

Index

- (n, r) -forms, 103
- RM -equivalence, 101
- adder, 273
- Advanced Encryption Standard, AES, 283
- algebra over a field, 18
- algebraic degree
 - of a function, 42
 - of a mapping, 249
- algebraic system, 1
- algorithm
 - deciphering, 281
 - decoding, 118
 - enciphering, 281
 - Euclidean, 13
 - Matsui 1, 296
 - Matsui 2, 296
- almost equivalent mappings, 105, 238
- array
 - of a code
 - standard, 118
 - orthogonal, 206
- attack on the key, 283
- automorphism
 - Frobenius, 30
 - internal, 6
 - of a field over another field, 30
 - of a group, 4
- avalanche criterion, 261
 - strict, 261
 - strong of order t , 262
- average
 - complexity, 285
 - reliability, 285
- ball, 111
- basis
 - biorthogonal, 189
 - canonical, 17
 - normal, 25
 - of a vector space, 17
 - polynomial, 25
- bent set, 173
- bent function, 166
 - partial, 173
- bent mapping, 243
 - almost, 247
- bias, 295
- binary operation, 1
 - associative, 1
- block cipher, 281
 - key, 281
- Boole, George, ix
- Boolean function
 - covering sequence of, 74
 - level of, 74
 - nontrivial, 74
 - degeneration structure of, 103
 - derivative of, 55
 - numerical normal form of, 50
 - weight of, 45
- boomerang method, 303
- bound
 - Bose–Chaudhuri–Hocquenghem (BCH), 133
 - Elias', 112
 - Hamming's, 111
 - Singleton's, 111
 - sphere-packing, 111
- branching, 70
 - linear, 71
- Burnside lemma, 80
- canonical factorization of a polynomial, 15
- center of a group, 7
- character
 - additive, 25
 - canonical, 25
 - distinguishing, 5
 - multiplicative, 26
 - nontrivial, 5
 - of a group, 4
 - trivial, 5
- characteristic
 - difference, 300
 - function, 239
 - global avalanche, 266
 - linear, 295

- of a field, 11
 - polynomial
 - of an LRS, 272
 - of a register, 273
- check polynomial, 123
- check symbols, 111
- cipher
 - A5, 70
 - stream, 70, 287
 - symmetric, 65
- cipher algorithm
 - DES, 283
 - GOST 28147-89, 283
- cipher standard
 - DES, 283
 - GOST 28147-89, 283
- ciphertext, 281
 - block, 281
 - intermediate, 282
- class
 - cyclotomic, 35, 54
 - equivalence, 2
 - Maiorana–McFarland, 173
 - of affine functions, 43
 - of maximum-nonlinear functions
 - \mathcal{M} , 173
 - complete, 172
- code
 - $[n, k, d]$, 107
 - automorphism group of, 110
 - binary Golay, 135, 136
 - complementary, 123
 - completely regular, 254
 - constructive distance of, 134
 - cyclic, 120
 - nonzeros, 123
 - primitive, 122
 - with two zeros, 259
 - zeros, 123
 - dual, 109
 - equidistant, 117
 - generator matrix of, 109
 - Hadamard, 190
 - Hamming's, 116
 - Kerdock, 159
 - linear
 - block, 107
 - determined by a mapping, 252
 - maximum length, 117
 - minimum distance of, 107
 - parity-check matrix of, 109
 - perfect, 117
 - Preparata, 160
 - primitive BCH, 134
 - narrow-sense, 134
 - punctured, 142
 - Reed–Muller, 139
 - set of code words of, 109
 - simplex, 117, 132
 - systematic, 111
 - uniformly packed, 254
 - weight function of, 114
 - weight spectrum of, 114
 - with maximum distance, 111
- code dimension, 107
- code distance, 107
 - dual, 250
 - external, 250
- code rate, 107
- code word, 107
- coefficient
 - Fourier, 46
 - Walsh–Hadamard, 46
- coefficients
 - spectral, 46
- communication channel
 - discrete, 108
 - quantum-cryptographic, 203
- completion of a class, 172
- complexity
 - linear, 276
 - average of statistical classification procedure, 285, 286
- confusion, 65
- conjugate set, 6
- constant, 12
- constructive enumeration problem, 88
- coordinates of a vector, 17, 37
- correlation
 - attack, 294
 - decoding, 152
- coset
 - leader, 118
 - of a code, 118
 - of a subgroup, 3
- covering radius of a code, 107
- covering sequence
 - perfect, 234
 - simple, 228
- crosscorrelation, 58
- cryptanalysis
 - linear, 295
 - method, 281
 - statistical, 281
- decision area, 284
- decoder
 - complete, 119
 - incomplete, 119
- decoding Hamming code, 117
- deep hole, 166
- delay device, 273
- Delsarte's inequality, 255
- dependence
 - essential, 38
 - quasi-linear, 223

- derivative
 - of a Boolean function, 55
 - of a polynomial, 16
- deviation, 295
- difference table, 239
- diffusion, 65
- dimension of a space, 18
- Dirac δ -function, 46
- discrepancy bits, 277
- distance
 - between Boolean functions, 45
 - from a Boolean function to a set, 49
 - Hamming, 44
- distance of uniqueness, 284
- distributed computations, 203
- distribution of random variables, 196
- distributivity, 7
- divisor of an element of a ring, 9
- domain, 7
- dual bases, 24
- element
 - of a ring
 - prime, 9
 - generator of a cyclic group, 2
 - of a code, 107
 - of a field
 - primitive, 23
 - of a ring
 - reversible, 9
 - of infinite order, 3
- elements
 - conjugate, 6
 - equivalent, 2
 - of a field
 - conjugate, 29
 - of a ring
 - associates, 9
 - congruent modulo an ideal, 8
- Elias bound, 112
- endomorphism of a group, 4
- entropy of a random variable, 196
 - conditional, 196
- enumerator, 81
- EPC($k, 0$), 264
- EPC(k, t), 264
- epimorphism, 4
- equivalence relation, 2
- equivalent codes, 110
- ergodic theory, 65
- EWHT, 188
- exponent of a group, 4
- extension degree, 17
- extension of a field, 10
 - of finite degree, 17
- fast correlation attack, 294
- field, 7
 - finite, 19
 - of decomposition, 20
 - prime, 11
- flag of subsets, 69
- form
 - algebraic normal (ANF), 41
 - alternating, 92
 - associated, 92
 - symplectic, 92
- Fourier transform, 114
- function
 - d -optimal, 203
 - d -resilient, 203
 - affine, 43
 - argument of, 38
 - balanced
 - with respect to a matrix, 266
 - Boolean, 37
 - (c_0, c_1) -regular, 44
 - \mathfrak{G} -invariant, 79
 - c -regular, 44
 - balanced, 45
 - bent, 166
 - correlation-immune, 198
 - functionally separable, 42
 - maximum-nonlinear, 166
 - maximum-nonlinear for a subspace, 178
 - nondegenerate, 102
 - partial, 181
 - regular, 44
 - weakly nondegenerate, 232
 - correlation-immune, 67
 - in a given direction, 201
 - cryptographic (discrete), 65
 - dual, 168
 - to a plateaued function, 180
 - dual to a partially defined mn-bent function, 182
 - Euler's, 4
 - given as a linear branching, 71
 - group-theoretic classification of, 80
 - hyperbent, 189
 - linear, 43
 - linearly dependent on a variable, 42
 - Möbius, 33
 - nonlinearity of, 50
 - nonlinearly dependent on a variable, 42
 - partially defined d -resilient, 217
 - plateaued, 180
 - quadratic, 92
 - resilient, 67
 - self-dual, 168
 - symmetric, 44
- functions
 - \mathfrak{G} -equivalent, 79
 - algebraically independent, 66

- generator matrix in the systematic form, 111
- generator polynomial, 122
- Gilbert–Varshamov bound, 112
- global avalanche characteristic, 169
 - absolute index, 266
 - sum of squares, 266
- GOST 28147-89, 283
- greatest common divisor of polynomials, 13
- Green's scheme, 152
- group, 1
 - abelian, 1
 - center of, 7
 - commutative, 1
 - complete affine, 86
 - cyclic, 2
 - finite, 2
 - Galois, 30
 - general linear, 85
 - infinite, 2
 - isomorphism, 4
 - of affine transformations, 86
 - of inverted variables, 84
 - of linear transformations, 85
 - of permutations of variables, 84
 - of residue classes, 2
 - of roots of unity, 3
 - of shifts, 84
- group action on a set of functions, 78
- Group Special Mobile, GSM, 70
- Hamming bound, 111
- Hamming code, 116
- homomorphism, 4
 - of rings, 9
- hyperbent function, 189
- ideal
 - minimal, 28
 - of a ring
 - maximal, 9
 - prime, 9
 - principal, 8
 - two-sided, 8
- idempotent, 125
 - primitive, 128
 - proper, 27, 125
- identity element of a group, 1
- image
 - branching, 70
 - of a group homomorphism, 4
- impossible differentials, 302
- independent random variables, 196
- index
 - of q modulo n , 34
 - of a subgroup, 3
 - of linearity, 70
- information
 - mutual, 197
 - information symbols, 111
- intersection of codes, 127
- invariant of a group, 88
 - complete, 88
- inverse element, 1
- isomorphic vector spaces, 17
- isomorphism, 4
- iteration cipher, 282
- Jensen's inequality, 114
- Jevons group, 85
- kernel
 - of a bilinear form, 159
 - of a homomorphism, 6
 - of a ring homomorphism, 9
 - of a symplectic matrix, 159
- key schedule, 283
- Kravchuk polynomials, 116, 227
- large set of orthogonal arrays, 207
- least common multiple of polynomials, 14
- length
 - of a code
 - primitive, 122
 - of a register, 273
- linear
 - combination, 17
 - complexity, 275
 - cryptanalysis method, 295
 - feedback shift register (LFSR), 272
 - recursive sequence (LRS), 272
 - space, 16
 - span, 275, 276
 - structure, 67
 - translator, 67
- linearity subspace of a mapping, 68
- Lloyd polynomial, 255
- locators of a vector, 255
- MacWilliams identity, 115
- mapping
 - (n, k, d) -resilient, 203, 205
 - almost perfect nonlinear, 245
 - associated with a function, 70
 - balanced, 66
 - branched, 70
 - branching, 70
 - complete, 261
 - defined by a polynomial, 16
 - linearity index, 70
 - perfect nonlinear, 243
 - plateaued, 247
 - polynomial, 250
 - resilient, 67, 203
- material, 283
 - volume of, 283
- matrix
 - Hadamard, 167

- symplectic, 92, 158
- Matsui
 - algorithm 1, 296
 - algorithm 2, 296
- maximum-nonlinear functions
 - \mathcal{PS} , 177
 - \mathcal{PS}^+ , 176
 - \mathcal{PS}^- , 176
 - class \mathcal{D} , 177
 - class \mathcal{D}_0 , 177
- method
 - boomerang, 303
 - of conditional differentials, 302
 - of multiple approximation, 302
 - of partial differentials, 302
 - rectangle, 303
- minimal polynomial of a sequence, 274
- minimum period of a sequence, 271
- mixing, 65
- mn-bent function
 - partially defined, 181
- mn-function
 - partially bent, 178
- multiplicity of a root, 16
- natural cryptographic assumption, 298
- Neyman–Pearson lemma, 290
- nonlinearity, 67
 - generalized, 188
- nonzeros of a cyclic code, 123
- norm, 24
 - absolute, 24
- normalizer
 - of a set, 7
 - of an element, 7
- operator
 - fixing some of the variables, 73
 - projection, 72
 - taking a Boolean derivative, 73
- optimal Bayes procedure, 287
- orbit index, 77
- order
 - lexicographic, 38
 - of a group, 2
 - of a polynomial, 31
 - of an element of a group, 3
 - partial, 41
- orthogonality equations, 47
- pair of variables
 - covering, 226
 - quasi-linear, 223
- Parseval’s equation, 48
- partial spreads, 177
- $PC(k, t)$, 264
- period, 271
 - of a polynomial, 31
 - of a sequence, 271
 - of a shortened row of values of a function, 189
- periodic sequence, 271
- Peterson–Gorenstein–Zierler decoder, 271
- piling-up lemma, 299
- plaintext, 281
 - block, 281
- plateaued function
 - complementary, 185
 - of order $2r$, 180
- Pless identities, 251
- Polya’s theorem, 82
- polynomial, 12
 - characteristic of an element, 30
 - constant, 12
 - constant term of, 12
 - cyclotomically homogeneous, 54
 - cyclotomically reduced, 54
 - degree of, 12
 - dual, 31
 - generator of a cyclic code, 122
 - irreducible, 14
 - Kravchuk, 227
 - leading coefficient of, 12
 - minimal, 28
 - monic, 12
 - primitive, 32
 - quadratic, 256
 - reducible, 14
 - root of, 16
 - multiple, 16
 - simple, 16
 - unitary, 12
 - Zhegalkin, 41
- pre-period of a sequence, 271
- procedure for statistical classification, 283
- product
 - Kronecker, 151
 - of elements of a group, 2
 - scalar, 26
 - of vectors, 45
- propagation criteria, 67, 201, 261
 - of degree k and order t , 264
 - extended, 264
- propagation matrix, 264
- property
 - reducible, 72
 - secondary, 73
- quotient group, 6
- quotient ring, 9
- rectangle method, 303
- Reed’s decoding algorithm, 146
- reflectivity, 2
- reliability
 - of an algorithm, 285
- representative of a cyclotomic class, 54
- residue class, 8

- resilient, 203
- Rijndael, 283
- ring, 7
 - commutative, 7
 - division, 7
 - domain, 7
 - irreducible, 27
 - of polynomials over a field, 12
 - principal ideal domain, 9
 - reducible, 27
 - with identity, 7
- root of unity, 34
 - primitive, 34
- Rothaus criterion, 169
- round, 282
 - subkey, 282
 - transformation, 282
- row operations, 110

- SAC(t), 262
- self-information of an event, 195
- set
 - difference, 169
 - simple Hadamard, 169
 - generating a subgroup, 3
 - of a code
 - characteristic, 250
 - generating, 255
- Shannon's principles, 66
- shift operator, 272
- Siegenthaler inequality, 202
- Singleton bound, 111
- skew field, 7
- space
 - r -nonlinearity of, 69
 - branching, 70
 - vector, 37
- stabilizer of a function, 79
- stable subspace, 170
- statistical classification, 283
- statistical cryptanalysis method, 281
- stream cipher, 65
- subalgebra, 18
- subfield, 10
 - proper, 10
- subfunction, 39
- subgroup, 3
 - generated by a set, 3
 - generated by an element, 3
 - nontrivial, 3
 - normal, 6
- subkey, 282
- subring, 8
- sum
 - of codes, 127
 - of elements of a group, 2
- summand
 - in ANF, 42
 - in Zhegalkin polynomial, 42
 - weight, 42
 - linear, 42
- support of an element, 206
- symmetry, 2
- syndrome vector, 118

- tabular method, 38
- trace, 23, 53
 - absolute, 23
 - relative, 54
- trace equivalence, 53
- transform
 - fast Hadamard, 151
 - Fourier, 46
 - Möbius, 41
 - Walsh–Hadamard, 46
 - extended, 188
 - incomplete, 181
- transitivity, 2
- triangle inequality, 45
- trigger, 273
- truth table, 206
- type of a permutation, 77

- ultimately periodic sequence, 271
- unknown, 12

- variable, 12
 - covering, 226
 - essential, 38
 - fictitious, 38
 - adding, 39
 - deleting, 39
 - linear, 223
 - nonessential, 38
- variable of a function, 38
- vector, 16, 37
 - r -covered by a code, 107
 - preceding, 41
 - strictly, 41
- vector space, 16
 - isomorphism of, 17

- weight
 - Hamming, 41
 - of a function, 81
 - of an equivalence class, 81
- word error probability, 120

- zero element
 - of a ring, 7
 - of a group, 2
- zero tail expansion, 276
- zerodivisors, 7
- zeros of a cyclic code, 123