

Index

- Aaronson, Scott, 261
 action, 42, 44, 61, 72
 addition
 of vectors, 30
 additive inverse
 of a vector, 32
 Adleman, Leonard, 266, 322
 adjoint, 39
 Aharonov, Dorit, 219
 Aharonov, Yakhir, 112
 algebraically complete, 14
 algorithm
 Deutsch–Jozsa, 4, 170, 179–187, 196, 218, 259, 321, 322
 Deutsch’s, 4, 170–180, 218, 230, 233
 Euclid’s, 217
 Grover’s search, 4, 170, 195–204, 218, 235, 259, 260, 322, 367
 Huffman’s, 298, 304
 Lempel–Ziv lossless compression, 296
 modular-exponentiation, 218
 Shor’s factoring, 4, 170, 204–219, 230, 259, 315, 322, 323, 361, 367
 Simon’s periodicity, 4, 170, 187–196, 209, 218, 259, 322
 amplification lemma, 250, 257
 analytic functions, 28
 Argand plane, *see* complex plane
 arXiv, 358, 359
 associativity
 of vector addition, 31
 authentication, 267

 B92 protocol, 273–275
 Barenco, Adriano, 321
 Barrow, John D., 239
 basis, 47–53, 68, 183
 canonical, 47–49, 59
 orthogonal, 57
 orthonormal, 57, 59, 64, 295
 standard, *see* basis, canonical
 BB84 protocol, 268–273, 275–277, 283, 323
 Bell basis, 278–283

 Bell, John, 277, 278, 364
 Bell’s inequality, 277, 364
 Benioff, Paul, 320
 Bennett, Charles, 153, 268, 273, 323, 324, 366
 Berggren, Karl, 317
 Bernstein, Ethan, 321, 322
 Berra, Yogi, 316
 Bettelli, Stefano, 222
 bijective, 15
 bilinear map, 68
 billiard ball
 quantum, 91
 stochastic, 84, 87, 91, 92
 bit, 138
 Bloch sphere, 161
 Bohm, David, 364
 Bohr, Niels, 316, 364
 Bombelli, Rafael, 28
 Boole, George, 277
 Bouwmeester, Dik, 324
 BPP, 249–251, 258
 BQP, 257, 258
 bra, 112
 Brassard, Gilles, 268, 323

 Caesar’s protocol, 263
 Calderbank, A.R., 324
 Cardano, Gerolamo, 28
 Cartesian product
 of graphs, 99, 100
 of sets, 45
 of vector spaces, 45, 49, 66, 68
 Cartesian representation, 18, 352
 Cauchy sequence, 59
 Chuang, Isaac L., xii, 315, 322
 ciphertext, 262
 Cirac, J.I., 311
 Cirasella, Jill, xii, xiii, xvi, 319, 357
 Collins, Graham P., 310
 complex algebra, 42
 complex analysis, 27
 complex conjugation, 14, 39
 complex plane, 16, 17, 21, 362

382 Index

- complex subspace, 42, 43
- complexity class, 243
- configuration, 242, 247, 252–255
- coNP, 245, 246, 251, 258, 369
- coP, 245, 246, 251, 258
- coRP, 249–251, 258
- Crépeau, Claude, 323
- Crow, Michael J., 363

- D-Wave Systems, 316
- dagger, *see* adjoint
- data compression, 295–302, 304
 - lossless, 295
 - lossy, 295
- De Broglie, Louis, 104
- De Moivre's formula, 25
- decoherence, 5, 303, 305–317, 324, 371
- decryption, 262
- decryption key, 263
- DeMorgan's law, 150, 151
- density operator, 288
- Deutsch, David, 169, 320, 321, 366
- Dick, Philip K., 103
- Dijkstra, E.W., 170
- dimension, 50–53, 183
- Diogenes Laertius, vi
- Dirac, P.A.M., 137
- distance function, 57
- DiVincenzo, David P., 310, 317, 321
- division, 11
- dot product, *see* inner product
- dynamics, 75, 79, 98

- Egan, Greg, 316
- eigenbasis, 64, 301, 302
- eigenspace, 62
- eigenvalue, 61–64, 354
- eigenvector, 61–62, 64, 354
- Eilenberg, Samuel, xv
- Einstein, Albert, 2, 104, 282, 364
- Ekert, Artur K., 275, 321
- elliptic curves, 267
- encryption, 262
- encryption key, 263
- entanglement, 2, 4, 100, 103, 132–137, 144, 164, 262, 275–278, 282, 306, 364, 370
- entropy, 5, 307, 371
- EPR paradox, 364
- EPR protocol, 275–277
- EQP, 258
- error-correcting, 302–310
- Euler's formula, 24
- Everett, Hugh, 364
- expected value, 120
- experiment
 - diffraction, 104
 - double-slit, 74, 93, 96, 102, 104, 105, 241, 256, 363
 - Elitzur–Vaidman bomb-tester, 363
 - probabilistic double-slit, 85
 - Stern–Gerlach, 110
- exponential form, 25

- Feynman, Richard, 96, 100, 102, 319, 320
- field, 14, 183
- Fine, Arthur, 364
- Fourier analysis, 1
- Fourier transform, 212, 367
 - discrete, 214, 368
 - fast, 368
 - quantum, 215, 368
- Frost, Robert, 262
- function
 - balanced, 171–187, 321
 - constant, 171–187, 321
 - transition, 240, 246, 252
- Fundamental theorem of algebra, 9

- Galilei, Galileo, 29
- gate
 - AND, 145, 147, 149–151, 155
 - controlled-NOT, 153–155, 158, 165, 311, 313, 355, 366
 - controlled-*U*, 164, 165
 - Deutsch, 165
 - Fredkin, 157, 158, 165, 168
 - Hadamard, 158, 165
 - identity, 151, 158
 - measurement, 159, 355
 - NAND, 146, 147, 156, 165
 - NOR, 147
 - NOT, 144, 145, 147, 149–151, 153, 155, 156, 158
 - OR, 146, 149, 150, 156
 - Pauli, 366
 - quantum, 3, 158–169, 366
 - reversible, 151–158
 - square root of NOT, 159
 - Toffoli, 154–156, 158, 165, 166, 168, 366
- Gay, J., 234
- Gershenfeld, Neil, 322
- Gibbs, Josia, 363
- Gödel, Kurt, 239
- Google, 354, 361
 - Blog Search, 357
 - News, 357
 - Scholar, 358, 359
- Grassmann, Hermann, 363
- group
 - Abelian, 32, 34
- Grover, Lov, 196, 322

- Hamilton, Sir William Rowan, 363
- Hamiltonian, 132
- HAMILTONIAN GRAPH, 259
- Heisenberg's uncertainty principle, 3, 120, 124, 125
- Held, Carsten, 365
- Heller, Alex, xv
- Heraclitus of Ephesus, vi
- Hilbert space, 60, 226, 311
- Huygens' principle, 363
- Holzscheiter, M., 317
- Huygens, Christiaan, 363

- id Quantique, 316, 323
- infinite
 - countably, 49
 - uncountably, 49
- inner product, 54, 65, 183
- inner product space, 54, 60
 - complete, 60
- instantaneous description, *see* configuration
- interference, 89, 92–95, 105, 256
- intrusion detection, 267

- inversion about the average, *see* inversion about the mean
 inversion about the mean, 198–204
 ion trap, 311–314
 isomorphism
 of fields, 15
 of graphs, 101
 of matrices, 101
 of vector spaces, 44, 50
- Jeans, Sir James, 138
 Jones, J.A., 315
 Josephson junctions, 315
 Jozsa, Richard, 321, 324
 Julius Caesar, 263
- Kernaghan, M., 365
 ket, 106
 Kirk, Captain James T., 283
 Knill, Emanuel, 238, 371
 Kochen–Specker theorem, 365
 Kronecker delta function, 57, 336
 Kryptonite, 262
 Kubinec, Mark, 322
 Kuhn, D. Richard, 370
- Landauer principle, 151, 365
 Landauer, Rolf, 151, 366
 length (of a vector), *see* norm
 linear combination, 45–47
 linear map, 43
 linear optics, 313–314
 linearly dependent, 47
 linearly independent, 46
 Lloyd, Seth, 321
 Lomonaco, Samuel J., 371
 Luthor, Lex, 262
- MagiQ Technologies, 316, 323
 MathWorks, 351, 352
 MATLAB, xii, xiii, xvi, 206, 260, 351–356
 matrix
 adjacency, 74, 97
 Boolean adjacency, 76
 change of basis, 51
 controlled-NOT, 226
 density, 302, 307
 diagonal, 64, 354
 doubly stochastic, 80, 83–85, 87
 Hadamard, 52, 53, 173–356
 hermitian, 62–64, 115–129
 identity, 41, 226
 invertible, 64
 multiplication, 40–42
 Pauli, 158
 phase shift, 226
 symmetric, 62, 63, 90
 transition, *see* matrix, change of basis
 unitary, 64–66, 89–96, 129–132, 171–173, 180, 181, 186, 188, 196–198, 200, 201, 214, 215, 217, 218, 336
 Vandermonde, 213
 Maxwell’s demon, 365
 mean value, 126
 measurement, 96, 115–129
 Meyer, David, 370
 Möbius transformation, 27, 362
 modulus, 13, 16
 Monroe, C., 311
 Mosca, M., 315
 Musil, Robert, 7
- Nagarajan, R., 225
 negative
 of a vector, 32
 Nielsen, Michael A., xii, 304
 NIST, 311, 315
 NMR, 315–316, 371
 No-cloning theorem, 166–169, 224, 268, 271, 278
 nonlocality, 2
 norm, 56, 65, 353
 normalization, 140, 141, 160
 normalized, 109
 NP, 244–246, 251, 258, 369
 NP-complete problem, 259
 numbers
 complex, 7–29, 361
 tractably computable, 251, 252
 imaginary, 9, 16
 natural, 8
 positive, 8
 rational, 8
 real, 8
 tractably computable, 246, 252
 whole, 8
- observables, 129
 Ömer, Bernhard, 234
 One-Time-Pad protocol, 265
 operations
 parallel, 148
 sequential, 147
 operator, 44
 self-adjoint, 62, 64
 oracle computation, 369
 orthogonal, 57
- P, 243–246, 250, 251, 258, 369
 Papanikolaou, N., 225
 parallelogram rule, 17
 pdf, *see* probability distribution
 Penrose, Sir Roger, 7, 316
 period (of a function), 188–195
 phase, 19
 phase change, 162
 phase inversion, 197–204
 phase shift, 356
 photoelectric effect, 96, 104
 plaintext, 262
 pointwise, 44
 polar representation, 18, 19, 352
 polarization, 313
 Pollard’s rho heuristic, 367
 polynomials, 9, 26, 43
 Pratt certificate, 369
 primality testing, 369
 probability distribution, 285
 PSPACE, 245, 246, 251, 258
 Pythagoras’ theorem, 16
- QFC, 236
 QRAM, 220–238, 256, 368
 sequential, 368

384 Index

- QSPACE, 258
 Quack, xiii, xvi, 354–356
 Quantiki, 357
 quantum assembler, 222
 quantum circuits, 222, 256
 quantum data compression scheme, 299
 quantum eraser, 363
 quantum error-correction, 371
 quantum error-detection, 371
 quantum finite automata, 369
 quantum games, 370
 quantum hardware interface, 223, 224
 quantum key exchange, 268–277
 quantum machine language, 222
 quantum register, 224
 qubit, xiii, 3, 138, 139
 qubyte, 143, 225
- Rüdiger, R., 234
 rational functions, 27
 reduced Planck constant, 117
 reflection
 imaginary axis, 14
 real axis, 14
 representation of an operator, 44
 Riemann sphere, 362
 Rivest, Ronald, 266, 322
 Rohde, Peter, xvi, 354
 Rohit Parikh, xv
 roots of unity, 25
 RP, 249–251, 258
 RSA, 266, 322, 323, 361, 370
- Saint Exupry, Antoine de, 305
 SAT, 259
 Savitch's theorem, 245, 258
 Sayood, Kahil, 304
 scalar, 33
 scalar multiplication, 33
 scalar product, *see* inner product
 Schrödinger equation, 131, 132
 Schrödinger, Erwin, 363–365
 Schrödinger's cat, 365
 Schumacher, Benjamin, 301, 324
 Schumacher's quantum coding theorem, 301, 304
 Scopus, 358, 359
 Selinger, Peter, 234, 236
 Shamir, Adi, 266, 322
 Shannon, Claude, 5, 284, 297, 304, 324
 Shannon entropy, 284–302
 Shannon's noiseless channel coding theorem, 297, 301
 Shor, Peter, 204, 219, 303, 322–324
 Simon, Daniel R., 322
 skew symmetric, 54
 Smart Quantum, 323
 snapshot, *see* configuration
 Spectral theorem for self-adjoint operators, 64, 292
 spin, 109, 141, 355
 SQP, 315
 stabilizer codes, 371
 state
 entangled, 135
 entangled, 71
 mixed, 307
 pure, 306
 separable, 71, 135
 well-defined, 288, 306, 311
 statistical mechanics, 2
 Steane, Andrew M., 324
 subfield, 14
 subtraction, 11
 Sudoku game, 316
 Suetonius, 263
 superconductor, 315
 superposition, 2–4, 96, 97, 107, 256
- Tartaglia, Niccol Fontana, 28
 Taylor expansion, 24
 Technorati, 357
 teleportation, 5, 262, 277–283, 324
 tensor product
 of matrices, 71, 99–101, 150, 354
 of vectors, 69, 98, 100
 of vector spaces, 66–73, 102, 132–137
 thesis
 classical Church–Turing, 241
 Cook–Karp, 243
 strong Church–Turing, 251, 259
 time symmetry, 82
 trace, 55, 353
 transporting, 167
 transpose, 39
 triangle inequality, 56, 57, 295
 Turing, Alan, 239
 Turing machine, 239, 260
 deterministic, 239–244, 258
 nondeterministic, 239, 243–246
 probabilistic, 239, 246–253, 260
 quantum, 5, 223, 239, 252–260, 320, 369, 370
 well-formed, 255
- unit circle, 24
 unit sphere, 65
 universal logical gates, 165
 universal quantum gates, 165
- Vazirani, Umesh, 321, 322
 vectors, 16
 vector space, 362
 F_2 , 183
 \mathbb{Z}_2 , 183
 complex, 29–73, 183, 254
 real, 34, 183
 Vernam cipher, *see* One-Time-Pad protocol
 von Neumann entropy, 288, 302
- Wang, Hao, 239
 wave mechanics, 1, 363
 Web of Science, 358, 359
 Wiesner, Stephen, 323
 Wigner's friend, 365
 Wikipedia, 358
 Williams, D., 225
 Wineland, D., 311
- Yao, Andrew Chi-Chih, 321
 Young, Thomas, 104, 105, 363
- zero vector, 32
 Zizzi, Paola, 316
 Zoller, P., 311
 ZPP, 250, 251, 258
 ZQP, 257, 258
 Zurek, Wojciech H., 317