

# Index

- A posteriori probability (APP) 172
- A priori probability 172
- Abelian group 11
- Additive channel 20, 65
- Application Layer 2
- Asymptotic code rate 46
  
- Basis 14
- Bayes' rule 172
- BCH bound 84
- BCH code 83, 86
  - (Primitive) BCH code 86
- BCJR algorithm 176
- Belief propagation 119
- Berlekamp-Massey algorithm 90
- Binary operation 11
- Block code 8
- Bounds
  - BCH bound 84
  - Elias-Bassalygo bound 48
  - Gilbert-Varshamov bound 47
  - Hamming bound 45
  - McElice-Rodemich-Rumsey-Welch bound 48
  - Plotkin bound 47
  - Singleton bound 81
  - Sphere-packing bound 45
- Branch metric 151
- Breadth first algorithm 162
  
- C-comparison 204
- Catastrophic convolutional code 150
- Catastrophic error propagation 150
- Channel 7
- Channel capacity 10
- Channel code 265
- Channel with additive noise 20
- Chien's search 89
- Ciphertext 213
- Code 8
  - BCH code 83, 86
    - (Primitive) BCH code 86
  - Block code 8
  - Catastrophic convolutional code 150
  - Channel code 265
  - Compression code 266
  - Convolutional code 141
  - Cryptocode 266
  - Cyclic code 25
  - Dual code 22
  - Equivalent code 22
  - Euclidean-geometry low density (EG) code 107
    - EG code of type 0 108
  - Gilbert code 116
  - Group code 21
  - Hamming code 77
  - Linear block code 21
  - Linear code 145
  - Low-density parity-check (LDPC) codes 103
  - LT code 258
  - Maximum distance separable (MDS) code 81
  - Parallel-concatenated convolutional (PCC) code 170
  - Perfect code 46
  - Random binary code 241
  - Recursive systematic convolutional (RSC) code 170
  - Reed-Solomon (RS) code 82
    - 1-extended RS code 83
  - Shortened cyclic code 39
  - Systematic code 22
  - Systematic convolutional code 146
  - Tornado code 253
  - Transport code 265
  - Turbo code 170
- Code rate 141
- Codebased signature 239
- Codebook 259
- Codeword 7
- Commutative group 11
- Compression code 266
- Constituent decoder 173
- Constraint length 141
- Convergence speed 121, 129
- Convolutional code 141
- Coordinate (arithmetic) space 14
- Coset 12

- Coset leader 23
- Covering polynomial 55
- Covering-set decoding 55, 58
- Cryptochannel 266
- Cryptocode 266
- Cryptography 213
- Cryptosystem
  - McEliece cryptosystem 220
  - Merkle-Hellman cryptosystem 217
  - Niederreiter cryptosystem 219
  - Public-key cryptosystem 214
  - RSA cryptosystem 237
  - Secret-key cryptosystem 213
- Cyclic code 25
- Cyclic group 11
  
- Data Link Layer 1
- Datagram routing 191
- Decoder 8
- Decision region 8
- Decoding depth 155
- Decoding error 8
- Decoding inefficiency of Tornado code 253
- Decoding procedure 8
- Degree of polynomial 17
- Density evolution 106
- Depth first algorithm 162
- Designed distance 85
- Discrete memoryless channel (DMC) 156
- Domain 258
- Dual code 22
  
- EG code of type 0 108
- Eigen subcode 224
- Elias-Bassalygo bound 48
- Encoder 8
- Encoding procedure 8
- Encryption 213
- Entropy 45
- Equivalent code 22
- Error detection 9
- Error-location number 87
- Error-location polynomial 87
- Error-value 87
- Euclidean geometry (EG) 138
- Euclidean-geometry low density (EG) code 107
- Euclidean ring 18
- Extrinsic information 173
  
- Factor group 12
- Fano algorithm 166
- Fano metric 162
- Fano branch metric 162
- Fano symbol metric 162
- Field 12
  
- Finite state machine (FSM) 145
- Free distance 148
- Full decoding 9
  
- Generalised covering-set decoding 60
- Generating function 104
- Generator element 12
- Generator matrix 21, 145
- Generator polynomial 26
- Gilbert code 116
  - Generalised Gilbert code 117
- Gilbert-Varshamov bound 47
- Girth 103
- Group 11
  - Abelian group 11
  - Commutative group 11
  - Cyclic group 11
  - Factor group 12
  - Isomorphic group 11
  - Subgroup 12
  - Symmetric group 11
- Group code 21
- Guruswami-Sudan algorithm 95
  
- Hamming bound 45
- Hamming code 77
- Hamming distance 8
- Hamming weight 20
- Hard-decision Viterbi decoding 155
- Hasse derivative 94
- High-probability set 269
- Homogeneous packing 80
- Homomorphism 11
  
- ISO 1
- Identity element 11
- Impulse response 141
- Incidence graph 103
- Information set 52
- Intrinsic information 173
- Inverse element 11
- Irreducible polynomial 19
- Irregular LDPC code 104
- Isomorphic group 11
- Isomorphism 11
- Iterative decoding 172
  
- Key distribution 213
- Knapsack problem 217
- Knapsack vector 217
  
- L1 1
- L2 1
- L3 1
- L4 1
- L5 2

- L6 2
- L7 2
- Layer 1
  - Application Layer 2
  - Data Link Layer 1
  - Network Layer 1
  - Physical Layer 1
  - Presentation Layer 2
  - Session Layer 2
  - Transport Layer 1
- Lexicographic monomial ordering 98
- Likelihood function 150
- Likelihood ratio (LR) 172
- Linear block code 21
- Linear code 145
- Linear filter 30
- Linear functional 15
- Linear (in)dependence 14
- Linear operator 15
- Linear subspace 15
- Log-likelihood ratio (LLR) 172
- Log-MAP algorithm 183
- Low-density parity-check (LDPC) codes 103
  - LDPC code ensemble 105
  - Irregular LDPC code 104
  - Regular LDPC code 104
- LT code 258
  
- Maximum a posteriori (MAP) algorithm 176
- Maximum a posteriori (MAP) rule 172
- Maximum distance separable (MDS) code 81
- Maximum likelihood (ML) decoding 23
- Max-Log-MAP algorithm 182
- McEliece cryptosystem 220
- McEliece-Rodemich-Rumsey-Welch bound 48
- Memoryless channel 7
- Merkle-Hellman cryptosystem 217
- Minimum distance 9
- Minimum distance (MD) decoding 9
- Min-sum algorithm 122
- Multiplicity matrix 98
- Multi-threshold (MT) decoder 122
  
- NP-complete problem 214, 217
- NP-hard problem 214, 217
- Network Layer 1
- Network unreliability parameter 247
- Niederreiter cryptosystem 219
- Nielsen interpolation algorithm 99
- Nondeterministic algorithm 214
- Nondeterministic state machine 216
- Normal subgroup 12
- Normalised polynomial 17
- Number of encoded symbols 141
- Number of information symbols 141
  
- OSIRM 1
- One-time pad 213
- Order of group 11
- Overall rate of superchannel 267
  
- PEG construction 112
- Packet switching 191
- Packing density 46
- Parallel class 114
- Parallel-concatenated convolutional (PCC) code 170
- Parity-check matrix 22
- Parity polynomial 27
- Partial decoding 9
- Partial path metric 151
- Path metric 151
- Perfect code 46
- Period of polynomial 78
- Permutation 11
- Permutation decoding 55
- Peterson-Gorenstein-Zierler algorithm 89
- Physical Layer 1
- Plotkin bound 47
- Presentation Layer 2
- Primitive BCH code 86
- Primitive element 19
- Principal ideal 19
- Principle of optimality 152
- Public-key cryptosystem 214
- Punctured split syndrome decoding 70
  
- Quality of service (QoS) 273
- Quantization level 258
- Quantization step 263
- Quotient ring 19
  
- RSA cryptosystem 237
- Random binary code 241
- Reconstruction level 258
- Recursive systematic convolutional (RSC) code 170
- Redundancy 10
- Reed-Solomon (RS) code 82
  - 1-extended RS code 83
- Regular LDPC code 104
- Relative distance 45, 65
- Residue 18
- Residue class ring 19
- Ring 13
  - Euclidean ring 18
  - Quotient ring 19
  - Residue class ring 19
- Roth-Ruckenstein algorithm 97
  
- S-comparison 204
- S-ordering 204

- Scalar multiplication 14
- Scalar quantization 258
- Secret-key cryptosystem 213
- Selection 39
- Self-orthogonal subspace 17
- Semigroup 11
- Sequential decoding 162
- Session Layer 2
- Shannon's noisy channel coding theorem 10
- Shortened cyclic code 39
- Sidelnikov-Shestakov attack 222
- Singleton bound 81
- Soft decision decoding of RS code 98
- Soft-decision Viterbi decoding 159
- Soft input / soft output (SISO) decoder 176
- Soft-In/Soft-Out Viterbi algorithm (SOVA) 184
- Sorger's attack on cryptosystem based on full decoding 224
- Space complexity 65
- Sphere-packing bound 45
- Split syndrome decoding 61
- Stack algorithm 163
- Standard array 23
- State diagram 145
- Subcode over subset 79
- Subgroup 12
- Sudan algorithm 93
- Superchannel 267
- Supercode decoding 63
- Survivor path 155
- Symbol metric 151
- Symmetric group 11
- Syndrome 22, 38
- Syndrome decoding 66
- Systematic code 22
- Systematic convolutional code 146
- Systematic encoding 22
- Tail symbols 156
- Tanner graph 103
- Time complexity 65
- Tornado code 253
- Transport channel 266
- Transport code 265
- Transport coding 193
- Transport Layer 1
- Trapdoor function 214
- Tree diagram 147
- Trellis diagram 148
- Turbo code 170
- UMP algorithm 122
- User authentication 213
- Vector space 14
- Videochannel 266
- Viterbi algorithm 151
- Weighted-degree monomial ordering 98
- Zero-neighbours algorithm 66