

Index

Author Index

Church, A., 165
Cobham, A., 165
Cook, S. A., 165–167
Edmonds, J., 165
Even, S., 167
Karp, R. M., 165–167
Ladner, R. E., 167
Levin, L. A., 165–167
Selman, A. L., 167
Shannon, C. E., 165
Turing, A. M., 164, 165
Yacobi, Y., 167

Subject Index

Algorithms, *see* Computability theory
Approximation, 173
Average-case complexity, 173

Boolean circuits, 32–40, 104–113
 bounded fan-in, 35
 constant-depth, 40
 depth, 39
 monotone, 40
 size, 35–36
 unbounded fan-in, 35, 38, 40
 uniform, 36
Boolean formulae, 33, 38–39, 177–178
 clauses, 38
 CNF, 38, 104–113, 178
 DNF, 39, 178
 literals, 38

Church-Turing Thesis, 16, 17, 27
Circuits, *see* Boolean circuits
CNF, *see* Boolean formulae
Cobham-Edmonds Thesis, 27, 28, 50, 52, 108
Complexity classes
 coNP, 94, 126, 154–158
 EXP, 66, 123
 generic, 40
 IP, *see* Interactive proofs
 NP, *see* NP
 NPC, *see* NP-completeness
 NPI, 126
 P, *see* P
 PC, 55–58, 63–66, 69, 77, 80–88, 98–102, 105, 109, 144, 151–154
 PCP, *see* Probabilistically checkable proofs
 PF, 54–55, 57–58, 63–65
 ZK, *see* Zero-knowledge
Computability theory, 1–31
Computational problems
 2SAT, 113
 3SAT, 112, 113, 123, 124, 126, 178
 3XC, 115
 Bipartiteness, 177
 Bounded Halting, 102
 Bounded Non-Halting, 102–103
 Clique, 117, 177
 Connectivity, 177
 CSAT, 104–112
 Entscheidungsproblem, 164
 Exact Cover, 115
 Factoring integers, 53, 72, 94, 157
 Graph 2-Colorability, 113, 177
 Graph 3-Colorability, 91, 113, 118, 123, 125, 177

- Computational problems (*cont.*)
 - Graph Isomorphism, 91, 177
 - Halting Problem, 19–21, 102, 103
 - Hamiltonian path, 53, 56, 58, 60, 61, 177
 - Independent Set, 117, 177
 - PCP, *see* Post Correspondence Problem
 - Perfect matching, 177
 - Primality testing, 72
 - SAT, 53, 57, 61, 85–86, 104–113, 154, 178
 - Set Cover, 114
 - Solving systems of equations, 53
 - Spanning trees, 53
 - TSP, 53, 57
 - Vertex Cover, 117, 177
- Computational tasks and models, 1–47
- Constant-depth circuits, *see* Boolean circuits
- Cook-reductions, *see* Reductions
- Cryptography, 125, 172
- Decision problems, 6–8, 58–65
- DNF, *see* Boolean formulae
- Exhaustive search, 50, 51, 66, 70
- Finite automata, 31
- Formulae, *see* Boolean formulae
- Graph theory, 175–177
- Halting Problem, *see* Computational problems
- Hilbert's Tenth Problem, 164
- Interactive proofs, 124, 172
- Karp-reductions, *see* Reductions
- Kolmogorov Complexity, 24–26, 35
- Levin-reductions, *see* Reductions
- Monotone circuits, *see* Boolean circuits
- NP, 48–158
 - as proof system, 59–62, 123, 125
 - as search problem, 55–58
 - Optimal search, 151–154
 - traditional definition, 66–69
- NP-completeness, 89–133, 155–158
- O-notation, 26
- One-way functions, 171
- Optimal search for NP, 151–154
- Oracle machines, 29–31
- P, 48–158
 - as search problem, 54–55, 57–58
- P versus NP Question, 48–70
- Polynomial-time reductions, *see* Reductions
- Post Correspondence Problem, 22, 24, 43
- Probabilistic proof systems, 123–126
- Probabilistically checkable proofs, 125–126
- Promise problems, 8, 52, 142–151, 156
- Proof systems
 - Interactive, *see* Interactive proofs
 - NP, *see* NP
 - PCP, *see* Probabilistically checkable proofs
 - Probabilistic, *see* Probabilistic proof systems
 - Zero-knowledge, *see* Zero-knowledge
- Pseudorandom generators, 171
- Pseudorandomness, 171
- Randomness extractors, 174
- Reductions
 - Cook-reductions, 76–99, 120–129, 155–157
 - Downward self-reducibility, 92
 - Karp-reductions, 77–81, 98–120, 155
 - Levin-reductions, 79–81, 83, 99–113
 - parsimonious, 139
 - Polynomial-time reductions, 74–129
 - Self-reducibility, 83–88
 - to sparse sets, 162–163
 - Turing-reductions, 21, 29–31
- Rice's Theorem, 21
- Search problems, 5–6, 52–58, 63–65
 - versus decision, 63–65, 77, 80, 83–88
- Self-reducibility, *see* Reductions
- Space complexity, 29
- Time complexity, 10, 26–29
- Turing machines, 11–18
 - multi-tape, 16
 - non-deterministic, 66–69
 - single-tape, 15
 - with advice, 36–37
- Turing-reductions, *see* Reductions
- Uncomputable functions, 18–22
- Undecidability, 19, 22
- Universal algorithms, 22–26, 28
- Universal machines, 22–26
- Worst-case complexity, 173
- Zero-knowledge, 124–125, 172