Index

∧, 6
∧, 6
∃, 318, 348
∃^+, 318, 379
¬, 6
⊢, 9
⊢^+, 64, 86
⊢_{yes}, 64, 86
\langle x, y \rangle, 5
\langle \langle \cdots \rangle \rangle, 287
\lceil X \rceil, 212
|x|, 4
|S|, 4
≤_T, 61, 65
≤_{log}, 225
≤_{NC^1}, 289
≤_{NP}, 290
≤_{NP}, 82
≤^P, 264
≤^P, 264
≤^P_m, 254
≤^P_{mio}, 254
≤^P_{XTR}, 263
≤^P_{mio}, 254
≤^P_{mio}, 254
≤^P_{XTR}, 263
≤_T, 49, 437
≤_T, 254
≤^P_{mio}, 284, 292
≤^P_{mio}, 77
≤_{T}, 61, 66
≤_{T}, 77, 263
≤_{T}, 278
≤_{T}, 114
⊕, 6
⊕(A), 346
⊕P, 346
⊕P^A, 356
#C, 339
#HC, 361
#P, 334
#P^A, 356
#P-complete function, 336
#SAT, 333, 336, 403
#SS, 361
#3-SAT, 337
#VC, 337
A_{mio}, 204
A_{sat}, 204
A^P, 4
(a, b)-acceptance, 242
A-reducibility, 455
Aanderaa, 198
INDEX

ACI, 223
accept_M(x), 304
adjacency matrix, 47, 152, 414
eigenvalue, 414
Adleman, L., 118, 330
adversary argument, 159
affine subspace, 287
Aho, A., 70
Aiello, W., 251, 406
Alon, N., 250
alphabet, 4
alternating tree, 97
alternating Turing machine (ATM), 95, 223
accepting computation subtree, 95
existential configuration, 95
existential state, 95
polynomial-time, 96
universal configuration, 95
universal state, 95
AM, 376
AM^p, 376
AM^A^0, 404
AM hierarchy, 379, 384
AM2 circuit, 249
AM2 CIRCUIT VALUE, 249
amplification of accepting probability, 310
AP-reduction, 456
APPROX-BP, 79
APPROX-GCOLOR, 79
APPROX-KS, 73
APPROX-SCS, 79
approximation, see also c-approximation and r-APPROX-II
ratio, 68, 437
to a counting function, 362
to an optimization problem, 68, 72, 437
to TSP, 69
approximation scheme, polynomial-time
(PTAS), 73
fully (FPTAS), 73
fully probabilistic, 363
arithmetic hierarchy, 83
Arora, S., 80, 455, 457
Arthur machine, 375
Arthur-Merlin proof system, 375, 376
Arvind, V., 406
ASPACE(O(n^2)), 96
assignment, see Boolean assignment
assignment tester, 414, 425, 428
assignment testing proof system, 433
ATIME(O(n^2)), 96
ATM, see alternating Turing machine
Aut(G), 403
automata theory, 102
automorphism, 176, 403
orbit of an, 177
axiomatizable theory, 131
sound, 131
theorem, 131
B, 8
B^P, 421
b-terminal, 219
Babai, L., 365, 406, 455
Bach, E., 148
Baker, T., 148
Balcázar, J., 293
Barrington, D., 189, 199
Beals, R., 250
Beame, C., 250
Beigel, R., 331
Belanger, J., 293
Bellare, M., 457
Bennett, C., 148, 331
Ben-Or, M., 251, 455
Berkowitz, S. J., 250
Berlekamp, E., 455
Berman, L., 293, 364
Berman, P., 293
Berman-Hartmanis Isomorphism Conjecture, 258
EXP version, 271, 275
Bern, M., 456
Bernstein, E., 24, 126
Bernstein-Schröder-Cantor Theorem, 254
Best, M. R., 198, 199
BFG, see BOOLEAN FORMULA GAME
BH, 115
BHP, see BOUNDED HALTING PROBLEM
bi-immune set, 271; see also strongly bi-immune set
relative, 291
BIN PACKING (BP), 79
binary tree, 154
binomial distribution, 421
bipartite graph, 153
bipartite graph property, 153, 163, 178
blank symbol (\lambda), 8
BLR test, see Blum–Luby–Rubinfeld test
Blum, A., 80
Blum, L., 148
Blum, M., 43, 456
INDEX

Blum, N., 240
Blum–Luby–Rubinfeld test, 429
Blum’s Speed-up Theorem, 19, 40
Bollobás, B., 199
Book, R., 44, 118, 148, 293
Boolean assignment, 6
  invariant, 176
  partial, 6
  truth, 6
Boolean circuit, 108, 200
  AM2, 249
  depth, 201
  encoding of a, 222
  fan-in, 200
  bottom, 230
  generated by a DTM, 109
  interpreter, 208
  levelable, 229, 355
  logical gates, 200
  monotone, 210
  planar, 237
  polynomial-size, 204, 270, 315
  random, 242
  size, 201
Boolean formula, 7
  bounded variable, 101
  clause, 7
  conjunctive normal form, 7, 53, 76
  disjunctive normal form, 7, 76
  quantified, see quantified Boolean formula
  𝑟-unsatisfiable, 408
  3-CNF, 53, 91, 113
  3-DNF, 91
Boolean Formula Game (BFG), 110, 111, 117
Boolean function, 6
  contravariant of a, 153
  dual of a, 153
  elusive, 157
  graph property, 152
  monotone, 152, 211
  restriction of a, 6
  random, 230
  symmetric, 162
  symmetric permutation, 176
  trivial, 153
  weakly symmetric, 162
Boolean hierarchy, 115
Boolean Matrix Multiplication, 224
Boppana, R., 242, 390, 440
Borel field, 136
Borel set, 136
Borodin, A., 250, 251, 286

Bounded Halting Problem (BHP), 50
  relativized, 89
bounded variable, in a Boolean formula, 101
BP, see Bin Packing
BP(𝐴), 349
BP-operator, 348
BPP, 309
BPP, 309
BPP, 309
BPP machine, universal, 315
BPP Theorem, 319
  generalized, 321
branching program, 187
  bounded-width, 188
  permutation, 188
  𝜎-computation, 189
Brightwell, G., 364
Broder, A. Z., 365
Buss, J., 68, 80
Busy Beaver, 41
  time-bounded version, 42

C, 262
C0, 248, 358
c(𝐹), 437
C(𝑓), 201
C(𝑓), 201
C/P, 206
c-approximation, by a Boolean circuit, 243, 357
C-hard problem, 67
Cai, J.-Y., 118, 199, 250, 293, 364, 365
Cantor, G., 29
Cantor space, 136
Carter, J. L., 406
Cauchy–Schwartz inequality, 415, 417
CC, 242
census function, 262
  certificate, 46
CFL, 116
CG-Sat, see Constraint Graph Satisfiability
Chandra, A., 118, 250
characteristic function, 19, 65
characteristic sequence, of a set, 136
χ, 19
χ, 204
Christofides, N., 80
Church-Turing Thesis, 11
  extended, 23
circuit, see Boolean circuit
circuit size complexity, 201, 204
Circuit Value Problem (CVP), 108, 236, 285
class, see complexity class and language class
INDEX

clause, 7
    prime, 7
    size of a, 7
clique, 55
CLIQUE, 55, 61, 253
CLIQUE_k,n, 211
clique indicator, 212
(CLIQUE, r-NOClique), 439
clocked machine, see Turing machine
CNF, see conjunctive normal form
Cobham, A., 44
coding, 4
Coffman, E., 80
collapsing degree, 285
COMPACT CIRCUIT VALUE, 242
comparator gate, 241
complementary predicates, 379
    AM_k(r)-, 379
    AM_k(n)-, 404
    MA_k(r)-, 379
completeness, 50
complexity core, polynomial-time, 291
complexity measure; see also Kolmogorov complexity, and time complexity measure
growth rate, 23
certainty class, 19
nonuniform, 222
uniform, 222
computable function (language), 11
    feasibly, 22
    partial, 11
computable real number, see real number
computational model, 11
    nondeterministic, 12
    nonuniform, 12
    probabilistic, 12
    reasonable, 12, 23
concatenation,
of strings, 4
    of languages, 4
Condon, A., 456, 457
configuration, 9
    existential, of an ATM, 95
game, 105
    losing, 105
    initial, 10
    of an oracle DTM, 64
    of a Merlin machine, 377
    of a PTM, 303
conjunction, 6
conjunctional normal form (CNF), 7, 53, 76
coNP, 386
const, 410
constraint graph, 411
    reduction, 426
degree-reduction, 418
    expanderization, 419
    gap amplification, 427
    power graph, 420
    t-step path, 420
CONTRAST GRAPH SATISFIABILITY (CG-SAT), 411
countable set, 29
counting problem, 334
    approximation to a, 362
    polynomial-time computable, 334
Cramer’s rule, 48, 49
creative set, see p-creative set and k-creative set
Crescenzi, P., 456
CRITICAL HC, 114
cryptography, 120, 122
cSA(n), 204
CSA(n), 204
Csansky, L., 251
CVP, see CIRCUIT VALUE PROBLEM
cycle, 47, 154
cycle cover, 339
cylinder, 136, 289
D(f), 155
D_1(f), 7, 155, 247
D_0(f), 7, 155
Daley, R., 44
de Morgan’s law, 201
decision problem, 61, 333
    partial, 437
decision tree, 154
    depth, 155
    randomized, see randomized decision tree
choice node, 154
decision tree complexity, 155
decision tree characterization, of BPP, 319
decision tree, 154
    depth, 155
    randomized, see randomized decision tree
choice node, 154
decision tree complexity, 155
decision tree characterization, of RP, 318
degree, 285
collapsing, 285
    iso-, 285
delayed diagonalization, 122
Δ, 15
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Delta^*$</td>
<td>170</td>
</tr>
<tr>
<td>$\Delta^\delta$</td>
<td>178</td>
</tr>
<tr>
<td>$\Delta^n$</td>
<td>83</td>
</tr>
<tr>
<td>$\delta$</td>
<td>9</td>
</tr>
<tr>
<td>$\delta$-close</td>
<td>425</td>
</tr>
<tr>
<td>$\delta$-far</td>
<td>425</td>
</tr>
<tr>
<td>DeMoivre-Laplace Limit Theorem</td>
<td>232</td>
</tr>
<tr>
<td>density</td>
<td>262</td>
</tr>
<tr>
<td>subexponential</td>
<td>274</td>
</tr>
<tr>
<td>derandomization</td>
<td>287</td>
</tr>
<tr>
<td>$\det X$</td>
<td>47</td>
</tr>
<tr>
<td>determinant</td>
<td>47</td>
</tr>
<tr>
<td>of an integer matrix</td>
<td>47</td>
</tr>
<tr>
<td>of a polynomial matrix</td>
<td>299</td>
</tr>
<tr>
<td>Determinant of a Polynomial Matrix (DPM)</td>
<td>299</td>
</tr>
<tr>
<td>Deterministic Finite Automata Intersection (DFA-INT)</td>
<td>116</td>
</tr>
<tr>
<td>deterministic Turing machine</td>
<td>116</td>
</tr>
<tr>
<td>see Turing machine</td>
<td></td>
</tr>
<tr>
<td>Deutsch, D.</td>
<td>126</td>
</tr>
<tr>
<td>DFA-INT, see Deterministic Finite Automata Intersection</td>
<td></td>
</tr>
<tr>
<td>DGISO</td>
<td>144</td>
</tr>
<tr>
<td>diagonalization</td>
<td>29</td>
</tr>
<tr>
<td>delayed</td>
<td>122</td>
</tr>
<tr>
<td>stage construction</td>
<td>140</td>
</tr>
<tr>
<td>Diffie, W.</td>
<td>148</td>
</tr>
<tr>
<td>digital signature</td>
<td>123</td>
</tr>
<tr>
<td>digraph</td>
<td>153</td>
</tr>
<tr>
<td>loop in a</td>
<td>153</td>
</tr>
<tr>
<td>dimension of a face</td>
<td>169</td>
</tr>
<tr>
<td>Dinur, I.</td>
<td>456</td>
</tr>
<tr>
<td>directed graph, see digraph</td>
<td></td>
</tr>
<tr>
<td>disjunction</td>
<td>6</td>
</tr>
<tr>
<td>disjunctive normal form (DNF)</td>
<td>7, 76</td>
</tr>
<tr>
<td>Distance Lemma</td>
<td>214</td>
</tr>
<tr>
<td>second</td>
<td>219</td>
</tr>
<tr>
<td>DNF, see disjunctive normal form</td>
<td></td>
</tr>
<tr>
<td>$DP$</td>
<td>114</td>
</tr>
<tr>
<td>$DP_{ac}$</td>
<td>115</td>
</tr>
<tr>
<td>DPM, see Determinant of a Polynomial Matrix</td>
<td></td>
</tr>
<tr>
<td>$DSPACE(n(n))$</td>
<td>19</td>
</tr>
<tr>
<td>$DTIME(n(n))$</td>
<td>19</td>
</tr>
<tr>
<td>DTM, see Turing machine, deterministic</td>
<td></td>
</tr>
<tr>
<td>Du, D.-Z.,</td>
<td>293</td>
</tr>
<tr>
<td>Du, X.</td>
<td>456</td>
</tr>
<tr>
<td>dual</td>
<td>153</td>
</tr>
<tr>
<td>Dunne, P. E.</td>
<td>250</td>
</tr>
<tr>
<td>dynamic programming</td>
<td>74</td>
</tr>
<tr>
<td>edge</td>
<td>44, 152</td>
</tr>
<tr>
<td>edge expansion</td>
<td>414</td>
</tr>
<tr>
<td>Edmonds, J.</td>
<td>44</td>
</tr>
<tr>
<td>elementary collapse</td>
<td>171</td>
</tr>
<tr>
<td>elementary product</td>
<td>7</td>
</tr>
<tr>
<td>elementary sum</td>
<td>7</td>
</tr>
<tr>
<td>Elgot, C. C.</td>
<td>44</td>
</tr>
<tr>
<td>elusive</td>
<td>157</td>
</tr>
<tr>
<td>empty string</td>
<td>4</td>
</tr>
<tr>
<td>enumerable set</td>
<td>29</td>
</tr>
<tr>
<td>Erdős-Rado Sunflower Lemma,</td>
<td>215</td>
</tr>
<tr>
<td>$er_{\delta}(x)$</td>
<td>305</td>
</tr>
<tr>
<td>error probability</td>
<td>of a PTM, 305</td>
</tr>
<tr>
<td>Euclidean graph</td>
<td>70</td>
</tr>
<tr>
<td>Euler characteristic</td>
<td>170</td>
</tr>
<tr>
<td>Euler function</td>
<td>128</td>
</tr>
<tr>
<td>Eulerian circuit</td>
<td>71</td>
</tr>
<tr>
<td>Eulerian circuit problem</td>
<td>71</td>
</tr>
<tr>
<td>Eulerian graph</td>
<td>71</td>
</tr>
<tr>
<td>Exact CLIQUE</td>
<td>61, 88, 114</td>
</tr>
<tr>
<td>Exact-TSP</td>
<td>78</td>
</tr>
<tr>
<td>exclusive-or</td>
<td>6</td>
</tr>
<tr>
<td>EXP</td>
<td>22, 108</td>
</tr>
<tr>
<td>EXP-BHP, see Exponential-time Bounded Halting Problem</td>
<td></td>
</tr>
<tr>
<td>EXP-complete set</td>
<td>108</td>
</tr>
<tr>
<td>EXP-CVP, see Exponential-size Circuit Value Problem</td>
<td></td>
</tr>
<tr>
<td>EXP-SAT</td>
<td>113</td>
</tr>
<tr>
<td>expander</td>
<td>414, 444</td>
</tr>
<tr>
<td>$(n, d, \lambda)$-expander</td>
<td>414</td>
</tr>
<tr>
<td>Lubotzky–Hillip–Sarnak</td>
<td>416</td>
</tr>
<tr>
<td>Marguli–Gaber–Galil</td>
<td>416</td>
</tr>
<tr>
<td>expecttime$_{EF}(x)$</td>
<td>306</td>
</tr>
<tr>
<td>Exponential-size Circuit Value Problem (EXP-CVP)</td>
<td>109</td>
</tr>
<tr>
<td>Exponential-time Bounded Halting Problem (EXP-BHP)</td>
<td>108</td>
</tr>
<tr>
<td>exponentiation</td>
<td>modulo an integer, 127</td>
</tr>
<tr>
<td>EXPSPACE</td>
<td>22</td>
</tr>
<tr>
<td>EXPSPACE-complete set</td>
<td>114</td>
</tr>
<tr>
<td>Extended Church-Turing Thesis</td>
<td>23</td>
</tr>
<tr>
<td>Extrating A Bit</td>
<td>224</td>
</tr>
<tr>
<td>$f^*$</td>
<td>153</td>
</tr>
<tr>
<td>$f_{\epsilon}$</td>
<td>6</td>
</tr>
<tr>
<td>$f_{con}$</td>
<td>152, 246</td>
</tr>
<tr>
<td>$f_{\text{SAT}}$</td>
<td>123</td>
</tr>
<tr>
<td>$f^*_p$</td>
<td>248, 359</td>
</tr>
<tr>
<td>face</td>
<td>169</td>
</tr>
<tr>
<td>dimension</td>
<td>169</td>
</tr>
<tr>
<td>free</td>
<td>171</td>
</tr>
<tr>
<td>maximal</td>
<td>171</td>
</tr>
<tr>
<td>FACTOR, see Integer Factoring</td>
<td></td>
</tr>
</tbody>
</table>
INDEX

false(τ), 159
fan-in, 200
FBPPNP, 363
FΔp, 362
feasible subgraph, 450
feasibly computable problem, 22
Feather, T., 251
Feige, U., 455, 457
Fenner, S., 293
FewP, 363
finite-to-one function, 271
Fischer, M., 249
fixed point, 175, 179
Fixed Point Theorem, 175, 179
Gacs, P., 331
Galos field, 180, 287
game, see two-person game
Gao, S.-X., 199
gap amplification, 414
GAP Constraint Graph Satisfiability, 411
Garey, M. R., 80, 456
gate-elimination method, 203
GC, see GRAPH CONSISTENCY
GColor, see GRAPH COLORING
GColorc, 115
Generalized Matching (GM), 361
Generalized BPP Theorem, 321
Generalized Ramsey Number (GRN), 92
Geography, 106, 116
geometric simplicial complex, 169
GF(m), 180, 287
Gill, J., 148, 330, 331
girth, 181
GIso, see GRAPH ISOMORPHISM
GIso, see GRAPH NONISOMORPHISM
GM, see GENERAL MATCHING
Goldman, M., 250
Goldreich, O., 406
Goldschläger, L. M., 250, 251
Goldsmith, J., 293
Goldwasser, S., 406
Graham, R. L., 456
graph(s), 46, 151; see also digraph
Boolean function representation, 151
clique of a, 55
complement, 253
connected, 152
cubic, 448
cycle in a, 47, 154
d-regular, 414
directed, see digraph
degree of a, 46, 152
degree expansion, 414
Euclidean, 70
Eulerian, 71
factor-critical, 198
girth of a, 181
isomorphic, 152
k-colored, 92
nonplaner, 194
path in a, 47, 152
planar, 70
scorpion, 195
vertex cover of a, 54
vertex of a, 46, 152
GRAPH ACCESSIBILITY (GAcc), 224
undirected graph, 248
GRAPH COLORING (GColor), 78, 413
GRAPH CONSISTENCY (GC), 115
GRAPH 3-COLORABILITY (G3C), 413
GRAPH ISOMORPHISM (GIso), 119, 144, 396, 405
GRAPH NONISOMORPHISM (GIso), 369, 403, 405
graph property, 152
bipartite, 153
monotone, 166
Greenlaw, R., 251
GRN, see GENERALIZED RAMSEY NUMBER
Grollman, J., 148
GCol, 4
G3C, see GRAPH 3-COLORABILITY
guess-and-verify algorithm, 18, 46
**INDEX**

$H^k_p$, 364
$H^k_{p,x}$, 364
Halldórsson, M., 440
halt$_M(x)$, 304
halting probability, of a PTM, 304
halting problem, 29, 50
relativized, 129
Hamiltonian Circuit (HC), 47, 56, 71
paddability, 259
Hamiltonian circuit, 47
Hamming distance, 425
hardness, 50
Hartmanis, J., 43, 44, 148, 292, 293, 364, 406
hashing function, 391
linear, 391
random, 391
universal, 391
Håstad, J., 148, 250, 365, 406, 438, 440, 457
HC, see Hamiltonian Circuit
Heller, H., 148, 331
Hellman, M., 148
Hemachandra, L. A., 293, 331, 364
HIX, 117
high hierarchy, 364
relativized, 364
Holt, R. C., 198
Homer, S., 293
Hoory, 456
Hopcroft, J., 44, 70, 102, 148
Hopf index formula, 178
Hu, X.-D., 199
Huang, M. A., 330
Hunt, H. B. III, 118
Ibarra, O. H., 75, 80
IEE, see Integer Expression Equivalence
Illies, N., 199
Immerman, N., 44, 250
immune set, 271
implicant, 7
prime, 7
independence results, 131
Independent Set (IS), 55, 252
independent set, 55
inner product, 287
integer expression, 115
Integer Expression Equivalence (IEE), 115
Integer Factoring (Factor), 120, 125
Integer Programming (IP), 47, 58
interactive proof system, 120, 368, 373, 402, 407
multi-prover, 452
probabilistic, 368
interactive protocol, 402
$k$-prover, 453
interactive Turing machine, 373
invariant assignment, of a symmetric permutation, 176
inverter, 246
inverted function, polynomial-time, 254
invertible reducibility, polynomial-time, 254
$\psi$, 5, 25
IP, see Integer Programming
$IP^p$, 374
$IP^p_{q(n), r(n)}$, 387
IS, see Independent Set
IS-b, 441
is-$\psi(G)$, 442
iso-degree, 285
Isolation Lemma, 244, 350
isomorphism, polynomial-time, 253
isomorphism type, 285
Jerrum, M. R., 365
Jiang, T., 118
Johnson, D., 80, 406
join, 84, 264
Joseph, D., 275, 293
Joseph-Young Conjecture, 275
$EXP$ version, 275
$K$, 29
$K_A$, 129, 140
$K(A)$, 325
$k$-colored graph, 92
$k$-creative set, 275, 290
$k$-truth-table reducibility, polynomial-time, 263
$k$-UP, 144
Kahn, J., 199
Kannan, S., 456
Karloff, H., 438, 456
Karmarkar, N., 80, 147
Karp, R. M., 80, 147, 199, 250, 251, 331
Karp conjecture, 168
Khachiyan, L., 147
Khanna, S., 80
Killian, J., 406, 457
Kim, C. E., 75, 80
King, V., 199
Kirkpatrick, D., 198
Kiwi, M., 457
Klee, S. C., 43
Klee closure, 4
Kleitman, D. J., 199
Knapsack (KS), 73
<table>
<thead>
<tr>
<th>Index Item</th>
<th>Page Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ko, K.</td>
<td>44, 80, 118, 148, 251, 292, 293, 331, 364, 365, 457</td>
</tr>
<tr>
<td>Köbler, J.</td>
<td>406</td>
</tr>
<tr>
<td>Kolmogorov, A. N.</td>
<td>136</td>
</tr>
<tr>
<td>Kolmogorov complexity</td>
<td>44</td>
</tr>
<tr>
<td>Kozen, D.</td>
<td>118</td>
</tr>
<tr>
<td>Kranakis, E.</td>
<td>148</td>
</tr>
<tr>
<td>KS, see Knapsack</td>
<td></td>
</tr>
<tr>
<td>Kuratowski’s Theorem</td>
<td>194</td>
</tr>
<tr>
<td>Kurtz, S.</td>
<td>293</td>
</tr>
<tr>
<td>Kwiatkowski, D. J.</td>
<td>250</td>
</tr>
<tr>
<td>LP_k</td>
<td>364</td>
</tr>
<tr>
<td>LP_k^X</td>
<td>364</td>
</tr>
<tr>
<td>L(M)</td>
<td>11</td>
</tr>
<tr>
<td>L(M, A)</td>
<td>82</td>
</tr>
<tr>
<td>L(M, f)</td>
<td>64</td>
</tr>
<tr>
<td>L-reduction</td>
<td>440</td>
</tr>
<tr>
<td>Ladner, R.</td>
<td>80, 148, 251</td>
</tr>
<tr>
<td>A, 4</td>
<td></td>
</tr>
<tr>
<td>A(G)</td>
<td>414</td>
</tr>
<tr>
<td>Landau, S.</td>
<td>250</td>
</tr>
<tr>
<td>language, 4</td>
<td></td>
</tr>
<tr>
<td>computable, 11</td>
<td></td>
</tr>
<tr>
<td>concatenation of, 4</td>
<td></td>
</tr>
<tr>
<td>context-sensitive, 37</td>
<td></td>
</tr>
<tr>
<td>recursive, 11</td>
<td></td>
</tr>
<tr>
<td>recursively enumerable (r.e.), 11</td>
<td></td>
</tr>
<tr>
<td>language class, 4</td>
<td></td>
</tr>
<tr>
<td>Laplace expansion</td>
<td>49</td>
</tr>
<tr>
<td>Laplante, S.</td>
<td>251</td>
</tr>
<tr>
<td>Lautemann, C.</td>
<td>331</td>
</tr>
<tr>
<td>Law of Quadratic Reciprocity</td>
<td>302</td>
</tr>
<tr>
<td>Lawler, E. L.</td>
<td>71, 75, 244</td>
</tr>
<tr>
<td>LE</td>
<td>361</td>
</tr>
<tr>
<td>Lebesgue measure</td>
<td>136</td>
</tr>
<tr>
<td>Lefschetz’ Fixed Point Theorem</td>
<td>175</td>
</tr>
<tr>
<td>Legendre symbol, 301</td>
<td></td>
</tr>
<tr>
<td>Legendre-Jacobi symbol, 301</td>
<td></td>
</tr>
<tr>
<td>length-increasing function, 254</td>
<td></td>
</tr>
<tr>
<td>levelable circuit, 229, 355</td>
<td></td>
</tr>
<tr>
<td>Levin, L.</td>
<td>80</td>
</tr>
<tr>
<td>Lewis, P. M.</td>
<td>43</td>
</tr>
<tr>
<td>lexicographic ordering, 5</td>
<td></td>
</tr>
<tr>
<td>Li, M.</td>
<td>44, 251</td>
</tr>
<tr>
<td>Lin, C.-L.</td>
<td>118, 457</td>
</tr>
<tr>
<td>linear congruence generator, see pseudorandom generator</td>
<td></td>
</tr>
<tr>
<td>linear extension</td>
<td>361</td>
</tr>
<tr>
<td>linear programming, 147</td>
<td></td>
</tr>
<tr>
<td>Linear Speed-up Theorem</td>
<td>21</td>
</tr>
<tr>
<td>link</td>
<td>173</td>
</tr>
<tr>
<td>Lipton, R. J.</td>
<td>199, 250, 251, 456</td>
</tr>
<tr>
<td>literal</td>
<td>7</td>
</tr>
<tr>
<td>Liu, C. L.</td>
<td>71</td>
</tr>
<tr>
<td>log</td>
<td>247, 410</td>
</tr>
<tr>
<td>log-space uniformity</td>
<td>223</td>
</tr>
<tr>
<td>LOGCFL</td>
<td>116</td>
</tr>
<tr>
<td>LOGSPACE</td>
<td>22</td>
</tr>
<tr>
<td>Long, T.</td>
<td>118, 148, 365</td>
</tr>
<tr>
<td>LONGEST DIRECT CIRCUIT</td>
<td>116</td>
</tr>
<tr>
<td>LONGEST PATH (LP)</td>
<td>454, 455</td>
</tr>
<tr>
<td>Lovász, L.</td>
<td>80</td>
</tr>
<tr>
<td>low hierarchy, 364</td>
<td></td>
</tr>
<tr>
<td>relativized, 364</td>
<td></td>
</tr>
<tr>
<td>Loxton, J. H.</td>
<td>148</td>
</tr>
<tr>
<td>LP, see Longest Path</td>
<td></td>
</tr>
<tr>
<td>Lund, C., 80, 406, 455–457</td>
<td></td>
</tr>
<tr>
<td>Lupanov, O. B.</td>
<td>249</td>
</tr>
<tr>
<td>Lynch, N.</td>
<td>80, 293</td>
</tr>
<tr>
<td>M, 329</td>
<td></td>
</tr>
<tr>
<td>M^A, 26</td>
<td></td>
</tr>
<tr>
<td>M^L, 26</td>
<td></td>
</tr>
<tr>
<td>M_{(x,y)}^A, 28</td>
<td></td>
</tr>
<tr>
<td>M^L, 82</td>
<td></td>
</tr>
<tr>
<td>M^L, 64, 82</td>
<td></td>
</tr>
<tr>
<td>MAJ</td>
<td>354</td>
</tr>
<tr>
<td>majority quantifier, 318</td>
<td></td>
</tr>
<tr>
<td>majority vote, 310</td>
<td></td>
</tr>
<tr>
<td>MAJ, 345</td>
<td></td>
</tr>
<tr>
<td>Manders, K., 118, 330</td>
<td></td>
</tr>
<tr>
<td>many-one reducibility, 49</td>
<td></td>
</tr>
<tr>
<td>log-space, 225</td>
<td></td>
</tr>
<tr>
<td>NC^1, 289</td>
<td></td>
</tr>
<tr>
<td>polynomial-time, 49, 78, 437</td>
<td></td>
</tr>
<tr>
<td>matching, 71, 361</td>
<td></td>
</tr>
<tr>
<td>MAX-Clique, 62, 68</td>
<td></td>
</tr>
<tr>
<td>MAX-SNP, 456</td>
<td></td>
</tr>
<tr>
<td>MAX-SNP-completeness, 456</td>
<td></td>
</tr>
<tr>
<td>maximal subset, 291</td>
<td></td>
</tr>
<tr>
<td>maximum satisfiability problem, 437</td>
<td></td>
</tr>
<tr>
<td>Mayr, E. W.</td>
<td>251</td>
</tr>
<tr>
<td>McKenzie, P.</td>
<td>250</td>
</tr>
<tr>
<td>McMillan’s Theorem, 5</td>
<td></td>
</tr>
<tr>
<td>MCV, see Monotone Circuit Value</td>
<td></td>
</tr>
<tr>
<td>Merlin machine, 377</td>
<td></td>
</tr>
<tr>
<td>accepting probability, 377</td>
<td></td>
</tr>
<tr>
<td>configuration, 377</td>
<td></td>
</tr>
<tr>
<td>Meyer, A.</td>
<td>117, 292</td>
</tr>
<tr>
<td>Micali, S.</td>
<td>406</td>
</tr>
<tr>
<td>Miller, G.</td>
<td>330</td>
</tr>
<tr>
<td>Milner, E. C.</td>
<td>199</td>
</tr>
<tr>
<td>MIN-BISECTION</td>
<td>454</td>
</tr>
</tbody>
</table>
MIN-NFA, see Minimal Nondeterministic Finite Automaton
MIN-TSP, 78
Minimal Nondeterministic Finite Automaton (MIN-NFA), 116
Minimax, 158
MINIMAX-CIRCUIT, 116
MINIMAX-CLIQUE, 115
MINIMAX-3DM, 116
minimum matching problem, 71
minimum spanning tree problem, 70
minterm, 7, 153
MIP, 455
Mitchell, J., 457
MOD function, 219
monoid, 4
monotone circuit, 210
MONOTONE CIRCUIT VALUE (MCV), 236
Moore, D., 293
Moran, S., 250, 406
Motwani, R., 330
μ, 136
μ(f), 162
Mulmuley, K., 251, 286, 365
multiplication, 129
of integers, 246
of permutations, 246
Myhill, J., 292
(n, d, δ)-expander, 414
NAND CIRCUIT VALUE, 249
NAND gate, 249
NC, 223
reducibility, 248
NC^1, 223,
NC^2, 289
NC^3, 285
 Neciporuk, E. I., 194
negation, 6
negligibility, 125
network, 237
flow, 237
NEXP, 22
NEXP-complete set, 113
NEEXPOLY, 410
Nick’s class, 250
Nisan, N., 331, 406
NLOGSPACE, 22, 226
NLOGSPACE-complete set, 226
nonadaptive proof system, 408
nondeterministic Turing machine
(NTM), 14; see also Turing machine
accepting a string, 15
accepting path, 15
computation, 15
computing a function, 16
halting path, 15
k-ambiguous, 144
oracle, see oracle nondeterministic Turing machine
output, 15
unambiguous, 124
universal, 27
nonuniform complexity class, 222
nonuniform-AC^0, 222
nonuniform-NC, 223
nonuniform-NC^1, 222
nonuniform-NC^2, 228
normal subgroup, 179
NOT-ALL-EQUAL-3SAT, 77
NP, 22, 45
characterization of, 45
PCP, 411
enumeration of, 28
NP^A, 82
NP^k, 82
NP(C), 82
NP(poly), 208
NP^k ∩ coNP^k, 140
NP-complete set, 50
natural, 51, 252, 258
NPSPACE, 35
NSPACE(s(n)), 20, 22
NTIME(t(n)), 20
NTM, see nondeterministic Turing machine
ODD MAXIMUM FLOW (OMF), 238
Ogihara, M., 293
Ogiwara, M., 293
Oliver, R., 199
Ω(f(n)), 41
ω(G), 438
OMF, see ODD MAXIMUM FLOW
1-factor, 194
1-IN-3-SAT, 76
(1,r)Gap-3SAT, 408
(1,δ)Gap-CG-SAT, see Gap Constraint
GRAPH SATISFIABILITY
one-one reducibility, polynomial-time, 254; see also invertible reducibility
one-sided error, 311
one-way function, 122, 145, 278
characterization, 124
k-to-one, 126
length-increasing, 277
strong, 125
INDEX

trapdoor, 127
weak, 123, 275
optimization problem, 63, 68, 440
approximation to an, see approximation
NP-hard, 437
solution, 68
value of a, 68
oracle, 61
function, 63
random, 135, 322, 358, 360
set, 64
oracle class, 136
oracle nondeterministic Turing machine, 82; see
also oracle Turing machine
answer state, 82
polynomial-time, 82
query state, 82
query tape, 82
oracle probabilistic Turing machine, 321; see
also oracle Turing machine
nonadaptive, 409
Oracle-SAT, 117
oracle Turing machine, 63
answer state, 63
computation, 77
function oracle, 63
polynomial-time, 65
positive, 77
query state, 63
query string, 64
query tape, 63
robust, 79
set oracle, 64
orbit, 177, 179
center of gravity, 177
Orponen, P., 80, 293

P, 22
enumeration of, 28
P^B, 66
P^C, 66
P^P, 335
P^poly, 161
P^log, 247
P\text{-}\text{bi-immune set}, 271
P\text{-}\text{complete set}, 108, 236
P\text{-}\text{creative set},
for \text{NP}, 290
for \text{P}, 290
P\text{-}\text{immune set}, 271
P\text{-}\text{isomorphic sets}, 253
P\text{-}\text{selective set}, 291
paddable set, 257
length-increasingly, 257
weakly, 275
padding function, 257
pairing function, 5, 38
Panconesi, A., 456
Papadimitriou, C. H., 118, 364, 456
parallel computation, 223
parallel random access machine (PRAM), 223
Parity, 223
parity_{x}(x), 346
parity function, 155, 223, 229
parity machine, 346
parity operator, 346
Parity-CVP, 286
Parseval’s Identity, 430
partial assignment, 6
partial computable function, 11
partial decision problem, 437
partial function, 9, 11
partial ordering, 264
polynomially related, 264
linear extension, 361
partial recursive function, 11
PARTITION, 60, 61
paddability, 259
Paterson, M., 292
path, 47, 152
simple, 47
Paul, W. J., 44
PCP, 409; see also probabilistic checkable proof
systems
PCP(F, G), 410
PCP(r(n), \phi(n)), 410
PCV, see PLANAR CIRCUIT VALUE
Perfect Matching (PM), 244
Peerm, 339, 370
perm(A), 339
permanent,
of a Boolean matrix, 344
of an integer matrix, 339
permutation,
cyclic, 164, 190
symmetric, 176
permutation branching program, 188
permutation group, 162
transitive subgroup, 162
PH, 83
characterization of, 87
PCP, 457
\phi_M, 334, 352
\phi(n), 128
\Pi, 68
\Pi^P, 85
Π²-predicate, 85
Π²-complete set, 92
Pippenger, N., 250, 251
planar circuit, 237, 244
Planar Circuit Value (PCV), 237
Plassmann, P., 456
plucking operation, 215
Plumstead, J., 148
PM, see Perfect Matching
poly, 206, 410
polynomial-size circuit, 204, 270, 315
polynomial-time approximation scheme, see approximation scheme
collapsing of, 87
PCP characterization of, 457
relativized, 114, 359
polynomial-time invertible function, 254
polynomial-time invertible reducibility, 254
polynomial-time isomorphism, 253
polynomially honest function, 76, 123
positive relativization, 133
Post's problem, 122
PP, 307, 335
PP-completeness, 345
PRAM, see parallel random access machine
Pratt, V., 250
prefix set, 76

Prep(G), 420
Primality Testing (Prime), 301
Prime, see Primality Testing
PrimeSAT, 362
private-key cryptosystem, 127
probabilistic algorithm, 120
probabilistic interactive proof system, see interactive proof system
probabilistic nondeterministic Turing machine, 377
probabilistic quantifier, 318
probabilistic Turing machine (PTM), 302
accepting an input, 305
accepting probability, 304
configuration, 303
equivalence of, 306
halting probability, 304
random state, 409
rejecting probability, 304
strong equivalence of, 306
probabilistically checkable proof (PCP) systems, 409
weak, 425, 433
program over a monoid, 198
projection, of a Boolean circuit, 214, 219
promise problem, 437
pseudo polynomial-time algorithm, 73
pseudorandom generator, 123, 145, 330
linear congruence generator, 145
n°-generator, 330
quadratic residue generator, 145
strongly unpredictable, 330

PSPACE, 22
counting of, 28
classification of, 34
PCP, 457
PSPACE-complete set, 100
PTAS, see approximation scheme
PTM, see probabilistic Turing machine

public-key cryptosystem, 122, 126
ciphertext, 127
decryption algorithm, 127
decryption key, 127
encryption algorithm, 126
encryption key, 127
plaintext, 127
Rivest-Shamir-Adleman (RSA), 127

QBF, see Quantified Boolean Formula
q(T), 96

QN, see Quadratic Nonresidues
QR, see Quadratic Residuosity
QB, 120, 369
QR, 313
Quadratic Nonresidues (QNR), 369
quadratic residue, 120, 301
quadratic residue generator, see pseudorandom

quadratic residue

Quadratic Residuosity (QR), 120, 396
Quantified Boolean Formula (QBF), 101, 105

quantifier, 101

Quantifier changes of an ATM, 96
quantum Turing machine, 24, 126
query bits, 407
Quicksort,

deterministic algorithm, 298
randomized algorithm, 298

R, 230
R+ = 248
R(f), 182
INDEX

r-APPROX-CLIQUE, 438
r-APPROX-Π, 437
r-APPROX-3SAT, 437
r-APPROX-TSP, 69
r-degree, 285
r.e., see recursively enumerable language
r-NOClique, 439
r-UNSAT, 438
Rabin, M., 120, 129, 148, 330
Rackoff, C., 148, 331, 406
Radhakrishnan, J., 456
Raghavan, P., 330
RAM, see random access machine
random access machine (RAM), 39
complexity measure, 40
random bit(s), 407
generator, 303
shared, 146
random circuit, 242
random oracle, 135, 322, 358, 360
random restriction, 230
random walk, in an expander, 416
randomization, 287
randomized algorithm, 297
randomized decision tree, 182
expected depth, 182
expected time, 182
randomized decision tree complexity, 182
randomized reduction, 348
rank, of a matrix, 286
Ravikumar, B., 118
Rayleigh quotient, 415
Raz, R., 457
Razborov, A. A., 250
reach(a, β, k), 97, 397
real number,
computable, 42
binary, 43
Cauchy, 42
Dedekind, 42
Turing, 43
polynomial-time computable, 43
binary, 43
Cauchy, 43
Dedekind, 43
recursion theory, 11
recursive function (language), 11
partial, 11
recursive function theory, 11
recursively enumerable (r.e.) language, 11
reducibility, 49; see also many-one reducibility,
one-one reducibility, strong NP reducibility,
truth-table reducibility
and Turing reducibility
adaptive, 77
conjunctive, see truth-table reducibility
disjunctive, see truth-table reducibility
NC, 248
polynomial-time invertible, 254
regular expression, 102
extended, 114
Reingold, E. M., 198
Reingold, N., 331
Reingold, O., 250, 456
reject_M(x), 304
relativization, 82, 129
positive, 133
restriction, 6, 230
random, 230
Rice, H., 44
Rivest, R., 148, 198
Rivest-Shamir-Adleman cryptosystem (RSA), 127
RNC, 244
Rogers, H. Jr., 11, 43, 79, 83, 118
Rogers, J., 293
Roman, S., 43, 455
Rosenberg, A. L., 198
RP, 311
RP^1, 321
RSA cryptosystem, see Rivest-Shamir-Adleman
   cryptosystem
RTIME(t(n)), 307
Rubinfeld, R., 456
running time, see time complexity
Russo, D., 293
Ruzzo, W., 80, 118, 331
S_i, 162
s_M(n), 19, 20, 96
Safra, S., 455
Saks, M., 331
SAT, see SATISFIABILITY
SAT^p, 89, 209
sat*(F), 437
(SAT, r-UNSAT), 438
SAT-UNSAT, 114
SATISFIABILITY (SAT), 46, 256
paddability, 258
self-reducibility, 263
Savitch, W., 44
Savitch’s Theorem, 34, 97, 397
SBHP, see SPACE BOUNDED HALTING PROBLEM
SC, see SET COVER
Schaefer, T. J., 80, 118
Schöning, U., 80, 147, 293, 365, 406
INDEX

Schwartz, J., 406
scorpion graph, 195
SCS, see shortest common superstring
search problems, 59, 333
second moment method, 421
Seiferas, J. I., 44
self-correction procedure, 331
self-reducibility, 263
c-, 264
d-, 264
cT-, 290
tc, 264
self-reducing tree, 263
Selman, A., 148, 293
SET COVER (SC), 450
SET SPLITTING, 77
Shallit, J., 406
Shamir, A., 406
Shannon, C. E., 249
Shepherdson, J. C., 44
Shou, M., 365
Shor, P. W., 24, 126
SHORTEST COMMON SUPERSTRING (SC), 79
STEINER MINIMUM TREE (SMT), 454
STEINER MINIMUM TREE IN GRAPH (SMT-G), 454
Stockmeyer, L., 117, 118, 365
Storer, J., 80
straight-line arithmetic program, 362
Strassen, V., 330
Straubing, H., 199
string, 3
empty, 4
length of a, 4
STRING MATCHING, 327
strong NP reducibility, 114, 145
strongly bi-immune set, 272
sparse, 273
strongly unpredictable pseudorandom
generator, 330
strongly unpredictable set, 126
Sturgis, H. E., 44
subexponential density, 274
SUBGRAPH ISOMORPHISM, 77, 120
Subramanian, A., 251
SUBSET INTERCONNECTION DESIGN (SID), 450
SUBSET SUM (SS), 59
Sudan, M., 456
Sudborough, J. H., 118
sunflower, 215
center, 215
petal, 215
Swapping Lemma, 318
second form, 329
Switching Lemma, 230
symmetric permutation, of a Boolean function, 176
Szelepcsényi, R., 44

\( t_M(n) \), 19, 20, 82, 96
\( t_M^A(n) \), 65, 82
\( \tilde{t}_M(n) \), 306
tally set, 41, 269, 316
Tape Compression Theorem, 20
Tardos, E., 250
Tarjan, R. E., 118, 251

TERE, see TOTALITY OF EXTENDED REGULAR EXPRESSIONS
terminal, 212; see also b-terminal
tetrahedron, 168

\( TH_{n,m} \), 203
3-CNF, 53, 101; see also Boolean formula and quantified Boolean formula
3-DNF, 91; see also Boolean formula
3-CNF-SAT, 92
3-CNF-\( \text{TAU}_k \), 92
3-DIMENSIONAL MATCHING (3DM), 77
3-DNF-SAT, 92
3-DNF-\( \text{TAU}_k \), 92
3-QBF, 102
3-SAT, 53, 256
3DM, see 3-DIMENSIONAL MATCHING
3SAT-3, 444
threshold function, 203
time complexity, 18–20, 65, 82, 96
\( t_M(x) \), 18, 20, 96, 305
\( t_M^A(x) \), 65, 82
time complexity of PTM, 305
uniform, 306
time complexity measure, 22, 40
logarithmic, 40
reasonable, 23
uniform, 306


truth assignment, 6
truth-table, 6
truth-table reducibility, polynomial-time, 77, 263; see also k-truth-table reducibility
bounded, 115
conjunctive, 264
disjunctive, 264
TSP, see TRAVELING SALESMAN PROBLEM

TT-condition, 263
Turing, A., 43, 44
Turing machine(s) (TM), 8
alternating, see alternating Turing machine
clocked, 27
enumeration of, 28
computation, 10
configuration, 9
deterministic (DTM), 8
encoding of a, 25
ten of enumeration, 25
halting of, 10, 29
interactive, 373
multi-tape, 12, 39
next configuration function, 9
non-deterministic, see nondeterministic Turing machine
oracle, see oracle Turing machine
poly-time, 22
program of a, 8
probabilistic, see probabilistic Turing machine
quantum, 24, 126
space complexity, see space complexity
storage tape, 12
time complexity, see time complexity
universal, 26

Turing reducibility, 61, 65
log-space, 78
polynomial-space, 67, 78
poly-time, 61, 66, 335
INDEX

Turing reducibility (Continued)
  positive, polynomial-time, 77
  work tape, 12
2-APPROX-SAT, 438
two-person game, 104, 366
  configuration, 105
  polynomially bounded, 105
  winning strategy, 105
2-SAT, 76
two-sided errors, 311
Tzeng, W.-G., 118
Ullman, J., 44, 70, 102
uniform complexity class, 222
uniformity, log-space, 223
universal hashing function, 391
universal BPP machine, 315
unrelativizable proof technique, 131
\text{UNSAT}(G), 411
\text{UNSAT}_w(G), 411
\text{UP}, 124; see also \text{k-UP}
\text{UP}^1, 144

\nu_0(y), 440
\nu_0^1(x), 440
VC, see \text{VERTEX COVER}
\text{vc}^*(G), 442
VC-9, 441
VC-IN-CUBIC-GRAPHS (VC-CG), 448
VC-CG, see VC-IN-CUBIC-GRAPHS
Valiant, L., 148, 364, 365
van Emde Boas, P., 250
van Melkebeek, D., 293
Vazirani, U. V., 24, 126
Vazirani, V. V., 365
vector space, 287
vertex, 46, 152
adjacent, 152
\text{VERTEX COVER (VC)}, 54, 253
  paddybility, 258
  vertex cover, 54
Vitányi, P., 44, 250
Vollmer, H., 148
Vuillemin, S., 198
Wagner, K., 148
Wang, J., 293
Watanabe, O., 293
weakly paddable set, 275
Wechsung, G., 331
Wegener, I., 250
Wegman, M. N., 406
well-formed formula, 131
Welsh, D. J. A., 199
Wigderson, A., 331, 406
Wilson, C., 80
Winkler, P., 364
winning strategy, 105
witness, 18, 46, 333
Wolfe, D., 118
Wrathall, C., 118
wreath product, 180
Wu, W., 199
Wyllie, J., 250

Yannakakis, M., 80, 118, 456
Yao, A., 199, 250, 331, 365
Young, P., 275, 293

\mathbb{Z}_n^*, 301
Zachos, S., 331, 364
zero-knowledge proof system, 405
  perfect, 405
Zero-One Law, 136
  \{0, 1\}^\omega, 136
Zhou, S., 331
ZPP, 311
Zuckerman, D., 406
Zwick, U., 438, 456