

Index

- alphabet, 5
 - channel, 6
 - code, 5
- alternant code, 192
- basis, 42
- BCH code, 161
 - Chien–Choy generalized, 211
 - narrow-sense, 161
 - primitive, 161
- bound
 - Gilbert–Varshamov, 82, 107
 - Griesmer, 101
 - Hamming, 83
 - linear programming, 103, 104
 - Plotkin, 95, 96
 - Reiger, 150
 - Singleton, 92
 - sphere-covering, 80
 - sphere-packing, 83
- burst, 150
- burst error, 150
- Cauchy–Schwarz inequality, 95
- channel
 - binary symmetric, 7
 - q -ary symmetric, 7
 - useless, 14
- characteristic, 21
- check digits, 59
- circulant, 186
- co-prime, 23
- code
 - alternant, 192
 - BCH, 159
 - block, 5
 - burst-error-correcting, 150
 - concatenated, 121
 - constacyclic, 157
 - constant-weight binary, 110
 - cyclic, 133
 - Delsarte–Goethals, 99
 - dual, 45
 - equivalent, 56
 - exactly u -error-correcting, 13
 - exactly u -error-detecting, 12
 - expurgated, 69
 - expurgated QR, 187
 - first order Reed–Muller, 121, 118
 - generalized Reed–Solomon, 191
 - Golay, 91, 92
 - Goppa, 196
 - Hadamard matrix, 98
 - Hamming, 84, 87
 - inner, 122
 - irreducible cyclic, 157
 - irreducible Goppa, 196
 - Kerdock, 99
 - linear, 39, 45
 - l -burst-error-correcting, 150
 - ℓ -quasi-cyclic, 157
 - MacDonald, 110
 - MDS, 93
 - negacyclic, 157
 - nonlinear, 96
 - Nordstrom–Robinson, 98
 - optimal, 76
 - outer, 122
 - perfect, 84
 - Preparata, 99
 - punctured, 79
 - QR, 180

code (*cont.*)

- quadratic-residue, 159, 180
 - quasi-cyclic, 157
 - r th order Reed–Muller, 121
 - Reed–Muller, 99, 118
 - Reed–Solomon, 159, 171
 - repetition, 3, 45
 - residual, 100
 - self-dual, 46
 - self-orthogonal, 46
 - separable Goppa, 200
 - simplex, 85, 88
 - Srivastava, 212
 - trace, 124
 - u -error-correcting, 13
 - u -error-detecting, 12
 - zeroth order Reed–Muller, 121
- code locator, 191
- codeword, 5
- coding
- algebraic, 4
 - channel, 1
 - source, 1
- communication channel, 6
- memoryless, 6
- complete set of representatives, 31
- congruent, 19
- constacyclic code, 157
- constant-weight binary code, 110
- correction
- burst-error, 133
 - random-error, 133
- coset, 59
- q -cyclotomic, 31
- coset leader, 60
- crossover probability, 7
- cyclic, 133
- run of 0, 147
- cyclic code, 133
- irreducible, 157
 - ℓ -quasi, 157
- cyclically shifting, 133
- cyclotomic coset, 31
- decoding, 8
- of BCH codes, 168
 - complete, 8, 10
 - of cyclic codes, 145
 - error trapping, 147
 - incomplete, 8, 10
 - list-, 202

- maximum likelihood, 8
 - minimum distance, 10
 - nearest neighbour, 10
 - Sudan, 202
 - syndrome, 62
- degree, 23
- Delsarte, 125
- detectable, 155
- dimension, 42, 45
- direct sum, 115
- discrete Fourier transform, 73, 210
- distance, 9
- Hamming, 8
 - minimum, 11
 - relative minimum, 75
- distance distribution, 103
- double-adjacent-error pattern, 156
- dual code, 45
- encoding, 58
- equivalent codes, 56
- error, 1
- pattern, 61
 - string, 61
 - trapping, 147
- error locator polynomial, 168, 169
- error pattern, 61
- Euclidean algorithm, 170
- field, 17
- finite, 19
- finite field, 19
- forward channel probabilities, 6
- generating idempotent, 155
- generating set, 41
- generator, 27, 135
- generator matrix, 52
- in standard form, 52
- generator polynomial, 138
- Golay code, 91, 92
- binary, 91
 - extended binary, 89
 - extended ternary, 91
 - ternary, 92
- Goppa code, 196
- irreducible, 196
 - separable, 200
- greatest common divisor, 23
- group theory, 59

- Hadamard matrix, 98
- Hamming code, 84, 87
 - binary, 84
 - extended binary, 86
 - q -ary, 87
- Hamming distance, 8
- Hamming weight, 46
 - enumerator, 74
 - minimum, 48
- hexacode, 67

- ideal, 134
 - principal, 135
- idempotent, 155, 186
- identity
 - additive, 18
 - multiplicative, 18
- information rate, 5
- inner code, 122
- integer ring, 19
- irreducible, 23

- Krawtchouk expansion, 102
- Krawtchouk polynomial, 102

- Lagrange interpolation formula, 38
- least common multiple, 23, 160
- lengthening, 114
- linear code, 39, 45
- linear combination, 41
- linear space, 39
- linear span, 41
- linearly dependent, 41
- linearly independent, 41
- list-decoding, 202
- Lloyd polynomial, 105

- MacWilliams identity, 74, 100
- matrix
 - generator, 52
 - Hadamard, 98
 - parity-check, 52
- Mattson–Solomon polynomial, 210
- maximum distance separable, 93
- maximum likelihood decoding, 8
- MDS code, 93
 - nontrivial, 94
 - trivial, 94
- message digits, 58

- minimal polynomial, 30
- minimum distance, 11
 - relative, 75
- minimum distance decoding, 10
- Möbius function, 38, 201
- modulo, 19
- monic, 23

- narrow-sense, 161
- nearest neighbour decoding, 10
- negacyclic, 157
- nonlinear code, 96

- optimal, 151
- order, 27
- orthogonal, 43
- orthogonal complement, 43
- outer code, 122

- (\mathcal{P}, k, t) -polynomial, 203
- (\mathcal{P}, k, t) -reconstruction, 202
- (\mathcal{P}, k, t) -sequence, 205
- parameters, 11
- parity-check coordinate, 78
- parity-check matrix, 52
 - in standard form, 52
- parity-check polynomial, 144
- polynomial, 19, 22
 - error locator, 168
 - generator, 138
 - Goppa, 196
 - Krawtchouk, 102
 - Lloyd, 105
 - Mattson–Solomon, 210
 - minimal, 30
 - (\mathcal{P}, k, t) -, 203
 - parity-check, 144
 - reciprocal, 142
 - syndrome, 169
- prime, 23
- primitive element, 27
- product
 - dot, 43
 - Euclidean inner, 43
 - Hermitian inner, 67
 - inner, 43
 - scalar, 43
 - symplectic inner, 68
- propagation rules, 113
- puncturing, 114

- quadratic nonresidue modulo p , 175
- quadratic reciprocity, 185
- quadratic residue modulo p , 175
- quadratic-residue code, 180
- quasi-cyclic, 157

- r -singular point, 203
- radius, 80
- reciprocal polynomial, 142
- reducible, 23
- redundancy, 1, 59
- Reed–Muller code, 118
- Reed–Solomon code, 171
 - generalized, 191
- Reiger bound, 150
- remainder, 20, 23
 - principal, 20, 23
- repetition code, 3, 45
- ring, 19
 - commutative, 19
 - integer, 19
 - polynomial, 22
 - principal ideal, 135
- row
 - echelon form, 49
 - equivalent, 49
 - operation, 49
- RS code, 171
 - punctured, 191

- scalar multiplication, 40
- self-dual code, 46
- self-orthogonal code, 46
- shortening, 127
- simplex code, 85, 88
- span, 41

- spanning set, 41
- sphere, 80
- standard array, 60
 - Slepian, 60
- standard decoding array, 62
- standard form, 52
- subcode, 70, 114
 - subfield, 123
- subfield, 21
- subspace, 40
- support, 100
- symmetric channel, 7
- syndrome, 62
 - look-up table, 62
- syndrome decoding, 62
- syndrome polynomial, 169

- tetracode, 108
- trace, 66
- trace code, 124

- $(\mathbf{u}, \mathbf{u} + \mathbf{v})$ -construction, 116

- Vandermonde product, 158
- vector addition, 40
- vector space, 39

- weight
 - Hamming, 46
 - symplectic, 68
- weight enumerator, 74

- x -degree, 203

- y -degree, 203

- Zech's log table, 29