

Contents

Preface

vii

Introduction

1

0 Preliminaries

5

- 0.1 Miscellany 5
- 0.2 Some Probability 11
- 0.3 Matrices 21

1 An Introduction to Codes

25

- 1.1 Strings and Things 25
- 1.2 What Are Codes? 33
- 1.3 Uniquely Decipherable Codes 37
- 1.4 Instantaneous Codes and Kraft's Theorem 42

I Information Theory

51

2 Efficient Encoding

53

- 2.1 Information Sources; Average Codeword Length 53
- 2.2 Huffman Encoding 57

2.3	The Proof that Huffman Encoding Is the Most Efficient	63
3	Noiseless Coding	69
3.1	Entropy	69
3.2	Properties of Entropy	75
3.3	Extensions of an Information Source	79
3.4	The Noiseless Coding Theorem	82
II	Coding Theory	89
4	The Main Coding Theory Problem	91
4.1	Communications Channels	91
4.2	Decision Rules	97
4.3	Nearest Neighbor Decoding	103
4.4	The Minimum Distance of a Code	106
4.5	Perfect Codes and the Sphere-Packing Condition	116
4.6	Making New Codes from Old Codes	124
4.7	The Main Coding Theory Problem	131
4.8	Sphere-Covering and Sphere-Packing Bounds	138
4.9	The Singleton and Plotkin bounds	142
4.10	Information Theory Revisited— the Noisy Coding Theorem	146
5	Linear Codes	149
5.1	The Vector Space $\mathbb{Z}_p^n$	149
5.2	Linear Codes	163
5.3	Correcting Errors in a Linear Code	169
5.4	The Dual of a Linear Code	182
5.5	Syndrome Decoding	195
5.6	Equivalent Linear Codes	199
5.7	Source Encoding with a Linear Code	208
6	Some Special Codes	217
6.1	The Hamming and Golay Codes	217
6.2	Reed-Muller Codes	234
6.3	Some Decimal Codes	245
6.4	Codes from Latin Squares	258

7 An Introduction to Cyclic Codes	269
7.1 Cyclic Codes	269
Answers to Selected Odd-Numbered Exercises	285
References	317
Index	319

In this book, we discuss two distinct aspects of the problem of transmitting data (called *source data*) from one location to another or, what amounts to the same thing, storing data and then retrieving the data at a later time. Both of these aspects involve encoding of the source data.

In Part I of the book, on information theory, we discuss the issue of encoding for *efficiency*, that is, encoding so that the source data takes up as little space as possible. (This is also known as *data compression*.) Our focus will be on the theoretical aspects of the problem, rather than on the practical aspects. As we will see, encoding for efficiency is best accomplished using variable-length encoding schemes, where the most frequently used source symbols are encoded with the shortest codewords. Also, we will assume for this discussion that errors do not occur in the handling of source symbols. Hence, this type of encoding is noiseless.

There are various ways in which we might model source data. The model we will adopt is that of a "black box" that emits source symbols from a given finite source alphabet at regular intervals. Each source symbol has a fixed probability of being emitted at any time. We must encode the source data, either a single symbol at a time or in predefined blocks of symbols, as it is being emitted from the black box—the point is that we are not privy to the entire message before encoding.