Index

A-law, 592
Action table (Turing machine), 97, 107
Adaptive coding, see Coding
Adder (plain), 299
Addition (quantum operation), 326
Additive noise, see Noise
Adleman L., 424, 536
ADSL, 225
Advanced encryption standard, see AES
AES (advanced encryption standard), 523, 541–3, 555, 563, 597, 672
Ait Sab O., 229
Algebra/arithmetic (modular), see Modular
Algorithm
continued fraction expansion, 399, 408–10, 648–52
Deutsch, 378–80
Deutsch–Jozsa, xv, xix, 378, 381, 394, 512
Diffie–Hellmann–Merkle algorithm, 534, 535, 541
Dixon, 411
extended Euclidian, 413, 428, 658, 673
Fermat, 411
general number field sieve, 400, 411, 538
Grover quantum database search, xv, xix, 378, 389–98
Hughes, 535
Lenstra, 411
order-finding (-), 399, 400, 405–8, 414
Pollard, 411
Shank, 411
triple data encryption (TDEA), 542
V (code), see Code
William, 411
Algorithmic
and logical unit, see ALU
complexity, see Kolmogorov
entropy, see Entropy
independence, 121
information theory, see Information
Alphabet (symbol), 57, 127
Alphabetic
poly (-) substitution, 526
substitution, 526
ALU (algorithmic and logical unit), 283, 288, 289
American
Automobile Association (AA), 159
Civil War, 132
wheel, 170
Ammeter, 360
Ampersand
Amplified coherent light, see Coherent
Analog-to-digital voice conversion, see Speech
Ancilla
bit, see Bit
qubit, see Qubit
space, 352
state, 354
AND (logical/Boolean), 70, 76, 291, 293, 299, 529
ANSI (American National Standards Institute), 541, 542
Arabic numerals, see Numerals
Araki–Lieb inequality, 442
Architecture
multi-processor, 289
parallel processor (-), 289
von Neumann, see Von Neumann
Arithmetic coding, see Coding
Arobase, 167
Arrangement without repetition, 10–11
Artificial intelligence, see Intelligence
ASCII (American standard code for information exchange), 112, 113, 130, 131, 133, 152, 156, 157, 159, 169, 192, 197, 426–8, 527, 528, 530
Aspect, A., xii
At sign or @, 167
Attack, see Cryptosystem
brute-force, see Cryptosystem
cryptosystem, see Cryptosystem
denial of service (DoS), 564
giant pulse, 563
impersonation, 563
key, see Key
man-in-the-middle (-), 562, 563
random-number generator, 563
ATM, 225
Atomic physics, 28
Authentication, 523, 542
B92 protocol, 523, 562
Backward error correction, 211
Balanced function, 381
Bandwidth
channel, see Channel

efficiency diagram, 271
expansion factor, 211
Basis
change of (-), 333, 337
computational, 306, 311, 432
orthonormal, 334, 337–9, 343, 345, 346, 363
Baudot code, 131
Bayes's theorem, see Theorem
BB84 protocol, 523, 556–62
BCH codes, see Code
Bean machine, 34
Bell
distribution, 29–30
state, see State
System Technical Journal (BSTJ), 85, 87
Bennet, C. H., 556, 558
BER, see Bit error rate
Berger, Vincent, xxi
Bernoulli distribution, see Probability
Beta probability distribution, see Probability
Binary
digit, see Bit
number, 128
pseudo (-), 132, 133
system, 128
Binomial
coefficient, 10, 25, 171
distribution, see Probability
Birefringence, 548
Birthday (sharing), 14
Bit, xvii, 43, 44, 128, 304
ancilla (-), 301
classical, 306, 357, 366
control (-), 209
error, 32
error rate, see Bit error rate
errored (-), 209
flip channel, see Quantum channel
parity (-), 210
payload (-), 210
phase-flip channel, see Quantum channel
rate, 210
redundancy (-), 209
single (-) error, 215
soft (-), 225
undetected (-) error, 216
Bit error rate, 208, 211, 243
corrected (-), 208, 226–30
uncorrected, 228
Bloch sphere, 304, 308, 311, 319, 322, 343, 509, 625–7, 630, 631
Block, 210
code, see Code
coding, see Coding
field, 162
header, 172, 177
length, 44
trailer, 172, 177
Blondel, Jean-Pierre, 47
Bluetooth, 224
Bohr, xii, xiii
Boltzmann, L., 50
Boltzmann’s constant, 65, 285
entropy, see Entropy
theorem, see Theorem
Books
arranging on a shelf, 8–10
Boolean
gate, see Gate
function, 78
logic, 76, 283
operators/operations, 76, 291, 529
variable, 11
Bose
Chaudhuri–Hocquenghem (BCH) codes, see Code
Einstein distribution, see Probability
Bra, 334
Brassard, G., 556
Brillouin, L., 285
Brownian motion, 286
Bruen, A. A., 246, 258
Brute-force attack, see Cryptosystem
Byte, 129
Caillet, X., xxi
Calderbank–Shor–Steane (CSS) error correction
code, see Quantum error correction
Capacity
classical channel (-), see Channel capacity
quantum channel (-), see Quantum channel
Cards (pulling), 16–17
Carry, 295
CARRY gate, 299, 300, 325
Cat
Schrödinger’s (-), 307
state, see State
Cauchy probability distribution, see Probability
Chit, 367, 369, 449
CCNOT gate, 299, 320, 323–5
CD, 592–3
CD-ROM, 593, 597
Cdma2000, 225
Cellular telephony (GSM), 594
Central
  limit theorem, see Theorem
  office, 563
Chain rule, 73, 78, 79, 81
Chaitin, G., 96, 122
Channel
  asymmetric (-) with non-overlapping outputs, 236, 251
  bandwidth, 269, 270
  binary (-), 232
  binary erasure (-), 235, 250
  binary symmetric (-), 232–4, 238, 241, 245, 249
  capacity, xix, 242, 244, 245, 250–2, 267, 269, 617–20
  capacity theorem, see Theorem
coding theorem, see Theorem
  communication (-), 208, 232
closed, 32
discrete, 232
discrete, 232
discrete, 232
discrete, 232
discrete, 232
discrete, 232
error rate, 243
Gaussian, 264–7, 269–75
ideal, 208, 234, 475
linearity, 277
memoryless, 227, 622
nonideal, 208
nonlinear/nonlinearity, 264, 277, 278, 281
noiseless, 233, 234, 248
noisy typewriter (-), 236, 250, 258
public, 557, 560, 561, 563
quantum, see Quantum
rational, 269
realistic, 208
secure (or absolutely secure) communication (-), 232
  symmetric, 234
useless, 234, 240, 241, 247, 273, 618
Z (-), 234, 243, 249
Character (symbol), 57, 58
Characteristic equation, 338, 436
Chi/Chi-squared probability distribution, see Probability
Chuang, I. L., 296, 372, 637
Church–Turing thesis, 107, 290
Cipher, 425
Ciphertext, 61, 424
Circular polarization, see Polarization
Clarke, A., 39
Clausius, R., 50
Clausius relation, 66
Closed quantum system, 432
Closure relation, see Completeness
CLT, see Theorem
Compact (UNIX), 199
CNOT gate, 293, 299, 316–18, 362, 365, 368, 372, 374, 375, 387, 389, 497, 504, 519, 637
CNRS, xxi
Co-prime, see Number
Code (see also Coding)
  algorithm V , 192, 200
  attack, see Cryptosystem
  breaking, 524, 525
  cracking, 525, 536
  block (or linear block), xix, 44, 151, 162–77, 186, 208, 210–17, 509, 592, 614
  Bose–Chaudhuri–Hocquenghem (BCH), 221
  breaking, 523
  concatenated (block), 222, 229
  convolutional, 223
  Calderbank–Shor–Steane (CSS), see Quantum
error correction
cyclic, xix, 208, 217–19
  cyclic redundancy check (CRC), see Cyclic
dual, 515
eight-to-fourteen modulation (8/14), 593
Elias, 179–81
Elias-delta, 179, 180, 183, 185
Elias-gamma, 179, 183, 185
Elias-omega, 181
Elias recursive, 181
entropy (effective), see Entropy
error correction, see Error (classical) or Quantum
Faller, 192
FGK, 192, 193
Fibonacci, 179, 181, 185
fixed-length, 145
gain, 225, 228
Gallager, 192
Golay, 220
Golomb, 183
Golomb–Rice, 179, 185, 594
Hadamard, see Hadamard
  Hadamard–Steane, see Quantum error correction
Hamming, see Hamming
Huffman, see Huffman
instantaneous, 140
Knuth, 192, 193
maximum-length shift-register, 221
Morse (-), see Morse
  recursive, 223
  singular, 139
  systematic, 223
optimal/optimality, see Coding
  optimization, 131
  prefix, 140, 142, 183
Concatenated (block) codes, see Code
Concavity
entropy, see Entropy
function, 443
Conditional
complexity, see Kolmogorov
entropy, see Entropy
probability, see Probability
Conditioning reduces entropy, 77, 78, 81, 85, 87
Conjugation/conjugate
complex, 328
Hermitian, 328, 337, 627
observable, see Observable
Constraint length (of code), 223
Consultant business, 38
Continued fraction expansion algorithm, see Algorithm
Continuous variable, 20
Controlled
controlled-NOT gate, see CCNOT
controlled-U gate (CCU), 321, 399
NOT gate, see CNOT
phase gate, 387, 646
Sign (CSIGN), 376
SWAP gate, 320
U gate, 319, 322, 401
Convergent of integer, 409, 648
Convolutional codes, see Code
Copenhagen interpretation, 308
Corrected bit-error-rate, see Bit error rate
Correction, see Error
Correlated events, see Events
Correlation, 58
Cost, 510
Costello, D. J., 614
Cover, T. M., 90, 111, 148, 206, 252, 578, 583, 587, 610, 621
CPU (central processing unit), 283, 289, 412, 537–9, 541
CRC, see Cyclic redundancy check
Crih, 526
CROSSOVER (or SWAP) gate, 293, 297, 318, 370, 387–9
Cryptanalysis, see Cryptoanalysis
Cryptoanalysis (or cryptanalysis), 524, 526
Cryptography, xv, xx, 130, 523
asymmetric key (-), 536, 541
public-key (-) or PKC, 400, 424–9, 523, 524, 527, 536–40, 543
quantum, 520, 523, 543–4, 564, 656, 659
symmetric key (-), 536
without key exchange, see Key
Cryptography, 424, 525
Cryptosystem, 524, 564
attack, 525
brute-force attack, 525, 526, 541
Cyclic
code, see Code
redundancy check (CRC) code, 220
Daishoya project, 192
Damping (amplitude/phase), 481
Dasher project, 192
Data
compression, see Compression
encryption, see Encryption
encryption standard, see DES
entry device (fast), 192
Database management, 185
De Broglie, L., xii
De Morgan’s law, 298, 302
Decimal number, 128
Decision (receiver), 226
Decoder/decoding, 190, 208
hard-decision, 226
maximum-likelihood (-), 216, 615, 616
soft-decision, 226
Decoherence (quantum), see Quantum
Decompression, 161
error, 162
Decryption, 61, 425, 523, 524
Deep Crack, 541
Degenerate eigenvalue, see Eigenvalue
Delta distribution, 90
Denial-of-service (attack), see Attack
Density matrix, see Matrix
Density operator, see Operator
Depolarizing channel, see Quantum channel
DES (data encryption standard), 523, 532, 540–3, 555, 563
double (-), 523, 541
triple (-), 523, 541
542
Desurvire, E., xiv–xvi, 51, 66, 130, 226, 275, 278, 345, 425, 426, 526, 542, 576, 578, 592, 603
Determinant, see Matrix
Deutsch
gate, see Algorithm
gate (or CCR gate), 322
Jozsa algorithm, see Algorithm
problem, 378, 380, 381, 383
Diagonal matrix, see Matrix
Diagonalizable, 340
Dice/die, see Rolling
Dictionary, 127, 201, 204
Diffie–Hellmann–Merkle algorithm, see Algorithm
Digital
cash, 543
high-definition (-) video, see HDV
signature, 523, 542
sound, see Sound
video (DV), see DV
video disk (DVD), see DVD
Discrimination, 80
Discord, 436
Distance
between PDF, 69, 79
definition, 79
Kullback–Leibler, 80, 81, 84, 85, 87–9, 143, 154, 214, 437, 584, 661
Distinct parsing, see Parsing
Distribution
exponential, see Probability
probability, see Probability
uniform, see Probability
Distributivity, 328
Diu, B., 635
Dixon algorithm, see Algorithm
DNA, 372
Double-key encryption, see Encryption
DV (digital video), 599
DVD (digital video disk), 603, 605–9
Dyadic (source, distribution), 149, 155
Dynamic coding, see Coding

Email, 596
Eavesdropping, 556, 561, 562
EBCDIC (extended binary coded decimal interchange code), 130, 527
Ebit, 364, 367, 374–6
ECC, see Error-correction/correcting code
Eckert, A. K., 559, 560
Efficiency
alphabet use, 63
coding, see Coding
Eigenspace, 339, 437
Eigenspace/eigenvalue, 333, 338–40, 360, 390, 432, 435, 437, 458
Eigenvector, 209, 333, 338–40, 437, 458
degenerate (-), 339
Eight-to-fourteen modulation (8/14) code, see Code
Einstein, xii–xiv
two-body, 367, 371, 559, 560
Einstein–Podolsky–Rosen (state), 310, 356, 362
Electromagnetic (EM) wave, 544
Electronic voting/polling, 543
Encryption, 40, 424, 523, 524
double or two-key (-), 523, 532–4
one-way, 523, 543
English
character source, 57, 58, 60, 61, 63, 151, 156, 159, 160, 165, 167, 183, 185, 189–91, 194
character/letter coding, 154
Enigma machine, 526, 527, 532
Ensemble, 75
Entangled qubits, see Qubit
Entropy, 50
Entropy, xviii, xix, 97, 111, 123, 232, 304, 342, 343, 431, 434, 435, 443, 475, 568–72
algorithmic, xix, 96, 97, 110, 111
as measure of disorder, 285
Boltzmann’s (-), 565–6
complexity and (-), 111
concavity, 443–4, 451
conditional (classical), 58, 69, 72, 77, 78, 85, 122, 238
conditional (quantum), 441–2
conditional relative (-), 81
continuous or differential, see Entropy (differential)
continuous source, 84
convergence with Kologorov complexity, 123–5
differential, 84, 85, 90, 265, 559–62
definition, 50, 52
effective code (-), 136
infinite, 85, 86
joint (classical), 61, 69, 72, 77, 122, 238
joint (quantum), 439–41
language, 57–63, 129
maximum/maximizing, 63–7, 80, 88, 91, 94, 246, 252, 265, 578
maximum (-) model (MEM), 67
maximum (-) principle, 67
relative (classical), 52, 69, 78–80, 85, 87–9, 584, 661
relative (quantum), 437
Shannon’s, see Entropy
Epistemic, 67
EPR
pair, 310
protocol, 523, 559–62
state (or Bell state), see State
Equi-probability, 4
Equivalence, 73, 238, 240, 245, 618
Eratosthenes, 538

© Cambridge University Press
www.cambridge.org
Erlang (-) distribution, see Probability
Error correction/correcting
classical, xix, 40, 162, 273, 591
code, 208, 244
function, see Complementary
quantum, see Quantum
Error
backward (-) correction, see Backward
bit (-) rate, see Bit error rate
decompression (-), see Decompression
forward (-) correction, see Forward
quantum (-) correction, see Quantum
symbol, 208, 209, 234, 242
symbol (-) rate (SER), 232, 242–4, 476
Esperluette, 167
Ethernet, 225
Euler’s theorem, see Theorem
Event(s)
anti-correlated, 15
combined, 11
complementary, 12
conditional, 70
correlated, 13, 15
correlation, 13
discrete, 20, 84
independent, 15, 16, 70
joint, 11, 70
mutually exclusive, 12
outcome, 2
probabilistic, 1–3
probability, see Probability
space/set, 2, 41
uncorrelated, 15, 16
Exams (taking), 13
Expectation value, 21, 433, 483, 502
Expected (codeword) length, 136
Exponential
distribution, see Probability
imaginary, 628
operator, see Operator
Exponentiation operation
classical, 302
quantum, 326
Extended
Euclidian algorithm, see Algorithm
source, see Source
F (probability distribution), see Probability
Factorial, 9
Factorization/factoring
into primes, 302, 389, 523
N = 12
Faller (code), see Code
Fang, J., 229
Fano’s inequality, 621
FANOUT gate, 293, 297, 299, 330, 331
Fast Fourier transform, see Fourier transform
Favoro I., xxx
FEC, see Forward error correction
Feldmann, D., 587
Fermat
algorithm, see Algorithm
theorem, see Theorem
Fermi
energy level, 27
function, 27
Feynmann, R., 286
FGK (code/algorithm), see Code
Fibonacci
code, see Code
numbers, 181, 182
Fidelity, 457, 458, 462, 466, 497, 498, 500
FLIP-FLOP gate, 294
Forcinto, M. A., 246, 258
Forward error correction, 211
Fouché-Gaines, H., 58, 69, 116
Fourier transform
discrete, 384
fast (FFT), 383, 389
inverse, 384, 399
quantum, see Quantum
Frame (audio-CD), 592
Fredkin gate, 297, 320
French
language source, 58, 160
revolution, 128
wheel, 170
Frequency analysis (cryptography), 526
Fruit-market shopping, 10–11
Function
failure, 29
reliability, 29
Gadsby (novel), 185
Galileo, 226
Gallager, R. G., 156, 193
Gallager (code), see Code
Galton box, 34
Gamma
function, 9
probability distribution, see Probability
Gate
CNOT, see CNOT
controlled, see Controlled
Hadamard, 312, 314, 362, 365, 379, 381, 385,
387, 395, 399, 401, 407, 410, 417, 501, 504,
511, 512, 519, 637
logic or Boolean, xx, 283, 291, 293, 311
quantum, see Quantum
reversible/logic (-), 288, 296–302, 310
Gaussian channel, see Channel distribution, see Probability
General number field sieve (GNFS) algorithm, see Algorithm
Generalized normal (-) probability distribution, see Probability
Generator
matrix, see Matrix polynomial, see Polynomial
German language source, 58, 160
Giant pulse attack, see Attack
GIF, 207, 600
GNU zip, 207
Golay code, see Code
Golomb–Rice code, see Code
Gottesmann, D., 372, 637
GPRS, 225
GPS, 226
Greatest common divisor (GCD), 405
Grenberger–Horne–Zeilinger (GHZ) state, see State
Group theory, 510
Grover iteration, 391
operator, see Operator quantum database search algorithm, see Algorithm
GSM, 225
Gzip, 207
Hacker, 39
Hadamard
codes, 220
gate, see Gate
matrix, see Matrix
Steane code, see Quantum error-correction code
HAL, 39, 40
Halting
problem, 108–10, 290
rule, 109, 110
Hamming
code, 213, 220, 261, 510, 514
distance, 214, 516
minimum (-) distance, 214, 216, 614
weight, 214, 216, 614
Hartley, R., 50, 264
Hartley’s law, 264
Hash
attack, 543
function, 543
Hashing, 523
Haykin, S., 272
HDV (high-definition video), 599, 603
Header (block), see Block
Heat, 285
Heisenberg, xii
uncertainty principle, 347, 348, 635
Hermitian
conjugation, see Conjugation operator, see Operator
Hexadecimal system, 128, 129
Hilbert space, 334
Hindu-Arabic numerals, see Numerals
Hirschberg, D. S., 183, 192, 207
Histogram, 4, 30–2
Holevo bound, xx, 431, 444, 450–4, 475, 485, 666–71
HSW Theorem, see Theorem
HTML, 131
Huang, Y.-F., 375
Huffman
code/coding, xix, 137, 145, 151–7, 160–3, 168, 169, 176, 179, 181, 186, 192, 193, 200, 600 compression, see Compression
IA2 (International Alphabet), 131
IBM (Lucifer cryptosystem), 523, 530, 532, 541
Image/picture compression, see Compression
Imaginary exponential, see Exponential
IMDD, see Intensity-modulation
Impersonation attack, see Attack
Independent
events, see Event sources, 75
Informatio (Latin), 37
Informatics, 39
Information, xi
algorithmic, 96, 97, 111
algorithmic (-) theory, 96, 111
bit, see Bit
classical, 305, 306
coding, xix, 127
concept, 37, 111
conditional, 43
contents, 40, 432
uncorrelated, 431, 441, 445–7, 449
definition, xvii
entropy concept, 286
erasure, 287
loss, 162
meaning, 38
measure/measuring, xviii, 37, 40, 50, 52, 53
mutual (classical), xix, 69, 74, 75, 77, 81, 85, 122, 238, 240, 241, 245, 266, 267, 624
mutual (quantum), 441, 447, 450, 475, 484, 486, 669
overhead, see Overhead
physical nature of (-), 283, 287
reconciliation, 524, 557
quantum, 435, 436, 441, 443
quantum coherent (-), 475, 486
Information (cont.)
    science, 39, 40
    self (-), 286
    spectral density, 270
    standards, 591
    theory (Shannon’s), xi–xii, xiv, xvii, 37, 39, 40,
    96, 287, 304, 342, 431
    uncorrelated (-), 445
Inner product of states, 330, 333–7
    distinguishable, 258, 259
    non-confusable (-) fan, 259
Instantaneous code, see Code
Integer coding, see Coding
Intelligence
    artificial, 39
    definition, 32, 38–9
Intensity-modulation/direct-detection (IMDD)
    format, 226
Interleaver, 224
International Alphabet, see IA2
Internet, 39, 40, 129–31, 226, 367, 398, 411, 424,
    428, 529, 564, 592
Inverse Fourier transform, see Fourier transform
IPv6, 425
Irreversible computation, see Computation
ISDN (integrated services digital network), 591
    Italian language source, 58, 160
ITU-T, 592
Jaynes, E. T., 50
Jelly beans, 11
Jensen’s inequality, 124
Joint
    entropy, see Entropy
events, see Event
    probability/distribution, see Probability
Jokes, 41
JPEG, 161, 191, 598–600
Kahn, D., 525
Kernel, 437
Ket, 306, 334
Key
    asymmetric (-) cryptography, see Cryptography
    attack, 563
double or two (-) encryption, see Encryption
    exchange, 523, 525, 532, 561
private, 425
public, 425
secret, 425, 523, 524, 529, 536, 541, 543, 555
    secret (-) distillation, 524, 557
    space, 525, 536, 541, 542
    symmetric (-) cryptography, see Cryptography
    without (-) exchange, 523, 527, 534–6
Keyspace, see Key
Klein’s inequality, 437, 440, 660
Knuth (code), see Code
Kolmogorov
    A., 96
    complexity xiii–xv, xix, 96, 97, 107, 110, 111, 123, 411
    conditional complexity, 116, 119, 122
    convergence with Shannon’s entropy, 123–5
    un-computationability of complexity, 117, 118
    upper bound, 117
    Kolmogorov–Chaitin complexity, see Kolmogorov
Kraft inequality, 142
Kraft–McMillan inequality, 142, 143, 589–90
Kronecker
    product, 328
    symbol, 233, 313, 335
Kubrick, S., 39
Kullback–Leibler distance, see Distance
Lagrange
    multiplier/parameter method, 64, 66, 91, 92, 142,
    573, 574, 579
    theorem, see Theorem
Laloe, F., 635
Landauer, R., 286
    bound/limit, 286
    principle, xv, xix, 283–8, 296
Language
    coding, see Coding
    entropy, see Entropy
    distribution, see Probability
    model, 190
    rule, 191
Laser, 32, 65
Lavor, C., 390
Lelewer, D. A., 183, 192, 207
Lempel, A., 200
Lempel–Ziv coding, see Coding
    length (codeword), see Codeword
    Lempel–Ziv algorithm, see Algorithm
Levi, S., 424, 525
Levi–Civita (symbol), 314
Lieb theorem, see Theorem
Lifetime (1/e), 28, 88
Ligature, 167
Limiting PDF, 33
Lin, S., 614
Linear
    block codes, see Code
    polarization, see Polarization
    locality, 367
    non (-), see Non
Logic gate, see Gate
Logistic (-) distribution, see Probability
Log-normal distribution, see Probability
<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lossless compression, see Compression</td>
<td>41</td>
</tr>
<tr>
<td>Lossy compression, see Compression</td>
<td></td>
</tr>
<tr>
<td>Lotto, 41</td>
<td></td>
</tr>
<tr>
<td>Lucifer cryptosystem, see IBM</td>
<td></td>
</tr>
<tr>
<td>LZ1/LZ2, see Coding</td>
<td></td>
</tr>
<tr>
<td>LZ77/LZ78, see Coding</td>
<td></td>
</tr>
<tr>
<td>$M$-ary modulation format</td>
<td></td>
</tr>
<tr>
<td>$M$-FSK, 274</td>
<td></td>
</tr>
<tr>
<td>$M$-PSK, 274</td>
<td></td>
</tr>
<tr>
<td>$M$-QAM, 275</td>
<td></td>
</tr>
<tr>
<td>MacKay, D. J. C., 155, 187, 207, 605</td>
<td></td>
</tr>
<tr>
<td>Majority logic, 210, 496</td>
<td></td>
</tr>
<tr>
<td>Man-in-the-middle attack, see Attack</td>
<td></td>
</tr>
<tr>
<td>Mangler, 531</td>
<td></td>
</tr>
<tr>
<td>Mangling function, 531</td>
<td></td>
</tr>
<tr>
<td>Markov chain, 82, 83, 581–4</td>
<td></td>
</tr>
<tr>
<td>Matrix</td>
<td></td>
</tr>
<tr>
<td>commutator/commuting, see Commuting</td>
<td>18</td>
</tr>
<tr>
<td>conditional, 18</td>
<td></td>
</tr>
<tr>
<td>density, 333, 341–3, 431, 432, 465</td>
<td></td>
</tr>
<tr>
<td>determinant, 338</td>
<td></td>
</tr>
<tr>
<td>diagonal form/representation, 333, 339, 341, 432–4, 460</td>
<td></td>
</tr>
<tr>
<td>elements, 337</td>
<td></td>
</tr>
<tr>
<td>generator, 212, 509, 515</td>
<td></td>
</tr>
<tr>
<td>Hadamard, 58, 220, 312, 314, 315, 319, 329, 339, 549</td>
<td></td>
</tr>
<tr>
<td>Hermitian-conjugate, 312, 627</td>
<td></td>
</tr>
<tr>
<td>identity, 304, 312</td>
<td></td>
</tr>
<tr>
<td>inverse, 312</td>
<td></td>
</tr>
<tr>
<td>operator (-) elements, 333, 337–8</td>
<td></td>
</tr>
<tr>
<td>parity-check, 212, 509, 514</td>
<td></td>
</tr>
<tr>
<td>partial trace/tracing, 438, 445, 446, 665</td>
<td></td>
</tr>
<tr>
<td>Pauli, xix, 304, 312–15, 319, 327, 329, 339, 478, 499, 503, 505, 551, 627, 631</td>
<td></td>
</tr>
<tr>
<td>trace, 333, 340–1, 433</td>
<td></td>
</tr>
<tr>
<td>transition, 18, 475, 582</td>
<td></td>
</tr>
<tr>
<td>transposed, 312</td>
<td></td>
</tr>
<tr>
<td>unitary, 304, 312, 627, 632</td>
<td></td>
</tr>
<tr>
<td>Vandermonde, 385, 386</td>
<td></td>
</tr>
<tr>
<td>Maximizing entropy, see Entropy</td>
<td></td>
</tr>
<tr>
<td>Maximum entropy, see Entropy</td>
<td></td>
</tr>
<tr>
<td>length shift-register codes, see Code</td>
<td></td>
</tr>
<tr>
<td>likelihood decoding, see Decoding</td>
<td></td>
</tr>
<tr>
<td>Maxwell, J. C., 283</td>
<td></td>
</tr>
<tr>
<td>Maxwell–Boltzmann probability distribution, see Probability</td>
<td></td>
</tr>
<tr>
<td>Maxwell's demon, xix, 283–8</td>
<td></td>
</tr>
<tr>
<td>Mean</td>
<td></td>
</tr>
<tr>
<td>codeword length, see Codeword</td>
<td>26</td>
</tr>
<tr>
<td>continuous-variable, 26</td>
<td></td>
</tr>
<tr>
<td>discrete-variable, 20</td>
<td></td>
</tr>
<tr>
<td>of observable, see Observable</td>
<td></td>
</tr>
<tr>
<td>time to failure (MTTF), 29</td>
<td></td>
</tr>
<tr>
<td>Measurement, 305, 343</td>
<td></td>
</tr>
<tr>
<td>basis-states (-), 333, 337</td>
<td></td>
</tr>
<tr>
<td>Bell states (-), 365–7</td>
<td></td>
</tr>
<tr>
<td>failure, 358</td>
<td></td>
</tr>
<tr>
<td>$N$-qubit (-), 361–5</td>
<td></td>
</tr>
<tr>
<td>operator, see Operator</td>
<td></td>
</tr>
<tr>
<td>post (-) state, see State</td>
<td></td>
</tr>
<tr>
<td>POVM (-), 333, 343, 348–51, 450, 451, 483, 666</td>
<td></td>
</tr>
<tr>
<td>projection/projective (-), 333, 346, 359</td>
<td></td>
</tr>
<tr>
<td>single qubit (-), 356–60</td>
<td></td>
</tr>
<tr>
<td>state, 341</td>
<td></td>
</tr>
<tr>
<td>success, 358</td>
<td></td>
</tr>
<tr>
<td>von Neumann (-), 333, 343, 346, 348, 359</td>
<td></td>
</tr>
<tr>
<td>Measuring information, see Information</td>
<td></td>
</tr>
<tr>
<td>MEM, see Entropy</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td></td>
</tr>
<tr>
<td>computer, 287–90</td>
<td>108</td>
</tr>
<tr>
<td>space, 108</td>
<td></td>
</tr>
<tr>
<td>Memoryless</td>
<td></td>
</tr>
<tr>
<td>channel, see Channel</td>
<td></td>
</tr>
<tr>
<td>source, see Source</td>
<td></td>
</tr>
<tr>
<td>Microscopic state, 51</td>
<td></td>
</tr>
<tr>
<td>Microstate, 51, 66, 67, 285</td>
<td></td>
</tr>
<tr>
<td>Mitra, P. P., 278</td>
<td></td>
</tr>
<tr>
<td>Mobile/radio/cellular/wireless/3G</td>
<td></td>
</tr>
<tr>
<td>communications, 224, 225, 371, 592, 603</td>
<td></td>
</tr>
<tr>
<td>Modular</td>
<td></td>
</tr>
<tr>
<td>algebra/arithmetic, 302, 656–8</td>
<td></td>
</tr>
<tr>
<td>reduction, 657</td>
<td></td>
</tr>
<tr>
<td>Modulation format, 225</td>
<td></td>
</tr>
<tr>
<td>Modulus of vector, see Vector</td>
<td></td>
</tr>
<tr>
<td>Moment (PDF), 66</td>
<td>66</td>
</tr>
<tr>
<td>Monogram, 134, 169</td>
<td></td>
</tr>
<tr>
<td>Moore's law, 539</td>
<td></td>
</tr>
<tr>
<td>Morin, E., xii, xiii</td>
<td></td>
</tr>
<tr>
<td>Morse code</td>
<td></td>
</tr>
<tr>
<td>code, 132–6, 138</td>
<td>152</td>
</tr>
<tr>
<td>symbols, 132</td>
<td></td>
</tr>
<tr>
<td>Motion picture, see Picture</td>
<td></td>
</tr>
<tr>
<td>MPEG, 161, 191, 599, 601–4</td>
<td></td>
</tr>
<tr>
<td>MP3, 161, 595–6</td>
<td></td>
</tr>
<tr>
<td>MS-DOS, 207</td>
<td></td>
</tr>
<tr>
<td>MTTF, see Mean</td>
<td></td>
</tr>
<tr>
<td>Mu-law (or µ-law), 592</td>
<td></td>
</tr>
<tr>
<td>Multiplication operation</td>
<td></td>
</tr>
<tr>
<td>classical, 302</td>
<td></td>
</tr>
<tr>
<td>quantum, 326</td>
<td></td>
</tr>
<tr>
<td>Multivariate normal probability distribution, see Probability</td>
<td></td>
</tr>
<tr>
<td>Music coding, see Coding</td>
<td></td>
</tr>
<tr>
<td>Mutual information, see Information</td>
<td></td>
</tr>
<tr>
<td>Mutually exclusive events, see Events</td>
<td></td>
</tr>
<tr>
<td>Term</td>
<td>Page(s)</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>NAND (logical/Boolean)</td>
<td>291, 293, 299</td>
</tr>
<tr>
<td>Nat, 42, 52, 53, 84, 578</td>
<td></td>
</tr>
<tr>
<td>Neologism</td>
<td>58</td>
</tr>
<tr>
<td>Nielsen, M. A., 296</td>
<td></td>
</tr>
<tr>
<td>NIST (National Institute of Standards and Technologies)</td>
<td>541</td>
</tr>
<tr>
<td>NO (logical/Boolean)</td>
<td>76, 529</td>
</tr>
<tr>
<td>Noise, xix, 32</td>
<td></td>
</tr>
<tr>
<td>additive, 9</td>
<td></td>
</tr>
<tr>
<td>optical amplifier, 278, 280</td>
<td></td>
</tr>
<tr>
<td>quantum, see Quantum</td>
<td></td>
</tr>
<tr>
<td>Non</td>
<td></td>
</tr>
<tr>
<td>cloning theorem, see Theorem</td>
<td></td>
</tr>
<tr>
<td>locality, 367, 560, 562</td>
<td></td>
</tr>
<tr>
<td>observable phase, 625</td>
<td></td>
</tr>
<tr>
<td>trivial composites, 417</td>
<td></td>
</tr>
<tr>
<td>Nonlinear channel, see Channel</td>
<td></td>
</tr>
<tr>
<td>Normal</td>
<td></td>
</tr>
<tr>
<td>distribution, see Probability operator, see Operator</td>
<td></td>
</tr>
<tr>
<td>Normality, 32</td>
<td></td>
</tr>
<tr>
<td>NOT (logical/Boolean), 291, 299</td>
<td></td>
</tr>
<tr>
<td>controlled (-), 293</td>
<td></td>
</tr>
<tr>
<td>quantum gate, 312, 313, 319</td>
<td></td>
</tr>
<tr>
<td>NRZ format, see On-off</td>
<td></td>
</tr>
<tr>
<td>Nucleotide sequence, 185</td>
<td></td>
</tr>
<tr>
<td>Null (cryptographic), 425</td>
<td></td>
</tr>
<tr>
<td>Number</td>
<td></td>
</tr>
<tr>
<td>co-prime, 405, 649, 658</td>
<td></td>
</tr>
<tr>
<td>complex, 305, 307, 627, 653–5</td>
<td></td>
</tr>
<tr>
<td>prime, 302, 672</td>
<td></td>
</tr>
<tr>
<td>rational, 649</td>
<td></td>
</tr>
<tr>
<td>relatively prime, 658</td>
<td></td>
</tr>
<tr>
<td>Numerals</td>
<td></td>
</tr>
<tr>
<td>Arabic, 128</td>
<td></td>
</tr>
<tr>
<td>Hindu-Arabic, 128</td>
<td></td>
</tr>
<tr>
<td>Roman, 127–8</td>
<td></td>
</tr>
<tr>
<td>Nyquist, H., 50</td>
<td></td>
</tr>
<tr>
<td>Nyquist sampling rate, 269</td>
<td></td>
</tr>
<tr>
<td>Observable</td>
<td></td>
</tr>
<tr>
<td>307, 346, 359, 433, 440, 502, 635</td>
<td></td>
</tr>
<tr>
<td>conjugate, 348</td>
<td></td>
</tr>
<tr>
<td>mean, 347</td>
<td></td>
</tr>
<tr>
<td>non (-), 313, 344, 345, 357</td>
<td></td>
</tr>
<tr>
<td>variance, 347</td>
<td></td>
</tr>
<tr>
<td>Octal representation, 221</td>
<td></td>
</tr>
<tr>
<td>On-off keying (OOK), 226, 228, 272</td>
<td></td>
</tr>
<tr>
<td>One</td>
<td></td>
</tr>
<tr>
<td>time-pad cipher, 529</td>
<td></td>
</tr>
<tr>
<td>way function, 534, 657</td>
<td></td>
</tr>
<tr>
<td>OOK, see On-off</td>
<td></td>
</tr>
<tr>
<td>Operator, 311</td>
<td></td>
</tr>
<tr>
<td>diagonal representation, 333</td>
<td></td>
</tr>
<tr>
<td>exponential, 628-9</td>
<td></td>
</tr>
<tr>
<td>Grover (-), 391, 397</td>
<td></td>
</tr>
<tr>
<td>Hermitian, 339</td>
<td></td>
</tr>
<tr>
<td>joint-state measurement (-), 353</td>
<td></td>
</tr>
<tr>
<td>matrix elements, see Matrix measurement, 343, 348, 356</td>
<td></td>
</tr>
<tr>
<td>normal, 340</td>
<td></td>
</tr>
<tr>
<td>projection/projector, 333, 336–7, 461, 500</td>
<td></td>
</tr>
<tr>
<td>reduced density (-), 446</td>
<td></td>
</tr>
<tr>
<td>rotation, 319, 357, 629–31, 634</td>
<td></td>
</tr>
<tr>
<td>spectral decomposition, 333, 339, 346</td>
<td></td>
</tr>
<tr>
<td>sum representation, 477, 479, 480, 508</td>
<td></td>
</tr>
<tr>
<td>tensor, 352</td>
<td></td>
</tr>
<tr>
<td>transformation, 343</td>
<td></td>
</tr>
<tr>
<td>transition, 338</td>
<td></td>
</tr>
<tr>
<td>unitary, 311, 312, 314, 357, 384, 476</td>
<td></td>
</tr>
<tr>
<td>Optical</td>
<td></td>
</tr>
<tr>
<td>amplifier, 277</td>
<td></td>
</tr>
<tr>
<td>communications/telecommunications, 227</td>
<td></td>
</tr>
<tr>
<td>fiber, 32, 208, 277, 371</td>
<td></td>
</tr>
<tr>
<td>Optimal/optimality (coding), see Coding OR</td>
<td></td>
</tr>
<tr>
<td>exclusive, see XOR</td>
<td></td>
</tr>
<tr>
<td>logical/Boolean, 76, 291, 293, 529</td>
<td></td>
</tr>
<tr>
<td>Oracle, 390, 396, 397</td>
<td></td>
</tr>
<tr>
<td>Order</td>
<td></td>
</tr>
<tr>
<td>finding algorithm, see Algorithm of (integer) modulo N, 405</td>
<td></td>
</tr>
<tr>
<td>Orthonormal basis, see Basis</td>
<td></td>
</tr>
<tr>
<td>Osgood, B., 170</td>
<td></td>
</tr>
<tr>
<td>Outcome, see Event</td>
<td></td>
</tr>
<tr>
<td>Output (non-confusable), 258</td>
<td></td>
</tr>
<tr>
<td>Overhead (information), 159, 160, 162, 199, 209, 210</td>
<td></td>
</tr>
<tr>
<td>Parallellism (quantum), see Quantum</td>
<td></td>
</tr>
<tr>
<td>Pareto probability distribution, see Probability</td>
<td></td>
</tr>
<tr>
<td>Parity</td>
<td></td>
</tr>
<tr>
<td>bit, see Bit</td>
<td></td>
</tr>
<tr>
<td>check matrix, see Matrix</td>
<td></td>
</tr>
<tr>
<td>check polynomial, see Polynomial</td>
<td></td>
</tr>
<tr>
<td>Parsing, 200</td>
<td></td>
</tr>
<tr>
<td>distinct (-), 200, 205, 610</td>
<td></td>
</tr>
<tr>
<td>Partial trace/tracing, see Matrix</td>
<td></td>
</tr>
<tr>
<td>Party (meeting), 15–16</td>
<td></td>
</tr>
<tr>
<td>Pauli, W., 312</td>
<td></td>
</tr>
<tr>
<td>Pauli matrices, see Matrix</td>
<td></td>
</tr>
<tr>
<td>vector, 630</td>
<td></td>
</tr>
<tr>
<td>Payload, 162, 209</td>
<td></td>
</tr>
<tr>
<td>bit, see Bit pattern, 225</td>
<td></td>
</tr>
<tr>
<td>PDF, see Probability</td>
<td></td>
</tr>
<tr>
<td>PDFH (plesiosynchronous digital hierarchy), 592</td>
<td></td>
</tr>
<tr>
<td>Perec, G., 186</td>
<td></td>
</tr>
<tr>
<td>Permutation, 9</td>
<td></td>
</tr>
</tbody>
</table>
Personal digital assistant, see Personal Phase, 345
eigenstates, 345 estimation, 399–404
flip channel, see Quantum channel
measurement operator, 345
non-observable (-) factor, 625, 631
Philips, 592
Photon, 65
Photocurrent, 278 Photon, 65, 544, 549, 551, 556 circularly-polarized, 552
communication channel, 551, 554–8
energy, 577
statistics, 576
Photonics, 32
Picture compression, see Compression motion, 161, 191
still, 191
PKARK, 207
PKZIP, 207
Plain text, 61, 424
Planck, xii, xiv
Planck’s constant, 65
Plenio, M. B., 296, 300, 326
PNG, 207, 600
Podolski, xiii
Point or presence (POP), 563
Poisson distribution, see Probability process, 24
Polarization
beamsplitter, 551
circular, 546, 549, 552
EM state, 549
horizontal (TM), 545
left-circular, 546
light, 545
linear, 545, 549
orthogonal, 545
right-circular, 546
state, 545, 547
vertical (TE), 545
Pollard algorithm, see Algorithm
Polynomial
generator, 218
irreducible, 218, 542, 672
multiplication, 672
parity-check, 218
representation (byte), 542, 672–5
syndrome, 219
time, 399, 410
time complexity, 400
Portuguese language source, 58, 160
Post-measurement state, see State
POVM measurement, see Measurement Prefix, see Codeword
Prefix code, see Code
Prime
decomposition into (-), 410, 424
factorization/factoring into (-), see Factorization number, see Number relatively, see Number Privacy amplification, 524, 557 Proakis, J. G., 221, 223, 589 Probability distribution
Bernoulli, 24, 25
binomial, 24, 25, 32
Boltzmann, 65
Bose–Einstein (BE), 23, 65, 91, 573, 574, 576
Cauchy, 90
character, 57
Chi/Chi-squared, 90
combined, 13
conditional, 14, 15, 70
continuous, 26
distance between (-), see Distance
Erlang, 90
exponential
continuous, 28, 88, 90, 93
discrete, 23, 57, 58, 65, 69, 91, 573, 574, 576
density function (PDF), 5, 20, 264
F, 90
Gamma, 90
gaussian, 25, 29–33, 66, 89, 90, 93
generalized normal, 90
joint, 13, 15, 42, 70, 73, 80, 81, 581
Laplace, 90
law of total (-), 17
log-normal, 32, 90
logistic, 90
Maxwell–Boltzmann, 90, 573, 576, 577
moments, see Moment
multivariate normal, 90
normal, 25, 29, 33, 89, 90, 93
of event, 3
optimization constraints, 65
Pareto, 90
Poisson, 23, 25, 32
Rayleigh, 90
stationary, 583
Student’s t, 90
theory, xvii
thermal (or Bose–Einstein), 573
triangular, 90
uniform
discrete, 6, 22, 26, 80, 90, 573, 583
continuous, 86, 87, 90, 241, 246
Weibull, 90
Projection/projector measurement, see Measurement operator, see Operator
Pseudo-binary code, see Binary
Psychoacoustics analysis, 595
Public-key cryptography, see Cryptography
Pulse code modulation (PCM), 592
Pure state, see State
Purification, see State
Purifying system, 442
Q-factor, 226
QIT, see Quantum information theory
QKD, see Quantum key distribution
Quanta (energy), 544
Quantum bit, see Qubit channel, 431, 450–4, 475, 476, 497, 559, 561, 667
capacity, 482, 487–93
communication, 476
bit-flip, 475, 479–80, 491–3, 496, 497
bit-phase-flip, 475, 480–1
depolarizing, 475, 477–8, 488–91
ideal or noiseless, 475, 476, 489
nonideal or noisy, 477, 481, 498
phase-flip, 475, 480, 496, 501
useless, 478, 493
channel capacity, 475
circuit, xx, 304, 314, 322–7
code, 484
codeword, 457
coherence, 561
coherent information, see Information compression, 457–64
computation/computing, xix, 305, 310, 311, 356, 378, 380
computer, xx, 310, 398, 399, 536
cryptography, see Cryptography decoherence, xx, 561
distributed (-) computing, 356
energy/light (quanta), 23, 25, 65
entanglement, see Entanglement error, 457
bit-flip (-), 506, 507
phase-flip (-), 505, 507
error correction, xx, 496, 497, 562
Calderbank–Shor–Steane (CSS), 496, 509, 511, 513
Hadamard–Steane, 496, 514–20
Shor (-) code, xx, 496, 503–9
Fourier transform, xv, xix, 378, 383–9, 403, 644–7
gate, xx, 311, 314, 374
gate teleportation, see Teleportation information, see Information
information theory (QIT), xii, xiv, xvii–xviii, 264, 283, 287, 304, 305, 342, 343, 431
inverse Fourier transform, 403
key distribution (QKD), xv, xvii, xx, 523, 544, 556–8, 561, 562, 564
measurement, see Measurement mechanics, 305
memory, 497
network, 356
noise, 475, 557, 561
noisy (-) channel, 475
operation, 451, 476, 477, 481, 488, 491, 492, 499, 508, 556, 667
parallelism, 378, 380, 383
repetition code, 496–503
state, see State
teleportation, see Teleportation wire, 381
Quarter-wave plate, see Wave plate
Qubit, xix, 304–10, 334, 435
amplitude, 306
ancilla, 370, 379, 401
control, 316
entangled, 356
joint, 356
target, 316, 370
teleportation, see Teleportation two (-), 309
vector, 334
wire, 381
Qudit, 372
Quincunx, 34
QuNit/qunit, 372, 435
Qutrit, 374
Random-number generation, 191, 563
Rate
bit error (-), see Bit error rate
code (-), see Code compression (-), see Compression parameter, 28
Rational number, 408
Rayleigh distribution, see Probability
Receiver, 208
Recipient, 37, 40, 41
Red Book, 592
Redundancy (code), see Code
Reed–Solomon codes, see Code
Register, 289, 290, 301, 382
Relative entropy, see Entropy
Reliability (theory), see Einstein
Reliability function, see Function
Rényi, A., 45
REPEAT gate, 294, 297, 312
Residue, 656
Return loss, 563

| Reversible computation/transformation, see Computation |
| Rice codes, see Code |
| Riemann integral, 587 |
| Rivest, R., 424, 536 |
| Rolling dice, 4, 16, 21, 22, 34, 44, 53–6 |
| Roman numerals, see Numerals |
| Rosen, xiii |
| Rotation operator, see Operator |
| Roulette game, 170 |
| Round (DES), 531 |
| RSA challenges, xv, 411, 415, 523, 537, 541 |
| cryptosystem, 523, 536–40 |
| modulus, 425 |
| Security, 537 |
| standard, 424, 428 |
| S-box, 542 |
| Sample space, 2 |
| Satellite communications, 224, 225 |
| Schmidt coefficients, 438, 439, 662 |
| decomposition, 438, 662–3 |
| Schneier, B., 425, 540 |
| Schrödinger’s cat, see Cat |
| SDH (or SONET), 592 |
| Second law/principle of thermodynamics, see Thermodynamics |
| Secret exchange (simultaneous), see Simultaneous key, see Key |
| Semantic-dependent coding, see Coding |
| Shamir, A., 424, 536 |
| Shank algorithm, see Algorithm |
| Shannon, C. E., 50, 52, 69, 85, 86, 256, 283, 568 |
| Shannon code, 144, 145, 148, 149, 152, 155 |
| Fano code, 144, 152, 154–6, 167, 168, 175, 176, 179 |
| first theorem, see Theorem, source-coding entropy, see Entropy |
| information definition, 37 |
| information theory, see Information limit, 272 |
| second theorem, see Theorem, channel coding source-coding theorem, see Theorem |
| Shannon–Hartley law, see Theorem theorem, see Theorem |
| Shift register, 223 |
| Shor factorization algorithm, see Algorithm |
| quantum error-correction code, see Quantum |
| Shumacher’s quantum coding theorem, see Theorem |
| quantum compression, 457, 469–74 |
|Sibling property (rule), 193 |
| Signal-to-noise ratio, 226, 267, 278 |
| Similarity transformation, 333, 338 |
| Simultaneous secret exchange, 543 |
| Singh, S., 61, 69, 424 |
| Sit, 45 |
| Solomonoff, R., 96 |
| SONET, 592 |
| Sony, 592 |
| Sound compression, 185 |
| digital, 161 |
| Source coding theorem, see Theorem continuous, 84 |
| discrete, see Events extension, 163, 206 |
| information, 53 |
| language, 57 |
| memoryless, 206 |
| quantum, 434 |
| random, 52, 53 |
| Space Odyssey (2001), 39 |
| Spanish language source, 160 |
| Spectral decomposition of operator, see Operator |
| density, see Information spectral efficiency |
| Speech/voice analog-to-digital (A–D), 592 |
| compression, 591 |
| Speed of light, 356, 371 |
| Standard audio and video, xix |
| compression, see Compression deviation, 21 |
| Stark, J. B., 278 |
| State ancilla, 354 |
| Bell or EPR (–), 310, 318, 356, 362–5, 367, 369, 370, 374, 388, 448, 559–61, 637 |
| cat (–), 307 |
| collapse, 307, 357, 358, 363, 371, 559–62 |
| eigen (–), see Eigenstate entangled, see Entanglement EPR, see State (Bell) GHZ, 374 |
| joint, 328, 351, 353, 437 |
| joint post-measurement (–), 353 mixed, 448 orthogonal, 306, 435 polarization, see Polarization post-measurement (–), 310, 344, 346, 352, 353, 357, 360, 498, 558–60, 641, 667 |
Index

State (cont.)
  pure, 304, 314, 330, 331, 432–4, 452, 454, 487, 664
  pure joint, 437, 445, 448
  purification, 486, 664–5
  quantum, 334, 343, 432, 450
  superposition, 305, 306
  tensor (-), see Tensor
  transport of quantum (-), 367
  unambiguous quantum state discrimination (UQSD), 333, 351

Static
  code, see Code
  coding, see Coding
  Statistical mechanics, 50
  Steane code, see Quantum error correction

Stirling’s formula or approximation theorem, 9, 119, 566

Stock exchange, 71, 73

Stream coding, see Coding

Student’s t probability distribution, see Probability

Subadditivity
  inequality, 439–41, 447
  strong (-), 451, 671

Subtraction (quantum operation), 326

SUM gate, 299, 325

Superdense
  coding, xv, xix, 356, 366
  teleportation, 374

Superposition of states, see State

Support space, 437, 443, 444, 452

Surprise, 41, 43, 45

Symbol, 44–5, 53

error, see Error

Syndrome, 212, 215

  polynomial, see Polynomial
  quantum, 497, 503, 505, 506, 508, 511

Systematic
  code representation, see Code

  output, 224

SWAP gate, see CROSSOVER

Szilárd, L., 50, 285, 286

Table
  look-up, 162
  of instructions (Turing machine), see Action
table
  truth, 291

TCP/IP, 225

Telecommunications, 32

Teleportation, xv, xix, 356, 450, 559, 560

  of quantum gates, 356
  of qubits, 372
  of two qubits, 372–4, 637–43

Temperature (absolute), 284

Tensor
  operator, see Operator
  product, 304, 316–19, 327–9
  state, 309, 316, 327–9, 351

Ternary code, 134

Theorem
  band-limited capacity (-), 270
  Bayes’s, 14, 15, 43, 71, 78, 239, 618
  Boltzmann’s, 52
  central limit (CLT), 32–4, 66
  channel capacity, xiv
  channel coding (-), 232, 245, 252, 255–62, 264, 475, 481, 482, 484, 621–4
  Euler, 426, 631–4, 656–9
  Fermat, 658
  Holevo–Schumacher–Westmoreland (HSW), xx, 475, 481–7
  information capacity (-), 269
  Lagrange, 510
  Lieb, 671
  noncloning (-), 304, 328, 330–1, 335, 369
  Schumacher’s quantum coding (-) or noiseless channel coding (-), 462, 464–9

  Shannon–Hartley, xiv, xix, 264, 269, 279
  Shannon’s second (-), 255
  source-coding (-), xix, 127, 138, 142–9, 163, 245
  Stirling, see Stirling
  typical subspace (-), 467

  Theory of information, see Information

  Thermal process, 23

  Thermodynamics, 286
  second law/principle, 50, 69, 82, 283, 285, 581, 584–6
  Thomas, J. A., 90, 111, 148, 206, 252, 578, 583, 587, 610, 621
  TIFF, 207, 601

  Time
    constant, 28
    division multiplexing (TDM), 591
    stamping, 543
  Todd, Odgen, 34
  Toffoli gate, 298, 299, 320, 322, 325
  Tongue, 57
  Tossing coins, see Coin
  Trace (matrix), see Matrix
  Trailer (block), see Block
  Transistor-transistor logic, see TTL

  Transition
    matrix, 233

    operator, see Operator
    Transmission pipe, 208
    Transmitter, 208
    Transposition (matrix/operator), 328
    Trapdoor function, 541
    Tree, see Coding
Triangle inequality, 442
Triangular probability distribution, see Probability
Trit, 134, 136
Trust interval, 22
Truth table, see Table
TTL, 294
Turbo codes, see Code
Turing, A., 97, 107
Turing complete computer, 290
equivalent computer, 290
machine, xiv, xix, 97, 108, 110, 111, 289
universal (-) machine (UTM), 96, 107, 114, 116, 289
Typewriter (noisy channel), see Channel
Typical sequence (classical), , 245, 252–5
sequence (quantum), 460, 464, 465
set, 245, 252–5
state (quantum), 460
subspace (quantum), 465, 469, 471–3, 483
subspace theorem, see Theorem
Typicality, 457
UMTS (3G), 225
Unambiguous quantum state discrimination (UQSD), see State
Unary number representation/system, 100, 128
Uncertainty, 347
Heisenberg (-) principle, see Heisenberg
Uncomputable number, 107
Uncorrelated events, see Event
Undecidable problem, 108, 110, 117, 290
Uniform distribution, see Probability
Uniquely decodable (code), see Code
Unitary
matrix, see Matrix
operator, see Operator
transformation, 311, 333, 337, 631
vector, 306
Universal Turing machine, see Turing
Universe, 50
UNIX, 199
UTM, see Turing
Vandermonde matrix, see Matrix
Variance, 21, 26
of observable, see Observable
Vector length/modulus, 334
Vedral, V., 296, 300, 326
Venn diagram, 12, 76, 79
Video compression, see Compression
Viterbi algorithm, 223
Vitter algorithm, 200
VLSI (very large scale integration), 540
von Neumann, J., 50, 286
von Neumann architecture/computer, 283, 288, 290, 301, 306, 378, 382, 383
entropy, see Entropy
Landauer bound, 286
Wave plate
half, 551
quarter, 548
Weibull probability distribution, see Probability
Wi-Fi (802.11), 225
William algorithm, see Algorithm
World
War (first), 132
War (second), 526
Wide Web, 207
XOR (logical/Boolean), 291, 293, 299, 368, 529
Z channel, see Channel
Zip, 207, 596–7
Ziv, J., 200
Ziv–Lempel coding, see Coding