

Index

Author Index

- Adleman, L. M., 227, 501
 Agrawal, M., 227
 Ajtai, M., 337
 Aleliunas, R., 228
 Arora, S., 406

 Babai, L., 405, 406, 578
 Barak, B., 498
 Ben-Or, M., 405
 Blum, M., 140, 227, 277, 278, 335
 Borodin, A., 140, 175
 Brassard, G., 407

 Chaitin, G. J., 285, 307
 Chaum, D., 407
 Church, A., 43
 Cobham, A., 43
 Cook, S. A., 97, 98, 229
 Crépeau, C., 407

 Diffie, W., 277, 501
 Dinur, I., 407

 Edmonds, J., 43
 Even, S., 99

 Feige, U., 406, 453
 Fortnow, L., 405, 406
 Furst, M. L., 474

 Goldreich, O., 277, 336, 405, 453, 492, 517
 Goldwasser, S., 335, 336, 405, 406, 453, 492, 502, 503, 505, 572

 Hartmanis, J., 140
 Hästad, J., 336, 453, 474
 Hellman, M. E., 277, 501
 Huang, M., 227

 Immerman, N., 175
 Impagliazzo, R., 278, 336

 Jerrum, M., 229

 Karchmer, M., 475
 Karloff, H., 405
 Karp, R. M., 97, 98, 121, 122, 228
 Kayal, N., 227
 Kilian, J., 405, 407
 Kolmogorov, A., 285, 307
 Komlos, J., 337

 Ladner, R. E., 98
 Lautemann, C., 228
 Levin, L. A., 97, 98, 277, 336, 406, 454
 Lipton, R. J., 122, 228, 278
 Lovász, L., 228, 406, 453
 Luby, M., 278, 336
 Lund, C., 405, 406

 Micali, S., 277, 335, 336, 405, 407, 492, 502, 503, 505, 517
 Miller, G. L., 227
 Moran, S., 578
 Motwani, R., 406

 Naor, J., 337
 Naor, M., 337
 Nisan, N., 277, 336, 337, 405

 Papadimitriou, C. H., 455

 Rabin, M. O., 227
 Rackoff, C., 228, 277, 405
 Raz, R., 475
 Razborov, A. R., 473
 Reingold, O., 175, 561

INDEX

- Rivest, R. L., 501
 Ron, D., 453
 Rubinfeld, R., 278, 453
- Safra, S., 406, 453
 Savitch, W. J., 175
 Saxe, J. B., 474
 Saxena, N., 227
 Selman, A. L., 99
 Shamir, A., 405, 501
 Shannon, C. E., 43, 285, 472, 500
 Sipser, M., 228, 229, 474, 572
 Solomonoff, R. J., 285
 Solovay, R., 227
 Stearns, R. E., 140
 Stockmeyer, L. J., 121, 229
 Strassen, V., 227
 Sudan, M., 278, 406, 453
 Szegedy, M., 406
 Szelepcsényi, R., 175
 Szemerédi, E., 337
- Toda, S., 229, 566
 Trevisan, L., 278, 542
 Turing, A. M., 43, 354
- Vadhan, S., 278, 561
 Valiant, L. G., 229
 Vazirani, V. V., 229
- Wigderson, A., 278, 336, 405, 475, 517, 561
- Yacobi, Y., 99
 Yannakakis, M., 455
 Yao, A. C., 277, 335, 336, 474, 517
- Zuckerman, D., 337
- Subject Index**
 algorithms, *see* computability theory
 approximate counting, 211–216, 221–224
 satisfying assignments to a DNF, 212–214
 approximation, 418–429
 counting, *see* approximate counting
 hardness, *see* hardness of approximation
 arithmetic circuits, 475–478
 average-case complexity, 429–452
- Blum-Micali Generator, *see* pseudorandom generators
 Boolean circuits, 37–42, 72–77, 109–113, 129, 304, 471–475
 bounded fan-in, 39
 constant-depth, 42, 314, 473–474
 depth, 42
 Monotone, 42, 472–473
 natural proofs, 306
 size, 39–40, 109–110
 unbounded fan-in, 39, 41, 42
 uniform, 40, 110–111, 155
 Boolean formulae, 37, 41–42, 474–475, 585–586
 clauses, 41
 CNF, 41, 72–77, 585–586
 DNF, 42, 585–586
 literals, 41
 Monotone, 475
 Quantified, 586
 Byzantine Agreement, 520
- Chebyshev's Inequality, 525–526, 530
 Chernoff Bound, 526–527
 Chinese Remainder Theorem, 409
 Church-Turing Thesis, 25, 33
 circuits, *see* Boolean circuits
 CNF, *see* Boolean formulae
 Cobham-Edmonds Thesis, 33, 46, 75, 128, 130
 coding theory, 546–554
 concatenated codes, 550–551
 connection to hardness amplification, 257, 266–270
 good codes, 551
 Hadamard code, 254, 255, 282, 386–387, 549
 list decoding, 254, 255, 266–270, 543, 547, 553
 locally decodable, 552–553
 locally testable, 552–553
 Long-Code, 549
 Reed-Muller code, 267, 549–550
 Reed-Solomon code, 549
 unique decoding, 547
 commitment schemes, *see* cryptography
 communication complexity, 474–475
 complexity classes
 $\oplus P$, 566–571
 $\sharp P$, 202–216, 465, 566–571
 AC0, 117, 314, 468
 AM, 365
 BPL, 200–201, 319, 323–325, 467
 BPP, 189–193, 195–199, 304–305, 308–312, 319, 465
 coNL, 143, 168–171
 coNP, 82, 94–97, 116, 143, 167, 469, 478
 coRP, 193–198, 199
 distNP, 434–442, 446–452
 distPC, 444
 DSPACE, 139, 144, 166
 DTIME, 130

INDEX

- complexity classes (*cont.*)
- DTiSp, 153
 - E, 466
 - EXP, 55, 466, 467
 - IP, *see* interactive proof systems, 352, 355, 359, 365, 377, 466
 - L, 154–156, 467
 - MA, 199, 365
 - NC, 155, 167, 468
 - NEXP, 466
 - NL, 143, 164–171, 200, 323, 467
 - NP, 44–97, 113–116, 119–121, 143, 164, 167, 315, 356, 359, 365, 377, 383–404, 465–467, 469, 477, 478
 - as proof system, 51–53
 - as search problem, 48–50
 - optimal search, 92–94
 - traditional definition, 55–57, 117–119, 163, 186
 - NPC, *see* NP-completeness
 - NPI, 82
 - NSPACE, 166
 - two models, 162–164
 - NTIME, 134
 - P, 44–97, 111, 112, 114, 116, 153–155, 164, 465, 469, 471, 473
 - as search problem, 48–50
 - P/poly, 108–113, 119–121, 468
 - PC, 48–50, 54–55, 57, 60–70, 72, 75, 88, 89, 92–95, 202–227, 419, 444
 - PCP, *see* probabilistic checkable proof systems
 - PF, 48–50, 54–55, 444
 - PH, 113–121, 191, 203, 466, 566–571
 - PSPACE, 172–175, 359, 467
 - quasi-P, 314, 466
 - RL, 200–202, 323, 467
 - RP, 193–199, 199, 465
 - sampNP, 446–452
 - SC, 152, 323
 - SZK, 378
 - TC0, 468
 - tpcBPP, 443
 - tpcP, 433, 435–436
 - tpcPF, 444
 - ZK, *see* zero-knowledge proof systems, 368, 371, 377
 - ZPP, 199, 465
- computability theory, 17–36
- computational indistinguishability, 289, 291, 292, 295–299, 335, 490–491
- multiple samples, 296–299
 - non-triviality, 296
 - the hybrid technique, 297–299, 303, 312, 322, 335
 - vs statistical closeness, 296
- computational learning theory, 306
- computational problems
- 3SAT, 77, 586
 - 3XC, 78
 - bipartiteness, 427, 428, 584
 - Bounded Halting, 70
 - Bounded Non-halting, 70–71
 - CEVL, 154
 - Clique, 80, 420–422, 427, 585
 - CSAT, 72–77
 - CSP, 395–399
 - Determinant, 205, 477–478, 587
 - Directed Connectivity, 164–171, 201
 - Exact Set Cover, 79
 - extracting modular square roots, 588
 - factoring integers, 97, 99, 102, 484, 488, 505, 588
 - Graph 2-Colorability, 584
 - Graph 3-Colorability, 80, 375, 428, 585
 - Graph Isomorphism, 358, 372, 585
 - Graph k-Colorability, 427
 - Graph Non-Isomorphism, 358
 - Halting Problem, 27–28, 70, 71, 354
 - Hamiltonian path, 585
 - Independent Set, 80, 585
 - kQBF, 123, 586
 - Perfect Matching, 205–211, 221, 585
 - Permanent, 205–211, 236, 477–478, 587
 - primality testing, 99, 192–193, 588
 - QBF, 172–175, 362, 408, 586
 - SAT, 64–65, 72–77, 94, 423, 586
 - Set Cover, 78
 - st-CONN, 164–171
 - testing Polynomial Identity, 194–195
 - TSP, 421
 - U-CONN, 155–162
 - Undirected Connectivity, 155–162, 165, 201–202, 584
 - Vertex Cover, 80, 420, 422, 585
- computational tasks and models, 17
- computationally sound proof systems
- arguments, 407
- constant-depth circuits, *see* Boolean circuits
- constraint satisfaction problems, *see* CSP
- Cook-reductions, *see* Reduction
- counting problems, 202–227
- approximation, *see* approximate counting
 - perfect matching, 205–211
 - satisfying assignments to a DNF, 204
- cryptology, 482–522
- coin tossing, 521–522
 - commitment schemes, 376, 495–496, 520–522

INDEX

- cryptography (*cont.*)
 computational indistinguishability, *see*
 computational indistinguishability
 encryption schemes, 500–507
 general protocols, 511–522
 hard-core predicates, *see* one-way functions
 hashing, *see* hashing
 message authentication schemes, 507–511
 modern vs classical, 483, 500
 Oblivious Transfer, 519–520
 one-way functions, *see* one-way functions
 pseudorandom functions, *see* pseudorandom
 functions
 pseudorandom generators, *see* pseudorandom
 generators
 secret sharing, 518–519, 521
 signature schemes, 507–511
 trapdoor permutations, 488–489, 505–506,
 509, 517, 519–520
 Verifiable Secret Sharing, 521
 zero-knowledge, *see* zero-knowledge proof
 systems
- CSP, *see* computational problems
- decision problems, 19, 20, 50–55, 444–446
 unique solutions, *see* unique solutions
- diagonalization, 133
- direct product theorems, 261–266, 277
- dispersers, 540
- error-correcting codes, *see* coding theory
- error reduction, 188, 190, 212, 214, 220,
 230–232, 351, 355, 356, 368, 383, 403,
 407, 572
- randomness-efficient, 539–540
- expander graphs, 332, 333, 554–565
 amplification, 556
 constructions, 560–565
 eigenvalue gap, 555–556
 expansion, 555–556
 explicitness, 556–557
 mixing, 557–559
 random walk, 333–334, 559–560
- extractors, *see* randomness extractors
- finite automata, 36
- finite fields, 586
- formulae, *see* Boolean formulae
- fourier coefficients, 329
- game theory
 Min-Max Principle, 272–273
- gap problems, *see* promise problems
- gap theorems, *see* time gaps
- GF(2), 586
- GF(2ⁿ), 587
- Gödel's Incompleteness Theorem, 354
- graph properties, 426
- graph theory, 583–585
- Hadamard code, *see* coding theory
- Halting Problem, *see* computational problems
- hard regions, *see* inapproximable predicates
- hardness of approximation
 Max3SAT, 401
 MaxClique, 403
 the PCP connection, 399–403, 421–424
- hashing, 527–533
 as a random sieve, 215–216, 218–220,
 224–227
 collision-free, 511
 collision-resistant, 511
 extraction property, 538
 highly independent, 529, 532–533
 Leftover Hash Lemma, 529–533
 mixing property, 319, 530
 pairwise independent, 529–532
 universal, 304, 529
 Universal One-Way, 511
- hierarchy theorems, *see* time hierarchies
- hitters, 535–536
- Hoefding Inequality, 527
- inapproximable predicates, 255–277
 hard regions, 271–274
- Information Theory, 249–250, 285, 483
- interactive proof systems, 352–368, 405
 algebraic methods, 359
 Arthur-Merlin, 364, 365, 571–582
 computational soundness, 367–368, 497
 constant-round, 314, 336, 365
 for Graph Non-Isomorphism, 358
 for PSPACE, 359–363
 hierarchy, 364–365, 571–582
 linear speedup, 365
 power of the prover, 366–367
 public-coin, 314, 364, 365, 571–582
 two-sided error, 364, 365
- Karp-reductions, *see* reduction
- knowledge complexity, 371
- Kolmogorov Complexity, 31–32, 39, 286, 307
- Levin-reductions, *see* reduction
- Linear Feedback Shift Registers, 330
- list decoding, *see* coding theory
- low-degree tests, *see* property testing
- lower bounds, 469–481

INDEX

- Markov's Inequality, 525
- Min-Max Principle, *see* game theory
- Monotone circuits, *see* Boolean circuits
- multi-prover interactive proof systems, 403, 405
- Nisan-Wigderson Generator, *see* pseudorandom generators
- non-interactive zero-knowledge, 499
- notation
- asymptotic, 16
 - combinatorial, 16
 - graph theory, 16
 - integrality issues, 16
- NP-completeness, 67–87, 95–97, 154, 377, 465
- one-way functions, 242–255, 296, 375, 377, 452, 483–484, 487–489, 492, 495–496, 506, 509
- hard-core predicates, 250–255, 336, 489, 496, 505, 519
 - strong vs weak, 245–250
- optimal search for NP, 92–94
- oracle machines, 35–36
- P versus NP Question, 46–58, 115, 430, 435, 436, 447, 471
- PCP, *see* probabilistically checkable proof systems
- polynomial-time reductions, *see* reduction
- Post Correspondence Problem, 29, 31
- probabilistic log-space, 199–202
- probabilistic polynomial time, 184–202
- probabilistic proof systems, 349–416
- probabilistically checkable proof systems, 380–407
- adaptive, 383, 403
 - approximation, *see* hardness of approximation
 - composition, 389–392, 395, 399
 - for NEXP, 405
 - for NP, 384–399, 402–404
 - free-bit complexity, 403, 412
 - non-adaptive, 383, 389, 390, 400, 403
 - non-binary queries, 403
 - of proximity, 391, 394, 404
 - proof length, 402
 - query complexity, 402
 - robustness, 391, 394
- probability theory
- conventions, 523–524
 - inequalities, 524–527
- promise problems, 20, 87–92, 95, 192, 217, 424–429
- gap problems, 421–424
 - proof complexity, 470, 478–481
 - proofs of knowledge, 378–380, 499
 - property testing, 424–429
 - codeword testing, *see* coding theory
 - for graph properties, 426–429
 - low-degree tests, 394, 395, 429
 - self-correcting, *see* self-correcting
 - self-testing, *see* self-testing
- pseudorandom functions, 306, 336, 492–493
- pseudorandom generators, 284–348
- archetypical case, 290–307, 335–336
 - Blum-Micali Construction, 303, 505
 - conceptual discussion, 306–307, 315
 - connection to extractors, 542–544
 - derandomization, 304–305, 307–315, 336
 - high end, 312
 - low end, 312 - discrepancy sets, 332
 - expander random walks, 276, 332–334
 - extractors, *see* randomness extractors
 - general paradigm, 285–290, 334–335
 - general-purpose, 290–307, 335–336
 - application, 292–295
 - construction, 301–304
 - definition, 290–292
 - stretch, 299–303 - hitting, 333–334, 536
 - Nisan-Wigderson Construction, 277, 310–315, 335, 336, 542
 - pairwise independence, 274, 326–329
 - samplers, *see* sampling
 - small-bias, 329–332, 393
 - space, 315–325, 336
 - special purpose, 325–334, 337
 - universal sets, 332
 - unpredictability, 301–303, 312, 335
- random variables, 523–527
- pairwise independent, 525–527
 - totally independent, 526–527
- randomized computation
- log-space, *see* probabilistic log-space
 - polynomial time, *see* probabilistic polynomial-time
 - proof systems, *see* probabilistic proof systems
 - reductions, *see* reductions
 - sub-linear time, *see* property testing
- randomness extractors, 336, 536–544
- connection to error reduction, 539–540
 - connection to pseudorandomness, 542–544
 - connection to samplers, 538–539
 - from few independent sources, 537
 - seeded extractors, 536–537
 - using weak random sources, 536–537

INDEX

- reductions
 - among distributional problems, 435–446, 448
 - Cook-reductions, 59–68, 81–85, 95–96, 202–227, 435
 - downward self-reducibility, 101, 125
 - gap amplifying, 401
 - Karp-reductions, 60–61, 68–81, 95, 203–204, 435, 465
 - Levin-reductions, 60–61, 63, 68–77
 - parsimonious, 105, 203–204, 217–224
 - polynomial-time reductions, 58–85, 188–189, 465, 466
 - randomized reductions, 195–198, 230
 - reducibility argument, 247–249, 251, 255, 298, 312, 436, 483, 489
 - self-reducibility, 63–67, 367
 - space-bounded, 149–152, 154–155, 158–162, 164–165
 - Turing-reductions, 28, 35–36
 - worst-case to average-case, 257–260, 266–269
- Rice’s Theorem, 29
- samplers, *see* sampling
- sampling, 533–536
 - averaging samplers, 535, 538–539
- search problems, 18–19, 47–50, 54–55, 152, 165, 444–446
 - uniform generation, *see* uniform generation
 - unique solutions, *see* unique solutions
 - versus decision, 54–55, 60–61, 63–67, 152, 165, 444–446
- self-correcting, 258–260, 278, 386–388, 394, 550, 552–553
- self-reducibility, *see* reduction
- self-testing, 386, 387, 550
- space complexity, 34–35, 143–183
 - Circuit Evaluation, 153–155
 - composition lemmas, 146–148, 161–162
 - conventions, 144–145
 - logarithmic space, 153–162
 - non-determinism, 162–172
 - polynomial space, 172–175
 - pseudorandomness, *see* pseudorandom generators
 - randomness, *see* probabilistic log-space reductions, *see* reductions
 - sub-logarithmic, 145–146
 - versus time complexity, 146–153
- space gaps, 139, 152
- space hierarchies, 139, 152
- space-constructible, 139
- speedup theorems, 138–139
- statistical difference, 296, 524
- st-CONN, *see* computational problems
- time complexity, 21–22, 32–34
- time gaps, 136–138
- time hierarchies, 129–136
- time-constructible, 130, 131, 136, 309
- Turing machines, 22–26
 - multi-tape, 24, 130
 - non-deterministic, 55–57
 - single-tape, 24
 - with advice, 40–41, 111–113, 128–129, 305
- Turing-reductions, *see* reductions
- UConn, *see* computational problems
- uncomputable functions, 26–29
- undecidability, 27, 29, 354
- uniform generation, 220–227
- unique solutions, 205, 216–220, 236, 445–446
- universal algorithms, 29–32, 34, 133–134
- universal machines, 29–32
- variation distance, *see* statistical difference
- witness indistinguishability, 499
- Yao’s XOR Lemma, 257, 260–266, 270–271
 - derandomized version, 274–277
- zero-knowledge proof systems, 368–380, 405, 493–500, 520–521
 - almost-perfect, 377
 - black-box simulation, 498
 - computational, 371, 499
 - for 3-Colorability, 375
 - for Graph Non-Isomorphism, 372
 - for NP, 374
 - honest verifier, 498
 - knowledge complexity, 371
 - perfect, 370, 377, 407, 498
 - statistical, 371, 377, 498
 - universal simulation, 498