

Index

- adjacency matrix
 - of digraphs, 486
 - of graphs, 398
 - Lee, 325
- alphabet, 3
- alternant code, 70, 157, 179
 - decoding of, 197, 204
 - Lee-metric, 306
 - list, 280, 328
 - designed minimum distance of, 157, 250
 - dual code of, 175, 180
 - Lee-metric, 302
 - list decoding of, 280, 328
 - over \mathbb{Z} , 328
- aperiodic irreducible digraph, 455
- aperiodic irreducible matrix, 445
- arc (in projective geometry), 361
 - complete, 363
- autocorrelation
 - of Legendre sequences, 80
 - of maximal-length sequences, 87
- AWGN channel, 17
- basis
 - complementary, 85
 - dual, 85
 - normal, 240
- BCH bound, 253
- BCH code, 162, 181, 244, 250
 - consecutive root sequence of, 163
 - decoding of, *see* alternant code, decoding of
 - designed minimum distance of, 163, 250
 - excess root of, 251
 - root of, 163, 250
- Berlekamp code, 314, 330
- Berlekamp–Massey algorithm, 200, 217
- Bhattacharyya bound, 21, 25, 493
- bi-connection, 454
- binary erasure channel, 15
- binary symmetric channel (BSC), 4, 450
- bipartite graph, 362, 398
- bit-shift error, 327
- Blahut's algorithm, 217
- block code, 5
- Blokh–Zyablov bound, 393
- bound
 - BCH, 253
 - Bhattacharyya, 21, 25, 493
 - Blokh–Zyablov, 393
 - Carlitz–Uchiyama, 179
 - Chernoff, 139
 - decoding-radius, 290
 - Elias, 108
 - Lee-metric, 332
 - Gilbert–Varshamov, 97, 137, 176, 181, 393
 - asymptotic, 107, 372
 - Lee-metric, 320, 330
 - Griesmer, 120, 136
 - Hamming, *see* bound, sphere-packing
 - Hartmann–Tzeng, 265
 - Johnson, 107, 128, 139, 289
 - Lee-metric, 330
 - linear programming, 103, 110, 138
 - MDS code length, 338
 - MRRW, 110
 - Plotkin, 37, 127, 131, 139, 294
 - Lee-metric, 326, 330
 - Reiger, 122
 - Roos, 265
 - Singleton, *see* Singleton bound
 - sphere-covering, 123
 - sphere-packing, 95, 122, 136
 - asymptotic, 107
 - Lee-metric, 318, 330
 - union, 137
 - Zyablov, 373, 392, 413, 422, 438, 440
- burst, 45, 122, 137, 257
- cap (in projective geometry), 47
- capacity, 10, 16, 24, 110
- Carlitz–Uchiyama bound, 179
- catastrophic error propagation, 496
- Cauchy matrix, 168, 336, 356, 362
- Cayley graph, 406, 447
- channel, 1
 - additive, 5
 - AWGN, 17
 - binary symmetric (BSC), 4, 450

- discrete memoryless (DMC), 19, 23, 46, 142, 466
- erasure, 15, 25, 126, 134, 391, 514
- Gaussian (AWGN), 17
- non-symmetric, 20, 46
- probabilistic, 3
- symmetric, 4, 19, 24, 32, 110, 113, 117, 125, 133, 145, 378, 390, 394, 424, 450, 467, 490
- character
 - of Abelian groups, 91, 447
 - additive, 85, 99, 447
 - multiplicative, 78
 - quadratic, 80
 - trivial, 79
- characteristic (of fields), 62
- check node, 449
- check polynomial, 246
- Chernoff bound, 139
- Chien search, 186, 215, 285
- circulant matrix, 325, 330, 356, 362
- code, 5
 - algebraic-geometry, 138
 - almost-MDS (AMDS), 363
 - alternant, *see* alternant code
 - array, 353
 - BCH, *see* BCH code
 - Berlekamp, 314, 330
 - block, 5
 - concatenated, *see* concatenated code
 - constant-weight, 121, 139, 352
 - convolutional, *see* convolutional code
 - cyclic, *see* cyclic code
 - Delsarte–Goethals, 328
 - dimension, 5
 - double-error-correcting, 70, 161
 - dual, *see* dual code
 - equidistant, 128
 - equivalence, 29, 47
 - generalized Reed–Solomon, *see* GRS code
 - Golay, 96, 136, 255
 - Goppa, 182, 389
 - graph, *see* graph code
 - Gray, 321, 328
 - group, 37, 299
 - Hamming, *see* Hamming code
 - inner (in concatenated codes), 154, 366
 - Justesen, 376
 - Kerdock, 328
 - LDPC, 362, 450
 - length, 5
 - lengthening of, 123
 - linear, *see* linear code
 - low-density parity-check, 362, 450
 - maximal, 123
 - maximum distance separable (MDS), *see* MDS code
 - minimum distance, 6
 - near-MDS (NMDS), 363
 - negacyclic, 323, 330
 - outer (in concatenated codes), 154, 366
 - parity, 27
 - perfect, 96, 137, 256
 - Lee-metric, 319, 330
 - Preparata, 328
 - product, 44, 178
 - punctured, 36
 - rate, 5
 - redundancy, 27
 - Reed–Muller, *see* Reed–Muller code
 - Reed–Solomon, *see* RS code
 - repetition, 28
 - self-dual, 31
 - shortened, 40
 - simplex, 41, 120
 - weight distribution of, 99
 - size, 5
 - spectral-null, 329
 - Spielman, 451
 - trellis, 460
 - decoding of, 466
 - encoding of, 464
 - free distance of, 463
 - turbo, 519
 - Wozencraft, 375
 - Wyner–Ash, 512
- codeword, 3, 460
- communication system, 1
- companion matrix, 73, 383, 510
- complementary basis, 85
- concatenated code, 154, 172, 178, 408, 420
 - decoding of, 178, 371, 396, 422
 - dual code of, 383
 - linearly-, 154, 367
- concave function, 9, 23
- conjugate element
 - in the complex field, 325
 - in cyclotomic extension fields, 241
 - in finite extension fields, 218
- conjugate transpose (of complex matrices), 326
- convex function, 9
- convolutional code, 477
 - constraint length of encoders of, 483
 - decoding of, 485, 519
 - encoding of, 479
 - free distance of, 478, 512
 - generator matrix of, 477
- coset
 - leader, 34
 - of linear codes, 34
 - of subgroups, 522
- cover (of arrays), 354, 362
- covering radius, 123, 137
 - of GRS codes, 166
 - of MDS codes, 166
- crisscross error, 362
- cycle (in graphs), 397
 - in digraphs, 454

- cyclic code, 242
 - dual code of, 247
 - encoding of, 245
 - Hamming, 244, 254, 264
 - of length q over $\text{GF}(q)$, 257, 265
 - of length $q+1$ over $\text{GF}(q)$, 262, 265
 - repeated-root, 265
 - root of, 248
 - shortened, 388
- cyclotomic coset, 230
- cyclotomic extension field, 240
- dB, 18
- decoding, 7
 - of alternant codes, *see* alternant code, decoding of
 - of BCH codes, *see* alternant code, decoding of
 - complexity, 48
 - of concatenated codes, 178, 371, 396, 422
 - of convolutional codes, 485, 519
 - error probability, 7, 110, 132, 133, 471, 485, 491, 519
 - generalized minimum distance (GMD), 178, 371, 396, 422
 - of graph codes, 414
 - of GRS codes, *see* GRS decoding
 - of Hamming codes, 35
 - hard-decision, 18
 - iterative, 414, 451
 - of linear codes, 33
 - list, *see* list decoding
 - of GRS codes, *see* GRS list decoding
 - maximum *a posteriori*, 8
 - maximum-likelihood, 8, 32, 140, 466
 - mis-detection probability, 22, 125, 132, 140, 440
 - nearest-codeword, 9, 33
 - sequential, 520
 - soft-decision, 18
 - standard array, 33
 - syndrome, 34
 - of trellis codes, 466
- degree (of extension fields), 57
- degree (of polynomials), 51
 - of bivariate polynomials, 268
- degree (of vertices in graphs), 396
- derivative, 65, 87, 194, 300, 322
 - Hasse (or hyper-), 87, 276, 310, 329
- designed minimum distance, 157, 163, 250
- diameter (of graphs), 397
- digraph (and labeled digraph), 400, 453
 - adjacency matrix of, 486
 - anticipation of, 503
 - aperiodic irreducible, 455
 - controllable, 454, 519
 - deterministic, 456
 - induced, 453
 - irreducible, 454, 519
 - irreducible component of, 455, 501
 - irreducible sink of, 455, 501
 - lossless, 456
 - period of, 455, 502
 - primitive irreducible, 455
 - regular, 459
 - sequence set of, 457
 - strongly-connected, 454, 519
 - tag in, 459
 - trellis diagram of, 458
- dimension (of codes), 5, 26
- direct product (of matrices), 45, 428
- directed graph, *see* digraph (and labeled digraph)
- discrete logarithm, 59, 81, 91
- discrete memoryless channel (DMC), 19, 23, 46, 142, 466
- distance
 - cover, 354, 362
 - free, 463, 478, 512
 - in graphs, 397
 - Hamming, 6
 - Kullback–Leibler, 111
 - Lee, 299
 - rank, 19, 353, 361
- divergence, 111
- dual basis, 85
- dual code, 30
 - of alternant codes, 175, 180
 - of concatenated codes, 383
 - of cyclic codes, 247
 - of extended GRS codes, 163
 - of GRS codes, 148
 - of Hamming codes, 41
 - of MDS codes, 119
 - of RS codes, 257
 - self-, 31
 - of subfield sub-codes, 175
- dual linear programming problem, 138
- dynamic programming, 519
- edge (in graphs), 396
 - cut, 397
 - in digraphs, 453
- Elias bound, 108
 - Lee-metric, 332
- encoder, 3
- entropy function
 - binary, 9
 - q -ary, 24, 105
- erasure, 15
 - burst, 45, 257
 - channel, 15, 25, 126, 134, 391, 514
- error, 12
 - bit-shift, 327
 - burst, 45, 122, 137, 257
 - correction, 12
 - crisscross, 362
 - detection, 13
 - evaluator polynomial, 186

- exponent, 143, 381, 393, 425
- location, 5
- locator polynomial, 185
 - Lee-metric, 307
- locator ratio, 307
- peak-shift, 327
- synchronization, 327
- value, 5
- word, 5
- error-evaluator polynomial, 186
- error-locator polynomial, 185
 - Lee-metric, 307
- error-locator ratio, 307
- Euclid's algorithm
 - for integers, 50, 501, 524
 - for polynomials, 52, 71, 90, 191, 215, 309
- Euler–Fermat Theorem, 526
- Euler function, 62, 229, 449, 522
- expander (graph), 404
- exponent (of polynomials), 206, 227, 247
- extension field, 57, 218
 - arithmetic in, 59, 74, 90
 - conjugate element in, 218, 241
 - cyclotomic, 240
- factorization of polynomials, 56, 90
- Fano's algorithm, 520
- Fermat's Little Theorem, 526
- field, 522
 - characteristic of, 62
 - extension, *see* extension field
 - finite, *see* finite field
 - Galois, *see* finite field
 - prime, 50
 - of rational functions, 268, 476
 - splitting, 65
- finite field, 50, 218, 240
 - characteristic of, 62
 - extension field of, *see* extension field
 - isomorphism, 227
 - prime, 50
 - product of elements in, 77
 - sum of powers of elements in, 77, 150
- finite-state machine (FSM), 460
 - linear, *see* linear finite-state machine (LFSM)
- formal derivative, *see* derivative
- formal power series, 189, 237, 300, 474
 - bivariate, 487
- Forney's algorithm, 195, 215
- Fourier transform, 81, 92, 217
- free distance, 463, 478, 512
- Frobenius mapping, 64
- Galois field, *see* finite field
- Gaussian (AWGN) channel, 17
- Gaussian elimination, 189, 274, 296
- Gaussian noise, 17
- generalized minimum distance (GMD) decoder, 178, 371, 396, 422
- generalized Reed–Solomon code, *see* GRS code
- generator matrix (of convolutional codes), 477
 - catastrophic, 497
 - LFSM realization of, 510
 - systematic, 477, 517
- generator matrix (of linear codes), 27
 - systematic, 29
- generator polynomial
 - of cyclic codes, 245
 - of negacyclic codes, 323
 - of RS codes, 152
- Gilbert–Varshamov bound, 97, 137, 176, 181, 393
 - asymptotic, 107, 372
 - Lee-metric, 320, 330
- GMD decoder, 178, 371, 396, 422
- Golay code, 96, 136, 255
- Goppa code, 182, 389
- graph
 - adjacency matrix of, 398
 - bipartite, 362, 398
 - transfer matrix of, 399
 - Cayley, 406, 447
 - code, *see* graph code
 - connected, 397
 - directed, *see* digraph (and labeled digraph)
 - edge cut in, 397
 - expander, 404
 - Hamming, 427
 - hyper-, 445
 - incidence matrix of, 399
 - induced, 397
 - isomorphism, 47
 - labeled directed, *see* digraph (and labeled digraph)
 - Laplace matrix of, 399
 - matching in, 362
 - oriented, 400
 - Ramanujan, 409, 447
 - regular, 401
 - undirected simple, 396
- graph code, 412
 - approaching the Singleton bound, 421
 - decoding of, 414
 - error detection with, 440
 - generalized, 420
- Gray code, 321, 328
- Griesmer bound, 120, 136
- group, 521
 - Abelian, 521
 - code, 37, 299
 - commutative, 521
 - cyclic, 521
 - factor, 525
 - projective special linear, 409

- quotient, 525
- special linear, 409
- GRS code, 148
 - canonical generator matrix of, 167
 - canonical parity-check matrix of, 148
 - code locator of, 148
 - decoding of, *see* GRS decoding
 - doubly-extended, 163, 335
 - dual code of, 148
 - encoding of, 152, 177, 216
 - extended, 150, 336
 - dual code of, 163
 - Lee-metric, 304
 - list decoding of, *see* GRS list decoding
 - narrow-sense, 150
 - normalized, 149
 - primitive, 149
 - singly-extended, 150, 335
 - systematic generator matrix of, 167
 - triply-extended, 165, 337
- GRS decoding, 184
 - Berlekamp–Massey, 200, 217
 - bivariate interpolation, 269
 - Blahut’s time-domain, 217
 - Chien search in, 186, 215
 - erasure, 207, 216
 - with Euclid’s algorithm, 191, 215
 - extended, 210, 216
 - Forney’s algorithm for, 195, 215
 - key equation of, 186, 215
 - Lee-metric, 308
 - Lee-metric, 312
 - list, *see* GRS list decoding
 - Peterson–Gorenstein–Zierler, 189, 215
 - singly-extended, 210, 216
 - Sugiyama *et al.* (SKHN), 215
 - Welch–Berlekamp, 215, 217
 - equations of, 211, 215, 271, 291, 295
- GRS list decoding, 271
 - Guruswami–Sudan, 278, 296
 - Koetter–Vardy, 282, 296
 - radius, 271
 - Sudan’s, 274, 296
- Guruswami–Sudan algorithm, 278, 296
- Hadamard matrix, 45, 49, 406, 436, 447
- Hamming bound, *see* sphere-packing bound
- Hamming code, 32, 47
 - binary, 32
 - cyclic, 244, 254, 264
 - decoding of, 35
 - list, 291
 - dual code of, 41
 - extended binary, 32
 - list decoding of, 291
 - weight distribution of, 101, 121
- Hamming distance, 6
- Hamming graph, 427
- Hartmann–Tzeng bound, 265
- Hasse derivative, 87, 310, 329
 - of bivariate polynomials, 276
 - hyper-derivative, *see* Hasse derivative
 - hyper-graph, 445
- ideal, 522
- incidence matrix, 399
- infinite formal power series, 189, 237, 300, 474
 - bivariate, 487
- integer (of fields), 63
- integer programming, 103, 137
- integral domain, 522
- interleaver, 44
- interpolation, 76
 - bivariate, 270
 - noisy, 151, 177
 - rational, 211
- invertible element (in a ring), 190
- irreducible matrix, 445
- irreducible polynomial, 54, 90
 - enumeration of, 225
- Jacobi’s Four Square Theorem, 410
- Jensen’s inequality, 23
- Johnson bound, 107, 128, 139, 289
 - Lee-metric, 330
- Justesen code, 376
- key equation, 186, 215
 - Lee-metric, 308
- Koetter–Vardy algorithm, 282, 296
- König’s Theorem, 362
- Krawtchouk polynomial, 103, 124, 137
- Kronecker product (of matrices), 45, 428
- Kullback–Leibler distance, 111
- labeled directed graph, *see* digraph (and labeled digraph)
- Lagrange’s Theorem, 525
- Laplace matrix, 399
- Latin square, 351, 361
- Laurent series, 476, 507
- Law of Large Numbers, 11
- Law of Quadratic Reciprocity, 411, 449
- LDPC code, 362, 450
- Lee
 - adjacency matrix, 325
 - distance, 299
 - weight, 299, 448
- Legendre sequence, 80
 - autocorrelation of, 80
 - linear recurrence of, 239, 241
- Legendre symbol, 80, 447
- length (of codes), 5
- likelihood ratio, 20
- linear code, 26
 - decoding of, 33
 - encoding of, 28
 - over rings, 43, 299, 328, 478
- linear-feedback shift register (LFSR), 198, 217

- maximal-length, 237
- linear finite-state machine (LFSM), 472
 - catastrophic, 496, 516
 - deterministic, 517
 - irreducible, 473, 505
 - length–weight enumerator of, 487
 - lossless, 476, 508
 - observable, 496, 506, 519
 - reduced, 496, 506
 - response matrix of, 474, 519
- linear programming, 137
 - bound, 103, 110, 138
- linearized polynomial, 83, 353
- list decoding, 267
 - of alternant codes, 280, 328
 - error probability, 267
 - of GRS codes, *see* GRS list decoding
 - of Hamming codes, 291
 - radius, 267
 - bound on, 290
- log likelihood ratio, 20
- low-density parity-check code, 362, 450
- MacWilliams' identities, 104, 124
- matching (in graphs), 362
- matrix
 - adjacency, 398, 486
 - aperiodic irreducible, 445
 - Cauchy, 168, 336, 356, 362
 - circulant, 325, 330, 356, 362
 - companion, 73, 383, 510
 - complex conjugate transpose of, 326
 - direct product of, 45, 428
 - generator, 27, 477
 - incidence, 399
 - irreducible, 445
 - Kronecker product of, 45, 428
 - Laplace, 399
 - Lee adjacency, 325
 - parity-check, 29
 - primitive irreducible, 445
 - super-regular, 335
 - Sylvester-type Hadamard, 45, 49, 406, 436, 447
 - transfer, 399
 - Vandermonde, 75
 - inverse of, 166
- maximum-likelihood decoder, 8, 32, 140, 466
- MDS code, 94, 119, 148, 164, 334
 - almost (AMDS), 363
 - bound on the length of, 338
 - conjecture, 342, 363
 - dual code of, 119
 - near (NMDS), 363
 - over polynomial rings, 355
 - uniqueness of, 347
 - weight distribution of, 104
- MDS conjecture, 342, 363
- Mersenne prime, 77
- message node, 449
- message-passing algorithm (MPA), 451
- metric, 6
 - cover, 354, 362
 - Hamming, 6
 - Lee, 299
 - rank, 19, 353, 361
- minimal polynomial, 219, 241
- minimum distance, 6
 - computation complexity of, 48, 177
 - designed, 157, 163, 250
 - Lee, 299
 - relative, 104
- Möbius function, 224, 523
- MRRW bound, 110
- multiplication circuit, 153
- multiplicative order
 - in fields, 51
 - in groups, 521
 - in rings, 72, 206, 228
- mutual information, 23
- negacyclic code, 323, 330
- Newton's identities, 301, 328
- node
 - check, 449
 - message, 449
 - variable, 449
- normal basis, 240
- normal rational curve, 362
- order, *see* multiplicative order
- orthogonal array, 334, 361
- parity-check matrix, 29
- parity code, 27
- path (in graphs), 397
 - in digraphs, 453
- peak-shift error, 327
- perfect code, 96, 137, 256
 - Lee-metric, 319, 330
- period (of irreducible digraphs), 455, 502
- period (of sequences), 206, 237, 305
- Perron–Frobenius Theorem, 445, 518
- Peterson–Gorenstein–Zierler algorithm, 189, 215
- phase-shift keying (PSK), 327
- Plotkin bound, 37, 127, 131, 139, 294
 - Lee-metric, 326, 330
- polynomial, 51
 - bivariate, 268
 - characteristic, 73
 - check, 246
 - degree, 51
 - error-evaluator, 186
 - error-locator, 185
 - Lee-metric, 307
 - evaluation, 177, 216
 - exponent of, 206, 227, 247
 - factorization, 56, 90
 - generator, 152, 245, 323
 - interpolation, 76, 151, 177, 211, 270

- irreducible, 54, 90
 - enumeration of, 225
- Krawtchouk, 103, 124, 137
- linearized, 83, 353
- minimal, 219, 241
- monic, 52
- multivariate, 177, 295
- primitive, 228
 - enumeration of, 229
- quadratic, 78, 88
 - root of, 59
 - syndrome, 185
- power series, 189, 237, 300, 474
 - bivariate, 487
- Prime Number Theorem, 411, 449
- primitive element, 51, 61, 91
- primitive irreducible digraph, 455
- primitive irreducible matrix, 445
- primitive polynomial, 228
 - enumeration of, 229
- product code, 44, 178
- projective geometry, 47, 361
- Prouhet–Tarry problem, 329

- q -ary erasure channel, 15, 25, 126, 134, 391, 514
- q -ary symmetric channel, 4, 19, 24, 32, 110, 113, 117, 125, 133, 145, 378, 390, 394, 424, 467, 490
- quadratic polynomial, 78, 88
- Quadratic Reciprocity Law, 411, 449
- quadratic residue, 77, 239, 410, 447
 - Euler's criterion for, 80, 448
 - Gauss' criterion for, 448

- random coding, 137
 - Gallager's error exponent of, 143
- rate, 5
 - of convolutional codes, 477
 - of trellis codes, 462
- recurrence order, 197, 214
- redundancy, 27
- Reed–Muller code, 41, 48, 177, 260, 265
 - first-order, 41, 46, 120, 139, 327, 385, 408
- Reed–Solomon code, *see* RS code
- Reiger bound, 122
- remaindering circuit, 73, 153
- repetition code, 28
- ring, 522
- Roos bound, 265
- root, 59
 - of BCH codes, 163, 250
 - of bivariate polynomials, 268
 - computation, 90, 284, 296
 - of cyclic codes, 248
 - multiplicity, 60, 76
 - of RS codes, 152, 163, 250
- RS code
 - conventional, 151, 243
 - dual code of, 257
 - encoding of, 152, 178
 - extended, 152
 - generalized, *see* GRS code
 - generator polynomial of, 152
 - root of, 152, 163, 250
- self-dual code, 31
- sequence, 189
 - Legendre, 80
 - autocorrelation of, 80
 - linear recurrence of, 239, 241
 - linear-recurring, 198, 217, 237
 - M -, 237, 241
 - maximal-length, 237, 241
 - autocorrelation of, 87
 - periodic, 206, 305
 - trace, 236, 240
- Shannon Coding Theorem, 139
 - for BSC, 10
 - with error detection, 132
 - for q -ary erasure channel, 135
 - for q -ary symmetric channel, 117
- Shannon Converse Coding Theorem, 139
 - for BSC, 10
 - for q -ary erasure channel, 134
 - for q -ary symmetric channel, 113
- shift register, 198, 217, 237
- signal-to-noise ratio (SNR), 18
- simplex code, 41, 120
 - weight distribution of, 99
- Singleton bound, 94, 136, 332, 334
 - asymptotic, 105, 421, 451
 - cover-metric, 354, 362
 - rank-metric, 353, 361
- size (of codes), 5
- spectral-null code, 329
- sphere, 12
 - Lee, 317
 - volume, 95
- sphere-covering bound, 123
- sphere-packing bound, 95, 122, 136
 - asymptotic, 107
 - Lee-metric, 318, 330
- splitting field, 65
- stack algorithm, 520
- standard array decoding, 33
- state (in digraphs), 453
- subfield sub-code, 174
- subgroup, 521
 - normal, 522
- subring, 522
- Sudan's algorithm, 274, 296
- Sugiyama *et al.* (SKHN) algorithm, 215
- super-multiplicative sequence, 331
- super-regular matrix, 335
- Sylvester-type Hadamard matrix, 45, 49, 406, 436, 447
- synchronization error, 327
- syndrome, 34

- polynomial, 185
- tag (of edges), 459
- term rank (of arrays), 362
- trace
 - of elements in a finite field, 83
 - of matrices, 331, 514
 - sequence, 236, 240
- transfer matrix (of bipartite graphs), 399
- trellis code, 460
 - decoding of, 466
 - encoding of, 464
 - free distance of, 463
- triangle inequality, 6
- turbo code, 519
- union bound, 137
- unit element (in a ring), 190
- unity element, 521
- variable node, 449
- vertex (in graphs), 396
- Viterbi's algorithm, 468, 519
- volume
 - of Hamming spheres, 95
 - of Lee spheres, 317
- weight, 6
 - cover, 354, 362
 - distribution, *see* weight distribution
 - enumerator, 99, 486
 - Lee, 299, 448
- weight distribution, 99
 - of cycles in LFSMs, 487
 - of Hamming codes, 101, 121
 - of MDS codes, 104
 - of simplex codes, 99
- Weil's Theorem, 179
- Welch–Berlekamp
 - algorithm, 215, 217
 - equations, 211, 215, 271, 291, 295
- Wyner–Ash code, 512
- Zyablov bound, 373, 392, 413, 422, 438, 440