

Index

Italic entries are to names.

- $\forall$, 7
- $\lceil \xi \rceil$, 99
- $\lfloor \xi \rfloor$, 16, 49
- $\stackrel{?}{=}$, 34
- $\mathbf{x}^\top$, 39
- a posteriori probability, 126
- a priori probability, 126
- additive white Gaussian noise channel, *see*
 - AWGN channel
- Alajaji, Fady*, 141
- arithmetic coding, 109
- arithmetics in the binary field, *see* modular arithmetic
- ASCII code, 19
- average codeword length, 57, 65, 96
- AWGN channel, 11, 145, 154
- Bayes' Theorem, 119
- BEC, 135
- BER, *see* bit error rate
- Berrou, Claude*, 153, 155
- Bertsekas, Dimitri P.*, 119, 123
- binary digit, 87
- binary tree, *see* tree
- bit, 5, 87
- bit error rate, 148, 150, 152
- Blahut, Richard E.*, 159
- block design, 182
- block error rate, 148
- bound
 - on average codeword length, 96, 101
 - on BER, 153
 - on entropy, 90
 - Gilbert–Varshamov, 53
 - Hamming, 51
 - Plotkin, 53
 - sphere, 51, 53
 - TVZ, 53
- Bryant, Victor*, 182
- BSC, 120
- byte, 9, 19, 41, 87
- CD, 3, 31, 41
- CDMA, 181
- channel, 2, 117
 - AWGN, 11, 145, 154
 - binary, 119
 - binary erasure, 135
 - binary symmetric, 119, 131
 - channel transition matrix, 117
 - Gaussian, 145
 - quasi-symmetric, 141
 - stationary, 118
 - uniformly dispersive, 134
- channel capacity, 131, 139, 143
 - of binary erasure channel, 136
 - of binary symmetric channel, 132
 - of Gaussian channel, 146
- KKT conditions, 136
- power constraint, 146
- of uniformly dispersive channel, 135
- channel coding, 2, 31, 138, 143, *see also* under code
- Channel Coding Theorem, 139
- Chen, Po-Ning*, 141
- code, 5, 55, 139
 - ASCII, 19
 - average codeword length, 57, 65, 96
 - block, 78, 110
 - concatenated, 153

Cambridge University Press

978-1-107-01583-8 - A Student's Guide to Coding and Information Theory

Stefan M. Moser and Po-ning Chen

Index

[More information](#)

188

constant-weight, 182
 cyclic, 30
 dual, 39, 40
 Elias–Willems, 110
 error-correcting, 37
 single-error-correcting, 36, 46
 t -error-correcting, 37
 error-detecting, 13, 37
 double-error-detecting, 29, 46
 e -error-detecting, 37
 Fano, 97, 108, 160
 generator matrix, 38
 Hamming, 42
 general, 52
 strategy, 177
 Venn diagram, 43
 hexadecimal, 10
 Huffman, 70, 160
 instantaneous, 57
 ISBN, 26
 LDPC, 153
 Lempel–Ziv, 110
 linear, 39
 octal, 9
 parity-check matrix, 38
 perfect, 51
 prefix-free, 57, 74
 rate, 37, 139, 144
 Reed–Solomon, 41
 repetition, 34
 Shannon, 108
 Shannon–Fano, *see* code, Fano
 single parity-check, 17, 40
 singular, 73
 Tunstall, 78, 108, 110
 turbo, 11, 155
 decoder, 158
 encoder, 155
 interleaver, 156
 uniquely decodable, 56, 73
 universal product, 26
 variable-length, 55
 weighted, 22
 codebook, 139
 codeword, 7, 17, 39, 55, 139
 coding scheme, 138
 Coding Theorem
 achievability part, 97
 Channel Coding Theorem, 139
 converse part, 95
 for a Discrete Memoryless Source, 107

Index

Information Transmission Theorem, 143
 Joint Source–Channel Coding Theorem, 143
 for a Single Random Message, 101
 coding theory, 1
 compression, *see* data compression
 compressor, 147
 concatenation of codewords, 75, 104
 concavity, 164
Conway, John, 53
Cooley, James, 41
Costello, Jr., Daniel J., 30, 52, 160
Cover, Thomas M., 109, 110, 138, 141, 147, 159
 covering, 179
 cryptography, 180

 data compression, 55, 160
 universal, 108
Davey, Matthew C., 154
Davies, Ian L., 141
 decoder, 2, 116, 145, 147
 of Hamming code, 42
 of turbo code, 158
 depth of leaf, 61
Desargues, Gerard, 167
 discrete memoryless source, *see* DMS
 DMS, 104, 107
 dual code, 39
 DVD, 3, 31, 41

Elias, Peter, 110
 encoder, 2, 106, 116, 145, 147
 of Hamming code, 42
 of turbo code, 155
 entropy, 87
 binary entropy function, 88, 132, 152
 branching, 92
 chain rule, 123, 124, 151
 conditional, 124
 conditioning reduces entropy, 129, 152
 joint, 105, 123, 130
 leaf, 92
 properties, 90
 source, 107, 143
 uniqueness, 111
 unit, 87
 equivocation, 125, 130
 error
 arbitrarily small, 138, 139, 143
 bit, 148

- block, 148
- burst, 21
- detectable, 18, 27
- independent, 15
- uncorrectable, 37
- undetectable, 18, 38
- error pattern, 21, 45
- error probability, 139
- error-correcting code, *see* code,
 - error-correcting
- error-detecting code, *see* code, error-detecting
- Euclid*, 167
- Euclidean geometry, 167
- extended root, 62
- extending a leaf, 61

- Fano, Robert M.*, 78, 108
- Fano code, 97, 108, 160
- Fano plane, 169
- Forney, Jr., G. David*, 153

- Gallager, Robert G.*, 110, 138, 141, 153, 159
- game theory, 175
 - Hamming code strategy, 177
 - one-player-guess strategy, 176
 - random strategy, 175
 - repetition code strategy, 176
- Gauss, Carl F.*, 41, 146
- Gaussian channel, 145
- Gaussian distribution, 146
- generator matrix, 38
- geometry
 - Euclidean, 167
 - Fano plane, 169
 - projective, 167–169
- Gilbert–Varshamov bound, 53
- Glavieux, Alain*, 153, 155
- Golay, Marcel J. E.*, 51
- Golomb, Solomon W.*, 181
- Grant, Alex*, 141

- Hamming, Richard W.*, 32, 40, 47
- Hamming bound, 51
- Hamming code, 42
 - general, 52
 - strategy, 177
 - Venn diagram, 43
- Hamming distance, 47
- Hamming weight, 47
- hard decoding, 158

- Hartley, 87
- Hartley, Ralph*, 83
- hat game, 175
- Heegard, Chris*, 160
- Høholdt, Tom*, 41
- Huffman, David A.*, 67, 78
- Huffman, W. Cary*, 53, 182
- Huffman code, 70, 160

- IEEE, 78
- independent random variables, 15, 106, 123, 125, 128, 145, 160
- information, 88, *see also* mutual information
- information theory, 1
- Information Theory Inequality, *see* IT Inequality
- Information Transmission Theorem, 143
- instantaneous code, 57
- ISBN, 26
- IT Inequality, 89

- Joint Source–Channel Coding Theorem, 143

- Karush, William*, 137
- Karush–Kuhn–Tucker conditions, *see* KKT conditions
- Khinchin, Aleksandr Y.*, 111, 112
- KKT conditions, 136
- Kraft Inequality, 63
- Kuhn, Harold W.*, 137
- Kuhn–Tucker conditions, *see* KKT conditions

- Latin square, 181
- LDPC code, 153
- Leaf Entropy Theorem, 93
- Leaf-Counting Lemma, 61
- Leaf-Depth Lemma, 61
- Lin, Shu*, 30, 52, 160
- linear code, 39
- LSB, 8

- m-sequences, 181
- McEliece, Robert J.*, 43, 180, 181
- MacKay, David*, 154
- McMillan's Theorem, 74
- MacWilliams, F. Jessie*, 30, 52, 53
- Massey, James L.*, 58, 73, 78, 89, 108, 110, 141
- MIT, 78
- modular arithmetic, 13, 33
- modulation, 3

Cambridge University Press

978-1-107-01583-8 - A Student's Guide to Coding and Information Theory

Stefan M. Moser and Po-ning Chen

Index

[More information](#)

190

modulo-2, *see* modular arithmetic
 mutual information, 127
 average, 127, 130, 131
 properties, 128
 system, 127
 Venn diagram, 130

 nat, 87
Norberg, Arthur L., 78
 normal distribution, 146

 packing, 48, 51, 53
Pappus of Alexandria, 167
 parity check
 ASCII code, 19
 LDPC code, 153
 matrix, 38
 of Hamming code, 42
 over words, 21
 single parity-check code, 17, 40
 universal product code, 26
 Path Length Lemma, 65
 perfect code, 51
 perfect secrecy, 180
Pinsker, Mark S., 141
Pless, Vera, 51, 53, 182
 Plotkin bound, 53
 power constraint, 146
 prefix-free code, 57, 74
 probability
 a posteriori, 126
 a priori, 126
 backward conditional, 119
 conditional, 118, 119
 conditional probability distribution, 117
 forward conditional, 119
 joint, 118
 probability density function, 146
 Gaussian, 146
 progressive digitizing, 24
 projective geometry, 167–169
 pseudo-random sequences, 180

 rate, 37, 139, 144
 rate distortion theory, 141
 receiver, *see* decoder
 redundancy, 19, 27
Reed, Irving S., 41
 reliable communication, 131, 139
Rezaeian, Mohammad, 141

Index

rooted tree, *see* tree

Sayir, Jossy, 110
Shannon, Claude E., 1, 11, 78, 84, 85, 108,
 109, 111, 138, 140, 141, 143, 180
 Shannon code, 108
 Shannon limit, 153, 155, 159
 Shannon–Fano code, *see* Fano code
 sign bit, 5
 singular code, 73
Sloane, Neil J. A., 30, 52, 53
 soft decoding, 158
Solomon, Gustave, 41
 source coding, 2, 55, 143, *see also* under code
 Source Coding Theorem, 107
 source entropy, 107, 143
 sphere bound, 51
 sphere packing, 48, 51, 53
 stationarity, 118
 statistical independence, 15, 106, 123, 125,
 128, 145, 160
Stinson, Douglas R., 180
Stix, Gary, 78
 strategy
 Hamming code, 177
 one-player-guess, 176
 random, 175
 repetition code, 176
 Sudoku, 181

Thitimajshima, Punya, 153, 155
Thomas, Joy A., 109, 110, 138, 141, 147, 159
Tietäväinen, Aimo, 51
 transition matrix, 117
 transmitter, *see* encoder
 tree, 58, 78
 depth of leaf, 61
 extended root, 62
 extending a leaf, 61
 with probabilities, 65, 92
 unused leaf, 59, 63, 68
 Tsfasman–Vlăduţ–Zink bound, *see* TVZ
 bound
Tsitsiklis, John N., 119, 123
Tucker, Albert W., 137
Tukey, John, 41
Tunstall, Brian P., 78, 108
 turbo code, 155
 decoder, 158
 encoder, 155
 interleaver, 156

TVZ bound, 53

uncertainty, *see* entropy

uniquely decodable code, 56, 73

unused leaf, 59, 63, 68

UPC, 26

van Lint, Jacobus H., 41, 51, 52, 182

vector message, 105

Venn diagram

 Hamming code, 43

 mutual information, 130

Vucetic, Branka, 160

white noise, 15

 Gaussian, 145

Wicker, Stephen B., 30, 52, 53, 160

Wilson, Richard M., 52, 182

Woodward, Philip M., 141

Yuan, Jinhong, 160