INFORMATION THEORY
AND CODING BY EXAMPLE

MARK KELBERT
Swansea University, and Universidade de São Paulo

YURI SUHOV
University of Cambridge, and Universidade de São Paulo

CAMBRIDGE UNIVERSITY PRESS
Contents

Preface  page vii

1 Essentials of Information Theory  1
  1.1 Basic concepts. The Kraft inequality. Huffman’s encoding  1
  1.2 Entropy: an introduction  18
  1.3 Shannon’s first coding theorem. The entropy rate of a Markov source  41
  1.4 Channels of information transmission. Decoding rules. Shannon’s second coding theorem  59
  1.5 Differential entropy and its properties  86
  1.6 Additional problems for Chapter 1  95

2 Introduction to Coding Theory  144
  2.1 Hamming spaces. Geometry of codes. Basic bounds on the code size  144
  2.2 A geometric proof of Shannon’s second coding theorem. Advanced bounds on the code size  162
  2.3 Linear codes: basic constructions  184
  2.4 The Hamming, Golay and Reed–Muller codes  199
  2.5 Cyclic codes and polynomial algebra. Introduction to BCH codes  213
  2.6 Additional problems for Chapter 2  243

3 Further Topics from Coding Theory  269
  3.1 A primer on finite fields  269
  3.2 Reed–Solomon codes. The BCH codes revisited  291
  3.3 Cyclic codes revisited. Decoding the BHC codes  300
  3.4 The MacWilliams identity and the linear programming bound  313
  3.5 Asymptotically good codes  328
  3.6 Additional problems for Chapter 3  340
### 4 Further Topics from Information Theory

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 Gaussian channels and beyond</td>
<td>366</td>
</tr>
<tr>
<td>4.2 The asymptotic equipartition property in the continuous time setting</td>
<td>397</td>
</tr>
<tr>
<td>4.3 The Nyquist–Shannon formula</td>
<td>409</td>
</tr>
<tr>
<td>4.4 Spatial point processes and network information theory</td>
<td>436</td>
</tr>
<tr>
<td>4.5 Selected examples and problems from cryptography</td>
<td>453</td>
</tr>
<tr>
<td>4.6 Additional problems for Chapter 4</td>
<td>480</td>
</tr>
</tbody>
</table>

* Bibliography                                                              | 501  |
* Index                                                                   | 509  |