 is an element.

Chapter 4

Linear Block Codes

This chapter deals with linear block codes covering their fundamental concepts, generator and parity check matrices, error-correcting capabilities, encoding and decoding, and performance analysis. The linear block codes discussed in this chapter are Hamming codes, cyclic codes, binary BCH codes, and Reed–Solomon (RS) codes.

4.1 Block Codes

The data stream is broken into blocks of k bits, and each k -bit block is encoded into a block of n bits with $n > k$ bits as illustrated in Fig. 4.1. The n -bit block of the channel block encoder is called the code word. The code word is formed by adding $(n - k)$ parity check bits derived from the k message bits.

Some important Properties of block codes are defined as

Block Code Rate

The block code rate (R) is defined as the ratio of k message bits and length of the code word n .

$$R = k/n \quad (4.1)$$

Code Word Weight

The weight of a code word or error pattern is the number of nonzero bits in the code word or error pattern. For example, the weight of a code word $c = (1, 0, 0, 1, 1, 0, 1, 0)$ is 4.

Hamming Distance

The Hamming distance between two blocks v and w is the number of coordinates in which the two blocks differ.

Electronic supplementary material The online version of this chapter (doi:[10.1007/978-81-322-2292-7_4](https://doi.org/10.1007/978-81-322-2292-7_4)) contains supplementary material, which is available to authorized users.

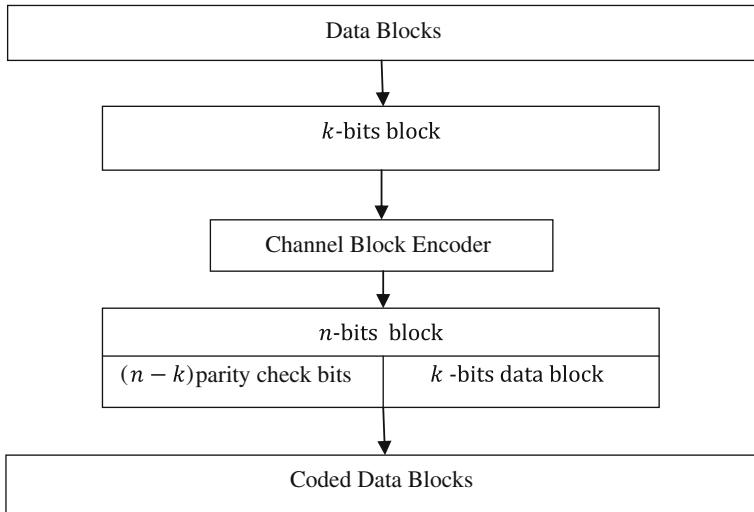


Fig. 4.1 Coded data stream

$$d_{\text{Hamming}}(v, w) = d(v, w) = |\{i | v_i \neq w_i, \quad i = 0, 1, \dots, n-1\}| \quad (4.2)$$

Example 4.1 Consider the code words $v = (00100)$ and $w = (10010)$; then, the Hamming distance $d_{\text{Hamming}}(v, w) = 3$. Hamming distance allows for a useful characterization of the error detection and error-correction capabilities of a block code as a function of the code's minimum distance.

The Minimum Distance of a Block Code

The minimum distance of a block code C is the minimum Hamming distance between all distinct pairs of code words in C .

A code with minimum distance d_{\min} can thus detect all error patterns of weight less than or equal to $(d_{\min} - 1)$.

A code with minimum distance d_{\min} can correct all error patterns of weight less than or equal to $[(d_{\min} - 1)/2]$.

Example 4.2 Consider the binary code C composed of the following four code words.

$$C = \{(00100), (10010), (01001), (11111)\}$$

Hamming distance of (00100) and $(10010) = 3$

Hamming distance of (10010) and $(01001) = 4$

Hamming distance of (00100) and $(01001) = 3$

Hamming distance of (10010) and (11111) = 3
 Hamming distance of (00100) and (11111) = 4
 Hamming distance of (01001) and (11111) = 3
 Therefore, the minimum distance $d_{\min} = 3$.

4.2 Linear Block Codes

A block code C consisting of n -tuples $\{(c_0, c_1, \dots, c_{n-1})\}$ of symbols from GF(2) is said to be binary linear block code if and only if C forms a vector subspace over GF(2). The code word is said to be systematic linear code word, if each of the 2^k code words is represented as linear combination of k linearly independent code words.

4.2.1 Linear Block Code Properties

The two important properties of linear block codes are

- Property 1:** The linear combination of any set of code words is a code word.
Property 2: The minimum distance of a linear block code is equal to the minimum weight of any nonzero word in the code. The two well-known bounds on the minimum distance are

1. Singleton Bound

The minimum distance of a (n, k) linear block code is bounded by

$$d_{\min} \leq n - k + 1 \quad (4.3a)$$

2. Hamming Bound

An (n, k) block code can correct up to t_{ec} errors per code word, provided that n and k satisfy the Hamming bound.

$$2^{n-k} \geq \sum_{i=0}^{t_{\text{ec}}} \binom{n}{i} \quad (4.3b)$$

The relation is the upper bound on the d_{\min} and is known as the Hamming bound. Where

$$\binom{n}{i} = \frac{n!}{(n-1)!i!}; \quad t_{\text{ec}} = (d_{\min} - 1)/2$$

4.2.2 Generator and Parity Check Matrices

Let $\{g_0, g_1, \dots, g_{k-1}\}$ be a basis of code words for the (n, k) linear block code C and $m = (m_0, m_1, \dots, m_{k-1})$ the message to be encoded. It follows from Theorem 3.1 that the code word $c = (c_0, c_1, \dots, c_{n-1})$ for the message is uniquely represented by the following linear combination of g_0, g_1, \dots, g_{k-1}

$$c = m_0g_0 + \dots + m_{k-1}g_{k-1} \quad (4.4)$$

for every code word $c \in C$. Since every linear combination of the basis elements must also be a code word, there is a one-to-one mapping between the set of k -bit blocks $(a_0, a_1, \dots, a_{x-1})$ over GF(2) and the code words in C . A matrix G is constructed by taking the vectors in the basis as its rows.

$$G = \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{bmatrix} = \begin{bmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{bmatrix} \quad (4.5)$$

This matrix is a generator matrix for the code C . It can be used to directly encode k -bit blocks in the following manner.

$$mG = (m_0, m_1, \dots, m_{k-1}) \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{bmatrix} = m_0g_0 + m_1g_1 + \dots + m_{k-1}g_{k-1} = c$$

The dual space of a linear block code C is the dual code of C , and a basis $\{h_0, h_1, \dots, h_{n-k-1}\}$ can be found for dual code of C , and the following parity check matrix can be constructed.

$$H = \begin{bmatrix} h_0 \\ h_1 \\ \vdots \\ h_{n-k-1} \end{bmatrix} = \begin{bmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,n-1} \\ h_{1,0} & h_{1,1} & \cdots & h_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n-k-1,0} & h_{n-k-1,1} & \cdots & h_{n-k-1,n-1} \end{bmatrix} \quad (4.6)$$

In a systematic linear block code, the last k bits of the code word are the message bits, that is,

$$c_i = m_{i-(n-k)}, \quad i = n - k, \dots, n \quad (4.7)$$

The last $n - k$ bits in the code word are check bits generated from the k message bits according to

$$\begin{aligned}
c_0 &= p_{0,0}m_0 + p_{1,0}m_1 + \cdots + p_{k-1,0}m_{k-1} \\
c_1 &= p_{0,1}m_0 + p_{1,1}m_1 + \cdots + p_{k-1,1}m_{k-1} \\
&\vdots \\
c_{n-k-1} &= p_{0,n-k-1}m_0 + p_{1,n-k-1}m_1 + \cdots + p_{k-1,n-k-1}m_{k-1}
\end{aligned}$$

The above equations can be written in matrix form as

$$[c_0, c_1, \dots, c_n] = [m_0, m_1, \dots, m_{k-1}] \begin{bmatrix} p_{0,0} & p_{0,1} & \cdots & p_{0,n-k-1} & 1000 & \cdots & 0 \\ p_{1,0} & p_{1,1} & \cdots & p_{1,n-k-1} & 0100 & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \ddots & \vdots \\ p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,n-k-1} & 0000 & \cdots & 1 \end{bmatrix}_{k \times n} \quad (4.8)$$

or

$$c = mG \quad (4.9)$$

where G is the matrix on the right-hand side of Eq. (4.8). The $k \times n$ matrix G is called the generator matrix of the code, and it has the form

$$G = [P \ : \ I_k]_{k \times n} \quad (4.10)$$

The matrix I_k is the identity matrix of order k and P is an arbitrary k by $n - k$ matrix. When P is specified, it defines the (n, k) block code completely. The parity check matrix H corresponding to the above generator matrix G can be obtained as

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & p_{0,0} & p_{1,0} & \cdots & p_{k-1,0} \\ 0 & 1 & 0 & 0 & \cdots & 0 & p_{0,1} & p_{1,1} & \cdots & p_{k-1,1} \\ \vdots & & \vdots & \vdots & & & \vdots & & & \\ 0 & 0 & 0 & 0 & \cdots & 1 & p_{0,n-k-1} & p_{1,n-k-1} & \cdots & p_{k-1,n-k-1} \end{bmatrix} \quad (4.11)$$

$$H = \begin{bmatrix} I_{n-k} & P^T \end{bmatrix} \quad (4.12)$$

The Parity Check Theorem

The parity check theorem states that “For an (n, k) linear block code C with $(n - k) \times n$ parity check matrix H , a code word $c \in C$ is a valid code word if and only if $cH^T = 0$.”

Example 4.3 Consider the following generator matrix of (7,4) block code. Find the code vector for the message vector $m = (1110)$, and check the validity of code vector generated.

$$G = \left[\begin{array}{c|cccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array} \right]$$

Solution The code vector for the message block $m = (1110)$ is given by

$$\begin{aligned} c = mG &= (1 \ 1 \ 1 \ 0) \left[\begin{array}{cccccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array} \right] \\ &= (0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0) \\ H &= \left[\begin{array}{c|ccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array} \right] \\ cH^T &= [0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0] \left[\begin{array}{c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{array} \right] = [0 \ 0 \ 0] \end{aligned}$$

Hence, the generated code vector is valid.

4.2.3 Weight Distribution of Linear Block Codes

An (n, k) code contains 2^k code words with the Hamming weights between 0 and n . For $0 \leq i \leq n$, let W_j be the number of code words in C with Hamming weight j . The w_0, w_1, \dots, w_{n-1} are the weight distribution of C so that $w_0 + w_1 + w_2 + \dots + w_n = 2^k$. The weight distribution can be written as the polynomial $W(x) = w_0 + w_1x + w_2x^2 + \dots + w_{n-1}x^{n-1}$ which is called as weight enumerator. The weight distribution of a linear block code is related to the parity check matrix H by the following theorem,

“The minimum weight (or minimum distance) of an (n, k) linear block code with a parity check matrix H is equal to the minimum number of nonzero columns in H whose vector sum is a zero vector.”

4.2.4 Hamming Codes

Hamming code is a linear block code capable of correcting single errors having a minimum distance $d_{\min} = 3$. It is very easy to construct Hamming codes. The parity check matrix H must be chosen so that no row in H^T is zero and the first $(n - k)$ rows of H^T form an identity matrix and all the rows are distinct.

We can select $2^{n-k} - 1$ distinct rows of H^T . Since the matrix H^T has n rows, for all of them to be distinct, the following inequality should be satisfied

$$2^{n-k} - 1 \geq n \quad (4.13)$$

implying that

$$\begin{aligned} (n - k) &\geq \log_2(n + 1) \\ n &\geq k + \log_2(n + 1) \end{aligned} \quad (4.14)$$

Hence, the minimum size n for the code words can be determined from Eq. (4.14).

Example 4.4 Design a Hamming code with message block size of eleven bits.

Solution It follows from Eq. (4.14) that

$$n \geq 11 + \log_2(n + 1)$$

The smallest n that satisfies the above inequality is 15; hence, we need a (15,11) block code. Thus, the transpose of the parity check matrix H will be 4 by 15 matrix. The first four rows of H^T will be 4×4 identity matrix. The last eleven rows are arbitrarily chosen, with the restrictions that no row is zero, and all the rows are distinct.

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$H^T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \dots & \dots & \dots & \dots \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} I_{n-k} \\ \dots \\ P^T \end{bmatrix}$$

Then, the generator matrix G is

$$G = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Example 4.5 Construct parity check and generator matrices for a (7,4) Hamming code.

Solution The parity check matrix (H) and generator matrix (G) for a (7,4) Hamming code are

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

4.2.5 Syndrome Table Decoding

Consider a valid code word c for transmission, and let e be an error pattern introduced by the channel during transmission. Then, the received vector r can be written as

$$r = c + e \quad (4.15a)$$

Multiplying the r by the transpose of the parity check matrix gives the syndrome S which can be expressed as

$$\begin{aligned} S &= rH^T \\ &= (c + e)H^T \\ &= cH^T + eH^T \\ &= 0 + eH^T \\ &= eH^T \end{aligned} \quad (4.15b)$$

Thus, the syndrome vector is independent of the transmitted code word c and is only a function of the error pattern e . Decoding is performed by computing the syndrome of a received vector, looking up the corresponding error pattern, and subtracting the error pattern from the received word.

Example 4.6 Construct a syndrome decoding table for a (7,4) Hamming code.

Solution For a (7,4) Hamming code, there are $2^{(7-4)}$ error patterns (e) as follows

$$\begin{array}{cccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}$$

The syndrome for (7,4) Hamming code is computed using the parity check matrix H as given in solution of Example 4.4 as follows

$$s = e * H^T$$

Thus, the syndrome decoding table for a (7,4) Hamming code is as follows (Table 4.1).

Table 4.1 Syndrome decoding table for a (7,4) Hamming code

Error pattern	Syndrome
0 0 0 0 0 0 0	0 0 0
1 0 0 0 0 0 0	1 0 0
0 1 0 0 0 0 0	0 1 0
0 0 1 0 0 0 0	0 0 1
0 0 0 1 0 0 0	1 1 0
0 0 0 0 1 0 0	0 1 1
0 0 0 0 0 1 0	1 1 1
0 0 0 0 0 0 1	1 0 1

4.2.5.1 Hamming Codes Decoding

Syndrome table is used to decode the Hamming codes. The syndrome table gives the syndrome value based on the simple relationship with parity check matrix. The single error-correcting codes, i.e., Hamming codes, are decoded by using syndrome value. Consider a code word c corrupted by e an error pattern with a single one in the j th coordinate position results a received vector r . Let $\{h_0, h_1, \dots, h_{n-1}\}$ be the set of columns of the parity check matrix H . When the syndrome is computed, we obtain the transposition of the j th column of H .

$$s = rH^T = eH^T = (0, \dots, 0, 1, 0, \dots, 0) \begin{bmatrix} h_0^T \\ h_1^T \\ \vdots \\ h_{n-1}^T \end{bmatrix} = h_j^T \quad (4.16)$$

The above-mentioned process can be implemented using the following algorithm.

1. Compute the syndrome s for the received word. If $s = 0$, the received code word is the correct code word.
2. Find the position j of the column of H that is the transposition of the syndrome.
3. Complement the j th bit in the received code word to obtain the corrected code word.

Example 4.7 Decode the received vector $r = (010000000000000)$ using the (15,11) parity check matrix.

Solution

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

The received vector is $r = (010000000000000)$

The corresponding syndrome $s = r * H^T$ is

$$s = (0100)$$

The syndrome is the transposition of 1st column of H . Inverting the 1st coordinate of r , the following code word is obtained

$$c = (000000000000000)$$

Example 4.8 Decode the received vector $r = (001100011100000)$ vector using the $(15,11)$ parity check matrix vector.

Solution The received vector is $r = (001100011100000)$. The corresponding syndrome $s = r * H^T$ is $s = (0011)$. The syndrome is the transposition of 7th column of H . Inverting the 7th coordinate of r , the following code word is obtained

$$c = (001100001100000)$$

4.3 Cyclic Codes

An (n, k) linear block code C is said to be a cyclic code if for every codeword $c = (c_0, c_1, \dots, c_{n-2}, c_{n-1}) \in C$, there is also a codeword $c_1 = (c_{n-1}, c_0, c_1, \dots, c_{n-2})$ obtained by shifting c cyclically one place to the right is also code word in C .

4.3.1 The Basic Properties of Cyclic Codes

Property 1: In an (n, k) cyclic code, there exists a unique polynomial called generator polynomial $g(x)$ of minimal degree $(n - k)$ of the following form:

$$g(x) = g_1x + g_2x^2 + \cdots + g_{n-k-1}x^{n-k-1} + g_{n-k}x^{n-k} \quad (4.17)$$

Property 2: Every code polynomial in an (n, k) cyclic code is multiple of $g(x)$. Thus, it can be expressed as $c(x) = m(x)g(x)$, where $m(x)$ is a polynomial over GF(2) of degree $k - 1$ or less.

Property 3: The generator polynomial $g(x)$ of an (n, k) cyclic code over GF(2) divides $x^n + 1$.

Property 4: The generator polynomial $g(x)$ and the parity check matrix $h(x)$ are factor of the polynomial $1 + x^n$.

In modulo-2 arithmetic $1 + x^n$ has the same value $1 - x^n$.

Example 4.9 Let C_1 be the binary cyclic code of length 15 generated by $g(x) = x^5 + x^4 + x^2 + 1$. Compute the code polynomial in C_1 and the associated code word for the message polynomial $m(x) = x^9 + x^4 + x^2 + 1$ using the polynomial multiplication encoding technique.

Solution Here

$$m(x) = x^9 + x^4 + x^2 + 1; \quad g(x) = x^5 + x^4 + x^2 + 1$$

code polynomial

$$c(x) = m(x)g(x) = x^{14} + x^{13} + x^{11} + x^8 + x^7 + x^5 + x^4 + 1$$

Code word = (100011011001011).

Example 4.10 Let C_1 be the binary cyclic code of length 15 generated by $g(x) = x^5 + x^4 + x^2 + 1$. Determine the dimensions of C_1 , and compute the number of code words in C_1 .

Solution Since the order of the generator polynomial is 5, the C_1 has dimension $(15, 10)$ with $k = (15 - 5) = 10$ and contains 2^{15-5} code words.

Example 4.11 Let C_1 be the binary cyclic code of length 15 generated by $g(x) = x^5 + x^4 + x^2 + 1$. Compute the parity check polynomial for C_1 , and show that $g(x)$ is a valid generator polynomial.

Solution $g(x) = x^5 + x^4 + x^2 + 1$. The parity check polynomial for C_1 is

$$h(x) = \frac{x^{15} + 1}{g(x)} = x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$$

$g(x)$ is valid generator polynomial since it has the minimum polynomials $x^4 + x + 1$ and $x + 1$ as factors, i.e., $g(x) = (x^4 + x + 1)(x + 1)$.

4.3.2 Encoding Algorithm for an (n, k) Cyclic Codes

In an (n, k) cyclic code C with generator polynomial $g(x)$, let $m = (m_0, m_1, \dots, m_{k-1})$ is the message block. By multiplying the message polynomial

$m(x)$ by x^{n-k} , we obtain a polynomial $x^{n-k}m(x) = m_0x^{n-k} + m_1x^{n-k+1} + \dots + m_{k-1}x^{n-1}$ of degree $n-1$ or less. Now, dividing $x^{n-k}m(x)$ by $g(x)$ yields

$$x^{n-k}m(x) = q(x)g(x) + p(x) \quad (4.18)$$

where $q(x)$ and $p(x)$ are the quotient and remainder, respectively.

Equation (4.18) can be rearranged as

$$p(x) + x^{n-k}m(x) = q(x)g(x) \quad (4.19)$$

Equation (4.19) shows that $p(x) + x^{n-k}m(x)$ is divisible by $g(x)$. Hence, it must be a valid code polynomial $c(x) = p(x) + x^{n-k}m(x)$ of the (n, k) cyclic code C with generator polynomial $g(x)$. The n -tuple representation of the code polynomial $c(x)$ is

$$c = (p_0, p_1, \dots, p_{n-k-1}, m_0, m_1, \dots, m_{k-1}) \quad (4.20)$$

The systematic encoding algorithm is summarized as

Step 1: Multiply the message polynomial $m(x)$ by x^{n-k}

Step 2: Divide the result of Step 1 by the generator polynomial $g(x)$. Let $d(x)$ be the remainder.

Step 3: Set $c(x) = x^{n-k}m(x) - d(x)$.

Example 4.12 Let C_1 be the binary cyclic code of length 15 generated by $g(x) = x^5 + x^4 + x^2 + 1$. Compute the code polynomial in C_1 and the associated code word for the message polynomial $m(x) = x^8 + x^7 + x^6 + x^5 + x^4$ using the systematic encoding technique. Verify that the message has been systematically encoded.

Solution

$$g(x) = x^5 + x^4 + x^2 + 1; \quad m(x) = x^8 + x^7 + x^6 + x^5 + x^4$$

$$\text{Step 1: } x^5m(x) = x^5(x^8 + x^7 + x^6 + x^5 + x^4) = x^{13} + x^{12} + x^{11} + x^{10} + x^9$$

$$\begin{array}{r}
 \textbf{Step 2 } x^5 + x^4 + x^2 + 1) \quad \frac{x^8 + x^6 + x^5 + x^2 + 1}{x^{13} + x^{12} + x^{11} + x^{10} + x^9} \\
 \qquad \qquad \qquad \frac{x^{13} + x^{12} + x^{10} + x^5}{x^{11} + x^9 + x^8} \\
 \qquad \qquad \qquad \frac{x^{11} + x^{10} + x^8 + x^6}{x^{10} + x^9 + x^6} \\
 \qquad \qquad \qquad \frac{x^{10} + x^9 + x^7 + x^5}{x^7 + x^6 + x^5} \\
 \qquad \qquad \qquad \frac{x^7 + x^6 + x^4 + x^2}{x^5 + x^4 + x^2} \\
 \qquad \qquad \qquad \frac{x^5 + x^4 + x^2 + 1}{1 = d(x)}
 \end{array}$$

Step 3: $c_m(x) = x^{13} + x^{12} + x^{11} + x^{10} + x^9 + 1 \leftrightarrow c_m = (10000011111110)$.

Example 4.13 Construct parity check and generator matrices for binary cyclic code of length 15 generated by $g(x) = x^5 + x^4 + x^2 + 1$.

Solution The systematic generator matrix is obtained by selecting as rows those code words associated with the message blocks (1000000000) , (0100000000) , (0010000000) , (0001000000) , (0000100000) , (0000010000) , (0000001000) , (0000000100) , (0000000010) , and (1000000001) .

$m(x)$	Code polynomial $c(x)$	Codeword
1	$1 + x^2 + x^4 + x^5$	$\leftrightarrow (101011000000000)$
x	$1 + x + x^2 + x^3 + x^4 + x^6$	$\leftrightarrow (111110100000000)$
x^2	$1 + x + x^3 + x^7$	$\leftrightarrow (110100010000000)$
x^3	$x + x^2 + x^4 + x^8$	$\leftrightarrow (011010001000000)$
x^4	$1 + x^3 + x^4 + x^9$	$\leftrightarrow (100110000100000)$
x^5	$1 + x + x^2 + x^{10}$	$\leftrightarrow (111000000010000)$
x^6	$x + x^2 + x^3 + x^{11}$	$\leftrightarrow (011100000001000)$
x^7	$x^2 + x^3 + x^4 + x^{12}$	$\leftrightarrow (001110000000100)$
x^8	$1 + x^2 + x^3 + x^{13}$	$\leftrightarrow (101100000000010)$
x^9	$x + x^3 + x^4 + x^{14}$	$\leftrightarrow (010110000000001)$

The generator matrix (G) and parity check matrix (H) for the cyclic code are

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The corresponding parity check matrix is

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

4.3.3 Encoder for Cyclic Codes Using Shift Registers

The systematic encoder for cyclic codes is shown in Fig. 4.2. The rectangular boxes represent flip-flops which reside either in 0 or 1 state. The encoder operation is as follows.

1. The switches are placed in position in 1. The k message bits are sent to the modulator and placed at the end of the systematic code word. As soon as the k th message bit is fed into the shift register, the flip-flops of the shift register contain $(n - k)$ parity bits.
2. The switches are moved to the position 2 to break the feedback connection.
3. The parity bits in the shift register are shifted out into the transmitter to form the parity bits of the systematic code word.

Example 4.14 Construct the shift register encoder for a cyclic code of length 7 generated by $g(x) = x^4 + x^3 + x^2 + 1$, and obtain the code word for message $m = (010)$.

Solution The shift register for encoding the (7,3) cyclic code with generator polynomial $g(x) = x^4 + x^3 + x^2 + 1$ is shown in Fig. 4.3. The given message bits are 010. The contents of the shift register are shown in Table 4.2. Hence, the four parity check bits are 0111. Therefore, the code word output is 0111010.

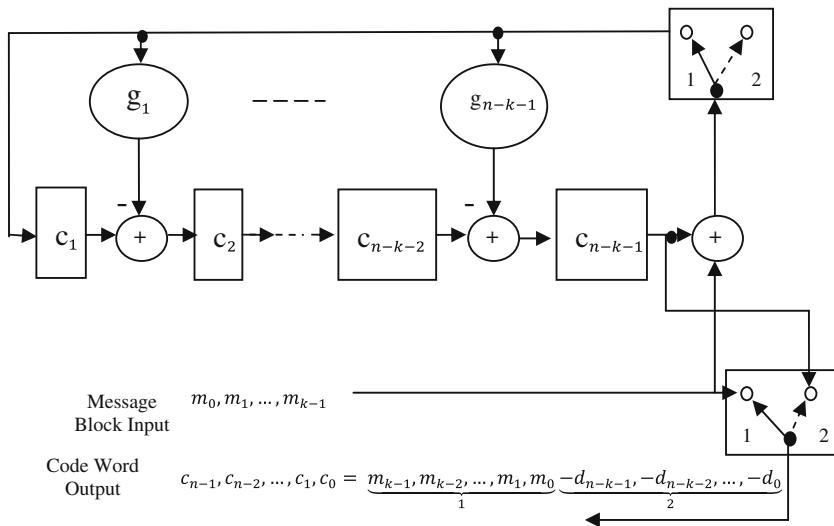


Fig. 4.2 Encoding circuit for (n, k) cyclic code

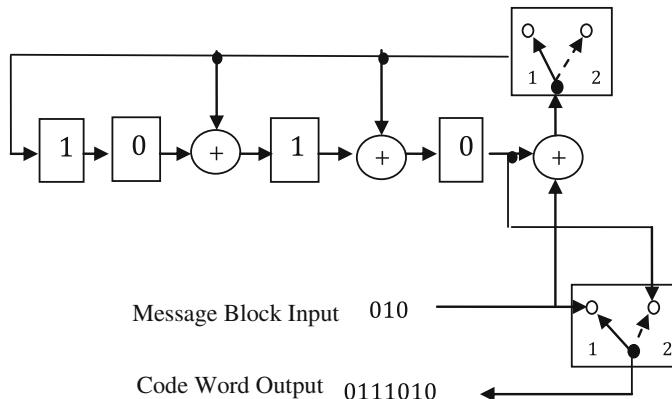


Fig. 4.3 Encoder for an $(7,3)$ cyclic code generated by $g(x) = x^4 + x^3 + x^2 + 1$

Table 4.2 Contents of the shift register in the encoder of Fig. 4.3 for message sequence (010)

Shift	Input	Register code words			
		0	0	0	0
1	0	0	0	0	0
2	1	1	0	1	0
3	0	0	1	1	1

4.3.4 Shift Register Encoders for Cyclic Codes

Suppose the code word $(c_0, c_1, \dots, c_{n-1})$ is transmitted over a noisy channel resulting in the received word $(r_0, r_1, \dots, r_{n-1})$. Let the received word be represented by a polynomial of degree $n - 1$ or less as

$$r(x) = r_0 + r_1x + \cdots + r_{n-1}x^{n-1} \quad (4.21)$$

Dividing the $r(x)$ by $g(x)$ results in the following

$$r(x) = q(x)g(x) + s(x) \quad (4.22)$$

where $q(x)$ is the quotient and $s(x)$ is the remainder known as syndrome. The $s(x)$ is a polynomial of degree $n - k - 1$ or less, and its coefficients make up the $(n - 1)$ -by-1 syndrome s . An error in the received word is detected only when the syndrome polynomial $s(x)$ is nonzero.

Syndrome Calculator

The syndrome calculator shown in Fig. 4.4 is similar to the encoder shown in the Fig. 4.2. The only difference is that the received bits are fed from left into the $(n - k)$ stages of the feedback shift register. At the end of the last received bit shifting, the contents of the shift register contain the desired syndrome s . If the syndrome is zero, there are no transmission errors in the received word or else the received code word contains transmission error. By knowing the value of syndrome, we can determine the corresponding error pattern and also make the appropriate correction.

Example 4.15 Consider the (7,4) Hamming code generator polynomial $g(x) = x^3 + x + 1$ and the transmitted code word 1100101. Show the fifth bit of the received word is an error (Table 4.3).

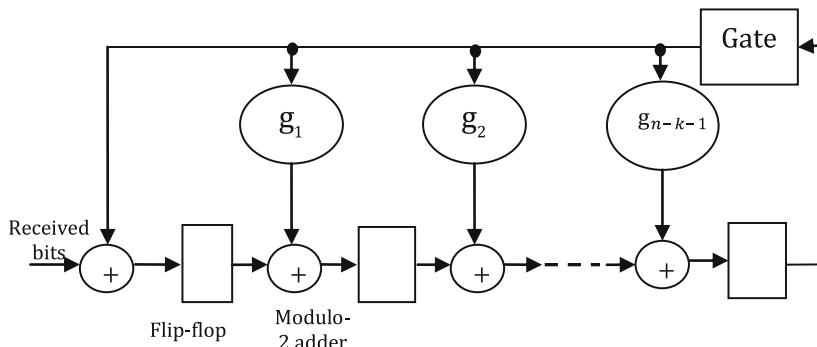


Fig. 4.4 Syndrome calculator

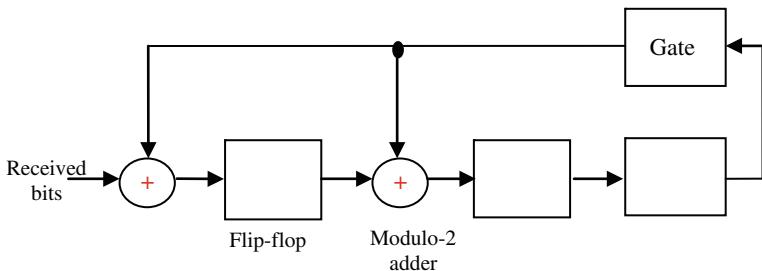


Fig. 4.5 Syndrome calculator of Example 4.15

Table 4.3 Contents of the shift register in the encoder of Fig. 4.5

Shift	Input bit	Contents of shift register
		000
1	1	100
2	0	010
3	1	101
4	0	100
5	1	110
6	1	111
7	1	001

Solution Given $g(x) = x^3 + x + 1$

Transmitted code word = 1100101

By considering the fifth bit as an error, the received word = 1110101.

At the end of the seventh shift, the contents of the shift register (syndrome) is 001. The nonzero value of the syndrome indicates the error, and the error pattern for the syndrome 001 is 0010000 from the Table 4.1. This shows that the fifth bit of the received word is an error.

4.3.5 Cyclic Redundancy Check Codes

Cyclic redundancy check (CRC) code is a cyclic code used for error detection. CRC codes are implemented from cyclic codes and hence the name, even when they are generally not cyclic. The following three CRC codes given in Table 4.4 have become international standard.

Table 4.4 International standard CRC codes

CRC code	Description	Error detection capability	Burst error detection capability
CRC-12	$g(x) = x^{12} + x^{11} + x^3 + x^2 + x + 1$ $= (x^{11} + x^2 + 1)(x + 1)$ Code length: 2047 Number of parity bits: 12 $d_{\min} = 4$	One-bit errors, two- and three-bit errors of length up to 2047. All error pattern with an odd number of error if the generator polynomial $g(x)$ for the code has an even number of nonzero coefficients	All burst errors up to length 12
CRC-16	$g(x) = x^{16} + x^{15} + x^2 + 1$ $= (x^{15} + x + 1)(x + 1)$ Code length: 32767 Number of parity bits: 16 $d_{\min} = 4$	All one-bit errors, two- and three-bit errors of length up to 32767. All error pattern with an odd number of error if the generator polynomial $g(x)$ for the code has an even number of nonzero coefficients	All burst errors up to length 16
CRC-CCITT	$g(x) = x^{16} + x^{12} + x^5 + 1$ $= (x^{15} + x^{14} + x^{13} + x^{12} + x^4 + x^3 + x^2 + x + 1)(x + 1)$ Code length: 32767 Number of parity bits: 16 $d_{\min} = 4$	All one-bit errors, two- and three-bit errors of length up to 32767. All error pattern with an odd number of error if the generator polynomial $g(x)$ for the code has an even number of nonzero coefficients	All burst errors up to length 16

4.4 BCH Codes

BCH codes are a subclass of cyclic codes. The BCH codes are introduced independently by Bose, Ray-Chauduri, and Hocquenghem. For $m > 3$ and $t_{\text{ec}} < 2^{m-1}$, there exists a BCH code with parity check bits $(n - k) \leq mt_{\text{ec}}$ and $d_{\min} \geq 2t_{\text{ec}} + 1$.

4.4.1 BCH Code Design

If a primitive element α of $\text{GF}(2^m)$ is chosen, then the generator polynomial $g(x)$ of the t_{ec} error-correcting binary BCH code of length $2^m - 1$ is the minimum degree polynomial over $\text{GF}(2)$ having $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{2t_{\text{ec}}}$ as roots. Suppose $\phi_i(\alpha)$ be the minimal polynomial of α^i , $1 \leq i \leq 2t_{\text{ec}}$ for t_{ec} error-correcting binary BCH code.

Then, the generator polynomial $g(x)$ is the least common multiple (LCM) of $\phi_1(\alpha), \phi_2(\alpha), \dots, \phi_{2t_{\text{ec}}}(\alpha)$, i.e.,

$$g(x) = \text{LCM}\{\phi_1(\alpha), \phi_2(\alpha), \dots, \phi_{2t_{\text{ec}}}(\alpha)\} \quad (4.23)$$

Let $c(x) = c_0 + c_1\alpha^i + c_2\alpha^{2i} + \dots + c_{2^m-2}\alpha^{(2^m-2)i}$ be a code polynomial. Since $c(x)$ is divisible by $g(x)$, a root of $g(x)$ is also a root of $c(x)$. Hence, for $1 \leq i \leq 2t_{\text{ec}}$,

$$c(\alpha^i) = c_0 + c_1\alpha^i + c_2\alpha^{2i} + \dots + c_{2^m-2}\alpha^{(2^m-2)i} = 0 \quad (4.24)$$

Equation (4.24) can be rewritten in matrix form as

$$(c_0, c_1, \dots, c_{2^m-2}) \cdot \begin{pmatrix} 1 \\ \alpha^i \\ \alpha^{2i} \\ \vdots \\ \alpha^{(2^m-2)i} \end{pmatrix} = 0 \quad (4.25)$$

It follows that $c \cdot H^T = 0$ for every code word $c = (c_0, c_1, \dots, c_{2^m-2})$ in the t_{ec} error-correcting BCH code of length $2^m - 1$ generated by $g(x)$. Hence, for $g(x)$, the corresponding $2t \times (2^m - 1)$ matrix over $\text{GF}(2^m)$ can be formed as

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{(2^m-2)} \\ 1 & \alpha^2 & (\alpha^2)^2 & \dots & (\alpha^2)^{2^m-2} \\ 1 & \alpha^3 & (\alpha^3)^2 & \dots & (\alpha^3)^{2^m-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2^l} & (\alpha^{2^l})^2 & \dots & (\alpha^{2^l})^{2^m-2} \end{bmatrix} \quad (4.26)$$

If $\phi(x)$ is the minimal polynomial of an element β of the $\text{GF}(2^m)$ and $l(l \leq m)$ is the smallest positive integer such that $\beta^{2^l} = \beta$, then from Theorem 3.7, $\phi(x)$ of degree m or less is given by

$$\phi(x) = \prod_{i=0}^{l-1} (X - \beta^{2^i}) \quad (4.27)$$

The conjugates of β are the roots of $\Phi_\beta(x)$ of the form β^{2^i} , $1 < i < l - 1$.

From Theorem 3.6, the roots of $\Phi_\beta(x)$ having the conjugacy class will have the same minimal polynomial.

The stepwise procedure to find the minimal polynomial $\Phi_\beta(x)$ is as follows:

Step 1: Determine the conjugates class of β

Step 2: Obtain $\Phi_\beta(x)$ using Eq. (4.27)

The design procedure of t_{ec} -error-correcting binary BCH code of length n is as follows:

1. Choose a primitive root α in a field $\text{GF}(2^m)$.
2. Select $2t_{\text{ec}}$ consecutive powers of α .
3. Obtain the minimal polynomials for all the $2t_{\text{ec}}$ consecutive powers of α having the same minimal polynomial for the roots in the same conjugacy class.
4. Obtain the generator polynomial $g(x)$ by taking the LCM of the minimal polynomials for the $2t_{\text{ec}}$ consecutive powers of α .

The construction of BCH codes are illustrated through the following examples.

Example 4.16 Compute a generator polynomial for a binary BCH code of length 15 and minimum distance 3, and find the code rate.

Solution Since 15 is of the form $2^m - 1$, the BCH codes are primitive. Let α be a primitive element in the field $\text{GF}(16)$ generated by the primitive polynomial $1 + x + x^4$. The elements of the field $\text{GF}(16)$ are given in Table 3.3. Since the code is to be single error correcting (minimum distance = 3), the generator polynomial thus must have α and α^2 as roots. The α and α^2 are conjugate elements and have the same minimal polynomial, which is $1 + x + x^4$. The generator polynomial is thus

$$g(x) = 1 + x + x^4$$

Since the degree of $g(x)$ is 4, the BCH code generator by $g(x)$ is a (15,11) code. The rate of the code is

$$R = \frac{k}{n} = \frac{11}{15}$$

Example 4.17 Design a double-error-correcting binary BCH code of length 15.

Solution Since 15 is of the form $2^m - 1$, the BCH codes are primitive. Let α be a primitive element in the field $\text{GF}(16)$ generated by the primitive polynomial $1 + x + x^4$. The elements of the field $\text{GF}(16)$ are given in Table 3.3.

Since the code is to be double error correcting, the generator polynomial thus must have $\alpha, \alpha^2, \alpha^3, \alpha^4$ as roots.

The α, α^2 and α^4 are conjugates and have the same minimal polynomial, which is $1 + x + x^4$. Thus,

$$\phi_\alpha(x) = \phi_{\alpha^2}(x) = \phi_{\alpha^4}(x) = 1 + x + x^4$$

By letting $\beta = \alpha^3$

$$\beta^{2^4} = (\alpha^3)^{16} = \alpha^{48} = \alpha^{45}\alpha^3 = 1 \cdot \alpha^3 = \alpha^3$$

Therefore, $l = 4$, and from Eq. (4.28), the minimal polynomial $\phi_{\alpha^3}(x)$ is given by

$$\begin{aligned}\phi_{\alpha^3}(x) &= \prod_{i=0}^{l-1} (x - \beta^{2^i}) = \prod_{i=0}^{4-1} (x - \beta^{2^i}) \\ &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24}) \\ \phi_{\alpha^3}(x) &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) \\ &= 1 + x + x^2 + x^3 + x^4\end{aligned}$$

Hence,

$$\begin{aligned}g(x) &= g(x) = (1 + x + x^4)(1 + x^4 + x^6 + x^7 + x^8) \\ &= 1 + x^4 + x^6 + x^7 + x^8\end{aligned}$$

Since the degree of $g(x)$ is 8, the BCH code generator by $g(x)$ is a (15,7) code with minimum distance 5.

Example 4.18 Design a triple-error-correcting binary BCH code of length 63.

Solution Let α be a primitive element in the field GF(16) generated by the primitive polynomial $1 + x + x^4$. The elements of the field GF(16) are given in Table 3.3. Since the code is to be triple error correcting, the generator polynomial thus must have $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$ as roots. α, α^2 and α^4 are conjugate elements and have the same minimal polynomial, which is $1 + x + x^6$.

Thus,

$$\phi_{\alpha}(x) = \phi_{\alpha^2}(x) = \phi_{\alpha^4}(x) = 1 + x + x^6$$

The elements α^3 and α^6 are conjugates and have the same minimal polynomial. By letting $\beta = \alpha^3$

$$\beta^{2^6} = (\alpha^3)^{64} = \alpha^{192} = \alpha^{63}\alpha^{63}\alpha^{63}\alpha^3 = 1 \cdot \alpha^3 = \alpha^3$$

Therefore, $l = 6$, and from Eq. (4.28), the minimal polynomials $\phi_{\alpha^3}(x)$ and $\phi_{\alpha^6}(x)$ are the same and are given by

$$\begin{aligned}\phi_{\alpha^3}(x) &= \phi_{\alpha^6}(x) = \prod_{i=0}^{l-1} (x - \beta^{2^i}) = \prod_{i=0}^{6-1} (x - \beta^{2^i}) \\ &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24})(x - \alpha^{48})(x - \alpha^{96}) \\ &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24})(x - \alpha^{48})(x - \alpha^{33}) \\ &= 1 + x + x^2 + x^4 + x^6\end{aligned}$$

By letting $\beta = \alpha^5$

$$\beta^{2^6} = (\alpha^5)^{64} = \alpha^{320} = \alpha^{63}\alpha^{63}\alpha^{63}\alpha^{63}\alpha^3 = 1 \cdot \alpha^5 = \alpha^5$$

Therefore, $l = 6$, and from Eq. (4.28), the minimal polynomial $\phi_{\alpha^3}(x)$ is given by

$$\begin{aligned}\phi_{\alpha^5}(x) &= \prod_{i=0}^{l-1} (x - \beta^{2^i}) = \prod_{i=0}^{6-1} (x - \beta^{2^i}) \\ &= (x - \alpha^5)(x - \alpha^{10})(x - \alpha^{20})(x - \alpha^{40})(x - \alpha^{80})(x - \alpha^{160}) \\ &= (x - \alpha^5)(x - \alpha^{10})(x - \alpha^{20})(x - \alpha^{40})(x - \alpha^{17})(x - \alpha^{34}) \\ &= 1 + x + x^2 + x^5 + x^6\end{aligned}$$

It follows from Eq. (4.24) that the generator polynomial of the triple-error-correcting BCH code of length 63 is given by

$$\begin{aligned}g(x) &= (1 + x + x^6)(1 + x + x^2 + x^4 + x^6)(1 + x + x^2 + x^5 + x^6) \\ &= 1 + x + x^2 + x^3 + x^6 + x^7 + x^9 + x^{15} + x^{16} + x^{17} + x^{18}\end{aligned}$$

Since the degree of $g(x)$ is 18, the BCH code generator by $g(x)$ is a (63,45) code with minimum distance 7.

Example 4.19 Construct generator and parity check matrices for a single-error-correcting BCH code of length 15.

Solution A parity check matrix for this code is obtained by using Eq. (4.27) as

$$H = \left[\begin{array}{cccccc} 1 & \alpha & \alpha^2 & \dots & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{11} & \alpha^{13} \end{array} \right]$$

This parity check matrix has redundancy because α and α^2 conjugates. Hence, the parity check matrix without redundancy is

$$H = \left[\begin{array}{cccccc} 1 & \alpha & \alpha^2 & \dots & \alpha^{13} & \alpha^{14} \end{array} \right]$$

Note that the entries of H are elements in $GF(2^4)$. Each element in $GF(2^4)$ can be represented by 4 tuples over $GF(2)$. If each entry of H is replaced by its corresponding 4 tuples over $GF(2)$ arranged in column form, we obtain a binary parity check matrix for the code as follows:

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

The corresponding generator matrix is

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

4.4.2 Berlekamp's Algorithm for Binary BCH Codes Decoding

Let code polynomial $c(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \dots + c_1x + c_0$, an error polynomial $e(x) = e_{n-1}x^{n-1} + e_{n-2}x^{n-2} + \dots + e_1x + e_0$, and received polynomial $r(x) = r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \dots + r_1x + r_0$.

Then, $r(x)$ can be written as

$$r(x) = c(x) + e(x) \quad (4.28)$$

Let $S = [S_1 S_2 \dots S_{2t_{\text{ec}}}]$ be syndrome sequence with $2t_{\text{ec}}$ known syndrome components. Then, the syndrome polynomial can be written as

$$S(x) = S_{2t_{\text{ec}}}x^{2t_{\text{ec}}} + S_{2t_{\text{ec}}-1}x^{2t_{\text{ec}}-1} + \dots + S_1x \quad (4.29)$$

where t_{ec} stands for error-correcting capability. By evaluating the received polynomial at $2t_{\text{ec}}$ zeros, the syndromes $S_1 S_2 \dots S_{2t_{\text{ec}}}$ can be obtained. Thus,

$$\begin{aligned} S_i = r(\alpha^i) &= r_{n-1}(\alpha^i)^{n-1} + r_{n-2}(\alpha^i)^{n-2} \\ &\quad + \dots + r_1(\alpha^i) + r_0 \quad \text{for } 1 \leq i \leq 2t_{\text{ec}} \end{aligned} \quad (4.30)$$

The syndrome sequence $S_1 S_2 \dots S_{2t_{\text{ec}}}$ can be rewritten as

$$\begin{aligned} S_i = e(\alpha^i) &= e_{n-1}(\alpha^i)^{n-1} + e_{n-2}(\alpha^i)^{n-2} \\ &\quad + \dots + e_1(\alpha^i) + e_0 \quad \text{for } 1 \leq i \leq 2t_{\text{ec}} \end{aligned} \quad (4.31)$$

Assuming that the received word r has v errors in positions j_1, j_2, \dots, j_v , the error locator polynomial can be expressed as

$$\begin{aligned} \Lambda(x) &= \Lambda_v x^v + \Lambda_{v-1} x^{v-1} + \dots + \Lambda_1 x + 1 \\ &= (1 - \alpha^{j_1} x)(1 - \alpha^{j_2} x) \dots (1 - \alpha^{j_v} x) \end{aligned} \quad (4.32)$$

The error magnitude polynomial is defined as

$$\Omega(x) = \Lambda(x)(1 + S(x)) \bmod x^{2t_{\text{ec}}+1} \quad (4.33)$$

This is useful in non-binary decoding.

Berlekamp's algorithm proceeds for binary decoding of BCH codes iteratively by breaking down into a series of smaller problems of the form

$$[1 + S(x)]\Lambda^{(2n)}(x) \equiv (1 + \Omega_2 x^2 + \Omega_4 x^4 + \dots + \Omega_{2n} x^{2n}) \bmod x^{2n+1} \quad (4.34)$$

where n runs from 1 to t_{ec} . The flowchart of the Berlekamp's iterative algorithm is shown in Fig. 4.6.

4.4.3 Chien Search Algorithm

A Chien search is shown in Fig. 4.7. The Chien search is a systematic means of evaluating the error locator polynomial at all elements in a field $\text{GF}(2^m)$. Each coefficient of the error locator polynomial is repeatedly multiplied by α^i , where α is primitive in $\text{GF}(2^m)$. Each set of products is then summed to obtain $A_i = \Lambda(\alpha^i) - 1$. If α^i is a root of $\Lambda(x)$, then $A_i = \Lambda(\alpha^i) - 1$ and an error is indicated at the coordinate associated with $\alpha^{-i} = \alpha^{n-i}$.

Example 4.20 Let the transmission code be the triple-error-correcting binary BCH code of length 15. The generator polynomial is $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$. Use Berlekamp's algorithm to decode the following received vector $r = (000101000000100)$.

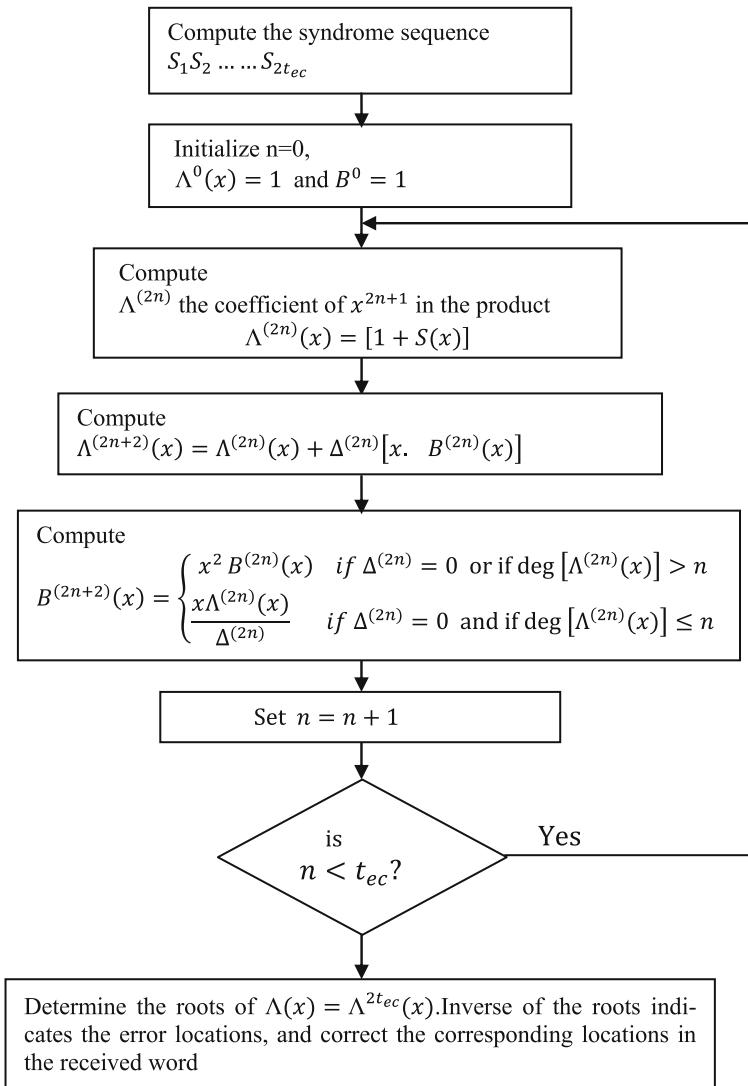
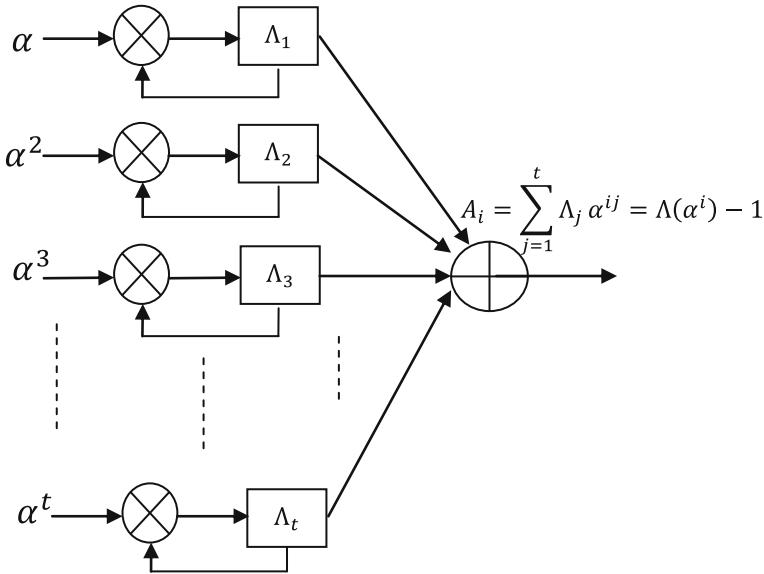


Fig. 4.6 Berlekamp iterative algorithm for decoding binary BCH codes

Solution For double error correction, the generator polynomial $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$ has roots which include six consecutive powers of α : $(\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6)$, where α is primitive in GF(16).

The received vector is $r = (000101000000100) \leftrightarrow r(x) = x^3 + x^5 + x^{12}$
The syndrome polynomial is written as

**Fig. 4.7** Chien search circuit

$$S(x) = S_1x + S_2x^2 + S_3x^3 + S_4x^4 + S_5x^5 + S_6x^6$$

$$S_1 = r(\alpha) = \alpha^3 + \alpha^5 + \alpha^{12} = 1$$

$$S_2 = r(\alpha^2) = \alpha^6 + \alpha^{10} + \alpha^{24} = 1$$

$$S_3 = r(\alpha^3) = \alpha^9 + \alpha^{15} + \alpha^{36} = \alpha^{10}$$

$$S_4 = r(\alpha^4) = \alpha^{12} + \alpha^{20} + \alpha^{48} = 1$$

$$S_5 = r(\alpha^5) = \alpha^{15} + \alpha^{25} + \alpha^{60} = \alpha^{10}$$

$$S_6 = r(\alpha^6) = \alpha^{18} + \alpha^{30} + \alpha^{72} = \alpha^5$$

Since $\alpha^{15} = 1$;

$$\alpha^{24} = \alpha^{15}\alpha^9 = \alpha^9;$$

$$\alpha^{36} = \alpha^{15}\alpha^{15}\alpha^6 = \alpha^6;$$

$$\alpha^{20} = \alpha^{15}\alpha^5 = \alpha^5;$$

$$\alpha^{48} = \alpha^{15}\alpha^{15}\alpha^{15}\alpha^3 = \alpha^3$$

$$\alpha^{25} = \alpha^{15}\alpha^{10} = \alpha^{10};$$

$$\alpha^{60} = \alpha^{15}\alpha^{15}\alpha^{15}\alpha^{15} = 1;$$

$$\alpha^{30} = \alpha^{15}\alpha^{15} = 1;$$

$$\alpha^{72} = \alpha^{15}\alpha^{15}\alpha^{15}\alpha^{15}\alpha^{12} = \alpha^{12}$$

$$S(x) = x + x^2 + \alpha^{10}x^3 + x^4 + \alpha^{10}x^5 + \alpha^5x^6$$

Applying Berlekamp algorithm, we obtain the following

n	$\Lambda(x)^{(2n)}$	$B(x)^{(2n)}$	$\Delta^{(2n)}$
0	1	1	1
1	$1 + x$	x	α^5
2	$1 + x + \alpha^5x^2$	$x(1 + x)/\alpha^5$	α^{10}
3	$1 + x + \alpha^5x^3$

The error locator polynomial is then

$$\Lambda(x) = 1 + x + \alpha^5x^3 = (1 + \alpha^3x)(1 + \alpha^5x)(1 + \alpha^{12}x)$$

indicating errors at the positions corresponding to α^3, α^5 and α^{12} . The corrected received word with the corrected positions is then

$$c = (0000000000000000) \\ \uparrow \\ c(x) = 0$$

Example 4.21 Let the transmission code be the double-error-correcting, narrow-sense, binary BCH code of length 15. The generator polynomial is $g(x) = 1 + x^4 + x^6 + x^7 + x^8$. Use Berlekamp's algorithm to decode the following received vector $r = (000110001100000)$.

Solution For double error correction, the generator polynomial $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ has roots which include four consecutive powers of α : $(\alpha, \alpha^2, \alpha^3, \alpha^4)$, where α is primitive in GF(16). The received vector is

$$r = (000110001100000) \\ \uparrow \\ r(x) = x^3 + x^4 + x^8 + x^9.$$

The syndrome polynomial is written as

$$S(x) = S_1x + S_2x^2 + S_3x^3 + S_4x^4 \\ S_1 = r(\alpha) = \alpha^3 + \alpha^4 + \alpha^8 + \alpha^9 = \alpha^2 \\ S_2 = r(\alpha^2) = \alpha^6 + \alpha^8 + \alpha^{16} + \alpha^{18} = \alpha^4 \\ S_3 = r(\alpha^3) = \alpha^9 + \alpha^{12} + \alpha^{24} + \alpha^{27} = 0 \\ S_4 = r(\alpha^4) = \alpha^{12} + \alpha^{16} + \alpha^{32} + \alpha^{36} = \alpha^8$$

Since $\alpha^{15} = 1$;

$$\begin{aligned}\alpha^{16} &= \alpha^{15}\alpha^1 = \alpha^1; \\ \alpha^{18} &= \alpha^{15}\alpha^3 = \alpha^3; \\ \alpha^{24} &= \alpha^{15}\alpha^9 = \alpha^9 \\ \alpha^{28} &= \alpha^{15}\alpha^{12} = \alpha^{12}; \\ \alpha^{32} &= \alpha^{15}\alpha^{15}\alpha^2 = \alpha^2; \\ \alpha^{36} &= \alpha^{15}\alpha^{15}\alpha^6 = \alpha^6\end{aligned}$$

$$S(x) = \alpha^2x + \alpha^4x^2 + \alpha^8x^4$$

Applying Berlekamp algorithm, we obtain the following

n	$\Lambda(x)^{(2n)}$	$B(x)^{(2n)}$	$\Delta^{(2n)}$
0	1	1	α^2
1	$1 + \alpha^2x$	$\alpha^{13}x$	α^6
2	$1 + \alpha^2x + \alpha^{19}x^2$

The error locator polynomial is then

$$\Lambda(x) = 1 + \alpha^2x + \alpha^{19}x^2 = (1 + \alpha^7x)(1 + \alpha^{12}x)$$

indicating errors at the positions corresponding to α^7 and α^{12} . The corrected received word with the corrected positions is then

$$\begin{aligned}c &= (000110011100100) \\ c(x) &= x^3 + x^4 + \overset{\uparrow}{x^7} + x^8 + x^9 + x^{12}\end{aligned}$$

4.5 Reed–Solomon Codes

The RS codes are the most powerful non-binary block codes which have seen widespread applications. These codes work with symbols that consist of several bits. A common symbol size for non-binary codes is 8 bits or a byte. The RS codes are good at correcting burst errors because the correction of these codes is done on the symbol level.

A given Reed–Solomon code is indicated by referring to it as an (n, k) code. The parameter n indicates the code word length in terms of the number of symbols in the code word. The parameter k indicates the number of message symbols in the

code word. The number of parity symbols added is thus (n, k) . The error-correcting capability of the code is $t_{\text{ec}} = (n - k)/2$. The minimum distance of Reed–Solomon code is $(n - k + 1)$.

4.5.1 Reed–Solomon Encoder

Generator Polynomial

A general form of the polynomial $g(x)$ used in RS code generation is

$$g(x) = (x - \alpha^i)(x - \alpha^{i+1}) \dots (x - \alpha^{i+2t_{\text{ec}}}) \quad (4.35)$$

where α is a primitive element of the Galois field.

The code word $c(x)$ is constructed using

$$c(x) = g(x) \cdot i(x) \quad (4.36)$$

where $i(x)$ is the information polynomial.

The code word $c(x)$ is exactly divisible by the generator polynomial $g(x)$. The remainder obtained by dividing $i(x) \cdot x^{n-k}$ by $g(x)$ gives the parity polynomial $p(x)$ as

$$p(x) = i(x) \cdot x^{n-k} / g(x) \quad (4.37)$$

The parity symbols are computed by performing a polynomial division using GF algebra. The steps involved in this computation are as follows:

- Step 1:** Multiply the message symbols by x^{n-k} (This shifts the message symbols to the left to make room for the $(n - k)$ parity symbols).
- Step 2:** Divide the message polynomial by the code generator polynomial using GF algebra.
- Step 3:** The parity symbols are the remainder of this division. These steps are accomplished in hardware using a shift register with feedback. The architecture for the encoder is shown in Fig. 4.8.

$g(x)$ is the generator polynomial used to generate parity symbols $p(x)$. The number of registers used is equal to $n - k$. Parity symbols are generated by serial entry of the information symbols into $i(x)$.

The resultant code word is given by

$$c(x) = i(x) \cdot x^{n-k} + p(x) \quad (4.38)$$

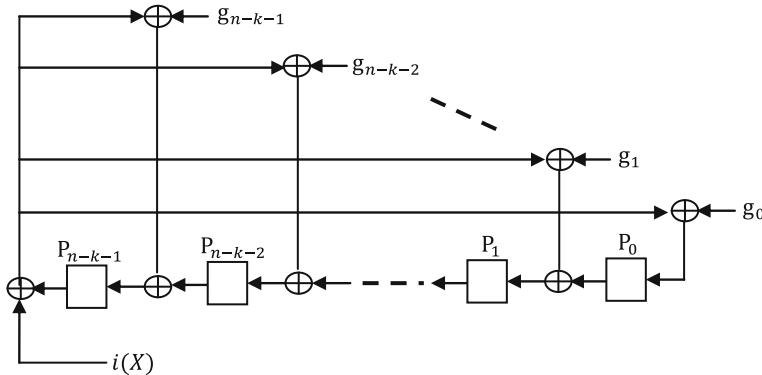


Fig. 4.8 Reed–Solomon encoder

Example 4.22 Construct a generator polynomial for a (15,11) Reed–Solomon code with elements in $\text{GF}(2^4)$.

Solution A (15,11) Reed–Solomon code has minimum distance 5. Thus, the (15,11) Reed–Solomon code is double error corrections. It must have 4 consecutive powers of α as zeros.

The generator polynomial is constructed as follows using the representation for GF(16) over GF(2).

$$\begin{aligned}
 g(x) &= (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4) \\
 &= (x^2 + (\alpha^2 + \alpha)x + \alpha^3)(x^2 + (\alpha^3 + \alpha^4)x + \alpha^7) \\
 &= (x^2 + \alpha^5x + \alpha^3)(x^2 + \alpha^7x + \alpha^7) \\
 &= (x^4 + (\alpha^5 + \alpha^7)x^3 + (\alpha^3 + \alpha^{12} + \alpha^7)x^2 + (\alpha^{10} + \alpha^{12})x + \alpha^{10}) \\
 &= (x^4 + \alpha^{13}x^3 + \alpha^6x^2 + \alpha^3x + \alpha^{10})
 \end{aligned}$$

Example 4.23 Compute a generator polynomial for a double-error-correcting Reed–Solomon code of length 31.

Solution Let α be a root of the primitive binary polynomial $x^5 + x^2 + 1$ and thus a primitive 31st of unity. The resulting code is to be a double-error-correcting code; it must have 4 consecutive powers of α as zeros. A narrow-sense generator is constructed as follows using the representation for GF(32).

$$\begin{aligned}
g(x) &= (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4) \\
&= (x^2 + (\alpha^2 + \alpha)x + \alpha^3)(x - \alpha^3)(x - \alpha^4) \\
&= (x^2 + \alpha^{19}x + \alpha^3)(x - \alpha^3)(x - \alpha^4) \\
&= (x^3 + \alpha^{19}x^2 + \alpha^3x^2 + \alpha^3x + \alpha^{22}x + \alpha^6)(x - \alpha^4) \\
&= (x^3 + (\alpha^{19} + \alpha^3)x^2 + (\alpha^3 + \alpha^{22})x + \alpha^6)(x - \alpha^4) \\
&= (x^3 + \alpha^{12}x^2 + \alpha^{14}x + \alpha^6)(x - \alpha^4) \\
&= x^4 + \alpha^{12}x^3 + \alpha^4x^3 + \alpha^{14}x^2 + \alpha^{16}x^2 + \alpha^6x + \alpha^{18}x + \alpha^{10} \\
&= x^4 + (\alpha^{12} + \alpha^4)x^3 + (\alpha^{14} + \alpha^{16})x^2 + (\alpha^6 + \alpha^{18})x + \alpha^{10} \\
&= x^4 + \alpha^{24}x^3 + \alpha^{19}x^2 + \alpha^{29}x + \alpha^{10}
\end{aligned}$$

Example 4.24 Compute a generator polynomial for a triple-error-correcting Reed–Solomon code of length 15.

Solution

$$\begin{aligned}
g(x) &= (x + \alpha)(x + \alpha^2)(x + \alpha^3)(x + \alpha^4)(x + \alpha^5)(x + \alpha^6) \\
&= (x^2 + (\alpha^2 + \alpha)x + \alpha^3)(x^2 + (\alpha^3 + \alpha^4)x + \alpha^7) \\
&\quad (x^2 + (\alpha^6 + \alpha^5)x + \alpha^{11}) \\
&= (x^2 + \alpha^5x + \alpha^3)(x^2 + \alpha^7x + \alpha^7)(x^2 + \alpha^9x + \alpha^{11}) \\
&= (x^4 + (\alpha^5 + \alpha^7)x^3 + (\alpha^3 + \alpha^{12} + \alpha^7)x^2 + (\alpha^{10} + \alpha^{12})x + \alpha^{10}) \\
&\quad (x^2 + \alpha^9x + \alpha^{11}) \\
&= (x^4 + \alpha^{13}x^3 + \alpha^6x^2 + \alpha^3x + \alpha^{10})(x^2 + \alpha^9x + \alpha^{11}) \\
&= (x^6 + (\alpha^9 + \alpha^{13})x^5 + (\alpha^{11} + \alpha^{22} + \alpha^6)x^4 + (\alpha^{24} + \alpha^{15} + \alpha^3)x^3 \\
&\quad + (\alpha^{10} + \alpha^{17} + \alpha^{12})x^2 + (\alpha^{14} + \alpha^{19})x + \alpha^{21}) \\
&= (x^6 + \alpha^{10}x^5 + \alpha^{14}x^4 + \alpha^4x^3 + \alpha^6x^2 + \alpha^9x + \alpha^6)
\end{aligned}$$

Basic Properties of Reed–Solomon Codes

1. Non-binary BCH codes are referred to as Reed–Solomon codes.
2. The minimum distance of Reed–Solomon code is $(n - k + 1)$.
3. RS codes are maximum distance separable (MDS). The singleton bound implies that $d_{\min} \leq (n - k + 1)$. RS (n, k) code is called MDS if the singleton bound is satisfied with equality.
4. The weight distribution polynomial of RS code is known. The weight distribution of an RS code with symbols from GF(q) and with block length $n = q - 1$ and minimum distance d_{\min} is given by

$$W_i = \binom{n}{i} n \sum_{j=0}^{1-d_{\min}} (-1)^j \binom{i-1}{j} (n+1)^{i-j-d_{\min}} d_{\min} \leq i \leq n \quad (4.39)$$

4.5.2 Decoding of Reed–Solomon Codes

The locations of the errors can be found from the error locator polynomial $\Lambda(x)$. Once the locations of the errors are known, the magnitudes of the errors are found by the Forney’s algorithm given by [1]

$$e_k = \frac{-x_k \Omega(x_k^{-1})}{\Lambda'(x_k^{-1})} \quad (4.40)$$

where e_k represents the error magnitude at the k th location and $\Lambda'(x_k)$ stands for formal derivative of the error locator polynomial $\Lambda(x)$. If locator polynomial $\Lambda(x) = \Lambda_v x^v + \Lambda_{v-1} x^{v-1} + \cdots + \Lambda_1 x + 1$ is a polynomial with coefficients in $\text{GF}(q)$, the formal derivative $\Lambda'(x)$ is defined as

$$\Lambda'(x) = v\Lambda_v x^{v-1} + (v-1)\Lambda_{v-1} x^{v-2} + \cdots + \Lambda_1 \quad (4.41)$$

The decoding of a RS code has to go through the following six steps:

- Step 1:** Compute Syndromes from the received polynomial $r(x)$
- Step 2:** Apply Berlekamp–Massey algorithm to compute error location polynomial $\Lambda(x)$
- Step 3:** Compute error magnitude polynomial

$$\Omega(x) = \Lambda(x)(1 + S(x)) \bmod x^{2t_{\text{ec}}+1}$$

- Step 4:** Find the roots of $\Lambda(x)$, the inverse of the roots indicates the locations of the errors
- Step 5:** Compute the error magnitudes and determine the error polynomial $e(x)$
- Step 6:** Subtract $e(x)$ from the received polynomial to correct the errors.

Syndrome generation is similar to parity calculation. A Reed–Solomon code word has $2t_{\text{ec}}$ syndromes that depend only on errors (not on the transmitted code word).

The syndrome sequence can be computed for the received word polynomial $r(x)$ by substituting the $2t_{\text{ec}}$ roots of the generator polynomial $g(x)$ into $r(x)$. The Berlekamp–Massey algorithm or Euclid’s algorithm can be used to find error locator polynomial. The Euclid’s algorithm is widely used in practice as it is easy for implementation. However, hardware and software implementations of the

Berlekamp–Massey algorithm are more efficient [2, 3]. Once the error locator polynomial is known, the error locations can be found by using the Chien search algorithm [4].

The Berlekamp–Massey Decoding Algorithm

The problem of decoding RS codes can be viewed as finding a linear feedback shift register (LFSR) of minimal length so that the first $2t_{\text{ec}}$ elements in the LFSR output sequence are the syndromes $S_1S_2\dots S_{2t_{\text{ec}}}$. The error locator polynomial $\Lambda(x)$ is provided by the taps of the LFSR.

The flowchart of the Berlekamp–Massey iterative algorithm is shown in Fig. 4.9. Here, $\Lambda^{(n)}(x)$ is the error location polynomial at the n th iteration step, $B(x)$ stands for the connection polynomial, L_n represents the length of LFSR at index n , and d_n is the discrepancy. Consider the error location polynomial $\Lambda^{(n)}(x)$ of length n . The coefficients of the polynomial specify the taps of a length n LFSR. The Berlekamp–Massey algorithm initially (i.e., $n = 0$) sets the tap coefficient and the length of the LFSR to 1 and 0, respectively, to indicate that the computed error locator polynomial $\Lambda^{(0)}(x)$, and its length is set to 1 and 0, respectively, and also sets $B(x) = x$ at every iteration, or a new syndrome component, and the discrepancy d_n is computed by subtracting the n th output of the LFSR defined by $\Lambda^{(n-1)}(x)$ from the n th syndrome. If the discrepancy is not equal to zero, a modified error locator polynomial is constructed using discrepancy and connection polynomial $B(x)$. Then, the length of the LFSR is to be tested. If $2L_n$ is greater than or equal to n , the length of the LFSR and connection polynomial $B(x)$ are to be updated. Otherwise, if $2L_n$ is less than n , the connection polynomial $B(x)$ is to be reset as $xB(x)$.

If the discrepancy is equal to zero, then the connection polynomial $B(x)$ is to be reset as $xB(x)$ and the previous error locator polynomials are used for the next iteration. The process is continued, and the algorithm stops at the end of the iteration $n = 2t_{\text{ec}}$ and $\Lambda^{(2t_{\text{ec}})}(x)$ is taken as the error locator polynomial $\Lambda(x)$.

Example 4.25 Let the transmission code be the double-error-correcting RS code of length 7. Use the Berlekamp–Massey algorithm to decode the following received vector $r = (00\alpha^5 1\alpha^2 0\alpha^2)$.

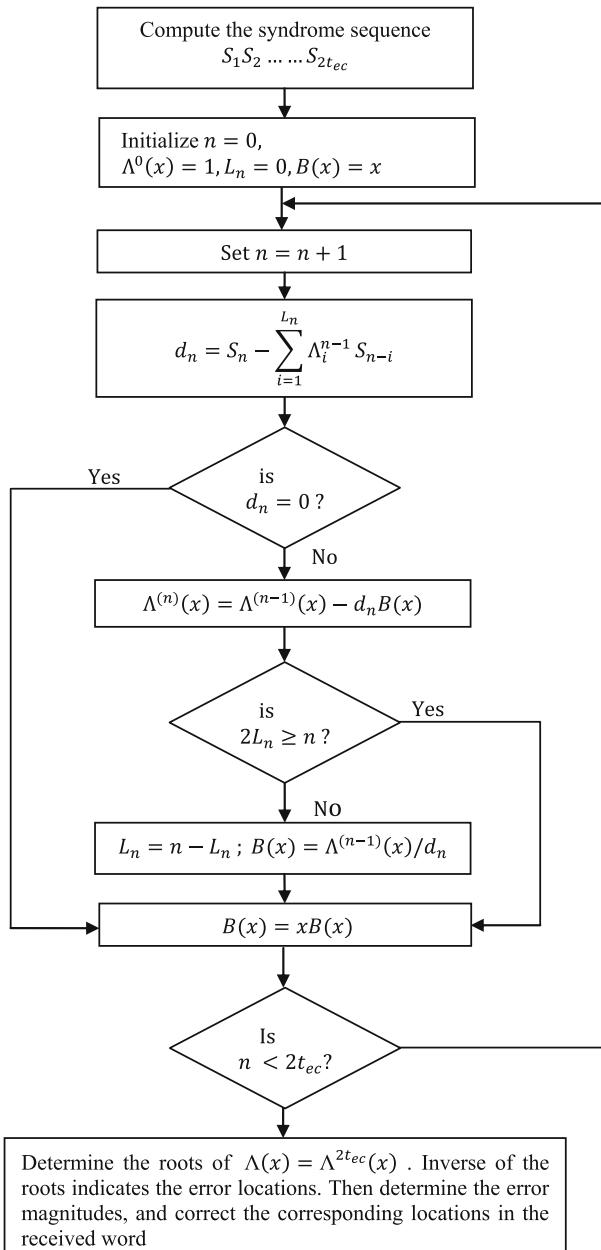
Solution

Step 1: The received polynomial is

$$r(x) = \alpha^5 x^2 + x^3 + \alpha^2 x^4 + \alpha^2 x^6; \quad \text{i.e., } r = (00\alpha^5 1\alpha^2 0\alpha^2)$$

For double-error-correcting code, the syndrome polynomial is

$$S(x) = S_1 x + S_2 x^2 + S_3 x^3 + S_4 x^4$$

**Fig. 4.9** Berlekamp–Massey iterative algorithm

The syndromes S_1, S_2, S_3 and S_4 for the above-mentioned received polynomial are computed using the representation for GF(8) as

$$\begin{aligned}S_1 &= r(\alpha) = \alpha^6 \\S_2 &= r(\alpha^2) = \alpha^3 \\S_3 &= r(\alpha^3) = \alpha^4 \\S_4 &= r(\alpha^4) = \alpha^3\end{aligned}$$

Thus, the

$$S(x) = \alpha^6x + \alpha^3x^2 + \alpha^4x^3 + \alpha^3x^4.$$

Step 2: Berlekamp–Massey algorithm proceeds as follows:

n	S_n	$\Lambda^{(n)}(x)$	d_n	L_n	$B(x)$
0	...	1	...	0	x
1	α^6	$1 + \alpha^6x$	$S_1 - 0 = \alpha^6$	1	αx
2	α^3	$1 + (\alpha^6 + \alpha^3)x$ $= 1 + \alpha^4x$	$S_2 - \alpha^6\alpha^6$ $= S_2 - \alpha^5 = \alpha^2$	1	αx^2
3	α^4	$1 + \alpha^4x + \alpha^5\alpha x^2$ $= 1 + \alpha^4x + \alpha^6x^2$	$S_3 - \alpha^4\alpha^3$ $= S_3 - 1 = \alpha^5$	2	$\left(\frac{1+\alpha^4x}{\alpha^5}\right)x =$ $(\alpha^2x + \alpha^6x^2)$
4	α^3	$1 + \alpha^2x + \alpha x^2$	$S_4 - (\alpha^4\alpha^4 + \alpha^6\alpha^3)$ $= S_4 - (\alpha + \alpha^2)$ $= S_4 - \alpha^4 = \alpha^6$

The error locator polynomial is then

$$\Lambda(x) = 1 + \alpha^2x + \alpha x^2$$

Step 3: The error magnitude polynomial is

$$\begin{aligned}\Omega(x) &= \Lambda(x)(1 + S(x)) \bmod x^{2t_{ec}+1} \\&= (1 + \alpha^2x + \alpha x^2)(1 + \alpha^6x + \alpha^3x^2 + \alpha^4x^3 + \alpha^3x^4) \bmod x^5 \\&= 1 + x + \alpha^3x^2\end{aligned}$$

Step 4:

$$\Lambda(x) = 1 + \alpha^2x + \alpha x^2 = (1 + \alpha^3x)(1 + \alpha^5x) = 0$$

The factorization of the error locator polynomial indicates that there are errors in the third and fifth positions of the received vector.

Hence, the error polynomial $e(x)$ is

$$e(x) = e_3x^3 + e_5x^5$$

Step 5: From the error locator polynomial, it is known that error positions are in locations 3 and 5. Now, the error magnitudes can be computed by using error evaluator polynomial $\Omega(x)$ and derivative of the error locator polynomial $\Lambda(x)$. The error magnitudes are given by

$$e_k = \frac{-x_k \Omega(x_k^{-1})}{\Lambda'(x_k^{-1})}$$

The magnitudes of errors are found to be

$$e_3 = \frac{-x_3 \Omega(x_3^{-1})}{\Lambda'(x_3^{-1})}$$

Since $\Lambda'(x_3^{-1}) = \alpha^2$

$$e_3 = \frac{-x_3(1 + x_3^{-1} + \alpha^3 x_3^{-2})}{\alpha^2}$$

where $x_3 = \alpha^3$

Thus,

$$e_3 = \frac{(\alpha^3 + 1 + 1)}{\alpha^2} = \alpha$$

Similarly,

$$e_5 = \frac{-x_5(1 + x_5^{-1} + \alpha^3 x_5^{-2})}{\alpha^2}$$

where $x_5 = \alpha^5$

Hence,

$$e_5 = \frac{(\alpha^5 + 1 + \alpha^{-2})}{\alpha^2} = \alpha^5$$

Thus, the error pattern

$$e(x) = \alpha x^3 + \alpha^5 x^5$$

Step 6:

$$c(x) = r(x) - e(x) = \alpha^5x^2 + x^3 + \alpha^2x^4 + \alpha^2x^6 + \alpha x^3 + \alpha^5x^5$$

Example 4.26 Consider a triple-error-correcting RS code of length 15. Decode the received vector $r = (000\alpha^700\alpha^300000\alpha^400)$ using Berlekamp–Massey algorithm.

Solution

Step 1: The received polynomial is

$$r(x) = \alpha^7x^3 + \alpha^3x^6 + \alpha^4x^{12}; \quad \text{i.e., } r = (000\alpha^700\alpha^300000\alpha^400)$$

The following syndromes are computed using the representation of GF(16) over GF(2). For triple error correction, the roots of the generator polynomial include $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$.

Thus,

$$\begin{aligned} S_1 &= r(\alpha) = \alpha^{10} + \alpha^9 + \alpha = \alpha^{12} \\ S_2 &= r(\alpha^2) = \alpha^{13} + 1 + \alpha^{13} = 1 \\ S_3 &= r(\alpha^3) = \alpha + \alpha^6 + \alpha^{10} = \alpha^{14} \\ S_4 &= r(\alpha^4) = \alpha^4 + \alpha^{12} + \alpha^7 = \alpha^{10} \\ S_5 &= r(\alpha^5) = \alpha^7 + \alpha^3 + \alpha^4 = 0 \\ S_6 &= r(\alpha^6) = \alpha^{10} + \alpha^9 + \alpha = \alpha^{12} \end{aligned}$$

$$S(x) = \alpha^{12}x + x^2 + \alpha^{14}x^3 + \alpha^{10}x^4 + \alpha^{12}x^6$$

Step 2: Berlekamp–Massey algorithm proceeds as follows:

n	S_n	$\Lambda^{(n)}(x)$	d_n	L_n	$B(x)$
0	...	1	...	0	x
1	α^{12}	$1 + \alpha^2x$	$S_1 - 0 = \alpha^2$	1	α^3x
2	1	$1 + \alpha^3x$	$S_2 - \alpha^0 = \alpha^7$	1	α^3x^2
3	α^{14}	$1 + \alpha^3x + \alpha^3x^2$	$S_3 - \alpha^3 = 1$	2	$x + \alpha^3x^2$
4	α^{10}	$1 + \alpha^4x + \alpha^{12}x^2$	$S_4 - \alpha^6 = \alpha^7$	2	$x^2 + \alpha^3x^3$
5	0	$1 + \alpha^4x + \alpha^3x^2 + \alpha^{13}x^3$	$S_5 - \alpha^{10} = \alpha^{10}$	3	$\alpha^5x + \alpha^9x^2 + \alpha^2x^3$
6	α^{12}	$1 + \alpha^7x + \alpha^4x^2 + \alpha^6x^3$	$S_6 - \alpha = \alpha^{13}$

The error locator polynomial is then

$$\Lambda(x) = 1 + \alpha^7x + \alpha^4x^2 + \alpha^6x^3 = (1 + \alpha^3x)(1 + \alpha^6x)(1 + \alpha^{12}x)$$

Step 3: The error magnitude polynomial is

$$\begin{aligned}\Omega(x) &= \Lambda(x)(1 + S(x)) = (1 + \alpha^7x + \alpha^4x^2 + \alpha^6x^3)(1 + \alpha^{12}x + x^2 \\ &\quad + \alpha^{14}x^3 + \alpha^{10}x^4 + \alpha^{12}x^6) \bmod x^7 \\ &= (1 + \alpha^2x + x^2 + \alpha^6x^3 + x^7 + \alpha x^8 + \alpha^3x^9) \bmod x^7 \\ &= (1 + \alpha^2x + x^2 + \alpha^6x^3)\end{aligned}$$

Step 4:

$$\Lambda(x) = 1 + \alpha^7x + \alpha^4x^2 + \alpha^6x^3 = (1 + \alpha^3x)(1 + \alpha^6x)(1 + \alpha^{12}x) = 0$$

The factorization of the error locator polynomial indicates that there are errors in the positions 3, 6, and 12 of the received vector.

Hence, the error polynomial $e(x)$ is

$$e(x) = e_{12}x^{12} + e_6x^6 + e_3x^3$$

Step 5: From the error locator polynomial, it is known that error positions are at locations 3, 6, and 12. Now, the error magnitudes can be computed by using error evaluator polynomial $\Omega(x)$ and derivative of the error locator polynomial $\Lambda(x)$. The error magnitudes are given by

$$e_k = \frac{-x_k \Omega(x_k^{-1})}{\Lambda'(x_k^{-1})}$$

The magnitudes of errors are found to be

$$e_3 = \frac{-x_3 \Omega(x_3^{-1})}{\Lambda'(x_3^{-1})}$$

Since $\Lambda'(x_3^{-1}) = \alpha^7 + \alpha^6x_3^{-2}$

$$e_3 = \frac{-x_3(1 + \alpha^2x_3^{-1} + x_3^{-2} + \alpha^6x_3^{-3})}{\alpha^7 + \alpha^6x_3^{-2}}$$

where $x_3 = \alpha^3$.

Thus,

$$e_3 = \frac{\alpha^3(1 + \alpha^2 \cdot \alpha^{12} + \alpha^9 + \alpha^{12})}{1 + \alpha^7} = \frac{\alpha^3(1 + \alpha^{14} + \alpha^9 + \alpha^{12})}{1 + \alpha^7} = \frac{\alpha^3 \cdot \alpha^{13}}{\alpha^9} = \alpha^7$$

Similarly,

$$e_6 = \alpha^3; \quad e_{12} = \alpha^4.$$

Thus, the error pattern

$$e(x) = \alpha^7 x^3 + \alpha^3 x^6 + \alpha^4 x^{12}$$

Step 6: The corrected received word is $c(x) = r(x) - e(x) = 0$

$$c = (00000000000000)$$

Example 4.27 Let the transmission code be the triple-error-correcting RS code of length 31. Decode the received vector $r = (00x^800x^20000x000000000000000000000000)$ using Berlekamp–Massey algorithm.

Solution

Step 1: The received polynomial is

$$r(x) = \alpha^8 x^2 + \alpha^2 x^5 + \alpha x^{10};$$

i.e, $r = (00\alpha^8 00\alpha^2 0000\alpha 000000000000000000000000000000)$

The following syndromes are computed using the representation of GF(16) over GF(2). For triple error correction, the roots of the generator polynomial include $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$.

Thus,

$$\begin{aligned} S_1 &= r(\alpha) = \alpha^{10} + \alpha^9 + \alpha^{11} = \alpha \\ S_2 &= r(\alpha^2) = \alpha^{12} + \alpha^{12} + \alpha^{21} = \alpha^{21} \\ S_3 &= r(\alpha^3) = \alpha^{14} + \alpha^{17} + \alpha^{31} = \alpha^{23} \\ S_4 &= r(\alpha^4) = \alpha^{16} + \alpha^{22} + \alpha^{20} = \alpha^{15} \\ S_5 &= r(\alpha^5) = \alpha^{18} + \alpha^{27} + \alpha^{20} = \alpha^2 \\ S_6 &= r(\alpha^6) = \alpha^{20} + \alpha + \alpha^{30} = \alpha^{13} \end{aligned}$$

$$S(x) = \alpha x + \alpha^{21}x^2 + \alpha^{23}x^3 + \alpha^{15}x^4 + \alpha^2x^5 + \alpha^{13}x^6.$$

Step 2: Berlekamp–Massey algorithm proceeds as follows:

n	S_n	$\Lambda^{(n)}(x)$	d_n	L_n	$B(x)$
0	1	...	0	x
1	α	$1 + \alpha x$	$S_1 - 0 = \alpha$	1	$\alpha^{30}x$
2	α^{21}	$1 + \alpha^{20}x$	$S_2 - \alpha^2 = \alpha^{13}$	1	$\alpha^{30}x^2$
3	α^{23}	$1 + \alpha^{20}x + \alpha^{23}x^2$	$S_3 - \alpha^{10} = \alpha^{24}$	2	$\alpha^7x + \alpha^{27}x^2$
4	α^{15}	$1 + \alpha^{20}x + \alpha^{23}x^2 + \alpha^{15}x + \alpha^4x^2$ $= 1 + \alpha^{17}x + \alpha^{15}x^2$	$S_4 - \alpha^{12} - \alpha^{13} = \alpha^8$	2	$\alpha^7x^2 + \alpha^{27}x^3$
5	α^2	$1 + \alpha^{17}x + \alpha^{22}x^2 + \alpha^{26}x^3$	$S_5 - \alpha - \alpha^7 = \alpha^{30}$	3	$\alpha^{16}x^3 + \alpha^{18}x^2 + \alpha x$
6	α^{13}	$1 + \alpha^{17}x + \alpha^{22}x^2 + \alpha^{26}x^3 + \alpha^2x^3$ $+ \alpha^{18}x + \alpha^4x^2 = 1 + \alpha^4x + \alpha^5x^2 + \alpha^{17}x^3$	$S_6 - \alpha^{19} - \alpha^6 - \alpha^{18} = \alpha^{17}$

The error locator polynomial is then

$$\Lambda(x) = 1 + \alpha^4x + \alpha^5x^2 + \alpha^{17}x^3 = (1 + \alpha^{21}x)(1 + \alpha^{26}x)(1 + \alpha^{29}x)$$

Step 3: The error magnitude polynomial is

$$\begin{aligned} \Omega(x) &= \Lambda(x)(1 + S(x)) = (1 + \alpha^4x + \alpha^5x^2 + \alpha^{17}x^3)(1 + \alpha x + \alpha^{21}x^2 + \alpha^{23}x^3 \\ &\quad + \alpha^{15}x^4 + \alpha^2x^5 + \alpha^{13}x^6) \bmod x^7 \\ &= (1 + \alpha^{30}x + \alpha^{21}x^2 + \alpha^{23}x^3) \end{aligned}$$

Step 4:

$$\Lambda(x) = 1 + \alpha^4x + \alpha^5x^2 + \alpha^{17}x^3 = (1 + \alpha^2x)(1 + \alpha^5x)(1 + \alpha^{10}x) = 0$$

The factorization of the error locator polynomial indicates that there are errors in the second, fifth, and tenth positions of the received vector.

Hence, the error polynomial $e(x)$ is

$$e(x) = e_{10}x^{10} + e_5x^5 + e_2x^2$$

Step 5: From the error locator polynomial, it is known that error positions are at locations 2, 5, and 10. Now, the error magnitudes can be computed by using error evaluator polynomial $\Omega(x)$, and derivative of the error locator polynomial $\Lambda(x)$. The error magnitudes are given by

$$e_k = \frac{-x_k \Omega(x_k^{-1})}{\Lambda'(x_k^{-1})}$$

The magnitudes of errors are found to be

$$e_2 = \frac{-x_2 \Omega(x_2^{-1})}{\Lambda'(x_2^{-1})}$$

Since $\Lambda'(x_2^{-1}) = \alpha^4 + \alpha^{17}x_2^{-2}$

$$e_2 = \frac{-x_2(1 + \alpha^2x_2^{-1} + x_2^{-2} + \alpha^6x_2^{-3})}{\alpha^4 + \alpha^{17}x_2^{-2}}$$

where $x_3 = \alpha^3$

Thus,

$$e_2 = \frac{\alpha^2(1 + \alpha^{30} \cdot \alpha^{-2} + \alpha^{21} \cdot \alpha^{-4} + \alpha^{23} \cdot \alpha^{-6})}{\alpha^4 + \alpha^{13}} = \frac{\alpha^2 + \alpha^{30}}{\alpha^{20}} = \frac{\alpha^{28}}{\alpha^{20}} = \alpha^8$$

Similarly,

$$e_5 = \alpha^2; e_{10} = \alpha.$$

Thus, the error pattern

$$e(x) = \alpha^8x^2 + \alpha^7x^5 + \alpha x^{10}$$

Step 6: The corrected received word is $c(x) = r(x) - e(x) = 0$

$$c = (0000000000000000)$$

4.5.3 Binary Erasure Decoding

For binary linear codes, erasure decoding is done by the following three steps:

- Step 1:** Replace all erasures with zeros in a received word, and decode it to a code word c_0 .
- Step 2:** Replace all erasures with ones in a received word, and decode it to a code word c_1 .
- Step 3:** Choose the final code word either c_0 or c_1 that is closest to the received word in the Hamming distance.

4.5.4 Non-binary Erasure Decoding

Suppose that a received word has v errors and f erasures. An erasure locator polynomial can be written as

$$\Gamma(x) = \prod_{l=1}^f (1 - Y_l x) \quad (4.42)$$

where Y_l stands for erasure locators. Now, the decoding has to find out error locations and compute the error magnitudes of the error locators and erasure magnitudes of the erasure locators. To find the error locator polynomial, a modified syndrome polynomial is to be formulated and Berlekamp–Massey algorithm is to be applied on the modified syndrome coefficients.

The modified syndrome polynomial is given by

$$S^M(x) \equiv (\Gamma(x)[1 + S(x)] - 1)x^{2t+1} \quad (4.43)$$

where the coefficients of the syndrome polynomial $S(x)$ are computed using the following

$$S_l = r(\alpha^l) \quad (4.44)$$

replacing all the erasures with zeros in the received polynomial $r(x)$.

After finding the error locator polynomial $\Lambda(x)$, obtain error magnitude polynomial and error/erasure locator polynomial as

$$\Omega(x) = \Lambda(x)[1 + S^M(x)]x^{2t+1} \quad (4.45)$$

$$\Psi(x) = \Lambda(x)\Gamma(x) \quad (4.46)$$

Then, using the modified Forney's algorithm, compute the error and erasure magnitudes as given by

$$e_k = \frac{-X_k \Omega(X_k^{-1})}{\Psi'(X_k^{-1})} \quad (4.47a)$$

$$f_k = \frac{-Y_k \Omega(Y_k^{-1})}{\Psi'(Y_k^{-1})} \quad (4.47b)$$

Knowing the magnitudes of the error locators and erasure locators, an error/erasure polynomial can be constructed and subtracted from the received polynomial to arrive at the desired code polynomial.

The stepwise procedure using Berlekamp–Massey algorithm for error/erasure decoding is as follows:

- Step 1:** Formulate the erasure polynomial $\Gamma(x)$ using the erasures in the received vector.
- Step 2:** Obtain the syndrome polynomial $S(x)$ replacing the erasures with zeros.
- Step 3:** Compute the modified syndrome polynomial using Eq. (4.43).
- Step 4:** Apply the Berlekamp–Massey on modified syndrome coefficients to find the error correction polynomial $\Lambda(x)$.
- Step 5:** Find the roots of $\Lambda(x)$, to determine the error locations.
- Step 6:** Compute the error magnitudes using Eq. (4.47a), and determine the error polynomial $e(x)$.
- Step 7:** Compute the erasure magnitudes using Eq. (4.47b), and determine the erasure polynomial $f(x)$.
- Step 8:** Subtract $e(x)$ and $f(x)$ from the received polynomial to correct the errors.

Example 4.28 Let the transmission code be the double-error-correcting RS code of length 7. Use the Berlekamp–Massey algorithm to decode the following received vector $r = (00\alpha^301f1)$.

Solution

Step 1: The received polynomial is $r(x) = \alpha^3x^2 + x^4 + fx^5 + x^6$; The f indicates an erasure. This erasure gives the erasure polynomial

$$\Gamma(x) = 1 + \alpha^5x$$

Step 2: Place a zero in the erasure location, and compute the syndromes. For double-error-correcting code, the syndrome polynomial is

$$\begin{aligned} S(x) &= S_1x + S_2x^2 + S_3x^3 + S_4x^4 \\ S_l &= \alpha^3(\alpha^l)^2 + (\alpha^l)^4 + (\alpha^l)^6 \end{aligned}$$

The syndromes S_1, S_2, S_3 and S_4 for the above-mentioned received polynomial are computed using the representation for GF(8) as

$$\begin{aligned} S_1 &= r(\alpha) = \alpha^5 + \alpha^4 + \alpha^6 = \alpha^2 \\ S_2 &= r(\alpha^2) = \alpha^7 + \alpha^8 + \alpha^{12} = \alpha^2 \\ S_3 &= r(\alpha^3) = \alpha^9 + \alpha^{12} + \alpha^{18} = \alpha^6 \\ S_4 &= r(\alpha^4) = \alpha^{11} + \alpha^{16} + \alpha^{24} = \alpha^4 \end{aligned}$$

Thus, the

$$S(x) = \alpha^2 x + \alpha^2 x^2 + \alpha^6 x^3 + x^4.$$

Step 3: Compute the modified syndrome polynomial,

$$\begin{aligned} 1 + S^M(x) &\equiv \Gamma(x)[1 + S(x)] \bmod x^{2r+1} \\ &\equiv (1 + \alpha^5 x)(1 + \alpha^2 x + \alpha^2 x^2 + \alpha^6 x^3 + x^4) \bmod x^5 \\ &\equiv 1 + \alpha^3 x + \alpha^6 x^2 + \alpha^2 x^3 + \alpha^5 x^4 \bmod x^5 \end{aligned}$$

$S^M(x)$ is thus $\alpha^3 x + \alpha^6 x^2 + \alpha^2 x^3 + \alpha^5 x^4$.

Step 4: Berlekamp–Massey algorithm proceeds as follows:

n	S_n^M	$\Lambda^{(n)}(x)$	d_n	L_n	$B(x)$
0	...	1	...	0	x
1	α^3	$1 + \alpha^3 x$	α^3	1	$\alpha^4 x$
2	α^6	$1 + \alpha^3 x$	0	1	$\alpha^4 x^2$
3	α^2	$1 + \alpha^3 x$	0	1	$\alpha^4 x^3$
4	α^5	$1 + \alpha^3 x$	0

Step 5: $\Lambda(x) = 1 + \alpha^3 x$, indicating a single error at $X_1 = \alpha^3$.

Step 6: The error magnitude polynomial is

$$\begin{aligned} \Omega(x) &= \Lambda(x)(1 + S(x)) = (1 + \alpha^3 x)(1 + \alpha^2 x + \alpha^2 x^2 + \alpha^6 x^3 + x^4) \bmod x^5 \\ &= (1 + (\alpha^2 + \alpha^3)x + (\alpha^2 + \alpha^5)x^2 + (\alpha^6 + \alpha^5)x^3 \\ &\quad + (1 + \alpha^9)x^4 + \alpha^3 x^5) \bmod x^5 \\ &= (1 + \alpha^5 x + \alpha^3 x^2 + \alpha x^3 + \alpha^6 x^4 + \alpha^3 x^5) \bmod x^5 \\ &= 1 + \alpha^5 x + \alpha^3 x^2 + \alpha x^3 + \alpha^6 x^4 \end{aligned}$$

The error/erasure locator polynomial

$$\begin{aligned} \Psi(x) &= \Lambda(x)\Gamma(x) \\ &= (1 + \alpha^3 x)(1 + \alpha^5 x) \\ &= (1 + \alpha^2 x + \alpha x^2) \end{aligned}$$

The error magnitude

$$e_k = \frac{-X_k \Omega(X_k^{-1})}{\Psi'(X_k^{-1})} = \frac{-X_k [1 + \alpha^5 X_k^{-1} + \alpha^3 X_k^{-2} + \alpha X_k^{-3} + \alpha^6 X_k^{-4}]}{\alpha^2} = \alpha^3$$

$$e_3 = \alpha^3$$

and erasure magnitude

$$f_k = \frac{-Y_k \Omega(Y_k^{-1})}{\Psi'(Y_k^{-1})}$$

$$f_5 = \alpha$$

The corrected code word is

$$\begin{aligned} c(x) &= r(x) + e(x) + f(x) \\ &= (\alpha^3 x^2 + x^4 + x^6) + \alpha^3 x^3 + \alpha x^5 \end{aligned}$$

4.6 Performance Analysis of RS Codes

A RS (n, k) code with minimum distance $d_{\min} = n - k + 1$ is able to correct $t_{\text{ec}} = (n - k)/2$ symbol errors. The bit error probability for RS codes using hard-decision decoding is often approximated by [5]

$$P_b \approx \frac{1}{n} \sum_{i=t_{\text{ec}}+1}^t i \binom{n}{i} P^i (1-P)^{n-i} \quad (4.48)$$

4.6.1 BER Performance of RS Codes for BPSK Modulation in AWGN and Rayleigh Fading Channels

The redundancy introduced by RS code increases the channel symbol transmission rate, reducing the received $\frac{E_b}{N_0}$. For a code with rate R , for BPSK in AWGN channel and Rayleigh fading channel, Eqs. (2.3) and (2.6) becomes

$$\begin{aligned} P &= Q\left(\sqrt{2R \frac{E_b}{N_0}}\right) \\ P &= \frac{1}{2} \left(1 - \sqrt{\frac{R\bar{\gamma}}{1+R\bar{\gamma}}}\right) \end{aligned} \quad (4.49)$$

where $R = k/n$.

The following MATLAB program is used to compare the theoretical decoding error probability of different RS codes with BPSK modulation in AWGN channel.

Program 4.1 Program to compare the decoding error probability of different RS codes

```
clearall;clc;
Eb_N0_dB = [0:0.3:15]; % multiple Eb/N0 values
EbN0Lin = 10.^ (Eb_N0_dB/10);
% Uncoded
P_b0 = 0.5* erfc( sqrt( EbN0Lin ) );
% RS (127, 106),t=10
m=7;
n6 = 2^m -1;
k6 = 106;
t6 = 10;
R_c6 = k6/n6;
p = 0.5* erfc( sqrt(R_c6 * EbN0Lin) );
sum = 0
for j=t6+1:n6
sum = sum +j*factorial(n6)/factorial(j)/factorial (n6-j) .*p.^j .* (1-p).^(n6-j)
end
P_b1 = sum/n6;
% RS (127, 106),t=10
m=5;
n6 = 2^m -1;
k6 = 15;
t6 = 8;;
R_c6 = k6/n6;
p = 0.5* erfc( sqrt(R_c6 * EbN0Lin) );
sum = 0
for j=t6+1:n6
sum = sum +j*factorial(n6)/factorial(j)/factorial (n6-j) .*p.^j .* (1-p).^(n6-j)
end
P_b2 = sum/n6;
m=5;
n6 = 2^m -1;
k6 = 21;
t6 = 5;
R_c6 = k6/n6;
p = 0.5* erfc( sqrt(R_c6 * EbN0Lin) );
```

```

sum = 0
for j=t6+1:n6
sum = sum +j*factorial(n6)/factorial(j)/factorial (n6-j) .*p.^j .* (1-p).^(n6-j)
end
P_b3 = sum/n6;
m=5;%6;
n6 = 2^m -1;
k6 = 27;
t6 = 2;
R_c6 = k6/n6;
p = 0.5* erfc( sqrt(R_c6 * EbN0Lin) );
sum = 0
for j=t6+1:n6
sum = sum +j*factorial(n6)/factorial(j)/factorial (n6-j) .*p.^j .* (1-p).^(n6-j)
end
P_b4 = sum/n6;
figure
semilogy(Eb_N0_dB, P_b0, '-.',Eb_N0_dB,P_b1, '-x', Eb_N0_dB, P_b2, '-*',
*,Eb_N0_dB, P_b3, '-+', Eb_N0_dB, P_b4, '-d');
xlabel('Eb/No (dB)'), ylabel('BER');
legend('Uncoded','RS (127,106)', 'RS (31,15)', 'RS (31,21)', 'RS (31,27)');
axis([0 15 1e-6 1e-0]);

```

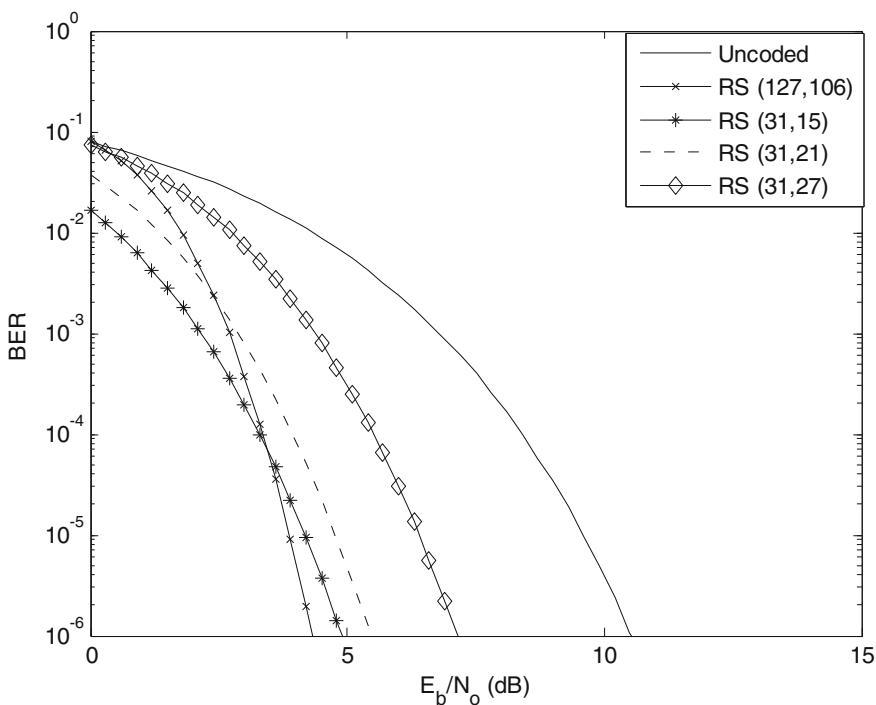


Fig. 4.10 Decoding error probability for RS codes using coherent BPSK over an AWGN channel

The decoding error probability obtained from the above program for RS (127,106) and for RS code of length 31 with different dimensions k is shown in Fig. 4.10.

From Fig. 4.10, it can be observed that the decoder error probability approach increasingly lowers as the E_b/N_0 and code dimension decrease. This can be attributed to the highly imperfect nature of RS codes.

The following MATLAB program compares the theoretical BER performance of (127,63) RS code with BPSK modulation in AWGN and Rayleigh fading channels

Program 4.2 Program to compare the decoding error probability of an RS code in AWGN and Rayleigh fading channels using coherent BPSK modulation

```
clearall;clc;
Eb_N0_dB = [0:0.3:15]; % multiple Eb/N0 values
EbN0Lin = 10.^ (Eb_N0_dB/10);
% Uncoded
P_bawgn = 0.5* erfc( sqrt( EbN0Lin ) );
p_bRay = 1/2 - 1/2*(1+1./EbN0Lin).^( -1/2 );
% RS (127, 106),t=10
m=7; n6 = 2^m -1;
k6 = 63;
t6 = 32;
R_c6 = k6/n6;
p = 0.5* erfc( sqrt(R_c6 * EbN0Lin ) );
p1 = 1/2 - 1/2*(1+1./(R_c6 * EbN0Lin)).^( -1/2 );
sum = 0
for j=t6+1:n6
    sum = sum +j*factorial(n6)/factorial(j)/factorial (n6-j) .*p.^j .* (1-p).^(n6-j)
end
P_b1 = sum/n6;
sum = 0
for j=t6+1:n6
    sum = sum +j*factorial(n6)/factorial(j)/factorial (n6-j) .*p1.^j .* (1-p1).^(n6-j)
end
P_b2 = sum/n6;
figure
semilogy(Eb_N0_dB, p_bRay, '- ', Eb_N0_dB, P_bawgn, '-- ', Eb_N0_dB, P_b1, '- ', Eb_N0_dB, P_b2, '-d');
xlabel('E_b/N_o (dB)', ylabel('BER');
legend('Uncoded Rayleigh ','Uncoded AWGN','RS (127,63) AWGN', 'RS (127,63) Rayleigh');
axis([0 15 1e-6 1e-0]);
```

The decoding error probability obtained from the above program for RS (127,63) is shown in Fig. 4.11.

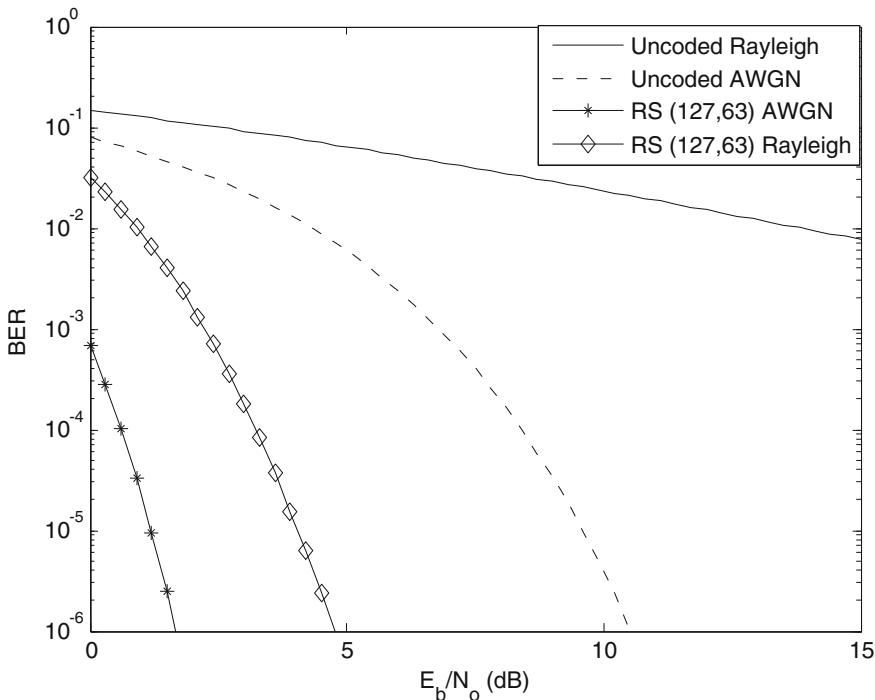


Fig. 4.11 Decoding error probability for (127,63) RS codes using coherent BPSK over an AWGN channel and Rayleigh fading channel

From Fig. 4.11, it is seen that the coded AWGN and Rayleigh fading channels exhibit much better BER performance than the uncoded AWGN and Rayleigh fading channels.

4.6.2 BER Performance of RS Codes for Non-coherent BFSK Modulation in AWGN and Rayleigh Fading Channels

From Eq. (2.25), for BFSK ($M = 2$), the probability of bit error P for AWGN and Rayleigh fading channels can be expressed as

$$P = \frac{1}{2} \exp\left[-\frac{RE_b}{2N_o}\right] \quad \text{AWGN}$$

$$P = \frac{1}{2 + R\bar{\gamma}} \quad \text{Rayleigh fading} \quad (4.50)$$

Program 4.3 Program to compare the decoding error probability of an RS code in AWGN and Rayleigh fading channels using non-coherent BFSK modulation

```

clearall;clc;
Eb_N0_dB = [0:0.3:15];
K=5; m= 7;
EbN0Lin = 10.^{Eb_N0_dB/10};
P_bawgn = 0.5*exp(-0.5*EbN0Lin); % theoretical ber
p_bRay = 1./{EbN0Lin+2};
n6 = 2^m -1;
k6 = 63;
t6 = 32;
R_c6 = k6/n6;
p = 0.5*exp(-0.5*R_c6*EbN0Lin);
p1 = 1./({2+R_c6 * EbN0Lin});
sum = 0
for j=t6+1:n6
sum = sum +j*factorial(n6)/factorial(j)/factorial (n6-j) .*p.^j .* (1-p).^(n6-j)
end
P_b1 = sum/n6;
sum = 0
for j=t6+1:n6
sum = sum +j*factorial(n6)/factorial(j)/factorial (n6-j) .*p1.^j .* (1-
p1).^(n6-j)
end
P_b2 = sum/n6;
figure
semilogy(Eb_N0_dB, p_bRay, '-',Eb_N0_dB,P_bawgn, '--', Eb_N0_dB, P_b1, '-*
',Eb_N0_dB, P_b2, '-d');
xlabel('E_b/N_o (dB)'), ylabel('BER');
legend('Uncoded Rayleigh ','Uncoded AWGN','RS (127,63) AWGN', 'RS
(127,63) Rayleigh');
axis([0 15 1e-6 1e-0]);

```

The decoding error probability obtained from the above program for RS (127,63) is shown in Fig. 4.12.

From Fig. 4.12, it is seen that the coded AWGN and Rayleigh fading channels exhibit much better BER performance than the uncoded AWGN and Rayleigh fading channels. However, the performance is not better as compared to that of BPSK modulation.

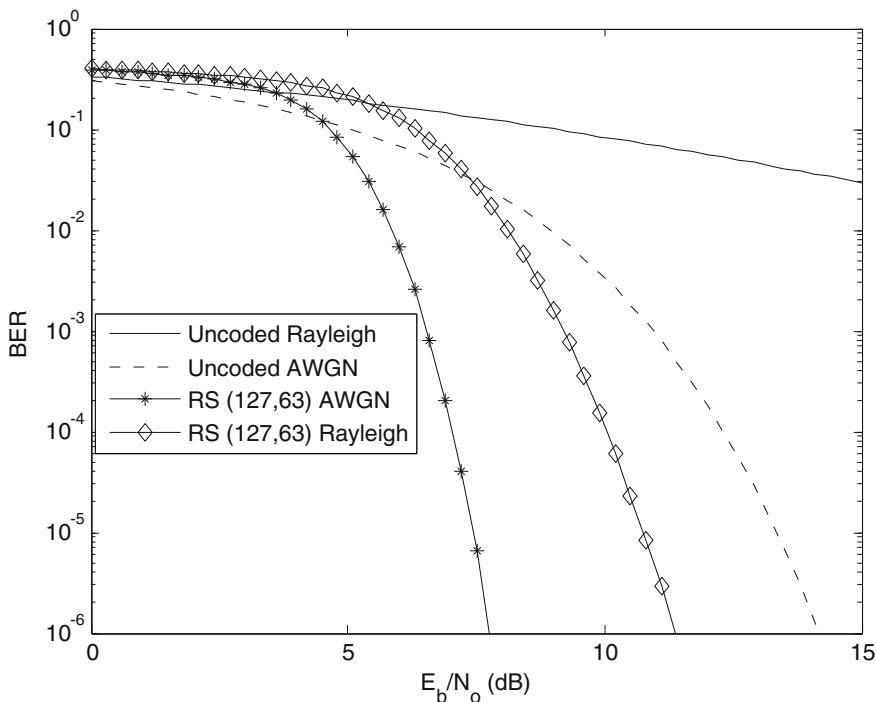


Fig. 4.12 Decoding error probability for (127,63) RS codes using non-coherent BPSK

4.7 Problems

1. Construct encoder circuit using shift register for (15,7) cyclic code generated by $g(x) = 1 + x^4 + x^6 + x^7 + x^8y$, and find the code word corresponding to the information sequence (1001011).
2. Construct a shift register decoder for the (15,11) cyclic Hamming code generated by $g(x) = 1 + x + x^4$, and decode the received word $r = (111100000100100)$.
3. Design a four-error-correcting binary BCH code of length 15.
4. Let the transmission code be the triple-error-correcting binary BCH code of length 31. The generator polynomial is $g(x) = 1 + x + x^2 + x^3 + x^5 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{15}$. Use Berlekamp's algorithm to decode the following received vector $r = (010000000000100000000000100000)$.
5. Let the transmission code be the double-error-correcting binary BCH code of length 15. The generator polynomial is $g(x) = 1 + x^4 + x^6 + x^7 + x^8$. Use Berlekamp's algorithm to decode the following received vector $r = (00f0000000000000000000000000000)$. The f indicates erasure.

6. Construct a generator polynomial for a double-error-correcting Reed–Solomon code of length 7, and determine the number of code words it does have.
7. Determine the weight distribution for the RS code of problem 1.
8. Compute a generator polynomial for a triple-error-correcting Reed–Solomon code of length 31.
9. Construct a generator polynomial for a (63,57) RS code, and determine the code words it does have.
10. Let the transmission code be the double-error-correcting RS code of length 7. Use the Berlekamp–Massey algorithm to decode the following received vector $r = (00010\alpha_0)$.
11. Let the transmission code be the double-error-correcting RS code of length 7. Use the Berlekamp–Massey algorithm to decode the following received vector $r = (1010000)$.
12. Let the transmission code be the double-error-correcting RS code of length 7. Use the Berlekamp–Massey algorithm to decode the following received vector $r = (\alpha^3\alpha_1\alpha\alpha^200)$.
13. Let the transmission code be the triple-error-correcting RS code of length 15. Decode the received vector $r = (000\alpha^7000000\alpha^{11}0000)$ using Berlekamp–Massey algorithm.
14. Let the transmission code be the double-error-correcting RS code of length 15. Use the Berlekamp–Massey algorithm to decode the following received vector $r = (100100000000000)$.
15. Let the transmission code be the triple-error-correcting RS code of length 31. Decode the following received vector $r = (\alpha^200000000000\alpha^{21}0000000\alpha^700000000)$ using the Berlekamp–Massey algorithm.
16. Let the transmission code be the double-error-correcting RS code of length 7. Use the Berlekamp–Massey algorithm to decode the following received vector $r = (00\alpha^3f101)$.

4.8 MATLAB Exercises

1. Write a MATLAB program to simulate the performance of BPSK modulation in AWGN and Rayleigh fading channels and compare with theoretical results shown in Chap. 2.
2. Write a MATLAB program to simulate the performance of RS-coded SFH-CDMA using BFSK modulation and compare with the uncoded theoretical results shown in Chap. 2.
3. Write a MATLAB program to simulate the BER performance of an RS code in AWGN and Rayleigh fading channels using BPSK modulation and compare with the theoretical results shown in Fig. 4.4.

4. Write a MATLAB program to simulate the BER performance of an RS code in AWGN and Rayleigh fading channels using BFSK modulation and compare with the theoretical results shown in Fig. 4.5.
5. Write a MATLAB program to simulate the BER performance of an RS code in AWGN and Rayleigh fading channels using MFSK modulation for $M > 2$.

References

1. Forney, G.D.: On decoding BCH codes. *IEEE Trans. Inf. Theory* **IT-11**, 549–557 (1965)
2. Massey, J.L.: Shift register synthesis and BCH decoding. *IEEE Trans. Inf. Theory* **IT-15**(1), 122–127 (1969)
3. Berlekamp, E.R.: Algebraic Coding Theory, rev edn. Aegean Park Press, Laguna Hills (1984)
4. Chien, R.T.: Cyclic decoding procedure for the Bose-Chaudhuri-Hocquenghem codes. *IEEE Trans. Inf. Theory* **IT-10**(1), 357–363 (1964)
5. Du, K.L., Swamy, M.N.S.: Wireless Communications: Communication Systems from RF Subsystems to 4G Enabling Technologies. Cambridge University Press, Cambridge (2010)

Chapter 5

Convolutional Codes

In the convolutional coding, the message bits come in serially instead of large blocks. The name convolutional codes are due to the fact that the redundant bits are generated by the use of modulo-2 convolutions in a convolutional encoder. The convolutional encoder can be considered as finite-state machine consisting of an M-stage shift register and modulo-2 adders multiplexers. The rate of a convolutional encoder with k inputs and n outputs is k/n . Often the manufacturers of convolutional code chips specify the code by parameters (n, k, L) . The quantity L is called the constraint length of the code that represents the maximum number of bits in a single-output stream that can be affected by any input bit.

5.1 Structure of Non-systematic Convolutional Encoder

Consider a rate 1/3 convolutional encoder as shown in Fig. 5.1. The binary data stream $x(n) = (x(0), x(1), x(2), \dots)$ is fed into shift register containing a series of memory elements. The contents of the memory elements are tapped and added according to modulo-2 addition to create the coded output data streams

$$\begin{aligned}y_1(n) &= (y_1(0), y_1(1), y_1(2), \dots), \\y_2(n) &= (y_2(0), y_2(1), y_2(2), \dots) \text{ and} \\y_3(n) &= (y_3(0), y_3(1), y_3(2), \dots).\end{aligned}$$

Then, these output coded data streams are multiplexed to create a single-coded output data stream

$$Y = (y_1(0), y_2(0), y_3(0), y_1(1), y_2(1), y_3(1), y_1(2), y_2(2), y_3(2), \dots)$$

Electronic supplementary material The online version of this chapter (doi:[10.1007/978-81-322-2292-7_5](https://doi.org/10.1007/978-81-322-2292-7_5)) contains supplementary material, which is available to authorized users.

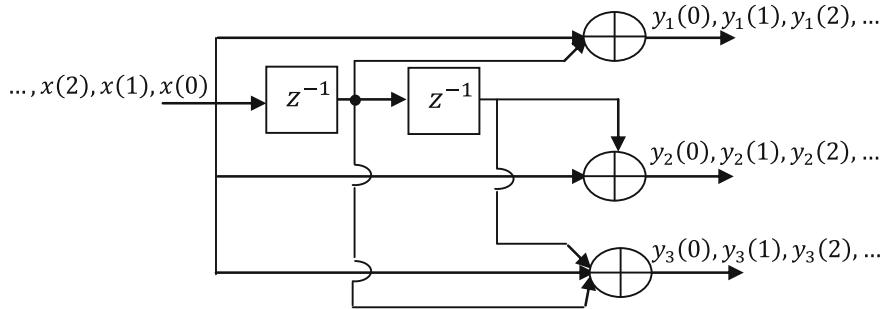


Fig. 5.1 A rate 1/3 linear convolutional encoder

The output streams $y_1(n)$, $y_2(n)$ and $y_3(n)$ can be represented as follows:

$$\begin{aligned}y_1(n) &= x(n) + x(n - 1) \\y_2(n) &= x(n) + x(n - 2) \\y_3(n) &= x(n) + x(n - 1) + x(n - 2)\end{aligned}$$

Example 5.1 Prove the encoder shown in Fig. 5.1 is linear convolutional encoder.

Proof Let the input $x_1(n) = (11101)$. Then, the corresponding coded output sequences

$$\begin{aligned}y_1(n) &= (1001110) \\y_2(n) &= (1101001) \\y_3(n) &= (1010011)\end{aligned}$$

The convolutional code word corresponding to $x_1(n) = (11101)$ is then

$$Y_1 = (111, 010, 001, 110, 100, 101, 011)$$

Let the input $x_2(n) = (10010)$

The corresponding coded output sequences are

$$\begin{aligned}y_1(n) &= (1101100) \\y_2(n) &= (1011010) \\y_3(n) &= (1111110)\end{aligned}$$

The convolutional code word corresponding to $x_2(n) = (10010)$ is

$$Y_2 = (111, 101, 011, 111, 101, 011, 000)$$

Let the input $x(n) = x_1(n) + x_2(n) = (01111)$.

The corresponding coded output sequences are given as

$$y_1(n) = (0100010)$$

$$y_2(n) = (0100010)$$

$$y_3(n) = (0101101)$$

The convolutional code word corresponding to $x(n) = (01111)$ is given as follows:

$$Y = (000, 111, 010, 001, 001, 110, 011)$$

$$\begin{aligned} Y_1 + Y_2 &= (111, 010, 001, 110, 100, 101, 011) + (111, 101, 011, 111, 101, 011, 000) \\ &= (000, 111, 010, 001, 001, 110, 011) \\ &= Y \end{aligned}$$

“A convolutional encoder is linear, if Y_1 and Y_2 are the code words corresponding to inputs $x_1(n)$ and $x_2(n)$, respectively, then $(Y_1 + Y_2)$ is the code word corresponding to the input $x_1(n) + x_2(n)$.” Hence, the convolutional encoder in the problem is proved to be linear.

5.1.1 Impulse Response of Convolutional Codes

The impulse response stream $g_i(n)$ for the input $x(n) = (1000 \dots)$ for the encoder shown in Fig. 5.1 can be represented as follows:

The impulse response $g_1(n)$ can be represented by

$$g_1(n) = x(n) + x(n - 1)$$

The impulse response $g_2(n)$ can be represented by

$$g_2(n) = x(n) + x(n - 2)$$

The impulse response $g_3(n)$ can be represented by

$$g_3(n) = x(n) + x(n - 1) + x(n - 2)$$

Thus, the impulse responses for the encoder are

$$\begin{aligned}g_1(n) &= (110) \\g_2(n) &= (101) \\g_3(n) &= (111)\end{aligned}$$

Since there are two memory elements in the shift register of the encoder, each bit in the input data stream can effect at most 3 bits, hence the length of the above impulse response sequence is 3.

Since the convolutional encoder can be described by discrete convolutional operation, if the information sequence $x(n)$ is input to the encoder, the three outputs are given by

$$\begin{aligned}y_1(n) &= x(n) * g_1(n) \\y_2(n) &= x(n) * g_2(n) \\y_3(n) &= x(n) * g_3(n)\end{aligned}$$

where $*$ represents the convolution operation. In the D -transform domain, the three outputs can be represented as

$$\begin{aligned}Y_1(D) &= X(D)G_1(D) \\Y_2(D) &= X(D)G_2(D) \\Y_3(D) &= X(D)G_3(D)\end{aligned}$$

The D denotes the unit delay introduced by the memory element in the shift register. The use of D transform is most common in the coding literature. The delay operator D is equivalent to the indeterminate z^{-1} of the z -transform. The D transforms of the impulse responses of the above encoder are

$$\begin{aligned}G_1(D) &= 1 + D \\G_2(D) &= 1 + D^2 \\G_3(D) &= 1 + D + D^2\end{aligned}$$

Hence, the encoder shown in Fig. 5.1 can be described by a generator matrix

$$G(D) = [G_1(D) \quad G_2(D) \quad G_3(D)]$$

The transform of the encoder output can be expressed as

$$Y(D) = X(D)G(D)$$

where

$$Y(D) = [Y_1(D) \quad Y_2(D) \quad Y_3(D)].$$

The $G(D)$ is called the transfer function matrix of the encoder shown in Fig. 5.1.

Example 5.2 Determine the output code word of the encoder shown in Fig. 5.1 using the transfer function matrix if the input sequence $X = (11101)$.

Solution The D transform of the input sequence x is given by

$$X(D) = 1 + D + D^2 + D^4$$

The D transform of the encoder output follows as

$$\begin{aligned} Y(D) &= [1 + D + D^2 + D^4][1 + D \quad 1 + D^2 \quad 1 + D + D^2] \\ &= [1 + D^3 + D^4 + D^5 \quad 1 + D + D^3 + D^6 \quad 1 + D^2 + D^5 + D^6] \end{aligned}$$

Inverting the D transform, we get

$$\begin{aligned} y_1(n) &= (1001110) \\ y_2(n) &= (1101001) \\ y_3(n) &= (1010011) \end{aligned}$$

Then, the output code word y is

$$y = (111, 010, 001, 110, 100, 101, 011)$$

5.1.2 Constraint Length

The constraint length “ L ” of a convolutional code is the length of longest input shift register with maximum number of memory elements plus one.

5.1.3 Convolutional Encoding Using MATLAB

The following MATLAB program illustrates the computation of the output code word of the encoder shown in Fig. 5.1 for input sequence $x_2 = (10010)$

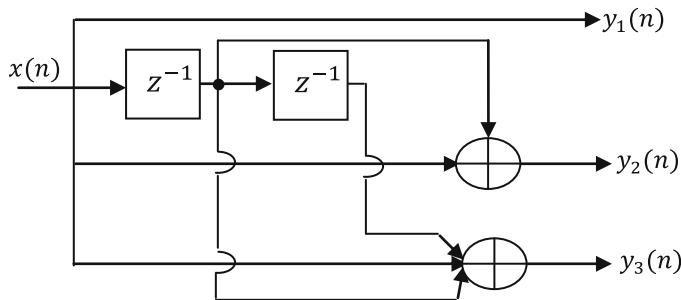


Fig. 5.2 A rate 1/3 systematic convolutional encoder

Program 5.1 MATLAB program to determine the output codeword of the encoder shown in Fig. 5.1

```

clear all;clc;
x=[1 0 0 1 0];
y1 = mod(conv(x, [1 1 0]),2);
y2 = mod(conv(x, [1 0 1]),2);
y3 = mod(conv(x, [1 1 1]),2);
Y123 = [y1;y2;y3];
Y = cip(:).'%; code word

```

The above program outputs the following codeword

$$Y = [1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0]$$

5.2 Structure of Systematic Convolutional Encoder

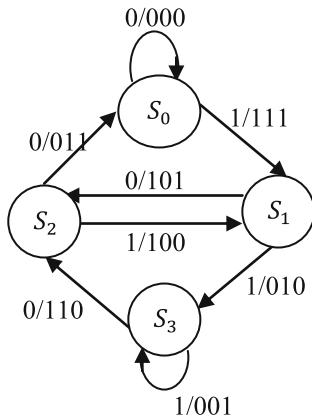
A convolutional code in which the input data appear as a part of the code sequence is said to be systematic. A rate 1/3 systematic convolutional encoder is shown in Fig. 5.2.

5.3 The Structural Properties of Convolutional Codes

5.3.1 State Diagram

The contents of memory elements of a convolutional encoder provide mapping between the input bits and the output bits. An encoder with j memory elements can assume any one of 2^j possible states. The encoder can only move between states.

Fig. 5.3 State diagram of non-systematic convolutional encoder shown in Fig. 5.1



Each branch in the state diagram has a label of the form $X/YYY\dots$, where X is the input bit that causes the state transition and $YYY\dots$ is the corresponding output bits. The encoder shown in Fig. 5.1 consists of two memory elements and hence the two binary elements can assume any one of the four states designated by $S_0 - 00$; $S_1 - 10$; $S_2 - 01$; $S_3 - 11$.

For the encoder shown in Fig. 5.1, the state diagram is shown in Fig. 5.3.

5.3.2 Catastrophic Convolutional Codes

A convolutional code is said to be catastrophic if its encoder generates all zero output sequence for a nonzero input sequence. A catastrophic code can cause an unlimited number of data errors for a small number of errors in the received code word. The following Theorem [1] can be used to verify whether a convolutional code is catastrophic.

Theorem 5.1 A rate $1/n$ convolutional code with transfer function matrix $G(D)$ with generated sequences having the transforms $\{G_0(D), G_1(D), \dots, G_{n-1}(D)\}$ is not catastrophic if and only if

$$\text{GCD}(G_0(D), G_1(D), \dots, G_{n-1}(D)) = D^l$$

for some non-negative integer l .

Example 5.3 Determine whether the encoder shown in Fig. 5.4 generates a catastrophic convolutional code or not.

Solution From the encoder diagram shown in Fig. 5.4, the impulse responses are $g_1 = (1110)$ and $g_2 = (1001)$.

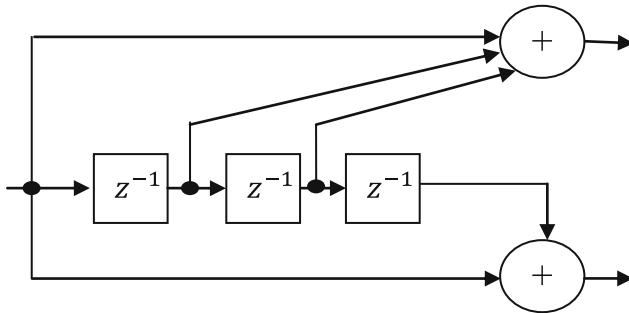


Fig. 5.4 A rate $-1/2$ convolutional encoder

The transform of the generator sequence $g_1 = (1110)$ is $G_1(D) = 1 + D + D^2$
 The transform of the generator sequence $g_2 = (1001)$ is $G_2(D) = 1 + D^3$

$$\begin{aligned} \text{GCD}[G_1(D), G_2(D)] &= \text{GCD}[1 + D + D^2, 1 + D^3] \\ &= 1 + D + D^2 \\ &\neq D^l \end{aligned}$$

Thus, the code is catastrophic for any integer l , where GCD stands for greatest common divisor.

5.3.3 Transfer Function of a Convolutional Encoder

The signal flow graph for a convolutional encoder can be obtained by splitting the state S_0 into a source node and sink node by modifying the labels of the branches. For a given branch, we label $Y^i X^j$ where j is the weight of the input vector X and i is the weight of the output vector Y (the number of nonzero coordinates).

Example 5.4 Determine the transfer function of the systematic convolutional encoder shown in Fig. 5.2.

Solution The state diagram of the systematic convolutional encoder is shown in Fig. 5.5.

The signal flow graph of the above state diagram is shown in Fig. 5.6. In this signal flow graph, the self loop at node S_0 is eliminated as it contributes nothing to the distance properties of a code relative to the all zero code sequence. Now, by using the signal flow graph reduction techniques and Mason's formula, the transfer function can be obtained.

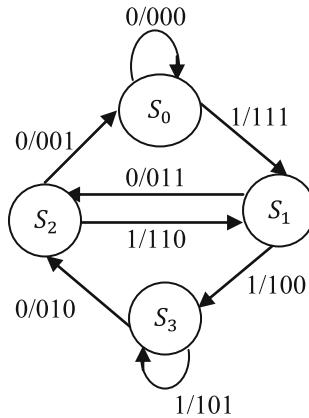


Fig. 5.5 State diagram of systematic convolutional encoder shown in Fig. 5.2

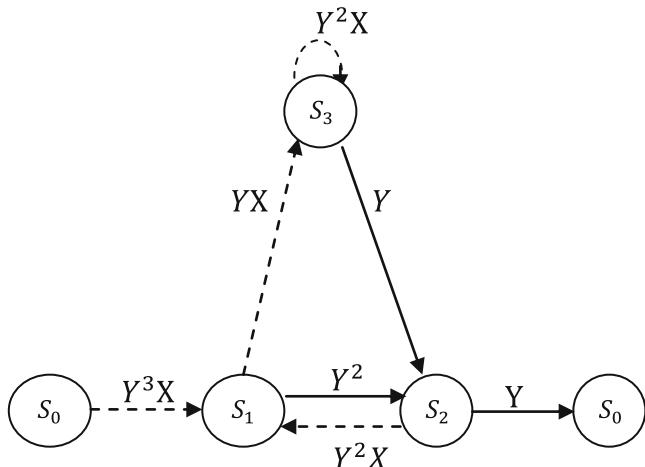
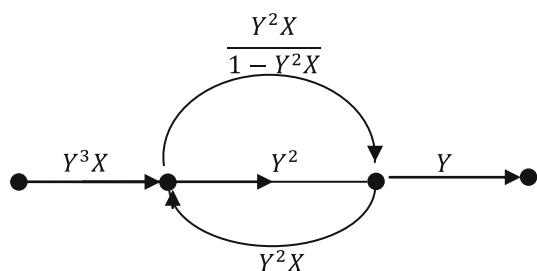
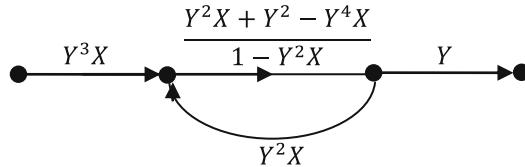


Fig. 5.6 Signal flow graph of the above state diagram is shown in Fig. 5.5

By using reduction techniques, the above signal flow graph can be simplified as

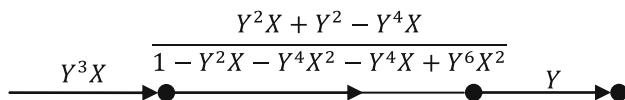


Further, the parallel branches with gains Y^2 and $\frac{Y^2X}{1-Y^2X}$ can be combined as a single branch with gain $Y^2 + \frac{Y^2X}{1-Y^2X} = \frac{Y^2X+Y^2-Y^4X}{1-Y^2X}$ as follows:



Further, the loop can be replaced by a branch with gain

$$\frac{\frac{Y^2X+Y^2-Y^4X}{1-Y^2X}}{1 - Y^2X \frac{Y^2X+Y^2-Y^4X}{1-Y^2X}} = \frac{Y^2X + Y^2 - Y^4X}{1 - Y^2X - Y^4X^2 - Y^4X + Y^6X^2}$$



Thus, the transfer function is given by

$$\begin{aligned} T(Y) &= Y^3X \frac{Y^2X + Y^2 - Y^4X}{1 - Y^2X - Y^4X^2 - Y^4X + Y^6X^2} Y \\ &= \frac{Y^6X^2 + Y^6X - Y^8X^2}{1 - Y^2X - Y^4X^2 - Y^4X + Y^6X^2} \end{aligned}$$

Example 5.5 Consider the following non-systematic convolutional encoder and determine its transfer function (Fig. 5.7).

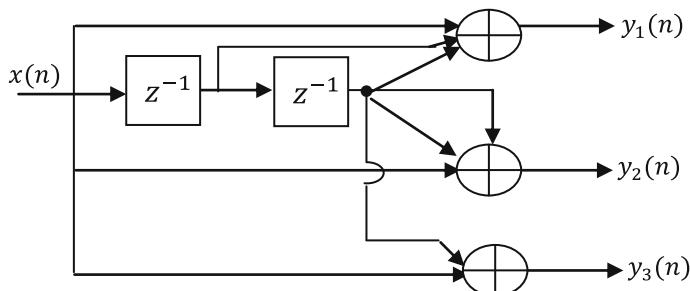


Fig. 5.7 Encoder for a rate $-1/3$ convolutional code

Solution The state diagram of the non-systematic convolutional encoder is shown in Fig. 5.8.

The signal flow graph of the above state diagram is shown in Fig. 5.9.

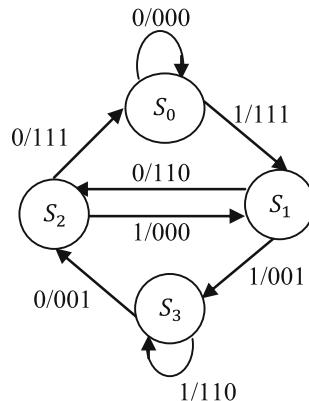


Fig. 5.8 State diagram of non-systematic convolutional encoder shown in Fig. 5.7

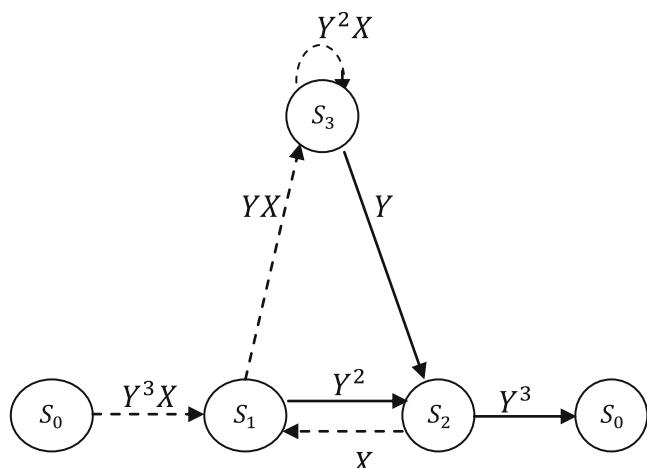
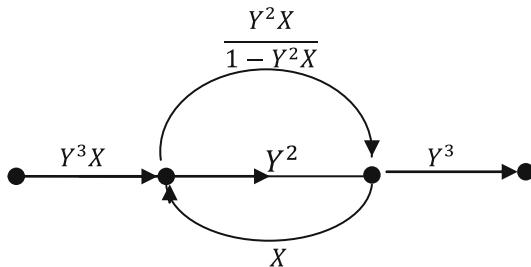
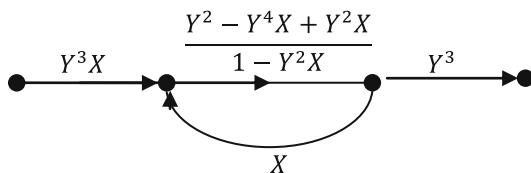


Fig. 5.9 Signal flow graph of the state diagram shown in Fig. 5.8

By using reduction techniques, the above signal flow graph can be simplified as follows:

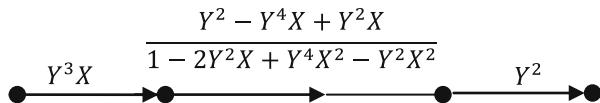


Further, the parallel branches with gains Y^2 and $\frac{Y^2X}{1-Y^2X}$ can be combined as a single branch with gain $Y^2 + \frac{Y^2X}{1-Y^2X} = \frac{Y^2 - Y^4X + Y^2X}{1 - Y^2X}$ as follows:



Further, the loop can be replaced by a branch with gain

$$\frac{\frac{Y^2 - Y^4X + Y^2X}{1 - Y^2X}}{1 - X \frac{Y^2 - Y^4X + Y^2X}{1 - Y^2X}} = \frac{Y^2 - Y^4X + Y^2X}{1 - 2Y^2X + Y^4X^2 - Y^2X^2}$$



Thus, the transfer function is given by

$$\begin{aligned} T(Y, X) &= Y^3X \frac{Y^2 - Y^4X + Y^2X}{1 - 2Y^2X + Y^4X^2 - Y^2X^2} Y^3 \\ &= \frac{Y^8X - Y^{10}X^2 + Y^8X^2}{1 - 2Y^2X + Y^4X^2 - Y^2X^2} \end{aligned}$$

5.3.4 Distance Properties of Convolutional Codes

An upper bound on the minimum free distance of a rate $1/n$ convolutional code is given by [2]

$$d_f \leq \max_{l > 1} \left\lfloor \frac{2^{l-1}}{2^l - 1} (L + l - 1)n \right\rfloor \quad (5.1)$$

where $\lfloor x \rfloor$ denotes the largest integer contained in x .

The transfer function also yields the distance properties of the code. The minimum distance of the code is called the minimum free distance denoted by d_f . The d_f is the lowest power in the transfer function.

In Example 5.4, since the lowest power in the transfer function is 6, the d_f for the systematic convolutional encoder considered in this example is 6, whereas in Example 5.5, the lowest power in the transfer function is 8. Hence, the minimum free distance for the non-systematic encoder considered in this example is 8.

From the above two examples, it is observed that the minimum free distance for non-recursive systematic convolutional code is less than that of a non-recursive non-systematic convolutional codes of the same rate and constraint length. The bounds on the minimum free distance for various codes are developed in [3, 4]. The bounds on the free distance for various systematic and non-systematic codes of the same rate and constraint length are tabulated in Table 5.1.

5.3.5 Trellis Diagram

The state diagram does not contain time information required in decoding. Hence, trellis diagram is developed to overcome the disadvantage. The trellis diagram is an expansion of state diagram by adding a time axis for time information. In the trellis

Table 5.1 The bounds on the free distance for various systematic and non-systematic codes of the same rate and constraint length

Rate	Constraint length	Systematic codes maximum free distance	Non-systematic codes maximum free distance
1/3	2	5	5
	3	6	8
	4	8	10
	5	9	12
1/2	2	3	3
	3	4	5
	4	4	6
	5	5	7

diagram, the nodes are arranged vertically representing the states of the encoder and each node corresponding to a state of the encoder after a transition from the previous node for an input bit, the horizontal axis represents time, and the labels on the branches represent the encoder output bits for a state transition and the input bit causing the transition.

For a (n, k) convolutional code with memory order m , there are 2^m nodes at each time increment t and there are 2^k branches leaving each node for $t \leq m$. For $t > m$, there are also 2^k branches entering the node.

For an encoder with single input sequence of B bits, the trellis diagram must have $B + m$ stages with the first and last stages starting and stopping, respectively, in state S_0 . Thus, there are 2^B distinct paths through trellis each corresponding to the code word of the length $n(B + m)$.

Example 5.6 The impulse responses of a convolutional encoder are given by $g_1 = [1\ 0\ 1]$; $g_2 = [1\ 1\ 1]$

1. Draw the encoder
2. Draw the state diagram
3. Draw the trellis diagram for the first three stages.

Solution

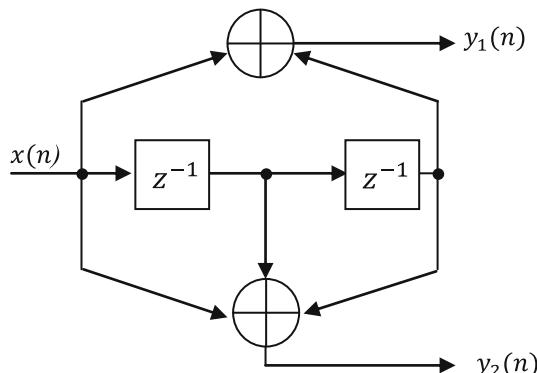
1. From the impulse responses $g_1 = [1\ 0\ 1]$; $g_2 = [1\ 1\ 1]$, the output stream $y_1(n)$ can be represented as follows:

$$y_1(n) = x(n) + x(n - 2)$$

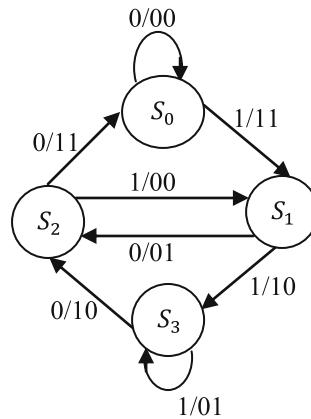
The output stream $y_2(n)$ can be represented as follows:

$$y_2(n) = x(n) + x(n - 1) + x(n - 2)$$

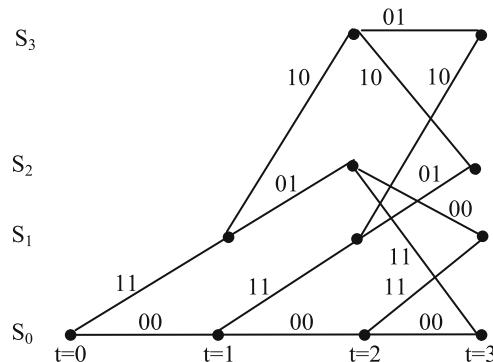
Hence, the corresponding encoder is as follows:



2. This rate $-1/2$ encoder has two memory cells. So, the associated state diagram has four states as shown below.



3. The trellis diagram is an extension of the state diagram that explicitly shows the passage of time. The first three stages of the trellis diagram corresponding to the encoder is as follows:



Example 5.7 The impulse responses of a convolutional encoder are given by $g_1 = [1 \ 1 \ 1]$; $g_2 = [1 \ 1 \ 1]$; $g_3 = [1 \ 1 \ 0]$

1. Draw the encoder
2. Draw the state diagram
3. Draw the trellis diagram for the length 3 input sequence.

Solution

1. From the impulse responses $g_1 = [1 \ 1 \ 1]$; $g_2 = [1 \ 1 \ 1]$; $g_3 = [1 \ 1 \ 0]$, the output stream $y_1(n)$ can be represented as follows:

$$y_1(n) = x(n) + x(n - 1) + x(n - 2)$$

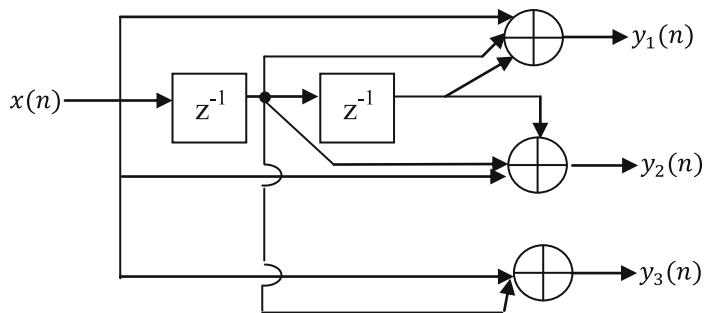
The output stream $y_2(n)$ can be represented as follows:

$$y_2(n) = x(n) + x(n - 1) + x(n - 2)$$

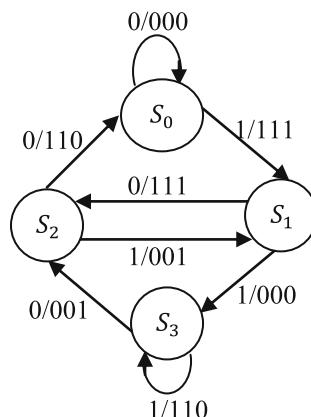
The output stream $y_3(n)$ can be represented as follows:

$$y_3(n) = x(n) + x(n - 1)$$

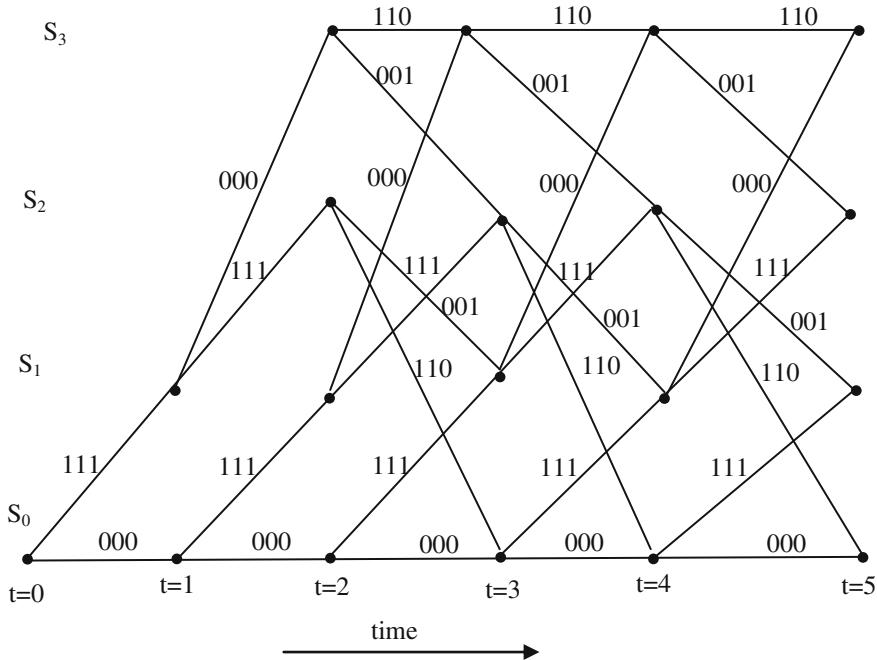
Hence the corresponding encoder is as follows:



2. This rate $-1/3$ encoder has three memory cells. So, the associated state diagram has four states as shown below.



3. The trellis diagram is an extension of the state diagram that explicitly shows the passage of time. The first five stages of the trellis diagram corresponding to the encoder are as follows:



5.4 Punctured Convolutional Codes

The computational complexity is an issue for implementation of Viterbi decoder for high-rate convolutional codes. This issue can be avoided by using punctured convolutional codes. The puncturing process deletes periodically selected coded bits from one or more of the output streams of a convolutional encoder. For a given fixed low rate convolutional encoder structure, high-rate codes can be achieved by puncturing the output of low rate convolutional encoder. The puncturing pattern is specified by a *puncturing matrix* \mathcal{P} of the form

$$\mathcal{P} = \begin{bmatrix} \mathcal{P}_{11} & \mathcal{P}_{12} & \dots & \mathcal{P}_{1P} \\ \mathcal{P}_{21} & \mathcal{P}_{22} & \dots & \mathcal{P}_{2P} \\ \vdots & \vdots & \vdots & \vdots \\ \mathcal{P}_{n1} & \mathcal{P}_{n2} & \dots & \mathcal{P}_{nP} \end{bmatrix} \quad (5.2)$$

The puncturing matrix will have n rows, one for each output stream in an encoder with n output bits. The number of columns in the puncturing matrix is the number of bits over which the puncturing pattern repeats. The encoder transmits the bit corresponding to $\mathcal{P}_{ij} = 1$ and detects the bit corresponding to $\mathcal{P}_{ij} = 0$. The search for optimum punctured codes has been done by [5–7].

Example 5.8 Construct a rate 2/3 code by puncturing the output of the rate 1/2, non-systematic convolutional encoder of Example 5.6.

Solution To generate rate 2/3 code from the rate 1/2 convolutional code with constraint length 3, the puncturing matrix is given as follows:

$$\mathcal{P} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

The zero entity in the second column of the second row indicates that every second bit in the output $y_1(n)$ is to be punctured. The generation of rate 2/3 code from a rate 1/2 convolutional code is shown in Fig. 5.10. The punctured encoder generates 6 code bits for every 4 message bits and thus the punctured code rate is 2/3.

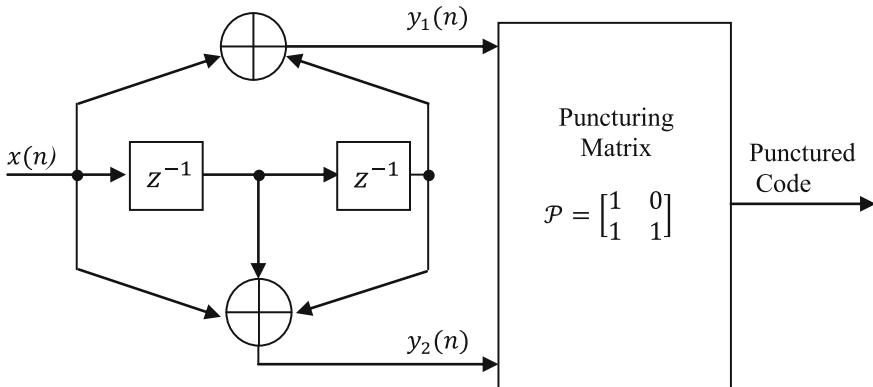
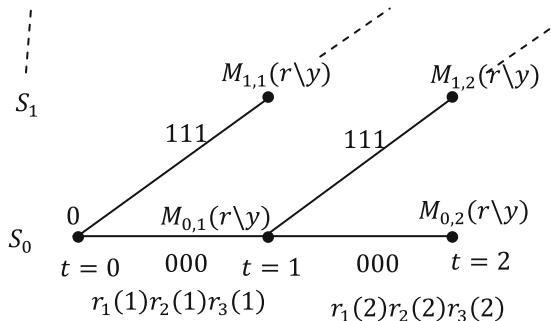


Fig. 5.10 Generation of rate 2/3 code from a rate 1/2 convolutional code

5.5 The Viterbi Decoding Algorithm

The Viterbi algorithm is a maximum likelihood decoding algorithm for convolutional codes involve in finding the path largest metric through the trellis by comparing the metrics of all branch paths entering each state with the corresponding received vector r iteratively. Let $S_{j,t}$ be the node corresponding to the state S_j at time t , and with an assigned value $M_{j,t}(r \setminus y)$. Let m be the memory order. A distance between the received pair of bits and branch output bits is defined as branch metric and sum of metrics of all the branches in a path is defined as path metric.

Partial path metric for a path is obtained by summing the branch metrics for the first few branches that the path traverses. For example, consider the trellis diagram of Example 5.7, the beginning of the trellis is as follows:



Each node in the trellis is assigned a number. This number is the partial path metric of the path that starts at state S_0 at time $t = 0$ and terminates at that node.

Let $M_{j,t}(r \setminus y)$ be the partial path metric entering the node corresponding to the state j at time t . For example, in the accompanying drawing, the label Y corresponds to the two-branch path that terminates at state S_1 at time $t = 2$. Given that the output bits corresponding to this path consist of three zeros followed by three ones, and the received sequence r with received bits of the form $r_k(t)$ indicating the k th bit in the sequence at time t .

$$M_{0,1}(r/y) = M(r_1(1)/0) + M(r_2(1)/0) + M(r_3(1)/0)$$

$$M_{1,1}(r/y) = M(r_1(1)/1) + M(r_2(1)/1) + M(r_3(1)/1)$$

$$M_{0,2}(r/y) = M_{0,1}(r/y) + M(r_1(2)/0) + M(r_2(2)/0) + M(r_3(2)/0)$$

$$M_{1,2}(r/y) = M_{0,1}(r/y) + M(r_1(2)/1) + M(r_2(2)/1) + M(r_3(2)/1)$$

The flowchart for the iterative decoding Viterbi algorithm is shown in Fig. 5.11.

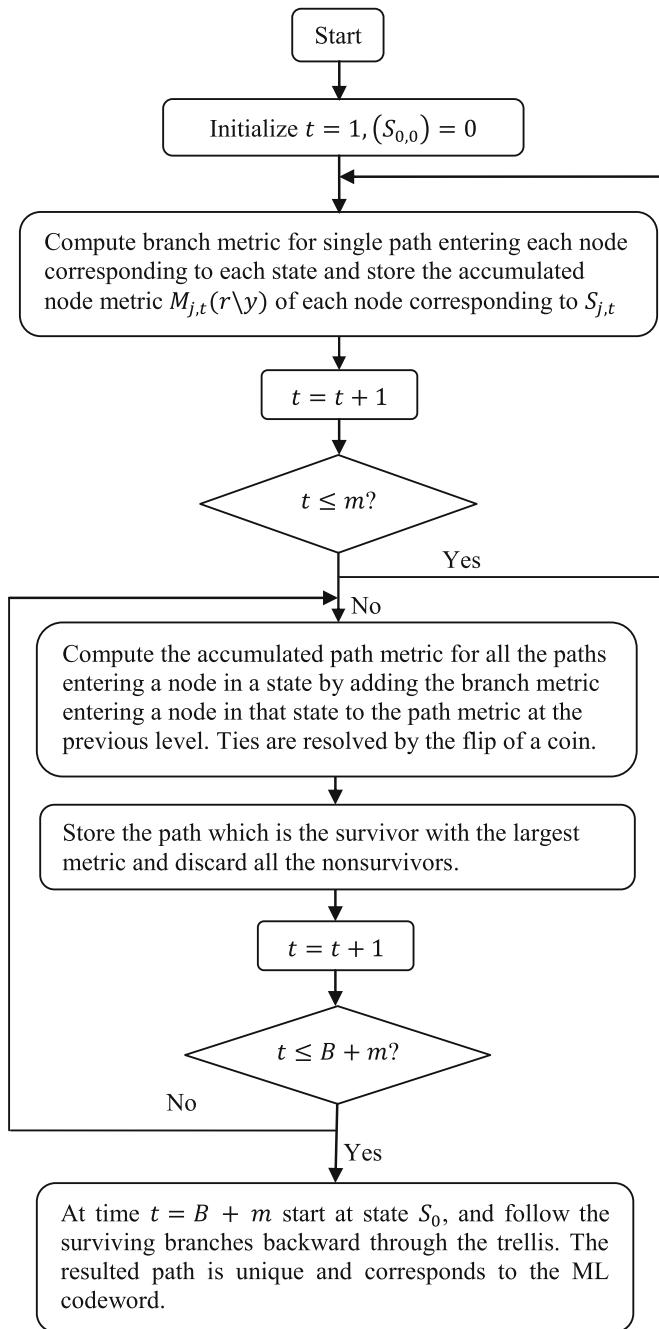


Fig. 5.11 Viterbi algorithm

5.5.1 Hard-decision Decoding

In hard-decision decoding, we will examine each received signal and make a “hard” decision to decide whether the transmitted signal is zero or one. These decisions form the input to the Viterbi decoder. From the decoder’s perspective and by considering the channel to be memory less, the compilation of the likelihood functions in a table is the primary step in defining the bit metrics for the channel. These conditional probabilities are first converted into log likelihood functions and then into bit metrics.

For the BSC case shown in Fig. 1.3 of Chap. 1, the path metric is simply a Hamming distance between code word y and received word r .

Then, the bit metric for BSC case is as follows:

$M(r/y)$	$r = 0$	$r = 1$
$y = 0$	1	0
$y = 1$	0	1

5.5.2 Soft-decision Decoding

In soft-decision decoding, “side information” is generated by the receiver bit decision circuitry and the receiver utilizes this. Instead of assigning zero or one to each received noisy binary signal as in hard-decision decoding, four regions, namely “strong-one,” “weak-one,” “strong-zero,” and “weak-zero,” are established for soft-decision decoding. Intermediate values are given to signals for which the decision is less clear. An increase in coding gain of 2–3 dB over the hard-decision Viterbi decoder is provided by soft-decision decoding for an additive white Gaussian noise channel.

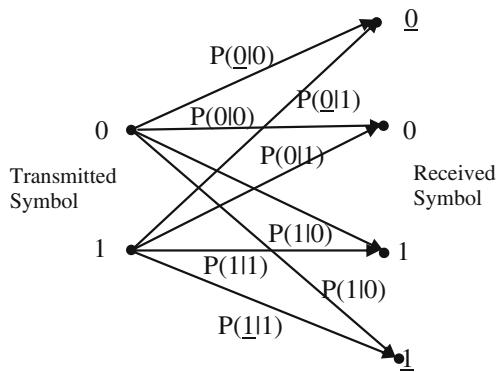
Figure 5.12 shows a discrete symmetric channel where the underlined zero and one indicate the reception of a clear, strong signal, while the non-underlined pair denotes the reception of a weaker signal and the receiver will assigns one of the four values to each received signal.

A hard limiter makes the bit decisions in a hard-decision receiver, whereas a multiple-bit analog-to-digital converter (ADC) is used in soft-decision receivers for this purpose. The channel model shown in Fig. 5.12 uses a 2-bit ADC in the decision circuitry. The soft-decision decoding is almost similar to the hard-decision decoding but uses the increased number (and resolution) of the bit metrics

Consider the following values for the conditional probabilities

$p(r/y)$	$r = 0$	$r = 0$	$r = 1$	$r = 1$
$y = 0$	0.50	0.25	0.15	0.05
$y = 1$	0.05	0.15	0.25	0.50

Fig. 5.12 A discrete symmetric channel model



They provide the following log likelihood functions.

$\log_2 p(r/y)$	$r = \underline{0}$	$r = 0$	$r = 1$	$\underline{1}$
$y = 0$	-0.73	-2	-2.73	-4.32
$y = 1$	-4.32	-2.73	-2	-0.73

Using the expression below, we obtain a set of bit metrics that can be easily implemented in digital hardware.

$$M(r/y) = 1.5[\log_2 M(r/y) - \log_2 M(0.05)]$$

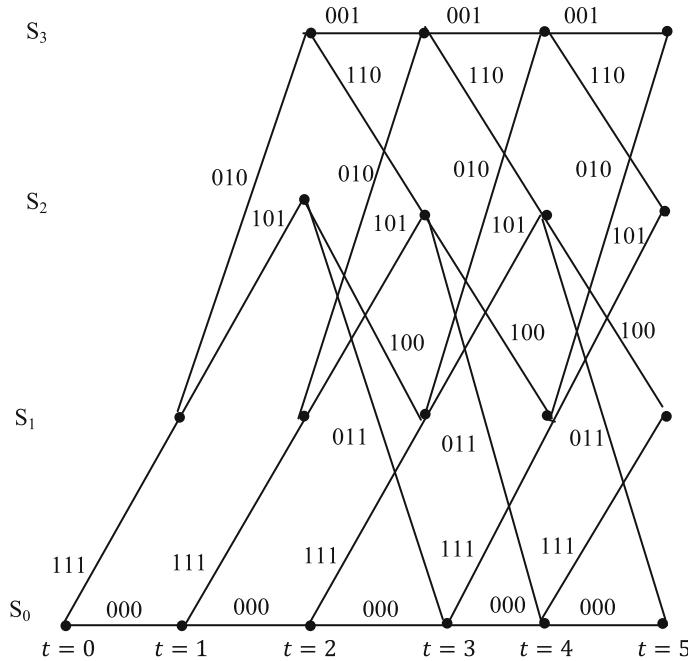
$M(r/y)$	$r = \underline{0}$	$r = 0$	$r = 1$	$\underline{1}$
$y = 0$	5	6	2	0
$y = 1$	0	2	6	5

Example 5.9 Consider the encoder shown in Fig. 5.1.

1. Construct the Trellis diagram for the length 3 input sequence.
2. If a code word from the encoder is transmitted over a BSC and that the received sequence is $r = (110, 110, 110, 111, 010)$, find the maximum likelihood code using Viterbi hard-decision decoding algorithm.

Solution

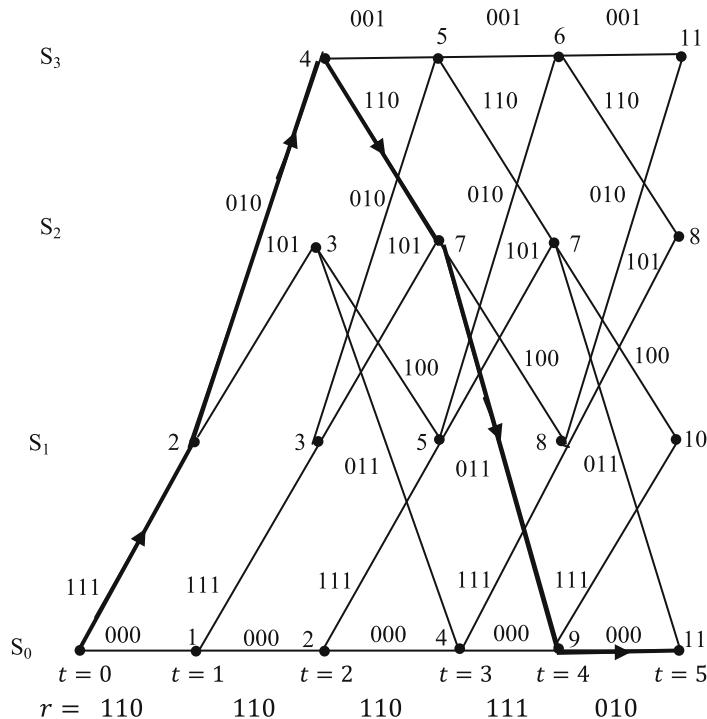
1. From the state diagram shown in Fig. 5.1, for the encoder of Fig. 5.1, the following trellis diagram is constructed.



2. For BSC, the bit metrics chosen for hard decision are as follows:

$M(r/y)$	$r = 0$	$r = 1$
$y = 0$	1	0
$y = 1$	0	1

Using the above bit metrics and following the Viterbi decoding algorithm procedure shown in Fig. 5.11, the results of the decoding operation using hard-decision decoding are shown in following figure.



In the above figure, the maximum likelihood code word is the word corresponding to the ML path denoted by thick line in the above trellis diagram. Thus, the maximum likelihood code word is given as follows:

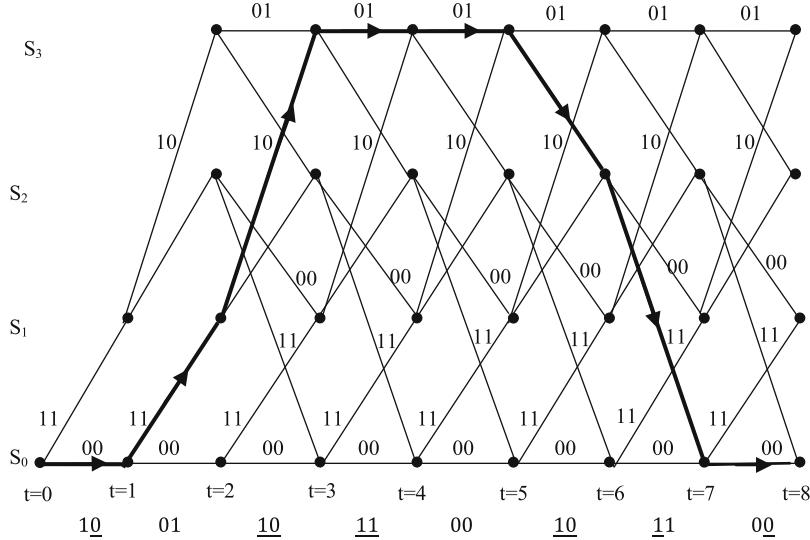
$$Y = (111, 010, 110, 011, 000)$$

Example 5.10 Considering the convolutional encoder of Example 5.5.

When the convolutional code is transmitted over a symmetric memoryless channel with the following bit metrics shown below in the table, find the transmitted code word for the following received code word \$(1\underline{0}, 01, \underline{10}, \underline{11}, 00, \underline{10}, \underline{11}, \underline{00})\$ using soft-decision decoding.

$M(r/y)$	$r = \underline{0}$	$r = 0$	$r = 1$	$r = \underline{1}$
$y = 0$	0	1	3	6
$y = 1$	6	3	1	0

Solution Using the above bit metrics and following the Viterbi decoding algorithm procedure shown in Fig. 5.11, the results of the decoding operation using soft-decision decoding are shown in the below figure.



In the above figure, the maximum likelihood code word is the word corresponding to the ML path denoted by thick line in the above trellis diagram. Thus, the maximum likelihood code word is $Y = (00, 11, 10, 01, 01, 10, 11, 00)$.

5.6 Performance Analysis of Convolutional Codes

5.6.1 Binary Symmetric Channel

The lower bound on the bit-error rate in the convolutional codes on the binary symmetric channel with a crossover probability P is given by [8]

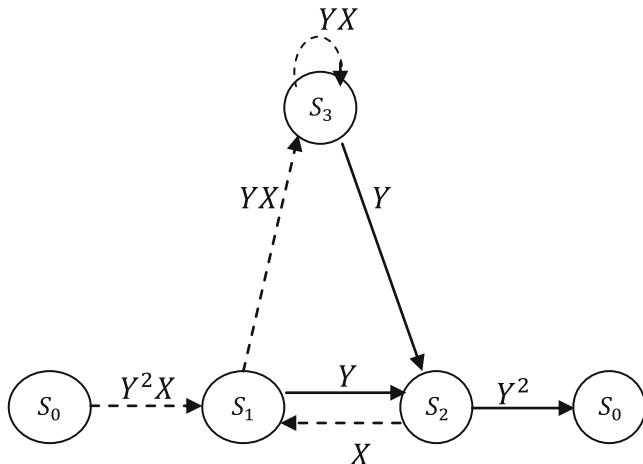
$$P_b = \begin{cases} \frac{1}{k} \sum_{k=(d_f+1)/2}^{d_f} \binom{d_f}{k} P^k (1-P)^{d_f-k} & d \text{ odd} \\ \frac{1}{2k} \binom{d_f}{d_f/2} P^{d_f/2} (1-P)^{d_f/2} + \frac{1}{k} \sum_{k=d_f/2+1}^{d_f} \binom{d_f}{k} P^k (1-P)^{d_f-k}, & d \text{ even} \end{cases} \quad (5.3)$$

whereas the upper bound on bit-error rate is given by [5]

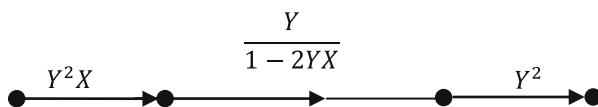
$$P_b < \frac{1}{k} \left. \frac{\partial T(Y, X)}{\partial X} \right|_{Y=2\sqrt{P(1-P)}, X=1} \quad (5.4)$$

Example 5.11 Consider the convolutional encoder from Example 5.6. Compute the upper bound and lower bound on BER for a binary symmetric channel with crossover probability $P = 0.01$.

Solution The signal flow graph of the encoder considered in Example 5.6 can be represented as follows:



By using reduction techniques, the signal flow graph can be simplified as follows:



The transfer function is given by

$$T(Y, X) = \frac{Y^5 X}{1 - 2YX}$$

$$\left. \frac{\partial T(Y, X)}{\partial X} \right|_{X=1} = \frac{Y^5}{(1 - 2Y)^2}$$

Upper bound on bit-error probability:

$$P < \left. \frac{1}{k} \frac{\partial T(X, Y)}{\partial y} \right|_{Y=2\sqrt{P(1-P)}, X=1} = \left. \frac{1}{k} \frac{Y^5}{(1 - 2Y)^2} \right|_{Y=2\sqrt{P(1-P)}},$$

Since $k = 1$ for this example

$$\begin{aligned} P_b &< \left. \frac{Y^5}{(1 - 2Y)^2} \right|_{Y=0.198997} \\ &= 8.61 \times 10^{-4} \end{aligned}$$

Lower bound on bit-error probability: $d_f = 5$

$$\begin{aligned} p_b &= \sum_{k=3}^5 (5_k) p^k (1-p)^{5-k} = 10p^3(1-p)^2 + 5p^4(1-p) + p^5 \\ &= 9.8501 \times 10^{-6} \end{aligned}$$

5.6.2 AWGN Channel

The upper and lower bounds on the bit-error rate at the output of the decoder in AWGN channel with BPSK for the unquantized soft decoding is given by

$$P_b \leq \frac{1}{k} e^{d_f E_b / N_0} Q \left(\sqrt{\frac{2 d_f R_c E_b}{N_0}} \right) \left. \frac{\partial T(Y, X)}{\partial X} \right|_{Y=e^{-E_b/N_0}, X=1} \quad (5.5)$$

Since the received signal is converted to a sequence of zeros and ones before it is sent to the decoder, for hard-decision decoding AWGN channel with BPSK modulation can be seen as BSC crossover probability p given by

$$P = Q \left(\sqrt{R_c \frac{2E_b}{N_0}} \right) \quad (5.6)$$

Substitution of the above P in Eq. (5.4) yields upper bound for the hard-decision decoding in AWGN channel with BPSK modulation.

The coding gain of a convolutional code over an uncoded BPSK or QPSK system is upper bounded by [7]

$$\text{Coding gain} = 10 \log_{10} \left(\frac{Rd_f}{2} \right) \text{dB for hard-decision} \quad (5.7a)$$

$$= 10 \log_{10}(Rd_f) \text{dB for soft-decision} \quad (5.7b)$$

Hence, the soft-decision decoding introduces 3 dB increases in the coding gain over the hard-decision decoding.

The BER performance of soft-decision and hard-decision decoding is compared through the following example.

Example 5.12 Consider the encoder used in the Example 5.10, and compare the BER performance of soft-decision and hard-decision decoding in an AWGN channel with BPSK modulation.

Solution The following MATLAB program is written and used for comparison of BER performance for different E_b/N_0 using soft-decision and hard-decision decoding. The comparison of BER performances with an encoder used in the Example 5.10 for hard-decision and soft-decision decoding over an AWGN channel is shown in Fig. 5.13

```
clear all; clc;
Eb_N0_dB = [4:12]; % multiple Eb/N0 values
EbN0Lin = 10.^((Eb_N0_dB/10));
d_free=5;
for i=1:length(Eb_N0_dB)
    p = 0.5* erfc ( sqrt(EbN0Lin(i)) );
    Ber_uncoded(i)=p;
    p = 0.5* erfc ( sqrt(0.5*EbN0Lin(i)) );
    y=2*sqrt(p*(1-p));
    Ber_Hd_Ub(i)=(y^5)/((1-2*y)^2);
    yy=exp(-EbN0Lin(i));
    yyy=(yy^5)/((1-2*yy)^2);
    Ber_Sd_Lb(i)=0.5*erfc(sqrt(d_free*0.5*EbN0Lin(i)));
    Ber_Sd_Ub(i)=Ber_Sd_Lb(i)*exp(d_free*EbN0Lin(i))*yyy;
end
semilogy(Eb_N0_dB,Ber_uncoded,'-'); grid on
hold on
semilogy(Eb_N0_dB,Ber_Sd_Ub,'-v');
semilogy(Eb_N0_dB,Ber_Hd_Ub,'-d');
legend('Uncoded','Soft decision Upper bound','Hard decision Upper bound ')
xlabel('Eb/No, dB');
ylabel('Bit Error Rate');
```

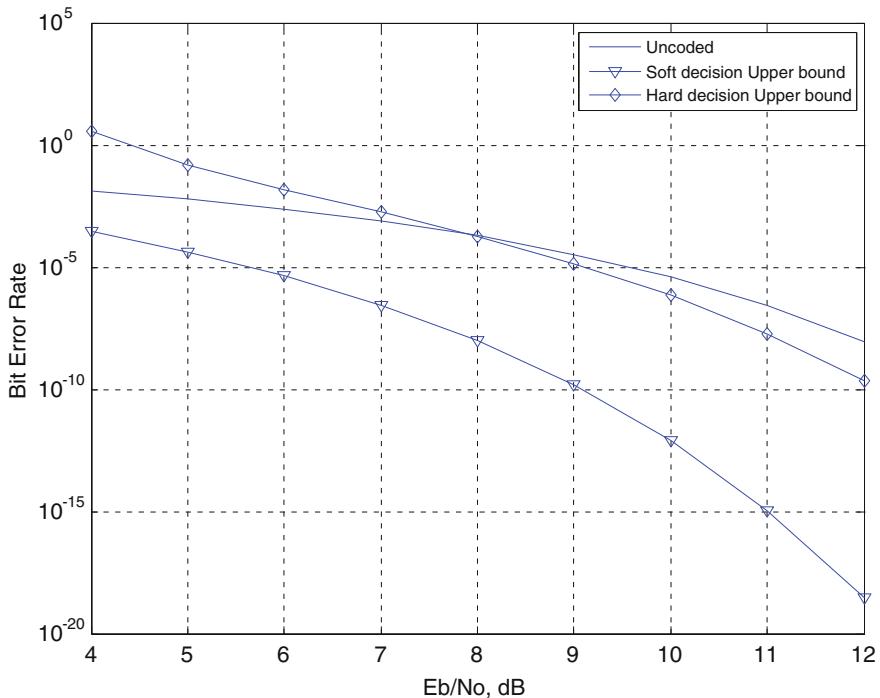


Fig. 5.13 BER performance comparisons of hard-decision and soft-decision decoding over an AWGN channel

From Fig. 5.13, it is observed that soft-decision decoding offers 3 dB increasing coding gain in over hard decision which satisfies the Eqs. (5.7a) and (5.7b).

5.6.3 Rayleigh Fading Channel

The union upper bound on the bit-error probability for better BER estimate for convolutional codes is given by [9]

$$P_b < \sum_{d=d_f}^{\infty} c_d P_d \quad (5.8)$$

where c_d is the information error weight for error events of distance d , and d_f is the free distance of the code. P_d is the pairwise error probability. For an AWGN channel, P_d is given by [9]

$$P_d = Q\left(\sqrt{2dR \frac{E_b}{N_0}}\right) \quad (5.9)$$

where R is the code rate, E_b is received energy per information bit, and N_0 is the double-sided power spectral density of the noise.

The pair wise error probability in a Rayleigh fading channel is given by [9]

$$P_d = (P_e)^d \sum_{k=0}^{d-1} \binom{d-1+k}{k} (1-P_e)^k \quad (5.10)$$

where $P_e = \frac{1}{2} \left(1 - \sqrt{\frac{\gamma_b R}{1+\gamma_b R}}\right)$ where γ_b is the average of $\frac{E_b}{N_0}$

A comparison of the upper bound on the BER in the AWGN and flat Rayleigh fading channels for ODS convolutional codes [9] with $R = 1/4$ and constraint length of seven is shown in Fig. 5.14.

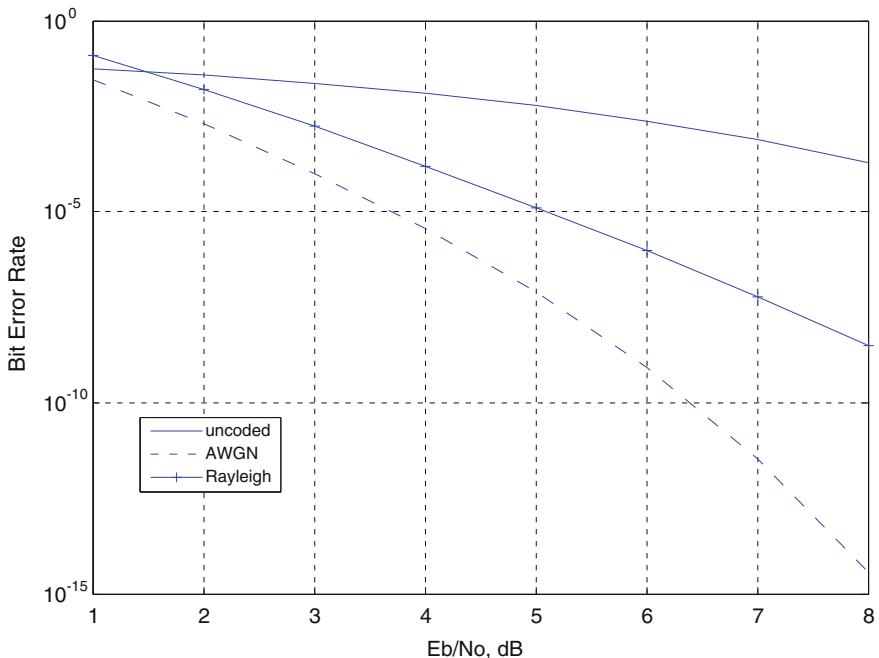


Fig. 5.14 A comparison of the upper bound on the BER in the AWGN and flat Rayleigh fading channels ODS convolutional codes with $R = 1/4$ and constraint length of 7

```

clear all;clic;
R=0.25;
pd2=[];
for i=1:8
    Eb_N0_dB=i;
    pb=0;pbr=0;
    d=20;
    for j=1:20
        cd=[];
        cd=[3;0;17;0;32;0;66;0;130;0;364;0;889;0;1975;0;5168;0;111
        13;0];
        EbNOLin=10.^{(Eb_N0_dB/10)};
        q1=sqrt((EbNOLin*R)/(1+(EbNOLin*R)));
        q=0.5*(1-q1);pd1=0;
        for k=0:(d-1)
            pd1=pd1+nchoosek((d-1+k),k)*((1-q)^k);
        end
        pd=(q^d)*pd1;
        pd1=0.5*erfc(sqrt(d*R*EbNOLin));
        pd2(j)=pd1; pdr(j)=pd;
        pb=pb+cd(j)*pd2(j);
        pbr=pbr+cd(j)*pdr(j);
        d=d+1;
    end
    berawg(i)=pb;
    barrayf(i)=pbr;
    p = 0.5* erfc ( sqrt(EbNOLin) );
    Ber_uncoded(i)=p;
end
semilogy(1:8,Ber_uncoded,'-'); grid on
hold on
semilogy(1:8,berawg,'--');
semilogy(1:8,barrayf,'-+');
legend('uncoded','AWGN','Rayleigh ')
xlabel('Eb/No, dB');ylabel('Bit Error Rate');

```

5.7 Problems

1. Consider the encoder shown in Fig. 5.15 and determine the output code word using D transform for the input sequence $x(n) = (1001)$.
2. Consider the encoder shown in Figure 5.15 and
 - i. Draw the state diagram for the encoder.
 - ii. Draw the trellis diagram for the encoder.
 - iii. Find the transfer function and the free distance of the encoder.

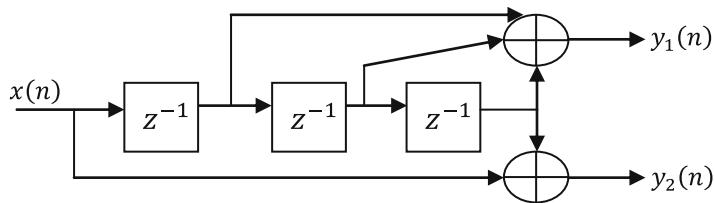


Fig. 5.15 A rate $-1/2$ convolutional encoder

3. Consider the encoder shown in Fig. 5.16

 - i. Find impulse response
 - ii. Find the transfer function matrix
 - iii. Use the transfer function matrix to determine the code word associated with the input sequence $x = (11, 10, 01)$

4. Consider an encoder with impulse responses $g_1 = (1111)$ and $g_2 = (1111)$. Determine whether the encoder generates a catastrophic convolutional code.
5. Construct a rate $\frac{3}{4}$ code by puncturing the output of the rate $1/3$, for systematic convolutional encoder shown in Fig. 5.2. And draw the trellis diagram of the punctured code.
6. If a code word from the encoder of Example 5.6 is transmitted over a BSC and that the received sequence is $r = (101, 100, 001, 011, 111, 101, 111, 110)$, find the maximum likelihood code using Viterbi hard-decision decoding algorithm.

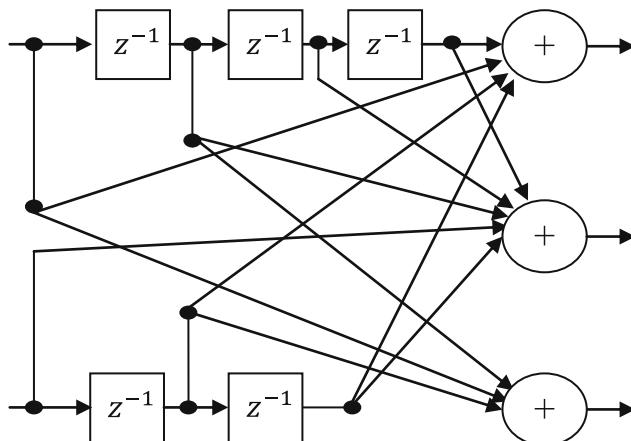


Fig. 5.16 A rate $-2/3$ convolutional encoder

7. If a code word from the encoder of Example 5.6 is transmitted over a BSC and that the received sequence is $r = (\underline{1}01, \underline{1}00, \underline{001}, 011, \underline{1}10, 110, \underline{111}, 1\underline{1}0)$, find the maximum likelihood code using Viterbi soft-decision decoding algorithm.

$M(r y)$	$r = \underline{0}$	$r = 0$	$r = 1$	$r = \underline{1}$
$y = 0$	5	4	2	0
$y = 1$	0	2	4	5

5.8 MATLAB Exercises

1. Write a MATLAB program to simulate BER performance of a convolutional encoder of your choice using hard-decision and soft-decision decoding over an AWGN channel and comment on the results.
2. Write a MATLAB program to simulate BER performance of a convolutional encoder of your choice using soft-decision decoding over an AWGN and Rayleigh Fading channel and comment on the results.

References

1. Massey, J.L., Sain, M.K.: Inverse of linear sequential circuits. *IEEE Trans. Comput.* **C-17**, 330–337 (1968)
2. Heller, J.A.: Short constraint length convolutional codes, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA Space Program Summary 37–54, Vol. 3, pp. 171–174, December (1968)
3. Costello, D.J.: Free distance bounds for convolutional codes. *IEEE Trans. Inf. Theory* **IT-20**(3), 356–365 (1974)
4. Forney Jr, G.D.: Convolutional codes II: maximum likelihood decoding. *Inf. Control* **25**, 222–266 (1974)
5. Cain, J., Clark, G., Geist, J.: Punctured convolutional codes of rate $(n-1)/n$ and simplified maximum likelihood decoding. *IEEE Trans. Inf. Theory* **IT-25**(1), 97–100 (1979)
6. Yasuda, Y., Kashiki, K., Hirata, Y.: High-rate punctured convolutional codes for soft decision Viterbi decoding. *IEEE Trans. Commun.* **3**, 315–319 (1984)
7. Hole, K.: New short constraint length rate $(N-1)/N$ punctured convolutional codes for soft decision Viterbi decoding. *IEEE Trans. Commun.* **9**, 1079–1081 (1988)
8. Wicker, S.B.: Error Control Systems for Digital Communication and Storage. Prentice Hall, New Jersey (1995)
9. Franger, P., Orten, P., Ottosson, T.: Convolutional codes with optimum distance spectrum. *IEEE Commun. Lett.* **3**(11), 317–319 (1999)

Chapter 6

Turbo Codes

The groundbreaking codes called turbo codes are introduced in [1, 2]. The best-known convolutional codes are mostly non-systematic. However, in turbo encoders, systematic convolutional codes are used. Turbo codes are generated by using the parallel concatenation of two recursive systematic convolutional (RSC) encoders. This chapter discusses turbo encoding, iterative turbo decoding, and performance analysis of turbo codes.

6.1 Non-recursive and Recursive Systematic Convolutional Encoders

A convolutional code is said to be systematic if the input sequence is reproduced unaltered in the output code word. The following rate-1/2 convolutional encoder is an example for a systematic convolutional encoder (Fig. 6.1).

6.1.1 Recursive Systematic Convolutional (RSC) Encoder

Consider the conventional convolutional encoder with rate 1/2 and constraint length 3 as shown in Fig. 6.2.

The generator sequences of the above non-recursive non-systematic encoder are $g_1 = [111]$ and $g_2 = [101]$.

The state diagram representation of the above non-recursive encoder is shown in Fig. 6.3.

Electronic supplementary material The online version of this chapter (doi:[10.1007/978-81-322-2292-7_6](https://doi.org/10.1007/978-81-322-2292-7_6)) contains supplementary material, which is available to authorized users.

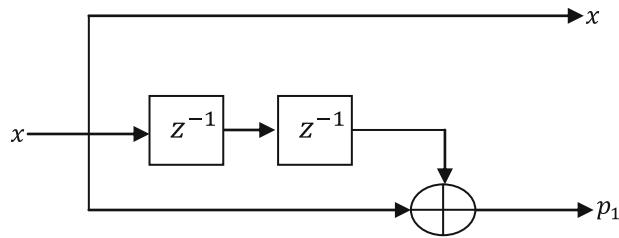


Fig. 6.1 Non-recursive systematic convolutional (SC) encoder

Fig. 6.2 Non-recursive non-systematic convolutional (NSC) encoder

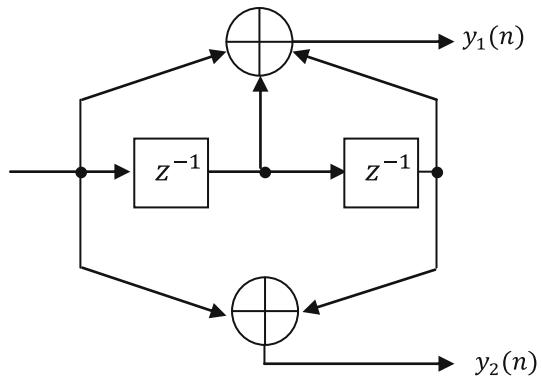
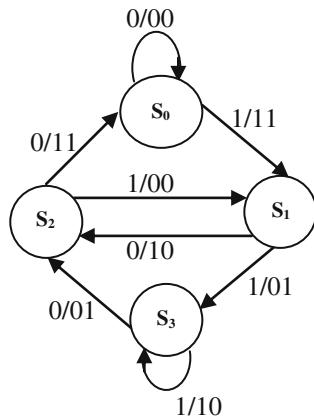


Fig. 6.3 NSC encoder state diagram



The equivalent RSC encoder of the non-recursive non-systematic encoder of Fig. 6.2 is shown in Fig. 6.4. It is obtained by feeding back the contents of the memory elements to the input with the generator function $G = \begin{bmatrix} 1 & g_2 \\ 1 & \frac{1+D^2}{1+D+D^2} \end{bmatrix}$.

The state diagram of the RSC encoder is shown in Fig. 6.5.

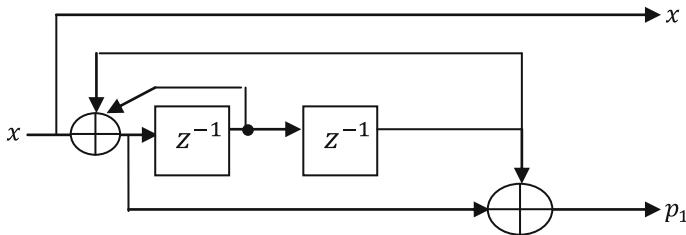
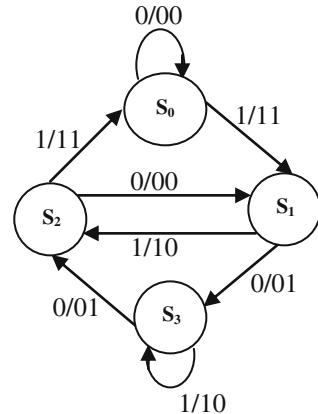


Fig. 6.4 Recursive systematic convolutional (RSC) encoder

Fig. 6.5 RSC encoder state diagram



From Figs. 6.3 and 6.5, it is clear that the state diagrams of the NSC and RSC encoders are very similar. Further, both the codes have the same minimum free distance and trellis structure. Hence, the first event error probability is same for both the codes; however, bit error rates (BERs) are different as BER depends on the encoder's input-output correspondence. At low signal-to-noise ratios E_b/N_o , the BER for a RSC code is lower than that of the corresponding NSC code.

6.2 Turbo Encoder

A turbo encoder structure consists of two identical RSC encoders in parallel concatenation as shown in Fig. 6.6. It is a rate 1/3 encoder.

The two RSC encoders work synergistically in parallel. The RSC encoder 1 takes the data bits x and produces a low-weight parity bits (p_{1k}) from them. The RSC encoder 2 gets the data bits x scrambled by an interleaver and computes high-weight parity bits (p_{2k}) from the scrambled input bits. Thus, moderate weight turbo

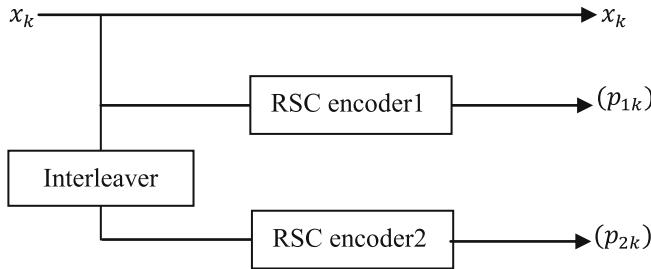


Fig. 6.6 Turbo encoder

code is generated with combined low-weight code from encoder 1 and high-weight code from encoder 2. Finally, the original input sequence x along with the two strings of parity bits is transmitted over the channel.

6.2.1 Different Types of Interleavers

The BER performance of turbo codes can be improved significantly by using interleaver as it affects the distance properties of the code by avoiding low-weight code words [3].

Block Interleaver

The block interleaver is one of the most frequently used types of interleavers in communication systems. It fills a matrix with the input data bit stream row-by-row and then sends out the contents column-by-column. A block interleaver is shown in Fig. 6.7. It writes in $[0\ 0 \dots 1\ 0\ 1 \dots 0 \dots 1 \dots 1\ 0\ 1 \dots 0\ 1]$ and reads out $[0\ 1 \dots 1\ 0\ 0 \dots 1 \dots 0\ 0\ 0 \dots 1\ 1]$.

Pseudo-random Interleaver

A random interleaver maps the input sequence according to the permutation order using a fixed random permutation. A random interleaver with input sequence of length 8 is shown in Fig. 6.8.

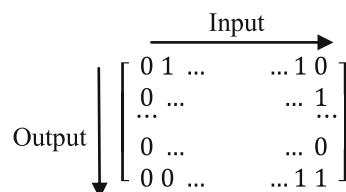


Fig. 6.7 Block interleaver

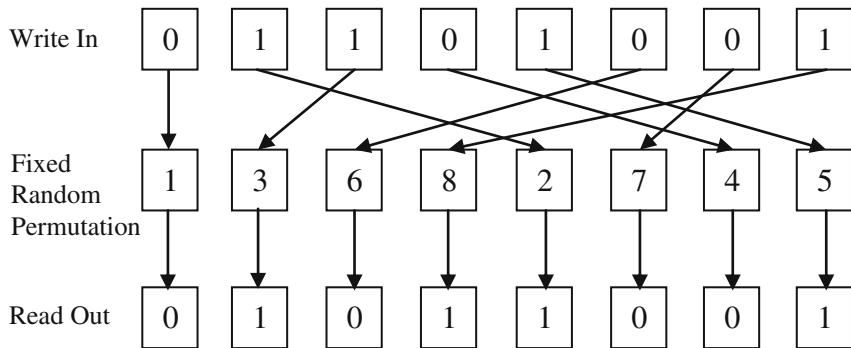


Fig. 6.8 Random interleaver

6.2.2 Turbo Coding Illustration

We consider the following numerical examples to illustrate turbo coding. The operation of the encoders used in these examples is characterized by the corresponding trellis diagram.

Example 6.1 For the turbo encoder shown in Fig. 6.9, find the output code word for the input data sequence $x = \{1\ 1\ 0\ 0\}$ assuming the RSC encoder 1 trellis is terminated. Let the interleaver be $\{5, 2, 4, 0, 1, 3\}$.

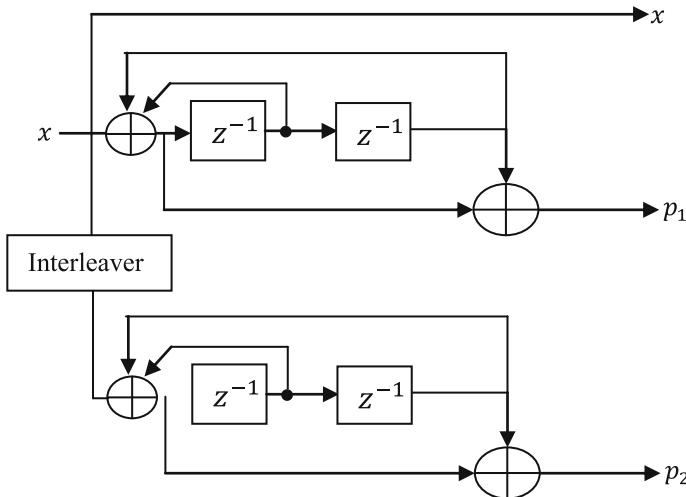


Fig. 6.9 Turbo encoder of Example 6.1

Table 6.1 Transitions for turbo encoder of Example 6.1

$x(n)$	State at n	State at $n + 1$	$P_1(n)$
0	S_0 (00)	S_0	0
1		S_1	1
0	S_1 (10)	S_3	1
1		S_2	0
0	S_2 (01)	S_1	0
1		S_0	1
0	S_3 (11)	S_2	1
1		S_3	0

Solution The two binary memory elements can assume any one of four states $S_0 - 00; S_1 - 10; S_2 - 01; S_3 - 11$ as shown in Table 6.1. The trellis diagram corresponding to Table 6.1 is shown in Fig. 6.10.

The input sequence is fed to the RSC encoder 1. The resultant path through the trellis is shown in Fig. 6.11.

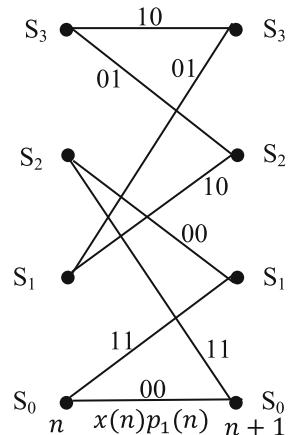
Now, the input is fed through the following pseudo-random interleaver shown in Fig. 6.12

The block of permuted data bits is then fed into RSC encoder 2 resulting in the path through the trellis is shown in Fig. 6.13.

The encoder output data bits and the parity bits are mapped to symbols as shown in 6.2.

Example 6.2 The UMTS (universal mobile telecommunications system) standard turbo encoder with RSC encoder generator function $G = \left[1 - \frac{1+D+D^3}{1+D^2+D^3} \right]$ is shown in Fig. 6.14, find the output code word for the input data sequence $x = \{1\ 1\ 0\ 0\}$ assuming RSC encoder 1 trellis is terminated. Let the interleaver be $\{2, 6, 4, 5, 0, 1, 3\}$.

Fig. 6.10 Trellis diagram for encoder of Example 6.1



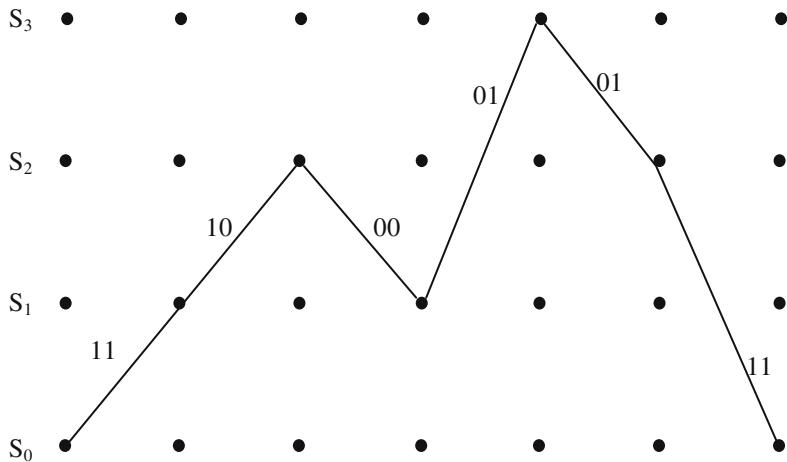


Fig. 6.11 Trellis path corresponding to input sequence of Example 6.1

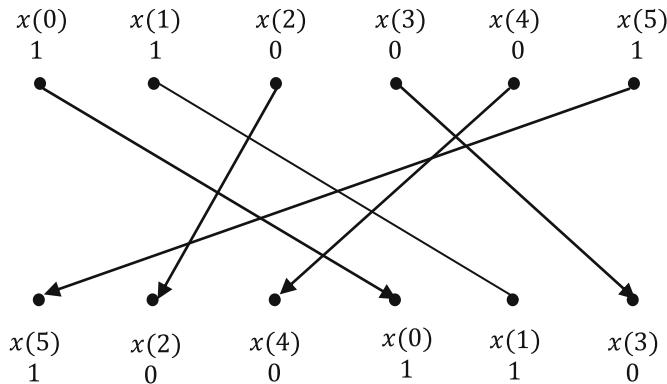


Fig. 6.12 Pseudo-random interleaver of Example 6.1

Solution The two binary memory elements can assume any one of four states $S_0 - 000$; $S_1 - 100$; $S_2 - 010$; $S_3 - 110$; $S_4 - 001$; $S_5 - 101$; $S_6 - 011$; $S_7 - 111$. as shown in Table 6.3. The trellis diagram corresponding to Table 6.3 is shown in Fig. 6.15.

The input sequence is fed to the RSC encoder 1. The resultant path through the trellis is shown in Fig. 6.16.

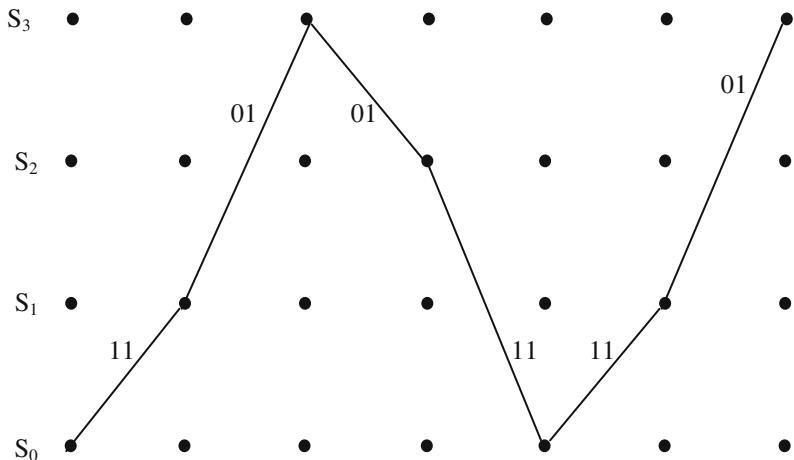


Fig. 6.13 Trellis path corresponding to interleaved input sequence of Example 6.1

Table 6.2 Output of encoder of Example 6.1

$x(n)$	$p_1(n)$	$p_2(n)$	→	$x(n)$	$p_1(n)$	$p_2(n)$
1	1	1		1	1	1
1	0	1		1	-1	1
0	0	1		-1	-1	1
0	1	1		-1	1	1
0	1	1		-1	1	1
1	1	1		1	1	1

Now, the input is fed through the following pseudo-random interleaver shown in Fig. 6.17.

The block of permuted data bits is then fed into RSC encoder 2 resulting in the path through the trellis is shown in Fig. 6.18.

The encoder output data bits and the parity bits are mapped to symbols as shown in 6.4.

6.2.3 Turbo Coding Using MATLAB

Example 6.3 Consider the turbo encoder given in [1] using the RSC encoders with the generator function.

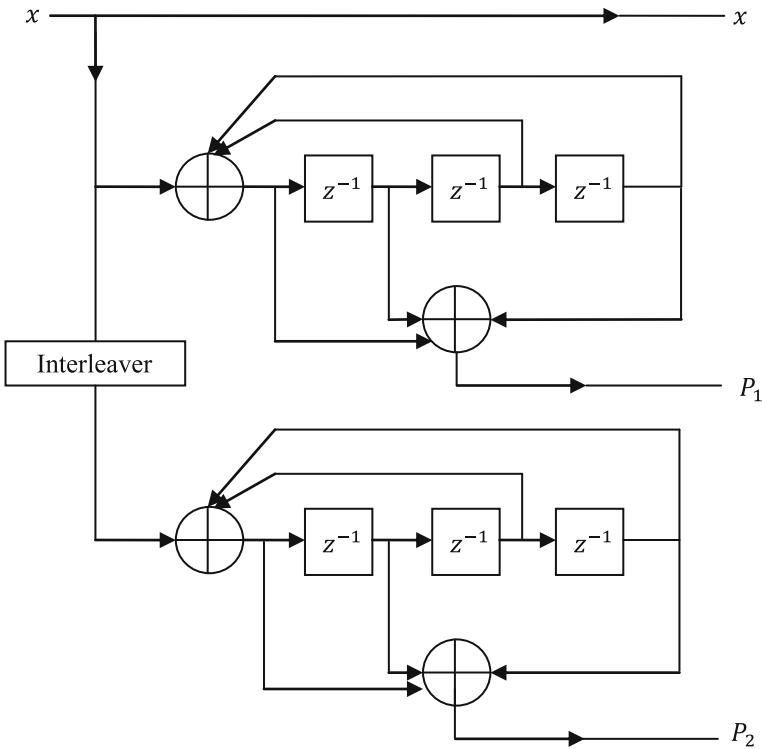
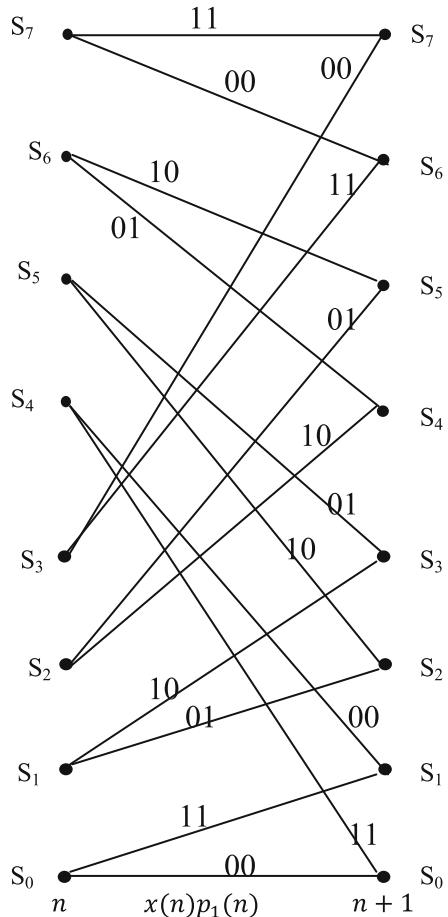


Fig. 6.14 Turbo encoder of Example 6.2

Table 6.3 Transitions for turbo encoder of Example 6.2

$x(n)$	State at n	State at $n + 1$	$P_1(n)$
0	$S_0 \text{ (000)}$	S_0	0
1		S_1	1
0	$S_1 \text{ (100)}$	S_2	1
1		S_3	0
0	$S_2 \text{ (010)}$	S_5	1
1		S_4	0
0	$S_3 \text{ (110)}$	S_7	0
1		S_6	1
0	$S_4 \text{ (001)}$	S_1	0
1		S_0	1
0	$S_5 \text{ (101)}$	S_3	1
1		S_2	0
0	$S_6 \text{ (011)}$	S_4	1
1		S_5	0
0	$S_7 \text{ (111)}$	S_6	0
1		S_7	1

Fig. 6.15 Trellis diagram for encoder of Example 6.2



$$G = \left[1 \quad \frac{1+D^4}{1+D+D^2+D^3+D^4} \right]$$

- (a) Assuming RSC encoder 1 trellis is terminated and determine the code word produced by the unpunctured encoder for the message $x = [1 \ 0 \ 0 \ 1 \ 1 \ 0]$ using MATLAB. Let the interleaver be $[3, 7, 6, 2, 5, 10, 1, 8, 9, 4]$.
- (b) Repeat (a) for punctured encoder with rate 1/2

The puncturing patterns are $P_{u1} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$; $P_{u2} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$.

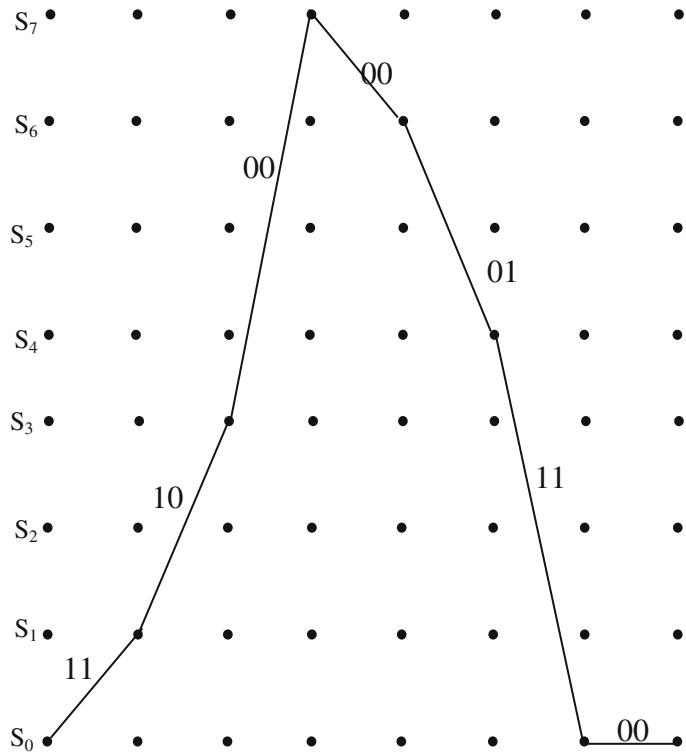


Fig. 6.16 Trellis path corresponding to input sequence of Example 6.2

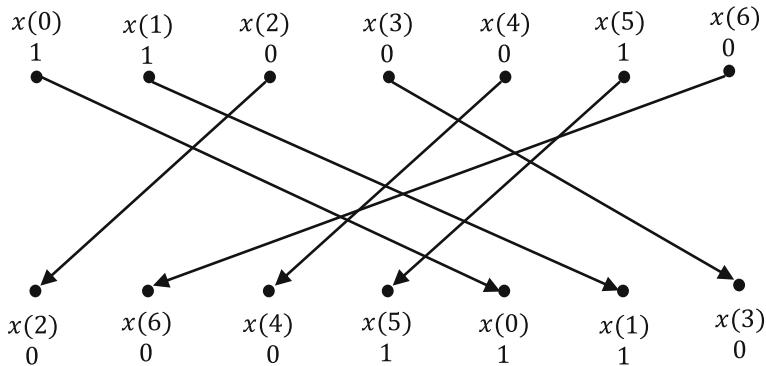


Fig. 6.17 Pseudo-random interleaver of Example 6.2

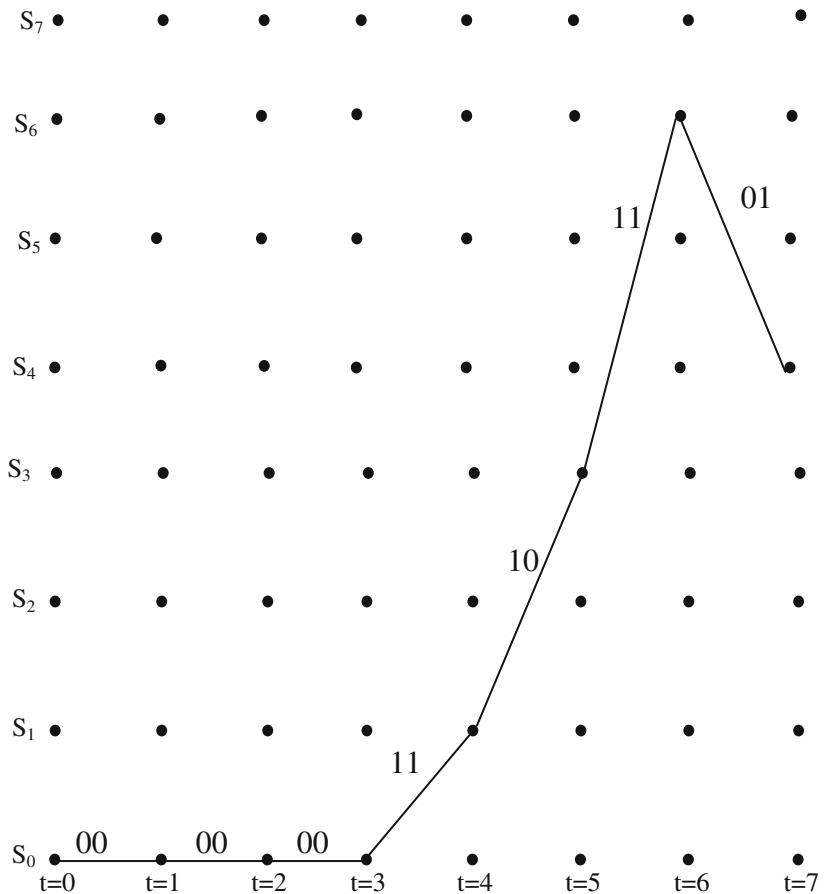


Fig. 6.18 Trellis path corresponding to interleaved input sequence of Example 6.2

Table 6.4 Output of the encoder of Example 6.2

$x(n)$	$p_1(n)$	$p_2(n)$	\longrightarrow	$x(n)$	$p_1(n)$	$p_2(n)$
1	1	0		1	1	-1
1	0	0		1	-1	-1
0	0	0		-1	-1	-1
0	0	1		-1	-1	1
0	1	0		-1	1	-1
1	1	1		1	1	1
0	0	1		-1	-1	1

- (c) Assuming RSC encoder 1 trellis is unterminated and determine the code word produced by the unpunctured encoder for the message $x = [1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0]$ using MATLAB. Let the interleaver be $[3, 7, 6, 2, 5, 10, 1, 8, 9, 4]$.
- (d) Repeat (c) for punctured encoder with rate 1/2 with the puncturing patterns same as in (b).

Solution The following MATLAB program and MATLAB functions are written and used to find the code words produced by the unpunctured and punctured encoders. For (a) and (b), the program is to be run with $ip = [1\ 0\ 0\ 1\ 1\ 0]$ and $term1 = 1$, whereas for (c) and (d), the program is to be run with $ip = [1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0]$ and $term1 = -1$.

- (a) The unpunctured turbo code obtained by running the MATLAB program and functions is

$$\begin{aligned}x &= [1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 0]; \\ p_1 &= [1\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 0]; \quad p_2 = [0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1]\end{aligned}$$

- (b) The punctured turbo code obtained is

$$x = [1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 0]; \quad p_1 = [1\ 0\ 1\ 0\ 0]; \quad p_2 = [1\ 0\ 0\ 1\ 1]$$

Since for every 10 information bits, there are 20 code word bits (10 information bits and five parity bits for each RSC encoder; thus, the rate of the punctured turbo code is 1/2).

- (c) The unpunctured turbo code obtained is

$$\begin{aligned}x &= [1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0]; \\ p_1 &= [1\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1]; \quad p_2 = [0\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 0]\end{aligned}$$

- (d) The punctured turbo code obtained is

$$x = [1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0]; \quad p_1 = [1\ 0\ 1\ 0\ 0]; \quad p_2 = [1\ 0\ 0\ 0\ 0]$$

Program 6.1 MATLAB program to find output code word

```
clear all;
g = [ 1 1 1 1 1;1 0 0 0 1];
ip =[1 0 0 1 1 0 ]; % info. bits
[n,K] = size(g);
m = K - 1;
term1=input('enter 1 terminated trellises, -1 for unterminated trellises');
term2=-1;
if(term1==1)
    L=length(ip)+m;
else
    L=length(ip);
end
op1 = turboencode(g, ip,term1);
y(1,:)= op1(1:2:2*L);
y(2,:)= op1(2:2:2*L);
interl=[3 7 6 2 5 10 1 8 9 4];
for i = 1:L
    ip1(1,i) = y(1,interl(i));% interleaved input
end
op2= turboencode(g, ip1,term2);
y(3,:)= op2(2:2:2*L);
punc=input('enter 1 for unpunctured code, 0 for punctured code');
if(punc==1)
x=y(1,:);p1=y(2,:);p2=y(3,:);
y=[x' p1' p2'];
y= 2*y-ones(size(y));
end
if(punc==0)
x=y(1,:);p1=y(2,1:2:end);p2=y(3,2:2:end);
y11=x';
y12=[p1' p2'];
y1p= 2*y11-ones(size(y11));
y23p=2*y12-ones(size(y12));
end
```

MATLAB function encodedbit.m

```
function [output, state] = encodedbit(g, input, state)
[n,k] = size(g);
m = k-1;
for i=1:n
    output(i) = g(i,1)*input;
    for j = 2:k
        output(i) = xor(output(i),g(i,j)*state(j-1));
    end;
end
state = [input, state(1:m-1)];
```

MATLAB function turboencode.m

```
function y = turboencode(g, ip, terminated)
[n,K] = size(g);
m = K - 1;
if terminated>0
    Linf = length(ip);
    L = Linf + m;
else
    L = length(ip);
    Linf = L - m;
end
% initialize the state vector
state = zeros(1,m);
% generate the codeword
for i = 1:L
    if terminated<0 | (terminated>0 & i<=Linf )
        xk = ip(1,i);
    elseif terminated>0 & i>Linf
        % terminate the trellis
        xk = rem( g(1,2:K)*state', 2 );
    end
    xak = rem( g(1,:)*[xk state]', 2 );
    [outputbits, state] = encodedbit(g, xak, state);
    outputbits(1,1) = xk;
    y(n*(i-1)+1:n*i) = outputbits;
end
```

6.3 Turbo Decoder

The iterative decoding turbo decoder block diagram is shown in Fig. 6.19.

During the first iteration, no extrinsic information is available from decoder 2, hence the a priori information is set to zero. Then, the decoder outputs the estimate of the systematic bit as the log-likelihood ratio (LLR)

$$L_1(\hat{x}(n)) = \left(\frac{P(x(n) = 1)|x', p'_1, L_a(\hat{x})}{P(x(n) = 0)|x', p'_1, L_a(\hat{x})} \right) \quad n = 1, 2, \dots, N \quad (6.1)$$

It is assumed that the message bits are statistically independent. Thus, the total LLR is given by

$$L_1(\hat{x}) = \sum_{n=1}^N L_1(\hat{x}(n)) \quad (6.2)$$

Hence, the message bits extrinsic information obtained from the first decoder is given as follows:

$$L_{e1}(x) = L_1(x) - L_a(x) - L_c x' \quad (6.3)$$

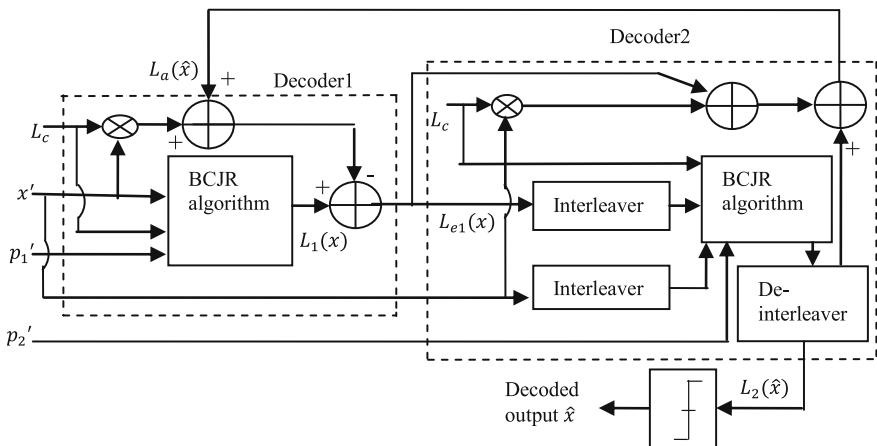


Fig. 6.19 The iterative decoding turbo decoder block diagram

The term $L_c x'$ is the information provided by the noisy observation. The extrinsic information $L_{e1}(x)$ and x' are interleaved before applying it as input to the BCJR algorithm in the second decoder. The noisy parity check bits p'_2 are also an additional input to the BCJR algorithm. The extrinsic information obtained from the BCJR algorithm is de-interleaved to produce the total log-likelihood ratio

$$L_2(x) = \sum_{n=1}^N \left(\frac{P(x(n) = 1) | x', p'_2, L_{e1}(x)}{P(x(n) = 0) | x', p'_2, L_{e1}(x)} \right) \quad (6.4)$$

is hard limited to estimating the information bit based only on the sign of the de-interleaved LLR, at the output of the decoder as expressed by

$$\hat{x} = \text{sgn}(L_2(x)) \quad (6.5)$$

The extrinsic information

$$L_a(x) = L_2(x) - (L_{e1}(x) + L_c x') \quad (6.6)$$

is fed back to the decoder 1. The extrinsic information of one decoder is used as the a priori input to the other decoder, and thus in the turbo decoder iterations, the extrinsic information ping-ponged back and forth between maximum a posteriori (MAP) decoders.

After a certain number of iterations, the log-likelihood $L_2(x)$ at the output of decoder 2 is de-interleaved and delivered to the hard decision device, which estimates the input.

If it is assumed that $x(n) = \pm 1$ is transmitted over a Gaussian or fading channel using BPSK modulation, the probability of the matched filter output $y(n)$ is given by Hanzo et al. [4]

$$P(y(n)|x(n) = +1) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{E_b}{2\sigma^2}(y(n) - a)^2\right) \quad (6.7a)$$

where E_b is the transmitted energy per bit, σ^2 is the noise variance, and a is the fading amplitude. Similarly,

$$P(y(n)|x(n) = -1) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{E_b}{2\sigma^2}(y(n) + a)^2\right) \quad (6.7b)$$

Therefore, when we use BPSK over a (possibly fading) Gaussian channel, the term $L_c x'(n)$ can be expressed as follows:

$$\begin{aligned}
 L_c(x'(n)|x(n)) &= \log \left(\frac{P(x'(n)|x(n) = +1)}{P(x'(n)|x(n) = -1)} \right) \\
 &= \log \left(\frac{\exp\left(-\frac{E_b}{2\sigma^2}(x'(n) - a)^2\right)}{\exp\left(-\frac{E_b}{2\sigma^2}(x'(n) + a)^2\right)} \right) \\
 &= \left(-\frac{E_b}{2\sigma^2} (x'(n) - a)^2 \right) - \left(-\frac{E_b}{2\sigma^2} (x'(n) + a)^2 \right) \\
 &= \frac{E_b}{2\sigma^2} 4a \cdot x'(n) \\
 &= L_c x'(n)
 \end{aligned} \tag{6.8}$$

where

$$L_c = 4a \frac{E_b}{2\sigma^2}$$

is defined as the channel reliability value.

6.3.1 The BCJR Algorithm

The BCJR algorithm was published in 1974. It is named after its inventors: Bahl, Cocke, Jelinek, and Raviv. It is for MAP decoding of codes defined on trellises [5]. It was not used in practical implementations for about 20 years due to more complexity than the Viterbi algorithm. The BCJR algorithm was reborn vigorously when the turbo code inventors Berrou et al. [1] used a modified version of the BCJR algorithm in 1993. Consider a trellis section with four states like the one presented in Fig. 6.20.

In the trellis section, the branches generated by input message bits 1 and -1 are represented by a dashed line and a solid line, respectively. The variable $\gamma(n)$ represents the branch probabilities at time n , and the variables $\alpha(n)$ and $\beta(n)$ are the forward and backward estimates of the state probabilities at time n based on the past and future data, respectively. Now the log-likelihood ratios expressed by Eqs. (6.2) and (6.4) can be computed, using branch probabilities, forward, and backward error probabilities of the states, as follows:

$$L_1(\hat{x}) = \log \left[\frac{\sum_{R_1} \alpha_{s'}(n-1) \cdot \gamma_{s',s}(n) \cdot \beta_s(n)}{\sum_{R_0} \alpha_{k-1}(s') \cdot \gamma_k(s',s) \cdot \beta_k(s)} \right] \tag{6.9}$$

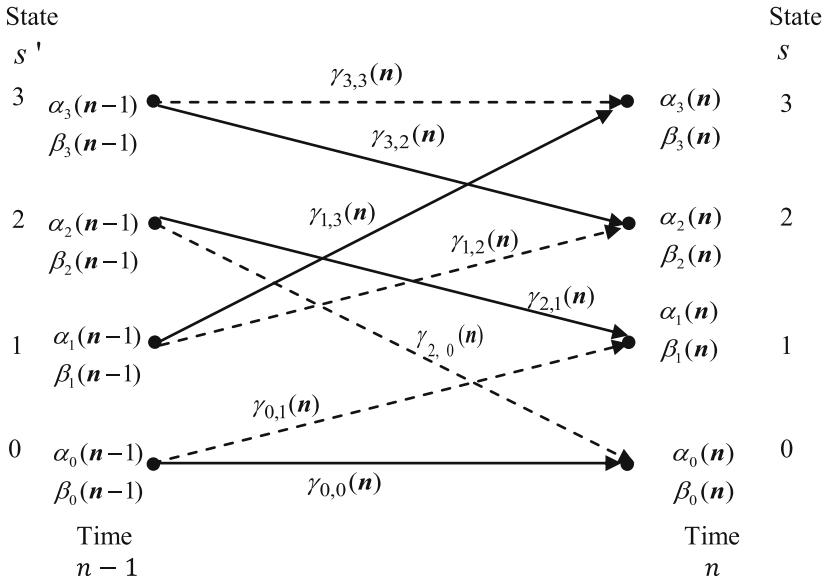


Fig. 6.20 Typical trellis section with α, β, γ as labels

where s represents the state at time n and s' stands for the previous state, i.e., the state at time instant $n - 1$ as in a typical trellis section shown in Fig. 6.20. The R_1 indicates the summation computed over all the state transitions from s' to s due to message bits $x(n) = +1$ (i.e., dashed branches). The denominator R_0 is the set of all branches originated by message bits $x(n) = -1$.

For a given state transition, the transmitted signal is the data bit and parity check bit pair. Also, for a given starting state, the data bit value determines the next state. Using the Bayes theorem, the branch probability can be expressed as [6]

$$\gamma_{s',s} = \Pr(x(n)) \Pr(y'(n)|y(n)) \quad (6.10)$$

The probability of the data bit $x(n)$ in terms of the a priori probability ratio can be written as follows:

$$\begin{aligned} \Pr(x(n)) &= \frac{\exp\left[\frac{1}{2}L_a(x(n))\right]}{1 + \exp[L_a(x(n))]} \cdot \exp\left[\frac{1}{2}x_k L_a(x(n))\right] \\ &= B_n \cdot \exp\left[\frac{1}{2}x(n)L_a(x(n))\right] \end{aligned} \quad (6.11)$$

$$L_a(x(n)) = \log \left[\frac{\Pr(x(n) = +1)}{\Pr(x(n) = -1)} \right] \quad (6.12)$$

The probability of the noisy data bit $x'(n)$ and parity bits $p'(n)$ can be expressed in terms of Gaussian probability distributions as follows:

$$\begin{aligned}\Pr(y'(n)|y(n)) &= \Pr(x'(n)|x(n)) \cdot \Pr(p'(n)|p(n)) \\ &= \frac{1}{\sqrt{2\pi\sigma^2}} \cdot \exp\left[\frac{-(x'(n) - x(n))^2}{2\sigma^2}\right] \cdot \Delta \\ &\quad \times \frac{1}{\sqrt{2\pi\sigma^2}} \cdot \exp\left[\frac{-(p'(n) - p(n))^2}{2\sigma^2}\right] \cdot \Delta \\ &= A_n \cdot \exp\left[\frac{x'(n)x(n) - p'(n)p(n)}{\sigma^2}\right]\end{aligned}\quad (6.13)$$

Since $\gamma_{s',s}$ appears in the numerator (where $x(n) = +1$) and denominator (where $x(n) = -1$) of Eq. (6.9), the A_nB_n factor will get canceled as it is independent of $x(n)$. Thus, the branch probability $\gamma_{s',s}(n)$ can be expressed as

$$\gamma_{s',s}(n) = \exp\left[\frac{1}{2}(x(n)L_a x(n) + x(n)L_c x'(n) + p(n)L_c p'(n))\right]\quad (6.14)$$

The forward recursion is computed as

$$\alpha_s(n) = \sum_{s'} \alpha_{s'}(n-1) \gamma_{s',s}(n)\quad (6.15)$$

The backward recursion is computed as

$$\beta_{s'}(n-1) = \sum_{s'} \gamma_{s',s}(n) \cdot \beta_s(n)\quad (6.16)$$

$$\alpha_0(n) = \alpha_0(n-1) \gamma_{0,0}(n) + \alpha_0(n-1) \gamma_{2,0}(n)\quad (6.17a)$$

$$\beta_0(n) = \beta_1(n+1) \gamma_{0,1}(n+1) + \beta_0(n+1) \gamma_{0,0}(n+1)\quad (6.17b)$$

The recursive calculation of $\alpha_0(n)$ and $\beta_0(n)$ as in Eqs. (6.17a) and (6.17b) is illustrated in Fig. 6.21.

The following simple example illustrates the recursive computation of forward and backward state error probabilities.

Example 6.4 Consider the following trellis diagram shown in Fig. 6.22 with the following probabilities.

$$\begin{aligned}\gamma_{00}(1) &= 0.48, & \gamma_{00}(2) &= 0.485, & \gamma_{00}(3) &= 0.6, \\ \gamma_{01}(1) &= 0.09, & \gamma_{01}(2) &= 0.1 \\ \gamma_{10}(2) &= 0.1, & \gamma_{10}(3) &= 0.7 & \gamma_{11}(2) &= 0.485\end{aligned}$$

Compute the forward and backward state error probabilities of the trellis.

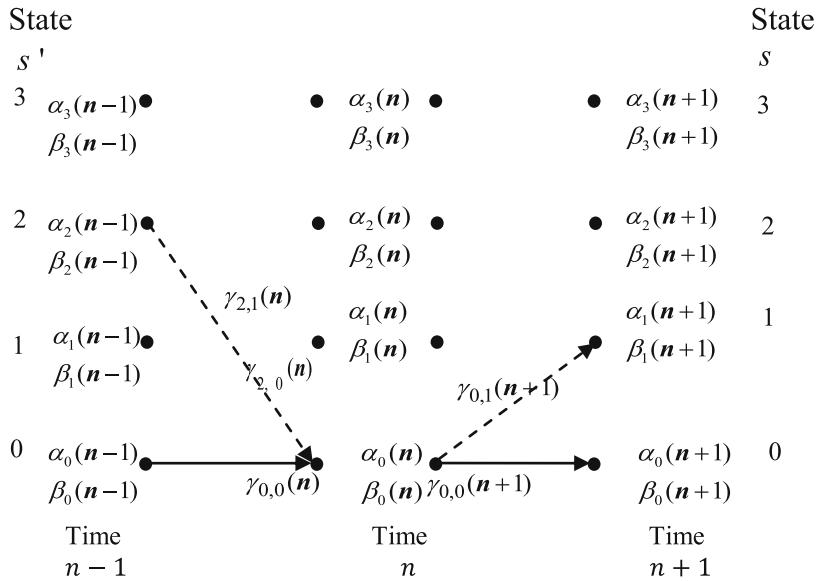


Fig. 6.21 Illustration of recursive calculation of $\alpha_0(n)$ and $\beta_0(n)$

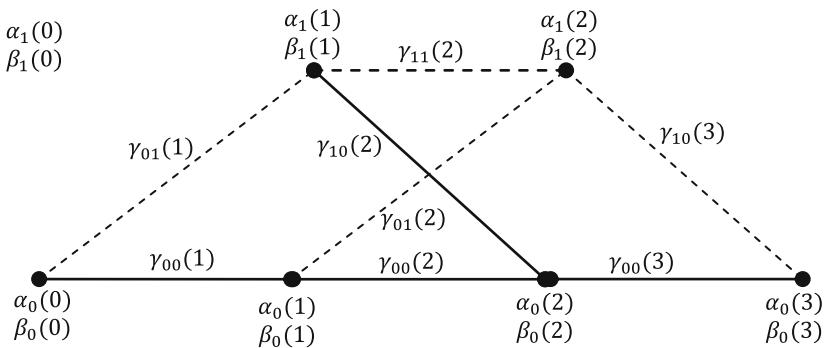


Fig. 6.22 Trellis diagram of Example 6.4

Solution With the initial value $\alpha_0(0) = 1$, the forward recursion yields the values

$$\begin{aligned}\alpha_0(1) &= \alpha_0(0)\gamma_{00}(1) = 0.48 \\ \alpha_1(1) &= \alpha_0(0)\gamma_{01}(1) = 0.09 \\ \alpha_0(2) &= \alpha_0(1)\gamma_{00}(2) + \alpha_1(1)\gamma_{10}(2) = 0.2418 \\ \alpha_1(2) &= \alpha_0(1)\gamma_{01}(2) + \alpha_1(1)\gamma_{11}(2) = 0.0916 \\ \alpha_0(3) &= \alpha_0(2)\gamma_{00}(3) + \alpha_1(2)\gamma_{10}(3) = 0.2092\end{aligned}$$

With the initial value $\beta_0(3) = 1$, the backward recursion yields the values

$$\begin{aligned}\beta_0(2) &= \beta_0(3)\gamma_{00}(3) = 0.6 \\ \beta_1(2) &= \beta_0(3)\gamma_{10}(3) = 0.7 \\ \beta_0(1) &= \beta_0(2)\gamma_{00}(2) + \beta_1(2)\gamma_{01}(2) = 0.3510 \\ \beta_1(1) &= \beta_0(2)\gamma_{10}(2) + \beta_1(2)\gamma_{11}(2) = 0.3995 \\ \beta_0(0) &= \beta_0(1)\gamma_{00}(1) + \beta_1(1)\gamma_{01}(1) = 0.2044\end{aligned}$$

6.3.2 Turbo Decoding Illustration

Example 6.5 Assume the channel adds unity variance Gaussian noise to the code generated by the turbo encoder considered in Example 6.1, decode the received sequence.

Solution For a random run with unity variance Gaussian noise, the received code is given as follows:

$x'(n)$	$p'_1(n)$	$p'_2(n)$
0.9039	0.1635	1.2959
-0.3429	-0.2821	2.6317
-1.6952	-0.1377	2.2603
-2.6017	-0.4482	1.5740
-1.4019	1.6934	1.8197
1.7155	2.2967	1.6719

Using the trellis diagram shown in Fig. 6.1, the branch probabilities for the first stage are computed as

$$\begin{aligned}\gamma_{0,0}(1) &= \exp(-x'(0) - p'_1(0)) = \exp(-0.9039 - 0.1635) = 0.34390149993822 \\ \gamma_{0,1}(1) &= \exp(x'(0) + p'_1(0)) = \exp(0.9039 + 0.1635) = 2.90780935872520 \\ \gamma_{1,2}(1) &= \exp(x'(0) - p'_1(0)) = \exp(0.9039 - 0.1635) = 2.09677405639736 \\ \gamma_{1,3}(1) &= \exp(-x'(0) + p'_1(0)) = \exp(-0.9039 + 0.1635) = 0.47692310811885 \\ \gamma_{2,0}(1) &= \exp(x'(0) + p'_1(0)) = \exp(0.9039 + 0.1635) = 2.90780935872520 \\ \gamma_{2,1}(1) &= \exp(-x'(0) - p'_1(0)) = \exp(-0.9039 - 0.1635) = 0.34390149993822 \\ \gamma_{3,2}(1) &= \exp(-x'(0) + p'_1(0)) = \exp(-0.9039 + 0.1635) = 0.47692310811885 \\ \gamma_{3,3}(1) &= \exp(x'(0) - p'_1(0)) = \exp(0.9039 - 0.1635) = 2.09677405639736\end{aligned}$$

Repeating the branch probabilities computation for other stages of the trellis, the branch probabilities for all stages of the trellis for this example are given as follows:

n	$\gamma_{0,0}(n)/\gamma_{2,1}(n)$	$\gamma_{0,1}(n)/\gamma_{2,0}(n)$	$\gamma_{1,2}(n)/\gamma_{3,3}(n)$	$\gamma_{1,3}(n)/\gamma_{3,2}(n)$
1	0.34390149993822	2.90780935872520	2.09677405639736	0.47692310811885
2	1.86824595743222	0.53526142851899	0.94101142324168	1.06268635566092
3	6.25199116868593	0.15994904231610	0.21066206860156	4.74693905095638
4	21.11323299367156	0.04736366052038	0.11607717585511	8.61495804522538
5	0.74714201360297	1.33843363349046	0.04526143199369	22.0938657031320
6	0.01809354561793	55.26832723205136	0.55922689149115	1.78818296332918

The forward state probabilities are computed using Eq. (6.15), and the resulting normalized forward state probabilities are given as follows:

n	$\alpha_0(n)$	$\alpha_1(n)$	$\alpha_2(n)$	$\alpha_3(n)$
0	1.000000000000000	0	0	0
1	0.10576017207126	0.89423982792874	0	0
2	0.09657271753492	0.02766854681958	0.41128905912021	0.46446967652529
3	0.11754442548550	0.45413087700815	0.38808965080132	0.04023504670503
4	0.16649906702111	0.54604949205154	0.02659440531342	0.26085703561394
5	0.00875863686136	0.01328728572633	0.31685999430997	0.66109408310235
6	0.89416277694224	0.02500892891120	0.06073869015360	0.02008960399296

The backward state probabilities are computed using Eq. (6.16), the resulting normalized backward probabilities for this example are given as follows:

n	$\beta_0(n)$	$\beta_1(n)$	$\beta_2(n)$	$\beta_3(n)$
6	0.45530056303648	0.09512620145755	0.07905302691388	0.37052020859209
5	0.02546276878415	0.09512620145755	0.01580448043695	0.50822864080378
4	0.02462941844490	0.01001105352469	0.96125810870846	0.00410141932195
3	0.00003769540412	0.98178511456649	0.00492923752535	0.01324795250404
2	0.00001104782103	0.00204434600799	0.00001979111732	0.99792481505365
1	0.00032726925280	0	0.99967273074720	0
0	1.000000000000000	0	0	0

Now, using Eq. (6.9), we compute the $L_1(x)$ the LLR from the decoder 1 as follows:

$$\begin{aligned} L_1(x(n)) \\ = \frac{\alpha_0(n-1)\beta_1(n)\gamma_{0,1}(n) + \alpha_1(n-1)\beta_2(n)\gamma_{1,2}(n) + \alpha_1(n-1)\beta_0(n)\gamma_{2,0}(n) + \alpha_1(n-1)\beta_3(n)\gamma_{3,3}(n)}{\alpha_0(n-1)\beta_0(n)\gamma_{0,0}(n) + \alpha_1(n-1)\beta_3(n)\gamma_{1,3}(n) + \alpha_1(n-1)\beta_1(n)\gamma_{2,1}(n) + \alpha_1(n-1)\beta_2(n)\gamma_{3,2}(n)} \end{aligned} \quad (6.18)$$

The resulting LLR from the decoder 1 is

$$L_1(x) = \begin{bmatrix} 5.00794986257243 \\ 4.52571043846903 \\ -5.03587871714769 \\ -6.73223129201010 \\ -5.45139857004191 \\ 11.61281973458293 \end{bmatrix} \quad \text{and} \quad L_c(x) = \begin{bmatrix} 1.807800000000000 \\ -0.685800000000000 \\ -3.390400000000000 \\ -5.203400000000000 \\ -2.803800000000000 \\ 3.431000000000000 \end{bmatrix}$$

The soft and hard decisions are given as:

$L_1(\hat{x}(n))$	$\hat{x}(n) = \text{sign}(L_1(\hat{x}(n)))$
5.0079	1
4.5257	1
-5.035	0
-6.732	0
-5.451	0
11.61	1

When compared to the trellis path of decoder 1 shown in Fig. 6.11, it is observed that the decoder has correctly estimated all data bits. Since a priori information for the first iteration is zero, the extrinsic information $L_{e1}(x)$ is given as

$$L_{e1}(x) = L_1(x) - L_c(x)$$

$$= \begin{bmatrix} 5.00794986257243 \\ 4.52571043846903 \\ -5.03587871714769 \\ -6.73223129201010 \\ -5.45139857004191 \\ 11.61281973458293 \end{bmatrix} - \begin{bmatrix} 1.8078 \\ -0.6858 \\ -3.3904 \\ -5.2034 \\ -2.8038 \\ 3.4310 \end{bmatrix} = \begin{bmatrix} 3.20014986257242 \\ 5.21151043846903 \\ -1.64547871714763 \\ -1.52883129201010 \\ -2.64759857004191 \\ 8.18181973458293 \end{bmatrix}$$

The extrinsic information $L_{e1}(x)$ from the decoder 1 and the noisy information bits $x'(n)$ are to be interleaved before feeding as inputs to the BCJR algorithm of the decoder 2. After relabeling, the following are the inputs to BCJR of the decoder 2.

$L_{e1}(x)$	$x'(n)$	$p'_2(n)$
8.18181973458293	1.7155	1.2959
-1.64547871714769	-1.6952	2.6317
-2.64759857004191	-1.4019	2.2603
3.20014986257242	0.9039	1.574
5.21151043846903	-0.3429	1.8197
-1.52883129201010	-2.6017	1.6719

Using the trellis diagram shown in Fig. 6.1, the branch probabilities for the first stage are computed as

$$\gamma_{0,0}(1) = \exp(-0.5 * L_{e1}(x) - x'(0) - p'_1(01))$$

$$= \exp(-0.5 * 8.18181973458293 - 1.7155 - 1.2959)$$

$$= 0.00082320123987$$

$$\gamma_{0,1}(1) = \exp(0.5 * L_{e1}(x) + x'(0) + p'_1(01))$$

$$= \exp(0.5 * 8.18181973458293 + 1.7155 + 1.2959)$$

$$= 1214.7697933.438$$

$$\gamma_{1,2}(1) = \exp(0.5 * L_{e1}(x) + x'(0) - p'_1(01))$$

$$= \exp(0.5 * 8.18181973458293 + 1.7155 - 1.2959)$$

$$= 90.9681883921071$$

$$\begin{aligned}\gamma_{1,3}(1) &= \exp(-0.5 * L_{e1}(x) - x'(0) + p'_1(01)) \\ &= \exp(-0.5 * 8.1818197345829 - 1.7155 + 1.2959) \\ &= 0.01099285385007\end{aligned}$$

$$\begin{aligned}\gamma_{2,0}(1) &= \exp(0.5 * L_{e1}(x) + x'(0) + p'_1(01)) \\ &= \exp(0.5 * 8.18181973458293 + 1.7155 + 1.2959) \\ &= 1214.7697933.438\end{aligned}$$

$$\begin{aligned}\gamma_{2,1}(1) &= \exp(-0.5 * L_{e1}(x) - x'(0) - p'_1(01)) \\ &= \exp(-0.5 * 8.18181973458293 - 1.7155 - 1.2959) \\ &= 0.00082320123987\end{aligned}$$

$$\begin{aligned}\gamma_{3,2}(1) &= \exp(-0.5 * L_{e1}(x) - x'(0) + p'_1(01)) \\ &= \exp(-0.5 * 8.1818197345829 - 1.7155 + 1.2959) \\ &= 0.01099285385007\end{aligned}$$

$$\begin{aligned}\gamma_{3,3}(1) &= \exp(0.5 * L_{e1}(x) + x'(0) - p'_1(01)) \\ &= \exp(0.5 * 8.18181973458293 + 1.7155 - 1.2959) \\ &= 90.9681883921071\end{aligned}$$

Repeating the branch probabilities computation for other stages of the trellis, the branch probabilities for all stages of the trellis for this example are given as follows:

n	$\gamma_{0,0}(n)/\gamma_{2,1}(n)$	$\gamma_{0,1}(n)/\gamma_{2,0}(n)$	$\gamma_{1,2}(n)/\gamma_{3,3}(n)$	$\gamma_{1,3}(n)/\gamma_{3,2}(n)$
1	0.00082320123987	1214.76979330438	90.96818839210695	0.010992853850
2	0.89247155103612	1.12048389536	0.00580149660962	172.369315590337
3	1.59264998322900	0.62788435032	0.00683294655359	146.349747090304
4	0.01694173912378	59.02581740243	2.53444564152908	0.394563601450
5	0.01686431851993	59.29679274132	1.55761408724524	0.642007547433
6	5.44237554167172	0.18374329231	0.00648660728077	154.163795758670

The forward recursion can be calculated using Eq. (6.15). The resulting normalized values are as follows:

n	$\alpha_0(n)$	$\alpha_1(n)$	$\alpha_2(n)$	$\alpha_3(n)$
0	1.000000000000000	0	0	0
1	0.00000067765982	0.99999932234018	0	0
2	0.0000000350858	0.0000000440497	0.00003365622987	0.99996633585658
3	0.00000014443156	0.00000036627375	0.99995279793500	0.00004669135969
4	0.99971058159622	0.00028708385150	0.00000032776038	0.00000200679189
5	0.00028464899198	0.99970462721982	0.00000756282988	0.00000316095832
6	0.00001006025926	0.00000060639718	0.00004523543737	0.99994409790619

The backward recursion can be calculated according to Eq. (6.16). The resulting normalized values are as follows:

n	$\beta_0(n)$	$\beta_1(n)$	$\beta_2(n)$	$\beta_3(n)$
6	0.99998080264562	0.00000062587196	0.00001074035175	0.00000783113066
5	0.00001006166024	0.99987703069337	0.00000834425763	0.00010456338877
4	0.00013868974158	0.00143501008710	0.00007080225952	0.99835549791180
3	0.01189148350941	0.00173100215279	0.98500767914419	0.00136983519361
2	0.93003760467044	0.01096095473547	0.03420391063551	0.02479752995857
1	0.01760402234259	0.48239597765741	0.01760402234259	0.48239597765741
0	0.250000000000000	0.250000000000000	0.250000000000000	0.250000000000000

Now, we compute the LLR from the decoder 2 using Eq. (6.18). The resulting LLR from the decoder 2 is

$$L_2(x) = \begin{bmatrix} 25.71127513129983 \\ -19.85060333367479 \\ -16.52345972282743 \\ 12.59341638166602 \\ 11.21364990579842 \\ -10.0677959239041 \end{bmatrix}$$

By slicing the soft decisions, we get the hard decisions 1 0 0 1 1 0. Comparing this with the encoder 2 trellis path in Fig. 6.13, it is observed that the decoder has correctly estimated all data bits.

6.3.2.1 Turbo Decoding Using MATLAB

The following example illustrates the turbo decoding using MATLAB.

Example 6.6 When the code generated by the turbo encoder shown in Fig. 6.9 is transmitted over an AWGN channel with channel reliability factor $L_2 = 2$, sequence is received. Then, decode the received sequence using MATLAB.

n	$x'(n)$	$p'_1(n)$	$p'_2(n)$
1	3.01	3.13	-1.7
2	-0.23	-1.45	-1.7
3	-0.25	-0.18	1.82
4	0.83	0.91	2.0
5	-0.26	-0.45	-3.0
6	-0.8	1.3	1.46
7	0.43	1.98	2.1
8	-0.74	-0.54	0.3

Solution The following MATLAB program and MATLAB functions are written and used to decode the received sequence. After the first iteration, the received sequence becomes as follows:

$L_1(\hat{x}(n))$	$\hat{x}(n) = \text{sign}(L_1(\hat{x}(n)))$	$L_1(\hat{x}(n))$	$\hat{x}(n) = \text{sign}(L_1(\hat{x}(n)))$
11.3900	1	11.9775	1
3.7217	1	7.1019	1
0.3753	1	-5.1767	0
0.4850	1	-4.5544	0
0.4167	0	4.8071	1
-4.4225	0	-11.0942	0
3.7418	1	5.7408	1
-3.8245	0	-11.3693	0

After the second iteration, the received sequence becomes as follows:

$L_1(\hat{x}(n))$	$\hat{x}(n) = \text{sign}(L_1(\hat{x}(n)))$	$L_1(\hat{x}(n))$	$\hat{x}(n) = \text{sign}(L_1(\hat{x}(n)))$
20.9509	1	20.9633	1
13.5723	1	28.2036	1
15.2116	0	-23.1493	0
-14.6617	0	-17.3413	0
13.4480	1	21.2953	1
-19.1687	1	-30.6052	0
15.5069	0	18.3074	1
-21.0533	1	-33.4231	0

Thus the transmitted input sequence $x(n) = (1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0)$.

Program 6.2 MATLAB program to decode the received sequence of Example 6.6

```

clear all;
g = [ 1 1 1;
      1 0 1 ];
[n,K] = size(g);
m = K - 1;
[n,K] = size(g);
% number of memories
m = K-1;
% number of states
nstates=2^m;
length=8;
r=[ 3.01      3.13      -1.7
    -0.23     -1.45      -1.7
    -0.25     -0.18      1.82
    0.83      0.91      2.0
    -0.26     -0.45      -3.0
    -0.8       1.3       1.46
    0.43      1.98      2.1
    -0.74     -0.54      0.3];
decin=[r(:,1)'; r(:,2)'; r(:,3)'];
xdec1=decin(1,:);
p1=decin(2,:);
interl =[ 8 6 2 3 5 4 7 1];
xdec2=xdec1(1,interl);
p2=decin(3,:);
La1=zeros(length,1);
for i=1:2
[L1 Le1] = turbodec(g, xdec1,p1,2, length,La1,nstates,1);
La2=Le1(interl');
[L2 Le2] = turbodec(g, xdec2,p2,2, length, La2, nstates,2);
deinterl=[8   3   4   6   5   2   7   1];
La1=Le2(deinterl');
L2=L2( deinterl');
end

```

MATLAB function trellis.m

```

function [trellismat, paritymat] = trellis(g);
[n,K] = size(g);
m = K - 1;
nstates = 2^m;
trellismat= zeros(nstates);
paritymat= zeros(nstates);
for s=1: nstates
decs=s-1; i=1;
% decimal to binary state
while decs >=0 & i<=m
    bins(i) = rem( decs,2 );
    decs = (decs- bins(i))/2;
    i=i+1;
end
bins=bins(m:-1:1);
% next state when input is 0
a = rem( g(1,:)*[0 bins ]', 2 );
v = g(2,1)*a;
for j = 1:K-1
    v = xor(v, g(2,j+1)*bins(j));
end;
nstate0 = [a bins(1:m-1)];
% binary to decimal state
d=2.^((m-1):-1:0);
j=nstate0*d'+1;
trellismat(s,j)= -1;
paritymat(s,j)= 2*v-1;
% next state when input is 1
a = rem( g(1,:)*[1 bins]', 2 );
v = g(2,1)*a;
for j = 1:K-1
    v = xor(v, g(2,j+1)*bins(j));
end;
nstate1 = [a bins(1:m-1)];
d=2.^((m-1):-1:0);
j=nstate1*d'+1;
trellismat(s,j)= 1;
paritymat(s,j)= 2*v-1;
end

```

MATLAB function turbodec.m

```
function [LMAP LE] = turbodec(g, x,p,Lc, bs, La,nst,ind)
[trellismat, paritymat]= trellis(g);
LMAP=zeros(bs,1);
LE=zeros(bs,1);
%Initialization Decoder
alpha= zeros(nst,bs+1);
alpha(1,1)=1;
beta= zeros(nst,bs+1);
if (ind==1)
beta(1,end)=1;
elseif(ind==2)
beta(:,end)=1/(nst)*ones(nst,1);
end
gamma(1,1:bs)= struct('gammamat',zeros(size(trellismat)));
for k=1:bs
    gamma(k).gammamat= exp(1/2*(trellismat.*(La(k) + Lc*x(k)') +
Lc*paritymat.*p(k)'));
    gamma(k).gammamat= gamma(k).gammamat.*(trellismat>0 | trellismat<0);
end
%Compute alpha1
for k=1:bs
    alpha(:,k+1)= (gamma(k).gammamat)*(alpha(:,k));
    alpha(:,k+1)=alpha(:,k+1)/sum(alpha(:,k+1));
end
%Compute beta1 with formula (15)
for k=bs:-1:1
    beta(:,k)=(gamma(k).gammamat)'*(beta(:,k+1));
    beta(:,k)=beta(:,k)/sum(beta(:,k));
end
for k=1:bs
    sumSplus=alpha(:,k)'*(gamma(k).gammamat.*(trellismat>0))*beta(:,k+1);
    sumSmminus=alpha(:,k)'*(gamma(k).gammamat.*(trellismat<0))*beta(:,k+1);
    LMAP(k)=log(sumSplus/sumSmminus);
end
LE=LMAP-La-Lc*x';
end
```

6.3.3 Convergence Behavior of the Turbo Codes

A typical BER curve for a turbo code is shown in Fig. 6.23. Three regions, namely low E_b/N_o region, waterfall region, and error floor region, can be identified. In the low E_b/N_o region, BER decreases slowly as E_b/N_o increases. For intermediate values of E_b/N_o , the BER decreases rapidly in the waterfall region with an increase in E_b/N_o . In this region, the coding gain approaches the theoretical limit. For large E_b/N_o , error floor occurs where the performance is dependent on the minimum Hamming distance of the code. The error floor is due to the weight distribution of turbo codes. Normally, turbo codes do not have large minimum distances. Hence, lowering the error floor results in better codes, which in some cases may result in faster convergence in decoding. One effective way of lowering the error floor is to use appropriate interleaver.

6.3.4 EXIT Analysis of Turbo Codes

Extrinsic information transfer (EXIT) chart [7] can be used as a tool to aid the construction of turbo codes. An EXIT chart is the reunion of two curves that characterize the two decoders used in a turbo decoder. Each curve represents a relation between the input and the output of one decoder. This relation is the mutual information between the output of the decoder (Le: the extrinsic information) and the initial message that was encoded before passing through the channel, with

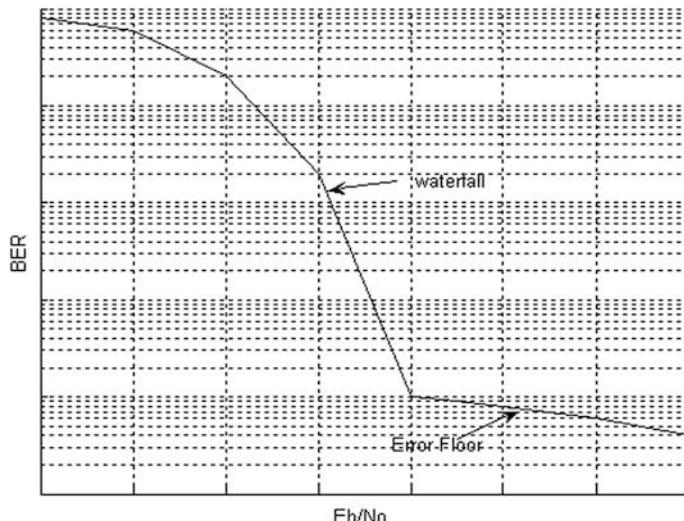


Fig. 6.23 Typical BER curve of turbo codes

respect to the mutual information between the input of the decoder (L_a : the a priori information) and the message:

In a turbo decoder, the extrinsic information of the first decoder (L_{e1}) is used as the a priori information of the second decoder (L_{e2}) and vice versa. It is suggested in [6] that a priori input to the constituent decoder can be modeled by

$$L_a = \mu_a \cdot x + \eta_a \quad (6.19)$$

where x is the known transmitted systematic bits, η_a is the Gaussian noise and $\mu_a = \frac{\sigma_a^2}{2}$.

For each L_a , the mutual information I_A and I_E are computed as [6]

$$I_A = \frac{1}{2} \int_{e \in E} \sum_{x \in \pm 1} p_A(e|x) \log_2 \left(\frac{2p_A(e|x)}{p_A(e|x=1) + p_A(e|x=-1)} \right) de \quad (6.20a)$$

$$0 \leq I_A \leq 1$$

where p_A is the probability density function of L_a . For Gaussian noise, Eq. (6.20a) can be rewritten as

$$I_A = 1 - \int \exp \left(\frac{-1}{2\sigma_a^2} \left(y - \frac{\sigma_a^2}{2} \right)^2 \right) \frac{\log_2(1 + e^{-y})}{\sqrt{2\pi\sigma_a^2}} dy \quad (6.20b)$$

$$I_E = \frac{1}{2} \int_{e \in E} \sum_{x \in \pm 1} p_E(e|x) \log_2 \left(\frac{2p_E(e|x)}{p_E(e|x=1) + p_E(e|x=-1)} \right) de \quad (6.21)$$

$$0 \leq I_E \leq 1$$

where p_E is the probability density function of L_e . Viewing I_E as a functions of I_E and $\frac{E_b}{N_o}$, the EXIT characteristics are defined as

$$I_E = T \left(I_A, \frac{E_b}{N_o} \right) \quad (6.22)$$

For fixed $\frac{E_b}{N_o}$, the above transfer characteristic can be rewritten as follows:

$$I_E = T(I_A) \quad (6.23)$$

Once I_{A1} and I_{E1} for decoder 1 and I_{A2} and I_{E2} for decoder 2 are obtained using Eqs. (6.20a) and (6.20b) and (6.21), they are drawn on a single chart that is I_{A1} on the x axis and I_{E1} on the y axis for decoder 1, and for decoder 2, I_{E2} on the x axis and I_{A2} on the y axis resulting in EXIT chart for the turbo decoder.

The steps involved in obtaining EXIT curve can be summarized as follows:

1. Specify the turbo code rate R and interested $\frac{E_b}{N_o}$ and determine AWGN $N_o/2$.
2. Specify μ_a of interest and determine $\sigma_a^2 = 2\mu_a$.
3. Run the turbo code simulator which yields encoded bits $y = [xp_1 p_2]$;
4. Find L_a using Eq. (6.19) and probability density function $p_A(e|x)$ using a histogram of L_a . Then, find mutual information I_A using Eq. (6.20a).
5. Run the BCJR decoder using the model $r = y + \eta$ with $\eta = \mathcal{N}(0, \sigma^2)$ $\sigma^2 = N_o/2$. In addition to the r , the decoder has $L_c = \frac{2r}{\sigma^2}$, and L_e given by Eq. (6.19).
6. Find L_e and then determine the probability density function $p_E(e|x)$ from the histogram of L_e and calculate mutual information I_E using Eq. (6.21).
7. If all values for μ_a of interest are exhausted, then stop and plot I_A versus I_E . Otherwise, go to step 2.

The EXIT charts at $\frac{E_b}{N_o} = 0.5$ dB and -0.2 dB are shown in Fig. 6.24 for rate 1/3 turbo encoder considered in [1].

From Fig. 6.24, it is observed that the curves cross for the EXIT chart at $\frac{E_b}{N_o} = -0.2$ dB and the turbo decoder does not converge. Hence, the ensemble threshold for rate 1/3 turbo encoder [1] must be at around -0.2 dB.

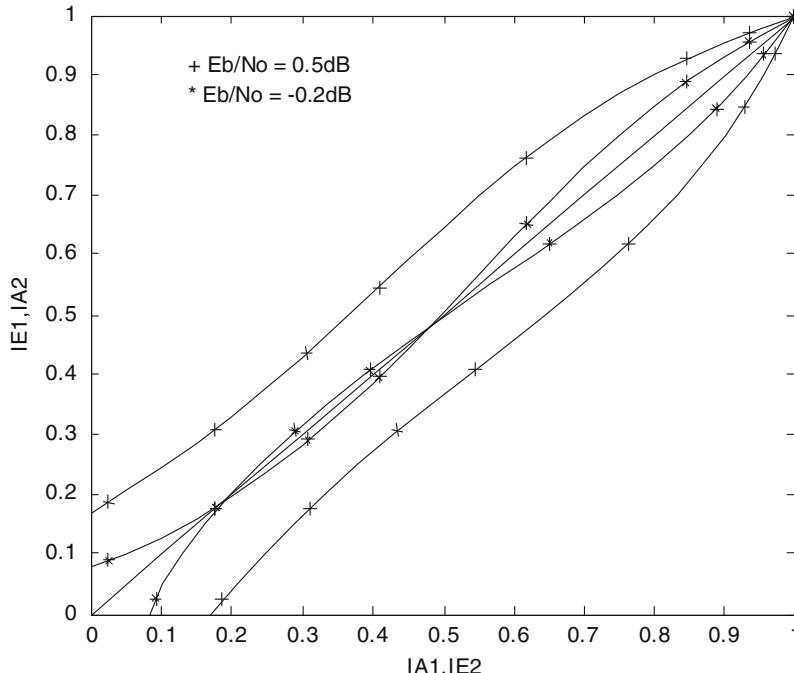


Fig. 6.24 EXIT charts for the rate 1/3 turbo encoder [1] at $\frac{E_b}{N_o} = 0.5$ dB and -0.2 dB

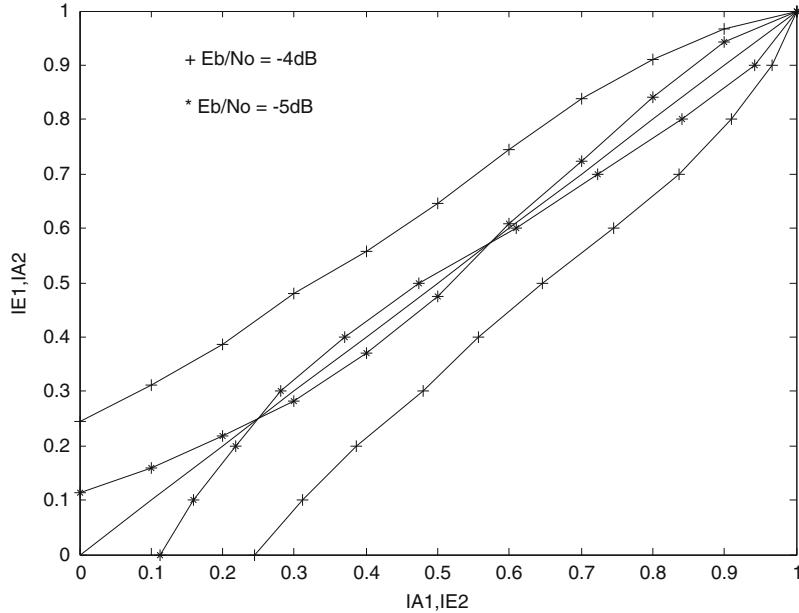


Fig. 6.25 EXIT charts for the rate 1/3 UMTS turbo encoder at $\frac{E_b}{N_o} = -4 \text{ dB}$ and -5 dB

The EXIT charts at $\frac{E_b}{N_o} = -5 \text{ dB}$ and -4 dB are shown in Fig. 6.25 for rate 1/3 UMTS turbo encoder considered in Example 6.2.

From Fig. 6.25, it is observed that the curves cross for the EXIT chart at $\frac{E_b}{N_o} = -5 \text{ dB}$ and the turbo decoder does not converge. Hence, the ensemble threshold for rate 1/3 UMTS turbo encoder must be at around -5 dB .

For a given code and channel, the decoding correctness of turbo decoder can check by examining whether the decoders EXIT curves cross. The ensemble threshold can be estimated by finding the $\frac{E_b}{N_o}$ for which the EXIT curves of the decoders cross. The speed of the decoder can be obtained from EXIT curves. The wider the gap between the EXIT curves of the two decoders, fewer the number of iterations required for convergence.

6.4 Performance Analysis of the Turbo Codes

6.4.1 Upper Bound for the Turbo Codes in AWGN Channel

Assuming that the transmitted data symbols are BPSK modulated which are coherently demodulated at the receiver, Bit error probability bounds for turbo codes on AWGN channels can be upper bounded by the union bound [8, 9].

$$\text{BER}_{\text{ub}} \leq \sum_{w=1}^N \sum_{d=d_f}^{\infty} A(w, d) \frac{w}{N} Q\left(\sqrt{2 \cdot d \cdot R \cdot \frac{E_b}{N_o}}\right) \quad (6.24)$$

where $A(w, d)$ is the number of code word of input weight w and the total weight d . The code's block size is given by the number of information bits N and the code rate R . Ignoring the effect of the tail (assuming that the tail length N), we can use our usual definition of N as being the length of the whole source sequence, including the tail. Thus, changing the order of summation:

$$\begin{aligned} \text{BER}_{\text{ub}} &\leq \sum_{d=d_f}^{\infty} \left[\sum_{w=1}^N A(w, d) \frac{w}{N} \right] Q\left(\sqrt{2 \cdot d \cdot R \cdot \frac{E_b}{N_o}}\right) \\ &\leq \sum_{d=d_f}^{\infty} A_d \cdot Q\left(\sqrt{2 \cdot d \cdot R \cdot \frac{E_b}{N_o}}\right) \end{aligned} \quad (6.25)$$

where A_d is the total information weight of all code words of weight d divided by the number of information bits per code word, as defined by

$$A_d = \sum_{w=1}^N A(w, d) \frac{w}{N} \quad (6.26)$$

Now, define N_d to be the number of code words of the total weight d and w_d to be their average information weight. Thus,

$$N_d \cdot w_d = \sum_{w=1}^N A(w, d) \cdot w \quad (6.27)$$

$$A_d = w_d \frac{N_d}{N} \quad (6.28)$$

where $\frac{N_d}{N}$ is called the *effective multiplicity* of code words of weight d . Substituting Eq. (6.28) in Eq. (6.25), we obtain

$$\text{BER}_{\text{ub}} \leq \sum_{d=d_f}^{\infty} w_d \frac{N_d}{N} Q\left(\sqrt{2 \cdot d \cdot R \cdot \frac{E_b}{N_o}}\right). \quad (6.29)$$

6.4.2 Upper Bound for Turbo Codes in Rayleigh Fading Channel

In MRC, the receiver weights the incoming signals on antennas by the respective conjugates of the complex fading random variables. The pair-wise bit error probability with MRC in a Rayleigh fading channel for BPSK case is given by [10]

$$P_{d,\text{MRC}} = \frac{1}{\pi} \int_{\theta=0}^{\frac{\pi}{2}} \left[\frac{\sin^2 \theta}{\sin^2 \theta + \frac{E_b}{N_o}} \right]^{Ld} d\theta \quad (6.30)$$

Recalling the result in [11]

$$\frac{1}{\pi} \int_{\theta=0}^{\frac{\pi}{2}} \left[\frac{\sin^2 \theta}{\sin^2 \theta + c} \right]^n d\theta = \pi [P_e]^n \sum_{k=0}^{n-1} \binom{n-k+1}{k} (1-P_e)^k \quad (6.31)$$

where

$$P_e = \frac{1}{2} \left(1 - \sqrt{\frac{\frac{E_b}{N_o}}{1 + \frac{E_b}{N_o}}} \right)$$

Using Eq. (6.31) in Eq. (6.30), in closed form, we obtain

$$P_{d,\text{MRC}} = [P_e]^{Ld} \sum_{k=0}^{Ld-1} \binom{Ld-1+k}{k} (1-P_e)^k \quad (6.32)$$

Then, the upper bound on the BER performance of turbo codes in Rayleigh fading channel with MRC diversity can be expressed as

$$\text{BER}_{\text{Rayleigh,MRC}} \leq \sum_{d=d_f}^{\infty} A_d P_{d,\text{MRC}} \quad (6.33)$$

If there is no diversity, i.e., $L = 1$, the upper bound on the BER performance of turbo codes in Rayleigh fading channel can be expressed as

$$\text{BER}_{\text{Rayleigh}} \leq \sum_{d=d_f}^{\infty} A_d P_d \quad (6.34)$$

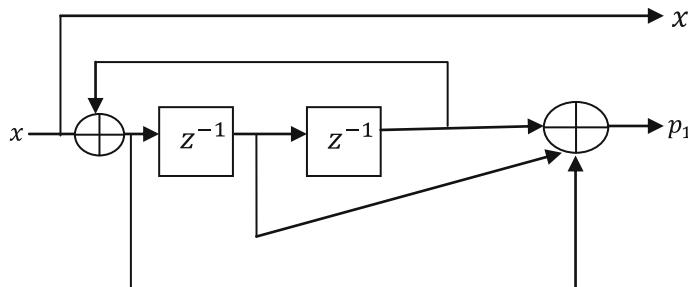


Fig. 6.26 RSC encoder of Example 6.7

where

$$P_d = [P_e]^d \sum_{k=0}^{d-1} \binom{d-1+k}{k} (1-P_e)^k$$

Example 6.7 Consider a turbo encoder using the following RSC encoder shown in Fig. 6.26 with free distance 5, plot the upper bound BER versus $\frac{E_b}{N_o}$ performance of the turbo encoder for interleaver length of 100 in AWGN, Rayleigh fading channel with MRC diversity for $L = 2$.

Solution The set of coefficients A_d used to compute the bound for interleaver length of 100 as quoted in [8] are given as follows:

d	A_d	d	A_d
8	0.039881	22	33.31
9	0.079605	23	54.65
10	0.1136	24	91.23
11	0.1508	25	154.9
12	0.1986	26	265.5
13	0.2756	27	455.6
14	0.4079	28	779
15	0.6292	29	1327
16	1.197	30	2257
17	2.359	31	3842
18	4.383	32	6556
19	7.599	33	11221
20	12.58	34	19261
21	20.46	35	33143

The following MATLAB program is written and used to plot the $\frac{E_b}{N_o}$ versus upper bound BER Performance of the turbo encoder with an interleaver length of 100 (Fig. 6.27).

Program 6.3 MATLAB program to compute upper bound BER for different $\frac{E_b}{N_o}$

```

clear all
close all
gamma_b_in_dB = [0:0.37:10];
gamma_b = 10.^(gamma_b_in_dB/10);
d = [8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
31 32 33 34 35 ];
R_c = 1/3;
Ad=[0.0039881 0.0079605 0.011918 0.015861 0.019887 0.024188
0.029048 0.034846 0.065768 0.1457 0.2984 0.5472 0.9171 1.437 2.144
3.09 4.465 6.716 10.67 17.65 29.61 49.31 80.57 128.6 201.3 311.5 481.2
748.8];
for i=1:28
    sum=0;sumr=0;summr=0;
    q1=sqrt((gamma_b(i)*R_c)/(1+gamma_b(i)*R_c));
    q2=sqrt((0.5*gamma_b(i)*R_c)/(1+0.5*gamma_b(i)*R_c));
    for j=1:28
        d1=d(j);
        q=0.5*(1-q1);
        q22=0.5*(1-q2);
        pd1=0;pd2=0;
        for k=0:d1-1
            pd1=pd1+nchoosek((d1-1+k),k)*((1-q)^k);
        end
        for k=0:2*d1-1
            pd2=pd2+nchoosek((2*d1-1+k),k)*((1-q22)^k);
        end
        pd=(q^d1)*pd1;
        sumr=sumr+Ad(j)*pd;
        pdm=q22^(2*d1)*pd2;
        summr=summr+Ad(j)*pdm;
        sum=sum+ Ad (j)* 0.5* erfc ( sqrt( d (j)* R_c * gamma_b(i) ) );
    end
    BER_boundg(i)=sum;
    BER_boundray(i)=sumr;
    BER_boundraym(i)=summr;
end
figure
semilogy(gamma_b_in_dB(1:28),BER_boundg, '-');
hold on
semilogy(gamma_b_in_dB(1:28),BER_boundray, '-o');
semilogy(gamma_b_in_dB(1:28),BER_boundraym, '-d');
xlabel('itE_b/N_o (dB)'), ylabel('itBER_b_o_u_n_d');
legend('Gaussian','Rayleigh','MRC ,itN_r=2');

```

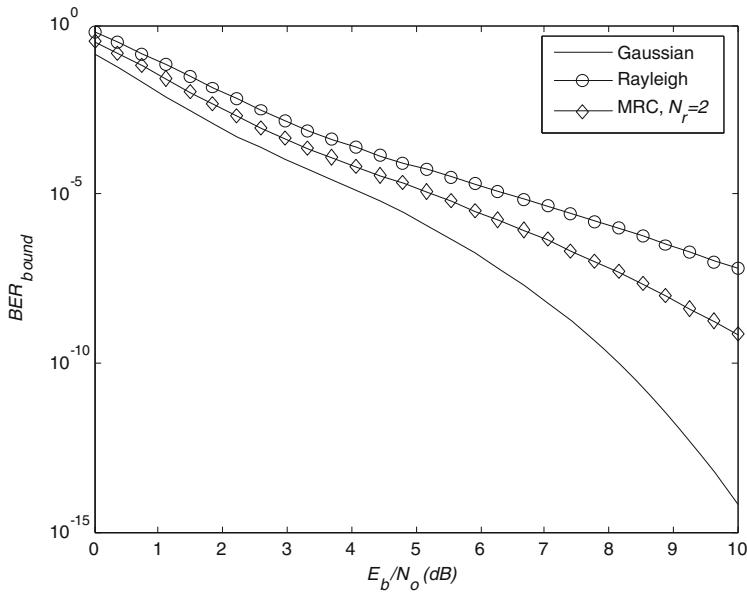


Fig. 6.27 Upper bound BER performance of turbo encoder of Example 6.7 with interleaver length of 100

6.4.3 Effect of Free Distance on the Performance of the Turbo Codes

The BER performance of turbo codes for ML decoding is upper bounded by Eq. (6.29). Since the BER performance of the code is dominated by the free distance term (for $d = d_f$) for moderate and high SNRs, for AWGN channel, Eq. (6.29) can be written as given below [12]

$$\text{BER}_{d_f, \text{AWGN}} \approx w_f \cdot \frac{N_f}{N} \cdot Q\left(\sqrt{2 \cdot d_f \cdot R \cdot \frac{E_b}{N_o}}\right) \quad (6.35)$$

where N_f and w_f correspond to N_d and w_d for $d = d_f$.

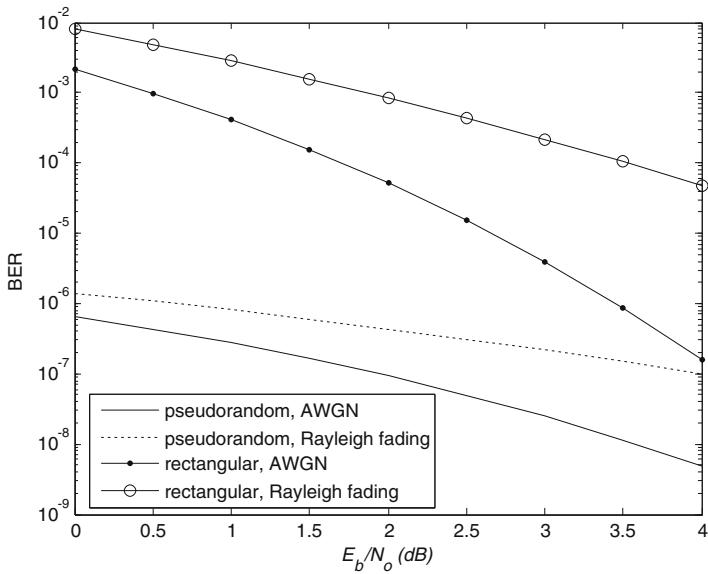


Fig. 6.28 Free distance asymptotes for turbo codes in AWGN and Rayleigh fading channels with two different interleavers

$$\text{BER}_{d_f, \text{Rayleigh}} \approx w_f \cdot \frac{N_f}{N} \cdot \sum_{k=0}^{d_f-1} \binom{d_f - 1 + k}{k} \left(1 - \frac{1}{2} \left(1 - \sqrt{\frac{\frac{E_b}{N_o} R}{1 + \frac{E_b}{N_o} R}} \right) \right)^k \quad (6.36)$$

For a turbo code considered in [13], the BER performance is evaluated in AWGN and Rayleigh fading channels with a pseudo-random interleave of length with 65536 with $N_f = 3$, $d_f = 6$, $w_f = 2$ and a 120×120 rectangular window with $N_f = 28,900$, $d_f = 12$, $w_f = 4$.

The following MATLAB program is written and used to evaluate the performance in AWGN and Rayleigh fading channels.

Program 6.4 MATLAB Program for free distance asymptotes in AWGN and Rayleigh fading channels for two different interleavers

```

clear all
close all
gamma_b_in_DB = [0:0.5:4];
gamma_b = 10.^ (gamma_b_in_DB/10);
N_free = 3;
tilde_w_free = 2;
d_free = 6;
R_c = 1/2;
N = 65536;
N_freerec = 28900;
tilde_w_freerec = 4;
d_freerec = 12;
R_c = 1/2;
Nrec = 14400;
d1=d_free;
P_b_free_pseudorandom = N_free * tilde_w_free /N * 0.5* erfc ( sqrt( d_free
* R_c * gamma_b ) );
P_b_free_rectangular = N_freerec * tilde_w_freerec /Nrec * 0.5* erfc ( sqrt(
d_freerec * R_c * gamma_b ) );
for i=1:length(gamma_b_in_DB)
    q1=sqrt((gamma_b(i)*R_c)/(1+gamma_b(i)*R_c));
    q=0.5*(1-q1);
    pd1=0;
    for k=0:d1-1
        pd1=pd1+nchoosek((d1-1+k),k)*((1-q)^k);
    end
    P_b_free_pseudorandomray(i) =( N_free * tilde_w_free /N)*(q^(d1))*pd1;
end
d1=d_freerec;
for i=1:length(gamma_b_in_DB)
    q1=sqrt((gamma_b(i)*R_c)/(1+gamma_b(i)*R_c));
    q=0.5*(1-q1);
    pd1=0;
    for k=0:d1-1
        pd1=pd1+nchoosek((d1-1+k),k)*((1-q)^k);
    end
    P_b_free_rectangulararray(i) =( N_freerec * tilde_w_freerec
/Nrec)*(q^(d1))*pd1;
end
figure
semilogy(gamma_b_in_DB, P_b_free_pseudorandom, '-', gamma_b_in_DB,
P_b_free_pseudorandomray, '--', gamma_b_in_DB, P_b_free_rectangular, '-.
', gamma_b_in_DB, P_b_free_rectangulararray, '-o');
xlabel('itE_b/N_o (dB)'), ylabel('BER');
Legend('pseudorandom,AWGN','pseudorandom ,Rayleigh
fading','rectangular,AWGN','rectangular,Rayleigh fading');

```

The free distance asymptotes for pseudo-random and rectangular interleavers in AWGN and Rayleigh fading channels obtained from the above MATLAB program are shown in Fig. 6.28.

From Fig. 6.28, it can be observed that the rectangular window exhibits relatively poor performance. It is due to the fact that the rectangular window has large effective multiplicity as compared to the effective multiplicity of the pseudo-random interleaver.

6.4.4 Effect of Number of Iterations on the Performance of the Turbo Codes

The BER performance of UMTS turbo codes for frame length of 40 is shown in Fig. 6.29. It can be seen that as the number of iterations increases, there is a significant improvement in BER performance. However, for certain number iterations, no improvement can be observed. For complexity reasons, in turbo decoding, 4–10 iterations are used.

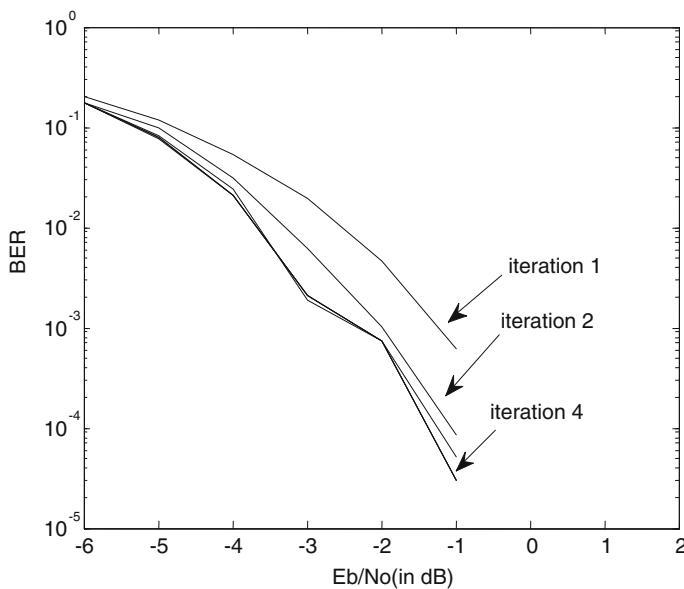


Fig. 6.29 Effect of number of iterations on the BER performance of turbo codes

6.4.5 Effect of Puncturing on the Performance of the Turbo Codes

The BER performance comparison of the unpunctured and the punctured turbo codes is shown in Fig. 6.30. For this, a turbo encoder is considered that uses RSC encoders with the generating function.

$$G = \begin{bmatrix} 1 & \frac{1+D^2}{1+D+D^2} \end{bmatrix}$$

A random interleaver of length 1,000 with odd–even separation is used. An AWGN channel with BPSK modulation assumed. In the decoding, Log BCJR algorithm for 3 iterations is used.

From Fig. 6.30, it can be observed that the unpunctured turbo codes give a gain of about 0.6 dB over the punctured turbo codes.

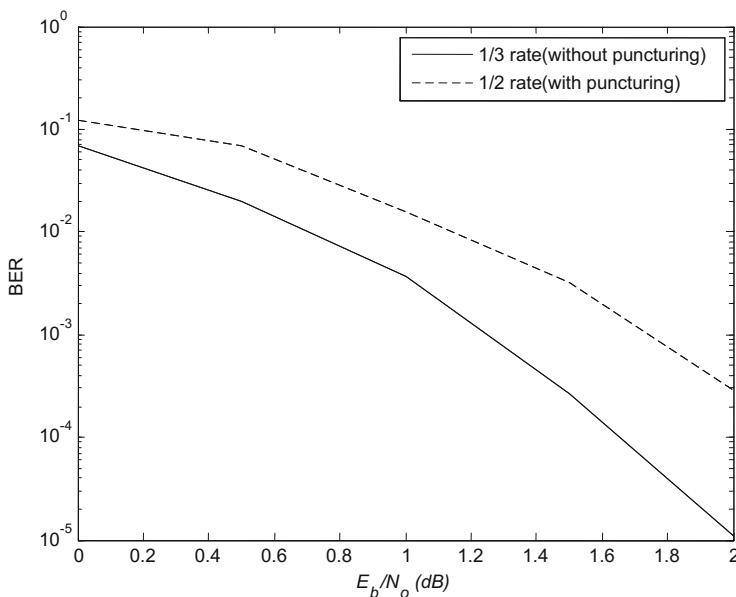


Fig. 6.30 Effect of puncturing on the BER performance of turbo codes

6.5 Problems

1. For the encoder shown in Fig. 6.31
 - (a) Find the impulse response
 - (b) Draw the state diagram
 - (c) Obtain its equivalent recursive encoder
 - (d) Find the impulse response of the recursive encoder obtained
 - (e) Draw the state diagram of the recursive encoder obtained
2. Draw the equivalent RSC encoder of the convolutional encoder with generator sequences $g_1 = [1 \ 1 \ 1 \ 1 \ 1]$; $g_2 = [1 \ 0 \ 0 \ 0 \ 1]$
3. For the turbo encoder shown in Fig. 6.14, find the code word for the input sequence $x = \{1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0\}$. Let the interleaver be $\{5 \ 3 \ 4 \ 0 \ 6 \ 2 \ 1\}$
4. For the turbo encoder shown in Fig. 6.9, find the code word for the input sequence $x = \{1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0\}$. Let the interleaver be $\{7 \ 5 \ 1 \ 2 \ 4 \ 3 \ 6 \ 0\}$
5. Consider the CDMA2000 standard encoder shown in Fig. 6.32. Find the code word for the input sequence $x = \{1 \ 0 \ 1 \ 1 \ 0 \ 0\}$ assuming that the encoders trellis is terminated. Let the interleaver be $\{0 \ 3 \ 1 \ 5 \ 2 \ 4\}$.
6. Decode the following received sequence when the turbo code generated in Example 6.2 was transmitted over an AWGN channel with unity noise variance

$x'(n)$	$p'_1(n)$	$p'_2(n)$
1.3209	2.4883	-1.3369
0.8367	-2.5583	-3.0404
-1.8629	-0.6555	-1.6638
-2.6356	0.3157	0.1266
-1.0138	0.999	-1.3059
1.4864	0.6762	-1.0409
-2.262	-0.7018	-0.5412

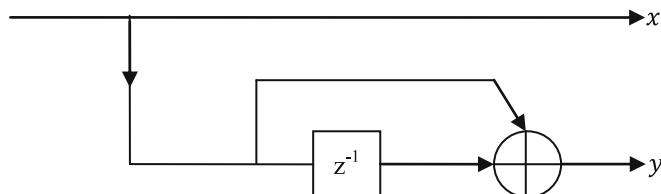


Fig. 6.31 Non-recursive systematic convolutional encoder

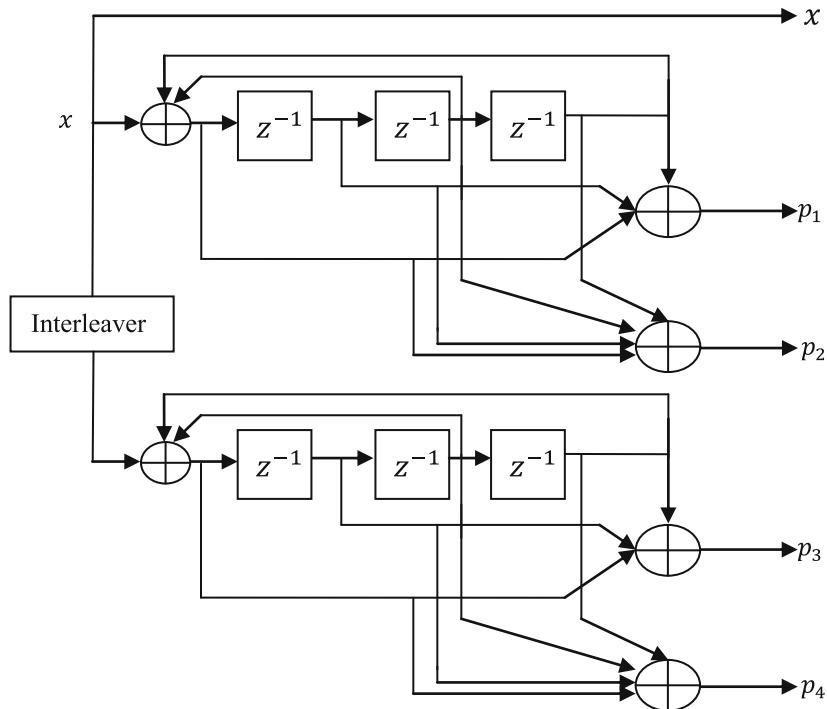


Fig. 6.32 CDMA2000 standard turbo encoder

6.6 MATLAB Exercises

1. Write a MATLAB program to construct an EXIT chart for turbo codes.
2. Write a MATLAB program to simulate the performance of unpunctured and punctured turbo codes.

References

1. Berrou, C., Glavieux, A., Thitimajshima, P.: Near Shannon limit error-correcting coding and decoding: turbo-codes. In: Proceedings of ICC 1993, Geneva, Switzerland, pp. 1064–1070 (1993)
2. Berrou, C., Glavieux, A.: Near optimum error correcting coding and decoding: turbo-codes. IEEE Trans. Commun. **44**(10), 1261–1271 (1996)
3. Jung, P., Nasshan, M.: Performance evaluation of turbo codes for short frame transmission systems. Electron. Lett. **30**(2), 111–113 (1994)
4. Hanzo, L., Liew, T.H., Yeap, B.L.: Turbo Coding, Turbo Equalisation and Space Time Coding for Transmission Over Fading Channels. IEEE Press, Wiley Ltd., Hoboken (2002)

5. Bahl, L., Cocke, J., Jelinek, F., Raviv, J.: Optimal decoding of linear codes for minimizing symbol Error rate. *IEEE Trans. Inf. Theor.* **20**, 284–287 (1974)
6. ten Brink, S.: Convergence behavior of iteratively decoded parallel concatenated codes. *IEEE Trans. Commun.* **49**(10), 1727–1737 (2001)
7. Ryan, W.E., Lin, S.: *Modern Codes: Classical and Modern*. Cambridge University Press, Cambridge (2009)
8. Benedetto, S., Montorsi, G.: Unveiling turbo codes: some results on parallel concatenated coding schemes. *IEEE Trans. Info. Theor.* **42**, 409–429 (1996)
9. Divsalar, D., Dolinar, S., McEliece, R.J., Pollara, F.: Transfer function bounds on the performance of turbo codes. TDA progress report 42-122, JPL, Caltech, August 1995
10. Ramesh, A., Chockalingam, A., Milstein, L.B.: Performance analysis of turbo codes on Nakagami fading channels with diversity combining. WRL-IISc-TR-108, Wireless Research Lab Technical Report, Indian Institute of Science, Bangalore, Jan 2001
11. Goldsmith, A., Alouini, M.-S.: A unified approach for calculating error rates of linearly modulated signals over generalized fading channels. *IEEE Trans. Commun.* **47**, 1324–1334 (1999)
12. Du, K.-L., Swamy, M.N.S.: *Wireless Communications: Communication Systems From RF Subsystems to 4G Enabling Technologies*. Cambridge University Press, Cambridge (2010)
13. Schlegel, C.B., Perez, L.C.: *Trellis and Turbo Coding*. IEEE Press, Piscataway (2004)

Chapter 7

Bandwidth Efficient Coded Modulation

The block codes, convolutional, and turbo codes discussed in the previous chapters achieve performance improvement expanding the bandwidth of the transmitted signal. However, when coding is t_p being applied to bandwidth limited channels, coding gain is to be achieved without signal bandwidth expansion. The coding gain for bandwidth limited channels can be achieved by a scheme called trellis coded modulation (TCM). The TCM is a combined coding and modulation technique that increases the number of signals over the corresponding uncoded system to compensate for the redundancy introduced by the code for digital transmission over band-limited channels. The term “trellis” is due to the fact that the trellis diagram for the TCM schemes is similar to the trellis diagrams of binary convolutional codes. In TCM schemes, the trellis branches are labeled with redundant non-binary modulation signals rather than with binary code symbols. The TCM schemes employ multilevel amplitude and phase modulation, such as PAM, PSK, DPSK, or QAM, in combination with a finite-state encoder which governs the selection of modulation signals to generate coded signal sequences. In the receiver, the received noisy signals are decoded using soft-decision Viterbi or BCJR decoder.

In the TCM, the “free distance” (minimum Euclidean distance) between the coded modulation signals exceeds the minimum distance between the uncoded modulation signals, at the same information rate, bandwidth, and signal power.

The basic principle of the TCM and further descriptions of it were published in [1–5]; the TCM has seen rapid transition from the research to the practical use in 1984, when the international telegraph and telephone consultative committee (CCITT) has adopted the TCM scheme with a coding gain of 4 dB for use in the high-speed voice band modems for 9.6/12.4 kbps standard [4, 6, 7].

The main idea in the TCM is to devise an effective method that perform mapping of the coded bits into the signal symbols so as to maximize the free distance between coded signal sequences. A method based on the principle of mapping by set partitioning was developed by Ungerboeck in [1]. This chapter describes the classical

Electronic supplementary material The online version of this chapter (doi:[10.1007/978-81-322-2292-7_7](https://doi.org/10.1007/978-81-322-2292-7_7)) contains supplementary material, which is available to authorized users.

bandwidth efficient TCM, turbo TCM (TTCM), bit-interleaved coded modulation (BICM), bit-interleaved coded modulation iterative decoding (BICM-ID), and comparison of their BER performance.

7.1 Set Partitioning

Set partitioning divides a signal set into the smaller sets with maximally increasing smallest intra-set distances. Finally, the obtained small signal constellations will be referred to as the “subsets.” Every constellation point is used only once, and if the subsets are used with equal probability, then the constellation points all appear with equal probability. The following two examples illustrate the set partitioning. The signal constellation is partitioned into the subsets that Euclidean minimum distance between signal symbols in a subset is increased with each partition.

Example 7.1 Set partitioning of 4-PSK signal Euclidian distance in a signal constellation is the distance between different points in the constellation diagram with respect to reference point.

The 4-PSK signal constellation shown in Fig. 7.1 is partitioned as shown in Fig. 7.2. In the 4-PSK signal set, the signal symbols are located on a circle of radius 1 and having a minimum distance separation of $\Delta_0 = 2\sin\left(\frac{\pi}{4}\right) = \sqrt{2}$.

Finally, the last stage of the partition leads to 4 subsets and each subset contains a single signal symbol.

Example 7.2 Set partitioning of 8-PSK signal The 8-PSK signal constellation shown in Fig. 7.3 is partitioned as shown in Fig. 7.4. In the 8-PSK signal set, the signal symbols are located on a circle of radius 1 and having a minimum distance separation of $\Delta_0 = 2\sin\left(\frac{\pi}{8}\right) = 0.765$. The eight symbols are subdivided into two subsets of four symbols each in the first partition with the minimum distance between two symbols increases to $\Delta_1 = 2\sin\left(\frac{\pi}{4}\right) = \sqrt{2}$.

Finally, the last stage of the partition leads to 4 subsets and each subset contains a single signal symbol.

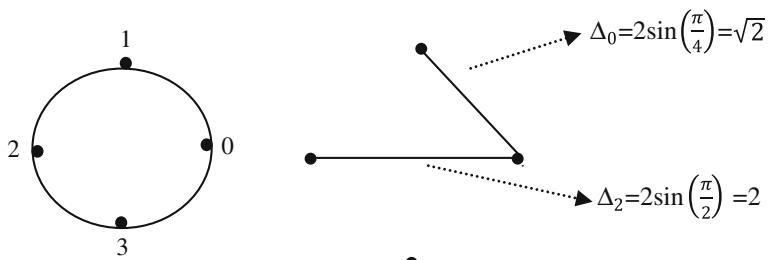
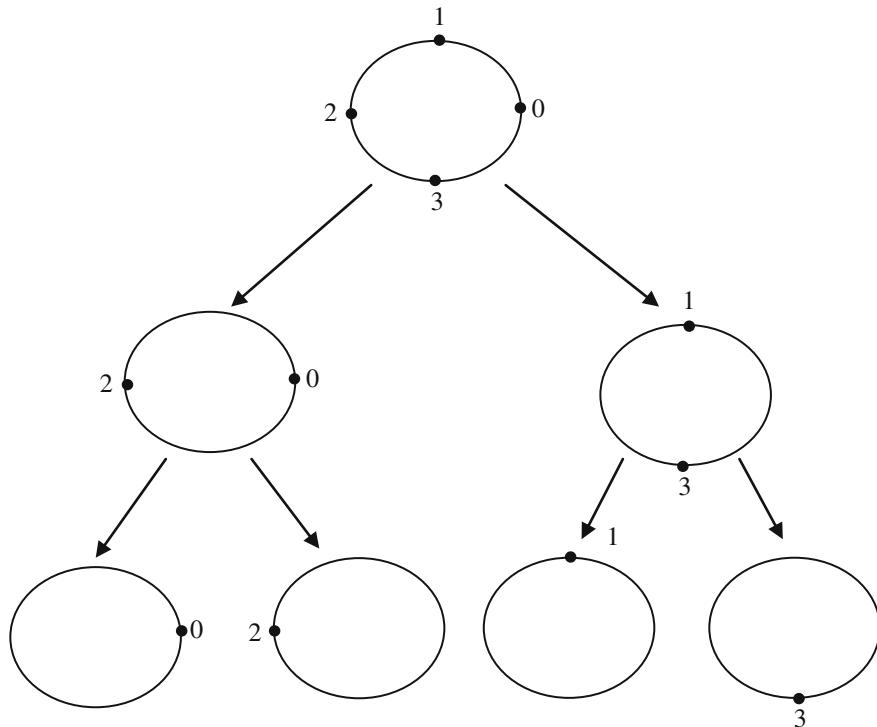
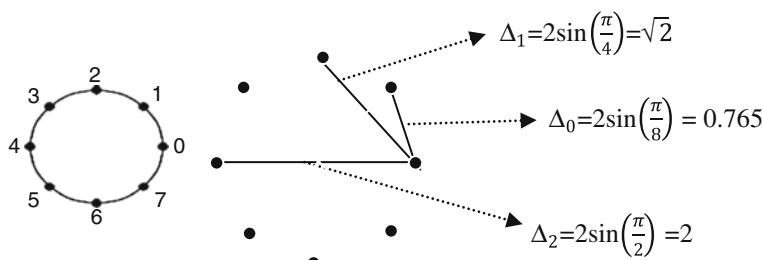


Fig. 7.1 Signal constellation diagram for the 4-PSK

**Fig. 7.2** 4-PSK set partitioning**Fig. 7.3** Signal constellation diagram for the 8-PSK

7.2 Design of the TCM Scheme

The general structure of a TCM scheme is shown in Fig. 7.5. In an operation, k information bits are transmitted. The $\tilde{k} (\tilde{k} < k)$ bits are encoded by binary convolutional encoder. The encoder output bits are used to select one of the possible subsets in the partitioned signal set—partition of the signal—while the remaining

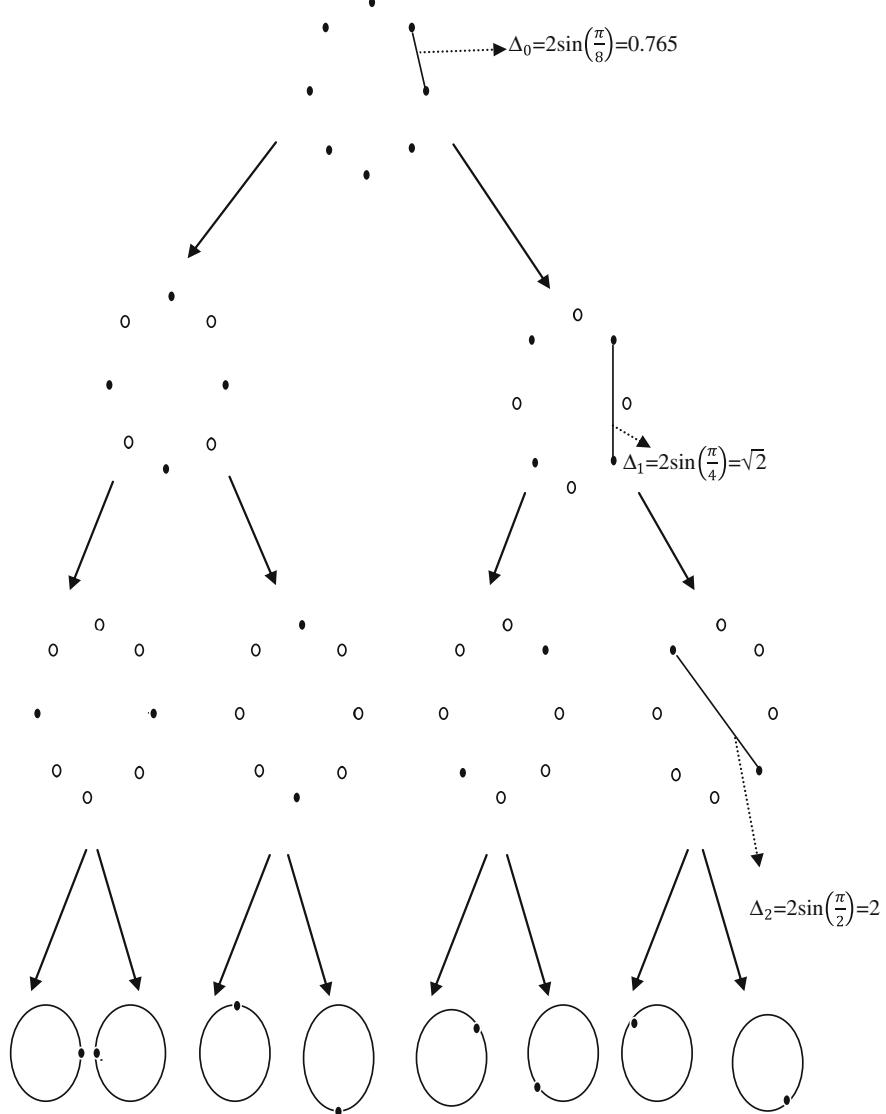


Fig. 7.4 8-PSK set partitioning

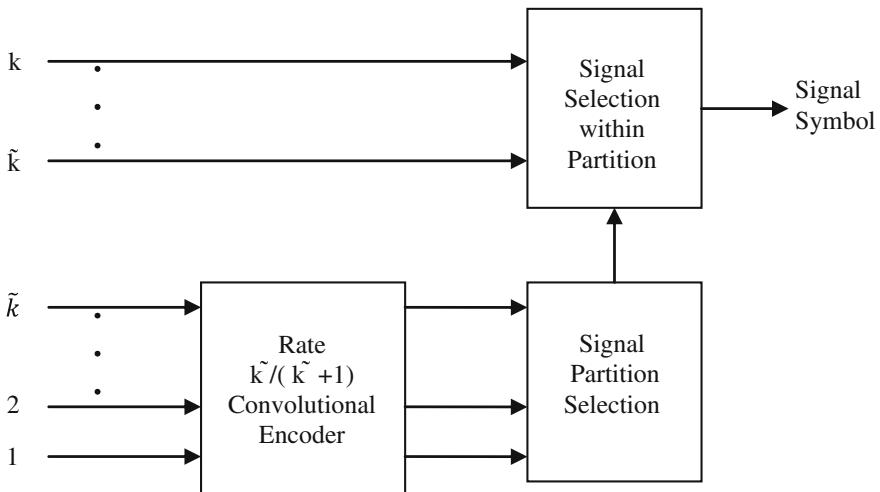


Fig. 7.5 General structure of a TCM scheme

$k - \tilde{k}$ bits are used to select one of $2^{m-\tilde{m}}$ signal symbols in each subset. When $\tilde{k} = k$, all the k information bits are encoded.

In the encoder short designing, Ungerboeck summarized the following rules that were to be applied to the assigned channel signals.

1. Transmission originating, or merging into any of the same state should receive signals from the subsets having maximum Euclidean distance between them.
2. Parallel state transitions are assigned the signal symbols separated by the largest Euclidean distance.
3. All the subsets are to be used with equal probability in trellis diagram.

The following examples illustrate the design of different TCM encoders.

Example 7.3 2-state 4-PSK TCM Encoder A simple 2-state 4-PSK TCM encoder is shown in Fig. 7.6a. In this encoder, a rate 1/2 convolutional encoder is used in which both the information bits are encoded. The output of the convolutional encoder is used to select from among the second level partitions of 4-PSK, wherein each partition contains only a single signal. Thus, it does not require an uncoded bit to complete the signal selection process. The two-state trellis diagram of the 4-PSK TCM encoder is shown in Fig. 7.6b, which has no parallel transitions.

The signal flow graph of the trellis diagram of Fig. 7.6b is shown in Fig. 7.7. Now, the transfer function can be obtained by using the signal flow graph techniques and Mason's formula. In the graph, the branch labels superscripts indicate the weight (SED) of the corresponding symbol of the transition branch in the trellis diagram.

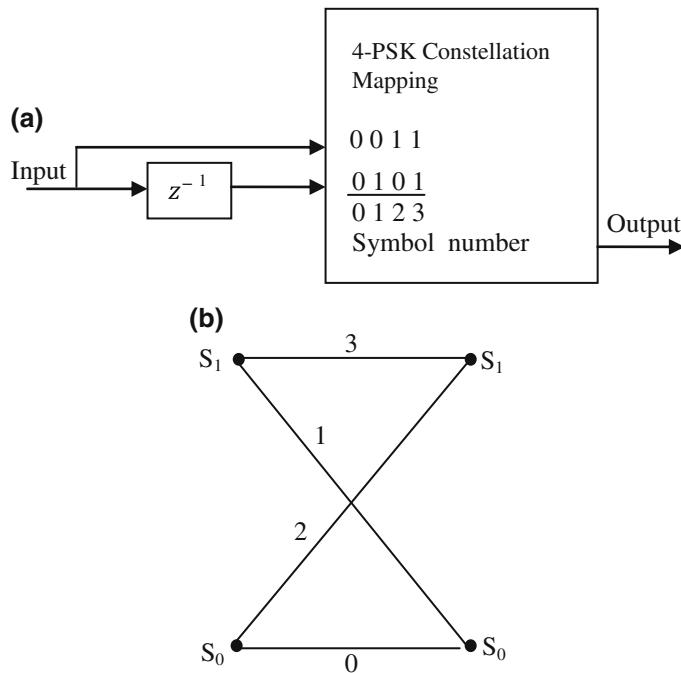


Fig. 7.6 **a** 2-State QPSK TCM encoder. **b** 2-state QPSK TCM encoder trellis diagram

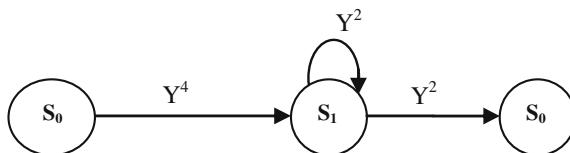
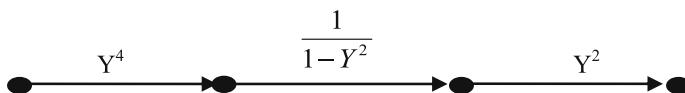


Fig. 7.7 Signal flow graph of the trellis shown in Fig. 7.6b

By using reduction techniques, the above signal flow graph can be simplified as follows:



Thus, the transfer function is given by

$$T(Y) = Y^4 \frac{1}{1-Y^2} Y^2 = \frac{Y^6}{1-Y^2}$$

Example 7.4 4-State 8-PSK TCM Encoder The Ungerboeck 4-state 8-PSK TCM encoder is shown in Fig. 7.8a. In this encoder, a rate 1/2 convolutional encoder partitions the 8-PSK constellation into four subconstellations $\{(0, 4), (1, 5), (2, 6), (3, 7)\}$. The unique two bit output from the convolutional encoder corresponds to a label assigned to each subconstellation. The output of the convolutional encoder selects one of the subconstellations, and the uncoded bit selects one of the two signals in the selected subconstellation.

The four-state trellis diagram of the TCM encoder is shown in Fig. 7.8b. In the trellis diagram, the states correspond to the contents of the memory elements in the convolutional encoder of the TCM encoder. The branch labels are the signals selected from the partitioned subconstellations for transmission associated with the given state transition. For example, if the convolutional encoder has to move from state S_0 to S_1 , then only signal 2 or 6 from subconstellation (2, 6) only may be selected for transmission.

The signal flow graph of the trellis diagram of Fig. 7.8b is shown in Fig. 7.8c. The transfer function can be obtained by using the signal flow graph techniques and Mason's formula.

The various distinct squared intersignal distances are as follows:

$$\begin{aligned}\Delta_{0,1} &= 2\sin\left(\frac{\pi}{8}\right) = 0.7654, \Delta^2(0, 1) = \Delta^2(000, 001) = 0.586 \\ \Delta_{0,2} &= 2\sin\left(2 * \frac{\pi}{8}\right) = 1.4142, \Delta^2(0, 2) = \Delta^2(000, 010) = 2.000 \\ \Delta_{0,3} &= 2\sin\left(3 * \frac{\pi}{8}\right) = 1.8478, \Delta^2(0, 3) = \Delta^2(000, 011) = 3.414 \\ \Delta_{0,4} &= 2\sin\left(4 * \frac{\pi}{8}\right) = 2.0000, \Delta^2(0, 4) = \Delta^2(000, 100) = 4.000\end{aligned}$$

By using the signal flow graph reduction techniques and Mason's formula, we obtain the following transfer function.

$$T(Y) = 4 \frac{(Y^{4.586} + Y^{7.414})}{1 - 2Y^{0.586} - 2Y^{3.414} - Y^{4.586} - Y^{7.414}}$$

Example 7.5 8-State 8-PSK TCM Encoder The Ungerboeck 8-state 8-PSK TCM encoder is shown in Fig. 7.9a. In this encoder, a rate 2/3 convolutional encoder is used in which both information bits are encoded. The output of the

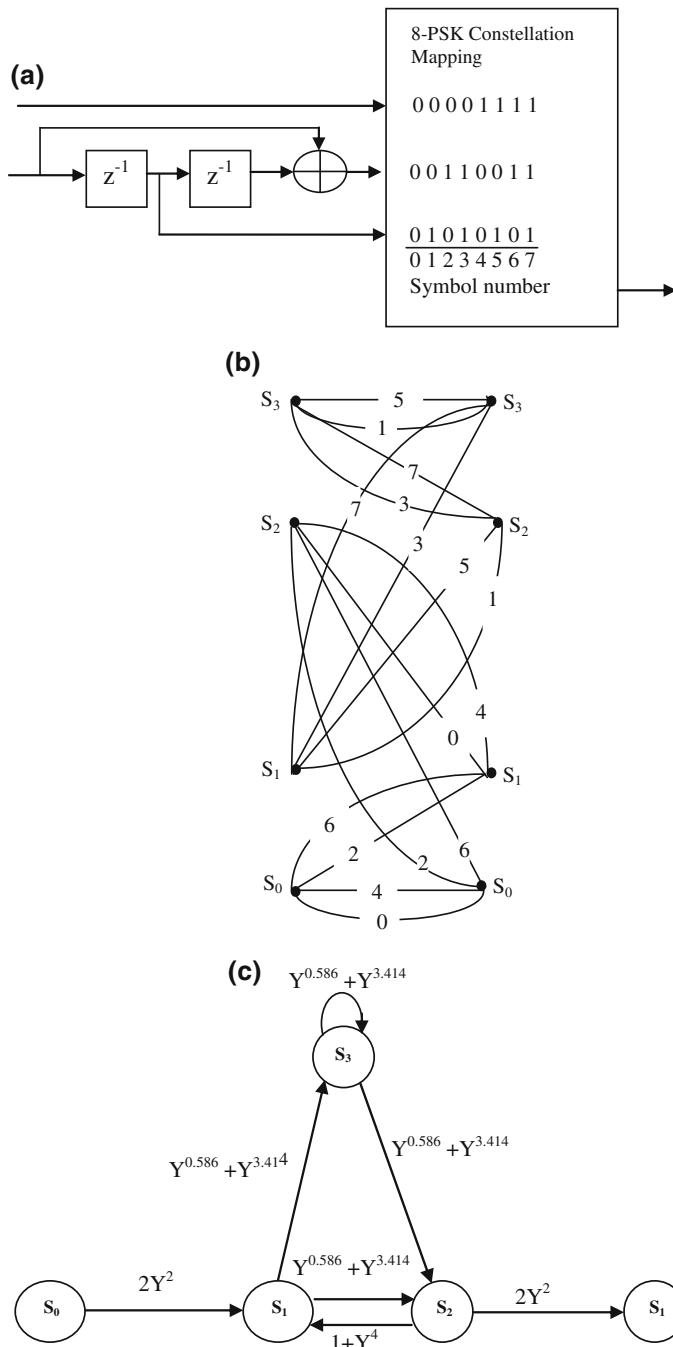


Fig. 7.8 a 4-State 8-PSK TCM encoder. b 4-state 8-PSK TCM encoder trellis. c Signal flow graph of the trellis shown in (b)

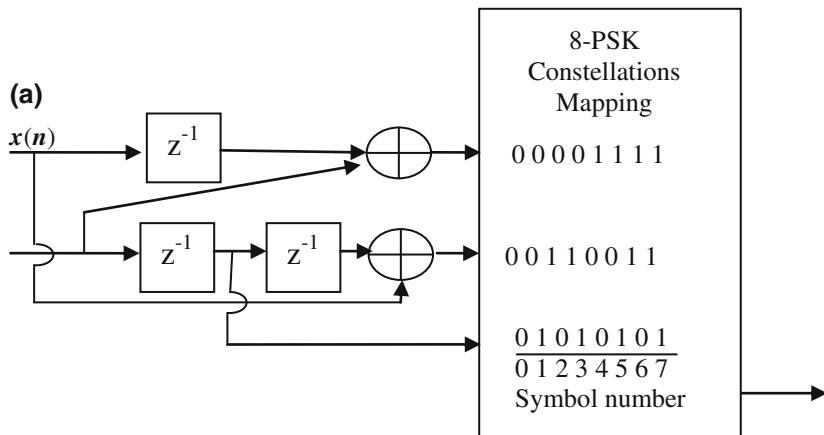


Fig. 7.9 a 8-state 8-PSK TCM encoder. b 8-state 8-PSK TCM encoder trellis

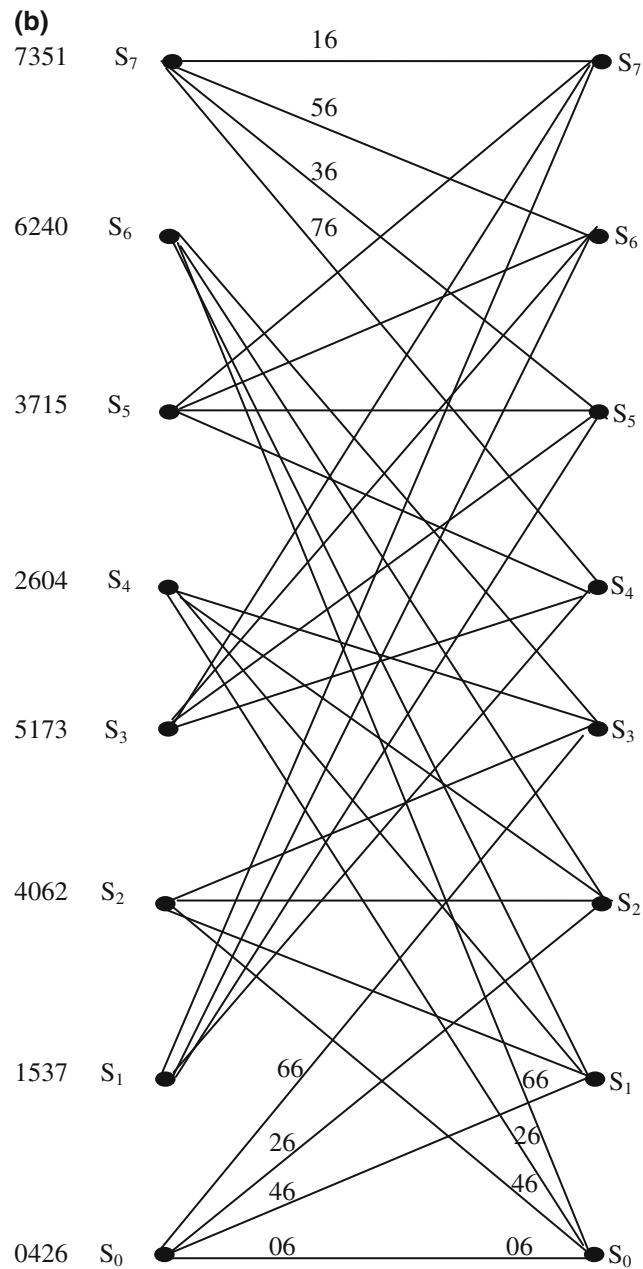
convolutional encoder is used to select from among the third level partitions of 8-PSK, wherein each partition contains only a single signal. Thus, it does not require an uncoded bit to complete the signal selection process.

The 8-state trellis diagram of the 8-PSK TCM encoder is shown in Fig. 7.9b, which has no parallel transitions.

7.3 Decoding TCM

In general, a subconstellation of the signals is assigned to each branch in the TCM trellis. The decoding of the TCM is performed using the soft-decision Viterbi algorithm in two steps.

1. Determine the best signal point within each subset by comparing the received signal to each of the signals allowed for a branch. The signal closest in distance to the received signal is considered as the best signal point and the corresponding branch metric is proportional to the distance between the best signal subset signal point and the received signal.
2. The signal point is selected from each subset and its squared distance is the signal path through the code trellis that has the minimum sum of squared distances from the received sequence.

**Fig. 7.9** (continued)

7.4 TCM Performance Analysis

The performance of a TCM scheme can be evaluated by the following performance measures.

7.4.1 Asymptotic Coding Gain

The coded system performance improvement relative to the uncoded system is measured in terms of asymptotic coding gain. The asymptotic coding gain is defined as follows:

$$\text{Asymtotic coding gain} = \left(\frac{E_{\text{uncoded}}}{E_{\text{coded}}} \right) \left(\frac{d_f^2/\text{coded}}{d_f^2/\text{uncoded}} \right) \quad (7.1)$$

where

- E_{uncoded} is the normalized average received energy of an uncoded system,
- E_{coded} is the normalized average received energy of the coded system,
- $d_f^2/\text{uncoded}$ is the squared minimum free distance of an uncoded system, and
- d_f^2/coded is the squared minimum free distance of the coded system

7.4.2 Bit Error Rate

A general lower bound for BER in an AWGN channel is given as follows:

$$\Psi Q \left(\sqrt{\frac{d_f^2 E_s}{2N_0}} \right) \quad (7.2)$$

The distance structure is independent of the transmitted sequence for the uniform TCM and

$$\Psi = 1$$

A closed form upper bound on BER can be expressed by

$$\text{BER}_{\text{UB}} = T(Y)|_{Y=\exp(-E_s/4N_0)} \quad (7.3)$$

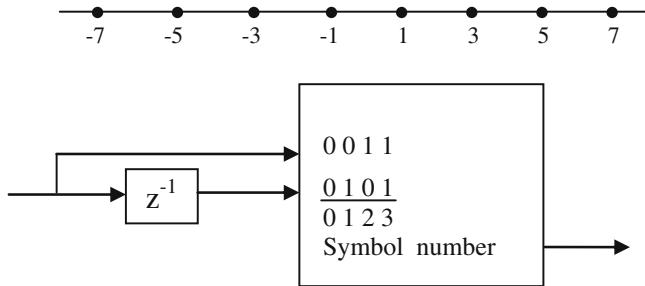


Fig. 7.10 2-state 8-AM TCM encoder

or in a tighter form as

$$\text{BER}_{\text{UB}} = Q\left(\sqrt{\frac{d_f^2 E_s}{2N_0}}\right) \cdot \exp\left(\frac{d_f^2 E_s}{4N_0}\right) T(Y)|_{Y=\exp(-E_s/4N_0)} \quad (7.4)$$

where $T(Y)$ is the transfer function.

The following example illustrates the performance of a TCM scheme.

Example 7.6 Consider the following 2-state encoder and the 8-AM constellation to construct a TCM scheme that provides 2 bits/sec/Hz. Determine the asymptotic coding gain for the TCM relative to the uncoded 4-AM system (Fig. 7.10).

Solution

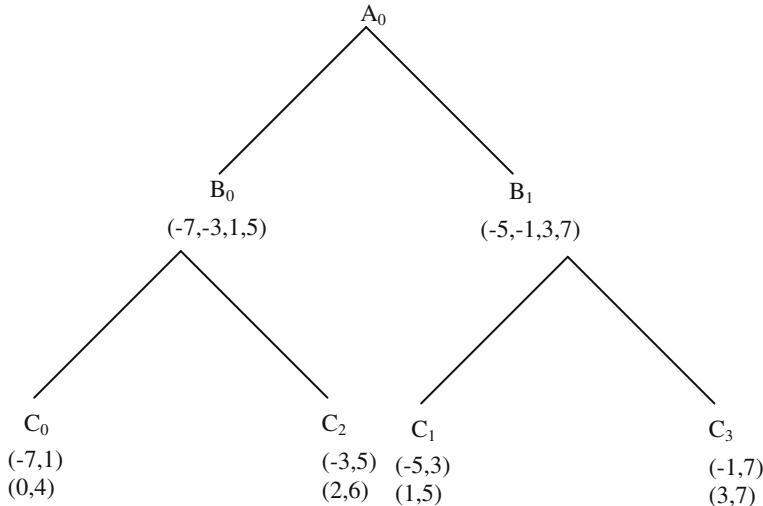
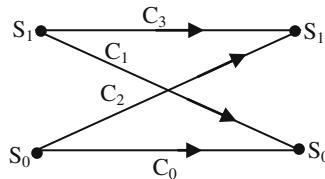
Label	0	1	2	3	4	5	6	7
-------	---	---	---	---	---	---	---	---

For a 2^m -ary AM constellation with the same minimum free distance as BPSK, the normalized average energy is given by average signal energy

$$E = \frac{(4^m - 1)}{m} = \frac{(4^3 - 1)}{3} = \frac{63}{3} = 21$$

or

$$= \frac{1}{8} (1^2 + 3^2 + 5^2 + 7^2 + (-1)^2 + (-3)^2 + (-5)^2 + (-7)^2) = 21$$

**Fig. 7.11** 8-AM set partitioning**8-AM Set partitioning (Fig. 7.11)****Trellis Diagram**

$$d_{f/\text{uncoded}} = 2$$

$$d_{f/\text{uncoded}} = \sqrt{\Delta_0^2 + \Delta_1^2} = \sqrt{2^2 + 4^2} = \sqrt{20}$$

since N-AM signal sets results in

$$E_{\text{uncoded}} = \frac{(4^m - 1)}{3} = \frac{(4^2 - 1)}{3} = 5$$

$$\text{coding gain} = \left(\frac{E_{\text{uncoded}}}{E_{\text{coded}}} \right) \left(\frac{d_{f/\text{coded}}^2}{d_{f/\text{uncoded}}^2} \right) = \frac{5}{21} \frac{20}{4} = 1.19 \approx 0.76 \text{ dB}$$

Example 7.7 Evaluate coding gain and the BER performance of a 4-state 4-PSK TCM with the following Trellis diagram.

The signal flow graph of the trellis diagram of Fig. 7.12 is shown in Fig. 7.13. Now, by using the signal flow graph reduction techniques and Mason's formula, the transfer function can be obtained.

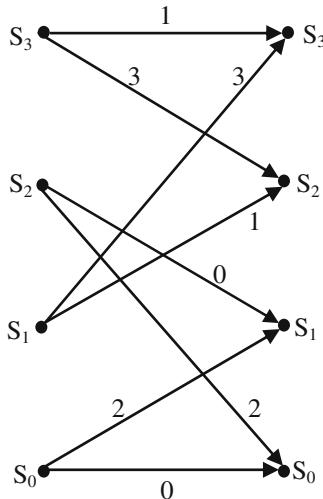


Fig. 7.12 Trellis diagram

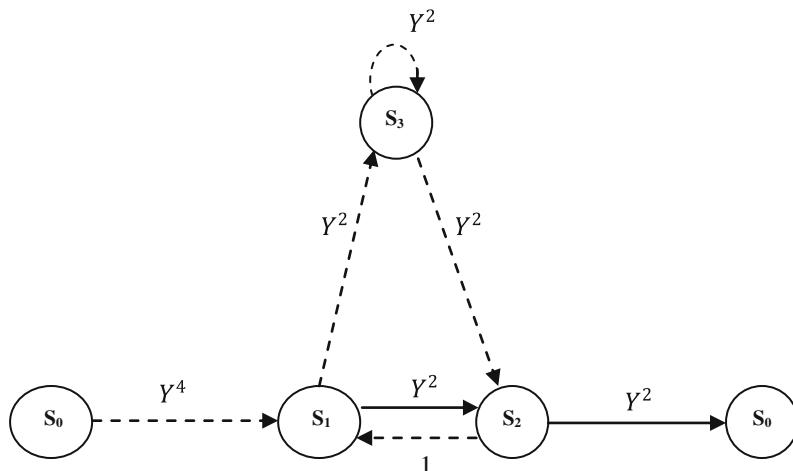
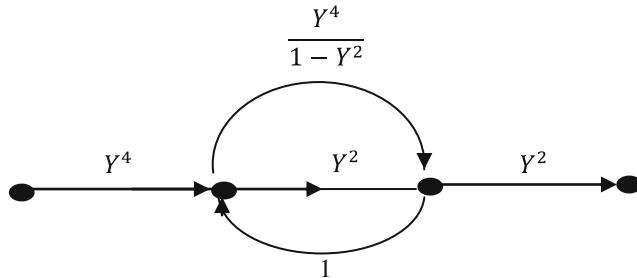


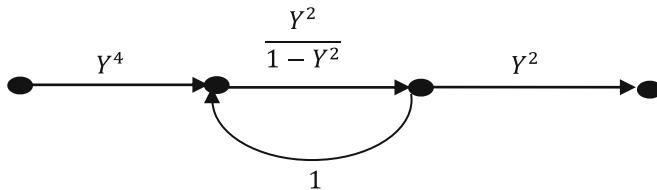
Fig. 7.13 Signal flow graph

By using reduction techniques, the above signal flow graph can be simplified as given below



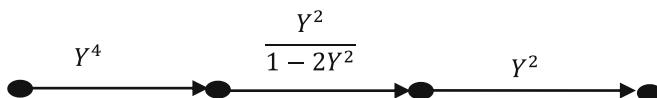
Further, the parallel branches with gains Y^2 and $\frac{Y^4}{1-Y^2}$ can be combined as a single branch with gain

$$Y^2 + \frac{Y^4}{1-Y^2} = \frac{Y^2 - Y^4 + Y^4}{1 - Y^2} = \frac{Y^2}{1 - Y^2} \text{ as follows:}$$



Further, the loop can be replaced by a branch with gain

$$\frac{\frac{Y^2}{1-Y^2}}{1 - \frac{Y^2}{1-Y^2}} = \frac{Y^2}{1 - 2Y^2} \text{ as follows:}$$



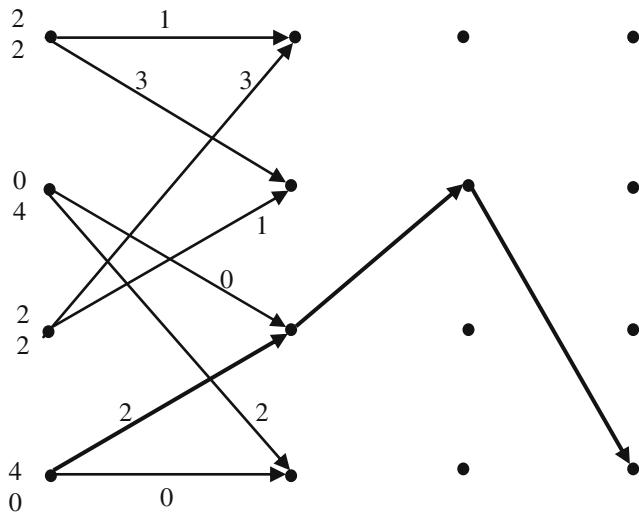


Fig. 7.14 Computation of d_f

Thus, the transfer function is given by

$$T(Y) = Y^4 \frac{Y^2}{1 - 2Y^2} Y^4 = \frac{Y^{10}}{1 - 2Y^2}$$

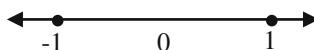
Computation of d_f (Fig. 7.14)

Since there are n_p parallel transitions in this trellis, only non-parallel paths are to be examined to determine minimum free distance of the code. At state S_0 , the symbol path 2 is chosen with the SED of 4, from there it leads us to state 1. From state S_1 , the symbol path 1 with the SED 2 is taken which takes to state S_2 . From state S_2 , we return to state S_0 via the symbol path 2 with SED of 4. There is no other path that can take us back to state S_0 with a smaller total SED.

Hence,

$$\begin{aligned} d_{f/\text{uncoded}}^2 &= \text{sum of the SEDs of the paths shown in bold} \\ &= 4 + 2 + 4 = 10. \end{aligned}$$

Asymptotic coding gain of the 4-state 4-PSK TCM



Since BPSK constellation is with antipodal signals +1 and -1 as shown in above figure. Thus

$$d_{f/\text{uncoded}}^2 = 4$$

Hence, the asymptotic coding gain is given by

$$\text{Asymtotic coding gain} = \left(\frac{E_{\text{uncoded}}}{E_{\text{coded}}} \right) \left(\frac{d_{f/\text{coded}}^2}{d_{f/\text{uncoded}}^2} \right) = \frac{10}{4} = 2.5$$

BER Performance of the 4-state 4-PSK TCM

The transfer function bounded for the BER for the 4-state 4-PSK TCM in an AWGN channel from Eq. (7.3) is given by

$$\begin{aligned} \text{BER} &= T(Y)|_{Y=\exp(-E_b/4N_0)} = \frac{Y^{10}}{1-2Y^2}\Big|_{Y=\exp(-E_b/4N_0)} \\ &= \frac{\exp(-10E_b/4N_0)}{1-2\exp(-2E_b/4N_0)} \end{aligned}$$

The distance structure is independent of transmitted sequence for the uniform TCM and

$$\psi = 1$$

Since $d_f^2 = 10$ for the 4-state 4-PSK TCM, the lower bound for BER from Eq. (7.2) can be written as

$$\text{BER}_{\text{LB}} = Q\left(\sqrt{\frac{5E_b}{N_0}}\right)$$

The following MATLAB program illustrates the BER performance of 4-state 4-PSK TCM in comparison with uncoded BPSK (Fig. 7.15).

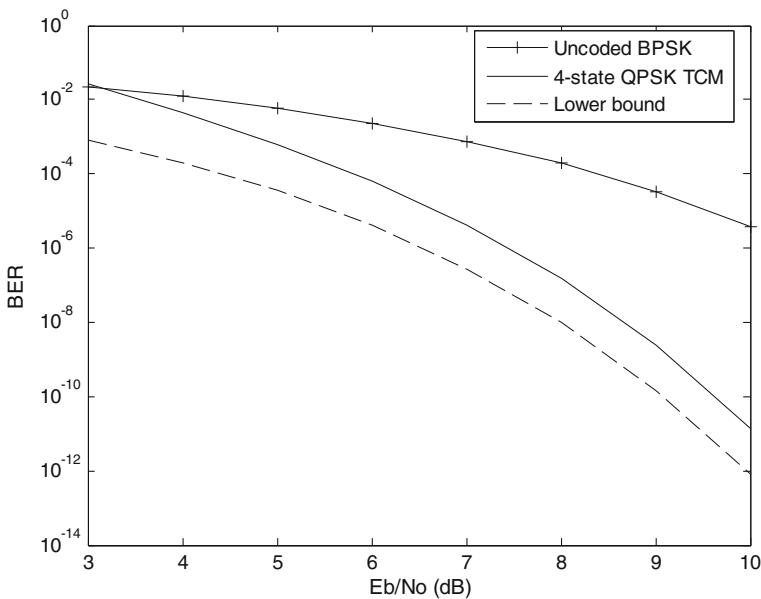


Fig. 7.15 BER performance comparison

Program 7.1 MATLAB program for BER performance of 4-state 4-PSK TCM

```

clear all;clc;
Eb_N0_dB=[3:1:10];
EbN0Lin = 10.^^(Eb_N0_dB/10);
BER_BPSK_AWGN = 0.5* erfc ( sqrt( EbN0Lin ) );
BER_QPSK_LB = 0.5* erfc ( sqrt(2.5* EbN0Lin) );
BER_QPSK =exp(-2.5*EbN0Lin)./(1-2*exp(-0.5*EbN0Lin));
semilogy(Eb_N0_dB,BER_BPSK_AWGN,'-+')
hold on
semilogy(Eb_N0_dB,BER_QPSK ,'-')
semilogy(Eb_N0_dB,BER_QPSK_LB,'--')
legend('Uncoded BPSK ','4-state QPSK TCM','Lower bound');
xlabel('Eb/No (dB)');
ylabel('BER');

```

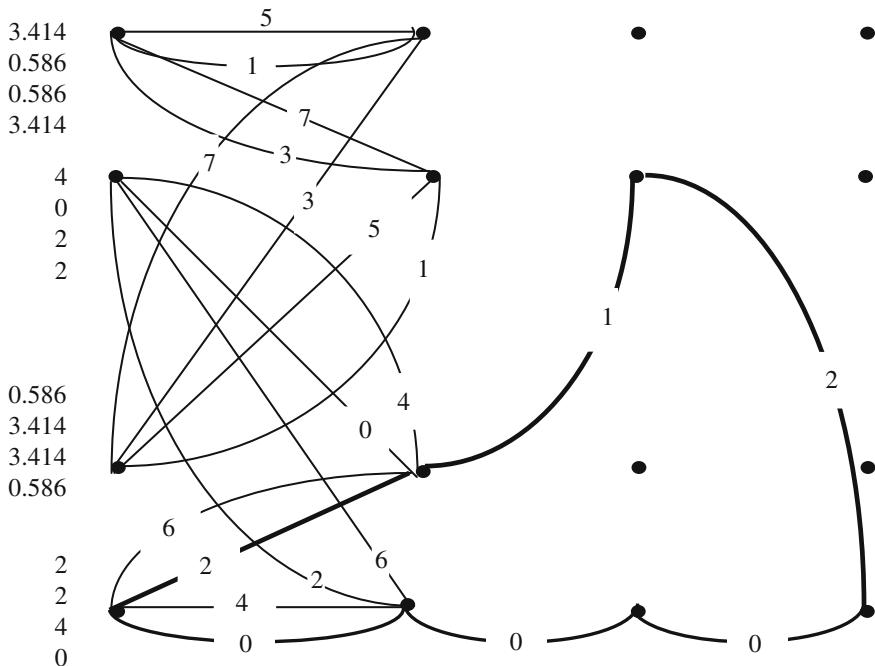


Fig. 7.16 Trellis diagram

Example 7.8 Evaluate coding gain of a 4-state 8-PSK TCM scheme of Example 7.7

Solution

Computation of d_f

In the Trellis diagram shown in Fig. 7.16, symbols originating from a state are replaced with their SEDs.

Since there are n_p parallel transitions in this trellis, both the parallel and the non-parallel transitions are to be examined to determine the minimum free distance of the code. The minimum free distance for the parallel transitions is the minimum free distance for the signals of the partition in the parallel transitions. For this encoder, the minimum free distance for the parallel transitions is the minimum free distance among $\{(0, 4), (1, 5), (2, 6), (3, 7)\}$.

Hence,

$$d_{f/\text{parallel}} = 2$$

To compute $d_{f/\text{parallel}}$, the minimum distance path is found by following from each state the path with the smallest squared distance but not 0. At state S_0 , the symbol path 2 is chosen as it has the SED of 2, from there it leads us to state 1.

From state 1, the symbol path 1 with the SED of 0.586 is taken which takes to state S_0 via the symbol path 2 with SED of 2.

There is no other path that can take us back to state S_0 with a smaller total SED. Thus, the total minimum squared Euclidean distance (MSED) is $2 + 0.586 + 2 = 4.586$ and hence the $d_{f/\text{nonparallel}} = \sqrt{4.586} = 2.14$. The minimum free distance for the TCM encoder is the minimum of $d_{f/\text{parallel}}$ and $d_{f/\text{nonparallel}}$. Thus, the

$$d_{f/\text{coded}} = \min(d_{f/\text{parallel}}, d_{f/\text{nonparallel}}) = \min(2, 2.14) = 2.$$

The minimum free distance for the uncoded 4-PSK is $\sqrt{2}$ and so the $d_f^2 = 2$ for the uncoded 4-PSK. Therefore, the asymptotic coding gain for the 4-state 8-PSK TCM is given by

$$\text{coding gain} = 10 \log_{10} \left(\frac{d_{f/\text{coded}}^2}{d_{f/\text{uncoded}}^2} \right) = 10 \log_{10} \frac{4}{2} = 3.01 \text{ dB}$$

Example 7.9 Evaluate coding gain of the 8-state 8-PSK TCM scheme of Example 7.5.

Solution

Computation of d_f

In the Trellis diagram shown in Fig. 7.17, symbols originating from a state are replaced with their SEDs. Ungerboeck encoder of Example 7.8, we have to compute d_f of this code in order to determine the asymptotic coding gain. The minimum distance path is found by following from each state the path with the smallest squared distance but not 0. At state S_0 , the symbol path 6 is chosen as it has the SED of 2, from there it leads us to state S_3 . From state S_3 , the symbol path 7 with the SED of 0.586 is taken which takes to state S_6 . From state S_6 , we return to state S_0 via the symbol path 6 with SED of 2.

There is no other path that can take us back to state S_0 with a smaller total SED. Thus, the total minimum squared Euclidean distance (MSED) is $2 + 0.586 + 2 = 4.586$, and hence, the $d_f^2 = 4.586$ for the coded system. The minimum free distance for uncoded 4-PSK is $\sqrt{2}$ and so the $d_{\text{free}}^2 = 2$ for the uncoded 4-PSK. Therefore, the asymptotic coding gain for the 8-state 8-PSK TCM is given by

$$\text{coding gain} = 10 \log_{10} \left(\frac{d_{f/\text{coded}}^2}{d_{f/\text{uncoded}}^2} \right) = 10 \log_{10} \frac{4.586}{2} = 3.6 \text{ dB}$$

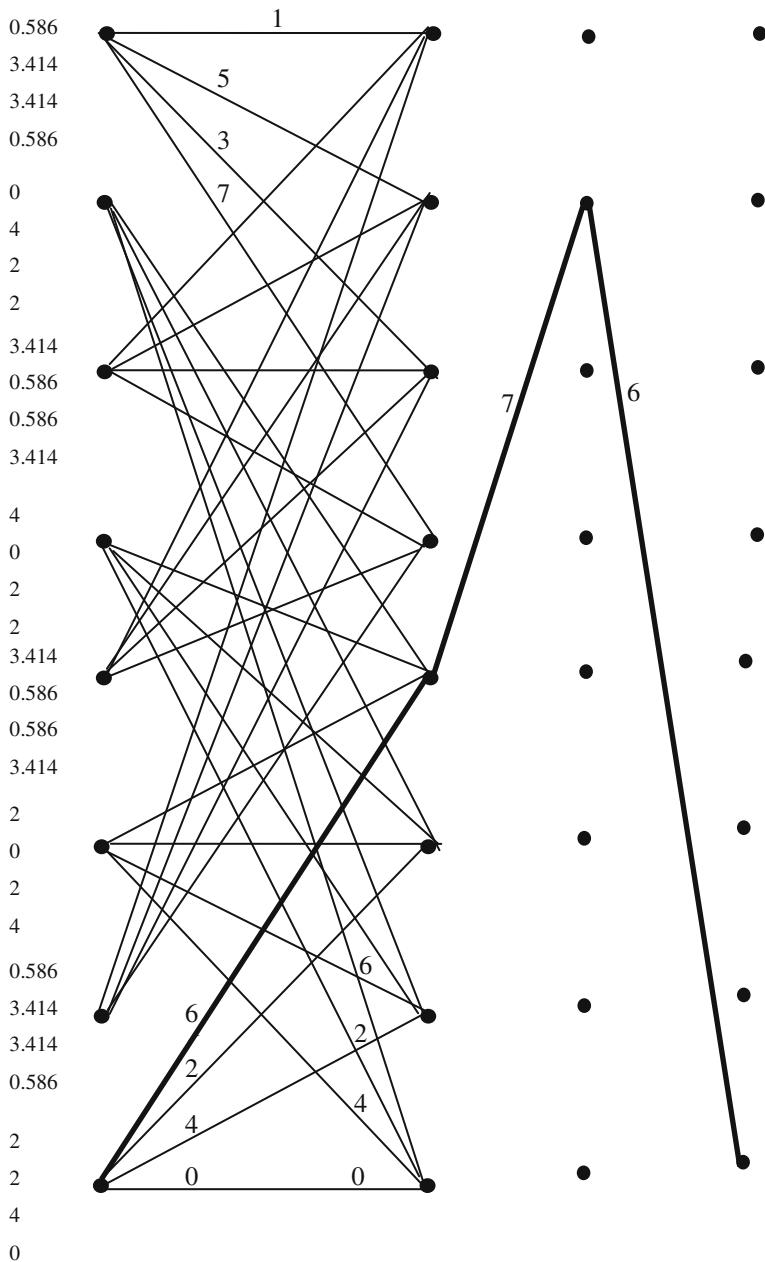


Fig. 7.17 Trellis diagram for Ungerboeck encoder shown in Fig. 7.16 replacing symbols with their SEDs

7.4.3 Simulation of the BER Performance of a 8-State 8-PSK TCM in the AWGN and Rayleigh Fading Channels Using MATLAB

The following MATLAB Program 7.2 and MATLAB functions given in Appendix A are used to simulate the BER performance of Ungerboeck 8-State 8-PSK TCM of Fig. 7.18 in both the AWGN and Rayleigh fading channels.

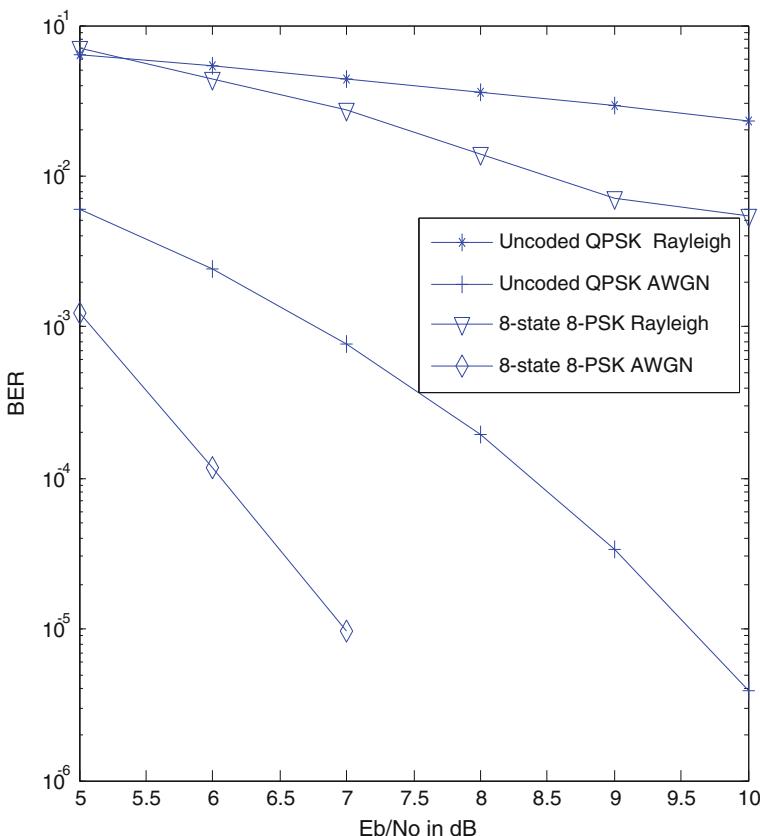


Fig. 7.18 BER performance

Program 7.2

```
%MATLAB program to simulate BER performance of 8-state 8_PSK TCM in
AWGN%and Rayleigh fading channels
clear all; clc; close all;
global n k L nis M N S smap nl bps; global Cw Nes Prs
n=2;k=3;L=3;nis=512;
[Cw, Nes, Prs]=genpoly(n,k,L);%Generation of Trellis%
%Cw=codeword,Prs=previous state,Nes=next state
M=bitshift(1,n); N=nis; S=bitshift(1,L); [smap,bps,nl] = PSKmodSP(k);
Ec=1; EbN0dB=5; i=1; EbN0dB_stop=10;
nis=nis*n;% number of information bits
ncb=nis*k;% number of coded bits
while (EbN0dB <= EbN0dB_stop)
    errorsa=0; bitsa=0; errorsr=0;
    bitsr=0; frame=0;EbN0=10^(EbN0dB/10);
    while (errorsa < 1000 && frame<=100)
        Eb=Ec/((nis*ncb)*bps); %Eb =energy per bit
        N0=Eb*(EbN0^2);%N0=variance
        inb=round(rand(1,nib));%inb=input bits
        symbols =bits2symbol(n,nis,inb);
        [Os,Ts]=tcmenc(symbols,Cw,Nes,smap);%Os=output sym-
        bols,Ts=Transmitted signal
        Rsa=Ts+ sqrt(N0/2)*(randn(size(Ts))+1i*randn(size(Ts))); %Rs=received
        signal in AWGN channel
        Rsr=Ts+sqrt(1/2)*0.3635*(randn(size(Ts))+1i*randn(size(Ts)))+
        sqrt(N0/2)*(randn(size(Ts))+1i*randn(size(Ts))); %Rs=received signal Ray-
        leigh fading channel
        Pra=demodsymbols(Rsa,N0);Prr=demodsymbols(Rsr,N0);
        decbitsa=bitsdecode(Pra);%decoded bits for AWGN
        decbitsr=bitsdecode(Prr);%decoded bits for Rayleigh
        errorsa=sum(decbitsa ~= inb);errorsa=errorsa+errora;
        errorsr=sum(decbitsr ~= inb);errorsr=errorsr+errorr;
        bitsa=bitsa+sum(decbitsa ~= inb)+sum(decbitsa == inb);
        bitsr=bitsr+sum(decbitsr ~= inb)+sum(decbitsr == inb);frame=frame+1;
    end
    EbN0dB=EbN0dB+1;
    berawgn(i)=errorsa/bitsa; berray(i)=errorsr/bitsr; i=i+1; end
figure,
EbN0dB=[ 5 6 7 8 9 10];
berqpskawgn=BERAWGN(EbN0dB, 'psk', 4,'nondiff' );
berqpskfad=BERFADING(EbN0dB, 'psk', 4,1 );
semilogy(EbN0dB,berqpskfad ,'-*')
hold on
semilogy(EbN0dB,berqpskawgn,'-+')
semilogy(EbN0dB,berray,'-v')
semilogy(EbN0dB,berawgn,'-d')
legend('Uncoded QPSK Rayleigh ','Uncoded QPSK AWGN ','8-state 8-PSK
Rayleigh','8-state 8-PSK AWGN'); xlabel('Eb/No in dB');ylabel('BER');
```

The BER performance obtained by using the programs for frame length of 512 bits for both the AWGN and the Rayleigh fading channels is shown in Fig. 7.18. The performance of the TCM in the AWGN channel is much better than the performance in the Rayleigh fading channel. The uncoded QPSK BER performance is also shown in Fig. 7.18 for both AWGN and Rayleigh fading channels, which will serve as reference to compare the performance of the coded modulation scheme in terms of coding gain.

7.5 Turbo Trellis Coded Modulation (TTCM)

Robertson has introduced the concept of the “Turbo Trellis Coded Modulation (TTCM)” in [8] by using two recursive TCM encoders in parallel concatenation. The system overview for TTCM is shown in Fig. 7.19.

7.5.1 TTCM Encoder

TTCM encoder contains the parallel concatenation of two TCM encoders as shown in Fig. 7.20. Let the size of the interleaver be N . The number of modulated symbols per block is $N - n$, with $n = D/2$, where D is the signal set dimensionality. The number of information bits transmitted per block is $N - m$. The encoder is clocked in steps of $n \cdot T$. Where T is the symbol duration of each transmitted $2^{((m+1)/n)}$ -ary symbol. In each step, m information bits are input and n symbols are transmitted, yielding a spectral efficiency of m/n bits per symbol usage. The first TCM encoder normally operates with the original bit sequence while the second encoder works with the interleaved version of the input bit sequence.

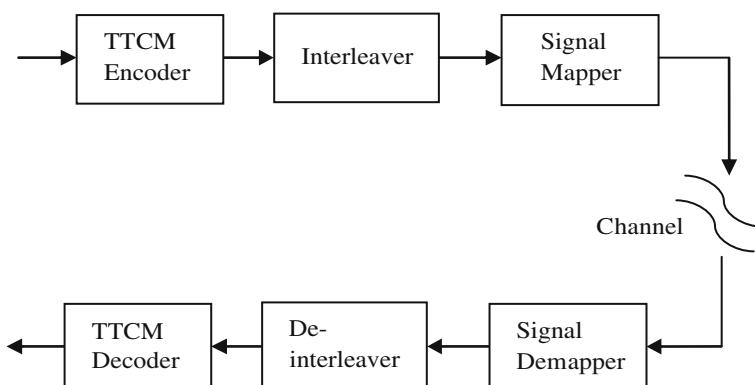
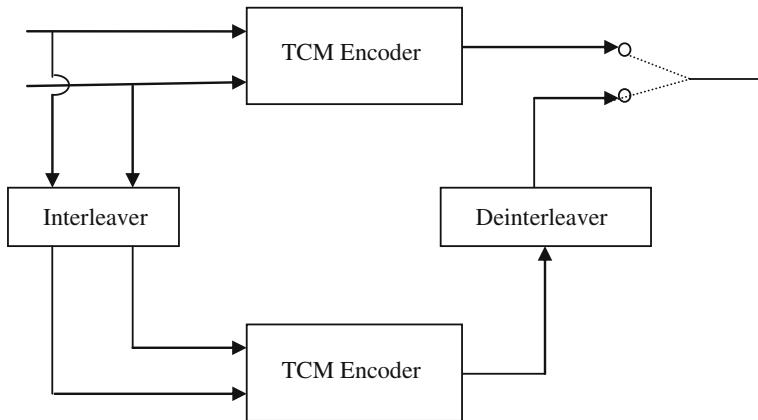
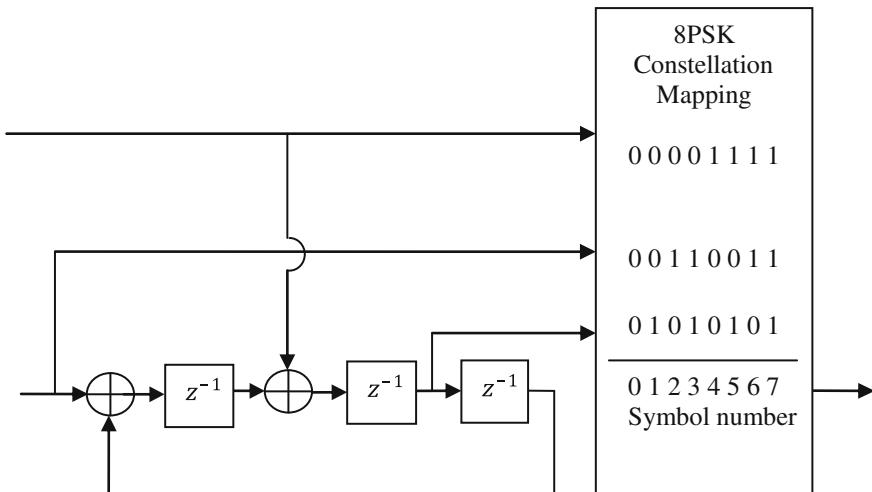


Fig. 7.19 System overview for TTCM

**Fig. 7.20** TTCM encoder structure

A simple example will now serve to clarify the operation of the TTCM encoder for the case of the following 8-state 8-PSK TCM with code rate 2/3 used in the TTCM encoder structure depicted in Fig. 7.21. A sequence of length 6 information bit pairs (00, 01, 11, 10, 00, 11) is encoded by the first encoder to yield the 8-PSK sequence (0, 2, 7, 5, 1, 6). The information bits are interleaved on a pair wise basis using a random interleaver (3, 6, 5, 2, 1, 4) and encoded again into the sequence (6, 7, 0, 3, 0, 4) by the second encoder. We de-interleave the second encoder's output symbols to ensure that the ordering of the two information bits partly defining each symbol corresponds to that of the first encoder, i.e., we now have the sequence (0, 3, 6, 4, 0, 7). Finally, we transmit the first symbol of the first encoder,

**Fig. 7.21** TCM encoder used in TTCM encoder structure

the second symbol of the second encoder, the third of the first encoder, the fourth symbol of the second encoder, and so on (0, 3, 7, 4, 1, 7). Thus, the transmitted signal will be of the symbols (0, 3, 7, 4, 1, 7).

7.5.2 TTCM Decoder

A block diagram of turbo decoder is shown in Fig. 7.22. The TTCM decoder is much similar to that of binary turbo codes, except the difference in the nature of the information passed from one decoder to other decoder, respectively, and the treatment of the very first decoding step. In symbol-based non-binary TTCM scheme, the systematic bit as well as the parity bits are transmitted together as in the form of complex enveloped symbol and cannot be separated from the extrinsic components, since the noise and the fading that effect the parity components will also affects the corresponding systematic components. Hence, in TTCM, the symbol-based information can be split into two components:

1. The a-priori component of the non-binary symbol provided by the alternative decoders.
2. The inseparable extrinsic information as well as the systematic components of the non-binary symbol.

In the first step of TTCM decoding, the received symbols are separated into two different symbols such that upper decoder receives only the symbols encoded by the upper encoder and vice versa for the second decoder. Next, based on log-based BCJR algorithms, each decoder produces its symbol-based probabilities and generates a priori and *extrinsic* information. Next to make sure that each of the decoder does not receive the same information more than once, the decoders provides the corresponding a posteriori which is subtracted with incoming a priori information. By the random interleavers, the extrinsic information is then interleaved/de-interleaved to become a priori information and made to iterate between them. Then, a posteriori information is de-interleaved from the decoder-2 and uses the hard decision for selecting the maximum a-posteriori probability associated with the information word during the final decoding. In the first iteration, the a priori input of the first decoder is initialized with the missing systematic information. Details of the iterative decoder computations are given in the paper by [13].

7.5.3 Simulation of the BER Performance of the 8-State 8-PSK TTCM in AWGN and Rayleigh Fading Channels

The schematic for the TTCM is illustrated in Fig. 7.20. The 8-state 8-PSK TCM encoder shown in Fig. 7.21 is used in this scheme for both the AWGN and Rayleigh fading channels. The source here will be producing some random information bits,

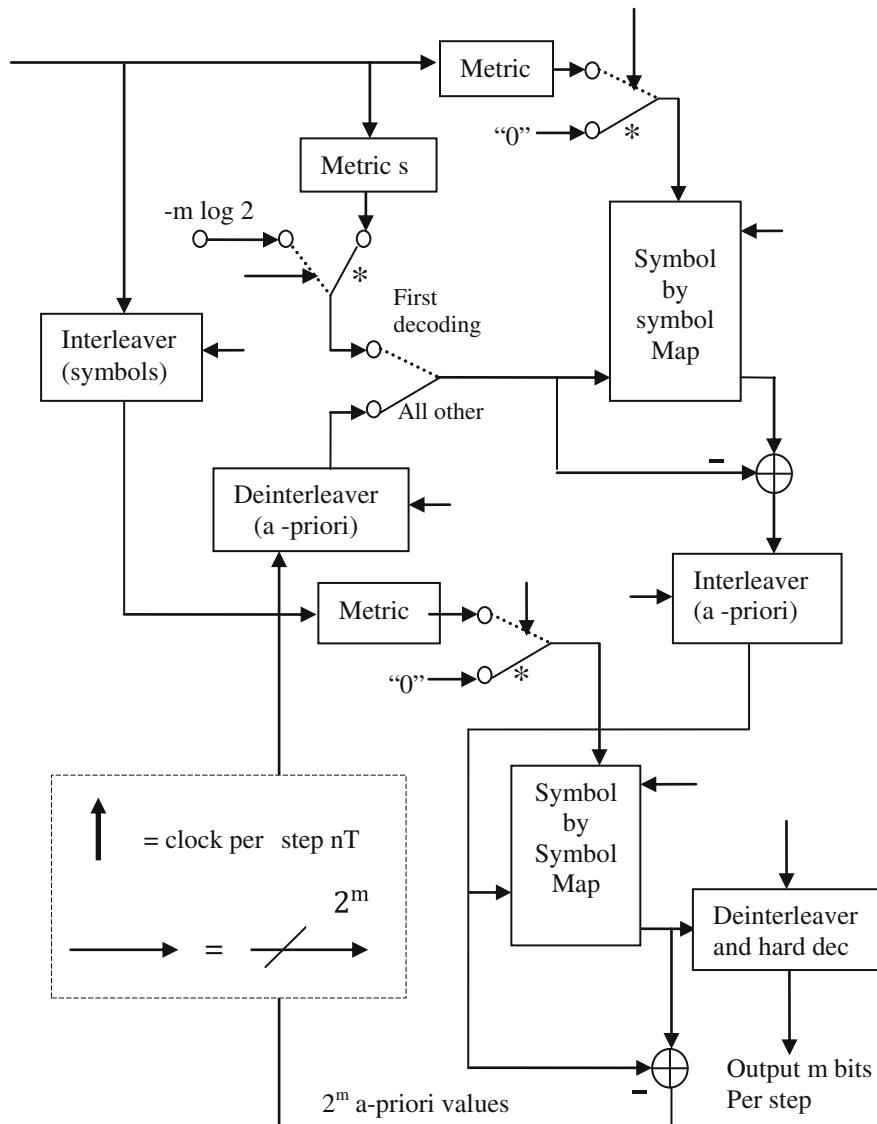


Fig. 7.22 TTCM decoder structure [from Robertson and Worz (1998); © 1998 IEEE.]

which is then encoded by one of the respective encoders and consecutively interleaved by random interleavers. The interleaved bits/symbols are then modulated according to symbol rule for each of the corresponding modulation schemes. The channel discussed here for the coded modulation schemes is that of the AWGN and Rayleigh-distributed flat fading.

The relationship between AWGN and Rayleigh fading channel can be expressed as follows:

$$y_t = \alpha_t x_t + n_t \quad (7.5)$$

where x_t is the transmitted discrete signal and y_t is received signal. α_t is the Rayleigh-distributed fading having an expected squared value of $E(\alpha_t^2)$, and n_t is the complex AWGN having a noise variance of $N_o/2$ per dimension.

For an AWGN channel $\alpha_t = 1$. The receiver side consists of demodulator or de-mapper followed by a de-interleaver and a TCM or TTCM decoder, which has been explained in the previous chapter. A comparison of the BER performance of 8-state 8PSK TTCM in the AWGN and Rayleigh fading channel is shown in Fig. 7.23.

A comparison of the BER performance of 8-state 8-PSK TCM and 8-state 8-PSK turbo TCM in AWGN channel is shown in Fig. 7.24.

An additional coding gain of about 1.7 dB has been achieved by the use of a turbo TCM compared to the conventional TCM, at error rates in the vicinity of 10^{-4} . This means that turbo TCM achieves a performance close to the Shannon information capacity on an AWGN channel.

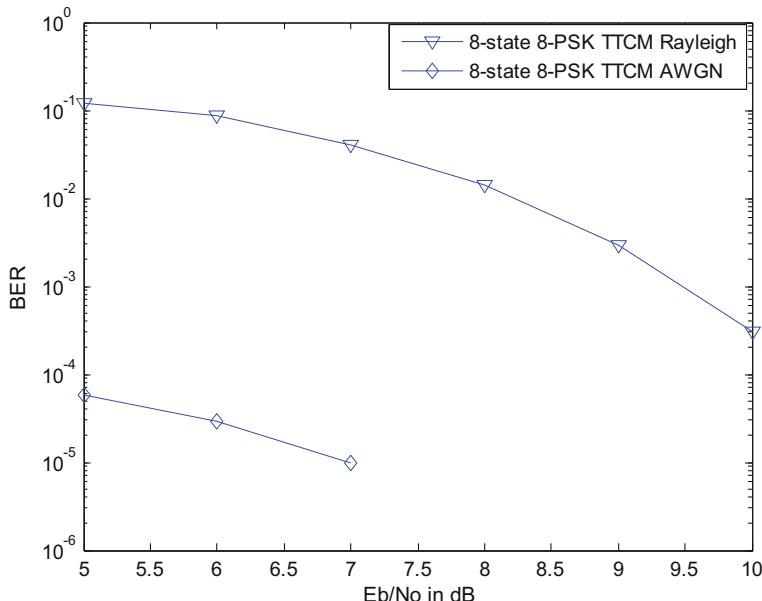


Fig. 7.23 Comparison of the BER performance of the 8-state 8-PSK TTCM in AWGN and Rayleigh fading channel

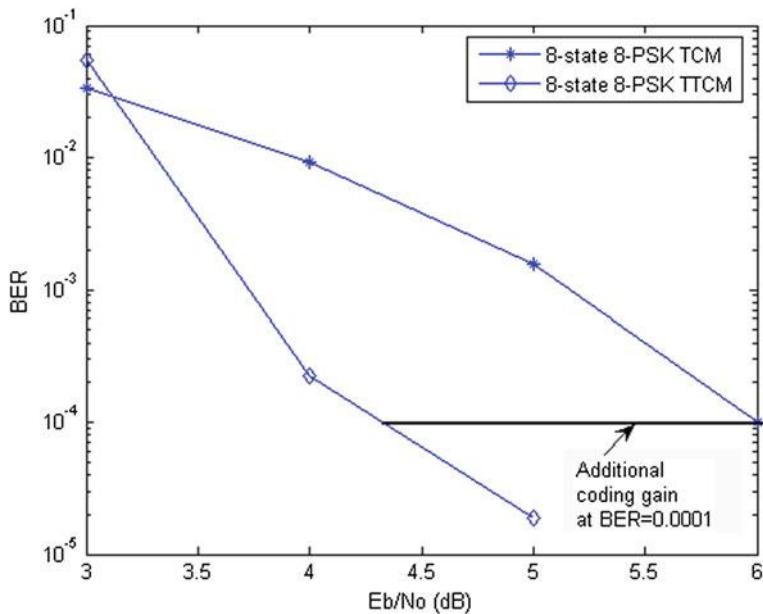


Fig. 7.24 Comparison of the BER performance of 8-state 8-PSK TCM and 8-state 8-PSK turbo TCM in AWGN channel

7.6 Bit-interleaved Coded Modulation

Bit-interleaved coded modulation (BICM) was the idea proposed by Zehavi [9] in order to improve the diversity order of TCM scheme. Zehavi's idea was to render the code's diversity equal to that smallest number of different bits by employing the bit-based interleaving as shown in Fig. 7.25. The bit-based interleaving purpose is:

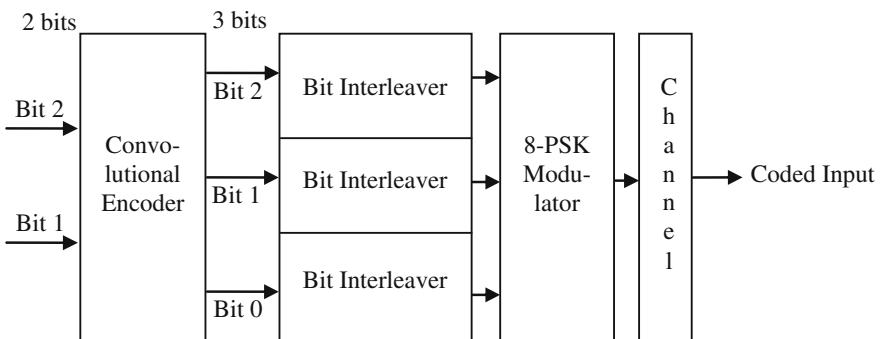


Fig. 7.25 BICM principle

- To maximize the diversity order of the system and to disperse the bursty error introduced by the correlated fading channel.
- To render the bit with respect to the Transmitted symbol uncorrelated or independent of each other.

7.6.1 BICM Encoder

The BICM encoder as shown in Fig. 7.26 uses Paaske's non-systematic eight-state code [10] of a rate 2/3 having a free bit-based hamming distance of four for optimum performance over Rayleigh fading channels. Initially, all the three shift registers contents are set to zero. After the bits are encoded, the each encoded bits will be interleaved by three individual parallel random interleavers of the length equal to each incoming coded bits resulting in a binary vector. These groups of three bits are then mapped to the 8-PSK signal set according to that of Gray Mapping.

The content of the three memory elements represents the state of the encoder at an instant. Denoting the state by $S = (s_2 s_1 s_0)$ as shown in Fig. 7.27, there are eight possible states S_0 to S_7 .

Figure 7.28 shows the trellis diagram with all possible transitions for the encoder shown in Fig. 7.27.

The two-bit information b_1 and b_2 the encoded code word and next states is given by

$$s_0 = b_1; s_1 = s_2; s_2 = b_2 \quad (7.6)$$

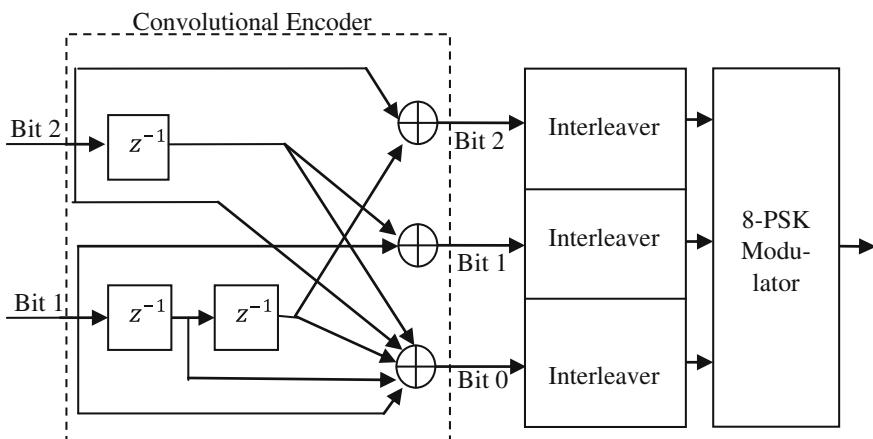


Fig. 7.26 BICM Encoder with Paaske's non-systematic convolutional encoder

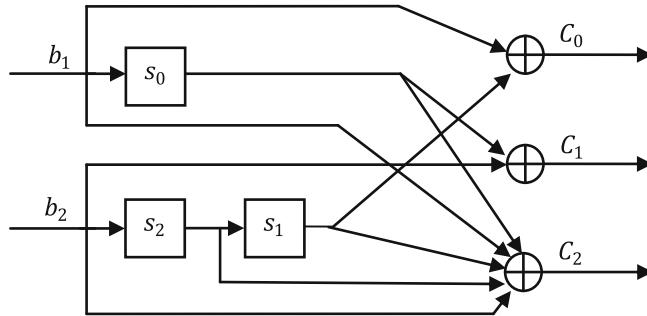


Fig. 7.27 Paaske's non-systematic convolutional encoder

$$C_0 = b_1 \oplus s_1; C_1 = b_2 \oplus s_0; C_2 = b_1 \oplus s_0 \oplus s_1 \oplus s_2 \oplus b_2 \quad (7.7)$$

for the given set of the information bits b_1 and b_2 ; all possible combinations of the code words, present, and next states are tabulated in Table 7.1.

7.6.2 BICM Decoder

The BICM decoder is shown in Fig. 7.29. The received faded noisy signal will be demodulated into six-bit metric associated with three bit positions, each having binary values of 0 and 1, from each received symbol. These bit metrics are then de-interleaved by the three independent bit de-interleavers to form the estimated code words. Then, the BCJR decoder is invoked for decoding these code words to generate the best possible estimate of the original information bits.

7.7 Bit-interleaved Coded Modulation Using Iterative Decoding

Li and Ritcey [11, 12] have proposed a new scheme of bit-interleaved coded modulation using iterative decoding for further improvement of Zehavi's BICM scheme. The BICM-ID employs set partitioning signal labeling system as that of Ungerboeck TCM and introduces soft-decision feedback from the decoder's output to the de-mapper/demodulator input to iterate between them. This is advantageous, since it improves the reliability of the soft information passed to the de-mapper/demodulator at each iteration.

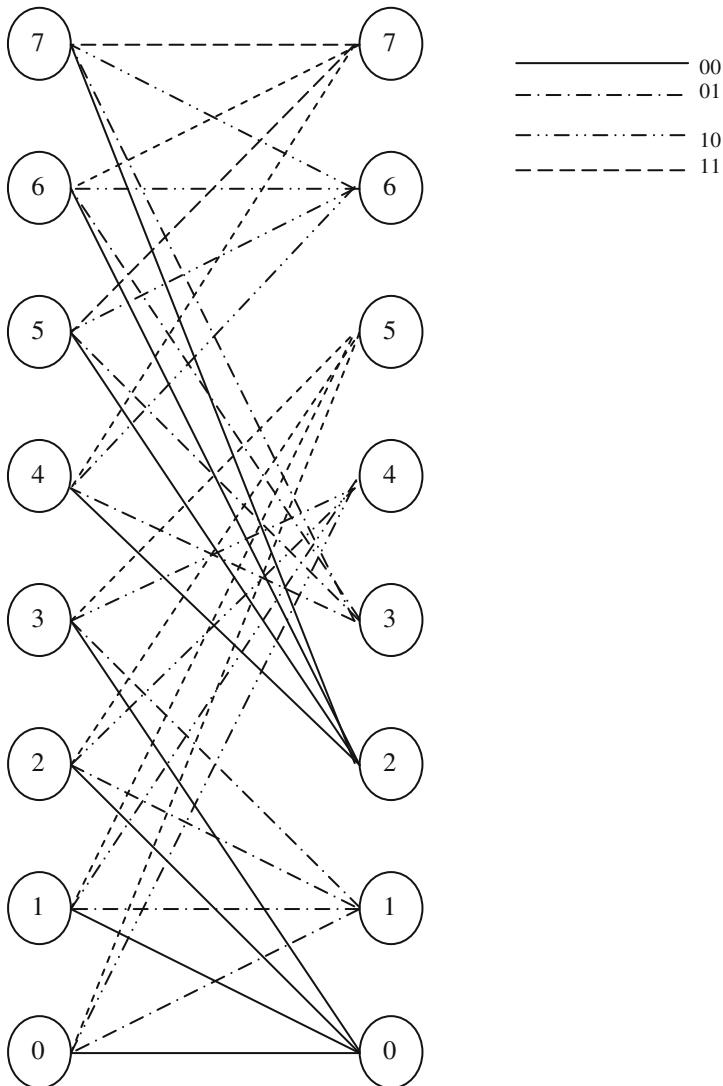


Fig. 7.28 Trellis diagram of the encoder shown in Fig. 7.27

7.7.1 BICM-ID Encoder and Decoder

The BICM-ID's encoder is similar to that BICM encoder explained in Fig. 7.26. The BICM-ID's decoder is almost similar to that of the BICM's encoder except that the iterative process is used to achieve global optimum through a step-by-step local search.

Table 7.1 Code word table for the Paaske's 8-state convolutional encoder shown in Fig. 7.27

Present states ($s_2s_1s_0$)	Information bits							
	00		01		10		11	
	Next state	Code word	Next state	Code word	Next state	Code word	Next state	Code word
000	000	000	001	101	100	110	101	011
001	000	110	001	011	100	000	101	101
010	000	101	001	000	100	011	101	110
011	000	011	001	110	100	101	101	000
100	010	100	011	001	110	010	111	111
101	010	010	011	111	110	100	111	001
110	010	001	011	100	110	111	111	010
111	010	111	011	010	110	001	111	100

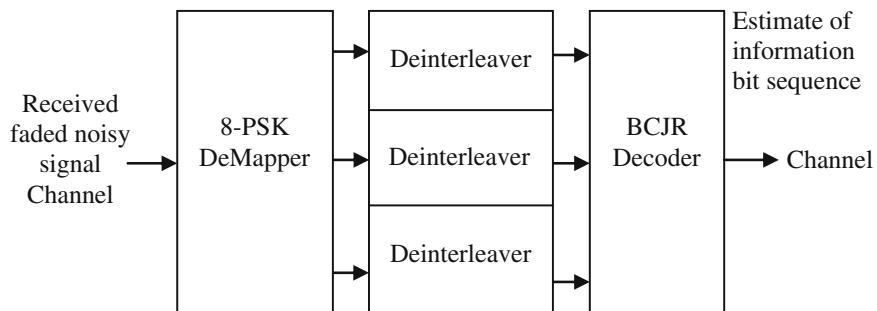
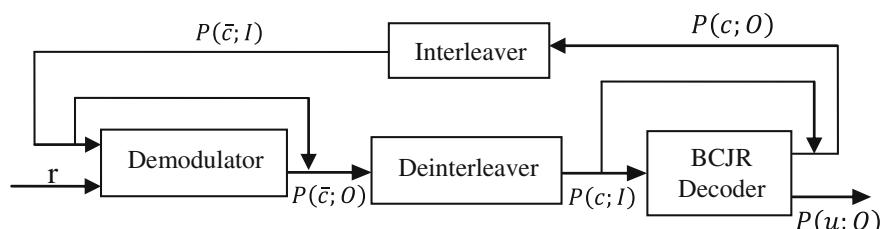
**Fig. 7.29** BICM decoder

Figure 7.30 shows the BICM-ID decoder. At the initial step, the received signal r is demodulated and generates the extrinsic information of the coded bits $P(\bar{c}; O)$ which is interleaved by corresponding de-interleavers to become the a priori information $P(c; I)$ to the log-based BCJR decoders to generate a posteriori bit probabilities for the information and the coded word.

**Fig. 7.30** BICM-ID

On the second pass the extrinsic, a posteriori vectors are interleaved as a priori information to the demodulator assuming that all the bits are independent of each other (by a design of a good interleaver) and will again iterate the above-said steps until the final step is reached. The total a posteriori probabilities of the information bits can be computed to make the hard decisions at the output of the decoder after the each iteration.

The SISO channel decoder uses the MAP algorithm similar to decoding of turbo codes; here, the demodulator and the channel decoder exchange the extrinsic information of the coded bits $P(\bar{c}; O)$ and $P(c; O)$ through an iterative process. After being interleaved, $P(\bar{c}; O)$ and $P(c; O)$ become a priori information $P(c; I)$ and $P(\bar{c}; I)$ at the input of the BCJR decoder and the demodulator, respectively.

7.7.2 *Simulation of the BER Performance of 8-State 8-PSK BICM and BICM-ID in AWGN and Rayleigh Fading Channels*

Simulations are carried out for BICM and BICM-ID with the 8-state 8-PSK encoders. The interleavers used here are three parallel independent random interleavers. The BER performance of BICM in an AWGN channel for three parallel 512 bits interleavers and three parallel 3,000 bits interleavers is shown in Fig. 7.31.

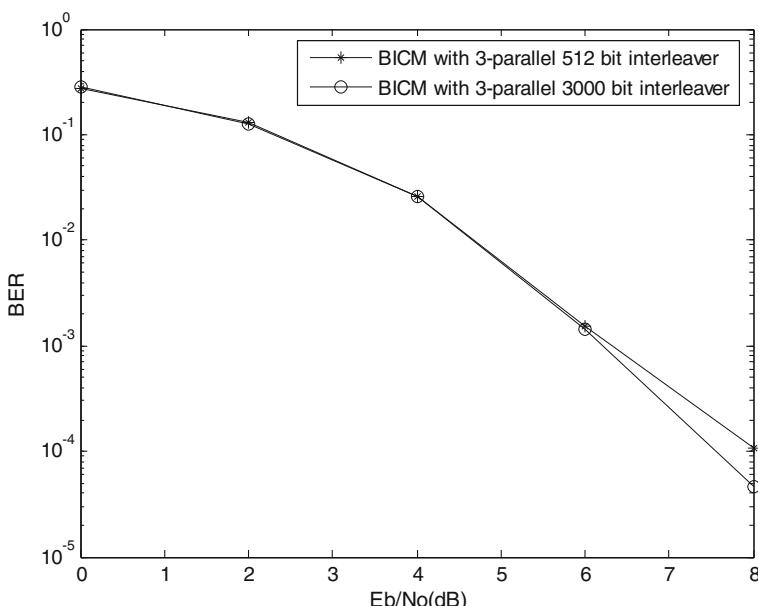


Fig. 7.31 BER performance of BICM in an AWGN channel

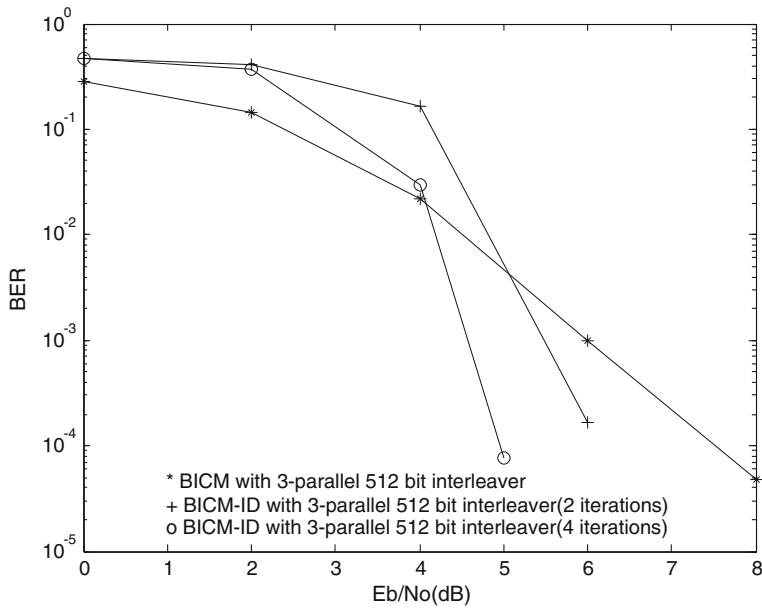


Fig. 7.32 BER performances of BICM and BICM-ID in AWGN channel

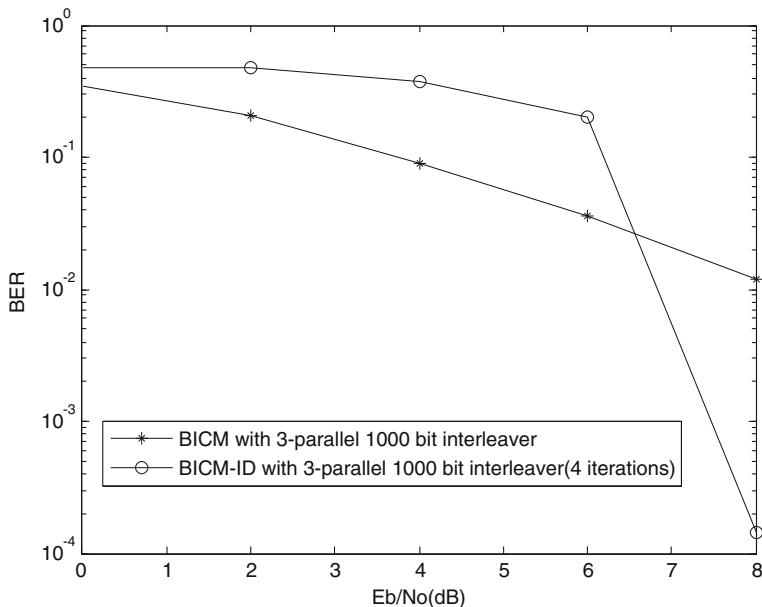
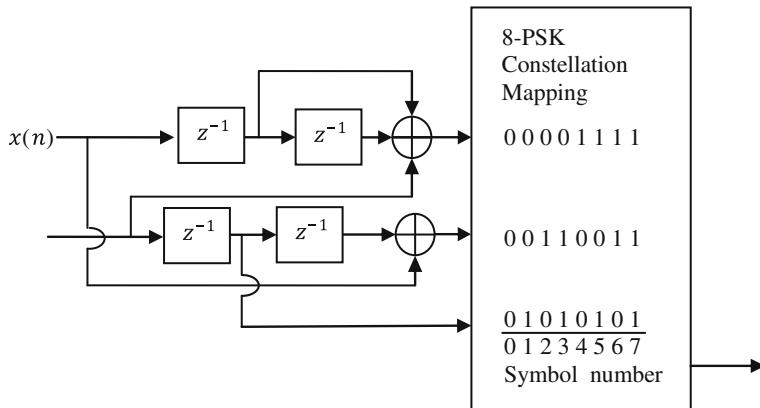


Fig. 7.33 BER performance of BICM and BICM-ID in Rayleigh fading channel

From Fig. 7.31, it is observed that the BER performance of BICM does not significantly depends on the frame length. The BER performance of BICM and BICM-ID (with 2 iterations and 4 iterations) in an AWGN channel for three parallel 512 bits interleavers is shown in Fig. 7.32. It is seen from Fig. 7.32 that the BER performance improves with the increased number of iterations. The BER performance of BICM and BICM-ID (with 4 iterations) in Rayleigh fading channel for three parallel 1,000 bits interleavers is shown in Fig. 7.33.

7.8 Problems

1. Obtain the set partition for 16 QAM.
2. Draw the Trellis diagram for the following 16-state 8-PSK TCM encoder and find the asymptotic coding gain.



3. Compute the output symbols of the 8-state 8-PSK TTCM encoder shown in figure for the input information bit pairs {00, 01, 11, 10, 00, 11}. Let the interleaver be {3, 6, 5, 2, 1, 4}.
4. Construct the schematic diagram for the 8-state 16-QAM TTCM encoder.

Appendix A

```

function [Codeword,Nextstate, Previousstate]= genpoly(k,n,L)
%Init the shift register for the TCM
L=L+1; cpoly=getgenpoly(k,L-1);
H=zeros(k+1,L); K=zeros(1,k+1); D=zeros(1,L);
Codeword=zeros(2^(L-1),2^k); Nextstate=zeros(2^(L-1),2^k);
Previousstate=zeros(2^(L-1),2^k); h=0;
for i=1:L
    h=mod(h,3);
    if (h==0)
        for m=1:k+1
            K(1,m)=mod(cpoly(1,m),10);      cpo-
ly(1,m)=floor(cpoly(1,m)/10);
        end; end
        h=h+1;
        for m=1:k+1
            H(m,i)=mod(K(1,m),2); K(1,m)=floor(K(1,m)/2); end;end
    if (H(1,1)~=1)
        error('TCM: the feedback poly is unacceptable');
    end
    for s=1:2^(L-1)
        h=s-1;
        for i=1:L-1
            D(1,i) = mod(h,2);      h = floor(h/2);   end
            for m=1:2^k
                h=m-1;
                for i=2:k+1
                    K(1,i) = mod(h,2);  h=floor(h/2); end
                    h=D(1,1);
                    for i=2:k
                        h = mod((h+ K(1,i)*H(i,1)),2);      end
                    Codeword(s,m) = 2*(m-1) + h;
                    K(1,1) = h;   c = 1;Nextstate(s,m) = 0; %///* compute new state */
                    for j=1:L-1
                        %/* bit from previous reg. */
                        if(j < (L-1))
                            h=D(1,j+1);
                        else
                            h=0;   end
                            for i=1:k+1      % /* input and feedback bits */
                                h = mod(h +K(1,i)*H(i,j+1),2); end
                                Nextstate(s,m)=Nextstate(s,m)+(h*c);      %/* add to state */
                                c=c*2; end;   end; end
                    for i=1:2^(L-1) %/Compute Previous State/
                    for j= 1:2^k
                        Previousstate((Nextstate(i,j)+1),j)=(i-1); end; end
                
```

```

function [GenPoly] = getgenpoly(k,L)
switch(k)
    case 1
        switch (L)
            case 1
                GenPoly(1,1) = 1; GenPoly(1,2) = 2;
            case 3
                GenPoly(1,1) = 13; GenPoly(1,2) = 6;
            case 4
                GenPoly(1,1) = 23; GenPoly(1,2) = 6;
            case 6
                GenPoly(1,1) = 117; GenPoly(1,2) = 26;
            case 7
                GenPoly(1,1) = 217; GenPoly(1,2) = 110;
            case 8
                GenPoly(1,1) = 427; GenPoly(1,2) = 230;
            case 9
                GenPoly(1,1) = 1017; GenPoly(1,2) = 120;
            otherwise
                error('no generator for such code yet for 4QAM');
        end
    case 2
        switch(L)
            case 3
                GenPoly(1,1) = 11; GenPoly(1,2) = 2; GenPoly(1,3) = 4;
            case 4
                GenPoly(1,1) = 23; GenPoly(1,2) = 2; GenPoly(1,3) = 10;
            case 6
                GenPoly(1,1) = 103; GenPoly(1,2) = 30; GenPoly(1,3) = 66;
            case 7
                GenPoly(1,1) = 277; GenPoly(1,2) = 54; GenPoly(1,3) = 122;
            case 8
                GenPoly(1,1) = 435; GenPoly(1,2) = 72; GenPoly(1,3) = 130;
            otherwise
                error('no generator for such code yet for 8 PSK');
        end
    end
end

```

```

function [smap,bps,nl] =PSKmodSP(varargin)
n=varargin{1};
nl=bitshift(1,n);
M=nl;
smap=zeros(1,nl);
bps=n;
for j=1:M
    smap(1,j)=complex((cos(2*pi*(j-1)/M)),(sin(2*pi*(j-1)/M)));
end

```

```

function [ symbols ] = bits2symbol(word_length,block_lenght,bits_seq)
    N=block_lenght*word_length;
    symbols=zeros(1,block_lenght);
    if (N ~= length(bits_seq))
        error('bits_seq_to_symbol: check bits_seq.length()');
    end
    k=1;
    for j=1:block_lenght
        for i=1:word_length
            symbols(1,j)= symbols(1,j)+ (bits_seq(1,(k))*bitshift(1,(i-1)));
            k=k+1;
        end
    end
end

```

```

function [ Output_symbols,Tx_signals ] = tcmenc(symbols,Codeword,
Nextstate,Smap)
    Output_symbols=zeros(1,length(symbols));
    s=1;
    for i=1:length(Output_symbols)
        m=symbols(1,i)+1;
        Output_symbols(1,i)=Codeword(s,m);
        s=Nextstate(s,m)+1;
    end
    Tx_signals=zeros(1,length(Output_symbols));
    for i=1:length(Tx_signals)
        Tx_signals(1,i)=Smap(Output_symbols(1,i)+1);
    end
end

```

```

function [ Pr ] = demodsymbols(varargin)
global M N smap nl nis;
recevied_signals= varargin{1};
sigma= varargin{2};
%Channel Matrix
Pr=zeros(N,2*M);
for k=1:nis
    for i=1:nl
dist=hypot((real(recevied_signals(1,k))- real(smap(1,i))), (imag (recevied_signals(1,k))- imag(smap(1,i))));
Pr(k,i)=-(dist*dist)/(sigma);
    end
end
end

```

```

function [ b_decoded_bits ] = bitsdecode(Pr)
    global M N S Cw Nes Prs MINF Interleave_mode_in;
    MINF=-100000; %// define Minimum Log probability (-infinity)
    Apr=zeros(N,M); Apo=zeros(N,M); OPr=zeros(N,2*M); Ip1=zeros(S,M,N);
    if (strcmp(Interleave_mode_in,'ON'))
        y=de_interleave(Pr); Pr=y; end
    for j=1:N
        for m=1:M
            Apr(j,m)=-log(M); for i=1:S
                Ip1(i,m,j)=Pr(j,Cw(i,m)+1); end; end; end
            Alpha=zeros(N+1,S+1);Beta=zeros(N+1,S+1); for i=2:S
                Alpha(1,i)=MINF; /* compute Alpha */ end
            for k=2:(N+1)
                max=MINF; for i=1:S
                    Alpha(k,i)=jacobianlog(Alpha(k-1,Prs(i,1)+1) + Ip1(Prs(i,1)+1,1,(k-1))+Apr(k-1,1),Alpha(k-1,Prs(i,2)+1) + Ip1(Prs(i,2)+1,2,(k-1))+Apr(k-1,2));
                    for m=3:M
                        Alpha(k,i)=jacobianlog(Alpha(k,i),Alpha((k-1),Prs(i,m)+1)+Ip1(Prs(i,m)+1,m,(k-1))+Apr(k-1,m)); end
                        if (max < Alpha(k,i))
                            max=Alpha(k,i); end; end
                    for i=1:S
                        Alpha(k,i)=Alpha(k,i)-max;
                    end end for i=1:S
                    Beta(N+1,i)=0; /* compute beta */
                end for k=N:-1:1
                max=MINF;for i=1:S
                    Beta(k,i)=jacobianlog(Beta(k+1,Nes(i,1)+1) + Ip1(i,1,k)+Apr(k,1),Beta(k+1,Nes(i,2)+1) + Ip1(i,2,k)+Apr(k,2));
                    for m=3:M
                        Beta(k,i)=jacobianlog(Beta(k,i),Beta(k+1,Nes(i,m)+1)+Ip1(i,m,k)+Apr(k,m));
                    end
                    if (max < Beta(k,i))
                        max=Beta(k,i); end; end
                    for i=1:S
                        Beta(k,i)=Beta(k,i)-max;
                    end end /* compute apo */
                end for k=1:N
                max=MINF; max_QPr=MINF;
                for m=1:(2*M)
                    OPr(k,m)=MINF;
                End for m=1:M
                    Apo(k,m)=MINF; for i=1:S
                        abc=Alpha(k,Prs(i,m)+1)+Beta(k+1,i)+Ip1(Prs(i,m)+1,m,k);
                    Apo(k,m)=jacobianlog(Apo(k,m),abc);
                    OPr(k,Cw(Prs(i,m)+1,m)+1)=jacobianlog(OPr(k,Cw(Prs(i,m)+1,m)+1),abc+Apr(k,m));
                end
                Apo(k,m)=Apo(k,m)+Apo(k,m); if (max < Apo(k,m))
                    max=Apo(k,m);
                end end
                for m=1:M
                    Apo(k,m)=Apo(k,m)- max;
                end end
                decoded_symbols=decode_symbols(Apo)
                b_decoded_bits=symbol2bits(decoded_symbols); end

```

```
function [ r ] = jacobianlog( x,y )
%/*----- jacobian logarithm -----*/
if (x > y)
    r=x + log ( 1 + exp(y-x));
else
    r=y + log ( 1 + exp(x-y));
end
end
```

```
function [ output_symbols ] = decode_symbols(Apo)
global N M
output_symbols=zeros(1,N);
for k=1:N
    i=0;
    max=Apo(k,1);
    for m=2:M
        if (Apo(k,m) > max)
            max=Apo(k,m);
            i=m-1;
        end
    end
    output_symbols(1,k)=i;
end
end
```

```
function [ bits ] = symbol2bits( symbols)
global n;
N=n*length(symbols);
bits=zeros(1,N);
if(N ~= length(bits))
    msgbox(N,length(bits))
end
h=1;
for j=1:length(symbols)
    for i=1:n
        bits(h)=bitand(bitshift(symbols(1,j),-(i-1)),1);
        h=h+1;
    end
end
end
```

References

1. Ungerboeck, G.: Channel coding with multilevel/phase signals. *IEEE Trans. Inf. Theory* **IT-28**, 55–67 (1982)
2. Forney Jr., G.D., Gallager, R.G., Lang, G.R., Longstaff, F.M., Qureshi, S.U.: Efficient modulation for band-limited channels. *IEEE Trans. Sel. Areas Commun.* **SAC-2**, 632–647 (1984)
3. Wei, L.F.: Rotationally invariant convolutional channel coding with expanded signal space—Part I: 180 degrees. *IEEE Trans. Sel. Areas Commun.* **SAC-2**, 659–672 (1984)
4. Wei, L.F.: Rotationally invariant convolutional channel coding with expanded signal space—Part II: nonlinear codes. *IEEE Trans. Sel. Areas Commun.* **SAC-2**, 672–686 (1984)
5. Calderbank, A.R., Mazo, J.E.: A new description of trellis codes. *IEEE Trans. Inf. Theory* **IT-30**, 784–791 (1984)
6. CCITT Study Group XVII, Recommendation V.32 for a family of 2-wire, duplex modems operating on the general switched telephone network and on leased telephone-type circuits. Document AP VIII-43-E, May 1984
7. CCITT Study Group XVII, Draft recommendation V.33 for 14400 bits per second modem standardized for use on point-to-point 4-wire leased telephone-type circuits. Circular No. 12, COM XVII/YS, Geneva, 17 May 1985
8. Robertson, P.: Bandwidth-efficient turbo trellis-coded modulation using punctured component codes. *IEE J. Sel. Areas Commun.* **16**, 206–218 (1998)
9. Zehavi, E.: 8-PSK trellis codes for Rayleigh fading channel. *IEEE Trans. Commun.* **40**, 873–883 (1992). [3, 23]
10. Lin, S., Constello Jr., D.: Error control coding: fundamentals and applications. Prentice Hall, Englewood Cliffs (1982). ISBN 013283796X
11. Li, X., Ritcey, J.A.: Bit interleaved coded modulation with iterative decoding. *IEEE Commun. Lett.* **1**, 169–171 (1997)
12. Li, X., Ritcey, J.A.: Trellis coded modulation with bit interleaving and iterative decoding. *IEEE J. Sel. Areas. Commun.* **17**, 715–724 (1999)
13. Robertson, P., Worz, P.: Bandwidth-Efficient Turbo Trellis-coded modulation using punctured component codes. *IEEE J. Sel. Areas. commun.* **16**, 206–218 (1998)

Chapter 8

Low Density Parity Check Codes

Low density parity check (LDPC) codes are forward error-correction codes, invented by Robert Gallager in his MIT Ph.D. dissertation, 1960. The LDPC codes are ignored for long time due to their high computational complexity and domination of highly structured algebraic block and convolutional codes for forward error correction. A number of researchers produced new irregular LDPC codes which are known as new generalizations of Gallager's LDPC codes that outperform the best turbo codes with certain practical advantages. LDPC codes have already been adopted in satellite-based digital video broadcasting and long-haul optical communication standards. This chapter discusses LDPC code properties, construction of parity check matrix for regular and irregular LDPC codes, efficient encoding and decoding of LDPC codes, and performance analysis of LDPC codes.

8.1 LDPC Code Properties

LDPC code is a linear error correction code that has a parity check matrix H , which is sparse, i.e., with less nonzero elements in each row and column. LDPC codes can be categorized into regular and irregular LDPC codes. When the parity check matrix $H_{(n-k) \times k}$ has the same number w_c of ones in each column and the same number w_r of ones in each row, the code is a regular (w_c, w_r) . The original Gallager codes are regular binary LDPC codes. The size of H is usually very large, but the density of nonzero element is very low. LDPC code of length n can be denoted as an (n, w_c, w_r) LDPC code. Thus, each information bit is involved with w_c parity checks, and each parity check bit is involved with w_r information bits. For a regular code, we have $(n - k)w_r = nw_c$, thus $w_c < w_r$. If all rows are linearly independent, the code rate is $\frac{(w_r - w_c)}{w_r}$; otherwise, it is k/n . Typically, $w_c \geq 3$ a parity check matrix with minimum column weight w_c will have a minimum distance $d_{\min} \geq w_c + 1$.

Electronic supplementary material The online version of this chapter (doi:[10.1007/978-81-322-2292-7_8](https://doi.org/10.1007/978-81-322-2292-7_8)) contains supplementary material, which is available to authorized users.

When $w_c \geq 3$, there is at least one LDPC code whose minimum distance d_{\min} grows linearly with the block length n [1]; thus, a longer code length yields a better coding gain. Most regular LDPC codes are constructed with w_c and w_r on the order of 3 or 4.

8.2 Construction of Parity Check Matrix H

8.2.1 Gallager Method for Random Construction of H for Regular Codes

In this method, the transpose of regular (n, w_c, w_r) parity check matrix H has the form

$$H^T = \left[H_1^T, H_2^T, \dots, H_{w_c}^T \right] \quad (8.1)$$

The matrix H_1 has n columns and n/w_r rows. The H_1 contains a single 1 in each column and contains 1s in its i th row from column $(i-1)w_r + 1$ to column iw_r . Permuting randomly the columns of H_1 with equal probability, the matrices H_2 to H_{w_c} are obtained.

The parity check matrix for $(n = 20, w_c = 3, w_r = 4)$ code constructed by Gallager [1] is given as

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (8.2)$$

The following MATLAB program can be used to generate Gallager regular parity check matrix H with different code rates.

Program 8.1 MATLAB program to generate Gallager regular parity check matrix

```
% MATLAB program to generate Gallager regular parity check matrix H
clear all;clc;
c = input(' enter the Length of parity check bits = ');
n = input(' enter the number of bits in the codeword= ');
wc = input(' enter the number of ones in each column= ');
wr=(n.*wc)/c; %the number of ones in each row
H=zeros(c,n); %generate the empty matrix and start assigning the 1s
j=1;
jj=wr;
for i = 1:c./wc
    H(i,jjj)=1;
    j=j+wr;
    jj=(i.*wr)+wr;
end
for i=1:wc-1
    for ii=1:n
        colind = (round(rand(1) * (n-1 )))+1;
        rCol=H(1:c./wc,colind);
        H((i.*c./wc))+1 : ((i.*c./wc))+1 + (c./wc)-1,ii )=rCol;
        end
    end
```

8.2.2 Algebraic Construction of H for Regular Codes

The construction of the parity check matrix H using algebraic construction as follows [2, 3]. Consider an identity matrix I_a where $a > (w_c - 1)(w_r - 1)$ and obtain the following matrix by cyclically shifting the rows of the identity matrix I_a by one position to the right.

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 \end{bmatrix} \quad (8.3)$$

Defining $A^0 = I_a$ the parity check matrix H can be constructed as

$$H = \begin{bmatrix} A^0 & A^0 & A^0 & \dots & A^0 \\ A^0 & A^1 & A^2 & \dots & A^{(w_r-1)} \\ A^0 & A^2 & A^4 & \dots & A^{2(w_r-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A^0 & A^{(w_c-1)} & A^{2(w_c-1)} & \dots & A^{(w_c-1)(w_r-1)} \end{bmatrix} \quad (8.4)$$

The constructed H matrix has $w_c a$ rows and $w_r a$ columns, and it is of a regular $(w_r a, w_c, w_r)$ having the same number of w_r ones in each row and the same number of w_c ones in each column. It is four-cycle free construction. The algebraic LDPC codes are easier for decoding than random codes. For intermediate n , well-designed algebraic codes yield a low BER [4, 5].

Example 8.1 Construct H matrix with $w_c = 2$ and $w_r = 3$ using algebraic construction method.

Solution Since $(w_c - 1)(w_r - 1) = 2$

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix};$$

$$H = \begin{bmatrix} A^0 & A^0 & A^0 \\ A^0 & A^1 & A^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

8.2.3 Random Construction of H for Irregular Codes

In the random construction of the parity check matrix H , the matrix is filled with ones and zeros randomly satisfying LDPC properties. The following MATLAB program generates rate 1/2 irregular parity check matrix H with ones distributed uniformly at random within the column.

Program 8.2 MATLAB program to generate rate 1/2 irregular parity check matrix H

```
%MATLAB program to generate rate 1/2 irregular parity check matrix H
% with 1s distributed uniformly at random within column
clear all;clc;
p = input(' enter the Length of parity check bits = ');
n = input(' enter the number of bits in the codeword= ');
col_ones= input(' enter the number of ones per column= ');
for i = 1:n
    ones_col(:, i) = randperm(p)';
end
r = reshape(ones_col(1:col_ones, :), n*col_ones, 1);
temp = repmat([1:n], col_ones, 1);
c = reshape(temp, n*col_ones, 1);
H= full(sparse(r, c, 1, p, n));% Creates sparse matrix H
for i = 1:p
    cr = randperm(n);
    if length(find(r == i)) == 0
        H(i, cr(1)) = 1;% adds two 1s if row has no 1
        H(i,cr(2)) = 1;
    elseif length(find(r == i)) == 1
        H(i, cr(1)) = 1;% adds one 1 if row has only one 1
    end
end % for i
```

An example of parity check matrix for irregular LDPC code is

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \quad (8.5)$$

8.3 Representation of Parity Check Matrix Using Tanner Graphs

The Tanner graph of the parity check matrix H is a bipartite graph. It has bit nodes or variable nodes (VN) equal to the number of columns of H , and check nodes (CNs) equal to the number of rows of H . If $H_{ji} = 1$, i.e., if variable i participates in the j th parity check constraint, then check node j is connected to variable node i .

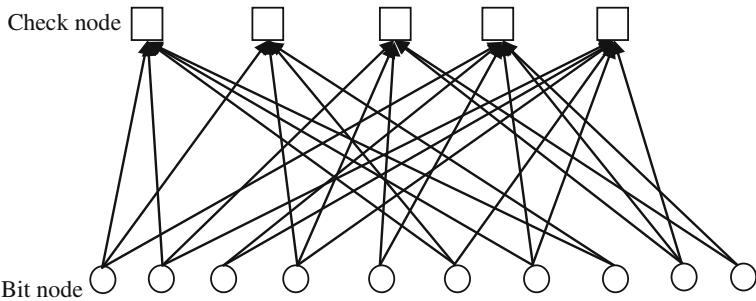


Fig. 8.1 Tanner graph of H matrix of Example 8.2

Example 8.2 Construct Tanner graph for the following parity check matrix

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Solution The H matrix has 10 columns and 5 rows. Hence, the associated tanner graph with 10 bit nodes and 5 CNs is shown in Fig. 8.1.

8.3.1 Cycles of Tanner Graph

Consider the following parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \quad (8.6)$$

The Tanner graph of the H matrix is shown in Fig. 8.2. A sequence of connected nodes starting and ending at the same node with no node more than once is a cycle of a Tanner graph. The number of edges in a cycle is called cycle length and the smallest size of the cycle in a graph represents the girth of the graph. Cycles of length 4 situations arise where pairs of rows share 1s in a particular pair of columns of the above H matrix. A cycle of length 4 is shown in bold in Fig. 8.2.

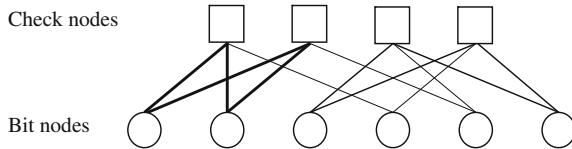


Fig. 8.2 A Tanner graph with a cycle of length 4

The minimum lower bound distance for four-cycle-free (w_c, w_r) regular LDPC code parity check matrix with girth g is given by [6]

$$d_{\min} \geq \begin{cases} 1 + w_c + w_c(w_c - 1) + w_c(w_c - 1)^2 + \cdots + w_c(w_c - 1)^{(g-6)/4} & \text{for odd } g/2 \\ 1 + w_c + w_c(w_c - 1) + w_c(w_c - 1)^2 + \cdots + w_c(w_c - 1)^{\frac{g-8}{4}} & \text{otherwise} \end{cases} \quad (8.7)$$

Thus, the minimum distance can be increased by increasing the girth or the column weight.

8.3.2 Detection and Removal of Girth 4 of a Parity Check Matrix

If the Tanner graph of a parity check matrix contains no loops, then this decoding is quickly computable. Unfortunately, LDPCs have loopy graphs, and so the algorithm needs to be repeatedly iterated until it converges to a solution. The effect of girth on the performance of LDPC codes can be reduced by choosing the codes having Tanner graphs with longer girths. However, longer girths are not helpful for finite length codes. A girth of 6 is sufficient, and hence, the removal of girth 4 is a required. A lemma in [7] states that the H matrix has no girth 4, if and only if all the entries of the matrix $[H^T H]$ are 1s except the diagonal line.

A standard approach [8] is to search the parity check matrix H forming a rectangle of four 1s in the matrix. Eliminating the rectangle by reshuffling some elements around while preserving the other relevant properties of the matrix is equivalent to removing a girth 4 from the Tanner graph.

The detection and removal of girth 4 is illustrated through the following numerical example using MATLAB.

Example 8.3 Consider the following (10, 3, 6) regular parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

The following MATLAB program can be used for detection and removal of girth of the given H matrix.

Program 8.3 MATLAB program for detection and removal of girth 4 of a given parity check matrix H

```
clear all;clc;
H=[1 1 1 0 1 1 0 0 0;0 0 1 1 1 1 1 0 0;0 1 0 1 0 1 0 1 1;1 0 1 0 1 0 0 1 1
1;1 0 0 1 0 1 1];
[row col]=size(H);
Gt=H'*H;
for i=1:row
Gt(i,i)=0;
end
figure(1),
mesh(Gt)% shows presence or absence of girth 4
d=find(Gt==2);
if(d~=0)
%removal of girth 4
for i = 1:row
for j = (i + 1):row
sp = and(H(i, :), H(j, :));
csp = find(sp);
cl = length(csp);
if cl > 1
if length(find(H(i, :))) < length(find(H(j, :)))
for cp = 1:cl - 1
H(j, csp (cp )) = 0;
end
else
for cp = 1:cl - 1
H(i, csp (cp )) = 0;
end
end % if
end % if
end % for j
end % for i
end %for if
figure(2),mesh(H) % shows girth 4 free H
```

The results obtained from the above MATLAB program are shown in Figs. 8.3 and 8.4.

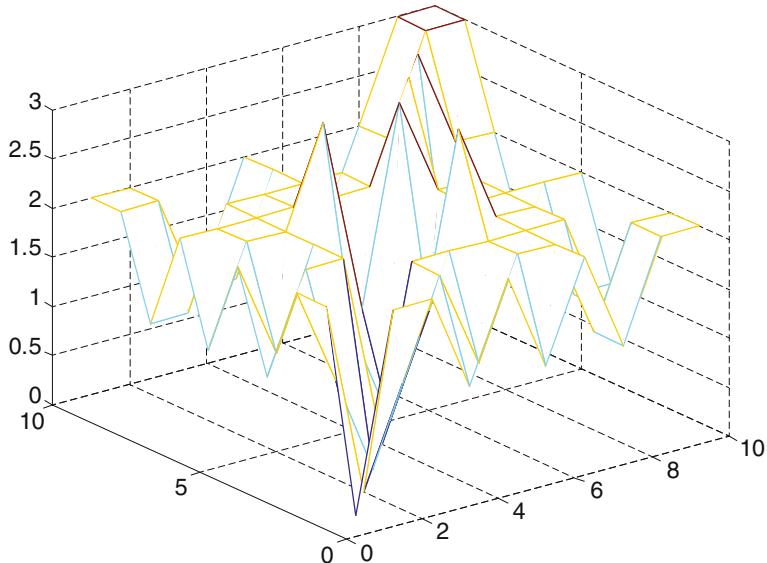


Fig. 8.3 Entries of H with girth 4

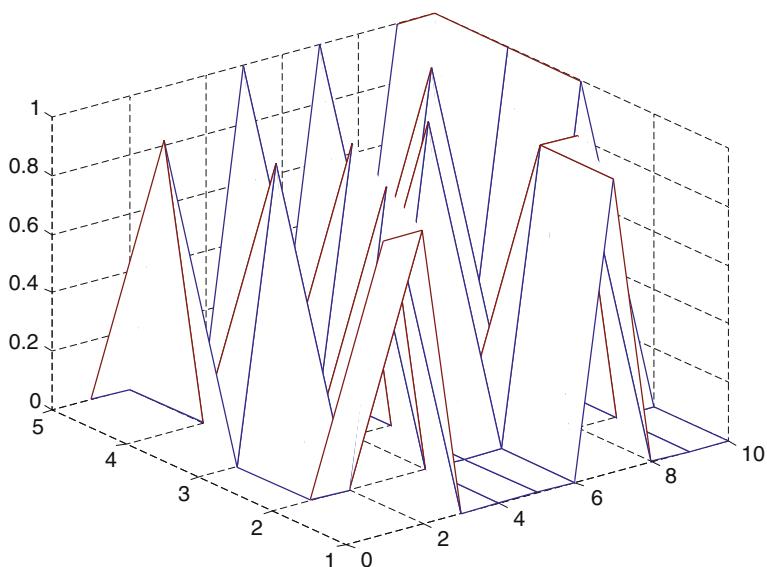


Fig. 8.4 Entries of girth 4 free H

From Fig. 8.3, it is observed that all the entries of the matrix $[H^T H]$ except diagonal line are not 1s. Hence, the given H matrix has girth 4, whereas Fig. 8.4 shows girth 4 free H .

8.4 LDPC Encoding

8.4.1 Preprocessing Method

For coding purposes, we may derive a generator matrix G from the parity check matrix H for LDPC codes by means of Gaussian elimination in modulo-2 arithmetic. Since the matrix G is generated once for a parity check matrix, it is usable in all encoding of messages. As such this method can be viewed as the preprocessing method.

1-by- n code vector c is first partitioned as

$$C = [b : m] \quad (8.8)$$

where m is k by 1 message vector, and b is the $n - k$ by 1 parity vector correspondingly the parity check matrix H is partitioned as

$$H^T = \begin{bmatrix} H_1 \\ \vdots \\ H_2 \end{bmatrix} \quad (8.9)$$

where H_1 is a square matrix of dimensions $(n - k) \times (n - k)$, and H_2 is a rectangular matrix of dimensions $k \times (n - k)$ transposition symbolized by the superscript T is used in the partitioning of matrix H or convenience of representation.

Imposing the constraint $CH^T = 0$.

We may write

$$[b : m] \begin{bmatrix} H_1 \\ \vdots \\ H_2 \end{bmatrix} = 0 \quad (8.10)$$

or equivalently,

$$bH_1 + mH_2 = 0 \quad (8.11)$$

The vectors m and b are related by

$$b = mP \quad (8.12)$$

where P is the coefficient matrix. For any nonzero message vector m , the coefficient matrix of LDPC codes satisfies the condition.

$$PH_1 + H_2 = 0 \quad (8.13)$$

which holds for all nonzero message vectors and, in particular, in the form $[0 \dots 0 1 0 \dots 0]$ that will isolate individual rows of the generator matrix. Solving Eq. (8.13) for matrix P , we get

$$P = H_2 H_1^{-1} \quad (8.14)$$

where H_1^{-1} is the inverse matrix of H_1 , which is naturally defined in modulo-2 arithmetic. Finally, the generator matrix of LDPC codes is defined by

$$G = [P : I_k] = [H_2 H_1^{-1} : I_k] \quad (8.15)$$

where I_k is the k by k identity matrix. The code word can be generated as

$$C = mG \quad (8.16)$$

Example 8.4 Construct generator matrix G for the following (10, 3, 5) regular parity check matrix.

$$\left[\begin{array}{ccccccccc|c} 1 & 1 & 0 & 1 & 0 & 1 & : & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & : & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & : & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & : & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & : & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & : & 1 & 1 & 1 & 1 \end{array} \right]$$

Solution

$$H = \underbrace{\left[\begin{array}{ccccccccc|c} 1 & 1 & 0 & 1 & 0 & 1 & : & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & : & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & : & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & : & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & : & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & : & 1 & 1 & 1 & 1 \end{array} \right]}_{H_1^T} \quad \underbrace{\left[\begin{array}{c} \\ \\ \\ \\ \\ \end{array} \right]}_{H_2^T}$$

$$H_1 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} \quad H_2 = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Letting $mH_2 = u$, the following relation can be written from Eq. (8.11)

$$\begin{bmatrix} b_0 & b_1 & b_2 & b_3 & b_4 & b_5 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} u_0 & u_1 & u_2 & u_3 & u_4 & u_5 \end{bmatrix}$$

The above relation between b and u leads to the following equations:

$$\begin{aligned} b_0 + b_1 + b_3 + b_5 &= u_0 \\ b_1 + b_2 + b_4 &= u_1 \\ b_0 + b_4 + b_5 &= u_2 \\ b_1 + b_2 + b_3 + b_5 &= u_3 \\ b_0 + b_2 + b_4 &= u_4 \\ b_3 &= u_5 \end{aligned}$$

Solving the above equations, using modulo-2 arithmetic, we obtain

$$\begin{aligned} b_0 &= u_1 + u_2 + u_3 + u_5 \\ b_1 &= u_2 + u_3 + u_4 + u_5 \\ b_2 &= u_0 + u_1 + u_2 + u_5 \\ b_3 &= u_5 \\ b_4 &= u_0 + u_3 + u_4 \\ b_5 &= u_0 + u_1 + u_4 + u_5 \end{aligned}$$

Since $b = uH_1^{-1}$, the above equations can be write in matrix form as

$$b = [u] \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Thus,

$$\begin{aligned}
 H_1^{-1} &= \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \\
 H_2H_1^{-1} &= \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \\
 &= \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}
 \end{aligned}$$

The generator matrix $G = [H_2H_1^{-1} I_k]$

$$= \underbrace{\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}}_{H_2H_1^{-1}} \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}}_{I_k}$$

Example 8.5 Construct LDPC code word for the following parity check matrix with the message vector $m = [1\ 0\ 0\ 0\ 1]$.

$$H = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Solution The parity check matrix H is of the order 5×10 . We know that $H^T = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix}$; then,

$$H^T = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$H_1 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix} \text{ and } H_2 = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Letting $mH_2 = u$, the following relation can be written from Eq. (8.11)

$$[b_0 \ b_1 \ b_2 \ b_3 \ b_4] \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix} = [u_0 \ u_1 \ u_2 \ u_3 \ u_4]$$

The above relation between b and u leads to the following equations

$$\begin{aligned} b_0 + b_1 + b_4 &= u_0 \\ b_0 + b_2 + b_3 &= u_1 \\ b_1 + b_3 + b_4 &= u_2 \\ b_0 + b_2 + b_4 &= u_3 \\ b_1 + b_2 + b_3 &= u_4 \end{aligned}$$

Solving the above equations, we obtain

$$\begin{aligned} b_0 &= u_2 + u_3 + u_4 \\ b_1 &= u_1 + u_2 + u_3 \\ b_2 &= u_0 + u_1 + u_2 \\ b_3 &= u_0 + u_3 + u_4 \\ b_4 &= u_0 + u_1 + u_4 \end{aligned}$$

Since $b = uH_1^{-1}$, the above equations can be written in matrix form as

$$b = [u] \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Thus,

$$H_1^{-1} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

$$H_2H_1^{-1} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

The generator matrix $G = [H_2H_1^{-1} I_k]$

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The code word can be generated as $C = mG$.

$$C = [1 \ 0 \ 0 \ 0 \ 1] \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$C = [1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1]$$

$$CH^T = [1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1] \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} = [0 \ 0 \ 0 \ 0 \ 0]$$

8.5 Efficient Encoding of LDPC Codes

The preprocessing method discussed in Sect. 8.4.1 for finding a generator matrix G for a given H can be used for encoding any arbitrary message bits vector of size $1 \times m$. However, it has a complexity of $O(n^2)$ [9]. LDPC code can be encoded using the parity check matrix directly by using the efficient encoding method [6] which has a complexity of $O(n)$. The stepwise procedure of efficient coding of LDPC coding [10] is as follows:

Step 1: By performing row and column permutations, the non-singular parity check matrix H is to be brought into a lower triangular form indicates in Fig. 8.5. More precisely, the H matrix is brought into the form

$$H_t = \begin{bmatrix} A & B & T \\ C & D & E \end{bmatrix} \quad (8.17)$$

with a gap g as small as possible. Where A is $(m - g) \times (n - m)$ matrix, B is $(m - g) \times g$ matrix, T is $(m - g) \times (m - g)$ matrix, C is $g \times (n - m)$ matrix, D is $g \times g$ matrix and E is $g \times (m - g)$ matrix. All of these matrices are sparse and T is lower triangular with ones along the diagonal.

Step 2: Premultiply H_t by $\begin{bmatrix} I_{m-g} & 0 \\ -ET^{-1} & I_g \end{bmatrix}$

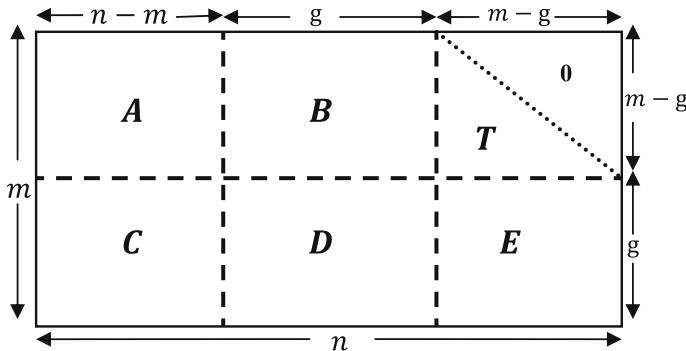


Fig. 8.5 The parity check matrix in approximate lower triangular form

$$\begin{bmatrix} I_{m-g} & 0 \\ -ET^{-1} & I_g \end{bmatrix} \begin{bmatrix} A & B & T \\ C & D & E \end{bmatrix} = \begin{bmatrix} A & B & T \\ -ET^{-1}A + C & -ET^{-1}B + D & 0 \end{bmatrix} \quad (8.18)$$

In order to check that $-ET^{-1}B + D$ is non-singular. It is to be ensured by performing column permutations further.

Step 3: Obtain p_1 using the following

$$p_1^T = -\emptyset^{-1}(-ET^{-1}A + C)s^T \quad (8.19)$$

where

$\emptyset = -ET^{-1}B + D$ and s is message vector.

Step 4: Obtain p_2 using the following

$$p_2^T = -T^{-1}(As^T + Bp_1^T) \quad (8.20)$$

Step 5: Form the code vector c as

$$c = [s \quad p_1 \quad p_2] \quad (8.21)$$

p_1 holds the first g parity and p_2 contains the remaining parity bits.

Example 8.6 Construct LDPC code word for the following parity check matrix with the message vector $m = [1 \ 0 \ 0 \ 0 \ 1]$.

$$H = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Solution

Step 1: Second and third rows and third and tenth columns are swapped to obtain

$$H_t = \left[\begin{array}{ccccc|cc|cc|c} 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ \hline 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{array} \right]$$

Step 2:

$$T^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \quad E = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} I_{m-g} & 0 \\ -ET^{-1} & I_g \end{bmatrix} \left[\begin{array}{ccccc|cc|cc|c} 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ \hline 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{array} \right] = \left[\begin{array}{ccccc|cc|cc|c} 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ \hline 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{array} \right]$$

Step 3:

$$p_1^T = -[-ET^{-1}B + D]^{-1}(-ET^{-1}A + C)s^T = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Step 4:

$$p_2^T = -T^{-1}(As^T + Bp_1^T) = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

Step 5:

$$c = [s \ p_1 \ p_2] = [1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1].$$

8.5.1 Efficient Encoding of LDPC Codes Using MATLAB

The following example illustrates the efficient encoding of LDPC codes using MATLAB.

Example 8.7 Write a MATLAB program to encode a random message vector with the following parity check matrix.

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Program 8.4 MATLAB program for efficient encoding of LDPC Codes

```
%Program for efficient encoding of LDPC Codes
clear all;clc;
H=[1 1 0 1 1 0 0 1 0 0 ;0 1 1 0 1 1 1 0 0 0 ;0 0 0 1 0 0 0 1 1 1 ;1 1 0 0 0 1 1 0 0 1
1 0 ;0 0 1 0 0 1 0 1 0 1];
Hlt=[1 1 0 1 1 0 0 1 0 0 ;0 0 0 1 0 1 0 1 1 0 ;0 1 1 0 1 0 1 0 0 1 ;1 1 0 0 0 1 1 0 0 0
1 0 1 1 ;0 0 1 0 0 1 0 1 0 1];
msg = round(rand(1,size(H,1)));
p=ldpclinearencode(Hlt,msg);
c=[msg p];
% Checking c'*Hlt'=0;
cs = mod(c'*Hlt',2);
if sum(cs)~= 0
    disp('Error')
```

```

function p=ldpclinearencode(H,msg);
n = size(H,2);
m = size(H,2) - size(H,1);
Hr = H(:,end);
% Find the 'gap' length
for i=1:size(H,2)
    if Hr(i) == 1
        g = i;
        break;
    end
end
g = size(H,1) - g;
% Extracting the submatrices A, B, C, D, E and T
A = H(1:m-g,1:n-m);
B = H(1:m-g,n-m+1:n-m+g);
T = H(1:m-g,n-m+g+1:end);
C = H(m-g+1:end,1:n-m);
D = H(m-g+1:end,n-m+1:n-m+g);
E = H(m-g+1:end,n-m+g+1:end);
% Calculate p1 and p2
invT = (inv(T)); % or abs(inv(T)) ?
ET1 = -(E*invT);
phi = ET1*B + D;
xtra = ET1*A + C;
p1 = mod(phi*xtra*(msg'),2)';
p2 = mod(invT*(A*(msg') + B*(p1')),2)';
p = [p1 p2];

```

8.6 LDPC Decoding

In the LDPC decoding, the notation B_j is used to represent the set of bits in the parity check equation of H , and the notation A_i is used to represent the parity check equations for the i th bit of the code. Consider the following parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \quad (8.22)$$

For the above parity check matrix, we get

$$\begin{aligned} B_1 &= \{1, 2, 3\}, & B_2 &= \{1, 4, 5\}, & B_3 &= \{2, 4, 6\}, & B_4 &= \{3, 5, 6\}, \\ A_1 &= \{1, 2\}, & A_2 &= \{1, 3\}, & A_3 &= \{1, 4\}, & A_4 &= \{2, 3\}, & A_5 &= \{2, 4\}, & A_6 &= \{3, 4\} \end{aligned}$$

8.6.1 LDPC Decoding on Binary Erasure Channel Using Message-Passing Algorithm

The message-passing algorithms are iterative decoding algorithms which passes the messages back and forward between the bit and CN iteratively until the process is stopped. The message-labeled M_i indicates 0 or 1 for known bit values and e for erased bit the stepwise procedure for LDPC decoding on BEC is as follows:

Step 1: Set $M = y$, find B_j and A_i of H

Step 2: $\text{iter} = 1$

Step 3: If all messages into check j other than M_i are known, compute all check sums by using the following expression

$$E_{j,i} = \sum_{i' \in B_j, i' \neq i} (M_{i'} \bmod 2)$$

else $E_{j,i} = e$

Step 4: If $M_i = e$ and if $j \in A_i$ subject to $E_{j,i} \neq e$, set $M_i = E_{j,i}$.

Step 5: If all M_i are known or $\text{iter} = \text{iter}_{\max}$, stop, else

Step 6: $\text{iter} = \text{iter} + 1$, go to Step 3.

Example 8.8 For the parity check matrix given by Eq. (8.22), $c = [1 \ 0 \ 1 \ 1 \ 0 \ 1]$ is a valid code word since $cH^T = 0$. If the code word is sent through BEC, the received vector is $y = [1 \ 0 \ e \ e \ e \ 1]$. Decode the received vector to recover the erased bits using message-passing algorithm.

Solution For Step 3 of the algorithm, the first check node is joined to the first, second, and third bit nodes having incoming messages 1, 0, and e , respectively. This check node has one incoming e message from the third bit node. Hence, we can calculate the outgoing message $E_{1,3}$ on the edge from the first check node to the third bit node:

$$\begin{aligned} E_{1,3} &= M_1 + M_2 \\ &= 1 \oplus 0 \\ &= 1. \end{aligned}$$

The second check node is joined to the first, fourth, and fifth bit nodes having incoming messages 1, e , and e , respectively. As this check node has two e messages, the outgoing messages from this check node are all e .

The third check node is joined to the second, fourth, and sixth bits receiving incoming messages 0, e , and 1, respectively. This check node has one incoming e

message from the fourth bit node. Hence, the outgoing message $E_{1,3}$ on the edge from the third check node to the fourth bit node is given by

$$\begin{aligned} E_{3,4} &= M_2 + M_6 \\ &= 0 \oplus 1 \\ &= 1. \end{aligned}$$

The fourth check node includes the third, fifth, and sixth bits and receives e , e , and 1 messages, respectively. Since this check node receives two e messages, the outgoing messages from this check node are all e .

In Step 4 of the algorithm, each bit node with an unknown value updates its value uses its incoming messages. The third bit is unknown and has incoming messages 1 ($E_{1,3}$) and e ($E_{4,3}$) and hence the third bit value becomes 1. The fourth bit is not known and it is set to 1 as it has incoming messages 1 ($E_{2,4}$) and e ($E_{3,4}$). The fifth bit is also unknown but its value cannot be changed because has e ($E_{2,5}$) and e ($E_{4,5}$) as incoming messages. Thus, at the end of the Step 4,

$$M = [1 \ 0 \ 1 \ 1 \ e \ 1].$$

Since the fifth bit is remaining unknown and hence the algorithm is to be continued. In the second iteration, in the Step 3 of the algorithm, the second check node is joined to the first, fourth and fifth bit nodes and so this check node has one incoming e message, M_5 . Hence, the outgoing message from this check node becomes

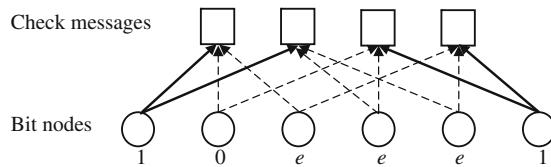
$$\begin{aligned} E_{2,5} &= M_1 + M_4 \\ &= 1 \oplus 1 \\ &= 0. \end{aligned}$$

The fourth check node is joined to the third, fifth, and sixth bit nodes having one incoming e message, M_5 . The outgoing message from this check to the sixth bit node, $E_{4,6}$, is the value of the sixth code word bit:

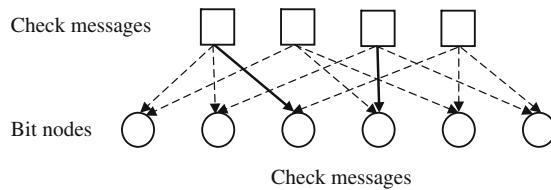
$$\begin{aligned} E_{4,5} &= M_3 + M_6 \\ &= 1 \oplus 1 \\ &= 0. \end{aligned}$$

In the second iteration, in the Step 4, the unknown fifth bit is changed to 0 as it has $E_{2,5}$ and $E_{4,5}$ as incoming messages with value 0. The algorithm is stopped and the decoded code word is

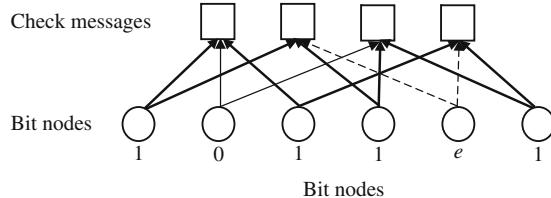
(a)

Initialization:

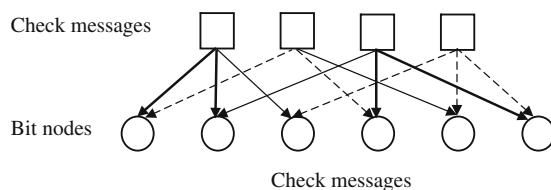
(b)

First iteration:

(c)



(d)

Second iteration:

(e)

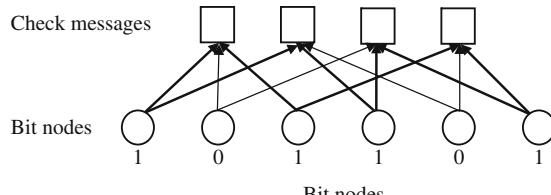


Fig. 8.6 Decoding of received vector $y = [1 \ 0 \ e \ e \ e \ 1]$ using message passing. The *dark line* corresponds to message bit 1, *solid line* corresponds to message bit 0, and the *broken line* corresponds to erasure bit e

$$\hat{c} = M = [1 \ 0 \ 1 \ 1 \ 0 \ 1]$$

as the decoded code word Fig. 8.6 shows the graphical representation of message-passing decoding.

8.6.2 LDPC Decoding on Binary Erasure Channel Using MATLAB

The following example illustrates decoding of LDPC codes on BEC using MATLAB.

Example 8.9 Write a MATLAB program to implement LDPC decoding on BEC by assuming received vector $y = [1 \ e \ e \ e \ e \ 1 \ 0 \ 0 \ 0 \ 1 \ e \ 1 \ e \ e \ e \ 1]$ when the following parity is used to encode the code word.

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Solution The following MATLAB program decodes the received vector y . In this program, known bit values are indicated by 1 or 0 and erased bit is indicated by -1.

Program 8.5 MATLAB program Decoding of LDPC Codes on BEC

```
% Program for Bit Flipping Decoding of LDPC Codes %%%
clear all;clc;
% y=[0 0 1 -1 -1];
y=[1 -1 -1 -1 1 0 0 0 1 -1 1 -1 -1 1];
M=y;
% H=[1 1 0 1 0 0;0 1 1 0 1 0;1 0 0 0 1 1 ; 0 0 1 1 0 1];
H=[1 1 1 0 1 1 0 0 0 0 0 0 0 0;1 0 0 1 1 1 0 1 0 0 0 0 0 0;
    0 0 1 1 0 0 0 1 0 0 0 0 0 0 0;0 1 1 1 0 0 0 0 1 0 0 0 0 0;
    0 1 0 0 0 0 0 1 1 0 0 0 0 0;1 1 0 1 1 0 0 0 0 1 0 0 0 0 0;
    1 1 0 1 0 0 0 0 0 0 1 0 0 0 0;1 1 0 0 0 1 0 0 0 0 0 1 0 0;
    1 1 1 0 1 0 0 0 0 0 0 0 1 0 0;0 1 1 1 0 0 0 0 0 0 0 0 0 1 0;
    1 0 0 0 0 0 0 0 0 0 0 0 0 0 1];
[N1 N2]=size(H);
iter=input('enter the number of iterations')
for i=1:iter
    for j=1:N1
        ci = find(H(j, :));
        d=find(M(ci)~-1);
        d1=find(M(ci)==-1);
        if ((length(d)>=2) & (length(d1)==1))
            E(j,ci(d1))=mod(sum(M(ci(d))),2);
        else
            E(j,ci(d1))=-1;
        end
    end
    for j=1:N2
        ri = find(H(:,j));
        if(M(j)==-1)
            for ii=1:length(ri)
                if( E(ri(ii),j)~-1)
                    M(j)=E(ri(ii),j);
                end
            end
        end
    end
end
end
```

8.6.3 Bit-Flipping Decoding Algorithm

The received symbols are hard decoded into 1s and 0s to form a binary received vector y . In each iteration, it computes all check sums, as well as the number of unsatisfied parity checks involving each of the n bits of the vector y . Next, the bits of y are flipped if they involve in the largest number of unsatisfied parity checks. The process is to be repeated until all check sums are satisfied or reaches a

predetermined number of iterations. The stepwise procedure of the Bit-flipping decoding algorithm is as follows:

Step 1: Set $M = y$, define B_j to represent the j th parity check equation of H

Step 2: $l = 0$

Step 3: Compute all check sums by using the following expression

$$E_{j,i} = \sum_{i' \in B_j, i' \neq i} (M_{i'} \bmod 2) \quad (8.23)$$

Step 4: Compute the number of unsatisfied parity checks involving each of n bits of message

Step 5: Flip the bits of message when they are involved in largest number of unsatisfied parity checks. The flipping on i th bit can be performed by using

$$M_i = (y_i + 1 \bmod 2) \quad (8.24)$$

Step 6: Compute s as follows

$$s = (MH^T) \bmod 2 \quad (8.25)$$

Step 7: If $s = 0$ or $l = l_{\max}$, stop, else

Step 8: $l = l + 1$, go to Step 3.

Example 8.10 For the parity check matrix given by Eq. (8.22), $c = [1\ 0\ 1\ 1\ 0\ 1]$ is a valid code word since $cH^T = 0$. If the code word is sent through AWGN channel, the received vector after a detector hard decision is $y = [0\ 0\ 1\ 1\ 0\ 1]$. Decode the received vector using bit-flipping algorithm.

Solution The decoder makes a hard decision on each code word bit and returns

$$y = [0\ 0\ 1\ 1\ 0\ 1].$$

Step 1: Initializing $M_i = y_i$, so

$$M = [0\ 0\ 1\ 1\ 0\ 1].$$

Step 2: $l = 0$

Step 3: The check messages are calculated. The first check node is joined to the first, second, and third bit nodes $B_1 = \{1, 2, 3\}$ and so that the messages from the first check node are

$$\begin{aligned}E_{1,1} &= M_2 \oplus M_3 = 0 \oplus 1 = 1, \\E_{1,2} &= M_1 \oplus M_3 = 0 \oplus 1 = 1, \\E_{1,3} &= M_1 \oplus M_2 = 0 \oplus 0 = 0,\end{aligned}$$

The second check includes the first, fourth, and fifth bits, $B_2 = \{1, 4, 5\}$ and so the messages from the second check are

$$\begin{aligned}E_{2,1} &= M_4 \oplus M_5 = 1 \oplus 0 = 1, \\E_{2,4} &= M_1 \oplus M_5 = 0 \oplus 0 = 0, \\E_{2,5} &= M_1 \oplus M_4 = 0 \oplus 1 = 1.\end{aligned}$$

The third check includes the second, fourth, and sixth bits, $B_3 = \{2, 4, 6\}$, and so the messages from the second check are

$$\begin{aligned}E_{3,2} &= M_4 \oplus M_6 = 1 \oplus 1 = 0, \\E_{3,4} &= M_2 \oplus M_6 = 0 \oplus 1 = 1, \\E_{3,6} &= M_2 \oplus M_4 = 0 \oplus 1 = 1,\end{aligned}$$

The fourth check includes the third, fifth, and sixth bits, $B_4 = \{3, 5, 6\}$, and so the messages from the second check are

$$\begin{aligned}E_{4,3} &= M_5 \oplus M_6 = 0 \oplus 1 = 1, \\E_{4,5} &= M_3 \oplus M_6 = 1 \oplus 1 = 0, \\E_{4,6} &= M_3 \oplus M_5 = 1 \oplus 0 = 1.\end{aligned}$$

Step 4: The first bit has messages 1 and 1 from the first and second checks, respectively, and 0 from the channel. Thus, the majority of the messages into the first bit node indicate a value different from the received value. The second bit has messages 1 and 0 from the first and third checks, respectively, and 0 from the channel, so it retains its received value. The third bit has messages 0 and 1 from the first and fourth checks, respectively, and 1 from the channel, so it retains its received value. The fourth bit has messages 0 and 1 from the second and third checks, respectively, and 1 from the channel, so it retains its received value. The fifth bit has messages 1 and 0 from the second and fourth checks, respectively, and 0 from the channel, so it retains its received value. The sixth bit has messages 1 and 1 from the third and fourth checks, respectively, and 1 from the channel, so it retains its received value. Thus, the majority of the messages into the first bit node indicate a value different from the received value.

Step 5: Hence, the first bit node flips its value. The new bit node to check node messages is thus given by

$$M = [1 \ 0 \ 1 \ 1 \ 0 \ 1].$$

Step 6: Compute $s = (MH^T) \bmod 2$

$$s = \left([1 \ 0 \ 1 \ 1 \ 0 \ 1] \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \right) \bmod 2 = [0 \ 0 \ 0 \ 0]$$

there are thus no unsatisfied parity check equations, and so the algorithm halts and returns

$$\hat{c} = M = [1 \ 0 \ 1 \ 1 \ 0 \ 1]$$

as the decoded code word. The received vector has therefore been correctly decoded without requiring an explicit search over all possible code words. Hence the process is stopped.

8.6.4 Bit-Flipping Decoding Using MATLAB

The following example illustrates the bit-flipping decoding of LDPC codes using MATLAB

Example 8.11 Write a MATLAB program to implement bit flipping decoding by assuming received vector $y = [0 \ 1 \ 1 \ 0 \ 1 \ 1]$ when the following parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

is used to encode the code word.

Solution The following MATLAB program decodes the received vector y .

Program 8.6 MATLAB program for Bit Flipping Decoding of LDPC Codes

```
% Program for Bit Flipping Decoding of LDPC Codes
clear all;clc;
y=[0 1 1 0 1 1];
H=[1 1 0 1 0 0;0 1 1 0 1 0;1 0 0 0 1 1 ; 0 0 1 1 0 1];
[N1 N2]=size(H);
iter=input('enter the number of iterations')
for i=1:iter
for j=1:N1
    ci = find(H(j, :));
    for k=1:length( ci)
        E(j, ci(k)) = mod(sum(y( ci ) ) + y( ci (k)), 2);
    end
end
for j=1:N2
    ri = find(H(:, j));
    numberofones=length(find(E(ri,j)));
    numberofzeros=length(ri)-numberofones;
    if(numberofones==numberofzeros)
        yd(j)=y(j);
    elseif(numberofones > numberofzeros)
        yd(j)=1;
    elseif(numberofones < numberofzeros)
        yd(j)=0;
    end
end
y=yd;
end
```

The output of the above program gives the decoded vector

$$\hat{c} = y_d = [0 \ 0 \ 1 \ 0 \ 1 \ 1]$$

Example 8.12 A valid code word is $c = [0 0 1 0 0 1]$ for the following parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

If the code word is transmitted over AWGN channel, the received vector after detector hard decision is $y = [1 0 1 0 0 1]$. Decode the received vector by bit-flipping using MATLAB and comment on the result.

Solution The Program 8.6 is run with the H matrix and the received vector. The output of the program gives the decoded vector $\hat{c} = y_d = [0\ 1\ 1\ 0\ 0\ 1]$. The received vector is not decoded correctly due to the girth 4 in the H matrix.

8.7 Sum–Product Decoding

The sum–product algorithm is similar to the bit-flipping algorithm as described in the previous section, but the messages representing each decision (whether the bit value is 1 or 0) are now probabilities. Bit-flipping decoding accepts an initial hard decision on the received bits as input, and the sum–product algorithm is a soft-decision message-passing algorithm which accepts the probability of each received bit as input. The input channel or received bit probabilities are known in advance before the LDPC decoder was operated, and so they are also called as the a priori probabilities of the received bit. In the sum–product decoder, the extrinsic information passed between nodes is also probabilities. The extrinsic information between check node j and bit node i is denoted by $E_{j,i}$. The $E_{j,i}$ gives the probability for the bit c_i to be 1 that causes the parity check equation j is satisfied. The $E_{j,i}$ cannot be defined if the bit i is not included in j as there will be no extrinsic information between check node j and bit node i .

The probability that an odd number of the bits in that parity check equation are 1s is given by

$$P_{j,i}^{\text{ext}} = \frac{1}{2} - \frac{1}{2} \prod_{i' \in B_j, i' \neq i} (1 - 2P_{j,i'}) \quad (8.26)$$

which is the probability that a parity check equation is satisfied for the bit c_i to be 1. The probability that the parity check equation is satisfied for the bit c_i to be 0 becomes $1 - P_{j,i}^{\text{ext}}$.

The metric for a binary variable is represented by the following log likelihood ratio (LLR)

$$L(x) = \log \frac{p(x=0)}{p(x=1)} \quad (8.27)$$

where by log we mean \log_e . The sign of $L(x)$ provides a hard decision on x and magnitude $|L(x)|$ is the reliability of this decision. Translating from LLRs back to probabilities,

$$p(x=1) = \frac{e^{-L(x)}}{1 + e^{-L(x)}} \quad (8.28)$$

$$p(x=0) = \frac{e^{L(x)}}{1 + e^{-L(x)}} \quad (8.29)$$

when probabilities need to be multiplied, LLRs need only be added and by this the complexity of the sum–product decoder is reduced. This makes the benefits of the logarithmic representation of probabilities. The extrinsic information from check node j to bit node i is expressed as a LLR,

$$E_{j,i} = L(P_{j,i}^{\text{ext}}) = \log \frac{1 - P_{j,i}^{\text{ext}}}{P_{j,i}^{\text{ext}}} \quad (8.30)$$

Now

$$\begin{aligned} E_{j,i} &= \log \frac{\frac{1}{2} + \frac{1}{2} \prod_{i' \in B_j, i' \neq i} (1 - 2P_{j,i'})}{\frac{1}{2} - \frac{1}{2} \prod_{i' \in B_j, i' \neq i} (1 - 2P_{j,i'})} \\ &= \log \frac{1 + \prod_{i' \in B_j, i' \neq i} \left(1 - 2 \frac{e^{-M_{j,i'}}}{1 + e^{-M_{j,i'}}} \right)}{1 - \prod_{i' \in B_j, i' \neq i} \left(1 - 2 \frac{e^{-M_{j,i'}}}{1 + e^{-M_{j,i'}}} \right)} \\ &= \log \frac{1 + \prod_{i' \in B_j, i' \neq i} \left(\frac{1 - e^{-M_{j,i'}}}{1 + e^{-M_{j,i'}}} \right)}{1 - \prod_{i' \in B_j, i' \neq i} \left(\frac{1 - e^{-M_{j,i'}}}{1 + e^{-M_{j,i'}}} \right)} \end{aligned} \quad (8.31)$$

where $M_{j,i'} \triangleq L(P_{j,i'}) = \log \frac{1 - P_{j,i'}}{P_{j,i'}}.$

Using the relationship

$$\tanh \frac{1}{2} \log \left(\frac{1 - p}{p} \right) = 1 - 2p \quad (8.32)$$

gives

$$E_{j,i} = \log \frac{1 + \prod_{i' \in B_j, i' \neq i} \tanh(M_{j,i'})/2}{1 - \prod_{i' \in B_j, i' \neq i} \tanh(M_{j,i'})/2} \quad (8.33)$$

Alternatively, using the relationship

$$2 \tanh^{-1} p = \log \frac{1 + p}{1 - p} \quad (8.34)$$

Then,

$$E_{j,i} = 2 \tanh^{-1} \prod_{i' \in B_j, i' \neq i} \tanh(M_{j,i'}/2) \quad (8.35)$$

The above equation is numerically challenging due to the presence of the product of the tanh and \tanh^{-1} functions. Following Gallager, we can improve the situation as follows. First, factor M_{ji} into its sign and magnitude (or bit value and bit reliability);

$$M_{ji} = \alpha_{ji} \beta_{ji} \quad (8.36)$$

$$\alpha_{ji} = \text{sign}(M_{ji}) \quad (8.36a)$$

$$\beta_{ji} = |M_{ji}| \quad (8.36b)$$

So that Eq. (8.35) may be rewritten as

$$\tanh\left(\frac{1}{2}M_{ji}\right) = \prod_{i'} \alpha_{ji'} \cdot \prod_{i' \in B_j, i' \neq i} \tanh\left(\frac{1}{2}\beta_{ji'}\right) \quad (8.37)$$

We then have

$$\begin{aligned} E_{ji} &= \prod_{i'} \alpha_{ji'} \cdot 2 \tanh^{-1} \left(\prod_{i'} \tanh\left(\frac{1}{2}\beta_{ji'}\right) \right) \\ &= \prod_{i'} \alpha_{ji'} \cdot 2 \tanh^{-1} \log^{-1} \log \left(\prod_{i'} \tanh\left(\frac{1}{2}\beta_{ji'}\right) \right) \\ &= \prod_{i'} \alpha_{ji'} \cdot 2 \tanh^{-1} \log^{-1} \sum_{i'} \log \left(\tanh\left(\frac{1}{2}\beta_{ji'}\right) \right) \end{aligned} \quad (8.38)$$

This yields a new form for Eq. (8.38) as

$$E_{ji} = \prod_{i'} \alpha_{ji'} \cdot \phi \left(\sum_{i'} \phi(\beta_{ji'}) \right) \quad (8.39)$$

where $\phi(x)$ is defined as

$$\phi(x) = -\log[\tanh(x/2)] = \log\left(\frac{e^x + 1}{e^x - 1}\right) \quad (8.40)$$

Using the fact that $\phi^{-1}(x) = \phi(x)$ when $x > 0$.

Each bit node has access to the input LLR, L_i , and to the LLRs from every connected check node. The total LLR of the i th bit is the sum of these LLRs:

$$L_i^{\text{total}} = L_i + \sum_{j \in A_i} E_{ji} \quad (8.41)$$

The hard decision on the received bits is simply given by the signs of the L_i^{total} . Check whether the parity check equations are satisfied (thus, $\hat{c}H^T = 0$ is also a stopping criterion for sum–product decoding); if not satisfied, update M_{ji}

$$M_{ji} = \sum_{j' \in A_i, j' \neq j} E_{j'i} + L_i \quad (8.42)$$

The algorithm outputs the estimated a posteriori bit probabilities of the received bits as LLRs.

The sum–product decoder immediately stops whenever a valid code word has been found by a checking of whether the parity check equations are satisfied (i.e., $\hat{c}H^T = 0$) or allowed maximum number of iterations achieved. The decoder is initialized by setting all VN messages M_{ji} equal to

$$L_i = L(c_i|y_i) = \log\left(\frac{\Pr(c_i = 0|y_i)}{\Pr(c_i = 1|y_i)}\right) \quad (8.43)$$

For all j, i for which $h_{ij} = 1$. Here, y_j represents the channel value that was actually received, that is, it is not a variable here. The L_i for different channels can be computed as [10].

BEC

In this case, $y_j \in \{0, 1, e\}$

$$L_i = L(c_i|y_i) = \begin{cases} +\infty & y_j = 0, \\ -\infty & y_j = 1, \\ 0 & y_j = e. \end{cases} \quad (8.44)$$

BSC

In this case, $y_j \in \{0, 1\}$, we have

$$L_i = L(c_i|y_i) = (-1)^{y_j} \log\left(\frac{1 - P}{P}\right) \quad (8.45)$$

The knowledge of crossover probability P is necessary.

BI-AWGNC

The i th received sample is $y_i = x_i + n_i$ where the n_i are independent and normally distributed as $\mathcal{N}(0, \sigma^2)$. $\sigma^2 = \frac{N_0}{2}$ where N_0 is the noise density.

Then, we can easily show that

$$\Pr(x_i = x|y_i) = \frac{1}{1 + \exp(-4y_i x/N_0)} \quad (8.46)$$

where $x \in \{\pm 1\}$ and, from this, that

$$L(c_i|y_i) = 4y_i/N_0 \quad (8.47)$$

An estimate of N_0 is necessary in practice.

Rayleigh

The model for Rayleigh fading channel is similar to that of the AWGNC: $y_i = \alpha_i x_i + n_i$ where $\{\alpha_i\}$ are independent Rayleigh random variable with unity variance. The channel transition probability can be expressed by

$$P(x_i = x|y_i) = \frac{1}{1 + \exp(-4\alpha_i y_i x/N_0)}$$

Then,

$$L(c_i|y_i) = 4\alpha_i y_i/N_0 \quad (8.48)$$

The estimates of α_i and σ^2 are necessary in practice.

Now, the stepwise procedure for the log domain sum–product algorithm is given in the following Sect. 8.8.

8.7.1 Log Domain Sum–Product Algorithm (SPA)

Step 1: Initialization: for all i , initialize L_i according to Eq. (8.44) for the appropriate channel model. Then, for all i, j for which $h_{ij} = 1$ set $M_{ji} = L_i$, and $1 = 0$. Define B_j to represent the set of bits in the j th parity check equation of H and A_i to represent the parity check equations for the i th bit of the code.

Step 2: CN update: compute outgoing CN message E_{ji} for each CN using Eqs. (8.36), (8.39), and (8.40).

$$\begin{aligned}
M_{ji} &= \alpha_{ji}\beta_{ji} \\
\alpha_{ji} &= \text{sign}(M_{ji}), \\
\beta_{ji} &= |M_{ji}| \\
E_{ji} &= \prod_{i'} \alpha_{j'i'} \cdot \phi \left(\sum_{i'} \phi(\beta_{j'i'}) \right) \\
\phi(x) &= -\log[\tanh(x/2)] = \log \left(\frac{e^x + 1}{e^x - 1} \right)
\end{aligned}$$

Step 3: LLR total: For $i = 0, 1, \dots, N - 1$ compute total LLR using Eq. (8.41)

$$L_i^{\text{total}} = L_i + \sum_{j \in A_i} E_{ji}$$

Step 4: Stopping criteria: For $i = 0, 1, \dots, N - 1$, set

$$\hat{c}_i = \begin{cases} 1 & \text{if } L_i^{\text{total}} < 0, \\ 0 & \text{else,} \end{cases}$$

To obtain \hat{c} . If $\hat{c}H^T = 0$ or the number of iterations equals the maximum limit ($l = l_{\max}$) stop;
else

Step 5: VN update: compute outgoing VN message M_{ji} for each VN using Eq. (8.42)

$$M_{ji} = L_i + \sum_{j' \in A_i, j' \neq j} E_{j'i} \cdot 1 = 1 + 1 \text{ go to Step 2}$$

8.7.2 The Min-Sum Algorithm

Consider Eq. (8.39) for E_{ji} . It can be noted from the shape of $\phi(x)$ that the largest term in the sum corresponds to the smallest β_{ji} . Hence, assuming that this term dominates the sum, the following relation is obtained [10]

$$\phi \left(\sum_{i'} \phi(\beta_{j'i'}) \right) \simeq \phi \left(\phi \left(\min_{i'} \beta_{j'i'} \right) \right) = \min_{i'} \beta_{j'i'} \quad (8.49)$$

Thus, the min-sum algorithm is simply the log domain SPA with Step 2 replaced by

$$\begin{aligned} M_{ji} &= \alpha_{ji} \beta_{ji} \\ \alpha_{ji} &= \text{sign}(M_{ji}), \\ \beta_{ji} &= |M_{ji}| \\ E_{ji} &= \prod_{j'} \alpha_{j'i} \cdot \min_{j'} \beta_{j'i} \end{aligned}$$

It can also be shown that, in the AWGNC case, the initialization $M_{ji} = 4y_i/N_0$ may be replaced by $M_{ji} = y_i$ when the simplified log domain sum–product algorithm is employed. The advantage, of course, is that an estimate of the noise power N_0 is unnecessary in this case.

Example 8.13 A code word generated using the parity check matrix $H =$

$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$ is sent through AWGN channel with $\text{No} = 0.3981$, the

received vector is $\mathbf{y} = [-0.9865 \ 0.3666 \ 0.4024 \ 0.7638 \ 0.2518 \ -1.6662]$. Decode the received vector using the sum–product algorithm.

Solution

$$L = -4 \frac{\mathbf{y}}{N_0} = [9.9115 \ -3.6830 \ -4.0430 \ -7.6738 \ -2.5295 \ 16.7415]$$

To begin decoding, we set

$$M_{j,i} = L_i$$

The first bit is included in the first and second checks, and so $M_{1,1}$ and $M_{2,1}$ are initialized to L_1 :

$$M_{1,1} = L_1 = 9.9115 \quad \text{and} \quad M_{2,1} = L_1 = 9.9115.$$

Repeating this for the remaining bits gives,

For $i = 1$, $M_{1,2} = L_2 = -3.6830$, $M_{3,2} = R_2 = -3.6830$;

For $i = 2$, $M_{1,3} = R_3 = -4.0430$, $M_{4,3} = R_3 = -4.0430$;

For $i = 4$, $M_{2,4} = R_4 = -7.6738$, $M_{3,4} = R_4 = -7.6738$;

For $i = 5$, $M_{2,5} = R_5 = -2.5295$, $M_{4,5} = R_5 = -2.5295$;

For $i = 6$, $M_{3,6} = R_6 = -16.7415$, $M_{4,6} = R_6 = -16.7415$;

Now the extrinsic probabilities are calculated for the check to bit messages, the first parity check includes the first, second, and fourth bits, and so the extrinsic probability from the first check node to the first bit node depends on the probabilities of the second and fourth bits:

$$\begin{aligned} E_{1,1} &= \log \frac{1 + \tanh(M_{1,2}/2) \tanh(M_{1,3}/2)}{1 - \tanh(M_{1,2}/2) \tanh(M_{1,3}/2)} \\ &= \log \frac{1 + \tanh(-3.6830/2) \tanh(-4.0430/2)}{1 - \tanh(-3.6830/2) \tanh(-4.0430/2)} = 3.1542 \end{aligned}$$

Similarly, the extrinsic probability from the first check node to the second bit node depends on the probabilities of the first and fourth bits:

$$\begin{aligned} E_{1,2} &= \log \frac{1 + \tanh(M_{1,1}/2) \tanh(M_{1,3}/2)}{1 - \tanh(M_{1,1}/2) \tanh(M_{1,3}/2)} \\ &= \log \frac{1 + \tanh(9.9115/2) \tanh(-4.0430/2)}{1 - \tanh(M_{1,1}/2) \tanh(M_{1,3}/2)} = -4.0402 \end{aligned}$$

And the extrinsic probability from the first check node to the 4th bit node depends on the LLRs sent from the first and second bit nodes to the first check node:

$$\begin{aligned} E_{1,3} &= \log \frac{1 + \tanh(M_{1,1}/2) \tanh(M_{1,2}/2)}{1 - \tanh(M_{1,1}/2) \tanh(M_{1,2}/2)} \\ &= \log \frac{1 + \tanh(9.9115/2) \tanh(-3.6830/2)}{1 - \tanh(9.9115/2) \tanh(-3.6830/2)} = -3.681 \end{aligned}$$

Next, the second check node connects to the second, third, and fifth bit nodes and so the extrinsic LLRs are

$$\begin{aligned} E_{2,1} &= \log \frac{1 + \tanh(M_{2,4}/2) \tanh(M_{2,5}/2)}{1 - \tanh(M_{2,4}/2) \tanh(M_{2,5}/2)} \\ &= \log \frac{1 + \tanh(-7.6738/2) \tanh(-2.5295/2)}{1 - \tanh(-7.6738/2) \tanh(-2.5295/2)} = 2.5237 \\ E_{2,4} &= \log \frac{1 + \tanh(M_{2,1}/2) \tanh(M_{2,5}/2)}{1 - \tanh(M_{2,1}/2) \tanh(M_{2,5}/2)} \\ &= \log \frac{1 + \tanh(9.9115/2) \tanh(-2.5295/2)}{1 - \tanh(9.9115/2) \tanh(-2.5295/2)} = -2.5289 \\ E_{2,5} &= \log \frac{1 + \tanh(M_{2,1}/2) \tanh(M_{2,4}/2)}{1 - \tanh(M_{2,1}/2) \tanh(M_{2,4}/2)} \\ &= \log \frac{1 + \tanh(9.9115/2) \tanh(-7.6738/2)}{1 - \tanh(9.9115/2) \tanh(-7.6738/2)} = -7.5724 \end{aligned}$$

Similarly for the remaining CNs

$$\begin{aligned} E_{3,2} &= -7.6737, \quad E_{3,4} = -3.6830, \quad E_{3,6} = 3.6647, \\ E_{4,3} &= -2.5295, \quad E_{4,5} = -4.0430, \quad E_{4,6} = -4.0430. \end{aligned}$$

To check for a valid code word, we calculate the estimated posterior probabilities for each bit, make a hard decision and check the syndrome s . The first bit has extrinsic LLRs from the first and second checks and an intrinsic LLR from the channel the total LLR is their sum:

$$L_1 = L_1 + E_{1,1} + E_{2,1} = 9.9115 + 3.1542 + 2.5237 = 15.5894.$$

Thus even though the LLR from the channel is negative, indicating that the first bit is a 1, both the extrinsic LLRs are positive, indicating that the bit is 0. The extrinsic LLRs are large enough to make the total LLR positive, and so the decision on the first bit has effectively been changed. Repeating for the second to sixth bits gives:

$$\begin{aligned} L_2 &= L_2 + E_{1,2} + E_{3,2} = -3.6830 - 4.0402 - 7.6737 = -15.3969, \\ L_3 &= L_3 + E_{1,3} + E_{4,3} = -4.0430 - 3.681 - 2.5295 = -10.2535, \\ L_4 &= L_4 + E_{2,4} + E_{3,4} = -7.6738 - 2.5289 - 3.6830 = -13.8857, \\ L_5 &= L_5 + E_{2,5} + E_{4,5} = -2.5295 - 7.5724 - 4.0430 = -14.1449, \\ L_6 &= L_6 + E_{3,6} + E_{4,6} = 16.7415 + 3.6647 - 4.0430 = 16.3632. \end{aligned}$$

The hard decision on the LLRs gives

$$\hat{c} = [0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0].$$

To check whether \hat{c} is a valid code word, consider

$$s = \hat{c}H' = [0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0] \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} = [0 \quad 0 \quad 0 \quad 0]$$

The decoding stops because $s = 0$ and the returned c is a valid code word.

8.7.3 *Sum–Product and Min-Sum Algorithms for Decoding of Rate 1/2 LDPC Codes Using MATLAB*

The following MATLAB program and functions are written and used to decode the rate $\frac{1}{2}$ LDPC codes using sum–product and min-sum algorithms for different SNRs.

Program 8.7 MATLAB program for LDPC decoding using log domain sum–product algorithm

```
% sum product algorithm for LDPC decoding
% rx      : Received signal vector (column vector)
% H       : LDPC parity check matrix
% N0     : Noise variance
% iter   : Number of iteration
% xHat   : Decoded vector (0/1)
clear all;clc;
x=[ 0 1 1 1 1 0 ];
H=[1 1 1 0 0 0;1 0 0 1 1 0;0 1 0 1 0 1 ;0 0 1 0 1 1];
[N1 N2] = size(H);
algtype= input('enter 1 forlogdomain, 2 for minsum');
EbN0 = input('Please enter Eb/N0 in dB : default [2.0]');
N0 = 1/(exp(EbN0*log(10)/10));
bpskMod = 2*x - 1;
rx =bpskMod+ sqrt(N0)*randn(size(bpskMod));
if(algtype==1)
    Li =(-4*rx./N0);
elseif(algtype==2)
    Li =-rx;
end
iter= input('enter the number of iterations=');
if(algtype==1)
    [Eji xHat]=logsumproduct(Li,H,N1,N2,iter);
elseif(algtype==2)
    [Eji xHat]=minsum (Li,H,N1,N2,iter);
end
```

```

function cHat=logsumproduct(Li,H,N1,N2,iter);
Eji = zeros(N1, N2);
Pibetaji = zeros(N1, N2);
Mji = H.*repmat(Li, N1, 1);
[row, col] = find(H);% Get non-zero elements
for n = 1:iter
fprintf('Iteration : %d\n', n);
    %step2 of sumproduct algorithm in log domain
    alphaji = sign(Mji); % Get the sign and magnitude of Mji)
    betaji = abs(Mji);
    for l = 1:length(row)
        Pibetaji(row(l), col(l)) = log((exp(betaji(row(l), col(l))) + 1)/...
            (exp(betaji(row(l), col(l))) - 1));
    end
    for i = 1:N1
        c1 = find(H(i, :));
        for k = 1:length(c1)
            Pibetaji_sum = 0;
            alphaji_prod = 1;
            Pibetaji_sum = sum(Pibetaji(i, c1)) - Pibetaji(i, c1(k));
            % Avoid division by zero/very small number, get
            Pi(sum(Pi(betaj)));
            if Pibetaji_sum < 1e-20
                Pibetaji_sum = 1e-10;
            end
            Pi_Pibetaji_sum= log((exp(Pibetaji_sum) + 1)/(exp(Pibetaji_sum) - 1));
            alphaji_prod = prod(alphaji(i, c1))*alphaji(i, c1(k));
            Eji(i, c1(k)) = alphaji_prod *Pi_Pibetaji_sum;
        end % for k
    end % for i
    for j = 1:N2
        r1 = find(H(:, j));
        %step 3 of sumproduct algorithm in log domain
        Litolal = Li(j) + sum(Eji(r1, j));
        % step 4 of sumproduct algorithm in log domain
        if Litolal < 0
            cHat(j) = 1;
        else
            cHat(j) = 0;
        end
        %step5 of sumproduct algorithm in log domain
        for k = 1:length(r1)
            Mji(r1(k), j) = Li(j) + sum(Eji(r1, j)) - Eji(r1(k), j);
        end % for k
    end % for j
    cs = mod(cHat*H',2);
    if sum(cs)== 0
        break;
    end
end % for n

```

Step 2 of min-sum algorithm

```
% step 2 of slgorithm
alphaij = sign(Mji); % Get the sign and magnitude of L(qij)
betaij = abs(Mji);
% ----- Horizontal step -----
for i = 1:N1
    % Find non-zeros in the column
    c1 = find(H(i, :));
    % Get the minimum of betaij
    for k = 1:length(c1)
        % Minimum of betaij\c1(k)
        minOfbetaij = realmax;
        for l = 1:length(c1)
            if l ~= k
                if betaij(i, c1(l)) < minOfbetaij
                    minOfbetaij = betaij(i, c1(l));
                end
            end
        end % for l
        Mji= prod(alphaij(i, c1))*alphaij(i, c1(k));
        Eji(i, c1(k)) = Mji*minOfbetaij;
    end % for k
end % for i
```

The MATLAB function min-sum is same as the log sum–product function program with the Step 2 in logsumproduct is replaced by the following MATLAB program segment has yielded.

For example, consider the parity check matrix of Example 8.11. $c = [0 \ 1 \ 1 \ 1 \ 1 \ 0]$ is a valid code word for the parity check matrix. When this code word is sent over an AWGN channel at $\frac{E_b}{N_o} = 2$ dB, decoding of the received vector using the above MATLAB program and functions has yielded $\hat{c} = [0 \ 1 \ 1 \ 1 \ 0]$.

8.8 EXIT Analysis of LDPC Codes

8.8.1 Degree Distribution

An irregular parity check matrix of LDPC codes has columns and rows with varying weights, i.e., a Tanner graph has bit nodes and CNs with varying degrees. Let D_v be the number of different variable node degrees, D_c be the number of different check node degrees. Then, the following functions can be defined as

$$\lambda(x) = \sum_{i=2}^{D_v} \lambda_i x^{i-1} = \lambda_2 x + \lambda_3 x^2 + \cdots + \lambda_{D_v} x^{D_v-1} \quad (8.50)$$

$$\rho(x) = \sum_{i=2}^{D_c} \rho_i x^{i-1} = \rho_2 x + \rho_3 x^2 + \cdots + \rho_{D_c} x^{D_c-1} \quad (8.51)$$

where λ_i is the fraction of edges that are connected to degree- i variable (bit) nodes, and ρ_i is the fraction of edges that are connected degree- i CNs. It should be noted that λ_i and ρ_i must satisfy that

$$\sum_{i=2}^{D_v} \lambda_i = 1 \quad \text{and} \quad \sum_{i=2}^{D_c} \rho_i = 1$$

The code rate can be expressed as

$$r = 1 - \frac{\int_0^1 \rho(x) dx}{\int_0^1 \lambda(x) dx} \quad (8.52)$$

Example 8.14 Find degree distribution of the following irregular code parity check matrix

$$H = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Solution $\lambda_2 =$ the fraction of edges connected to degree 2 bit nodes $= \frac{16}{22} = 0.7273$

$\lambda_3 =$ the fraction of edges connected to degree 3 bit nodes $= \frac{6}{22} = 0.2727$

$\rho_4 =$ the fraction of edges connected to degree 4 CNs $= \frac{12}{22} = 0.5455$

$\rho_5 =$ the fraction of edges connected to degree 5 bit nodes $= \frac{10}{22} = 0.4545$

Thus, the irregular code has degree distribution

$$\begin{aligned} \lambda(x) &= 0.7273x + 0.2727x^2 \\ \rho(x) &= 0.5455x^4 + 0.4545x^5 \end{aligned}$$

8.8.2 Ensemble Decoding Thresholds

The decoding threshold in terms of the noise standard deviation (σ^*) of a given degree distribution for iterative sum–product or min-sum decoding is defined as the supreme of the channel noises for which the probability of decoding error goes to zero as the number of iterations tends to infinity. Thus, the threshold can be expressed as

$$\sigma^* = \sup \left\{ \sigma > 0 : \lim_{i \rightarrow \infty} p_b^i(\sigma) = 0 \right\} \quad (8.53)$$

If $\sigma \leq \sigma^*$, $p_b^i(\sigma)$ converges to zero, otherwise converges to a value greater than zero.

The stability condition for AWGN channel is given by [11]

$$\lambda'(0)\rho'(1) < \exp\left(\frac{1}{2\sigma^2}\right) \quad (8.54)$$

whereas the stability condition for uncorrelated Rayleigh fading channel with SI is given by

$$\lambda'(0)\rho'(1) < 1 + \frac{1}{2\sigma^2} \quad (8.55)$$

The threshold value σ^* and the maximum allowed value σ_{\max} and the corresponding $\left(\frac{E_b}{N_o}\right)_s$ on the binary AWGN channel for various regular code parameters are given in Table 8.1 [12].

Table 8.1 Thresholding values on binary AWGN channel for Various regular code parameters

d_v	d_c	Rate	σ^*	$\left(\frac{E_b}{N_o}\right)^* \text{ dB}$	σ_{\max}	$\left(\frac{E_b}{N_o}\right)_{\max} \text{ dB}$
3	6	0.5	0.88	1.1103	0.979	0.1843
3	5	0.4	1.0	0	1.148	-1.1988
3	4	0.25	1.26	-2.0074	1.549	-3.8010
4	8	0.5	0.83	1.6184	0.979	0.1843
4	6	0.333	1.01	-0.0864	1.295	-2.2454
5	10	0.5	0.79	2.0475	0.979	0.1843

8.8.3 EXIT Charts for Irregular LDPC Codes in Binary Input AWGN Channels

Under the consistent Gaussian assumption, the mutual information ($I_{A,V}$) between the VN (a priori) inputs and the code bit associated with that VN can be computed by using the following approximation [11] for Eq. (6.20b). Thus,

$$I_{A,V} = J(\sigma) = \begin{cases} -0.0421061\sigma^3 + 0.209252\sigma^2 - 0.00640081\sigma & 0 \leq \sigma < 1.6363 \\ 1 - \exp(0.00181491\sigma^3 - 0.142675\sigma^2 - 0.0822054\sigma + 0.0549608) & 1.6363 \leq \sigma < 10 \\ 1 & \sigma \geq 10 \end{cases} \quad (8.56)$$

The approximation for inverse function $\sigma = J^{-1}(I_{A,V})$ is

$$\sigma = J^{-1}(I_{A,V}) \approx \begin{cases} 1.09542I_{A,V}^2 + 0.214217I_{A,V} + 2.33727\sqrt{I_{A,V}} & 0 \leq I_{A,V} \leq 0.3646 \\ -0.706692\log_e 0.386013(1 - I_{A,V}) - 1.75017I_{A,V} & 0.3646 < I_{A,V} \end{cases} \quad (8.57)$$

Using $J(\sigma)$, the EXIT chart of an irregular code $I_{E,V}$ describing the variable node function can be computed as follows.

$$I_{E,V} = \sum_{i=2}^{D_v} \lambda_i J\left(\sqrt{(i-1)[J^{-1}(I_{A,V})]^2 + \sigma_{ch}^2}\right) \quad (8.58)$$

where i is the variable node degree, $I_{A,V}$ is the mutual information of the message entering the variable node with the transmitted code word, $\sigma_{ch}^2 = 8R\frac{E_b}{N_0}$.

The EXIT chart of an irregular code $I_{E,C}$ describing the check node function can be computed as follows:

$$I_{E,C} = \sum_{i=2}^{D_c} \rho_i \left(1 - J\left(\sqrt{(i-1)}J^{-1}(1 - I_{A,C})\right) \right) \quad (8.59)$$

where i is the check node degree, $I_{A,C}$ is the mutual information of the message entering the check node with the transmitted code word.

In order for the decoding to converge to a vanishingly small probability of error, the EXIT chart of the VN has to lie above the inverse of the EXIT chart for the CNs.

Example 8.15 Consider the following rate 1/2 irregular LDPC codes with good degree distributions for a binary AWGN channel given in [13].

Code 1

$$\begin{aligned}\lambda(x) &= 0.33241x + 0.24632x^2 + 0.11014x^3 + 0.31112x^5 \\ \rho(x) &= 0.76611x^5 + 0.234389\end{aligned}$$

with a decoding EXIT threshold of $\frac{E_b}{N_o} = 0.6266$ dB.

Code 2

$$\begin{aligned}\lambda(x) &= 0.19606x + 0.24039x^2 + 0.00228x^5 + 0.05516x^6 \\ &\quad + 0.16602x^7 + 0.04088x^8 + 0.01064x^9 + 0.00221x^{27} + 0.28636x^{29} \\ \rho(x) &= 0.00749 + 0.99101x^8 + 0.0015\end{aligned}$$

with a decoding EXIT threshold of $\frac{E_b}{N_o} = 0.2735$ dB.

The EXIT charts of the two codes are shown in Fig. 8.7. From Fig. 8.7, it can be observed that the code 2 with lower threshold has better fit between variable node and check node EXIT curves.

The good degree distributions for rate 1/2 and 1/3 irregular LDPC codes for uncorrelated Rayleigh fading channels can be found in [14].

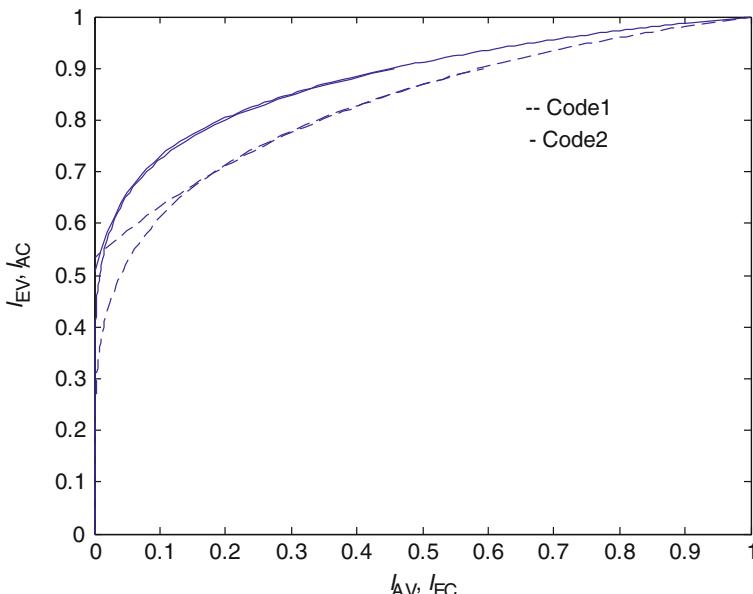


Fig. 8.7 EXIT charts for two irregular LDPC codes with different degree distributions on a binary AWGN channel

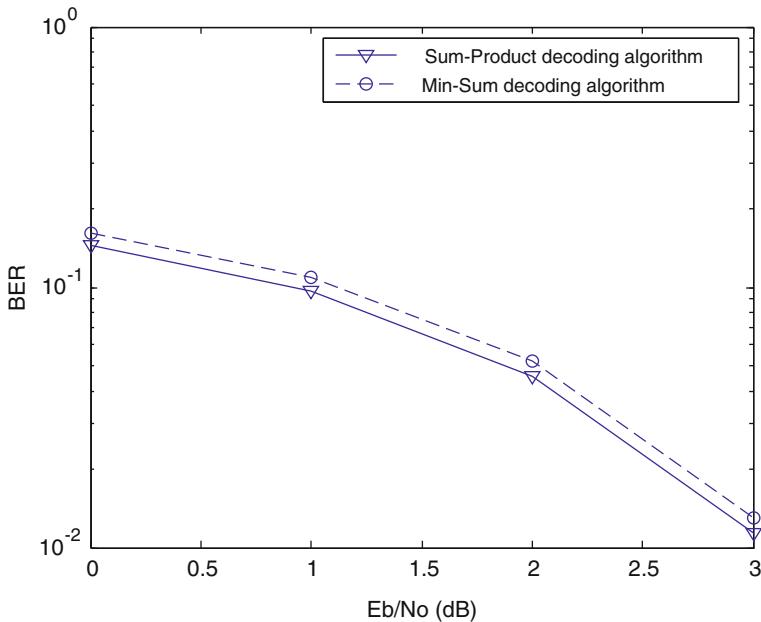


Fig. 8.8 BER performance of sum–product and min-sum decoding algorithms

8.9 Performance Analysis of LDPC Codes

8.9.1 Performance Comparison of Sum–Product and Min–Sum Algorithms for Decoding of Regular LDPC Codes in AWGN Channel

The BER performance of the sum–product and min-sum LDPC decoding algorithms is evaluated through a computer simulation assuming that the channel adds white Gaussian noise to the code generated by a (256, 3, 6) regular parity check matrix. In this simulation, four hundred frames of each of length 256 and three iterations are used. The BER performance of the sum–product and min-sum algorithms is shown in Fig. 8.8.

8.9.2 BER Performance Comparison of Regular and Irregular LDPC Codes in AWGN Channel

The performance of rate 1/2 regular and irregular codes having the same length is evaluated through a computer simulation. The BER performance of the two codes is shown in Fig. 8.9.

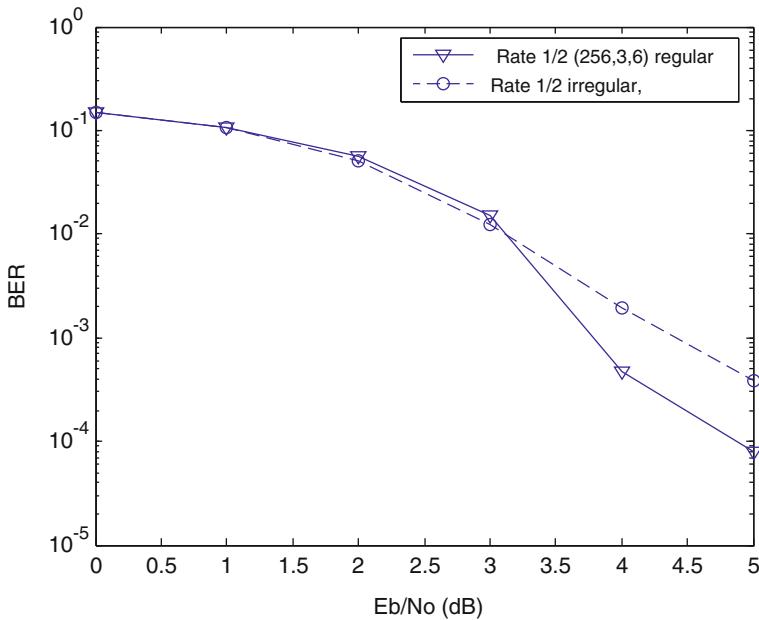


Fig. 8.9 BER performance of rate 1/2 regular and irregular LDPC codes using min-sum decoding algorithms

From Fig. 8.9, it is observed that there is no significant difference between the BER performance of the sum–product and the min-sum algorithms.

The irregular codes can have improved thresholds for long codes but with an error floor at higher BER than for regular codes of the same rate and length.

8.9.3 Effect of Block Length on the BER Performance of LDPC Codes in AWGN Channel

The effect of block length on the performance of LDPC codes is illustrated through a computer simulation. In this experiment, two 1/2 rate irregular codes of block lengths 256 and 512 are considered and added white Gaussian noise to them, and the noisy codes are decoded using min-sum decoding algorithm with 10 iterations. The BER performance of the two codes is shown in Fig. 8.10.

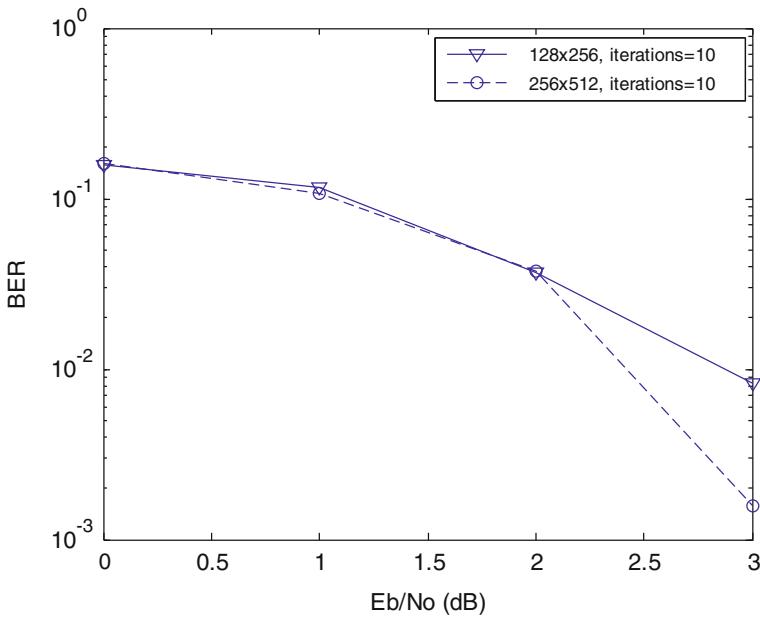


Fig. 8.10 BER performance of two 1/2 rate irregular LDPC codes using min-sum logarithm for decoding in AWGN channel

8.9.4 Error Floor Comparison of Irregular LDPC Codes of Different Degree Distribution in AWGN Channel

The error floor of an LDPC code is characterized by the phenomenon that as the SNR continues to increase, the error probability suddenly drops at a rate much slower than that in the region of low-to-moderate SNR can be approximated by [15].

$$\text{BER}_{\text{ef}} \approx \frac{2}{N} \frac{(\lambda_2 \rho(\mathbf{1})')^2}{4} Q\left(\sqrt{\frac{4RE_b}{N_o}}\right) \quad (8.60)$$

with the constraint $\lambda_2 \rho(\mathbf{1})' \leq E \exp\left(\frac{1}{2\sigma^2}\right)$. where E varies from 0 to 1, $E = 1$ for the traditional optimized degree distributions, E is greater than zero but less than 1 for constrained degree distributions, N is the length of the code and R is the code rate. A trade-off between the threshold and error floor can be achieved with the constrained distributions.

Example 8.16 Consider the following rate 1/4 irregular LDPC codes with optimal degree distribution and constrained degree distributions given in [15].

Code 1: Traditional code with optimal degree distribution with $E = 1$.

$$\lambda(x) = 0.431x + 0.2203x^2 + 0.0035x^3 + 0.0324x^5 + 0.1587x^6 + 0.1541x^9$$

$$\rho(x) = 0.0005x^2 + 0.9983x^3 + 0.0012x^4$$

Code 2: Code with constrained degree distribution with $E = 0.19$.

$$\lambda(x) = 0.0872x + 0.865x^2 + 0.0242x^3 + 0.0032x^5 + 0.0027x^6 + 0.0127x^9$$

$$\rho(x) = 0.0808x^2 + 0.8945x^3 + 0.0247x^4$$

Code 3: Code with constrained degree distribution with $E = 0.02$.

$$\lambda(x) = 0.0086x + 0.9711x^2 + 0.0006x^3 + 0.0059x^5 + 0.011x^6 + 0.0028x^9$$

$$\rho(x) = 0.0118x^2 + 0.9332x^3 + 0.055x^4$$

The error floor BER of the three codes is evaluated using Eq. (8.60) and shown in Fig. 8.11 along with the error floor region.

From Fig. 8.11, it can be observed that the codes with constrained degree distributions have yielded improved error floor performance. It indicates that a balance between threshold and error floor BER can be obtained.

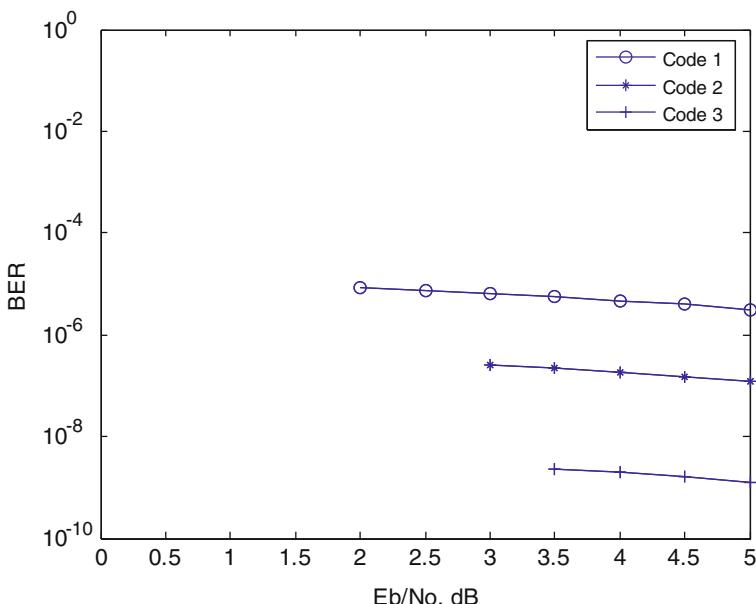


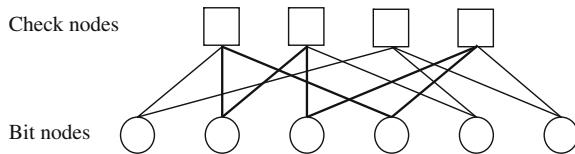
Fig. 8.11 The error floor BER of the three codes

8.10 Problems

1. Plot the Tanner graph for the following parity check matrix H . Show that the girth of the Tanner graph is 6

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

2. Find the girth of the Tanner graph given below



$$H = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

3. Determine the code word for LDPC code with following parity check matrix using efficient encoding method when the message sequence $s = [1\ 0\ 0\ 0\ 0\ 0\ 0]$

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

4. A code word is generated using the following parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

When the code word is sent through a BEC, the received signal is

$$y = [0 \ 0 \ 1 \ e \ e \ e]$$

Decode the received vector to recover the erased bits.

5. Consider the code word generated in Example 8.5. If it is sent through AWGN channel, the received vector after detector hard decision is $y = [1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1]$. Decode the received vector using bit-flipping algorithm and comment on the result.
6. A code word is generated with following parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

When the code word is sent through a BSC with crossover probability $\epsilon = 0.2$, the received signal is

$$y = [0 \ 0 \ 1 \ 0 \ 0 \ 0]$$

Decode the received vector using log domain sum–product algorithm.

7. Consider the code word generated in Example 8.6. If it is sent through AWGN channel with noise density $No = 0.3981$, the received vector is $y = [0.7271 \ -2.0509 \ -0.9209 \ -0.8185 \ 0.2766 \ -0.2486 \ -0.2497 \ -1.0237 \ 1.2065 \ 1.1102]$. Decode the received vector using sum–product algorithm and comment on the result.
8. Repeat the problem 6 using min-sum decoding algorithm and comment on the result
9. Find the degree distribution of the following irregular code parity check matrix

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

10. Obtain an EXIT chart for a rate 0.49303 irregular LDPC code with the following degree distribution at $\sigma^2 = 0.97869$.

$$\lambda(x) = 0.135x + 0.2816x^2 + 0.2576x^3 + 0.0867x^{33}$$

$$\rho(x) = x^{10}$$

8.11 MATLAB Exercises

1. Write MATLAB program to generate parity check matrix H having a normalized degree distribution (from node perspective) defined as

$$\lambda(x) = \sum_{i=1}^{\lambda_{\max}} \lambda_i x^i \quad \text{and} \quad \rho(x) = \sum_{i=1}^{\rho_{\max}} \rho_i x^i,$$

with $\lambda = [0 \ 0.4994 \ 0.3658 \ 0 \ 0 \ 0 \ 0.0581 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0.0767]$;
 $\rho = [0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1]$;

2. Write a MATLAB program to compare the performance of LDPC codes in AWGN and Rayleigh fading channels.

References

- Gallager, R.G.: Low-density parity-check codes. *IRE Trans. Inf. Theor.* 21–28 (1962)
- Fan, J.L.: Array codes as low-density parity-check codes. In: Proceedings of 2nd International Symposium on Turbo Codes and Related Topics, Brest, France, 4–7 Sept 2000, pp. 543–546
- Honary, B., et al.: On construction of low density parity check codes. In: 2nd International Workshop on Signal Processing for Wireless Communication (SPWC 2004), London, UK, 2–4 June 2004
- Ammar, B., Honary, B., Xu, Y., Lin, S.: Construction of low-density parity-check codes on balanced incomplete block designs. *IEEE Trans. Inf. Theor.* **50**(6), 1257–1268 (2004)
- Miladinovic, N., Fossorier, M.: Systematic recursive construction of LPDC codes. *IEEE Commun. Lett.* **8**(5), 302–304 (2004)

6. Johnson, S.J.: Iterative Error Correction Turbo, Low- Density Parity-Check and Repeat-Accumulate Codes. Cambridge University Press, Cambridge (2010)
7. Xiao, Y., Lee, M.-H.: Low complexity MIMO-LDPC CDMA systems over multipath channels. IEICE Trans. Commun. **v E89-B(5)**, 1713–1717 (2006)
8. MacKay, D.J.C., Neal, R.M.: Near Shannon limit performance of low density parity check codes. Electron. Lett. **33**, 457–458 (1997)
9. Richardson, T., Urbanke, R.: Efficient encoding of low-density parity-check codes. IEEE Trans. Inf. Theor. **47**(2), 638–656 (2001)
10. Ryan, W.E., Lin, S.: Channel Codes Classic and Modern. Cambridge University Press, Cambridge (2009)
11. ten Brink, S., Kramer, G., Ashikhmin, A.: Design of low-density parity-check codes for modulation and detection. IEEE Trans. Commun. **52**(4), 670–678 (2004)
12. Richardson, T.J., Urbanke, R.L.: The capacity of low-density parity-check codes under message-passing decoding. IEEE Trans. Inf. Theor. **47**(2), 599–618 (2001)
13. Richardson, T.J., Amin Shokrollahi, M., Urbanke, R.L.: Design of capacity-approaching irregular low-density parity-check codes. IEEE Trans. Inf. Theor. **47**(2), 619–637 (2001)
14. Hou, J., Siegel, P.H., Milstein, L.B.: Performance analysis and code optimization of low density parity-check codes on rayleigh fading channels. IEEE J. Sel. Areas Commun. **19**(5), 924–934 (2001)
15. Johnson,S.J., Weller, S.R.: Constraining LDPC degree distributions for improved error floor performance. IEEE Commun. Lett. **10**(2), 103–105, (2006)

Chapter 9

LT and Raptor Codes

To partially compensate the inefficiency of random codes, we can use Reed–Solomon codes, these codes can be decoded from a block with the maximum possible number of erasures in time quadratic in the dimension. But in practice, these algorithms are often too complicated and quadratic running times are still too large for many applications. Hence, a new class of codes is needed to construct robust and reliable transmission schemes and such a class of codes is known as fountain codes. This fountain codes should possess a fast encoder and decoder to work in practice. Luby invented the first class of universal fountain codes [1], in which the decoder is capable of recovering the original symbols from any set of output symbols whose size is close to optimal with high probability. The codes in this class are called LT codes. It is important to construct universal Fountain codes to many applications which have fast decoding algorithms and the average weight of an output symbol is a constant, such a class of Fountain codes are called as *Raptor codes* [2] and the basic idea behind Raptor codes is a pre-coding of the input symbols prior to the application of an appropriate LT code. This chapter discusses the encoding and decoding of LT and Raptor codes.

9.1 LT Codes Design

The rateless LT codes generate the limitless number of output symbols by using the encoding of a finite number of message symbols.

By receiving a given number of output symbols, each receiver can decode them successfully. The LT codes are the first universal erasure-correcting codes that provide successful communication over a binary erasure channel (BEC) for any erasure probability. The LT codes have a various types of applications and advantages.

Electronic supplementary material The online version of this chapter (doi:[10.1007/978-81-322-2292-7_9](https://doi.org/10.1007/978-81-322-2292-7_9)) contains supplementary material, which is available to authorized users.

In particular, a transmitter having a LT code uses a single code for efficient transmission in broadcast networks, where a single transmitter transferring a message to multiple receivers simultaneously over different channels.

The transmitter with information message u consisting of k source symbols generates an infinite number of encoding symbols, which are broadcasted successively. Due to the property of an *ideal Fountain code*, the receiver is able to reconstruct the entire source message reliably from any k received encoding symbols. If symbols are erased, an ideal Fountain code receiver will just wait for k encoding symbols before reconstruct the information message.

In the practical implementations of LT code, random number generator was employed to determine the degree and neighbors of an encoding symbol. However, the key to make LT code work well is the degree distribution used in the encoding procedure.

9.1.1 LT Degree Distributions

Choosing a good degree distribution is the key to make LT code work well in practice and a couple of them are as follows:

A good degree distribution should meet the following two requirements: First, as few encoding symbols as possible on average are required to ensure successful recovery of source symbols; Secondly, the average degree of the encoding symbols shall be as low as possible.

Ideal Soliton Distribution [1]

Addition of input symbols to the ripple at the same rate as they are processed is the basic property required for a good degree distribution and hence the name Soliton distribution, as a soliton wave balances dispersion and refraction perfectly. The ideal soliton distribution is given by

$$\mu_{ISD}(i) = \begin{cases} 1/k & i = 1 \\ 1/i(i-1) & i = 2, 3, \dots, k \end{cases} \quad (9.1)$$

Ideal soliton distribution ensures that at each subsequent step, all the release probabilities are identical to $1/k$. When the number of encoding symbols is equal, there is one expected ripple generated at each processing step and the source symbols can be ideally recovered after k processing step. In practice, ideal soliton distribution works poorly.

Robust Solition Distribution [1]

Define $R_{SD} = c \cdot \ln(k/\varepsilon) \sqrt{k}$. In this distribution, we computed μ_{RSD} as follows:

$$\tau(i) = \begin{cases} R_{SD}/ik & i = 1, 2, \dots, \text{round}(k/R_{SD}) - 1 \\ R_{SD} \ln(R_{SD}/\varepsilon)/k & i = \text{round}(k/R_{SD}) \\ 0 & \text{else} \end{cases} \quad (9.2)$$

$$\beta = \sum_{i=1}^k \mu_{ISD}(i) + \tau(i)$$

$$\mu_{R_{SD}}(i) = (\mu_{ISD}(i) + \tau(i))/\beta, \quad i = 1, 2, \dots, k \quad (9.3)$$

Robust solition distribution is an improvement of the ideal solition distribution which is not only viable but practical too.

The term R_{SD} is used for the RSD above is thought as the size of the ripple.

R_{SD} is simply understood as the number of information symbols, and at each decoding step, its degree is one. The ripple is the set of covered input symbols that have not yet been processed. By following relation, we can predetermined this value

$$R_{SD} = c \cdot \ln(k/\varepsilon) \sqrt{k}, \quad (9.4)$$

where c and ε are two parameters. c controls the mean of degree distribution and ε is the allowable failure probability of the decoder to recover the source symbols. The smaller the value of c , the greater the probability of low degrees.

In the encoding for LT codes, the degree distribution of information symbols and output symbols should be a uniform distribution and a RSD, respectively.

Luby suggested that the number of received encoded symbols be βk . Then, the corresponding decoding overhead is

$$\begin{aligned} \varepsilon &= n/k - 1 \\ &= 1/R_{SD} - 1 \\ &= \beta - 1 \end{aligned} \quad (9.5)$$

The average degree increases logarithmically versus the code dimension. As the code dimension k is getting larger, the overhead decreases; this is because β is a decreasing function with k , but the sparseness of the generator matrix becomes lower and lower.

9.1.2 Important Properties of the Robust Soliton Distribution

Property 1: The number of encoding symbols is $n = k + O(\sqrt{k} \cdot \ln^2(k/\epsilon))$.

Property 2: The average degree of an encoding symbol is $D = O(\ln(k/\epsilon))$.

Property 3: The decoder fails to recover the data with probability at most ϵ from a set of n encoding symbols.

One can refer [1] for proofs of these properties.

9.1.3 LT Encoder

The stepwise procedure to produce infinite output symbols, from k input symbols $\{S_1, S_2, \dots, S_k\}$ is as follows:

Step 1: Consider an output degree d randomly from a degree distribution $\rho(d)$

Step 2: Select d distinct input symbols uniformly at random from $\{S_1, S_2, \dots, S_k\}$

Step 3: Perform exclusive-OR of these d input symbols to obtain the output symbol

$$c_i = S_{i,1} \oplus S_{i,2} \oplus \dots \oplus S_{i,d}$$

A generator matrix G also can be defined such that the output symbols can be expressed as follows:

$$c = s \cdot G, \quad (9.6)$$

where s denotes the input vector. Modulus-2 addition is used during the matrix multiplication.

The following MATLAB function generates the matrix G by using robust soliton density.

Program 9.1 MATLAB function to generate G using robust soliton density

```

function G = Grsd(K, N)
if nargin < 3
    ColTH = 1.3; %bound for number of 1's in each column
end
if nargin < 4
    Num_Try = 10;
end
G_Try = {};
Mean_SR = zeros(1, Num_Try);
Min_SR = zeros(1, Num_Try);
for Ind_Try = 1: Num_Try
    while(1)
        %create pdf
        c = 0.2;
        delta = 0.5;
        R_SD = c*log(K/delta)*sqrt(K);
        rho = zeros(1, K);
        thu = zeros(1, K);
        d = 1: K;
        rho(1) = 1/K;
        rho(2:K) = 1 ./ (d(2:end) .* (d(2:end)-1));
        loc = floor(K/R_SD-1);
        thu(1: loc) = R_SD/K ./ d(1: loc);
        thu(loc+1) = R_SD/K*log(R_SD/delta);
        Z = sum(rho + thu);
        mu = (rho + thu) / Z;
        %threshold for maximum number of ones per column
        MaxColTH = K/R_SD * ColTH;
        G = zeros(K, N);
        for n = 1: N
            while(1)
                %draw a number
                Cmu = cumsum(mu)/sum(mu);
                u = rand(1,1);
                diff = abs(u - Cmu);
                [M, loc] = min(diff);
                Num = d(loc);
                if Num <= MaxColTH
                    break;
                end
            end
            row = randperm(K);
            G(row(1: Num), n) = 1;
        end
        SR = sum(G, 2);
        if min(SR) > 0
            Mean_SR(Ind_Try) = mean(SR);
            Min_SR(Ind_Try) = min(SR);
            G_Try{Ind_Try} = sparse(G);
            break;
        end
    end
end
%maximize weight per row and minimize weight per col
[V, loc] = max(Mean_SR);
G = G_Try{loc};
G = full(G);

```

9.1.4 Tanner Graph of LT Codes

The Tanner Graph of LT codes is similar to the Tanner graph used in LDPC codes, whereas the check nodes and variable nodes usually used in LDPC codes are replaced with input nodes and output nodes of LT codes as shown in Fig. 9.1.

9.1.5 LT Decoding with Hard Decision

The decoder uses the Decoder recovery rule [1] to repeatedly recover input symbols. The Decoder recovery rule is as follows:

If there is at least one encoding symbol that has exactly one neighbor then the neighbor can be recovered immediately since it is a copy of the encoding symbol. The value of the recovered input symbol is exclusive-ORed into any remaining encoding symbols that also have that input symbol as a neighbor, the recovered input symbol is removed as a neighbor from each of these encoding symbols and the degree of each such encoding symbol is decreased by one to reflect this removal.

Based on the above rule, the stepwise decoding process can be described as follows:

Step 1: Find an output symbol y_i connected to only one input symbol m_j .

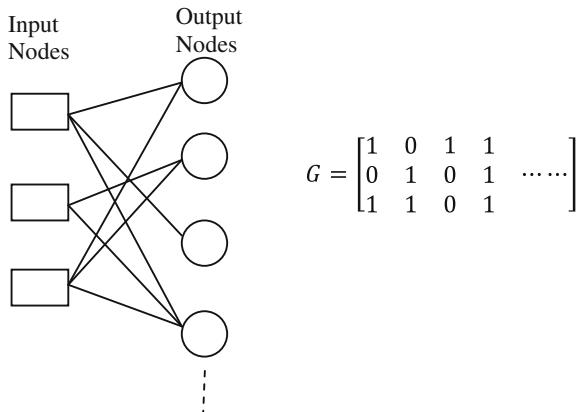
Step 2: Set $m_j = y_i$.

Step 3: Exclusive-OR m_j to all the output symbols connected to m_j .

Step 4: Remove all the edges connected to m_j .

Step 5: Repeat step 1 to 4 until all input symbols are recovered.

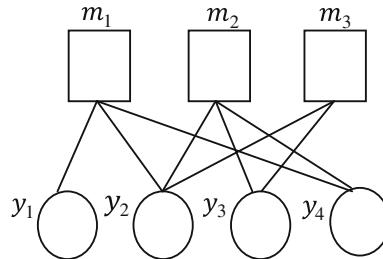
Fig. 9.1 Tanner graph of LT codes



The output degree distribution is a critical part of LT codes. If there is no output symbol with degree one during the iteration, the decoding process will halt, which indicates a decoding failure. Thus, optimal output degree is required to ensure a successful decoding. In Luby's paper, two output degree distributions, i.e., ideal soliton distribution and robust soliton distribution, are presented [1].

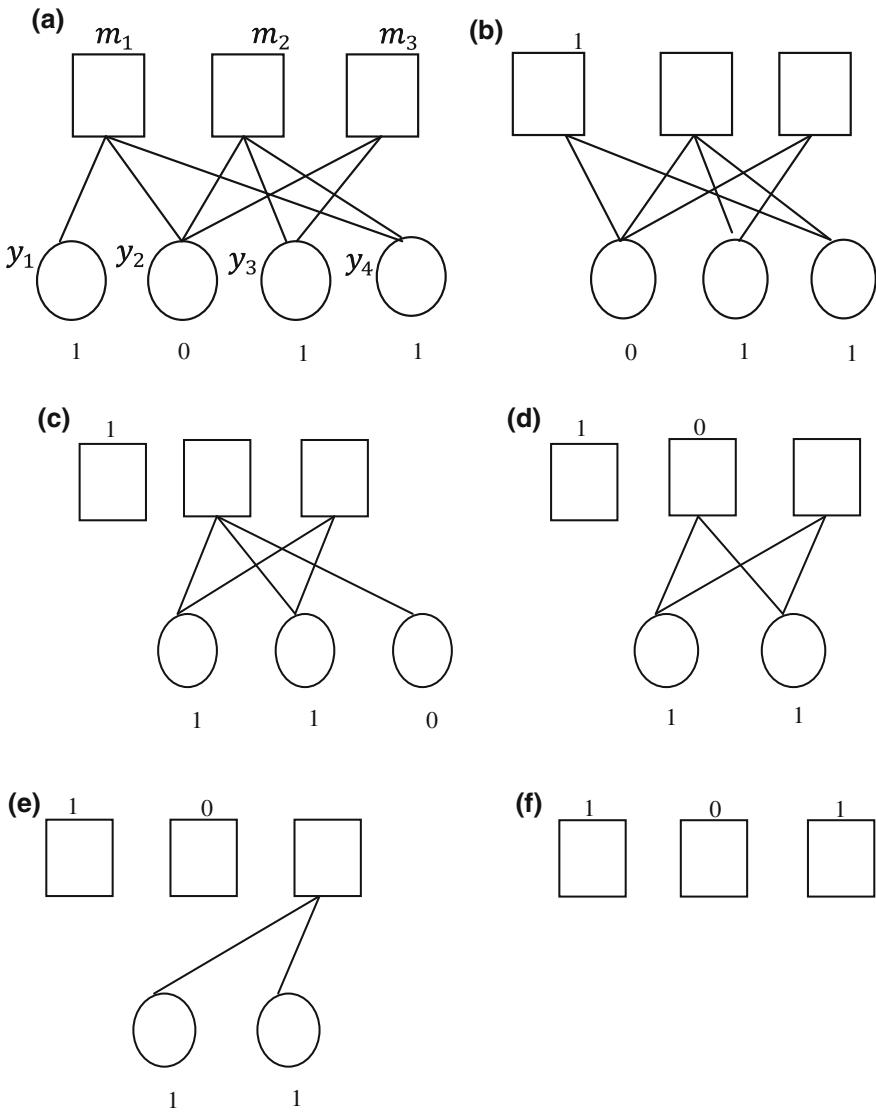
Ideal soliton distribution adds only one input node to the ripple each iteration round, consuming the fewest output symbols to recover all of the input symbols. However, it performs poorly in practice because the probability of ripple vanishing, i.e., the error probability or the decoding failure rate is high. Robust soliton distribution attempts to lower the error probability by slightly increasing the probability of degree one. The following example illustrates the decoding process.

Example 9.1 Consider the following Tanner graph of a LT code



and if the received bits vector $y = [1 \ 0 \ 1 \ 1]$. Decode the received bits vector to obtain the message bits.

Solution The boxes represent the message bits, while circles represent output bits. An output bit is the factor graph. There are three message bits and four output bits, which have values $y_1 y_2 y_3 y_4 = [1 \ 0 \ 1 \ 1]$. During the first iteration, the only output bit that is connected to one message bit is the first output bit (see Fig. a). This value is copied to m_1 , delete the output bit (see Fig. b), and then the new value of m_1 gets added to y_2 and y_4 . This disconnects m_1 from the graph (see Fig. c). At the start of the second iteration, y_4 is connected to the single message bit m_2 . Now one sets m_2 equal to y_4 (see Fig. d), and then adds this value to y_2 and y_3 . This disconnects m_2 from the graph (see Fig. e). Finally, one sees that the output bits connected to m_3 are equal as expected and can be used to restore m_3 (see Fig. f).



For success of the LT decoder with high probability, decoding graph of LT codes needs to have at least $k \ln(k)$ edges. In [2], Raptor codes are introduced to relax this lower bound on the number of edges in the decoding graph.

9.1.6 Hard-Decision LT Decoding Using MATLAB

The following example illustrates decoding of LT codes using MATLAB.

Example 9.2 Write a MATLAB program to implement hard-decision LT decoding assuming received vector $y = [1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1]$ when the following generator matrix is used to encode the code word.

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Solution The following MATLAB program decodes the received vector y . The output of the program gives the decoded vector $[0 \ 0 \ 1 \ 1]$.

Program 9.2 MATLAB program for Hard Decision LT Decoding

```

clear all;clc;
G=[ 1 1 0 1 0 0 0;0 0 0 1 1 0 0 1;1 0 0 1 1 0 0;0 0 1
0 1 1 1];
Y=[1 0 1 1 0 1 1]';
Yd=decodeLT(G,Y,1);

function Yd = decodeLT(G, Y, B)
K = size(G, 1);
N = size(G, 2);
GT = G;
Yd = -ones(K, 1);
Summer = zeros(1, K);
while(1)
    loc = find(sum(GT,1) == 1);
    if isempty(loc)
        %code fails
        break;
    end
    for ind = 1: length(loc)
        pos = find(GT(:, loc(ind)) == 1);
        loc2 = find(GT(pos, :) == 1);
        GT(pos, :) = 0;
        Summer(pos) = 1;
        Yd(pos) = Y(loc(ind));
        Y(loc2) = mod(Y(loc2)-Yd(pos), 2^(B));
    end
    if sum(Summer) == K
        break;
    end
end

```

9.1.7 BER Performance of LT Decoding over BEC Using MATLAB

At the receiving end, a receiver collects $n = k(1 + \eta)$ output symbols. Here, η is called the overhead. Note that several erasures need to be discarded till n unerased output symbols are obtained. The following MATLAB program illustrates the BER performance of LT codes over BEC for different overheads and for different erasure probabilities.

Program 9.3 MATLAB program for the BER Performance of LT Decoding over BEC

```

clear all; clc;
K=1000; frame=100;
M=[500 600 700 800 900 1000];
Pe=[0.1 0.2 0.3 ];
for ii=1:length(Pe)
    for i = 1:length(M )
        G=Grsd(K,(K+M(i)));
        ber1(i) = 0;
        for j = 1:frame
            msg = randi(255,125,1);
            Bits = (dec2bin(msg, 8))';
            Bits = (Bits(:))';
            BitsVec = zeros(1, length(Bits));
            for Ind = 1: length(Bits)
                BitsVec(Ind) = str2double(Bits(Ind));
            end
            Y=mod(G'*BitsVec',2);
            ErrLocBit = find(rand(length(Y), 1)< Pe(ii));
            ErasureBit = zeros(length(Y),1);
            ErasureBit(ErrLocBit)= 1;
            Y(ErasureBit==1)=[];
            DecBits = decodeLT(G(:,ErasureBit==0),Y);
            DecBits(find(DecBits < 0)) = 0;
            DecBits = DecBits';
            %calculate error
            [numl,rat1]=biterr(DecBits,BitsVec);
            ber1(i) = (ber1(i)+rat1);
        end % for j
        ber1(i) = ber1(i)/frame; % Get average of BER
    end % for i
    ber(ii,:)=ber1;
end
semilogy(M/1000, ber(1,:), '-v');
hold on
semilogy(M/1000, ber(2,:), '-d');
semilogy(M/1000, ber(3,:), '-s');
xlabel('Overhead'); ylabel('BER')
legend('Pe=0.1','Pe=0.2','Pe=0.3')

```

The overhead versus BER performance of LT decoding obtained from the above program for three different erasure probabilities is shown in Fig. 9.2.

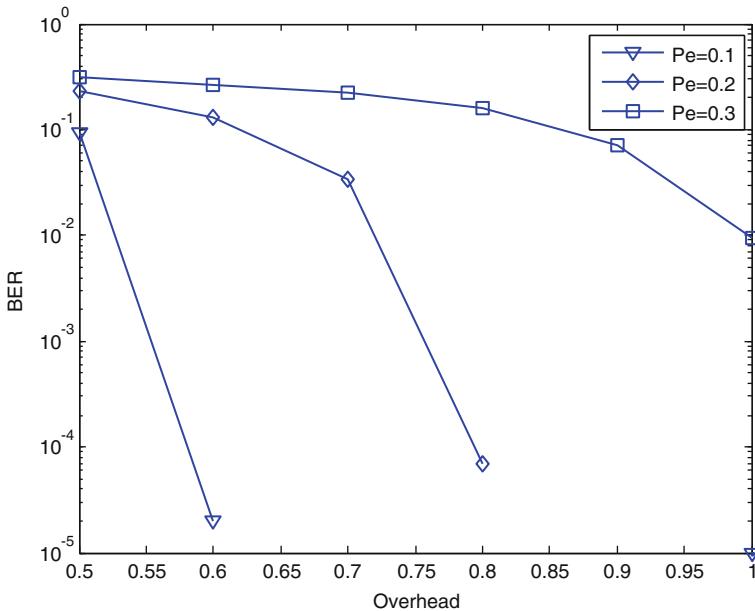


Fig. 9.2 BER performance of LT decoding over BEC

From Fig. 9.2, it is observed that the BER decreases as overhead increases for a fixed erasure probability and further the BER for low erasure probability is less than that the high erasure probability.

9.2 Systematic LT Codes

Many researchers endeavored to improve the performance of LT codes to protect the data over the wireless Internet, where fading, noise, and packet erasures are encountered. For the sake of improving, the error correction capability of LT codes and the complexity of these schemes tend to be increased. The soft decoding of LT codes is using the probabilistic decoding technique of low density parity check codes (LDPC) [3].

Hence, to improve the LT code's performance in hostile wireless channels, a systematic LT code as shown in Fig. 9.3 has been suggested in [4] by expanding LT code's $[K \times N]$ generator matrix with the aid of a unity matrix having a size of $[K \times K]$.

The relation between the systematic LT generator matrix G and the parity check matrix H is as follows:

Consider a generator matrix $G_{K \times N} = [I_{K \times K}/A_{K \times M}]$, where I is an identity matrix having a size of $[K \times K]$ and A is a non-singular matrix having a size of $[K \times M]$.

1 0 0 0 0 0 0 0 0	1 0 1 1 1 1 1 1 1 0 1 1 1 1 0
0 1 0 0 0 0 0 0 0	0 0 0 0 0 1 0 0 0 0 0 1 0 1 0
0 0 1 0 0 0 0 0 0	1 1 0 1 1 1 1 1 1 0 1 1 1 0
0 0 0 1 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 1
0 0 0 0 1 0 0 0 0	0 0 0 0 0 0 1 0 0 0 0 1 0 0 0
0 0 0 0 0 1 0 0 0	0 0 0 0 1 0 0 0 0 0 0 0 1 0 0
0 0 0 0 0 0 1 0 0	1 1 1 1 1 1 1 0 0 0 0 1 1 0 0
0 0 0 0 0 0 0 1 0	1 1 0 1 1 1 1 0 0 0 1 1 1 1 1

K N

Fig. 9.3 The systematic LT generator matrix

Then, the parity check matrix is calculated as $H = [A^T / I']$, where A^T is the transpose of A and I' is an identity matrix having a size of $[M \times M]$ [5], where $N = K + M$ is the number of columns in G and K is the number of rows in G .

9.2.1 Systematic LT Codes Decoding

The implementation of the LT decoding process is similar to that of the classic LDPC decoding procedure. The LT decoder's soft values are set to a value corresponding to the demodulator's soft output. The decoder's soft values which denote the log likelihood ratios (LLRs) are passed from the check nodes to the variable nodes and vice versa are then iteratively updated after each decoding iteration.

The LT decoder outputs its tentative hard decision and checks after each iteration whether the product of the corresponding code word and the transpose of the PCM H is equal to zero, if not, the LT decoding process will be continued iteratively until the output code word becomes legitimate or the maximum affordable number of iterations is exhausted.

9.2.2 BER Performance Analysis of Systematic LT Codes Using MATLAB

9.2.2.1 BER Performance of Systematic LT Codes Over BEC

The performance of the systematic LT(1000, 3000) code on BEC channel with erasure probabilities $[0.1 \ 0.2 \ 0.4 \ 0.6 \ 0.8]$ is illustrated using the following MATLAB program. In this, the Robust Soliton degree distribution with parameters $c = 0.1$ and $\varepsilon = 0.5$ is used.

Figure 9.4 shows the performance analysis of the systematic LT code over the BEC having different erasure probabilities ρ_e .

Program 9.4 MATLAB program for the BER Performance of systematic LT code in BEC channels

```

clear all; clc;
K=1000;
M=1000;
Pe = [0.1 0.2 0.4 0.6 0.8 ];
frame=10;
A1=GenerateGrsd(K,M);
G1=[eye(K) A1];
H1=[ A1' eye(M)];
[N1 N2]=size(H1);
for i = 1:length(Pe )
    ber1(i) = 0;
    for j = 1:frame
        msg = randi(255,125,1);
        Bits = (dec2bin(msg, 8))';
        Bits = (Bits(:))';
        BitsVec = zeros(1, length(Bits));
        for Ind = 1: length(Bits)
            BitsVec(Ind) = str2double(Bits(Ind));
        end
        F1=mod(G1'*BitsVec', 2);
        xHat1b=bec_channel(F1,Pe(i));
        xHat1be=becebest(xHat1b,H1,50);
        [num1, rat1] = biterr(abs(xHat1be(1:1000)'),F1(1:1000)');
        ber1(i) = (ber1(i) + rat1);
    end % for j
    % Get average of BER
    ber1(i) = ber1(i)/frame;
end % for
semilogy(1-Pe, ber1, '-v');
xlabel('1-Pe');
ylabel('BER')

function [y] = bec_channel(x, e) %BEC_CHANNEL Simulates binary erasure channel with
erasure probability e
y = x;
y( rand(size(abs(x)))<e ) =1;% = erasure, otherwise 0s and 1s are bits
end

function M=becebtest(xHat1b,H1,iter)
H=H1;
M=xHat1b;
[N1 N2]=size(H);
for i=1:iter
    for j=1:N1
        ci = find(H(j,:));
        d=find(M(ci)==-1);
        d1=find(M(ci)==-1);
        if ((length(d)>=2) & (length(d1)==1))
            E(j,ci(d1))=mod(sum(M(ci(d))),2);
        else
            E(j,ci(d1))=-1;
        end
    end
    for j=1:N2
        ri = find(H(:,j));
        if(M(j)==-1)
            for ii=1:length(ri)
                if( E(ri(ii),j)~-1)
                    M(j)=E(ri(ii),j);
                end
            end
        end
    end
end
end
end

```

9.2.2.2 BER Performance of Systematic LT Codes Over AWGN Channel

The performance of the systematic LT(1000, 2000) code on AWGN channel is illustrated using the following MATLAB program. In this, the Robust Soliton degree distribution with parameters $c = 0.1$ and $\varepsilon = 0.5$ is used.

Figure 9.5 shows the performance analysis of the systematic LT code over the AWGN having different E_b/N_0 s.

Program 9.5 MATLAB program for the BER Performance of systematic LT code in AWGN channels using BPSK modulation

```

clear all; clc;
K=1000;M=1000; frame=10;
EbN0 = [ 0 1 2 3 4 ];
iter1=1;iter2=2;iter4=4;iter6=6;
A1=GenerateGrsd(K,M);
G1=[eye(K) A1];
H1=[ A1' eye(M) ];
[N1 N2]=size(H1);
for i = 1:length(EbN0)
    ber1(i) = 0;
    ber2(i) = 0;
    ber3(i) = 0;
    ber4(i) = 0;
    for j = 1:frame
        msg = randi(255,125,1);
        Bits = (dec2bin(msg, 8))';
        Bits = (Bits(:))';
        BitsVec = zeros(1, length(Bits));
        for Ind = 1: length(Bits)
            BitsVec(Ind) = str2double(Bits(Ind));
        end
        F1=mod(G1'*BitsVec', 2);
        bpskMod1 = 2*F1 - 1;
        N0 = 1/(exp(EbN0(i)*log(10)/10));
        Ftx1 = bpskMod1 + sqrt(N0)*randn(size(bpskMod1 ));
        L1 =(-4*Ftx1./N0)';
        xHat1=logsumproduct(L1,H1,N1,N2,iter);
        xHat2=logsumproduct(L1,H1,N1,N2,iter2);
        xHat3=logsumproduct(L1,H1,N1,N2,iter4);
        xHat4=logsumproduct(L1,H1,N1,N2,iter6);
        [num1,rat1]= biterr(abs(xHat1(1:1000)'),F1(1:1000));
        [num2,rat2]= biterr(abs(xHat2(1:1000)'),F1(1:1000));
        [num3,rat3]= biterr(abs(xHat3(1:1000)'),F1(1:1000));
        [num4,rat4]= biterr(abs(xHat4(1:1000)'),F1(1:1000));
        ber1(i) = (ber1(i) + rat1);
        ber2(i) = (ber2(i) + rat2);
        ber3(i) = (ber3(i) + rat3);
        ber4(i) = (ber4(i) + rat4);
    end % for j
    % Get average of BER
    ber1(i) = ber1(i)/frame;
    ber2(i) = ber2(i)/frame;
    ber3(i) = ber3(i)/frame;
    ber4(i) = ber4(i)/frame;
end % for i
semilogy(EbN0, ber1, '-v');hold on
semilogy(EbN0, ber2, '-d');semilogy(EbN0,ber3,'-s');
semilogy(EbN0, ber4, '-*');
legend('Systematic LT(1000,2000),AWGN channel, iterations=1',...
    'Systematic LT(1000, 2000),AWGN channel, iterations=2',...
    'Systematic LT(1000, 2000),AWGN channel, iterations=4',...
    'Systematic LT(1000, 2000),AWGN channel, iterations=6')
xlabel('Eb/N0(dB)');
ylabel('BER')

```

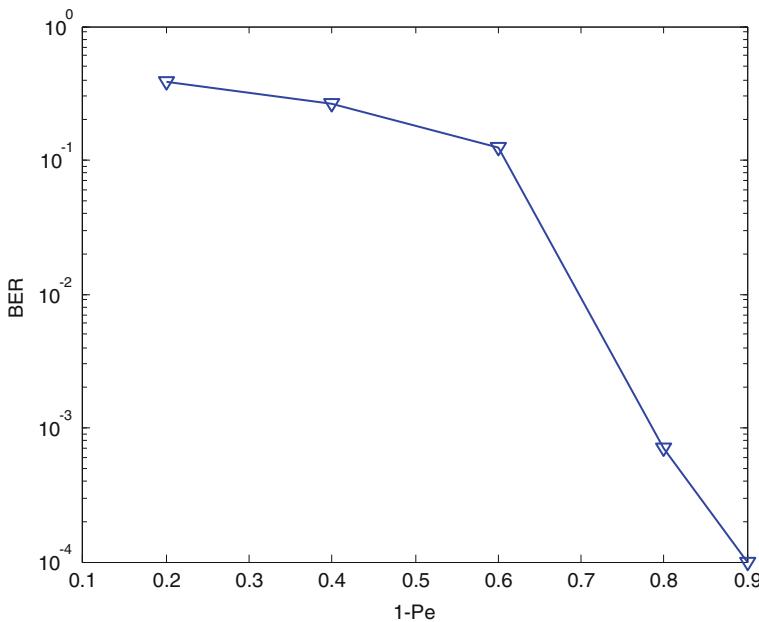


Fig. 9.4 BER versus 1-Pe performance of the systematic LT code in BEC channels

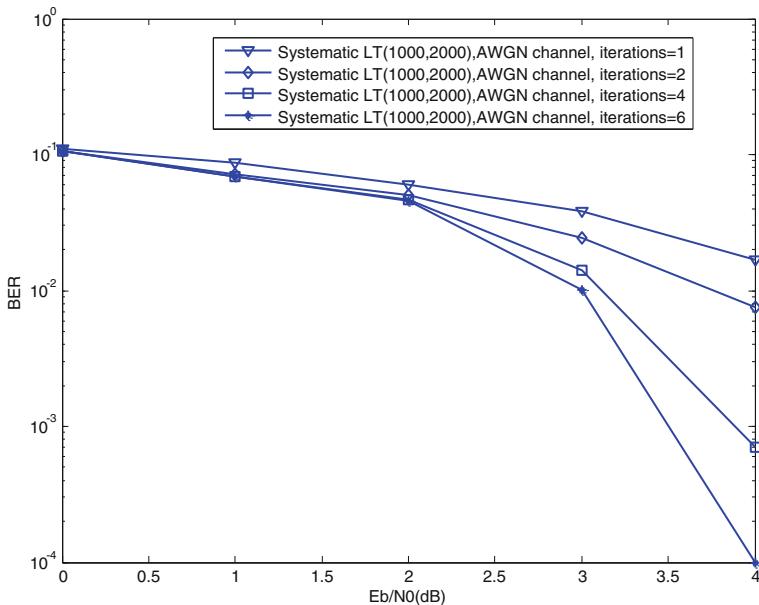


Fig. 9.5 BER versus E_b/N_0 performance of the systematic LT code in AWGN channels using BPSK modulation

9.2.2.3 BER Performance of Systematic LT Codes Over AWGN-Contaminated BEC

The schematic of the encoding and decoding of the LT coding over AWGN-contaminated BEC is shown in Fig. 9.6.

The performance of the systematic LT(1000, 3000) code on AWGN-contaminated BEC with erasure probability 0.1 is shown in Fig. 9.7. In this, the Robust Soliton degree distribution with parameters $c = 0.1$ and $\varepsilon = 0.5$ is used.

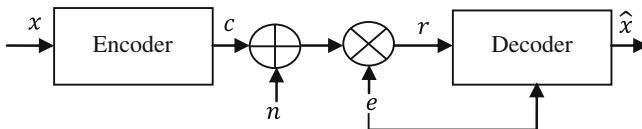


Fig. 9.6 LT encoding and decoding over AWGN-BEC

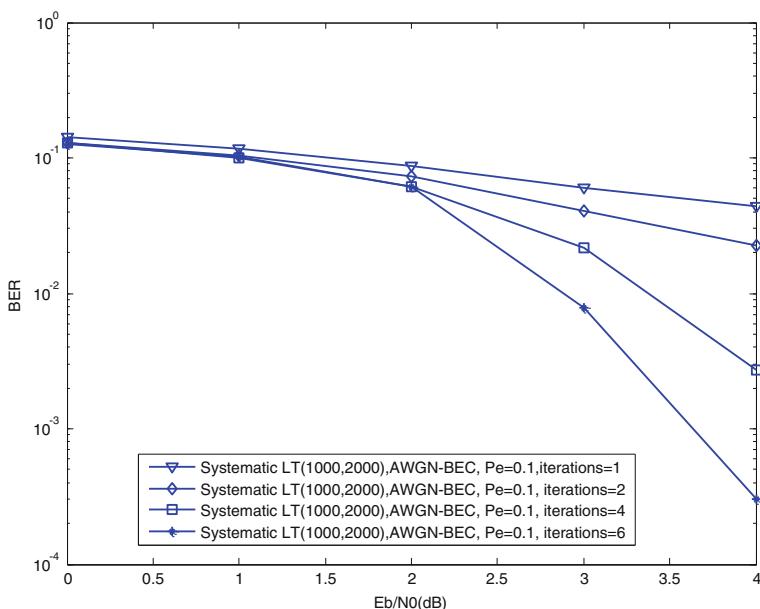


Fig. 9.7 BER versus Eb/N0 performance of the systematic LT code in AWGN-contaminated BEC channel

9.3 Raptor Codes

Raptor codes are concatenation of an erasure-correcting pre-code and an LT code [2]. Figure 9.8 shows a graphical presentation of a Raptor code. The output symbols of the Raptor code are sampled independently from the distribution. Low density parity check (LDPC) codes and Tornado codes are examples of the pre-code. The decoding graph of the LT code with k -symbol message block should have at least $k \ln(k)$ edges, which results in large overhead or higher complexity of encoding and decoding. The raptor codes reduce the lower bound on the number of edges in the bipartite graph, and hence, recover message symbols at a lower overhead at almost linear complexity. The pre-code of the raptor code recovers the Message symbols that are left undecoded by the LT decoders due to lower head.

Raptor codes are being used in commercial systems of Digital Fountain. For example, a Silicon Valley-based startup specializing in fast and reliable delivery of data over heterogeneous networks.

The k symbols are input symbols of a Raptor code which are used to construct the code word in C consisting of n *intermediate symbols* and output symbols are the symbols generated by the LT code from the n intermediate symbols.

Raptor code encoding algorithm is as follows: an encoding algorithm for \mathcal{C} is used to generate a code word in \mathcal{C} corresponding to the given k input symbols. Then, an encoding algorithm for the LT code with distribution $\Omega(x)$ is used to generate the output symbols.

Raptor code decoding algorithm of length m can recover the k input symbols from any set of m output symbols and errors with probability which is at most $1/k^c$ for some positive constant.

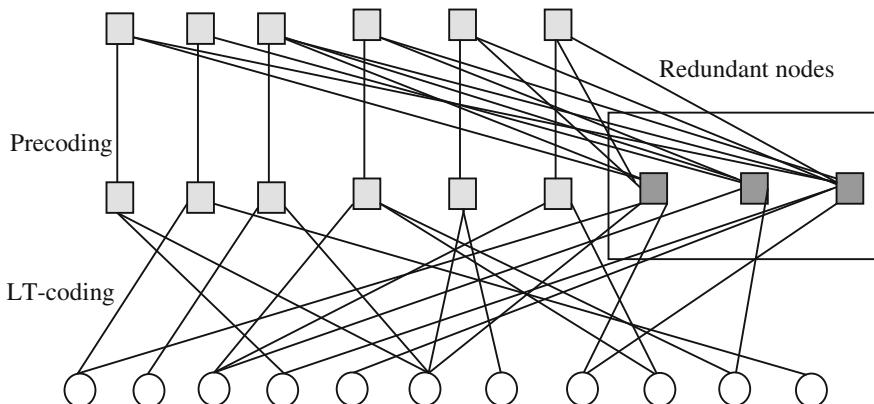


Fig. 9.8 Raptor codes

9.4 Problems

- Suppose the generator matrix G of the LT code is

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

and the received encoded symbols are $[1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0]$. Decode the received vector to obtain message symbols.

- Show that the number of encoding symbols is $n = k + O(\sqrt{k} \cdot \ln^2(k/\varepsilon))$.
- Show that the average degree of an encoding symbol is $D = O(\ln(k/\varepsilon))$
- Show that the decoder fails to recover the data with probability at most ε from a set of N encoding symbols.

9.5 MATLAB Exercises

- Write a MATLAB program for LT encoding and decoding with non-binary message symbols using robust Soliton distribution.
- Write a MATLAB program to generate H matrix for a systematic LT code with k message symbols and 0.5 overhead.

References

- Luby, M.: LT codes. In: Proceeding of the 43rd Annual IEEE Symposium on Foundations of Computer Science, pp. 271–282 (2002)
- Shokrollahi, A.: Raptor codes. IEEE Trans. Inf. Theor. **52**(6), 2551–2567 (2006)
- Richardson, T.J., Urbanke, R.L.: The capacity of low density parity check codes under message-passing decoding. IEEE Trans. Inf. Theor. **47**(2), 599–618 (2001)
- Nguyen, T.D., Yang, L.-L., Hanzo, L.: Systematic luby transform codes and their soft decoding. In: IEEE SiPS'07, pp. 67–72. Shanghai, 17–19 Oct 2007
- Gallager, R.: Low density parity check codes. IRE Trans. Inf. Theor. **8**(1), 21–28 (1962)

Chapter 10

MIMO System

10.1 What Is MIMO?

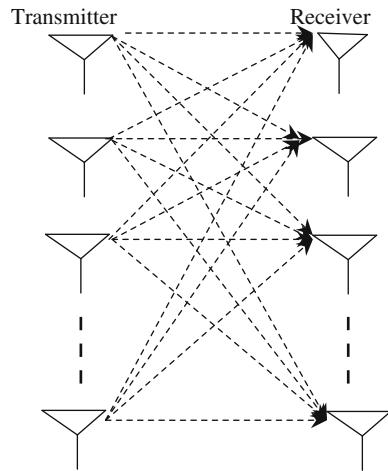
A channel with multiple antennas at the transmitter and multiple antennas at the receiver is called as a multiple-in-multiple-out (MIMO) channel, whereas the SISO channel has single antenna at the transmitter and a single antenna at the receiver. A MIMO channel representation is shown in Fig. 10.1.

The key advantages of MIMO system are increased reliability obtained through *diversity* and higher data rate obtained through *spatial multiplexing* [1]. These two concepts are used together in MIMO systems.

In a diversity system, the same information is transmitted through multiple transmit antennas and received at multiple receive antennas simultaneously. Since the fading for each link between a pair of transmit and receive antennas is considered to be independent and the same information travels through diverse paths and if one path is weak, a copy of information received through the other path may be good, and hence, the probability for accurate detection of the information increases.

In a spatial multiplexing, different information can be transmitted simultaneously over multiple antennas, similar to the idea of an OFDM signal, thereby boosting the system throughput or capacity of the channel.

Electronic supplementary material The online version of this chapter (doi:[10.1007/978-81-322-2292-7_10](https://doi.org/10.1007/978-81-322-2292-7_10)) contains supplementary material, which is available to authorized users.

Fig. 10.1 A MIMO channel

10.2 MIMO Channel Model

10.2.1 The Frequency Flat MIMO Channel

Let h_{ji} be a complex number represents the channel gain between i th transmit antenna and j th receive antenna. At a certain time instant, if the symbols $\{s_1, s_2, \dots, s_{N_T}\}$ are transmitted via N_T antennas, then the received signal at antenna j can be expressed as

$$y_j = \sum_{i=1}^{N_T} h_{ji} s_i + \eta_i \quad (10.1)$$

With $i = 1, 2, \dots, N_T$ transmitter antennas and $j = 1, 2, \dots, N_R$ receiver antennas, Eq. (10.1) can be represented in matrix form as

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{N_R} \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1N_T} \\ h_{21} & h_{22} & \cdots & h_{2N_T} \\ \vdots & \vdots & \ddots & \vdots \\ h_{N_R 1} & h_{N_R 2} & \cdots & h_{N_R N_T} \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_{N_T} \end{bmatrix} + \begin{bmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_{N_R} \end{bmatrix} \quad (10.2)$$

or more compactly as

$$y = Hs + \eta \quad (10.3)$$

The fading coefficients H are independent (with respect to both i and j) and identically distributed (i.i.d.). The additive noise at receiver antenna is independent

(with respect to η), identically distributed. It is assumed that the signaling is subject to the average power constraint

$$E[\|s^2\|] \leq P \quad (10.4)$$

The H matrix contains the channel coefficients that distort the transmitted signal amplitude and phase in time domain. The channel matrix H is estimated at the receiver and transmitter transmits blindly without any idea of channel information. If the receiver sends back the channel information to the transmitter, then the transmitter is able to adjust the powers allocated to the antennas.

One attractive merit of MIMO systems is the increased antenna diversity, which can alleviate the detrimental effect of flat fading. In a MIMO system with N_T transmit antennas and N_R receive antennas, if the channels for any pair of transmit–receive antennas are independent and experience flat fading, the maximum or full diversity gain is $N_T N_R$. A common way of achieving the full diversity is through space–time (ST) coding, which is discussed in the next chapter.

10.2.2 The Frequency-Selective MIMO Channel

In MIMO systems where any transmit–receive link is subject to multipath fading independently and the channel impulse response is characterized by L resolvable paths, the full diversity gain is $N_T N_R L$ [2, 3]. In frequency-selective MIMO channels, OFDM is usually applied to eliminate the ISI and ICI. To achieve full diversity, coding is used across OFDM subchannels, OFDM blocks, and transmit antennas.

10.2.3 MIMO–OFDM System

In broadband wireless systems, the MIMO channels are severely affected by the frequency-selective fading or potential multipath fading. This fading effect complicates the design of ST codes because of ISI. To overcome this problem, MIMO can be combined with OFDM system, which is referred to as MIMO–OFDM. The combination of MIMO and OFDM has the potential of meeting this stringent requirement since MIMO can improve the capacity and the diversity gain and OFDM can mitigate the detrimental effects due to multipath fading. The schematic block diagram of the MIMO–OFDM system is shown in Fig. 10.2.

The schematic block diagram of MIMO–OFDM system with N_T transmit, N_R receive antennas, and N -tone OFDM is illustrated in Fig. 10.2. The incoming bit

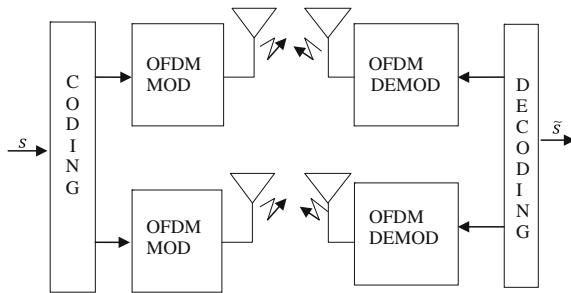


Fig. 10.2 MIMO OFDM system

stream is first mapped into a number of data symbols by using modulation techniques such as BPSK, QPSK, and QAM. Then, a block of data symbols is encoded into a code word matrix of size $NT \times N_T$, and transmitted through N_T transmit antennas in T OFDM blocks, each block having N subchannels. After appending the cyclic prefix on each OFDM block, the blocks will be transmitted through N_T transmit antennas. After passing through the MIMO channels, first the received signals will be sent to the reverse OFDM (cyclic prefix removal, DFT) and then sent to the decoder. If the channel state information (CSI) is available at the receiving side, the optimal ML detection will be performed.

10.3 Channel Estimation

In training-based channel estimation, the used training symbols or pilot tones are known to both the transmitter and the receiver. The knowledge of transmitted pilot symbols at the receiver is exploited to estimate the channel. The block-type pilot

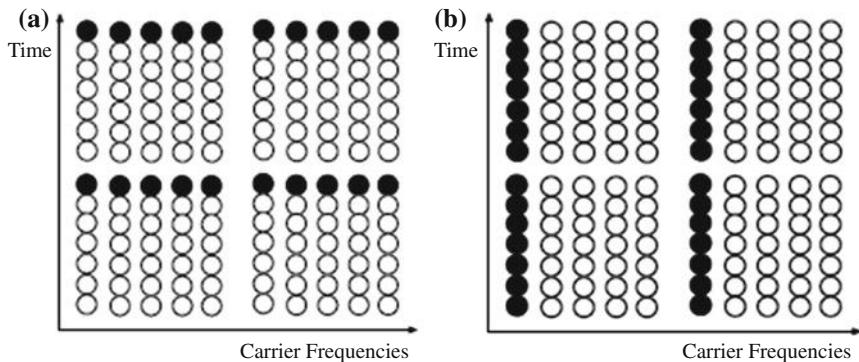


Fig. 10.3 **a** Block pilot. **b** Comb pilot

arrangement is shown in Fig. 10.3a in which pilot symbols are transmitted periodically for channel estimation. The comb-type pilot arrangement is shown in Fig. 10.3b, where the pilots are transmitted at all times but with an even spacing on the subcarriers for channel estimation.

The estimation can be performed by using LS [4–7]. The training symbols for N subcarriers can be represented by the following diagonal matrix assuming that all subcarriers are orthogonal.

$$S = \begin{bmatrix} s(0) & 0 & \cdots & 0 \\ 0 & s(1) & \square & \vdots \\ \vdots & \square & \ddots & 0 \\ 0 & \cdots & 0 & s(N-1) \end{bmatrix} \quad (10.5)$$

where $s(k)$ denotes a pilot tone at the k th subcarrier, with $E\{s(k)\} = 0$, $\text{Var}\{s(k)\} = \sigma_s^2$, $k = 0, 1, 2, \dots, N-1$. For a given channel gain $H(k)$ corresponding to the k th subcarrier, the received training signal $Y(k)$ can be represented as

$$\begin{aligned} Y \triangleq \begin{bmatrix} Y(0) \\ Y(1) \\ \vdots \\ Y(N-1) \end{bmatrix} &= \begin{bmatrix} s(0) & 0 & \cdots & 0 \\ 0 & s(1) & \square & \vdots \\ \vdots & \square & \ddots & 0 \\ 0 & \cdots & 0 & s(N-1) \end{bmatrix} \begin{bmatrix} H(0) \\ H(1) \\ \vdots \\ H(N-1) \end{bmatrix} + \begin{bmatrix} \eta(0) \\ \eta(1) \\ \vdots \\ \eta(N-1) \end{bmatrix} \\ &= SH + \eta \end{aligned} \quad (10.6)$$

where η is a noise vector with $E\{\eta(k)\} = 0$, $\text{Var}\{\eta(k)\} = \sigma_\eta^2$, and $k = 0, 1, 2, \dots, N-1$.

10.3.1 LS Channel Estimation

The LS is a well-known method and widely used for estimation due to its simplicity. LS channel estimate is represented by

$$\hat{H}_{\text{LS}} = S^{-1}Y \quad (10.7)$$

The pilot subcarriers are interpolated to estimate the channel for data symbols.

10.3.2 DFT-Based Channel Estimation

The DFT-based channel estimation technique improves the performance of LS channel estimation by removing the effect of noise outside the maximum channel delay [8].

The IDFT of the channel estimate $\{\hat{H}(k)\}_{k=0}^{N-1}$ is written as

$$\text{IDFT}\{\hat{H}(k)\} = h(n) + \eta(n) \triangleq \hat{h}(n), \quad n = 0, 1, \dots, N - 1 \quad (10.8)$$

where $\hat{H}(k)$ is the estimate of the channel H at the k th subcarrier, obtained by LS, and $\eta(n)$ denotes the noise component. If the maximum channel delay is δC_d , then

$$\hat{h}_{\text{DFT}}(n) = \begin{cases} h(n) + \eta(n), & n = 0, 1, \dots, \delta C_d - 1 \\ 0, & \text{otherwise} \end{cases} \quad (10.9)$$

and transformed back to the frequency domain as follows:

$$\hat{H}_{\text{DFT}}(n) = \text{DFT}\{\hat{h}_{\text{DFT}}(n)\} \quad (10.10)$$

10.3.3 MIMO–OFDM Channel Estimation

Using Eq. (10.7), the LS estimate of the channel between j th transmitter and i th receiver antenna for MIMO–OFDM system can be expressed as

$$\hat{H}_{\text{LS}}^{(j,i)} = \left(s^{(j)}\right)^{-1} Y^{(i)} \quad (10.11)$$

$s^{(j)}$ is an $N \times N$ diagonal matrix with the pilots of the j th transmit antenna as diagonal elements, and $Y^{(i)}$ is received vector of length N at receiver antenna i .

10.3.4 Channel Estimation Using MATLAB

The following MATLAB program is written using built-in MATLAB function “interpolation” to evaluate the MSE performance of LS and LS-DFT methods for channel estimation. For different E_b/N_0 's, the mean square errors (MSE) for LS and LS-DFT are shown in Fig. 10.4. From Fig. 10.4, it is observed that LS-DFT performs better than the LS method for channel estimation.

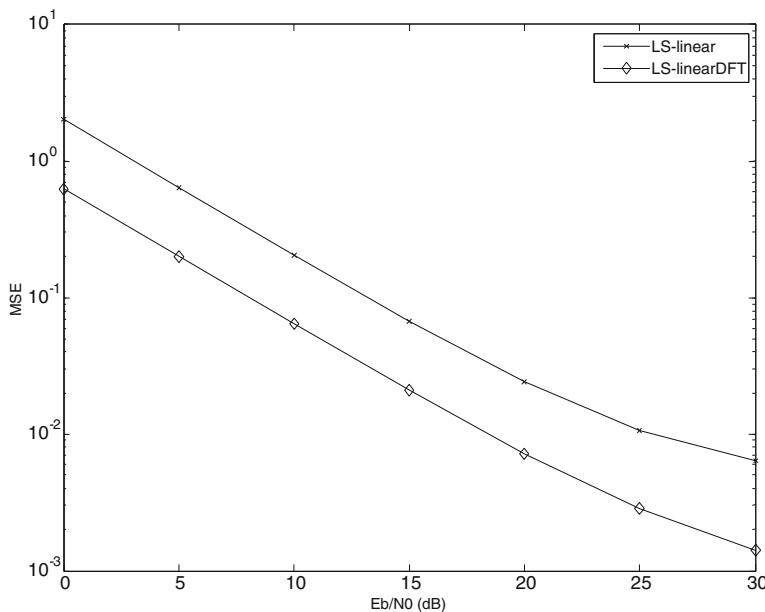


Fig. 10.4 E_b/N_0 versus MSE for channel estimation using LS and LS-DFT

Program 10.1 MATLAB program for Channel Estimation Using LS and LS-DFT methods

```
%channel_estimation.m
% for LS/DFT Channel Estimation with linear/spline interpolation
clear all; close all;
N_fft=32; N_g=N_fft/8; N_ofdm=N_fft+N_g; N_sym=100;
N_ps=4; N_p=N_fft/N_ps; N_d=N_fft-N_p; % Pilot spacing, Numbers of
pilots and data per OFDM symbol
N_bps=4; M=2^N_bps; % Number of bits per (modulated) symbol
mod_object = modem.qammod('M',M, 'SymbolOrder','gray');
demod_object = modem.qamdemod('M',M, 'SymbolOrder','gray');
Es=1; A=sqrt(3/2/(M-1)*Es); % Signal energy& QAM normalization factor
EbN0s = [0:5:30]; sq2=sqrt(2);
for i=1:length(EbN0s)
    EbN0 = EbN0s(i);
    rand('seed',1); randn('seed',1);
    MSE_LSi = 0; MSE_DFTi=0;
    for nsym=1:N_sym
        X_p = 2*(randn(1,N_p)>0)-1; % Pilot sequence generation
        msg_int=randint(1,N_fft-N_p,M); % bit generation
        Data = modulate(mod_object,msg_int)*A;
        ip = 0; pilot_loc = [];
        for k=1:N_fft
            if mod(k,N_ps)==1
                X(k) = X_p(floor(k/N_ps)+1); pilot_loc = [pilot_loc k]; ip = ip+1;
            else
                X(k) = Data(k-ip);
            end
        end
        x = ifft(X,N_fft); % IFFT
        xt = [x(N_fft-N_g+1:N_fft) x]; % Add CP
        h = [(randn+j*randn) (randn+j*randn)/2]; % generates a (2-tap) channel
        H = fft(h,N_fft); channel_length = length(h); % True channel and its
time-domain lenght
        y_channel = conv(xt,h); % Channel path (convolution)
        yt = awgn(y_channel,EbN0,'measured');
        y = yt(N_g+1:N_ofdm); % Remove CP
        Y = fft(y); % FFT
        k=1:N_p; Est_LS(k) = Y(pilot_loc(k))./X_p(k); % LS channel estimation
        Est_HLS = interpolate(Est_LS,pilot_loc,N_fft,'linear');
        h_estLS = ifft(Est_HLS); h_DFT = h_estLS(1:channel_length);
        Est_HDFT = fft(h_DFT,N_fft); % DFT-based channel estimation
        MSE_LSi = MSE_LSi+ (H-Est_HLS)*(H-Est_HLS)';
        MSE_DFTi = MSE_DFTi+ (H-Est_HDFT)*(H-Est_HDFT)';
    end
    MSE_LS(i)=MSE_LSi; MSE_DFT(i)=MSE_DFTi;
end
MSE_LS = MSE_LS/(N_fft*N_sym);
MSE_DFT = MSE_DFT/(N_fft*N_sym);
figure(1), semilogy(EbN0s',MSE_LS,'x', EbN0s',MSE_DFT,'d')
legend('LS-linear','LS-linearDFT')
xlabel ('Eb/N0 (dB)') ylabel ('MSE')
```

10.4 MIMO Channel Decomposition

A MIMO channel can be looked as a set of independent SISO channels using the singular value decomposition (SVD). The process requires precoding at the transmitter and receiver shaping at the receiver as shown in Fig. 10.5. This requires knowledge of the channel at the transmitter. The H matrix can be written in SVD form as

$$H = U\Sigma V^H \quad (10.12)$$

where U and V are unitary matrices ($U^H U = I_{N_R}$ and $V^H V = I_{N_T}$) and Σ is a $N_R \times N_T$ diagonal matrix of the singular values (σ_j) of H matrix. If H is a full-rank matrix, there are $\min(N_R, N_T)$ of nonzero singular values and hence with the same number of independent channels.

The received signal \tilde{y} is given by

$$\tilde{y} = U^H y \quad (10.13)$$

The above equation can be rewritten as

$$\tilde{y} = U^H(Hs + \eta) \quad (10.14)$$

Now, substituting Eq. (10.12) in the above equation, we obtain

$$\tilde{y} = U^H(U\Sigma V^H s + \eta) \quad (10.15)$$

Since $s = V\tilde{s}$, Eq. (10.15) can be rewritten as

$$\begin{aligned} \tilde{y} &= U^H(U\Sigma V^H V\tilde{s} + \eta) \\ &= U^H U\Sigma V^H V\tilde{s} + U^H \eta \\ &= \Sigma\tilde{s} + \tilde{\eta} \end{aligned} \quad (10.16)$$

From Eq. (10.16), it can be observed that the output is the product of precoded input signal \tilde{s} and the singular value matrix Σ . The distribution of the noise does not change by multiplying the noise η by the unitary matrix U^H .

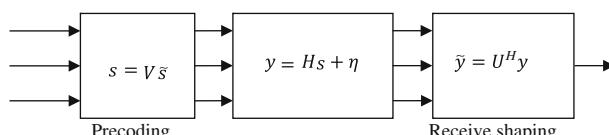


Fig. 10.5 Decomposition of a MIMO channel with full CSI

Example 10.1 Find a parallel channel model for a MIMO system, the H matrix of which is given by

$$H = \begin{bmatrix} 0.4 + j0.6 & j & 2 \\ -0.8 & 0.4 + j0.2 & 1.5 - j0.6 \\ j0.6 & -0.7 & -0.1 + j1.1 \end{bmatrix}$$

Solution The SVD decomposition using MATLAB gives

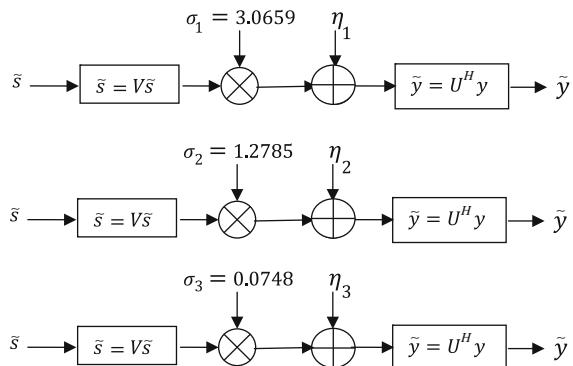
$$U = \begin{bmatrix} -0.4390 - j0.6062 & 0.2203 + j0.3263 & 0.2389 - j0.4773 \\ -0.4426 - j0.2417 & -0.8023 - j0.0633 & -0.2637 + j0.1685 \\ 0.3571 - j0.2408 & 0.0817 + j0.4366 & -0.7817 - j0.0777 \end{bmatrix}$$

$$\Sigma = \begin{bmatrix} 3.0659 & 0 & 0 \\ 0 & 1.2785 & 0 \\ 0 & 0 & 0.0748 \end{bmatrix}$$

$$V = \begin{bmatrix} -0.1075 & 0.9289 & -0.3543 \\ -0.3528 + j0.1955 & -0.0505 - j0.3056 & -0.0252 - j0.8607 \\ -0.5537 - j0.7206 & -0.1978 - j0.0449 & -0.3505 + j0.1011 \end{bmatrix}$$

The center matrix Σ contains the singular values (σ_j) of the H matrix. The rank of the matrix is equal to the number of singular values. This process decomposes the matrix channel into three independent SISO channels, with gains of 3.0659, 1.2785 and 0.0748, respectively, as shown in Fig. 10.6. The number of significant eigenvalues specifies the maximum degree of diversity. The larger a particular eigenvalue, the more reliable is that channel. The most important benefit of the SVD approach is that it allows for enhanced array gain—the transmitter can send more power over the better channels and less (or no) power over the worst ones. Thus, the first channel with the gain of 3.0659 will have better performance than the other two. The number of principle components is a measure of the maximum degree of diversity that can be realized in this way.

Fig. 10.6 SVD decomposition of a matrix channel into three independent SISO channels



10.5 MIMO Channel Capacity

Let s and y be N_T and N_R length vectors containing the transmitted and received symbols, respectively, for a MIMO system with N_T transmit and N_R receive antennas. Then, the received signal y can be rewritten in a matrix form as follows:

$$y = \sqrt{\frac{E_s}{N_T}} H s + \eta \quad (10.17)$$

where

$$y = [y_1 \ y_2 \ \dots \ y_{N_R}]$$

$$s = [s_1 \ s_2 \ \dots \ s_{N_T}]$$

$$\eta = [\eta_1 \ \eta_2 \ \dots \ \eta_{N_R}]$$

E_s is the total energy of N_T symbols transmitted.

10.5.1 Capacity of Deterministic MIMO Channel When CSI Is Known to the Transmitter

The capacity of a deterministic channel is defined by Shannon as

$$C = \max_{f(s)} I(s, y) \quad \text{bits/channel use} \quad (10.18)$$

$I(s, y)$ is called the mutual information of s and y . The capacity of the channel is the maximum information that can be transmitted from s to y by varying the channel probability density function (*pdf*). $f(s)$ is the *pdf* of the transmit signal s . From information theory, we get the relationship of mutual information between two random variables as a function of their entropy as

$$I(s, y) = H(y) - H(y|s) \quad (10.19)$$

$$H(y|s) = H(\eta) \quad (10.20)$$

Using Eq. (10.20), Eq. (10.19) can be rewritten as

$$I(s, y) = H(y) - H(\eta) \quad (10.21)$$

The second term is constant for a deterministic channel because it is a function of noise. Hence, mutual information is maximum only when the term $H(y)$ is maximum.

Using Eq. (10.17), the autocorrelation matrix of y can be written as

$$\begin{aligned}
R_{yy} &= E[yy^H] = E\left[\left(\sqrt{\frac{E_s}{N_T}}Hs + \eta\right)\left(\sqrt{\frac{E_s}{N_T}}Hs + \eta\right)^H\right] \\
&= E\left[\left(\frac{E_s}{N_T}Hss^HH^H + \eta\eta^H\right)\right] \\
&= \frac{E_s}{N_T}E[Hss^HH^H + \eta\eta^H] \\
&= \frac{E_s}{N_T}HE[ss^H]H^H + E[\eta\eta^H] \\
&= \frac{E_s}{N_T}HR_{ss}H^H + N_oI_{N_R}
\end{aligned} \tag{10.22}$$

where R_{ss} is the autocorrelation of the transmitted signal vector s and N_o is the power spectral density of the additive noise $\{\eta_i\}_{i=1}^{N_R}$. The entropy $H(y)$ is maximized when both s and y are zero-mean circular symmetric complex Gaussian (ZMCSCG) random variables. Then, the $H(y)$ and $H(\eta)$ are given by

$$H(y) = \log_2\{\det(\pi e R_{yy})\} \tag{10.23}$$

$$H(\eta) = \log_2\{\det(\pi e N_o I_{N_R})\} \tag{10.24}$$

Using Eqs. (10.23) and (10.24), it is shown in [9] that the mutual information given by Eq. (10.21) can be expressed as

$$I(s, y) = \log_2 \det\left\{I_{N_R} + \frac{E_s}{N_T N_o} HR_{ss}H^H\right\} \text{ bits/s/Hz} \tag{10.25}$$

Since $\text{SNR} = \frac{E_s}{N_o}$, Eq. (10.25) can be rewritten as

$$I(s, y) = \log_2 \det\left\{I_{N_R} + \frac{\text{SNR}}{N_T} HR_{ss}H^H\right\} \text{ bits/s/Hz} \tag{10.26}$$

From the above equation, we can write the expression for capacity as

$$C = I(s, y) = \max_{\text{Tr}(R_{ss})=N_T} \log_2 \det\left\{I_{N_R} + \frac{\text{SNR}}{N_T} HR_{ss}H^H\right\} \tag{10.27}$$

It should be noted here that trace of R_{ss} matrix is $\text{Tr}(R_{ss}) = N_T$, when the transmission power for each transmit antenna is assumed to be 1.

10.5.2 Deterministic MIMO Channel Capacity When CSI Is Unknown at the Transmitter

When H is not known at the transmitter side, we can assume equal power distribution among the transmitters, R_{ss} is an identity matrix, that is, $R_{ss} = I_{N_T}$, and Eq. (10.27) becomes

$$C = \log_2 \det \left\{ I_{N_T} + \frac{\text{SNR}}{N_R} H H^H \right\} \quad (10.28)$$

This is the capacity equation for the MIMO channels with equal power. It should be noted that for a large number of transmit antennas and a fixed number of receive antennas, the law of large numbers yields

$$\lim_{N_T \rightarrow \infty} \frac{1}{N_R} H H^H = I_{N_T} \quad (10.29)$$

Thus, the MIMO channel capacity for large N_T becomes

$$C = N_R \log_2 \det \{ I_{N_T} + \text{SNR} \} \quad (10.30)$$

Example 10.2 Given the following $(3 \times 3$ MIMO) channel, find the capacity of this channel, when CSI is known at the receiver and unknown at the transmitter, SNR = 10 dB and bandwidth equal to 1 kHz. Compare this capacity calculation to that using SVD.

$$H = \begin{bmatrix} 0.4 + j0.6 & j & 2 \\ -0.8 & 0.4 + j0.2 & 1.5 - j0.6 \\ j0.6 & -0.7 & -0.1 + j1.1 \end{bmatrix}$$

Solution

$$\begin{aligned} H H^H &= \begin{bmatrix} 5.52 & 2.88 + j1.12 & 0.16 - j3.14 \\ 2.88 - j1.12 & 3.45 & -1.09 - j1.25 \\ 0.16 + j3.14 & -1.09 + j1.25 & 2.07 \end{bmatrix} \\ C &= B \log_2 \left(\det \left\{ I_{N_R} + \frac{\text{SNR}}{N_T} H H^H \right\} \right) \\ &= 7.7306 \text{ kbps} \end{aligned}$$

The singular values are equal to 3.0659, 1.2785 and 0.0748.

The sum of the capacity of the three independent channels is equal to the same quantity as above equation.

$$\begin{aligned} C &= B(\log 2(1 + 3.0659^2 \cdot 3.33) + \log 2(1 + 1.2785^2 \cdot 3.33) \\ &\quad + \log 2(1 + 0.0748^2 \cdot 3.33)) \\ &= 7.7306 \text{ kbps} \end{aligned}$$

10.5.3 Random MIMO Channel Capacity

10.5.3.1 Random MIMO Channel Capacity with CSI Known at the Transmitter

It is assumed in Sect. 10.5.1 that the MIMO channels are deterministic. In general, the MIMO channels are varying randomly. Hence, H is a random matrix and its channel capacity is also randomly time-varying. In practice, assuming that the random channel is an ergodic process, the MIMO channel capacity can be expressed by

$$C_{\text{erg}} = E \left[\max_{\text{Tr}(R_{ss})=N_{\text{T}}} \log_2 \det \left\{ I_{N_{\text{R}}} + \frac{\text{SNR}}{N_{\text{T}}} H R_{ss} H^H \right\} \right] \quad (10.31)$$

where the subscript erg stands for ergodic.

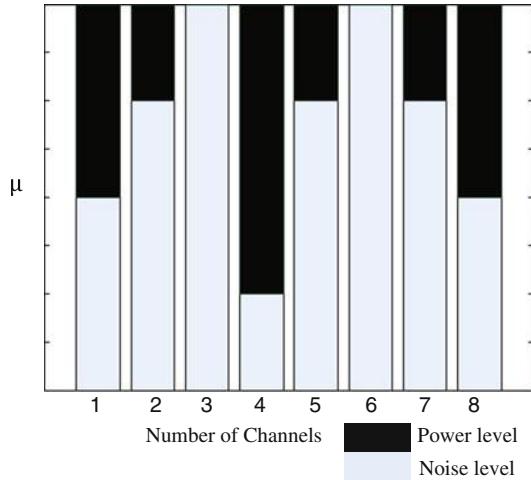
If r is the rank of the matrix H and $\lambda_i (i = 1, 2, \dots, r)$ are the eigenvalues (positive real numbers) obtained by the eigen decomposition of HH^H and if the transmit power for the i th transmit antenna is given by $p_i = E[|s_i|^2]$, Eq. (10.31) can be rewritten [8] as

$$C_{\text{erg}} = E \left[\log_2 \det \left\{ I_{N_{\text{R}}} + \frac{\text{SNR}}{N_{\text{T}}} p_i^{\text{opt}} \lambda_i \right\} \right] \quad (10.32)$$

$$p_i^{\text{opt}} = \left(\mu - \frac{N_{\text{T}}}{\text{SNR}} \frac{1}{\lambda_i} \right)^+ \quad (10.33)$$

$$\sum_{i=1}^r p_i^{\text{opt}} = N_{\text{T}} \quad (10.34)$$

Fig. 10.7 Water-filling power allocation algorithm



where μ is a constant and $(x)^+$ is defined by

$$\begin{aligned}(x)^+ &= x \text{ for } x \geq 0 \\ (x)^+ &= 0 \text{ for } x < 0\end{aligned}\quad (10.35)$$

Equation (10.33) satisfying the constraint in Eq. (10.34) is the well-known water-filling power allocation algorithm, which is illustrated in Fig. 10.7.

Figure 10.7 shows that more power must be allocated to the channel with higher SNR. Furthermore, if an SNR is below the threshold given in terms of μ , no power is allocated to the corresponding channels. As can be seen from Fig. 10.7, power is not allocated to the channels 3 and 6.

10.5.3.2 Random MIMO Channel Capacity with CSI Unknown at the Transmitter

When CSI is unknown at the transmitter, from Eq. (10.31), the ergodic capacity of the random MIMO channel is given by

$$C_{\text{erg}} = E \left[\log_2 \det \left\{ I_{N_{\text{R}}} + \frac{\text{SNR}}{N_{\text{T}}} H H^H \right\} \right] \quad (10.36)$$

Equation (10.36) can be written in terms of the positive eigenvalues as [8]

$$C_{\text{erg}} = E \left[\log_2 \det \left\{ I_{N_{\text{R}}} + \frac{\text{SNR}}{N_{\text{T}}} \lambda_i \right\} \right] \quad (10.37)$$

which is frequently known as an ergodic channel capacity.

The following MATLAB programs illustrate the ergodic capacity of i.i.d random MIMO channel with CSI unknown at the transmitter.

Program 10.2 MATLAB program for ergodic capacity

```
clear all, close all
SNRdB = [0:35];
iter=1000;
C1=ergcap(SNRdB,1,1,iter);
C2=ergcap(SNRdB,2,2,iter);
C3=ergcap(SNRdB,4,4,iter);
figure, plot(SNRdB,C1(1,:),'b-o', SNRdB,C2(1,:),'b-*', SNRdB,C3(1,:),'b-+');
xlabel('SNR(dB)'); ylabel('bps/Hz'); set(gca,'fontsize',10);
legend('{\it N_T}=1,{\it N_R}=1','{\it N_T}=2,{\it N_R}=2','{\it N_T}=4,{\it N_R}=4')
```

Program 10.3 MATLAB Function program for ergcap

```
function C=ergcap(SNRdB,nT,nR,iter)
n=min(nT,nR); I = eye(n);SNRlin=10.^^(SNRdB/10.);
C(1,:) = zeros(1,length(SNRdB));
for ii=1:iter
    H = sqrt(0.5)*(randn(nR,nT)+j*randn(nR,nT));
    if nR>=nT, HH = H'*H; else HH = H*H'; end
    for i=1:length(SNRdB) %random channel generation
        C(1,i) = C(1,i)+log2(real(det(I+SNRlin(i)/nT*HH)));
    end
end
C = C/iter;
```

The ergodic capacity of i.i.d random MIMO channel with CSI unknown at the transmitter with different transmitting and receiving antennas is shown in Fig. 10.8.

From Fig. 10.8, it is observed that the number of the transmitting and the receiving antennas increases, the ergodic capacity increases.

10.5.3.3 Capacity of Correlated Random MIMO Channel

In general, the elements of H are correlated by an amount that depends on the propagation environment as well as the polarization of the antenna elements and spacing between them [10]. One possible model for H that takes the fading

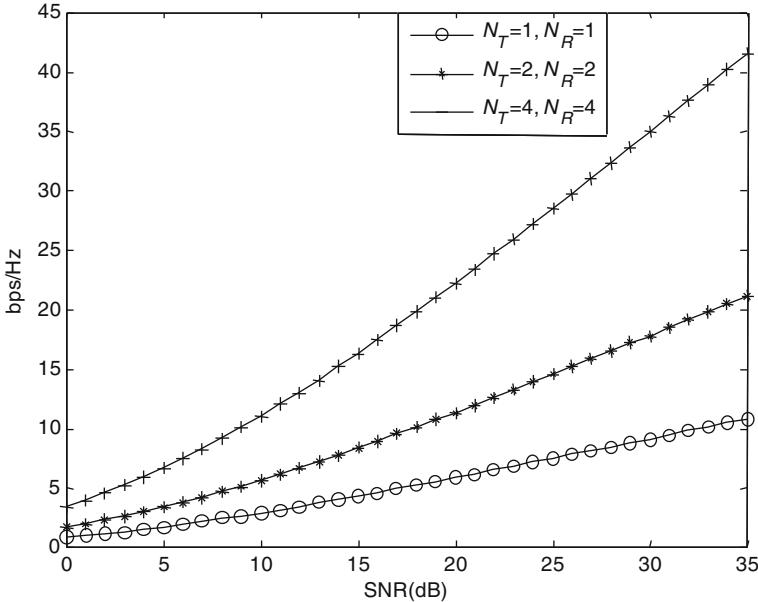


Fig. 10.8 Ergodic capacity of i.i.d random MIMO channel with CSI unknown at the transmitter

correlation into account splits the fading correlation into two independent components called receive correlation and transmit correlation, respectively [11, 12]. This amounts to modeling H as follows

$$H = R_r^{1/2} H_w R_t^{1/2} \quad (10.38)$$

where R_t and R_r are the transmit correlation and the receive correlation matrices, respectively, H_w is a matrix with independent Gaussian elements with unity variance, and the superscript $\frac{1}{2}$ stands for the Hermitian square root of a matrix. The matrix R_r determines the correlation between the rows of H , and the matrix R_t determines the correlation between the columns of H . The diagonal entries of R_t and R_r are constrained to be unity. The correlation matrices R_t and R_r can be measured or computed by assuming the scattering distribution around the transmit and receive antennas. For uniform linear array at the transmitter and the receiver, the correlation matrices R_t and R_r can be calculated according to two different methods given in [13, 14]. From [14], we have the following Toeplitz structure correlation matrices:

$$R_t = \begin{bmatrix} 1 & r_t & \cdots & r_t^{(N_T-1)^2} \\ r_t & 1 & \cdots & \cdots \\ \vdots & \vdots & & \vdots \\ r_t^{(N_T-1)^2} & \cdots & \cdots & 1 \end{bmatrix}; \quad R_r = \begin{bmatrix} 1 & r_r & \cdots & r_r^{(N_R-1)^2} \\ r_r & 1 & \cdots & \cdots \\ \vdots & \vdots & & \vdots \\ r_r^{(N_R-1)^2} & \cdots & \cdots & 1 \end{bmatrix} \quad (10.39)$$

where R_t and R_r represent $r(d_t)$ and $r(d_r)$, respectively, and $r(d)$ is the approximation for the fading correlation between two adjacent antenna elements averaged over all possible orientations of the two antennas in a given wave field which can be expressed as [15]

$$r(d) \approx \exp(-23\Lambda^2 d^2) \quad (10.40)$$

where d is the distance in wavelengths between two antennas and Λ is the angular spread.

From Eq. (10.28), then, the MIMO channel capacity is given as

$$C = \log_2 \det \left\{ I_{N_R} + \frac{\text{SNR}}{N_T} R_r^{1/2} H_w R_t H_w^H R_r^{H/2} \right\} \quad (10.41)$$

The following examples demonstrate the performance of the correlated random MIMO channels with and without CSI known at the transmitter using MATLAB.

Example 10.3 Compare the capacity of spatially correlated random 4×4 channels with unknown CSI at the transmitter for a non-uniform antenna array structure with the following correlation matrices [14]

$$R_t = \begin{bmatrix} 1 & 0.3169 & 0.3863 & 0.0838 \\ 0.3169 & 1 & 0.7128 & 0.5626 \\ 0.3863 & 0.7128 & 1 & 0.5354 \\ 0.0838 & 0.5626 & 0.5354 & 1 \end{bmatrix};$$

$$R_r = \begin{bmatrix} 1 & 0.1317 & 0.1992 & 0.2315 \\ 0.1317 & 1 & 0.1493 & 0.1907 \\ 0.1992 & 0.1493 & 1 & 0.1996 \\ 0.2315 & 0.1907 & 0.1996 & 1 \end{bmatrix}$$

and an uniform antenna array structure with $r_t = r_r = 0.2$.

Program 10.4 MATLAB program for random MIMO channel capacity

```
%Program to compute the capacity of random MIMO channels without CSI
with uniform and non-uniform correlated matrices
clear all, close all
SNRdB = [0:25];iter=1000; nT=4; nR=4;
n=min(nT,nR); I = eye(n);SNRlin=10.^((SNRdB/10.);rho=0.2;
Rtx=[1 0.3169 0.3863 0.0838; 0.3169 1 0.7128 0.5626;
0.3863 0.7128 1 0.5354; 0.0838 0.5626 0.5354 1];
Rrx=[1 0.1317 0.1992 0.2315; 0.1317 1 0.1493 0.1907;
0.1992 0.1493 1 0.1996; 0.2315 0.1907 0.1996 1];
Rtxu=[1 rho rho^2 rho^3; rho 1 rho rho^2;
rho^2 rho 1 rho; rho^3 rho^2 rho 1];
Rrxu=Rtxu;
C1(1,:)=zeros(1,length(SNRdB)); C2(1,:)=zeros(1,length(SNRdB));
for ii=1:iter
    Hw = sqrt(0.5)*(randn(nR,nT)+j*randn(nR,nT));
    H = Rrx^(1/2)*Hw*Rtx^(1/2); tmp = H'*H/nT;
    Hu = Rrxu^(1/2)*Hw*Rtxu^(1/2); tmp1 = Hu'*Hu/nT;;
    for i=1:length(SNRdB) %random channel generation
        C2(1,i) = C2(1,i)+log2(real(det(I+SNRlin(i)*tmp)));
        C1(1,i) = C1(1,i)+log2(real(det(I+SNRlin(i)*tmp)));
    end
end
C1 = C1/iter; C2=C2/iter;
figure, plot(SNRdB,C1(1,:),'-', SNRdB,C2(1,:),'--');
xlabel('SNR(dB)'); ylabel('bps/Hz'); set(gca,'fontsize',10);
legend('with non-uniform correlation matrices' , 'with uniform correlation
matrices')
```

The capacity of the random MIMO channels without CSI with uniform and non-uniform correlated matrices is shown in Fig. 10.9.

From Fig. 10.9, it is observed that the capacity of a random MIMO channel without CSI and with uniform correlated matrices gives the better performance than the non-uniform correlated matrices.

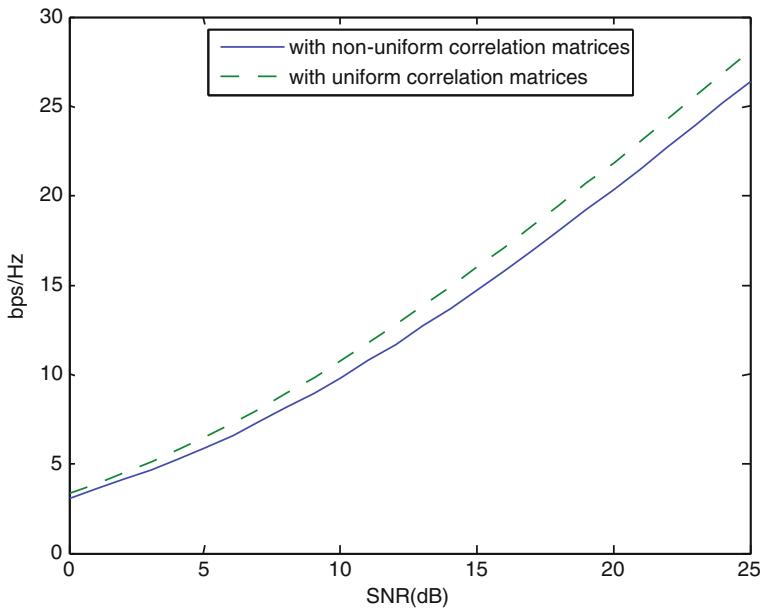


Fig. 10.9 Random MIMO channel capacity without CSI with uniform and non-uniform correlated matrices

Example 10.4 Compare the capacity of spatially correlated random 4×4 channels with known and unknown CSI at the transmitter for an uniform antenna array structure with $r_t = r_r = 0.2$.

Program 10.5 MATLAB program for spatially correlated 4×4 channel capacity

```
%Program to compute the capacity of random MIMO channels with and  
without CSI with uniform correlated matrices  
clear all, close all  
SNRdB = [0:25]; iter=1000; nT=4; nR=4;  
n=min(nT,nR); I = eye(n);SNRlin=10.^((SNRdB/10.);rho=0.2;  
Rtx=[1 rho rho^2 rho^3; rho 1 rho rho^2;  
rho^2 rho 1 rho; rho^3 rho^2 rho 1];  
Rrx=Rtx;  
C1(1,:)= zeros(1,length(SNRdB));  
C2(1,:)= zeros(1,length(SNRdB));  
for ii=1:iter  
Hw = sqrt(0.5)*(randn(nR,nT)+j*randn(nR,nT));  
H = Rrx^(1/2)*Hw*Rtx^(1/2);tmp = H'*H/nT;HH= H'*H; Lamda = svd(H'*H);  
for i=1:length(SNRdB) %random channel generation  
C1(1,i) = C1(1,i)+ log2(real(det(I+SNRlin(i)*tmp)));  
gama = WaterFilling(Lamda,SNRlin(i),nT);  
C2(1,i) = C2(1,i)+log2(real(det(I+(SNRlin(i)/nT)*diag( gama  
)*diag(Lamda))));  
end  
end  
C1 = C1/iter; C2=C2/iter;  
figure, plot(SNRdB,C1(1,:),'-', SNRdB,C2(1,:,'--');  
xlabel('SNR(dB)'); ylabel('bps/Hz'); set(gca,'fontsize',10);  
legend('with unknown CSI at the transmitter', 'with known CSI at the transmitter')
```

Program 10.6 MATLAB function program for water filling

```

function [gamat]=WaterFilling(Lamda,SNR,nT)
r=length(Lamda); gama = zeros(1,r);
index=[1:r]; indext=index;
p=1;
while p<r
    ir=[1:r-p+1].';
    temp= sum(1./Lamda(indext(ir)));
    mu= nT/(r-p+1.)*(1+1/SNR*temp);
    gama(indext(ir))=mu-nT./(SNR*Lamda(indext(ir)));
    if min(gama(indext))<0
        i=find(gama==min(gama)); ii=find(indext==i);
        indext1=[indext([1:ii-1]) indext([ii+1:end])];
        indext=indext1;
        p=p+1;
        clear gama;
    else
        p=r;
    end
end
gamat=zeros(1,length(Lamda)); gamat(indext)=gama(indext);

```

The comparison of the capacity of spatially correlated 4×4 channels with known and unknown CSI at the transmitter is shown in Fig. 10.10.

From Fig. 10.10, it is observed that the capacity of spatially correlated 4×4 channels with known CSI at the transmitter gives better performance than with unknown CSI at the transmitter.

When $N_T = N_R$ and SNR is high, Eq. (10.41) can be approximated as

$$C = \log_2 \det \left\{ I_{N_R} + \frac{\text{SNR}}{N_T} H_w H_w^H \right\} + \log_2 \det(R_t) + \log_2 \det(R_r) \quad (10.42)$$

From Eq. (10.42), it can be observed that the MIMO channel capacity is reduced due to the correlation between the transmit and receive antennas and the reduction is

$$\log_2 \det(R_t) + \log_2 \det(R_r) \quad (10.43)$$

It is shown in [8] that the value in Eq. (10.43) is always negative by the fact that $\log_2 \det(R_t) \leq 0$ for any correlation matrix R .

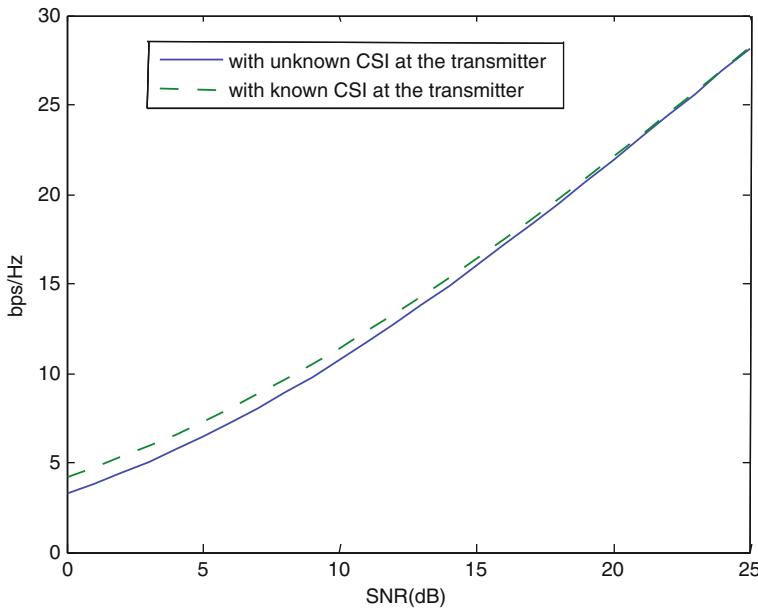


Fig. 10.10 Comparison of the capacity of spatially correlated 4×4 channels with known and unknown CSI at the transmitter

The following example illustrates how correlation reduces the channel capacity using MATLAB.

Example 10.5 Compare the capacity of i.i.d and correlated random 2×2 channels with CSI unknown at the transmitter assuming $R_t = \begin{bmatrix} 1 & 0.76\exp(0.17j\pi) \\ 0.76\exp(0.17j\pi) & 1 \end{bmatrix}$; R_r is a 2×2 identity matrix, i.e., no correlation exists between the receive antennas.

Program 10.7 MATLAB program for i.i.d and correlated MIMO channels capacity

```
%Program to compute the capacity of iid and correlated MIMO channels
clear all, close all;
SNRdB=[0:5:25]; SNRlin=10.^ (SNRdB/10);
iterations=1000; nT=2; nR=2;
n=min(nT,nR); I = eye(n); sq2=sqrt(0.5);
R=[1 0.76*exp(0.17j*pi) ; 0.76*exp(-0.17j*pi) 1 ];
Ciid=zeros(1,length(SNRdB)); Ccorr=zeros(1,length(SNRdB));
for iter=1:iterations
    H = sq2*(randn(nR,nT)+j*randn(nR,nT));
    Hc = H*R^(1/2);
    temp1 = H'*H/nT; temp2 = Hc'*Hc /nT;
    for i=1:length(SNRdB)
        Ciid(i) = Ciid(i) + log2(det(I+SNRlin(i)*temp1));
        Ccorr(i) = Ccorr(i) + log2(det(I+SNRlin(i)*temp2));
    end
end
Ciid = real(Ciid)/iterations; Ccorr = real( Ccorr)/iterations;
plot(SNRdB,Ciid, SNRdB, Ccorr,'.');
xlabel('SNR (dB)'); ylabel('Capacity(bps/Hz)'); set(gca,'fontsize',10)
legend('iid 2x2 fading channels','correlated 2x2 fading channels');
```

A comparison of the capacity of i.i.d and correlated 2×2 channels is shown in Fig. 10.11. From Fig. 10.11, it is observed that the capacity of the i.i.d with unknown CSI at the transmitter gives the better performance than correlated random 2×2 channels with unknown CSI at the transmitter.

10.6 MIMO Channel Equalization

Consider a wireless communication system in which the transmitter contains N_T antennas and the receiver possesses N_R antennas. Let us consider a 2×2 MIMO channel ($N_T = 2$, $N_R = 2$) as shown in Fig. 10.12. The received signal for the 2×2 MIMO channel can be expressed as

$$y_j = \sum_{i=1}^2 h_{j,i} s_i + \eta_j \quad (10.44)$$

where $h_{j,i}$ ($i = 1, 2; j = 1, 2$) are independent and identically distributed (i.i.d) complex random variables, representing the channel coefficients from the i th transmitter antenna to the j th receiver antenna, s_i are transmitted symbols, and η_j are noise samples and i.i.d complex AWGN variables.

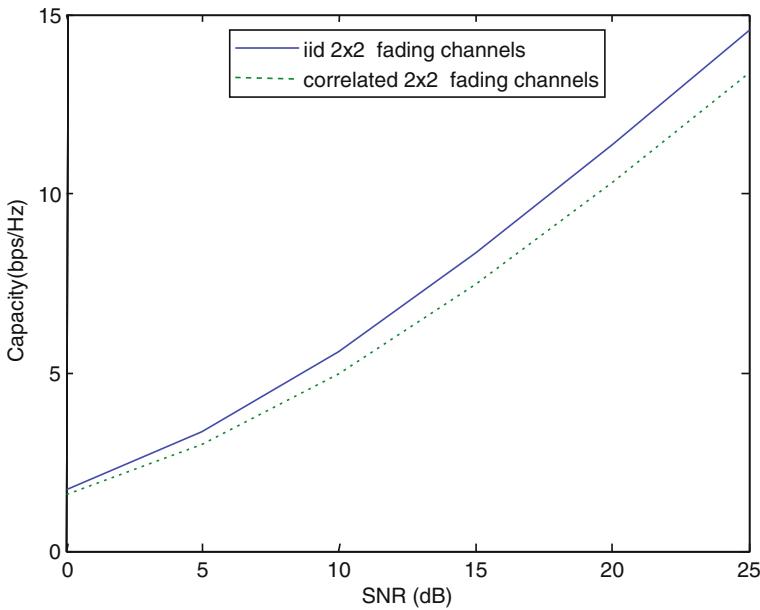
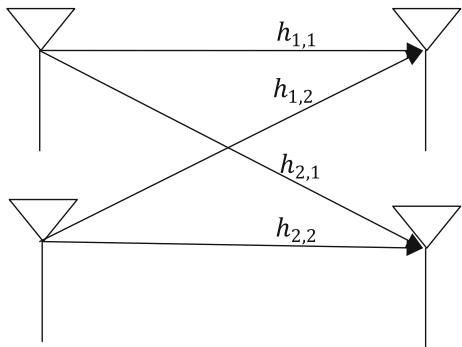


Fig. 10.11 The comparison of the capacity of i.i.d and correlated 2×2 channels

Fig. 10.12 A 2×2 MIMO channel



The Eq. (10.44) can be represented in matrix form as

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} h_{1,1} & h_{1,2} \\ h_{2,1} & h_{2,2} \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} + \begin{bmatrix} \eta_1 \\ \eta_2 \end{bmatrix} \quad (10.45)$$

equivalently,

$$y = Hs + \eta$$

10.6.1 Zero Forcing (ZF) Equalization

To solve for s , we know that we need to find a matrix W which satisfies $WH = I$. The zero forcing (ZF) linear detector for meeting this constraint is given by,

$$W = (H^H H)^{-1} H^H \quad (10.46)$$

This matrix is also known as the pseudo-inverse for a general $m \times n$ matrix. The term

$$\begin{aligned} H^H H &= \begin{bmatrix} h_{1,1}^* & h_{2,1}^* \\ h_{1,2}^* & h_{2,2}^* \end{bmatrix} \begin{bmatrix} h_{1,1} & h_{1,2} \\ h_{2,1} & h_{2,2} \end{bmatrix} \\ &= \begin{bmatrix} |h_{1,1}|^2 + |h_{2,1}|^2 & h_{1,1}^* h_{1,2} + h_{2,1}^* h_{2,2} \\ h_{1,2}^* h_{1,1} + h_{2,2}^* h_{2,1} & |h_{1,2}|^2 + |h_{2,2}|^2 \end{bmatrix} \end{aligned}$$

10.6.2 Minimum Mean Square Error (MMSE) Equalization

The minimum mean square error (MMSE) approach tries to find W which minimizes the criterion $E\{\|W_{y-s}\|^2\}$. Solving $W = [H^H H + N_0 I]^{-1} H^H$ when the noise term is zero, the MMSE equalizer reduces to zero forcing equalizer.

10.6.3 Maximum Likelihood Equalization

ML detection shows the best performance in all the MIMO detection algorithms. It finds the \hat{s} , which minimizes

$$J = \|y - H\hat{s}\|^2 \quad (10.47)$$

$$J = \left\| \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} - \begin{bmatrix} h_{1,1} & h_{1,2} \\ h_{2,1} & h_{2,2} \end{bmatrix} \begin{bmatrix} \hat{s}_1 \\ \hat{s}_2 \end{bmatrix} \right\|^2 \quad (10.48)$$

If the modulation is BPSK, the possible value of s_1 is $+1$ or -1 . Similarly, s_2 also take values $+1$ or -1 . So, to find the maximum likelihood estimate, we need to find the minimum from the all four combinations of s_1 and s_2 with J defined for the four combinations as

$$J_{+1,+1} = \left| \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} - \begin{bmatrix} h_{1,1} & h_{1,2} \\ h_{2,1} & h_{2,2} \end{bmatrix} \begin{bmatrix} +1 \\ +1 \end{bmatrix} \right|^2 \quad (10.49)$$

$$J_{+1,-1} = \left| \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} - \begin{bmatrix} h_{1,1} & h_{1,2} \\ h_{2,1} & h_{2,2} \end{bmatrix} \begin{bmatrix} +1 \\ -1 \end{bmatrix} \right|^2 \quad (10.50)$$

$$J_{-1,+1} = \left| \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} - \begin{bmatrix} h_{1,1} & h_{1,2} \\ h_{2,1} & h_{2,2} \end{bmatrix} \begin{bmatrix} -1 \\ +1 \end{bmatrix} \right|^2 \quad (10.51)$$

$$J_{-1,-1} = \left| \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} - \begin{bmatrix} h_{1,1} & h_{1,2} \\ h_{2,1} & h_{2,2} \end{bmatrix} \begin{bmatrix} -1 \\ -1 \end{bmatrix} \right|^2 \quad (10.52)$$

In case of 4×4 MIMO, the Eq. (10.44) can be written as

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} h_{1,1} & h_{1,2} & h_{1,3} & h_{1,4} \\ h_{2,1} & h_{2,2} & h_{2,3} & h_{2,4} \\ h_{3,1} & h_{3,2} & h_{3,3} & h_{3,4} \\ h_{4,1} & h_{4,2} & h_{4,3} & h_{4,4} \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} + \begin{bmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \\ \eta_4 \end{bmatrix} \quad (10.53)$$

ML detection minimizes

$$J = \left| \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} - \begin{bmatrix} h_{1,1} & h_{1,2} & h_{1,3} & h_{1,4} \\ h_{2,1} & h_{2,2} & h_{2,3} & h_{2,4} \\ h_{3,1} & h_{3,2} & h_{3,3} & h_{3,4} \\ h_{4,1} & h_{4,2} & h_{4,3} & h_{4,4} \end{bmatrix} \begin{bmatrix} \hat{s}_1 \\ \hat{s}_2 \\ \hat{s}_3 \\ \hat{s}_4 \end{bmatrix} \right|^2 \quad (10.54)$$

with BPSK modulation for maximum likelihood estimate, we need to calculate minimum from all sixteen combinations of s_1, s_2, s_3 and s_4 .

The performance comparison of MIMO channel equalization using ZF, MMSE, and ML is shown in Fig. 10.13. From Fig. 10.13, it is observed that the performance of MMSE is better than ZF and the performance of ML is better than both the MMSE and ZF.

10.7 Problems

- Find a parallel channel model for a MIMO system, the H matrix of which is given by

$$H = \begin{bmatrix} 0.8 & 0.5 - j0.2 & 0.3 + j0.6 \\ 0.4 - j0.6 & 1.0 - j0.1 & 0.2 - j0.9 \\ 0.5 + j0.3 & 0.5 + j1.5 & 0.6 + j1.2 \end{bmatrix}$$

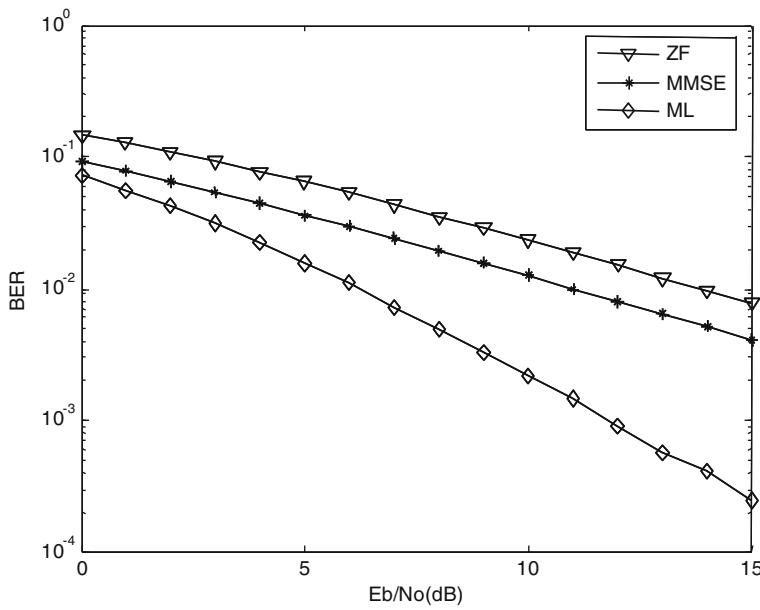


Fig. 10.13 Performance comparison of MIMO channel equalization using ZF, MMSE, and ML

2. Given the following (3×3) MIMO channel, find the capacity of this channel, with known CSI at the receiver, unknown CSI at the transmitter, SNR = 20 dB, and bandwidth equal to 2 kHz. Compare this capacity calculation to that using SVD.

$$H = \begin{bmatrix} 0.8 & 0.5 & 0.3 \\ 0.4 & 1.0 & 0.2 \\ 0.5 & 0.5 & 0.6 \end{bmatrix}$$

3. Consider a MIMO channel with two transmit antennas and one receive antenna. Assume zero-mean unit variance AWGN and an average power constraint of one per antenna. The path gains from the first and second transmit antennas to the receiver antenna are $h_1 = 0.5$ and $h_2 = 0.5 + j1.5$, respectively.
- What is the channel capacity?
 - What is the channel capacity if CSI is known at the transmitter and the average power constraint is 2 over sum of the transmission powers from both the antennas?
4. Assuming total power is 1 W, noise power is equal to 0.1 W, and the signal bandwidth is 50 kHz, find the channel capacity and optimal power allocation for MIMO channel, the H matrix of which is given by

$$H = \begin{bmatrix} 0.8 & 0.5 - j0.2 & 0.3 + j0.6 \\ 0.4 - j0.6 & 1.0 - j0.1 & 0.2 - j0.9 \\ 0.5 + j0.3 & 0.5 + j1.5 & 0.6 + j1.2 \end{bmatrix}$$

10.8 MATLAB Exercises

1. Write a MATLAB program for the simulations to estimate the achievable information capacity for BPSK input and QPSK input over a MIMO system, the H matrix of which is given by

$$H = \begin{bmatrix} 0.8 & 0.5 - j0.2 & 0.3 + j0.6 \\ 0.4 - j0.6 & 1.0 - j0.1 & 0.2 - j0.9 \\ 0.5 + j0.3 & 0.5 + j1.5 & 0.6 + j1.2 \end{bmatrix}$$

2. Write a MATLAB program to plot the ergodic channel capacity of a 2×2 MIMO system over ergodic Rayleigh fading channel with transmit correlation matrix $R_t = \begin{bmatrix} 1 & r \\ r & 1 \end{bmatrix}$ and receive correlation matrix $R_r = R_t$ for $r = 0, 0.5, 0.6, 0.8$.

References

1. Murch, R.D., Letaief, K.B.: Antenna systems for broadband wireless access. *IEEE Commun. Mag.* **40**, 76–83 (2002)
2. Bölcseki, H., Paulraj, A.: Space-frequency coded broadband OFDM systems. In: Proceedings of IEEE WCNC, Chicago, pp. 1–6, 23–28 Sept 2000
3. Lu, B., Wang, X.: Space-time code design in OFDM systems. In: Proceedings of IEEE Global Communications Conference, pp. 1000–1004 (2000)
4. Tufvesson, F., Maseng, T.: Pilot assisted channel estimation for OFDM in mobile cellular systems. In: IEEE VTC'97, vol. 3, pp. 1639–1643 (1997)
5. Heiskala, J., Terry, J.: OFDM Wireless LANs: A Theoretical and Practical Guide. SAMS, Carmel (2002)
6. van Nee, R., Prasad, R.: OFDM for Wireless Multimedia Communications. Artech House Publishers, London (2000)
7. Lau, H.K., Cheung, S.W.: A pilot symbol aided technique used for digital signals in multipath environments. In: IEEE ICC'94, vol. 2, pp. 1126–1130 (1994)
8. Cho, Y.S., Kim, J., Yang, W.Y., Kang, C.G.: MIMO-OFDM Wireless Communications with MATLAB. Wiley, Hoboken (2010)
9. Telatar, I.: Capacity of multi antenna Gaussian channels. *Eur. Trans. Tel.* **10**(6), 585–595 (1999)

10. Ertel, R.B., Cardieli, P., Sowerby, K.W., Rapport, T.S., Reed, J.H.: Overview of spatial channel models for antenna array communication systems. *IEEE Pers. Commun.* **5**(1), 10–22 (1998)
11. Kermoal, J.P., Schumacher, L., Pederson, K.I., Modensen, P.E., Fredriksen, F.: A stochastic MIMO radio channel model with experimental validation. *IEEE J. Sel. Areas Commun.* **20**(1), 1211–1226 (2002)
12. Gesbert, D., Bolcskei, H., Gore, D., Paulraj, A.: Outdoor MIMO channels: models and performance prediction. *IEEE Trans. Commun.* **50**(12), 1926–1934 (2002)
13. Loyka, S., Tsoulos, G.: Estimating MIMO system performance using the correlation matrix approach. *IEEE Commun. Lett.* **6**(1), 19–21 (2002)
14. van Zelst, A., Hammerschmidt, J.S.: A single coefficient spatial correlation model for multiple-input multiple-output (MIMO) radio channels. In: Proceedings of URSI 27th General Assembly Maastricht, Netherlands, pp. 657–660 (2002)
15. Durgin, G.D., Rappaport, T.S.: Effects of multipath angular spread on the spatial cross-correlation of received voltage envelopes. In: 49th IEEE Vehicular Technology Conference (VTC), vol. 2, pp. 996–1000 (1999)

Chapter 11

Space–Time Coding

In MIMO systems, diversity can be achieved by repetition coding in which different antennas at the transmitter transmit the same information at different time slots. The space–time (ST) coding is more bandwidth-efficient coding scheme, which transmits an information symbol block in a different order from each antenna. The diverse copies of the data transmitted are received with multiple receiving antennas. All the copies of the received signal are combined in an optimal way to extract information from each of them. This chapter describes different space–time coding schemes and analyzes their performance in Rayleigh fading.

11.1 Space–Time-Coded MIMO System

A ST-coded MIMO system with N_T transmit antennas and N_R receive antennas is shown in Fig. 11.1. In this MIMO system, the bit stream is mapped into a symbol stream $S_i, i = 1, \dots, N$. The N symbols are ST encoded into $s_{ij}, i = 1, 2, \dots, N_T, j = 1, 2, \dots, T$, where i represents antenna index and j stands for the symbol time index. Thus, $s_{ij}, i = 1, 2, \dots, N_T, j = 1, 2, \dots, T$ forms a ST code word with the number of symbols $N = N_T \cdot T$.

Space–time codes are categorized as space–time block codes (STBC) and ST trellis codes (STTC). Sections 11.2 through 11.5 discuss these codes. The performance of STTCs is better than that of STBCs. However, STTCs' complexity is more due to the maximum likelihood (ML) decoder in the receiver.

Electronic supplementary material The online version of this chapter (doi:[10.1007/978-81-322-2292-7_11](https://doi.org/10.1007/978-81-322-2292-7_11)) contains supplementary material, which is available to authorized users.

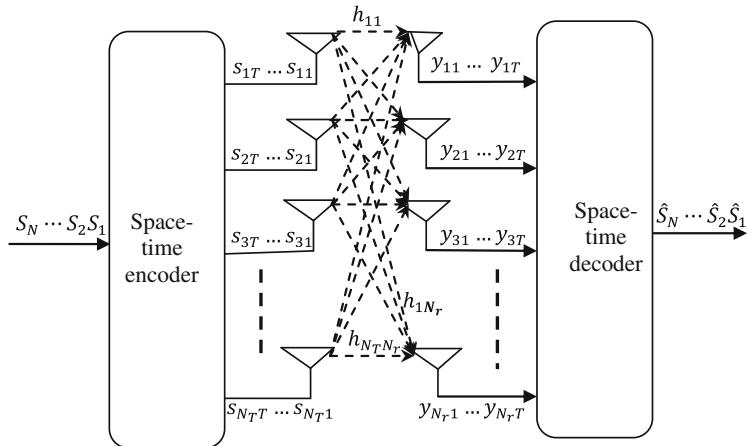


Fig. 11.1 Space–time-coded MIMO system

11.2 Space–Time Block Code (STBC)

An STBC is represented by the following code matrix S , in which each row represents one antenna's transmissions over time and each column represents a time slot.

$$S = \begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1T} \\ s_{21} & s_{22} & \cdots & s_{2T} \\ \vdots & \vdots & & \vdots \\ s_{N_T 1} & s_{N_T 2} & \cdots & s_{N_T T} \end{bmatrix} \quad (11.1)$$

where s_{ij} is the modulated symbol to be transmitted from antenna i in time slot j . T and N_T represent time slots and transmit antennas, respectively. The code rate of an STBC is defined as how many symbols per time slot it transmits on average. If k symbols are transmitted over T time slots, the code rate of STBC is

$$r = \frac{k}{T} \quad (11.2)$$

The matrix of STBC is to be designed so that it achieves highest possible diversity of $N_T N_R$ and highest possible code rate with minimum complexity of the decoder.

11.2.1 Rate Limit

It is proved in [1] that a code with N_T transmit antennas will yield the highest rate given by

$$r_{\max} = \frac{a_0 + 1}{2a_0} \quad (11.3)$$

where $N_T = 2a_0$ or $N_T = 2a_0 - 1$

11.2.2 Orthogonality

STBC is to be designed such that any pair of columns taken from the code matrix is orthogonal in order to make the decoding process at the receiver to be simple, linear, and optimal. However, a code that satisfies this criterion must sacrifice a part of its rate.

11.2.3 Diversity Criterion

Orthogonal STBCs can be shown to achieve the maximum diversity allowed by diversity criterion derived in [2]. Consider a code word

$$c = [c_{11} c_{21}, \dots, c_{N_T 1} \quad c_{12} c_{22}, \dots, c_{N_T 2} \quad \dots \quad c_{1T} c_{2T}, \dots, c_{N_T T}] \quad (11.4)$$

and let the corresponding erroneously decoded code word

$$\tilde{c} = [\tilde{c}_{11} \tilde{c}_{21}, \dots, \tilde{c}_{N_T 1} \quad \tilde{c}_{12} \tilde{c}_{22}, \dots, \tilde{c}_{N_T 2} \quad \dots \quad \tilde{c}_{1T} \tilde{c}_{2T}, \dots, \tilde{c}_{N_T T}] \quad (11.5)$$

Then, the $N_T \times T$ difference matrix $E(c, \tilde{c})$ can be defined as

$$E(c, \tilde{c}) = \begin{bmatrix} \tilde{c}_{11} - c_{11} & \tilde{c}_{12} - c_{12} & \cdots & \tilde{c}_{1T} - c_{1T} \\ \tilde{c}_{21} - c_{21} & \tilde{c}_{22} - c_{22} & \cdots & \tilde{c}_{2T} - c_{2T} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{c}_{N_T 1} - c_{N_T 1} & \tilde{c}_{N_T 2} - c_{N_T 2} & \cdots & \tilde{c}_{N_T T} - c_{N_T T} \end{bmatrix} \quad (11.6)$$

Rank and determinant criteria

Let $\rho(\rho \leq N_T)$ be the rank of difference matrix $E(c, \tilde{c})$. The $E(c, \tilde{c})$ should be full-rank matrix for any pair of distinct code words c and \tilde{c} to yield maximum possible diversity order of $N_T N_R$. Instead, if $E(c, \tilde{c})$ has minimum rank ρ over the set distinct

code word pairs, then diversity order is ρN_{R} [2]. Consider the following distance matrix

$$A(c, \tilde{c}) = E(c, \tilde{c})E^*(c, \tilde{c}) \quad (11.7)$$

where $E^*(c, \tilde{c})$ denotes the transpose conjugate of $E(c, \tilde{c})$.

The determinant criterion states that the minimum determinant of $A(c^i, c^j) = E(c^i, c^j)^H E(c^i, c^j)$ among all $i \neq j$ should be large to achieve high coding gains.

Trace criterion

A good design criterion is to maximize the minimum distance $\|E(c, \tilde{c})\|_F$ for all $i \neq j$. This is called the trace criterion because $\|E(c, \tilde{c})\|_F^2 = \text{Tr}[A(c, \tilde{c})]$. The metric $\|E(c, \tilde{c})\|_F$ provides all the good properties of a distance measure.

11.2.4 Performance Criteria

The rank of A is ρ , the kernel of A has a minimum dimension $N_{\text{Tx}} - \rho$, and exactly $N_{\text{Tx}} - \rho$ eigenvalues of A are zero. The nonzero eigenvalues of A can be denoted by $\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_\rho$. Assuming perfect channel state information (CSI), the probability of transmitting c and deciding in favor of \tilde{c} at the decoder is given by [3, 4]

$$P(c \rightarrow \tilde{c} | h_{ij}, i = 1, 2, \dots, N_{\text{Tx}}, j = 1, 2, \dots, N_{\text{Rx}}) \leq \exp\left(-d^2(c, \tilde{c}) \frac{E_s}{4N_0}\right) \quad (11.8)$$

where $\frac{N_0}{2}$ is the noise variance per dimension and

$$d^2(c, \tilde{c}) = \sum_{j=1}^{N_{\text{Rx}}} \sum_{t=1}^T \left| \sum_{i=1}^{N_{\text{Tx}}} h_{ij} (c_t^i - \tilde{c}_t^i) \right|^2 \quad (11.9)$$

is the Euclidean distance.

It follows from [3] that the pairwise error bound is given by

$$P(c \rightarrow \tilde{c}) \leq \left(\prod_{i=1}^{\rho} \lambda_i \right)^{-N_{\text{Rx}}} \left(\frac{E_s}{4N_0} \right)^{-\rho N_{\text{Rx}}} \quad (11.10)$$

To achieve the best performance for a given system, the rank and determinant criteria should be satisfied [4].

11.2.5 Decoding STBCs

One particular attractive feature of orthogonal STBCs is that ML decoding can be achieved at the receiver with only linear processing. In order to consider a decoding method, a model of the wireless communication system is needed.

At time t , the signal y_{jt} received at antenna j is

$$y_{jt} = \sum_{i=1}^{N_T} h_{ij} s_{it} + \eta_{jt} \quad (11.11)$$

where h_{ij} is the path gain from transmit antenna i to receive antenna j , s_{it} is the signal transmitted by transmit antenna i , and η_{jt} is the additive white Gaussian noise (AWGN).

The decision variables are formed by the maximum likelihood detection rule [7]

$$Y_i = \sum_{t=1}^{N_T} \sum_{j=1}^{N_R} y_{jt} h_{ek(i)j} \delta_k(i) \quad (11.12)$$

where $\delta_k(i)$ is the sign of s_i in the k th row of the coding matrix, $\epsilon_k(p) = q$ denotes that s_p is (up to a sign difference), the (k, q) element of the coding matrix, for $i = 1, 2, \dots, n_T$ and then decides on constellation symbol s_i that satisfies

$$s_i = \arg \min_{s \in A} \left(|Y_i - s|^2 + \left(-1 + \sum_{k,l} |h_{kl}|^2 \right) |s|^2 \right) \quad (11.13)$$

with A the constellation alphabet. Despite its appearance, this is a simple, linear decoding scheme that provides maximal diversity.

11.3 Alamouti Code

The very first and well-known STBC is the Alamouti code [6]. In the Alamouti encoder, two consecutive symbols s_1 and s_2 are encoded with the following ST code word matrix:

$$S = \begin{bmatrix} s_1 & -s_2^* \\ s_2 & s_1^* \end{bmatrix} \quad (11.14)$$

This indicates that during the first time slot, signals s_1 and s_2 are transmitted from antenna 1 and antenna 2, respectively. During the next time slot, antenna 1 and antenna 2 transmit $-s_2^*$ and s_1^* , respectively. It is only STBC in which maximum diversity can be achieved without sacrificing its data rate because Alamouti code has rate 1 as it takes two time slots to transmit two symbols.

11.3.1 2-Transmit, 1-Receive Alamouti STBC Coding

For Alamouti Scheme with two transmit and one receive antennas shown in Fig. 11.2, if y_1 and y_2 denote the signals received at first time slot and second time slot, respectively, we have

$$\begin{aligned} [y_1 \quad y_2] &= [h_1 \quad h_2] \begin{bmatrix} s_1 & -s_2^* \\ s_2 & s_1^* \end{bmatrix} [\eta_1 \quad \eta_2] \\ &= [h_1 s_1 + h_2 s_2 + \eta_1 \quad -h_1 s_2^* + h_2 s_1^* + \eta_2] \end{aligned} \quad (11.15)$$

where s_1, s_2 are the transmitted symbols, h_1 is the channel from first transmit antenna to receive antenna, h_2 is the channel from second transmit antenna to receive antenna, and η_1, η_2 are the noise at time slot 1 and time slot 2.

The combiner generates [2].

$$\tilde{s}_1 = h_1^* y_1 + h_2^* y_2 \quad (11.16)$$

and

$$\tilde{s}_2 = h_2^* y_1 - h_1^* y_2 \quad (11.17)$$

To decode, the ML decoder minimizes the following decision metric (for decoding) s_1 and s_2 , respectively [5].

$$|\tilde{s}_1 - s_1|^2 + \xi |s_1|^2 \quad (11.18)$$

$$|\tilde{s}_2 - s_2|^2 + \xi |s_2|^2 \quad (11.19)$$

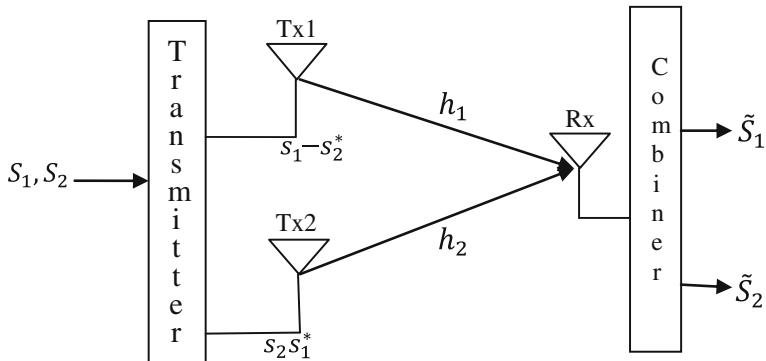


Fig. 11.2 Alamouti scheme with two transmit and one receive antennas

where

$$\xi = \left(-1 + \sum_{i=1}^{N_t} |h_i|^2 \right) \quad (11.20)$$

BER with Alamouti (2×1) STBC

From Eq. (2.44), BER for a 2-branch MRC (i.e., with one transmitting and two receiving antennas) with BPSK modulation can be expressed as

$$\text{BER}_{\text{MRC}(1 \times 2)} = p_{\text{MRC}}^2 [1 + 2(1 - p_{\text{MRC}})] \quad (11.21)$$

where

$$p_{\text{MRC}} = \frac{1}{2} - \frac{1}{2} \left(1 + \frac{1}{E_b/N_0} \right)^{-1/2} \quad (11.22)$$

Then, the BER for the Alamouti 2-transmit, 1-receive antenna STBC case with BPSK modulation can be written as

$$\text{BER}_{\text{Alamouti}(2 \times 1)} = p_{\text{Alamouti}}^2 [1 + 2(1 - p_{\text{Alamouti}})] \quad (11.23)$$

where

$$p_{\text{Alamouti}} = \frac{1}{2} - \frac{1}{2} \left(1 + \frac{2}{E_b/N_0} \right)^{-1/2} \quad (11.24)$$

It can be easily shown [6] that the performance of the Alamouti scheme with two transmitters and a single receiver is identical to that of the two-branch MRC provided that each transmit antenna in the Alamouti scheme radiates the same energy as the single transmit antenna for MRC.

11.3.2 2-Transmit, 2-Receive Alamouti STBC Coding

For Alamouti Scheme with two transmit and two receive antennas shown in Fig. 11.3, if y_{11} , y_{12} , y_{21} , and y_{22} denote the signals received by antenna 1 at first time slot, by antenna 1 at second time slot, by antenna 2 at first time slot, and by antenna 2 at second time slot, respectively, we have

$$\begin{bmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{bmatrix} \begin{bmatrix} s_1 & -s_2^* \\ s_2 & s_1^* \end{bmatrix} + \begin{bmatrix} \eta_{11} & \eta_{12} \\ \eta_{21} & \eta_{22} \end{bmatrix} \quad (11.25)$$

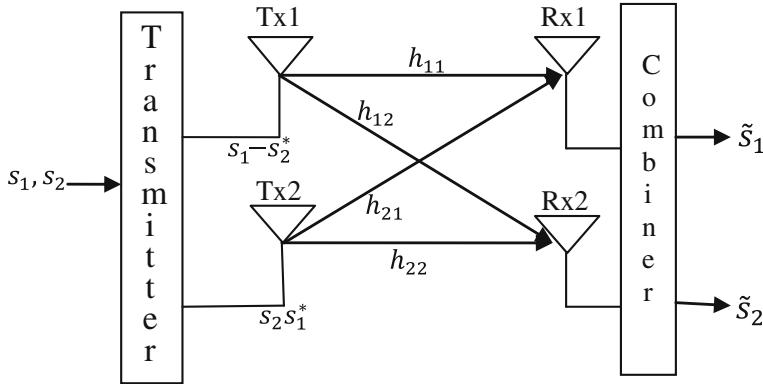


Fig. 11.3 Alamouti scheme with two transmit and two receive antennas

$$= \begin{bmatrix} h_{11}s_1 + h_{12}s_2 + \eta_{11} & -h_{11}s_2^* + h_{12}s_1^* + \eta_{21} \\ h_{21}s_1 + h_{22}s_2 + \eta_{21} & -h_{21}s_2^* + h_{22}s_1^* + \eta_{22} \end{bmatrix} \quad (11.26)$$

where h_{ij} is the channel from i th transmit antenna to j th receive antenna, s_1, s_2 are the transmitted symbols, $\begin{bmatrix} \eta_{11} \\ \eta_{12} \end{bmatrix}$ are the noise at time slot 1 on receive antennas 1 and 2, respectively, and $\begin{bmatrix} \eta_{21} \\ \eta_{22} \end{bmatrix}$ are the noise at time slot 2 on receive antennas 1 and 2, respectively.

The combiner generates [2]

$$\tilde{s}_1 = h_{11}^*y_{11} + h_{12}^*y_{12}^* + h_{21}^*y_{21} + h_{22}^*y_{22}^* \quad (11.27)$$

and

$$\tilde{s}_2 = h_{12}^*y_{11} - h_{11}^*y_{12}^* + h_{22}^*y_{21} - h_{21}^*y_{22}^* \quad (11.28)$$

To decode, the ML decoder minimizes the following decision metric (for decoding) s_1 and s_2 , respectively [5].

$$|\tilde{s}_1 - s_1|^2 + \xi |s_1|^2 \quad (11.29)$$

$$|\tilde{s}_2 - s_2|^2 + \xi |s_2|^2 \quad (11.30)$$

where

$$\xi = \left(-1 + \sum_{i=1}^{N_r} \sum_{j=1}^{N_t} |h_{ij}|^2 \right) \quad (11.31)$$

BER with Alamouti (2×2) STBC

From Eq. (2.44), BER for 4-branch MRC (i.e., with one transmitting and four receiving antennas) with BPSK modulation can be expressed as

$$\text{BER}_{\text{MRC}(1 \times 4)} = p_{\text{MRC}}^4 \left[1 + 4(1 - p_{\text{MRC}}) + 10(1 - p_{\text{MRC}})^2 + 20(1 - p_{\text{MRC}})^3 \right] \quad (11.32)$$

BER for Alamouti (2×2) STBC case with BPSK modulation can be written as

$$\text{BER}_{\text{Alamouti}(2 \times 2)} = p_{\text{Alamouti}}^4 \left[1 + 4(1 - p_{\text{Alamouti}}) + 10(1 - p_{\text{Alamouti}})^2 + 20(1 - p_{\text{Alamouti}})^3 \right] \quad (11.33)$$

11.3.3 Theoretical BER Performance of BPSK Alamouti Codes Using MATLAB

The following MATLAB program illustrates the BER performance of uncoded coherent BPSK for MRC and Alamouti STBC in Rayleigh fading channel.

Program 11.1 BER performance of MRC and Alamouti coding

```
% BER performance of Alamouti(2x1),Alamouti(2x2) using BPSK modulation
clear; clc;
Eb_N0_dB=[0:2:20];
for i=1:length(Eb_N0_dB);
    EbN0=Eb_N0_dB(i); sigma=sqrt(0.5/(10^(EbN0/10)));
    EbN0Lin = 10.^(EbN0/10);p = 1/2 - 1/2*(1+1./EbN0Lin).^(1/2);
    p1 = 1/2 - 1/2*(1+2./EbN0Lin).^(1/2);
    BER1(i) = 0.5.*((1-p).^(1+1./EbN0Lin)).^(1/2);
    BER2(i) = p1.^2.*((1-p).^(1+2*(1-p)));
    BER3(i) = p.^2.*((1-p).^(1+2*(1-p)));
    BER4(i) = p1.^4.*((1-p).^(1+4*(1-p))+(10*(1-p)).^2)+(20*(1-p)).^3);
    BER5(i) = p.^4.*((1-p).^(1+4*(1-p))+(10*(1-p)).^2)+(20*(1-p)).^3);
end % End of FOR loop for Eb_N0_dB
semilogy(Eb_N0_dB,BER1,'-o');
semilogy(Eb_N0_dB,BER2,'-+');
semilogy(Eb_N0_dB,BER3,'-o');
semilogy(Eb_N0_dB,BER4,'-*');
semilogy(Eb_N0_dB,BER5,'-x');
axis([Eb_N0_dB([1 end]) 1e-6 1e0]);
grid on; xlabel('Eb/No(dB)'); ylabel('BER');
legend('SISO (no diversity)', 'Alamouti(2x1)', 'MRC(1x2)', 'Alamouti(2x2)', 'MRC(1x4)');
```

BER performance obtained by using Program 11.1 is shown in Fig. 11.4.

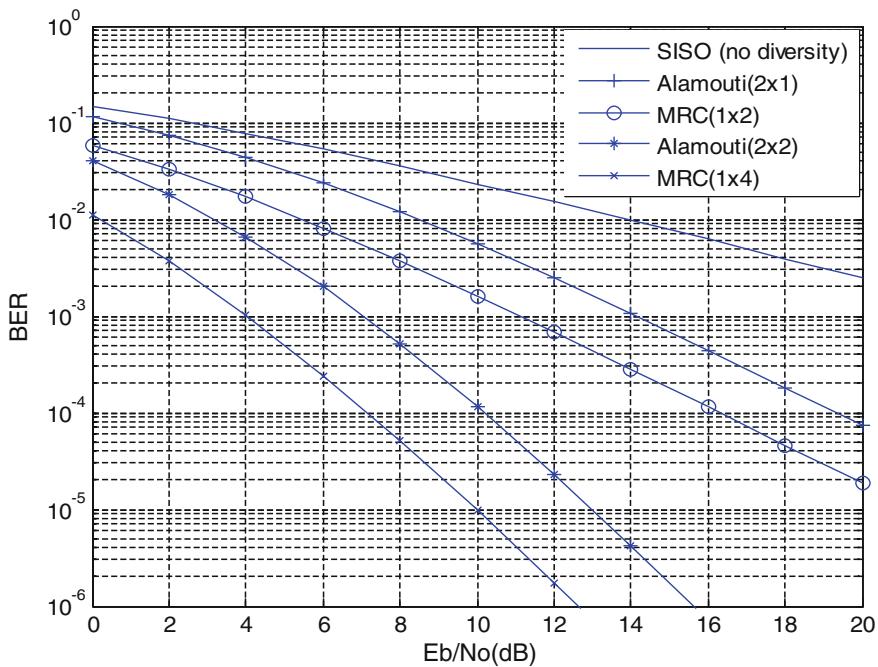


Fig. 11.4 BER performance comparison of coherent BPSK with MRC and Alamouti STBC

From Fig. 11.4, the performance of Alamouti 2×1 STBC and Alamouti 2×2 STBC is 3 dB worse as compared to 1×2 MRC and 1×4 MRC, respectively. The 3-dB penalty is due to the assumption that each transmit antenna in the Alamouti STBC scheme radiates half the energy in order to ensure the same total radiated power as with one transmit antenna of MRC. If each transmit antenna in Alamouti scheme radiates the same energy as the single transmit antenna for MRC, then the performance of Alamouti scheme and MRC is identical.

11.4 Higher-Order STBCs

The Alamouti scheme discussed in Sect. 11.3 is part of a general class of STBCs known as orthogonal space–time block codes (OSTBCs) [2]. It is proved in [5, 7] that no code for more than 2 transmit antennas can achieve full rate. This section briefly discusses the full diversity complex orthogonal codes for $N_T > 2$.

3 transmit antennas

The full diversity, rate 1/2 code for $N_T = 3$ is given by [5, 7]: This code transmits 4 symbols every 8 time intervals and therefore has rate 1/2.

$$G_3 = \begin{bmatrix} S_1 & -S_2 & -S_3 & -S_4 & S_1^* & -S_2^* & -S_3^* & -S_4^* \\ S_2 & S_1 & S_4 & -S_3 & S_2^* & S_1^* & S_4^* & -S_3^* \\ S_3 & -S_4 & S_1 & S_2 & S_3^* & -S_4^* & S_1^* & S_2^* \end{bmatrix} \quad (11.34)$$

4 transmit antennas

In the case of 4 transmit antennas, the rate 1/2 code block is given by [5, 7], where similar to Eq. (11.34) has rate 1/2 as 4 symbols are transmitted in 8 time intervals

$$G_4 = \begin{bmatrix} s_1 & -s_2 & -s_3 & -s_4 & s_1^* & -s_2^* & -s_3^* & -s_4^* \\ s_2 & s_1 & s_4 & -s_3 & s_2^* & s_1^* & s_4^* & -s_3^* \\ s_3 & -s_4 & s_1 & s_2 & s_3^* & -s_4^* & s_1^* & s_2^* \\ s_4 & s_3 & -s_2 & s_1 & s_4^* & s_3^* & -s_2^* & s_1^* \end{bmatrix} \quad (11.35)$$

11.4.1 3-Transmit, 4-Receive STBC Coding

A STBC scheme with three transmit and four receive antennas is shown in Fig. 11.5. If $y_{11}, y_{12}, \dots, y_{18}$, $y_{21}, y_{22}, \dots, y_{28}$, $y_{31}, y_{32}, \dots, y_{38}$, and $y_{41}, y_{42}, \dots, y_{48}$ denote the signals received by antenna 1, antenna 2, antenna 3, and antenna 4 at

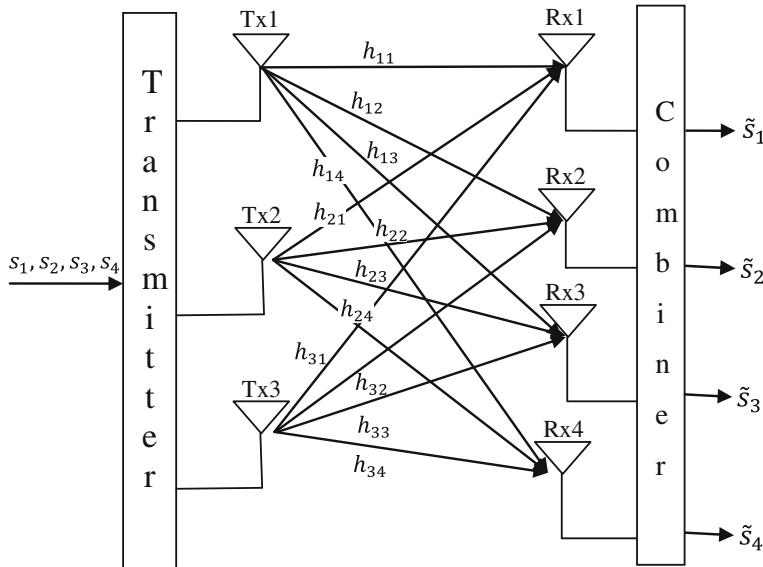


Fig. 11.5 STBC scheme with three transmit and four receive antennas

time slots 1, 2, ..., 8, respectively, and $h_{ij}(i = 1, 2, 3; j = 1, 2, 3, 4)$ are path gains from antenna i to antenna j , we have

$$\begin{aligned}
 & \begin{bmatrix} y_{11} & y_{12} & y_{13} & y_{14} & y_{15} & y_{16} & y_{17} & y_{18} \\ y_{21} & y_{22} & y_{23} & y_{24} & y_{25} & y_{26} & y_{27} & y_{28} \\ y_{31} & y_{32} & y_{33} & y_{34} & y_{35} & y_{36} & y_{37} & y_{38} \\ y_{41} & y_{42} & y_{43} & y_{44} & y_{45} & y_{46} & y_{47} & y_{48} \end{bmatrix} \\
 &= \begin{bmatrix} h_{11} & h_{21} & h_{31} \\ h_{12} & h_{22} & h_{32} \\ h_{13} & h_{23} & h_{33} \\ h_{14} & h_{24} & h_{34} \end{bmatrix} \begin{bmatrix} S_1 & -S_2 & -S_3 & -S_4 & S_1^* & -S_2^* & -S_3^* & -S_4^* \\ S_2 & S_1 & S_4 & -S_3 & S_2^* & S_1^* & S_4^* & -S_3^* \\ S_3 & -S_4 & S_1 & S_2 & S_3^* & -S_4^* & S_1^* & S_2^* \end{bmatrix} \\
 &+ \begin{bmatrix} \eta_{11} & \eta_{12} & \eta_{13} & \eta_{14} & \eta_{15} & \eta_{16} & \eta_{17} & \eta_{18} \\ \eta_{21} & \eta_{22} & \eta_{23} & \eta_{24} & \eta_{25} & \eta_{26} & \eta_{27} & \eta_{28} \\ \eta_{31} & \eta_{32} & \eta_{33} & \eta_{34} & \eta_{35} & \eta_{36} & \eta_{37} & \eta_{38} \\ \eta_{41} & \eta_{42} & \eta_{43} & \eta_{44} & \eta_{45} & \eta_{46} & \eta_{47} & \eta_{48} \end{bmatrix} \quad (11.36)
 \end{aligned}$$

The Decoding Algorithm

ML decoding of any space-time block code can be achieved using only linear processing at the receiver, and we illustrate this by example. The space-time block code G_3 has s_1, s_2, s_3 and s_4 and their conjugates. These symbols are transmitted simultaneously from antennas one, two, and three, respectively. Then, ML detection amounts to minimizing the decision metric

$$\begin{aligned}
 & \sum_{j=1}^m \left(|y_{1j} - h_{1j}s_1 - h_{2j}s_2 - h_{3j}s_3|^2 + |y_{2j} + h_{1j}s_2 - h_{2j}s_1 + h_{3j}s_4|^2 \right. \\
 & \quad + |y_{3j} + h_{1j}s_3 - h_{2j}s_4 - h_{3j}s_1|^2 + |y_{4j} + h_{1j}s_4 + h_{2j}s_3 - h_{3j}s_2|^2 \\
 & \quad + |y_{1j} - h_{1j}s_1^* - h_{2j}s_2^* - h_{3j}s_3^*|^2 + |y_{6j} + h_{1j}s_2^* - h_{2j}s_1^* + h_{3j}s_4^*|^2 \\
 & \quad \left. + |y_{7j} + h_{1j}s_3^* - h_{2j}s_4^* - h_{3j}s_1^*|^2 + |y_{8j} + h_{1j}s_4^* + h_{2j}s_3^* - h_{3j}s_2^*|^2 \right) \quad (11.37)
 \end{aligned}$$

over all possible values of s_1, s_2, s_3 and s_4 . Note that due to the quasi-static nature of the channel, the path gains are constant over transmissions. The minimizing values are the receiver estimates of s_1, s_2, s_3 and s_4 , respectively. We expand the above metric and delete the terms that are independent of the code word and observe that the above minimization is equivalent to minimizing

$$\begin{aligned}
& - \sum_{j=1}^m \left[y_{1j} h_{1j}^* s_1^* + y_{1j} h_{2j}^* s_2^* + y_{1j} h_{3j}^* s_3^* - y_{2j} h_{1j}^* s_2^* + y_{2j} h_{2j}^* s_1^* - y_{2j} h_{3j}^* s_4^* \right. \\
& \quad - y_{3j} h_{1j}^* s_3^* + y_{3j} h_{2j}^* s_4^* + y_{3j} h_{3j}^* s_1^* - y_{4j} h_{1j}^* s_4^* - y_{4j} h_{2j}^* s_3^* + y_{4j} h_{3j}^* s_2^* \\
& \quad + (y_{5j})^* h_{1j} s_1 + (y_{5j})^* h_{3j} s_3 - (y_{6j})^* h_{1j} s_2 + (y_{6j})^* h_{2j} s_1 - (y_{6j})^* h_{3j} s_4 \\
& \quad - (y_{7j})^* h_{1j} s_3 + (y_{7j})^* h_{2j} s_4 + (y_{7j})^* h_{3j} s_1 - (y_{8j})^* h_{1j} s_4 - (y_{8j})^* h_{2j} s_3 \\
& \quad \left. + (y_{8j})^* h_{3j} s_2 \right] + \left(|s_1|^2 + |s_2|^2 + |s_3|^2 + |s_4|^2 \right) \sum_{j=1}^m \sum_{i=1}^3 |h_{ij}|^2
\end{aligned} \tag{11.38}$$

The above metric decomposes into four parts; the function of s_1 is

$$\begin{aligned}
& - \sum_{j=1}^m \left(y_{1j} h_{1j}^* s_1^* + y_{2j} h_{2j}^* s_1^* + y_{3j} h_{3j}^* s_1^* + (y_{5j})^* h_{1j} s_1 + (y_{6j})^* h_{2j} s_1 \right. \\
& \quad \left. + (y_{7j})^* h_{3j} s_1 \right) + \left(|s_1|^2 \right) \sum_{j=1}^m \sum_{i=1}^3 |\alpha_{ij}|^2
\end{aligned} \tag{11.39}$$

The function of s_2 is

$$\begin{aligned}
& - \sum_{j=1}^m \left(y_{1j} h_{2j}^* s_2^* - y_{2j} h_{1j}^* s_2^* + y_{4j} h_{3j}^* s_2^* + (y_{5j})^* \alpha_{2j} s_2 - (y_{6j})^* \alpha_{1j} s_2 \right. \\
& \quad \left. + (y_{8j})^* \alpha_{3j} s_2 \right) + \left(|s_2|^2 \right) \sum_{j=1}^m \sum_{i=1}^3 |h_{ij}|^2
\end{aligned} \tag{11.40}$$

The function of s_3 is

$$\begin{aligned}
& - \sum_{j=1}^m \left(y_{1j} h_{3j}^* s_3^* - y_{3j} h_{1j}^* s_3^* - y_{4j} h_{2j}^* s_3^* + (y_{5j})^* h_{3j} s_3 - (y_{7j})^* h_{1j} s_3 \right. \\
& \quad \left. - (y_{8j})^* h_{2j} s_3 \right) + \left(|s_3|^2 \right) \sum_{j=1}^m \sum_{i=1}^3 |h_{ij}|^2
\end{aligned} \tag{11.41}$$

The function of s_4 is

$$\begin{aligned}
& - \sum_{j=1}^m \left(y_{2j} h_{3j}^* s_4^* + y_{3j} h_{2j}^* s_4^* - y_{4j} h_{1j}^* s_4^* + (y_{6j})^* h_{3j} s_4 + (y_{7j})^* h_{2j} s_4 \right. \\
& \quad \left. - (y_{8j})^* h_{1j} s_4 \right) + \left(|s_4|^2 \right) \sum_{j=1}^m \sum_{i=1}^3 |h_{ij}|^2
\end{aligned} \tag{11.42}$$

Thus, the minimization of (11.38) is equivalent to minimizing these four parts separately. This in turn is equivalent to minimizing; the decision metric for detecting s_1 is

$$\left| \sum_{j=1}^m \left(y_{1j} h_{1j}^* + y_{2j} h_{2j}^* + y_{3j} h_{3j}^* + (y_{5j})^* h_{1j} + (y_{6j})^* h_{2j} + (y_{7j})^* h_{3j} \right) - s_1 \right|^2 + \left(-1 + 2 \sum_{j=1}^m \sum_{i=1}^3 |h_{ij}|^2 \right) |s_1|^2 \quad (11.43)$$

The decision metric for detecting s_2 is

$$\left| \sum_{j=1}^m \left(y_{1j} h_{2j}^* - y_{2j} h_{1j}^* + y_{4j} h_{3j}^* + (y_{5j})^* h_{2j} - (y_{6j})^* h_{1j} + (y_{8j})^* h_{3j} \right) - s_2 \right|^2 + \left(-1 + 2 \sum_{j=1}^m \sum_{i=1}^3 |h_{ij}|^2 \right) |s_2|^2 \quad (11.44)$$

The decision metric for detecting s_3 is

$$\left| \sum_{j=1}^m \left(y_{1j} h_{3j}^* - y_{3j} h_{1j}^* - y_{4j} h_{2j}^* + (y_{5j})^* h_{3j} - (y_{7j})^* h_{1j} - (y_{8j})^* h_{2j} \right) - s_3 \right|^2 + \left(-1 + 2 \sum_{j=1}^m \sum_{i=1}^3 |h_{ij}|^2 \right) |s_3|^2 \quad (11.45)$$

The decision metric for detecting s_4 is

$$\left| \sum_{j=1}^m \left(-y_{2j} h_{3j}^* + y_{3j} h_{2j}^* - y_{4j} h_{1j}^* - (y_{6j})^* h_{3j} + (y_{7j})^* h_{2j} - (y_{8j})^* h_{1j} \right) - s_4 \right|^2 + \left(-1 + 2 \sum_{j=1}^m \sum_{i=1}^3 |\alpha_{ij}|^2 \right) |s_4|^2 \quad (11.46)$$

11.4.2 Simulation of BER Performance of STBCs Using MATLAB

The following MATLAB Program 11.2 and MATLAB function Programs 11.3, 11.4, 11.5, and 11.6 are used to simulate the BER performance of QPSK and 16-QAM for STBC (3×4), Alamouti (2×2), and Alamouti (2×1).

Program 11.2 “STBC simulation.m” for BER performance comparison of STBC (3×4), Alamouti(2×2), and Alamouti (2×1) in Rayleigh fading channel

```
%STBCsimulation.m
% BER performance of Alamouti(2x1),Alamouti(2x2),STBC(3x4)
clear;clc;
framesize=128; Packets=4*1024; % Number of frames/packet and Number of
packets
b=input('enter the value b=1 for BPSK,b=2 for QPSK,b=4 for 16-QAM');
M=2^b;
Eb_N0_dB=[0:2:20];
for i=1:length(Eb_N0_dB)
    EbN0=Eb_N0_dB(i); sigma=sqrt(0.5/(10^(EbN0/10)));
    for i1=1:Packets
        [Xo1 Xe1]=stbc2by1(framesize,Packets,2,M,sigma,b);
        [Xo2 Xe2]=stbc2by2(framesize,Packets,2,M,sigma,b);
        [Xo3 Xe3]=stbc3by4(framesize,Packets,3,M,sigma,b);
        packet_error1(i1) = sum(sum(Xo1~=Xe1));
        packet_error2(i1) = sum(sum(Xo2~=Xe2));
        packet_error3(i1) = sum(sum(Xo3~=Xe3));
    end % End of FOR loop for packets
    BER1(i) = sum(packet_error1)/(Packets*framesize*b);
    BER2(i) = sum(packet_error2)/(Packets*framesize*b);
    BER3(i) = sum(packet_error3)/(Packets*framesize*b);
end % End of FOR loop for Eb_N0_dB
semilogy(Eb_N0_dB,BER1,'x'),hold on;
semilogy(Eb_N0_dB,BER2,'+'), hold on;
semilogy(Eb_N0_dB,BER3,'o'),axis([Eb_N0_dB([1 end]) 1e-6 1e0]);
grid on; xlabel('Eb/No(dB)'), ylabel('BER');
legend('Alamouti(2x1)', 'Alamouti(2x2)', 'STBC(3x4)')
```

Program 11.3 MATLAB function for stbc2by1

```

function [So Se]=stbc2by1(framesize,Packets,NT,M,sigma,b)
inp_bits=randint(framesize*b,M);
bitsequence=inp_bits.';
tmp=[]; tmp1=[];
for i=1:NT
[tmp1,symbols] = modulation(bitsequence(i,:),b); tmp=[tmp; tmp1];
end
S=tmp.';
S1=S; S2=[-conj(S(:,2)) conj(S(:,1))];
H=(randn(framesize,NT)+j*randn(framesize,NT))/sqrt(2);
Habs=sum(abs(H).^2,2);
y11 = sum(H.*S1,2)/sqrt(2) + sigma*(randn(framesize,1)+j*randn(framesize,1));
y12 = sum(H.*S2,2)/sqrt(2)+ sigma*(randn(framesize,1)+j*randn(framesize,1));
S1e = y11 .*conj(H(:,1)) + conj(y12).*H(:,2);
S2e = y11.*conj(H(:,2))- conj(y12).*H(:,1);
for m=1:M
eta = (-1+sum(Habs,2))*abs(symbols(m))^2;
d1(:,m) = abs(sum(S1e,2)-symbols(m)).^2 + eta;
d2(:,m) = abs(sum(S2e,2)-symbols(m)).^2 + eta;
end
[y1,i1]=min(d1,[],2); S1d=symbols(i1).'; clear d1
[y2,i2]=min(d2,[],2); S2d=symbols(i2).'; clear d2
Sd =[S1d S2d]; So=S>0; Se=Sd>0;

```

Program 11.4 MATLAB function for stbc2by2

```

function [So Se]=stbc2by2(framesize,Packets,NT,M,sigma,b)
inp_bits=randint(framesize*b,M);
bitsequence=inp_bits.';
tmp=[]; tmp1=[];
for i=1:NT
[tmp1,symbols] = modulation(bitsequence(i,:),b); tmp=[tmp; tmp1];
end
S=tmp.';
S1=S; S2=[-conj(S(:,2)) conj(S(:,1))];
H=(randn(framesize,2*NT)+j*randn(framesize,2*NT))/sqrt(2);Habs=sum(abs(H).^2,2);
y11 = sum(H(:,1:2).*S1,2)/sqrt(2) + sigma*(randn(framesize,1)+j*randn(framesize,1));
y12 = sum(H(:,1:2).*S2,2)/sqrt(2)+ sigma*(randn(framesize,1)+j*randn(framesize,1));
y21 = sum(H(:,3:4).*S1,2)/sqrt(2) + sigma*(randn(framesize,1)+j*randn(framesize,1));
y22 = sum(H(:,3:4).*S2,2)/sqrt(2)+ sigma*(randn(framesize,1)+j*randn(framesize,1));
S1e = y11 .*conj(H(:,1)) + conj(y12).*H(:,2)+y21 .*conj(H(:,3)) + conj(y22).*H(:,4);
S2e = y11.*conj(H(:,2))- conj(y12).*H(:,1)+y21.*conj(H(:,4))- conj(y22).*H(:,3);
for m=1:M
eta = (-1+sum(Habs,2))*abs(symbols(m))^2;
d1(:,m) = abs(sum(S1e,2)-symbols(m)).^2 + eta;
d2(:,m) = abs(sum(S2e,2)-symbols(m)).^2 + eta;
end
[y1,i1]=min(d1,[],2); S1d=symbols(i1).'; clear d1
[y2,i2]=min(d2,[],2); S2d=symbols(i2).'; clear d2
Sd =[S1d S2d]; So=S>0; Se=Sd>0;

```

Program 11.5 MATLAB function for stbc3by4

```

function [So Se]=stbc3by4(framesize,Packets,NT,M,sigma,b)
inp_bits=randint(framesize*b,M);
bitsequence=inp_bits.';
temp=[]; temp1=[];
for i=1:4
[temp1,symbols]=modulation(bitsequence(i,:),b); temp=[temp; temp1];
end
S=temp.';
% Block signals in the l-th time slot % Block coding for G3 STBC
S1=S(:,1:3); S5=conj(S1);
S2 = [-S(:,2) S(:,1) -S(:,4)]; S6=conj(S2);
S3 = [-S(:,3) S(:,4) S(:,1)]; S7=conj(S3);
S4 = [-S(:,4) -S(:,3) S(:,2)]; S8=conj(S4);
for n=1:NT
Hr(n,:,:)=(randn(framesize,NT)+j*randn(framesize,NT))/sqrt(2);
end
for n=1:NT
H = reshape(Hr(n,:,:),framesize,NT); Hc=conj(H);
Habs(:,n) = sum(abs(H).^2,2);
y1 = sum(H.*S1,2)/sqrt(NT)+sigma*(randn(framesize,1)+j*randn(framesize,1));
y2 = sum(H.*S2,2)/sqrt(NT)+sigma*(randn(framesize,1)+j*randn(framesize,1));
y3 = sum(H.*S3,2)/sqrt(NT)+sigma*(randn(framesize,1)+j*randn(framesize,1));
y4 = sum(H.*S4,2)/sqrt(NT)+sigma*(randn(framesize,1)+j*randn(framesize,1));
y5 = sum(H.*S5,2)/sqrt(NT)+sigma*(randn(framesize,1)+j*randn(framesize,1));
y6 = sum(H.*S6,2)/sqrt(NT)+sigma*(randn(framesize,1)+j*randn(framesize,1));
y7 = sum(H.*S7,2)/sqrt(NT)+sigma*(randn(framesize,1)+j*randn(framesize,1));
y8 = sum(H.*S8,2)/sqrt(NT)+sigma*(randn(framesize,1)+j*randn(framesize,1));
Se(:,n,1) = y1.*Hc(:,1) + y2.*Hc(:,2) + y3.*Hc(:,3)+ conj(y5).*H(:,1) +
conj(y6).*H(:,2) + conj(y7).*H(:,3);
Se(:,n,2) = y1.*Hc(:,2) - y2.*Hc(:,1) + y4.*Hc(:,3)+ conj(y5).*H(:,2) -
conj(y6).*H(:,1) + conj(y8).*H(:,3);
Se(:,n,3) = y1.*Hc(:,3) - y3.*Hc(:,1) - y4.*Hc(:,2)+ conj(y5).*H(:,3) -
conj(y7).*H(:,1) - conj(y8).*H(:,2);
Se(:,n,4) =-y2.*Hc(:,3) + y3.*Hc(:,2) - y4.*Hc(:,1)+ (-conj(y6)).*H(:,3) +
conj(y7).*H(:,2) - conj(y8).*H(:,1);
end
for m=1:M
tmp = (-1+sum(Habs,2))*abs(symbols(m))^2;
for i=1:4
d(:,m,i) = abs(sum(Se(:, :, i), 2)-symbols(m)).^2 + tmp;
end
end
Sd = [];
for n=1:4, [yn,in]=min(d(:, :, n),[],2); Sd = [Sd symbols(in).'];
end
So=S>0; Se=Sd>0;
```

Program 11.6 MATLAB function for BPSK, QPSK and 16-QAM mapping

```

function [modsymbols,symbols] = modulation(inp,b)
bitlength = length(inp);
switch b
case {1} % BPSK modulation
symbols=exp(j*[0 -pi]); symbols=symbols([1 0]+1);
modsymbols=symbols(inp+1);
case {2} % QPSK modulation
symbols = exp(j*pi/4*[-3 3 1 -1]); symbols=symbols([0 1 3 2]+1);
inp=reshape(inp,b,bitlength/b);
modsymbols=symbols([2 1]*inp+1);
case {4} % 16-QAM modulation
m=0;
for k=-3:2:3
for l=-3:2:3
m=m+1; symbols(m) = (k+j*l)/sqrt(10); % power normalization
end
end
symbols = symbols([0 1 3 2 4 5 7 6 12 13 15 14 8 9 11 10]+1);
inp = reshape(inp,b,bitlength/b);
modsymbols = symbols([8 4 2 1]*inp+1);
% maps transmitted bits into 16QAM symbols
otherwise
disp ('Unimplemented modulation!');
end

```

The BER performance obtained by using above programs for QPSK and 16-QAM with STBC (3×4), Alamouti (2×2), and Alamouti (2×1) are shown in Figs. 11.6 and 11.7, respectively.

From Figs. 11.6 and 11.7, it can be seen that the BER performance of STBC (3×4) is better than Alamouti (2×2) and Alamouti (2×1).

11.5 Space–Time Trellis Coding

In contrast to STBCs, STTCs provide both coding gain and diversity gain and have a better bit error rate performance. However, STTCs are more complex than STBCs to encode and decode.

In [2], Tarokh et al. derived the design criteria for STTCs over slow-frequency non-selective fading channels. The design criteria were shown to be determined by the distance matrices constructed from pairs of distinct code words. The minimum rank of the distance matrices was used to determine the diversity gain, and the minimum distance of the distance matrices was used to determine the coding gain [3]. The system model for STTC modulation is shown in Fig. 11.8.

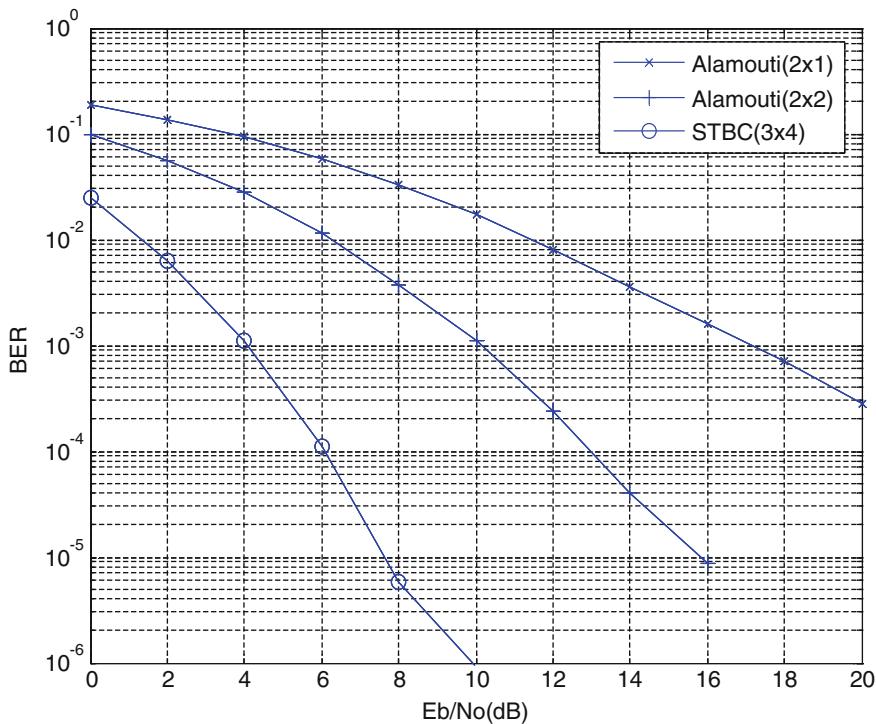


Fig. 11.6 BER performance for QPSK with STBC (3 × 4), Alamouti (2 × 2), and Alamouti (2 × 1)

11.5.1 Space-Time Trellis Encoder

Let $I_t = \begin{bmatrix} I_t^1 \\ I_t^2 \\ \vdots \\ I_t^m \end{bmatrix}$ denote input data symbol of $m = \log_2 M$ bits, which is input to the encoder at time $t = 0, 1, 2, \dots$; then, a sequence of input data symbols is represented as

$$I = \begin{bmatrix} I_0^1 & I_1^1 & \cdots & I_t^1 \cdots \\ I_0^2 & I_1^2 & \cdots & I_t^2 \cdots \\ \vdots & \vdots & \ddots & \vdots \\ I_0^m & I_1^m & \cdots & I_t^m \cdots \end{bmatrix} \quad (11.47)$$

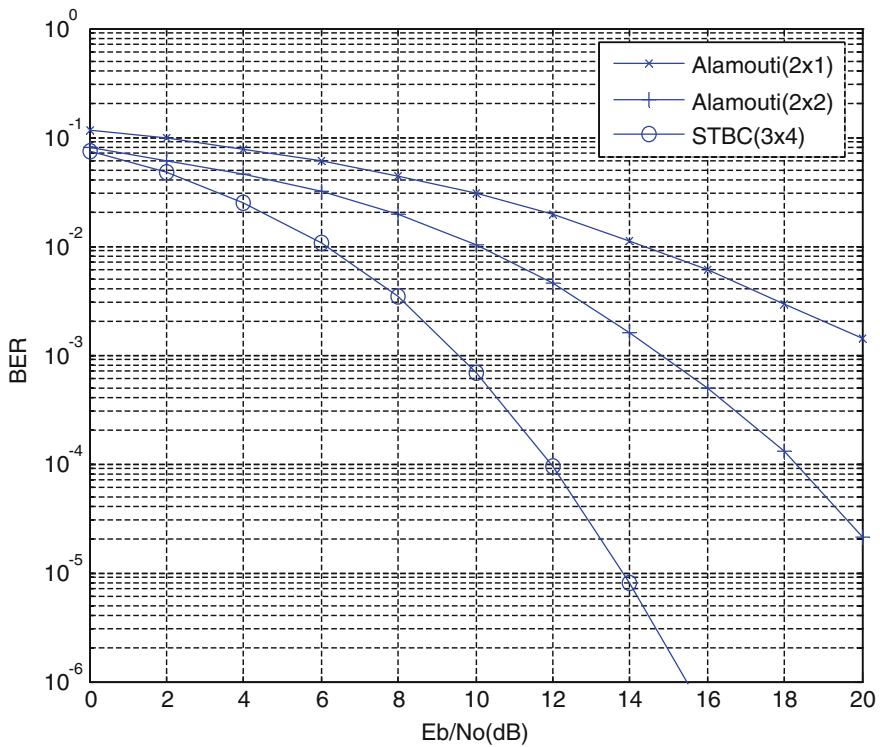


Fig. 11.7 BER performance for 16-QAM with STBC (3×4), Alamouti (2×2), and Alamouti (2×1)

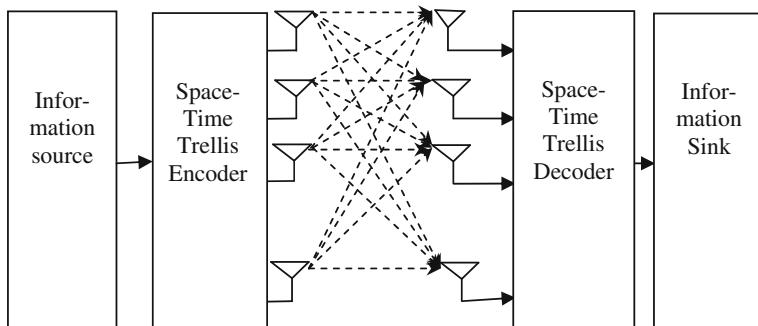


Fig. 11.8 Space-time trellis code system model

The STTC encoder can be considered as a convolutional encoder with the memory size of v_k delay units for the k th branch for each output symbol. Let $\{v_k\}_{k=1}^m$ denote the size of memory used to store the k th branch metrics that is calculated as

$$v_k = \left\lfloor \frac{v + k - 1}{\log_2 M} \right\rfloor \quad (11.48)$$

where $\lfloor x \rfloor$ denotes the largest integer smaller than x . v is the size of total required memory for the ST trellis code, that is,

$$v = \sum_{k=1}^m v_k \quad (11.49)$$

Then, the output of the STTC encoder is specified by the following generator polynomials:

$$\begin{aligned} a^1 &= \left[\left(a_{0,1}^1, a_{0,2}^1, \dots, a_{0,N_r}^1 \right), \left(a_{1,1}^1, a_{1,2}^1, \dots, a_{1,N_r}^1 \right), \dots, \left(a_{v_1,1}^1, a_{v_1,2}^1, \dots, a_{v_1,N_r}^1 \right) \right] \\ a^2 &= \left[\left(a_{0,1}^2, a_{0,2}^2, \dots, a_{0,N_r}^2 \right), \left(a_{1,1}^2, a_{1,2}^2, \dots, a_{1,N_r}^2 \right), \dots, \left(a_{v_2,1}^2, a_{v_2,2}^2, \dots, a_{v_2,N_r}^2 \right) \right] \\ a^m &= \left[\left(a_{0,1}^m, a_{0,2}^m, \dots, a_{0,N_r}^m \right), \left(a_{1,1}^m, a_{1,2}^m, \dots, a_{1,N_r}^m \right), \dots, \left(a_{v_m,1}^m, a_{v_m,2}^m, \dots, a_{v_m,N_r}^m \right) \right] \end{aligned} \quad (11.50)$$

where $a_{j,i}^k$ denotes M-PSK symbols, $k = 1, 2, \dots, m; j = 1, 2, \dots, v_k; i = 1, 2, \dots, N_T$. Let y_t^i denote the outputs of the STTC encoder for the i th transmit antenna at time t , $i = 1, 2, \dots, N_T$, which are given as

$$X_t^i = \sum_{k=1}^m \sum_{j=0}^{v_k} a_{j,i}^k I_{tj}^k \bmod M \quad (11.51)$$

Space-time trellis-encoded M-PSK symbols are now expressed as

$$X = [X_0 \ X_1 \ \dots \ X_t \ \dots] = \begin{bmatrix} x_0^1 & x_1^1 & \dots & x_t^1 & \dots \\ x_0^2 & x_1^2 & \dots & x_t^2 & \dots \\ \vdots & \vdots & \ddots & & \vdots \\ x_0^{N_T} & x_1^{N_T} & \dots & x_t^{N_T} & \dots \end{bmatrix} \quad (11.52)$$

where $X_t = [x_t^1 \ x_t^2 \ \dots \ x_t^{N_T}]^T$ is the output of the encoder that is composed of N_T M-PSK symbols, $t = 0, 1, 2, \dots$. Figure 11.9 shows an example of the STTC encoder for $N_T = 2$, $m = 3$, and $v = 3$.

Some of the coefficients for 4-PSK STTC and 8-PSK STTC codes [8] are summarized in Tables 11.1 and 11.2, respectively.

The Viterbi algorithm can be used for decoding the space-time trellis-coded systems. In the Viterbi algorithm, the branch metric is given by the following squared Euclidian distance:

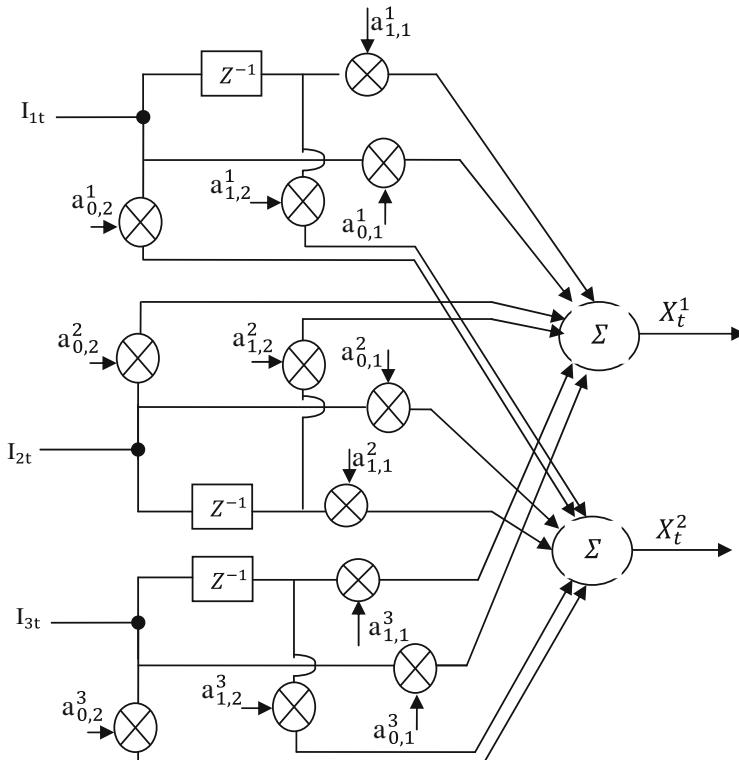


Fig. 11.9 8-state, 8-PSK encoder structure

Table 11.1 Coefficient pairs for 4PSK, 4-, 8-, and 16-state STTC

V	$(a_{0,1}^1, a_{0,2}^1)$	$(a_{1,1}^1, a_{1,2}^1)$	$(a_{2,1}^1, a_{2,2}^1)$	$(a_{0,1}^2, a_{0,2}^2)$	$(a_{1,1}^2, a_{1,2}^2)$	$(a_{2,1}^2, a_{2,2}^2)$	$\det(v)$	$\text{tr}(v)$
2	(0, 2)	(2, 0)	—	(0, 1)	(1, 0)	—	4	4
3	(0, 2)	(2, 0)	—	(0, 1)	(1, 0)	(2, 2)	12	8
4	(0, 2)	(2, 0)	(0, 2)	(0, 1)	(1, 2)	(2, 0)	12	8

Table 11.2 Coefficient pairs for 8PSK, 8-state STTC

V	$(a_{0,1}^1, a_{0,2}^1)$	$(a_{1,1}^1, a_{1,2}^1)$	$(a_{2,1}^1, a_{2,2}^1)$	$(a_{3,1}^1, a_{3,2}^1)$	$(a_{0,1}^2, a_{0,2}^2)$	$(a_{1,1}^2, a_{1,2}^2)$	$\det(v)$	$\text{tr}(v)$
3	(0, 4)	(4, 0)	(0, 2)	(2, 0)	(0, 1)	(5, 0)	2	4

$$\sum_{t=1}^T \sum_{j=1}^{N_R} \left| y_t^j - \sum_{i=1}^{N_T} h_{j,i} x_t^i \right|^2 \quad (11.53)$$

where y_t^j is the received signal at the j th receive antenna during t th symbol period and $h_{j,i}$ is the channel gain between the i th transmit antenna and j th receive antenna. Using the branch metric in Eq. (11.53), a path with the minimum accumulated Euclidian distance is selected for the detected sequence of transmitted symbols.

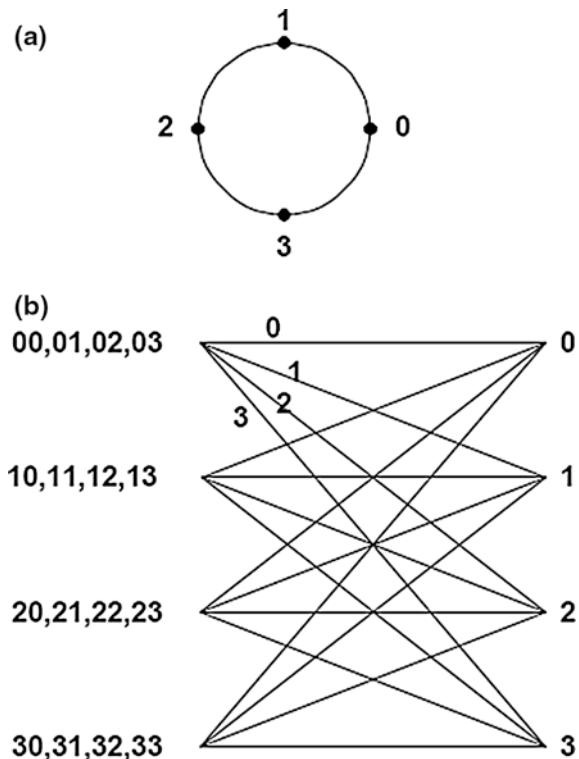
11.5.1.1 4-State QPSK Space-Time Trellis Encoder

STTCs can be represented and analyzed in their trellis form or by their generator matrix, G . For example, consider the 4-PSK signal constellation shown in Fig. 11.10a, where the signal points are labeled as 0, 1, 2, and 3.

The 4-State trellis structure is shown in Fig. 11.10b for a rate of 2 b/s/Hz.

The input signal can take on any value from the signal constellation (in this case 0, 1, 2, or 3); they are shown on the trellis diagram on the transition branches. In general, for each state, the first transition branch to state 0 results from input 0, the

Fig. 11.10 a 4PSK signal constellation, b 4-state, 4-PSK trellis diagram



second transition branch to state 1 results from input 1, and so on. The output depends on the input and on the current state. The states are labeled on the right. The labels on the left of the trellis represent the possible outputs from that state. The leftmost output is assumed to be the output for the first trellis branch for that particular state, and the second leftmost label is assumed to be the output for the second trellis branch for the same state, and so on. These assumptions were verified to be correct and can be manually traced through the encoder structure.

It was proved in [2] that the above code provides a diversity gain of 2 (assuming one receive antenna), and has a minimum determinant of 2 [4].

The encoder structure for the 4-state ($v = 2$) trellis, QPSK scheme with two transmit antennas is shown in Fig. 11.11.

At time t , two binary inputs I_t^1 and I_t^2 are fed into the branches of the encoder with I_t^1 being the MSB. The memory order of the upper and lower branches is V_1 and V_2 , respectively, where $V = V_1 + V_2$, and hence, the number of states is 2^V . V_i is calculated as

$$V_i = \left\lfloor \frac{V + i - 1}{2} \right\rfloor, \quad i = 1, 2 \quad (11.54)$$

where $\lfloor X \rfloor$ denotes the largest integer smaller than or equal to X . For each branch, the output is the sum of the current input scaled by a coefficient and the previous input scaled by another coefficient. Each of the different coefficients in the coefficient pairs, (0, 2), (2, 0), (0, 1), and (1, 0), applied to I_t^1 and I_t^2 , respectively.

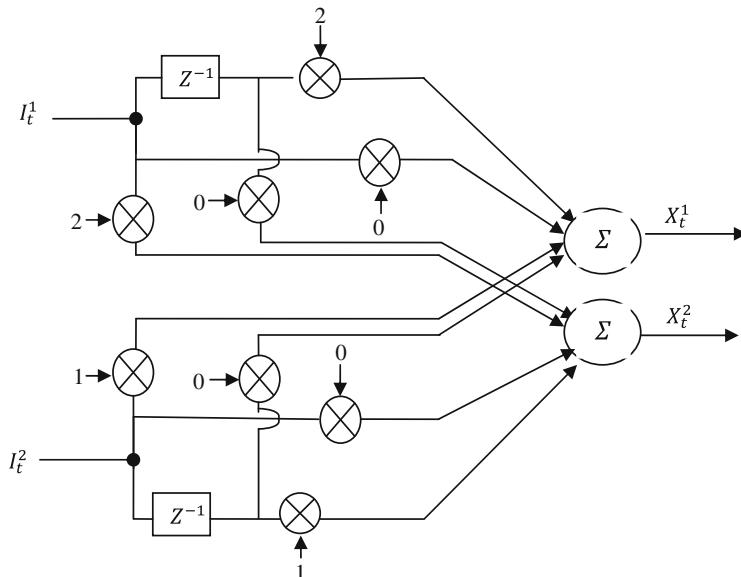


Fig. 11.11 4-state, 4-PSK encoder structure

By using Eq. (11.52), we can get the output values as follows

$$X_t^1 = (2I_{t-1}^1 + I_{t-1}^2) \bmod 4 \quad (11.55)$$

$$X_t^2 = (2I_t^1 + I_t^2) \bmod 4 \quad (11.56)$$

X_t^1 and X_t^2 are transmitted simultaneously on the first and second antennas, respectively. From Eqs. (11.55) and (11.56), it can be seen that $X_t^1 = X_{t-1}^1$; that is, the signal transmitted from the first antenna is a delayed version of the transmitted signal from the second transmit antenna. Note that the output X_t^2 at time t becomes the encoder state at time $(t+1)$ in this particular example.

Example 11.1 Consider the STTC encoder shown in Fig. 11.11 and determine the trellis-encoded symbol stream if the two input bit sequences are

$$\begin{bmatrix} I_t^1 \\ I_t^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Figure 11.11 shows a structure of the STTC encoder for this example. The encoder state at time t is $(I_{t-1}^1 I_{t-1}^2)$ or $2I_{t-1}^1 + I_{t-1}^2$. The output for the i th transmit antenna at time t is calculated as

$$X_t^1 = (2I_{t-1}^1 + I_{t-1}^2) \bmod 4$$

and

$$X_t^2 = (2I_t^1 + I_t^2) \bmod 4$$

$$\mathbf{Y} = \begin{bmatrix} X_t^1 \\ X_t^2 \end{bmatrix} = \begin{bmatrix} 0 & 2 & 0 & 3 & 1 \\ 2 & 0 & 3 & 1 & 0 \end{bmatrix}$$

Figure 11.12 shows the corresponding trellis diagram, in which the branch labels indicate two output symbols, X_t^1 and X_t^2 .

At time $t = 1$, we have $x_t^1 = 0$ and $x_t^2 = 2$. Therefore, 1 and -1 are transmitted from first and second antennas, respectively.

At time $t = 2$, we have $x_t^1 = 2$ and $x_t^2 = 0$. Therefore, -1 and 1 are transmitted from first and second antennas, respectively.

At time $t = 3$, we have $x_t^1 = 0$ and $x_t^2 = 3$. Therefore, 1 and $-j$ are transmitted from first and second antennas, respectively.

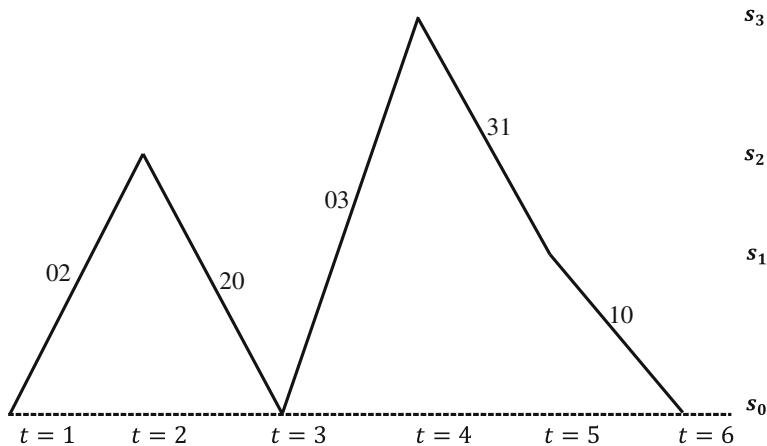


Fig. 11.12 4-state, 4-PSK encoder's output for Example 11.1

At time $t = 4$, we have $x_t^1 = 3$ and $x_t^2 = 1$. Therefore, $-j$ and j are transmitted from first and second antennas, respectively.

At time $t = 5$, we have $x_t^1 = 1$ and $x_t^2 = 0$. Therefore, j and 1 are transmitted from first and second antennas, respectively.

11.5.1.2 8-State 8-PSK Space-Time Trellis Encoder

The 8-state 8-PSK signal constellation and trellis diagram are shown in Figs. 11.13 and 11.14, for a rate of 3 b/s/Hz.

Fig. 11.13 8-PSK signal constellation

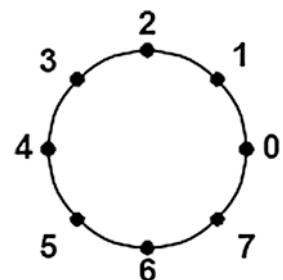
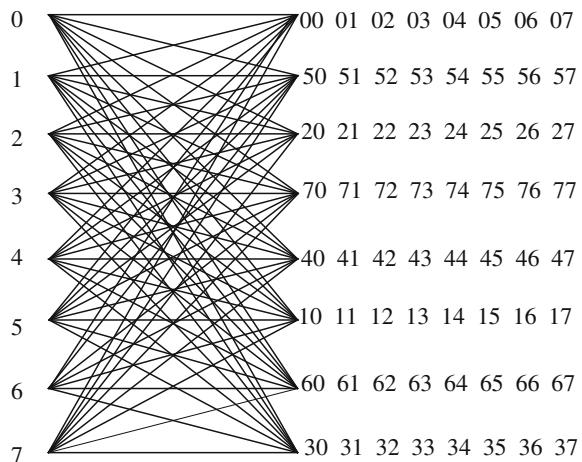


Fig. 11.14 8-state 8-PSK trellis diagram



11.5.2 Simulation of BER Performance of 4-State QPSK STTC Using MATLAB

The following MATLAB Program 11.7 and MATLAB function Programs 11.8 through 11.15 are used to simulate the BER performance of 4-state QPSK STTC.

Program 11.7 for space–time trellis code (STTC) for 4-state QPSK

```
clear all,clc,
Eb_N0_dB=0:2:20; iter= 1000;
g1=[0 2;2 0]; % 1-st generator
g2=[0 1;1 0]; % 2-nd generator
M = 4; % M-PSK = QPSK
BER1=qpsksttc(1,g1,g2,M,Eb_N0_dB,iter );
BER2=qpsksttc(2,g1,g2,M,Eb_N0_dB,iter);
BER4=qpsksttc(4,g1,g2,M,Eb_N0_dB,iter);
figure; % BER vs Eb/No in logarithmic value
semilogy(Eb_N0_dB,BER1,'-');hold on;
semilogy(Eb_N0_dB,BER2,'+');hold on;
semilogy(Eb_N0_dB,BER4,'-*');
grid on; xlabel('Eb/No(dB)'); ylabel('BER');
legend('Nrx =1', 'Nrx =2', 'Nrx =4');
```

Program 11.8 MATLAB function for qpsksttc

```
function BER=qpsksttc(Nrx,g1,g2,M,Eb_N0_dB,iter)
Ntx=2;
data=randint(1,48,2);
% ===== Encoder STTC =====
[s,moddata,v] = sttcenc(g1,g2,data,M);
modinp = moddata;
for i1=1:iter
    H=[randn(Nrx,Ntx) + j*randn(Nrx,Ntx)]; % MIMO channel
    txs=H*modinp;
    for k = 1:length(Eb_N0_dB)
        % ===== Noise Addition =====
        rxs=awgn(txs,Eb_N0_dB(k),'measured');
        % ===== STTC Detection =====
        symbol = symbolmap(g1,g2,M);
        sum1 = MaxLike(rxs,symbol,H,Nrx);
        [data_detect] = viterbi (sum1,v,M,g1,g2);
        % ===== BER computation =====
        error(1,k) = sum(data~=data_detect); % BER
    end
    total_error(i1,:)=error;
end
BER = sum(total_error)/(length(data)*iter);
```

Program 11.9 MATLAB function for sttcenc

```

function [s,moddata,v] = sttcenc(g1,g2,data,M)
[a b]= size(data);
v1 = length(g1)-1;
v2 = length(g2)-1;
v = v1+v2; % memory degree
m =log2 (M);
% serial to paralel
ncol = b/m;
for index=0:ncol -1
    c(:,index+1) = data(1,(m * index)+1:m*(index+1));
end
temp1 = zeros (m,v);
for k=0:ncol -1 % time
    % initialization
    for in=0:v-2
        temp1(:,v-in)=temp1(:,v-in-1);
    end
    temp1(:,1)=c(:,k+1);
    % symbol = g*c
    for l=1:m
        for j=0:v1
            temp2(l,j+1)= g1(l,j+1)*temp1(1,j+1);
        end
        for j=0:v2
            temp3(l,j+1)= g2(l,j+1)*temp1(2,j+1);
        end
        shat(l,k+1) = sum(sum(temp2)) + sum(sum(temp3));
        temp2=[];temp3=[];
    end
    temp1;
end
s = mod(shat,M);
[n m]=size(s);
moddata=[];
% Mapper QPSK from symbol STTC
for a=1:n
    for b=1:m
        if s(a,b)==[0]
            moddata(a,b) = 1+i;
        elseif s(a,b)==[1]
            moddata(a,b) = 1-i;
        elseif s(a,b)==[2]
            moddata(a,b) = -1-i;
        elseif s(a,b)==[3]
            moddata(a,b) = -1+i;
        end;
    end;
end;

```

Program 11.10 MATLAB function for symbolmap

```

function symbol = symbolmap(g1,g2,M)
[trellis1,trellis2,statego]=gen2trellis(g1,g2,M);
[c d] = size (trellis1);
for l=0:c-1
    for j=1:d
        map1(l*M+j,1) = trellis1 (l+1,j);
        map1(l*M+j,2) = trellis2 (l+1,j);
    end
end
[n m]=size(map1);
map1;
symbol = [];
for c=1:n
    for d=1:m
        if map1(c,d)== 0
            symbol(c,d) = 1+i;
        elseif map1(c,d)== 1
            symbol(c,d) = 1-i;
        elseif map1(c,d)== 2
            symbol(c,d) = -1-i;
        elseif map1(c,d)== 3
            symbol(c,d) = -1+i;
        end;
    end;
end;
```

Program 11.11 MATLAB function for MaxLike

```

function dist = MaxLike(symrec,symref,H,Nrx);
for c=1:length(symrec)
    for p=1:size(symref,1)
        for d=0:Nrx-1
            disthat(1,d+1)=norm((H(d+1,:)*symref(p,:).' - sym-
            rec(d+1,c)),'fro');
        end
        dist(p,c) = sum(disthat)/Nrx;
    end
end
```

Program 11.12 MATLAB function for viterbi

```

function [data] = viterbi (distance,v,M,g1,g2)
nstates = 2^v;
dist = [];
[brs kol]=size (distance);
[trellis1,trellis2,statego]=gen2trellis(g1,g2,M);
for a = 1:kol
    if a == 1
        dist(:,a) = distance(1:nstates,a);
    else
        disthat = [];
        for b=0:M-1
            for bb=1:nstates
                if bb < 5
                    disthat(bb,b+1) = dist(b*(v-1)+1,a-1)+ distance(b*nstates+bb,a);
                else
                    disthat(bb,b+1) = dist(b*(v-1)+2,a-1)+ distance(b*nstates+bb,a);
                end
            end
        end
        disthat;
        for b=1:nstates
            dist(b,a)=min (distrhat(b,:));
        end
    end
end
state= 0;
for a = 1:kol
    p = statego(state+1,1)+1;
    q = statego(state+1,4)+1;
    [mindist(:,a) ind(:,a)] = min (dist(p:q,a));
    if p ~= 1
        ind(:,a)=ind(:,a)+4;
    end
    state = ind(:,a)-1;
    end
    survpath = ind -1;
    demap = [0 0; 0 1; 1 0; 1 1]';
    for a = 1:kol
        if a == 1
            srx(1,a) = trellis1(1,ind(1,a));
            srx(2,a) = trellis2(1,ind(1,a));
            data(1,2*(a-1)+1:2*(a-1)+2)= demap(:,ind(1,a))';
        else
            dd = find (survpath(1,a) == statego(ind(1,a-1),:));
            srx(1,a) = trellis1(ind(1,a-1),dd);
            srx(2,a) = trellis2(ind(1,a-1),dd);
            data(1,2*(a-1)+1:2*(a-1)+2)= demap(:,dd)';
        end
    end
end

```

Program 11.13 MATLAB function for gen2trellis

```

function [trellis1,trellis2,statego]=gen2trellis(g1,g2,M)
% function to change generator code to trellis
% trellis1 = trellis antenna 1
% trellis2 = trellis antenna 2
% statego = state moving
v1 = length(g1)-1;
v2 = length(g2)-1;
v = v1+v2;
nstates = 2^v;
m =log2 (M);
state = 0:nstates-1;
for a=1:nstates
    for b=1:4
        input = [getbits(state (1,a),nstates/2),getbits(state(1,b),2)];
        % serial to parallel
        ncol = length (input)/2;
        for index=0:ncol-1
            c(:,index+1) = input(1,(m * index)+1:m*(index+1));
        end
        temp1 = zeros (m,v);
        for k=0:ncol-1 % time
            % initialization
            for in=0:v-2
                temp1(:,v-in)=temp1(:,v-in-1);
            end
            temp1(:,1)=c(:,k+1);
            % symbol = g*c
            for l=1:m
                for j=0:v1
                    temp2(l,j+1)= g1(l,j+1)*temp1(1,j+1);
                end
                for j=0:v2
                    temp3(l,j+1)= g2(l,j+1)*temp1(2,j+1);
                end
                shat(l,k+1) = sum(sum(temp2)) + sum(sum(temp3));
                temp2=[];temp3=[];
            end
            temp1;
        end
        s = mod(shat,M);
        trellis1(a,b) = s(1,ncol);
        trellis2(a,b) = s(2,ncol);
        statego(a,b) = bit2num(input(1,(length(input)-v2):length(input)));
    end
end

```

Program 11.14 MATLAB function for getbits

```
function [bits] = getbits(x, n)
bits = zeros(1, n);
ind = 1;
while (x~=0)
    bits(ind) = mod(x,2);
    x = floor(x/2);
    ind = ind + 1;
end
bits = fliplr(bits);
```

Program 11.15 MATLAB function for bit2num

```
function [y] = bit2num(x)
y = 0; mul = 1;
for i=(length(x):-1:1)
    y = y + mul*x(i);
    mul = mul*2;
end
```

The BER performance obtained by using above programs for 4-state QPSK STTC is shown in Fig. 11.15.

From Fig. 11.15, it is observed that the STTC with four receiving antennas outperforms the STTC with one and two receiving antennas.

11.6 MIMO-OFDM Implementation

A MIMO-OFDM system is shown in Fig. 11.16 where OFDM utilizes N_T transmit antennas, N_R receive antennas, and N_c subcarriers per antenna. MIMO-OFDM can be implemented as ST-coded OFDM (ST-OFDM), space-frequency-coded OFDM (SF-OFDM), and ST-frequency-coded OFDM (STF-OFDM). Let $x_n^\mu(i)$ be the data symbol transmitted on the i th subcarrier (frequency bin) from the μ th transmit antenna during the n th OFDM symbol interval. Then, the difference among these coded systems lies in how $x_n^\mu(i)$ are generated from the information symbols S_n [9].

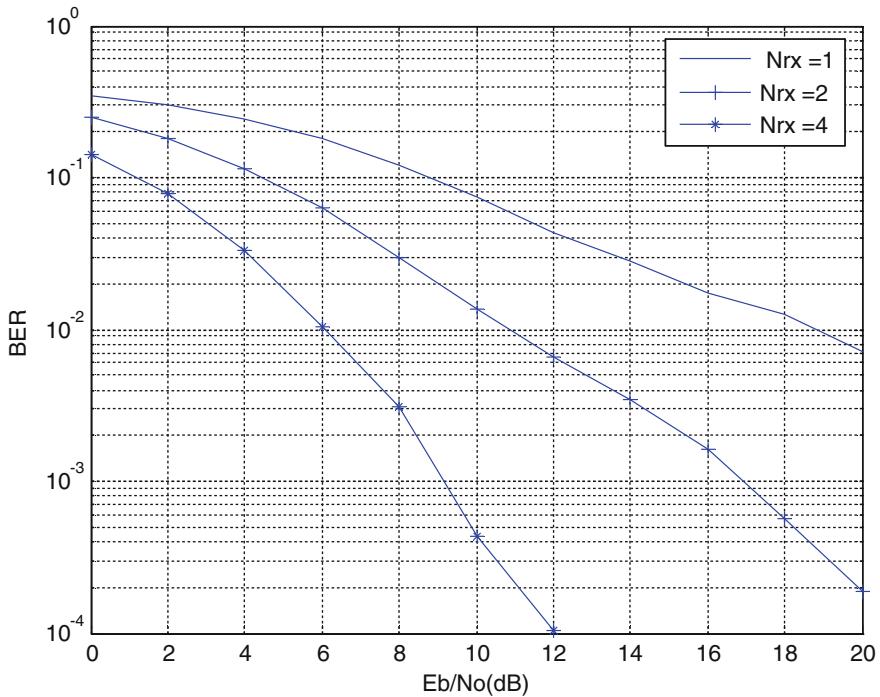


Fig. 11.15 BER performance of 4-state QPSK STTC

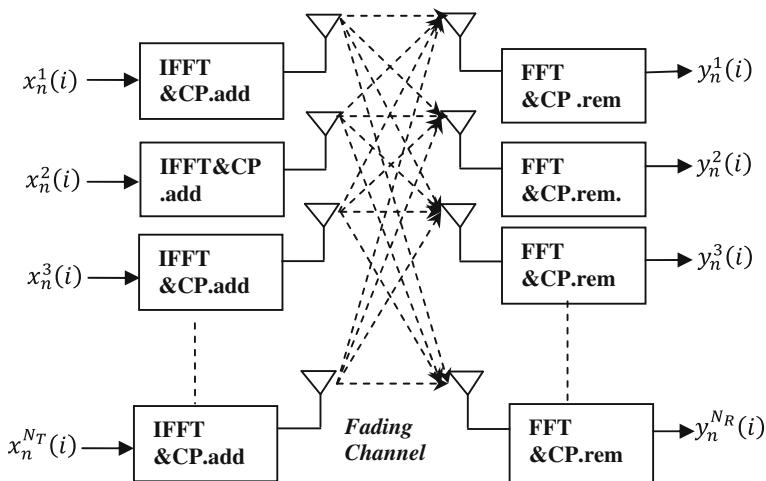
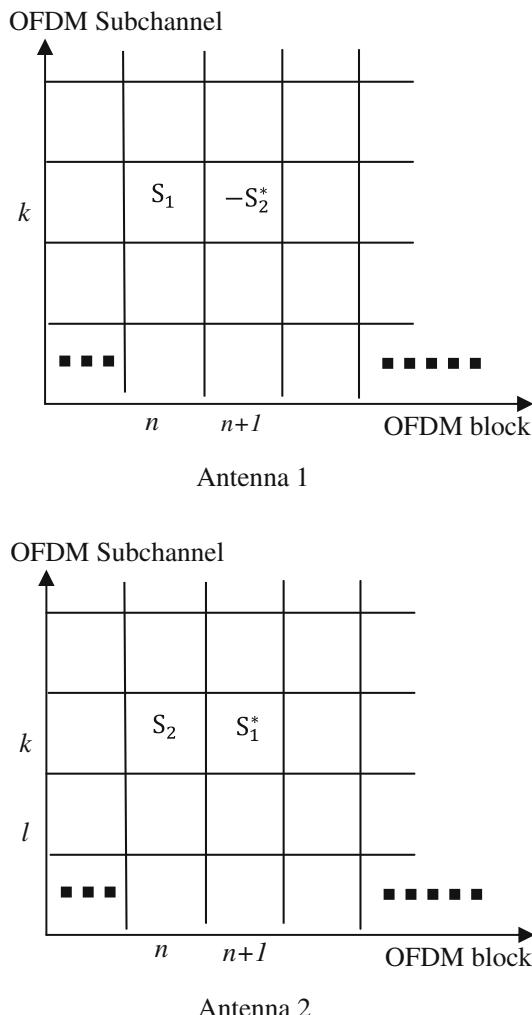


Fig. 11.16 A MIMO-OFDM system

11.6.1 Space-Time-Coded OFDM

The ST coding for a MIMO-OFDM with two transmit antennas is illustrated in Fig. 11.17. Two information symbols s_1 and $-s_2^*$ are sent through subchannel k of antenna 1 in OFDM blocks n and $n + 1$, respectively. Meanwhile, s_2 and s_1^* are sent through subchannel k of antenna 2 in OFDM blocks n and $n + 1$, respectively.

Fig. 11.17 ST coding



11.6.2 Space-Frequency-Coded OFDM

In space-time-coded OFDM, the frequency diversity and the correlation among different subcarriers are ignored. The strategy that consists of coding across antennas and different subcarriers of OFDM is called SF-coded OFDM [10]. The schematic diagram of SF-coded OFDM is shown in Fig. 11.18. The STBC encoder generates $N_c \times N_T$ symbols for each OFDM block (time slot). One data burst therefore consists of N_c vectors of size $N_T \times 1$ or equivalently one spatial OFDM symbol. The channel is assumed to be constant over at least one OFDM symbol. The interleaver transmits the (l, n) symbol on the l th subcarrier of the n th antenna [11].

The SF coding for two transmit antennas can be realized in a straightforward way by spreading directly the Alamouti code over two subchannels in one OFDM block. An example of SF coding for two transmit antennas is shown in Fig. 11.19. The two symbols S_1 and $-S_2^*$ are sent from subchannels k and l of the same OFDM block n at antenna 1, respectively, where k and l denote the indices of two separated subchannels. Meanwhile, S_2 and S_1^* are sent from subchannels k and l of the same OFDM block n at antenna 2, respectively [12].

11.6.3 Space-Time-Frequency-Coded OFDM

In STF coding, each $x_n^\mu(i)$ is a point in 3D as shown in Fig. 11.20; STF code word can be defined [9] as the collection of transmitted symbols within the

Fig. 11.18 Block diagram of SFBC-coded OFDM

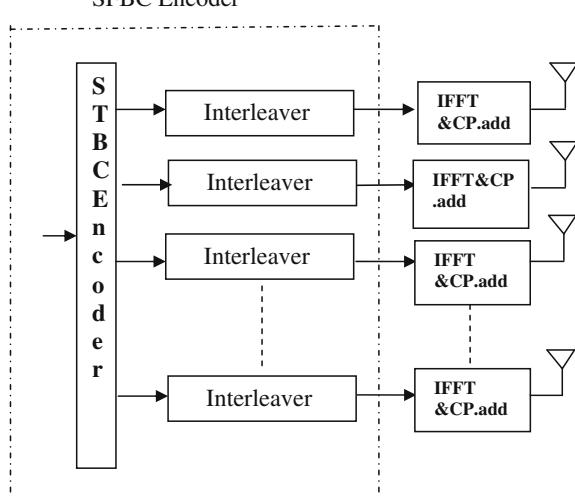
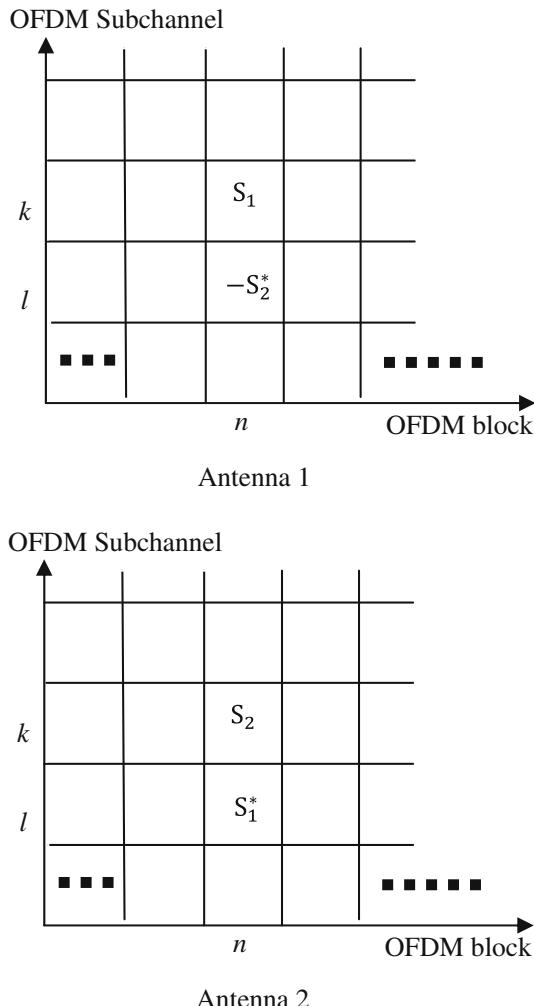


Fig. 11.19 SF coding

parallelepiped, spanned by N_T transmit antennas, N_x OFDM symbol intervals, and N_c subcarriers. Thus, one STF code word contains $N_T N_x N_c$ transmitted symbols

$$\{x_n^\mu(i), \mu = 1, \dots, N_T, n = 0, \dots, N_{x-1}, i = 0, \dots, N_{c-1}\}$$

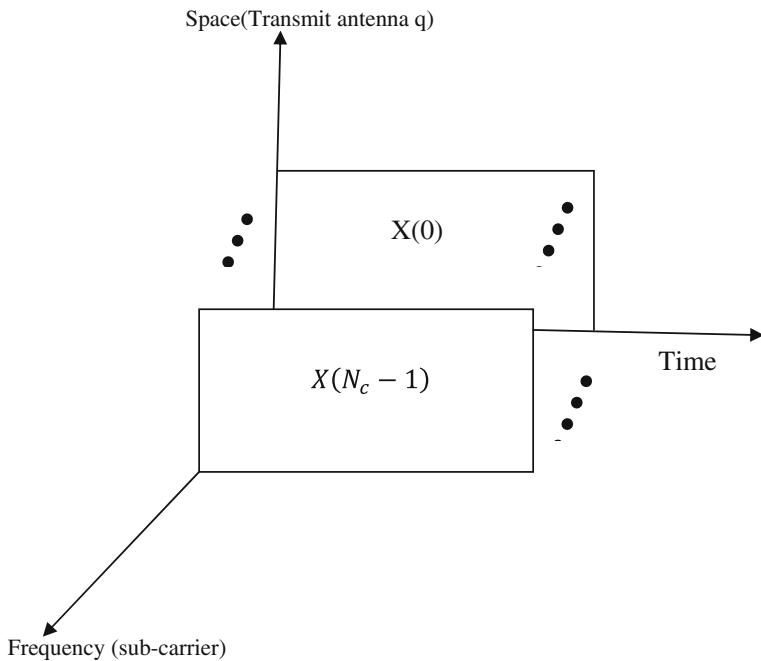


Fig. 11.20 STF-coded OFDM

11.7 Problems

1. Consider Alamouti STBC with 2 transmit antennas. If the input bit stream is 11011110001001, determine the transmitted symbols from each antenna for each symbol interval with (i) QPSK modulation and (ii) 16-QAM modulation.
2. A code matrix for STBC is given by

$$\begin{bmatrix} S_1 & S_2 & S_3 & S_4 \\ -S_2^* & S_1^* & -S_4^* & S_3^* \\ -S_3^* & -S_4^* & S_1^* & S_2^* \\ S_4 & -S_3 & -S_2 & S_1 \end{bmatrix}$$
 - (i) Check for Orthogonality of the code
 - (ii) Find the diversity order achieved by this code.
3. Consider a MIMO system with AWGN employing Alamouti STBC with two transmit and one receiving antennas. Determine the outage probabilities for the system
 - (i) When the channel is known at the receiver
 - (ii) When the channel is known at the transmitter

4. Consider a 4-state QPSK STTC system. Determine the trellis-encoded symbol stream if the two input bit sequences are

$$\begin{bmatrix} I_t^1 \\ I_t^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & \dots \\ 0 & 1 & 1 & 0 & 1 & \dots \end{bmatrix}$$

5. Consider a 4-state QPSK STTC system. Determine the trellis-encoded symbol stream if the two input bit sequences are

$$\begin{bmatrix} I_t^1 \\ I_t^2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & \dots \\ 0 & 0 & 1 & 1 & 0 & \dots \end{bmatrix}$$

6. Consider a STTC 4-PSK system where the transmitted code word is $C = 220313$, and a possible erroneous code word is $c = 330122$. Determine the diversity gain of the system.
7. Consider the same data from the Problem 11.5, determine the coding gain

11.8 MATLAB Exercises

1. Write a MATLAB program to simulate the BER performance of 2-transmit 1-receive antenna Alamouti scheme using MMSE detection.
2. Write a MATLAB program to simulate the BER performance of 2-transmit 2-receive antenna Alamouti scheme using MMSE detection.
3. Write a MATLAB program to simulate the BER performance of MRC diversity technique with 4 receiving antennas and compare with the result of problem 2.
4. Write a MATLAB program to simulate the performance of 8-state QPSK STTC.
5. Write a MATLAB program to simulate the BER performance of STBC OFDM.

References

1. Liang, X.-B.: Orthogonal designs with maximum rates. *IEEE Trans. Inf. Theor.* **49**(10), 2468–2503 (2003)
2. Tarokh, V., Seshadri, N., Calderbank, A.R.: Space-time codes for high data rate wireless communications: performance criterion and code construction. *IEEE Trans. Inf. Theor.* **44**(2), 744–765 (1998)
3. Tarokh, V., Naguib, A., Seshadri, N., Calderbank, A.R.: Space-time codes for high data rate wireless communication: performance criteria in the presence of channel estimation errors, mobility, and multiple paths. *IEEE Trans. Commun.* **47**(2), 199–207 (1999)
4. Tarokh, V., Seshadri, N., Calderbank, A.R.: Space-time codes for wireless communication: code construction. In: *IEEE 47th Vehicular Technology Conference*, vol. 2, pp. 637–641. Phoenix, Arizona, 4–7 May 1997

5. Tarokh, V., Jafarkhani, H., Calderbank, A.: Space-time block coding for wireless communications: performance results. *IEEE J. Sel. Areas Commun.* **17**(3), 451–460 (1999)
6. Alamouti, S.M.: A simple transmit diversity technique for wireless communications. *IEEE J. Sel. Areas Commun.* **16**(8), 1451–1458 (1998)
7. Tarokh, V., Jafarkhani, H., Calderbank, A.: Space-time block codes from orthogonal designs. *IEEE Trans. Inf. Theor.* **45**(5), 1456–1467 (1999)
8. Chent, Z., Yuant, J., Vucetict, B.: An improved space-time trellis coded modulation scheme on slow Rayleigh fading channels. In: *IEEE ICC*, pp. 1110–1116 (2001)
9. Liu, Z., Xin, Y., Giannakis, G.B.: Space-time-frequency coded OFDM over frequency-selective fading channels. *IEEE Trans. Signal Process.* **50**(10), 2465–2476 (2002)
10. Lee, K.F., Williams, D.B.: A space-frequency transmitter diversity technique for OFDM systems. In: *IEEE Global Communications Conference*, vol. 3, pp. 1473–1477, Nov. 27–Dec. 1, 2000
11. Jafarkhani, H.: *Space-Time Coding Theory and Practice*. Cambridge University Press, Cambridge (2005)
12. Zhang, W., Xia, X.-G., Ben Letaief, K.: Space-time/frequency coding for MIMO-OFDM in the next generation broadband wireless systems. In: *IEEE Wireless Communications*, pp. 32–43, June 2007