

Index

- 2×2 SM-constraint, 521, 563
- $2 \times 2/3 \times 3$ SM-constrained matrix, 563
- $2 \times 2/3 \times 3$ SM-constraint, 563
- 0-replacement, 383
- 1-replacement, 383
- absorbing set, 443, 465, 695
 - elementary absorbing set, 443
- ACE (approximate cycle extrinsic), 674
- additive white Gaussian noise, 6
- affine geometries, 266
- algebraic codes, 562
- APP (a posteriori probability), 430
- ARQ (automatic repeat request), 15
 - ACK (positive acknowledgment), 15, 353
 - continuous ARQ, 15
 - GBN-ARQ, 353
 - go-back- N ARQ, 15
 - NAK (negative acknowledgment), 15, 353
 - SR-ARQ, 15
 - ST-ARQ, 353
 - stop-and-wait ARQ, 15
 - SW-ARQ, 353
- array-decomposition, 498
- AWGN, *see* additive white Gaussian noise
- balanced incomplete block designs, 518
- BCH (Bose–Chaudhuri–Hocquenghem) codes, 185, 685
- BCH bound, 194
- Berlekamp–Massey iterative algorithm, 201
- binary BCH codes, 185
- binary parity-check matrix, 191
- code construction field, 187
- consecutive powers, 186
- designed error-correcting capability, 185
- designed minimum distance, 185
- elementary-symmetric functions, 199
- error-location numbers, 198
- error-location polynomial, 199
- even-weight BCH code, 195
- Newton’s identities, 200
- nonbinary BCH codes, 220
- nonbinary parity-check matrix, 191
- nonprimitive BCH codes, 213
- primitive BCH codes, 187
- root field, 187
- syndrome, 197
- Berlekamp–Massey iterative algorithm, 201
- error-location numbers, 198
- error-location polynomial, 199
- error-value evaluator, 231
- error values, 226

- generalized Newton's identities, 228
- key-equation, 235
- Newton's identities, 200
- BF (bit-flipping) decoding, 416, 422
- threshold, 422
- BIBDs, *see* balanced incomplete block designs
- base blocks, 541, 550
- BIBD-PaG, 540
- blocks, 538
- class-1 Bose-BIBD, 541
- class-1 Bose-BIBD-PaG, 542
- class-2 Bose-BIBD-PaG, 549
- class-2 Bose-BIBD, 550
- objects, 538
- sets, 538
- binary burst erasure channel, 14
- binary erasure channel, 14
- binary image, 381
- binary symmetric channel, 7
- binary symmetric erasure channel, 14
- bipartite graph, 82
 - adjacency matrix, 82
- bit-error rate, 12
- block-cyclic structure, 642
- block-error rate, 11
- BM-HDDA, 703
- bound
 - BCH bound, 194, 222, 236
 - Hamming bound, 115
 - Reiger bound, 369
 - Singleton bound, 108, 686
 - sphere packing bound, 444, 528
 - UB (union bound), 700
 - UB-MLD, 700
- bounded distance decoding, 118, 263
- burst-error-correcting capability, 368
- bursts
 - m*-bit byte, 380
 - burst-error-correcting efficiency, 370
 - erasure-bursts, 367
 - error-bursts, 367
 - optimal-discrepancy, 369
 - phased-error-burst, 380
 - solid burst, 368, 608
- Burton codes, 381
- cascading, 684
- Cayley table, 27
- CC (cascaded composite), 689
- ceiling function, 114
- channel
 - AWGN channel, 6
 - BBEC, *see also* binary burst erasure channel, 383, 608
 - BEC, *see also* binary erasure channel, 382, 435, 746
 - BI-AWGN channel, 6, 435
 - BI-DMC, 7, 747
 - BSC, *see also* binary symmetric channel, 435, 746
 - BSEC, *see also* binary symmetric erasure channel, 383
 - compound channels, 14
 - DMC, *see* discrete memoryless channel
 - NBEC, *see* nonbinary erasure channel
 - noiseless channel, 746
 - perfect channel, 746
 - useless channel, 746
- channel capacity, 12
- channel information inclusion, 475
- channel polarization, 744, 747
 - 1-fold vector channel, 747
 - 2-fold channel polarization, 753
 - 3-fold Kronecker polarization, 755
- base channel, 748
- bit-coordinate channels, 747, 748, 766
- channel polarization theorem, 760

- channel polarization (cont.)
 - combine-and-split process, 749
 - free channels, 760
 - frozen channels, 757, 760
 - polarization transformation, 747
 - virtual channel, 748
- Chien search algorithm, 229
- Chien search procedure, 211
- circulant-decomposition, 496
 - column-decomposition, 497
 - column-descendants, 497
 - column-generator, 496
 - row-decomposition, 497
 - row-descendants, 497
 - row-splitting factor, 498
 - row-splitting weights, 498
- CN-redundancy, 442
- CNPU (CN processing unit), 474
- coding gain, 16
- collective decoding, 684
- collective encoding, 684
- combinatorial designs, 538
- complex-number field, 33
- component-wise mod-2 addition, 797
- component-wise multiplication, 797
- composite codeword, 688
- compound code, 684
- concatenation, 341
 - global errors, 341, 343
 - inner code, 342
 - inner encoding, 342
 - interleaver, 346
 - local errors, 341, 343
 - outer code, 342
 - outer encoding, 342
 - parallel concatenated coding system, 341
 - serial concatenated coding system, 341
 - turbo concatenated code, 347
 - turbo decoding, 347
 - type-1 serial concatenated code, 342
 - type-2 serial concatenated code, 345
- connection number, 442
- constituent codewords, 688
- constituent vectors, 695
- convergence threshold, 441
- copy-and-grouping operation, 630
- coset
 - coset decomposition, 31
 - coset leader, 30
 - left coset, 30
 - partition, 31
 - right coset, 30
- CPM, *see also* matrix, circulant permutation matrix (CPM), 482, 519, 563
- CPM-column-blocks, 482
- CPM-decomposition, 499
- CPM-dispersion, 489
 - base matrix, 490, 520
 - CPM-dispersion factor, 519
 - ln -fold CPM-dispersion, 519
 - n -fold CPM-dispersion, 519
 - $(q - 1)$ -fold CPM-dispersion, 489
- CPM-RID scheme, 504
 - CPM-RID-MSA, 506
 - CPM-RMSA, 506
 - decoding matrix, 506
 - decoding subiteration, 506
 - section-wise cyclic-shift, 504
- CPM-row-blocks, 482
- CRC-aided SCL decoding, 779
- cyclic codes, 125
 - BCH codes, 185
 - binary cyclic codes, 125
 - code polynomial, 126
 - cyclic-shift, 126
 - error polynomial, 142
 - error-trapping decoding, 150
 - generator codeword, 133
 - generator matrix, 134
 - generator polynomial, 130
 - Meggitt decoding process, 146
 - minimum-degree code polynomial, 127

- nonbinary cyclic codes, 176
- parity-check matrix, 135
- parity-check polynomial, 135
- QC (quasi-cyclic) codes, 161
- QR code, 159
- received polynomial, 142
- reciprocal polynomial, 135
- syndrome polynomial, 142
- cyclic convolution, 796
- cyclic grouping, 472
- cyclic redundancy check code, 158
- cyclic RM code, 324
- cyclic shift-register-adder-accumulator circuit, 165
- DE (density evolution), 441
- decoding
 - MAP, *see* maximum a posteriori
 - MLD, *see* maximum likelihood decoding
- decoding convergence, 442
- decoding regions, 109
- decoding threshold, 441, 633
- decomposition factor, 642
- decomposition set, 642
- demodulator, 7
- direct product code, 335
 - codeword array, 335
 - received array, 338
- discrete memoryless channel, 7
- EG, *see* Euclidean geometries
- entropy, 745
 - channel capacity, 746
 - conditional entropy, 745
 - joint entropy, 745
 - mutual information, 745
 - probability mass function, 745
 - uncertainty, 745
- erasures, 367
 - CPM-phased erasure-burst, 608
 - erasure-bursts, 367
 - random erasures, 367
- error detection
 - decoding error, 101
 - error pattern, 100
 - error-detecting capability, 109
 - guaranteed detectable error patterns, 109
 - Hamming weight, 103
 - minimum weight, 103
 - syndrome, 101
 - undetectable error pattern, 101
 - undetected error rate, 104
 - undetected error rate upper bound, 105
 - weight distribution, 103
 - weight spectrum, 103
- error rate
 - BER, *see also* bit-error rate, 16
 - BLER, *see also* block-error rate, 16, 243
 - FER, *see* frame error rate
 - SER, *see also* symbol-error rate, 243
 - UEBLR, *see* unresolved erasure block rate
 - UEBR, *see* unresolved erasure bit rate
- error-control strategies
 - ARQ, 331
 - ARQ (automatic repeat request), 15
 - FEC, 15, 331
 - HARQ (hybrid-ARQ), 16, 332
- error-correcting codes, 4
 - BCH codes, 185
 - block codes, 4
 - code dimension, 4, 89
 - code length, 4, 89
 - code rate, 4, 89
 - codeword, 89
 - message, 89
 - parity-check bits, 90
 - redundant bits, 90

<i>Index</i>	806
error-correcting codes (cont.)	
burst-error-correcting codes,	
14, 367	
convolutional codes, 4, 5	
memory order, 5	
cyclic codes, 125	
error-correcting capability, 115	
finite-geometry codes, 258	
LDPC codes, 406	
linear block codes, 89	
perfect code, 115	
QR codes, <i>see</i> quadratic	
residue	
RM (Reed–Muller) codes, 303	
SPC code, <i>see</i> single	
parity-check	
error-detection codes, 105	
CRC code, <i>see</i> cyclic	
redundancy check code	
error-floor region, 439	
error-location numbers, 198	
error-location polynomial, 199	
error-trapping decoder, 373	
error-trapping decoding, 150	
Euclidean algorithm, 220	
Euclidean geometries, 266	
μ -flat (hyperplane), 268	
affine geometries, 266	
cyclic class of lines, 276	
intersecting bundle, 268	
one-dimensional subspace, 267	
origin, 267	
parallel bundle, 267	
subgeometry, 275	
two-dimensional Euclidean	
geometries, 278	
Euclidean geometry codes	
cyclic-EG-LDPC code, 465	
masked QC-EG-LDPC codes,	
495	
QC-EG-LDPC code, 480	
two-dimensional cyclic EG	
code, 279	
Euler ϕ function, 38	
Euler totient function, 38	
EXIT (extrinsic-information-	
transfer chart),	
442	
experimental designs, 538	
extended code, 119	
FG, <i>see also</i> finite geometries, 464	
FG codes, <i>see also</i> finite-geometry	
codes, 464	
field, 31	
cardinality, 33	
characteristic, 34	
extension field, 33, 221	
finite field, 33	
Galois field, 35	
ground field, 50	
infinite field, 33	
order, 33	
prime field, 33, 35	
subfield, 33, 222	
finite field, 35, 562	
binary field, 35	
conjugate, 51, 222	
conjugate roots, 49	
conjugate set, 51	
conjugates with respect to	
GF(q), 226	
decimal form, 48	
exponent, 51	
nonbinary field, 67	
polynomial basis, 46	
polynomial form, 48	
polynomial representation, 46	
power form, 48	
primitive element, 38	
vector form, 48	
finite geometries, 258	
Euclidean geometries, 258	
incidence matrix, 259	
incidence vector, 259	
intersecting bundle, 259	
line-point adjacency matrix,	
259	
lines, 259	
orthogonal structure, 259	
partial geometries, 518, 522	

<i>Index</i>	807
points, 259	
projective geometries, 258	
finite group, 26	
additive group, 27	
cyclic group, 29	
generator, 29	
modulo- m addition, 26	
modulo- m multiplication, 26	
multiplicative group, 28	
finite-geometry codes, 258, 261	
cyclic-EG-LDPC code, 465	
cyclic-PG-LDPC code, 469	
FG-LDPC codes, 464	
QC-EG-LDPC code, 480	
QC-PaG-LDPC codes, 524	
QC-PG-LDPC code, 487	
Fire codes, 370, 374	
designed burst-error-correcting capability, 374	
flooding schedule, 431	
floor function, 114	
forward error correction, 15	
frame error rate, 700	
GA (Gaussian approximation), 441	
Galois Fourier transform, 74	
GCD (greatest common divisor), 243	
generalized Fire codes, 382	
generalized Newton's identities, 228	
GFT, <i>see also</i> Galois Fourier transform, 692	
GFT domain, 685	
GFT-ICC codes, 693	
GFT-ICC-BCH-LDPC codes, 706	
GFT-ICC-Golay-LDPC code, 709	
GFT-ICC-QR-LDPC codes, 709	
GFT-ICC-RS-LDPC codes, 702	
GFT-ISDD scheme, 699	
GFT-ISDD/MSA, 700	
Golay code, 115, 159	
graph, 78	
acyclic graph, 81	
adjacency matrix, 81	
bipartite graph, 82	
branches, 78	
CNs (check nodes), 411	
cycle, 80	
degree distribution, 78	
edge set, 78	
edges, 78	
end-node, 78	
finite graph, 78	
girth, 80	
incidence matrix, 81	
infinite graph, 78	
irregular graph, 79	
node set, 78	
nodes, 78	
parallel edge, 78	
path, 79	
regular graph, 79	
simple graph, 79	
subgraph, 79	
Tanner graphs, 411	
tree, 81	
vertices, 78	
VNs (variable nodes), 411	
graph-theoretic LDPC codes, 628	
connection matrix, 631	
copy-and-permute, 629, 630	
edge-growth, 629, 670	
lifting degree, 630	
protomatrix, 631	
PTG-based LDPC code, 629	
PTG-LDPC codes, 629	
QC-PTG-LDPC codes, 632	
group, 25	
abelian group, 26	
cardinality, 26	
commutative group, 26	
finite group, 26	
identity element, 26	
infinite group, 26	
inverse, 26	
order, 26	
subgroup, 29	
Hadamard equivalent, 686	
Hadamard permutation, 684, 686	

<i>Index</i>	808
Hadamard power, 686, 689	
Hamming codes, 95, 125, 154	
cyclic Hamming codes, 188	
distance-4 Hamming code, 158, 195	
Hamming distance, 11, 105	
hard-decision decoding, 9	
BF decoding, 416	
multilevel majority-logic decoding, 303	
OSMLD, 263	
SPL (successive peeling), 386	
HARQ (hybrid-ARQ), 16	
HDD, 709	
HDD algorithm, 709	
hyperbolic tangent, 433	
ICC (interleaved cascaded composite), 690	
IDBP, <i>see also</i> iterative decoding based on belief-propagation, 694	
information sharing, 685	
interleaving, 332, 684	
base code, 332	
constituent codewords, 332	
interleaved code, 332	
interleaved matrix, 333	
interleaved vector, 332	
interleaving degree, 332	
inverse GFT, 692	
inverse hyperbolic tangent, 433	
ISDD (iterative soft-decision decoding), 699	
iterative decoding based on belief-propagation, 417	
joint-decoding, 685	
joint-decoding gain, 685, 700	
key-equation, 235, 247	
Kronecker codes, 721, 736	
Kronecker–RM codes, 736	
Kronecker mapping	
ℓ -fold Kronecker mapping, 724	
ℓ -fold connection matrix, 731	
2-fold connection matrix, 727	
3-fold Kronecker mapping, 728	
decomposition process, 732	
inverse Kronecker mapping, 725	
splitting process, 732	
Kronecker matrices, 721	
ℓ -fold Kronecker matrix, 723	
2-fold Kronecker matrix, 722	
3-fold Kronecker matrix, 722	
4-fold Kronecker matrix, 723	
kernel, 722	
Kronecker product, 348	
Kronecker vector space, 736	
Latin square, 575	
LCM (least common multiple), 186	
LDPC codes, <i>see</i> low-density parity-check codes	
cyclic LDPC codes, 408	
doubly QC-LDPC codes, 644	
finite-field-based QC-LDPC codes, 564	
Gallager LDPC codes, 415	
GFT-ICC-LDPC code, 694	
graph-theoretic LDPC code, 628	
irregular LDPC codes, 408	
low-density matrix, 407	
MacKay codes, 416	
PEG-LDPC codes, 528, 629	
QC-LDPC codes, 408	
QC-RS-LDPC codes, 590	
RC-constraint, 408, 520	
regular LDPC codes, 407	
RS-based QC-LDPC codes, 590	
sparse matrix, 407	
LFSR, <i>see also</i> linear feedback shift-register, 139	
linear block codes, 89	
P-submatrix, 96	
k -dimensional subspace, 90	
q -ary linear block code, 120	
binary linear block code, 90, 120	

<i>Index</i>	809
cyclic codes, 125	
dual code, 93	
dual space, 93	
elementary row operations, 98	
extended code, 119	
generator matrix, 92	
minimum distance, 107	
minimum weight, 107	
mother code, 119	
nonbinary linear block code, 120	
null space, 93	
parity submatrix, 97	
parity-check equations, 97	
parity-check matrix, 93	
parity-check sums, 97	
row space, 92	
shortened code, 119	
standard array, 110	
systematic form, 96	
linear feedback shift-register, 125, 139	
LLR, <i>see</i> log-likelihood ratio	
local cycle structure, 608, 609	
local girth, 672	
log-likelihood ratio, 428	
low-density parity-check codes, 406	
LR (likelihood ratio), 430	
MacWilliams identity, 104	
masking, 493, 580	
building blocks, 580	
Hadamard matrix product, 493	
masked base matrix, 495	
masking matrix, 495	
mother base matrix, 586	
SMC-MMSA, <i>see</i>	
SM-constrained 4×8	
masked matrix search algorithm	
type-1 masking matrix, 581	
type-2 masking matrix, 582	
type-3 masking matrix, 585	
matrix	
binary matrix, 67	
circulant, 70	
circulant permutation matrix (CPM), 70	
column weight, 68	
dual space, 72	
full column rank matrix, 68	
full row rank matrix, 68	
generator, 70	
Hadamard matrix product, 493	
identity matrix, 70	
inverse, 70	
irregular matrix, 68	
nonbinary matrix, 73	
nonsingular matrix, 68	
null space, 72	
permutation matrix, 70	
rank, 68	
redundant columns, 68	
redundant rows, 68	
regular matrix, 68	
row space, 71	
row weight, 68	
singular matrix, 68	
square matrix, 67	
transpose, 68	
Vandermonde determinant, 78	
Vandermonde matrix, 73	
ZM (zero matrix), 164	
matrix-dispersion, 632	
maximum a posteriori, 10	
maximum-distance separable, 108	
maximum likelihood decoding, 11	
MDS, <i>see</i> maximum-distance separable	
MDS code, 108, 236	
Meggitt decoding process, 146	
minimum-distance decoding, 12, 109, 113	
modulator, 6	
mother code, 119	
MSA (min-sum algorithm), 437	
attenuating factor, 437	
scaling factor, 437	
multilevel majority-logic decoding, 303	
multiplicative inverse, 28	

<i>Index</i>	810
nonbinary BCH codes, 220	
q -ary BCH codes, 222	
nonbinary erasure channel, 395	
one-step majority-logic decoding, 258	
orthogonal syndrome check-sums, 262	
OSML decoding, <i>see also</i> one-step majority-logic decoding, 419	
OSML decision function, 419	
OSMLD, <i>see also</i> one-step majority-logic decoding, 466	
OSMLD decodable, 263	
PaG (partial geometry) codes	
QC-BIBD-PaG-LDPC codes, 543	
QC-PaG-LDPC codes, 524	
QC-RS-PaG-LDPC codes, 527	
PaGs (partial geometries), 522	
BIBD-PaGs, 538	
class-1 Bose-BIBD-PaG, 542	
class-2 Bose-BIBD-PaG, 549	
connection number, 523	
net, 523	
parameters, 522	
RS-based partial geometry, 527	
pair-wise RC-constraint, 497, 498, 645	
parity-check sums, 261, 410	
parity-check vector, 391	
PEG (progressive edge-growth), 628, 670, 673	
ACE, 674	
ACE-PEG, 675	
PEG-LDPC code, 673	
perfect code, 115	
polar codes, 721	
encoding vector, 738	
free bit locations, 739	
free bits, 739	
frozen bit locations, 739	
frozen bits, 739	
polarized encoding, 738	
polarized partition, 739	
polynomial	
irreducible polynomial, 41	
minimal polynomial, 52	
primitive polynomial, 42	
reciprocal polynomial, 135	
primitive Fire codes, 374	
product-form, 576	
projective geometries, 288	
projective geometry codes, 292	
cyclic-PG-LDPC code, 469	
QC-PG-LDPC code, 487	
PSD (power spectral density), 417	
PTG (protograph), 628, 629	
puncturing, 119	
QC (quasi-cyclic) codes, 161	
CSRAA, <i>see</i> cyclic shift-register-adder-accumulator circuit	
QC structure, 161	
section size, 162	
section-wise cyclic-shift, 162	
semi-systematic circulant form, 169	
shifting constraint, 161	
systematic circulant form, 164	
QR (quadratic residue) codes, 685	
quadratic residue, 159	
rate compatible, 685	
rational-number field, 33	
RC-constrained matrix, 520	
RC-constraint, 408, 520	
real-number field, 33	
RID (revolving iterative decoding), 474	
CII, <i>see</i> channel information inclusion	
RID-MSA, 474	
RMSA, 474	

- RM (Reed–Muller) codes, 303
 - dual code, 309
 - inclusion chain, 309
 - multilevel encoding, 313
 - mutually orthogonal structure, 309
 - self-dual, 310
 - successive cancellation
 - information retrieval, 317
- row-redundancy, 442, 507
- RS (Reed–Solomon) codes, 220, 685
 - nonprimitive RS code, 238
 - primitive RS code, 236
 - probability of an undetected error, 252
 - weight distribution, 251
- RS matrices, 591
 - RS base matrices, 593
 - type-1 $2 \times 2/3 \times 3$
 - SM-constrained RS matrix, 599
 - type-1 RS matrices, 592
 - type-2 $2 \times 2/3 \times 3$
 - SM-constrained RS matrix, 600
 - type-2 RS matrices, 592
 - type-3 $2 \times 2/3 \times 3$
 - SM-constrained RS matrix, 600
 - type-3 RS matrices, 592
- SC (successive cancellation)
 - decoding, 769
 - SC kernel decoder, 771
- SCIR, *see also* successive cancellation information retrieval, 388
- SCL (successive cancellation list)
 - decoding, 779
- section-wise cyclic structure, 644
- self-dual, 66, 310
- Shannon limit, 18
- shortened code, 119
- simplex code, 157
- single parity-check, 120
- SM-constrained 4×8 masked
 - matrix search algorithm, 588
- SNR (signal-to-noise ratio), 16
- soft-decision decoding, 9
 - IDBP, 417
 - MSA, 437
 - SPA, 429
 - weighted BF decoding, 416
 - weighted OSM decoding, 417
- SPA (sum-product algorithm), 429, 433
- SPB, *see* bound, sphere packing bound
- SPL (successive peeling), 386, 610
- SPL/SCIR-decoding, 388
- standard array, 110
 - coset, 110
 - coset leader, 110
 - optimal standard array, 113
 - syndrome decoding, 117
 - table look-up decoding, 117
- stopping set, 447
 - maximum stopping set, 448
 - minimum stopping set, 449
 - SFS (stopping-free set), 448
- successive cancellation information retrieval, 317
- sum-form, 565
- symbol-error rate, 16
- Tanner graphs, 411
 - degree distribution
 - polynomials, 412
- trapping set, 439, 442, 695
 - elementary trapping set, 442
 - small trapping set, 442
- two-sided power spectral density, 794
- uncoded BPSK system, 16
- universal coding scheme, 684
- unresolved erasure bit rate, 447
- unresolved erasure block rate, 447

Vandermonde matrices, 73, 692	
vector space, 60	
basis, 64	
component-wise addition, 62	
component-wise product, 304	
dull space, 65	
inner product, 65	
linear combination, 64	
linearly dependent, 64	
linearly independent, 64	
null space, 65	
orthogonal, 65	
scalar multiplication, 61, 62	
subspace, 64	
vector, 61	
vector addition, 61	
vector product, 304	
	zero vector, 61
	VNPU (VN processing unit), 474
	waterfall region, 439
	weight distribution, 103
	weight enumerator, 104, 156
	weight spectrum, 103
	weighted BF decoding, 416, 426
	weighted OSML decoding, 417, 426
	zero divisor, 83
	zero-span, 135, 391
	end-around zero-span, 391
	longest zero-span, 391
	maximal zero-span, 391
	null zero-span, 391
	zero-covering span, 392
	ZM, <i>see</i> matrix, ZM (zero matrix)