

Index

- #P (complexity class), 253–257, 260, 286, 288
 1-norm, 112–113, 117, 119, 146
 2-norm, 112–113, 117, 119, 146
 2SAT, 70
 3-coloring, 191–193
 3SAT, 59–64, 70, 194, 203–204, 219, 250, 289
- AC⁰** (complexity class), 259–261
ACC⁰ (complexity class), 260–261
 Adleman, Leonard, 87–88, 91, 102, 139, 283
 AdS/CFT, 346
 advice, 83–90, 202, 211–215, 217, 320
 Agrawal, Manindra, 77, 88
 Aharonov, Dorit, 223
 Aharonov, Yakir, 211
 Ahn, Louis von, 36
 Ajtai, Miklos, 100, 106, 258–259
 algebrization, 258, 260
 Alice, 69–70, 103, 127–128, 130–131, 176–178, 209–210, 303–305, 348–349, 354
ALL (complexity class), 213–214
 Allen, Woody, 214
 Alon, Noga, 239
AM (complexity class), 189, 245, 249, 265, 355
 Amazon, 102
 Ambainis, Andris, 210, 239, 341
 amplitudes, 28, 71, 109, 114–116, 119–123, 125, 131, 139, 146–148, 160, 179, 201, 217, 220, 223, 283, 285, 341
 analog computer, 217, 222, 224
 Anderson, Pamela, 164
 anthropic principle, 169, 230, 266, 276–279, 282, 286, 289, 331, 358
 anyon, 226
 Appel, Kenneth, 37, 187
 Aristotle, 1–2
 arithmetization, 250, 258
- Arkhipov, Alex, 287–288
 Arora, Sanjeev, 51
 Arthur, 188–189, 203, 253–255, 257, 265
 Axiom of Choice, 14–16, 26–28
- Babai, Laszlo, 188, 206
 Babbage, Charles, 33
 Baez, John, 276
 Banach-Tarski paradox, 15
 Barak, Boaz, 51
 Bayesianism, 229, 232
 Bayesians, 5, 205, 232–233, 267, 271, 276, 289
 Bayes's Theorem, 228, 232, 266–268, 274, 276
 BB84 states, 127–128
 Beame, Paul, 319
 beamsplitter, 287
 Beigel-Reingold-Spielman Theorem, 285
 Bekenstein, Jakob, 32, 333–334
 Bekenstein bound, 333–334
 Bell, John, 162, 171, 176, 198
 Bell inequality, 6, 109, 171–172, 176, 302–305, 354
 Bennett, Charles, 127, 130, 137, 145–146, 149, 320–321
 Bernstein, Ethan, 139, 142–143, 145, 149, 224, 351
 Bierce, Ambrose, 291
 Big Bang, 85, 184, 212, 325–326, 328–330
 Big Crunch, 325–326
 birthday paradox, 196–197
 black box, 29, 141–142, 146, 153, 205, 248
 black-box group, 205
 black hole, 32, 202, 221–222, 307–308, 333–336, 344–349
 block universe, 301
 Blum, Lemoore, 98
 Blum, Manuel, 98
 Blum-Blum-Shub generator, 98
 Blum Speedup Theorem, 49, 82, 85

364 INDEX

- Bob. *See* Alice
 Bohm, David, 183–185
 Bohmian mechanics, 5, 183, 201
 Bohr, Niels, 5, 202, 216
 Boltzmann, Ludwig, 167, 334
 Boltzmann's constant, 334
 Boolean formula, 29, 64, 70, 79, 85–86, 138, 212, 247, 250, 255, 312
 Boolean function, 84, 133, 213, 231, 239, 241, 250, 256, 284
 BosonSampling, 287
 Bostrom, Nick, 267, 272–274, 288
 Bousso, Raphael, 32, 332, 336–337
BPP (complexity class), 79–82, 84, 86–91, 132, 135, 138, 140, 142, 144, 147, 188–189, 219, 246–247, 258, 279–282, 286, 291, 355–358
BPP_{path} (complexity class), 279–282, 286
BPP/poly (complexity class), 214
BPP/qpoly (complexity class), 211–214, 217, 320
BQP_{CTC} (complexity class), 317–318, 320, 322
 Brassard, Giles, 127, 130, 145, 196–197, 355
 Bremner, Michael, 297
 Buhrman, Harry, 214
 Busy Beaver, 28, 42–43

 Caesar cipher, 94
 Cantor, Georg, 12
 CAPTCHAs, 36
 cardinality, 11–12, 14, 16, 18
 Carmichael numbers, 77
 Carter, Brandon, 273
 causal consistency, 311, 320, 322, 325
 causal diamond, 337
 cellular automaton, 99
 Chaitin, Gregory, 213
 Chalmers, David, 42
 Chernoff bound, 73–74, 80
 chess, 38, 254–255
 Chinese Roon, 38–39
 Chiribella, Giulio, 131
 Choice, Axiom of, 14–16, 26–28
 Christiano, Paul, 129
 CHSH game, 354
 Chuang, Isaac, 149
 Church, Alonzo, 31
 Church-Turing Thesis, 31–33
 ciphertext, 94–97, 105, 107
 circuit, 54, 60–61, 135–136, 145, 156, 189, 241, 243, 247–248, 255–257, 259–262, 312, 314, 316–319, 322–323, 356–357
 CircuitSAT, 60–62, 107
 Clique, 63
 closed timelike curves, 308–324, 328, 350
 Cohen, Paul, 26
 Colbeck, Roger, 305
 Completeness Theorem, 18, 24–25
 computable, 19, 22, 28, 30–31, 42, 66, 84, 90, 96, 101, 149, 219, 259, 284, 307
 computational complexity, 39, 44, 51, 71, 94, 132, 156, 186, 202, 240, 248, 287, 304, 310, 313, 339, 354–355
 computational learning theory, 229, 232–233, 236, 238
 computational zero-knowledge proof, 193
 concept class, 231, 233–236, 239–240, 242
coNP (complexity class), 64–67, 86, 88, 193, 247, 249, 253, 263
 consciousness, 40–41, 53, 151, 155–157, 276
 consistency, 23, 25–27, 152, 248, 311
 constant-depth circuits, 145, 242, 259–260
 contextuality, 71, 171, 175
 continuum, 2, 16, 26–27
 Continuum Hypothesis, 14, 16, 26–28
 Controlled-NOT gate, 125, 130, 135–136, 283
 Conway, John, 302, 304
 Cook, Stephen, 58–59, 203, 319
 Cook-Levin Theorem, 62, 203
 Cook reduction, 58–59
 Copenhagen interpretation, 5, 201–202
 Coppersmith Don, 49
coRP (complexity class), 81, 88
 correlation, 71, 172
 cosmological constant, 325–327, 330–332, 337, 339
 cosmological horizon, 331, 337–338, 340, 342
 countable, 8, 12, 16, 18, 23
 Cramér's Conjecture, 76
 creationists, 163, 358–359
 Crépeau, Claude, 130
 Crick, Francis, 52
 cryptography, 74, 89, 93–95, 97, 100, 102, 107–108, 127, 241, 244, 248
 Csanky's algorithm, 319
CZK (complexity class), 193

- Dam, Win van, 355
 Darrow, Clarence, 290–291
 Darwin, Charles, 361
 Darwinians, 214–215, 257, 359
 Davies, Paul, 359
 Dawkins, Richard, 358–359, 361
 decoherence, 160, 163, 165–170, 218, 224–225
 Deep Blue, 37
 Democritus, 1–4, 147
 density matrix, 316
 dequantization, 91
 derandomization, 84, 88–91, 193, 247, 282, 356–358
 Deutsch, David, 5, 147–148, 201, 245, 311–313, 317, 320–322, 324
 diagonalization, 84, 256, 260–261
 digital commitment, 192
 Doomsday Argument, 272–277, 288–289
 double-slit experiment, 184
DQP (complexity class), 195, 198–199
 Dr. Evil paradox, 306
 Drucker, Andrew, 214
 Dwork, Cynthia, 100, 106
 Dyakonov, Michel, 224
- eigenvalue, 121, 208, 237
 eigenvector, 208, 318
 Einstein, Albert, 122, 160, 171, 175, 304
 Einstein-Podolsky-Rosen channels, 130
 Elga, Adam, 306
 ELIZA, 35
 entanglement, 71, 159, 163, 177, 220, 264, 301, 354
 entropy, 32, 90, 166–169, 185, 236, 333–337
 EPR (Einstein-Podolsky-Rose) pair, 122, 124, 130, 171, 262
 Eratosthenes, 343
 Euclid, 105
 Euclidean norm. *See* 2-norm
 event horizon, 221–222, 333, 344–349
 evolution (biological), 34, 38, 111, 358–359.
See also natural selection
 Evolutionary Principle, 324
EXP (complexity principle), 55, 70, 138–139, 262, 307, 317, 355
 expectation, 72
 exponential time, 54–55, 64, 70, 89, 138, 240, 260, 263
EXPSPACE (complexity principle), 317
- Extended Church-Turing Thesis, 31, 217, 219
 Extended Riemann Hypothesis, 76
- factoring, 57, 64–65, 77, 91, 98–100, 105–106, 140, 146–147, 157, 192, 218–219, 244–245, 286, 351
 fat-shattering dimension, 240
 fault-tolerance, 165, 218, 223, 225–226
 Fermat’s Last Theorem, 18
 Fermat’s Little Theorem, 18
 Feynman, Richard, 57, 139–140, 283, 343
 Feynman path integral, 283
 Fields Medal, 27, 353
 finite field, 205, 250, 253, 255, 258, 357
 firewall, 347
 first-order logic, 8–10, 18
 fixed point, 312, 317, 319, 321–324, 328
 fMRI, 159, 299
 FOCS (Foundations of Computer Science), 62
 forcing, 26
 Fortnow, Lance, 248–249, 254
 Four-Color Theorem, 37, 40–41, 63, 187
 Fourier Checking, 145
 Franzén, Torkel, 18
 Fredkin, Ed, 244
 free will, 290–291, 293–294, 296–299, 301–303, 307
 Free Will Theorem, 302, 304, 307
 Frege, Gottlob, 8, 52, 187
 Friedberg, Richard, 30
 Fuchs, Chris, 131, 202, 305
 Fundamental Theorem of Algebra, 252
 fuzball, 346–347
- garbage, 206
 Gauss, Carl Friedrich, 57, 157, 301, 352
 gavagai, 228
 general relativity, 110, 222, 277, 308–309, 344, 347–348
 geodesics, 336
 Geometric Complexity Theory (GCT), 261
 Gill, John, 78–79
 GMW (Goldreich-Micali-Wigderson) protocol, 190
 Gödel, Kurt, 18–19, 22, 26, 150–152, 156, 187, 308, 329. *See also* Completeness Theorem; Incompleteness Theorem
 God’s Coin Toss, 265, 267, 273–274

366 INDEX

- Goldbach's Conjecture, 21, 213, 252
 Goldilocks Principle, 277
 Goldreich, Oded, 97, 190, 217, 241
 Goldwasser, Shafi, 241
 Google, 37, 230
 Gott, Richard, 273
 Gottesman, Daniel, 135, 227
 Gottesman-Knill Theorem, 135
 Graham, Paul, 362
 Grandfather Paradox, 311–313, 321–323
 Graph Isomorphism, 186, 195, 198–199, 219, 350–351
 Graph Nonsomorphism, 193–194
 Grochow, Joshua, 261
 group non-membership problem, 205, 208, 212
 Grover's algorithm, 109, 146, 197, 199, 287, 341–342
 grue, 228
- Hadamard gate, 133, 135, 138, 198, 207, 264, 284
 Haken, Wolfgang, 37, 187
 halting problem, 21–22, 29–31, 42, 45, 47, 84, 136, 154, 156, 213
 Hamiltonian, 204, 220, 287
 hard on average, 99–100
 Hardy, Lucien, 131
 Hartmanis, Juris, 47
 Hästad, Johan, 101, 241
 hat problem, 91–93
 Hawking, Stephen, 345
 Hawking radiation, 222, 344–349
 Heisenberg, Werner, 216
 Hempel, Carl, 242
 Hidden Subgroup Problem, 351
 hidden variables, 166, 169–171, 177–178, 185–186, 195, 197, 302, 359
 hidden-variable theories, 160, 170–179, 181, 183, 185, 195, 198–199, 293, 303
 Hilbert, David, 14
 Hilbert space, 28, 169, 184–185, 210, 317
 Hitchens, Christopher, 361
 Holevo's Theorem, 209–221
 holographic bound, 221–222, 332–333, 335–336, 339
 Hoof, Gerard 't, 345
 Hoover, H.J., 319
 Hoyer, Peter, 196–197
- Hume, David, 229, 361
 Hume's Problem of Induction, 228
 hypercomputation, 31
- Immirzi parameter, 333
 Impagliazzo, Russell, 87, 89, 91, 101, 241, 247, 357
 Incompleteness Theorem, 19, 22–25, 41, 150–151
 independent (random variables), 73
 indeterminism, 160
 information-theoretically secure, 94–95
 inference, 71
 intelligent design, 358
 interactive proof, 186, 190, 246, 249, 255, 257–258, 260, 262–263
 interference, 71, 114–115, 143, 148–149, 160, 164, 168, 207, 220
 International Obfuscated C Code Contest, 51
 ion trap, 204
 IP (complexity class), 193, 249, 253–254, 258, 262–263, 265
 irrationality, 360–362
- Jennings, Ken, 37
Jeopardy!, 37
 Jozsa, Richard, 130, 287
- Kabanets, Valentine, 91, 357
 Kahn, David, 94
 Kant, Immanuel, 218
 Karloff, Howard, 249
 Karp, Richard, 58–59, 83, 86
 Karp-Lipton Theorem, 86, 88
 Karp reduction, 58–59
 Kasparov, Garry, 37
 Kayal, Neeraj, 77, 88
 Kearns, Michael, 230
 Kempe, Julia, 204
 Kitaev, Alexei, 134, 204, 262–263
 Kleene, Stephen, 30
 Kochen, Simon, 171–172, 174–175, 302, 304
 Kochen-Specker Theorem, 171–172, 174–175
 Kolmogorov, Andrei, 71
 Kripke, Saul, 52–53
 Kuperberg, Greg, 208–209, 214, 343
 Kurtzweil, Ray, 158

- Ladner's Theorem, 63, 65
 large cardinals, 23
 lattice, 99, 106–107
 Laughlin, Robert, 223
 Leibniz, Gottfried, 33, 187
 Leslie, John, 270
 Leucippus, 1
 Leung, David, 320
 Levin, Leonid, 57–59, 101, 203, 217, 220, 227, 241
 Libet, Benjamin, 298
 linearity, 73, 123, 125, 220–221, 223–224, 320
 linearity of expectation, 73
 linear-optical quantum computers, 287
 linear programming, 54
 Lipton, Richard, 83, 86
 Lloyd, Seth, 124, 321–322
 Löb's Theorem, 26
 Loebner, Hugh, 36
LOGSPACE (complexity class), 352, 356
 loop quantum gravity, 332–333
 Lovelace, Ada, 33
 Löwenheim–Skolem Theorem, 18
 Luby, Michael, 101, 241
 Lund, Carsten, 249, 255
 Lutomirski, Andy, 209
- MA** (complexity class), 188–189, 203, 249, 255–256, 265, 281, 355, 358
- Maldacena, Juan, 221
 Many-Worlds Interpretation, 201, 300
 Map Colorability, 62
 Markov, A.A., 73
 Markov chain, 311
 Markov's inequality, 73–74
 Mathur, Samir, 346–347
 matrix multiplication, 49
 Maudlin, Tim, 322
 Max-Flow/Min-Cut Theorem, 180–181
 maximally mixed state, 164, 167, 215, 317, 319
 measurement, 4
 mediocrity principle, 273
 Merlin. *See* Arthur
 Mertens, Stephen, 51
 metamathematics, 10
 metaphysics, 269, 298
 Micali, Silvio, 190, 241
 Miller, Gary, 77
- mixed states, 115–117, 121–122, 125–126, 131, 164, 167, 215, 222, 236, 238, 316–320
 model (logic), 9, 18, 23–25
 modus ponens, 9
 Monte Carlo simulation, 9, 74
 Moore, Christopher, 51
 Moshkovitz, Dana, 194
 Muchnik, A.A., 30
 Mulmuley, Ketan, 261
 multiverse, 147–149, 167–169, 179
- Nagasawa, Masao, 182
 Naor, Moni, 260
 natural proofs, 250, 259
 natural selection, 352–353. *See also* evolution
 Nayak, Ashwin, 210, 239
 Neal, Radford, 296
 Neumann, Jon von, 33, 52, 74, 93, 167, 223, 226
 Newcomb's Paradox, 294, 298
NEXP (complexity class), 70, 258, 260
 Nielsen, Michael, 149
 Nisan, Noam, 87, 249
 Nobel Prize, 140, 225, 283, 289
 No-Cloning Theorem, 126–128, 131, 158, 345
 nondeterminism, 292
 nonlocal boxes, 354–355
 nonlocality, 171
 nonrelativizing, 209, 246–247, 255, 257, 352
 nonuniformity, 82–83, 87–90
 Nozick, Robert, 295
NP (complexity class), 56–67, 70, 79, 82, 85–86, 88, 91, 98–99, 137, 145–146, 156, 188–189, 194, 203–204, 241, 245–246, 248, 255, 257–258, 261, 281–282, 291, 298, 307, 318, 321, 351–352, 354–355, 358
NP \cap **coNP** (complexity class), 64–66
NP-complete, 59–60, 62–65, 67, 70, 79, 85–88, 100, 108, 124, 145, 154, 190–191, 198–199, 203, 212, 219, 227, 241, 250, 279, 289, 307, 310, 312–314, 317, 324–325, 350–354
NP-completeness, 29, 42, 45, 58, 62, 100, 194, 298
NP-hard, 58
NP-intermediate, 219

368 INDEX

- NSA (National Security Agency), 95, 102
 null hypersurfaces, 336
 NUMB3RS, 59
 Number Field Sieve, 105, 108
- Obama, Barack, 246
 observable universe, 156, 201, 326, 338–339, 341
 Occam's Razor, 230, 235–236
 one-time pad, 94
 one-way function, 36, 101–103, 190–191, 193, 241, 350
 oracle, 29–30, 58–60, 67, 82, 137, 142, 144–145, 154, 156, 199, 208–209, 245–246, 248–249, 254–255, 257–258, 281, 298, 351–352, 354
 ordinal numbers, 13–14
 Otter (computer program), 37
- P** (complexity class), 45, 54–57, 62–64, 66–67, 70, 83–85, 88–91, 98–100, 131, 140, 145, 156, 241, 244–248, 255, 257–258, 261, 286, 288, 305, 312, 328, 351–352, 355–358
- Packing, 63
 PAC learning, 230, 235
 Papadimitriou, Christos, 51
 passive optical elements, 287
 PCP (Probabilistically Checkable Proof), 193–194
 PCP Theorem, 194
P_{CTC} (complexity class), 312, 314–315, 318
 Peano Arithmetic, 23–24, 27
 Peano axioms, 9–10
 Peikert, Chris, 106
 Penrose, Roger, 33, 41, 150–156, 158, 187, 301, 353
 Peres, Asher, 103, 130
 permanent (matrix), 288
 perturbation, 248, 351
PH. *See* polynomial hierarchy
 Pinker, Steven, 244
 plaintext, 94–97, 105, 107
 Planck area, 221, 332
 Planck scale, 2, 32, 185
 Planck time, 330
 Plato, 330
 Platonism, 152, 186–187, 200
 Poincaré Conjecture, 18
- polynomial hierarchy, 66–67, 82, 86, 88, 144–145, 193, 245, 254, 282–283, 286–288
 polynomial identity testing, 356–357
 polynomials, 129, 250–252, 254, 286
 polynomial time, 54–61, 63–68, 70, 77–85, 87–88, 90, 96–98, 100–102, 104–106, 124, 136–138, 140, 154, 188, 192–193, 195, 199, 203, 206, 208, 219, 241, 247–248, 253, 255, 258, 262, 279–283, 287, 307, 312, 318–319, 321, 325, 350, 352, 354
- Post, Emil, 30
PostBPP (complexity class), 280–283, 286–288
PostBQP (complexity class), 214, 282–283, 286–288, 321
 postselection, 214, 280–284, 286, 321–322
 POVM (positive operator-valued measurement), 236–237
PP (complexity class), 78–79, 138–140, 189, 212–213, 254–257, 262, 282–286, 321, 325, 350
- P/poly** (complexity class), 83–88, 255, 258, 260
- Pratt, Vaughn, 88
 Preskill, John, 165, 223, 305
 Presumptuous Philosophers, 288–289
 primality testing, 54, 57, 77–78, 88, 356
 Prime Number Theorem, 76
 primes, 21, 64, 75–77, 250
 Principle of Deferred Measurement, 283
 private-key cryptosystems, 102
 probabilities, 4, 7, 28, 71–72, 109–113, 115, 121, 123, 146, 162, 168, 174, 181–183, 201, 220, 238, 266–267, 275–276, 281, 295, 322, 344
- Problem of Induction, 228
PromiseMA (complexity class), 257
 promise problem, 196, 203–204, 257
 pseudorandom function, 241, 259–260, 350
 pseudorandom generator, 89–90, 96–101, 241, 247, 356
- PSPACE** (complexity class), 55–56, 139, 193, 214, 245, 253–254, 258, 262–263, 265, 307, 312, 314–315, 317–319, 321–322, 324, 328, 350, 355
- public-key cryptography, 102, 128–129

- public-key quantum money, 129
P versus **NP** question, 56–57, 91, 156, 246,
 258, 261, 298
- QAM** (complexity class), 165
QCMA (complexity class), 208–209
QIP (complexity class), 262–265
QIP[2] (complexity class), 262–265
QMA (complexity class), 203–204, 208–209,
 212, 214, 265
QMA-complete, 203
QMAM (complexity class), 203
 qualia, 34
 quantifier, 34
 quantitative epistemology, 200
 quantum advice, 211–212, 214–215, 217, 320
 quantum advice state, 212, 215
 quantum computer, 19, 65, 82, 105–107, 134,
 138–140, 144–145, 147–149, 153,
 157, 159, 165, 195, 203, 211–212,
 218, 222–223, 225–226, 246, 282,
 287–288, 301, 315, 325, 350, 352
 quantum computing, 3, 6, 8, 28, 31–32, 64,
 71, 140, 144–145, 147–149, 157,
 163, 195, 199, 202–203, 217–220,
 225–227, 237, 244, 284, 286–287,
 320, 343, 350–351
 Quantum Cook-Levin Theorem, 203
 quantum fault-tolerance, 223
 quantum gravity, 32, 150–151, 301, 308–309,
 323, 332–333, 344, 346–347
 quantum interactive proof, 262
 quantum key distribution, 127, 159
 quantum mechanics, 3–6, 27–28, 44, 71,
 109–112, 115–119, 121, 123–127,
 129, 131–132, 146–148, 150,
 156–158, 160–164, 168–170, 172,
 178, 180, 182, 184, 201–202, 217,
 220, 223, 225, 236–238, 286, 293,
 302, 304, 309, 311, 316, 320–321,
 343–344, 346, 349, 354–355
 quantum money, 128–129
 quantum oracle, 208
 quantum robot, 341
 quantum state, 5, 115, 117, 123, 125–126,
 148, 163–164, 171–172, 176,
 201–203, 206–210, 214–215, 217,
 221, 236–241, 265, 282, 300–301,
 303, 320
 quantum state tomography, 237–238
 quantum teleportation. *See* teleportation
 qubit, 114, 121–122, 125, 127–130, 132–139,
 143, 159, 163–165, 167, 198,
 202–204, 207–212, 214, 220–221,
 223, 225–227, 237–240, 264,
 283–284, 287, 301, 316–318,
 321–322, 348, 354
 query complexity, 197, 340
- Rabin, Michael, 77, 88, 105
 randomized algorithm, 74, 77–81, 88–89,
 143, 188, 247, 356–357
 randomness, 71, 74–78, 82, 87–90, 98, 166,
 247, 295, 302, 305, 312, 356
 random walk, 206–207, 340
 rational numbers, 12, 16, 119
 Razborov, A.A., 259–260
 Recursive Fourier Sampling, 142–145, 351
 reduction, 42, 58–59, 64, 97, 100–102, 106
 Regev, Oded, 100, 106–107, 204
 Reingold, Oded, 256, 260, 285–286
 relativize, 30, 246, 258
 reliability of memory, 162, 168
 religion, 5, 343, 358–361
 Riemann Hypothesis, 26, 76, 124, 213, 352
 Robbins Conjecture, 37
 Rommnet, Mitt, 246
RP (complexity class), 80–81, 355
RSA, 102–103, 105, 107–108, 124
 Rudich, Steven, 259–260
 Rule 110, 99
 Russel, Bertrand, 8, 15, 52
- Sagan, Carl, 307
 Sahai, Amit, 196
 sample distribution, 233
 sample space, 230–232, 234
 Santhanam, Rahul, 257–258
 Saxena, Nitin, 77, 88
 Schöning, Uwe, 254
 Schrödinger, Erwin, 3, 131, 181–182, 225
 Schwarzschild bound, 334
 Scopes Monkey Trial, 290
 Searle, John, 33, 39
 Second Incompleteness Theorem, 23–24, 151
 Second Law of Thermodynamics, 124,
 166–167, 333–334
 self-checking programs, 255

370 INDEX

- Self-Indication Assumption, 274, 289
 self-printing program, 51
 Self-Sampling Assumption, 274, 289
 semidefinite programming, 262
 sets, 8, 11–12, 14–15
 set theory, 8, 10–11, 18, 23, 26–27, 29, 63,
 151–152
 Shamir, Adi, 254
 Shannon, Claude, 74, 95, 166
 shattering, 234
 Shepherd, Dan, 287
 Shi, Yaoyun, 134, 197
 Shor's algorithm, 65, 106, 140–142, 144,
 146–147, 201, 245, 287
 Shortest Vector Problem, 99–100,
 106
 Shub, M., 98
 Sipser, Michael, 82, 91, 248–249, 258
 Smith, Graeme, 320
 Smolensky, Roman, 259
 Smolin, John A., 320
 Solovay, Robert, 88, 134, 258
 Solovay-Kitaev Theorem, 134
 $\text{SPACE}(f(n))$, 47, 54
 Space Hierarchy Theorem, 49
 special relativity, 111, 175, 301, 303
 Specker, Ernst, 171, 174–175
 Stable Marriage Problem, 67–68
 Standard Model, 102, 323
 Star Trek, 313
 stationary distribution, 311, 313–315
 statistical zero-knowledge proof, 186, 193,
 195–196, 352
 Stearns, Richard, 47
 Stern-Gerlach experiment, 176
 STOC (Symposium on Theory of
 Computing), 62
 stochastic matrix, 113, 171–172, 179,
 181–182
 Stothers, Andrew, 49
 Strassen, Volker, 49, 88
 string theory, 332
 strong AI, 33, 38, 41, 155
 superoperator, 316–318, 321
 superposition, 3–6, 133, 137, 141, 161–162,
 165, 206–208, 212, 263–264
 Susskind, Lenny, 345
 Szemerédi, Endre, 264
 SZK (complexity class), 193, 195, 352
 Tapp, Alain, 196–197
 Tarski, Alfred, 15, 37, 45–46
 TC^0 (complexity class), 260
 teleportation, 129, 131, 158–159, 299–300,
 321
 Thorne, Kip, 309
 Threshold Theorem, 223–224, 226
 time-constructibility, 48
 time dilation, 221
 $\text{TIME}(f(n))$, 47, 49, 54
 Time Hierarchy Theorem, 47, 49
 time travel, 307–308, 310, 313–314, 321, 323
 Toda's Theorem, 254, 286
 transistor, 223
 transition probabilities, 162, 174, 181–183
 trapdoor one-way function, 103, 108
 Tsirelson's inequality, 354–355
 Turing, Alan, 18, 20–22, 29–36, 38, 47, 74,
 94, 138, 151–156
 Turing Award, 47
 Turing degree, 30–31
 Turing equivalent, 29
 Turing machine, 20, 28–31, 42, 47, 55, 59,
 61, 78, 83–84, 87, 136, 138, 153,
 156, 200, 219, 336, 339–340
 Turing reducible, 29
 Turing Test, 35–38, 155

 union bound, 72–73, 87, 141, 233
 unitarity, 222, 344–345
 unitary matrix, 113–114, 134, 171–172, 179,
 182
 universal programmable computers, 21

 vacuum energy, 169, 332, 337
 Vadhan, Salil, 196
 Valiant, Leslie, 230, 232–233, 253
 Vassilevska Williams, Virginia, 49
 Vazirani, Umesh, 139, 142–143, 145, 149,
 210, 224, 230, 238, 305, 351
 VC dimension, 234–236, 239–240
 Vidick, Thomas, 128, 305
 Vinodchandran, N.V., 256–257
 von Neumann, John. *See* Neumann, Jon von
 von Neumann trick, 93

 Watrous, John, 128, 205–207, 212, 262–263,
 318, 323
 Watson (Jeopardy computer), 37

- Watson, James, 52
wavefunction, 160, 164, 167, 183, 185, 201,
301
weak measurement, 211
Weinberg, Steven, 123, 358
Weizebaum, Joseph, 35
well ordered, 13–15
Wiesner, Stephen, 127–128
Wigderson, Avi, 87, 89, 91, 190, 247,
258
Wiles, Andrew, 109, 352–353
Williams, Ryan, 260
Winograd, Shmuel, 49
Witten, Edward, 221
Wittgenstein, Ludwig, 295–296
Wolfram, Stephen, 99, 303
Wootters, William, 123, 130
worst-case/average-case equivalence, 99–100
Yahoo, 37
Yao, Andy, 90, 102, 356
you-complete, 296–297
Zeilinger, Anton, 225
Zermelo-Fraenkel axioms, 11, 14, 23
Zermelo-Fraenkel set theory, 26
zero-knowledge proof, 189–193, 195
ZPP (complexity class), 81, 88, 355
 Ω (constant), 213