

Index

- action, 41
- adjacent, 304
- Adleman, 410
- AES, 376
- algebra, 2, 504
- algebraic
 - closure, 158
- algorithm, 277
 - APGZ, 191
 - basic, 255
 - Buchberger, 440
 - efficient, 27
 - Euclid–Sugiyama, 244
 - Euclidean, 143, 244
 - exponential, 284
 - polynomial, 284
 - subexponential, 284
 - Sudan, 267
- alphabet, 7
- ambiguity, 138
- anti-symmetric, 330
- arc, 327
- Arimoto, 191
- arrangement, 109
 - central, 109
 - essential, 109
 - graphic, 308
 - hyperplane
 - equivalent, 110
 - simple, 109
- array
 - orthogonal, 362, 364
 - linear, 364
- Artin, 502
- atom, 337
- atomic, 337
- attack
 - adaptive chosen-ciphertext, 374
 - adaptive chosen-plaintext, 374
 - chosen-plaintext, 374
 - ciphertext
 - chosen, 374
 - ciphertext-only, 374
 - known-plaintext, 374
 - related-key, 374
- authentication code, 393
 - MAC, 393
 - message, 393
- automorphism, 44
 - monomial, 44
 - permutation, 44
- axiom
 - circuit elimination, 313
 - independence augmentation, 310
- balanced, 102
- ball, 9
- basis, 13, 310
 - Gröbner, 436
 - reduced, 436
 - MDS, 453
 - ordered, 453
- Berlekamp, 302, 390, 450
- bilinear, 23
- binary cipher, 385
- binomial
 - Gaussian, 40, 323
- Boole, 278

- Bose, 173, 199, 367
- bound
 - asymptotic, 95
 - BCH, 173
 - Bush, 116, 364
 - Drinfeld–Vlăduț, 500
 - Feng-Rao, 518, 523
 - Gilbert, 84
 - Gilbert–Varshamov, 86
 - greatest lower, 334
 - Griesmer, 76
 - Hamming, 81
 - Hasse–Weil–Serre, 497
 - HT, 180
 - Johnson, 260
 - Johnson–Guruswami, 260
 - Jouhanson, 95
 - least upper, 334
 - order, 518, 523
 - Plotkin, 79
 - asymptotic, 88
 - redundancy, 87
 - Roos, 184
 - shift, 523
 - Singleton, 71
 - asymptotic, 88
 - sphere-covering, 82
 - sphere-packing, 81
 - Tsfasman–Vlăduț–Zink, 500, 522
 - TVZ, 500, 522
 - Varshamov, 84
- box
 - delay, 387
- Brickell, 417
- bridge, 308
- broken
 - partially, 373
 - totally, 373
- Buchberger, 440
- Busch, 367
- capability
 - error-correcting, 28, 260
- capacity, 2, 38
- certificate, 284
- chain
 - extension of, 338
 - maximal, 338
 - of length, 330
- channel
 - binary symmetric, 35
 - discrete memoryless, 35
 - q-ary symmetric, 35
- character, 104
 - principal, 104
- characteristic, 156
- Chaudhuri, 173, 199
- Chen, 446
- Chien, 450
- Chinese remainder, 163
- cipher
 - alphabetic substitution, 371
 - block, 370
 - Caesar, 369
 - Feistel, 376
 - iterative block, 376
 - permutation, 371
 - self-synchronizing stream, 386
 - stream, 385
 - substitution, 370, 371
 - transposition, 371
 - Vigenère, 371
- ciphertext, 369, 370
- confusion, 371
 - diffusion, 371
- circuit, 310
 - Boolean, 278, 282
- class
 - parallel, 321
- clause, 280
- closed
 - algebraically, 158
- closed set, 310
- closure, 310
 - algebraic, 470
- cocircuit, 312
- code
 - affine variety, 452
 - algebraic geometry, 494
 - alternant, 225
 - augmented, 54
 - BCH, 174
 - narrow sense, 174
 - primitive, 174
 - block, 7
 - Cauchy, 75
 - generalized, 76
 - concatenated, 68
 - constant weight, 79
 - convolutional, 7
 - cycle, 308
 - degenerate, 107, 324

- dual, 24
 - complementary, 24
 - self, 24
 - weakly self, 24
- equidistant, 79
- error-correcting, 1
- evaluation, 514
- expurgated, 55
- extended, 51
- extension by scalars, 117, 215
- geometric Goppa, 495
- geometric Reed–Solomon, 494
- Golay, 62
 - binary, 61, 62, 178
 - ternary, 26, 178
- good, 497
- Goppa, 226
 - classical, 495
- graph, 308
- Hadamard, 23
- Hamming, 5
 - q -ary, 22, 177
- hexa, 499
- hull, 24
- inner, 68
- lengthened, 55
- linear, 11
- maximum distance separable, 71
- MDS, 71
 - almost, 71
 - near, 73
- Melas, 185
- Muller, 519
- one point, 515
- orthogonal, 24
 - self, 24
- outer, 68
- product, 63
 - direct, 63
 - tensor, 63
- projective, 324
- punctured, 49, 120
- Reed, 494, 519
- Reed–Muller, 519
 - q -ary, 235
 - binary, 58
- Reed–Solomon, 74, 201
 - extended, 202
 - generalized, 204
- residual, 77
- restricted, 50
 - restriction by scalars, 173, 215
 - reverse, 150
 - shortened, 52, 120
 - simplex, 22, 78, 98, 178
 - simplified, 342
 - sub, 12
 - even weight, 12
 - subfield, 173, 215
 - super, 12, 173, 215
 - trivial, 13
 - Zetterberg, 185
- codeword, 7
 - consistent
 - t , 260
 - minimal, 348
 - nearest, 28
- codimension, 322
- coding
 - source, 1
- coefficient, 436
 - leading, 436
- color, 305
- combinatorics, 2
- comparable, 330
- complexity
 - data, 374
 - depth, 283
 - implementation, 376
 - linear, 390
 - space, 277, 283
 - time, 277, 283
 - work, 277
- component, 471
 - connected, 308
- compression
 - data, 1
- computation
 - secure multi-party, 427
- conjecture
 - MDS, 117, 139
- connected, 307
- connection, 388
- consecutive, 175
- constant
 - S-box, 382
 - structure, 454
- constraints, 364
- construction
 - $(a + x|b + x|a + b - x)$, 60
 - $(u + v|u - v)$, 58
 - $(u|u + v)$, 57

- $(u|v)$, 56
- Plotkin, 57
- contraction
 - matroid, 316
- Cook, 302
- Cooper, 445
- coordinate
 - homogeneous, 321
- coordinates
 - homogeneous
 - standard, 322
- correlation
 - immune, 391
- coset, 29, 144
 - cyclotomic, 165
 - leader, 29
- cover, 333
- covering
 - Artin–Schreier, 502
- Cramer, 192
- criterion
 - product, 444
- cryptanalysis, 373
 - algebraic, 384
- cryptography, 373
 - multivariate, 416
- cryptology, 373
- cryptomorphic, 341
- cryptosystem, 368
 - asymmetric, 369
 - knapsack, 416
 - public, 369
 - RSA, 408, 410
 - symmetric, 368
- curve
 - affine, 470
 - algebraic, 469
 - Fermat, 473
 - good
 - asymptotically, 499
 - Hermitian, 473
 - Klein, 474
 - modular, 500
 - plane, 470
 - projective, 471
 - regular, 472
 - singular, 472
 - non, 472
- cycle, 308, 482
 - degree, 482
 - intersection, 482
- cyclic, 45, 141
- Daemen, 376
- decision
 - hard, 5
 - soft, 5
- decodable
 - (t, l) , 260
- decoder, 28
 - brute force, 30
 - complete, 28
 - coset leader, 30
 - half the minimum distance, 28
 - incomplete, 4
 - list, 5, 31, 260
 - (t, l) , 260
 - minimum distance, 28
 - nearest neighbor, 28
- decoding
 - ambiguity, 138
 - correct, 28
 - erasure set, 295
 - error, 28
 - failure, 28
 - formal, 450
 - information set, 290
 - online, 450
- decryption, 369
 - El Gamal, 415
 - McEliece, 420
 - Niederreiter, 422
 - RSA, 411
- defect
 - Singleton, 71
- degree, 471
 - weighted, 267, 508
- deletion, 350
 - matroid, 316
- Delsarte, 95, 224
- demodulation, 5
- dependent, 310
- depth, 283, 362
- derivation, 486
- derivative
 - formal, 157
 - partial, 471
- DES, 376
 - triple, 380
- detection
 - error, 18
- diagram

590

Hasse, 333, 338
 Diffie, 407, 415
 dimension, 11
 distance
 bounded, 28
 strict, 29
 Hamming, 8
 minimum, 9
 designed, 174
 distribution
 weight, 96
 division
 with quotient, 143
 with remainder, 143
 divisor, 484
 canonical, 488
 degree, 484
 effective, 484
 greatest common, 143
 intersection, 484
 linearly equivalent, 485
 principal, 485
 support, 484
 DLP, 409
 domain
 Euclidean, 143
 order, 523
 Drinfeld, 500, 522
 dual, 24, 323
 self
 formally, 108
 quasi, 47
 duality
 Delsarte, 224

 edge, 304
 acyclic, 308
 bad, 346
 El Gamal, 368, 414
 elimination
 Gaussian, 14
 embedded, 321
 encoder, 8
 systematic, 16
 encoding, 13, 149
 encryption, 369
 confusion, 379
 diffusion, 379
 El Gamal, 414
 McEliece, 419
 Niederreiter, 421

Index

RSA, 411
 end, 304
 enumerator
 weight, 97
 average, 102
 coset leader, 29
 extended, 118
 generalized, 128
 homogeneous, 97
 equality
 modular, 338
 equation
 defining, 470, 471
 Euler, 472
 field, 442
 Key, 195
 equivalent, 44, 279
 computational, 285
 generalized, 44
 monomial, 44
 permutation, 44
 erasure, 4, 31
 error, 28
 decoding, 3
 number of, 18, 27
 undetected, 135
 Euclid, 143, 244
 Euler, 163, 472
 evaluation, 203
 expand, 376
 explicit, 18, 320
 exponent
 complexity, 287
 universal, 417

 factor
 trivial, 471
 failure
 decoding, 4
 family
 almost universal, 399
 feedback, 388
 Feistel, 376
 Feng, 518, 522, 523
 Fermat, 473
 field
 function, 468
 Galois, 158
 prime, 155
 splitting, 158
 sub, 155

- finite
 - locally, 330
- Fitzgerald, 452
- flat, 310
- force
 - brute, 374
- form
 - differential, 487
 - regular, 488
 - echelon, 14
 - reduced row, 14
 - normal
 - algebraic, 280
 - conjunctive, 280
- formula
 - Boolean, 279
 - closed, 192
 - deletion–contraction, 307, 317
 - deletion–restriction, 350
 - Forney, 195
 - Hurwitz–Zeuthen, 502
 - Möbius inversion, 332
 - Plücker, 489
 - Stirling, 90
- Forney, 195
- Fourier, 186
- free
 - square, 228
- Frobenius, 219
- function
 - Boolean, 280
 - degree, 506
 - entropy, 88
 - q -ary, 88
 - Euler’s phi, 336
 - Möbius, 161, 331, 336
 - one-way, 408
 - trapdoor, 408
 - order, 506
 - pole, 475
 - rational, 468
 - regular, 469
 - state, 386
 - sum, 332
 - generalized power, 445
 - symmetric, 188
 - weight, 506
 - zero, 475
- Gödel, 302
- Galois, 219
- gap, 491
 - non, 491
 - Weierstrass, 491
- Garcia, 502, 522
- gate, 282
 - Boolean, 279
- Gauss, 14, 40
- generation
 - key
 - El Gamal, 414
 - McEliece, 419
 - Niederreiter, 421
 - RSA, 411
- generator
 - clock-controlled, 391
 - nonlinear combination, 391
 - nonlinear filter, 391
 - shrinking, 392
- generic, 192
- genus, 71, 489
- Gilbert, 84, 86
- girth, 308
- Golay, 26, 61, 62, 178
- good
 - asymptotically, 88
- Goppa, 226, 522
- Gorenstein, 191
- Gröbner, 436
- graph, 304
 - coloring, 305
 - connected, 308
 - contraction, 307
 - deletion, 307
 - planar, 304
 - simple, 304
- greatest common divisor, 244
- Griesmer, 76
- group
 - automorphism, 44
 - monomial, 44
 - permutation, 44
 - dihedral, 151
 - Galois, 219
 - general linear, 40
 - symmetric, 42
- Guruswami, 260
- Hadamard, 23
- Hamming, 2, 5, 8, 81, 95
- Hartmann, 180, 450
- Hasse, 497

592

Helleseth, 446
 Hellman, 407, 415, 416
 Hermite, 473, 522
 hierarchy
 weight, 126
 Hilbert, 468
 Hocquenghem, 173, 199
 homogeneous, 471
 Hurwitz, 502
 hyperplane, 109, 322
 homogeneous, 109
 projective, 322
 ideal, 143, 435
 CRHT-syndrome, 446
 generated, 143
 leading, 436
 prime, 468
 vanishing, 467
 zero-dimensional, 441
 identity
 generalized Newton, 188, 449
 MacWilliams, 103, 139
 Ihara, 522
 image, 42
 impersonation, 393
 implicit, 18, 320
 incident, 304, 322
 index, 364
 speciality, 491
 inequality
 semimodular, 338
 triangle, 8
 input, 280
 interpolation, 266
 Lagrange, 207
 interval, 330
 invariant, 42, 46, 219
 Galois, 219
 permutation, 46
 inversion, 382
 irreducible
 absolutely, 471, 493
 isometry, 42
 linear, 42
 isomorphic
 graph, 305
 poset, 337
 isomorphism
 of matroids, 311
 isthmus

Index

graph, 308
 Johnson, 260
 join, 334
 juxtaposition, 56
 Kasiski method, 373
 Katsman, 139
 kernel, 253
 key
 decryption, 369, 408
 dual, 379
 encryption, 369, 408
 private, 407
 public, 407
 schedule, 376
 secret, 369
 size, 375
 weak, 370, 379
 semi, 379
 keystream, 385
 Klein, 474, 522
 Lagrange, 207
 Landau, 90
 lattice, 334
 geometric, 337
 modular, 337
 of flats, 341
 rank, 337
 semimodular, 337
 uniform, 342
 Lax, 452
 Leibniz, 157, 486
 length, 7
 level, 338
 levels, 364
 Levin, 302
 LFSR, 385
 line
 affine, 320
 at infinity, 321, 472
 parallel, 320
 projective, 320
 tangent, 471
 linear complexity, 247
 linearization, 431
 lines, 320
 literal, 280
 locator, 188
 error, 190, 255

- logarithm, 159
 - Zech, 159
- loop
 - graph, 304
- Möbius, 331
- machine
 - Turing, 278
- MacWilliams, 103, 139
- Manin, 92
- map
 - \mathbb{F}_2 -linear, 382
 - authentication, 393
 - evaluation, 201–203, 234, 452
 - Frobenius, 219, 493
 - trace, 223
- Massey, 390
- matching, 299
- matrix
 - Cauchy, 75
 - generalized, 75
 - diagonal, 42
 - generator, 13
 - incidence, 299, 308
 - MDS, 453
 - monomial, 42
 - parity check, 18
 - permutation, 42
 - simplified, 342
 - Sylvester, 477
 - syndrome, 254, 517
- matroid, 309
 - cographic, 313
 - cycle, 313
 - dual, 311
 - element, 310
 - loop, 310
 - parallel, 311
 - free, 310
 - graphic, 313
 - realizable, 312
 - representable, 312
 - simple, 311
 - uniform, 310
- Mattson, 186
- maximum, 332
- McEliece, 302, 368
- meet, 334
- Melas, 185
- memory, 277, 374
- Merkle, 416
- message, 8
- method
 - Fitzgerald–Lax, 452
 - Stinson’s composition, 400
- minimum, 332
- modulation, 5
- monomial, 435
 - leading, 436
- monotone, 336
 - strictly, 336
- morphism
 - algebra, 514
 - graph, 305
 - of a matroid, 311
- Muller, 58, 235
- multiplicity
 - intersection, 481
- Nash, 302
- neighbor, 304
- Newton, 156, 188
- Niederreiter, 368
- node, 282
- nondegenerate, 23
- normal form, 438
- normalization, 516
- NP, 284
- Nullstellensatz, 468
- operation
 - elementary, 277
 - elementary row, 14
- optimal, 81
- order, 361, 362, 487
 - admissible, 435, 504
 - block, 435
 - bound, 516
 - elimination, 435
 - lexicographic, 435, 504
 - degree reverse, 435
 - total degree, 505
 - weighted degree, 508
 - monomial, 435, 504
 - multiplicative, 435, 504
 - product, 435
 - reduction, 504
 - term, 504
 - total, 435
 - well, 435
- ordering: see order, 435
- output, 280, 385

594

Index

- pad
 - one-time, 385
- pair
 - critical, 439
 - error-correcting, 255
- parallel
 - graph, 304
- parameter, 11
 - local, 475
 - uniformizing, 475
- parametric, 320
- parity check, 18
- partial order, 330
- path, 307
- pay-off, 395
- perfect, 82
- period, 371, 390
- periodic, 390
 - ultimately, 390
- permutation
 - substitution, 381
- Peterson, 191
- philosophy
 - Cooper, 445, 465
- pivot, 14, 16
- Plücker, 489
- plaintext, 369, 370
- plane
 - affine, 320
 - projective, 321
- Plotkin, 79, 94
- point
 - anti-fixed, 379
 - at infinity, 321, 470, 471
 - fixed, 379
 - rational, 349, 470
 - regular, 471
 - singular, 471
- points, 320
- polynomial
 - characteristic, 343, 388
 - two variable, 343
 - chromatic, 305
 - coboundary, 343
 - cyclotomic, 164
 - defect, 344
 - dichromatic, 345
 - error-evaluator, 195
 - error-locator, 190, 449
 - general, 447
 - generator, 146
 - locator, 188
 - Möbius, 346
 - Mattson–Solomon, 186
 - minimal, 162
 - parity check, 152
 - Poincaré, 343
 - primitive, 159
 - syndrome, 194
 - Tutte, 314
 - Whitney rank generating, 314
- poset, 330
- position
 - error, 27, 191
 - general, 327
- Prange, 199
- primitive, 159
 - cryptographic, 370
- principle
 - inclusion/exclusion, 111
 - of inclusion/exclusion, 335
- probability, 2
 - averaged, 136
 - cross-over, 35
 - deception, 394
 - decoding
 - ambiguity, 138
 - correct, 36
 - erasure, 137
 - error, 36
 - failure, 36
 - error, 2, 36
 - undetected, 135, 136
 - retransmission, 136
- problem
 - decision, 284
 - Diffie–Hellman, 415
 - discrete log, 284
 - discrete logarithm, 409, 413
 - DLP, 409, 413
 - factorization, 284
 - football pools, 83
 - graph isomorphism, 285
 - multivariate quadratic, 416
 - RSA, 412
 - subset sum, 416
- processing, 374
- product, 157
 - direct, 63
 - inner, 23
 - Kronecker, 63
 - star, 181, 203

- tensor, 63
- projective plane, 321
- property
 - Jordan–Hölder, 338
- pseudorandom, 391
- quotient, 143
- radical, 468
- radius
 - covering, 29
 - decoding, 28, 260
- rank
 - of a matroid, 310
 - of a subset, 310
- Rao, 367, 518, 522, 523
- rate
 - error, 36
 - information, 2, 3, 7
- rational, 321
- rational point, 476
- reciprocal, 151
 - monic, 151
- reduced, 234, 521
- reducible, 471
 - polytime, 285
- redundant, 1, 7
- Reed, 58, 201, 235, 446
- reflexive, 330
- register
 - linear feedback shift, 385
- relation
 - reverse, 333
- remainder, 143
- representation
 - exponential, 159
 - principal, 156
- residue, 489
- restriction, 350
- resultant, 478
- retransmission, 18, 135
- reverse, 150
- Riemann, 490
- Rijmen, 376
- Rijndael, 376
- ring
 - coordinate, 468
 - factor, 144
 - local, 469
- Rivest, 410
- Roch, 490
- Roos, 184
- root
 - finding, 266
- RSA, 368
- rule
 - Leibniz, 486
 - product, 486
- S-box, 379
- s-polynomial, 437
- satisfiable, 279
- scheme
 - El Gamal, 409
 - encryption, 368
 - asymmetric, 407
 - symmetric, 369
 - Rabin, 409
 - secret sharing, 403
 - split-knowledge, 406
 - threshold, 402
- Schreier, 502
- secrecy
 - perfect, 375
- security
 - computational, 375
 - provable, 375
 - state-of-the-art, 375
 - unconditional, 375
- seed, 386
- semigroup
 - Weierstrass, 491, 522
- sequence, 390
 - asymptotic, 87
 - initial state, 388
 - linear recurring, 387
 - homogeneous, 388
 - maximal period, 390
 - super increasing, 417
- Serre, 497, 522
- set
 - access, 405
 - general, 405
 - algebraic, 467
 - irreducible, 468
 - check, 16, 293
 - defining, 170
 - complete, 170
 - generating, 183
 - information, 16
 - root, 170
 - shift, 181

zero, 170, 467
 Shamir, 402, 410, 417
 Shannon, 2, 38
 shift
 cyclic, 141
 sieve
 number field, 428
 simplification, 305, 311
 Singleton, 71
 size, 283, 364
 Solomon, 186, 201, 494
 solution
 formal, 450
 generic, 450
 one-step, 450
 space, 322
 ciphertext, 369, 408
 key, 369, 370, 393, 408
 message, 393
 null, 254
 plaintext, 369, 408
 projective, 322
 spectrum
 weight, 96
 sphere, 9
 spoiling, 55
 square
 Latin, 361
 Greek, 362
 mutually orthogonal, 362
 standard
 advanced encryption, 376
 AES, 376
 data encryption, 376
 DES, 376
 state, 385
 initial, 386
 source, 393
 Stevens, 450
 Stichtenoth, 502, 522
 Stinson, 400
 storage, 374
 strategy
 wide trail, 382, 426
 strength, 364
 subcode
 minimal, 348
 subgraph, 307
 subspace
 affine, 322
 substitution, 371, 394

Sudan, 267
 Sugiyama, 244
 sum
 direct, 56
 support, 11, 126, 484
 Sylvester, 477
 symmetric, 23
 syndrome, 18, 30, 517
 known, 190, 445
 unknown, 445
 system
 covering, 293
 projective, 324
 equivalent, 325
 simple, 324
 systematic, 16, 149

 table
 truth, 279
 tag
 authentication, 393
 term, 436
 leading, 436
 theorem
 principal, 477
 residue, 490
 Riemann–Roch, 490
 theory
 class field, 522
 elimination, 479
 information, 2
 Tilborg, van, 302
 time, 374
 tower
 Garcia–Stichtenoth, 522
 first, 502
 second, 503
 transform
 discrete Fourier, 186
 Hadamard, 105
 transformation
 decryption, 370
 encryption, 370
 fractional, 211
 projective, 325
 round, 376
 transitive, 330
 trapdoor, 408
 trivial, 142
 Truong, 446
 Tsfasman, 139, 500, 522

- Turing, 278
- Tzeng, 180, 450, 522

- uniform, 38

- Valiant, 302
- valuation, 487
 - discrete, 475
- value, 188
 - error, 28
- Vandermonde, 73
- Vardy, 302
- variety
 - affine, 349, 468
 - dimension, 468
 - projective, 469
- Varshamov, 86
- vector
 - error, 18, 27
- Venn diagram, 6
- vertex, 282, 304
- Vlăduț, 500, 522

- Wei, 522
- Weierstrass, 491, 522
- weight, 11, 126
 - constant, 23
 - even, 12
 - generalized, 126
 - minimum, 11
 - multivariate, 508
 - q, 237
- Weil, 497
- Whitney number, 347
 - first kind, 347
 - second kind, 347
- word
 - message, 8
 - source, 8

- zero
 - multiplicity, 268
- Zetterberg, 185
- Zeuthen, 502
- Zierler, 191
- Zink, 500, 522