Coding Theory
Coding Theory

Algorithms, Architectures, and Applications

André Neubauer
Münster University of Applied Sciences, Germany

Jürgen Freudenberger
HTWG Konstanz, University of Applied Sciences, Germany

Volker Kühn
University of Rostock, Germany
Contents

Preface ix

1 Introduction 1
1.1 Communication Systems .............................................. 1
1.2 Information Theory .................................................. 3
   1.2.1 Entropy .............................................. 3
   1.2.2 Channel Capacity ......................................... 4
   1.2.3 Binary Symmetric Channel ................................. 5
   1.2.4 AWGN Channel ........................................... 6
1.3 A Simple Channel Code ............................................. 8

2 Algebraic Coding Theory 13
2.1 Fundamentals of Block Codes ...................................... 14
   2.1.1 Code Parameters ......................................... 16
   2.1.2 Maximum Likelihood Decoding .............................. 19
   2.1.3 Binary Symmetric Channel ................................. 23
   2.1.4 Error Detection and Error Correction ..................... 25
2.2 Linear Block Codes ................................................. 27
   2.2.1 Definition of Linear Block Codes ......................... 27
   2.2.2 Generator Matrix ......................................... 27
   2.2.3 Parity-Check Matrix ..................................... 30
   2.2.4 Syndrome and Cosets ..................................... 31
   2.2.5 Dual Code ............................................ 36
   2.2.6 Bounds for Linear Block Codes ......................... 37
   2.2.7 Code Constructions ...................................... 41
   2.2.8 Examples of Linear Block Codes ......................... 46
2.3 Cyclic Codes ....................................................... 62
   2.3.1 Definition of Cyclic Codes ................................ 62
   2.3.2 Generator Polynomial .................................... 63
   2.3.3 Parity-Check Polynomial ................................ 67
   2.3.4 Dual Codes ............................................. 70
   2.3.5 Linear Feedback Shift Registers ......................... 71
   2.3.6 BCH Codes ............................................. 74
   2.3.7 Reed–Solomon Codes ..................................... 81
## CONTENTS

4.2.2 Iterative Decoding of Product Codes .............................................. 180
4.3 Concatenated Convolutional Codes .................................................. 182
  4.3.1 Parallel Concatenation ............................................................... 182
  4.3.2 The UMTS Turbo Code ............................................................... 183
  4.3.3 Serial Concatenation ............................................................... 184
  4.3.4 Partial Concatenation ............................................................... 185
  4.3.5 Turbo Decoding ...................................................................... 186
4.4 EXIT Charts ...................................................................................... 188
  4.4.1 Calculating an EXIT Chart ......................................................... 189
  4.4.2 Interpretation ............................................................................ 191
4.5 Weight Distribution ........................................................................... 196
  4.5.1 Partial Weights ........................................................................ 196
  4.5.2 Expected Weight Distribution ....................................................... 197
4.6 Woven Convolutional Codes ............................................................... 198
  4.6.1 Encoding Schemes ..................................................................... 200
  4.6.2 Distance Properties of Woven Codes ........................................... 202
  4.6.3 Woven Turbo Codes ................................................................. 205
  4.6.4 Interleaver Design .................................................................... 208
4.7 Summary ............................................................................................ 212

5 Space–Time Codes .................................................................................. 215
  5.1 Introduction ...................................................................................... 215
    5.1.1 Digital Modulation Schemes ....................................................... 216
    5.1.2 Diversity .................................................................................... 223
  5.2 Spatial Channels ................................................................................ 229
    5.2.1 Basic Description ...................................................................... 229
    5.2.2 Spatial Channel Models ............................................................. 234
    5.2.3 Channel Estimation ................................................................. 239
  5.3 Performance Measures ...................................................................... 241
    5.3.1 Channel Capacity ..................................................................... 241
    5.3.2 Outage Probability and Outage Capacity ................................... 250
    5.3.3 Ergodic Error Probability ............................................................ 252
  5.4 Orthogonal Space–Time Block Codes ................................................. 257
    5.4.1 Alamouti’s Scheme .................................................................. 257
    5.4.2 Extension to More than Two Transmit Antennas ....................... 260
    5.4.3 Simulation Results ................................................................... 263
  5.5 Spatial Multiplexing ........................................................................... 265
    5.5.1 General Concept ....................................................................... 265
    5.5.2 Iterative APP Preprocessing and Per-layer Decoding ............... 267
    5.5.3 Linear Multilayer Detection ....................................................... 272
    5.5.4 Original BLAST Detection ......................................................... 275
    5.5.5 QL Decomposition and Interference Cancellation .................... 278
    5.5.6 Performance of Multi-Layer Detection Schemes ...................... 287
    5.5.7 Unified Description by Linear Dispersion Codes ..................... 291
  5.6 Summary ............................................................................................ 294
## CONTENTS

### A Algebraic Structures
- A.1 Groups, Rings and Finite Fields ........................................ 295
  - A.1.1 Groups .............................................................. 295
  - A.1.2 Rings .............................................................. 296
  - A.1.3 Finite Fields ....................................................... 298
- A.2 Vector Spaces ............................................................ 299
- A.3 Polynomials and Extension Fields ....................................... 300
- A.4 Discrete Fourier Transform ............................................. 305

### B Linear Algebra .............................................................. 311

### C Acronyms ................................................................. 319

Bibliography ................................................................. 325

Index ....................................................................... 335
Preface

Modern information and communication systems are based on the reliable and efficient transmission of information. Channels encountered in practical applications are usually disturbed regardless of whether they correspond to information transmission over noisy and time-variant mobile radio channels or to information transmission on optical discs that might be damaged by scratches. Owing to these disturbances, appropriate channel coding schemes have to be employed such that errors within the transmitted information can be detected or even corrected. To this end, channel coding theory provides suitable coding schemes for error detection and error correction. Besides good code characteristics with respect to the number of errors that can be detected or corrected, the complexity of the architectures used for implementing the encoding and decoding algorithms is important for practical applications.

The present book provides a concise overview of channel coding theory and practice as well as the accompanying algorithms, architectures and applications. The selection of the topics presented in this book is oriented towards those subjects that are relevant for information and communication systems in use today or in the near future. The focus is on those aspects of coding theory that are important for the understanding of these systems. This book places emphasis on the algorithms for encoding and decoding and their architectures, as well as the applications of the corresponding coding schemes in a unified framework.

The idea for this book originated from a two-day seminar on coding theory in the industrial context. We have tried to keep this seminar style in the book by highlighting the most important facts within the figures and by restricting the scope to the most important topics with respect to the applications of coding theory, especially within communication systems. This also means that many important and interesting topics could not be covered in order to be as concise as possible.

The target audience for the book are students of communication and information engineering as well as computer science at universities and also applied mathematicians who are interested in a presentation that subsumes theory and practice of coding theory without sacrificing exactness or relevance with regard to real-world practical applications. Therefore, this book is well suited for engineers in industry who want to know about the theoretical basics of coding theory and their application in currently relevant communication systems.

The book is organised as follows. In Chapter 1 a brief overview of the principle architecture of a communication system is given and the information theory fundamentals underlying coding theory are summarised. The most important concepts of information theory, such as entropy and channel capacity as well as simple channel models, are described.
Chapter 2 presents the classical, i.e. algebraic, coding theory. The fundamentals of the encoding and decoding of block codes are explained, and the maximum likelihood decoding rule is derived as the optimum decoding strategy for minimising the word error probability after decoding a received word. Linear block codes and their definition based on generator and parity-check matrices are discussed. General performance measures and bounds relating important code characteristics such as the minimum Hamming distance and the code rate are presented, illustrating the compromises necessary between error detection and error correction capabilities and transmission efficiency. It is explained how new codes can be constructed from already known codes. Repetition codes, parity-check-codes, Hamming codes, simplex codes and Reed–Muller codes are presented as examples. Since the task of decoding linear block codes is difficult in general, the algebraic properties of cyclic codes are exploited for efficient decoding algorithms. These cyclic codes, together with their generator and parity-check polynomials, are discussed, as well as efficient encoding and decoding architectures based on linear feedback shift registers. Important cyclic codes such as BCH codes and Reed–Solomon codes are presented, and an efficient algebraic decoding algorithm for the decoding of these cyclic codes is derived.

Chapter 3 deals with the fundamentals of convolutional coding. Convolutional codes can be found in many applications, for instance in dial-up modems, satellite communications and digital cellular systems. The major reason for this popularity is the existence of efficient decoding algorithms that can utilise soft input values from the demodulator. This so-called soft-input decoding leads to significant performance gains. Two famous examples for a soft-input decoding algorithm are the Viterbi algorithm and the Bahl, Cocke, Jelinek, Raviv (BCJR) algorithm which also provides a reliability output. Both algorithms are based on the trellis representation of the convolutional code. This highly repetitive structure makes trellis-based decoding very suitable for hardware implementations.

We start our discussion with the encoding of convolutional codes and some of their basic properties. It follows a presentation of the Viterbi algorithm and an analysis of the error correction performance with this maximum likelihood decoding procedure. The concept of soft-output decoding and the BCJR algorithm are considered in Section 3.5. Soft-output decoding is a prerequisite for the iterative decoding of concatenated convolutional codes as introduced in Chapter 4. Finally, we consider an application of convolutional codes for mobile communication channels as defined in the Global System for Mobile communications (GSM) standard. In particular, the considered hybrid ARQ protocols are excellent examples of the adaptive coding systems that are required for strongly time-variant mobile channels.

As mentioned above, Chapter 4 is dedicated to the construction of long powerful codes based on the concatenation of simple convolutional component codes. These concatenated convolutional codes, for example the famous turbo codes, are capable of achieving low bit error rates at signal-to-noise ratios close to the theoretical Shannon limit. The term turbo reflects a property of the employed iterative decoding algorithm, where the decoder output of one iteration is used as the decoder input of the next iteration. This concept of iterative decoding was first introduced for the class of low-density parity-check codes. Therefore, we first introduce low-density parity-check codes in Section 4.1 and discuss the relation between these codes and concatenated code constructions. Then, we introduce some popular encoding schemes for concatenated convolutional codes and present three methods to analyse the performance of the corresponding codes. The EXIT chart method
in Section 4.4 makes it possible to predict the behaviour of the iterative decoder by looking at the input/output relations of the individual constituent soft-output decoders. Next, we present a common approach in coding theory. We estimate the code performance with maximum likelihood decoding for an ensemble of concatenated codes. This method explains why many concatenated code constructions lead to a low minimum Hamming distance and therefore to a relatively poor performance for high signal-to-noise ratios. In Section 4.6 we consider code designs that lead to a higher minimum Hamming distance owing to a special encoder construction, called the woven encoder, or the application of designed interleavers.

The fifth chapter addresses space–time coding concepts, a still rather new topic in the area of radio communications. Although these techniques do not represent error-correcting codes in the classical sense, they can also be used to improve the reliability of a data link. Since space–time coding became popular only a decade ago, only a few concepts have found their way into current standards hitherto. However, many other approaches are currently being discussed. As already mentioned before, we restrict this book to the most important and promising concepts.

While classical encoders and decoders are separated from the physical channel by modulators, equalisers, etc., and experience rather simple hyperchannels, this is not true for space–time coding schemes. They directly work on the physical channel. Therefore, Chapter 5 starts with a short survey of linear modulation schemes and explains the principle of diversity. Next, spatial channel models are described and different performance measures for their quantitative evaluation are discussed. Sections 5.4 and 5.5 introduce two space–time coding concepts with the highest practical relevance, namely orthogonal space–time block codes increasing the diversity degree and spatial multiplexing techniques boosting the achievable data rate. For the latter approach, sophisticated signal processing algorithms are required at the receiver in order to separate superimposed data streams again.

In the appendices a brief summary of algebraic structures such as finite fields and polynomial rings is given, which are needed for the treatment especially of classical algebraic codes, and the basics of linear algebra are briefly reviewed.

Finally, we would like to thank the Wiley team, especially Sarah Hinton as the responsible editor, for their support during the completion of the manuscript. We also thank Dr. rer. nat. Jens Schlembach who was involved from the beginning of this book project and who gave encouragement when needed. Last but not least, we would like to give special thanks to our families – Fabian, Heike, Jana and Erik, Claudia, Hannah and Jakob and Christiane – for their emotional support during the writing of the manuscript.

**André Neubauer**
Münster University of Applied Sciences

**Jürgen Freudenberg**
HTWG Konstanz University of Applied Sciences

**Volker Kühn**
University of Rostock
1 Introduction

The reliable transmission of information over noisy channels is one of the basic requirements of digital information and communication systems. Here, transmission is understood both as transmission in space, e.g. over mobile radio channels, and as transmission in time by storing information in appropriate storage media. Because of this requirement, modern communication systems rely heavily on powerful channel coding methodologies. For practical applications these coding schemes do not only need to have good coding characteristics with respect to the capability of detecting or correcting errors introduced on the channel. They also have to be efficiently implementable, e.g. in digital hardware within integrated circuits. Practical applications of channel codes include space and satellite communications, data transmission, digital audio and video broadcasting and mobile communications, as well as storage systems such as computer memories or the compact disc (Costello et al., 1998).

In this introductory chapter we will give a brief introduction into the field of channel coding. To this end, we will describe the information theory fundamentals of channel coding. Simple channel models will be presented that will be used throughout the text. Furthermore, we will present the binary triple repetition code as an illustrative example of a simple channel code.

1.1 Communication Systems

In Figure 1.1 the basic structure of a digital communication system is shown which represents the architecture of the communication systems in use today. Within the transmitter of such a communication system the following tasks are carried out:

- source encoding,
- channel encoding,
- modulation.