

## Index

- additive stream cipher, 463
- algebra (a commutative ring and a linear space), 318
  - group algebra, 317
  - polynomial algebra, 214
  - $\sigma$ -algebra, 440
- algebraic-geometric code, 340
- algorithm, 9
  - Berlekamp–Massey (BM) decoding algorithm for BCH codes, 240
  - Berlekamp–Massey (BM) algorithm for solving linear equations, 460
  - division algorithm for polynomials, 214
  - Euclid algorithm for integers, 473
  - extended Euclid algorithm for integers, 470
  - Euclid algorithm for polynomials, 242
  - Guruswami–Sudan (GS) decoding algorithm for Reed–Solomon codes, 298
  - Huffman encoding algorithm, 9
- alphabet, 3
  - source alphabet, 8
  - coder (encoding) alphabet, 3
  - channel input alphabet, 60
  - channel output alphabet, 65
- asymptotic equipartition property, 44
- asymptotically good sequence of codes, 78
- automorphism, 283
  
- band-limited signal, 411
- bandwidth, 409
- basis, 149, 184
- BCH (Bose–Ray–Chaudhuri–Hocquenghem) bound, or BCH theorem, 237, 295
- BCH code, 213
  - BCH code in a narrow sense, 235
  - binary BCH code in a narrow sense, 235
- Bernoulli source, 3
- bit (a unit of entropy), 9
- bit commitment cryptosystem, 468
  
- bound
  - BCH bound, 237, 295
  - Elias bound, 177
  - Gilbert bound, 198
  - Gilbert–Varshamov bound, 154
  - Griesmer bound, 197
  - Hamming bound, 150
  - Johnson bound, 177
  - linear programming bound, 322
  - Plotkin bound, 155
  - Singleton bound, 154
- bar-product, 152
  
- capacity, 61
- capacity of a discrete channel, 61
- capacity of a memoryless Gaussian channel with white noise, 374
- capacity of a memoryless Gaussian channel with coloured noise, 375
  - operational channel capacity, 102
- character (as a digit or a letter or a symbol), 53
- character (of a homomorphism), 313
  - modular character, 314
  - trivial, or principal, character, 313
- character transform, 319
- characteristic of a field, 269
- channel, 60
  - additive Gaussian channel (AGC), 368
  - memoryless Gaussian channel (MGC), 368
  - memoryless additive Gaussian channel (MAGC), 366
  - memoryless binary channel (MBC), 60
  - memoryless binary symmetric channel (MBSC), 60
  - noiseless channel, 103
- channel capacity, 61
  - operational channel capacity, 102
- check matrix: *see* parity-check matrix
- cipher (or a cryptosystem), 463
  - additive stream cipher, 463

510

cipher (or a cryptosystem) (cont.)  
 one-time pad cipher, 466  
 public-key cipher, 467  
 ciphertext, 468  
 code, or encoding, viii, 4  
 alternant code, 332  
 BCH code, 213  
 binary code, 10, 95  
 cardinality of a code, 253  
 cyclic code, 216  
 decipherable code, 14  
 dimension of a linear code, 149  
 $D$  error detecting code, 147  
 dual code, 153  
 equivalent codes, 190  
 $E$  error correcting code, 147  
 Golay code, 151  
 Goppa code, 160, 334  
 Hamming code, 199  
 Huffman code, 9  
 information rate of a code, 147  
 Justesen code, 240, 332  
 lossless code, 4  
 linear code, 148  
 maximal distance separating (MDS), 155  
 parity-check code, 149  
 perfect code, 151  
 prefix-free code, 4  
 random code, 68, 372  
 rank of a linear code, 184  
 Reed–Muller (RM) code, 203  
 Reed–Solomon code, 256, 291  
 repetition code, 149  
 reversible cyclic code, 230  
 self-dual code, 201, 227  
 self-orthogonal, 227  
 simplex code, 194  
 codebook, 67  
 random codebook, 68  
 coder, or encoder, 3  
 codeword, 4  
 random codeword, 6  
 coding: *see* encoding  
 coloured noise, 374  
 concave, 19, 32  
 strictly concave, 32  
 concavity, 20  
 conditionally independent, 26  
 conjugacy, 281  
 conjugate, 229  
 convergence almost surely (a.s.), 131  
 convergence in probability, 43  
 convex, 32  
 strictly convex, 104  
 convexity, 142

Index

core polynomial of a field, 231  
 coset, 192  
 cyclotomic coset, 285  
 leader of a coset, 192  
 cryptosystem (or a cipher), 468  
 bit commitment cryptosystem, 468  
 ElGamal cryptosystem, 475  
 public key cryptosystem, 468  
 RSA (Rivest–Shamir–Adelman) cryptosystem, 468  
 Rabin, or Rabin–Williams cryptosystem, 473  
 cyclic group, 231  
 generator of a cyclic group  
 cyclic shift, 216  
 data-processing inequality, 80  
 detailed balance equations (DBEs), 56  
 decoder, or a decoding rule, 65  
 geometric (or minimal distance) decoding rule, 163  
 ideal observer (IO) decoding rule, 66  
 maximum likelihood (ML) decoding rule, 66  
 joint typicality (JT) decoder, 372  
 decoding, 167  
 decoding alternant codes, 337  
 decoding BCH codes, 239, 310  
 decoding cyclic codes, 214  
 decoding Hamming codes, 200  
 list decoding, 192, 405  
 decoding Reed–Muller codes, 209  
 decoding Reed–Solomon codes, 292  
 decoding Reed–Solomon codes by the Guruswami–Sudan algorithm, 299  
 syndrome decoding, 193  
 decrypt function, 469  
 degree of a polynomial, 206, 214  
 density of a probability distribution (PDF), 86  
 differential entropy, 86  
 digit, 3  
 dimension, 149  
 dimension of a code, 149  
 dimension of a linear representation, 314  
 discrete Fourier transform (FFT), 296  
 discrete-time Markov chain (DTMC), 1, 3  
 discrete logarithm, 474  
 distributed system, or a network (of transmitters), 436  
 Dirac  $\delta$ -function, 318  
 distance, 20  
 Kullback–Leibler distance, 20  
 Hamming distance, 144  
 minimal distance of a code, 147  
 distance enumerator polynomial, 322  
 divisor, 217  
 greatest common divisor (gcd), 223  
 dot-product, 153  
 doubly stochastic (Cox) random process, 492

- electronic signature, 469, 476  
 encoding, or coding, vii, 4  
   Huffman encoding, 9  
   Shannon–Fano encoding, 9  
   random coding, 67  
 entropy, vii, 7  
   axiomatic definition of entropy, 36  
   binary entropy, 7  
   conditional entropy, 20  
   differential entropy, 86  
   entropy of a random variable, 18  
   entropy of a probability distribution, 18  
   joint entropy, 20  
   mutual entropy, 28  
   entropy–power inequality, 92  
    $q$ -ary entropy, 7  
   entropy rate, vii, 41  
   relative entropy, 20  
 encrypt function, 468  
 ergodic random process (stationary), 397  
 ergodic transformation of a probability space, 397  
 error locator, 311  
 error locator polynomial, 239, 311  
 error-probability, 58  
 extension of a code, 151  
   parity-check extension, 151  
 extension field, 261  
  
 factor (as a divisor), 39  
 irreducible factor, 219  
   prime factor, 39  
 factorization, 230  
 fading of a signal, 447  
   power fading, 447  
   Rayleigh fading, 447  
 feedback shift register, 453  
   linear feedback shift register (LFSR), 454  
 feedback polynomial, 454  
 field (a commutative ring with inverses), 146, 230  
   extension field, 261  
   Galois field, 272  
   finite field, 194  
   polynomial field, 231  
   primitive element of a field, 230, 232  
   splitting field, 236, 271  
 Frobenius map, 283  
  
 Gaussian channel, 366  
   additive Gaussian channel (AGC), 368  
   memoryless Gaussian channel (MGC), 368  
   memoryless additive Gaussian channel (MAGC), 366  
 Gaussian coloured noise, 374  
 Gaussian white noise, 368  
 Gaussian random process, 369  
 generating matrix, 185  
  
 generator (of a cyclic code), 218  
   minimal degree generator polynomial, 218  
 generator (of a cyclic group), 232  
 geometric (or minimal distance) decoding rule, 163  
 group, 146  
   group algebra, 317  
   commutative, or Abelian, group, 146  
   cyclic group, 231  
   linear representation of a group, 314  
 generalized function, 412  
 greatest common divisor (gcd), 223  
  
 ideal observer (IO) decoding rule, 66  
 ideal of a ring, 217  
   principal ideal, 219  
 identity (for weight enumerator polynomials), 258  
   abstract MacWilliams identity, 315  
   MacWilliams identity for a linear code, 258, 313  
 independent identically distributed (IID) random variables, 1, 3  
 inequality, 4  
   Brunn–Minkovski inequality, 93  
   Cauchy–Schwarz inequality, 124  
   Chebyshev inequality, 128  
   data-processing inequality, 80  
   entropy–power inequality, 92  
   Fano inequality, 25  
   generalized Fano inequality, 27  
   Gibbs inequality, 17  
   Hadamard inequality, 91  
   Kraft inequality, 4  
   Ky–Fan inequality, 91  
   log-sum inequality, 103  
   Markov inequality, 408  
   pooling inequalities, 24  
 information, 2, 18  
   mutual information, or mutual entropy, 28  
   information rate, 15  
   information source (random source), 2, 44  
   Bernoulli information source, 3  
   Markov information source, 3  
 information symbols, 209  
 initial fill, 454  
 intensity (of a random measure), 437  
 intensity measure, 437  
  
 joint entropy, 20  
 joint input/output distribution (of a channel), 67  
 joint typicality (JT) decoder, 372  
  
 key (as a part of a cipher), 466  
   decoding key (a label of a decoding, or decrypting, map), 469  
   encoding key (a label of an encoding, or encrypting, map), 468  
   random key of a one-pad cipher, 466

- key (as a part of a cipher) (cont.)
  - private key, 470
  - public key, 469
  - secret key, 473
- Karhunen–Loève decomposition, 426
- law of large numbers, 34
  - strong law of large numbers, 438
- leader of a coset, 192
- least common multiple (lcm), 223
- lemma
  - Borel–Cantelli lemma, 418
  - Nyquist–Shannon–Kotelnikov–Whittaker lemma, 431
- letter, 2
- linear code, 148
- linear representation of a group, 314
  - space of a linear representation, 314
  - dimension of a linear representation, 314
- linear space, 146
  - linear subspace, 148
- linear feedback shift register (LFSR), 454
  - auxiliary, or feedback, polynomial of an LFSR, 454
- Markov chain, 1, 3
  - discrete-time Markov chain (DTMC), 1, 3
  - coupled Markov chain, 50
  - irreducible and aperiodic Markov chain, 128
  - $k$ th-order Markov chain approximation, 407
  - second-order Markov chain, 131
  - transition matrix of a Markov chain, 3
- Markov inequality, 408
- Markov property, 33
  - strong Markov property, 50
- Markov source, 3
  - stationary Markov source, 3
- Markov triple, 33
- Matérn process (with a hard core), 451
  - first model of the Matérn process, 451
  - second model of the Matérn process, 451
- matrix, 13
  - covariance matrix, 88
  - generating matrix, 185
  - generating check matrix, canonical, or standard, form of, 189
  - parity-check matrix, 186
  - parity-check matrix, canonical, or standard, form of, 189
  - parity-check matrix of a Hamming code, 191
  - positive definite matrix, 91
  - recursion matrix, 174
  - Töplitz matrix, 93
  - transition matrix of a Markov chain, 3
  - transition matrix, doubly stochastic, 34
  - Vandermonde matrix, 295
- maximum likelihood (ML) decoding rule, 66
- measure (as a countably additive function of a set), 366
  - intensity (or mean) measure, 436
  - non-atomic measure, 436
  - Poisson random measure, 436
  - product-measure, 371
  - random measure, 436
  - reference measure, 372
  - $\sigma$ -finite, 436
- Möbius function, 277
  - Möbius inversion formula, 278
- moment generating function, 442
- network: *see* distributed system
  - supercritical network, 449
- network information theory, 436
- noise (in a channel), 2, 70
  - Gaussian coloured noise, 374
  - Gaussian white noise, 368
- noiseless channel, 103
- noisy (or fully noisy) channel, 81
- one-time pad cipher, 466
- operational channel capacity, 102
- order of an element, 267
- order of a polynomial, 231
- orthogonal, 185
  - ortho-basis, 430
  - orthogonal complement, 185
  - orthoprojection, 375
  - self-orthogonal, 227
- output stream of a register, 454
- parity-check code, 149
- parity-check extension, 151
- parity-check matrix, 186
- plaintext, 468
- Poisson process, 436
- Poisson random measure, 436
- polynomial, 206
  - algebra, polynomial, 214
  - degree of a polynomial, 206, 214
  - distance enumerator polynomial, 322
  - error locator polynomial, 239
  - Goppa polynomial, 335
  - irreducible polynomial, 219
  - Mattson–Solomon polynomial, 296
  - minimal polynomial, 236
  - order of a polynomial, 231
  - reducible polynomial, 221
  - primitive polynomial, 230, 267
  - Kravchuk polynomial, 320
  - weight enumerator polynomial, 319, 351
- probability distribution, vii, 1
  - conditional probability, 1
  - probability density function (PDF), 86

- equiprobable, or uniform, distribution, 3, 22
- exponential distribution (with exponential density), 89
- geometric distribution, 21
- joint probability, 1
- multivariate normal distribution, 88
- normal distribution (with univariate normal density), 89
- Poisson distribution, 101
- probability mass function (PMF), 366
- probability space, 397
- prolate spheroidal wave function (PSWF), 425
- protocol of a private communication, 469
  - Diffie–Hellman protocol, 474
- prefix, 4
  - prefix-free code, 4
- product-channel, 404
- public-key cipher, 467
- quantum mechanics, 431
- random code, 68, 372
- random codebook, 68
- random codeword, 6
- random measure, 436
  - Poisson random measure (PRM), 436
- random process, vii
  - Gaussian random process, 369
  - Poisson random process, 436
  - stationary random process, 397
  - stationary ergodic random process, 397
- random variable, 18
  - conditionally independent random variables, 26
  - equiprobable, or uniform, random variable, 3, 22
  - exponential random variable (with exponential density), 89
  - geometric random variable, 21
  - independent identically distributed (IID) random variables, 1, 3
  - joint probability distribution of random variables, 1
  - normal random variable (with univariate normal density), 89
  - Poisson random variable, 101
- random vector, 20
  - multivariate normal random vector, 88
- rank of a code, 184
- rank-nullity property, 186
- rate, 15
  - entropy rate, vii, 41
  - information rate of a source, 15
  - reliable encoding (or encodable) rate, 15
  - reliable transmission rate, 62
  - reliable transmission rate with regional constraint, 373
  - regional constraint for channel capacity, 367
- register, 453
  - feedback shift register, 453
    - linear feedback shift register (LFSR), 454
  - feedback, or auxiliary, polynomial of an LFSR, 454
  - initial fill of register, 454
  - output stream of a register, 454
- repetition code, 149
- repetition of a code, 152
- ring, 217
  - ideal of a ring, 217
  - quotient ring, 274
- root of a cyclic code, 230
  - defining root of a cyclic code, 233
  - root of a polynomial, 228
- root of unity, 228
  - primitive root of unity, 236
- sample, viii, 2
- signal/noise ratio (SNR), 449
- sinc function, 413
- size of a code, 147
- space, 35
  - Hamming space, 144
  - space  $L_2(\mathbb{R}^1)$ , 415
  - linear space, 146
  - linear subspace, 148
  - space of a linear representation, 314
  - state space of a Markov chain, 35
  - vector space over a field, 269
- stream, 463
- strictly concave, 32
- strictly convex, 104
- string, or a word (of characters, digits, letters or symbols), 3
- source of information (random), 2, 44
  - Bernoulli source, 3
  - equiprobable Bernoulli source, 3
  - Markov source, 3
    - stationary Markov source, 3
- spectral density, 417
- stationary, 3
  - stationary Markov source, 3
  - stationary random process, 397
    - stationary ergodic random process, 397
- supercritical network, 449
- symbol, 2
- syndrome, 192
- theorem
  - Brunn–Minkovski theorem, 93
  - Campbell theorem, 442
  - Cayley–Hamilton theorem, 456
  - central limit theorem (CLT), 94
  - Doob–Lévy theorem, 409
  - local De Moivre–Laplace theorem, 53
  - mapping theorem, 437

514

*Index*

- theorem (cont.)  
 product theorem, 444  
 Shannon theorem, 8  
 Shannon's noiseless coding theorem (NLCT), 8  
 Shannon's first coding theorem (FCT), 42  
 Shannon's second coding theorem (SCT), or noisy  
 coding theorem (NCT), 59, 162  
 Shannon's SCT: converse part, 69  
 Shannon's SCT: strong converse part, 175  
 Shannon's SCT: direct part, 71, 163  
 Shannon–McMillan–Breiman theorem, 397  
 totient function, 270  
 transform  
 character transform, 319  
 Fourier transform, 296  
 Fourier transform, discrete, 296  
 Fourier transform in  $L_2$ , 413  
 transmitter, 443  
 uncertainty principle, 431  
 Vandermonde determinant, 237  
 Vandermonde matrix, 297  
 wedge-product, 149  
 weight enumerator polynomial, 319  
 white noise, 368  
 word, or a string (of characters, digits, letters or  
 symbols), 3  
 weight of a word, 144